PARRY AFTAB

PORADNIK DLA RODZICÓW I NAUCZYCIELI

INTERNET A DZIECI. UZALEŻNIENIA I INNE NIEBEZPIECZEŃSTWA

Prószyński i S-ka

Nikt nie zrobił więcej niż Parry Aftab,
by Internet stał się bezpieczniejszy dla dzieci.
Robin Raskin, dziennikarka „Family PC"

„Internet a dzieci. Uzależnienia i inne niebezpieczeństwa"
jest czymś w rodzaju mapy, sporządzonej z myślą o rodzicach,
którzy chcą mieć na oku swoje dzieci odbywające podróże
po informatycznej autostradzie.
Barbara Feldman, dziennikarka „Serfing the Net with Kids".

Wspaniały informator dla rodziców. Daje rozeznanie,
jak bezpiecznie korzystać z Internetu. Zdaje sprawę z różnych kontrowersji,
ciągle otaczających Internet. Rozsądne, zdecydowane podejście Aftab
do spraw bezpieczeństwa w Internecie daje rodzicom wiedzę konieczną
do ustalenia własnych zasad i wskazówek dla dzieci.
Ernie Allen,
Prezes Krajowego Centrum Dzieci Zaginionych i Wykorzystywanych

Rodzice, którzy niewiele wiedzą o Internecie, mają w Parry Aftab
sprzymierzeńca. Podobnie jak w swojej pierwszej książce,
Aftab interpretuje – i demistyfikuje – cyberświat.
Wspaniałe w tej książce jest to, że informuje i wzmacnia rodziców,
nie przytłaczając ich. Polecam ją wszystkim gorąco.
Lektura obowiązkowa dla odpowiedzialnych rodziców
wszystkich korzystających z Internetu dzieci.
Len Pagano, Prezes Fundacji Bezpieczna Ameryka

Jako młody ojciec, który dużo czasu spędza w Internecie,
zastanawiam się, jak będzie, gdy moje dzieci dorosną na tyle,
by się tam poruszać. Myślę o tym, jak mogłyby korzystać z jego dobrych stron,
unikając zagrożeń. To pocieszające, że tak uznany autorytet
jak Parry Aftab angażuje się w poszukiwanie rozwiązań w tych sprawach.
Najwyższy czas.
Joshua Blackman, wydawca „The Internet Lawyer"

Nowa książka Parry Aftab zasługuje na platynowy medal za to,
że nie tylko daje rodzicom (także tym, którzy nigdy nie korzystali z Internetu)
narzędzia i wiedzę potrzebną, by dopilnować dzieci serfujące
po cyberprzestrzeni, ale i za to, że jest pełna humoru, mądrych rad
i napisana przystępnym językiem.
Michael J.Madonna, Prezes Stowarzyszenia Policjantów Stanu New Jersey

Jeśli chcecie dowiedzieć się czegoś o dzieciach i o Internecie, osobą,
do której koniecznie powinniście się zwrócić, jest Parry Aftab. Parry wie,
co rodzice chcą i co powinni wiedzieć, i przekazuje im to w tej zabawnej
i łatwej do czytania książce. Jako rodzic jestem wdzięczny za tę książkę.
Dr Stoyan Ganew, Zgromadzenie Ogólne Narodów Zjednoczonych, sesja 87

Parry Aftab to odpowiedzialna internautka, zdecydowana uczynić Internet bezpiecznym miejscem dla dzieci, zachowując zarazem prawo dorosłych do posiadania dorosłych spraw. Zawsze optymistyczna i niezłomna, Parry pisze o trudnych sprawach w zwykłych, łatwych do zrozumienia słowach. Zachęca nas, rodziców, do wzbogacenia życia naszych dzieci poprzez Internet.
Vint Cerf, prezes rady nadzorczej Towarzystwa Internetowego (człowiek, który wynalazł Internet)

Parry Aftab uchwyciła to, co najistotniejsze dla zachowania bezpieczeństwa dzieci serfujących po Internecie. Ma ona rzadką umiejętność przekazywania wiedzy o zagrożeniach i sposobach obrony przed nimi i dodawania otuchy rodzicom. Świadoma wielkiej różnorodności rodzin, zachęca do dokonywania indywidualnych wyborów. Pozostaje nieugięta w przekonaniu, że rodzice muszą pełnić aktywną rolę w działaniach dziecka w Internecie. Całą energię, wrażliwość i wiedzę Parry zaangażowała w poradnik dla każdego, kto ma do czynienia z dziećmi. Powinna to być lektura obowiązkowa dla rodziców, nauczycieli i wszystkich zawodowo zajmujących się młodym pokoleniem.
Michael Berson, University of South Florida

Energia Parry, jej poświęcenie i wspaniałomyślność są prawdziwym natchnieniem dla tych, którzy mieli szczęście się z nią spotkać.
Art Wolinsky

Parry Aftab jest wybitną obywatelką tego kraju – zwalcza przestępczość i broni użytkowników Internetu. To m.in. jej pomysłom Cyberangels zawdzięczają swój sukces. To ona zaszczepiła tę ideę w innych krajach. Każdy zainteresowany tym, by z Internetu uczynić bezpieczne miejsce, powinien przeczytać tę ważną, bardzo konkretną i dowcipnie napisaną książkę.
Curtis Sliwa (założyciel Guardian Angels)

PARRY AFTAB

INTERNET A DZIECI. UZALEŻNIENIA I INNE NIEBEZPIECZEŃSTWA

PRZEŁOŻYŁA BARBARA NICEWICZ

Prószyński i S-ka

Tytuł oryginału
THE PARENT'S GUIDE TO PROTECTING YOUR CHILDREN
IN CYBERSPACE

Copyright © 2000 by Parry Aftab, Esq.
All Rights Reserved

Projekt okładki
Ewa Szydłowska

Zdjęcie na okładce
Mauritius/BE&W

Redaktor prowadzący serię
Grażyna Bruszkiewicz

UNIWERSYTET ZIELONOGÓRSKI BIBLIOTEKA GŁÓWNA
ks2 176807

Redakcja
Aldona Kubikowska

Redaktor techniczny
Małgorzata Kozub

Korekta
Jadwiga Przeczek

Łamanie
Monika Lefler

ISBN 83-7337-241-5

Warszawa 2003

Wydawca
Prószyński i S-ka SA
02-651 Warszawa, ul. Garażowa 7

Druk i oprawa
OPOLGRAF Spółka Akcyjna
45-085 Opole, ul. Niedziałkowskiego 8–12

Moim dzieciom, Michaelowi i Taylor Caprio, które zawsze przekraczały moje najśmielsze nadzieje i marzenia i które nadal zaskakują mnie swoją inteligencją, wrażliwością i pomysłowością... które kochają mnie i wierzą we mnie tak samo, jak ja je kocham i wierzę w nie. One są moim największym dokonaniem!

Pamięci mojego ojca Mansura T. Aftaba, mojego brata Richarda Aftaba i mojego dziadka Raymonda H. Hathawaya. Myślę o nich każdego dnia i chciałabym, by byli tutaj i uczestniczyli w tym wszystkim razem ze mną.

Moim wszystkim Cyberangels i innym wolontariuszom, którzy każdego dnia zabiegają, by żadne dziecko nie zostało w tyle w tej wspaniałej informatycznej podróży i by wszystkie one cieszyły się bezpieczeństwem w Internecie.

Spis treści

Podziękowania

Chciałabym podziękować Lanell Sauer za to, że przez wszystkie te lata była najlepszą przyjaciółką, odbierała telefony o najdziwniejszych porach dnia i nocy, i wierzyła we mnie i moje szalone pomysły, a także za nauki o życiu, lojalności i Bogu.

Wyrazy wdzięczności należą się również Nancy L. Savitt, partnerce w naszej firmie prawniczej i mojej prywatnej redaktorce. Niestrudzenie wyszukiwała strony internetowe, studiowała akty prawne, potrzebne mi do tej książki. Starannie przeglądała wszystkie dygresje i recenzowała materiały, skracała niektóre rozdziały, przenosząc spore ich części do kosza. Gdy prosiłam o pomoc – udzielała jej bez słowa. A co ważniejsze, prowadziła firmę prawniczą pod moją fizyczną i duchową nieobecność w ciągu ostatnich miesięcy. Występowała zamiast mnie w sądach, przygotowywała materiały, z którymi powinnam się zapoznać przed wystąpieniami telewizyjnymi, i usiłowała ułagodzić naszych klientów, gdy ja byłam zajęta pisaniem. Ona we mnie wierzy. Nancy jest jednym z najlepszych prawników, jakich znam, i cudowną przyjaciółką od czasów naszego spotkania na wydziale prawa. Jest jedyną osobą, której mogłam z całym zaufaniem powierzyć zredagowanie tej książki. To niewiarygodne, jak bardzo zyskał mój styl, gdy Nancy go nieco wygładziła. Pamiętam, jak zadzwoniłam do niej z Waszyngtonu, gdzie miałam złożyć wyjaśnienia przed Federalną Komisją Handlu (Federal Trade Comission), po nocy spędzonej nad szlifowaniem rozdziału książki, bliska nerwowego załamania. Całe dnie spędzała w moim domu, wprowadzając kolejne poprawki, taktownie mnie wspierając. Zawdzięczam jej wszystko. Jestem też winna wdzięczność i miłość jej rodzicom za to, co zrobili, żebym czuła się częścią ich rodziny. To najlepsi rodzice na świecie, a Nancy i jej siostra Susan są nadzwyczajnymi szczęściarami!

Chciałabym podziękować mojej matce, Shirley Hammond, i mojej siostrze, Deannie Aftab Guy, za to, że były wspaniałe i zechciały przyjąć moją książkę. Dziękuję też mężowi Deanny, dr. Jeffowi Guyowi, który siedem lat temu podłączył modem do mojego komputera i wprowadził mnie do sieci.

Słowa podzięki kieruję do Kelley Beatty, dyrektorki Cyberangels, która czuwała nad wszystkim, gdy ja pisałam książkę. Kelley jest cudowną, troskliwą kobietą, która poświęca innym wiele swego czasu. Chciałabym też podziękować Laurze, Jean, Trish, Shannon, Mike'owi C., Janice, Cougar, Toby'emu i innym, którzy przyczynili się do tego, że Cyberangels są najniezwyklejszą instytucją na świecie, którzy poświęcali czas – a nie mieli go wiele – by Internet stał się bezpieczniejszy dla innych. Ich oddanie, niewyczerpana energia i nadzwyczajne zdolności stworzyły naprawdę niezwykłe przedsięwzięcie. Jestem zaszczycona, że mogę stać na czele tej grupy. Nauczyli mnie o wiele więcej, niż ja kiedykolwiek będę mogła nauczyć ich.

Curtisowi Sliwie jestem wdzięczna za dalekowzroczność, która pozwoliła mu w 1995 r., zanim ktokolwiek inny się zorientował, jak wiele mogą zrobić w sieci zaangażowani wolontariusze, stworzyć Cyberangels. Mary Galdzie dziękuję za przydanie wdzięku naszej pracy.

Chcę też podziękować moim pierwszym Cyberangels (Cybernetycznym Aniołom Stróżom): Brittany, Kathy, Jennifer, Stephanie i Susan, a także Alyssie, Lauren i Maggie, moim małym początkującym Teenangels, za napisanie wskazówek dzieci w sprawach bezpieczeństwa w sieci i za podzielenie się ze mną przemyśleniami.

Dziękuję memu pomocnikowi, Sagarowi S. Mungekarowi. Sagar wygłaszał w imieniu swojej klasy mowę pożegnalną po maturze. Teraz jest gwiazdą Cornell University. Przez kilka lat pracował z nami podczas wakacji, pomagał nam zbudować naszą stronę WWW i zrozumieć tajniki nowej technologii. Był moim przewodnikiem po zakamarkach Internetu, do których nie dotarłam, pisząc moją pierwszą książkę. Tym razem Sagar czuwał, by wszystkie wykresy zostały zrobione dobrze i wykonał niezliczoną ilość telefonów, pomagając mi uzyskać niezbędne informacje. Wiem, że to on któregoś dnia wynajdzie lekarstwo na raka, ale chciałabym, by został z nami trochę dłużej.

Chciałabym podziękować mężczyźnie, którego kocham. On wie, kogo mam na myśli.

Chciałabym podziękować rodzinom i wszystkim przyjaciołom, którzy pomogli mi, dzieląc się swoimi doświadczeniami. I znajomym, spotkanym w Internecie, którzy pomogli mi przejść przez to wszystko. Na moją wdzięczność zasługują zwłaszcza Robin Raskin, redaktorka Susan Barry, Art Wolinsky, Della Curtis i Sherry Glover, za cierpliwość, wsparcie, pomoc. (Myślę, że na miejscu byłby tu cytat ze „Świata Wayne'a": „Nie zasłużyłam... Nie zasłużyłam...").

Dziękuję Audrey Smith, wydawcy mojej poprzedniej książki, wieloletniej przyjaciółce i powierniczce; bez jej talentów moja pierwsza książka, a zatem i obecna, nie ujrzałyby światła dziennego.

Dziękuję moim przyjaciołom z organów ścigania, szczególnie z FBI, Federalnego Urzędu Celnego, Policji Stanu New Jersey, Królewskiej Policji Kanadyjskiej, Metropolitan Police i Interpolu, którzy codziennie ryzykują życiem, by zapewnić bezpieczeństwo naszym rodzinom.

Chciałabym również podziękować administratorce naszej firmy prawniczej, Patricii Peters, która była też moją pierwszą czytelniczką recenzentką, odpowiedzialną za to, by temat został wyczerpująco omówiony bez zanudzenia czytelnika. (Jeśli jesteście znudzeni, miejcie pretensje do Patricii, nie do mnie). Po wielu godzinach pracy w biurze brała do domu kolejne rozdziały książki, czytała, co napisałam, a potem stawała przed niewdzięcznym zadaniem powiedzenia mi, jakie poprawki powinnam wnieść. (W końcu to ja podpisuję listę płac).

Chciałabym podziękować Eileen Scanlon, przyjaciółce i asystentce w biurze prawniczym, za zachowanie ładu w moim życiu w czasie tego zamętu i za przeczytanie wszystkich nadesłanych ankiet. Oraz Fay, twórczyni mojej strony internetowej i przewodniczce, najgłębsze podziękowania za odkrywcze pomysły i wspaniałomyślność.

I wszystkim ludziom, którzy poprzez proste gesty troski i wsparcia tak dużo wnieśli.

I dziękuję Bogu, bez którego to wszystko nie miałoby znaczenia.

ZIELONOGÓRSKI

Przedmowa

Zostałam zmuszona, choć wierzgałam i skamlałam, do roli obrońcy dzieci w cyberprzestrzeni. Byłam sobie prawnikiem internetowym, robiłam swoje, gdy zostałam powołana. Wtedy byłam dumna z faktu, że jestem prawnikiem, specjalistką e-handlu, i że nie zajmuję się branżą „dziecinną". A teraz zajmuję się wyłącznie tym. Kiedy przeznaczenie cię wzywa... musisz słuchać.

Moje zaangażowanie w sprawy bezpieczeństwa w Internecie zaczęło się kilka lat temu, kiedy telewizja CNN zaprosiła mnie do dyskusji na temat swobody wypowiedzi w sieci, uchwały o etyce w mediach (Comunication Decency Act) i oprogramowania filtrującego. Choć bez trudu mogłam wypowiadać się na tematy prawne (prowadziłam w America Online – AOL – prawne dyskusje i stworzyłam Telewizyjne Centrum Pomocy Prawnej), nie wiedziałam nic o oprogramowaniu filtrującym. Moje dzieci były starsze, a ja byłam prawnikiem firm internetowych. Znałam się na problemach bezpieczeństwa korporacji, nie dzieci. Ale gdy dzwoni CNN, uczysz się wszystkiego, o czym chcą, żebyś mówiła... i to w przyspieszonym tempie!

Po programie (byłam tam okropnie nudna, ale miałam świetną fryzurę!) rozdzwoniły się telefony, zaczęłam dostawać e-maile, faksy, listy. Rodzice i nauczyciele pytali, jak mają zapewnić dzieciom bezpieczeństwo w korzystaniu z sieci. Wyjaśniałam, że nie zajmuję się „dziecięcą" dziedziną. Że jestem prawnikiem od handlu internetowego. Ale zalew nie ustawał, choć głośno protestowałam.

Zadzwoniłam do mojej siostry, która jest pediatrą, czyli z definicji zajmuje się tylko dziećmi. Chciałam, żeby wskazała mi książkę dotyczącą bezpieczeństwa dzieci korzystających z Internetu, bym mogła ją polecić tym rodzicom, którzy chcieli się czegoś dowiedzieć. Po długich poszukiwaniach powiedziała mi, że nie ma takiej książki, i zasugerowała, żebym sama ją napisała. 1 maja w Moskwie, siedząc w pokoju hotelowym nad miską barszczu, z nowym laptopem, zaczęłam moją pierwszą książkę – „A Parent's Guide to the Internet" („Przewodnik po Internecie dla rodziców"). Odwiedzałam szkoły i mówiłam rodzicom o sprawach bezpieczeństwa dzieci w sieci. Zostałam zaproszona przez Microsoft i Net Nanny do Seattle, gdzie również wypowiadałam się o problemach bezpieczeństwa. Przeprowadziłam nawet pogawędkę z jednym z disneyowskich bohaterów, ucząc go (i wszystkie słuchające dzieci), jak unikać kłopotów. Moja praktyka prawnicza na tym cierpiała, ale z drugiej strony robiłam to, co chciałam robić – zabiegałam, by wszystkie dzieci, nawet te, które nie mogły sobie pozwolić na komputer w domu, umiały bezpiecznie korzystać z Internetu. Chciałam także mieć pewność, że nauczyciele i bibliotekarze uzyskają pomoc i wsparcie, jakie jest im potrzebne. A przede wszystkim pragnęłam nauczyć wszystkich rodziców, jak ich dzieci mogą bezpiecznie serfować po Internecie, znajdując pożyteczne rzeczy i unikając złych. Jeździłam po całym kraju, przemawiałam na różnych spotkaniach poświęconych bezpiecznemu serfowaniu. Byłam w Białym Domu na konferencji dotyczącej problemów bezpieczeństwa dzieci korzystających z Internetu. Odwiedzałam szkoły i społeczności lokalne. W połowie 1998 roku Curtis Sliwa, organizator Guardian Angels (sławne patrole w czerwonych beretach, które pojawiły się w metrze i na ulicach), poprosił mnie o pomoc. Trzy lata wcześniej, w odpowiedzi na wątpliwości co do bezpieczeństwa w sieci, stworzył Cyberangels, czyli odpowiednik Guardian Angels w cyberprzestrzeni. Chciał, bym poprowadziła to przedsięwzięcie. Zgodziłam się to robić przez kilka tygodni, dopóki nie znajdzie kogoś innego. Ale gdy ktoś podesłał mi informacje o stronie internetowej z pornografią dziecięcą, całe moje życie się zmieniło. Zobaczyłam małą dziewczynkę, która była krzywdzona, i nie mogłam przejść obojętnie wobec tej sprawy. Zgodziłam się prowadzić Cyberangels, organizację złożoną wyłącznie z wolontariuszy.

Od tego czasu Cyberangels zostali w 1998 roku uhonorowani nagrodą President's Service Award i rozszerzyli zasięg swojej działalności. Nie tylko udzielają cybersąsiedzkiej pomocy w sprawach poważnych przestępstw, takich jak dziecięca pornografia, cybernapastowanie i seksualne wykorzystywanie dzieci w Internecie, ale stali się również głównym ośrodkiem edukacyjnym w sprawach bezpieczeństwa, udzielają pomocy, dysponują ponad tysiącem aktywnych

wolontariuszy. Nasze programy dotyczą edukacji w sprawach bezpieczeństwa w sieci i są skierowane do dzieci, rodziców i nauczycieli. Prezentujemy przyjazne rodzinie strony WWW oraz programy i serwisy zapewniające filtrowanie. Dzieciom umożliwiamy udział w testach i uzyskanie świadectwa umiejętności bezpiecznego serfowania.

W roku 1999, gdy UNESCO przystąpiło do realizacji programu walki z pornografią dziecięcą i pedofilią w Internecie (nazwanego Innocence in Danger – Niewinność w niebezpieczeństwie), zostałam poproszona przez szefa światowego programu, Homayra Selliera (międzynarodowy obrońca praw dziecka) i generalnego dyrektora UNESCO o pokierowanie amerykańską częścią programu (nazywa się Innocence in Danger – U.S.). Program będzie służył jednoczeniu wysiłków różnych grup zwalczających seksualne wykorzystywanie dzieci korzystających z Internetu, koordynowaniu działań agend zmierzających do zmiany prawa i edukowania rodziców w tych sprawach. To pierwsza naprawdę ogólnoświatowa inicjatywa zmierzająca do okiełznania niebezpieczeństw Internetu.

Amerykańska część programu „Niewinność w niebezpieczeństwie" stanie się elementem szerszej akcji, którą prowadzę, nazwanej WiredKids. Jej celem jest zapewnienie dostępu do Internetu wszystkim dzieciom (żadne nie powinno zostać w tyle tej rewolucji technologicznej), przekonanie nauczycieli, że Internet jest bezpiecznym narzędziem edukacyjnym i że jego potęga może być wykorzystana do dostarczania informacji i pomocy dzieciom i rodzinom. Ważną częścią tej misji jest szkolenie rodziców, by byli w stanie uczyć dzieci bezpiecznego poruszania się po tym niezwykłym skarbcu.

O tym wszystkim jest ta książka. Pamiętaj, choć musimy wiedzieć, gdzie tkwią niebezpieczeństwa i jak ich unikać, że największym zagrożeniem dla naszych dzieci w związku z Internetem jest uniemożliwienie im dostępu do tego podstawowego narzędzia.

Rozdział 1

Krótkie wprowadzenie w problematykę

Dzieci w Internecie

Internet jest niezwykłym miejscem. Pozwala jednocześnie porozumiewać się, uczyć i bawić. Ponad 50% dzieci w USA korzysta z Internetu w szkole, w domu lub w miejscach publicznych. Od 1996 roku liczba dzieci mających dostęp do Internetu wzrosła z 4 do 19 milionów (mniej więcej tyle samo chłopców co dziewcząt). Odsetek szkół mających dostęp do Internetu wzrósł z 34 w 1994 roku do ponad 89 w 1998 roku Jeśli to tempo się utrzyma, za kilka lat każdy mężczyzna, kobieta, dziecko i pies będą mieli dostęp do Internetu.

Wielu rodziców jednak nadal pełnych jest nieufności. Czytali o niebezpieczeństwach Internetu, oglądali reportaże telewizyjne i specjalne programy o ciemniejszej jego stronie. Są przekonani, że istnieje tylko jedno wyjście: należy trzymać dzieci z dala od Internetu.

Jaka szkoda! Jest tyle sposobów, żeby uchronić dziecko przed ciemnymi stronami Internetu, nie pozbawiając go dostępu do sieci. Nie wylewajmy dziecka z kąpielą! Nasze dzieci nie mogą być internetowymi analfabetami, jeśli mają otrzymać pracę, kończyć szkoły czy wstępować na uniwersytet. Odmawiając im dostępu do sieci, ograniczamy ich szanse na sukces.

Internet przestał być sprawą wyboru, stał się koniecznością, jeśli myślimy serio o przyszłości naszych dzieci. To także jeden z powodów, dla których musimy dbać, by *wszystkie* dzieci, niezależnie od ich zamożności, rasy, pochodzenia etnicznego czy języka, którym mówią rodzice, mogły korzystać z nowej technologii.

Zamiast się niepotrzebnie zamartwiać, musimy coś z tym zrobić. Musimy stać się cyberbywalcami, żeby poprowadzić nasze dzieci w sieci z taką samą pewnością, z jaką prowadzimy je przez życie w realnym świecie. To nie znaczy, że mamy stać się technologicznymi ekspertami. Oznacza to tylko, że musimy rozumieć, jakie niebezpieczeństwa grożą dziecku i jak sobie z nimi radzić – w naszym własnym stylu.

Nie masz pojęcia? Zaraz poczujesz się jak w domu!

Nie pozwólcie, by strach przed techniką czy komputerami paraliżował was – to wszystko jest naprawdę prostsze, niż myślicie.

Przede wszystkim pamiętajcie, że nie jesteście sami. Większość z nas śmiertelnie się boi – tylko po prostu tego nie okazujemy. Komputery mogą onieśmielić każdego. A ludzie, którzy się na nich znają, mówią żargonem, którego nikt z nas nie rozumie (ani nie chce rozumieć).

Nasze pecety rzadko robią to, co byśmy chcieli, a metoda skuteczna wobec większości wyrafinowanych urządzeń domowych (porządny, zamaszysty kopniak) na ogół się nie sprawdza. (Choć, wierzcie mi, próbowałam).

Wielu rodziców sądzi, że potrzeba specjalistycznej wiedzy, by korzystać z sieci. To nieprawda.

Większość z nas jest w stanie użytkować wideo, choć tylko nieliczni rozumieją, jak to działa. Jeśli potrafimy włożyć kasetę wideo, nacisnąć przyciski „zasilanie" i „start", możemy oglądać film. (A tym, których złości migające na wyświetlaczu 12:00, proponuję rozwiązanie technicznie mało wyrafinowane: czarna taśma izolacyjna nalepiona na okienko wyświetlacza).

Użytkowanie komputerów nie jest niczym innym. Jeśli potraficie to włączyć, kliknijcie dwa razy myszką, wprowadźcie swoje imię i hasło, i już jesteście w sieci!

I tak trudno być rodzicem!

Ciągle słyszę lament (no, może raczej kwilenie niż lament): „Czy wychowywanie dzieci nie jest wystarczająco trudne, nawet gdy nie musimy kierować nimi w cyberprzestrzeni i zamartwiać się o ich bezpieczeństwo w Internecie? Jak możemy ostrzec je przed niebezpieczeństwami, jeśli sami nie wiemy, skąd zagrażają? Jak możemy pomóc dzieciom, odpowiedzieć na ich pytania, jeśli nie umiemy nawet włączyć komputera? Jak można się spodziewać, że zostaniemy komputerowymi geniuszami, jeśli nie umiemy zaprogramować naszego magnetowidu?". (Prawda, że to przerabialiście?).

Zgadzam się, że kiedy wasz ośmiolatek wie więcej niż wy o komputerach – trudno jest utrzymać kontrolę. (I nie sądźcie, że oni o tym nie wiedzą). Ale z niewielką pomocą nauczycie się wszystkiego, co wam potrzebne, by ochronić dzieci przed problemami i zyskać pewność, że odnoszą wiele korzyści z buszowania w sieci. (A dodatkowo serfowanie może się wam tak spodobać, że sami zechcecie nauczyć się korzystania z Internetu).

W tej książce znajdziecie wszystko, co, jak sądzę, musicie wiedzieć. A jeśli macie pytania, na które nie odpowiedziałam, wyślijcie mi e-mail na adres parry@aftab.com albo odwiedźcie stronę: www.familyguidebook.com. Jest tam sekcja, którą stworzyłam specjalnie dla czytelników tej książki. Nazywa się ona: Dla czytelników „Internet a dzieci. Uzależnienia i inne niebezpieczeństwa" (świetne, nie?), a hasło brzmi: „empowered".

Wszyscy mamy ten sam problem! Napisałam tę książkę, by dodać pewności siebie każdemu rodzicowi! Więc czemu wyglądacie na zmartwionych?

Powtarzaj za mną: „Nadal jestem rodzicem!"

Kiedy mówię do rodziców o problemach bezpieczeństwa w Internecie, przynajmniej jedna osoba z grupy zawsze wygłasza takie zdanie: „Ja się nie boję. Ufam moim dzieciom". (Wtedy zazwyczaj można też usłyszeć, jak zaczynam głośno ziewać).

Zaufanie do dziecka to wspaniała rzecz. Ale to jest bez znaczenia, gdy mówimy o bezpieczeństwie w sieci, bo tymi, którym tak naprawdę powinieneś móc ufać, są wszyscy inni użytkownicy Internetu. Jednakże nie możemy liczyć na to, że oni będą się troszczyli o bezpieczeństwo naszych dzieci. To nasze zadanie.

Choć wielu z nas może ufać dzieciom, że nie będą wchodziły na nieodpowiednie strony (jakkolwiek *twoja* rodzina definiuje *nieodpowied-*

nie), problem jest bardziej złożony. Wiele godnych zaufania dzieci wpada w kłopoty, spotykając się z obcymi ludźmi twarzą w twarz poza siecią, bo nie powiedzieliśmy im, że to może być niebezpieczne. Ponadto niewinne serfowanie może narazić nasze pociechy na niepożądane niespodzianki. Nazwy stron dla dorosłych bywają łudząco podobne do nazw popularnych witryn dla dzieci, pisanych z często spotykanymi błędami. Wystarczy zwykła literówka – taka, jaka nam samym często się przytrafia i jaka każdego dnia może przydarzyć się naszemu dziecku.

Rodzice muszą pamiętać, że niezależnie od tego, czy rozumiemy, jak funkcjonuje Internet, czy nie, a także wtedy, gdy nie umiemy nawet włączyć komputera – *nadal* jesteśmy rodzicami. *Nadal* jesteśmy odpowiedzialni. *Nadal* mamy lepszy osąd. Nie możemy zamknąć sprawy, mówiąc, że „mamy zaufanie" do naszych dzieci. Musimy mieć pewność, że nauczyliśmy je, jak zasługiwać na zaufanie i jak unikać zagrożeń stwarzanych przez innych.

Jako rodzice uczymy dzieci odpowiedzialnie podejmować decyzje. Musimy pamiętać, że ich umiejętności w zakresie posługiwania się nową technologią znacznie wyprzedzają ich zdolność oceny, osądu. To nasz rodzicielski obowiązek wypełnić tę lukę *naszym* lepszym osądem i większym doświadczeniem. (Nikt nigdy nie obiecywał nam, że bycie rodzicem będzie łatwe).

Jednym słowem: to nie wobec własnych dzieci mamy być nieufni, ale wobec milionów innych użytkowników sieci. Musimy wyposażyć nasze dzieci w umiejętności potrzebne do tego, by były bezpieczne w wirtualnym otoczeniu, a przy tym ciągle czerpały przyjemność z obcowania z nim.

Pamiętaj: Ty jesteś rodzicem. Internet tego nie zmienił.

Nie tracąc z oczu zagrożeń

Mimo że bardzo bym chciała, nie mogę napisać tej książki, nie koncentrując się na niebezpieczeństwach w cyberprzestrzeni. Nie sposób ich unikać, gdy się nie wie, na czym polegają. Nie chcę nikogo odstraszyć od Internetu, ale chcę nauczyć rodziców, jak mogą pomóc dzieciom bezpiecznie poruszać się po cyberprzestrzeni.

Choć nie można zaprzeczyć, że istnieją w Internecie zagrażające rzeczy, to ich liczba jest mocno przeceniana. Po prostu one bardziej przyciągają uwagę.

Zawsze gdy rozmawiam z dziennikarzami lub uczestniczę w przesłuchaniach przed rządowymi komisjami, jestem proszona o „obiektywne przedstawienie sprawy". Każdy chce wiedzieć, jak istotny jest problem. Zawsze posługuję się relacją 90:10 (ale trzeba wiedzieć, że sama to wymyśliłam). Zawsze mówię, że 90% zawartości Internetu to rzeczy wspaniałe, edukacyjne, twórcze i bezpieczne. O pozostałych 10% nie można tego powiedzieć. Ale to te 10% przyciąga więcej uwagi i jest częściej odwiedzane niż cała reszta.

❖ Jak poważny jest problem?

Każdy chciałby wiedzieć, ilu napastników jest w Internecie i jakie jest prawdopodobieństwo, że nasze dzieci staną się ofiarami. Ludzie, którzy nie korzystają z Internetu, przeceniają problem, a wielu doświadczonych użytkowników sieci nie docenia go. Choć mamy trochę danych o aktualnych dochodzeniach i aresztowaniach, nie są one dokładną miarą rzeczywistej skali problemu. Choć próbujemy zdobyć dane do liczbowego ujęcia sprawy, nie udaje się nam tego dokonać, bo zaledwie część incydentów z cyberprześladowcami jest zgłaszana.

Opierając się na rozmowach ze stróżami internetowego prawa, tak przedstawiłabym to, co wiemy: do CyberLinii Krajowego Centrum Dzieci Zaginionych i Wykorzystywanych (National Center for Missing and Exploited Children CyberTipline), działającej od 1998 roku, w pierwszym roku jej istnienia zgłoszono ponad 7500 skarg dotyczących seksualnego wykorzystywania dzieci i Internetu. Większość zgłoszeń (około 5700) dotyczyła pornografii dziecięcej, a około 1000 – namawiania dzieci przez dorosłych za pomocą Internetu do seksualnych działań w realnym życiu.

Ale Krajowe Centrum, największa z linii zgłoszeniowych, nie jest jedyną. FBI ma własną linię, podobnie Wydział Cyberprzemytu Amerykańskiego Urzędu Celnego. Tylko ten ostatni otrzymuje dziennie około 50 informacji o dziecięcej pornografii w Internecie. Urząd Celny w 1998 roku donosił o aresztowaniu 230 osób szerzących pornografię dziecięcą, a w ciągu kwartału otrzymuje z Krajowego Centrum około 2000 informacji o pornografii dziecięcej. (Szczegółowo omawiam to w rozdziale 5).

Wiele lokalnych grup samopomocy także ma własne linie. W Cyberangels otrzymujemy wiele doniesień dotyczących Internetu i sek-

sualnego wykorzystywania dzieci. Na ogół chodzi o strony z pornografią dziecięcą. Prawdopodobnie jeden przypadek na tydzień dotyczy oskarżeń o uwodzenie w Internecie, a jeszcze mniej dotyczy dzieci, które spotkały się z pedofilem i wróciły do domu lub zaginęły oraz takich, które wysłały własne zdjęcia o jawnie seksualnym charakterze pedofilowi jako wstęp do spotkania twarzą w twarz. Cyberangels przekazują takie sprawy policji. Kilkanaście doniesień o uwodzeniu dzieci zakończyło się aresztowaniem cyberprzestępców.

Tysiące zatrudnionych w terenowych komendach policjantów podejmuje w akademiach policyjnych lub w prywatnych grupach szkolenie w zakresie prowadzenia śledztw internetowych.

Z danych pochodzących od policji i prokuratury wynika, że w 1998 roku w USA spraw, w których ktoś został aresztowany za uwodzenie dzieci poprzez Internet, było mniej niż 500. (Chociaż FBI otworzyło 700 nowych spraw w okresie od stycznia do lipca 1999, prawie dwa razy więcej niż w tym samym okresie roku poprzedniego).

Ucieszycie się, słysząc, że prawie wszystkie aresztowania zakończyły się osadzeniem w więzieniu. Prokuratorzy FBI i Urzędu Celnego mają w tym zakresie prawie 99% sukcesów!

Jeśli jednak coś złego stanie się twojemu dziecku, statystyki nie mają znaczenia. Nawet jeśli zdarzyłoby się to tylko jednemu dziecku na świecie, gdyby było to *twoje* dziecko, to zdarzyłoby się jednemu dziecku za dużo.

Nie obwiniajcie Internetu

Nawet jeśli coś złego się zdarzy, nie jest to wina Internetu. Zawinił określony człowiek, który go nadużywa. Ale to właśnie Internet jest obwiniany o całe zło w sieci.

Kiedy tylko pojawi się bulwersująca wiadomość, która w jakiś sposób wiąże się z Internetem, programy telewizyjne zapełniają się ludźmi, którzy wyklinają sieć. (Wiem, bo zazwyczaj jestem jedną z osób zapraszanych do studia, by zaproponowały jakieś rozwiązania). Zrozumiałe więc, że rodzice są przestraszeni i wielu z nich wykrzykuje, że dzieci nie powinny być w ogóle dopuszczane do Internetu.

Ale to dopiero byłaby prawdziwa tragedia! To tak jakby nigdy nie zabrać dziecka na przedstawienie na Broadway, do Empire State Building, Statui Wolności czy Muzeum Historii Naturalnej, dlatego że niektóre rejony Nowego Jorku są bardziej niebezpieczne niż inne.

Fakt, że istnieją „gorsze" dzielnice, nie może trzymać nas z dala od miasta w ogóle.

❖ Internet jest chętnie oskarżanym „przestępcą"

Kobieta (i cyberosobistość), którą podziwiam, Robin Raskin, wydawca magazynu „Family PC", znana jako „Internetowa Mama", wkrótce po masowym samobójstwie członków sekty Heaven's Gate napisała artykuł zatytułowany: „Oskarżanie Internetu. Rodzice rozpaczają: Dlaczego musiał pojawić się Internet?". Po latach mam ciągle w pamięci jej artykuł i chciałabym przedstawić jego część.

„Kiedy usłyszałam, że sekta Heaven's Gate używała Internetu, by propagować swoje dogmaty i rekrutować członków, było to dla mnie tak przykre, jakby używali domu w moim sąsiedztwie. W końcu zachęcałam rodziny do korzystania z Internetu i wiem, że teraz w znacznym stopniu będzie obwiniany o tragedię. Zastanawiam się: dlaczego oskarżamy Internet? Gdyby sekta używała późnych reklam w telewizji do rekrutacji nowych członków, nikt z tego powodu nie kwestionowałby wartości telewizji".

Zgadzam się. Przypisywanie winy Internetowi stało się reakcją automatyczną.

❖ Teraz wszystko ma jakiś związek z Internetem

Wszyscy kulimy się, kiedy w wiadomościach na pierwszy plan wysuwa się jakaś tragedia – po prostu czekamy, kiedy zaczną się sypać kamienie na Internet. W miarę jak coraz więcej ludzi z niego korzysta, okazuje się, że zawsze można znaleźć jakieś powiązanie z Internetem. Albo przestępca miał stronę internetową, albo ofiara ją miała, albo ktoś otrzymał e-mail. Zawsze jest jakiś związek.

Jeden z moich przyjaciół często mówi, że to niesprawiedliwe. W komentarzach do historii o porwaniach nie wskazuje się na zagrożenia związane z telefonem na tej podstawie, że porywacz przekazywał swoje żądania za pośrednictwem telefonu. Sądzę, że jest tak dlatego, iż wszyscy wiemy, jak działa telefon. (Uczymy dzieci, by nie rozmawiały przez telefon z nieznajomymi i by nigdy nie mówiły, że są w domu same, nieprawdaż?). Internet to inna sprawa; niewielu

z nas wie, jak go używać – dlatego budzi tyle lęku. Boimy się tego, czego nie rozumiemy.

Na domiar złego trzeba uczciwie przyznać, że Internet rzadko rozczarowuje poszukiwaczy skandalu i sensacji. Naśladowcy przestępców pojawiają się w sieci prawie natychmiast. Ogłaszają oni, że są współwinni, a dostawcy usług internetowych tropią fałszywe ślady i wpadają w ślepe zaułki. A wszystko to stanowi pożywkę dla ludzkich emocji.

Nie powinniśmy jednak oskarżać Internetu. Powinniśmy oskarżać ludzi, którzy go źle wykorzystują.

Przewodnik po tej książce

Rozmawiałam z rodzicami na całym świecie na temat bezpieczeństwa w sieci. Dzięki temu zorientowałam się, że są pewne rzeczy, które większość rodziców wie o Internecie (niezależnie od tego, czy go używają, czy nie) i wiele, wiele nieporozumień. (Im częściej ludzie korzystają z Internetu, tym więcej dowiadują się o rzeczywistych zagrożeniach z nim związanych. Ale nawet doświadczeni użytkownicy nie zawsze są w stanie zlokalizować wszystkie zagrożenia dla dzieci i nie wiedzą, jak im zapobiec).

Porównuję różne dostępne w Internecie zajęcia i obszary do świateł ulicznych: czerwone światło – stop, nie chodź, chyba że jesteś przygotowany na to, co tam znajdziesz, i dostatecznie dorosły na podjęcie takiej decyzji; zielone światło – odpowiednie dla wszystkich, niezależnie od wieku; i żółte światło – dotyczy znacznej większości zawartości Internetu: można iść, ale z zachowaniem ostrożności.

Niestety, odkryłam, że wielu rodziców mówi dzieciom, że wszędzie jest zielone światło, nie przygotowując ich na nieuniknione kolizje, wtedy gdy inni nie stosują się do tych samych zasad ruchu. Inni rodzice, oczekujący biernie na pojawienie się jakiegoś cudownego puklerza, gwarantującego bezpieczeństwo, widzą wszystko jako „czerwone światło" i trzymają swoje dzieci z dala od Internetu w ogóle.

Chciałabym, by rodzice uświadomili sobie, że większość treści i ofert Internetu mieści się w kategorii „żółte światło", co oznacza, że musimy starać się myśleć krytycznie, decydując, czy im uwierzyć; że musimy starannie chronić swoją prywatność i unikać zarówno nieetycznych chwytów reklamowych, jak i sytuacji, które mogą doprowadzić dzieci do kontaktu z ludźmi mającymi złe intencje. I podobnej ostrożności musimy nauczyć dzieci. Powinny wiedzieć, że na tej informatycznej autostradzie trzeba uważnie popatrzeć najpierw w jedną, potem w drugą stronę.

W tej książce wyjaśniam, gdzie znajdują się ukryte niebezpieczeństwa. Wspaniałe rzeczy, które możemy robić dzięki Internetowi, są często używane niewłaściwie, co czyni z nich „działania przy żółtym świetle". Pewne miejsca w sieci są bardziej niebezpieczne niż inne – tam nasze dzieci muszą poruszać się ze zdwojoną ostrożnością, gdy są już dość dorosłe, by poradzić sobie ze sobą i z tym, co mogą tam znaleźć.

Oto jak uporządkowałam tę książkę: działanie, jak powinno być używane, jak może być nadużywane i jak można się przed nadużywaniem bronić. Najryzykowniejsze obszary, jak je zlokalizować, jak trzymać się od nich z daleka. Jak edukować dzieci, jak decydować, co wolno im robić w sieci, jak wprowadzić te decyzje w życie i wymusić ich przestrzeganie. Omawiam nawet stosowanie Internetu w szkołach i w jaki sposób sami możemy włączyć się w akcję poprawiania bezpieczeństwa.

Książka składa się z 9 rozdziałów:

- Rozdział 1 „Krótkie wprowadzenie w problematykę" zawiera podstawowe informacje, co dzieci mogą robić w sieci, jak nie przeoczyć zagrożeń, a najważniejsze – co zrobić, by nie wpaść w panikę.
- Rozdział 2 „Dobro, zło i zachowanie ostrożności" mówi, jak działa Internet i co może się stać niedobrego. Nawet najbardziej doświadczeni użytkownicy Internetu mogą nie wiedzieć, że niektóre możliwości w sieci mogą być nadużywane. W tym rozdziale pokazuję rodzicom, w jaki sposób niewinne serfowanie może zaprowadzić w ciemniejsze rejony, i mówię im, co mogą w tej sytuacji zrobić.
- Rozdział 3 „Ciemna strona Internetu" opisuje zagrożenia dla twojego dziecka, omawia treści, które możesz uznać za niestosowne dla dzieci, oraz poważniejsze niebezpieczeństwa, takie jak cybernękanie i napastowanie. W tym rozdziale jest też część poświęcona zagrożeniom dla komputera ze strony wirusów i hakerów oraz zagrożeniom dla ciebie i innych, stwarzanym przez twoje dzieci i ich kolegów.

- Rozdział 4 „A teraz naprawdę poważne sprawy" mówi o zagrożeniach związanych z dokonywaniem zakupów w Internecie, wydostawaniem danych osobowych od dzieci i problemach ochrony prywatności. Dostarcza także szczegółowych wskazówek, jak radzić sobie z cyberprześladowaniem, zawiera prawdziwe opisy działań napastników wabiących dzieci w pułapkę.
- Rozdział 5 „A teraz o tym, co naprawdę nudne: prawo" dotyczy funkcjonowania prawa w Internecie, mówi, kto je wdraża, gdzie zgłaszać przypadki przestępstw i uzyskać pomoc. Pokazuje także, jak każdy z nas może coś zmienić, zgłaszając się jako wolontariusz, by pomóc innym w sieci, w swojej społeczności lokalnej czy szkole.
- Rozdział 6 „Internet w szkołach" wyjaśnia, w jaki sposób problemy bezpieczeństwa w Internecie dotyczą szkół. Przedstawia także wyniki badań, które pokazują, że wprowadzenie Internetu do klasy ułatwia dzieciom uczenie się.
- Rozdział 7 „Ucz swoje dzieci dobrze" sugeruje, jak rozmawiać o tych sprawach z dziećmi i jak je uczyć unikania niebezpieczeństw, podaje proste wskazówki, z których możesz skorzystać, by pomóc dzieciom bezpiecznie poruszać się po Internecie. Wyjaśnia także zasady cyberetykiety i prezentuje „Zasady dobrego zachowania w Internecie według pani Parry".
- Rozdział 8 „Dokonywanie wyborów i ich realizacja" mówi o tym, co masz do wyboru, co robią inni rodzice, podaje adresy kilku cudownych, bezpiecznych serwisów dla dzieci. Opisuje także dostępne narzędzia, takie jak programy blokujące i filtrujące, i porównuje dokładnie najpopularniejsze z nich. Testowaliśmy je i wiemy, które najlepiej się sprawdzają.
- Rozdział 9 „A teraz słowo od prawdziwych ekspertów – dzieci i nastolatków" jest w dużej części napisany przez dzieci i nastolatki. Zawiera rezultaty badań prowadzonych w grupie nastoletnich dziewcząt, przemyślenia uczniów ze śródmiejskiej szkoły i wskazówki dotyczące bezpieczeństwa w Internecie, napisane przez naszych małych i nastoletnich Cyberangels (grupę nastolatków, którzy zostali przeszkoleni w sprawach bezpieczeństwa internetowego i działają jako ambasadorowie idei bezpieczeństwa wśród uczniów na całym świecie).

Można czytać tę książkę na kilka sposobów. Najlepsza metoda to zaczynanie od początku, z poświęceniem szczególnej uwagi dedykacjom i podziękowaniom, a następnie czytanie po kolei, bez odkładania, aż do samego końca. (Chciałabym znaleźć choć jedną osobę, która tak postąpi!).

Można także zaczynać od końca, ale ponieważ nie jest to opowieść kryminalna, niewiele przyjdzie ci z tego, że dowiesz się, jak się kończy. Albo możesz czytać to, co cię interesuje w dowolnym porządku. Rozdziały i sekcje są od siebie niezależne.

Rozdziały, które mogą niektórych z was uśpić, zostały włączone jako materiał dodatkowy dla tych, którzy muszą znać wszystkie szczegóły. Możesz je więc opuścić i dalej rozumieć temat. Jeśli jesteś ciekaw spraw technicznych, zawarłam obszerne informacje pod adresem www.cyberangels.org i www.familyguidebook.com. Reszta zależy od ciebie.

O jakie sprawy związane z bezpieczeństwem w Internecie rodzice pytają najczęściej

Rodzice zadają pytania, mnóstwo pytań. Na szczęście w większości przypadków znamy odpowiedzi. Zanim przejdziemy do miłej pogawędki, odpowiem na najczęściej pojawiające się pytania.

Wszystko, co mi się obija o uszy, dotyczy śmieci, przemocy, pornografii. Czemu w ogóle mam zawracać sobie głowę zakładaniem dostępu do Internetu dla moich dzieci?

Musisz zawracać sobie głowę. Internet to największa dostępna ludzkości biblioteka. W sieci na jej różnych poziomach istnieje ponad bilion stron. Dzisiaj do wykonywania większości kwalifikowanych prac niezbędna jest znajomość komputera i Internetu, a wtedy, gdy twoje dzieci będą szukały pracy – pewnie będzie ona wymagana na każdym stanowisku. Nasze dzieci potrzebują tych umiejętności dla swojej przyszłej kariery.

Internet to wielka pomoc przy odrabianiu lekcji i wykonywaniu zadań szkolnych. To także wspaniały sposób poznawania ludzi z in-

nych stron świata, z innych kultur. To najtańszy bilet w podróż dookoła świata.

To także cudowne miejsce, gdzie twoje dzieci mogą dzielić się swoimi pomysłami z innymi. Mogą pisać, opowiadać o różnych rzeczach, mogą rysować i prezentować swoje dzieła i muzykę milionom ludzi na świecie. To największa scena świata. To przestało być sprawą wyboru. Internet stał się *koniecznością* dla przyszłości naszych dzieci.

Wiem, że moje dzieci nie będą robiły nic innego, tylko odwiedzały strony dotyczące seksu, bo łatwo je znaleźć w sieci. Czy moje obawy są uzasadnione?

Dzieci mówią mi, że po kilku spojrzeniach większość stron dla „dorosłych" zaczyna je nudzić. Ciekawe, że kiedy dzieci odwiedzają „niestosowne" strony, częściej są to strony dotyczące morderstw niż seksu. Poza tym, choć dużo jest stron z brutalnym seksem dostępnych dla każdego, coraz więcej z nich wymaga dowodu, że odwiedzający jest pełnoletni.

Edukacja i budowanie solidnych, opartych na zaufaniu relacji z dzieckiem jest pierwszą linią obrony przeciw tym zagrożeniom. Taką samą rolę może spełnić wyszukiwanie zabawnych, ciekawych witryn odpowiednich dla dzieci, by miały alternatywę dla serfowania po „niestosownych" stronach.

Ufam moim dzieciom, że nie będą wędrowały tam, gdzie nie należy, ale obawiam się, że gdziekolwiek pójdą – znajdą pornografię. Nie będą w stanie tego uniknąć, nawet gdy zastosują się do moich reguł.

Jest wiele sposobów, by utrzymać dzieci na prostej drodze. By zapobiec problemom, które omawiam w punkcie „Zabłąkani na ciemnej stronie Internetu", można używać przeglądarek przyjaznych dzieciom i list stron zaaprobowanych, a także innych specjalnych, przyjaznych dzieciom możliwości.

Słyszałem, że Internet pełen jest kryminalistów. Czy to prawda?

Internet jest społecznością i jak każda społeczność ma swoje dobre i złe charaktery, miejsca bezpieczne i niebezpieczne. Przestępcy istnieją wszędzie, w świecie realnym i wirtualnym. Odsetek złych charakterów w cyberprzestrzeni nie jest inny niż w prawdziwym świecie.

Jak długo będą na tym świecie kryminaliści, znajdą się ludzie, którzy będą wykorzystywali system, używając nowych technologii. To oni pierwsi uczą się posługiwać nowym medium. Cały problem polega na tym, by wiedzieć, jak unikać niebezpieczeństw, i zrobić wszystko, by ochronić siebie, rodzinę i uniknąć kłopotów.

Sądzę, że jedynym sposobem ochronienia dziecka jest trzymanie go z dala od Internetu. Czy mam rację?

Jedyne, co osiągniemy, trzymając dzieci z dala od sieci, to to, że pozostaną one w tyle za rówieśnikami, gdy chodzi o umiejętności posługiwania się najpotężniejszym narzędziem edukacji i komunikacji w historii ludzkości.

Jest wiele rzeczy, które możesz zrobić, aby zapewnić dziecku bezpieczeństwo w cyberprzestrzeni. To prawie tak jak zapewniać im bezpieczeństwo w innych miejscach. Nie pozwalamy, by sześciolatki, zdane wyłącznie na własne siły, wałęsały się po wielkim mieście. Wy, rodzice, wiecie, jakie niebezpieczeństwa tam na nie czyhają, i uczycie dzieci, jak ich unikać. Wy ustalacie reguły gry i wy je egzekwujecie.

Ochranianie dzieci w cyberprzestrzeni nie jest niczym innym. Jedyny problem polega na tym, że nie wiecie, jakie są zagrożenia. Ale gdy je poznacie, ustalicie zasady i wyegzekwujecie je, tak jak to robicie w realnym świecie. To naprawdę jest proste!

Moje dzieci otrzymują pornograficzne e-maile. Czy to oznacza, że odwiedzały strony przeznaczone dla dorosłych?

Niekoniecznie. E-maile, które otrzymują, są odpowiednikiem „śmieci", które znajdujemy w naszych skrzynkach pocztowych. Nadawcy takich przesyłek wyłapują adresy w różnych miejscach, w kawiarenkach, klubach dyskusyjnych (nawet przyjaznych dzieciom), w książkach adresowych. Określają to jako „żniwa". Choć jest możliwe, że twoje dziecko wędrowało po stronach dla dorosłych, bardziej prawdopodobne, że reklamy dla dorosłych otrzymuje przez czysty przypadek.

Dobrze, przekonałaś mnie. Ale nie jestem typem technicznym, nie umiem nawet zaprogramować swojego wideo. Jak mogę nadzorować swoje dzieci w Internecie?

To prostsze, niż myślisz. Muszę się przyznać, że ja też nie umiem zaprogramować magnetowidu, a mimo to jestem uważana za światowego eksperta w sprawach bezpieczeństwa dzieci w Internecie. (Wyobraźcie sobie!). Wszystko opiera się w gruncie rzeczy na zdrowym rozsądku, gdy już zrozumiesz, o co chodzi. To nie jest sprawa technologii, ale komunikacji i edukacji.

Słyszałem, że w cyberprzestrzeni nie działa żadne prawo. Czy to prawda?

Nie. W zasadzie wszystko, co jest bezprawne poza siecią, jest bezprawne także w sieci. I choć nie mamy cyberpolicji wyłącznie dla In-

ternetu, mamy wydzielone jednostki, które pełnią funkcje policji internetowej. Problemem nie jest brak prawa, ale niewystarczająca liczba odpowiednio wyszkolonych funkcjonariuszy, oprzyrządowania i funduszy.

Obawiam się, że moje dzieci mogą zostać porwane lub być molestowane przez kogoś, kogo spotkają w sieci. Czy takie ryzyko rzeczywiście istnieje?

Istotnym terminem tutaj jest określenie „w sieci". Nikt nie może molestować dziecka w sieci ani porwać go w sieci. Można to zrobić tylko w realnym świecie (poza siecią). Więc łatwiej tego uniknąć, niż ludziom się wydaje. Po prostu naucz dziecko, że nie wolno mu spotykać się w realnym świecie z kimś, kogo poznało w świecie wirtualnym. W większości przypadków, kiedy takie zdarzenia miały miejsce, dzieci z własnej woli spotkały się z nieznajomymi. A to sprawa rodziców, nie Internetu.

Nawet jedno dziecko ofiara to o jedną ofiarę za dużo, ale zdarza się to bardzo rzadko: aresztowano mniej niż tysiąc osób molestujących dzieci, które uwodziły je lub przynajmniej usiłowały to robić poprzez Internet (prawie 98% z nich uznano za winne). (Tylko w Stanach Zjednoczonych jest 19 milionów dzieci, które mają dostęp do Internetu).

Czy pornografia nie jest nielegalna? A jeśli tak, to dlaczego w Internecie nic się z tym nie robi?

Nie ma prawnej definicji pornografii. To coś takiego, co zwykli ludzie określają jako „treści jawnie seksualne", a prawnicy – jako „obsceniczne". Obsceniczny materiał jest brutalny i nie ma innych (np. artystycznych czy naukowych) wartości. (Więcej na ten temat w rozdziale 5).

Jednak nawet gdy materiał prezentowany w Internecie jest wyraźnie nielegalny w Stanach Zjednoczonych, może być legalny tam, gdzie został wyprodukowany i wprowadzony do sieci. Ponadto nawet gdy coś niezgodnego z prawem zostało wyprodukowane w USA, istnieją inne zagrożenia (choćby takie jak cyberprześladowcy), które uznawane są za istotniejsze (i tak powinno być) przez instytucje zajmujące się przestrzeganiem prawa, które nie mają dość pieniędzy, by zajmować się wszystkimi problemami prawnymi występującymi w wirtualnym świecie.

Czy witryny porno nie mają obowiązku domagania się dowodu, że osoba oglądająca jest pełnoletnia?

W Stanach Zjednoczonych przygotowano ustawę, zakazującą na wszelkich stronach komercyjnych prezentowania jawnie seksualnych obrazów bez żądania dowodu pełnoletności od odwiedzających witrynę, ale została ona uznana za niezgodną z konstytucją. W chwili gdy to piszę, nie ma prawa nakazującego operatorom stron dla dorosłych ograniczanie dostępu do nich nieletnim czy żądanie od odwiedzających dowodu pełnoletności.

To jeden z powodów, dla których to na nas, rodzicach, spoczywa obowiązek doglądania dzieci poruszających się po Internecie.

Nie mam wiele pieniędzy. Jak mam sobie pozwolić na oprogramowanie filtrujące?

Większość narzędzi filtrujących kosztuje poniżej 30 dolarów, a są też bezpłatne. Powiem więcej o tych narzędziach – czym są, gdzie je dostać i ile kosztują – w rozdziale 8, w części zatytułowanej „Coś z kolumny A, coś z kolumny B".

Co Internet może zaoferować rodzicom i dzieciom?

Będę dużo mówiła o ciemnych stronach Internetu i potrzebie ochraniania dzieci, które tam się poruszają. Ale, jak już powiedziałam, Internet to wspaniałe miejsce, z milionami interesujących witryn dla rodzin i dzieci. Otwiera cały nowy świat nam, rodzicom, i naszym bliskim.

Rodziny, które używają Internetu, powtarzają mi stale, jak bardzo to ułatwiło i wzbogaciło ich życie. Poświęcę chwilę na zasygnalizowanie różnych rzeczy, które możemy robić z dziećmi w Internecie.

Gdy dzieci uczą się porozumiewania się w sieci, spotykają ludzi z innych krajów i kultur, wymieniają informacje, zdjęcia i opowieści ze światem i innymi członkami rodziny, uczą się nie tylko twórczego patrzenia na świat, ale i dzielenia się swoimi spostrzeżeniami i pomysłami. Mogą też wprost z domu zgłębiać problemy naukowe i utrzymywać kontakt z nauczycielami.

Członkowie rodzin dzięki Internetowi mogą nawzajem wspierać się w tragicznych chwilach i dzielić się radością w szczęśliwych. Młodzi rodzice mogą uczyć się rodzicielstwa, znaleźć odpowiedzi na różne pytania i kogoś zawsze chętnego do udzielenia pomocy. Rodzina

może zaplanować wakacje poprzez Internet. Listę mogłabym wydłużać w nieskończoność.

❖ Aktualności

Chcesz sprawdzić ostatnie wiadomości lub pogodę? Nie ma łatwiejszej drogi niż sprawdzenie w Internecie. „New York Times" (www.nytimes.com) oferuje w sieci swoje publikacje za darmo. W Internecie znajdziesz zapewne lokalną gazetę, a także witryny prezentujące lokalne wiadomości i pogodę.

❖ Informacje i wyniki sportowe

Wszystkie znajdziesz w sieci. Kiedy chcesz, możesz sprawdzić wyniki. Chcesz nabyć bilety na mecz? Zrób to w Internecie.

❖ Gry

Masz dość wyrzucania pieniędzy na gry komputerowe i telewizyjne dla dzieci? Jest tyle wspaniałych stron internetowych, które oferują gry za darmo. Bonus, jeden z ulubionych portali dla dzieci (www.bonus.com), podaje, że ich najpopularniejszą sekcją jest sekcja gier. A wypróbowaliście www.games.com?

❖ Jaś może pisać (i wyszukiwać informacje)

Kiedy ja sama dorastałam (gdybyście zapytali moje dzieci, powiedziałyby, że było to wtedy, gdy nie było elektryczności i bieżącej wody w mieszkaniach), pisanie to było coś, co robiliśmy, bo *musieliśmy*. Musieliśmy pisać kartki z podziękowaniami za prezenty urodzinowe. Musieliśmy pisać wypracowania do szkoły. Pisanie było bolesne i konieczne. (Może dlatego tak dużo czasu zajęło mi napisanie tej książki!).

Nic dziwnego, że wszyscy narzekali, że Jaś nie umie pisać. Ale tak się działo, zanim Jaś miał dostęp do Internetu! Internet zmienił to wszystko. Dzieci muszą pisać, żeby się porozumieć. To w ten sposób „rozmawiają" w sieci. Poza tym nasze dzieci uczą się, jak wyszukiwać różne rzeczy w Internecie. Znajdują informacje tak różnorodne jak badania naukowe (www.studyweb.com), możliwości podróżowania, dane o szkołach i uczelniach, informacje handlowe.

A jakąż cudowną sprawą jest Internet, gdy alternatywą dla niego jest włóczenie się po mieście w siąpiącym deszczu. Podczas pluchy nawet najbardziej atechniczni z nas docenią dostęp do biblioteki przez 24 godziny z domowego komputera.

Poza wyszukiwaniem materiałów do prac szkolnych dzieci poznają same szkoły. Nastolatki mogą sprawdzić wybrane szkoły średnie, a nawet składać podania o przyjęcie poprzez Internet, a rodzice mogą dowiedzieć się wszystkiego o rozpatrywaniu podań i stypendiach.

Wiele rodzin, z którymi miałam kontakt, stwierdziwszy, jak dobrze dzieci poruszają się w sieci, planuje swoje wakacje poprzez Internet. Większość linii lotniczych ma swoje strony w Internecie, podobnie – sieć większych hoteli. Przez Internet można zarezerwować różne zniżkowe pakiety wakacyjne i specjalne internetowe oferty linii lotniczych. Często rodzice wręcz przekazują sprawę rozplanowania wakacji w ręce nastolatków. To one wyszukują atrakcyjne miejscowości, drogi dojazdu, obiekty warte obejrzenia, możliwości noclegu.

Zakupy także są łatwiejsze przez Internet. Wiele dużych firm ma łatwe do odszukania witryny, które oferują konsumentom możliwość dokonywania zakupów. Jest to usługa szczególnie cenna dla rodziców pracujących lub mających małe dzieci, którym trudno jest tak często bywać w sklepach, jak by chcieli. Internetowe sklepy mają szczególne sposoby transmisji danych, więc informacje z karty kredytowej są bezpieczne.

Poprzez Internet możesz też zaaranżować wieczór dla rodziny, sprawdzić repertuar w okolicznych kinach i teatrach oraz kupić bilety. W sieci jest wiele stron filmowych, gdzie wyjaśniony jest system oceniania filmów oraz powody, dla których interesujący cię film podlega ocenie.

Internet jest globalny, pamiętacie? To jedna z najwspanialszych jego cech. Z tego też względu jest to wspaniała droga do wprowadzenia naszych dzieci w przyszłość. Czasy, gdy świat dzielił się na małe księstwa lenne, już dawno minęły. Cała gospodarka jest globalna. Każdy osiedlowy warzywniak posiada zagraniczne frykasy, a wszystkie lokalne firmy kupują, sprzedają, wymieniają doświadczenia z innymi na całym świecie. Jaki znajdziemy lepszy sposób nauczenia dzieci globalnego myślenia i przygotowania ich do zawodowej kariery, niż pozwalając im rozmawiać ze światem już teraz?

Chciałbyś co miesiąc pojechać do jakiegoś kraju? Zrób to zaraz ze swojego fotela przed komputerem. Chcesz dowiedzieć się czegoś

o dzieciach z innych części świata? Jest wiele witryn prowadzących godne zaufania kluby korespondencyjnych przyjaciół. (Zazwyczaj mają bardzo restrykcyjne warunki serwisu, ustalone tak, by chronić dzieci przed dorosłymi udającymi dzieci). A e-mail? W czerwcu 1999 roku tylko w America Online (AOL) – najpopularniejszym na świecie dostawcy usług internetowych przesyłano średnio 63 miliony listów dziennie. Wszyscy używają poczty elektronicznej z wielu różnych powodów. A poza tym jest szybka i bezpłatna.

❖ Szczególne rodziny... Szczególne dzieci

Zajmowanie się dziećmi może odizolować człowieka od świata, zwłaszcza gdy musimy dzielić swój czas między role zawodowe, domowe, działalność w społeczności lokalnej. Dawno minęły czasy, kiedy ludzie mający dzieci zasiadali razem do stołu, wymieniali wrażenia i plotkowali przy filiżance herbaty czy dzielili się pomysłami, wizjami i zmartwieniami, spotykając się przy płocie z sąsiadami. Ledwie starcza nam czasu i energii na zrobienie prania czy zawiezienie dzieci na trening.

Kiedy rodzina ma szczególne potrzeby, izolacja jest jeszcze większa. Rodzice adopcyjni potrzebują rozmowy z innymi rodzicami adopcyjnymi. Samotni rodzice (już nie mniejszość w naszym społeczeństwie, ale przecież zmagający się ze szczególnymi obciążeniami) potrzebują kontaktu z innymi samotnymi rodzicami. Dziadkowie, którzy stali się nieoczekiwanie głównymi opiekunami wnuków, potrzebują kogoś, kto mógłby pomóc im odnaleźć się w roli rodziców kolejnego pokolenia. Rodzice dzieci specjalnej troski (niepełnosprawnych i poważnie chorych) potrzebują kontaktu z ludźmi w podobnej sytuacji. Rodziny zastępcze także mają szczególne potrzeby i powinny móc podzielić się swoimi problemami z innymi ludźmi, którzy przeszli przez podobne doświadczenia. Rodzice są dla siebie wielkim wsparciem, ale dotąd wzajemne „odszukanie się" było niemałym problemem.

Teraz wszyscy mogą uzyskać pomoc i wsparcie poprzez Internet. Sieć stała się nowoczesną wersją płotu, przy którym spotykają się sąsiedzi, i lokalnym centrum, gdzie rodziny w szczególnej sytuacji uzyskują większe wsparcie niż gdziekolwiek indziej. I nie muszą w tym celu wychodzić z domu.

Nie tylko rodzice mogą kontaktować się z innymi w podobnej sytuacji poprzez Internet. Dzieci znajdują w sieci miejsca zaprojektowane specjalnie dla nich. Pamiętajcie, że w Internecie nie mamy określonego koloru skóry, nie nosimy uniformów, nie musimy być w stanie biegać czy chodzić, widzieć czy słyszeć. Internet pozwala nam być tym, czym jesteśmy, niezależnie od dzielących nas różnic: po prostu zwykłymi ludźmi.

Wymieniłam tylko niektóre z cudownych rzeczy, które można robić w sieci.

Krótko – jakie są zagrożenia?

Poza niebezpieczeństwem stwarzanym przez ludzi, którzy mogą próbować spotkać się z naszym dzieckiem w realnym świecie (co uważam za najgorsze zagrożenie i omawiam szczegółowo w rozdziale 4), istnieją mniej poważne zagrożenia, z którymi dzieci mogą zetknąć się w sieci. Mam tu na myśli dostęp do informacji dla nich nieodpowiednich: do stron oferujących dobra pochodzące z przemytu lub propagujące nielegalne działania oraz stron, które zagrażają naszej prywatności.

Mimo że najwięcej uwagi skupiają obszary zawierające treści seksualne i pornografię, istnieją łatwo dostępne strony zawierające inne informacje nieodpowiednie dla dzieci. Chodzi mi o reklamy papierosów i alkoholu, zachęty do brania narkotyków, a także literaturę szerzącą nieprawdziwe informacje, nienawiść, przemoc. Niektóre sprzedają nawet broń, narkotyki, trucizny, alkohol, pozwalają dzieciom na uprawianie hazardu poprzez sieć. Inne zbierają i sprzedają poufne informacje o dzieciach i rodzinie i stosują nieuczciwe strategie marketingu interaktywnego, których celem są serfujące w cyberprzestrzeni dzieci. Te rzeczy mogą być znacznie bardziej niebezpieczne dla naszych dzieci niż kontakt z treściami jawnie seksualnymi.

Na koniec, ponieważ naszym zadaniem jest rozmawiać o zagrożeniach i sposobach unikania ich, muszę ostrzec was przed zagrożeniami, jakie wasze dzieci (i ich przyjaciele) mogą stanowić dla *innych* w cyberprzestrzeni, także dla was samych. Mogą przekazać numery i hasła waszych kart kredytowych, różne poufne informacje dotyczące rodziny, zakupić rzeczy, za które wy będziecie płacili, naruszyć prawa autorskie, popełnić przestępstwo komputerowe; mogą zniszczyć lub skasować ważne pliki. W niektórych przypadkach mogą nawet nie wiedzieć, że to robią, ale niebezpieczeństwo nie jest przez to

mniejsze (zapytajcie moją siostrę o wyczyny jej trzyletniego cherubinka. Opowiem tę historię później).

Wreszcie istnieje zagrożenie, że twój komputer zaatakują wirusy lub hakerzy.

Jest o czym myśleć. Ale w tej książce proponuję pomoc, rozwiązania i rady na wszystkie problemy. Nie martwcie się. (Zauważyliście, że często to powtarzam? Czy wam to pomaga?).

Rozdział 2

Dobro, zło i zachowanie ostrożności

Codziennie dostaję setki e-mailów od rodziców, którzy niepokoją się bezpieczeństwem dzieci w Internecie. Często są to listy od rodziców, którzy właśnie odkryli, jak łatwo ich pociechy mogą znaleźć niestosowne materiały i jak wiele jest sposobów popadania w kłopoty. Wszystko to może złościć rodziców. Mogą mieć wrażenie, że zostali jakoś zmanipulowani. (I może zostali).

Znamy sposoby nadużywania i złego używania Internetu. Choć codziennie pojawiają się nowe (ludzie, którzy wymyślają sposoby nadużywania Internetu, bywają bardzo twórczy), zrozumienie, jak to się najczęściej robi, i świadomość intencji przestępców, daje nam przewagę nad nimi. Musimy nauczyć się, jak wykorzystać dobre strony Internetu, unikając zarazem zagrożeń, które stwarza.

Poznawanie gorszej strony Internetu

Możliwość komunikacji ze wszystkimi, wyszukiwanie informacji, wymiana opinii to rzeczy, do których Internet służy najlepiej. Z drugiej strony te możliwości mogą zostać źle użyte. Każdy może kontaktować się z tobą i twoimi dziećmi, także ci, z którymi kontaktów wolałbyś unikać. Wyszukiwanie informacji może doprowadzić do znalezienia takich, których wolałbyś nie znaleźć. A poznając różnorodne opinie, zetkniesz się również z takimi, których nie będziesz w stanie przyjąć spokojnie.

Jako rodzice musimy umieć ocenić i okiełznać te zagrożenia. Oto wyzwanie dla nas. (Jest to łatwiejsze, niż może się wydawać, wierzcie mi).

Kiedy zdjąć dodatkowe kółka

Kiedy nasze dzieci wchodzą w określone obszary sieci lub podejmują określone działania, są nie tylko wystawione na wielką liczbę różnych treści, ale i stają przed większymi zagrożeniami. Te doświadczenia mogą być cenne i zabawne, gdy dzieci są przygotowane, by sobie z nimi poradzić, ale i wtedy zawierają pewne ryzyko, zmieniające się zależnie od wieku dziecka i stopnia przygotowania.

Jako rodzice stale pomagamy dzieciom radzić sobie ze wzrastającym zagrożeniem. Kiedy uczymy je jazdy na rowerze, używamy najpierw dodatkowych kółek. Potem, gdy sądzimy, że są przygotowane, uczymy je zachowania równowagi na rowerze już bez dodatkowych zabezpieczeń. Ale stale dzieci obserwujemy, podążamy obok, podnosimy i przytulamy, gdy – co nieuchronne – wpadają na przeszkody. W końcu pozwalamy im jechać samodzielnie i wybrać się na dalszą przejażdżkę. Gdy radzą sobie na tyle, by wybrać się na 25-kilometrową wycieczkę, już nas nie potrzebują.

Tak samo jest z Internetem.

Podstawy

Musicie dowiedzieć się więcej o różnych zakresach Internetu i serwisach, które oferuje (wiele z nich dzieci uwielbiają), żebyście, mili czytelnicy, mogli posługiwać się zdrowym rozsądkiem, tak jak posługujecie się nim wtedy, gdy dziecko chce udać się do centrum handlowego, jechać metrem czy samodzielnie wybrać się do miasta. Różne zwykłe rodzicielskie działania – jak poznanie kolegów dziecka, kontrolowanie go, upewnianie się, że wiemy, co dzieci mają zamiar robić – są tak samo skuteczne jak zawsze. (Pamiętajmy, że zdrowy rozsądek sprawdza się równie dobrze w sieci, jak i poza nią).

Obszary sieci, wobec których musimy zachować szczególną ostrożność, obejmują: różnego rodzaju grupy dyskusyjne i określone czynności, jak pogawędki (czaty), wyszukiwanie haseł, przesyłanie wiadomości za pomocą programów komunikator internetowy, rejestracja w witrynach, włączanie się do klubów korespondencyjnych przyjaciół, wypełnianie profilu i tworzenie własnych stron WWW.

Tym, czego chciałabym was nauczyć, jest umiejętność oceny zagrożeń i korzyści, byście świadomie dokonali wyboru obszarów, po których dziecko może serfować, i zajęć, do których może się włączać.

Gdy zrozumiecie, jak powstają zagrożenia, będziecie wiedzieli, jak im przeciwdziałać i jak dokonać własnego wyboru. Rzadko jest to wybór wszystko albo nic. I pamiętajcie, że nic nie jest niezmienne. Klucz do sukcesu leży w znalezieniu tego, co odpowiada tobie i twoim dzieciom. Gdy dzieci dorastają, dojrzewają i zdobywają więcej samodzielności, restrykcje i zasady muszą ulegać zmianom.

Zabłąkani na ciemnej stronie Internetu

Nawet gdy wasze dzieci próbują unikać kłopotów i chcą stosować się do zasad bezpiecznego serfowania, mogą wpaść w kłopoty przez przypadek. Pamiętacie, mówiłam, że nawet gdy ufacie swoim dzieciom, nie możecie ufać Internetowi? To właśnie mam tu na myśli.

❖ Wyszukiwanie kłopotów

Umiejętność znalezienia tego, czego szukamy, jest niezbędna do poznania wszystkich cudów Internetu. Ale gdy czegoś poszukujesz w sieci, jest bardzo prawdopodobne, że znajdziesz więcej, niż byś chciał. By zrozumieć, jak można nadużywać wyszukiwania, musisz wiedzieć, jak powinno się odbywać. (Postaram się wytłumaczyć to tak bezboleśnie, jak się tylko da).

Mówiłam, że Internet to świat fascynujących informacji wcześniej niedostępnych dla niewtajemniczonych. Miliony stron na każdy możliwy temat... za darmo! Chwileczkę! Powinieneś już wiedzieć, że gdy prawnik oferuje coś tak atrakcyjnego za darmo, zawsze tkwi w tym jakaś pułapka.

Co jest tą pułapką? Że musisz to znaleźć sam! Ale przy takiej ilości informacji jak w Internecie to jak szukanie igły w wirtualnym stogu siana. Więc jak znaleźć cokolwiek w Internecie?

Dzisiaj już większość z nas jest obznajomiona z nazwami domenowymi, zarejestrowanymi przez największe korporacje, takimi jak: www.disney.com, www.sony.com, czy www.nbc.com. (Kilka lat temu nikt z nas nie miał pojęcia, co oznacza „kropka com", a teraz to część

naszego codziennego słownika). Gdy poszukujesz witryny znanej firmy, często wystarcza, że napiszesz nazwę firmy, dodasz „.com" i znajdziesz się tam.

Ale co się dzieje, jeśli szukasz informacji na jakiś temat i nie wiesz, czy istnieje strona dostarczająca takich informacji? Albo gdy szukasz firmy czy osoby i nie znasz nazwy domeny (a chwyt z „kropka com" nie daje rezultatów)?

W takich wypadkach musisz użyć wyszukiwarki (to tak jak dzwonić pod 913 lub używać książki telefonicznej). Istnieje wiele wyszukiwarek. Najpopularniejsze to: AltaVista, Excite, Go (wyszukiwarka Disney/ABC), Hot Bot, Infoseek, Lycos, Snap (wyszukiwarka NBC), WebCrawler, AlltheWeb, Yahoo! Gdy poznasz trochę Internet, zorientujesz się, że jedne wyszukiwarki są dla ciebie lepsze, niż inne. Może się też okazać, że używasz jednej do jakichś określonych poszukiwań, a innej – do pozostałych.

Wyszukiwarki pozwalają na odnajdowanie stron według nazwy lub według głównego tematu. Działają na tej samej zasadzie co książka telefoniczna. Szukasz na żółtych stronach, jeśli znasz tylko rodzaj usługi, której potrzebujesz, albo na białych, jeśli znasz nazwisko poszukiwanej osoby. By zacząć wyszukiwanie w Internecie, należy wpisać nazwę lub słowa, które, jak sądzisz, powinny na poszukiwanej stronie występować (tzw. hasło wyszukiwania). Jeśli szukasz kwiaciarni Kowalskiego, mogą to być np. słowa: Kowalski, kwiaty, albo Kowalski + kwiaty, a możesz też przeglądać listy stron, uporządkowane w katalogi tematyczne – np. przeglądasz katalogi: kwiaty, kwiaciarnie, rozprowadzanie kwiatów.

Większość wyszukiwarek zbiera informacje o stronach, używając programów (nazywanych *spiders* lub *bots*), które przeglądają sieć w poszukiwaniu stron i informacji na nich zawartych. Wyszukują one wszystkie słowa na stronie, a w niektórych przypadkach na wszystkich stronach, do których umieszczono odsyłacze na danej stronie. Potem tworzą spis tych stron, opierając się na liczbie i częstości występowania słów kluczowych. Jeśli wyszukiwarka ma też opcję wyszukiwania katalogów, strony są potem czytane przez recenzentów, którzy umieszczają je w odpowiedniej dla ich zawartości treściowej kategorii tematycznej.

❖ Kot w worku

Ale ze sposobu, w jaki wyszukiwarki kategoryzują strony, rodzi się wiele problemów. Twórcy stron (*webmasters*) używają słów kluczowych – w niektórych przypadkach pierwszych 25–30 słów ze strony – by wyszukiwarka mogła umieścić stronę w odpowiedniej kategorii. Te słowa kluczowe i opisy, zapisane specjalnym kodem, noszą nazwę *metatags*. Są one ogromnie pomocne, bo bez nich niejedna strona mogłaby zostać skategoryzowana na podstawie wstępu, np: „Witamy na naszej stronie! Uaktualniamy ją regularnie i czekamy na wasze opinie. Zaglądajcie tu często, by obejrzeć nasze nowe produkty i wzory". To nie mówi nic o stronie, o tym, do kogo należy czy jakie informacje zawiera, choć takie właśnie może być 25 pierwszych słów i bez *metatags* byłyby użyte przez programy typu *spiders* i *bots* do umieszczenia strony w jakimś katalogu.

Dobry webmaster, by zapewnić umieszczenie strony w odpowiedniej kategorii, użyje jako metatags np. słów: nartodeski, urządzenia sportowe, sport dla dzieci, gry, zajęcia na powietrzu, gdy chce powiedzieć wyszukiwarkom, że jego strona dotyczy sprzętu sportowego dla dzieci. Wówczas, ilekroć wpiszesz w okienku wyszukiwarki któreś z wymienionych słów, pojawi się jego strona. Bez metatags wyszukiwarka mogłaby „nie wiedzieć", że ta strona dotyczy nart.

Wiele witryn zarabia, umieszczając na swoich stronach reklamy. Właściciele stron częściej odwiedzanych mogą domagać się większych pieniędzy za miejsce reklamowe. Robią więc co mogą, by zwiększyć liczbę zaglądających do nich ludzi. Dla kontrolera ruchu internetowego wizyta dziecka liczy się tak samo jak wizyta dorosłego. Ruch jest ruchem.

Jakich zatem sztuczek można użyć, by zwiększyć liczbę odwiedzających? Można posłużyć się popularnymi słowami i popularnymi tematami (takimi jak postacie Disneyowskie) czy zwrotami typu „amerykańska dziewczyna" w opisach zawartości strony (metatags). Spróbuj wyszukać hasła „zabawki" czy „dziewczynki" (typowe hasła, gdy szukasz zabawek dla dziecka płci żeńskiej), a dowiesz się o przemyśle pornograficznym więcej, niż chcesz wiedzieć.

Stosuje się też chwyt z „podstawianiem" strony, który polega na tym, że w wyszukiwarce najpierw ukazuje się na liście „podstawiona" strona, a dopiero potem prawdziwa. Możesz sądzić, że czekasz na otwarcie wybranej strony, a tymczasem wpadasz na stronę dla dorosłych.

Niektóre witryny tylko dla dorosłych, nawet jeśli nie mają zamiaru nikogo zwodzić, używają w opisach języka, który jest zwodniczy. Poszukujesz np. informacji na temat zespołu Spice Girls czy Bambi i trafiasz nieoczekiwanie na stronę o *spicy girls* czy „Bambi, pulchnej, gorącej blondynce".

To wszystko oznacza, że za każdym razem, gdy poszukuje się czegoś, korzystając z wyszukiwarki, można natrafić na strony zawierające treści jawnie seksualne czy inne nieodpowiednie dla dziecka.

Co można na to poradzić?

Łatwym rozwiązaniem problemu jest stosowanie wyszukiwarek filtrujących. Taka wyszukiwarka wybiera tylko sprawdzone, przyjazne dzieciom strony. Najpopularniejsze „cenzurowane" wyszukiwarki to: Yahooligans! (www.yahooligans.com) i Ask Jeeves for Kids (www.ajkids.com). Również niektóre popularne wyszukiwarki dla dorosłych mają dodatkowo opcję wyszukiwania dla dzieci. (Dokładniej przedstawiam tę sprawę w rozdziale 8).

Inną metodą jest posługiwanie się katalogami w wyszukiwarkach. Lycos i Yahoo! to dwa doskonałe przykłady wyszukiwarek katalogowych, gdzie recenzenci czytają i kategoryzują strony pod kątem głównych tematów. Innym przykładem jest About.com, którego eksperci także przeglądają strony i tworzą listy odpowiednich stron.

Ale z tego, że strony umieszczone w katalogu są przeglądane, nie wynika, że wszystkie tematy wyszukiwania są przyjazne dzieciom. Więc upewnij się, że wybierasz temat odpowiedni dla dzieci. W innym przypadku możesz znaleźć strony, które choć są przypisane do jakiejś kategorii zgodnie ze swoją zawartością, mogą nie być odpowiednie dla dzieci.

❖ Ważna jest znajomość ortografii!

Pamiętaj, że w przypadku stron dla dorosłych gra toczy się o ruch na stronie. Właściciele nie chcą więc liczyć tylko na to, że kluczowe słowa zapewnią ten ruch. Jak jeszcze mogą go zwiększać? Mogą używać nazwy domeny, która będzie podobna do nazwy bardzo popularnej strony i pisać ją z błędem – wtedy ludzie, którzy chcą się dostać na ową stronę i popełnią prosty błąd w pisaniu czy ortografii, lądują na

stronie dla dorosłych. (A przynajmniej ja sądzę, że tak się to dzieje. Ale może oni naprawdę nie znają ortografii...).

W ostatnich latach „literowe oszustwa" objęły Yahhoo.com (strona z brutalną pornografią), zamiast przeglądarki Yahoo.com (ta sprawa już została załatwiona), i kilka innych popularnych wyszukiwarek. Ponieważ nawet najbardziej biegłe w technice dzieci czasem robią błędy w pisaniu czy ortografii, nie jest nieprawdopodobne, że znajdą się nieoczekiwanie na jednej ze stron, które zostały zaprogramowane tak, by wyprowadzić ludzi w pole.

Co można na to poradzić?

Warto zajrzeć pod adres: www.domainserfer.com. Zorientujesz się, czy ktoś inny próbuje używać nazw stron najczęściej przez ciebie wybieranych (właściciele nazw firmowych powinni robić to szczególnie często). Sprawdzisz, czy istnieją adresy podobne do tych najczęściej używanych przez twoje dzieci.

Jeśli znajdziesz strony dla dorosłych używające nazw, które twoje dzieci przez pomyłkę mogą wpisać, szukając swoich ulubionych stron, uczul je, by były szczególnie uważne, pisząc dany adres.

Jeśli używasz programu filtrującego, możesz dodać znalezione przez siebie niestosowne strony do listy stron, do których dostęp jest zablokowany. W przeciwnym razie powinieneś zrobić zakładki na ulubionych stronach swoich dzieci za pomocą swojej przeglądarki. (Więcej na ten temat piszę później, więc się nie martwcie). Wówczas, gdy dzieci będą chciały dostać się na taką stronę, po prostu klikają odpowiednią zakładkę. Tym sposobem nie trafią do niestosownych miejsc z powodu zwykłej literówki czy nieznajomości ortografii. Zwiększy to zarazem szybkość serfowania.

❖ Udawanie znanej strony: sztuczka z „kropka com"

Słyszymy to w radio, telewizji, czytamy na plakatach, w gazetach. Gdziekolwiek się obrócimy, natykamy się w taki czy inny sposób na „kropka com". Twórcy stron WWW (*webmasters*) także to wiedzą. I wykorzystują przeciw nam braki naszej wiedzy o nazwach domen. Większość z nas nauczyła się, że gdy szukamy dużej firmy czy znanej instytucji, dodajemy do nazwy „.com" i najczęściej znajdujemy się tam, gdzie chcemy. Ale nie zawsze.

Szybko! Jak odszukacie stronę Białego Domu lub agencji NASA? (Nie oszukujcie i nie zaglądajcie do następnego akapitu). Prawdopodobnie większość z nas odpowie, że należy użyć domeny .com. Niestety, źle!

Większość stron rządowych w USA ma końcówkę .gov. Dwa najsłynniejsze przykłady „zawłaszczania" ruchu poprzez użycie słynnych nazw to właśnie prowadzące na strony z pornografią, użycie .com zamiast prawdziwego adresu strony Białego Domu w Waszyngtonie, który brzmi www.whitehouse.gov, i zamiast oficjalnej strony agencji NASA, której adres to www.nasa.gov.

Wszystkie nazwy domen muszą zawierać trzyliterowy sufiks, który wskazuje na typ organizacji lub istotę zawartości. Końcówka .com wskazuje raczej na instytucję komercyjną niż sieć Internetową (.net), organizację międzynarodową (.int), instytucję oświatową (.edu), organizację non-profit (.org), militarną (.mil) lub rządową (.gov)..Com jest zdecydowanie najpopularniejszą końcówką, następne w kolejności są .edu i .org.

W stronach WWW tworzonych poza USA używa się raczej dwuliterowych kodów kraju niż końcówek trzyliterowych. Zakłada się, że strony bez oznaczenia kraju pochodzenia są stronami amerykańskimi.

Kiedyś uczestniczyłam w seminarium na temat mądrego serfowania, w trakcie którego uczono rodziców, jak bezpiecznie używać Internetu. W pewnej chwili z przerażeniem patrzyliśmy, jak stażysta wystukuje na klawiaturze „whitehouse.com", gdy mówiliśmy o prawdziwej stronie Białego Domu. Urządzenia filtrujące nie były włączone. Gdy my wszyscy czekaliśmy ze zgrozą na to, co się zaraz stanie, rodziny zebrane na seminarium zobaczyły na własne oczy, jakie mogą być skutki takich pomyłek. To była bardzo pożyteczna lekcja.

Taki błąd może popełnić każdy z nas. Jak możemy oczekiwać, że naszym dzieciom się to nie zdarzy?

Co można z tym zrobić?

To jeszcze jeden przypadek, gdy pomóc może oprogramowanie filtrujące. Odrzuca ono określone strony i prawie zawsze je wychwytuje. Małym dzieciom można też ograniczyć dostęp do Internetu wyłącznie do stron uznanych za przyjazne, zalecić korzystanie z wyszukiwarek dla dzieci lub wyposażonych w opcje filtrowania, gdy nie są pewne jakiegoś adresu. Gdy dzieci poznają znaczenie końcówek .com, .gov, .org, .edu, prawdopodobieństwo błędnego wypisania adresu będzie mniejsze.

Rodzice mogą też przeglądać wszystkie strony, zanim pozwolą dzieciom na nie się dostać. Następnie mogą utworzyć listę sprawdzonych stron w swoim folderze zakładki. Wtedy dzieci po prostu klikają określony znaczek, by otworzyć daną stronę. Rozwiązaniem może być także korzystanie z listy stron rekomendowanych dla dzieci przez American Library Association czy z innych rzetelnie przygotowanych zestawów stron, które podaję w rozdziale „Tak, Wirginio...".

Zakładki – trop z okruszków chleba

Więc jak zabrać się do tworzenia własnej listy sprawdzonych stron? Przeczytaliście podrozdział o znajdowaniu drogi w Internecie. Znaleźliście stronę. I to tę, którą chcieliście znaleźć. Gratulacje! Jest tam wszystko, czego szukaliście, wszystkie informacje lub wszystkie potrzebne odnośniki do innych miejsc. Ale nie chcesz czytać tego w tej chwili. Więc co? Jak odnajdziesz drogę znowu, jeśli nie zostawiasz śladów z okruszków chleba?

Tworzenie zakładek jest najłatwiejszym sposobem odnajdowania drogi powrotnej do danej strony. Tak jak wkładasz zakładkę do książki, by od razu znaleźć właściwe miejsce, to samo możesz zrobić w komputerze. Każda przeglądarka ma własny sposób oznaczania wyróżnionych stron. Określają je też różnymi nazwami. Netscape używa nazwy „zakładka", ale Explorer używa nazwy „ulubione" (*favorites*). Niezależnie od nazwy zasada działania jest taka sama.

Posłużmy się przykładem Netscape Navigator. Klikasz na słowie „zakładka" (*bookmark*) na pasku narzędzi u góry ekranu monitora. Następnie umieszczasz kursor na „Dodaj zakładkę" i klikasz. Program zachowuje na liście zakładek nazwę i adres strony, na której w danej chwili jesteś. Kiedy chcesz tam wrócić, otwierasz menu zakładek, przewijasz na żądaną stronę – i już! Nie musisz za każdym razem wpisywać adresu, nie musisz pamiętać, co pisane jest małą literą, co dużą. A poza tym nie ma obawy, że twoje dziecko przez błąd w pisowni wyląduje na stronie z pornografią.

Pamiętaj jednak, że jeśli na swojej liście masz strony, których nie chciałbyś pokazywać swoim dzieciom (a nie masz programu do zablokowania ich), używaj tej opcji ostrożnie, może zmień nazwy stron na mniej ekscytujące (np. zamiast „Pulchne ślicznotki w bikini" daj np.

tytuł „Księgowość w aspekcie krótkoterminowych zwyżek"), by zmniejszyć prawdopodobieństwo, że ktokolwiek będzie chciał otwierać zakładkę. (Dorośli mają prawo uczestniczyć w różnych rzeczach, nawet jeśli nie chcą, by ich dzieci robiły to samo. Ten sposób pozwoli ci zaznaczyć stronę, a jednocześnie zachować prywatność).

Kiedy zbliża się niebezpieczeństwo...

Nawet gdy twoje dzieci potrafią unikać stron dla dorosłych i oszustw, czasem takie strony poszukują ich. Robią to, wysyłając nam z własnej inicjatywy pliki e-mailów, określane jako *spam*.

Przed erą Internetu słowo „spam" istniało głównie jako nazwa firmowa konserwy mięsnej, sławnej w czasie II wojny światowej. Było także centralnym elementem komicznym jednej ze scen w filmie „Latający cyrk Monty Pythona" (Wikingowie wyśmiewają się z mielonego mięsa, podśpiewując „spam, spam, spam", kiedy klienci w restauracji zamawiają „Spam(r) ze Spamem(r), a na przystawkę Spam(r)").

Prawdopodobnie dzięki Monty Pythonowi spam jest najbardziej znanym żargonowym określeniem na śmieci z poczty elektronicznej, przysyłane do naszych elektronicznych skrzynek, dostarczające tak niezmiernie użytecznych informacji, jak oferty piramid finansowych, nachalny marketing czy odsyłacze do stron z pornografią. (Odsyłacz [*link*] to specjalny kod zawarty w dokumencie lub e-mailu, który, gdy się na nim kliknie, przenosi serfującego do innej witryny lub w inne miejsce w tej samej witrynie).

❖ Spam – to nie jest po prostu mielone mięso

Wszyscy nienawidzimy spamu (mam na myśli śmieci e-mailowe, nie wypowiadam się o konserwie). Większość z nas otwiera swoje skrzynki internetowe i znajduje tam mnóstwo niechcianych wiadomości, z których wiele zawiera odsyłacze do stron dla dorosłych. Wystarczy, by dzieci kliknęły w wyróżnionym w wiadomości miejscu, a znajdują się na stronach wypełnionych pornograficznymi obrazami. Niekiedy odsyłacze są wyraźnie oznaczone jako związane z seksem, czasami nie. Na przykład te jasno opisane mogą być nazwane „xxxBlondynki", te zakamuflowane mogą zawierać taki przekaz: „Cześć. Przed tygodniem obiecałem dostarczyć ci adres tej strony. Oto on". Możesz nie

rozpoznać nadawcy wiadomości i zachodzić w głowę, kto obiecał podać ci jakiś adres, ale klikasz w oznaczonym miejscu i już jesteś na stronie eksponującej pornografię. To samo dzieje się, gdy klika twoje dziecko.

Kto kogo ochrania? Ochranianie wrażliwości niewinnych

Otrzymuję więcej skarg na niechciane e-maile z odsyłaczami do stron dla dorosłych niż na cokolwiek innego. Każdego dnia odbieram przynajmniej 40 listów od rodziców, pytających, co z tym zrobić. Wielu rodziców, nie rozumiejących, jak nadawcy takich wiadomości zdobywają adresy e-mailowe czy ICQ ich dzieci, sądzi, że musiały one odwiedzać strony dla dorosłych i dlatego otrzymują reklamy. Nie policzę, ilu nastolatków ocaliłam od kary, wyjaśniając, że wcale nie trzeba odwiedzać stron dla dorosłych, by być zasypywanym takimi wiadomościami.

Ale nie tylko dzieci trzeba chronić przed pornograficzną pocztą. Pewna nastolatka ostatnio przyznała mi się, że choć miała wspaniały kontakt z matką, martwiła się, jak mama może zareagować, kiedy zorientuje się, ile pornograficznych śmieci znajduje się co dzień w skrzynce jej córki. (Córka nie robiła nic, by sprowadzać te śmieci, był to zwykły *spam* dostarczany wszystkim klientom AOL).

Kiedy matka zdecydowała się w końcu korzystać z ich konta internetowego, musiała poprosić córkę o pomoc. Ta założyła jej skrzynkę, wybierając drugą co do restrykcyjności opcję kontroli rodzicielskiej, dostępną w AOL, stworzoną z myślą o młodszych nastolatkach (blokowane są e-maile od wszystkich nadawców niewymienionych na liście). Matka oczywiście nie miała pojęcia, że jej dostęp do Internetu jest ściśle filtrowany i że córka próbuje ją ochraniać i oszczędzać jej uczucia.

Kiedy przestałam się śmiać, uświadomiłam sobie, jak bardzo w wielu naszych rodzinach władza przesunęła się w stronę młodego pokolenia, przynajmniej jeśli chodzi o Internet. Dzieci często mają kontrolę nad warunkami naszego dostępu do Internetu, jeśli to one kontrolują hasło. Często też to one instalują programy filtrujące, które kupiliśmy dla nich. (Szczęśliwie programy te instaluje się bardzo łatwo. W innym przypadku – już to słyszę: „Małgosiu, popatrz, kupiłam tu wspaniałą rzecz, która zablokuje ci dostęp do tych wszystkich rzeczy, które masz ochotę oglądać w Internecie, a ja nie chcę, abyś oglądała. Pomóż mi to zainstalować").

Teraz dzieci próbują chronić nas przed niestosownymi treściami. Jedna z moich Teenangels (przedstawiam je w rozdziale 9) powiedziała mi, że gdy kilka lat temu pierwszy raz znalazła pornograficzne oferty w swojej skrzynce, była ogromnie zszokowana i skrępowana (ma 15 lat). Teraz to nie robi na niej żadnego wrażenia. Usuwa takie przesyłki bez zastanowienia. Stwierdziła, że wprawdzie internetowy kontakt z obrzydliwościami nie uodpornił jej na nie (pewnie nigdy nie można stać się w pełni odpornym na różne formy pornografii), ale jest coraz lepsza w ignorowaniu ich. (Choć możemy nie czuć się najlepiej, słysząc o „uodpornianiu się" naszych dzieci na pornografię, pociechą jest świadomość, że one często usuwają taki materiał nawet nie rzucając nań okiem. Może nie jest to już zakazany owoc).

Jak spam działa?

Ogłoszeniodawcy – spamerzy – zdobywają nasze adresy e-mail, ICQ i komunikatora internetowego na wiele sposobów. Czasem biorą adresy od tych, którzy odwiedzili ich strony, ale znacznie częściej używają programów i ludzi do zdobywania tych adresów w kawiarenkach (*chatrooms*), grupach dyskusyjnych i z tzw. profilów użytkownika. Proces ten określa się jako „żniwa". Następnie miliony adresów są często sprzedawane innym reklamodawcom.

Ale choć dany adres był aktualny w momencie „żniw", nie wiadomo, czy jest używany nadal – dopóki adresat nie zareaguje na przesyłane reklamy, składając skargę lub prosząc o skreślenie z listy adresowej. Wówczas nadawcy ogłoszeń dowiadują się, że to nadal aktualny adres. Oznacza to, że będzie on znacznie cenniejszy, kiedy będą go sprzedawać następnemu zainteresowanemu przesyłaniem niechcianej reklamy. Jeśli w jakikolwiek sposób zareagujesz na przysyłane śmieci, możesz oczekiwać zwiększonej ilości spamu.

Sądzisz, że to tylko TY nie znosisz spamu!

Tymi, którzy nienawidzą „śmieci" jeszcze bardziej niż my, są dostawcy usług internetowych. Wydają miliony dolarów na zwalczanie spamerów w sądach, próbując powstrzymać ich od używania swoich serwerów do przesyłania reklam. Ale gdy tylko uda się uciszyć jednego, pojawia się następny.

Dostawcy Internetu stworzyli aplikacje zatrzymujące e-maile wysyłane przez zidentyfikowanych spamerów. Ci z kolei rozwinęli kontrofensywę z użyciem własnej technologii i dalej wysyłają spam, udając innych nadawców, by przemknąć się przez filtry. Ze wzrostem liczby posiadanych przez spamerów list adresowych wzrasta ilość niemożliwych do przesłania „śmieci".

Kiedy wiadomość nie może być przesłana, jest zwracana nadawcy. To powoduje, że spamerzy są zalewani zwrotami. Używanie fałszywego adresu nadawcy sprawia, że zalany listami zostaje każdy podany jako nadawca. Operator wybranego fałszywego nadawcy otrzymuje więc niedoręczone wiadomości i zwroty spamu. To powoduje, że serwery popularnych dostawców Internetu są przeciążone zwracanymi wiadomościami. By mieć pojęcie o skali problemu, zauważmy: AOL donosi, że duży procent internetowych e-mailów (nie tych wysyłanych przez rzeczywiście zarejestrowanych w AOL użytkowników Internetu), które przechodzą przez ich serwery każdego dnia, to właśnie spam. Kosztuje to ich mnóstwo pieniędzy i bardzo spowalnia działanie systemu dla klientów. Więc jest to problem dla wszystkich.

Co można na to poradzić?

Może to zaskakujące, ale nie ma prawa, które zmuszałoby nadawców spamu do skreślenia cię z listy adresatów czy regulującego wysyłanie „e-śmieci" (inaczej niż z tradycyjnie doręczaną „śmieciową pocztą"). Oczywiście należy podjąć działania przeciw oszustwom dokonywanym w sieci i nieuczciwym schematom marketingowym, reklamowanym w spamach, ale nie ma mocy, by ograniczyć samo zjawisko.

Choć generalnie jestem przeciwna regulacjom odnoszącym się do Internetu, wysyłanie spamu jest jedną ze spraw, które wymagają działań ze strony rządu. Jeśli zgadzacie się ze mną, skontaktujcie się ze swoimi reprezentantami w parlamencie. Powiedzcie im o swoich doświadczeniach z niechcianymi reklamami, szczególnie zawierającymi odsyłacze do stron z pornografią, interaktywny marketing i nieuczciwe oferty. Poproście ich o pomoc. By coś naprawdę się zmieniło, potrzebne jest prawo.

Samopomoc – jak się bronić?

Dopóki nie powstanie prawo dotyczące spamu, możemy podejmować pewne kroki we własnym zakresie, by ograniczyć ilość śmieci w naszych skrzynkach poczty internetowej.

Wielu dostawców Internetu, operatorzy serwisów sieciowych, mają specjalne adresy, gdzie należy zgłaszać spam. Sprawdź u swojego dostawcy.

Możesz też skontaktować się ze swoim dostawcą usług internetowych, by dowiedzieć się, czy dostępne są programy filtrujące e-maile. Jeśli dostawca nie może nic pomóc, operatorzy określonych usług w sieci informują odbiorców spamu, jak blokować lub filtrować e-maile.

Chwyt z podwójnym kontem

Ponieważ „żniwa" adresów często odbywają się w miejscach publicznych, takich jak kawiarenki (*chatrooms*), grupy dyskusyjne i profile, możesz uniknąć przekazania adresu, używając dwóch – publicznego i prywatnego. Używając publicznego w miejscach publicznych i programów filtrujących, możesz zablokować wszystkie nadchodzące e-maile, także śmieci. A prywatnego adresu używać do kontaktowania się z ludźmi, których znasz. Nie potrzebujesz wówczas filtra, bo tego adresu nie ujawniasz publicznie i znacznie trudniej będzie go zdobyć. Posługiwanie się dwoma adresami nie jest wyjściem doskonałym, ale może pomóc.

Korzystanie z narzędzi wspomagających rodzicielską kontrolę

Jest wiele programów filtrujących, które umożliwiają ci zablokowanie wszystkich nadchodzących e-mailów oprócz wysłanych przez ludzi, których umieścisz na liście. To pozwala twoim dzieciom odbierać wiadomości od przyjaciół i cioci Geni, ale zatrzymuje listy od obcych, w tym również i od spamerów. Niestety, blokuje to także listy od kolegi z klasy i wujka Franka, jeśli nie figurują na liście.

Nie znam narzędzi kontroli rodzicielskiej, które zatrzymywałyby niechciane przesyłki inaczej niż blokując wszystkie nadchodzące e-maile (oprócz wysłanych od określonych nadawców). Jeśli dopuścisz jakieś przesyłki od niesprawdzonych nadawców, trochę spamu zawsze się przedrze. Musisz więc rozważyć: stosować nadmierne ograniczenia czy znosić denerwujący *spam*.

Niektóre programy filtrujące blokują nadchodzące wiadomości i wiadomości tekstowe, zawierające wyszczególnione wcześniej słowa i zdania. Choć niewiele programów filtrujących może zablokować nadsyłany tekst, większość z nich może blokować dostęp do innych stron, do których odnośniki są zawarte w spamie. Nawet więc wtedy, gdy nie zablokują samej wiadomości, ustrzegą twoje dziecko od wchodzenia na powiązane strony.

Jeśli poszukujesz specjalnych programów do filtrowania spamu, sprawdź Spam Exterminator. Zawiera on listę znanych spamerów, dzięki czemu blokuje wysłane przez nich e-maile. Spam Exterminator usunie śmieciową przesyłkę, zanim ktoś ją otworzy (wspaniała cecha, gdy idzie o dzieci). Jednak klienci AOL muszą wiedzieć, że nie pracuje on w systemie AOL, który ma własne produkty filtrujące, służące do kontroli e-mailów.

Przede wszystkim musisz nauczyć dzieci ignorowania i usuwania e-mailów wysłanych przez nieznane osoby. Mogą one zawierać nie tylko odsyłacze do stron, na które wolisz dziecka nie wprowadzać, mogą też być zainfekowane wirusami lub wyposażone w specjalny kod, który da hakerowi dostęp do waszego komputera. Mogą pochodzić od kogoś, kogo wolałbyś, żeby nie poznały.

Nasze dzieci mogą nie przejmować się pornografią czy dziwnymi korespondentami, ale bardzo dbają o to, by wirusy nie zniszczyły ich własnych plików i gier i by hakerzy nie dostali się do systemu. Wykorzystaj te obawy jako zachętę do przestrzegania rozsądnych zasad. Stosowny poziom lęku będzie potężną pomocą w uczeniu ich ostrożności. (Sprawę zabezpieczenia przed wirusami szerzej omawiam w rozdziale 3).

Uwaga, obcy! A w Internecie powinieneś kontaktować się z nieznajomymi

Nie pozwalamy, by dzieci prowadziły telefonicznie rozmowy z obcymi osobami, które dzwonią do naszego domu. Ale nieznajomi mogą kontaktować się z dziećmi poprzez kawiarenki, ICQ, e-mail, kluby korespondencyjnych przyjaciół i mieć je na oku dzięki tzw. listom kumpli (*buddy lists*) – a o tym często nie myślimy. W tej części postaram się przedstawić ryzyko stwarzane przez różne formy porozumiewania

się i proponuję, co można zrobić, by mieć pewność, że dziecko używa ich rozsądnie.

Możliwość skontaktowania się i „rozmawiania" z innymi w sieci to jedna z najwspanialszych ofert Internetu. Ale może być również najbardziej ryzykowna. Źródłem największych niebezpieczeństw, które grożą dzieciom w cyberprzestrzeni, są nieznajomi ludzie, nie informacje. Zawsze, gdy dzieci mają możliwość kameralnego (w cztery oczy) kontaktu z kimś, kogo nie znają (ani one, ani wy) z realnego życia, są narażone na szczególne ryzyko.

Prawdziwe niebezpieczeństwo wynika ze spotkania się z ludźmi w realnym świecie.

Ale nie wpadaj w panikę. Pamiętaj, że technologia nie pozwala jeszcze na to, żeby zarośnięty, uzbrojony napastnik wtargnął do twojego modemu i wciągnął tam dziecko. W większości wypadków, jeśli dochodzi do spotkania twarzą w twarz, twoje dziecko musi tego chcieć.

I tak właśnie powstają prawdziwe problemy. Związane z Internetem molestowanie nie polega na tym, że uwodziciel nocą wkrada się do twojego domu. Większość ofiar z własnej woli spotyka się z napastnikiem w realnym świecie. Mogą nie być świadome jego prawdziwego wieku czy intencji, ale są świadome, że mają spotkać się z kimś twarzą w twarz. Wiele ofiar to zakochane nastolatki. Więc edukacja odgrywa tu niezmiernie ważną rolę. Musimy uprzedzić nasze dzieci o możliwych zagrożeniach, by mogły ich unikać. To jest najważniejsza sprawa. (Co powinny wiedzieć dzieci i nastolatki, powiem w różnych miejscach tej książki, a zwłaszcza w rozdziale 7).

❖ Kawiarenki (*chatrooms*)

Często rozmawiam z dziećmi o tym, co robią w sieci. Wszystkie mówią mi, że najbardziej lubią pogawędki – czaty i wysyłanie wiadomości za pomocą komunikatora internetowego (*instant messages*). Mówiły też, że lubią gadać z kolegami ze szkoły. Najwyraźniej rozmowy za pośrednictwem komputerów są dla tego pokolenia ekwiwalentem rozmowy telefonicznej. My dzwoniliśmy do kolegów z klasy natychmiast po powrocie ze szkoły; oni łączą się poprzez Internet. Im bardziej wszystko się zmienia, tym bardziej pozostaje takie samo.

Co to jest kawiarenka?

Kawiarenki to miejsca w sieci, gdzie wiele osób może rozmawiać ze sobą w czasie rzeczywistym. To tak jak wielkie telefoniczne przyjęcie, do którego możesz się przyłączyć dzwoniąc. Kawiarenki [coraz popularniejsze staje się określenie czaty – przyp. tłum.] istnieją w serwisach usług internetowych (takich jak AOL, która ma ponad piętnaście tysięcy kawiarenek), w specjalnych serwisach opartych na sieci stron WWW, w różnych portalach, które mają własne kawiarenki tylko dla zarejestrowanych członków. Są wreszcie grupy dyskusyjne na IRC (Internet Relay Chat, do którego dostęp wymaga specjalnego oprogramowania. Na IRC określa się je jako kanały).

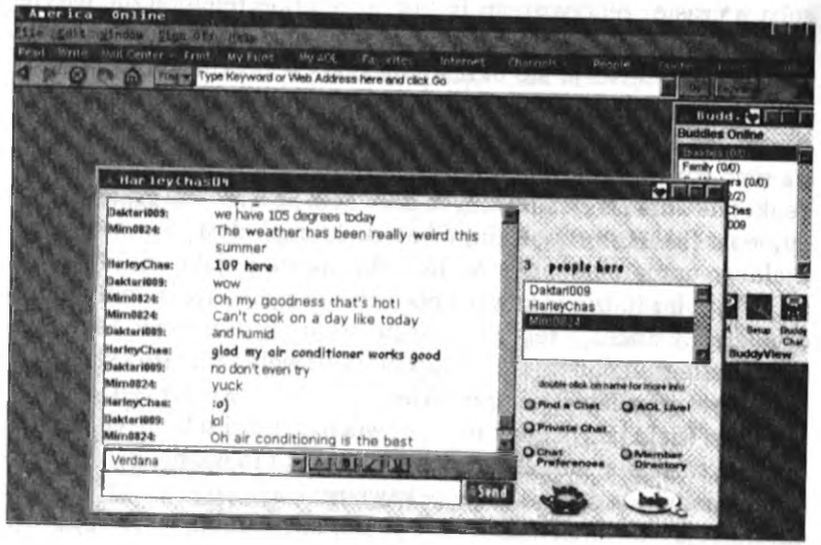
Gdy jedni ludzie w kawiarence ochoczo rozmawiają, inni po prostu patrzą i słuchają tego, o czym się mówi i kto co mówi. Takich ludzi określa się mianem „przyczajeni", a przyglądanie się i słuchanie zamiast rozmawiania to „przyczajenie". Czasem wiadomo o ich obecności, bo wiele kawiarenek przedstawia listę ludzi zebranych, w przeciwnym razie nie zauważa się ich obecności. (To ważne, bo wielu cybernapastników przyczaja się w kawiarenkach, po cichu gromadząc informacje o naszych dzieciach. I ponieważ nie robią nic, co by zwróciło na nich uwagę innych, nikt ich nie dostrzega, z moderatorami włącznie).

Wiele kawiarenek jest zorganizowanych tematycznie. Najczęściej nazwa kawiarenki lub kanału wskazuje na dominującą tematykę. Istnieje dużo grup o wojowniczych nazwach, niemało ma w nazwie coś związanego z uczuciami, z dodatkiem słówka cyber (to cyberokreślenie dla rozmów o cyberseksie, który polega na tym, że ludzie angażują się w rozmowy i rysunkowe fantazje seksualne). To prawdopodobnie w dużym stopniu przydaje im popularności. (Na IRC proponują takie tematy jak: „seks między ojcem a córką", „piractwo oprogramowania" i „porno z dziećmi między 4 a 6 rokiem życia". Dlatego właśnie jestem zdania, że dzieci należy trzymać z daleka od IRC).

Jak one działają?

Nieważne, gdzie znajdziesz swoją kawiarenkę, wszystkie działają na podobnych zasadach. Każdy pisze na klawiaturze to, co chce powiedzieć (tak właśnie rozmawia się w sieci), a inni zebrani odpowiadają. Czasem bywa to nieźle pogmatwane, bo napisane teksty ukazują się na ekranie w takiej kolejności, w jakiej zostały wysłane.

Grupy dyskusyjne są mniej lub bardziej liczne, od dwóch do kilkuset osób (w niektórych kanałach IRC).



Czy możesz kontrolować obecność w kawiarence?

Niektóre kawiarenki są publiczne, otwarte, i każdy może tam wejść. Inne są prywatne, zamknięte, i mogą do nich wejść tylko zaproszeni goście, podając hasło (*password*). Dzieci, a zwłaszcza nastolatki, chętnie tworzą zamknięte grupy dla kolegów ze szkoły, klubu sportowego, harcerstwa itp. Mogą wtedy porozmawiać we własnym gronie.

Pedofile również mają wiele prywatnych miejsc spotkań. (Jest ich więcej, niż mogłoby się niektórym z nas wydawać). Zazwyczaj zapraszają dziecko do wejścia, wysyłając osobiste zaproszenie. Częstokroć dzieci godząc się, wiedzą, że wchodzą do pedofilskiej grupy dyskusyjnej. (Z jakichś powodów kawiarenki są używane częściej, gdy pedofile wabią chłopców niż dziewczęta. Zazwyczaj mają też one homoseksualny temat, np. miłość między chłopcem a mężczyzną).

Akronimy

Ze względu na tempo pogawędek w sieci wprowadzono specjalne skróty dla często używanych słów i zwrotów. Jeśli ich nie poznacie,

stracicie większość z tego, co się dzieje na czacie i każdemu dacie poznać, że jesteście tam nowicjuszami.

Akronimów używa się też często po to, by skrócić pisanie.

A teraz mały quiz! (Tylko żartuję. :->). (Te znaczki to uśmieszek albo *emoticon* – powiem o tym w rozdziale 7 w punkcie o netykiecie: „Netykieta – uczenie dziecka poprawnego zachowania w Cyberprzestrzeni". Obróć stronę o 90 stopni, a zobaczysz uśmiechniętą twarz, co oznacza, że żartuję).

Czy ktoś pilnuje tego interesu?

Choć ogólne zasady netykiety zazwyczaj stosują się również do kawiarenek, dodatkowo obowiązują tam zasady uczestnictwa ustalane przez gospodarza (operatora) kawiarenki lub kanału, a te często nie są ściśle przestrzegane, dopóki ktoś nie zaprotestuje.

Niektóre kawiarenki są monitorowane, ale większość nie. Kiedy są monitorowane, to na ogół przez *bots* lub przez żywych ludzi. *Bots* to specjalne programy, które rejestrują, co się dzieje na czacie. Choć nie mogą spełnić zadań, do których nie zostały zaprogramowane, mogą wymusić przestrzeganie zasad udziału, wyrzucając gości, którzy te zasady łamią. Używane są głównie do monitorowania języka, jakim posługują się rozmówcy. Ale gdy chodzi o kontrolowanie aktywności – nic nie zastąpi prawdziwego, żywego „czatowego policjanta". Są oni przyzwyczajeni do tego, co dzieci mówią i jak mówią. Tylko doświadczony „policjant" nadąży za nimi. „Policjantami" bywają rodzice wolontariusze lub opłacani profesjonaliści.

Nadużywanie kawiarenek

Ten podrozdział zapewne mogliby napisać sami rodzice. Dotyczy on niestosownego zachowania się dzieci i nastolatków w kawiarence. A są tego niezliczone sposoby.

Kiedy wiedzą, że są monitorowani, używają wulgarnych słów, wyrażeń i zdań, próbując, czy zdołają przemknąć się przez sito. Kiedy monitorujący się podszkoli, dzieci tworzą nowe słowa, w nadziei, że znowu wyprowadzą go w pole.

Obrażają siebie nawzajem, a kiedy język staje się zbyt gorący, wracają do starych, wypróbowanych wyzwisk typu: „ty śmierdzielu". (Okazuje się, że to działa niezależnie od pokolenia).

Włóczą się w grupach, niektórzy są „banitami", inni należą do „paczki", zupełnie jak w szkole. Mówią głupstwa, rozmawiają o takich rzeczach, o których pewnie wolelibyśmy nie wiedzieć, i flirtują. Czasami nie obchodzi ich, czy osoba, z którą flirtują, jest dorosła, czy jest to inne dziecko. Bo to jest ubaw. Wszystko jest grą – chłopcy udają, że są dziewczynami, dziewczyny udają, że są chłopcami, a każdy udaje, że jest ważniejszy i starszy niż jest. (Oprócz dorosłych, którzy chcą być młodsi niż są, szczuplejsi i, jeśli chodzi o dorosłych mężczyzn – mieć bujniejsze włosy).

Jednak ponieważ nie ma niezawodnego sposobu, by nie dopuścić do wchodzenia dorosłych do najlepiej nawet zabezpieczonych kawiarenek dla dzieci (bo w sieci każdy może być tym, kim zechce), dzieci muszą wiedzieć, że może tam być ktoś, kto się im przygląda z wielkim zainteresowaniem. I na ogół nie zdradza swojej obecności, kiedy patrzą kontrolujący. Siedzi cicho i uważnie obserwuje dzieci. (Więcej na ten temat w rozdziale 4).

Rodzice patrzą... I inne tajne kody

Dzieci wiedzą, że rodzice mogą próbować kontrolować ich rozmowy i obserwować, o czym się mówi w kawiarence. Wiedzą, że większość rodziców nie zrozumie nawet połowy z tego, co się tam dzieje. Opracowały więc specjalne akronimy, by ostrzec innych, że rodzice czy inne „niepowołane" osoby kręcą się w pobliżu.

Co można z tym zrobić?

Gdy chodzi o nastolatki i starsze dzieci, powinieneś nalegać, by odwiedzały wyłącznie kawiarenki monitorowane przez realne, żywe osoby, nie przez *bots* (czyli specjalne programy). Zalecałabym także zakaz używania IRC, który ciągle uważany jest za Dziki Zachód Internetu. Nawet gdy dzieci są starsze, lepiej upewnić się, że używają „czystych" kanałów IRC.

Musisz także sprawdzić, czy monitorowane kawiarenki są nadzorowane przez całą dobę, czy tylko w określonych godzinach. Wielu rodziców skarżyło mi się, że wybrali jakieś określone miejsce do pogawędek dla dziecka tylko dlatego, że było monitorowane, a potem odkrywali, że jest monitorowane tylko w pewnych godzinach. Większość odpowiedzialnych kawiarenek informuje o godzinach otwarcia

i monitoringu. Co rozsądniejsze serwisy dla dzieci wymagają od swoich operatorów, by zamykali kawiarenkę, gdy osoba monitorująca jest nieobecna.

Powinieneś nauczyć się, jak zapisywać wszystkie rozmowy i nauczyć tego również swoje dziecko. Można zrobić kopię rozmów w kawiarence i kanale, w którym przebywasz. Kiedy zdarzy się coś złego, taki zapis będzie miał nieocenioną wartość w zrekonstruowaniu wydarzeń. Każdy program działa nieco inaczej, więc musisz zwrócić się do pakietu pomocy danego serwisu czatowego, by dowiedzieć się, jak uruchomić zapisywanie. Nie potrzebujesz do tego żadnego specjalnego oprogramowania, bo większość aplikacji czatowych ma wbudowaną taką opcję.

Kluczem do zachowania bezpieczeństwa twoich dzieci podczas czatowania jest nauczenie ich, by nie przekazywały nikomu w sieci danych osobowych. Ale mimo nauk niektóre dzieci przekazują więcej informacji, niż jest to bezpieczne. Jeśli próbowałeś wszystkiego, a twoje dzieci nadal podają zbyt wiele informacji, istnieją programy służące do zablokowania określonych wiadomości wychodzących, takich jak nazwisko, adres, numer telefonu. Ale powinieneś wiedzieć, że dzieci potrafią też „oszukiwać" programy blokujące – zamiast napisać swoje nazwisko po prostu: Jan Nowak, mogą zapisać je tak: J*****A*****N i litera następująca po M****N****U i litery A****K. Potrafią to samo zrobić z numerami telefonów, adresami i innymi informacjami, o których nieujawnianie prosimy. Jedyny sposób, by mieć pewność, że zatrzymamy je podczas akcji, jest użycie programów takich jak: Cyber Snoop lub Disc Tracy, które przechwytują wszystkie informacje i pozwalają zobaczyć dokładnie, słowo po słowie, co dzieci mówią w Internecie. (Ale wiele osób ma poczucie, że to straszne narzędzie. Jeśli się na nie zdecydujesz, powinieneś ostrzec swoje dzieci, że stosujesz oprogramowanie monitorujące ich poczynania w sieci, inaczej będzie to jak czytanie ich pamiętników).

Omawiam dokładniej te i inne programy służące rodzicielskiej kontroli w rozdziale 8. Pamiętaj jednak, że nastolatki i dzieci nienawidzą programów kontrolujących każde ich słowo. Odbierają je jako ingerencję w sferę prywatności. A ja nie jestem pewna, czy się z nimi nie zgadzam.

❖ E-mail – poczta elektroniczna

Co to jest e-mail

Wstąp do klubu. Wyślij komuś wiadomość przez Internet. To jedna z prostszych rzeczy, które można robić w sieci. Jest też jedną z najpopularniejszych. Każdy posługuje się tym w domu, w szkole, w pracy. Poczta jest używana o 150% częściej niż strony WWW. Chcesz posłać kartkę swojej siostrze? Wyślij ją e-mailem. Chcesz wysłać mężowi kopię świadectwa szkolnego córki? Masz fotografię nowo narodzonego dziecka, którą chciałbyś pokazać całej rodzinie? Masz... więc wysyłasz e-mailem!

A najprzyjemniej jest, gdy odpisują. To natychmiastowa nagroda. Szybko okazuje się, że nie ma przyjemniejszego sygnału niż sygnał: „Dostałeś pocztę!", kiedy włączasz się do AOL. (Moja 5-letnia siostrzenica ciągle to śpiewa, gdy rodzice siadają do komputera).

E-mail to wiadomość, którą wysyłasz komuś przez Internet. Dociera do adresata w ciągu dosłownie paru sekund, chyba że Internet jest szczególnie przeładowany. I nie idzie dłużej do osoby po drugiej stronie globu niż do kogoś mieszkającego po drugiej stronie ulicy. Mieści się to w ramach opłat za dostęp do Internetu. (Nie zwracaj uwagi na plotki o rychłym nałożeniu podatków na usługi pocztowe. Niektóre nowe serwisy pocztowe znajdujące się w Internecie na stronach WWW także są darmowe).

E-mail to wspaniały sposób na pozostawanie w kontakcie z geograficznie odległymi krewnymi i przyjaciółmi. Pozwala ludziom wysyłać wiadomości, kiedy chcą i odpowiadać, kiedy mogą.

Jak to działa?

Twój dostawca usług internetowych lub serwis sieciowy dostarczy ci oprogramowanie, którego częścią jest program e-mail. Należy go skonfigurować. (Nie pobiera się dodatkowych opłat za to oprogramowanie). Serwisy usług sieciowych automatycznie konfigurują twój e-mail, tak że możesz odbierać i wysyłać wiadomości, gdy tylko uzyskasz dostęp do Internetu. Gdy korzystasz z Internetu poprzez ISP, nie jest to tak łatwe, bo wymaga skonfigurowania przeglądarki. To bolesny etap, ale gdy zostanie pokonany, poczta elektroniczna jest bardzo łatwa w obsłudze.

Wytrzymaj jeszcze chwilę, a obiecuję, że nawet się nie zorientujesz, kiedy skończymy z tym galimatiasem.

Jeśli znasz kogoś, kto potrafi skonfigurować twoją przeglądarkę, to dobry moment, żeby zadzwonić do niego i błagać o pomoc – drobny bakszysz mile widziany. (Myślę, że Prince Polo, Wafelki Teatralne i batoniki Mars są bakszyszem z wyboru dla komputerowych „znawców"). Poproś też tę osobę o wprowadzenie hasła e-mailowego, byś miał dostęp do swojego konta pocztowego. (A jak już jest, to może niech przy okazji ustawi zegar na twoim magnetowidzie).

Jeden produkt, który testowaliśmy, Serf Monkey, potrafi nawet głośno czytać dziecku wiadomości, używając programów rozpoznających głos. Więc dzieci mogą odbierać listy od zaakceptowanych nadawców, zanim jeszcze nauczą się czytać. (Więcej na ten temat możesz dowiedzieć się z rozdziału 8).

Skrzynka pocztowa

Każdy adres poczty elektronicznej składa się z dwóch części – nazwy użytkownika skrzynki i nazwy serwera, które przedzielone są znakiem @ (małpa). Mój adres brzmi: parry@aftab.com, gdzie „parry" to nazwa użytkownika, a aftab.com to nazwa serwera. Ale wielu ludzi korzystających z serwisów internetowych zazwyczaj używa tylko swojego imienia czy nazwiska i imienia osoby korzystającej z tego samego serwisu, by wysłać wiadomość, opuszczając @ i nazwę domeny. Tych skróconych adresów mogą używać tylko osoby podłączone do tego samego systemu e-mailowego. Jeśli obydwaj korespondenci należą np. do AOL, podają tylko imię i nie muszą dodawać „@aol.com". Serwer domyślnie przyjmuje, że wysyłasz wiadomość do kogoś korzystającego również z tego samego systemu, jeśli nie podasz innej nazwy serwera. To tak jak z podawaniem adresu komuś, o kim wiesz, że mieszka w tym samym mieście. Podajesz nazwę ulicy, pomijając nazwę miasta. Ale to nie zadziała, jeśli wysyłasz list do kogoś spoza systemu AOL.Twoje listy są przesyłane do serwera ISP. To tak jak wrzucanie wszystkich listów do skrzynki pocztowej lokalnej poczty. Zamiast wyjmować listy osobiście ze swojej skrzynki, wysyłasz program komputerowy, żeby to zrobił za ciebie. (Gdybym go jeszcze potrafiła wyuczyć, jak przynosić do domu tradycyjne listy, nie musiałabym wcale wstawać z fotela). Możesz trzymać swoje listy na e-mailowym serwerze, by zajrzeć do nich później z innego komputera, możesz je usunąć z serwera po przeczytaniu.

Włączywszy się do Internetu, występujesz o konto e-mailowe. Są to usługi pocztowe oparte na sieci stron WWW. Oznacza to, że nie potrzebujesz specjalnego oprogramowania, by dostać się do swojej skrzynki (używasz przeglądarki internetowej) i masz do niej dostęp z każdego miejsca na świecie, w którym masz dostęp do Internetu. Oferujący darmowe konto e-mail sprzedają powierzchnie reklamowe, by pokryć koszty tych usług. Jeśli jesteś skłonny znieść reklamy, możesz mieć bezpłatną skrzynkę.

Do „zwykłej"skrzynki, przydzielanej wraz z dostępem do Internetu, nie można dostać się z innego komputera, jeśli nie ma on zainstalowanego i skonfigurowanego oprogramowania. To dlatego nowe darmowe systemy pocztowe oparte na sieci stron WWW są tak cenne. Można dostać się do skrzynki z każdego miejsca, z każdego komputera, który ma połączenie z Internetem, używając dowolnej przeglądarki. Z tego właśnie powodu są one tak niebezpieczne dla naszych dzieci. Nasze pociechy mogą otwierać swoje skrzynki, będąc poza domem, w szkole, u kolegi, w bibliotece czy w innym publicznym miejscu oferującym dostęp do Internetu. Jeśli rodzice chcą monitorować ich korespondencję, one spokojnie mogą to obejść, używając opartego na sieci stron WWW konta pocztowego.

Jest wiele sposobów, żeby opublikować twój adres e-mailowy w sieci i udostępnić go ludziom, którzy chcieliby cię znaleźć. (Więcej na temat, jak odnaleźć ludzi w Internecie, podaję w podrozdziale „Największa tablica ogłoszeniowa świata" w dalszej części rozdziału). Upewnijcie się, czy adresy e-mailowe waszych dzieci nie zostały gdzieś opublikowane).

Nadużywanie poczty elektronicznej

Najczęstsze nadużycia poczty elektronicznej to przysyłanie niechcianych reklam i podobnych materiałów; przesyłanie obraźliwych wiadomości, molestowanie i nękanie ofiary, oszustwa (gdy ludzie wysyłają e-maile, podając się za kogoś innego) i pocztowe bomby (czyli wielka liczba e-maili, które zapychają twój system). E-mail jest nadużywany intensywniej niż jakiekolwiek inne narzędzie komunikacji. (Ale szybko gonią go programy przekazywania wiadomości w czasie rzeczywistym).

Reklamy i ogłoszenia to prawdopodobnie najpopularniejsze formy niestosownego korzystania z systemu e-mailowego. „Śmieci" informacyjne zatykają codziennie twoją skrzynkę, przynosząc pornografię i oferty piramid finansowych, dla dorosłych i dla dzieci. Kiedy reagujemy na takie wiadomości, prosząc np. o nieprzysyłanie ich, nasz adres natychmiast zyskuje na rynku nieuczciwych ogłoszeniodawców wyższą cenę, bo wiadomo, że ktoś odbiera wiadomości. To oznacza, że będziemy dostawać więcej śmieci.

Jeśli nie będziemy uważać, e-mail stanie się czymś w rodzaju otwartych drzwi do naszych domów i naszych komputerów. Poczta może być wykorzystana nie tylko do tego, by nas napastować czy obrzucać wulgarnymi wyzwiskami. Wirusy mogą być przesłane jako pliki dołączone do e-maila (a nawet jako jego część). Kiedyś można było zalecać ludziom, żeby po prostu nie otwierali e-mailów od osób, których nie znają, ale od czasów wirusa Melissa wszystko się zmieniło. Ten wirus przybywa udając, że jest wiadomością od przyjaciela. (Wirusy Melissa i Bubble Boy działają tak, że kopiują twoją książkę adresową i przedostają się do figurujących w niej osób, podszywając się pod list od ciebie. Potem dostają się do kolejnej książki adresowej i robią to samo, i tak rozprzestrzeniają się dalej). Bubble Boy może zainfekować twój komputer nawet nie jako plik dołączony, ale ukryty w samej wiadomości.

„Konie trojańskie" umożliwiają hakerom wejście tylnymi drzwiami do twego komputera. Dzięki nim haker może wykraść nasze pliki, dostać się do informacji finansowych, które przechowujemy w komputerze, poznać nasze hasło, a nawet usunąć wszystko z twardego dysku.

Połączenia do pornograficznych stron (prezentujących seksualne zdjęcia nastolatek) mogą dotrzeć do dzieci poprzez e-mail. Dzieci mogą też otrzymywać zdjęcia od osób, z którymi wolelibyśmy, żeby się nie kontaktowały, mogą także wysyłać tą drogą własne zdjęcia. Ponadto poprzez e-mail cyberprześladowcy mogą szykanować nasze dzieci, a dzieci mogą ujawniać obcym dane personalne.

Coraz większym problemem stają się e-mailowe „łańcuszki listowe". Tak jak ich tradycyjne odpowiedniki (różne postacie łańcuszków św. Antoniego) obiecują szczęście, bogactwo lub miłość temu, kto wyśle je do 25 przyjaciół w sieci, a straszą koszmarnymi konsekwencjami tych, którzy ich nie odeślą. Ponieważ tradycyjny „łańcuszek" wymaga przepisania oryginalnego tekstu, włożenia go do koperty zaopatrzonej w znaczki, tylko najbardziej łatwowierni spośród nas je wysyłają. Ale w Internecie, by wyjść naprzeciw losowi, wystar-

czy wcisnąć kilka klawiszy i już wiadomość jest wysłana do kilkudziesięciu osób z książki adresowej. Więc wszyscy je przesyłają. Konsekwencją tej masy listów jest zapchanie serwerów i spowolnienie całego systemu. Są też one zmorą szkolnych sieci komputerowych z dostępem do Internetu.

Ostatnio Maggie (lat 10), jedna z naszych szkolących się przyszłych doradczyń w sprawach ochrony przed zagrożeniami w sieci, przybiegła do rodziców z pobladłą twarzą, zanosząc się płaczem. Zawsze usuwała e-maile wysyłane przez ludzi, których nie znała. Ktoś przysłał jej łańcuszek, w którym straszono, że umrze, jeśli nie prześle go do trzech osób. Usunęła go natychmiast, a kiedy się okazało, że już nie może go odzyskać i wysłać dalej, wpadła w panikę, że umrze. Rodzice przez godzinę uspokajali ją, wyjaśniając, że łańcuszek to zwykłe nabieranie ludzi.

Jeśli zważysz wszystkie zagrożenia i korzyści, to e-mail ciągle pozostaje wspaniałym narzędziem komunikacji. Ale to jedna z usług, które wymagają szczególnego nadzoru i wiedzy o możliwych zagrożeniach związanych z posługiwaniem się nimi.

E-mail powinien być dostępny tylko dla tych dzieci, które mają odpowiednią zdolność oceny, co najczęściej oznacza, że muszą być w określonym wieku. Ten wiek to zawsze sprawa indywidualna, ale na ogół swobodny dostęp do poczty powinien być zabroniony dzieciom poniżej 11 lat. Serf Monkey, darmowa przyjazna dzieciom przeglądarka stron WWW, ma mądry system doręczania e-mailów do skrzynki rodziców. Te, które oni uznają za „czyste", mogą być następnie przekazane do skrzynki dziecka. Inne są usuwane (więcej o tym w rozdziale 8).

Kiedy się wie, jak cennym narzędziem jest Internet, tym smutniej jest, że tak często bywa źle wykorzystywany.

Co na to poradzić?

Często dzieci mają bezpłatne konta e-mail, a my wcale o tym nie wiemy. To źle. Nawet jeśli nie kontrolujemy listów naszych dzieci, zawsze powinniśmy wiedzieć, gdzie mają swoje konta pocztowe i znać hasła. Niektóre z serwisów oferujących darmowe konta pocztowe publikują dane personalne, które podajesz zakładając konto, w książce adresowej członków lub na „białych stronach". Sprawdź, czy nie figuruje tam twoje dziecko.

Wiele programów filtrujących całkowicie blokuje e-maile. Inne mogą filtrować wiadomości tekstowe w listach. Wiele witryn dziecięcych posiada zamknięty system pocztowy, umożliwiający korzystanie tylko z adresów w obrębie tej witryny i sprawdzanie każdej wiadomości. Inne, jak Serf Monkey, przesyłają nagłówki wszystkich listów do skrzynki rodziców, którzy decydują, co może być przekazane dziecku. Jeszcze inne narzędzia rodzicielskiej kontroli pozwalają na zablokowanie listów od wszystkich nadawców, poza wyszczególnionymi wcześniej osobami (te programy mogą więc zablokować i reklamy, i list od ciotki Matyldy). Jest wiele produktów i sposobów radzenia sobie z zagrożeniami, dostępnych dla rodziców. Dokładniej omawiam je w części „Coś z kolumny A, coś z kolumny B".

Oto kilka prostych zaleceń dotyczących korzystania z poczty, które należy zapamiętać:

- Zmieniaj często swoje hasło (i trzymaj je w miejscu, w którym twoje dziecko go nie znajdzie).
- Nikomu nie przekazuj swojego hasła (zwłaszcza dzieciom).
- Nie otwieraj żadnych plików dołączonych do listu, zanim nie zostaną sprawdzone przez program antywirusowy.
- Wyloguj się, kiedy skończysz.
- Nie reaguj na niechciane reklamy, napastliwe lub obraźliwe listy.
- Zachowaj zdrowy rozsądek i zatrzymuj poufne informacje przy sobie.
- Usuwaj, nie otwierając, wszystkie e-maile od osób, których nie znasz.
- Nie daj się złapać na znany chwyt twórców spamu: „nie pamiętasz mnie?".

❖ ICQ i inne serwisy przekazywania wiadomości w czasie rzeczywistym

Co to jest?

Instant messaging to komunikowanie się w czasie rzeczywistym [w Polsce tego typu programy najczęściej określa się nazwą komunikator internetowy – przyp. tłum.]. To usługa łącząca w sobie cechy e-mailu i czatów (bo wysyłasz komuś wiadomość i masz kontakt w czasie rze-

czywistym), tylko lepsza. Wypiera szybko e-mail z pozycji najpopularniejszego internetowego narzędzia komunikacji.

Żeby mieć pewne pojęcie o jej popularności: AOL donosi, że w czerwcu 1999 za pośrednictwem ich serwerów przepływało średnio 63 miliony e-mailów dziennie, w porównaniu z 432 milionami wiadomości przesłanych za pomocą programów typu komunikator.

ICQ to program przekazywania wiadomości i wymiany informacji, który pozwala sprawdzić, czy twoi przyjaciele lub krewni są aktualnie podłączeni do sieci i jeśli są – wysłać im natychmiast wiadomość. (ICQ oznacza: *I seek you* – poszukuję cię). Zostało wprowadzone przez AOL w 1998 roku.Użytkownicy AOL mają serwis o podobnych właściwościach, zwany *instant messages*, w skrócie IM. Oferowany przez AOL Instant Messenger [program typu komunikator internetowy – przyp. tłum.] jest dostępny za darmo dla wszystkich użytkowników Internetu.

AT&T, Microsoft, Mindspring, i Yahoo! również oferują podobne programy, a przyjazne dzieciom portale, jak Headbone, Disney Blast Pad, oferują takie usługi dla dzieci. Ale niezależnie od tego, którego z nich używasz, ten sposób wysyłania wiadomości już jest bardzo popularny i ta popularność stale rośnie.

Jak to działa?

W serwisie ICQ otrzymujesz UIN (Universal Internet Number – Uniwersalny Numer Internetowy), który jest dla tego systemu ekwiwalentem adresu e-mailowego. To dzięki niemu inni mogą cię znaleźć i skontaktować się z tobą. (Możesz nawet włączać się do grup dyskusyjnych i przesyłać dodatkowe pliki, np. fotografie, innym osobom). W AOL twój identyfikator jest adresem dla systemu komunikatora internetowego.

Wysyłanie wiadomości w tym systemie jest łatwiejsze niż wysyłanie normalnych e-mailów, ponieważ wszystkie programy typu komunikator pracują w „tle". To oznacza, że podczas pracy na innych aplikacjach mogą wyrzucić na ekranie wiadomość albo podświetlić specjalną ikonkę na pasku zadań. Różnica między IM a zwykłą pocztą elektroniczną jest taka jak między używaniem pagera a używaniem zwykłego telefonu: IM znajdzie cię wszędzie i przerwie każde zajęcie, choć możesz to zignorować, tak jak pager. Gdy korzystasz z drugiej metody (e-mail), otrzymasz wiadomość tylko wtedy, gdy zajrzysz do skrzynki (to jak podniesienie słuchawki telefonu).

Jak są nadużywane?

Komunikator informuje też innych, że jesteś podłączony do sieci, by mogli kontaktować się „na żywo". To jeden z głównych powodów, dla których ludzie go używają. To także jedno z największych zagrożeń, jeśli chodzi o dzieci. Cybernapastnicy mogą włączyć UIN czy inny identyfikator twojego dziecka do swojej listy ważnych osób (AOL nazywa je *buddy lists* – listy kumpli), dzięki czemu zawsze, gdy dziecko włącza się do Internetu, oni będą o tym wiedzieli. Skontaktowanie się wówczas jest tak proste jak wysłanie wiadomości. (Więcej o „listach kumpli" powiem później).

ICQ ma też dodatkowe możliwości, dostarczające innym jeszcze więcej wiadomości. Użytkownik może być po prostu „podłączony", ale także „nieobecny"; może pracować w trybie „nie przeszkadzać", może być dostępny wyłącznie dla „wybranych rozmów". Są też inne opcje. Poza tym, jeśli użytkownik jest „podłączony", a odchodzi od komputera na kilka minut, program automatycznie przełącza tryb na „nieobecny". To oznacza, że wirtualni prześladowcy mogą nie tylko wiedzieć, kiedy dziecko jest w sieci, ale kiedy komputer jest podłączony do Internetu, a dziecko na kilka minut odeszło od klawiatury.

Co właściwie prześladowca zyskuje, mając taką wiedzę? Może nic, ale może jednak coś – np. wie, że dziecko odeszło od komputera, by przywołać rodzica.W efekcie dziecko przekazuje trochę więcej informacji i traci nieco prywatności.

Na szczęście zarówno ICQ, jak i IM pozwalają przeciwdziałać temu, by inni umieścili cię na swoich „listach kumpli" bez twojej zgody. ICQ pozwala ci zrobić się „niewidzialnym" dla jednego lub więcej użytkowników z twojej listy kontaktów, albo dla każdego. Użytkownicy, wobec których zastosujesz taką opcję, będą cię widzieli zawsze jako osobę pozostającą w danej chwili poza siecią, niezależnie od twego prawdziwego statusu. Doradzam, byś w przypadku, gdy twoje dzieci mają zgodę na korzystanie z ICQ, ustawił tę właśnie opcję, by pomóc im zachować prywatność.

Większość usług natychmiastowego przesyłania wiadomości jest darmowa, ale trzeba zainstalować oprogramowanie i zarejestrować się jako użytkownik.

Kiedy się rejestrujesz, operator prosi o wiele danych personalnych i wystarczy chwila nieuwagi, a informacje te mogą stać się ogólnie dostępne. To oznacza, że dzielisz się informacjami o sobie nawet o tym nie wiedząc.Więc rejestrując się w jakiejś witrynie, upewnij się, że poznałeś stosowane tam zasady ochrony danych osobowych i kliknąłeś na wszystkich okienkach zapewniających poufność podawanych informacji. Poza tym podawaj wyłącznie te dane, które *musisz* podać, nie podawaj tych, których podawanie nie jest konieczne.

Jaka szkoda, że technologia, która mogłaby być tak wspaniałą rzeczą, gdyby używano jej tylko w dobrej wierze, tak często bywa nadużywana i służy niegodziwym celom. Najlepiej wiedzą o tym w AOL i dopuszczają używanie komunikatora internetowego przez dzieci nie młodsze niż nastoletnie. Nie pozwalaj więc posługiwać się tym programem, dopóki dzieci nie są na tyle duże, by używać go ostrożnie i rozsądnie – i gdy możesz mieć pewność, że zastosują się do ustalonych w domu zasad. Poczytaj o zabezpieczeniach, które wprowadziły serwisy dziecięce, by umożliwiać dzieciom bezpieczne korzystanie z programów przekazywania wiadomości. Pamiętaj jednak, że dorośli mogą wejść do większości przeznaczonych dla dzieci miejsc, udając, że są dziećmi, i w ramach takiego serwisu mogą kontaktować się z twoim dzieckiem.

Tak więc nawet w witrynach przyjaznych dzieciom twoje dziecko musi używać czujnika „uwaga, obcy". Upewnij się, że ustawiłeś parametry konta pocztowego dziecka tak, że dane personalne pozostaną poufne, a obce osoby nie będą mogły się z nim kontaktować. Często sprawdzaj nowe rozwiązania dotyczące zachowania bezpieczeństwa i prywatności oferowane przez serwisy dla dzieci. Pojawiają się one stale i warto z nich korzystać.

❖ Listy kumpli (*buddy lists*)

Co to jest?

Listy kumpli to wspaniały sposób, by wiedzieć o poczynaniach przyjaciół mających dostęp do Internetu. Najpierw wprowadziła je AOL, by umożliwić obserwowanie innych użytkowników i pokazywać, kiedy są w sieci, by można się było z nimi skontaktować. Teraz wielu dostawców Internetu i liczne serwisy sieciowe także je

oferują. Większość programów typu komunikator i ICQ korzysta z nich, choć mogą tam występować pod innymi nazwami, jak np. *notifying lists*.

Jak to działa?

Dodanie kogoś do listy kumpli polega po prostu na dopisaniu do tej listy czyjegoś adresu e-mailowego lub identyfikatora. Jeśli sam używasz AOL i trzech twoich przyjaciół też go używa, dodajesz ich identyfikatory do swojej listy i zawsze wiesz, kiedy oni są w Internecie i wtedy możesz im wysłać wiadomość. Jeśli korzystasz z komunikatora w AT&T, możesz dodać do swojej listy innych użytkowników sieci niż korzystający z serwera AOL.

Jakie wspaniałe możliwości. Tylko pomyśl, jakie to mogłoby być cudowne, gdybyś w jakiś sposób został poinformowany o tym, że osoba, do której chcesz zadzwonić, wróciła do domu. A to właśnie sprawia lista kumpli – daje ci znać, kiedy ktoś, kogo szukasz, może odebrać wiadomość lub „pogawędzić".

Poza tym, jeśli umieścisz swoje dziecko na własnej liście, a nie używacie tego samego konta AOL (tylko jedna osoba może go używać w danym czasie), możesz sprawdzić, czy przebywa ono w Internecie, kiedy ty jesteś w pracy. Wtedy zorientujesz się, czy dziecko przekracza ustalone limity czasu korzystania z Internetu. (Tylko uprzedź, że będziesz je kontrolować).

W jaki sposób listy kumpli mogą być nadużywane?

Wszystkie osoby podglądające innych, zabawiające się wysyłaniem im obraźliwych czy denerwujących wiadomości, i uwodziciele uwielbiają listy kumpli. Tak jak normalny użytkownik może sprawdzić, kiedy jego przyjaciele są w sieci, ci osobnicy, posługując się aplikacją „lista kumpli", też wiedzą, kiedy twoje dziecko jest w sieci. Mogą w profilach użytkowników wyszukać potencjalną ofiarę i po prostu umieścić jej identyfikator na swojej liście kumpli. Kiedy dziecko wchodzi do sieci, program informuje o tym tych facetów, a wtedy oni mogą rozpocząć dokuczanie, uwodzenie, molestowanie lub hakowanie.

Co można na to poradzić?

Przede wszystkim upewnij się, że skorzystałeś z tych opcji ochrony prywatności, które nie pozwalają innym umieścić twojego dziecka na ich listach kumpli. Zwłaszcza w przypadku młodszych dzieci jedynymi osobami, które mogą mieć prawo umieszczenia twego dziecka na swoich listach, są ci, których znasz i którym ufasz w realnym świecie.

Jeśli ktoś niepowołany kontaktuje się z dzieckiem i podejrzewasz, że może je śledzić w sieci, zablokuj odbieranie wiadomości od tej osoby (albo, zależnie od programu, którego używasz, umieść taką osobę na swojej liście „zignoruj") i upewnij się, że opcje ochrony prywatności są ustawione na najbardziej restrykcyjną wersję.

Powinieneś także wiedzieć, kto znajduje się na liście kumpli twojego dziecka. Sprawdź, czy wszystkich znasz osobiście, uważnie przeglądając listę i pytając dziecko o każdego.

Upewnij się ponadto, że osoby figurujące na liście są rzeczywiście tymi, za które twoje dziecko je uważa. Powszechnym błędem popełnianym przez dzieci jest umieszczanie na liście kumpli tylko imion przyjaciół, bez ich pełnego e-mailowego adresu, w rezultacie wpisują nie wiadomo kogo na swoją listę, wcale sobie tego nie uświadamiając.

❖ Kluby korespondencyjnych przyjaciół

Co to jest internetowy klub korespondencyjnych przyjaciół?

Programy korespondencyjnych przyjaźni umożliwiają dzieciom znalezienie w sieci innych osób mających takie same zainteresowania i korespondowanie czy pogawędki z nimi, nawet jeśli mieszkają w najodleglejszych zakątkach kuli ziemskiej. Są one szczególnie popularne, gdy w szkole przygotowuje się prace domowe z zakresu geografii. KidsCom (najpopularniejszy dostawca programu korespondencyjnych przyjaciół) jest w stanie powiedzieć, kiedy jakiś temat jest zadawany, bo setki dzieci z jednej szkoły wysyłają w tym samym czasie wiadomość o poszukiwaniu korespondenta z określonego kraju. „Pomocy! Jaki jest wasz dochód narodowy brutto i główne bogactwo naturalne?" – to typowy list, jak podaje KidsCom.

Jak one działają?

Istnieją dwa sposoby znajdowania programów korespondencyjnych przyjaźni. Poprzez strony WWW, takie jak KidsCom (www.kidscom.com), albo poprzez szkolne programy, powstające w ten sposób, że szkoła przyłącza się do sieci szkół z całego świata, które biorą udział w programach nawiązywania korespondencyjnych przyjaźni. Większość przyjaznych dzieciom programów posługuje się anonimowymi identyfikatorami internetowymi i ostrzega dzieci przed przekazywaniem danych personalnych, które pozwolą ustalić ich tożsamość.

Jak są nadużywane?

Wielu z nas miało korespondencyjnych przyjaciół, kiedy dorastaliśmy. (Ja miałam kilkanastu, ale nigdy nie odpisywałam na czas, więc żadna znajomość nie trwała długo). Ale internetowe korespondencyjne przyjaźnie to inna sprawa. Może dlatego, że nie wiemy, gdzie naprawdę „przyjaciel" mieszka, gdy korespondujemy z nim w Internecie. Ktoś, o kim myślisz, że jest gdzieś w bezpiecznej odległości, np. w Hongkongu, może mieszkać na tej samej ulicy. A nawet jeśli mieszka w Hongkongu, podróże międzykontynentalne to dzisiaj zwykła sprawa. Tak czy inaczej, korespondencyjne przyjaźnie w Internecie są inne. Programy korespondencyjnych przyjaciół mogą być bogatym źródłem potencjalnych ofiar dla cyberprzestępców. Nigdy nie wiesz, z kim prowadzisz korespondencję. A przecież nawet dzieci, które mają zakaz wysyłania e-mailów do obcych, wchodzenia do niemonitorowanych grup dyskusyjnych i kawiarenek, używania programów ICQ lub komunikatów, mogą mieć internetowych korespondencyjnych przyjaciół i nikt się tym nie martwi.

Co można na to poradzić?

Dopóki ktoś nie wymyśli technologii, która pozwoli nam z całą pewnością wiedzieć, z kim korespondujemy, dzieci powinny mieć dostęp tylko do szkolnych programów nawiązywania znajomości. Chodzi o sytuację, gdy klasa lub szkoła zawiera porozumienie z inną klasą lub szkołą w innym województwie czy kraju. Jedyny sposób, by wiedzieć, że dziecko jest rzeczywiście dzieckiem, to zapytać o to w szkole. Jeśli szkoła potwierdzi udział dziecka w klubie korespondencyjnych przyjaźni, wtedy korespondowanie jest bezpieczne.

Nie zalecałabym rodzicom, by pozwalali dzieciom włączać się do innych programów korespondencyjnych przyjaźni, nawet do tych tworzonych w przeznaczonych dla dzieci witrynach, jeśli rodzice nie kontrolują całości korespondencji. Nawet i wówczas upewnij się, że klub korespondencyjnych przyjaciół nie ma pełnego adresu e-mailowego twojego dziecka. Załóż oddzielne konto (bezpłatne usługi e-mail, takie jak hotmail, są bardzo dobre do tego celu) wyłącznie na potrzeby korespondencyjnych przyjaźni. Tym sposobem, jeśli będzie się działo coś niedobrego, po prostu zamkniesz konto.

Dzieci powinny przystępować do otwartych programów nawiązywania korespondencyjnych przyjaźni wtedy, gdy rodzice stwierdzą, że są dość duże, by stosować się do określonych zasad i wiedzieć, jak zachować się wobec awansów czynionych przez różnych cybernapastników.

Kiedy uznasz, że są już dość duże, KidsCom (www.kidscom.com) ma dobry program, do którego przystąpienie wymaga zgody rodzica. Uczestniczą w nim dzieci ze 121 krajów, co daje szanse na znaczną różnorodność grup. Ale nie zapominaj, że każdy w sieci może udawać, że jest dzieckiem, i zarejestrować się jako dziecko w dziecięcych witrynach. Więc spotkanie kogoś w miejscu przeznaczonym dla małolatów nie jest gwarancją tożsamości.

Zatem nawet jeśli dziecko przystępuje do programu korespondencyjnych przyjaźni w serwisie, któremu ufasz, powinieneś mieć wgląd w korespondencję (ale zawsze uprzedź dziecko o swojej kontroli). Poza tym często rozmawiaj z dzieckiem o jego wirtualnych przyjaciołach. Otwarta, szczera komunikacja między dzieckiem a rodzicami stanowi zaporę nie do przebycia dla cybernapastników.

Największa tablica ogłoszeniowa świata

Wiele informacji wrzucamy do cyberprzestrzeni po prostu zapominając kliknąć opcję poufności lub udzielając więcej informacji, niż jest to konieczne. Istnieją jeszcze trzy inne sposoby, w jakie dzieci nieświadomie mogą przekazać informacje o sobie: wysyłając profil użytkownika, wypełniając różne formularze konkursowe i zgłoszeniowe oraz tworząc własną stronę WWW. Istnieją też inne bazy danych, które mogą mieć adres dziecka, numer telefonu, adres e-mail.

Wiedza o tym, jak niechcący dzieci przekazują informacje w sieci i jak łatwo obcy mogą wyszukać informacje o nich, to jedna z najważniejszych rzeczy, które chciałabym rodzicom przekazać w tej książce.

❖ Profil użytkownika – ogłoszenie w poszukiwaniu kłopotów

Co to jest?

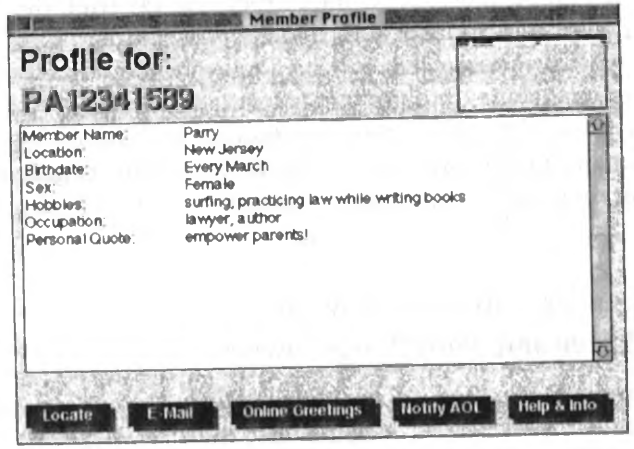
Profil to lista osobistych cech, którą określone serwisy pozwalają wysłać, dzięki czemu inni subskrybenci mogą więcej dowiedzieć się o tobie, twoich zainteresowaniach itp. Profile pomagają ci znaleźć w sieci inne osoby mające podobne zainteresowania. Pomaga to także innym odnaleźć ciebie (lub twoje dziecko).

Jak działają profile?

Profile są często oferowane jako opcja przez dostawców usług internetowych i bezpłatnych kont pocztowych. Program zadaje ci pytania, ty na nie odpowiadasz, a odpowiedzi są „widoczne" dla innych. Zazwyczaj są tam pytania o wiek, płeć, miejsce zamieszkania. (Na ogół są to pierwsze pytania zadawane nowicjuszom w kawiarenkach).

W jaki sposób profile mogą być nadużywane?

Oto typowy wygląd okna „profil klienta":



Wiele naiwnych dzieci bez zastanowienia podaje w profilu swoje prawdziwe nazwisko i inne dane. Profile można odnaleźć w sieci za pomocą programu wyszukującego. Dzięki temu znajdziesz inne osoby zainteresowane np. jazdą na rowerze czy muzyką określonego zespołu. Ale mogą też być źle używane. (Nie jesteś tak naprawdę zdziwiony. Teraz już orientujesz się trochę w działaniu Internetu).

Ludzie, którym nie leży na sercu dobro twojego dziecka, przeglądają daty urodzenia, dzięki czemu mogą znaleźć dzieci czy nastolatki urodzone w określonym roku. Wyświetlają się wówczas profile wszystkich dwunasto- czy trzynastolatków. Poszukują dalej pod kątem płci, miejsca zamieszkania, co pozwala im znaleźć dokładnie to, czego szukają, w dogodnej dla nich lokalizacji.

Czasem, mimo że dzieci są ostrożne w przekazywaniu informacji o sobie, przekazują zdania prowokujące lub obrażające innych. Nastolatki często robią sobie nawzajem głupie żarty, używają haseł kolegów, by wejść na stronę z ich profilem, i dopisują tam jakieś prowokujące informacje. (A w sieci prowokujące rzeczy nie muszą długo czekać na czyjąś odpowiedź). To dlatego musimy nalegać, by dzieci nie przekazywały swoich haseł nikomu, nawet kolegom (albo zwłaszcza kolegom!).

Co można na to poradzić?

Najprostszym rozwiązaniem jest zakaz wypełniania profilów. Drugie dobre wyjście to sprawdzanie, czy profile, które wysyłają, nie zawierają danych osobowych, takich jak prawdziwe nazwisko, adres, nazwa szkoły, klubu sportowego, data urodzenia czy wiek (lepiej, żeby mówiły, w której są klasie) lub jakichś prowokujących informacji. Należy sprawdzić to, co chcą wysłać, i upewnić się, że zawartość jest odpowiednio ogólna i nie ma tam nic skandalicznego.

Jeśli już wysłały jakieś profile, odszukaj je i poproś, by zmieniły wszystkie informacje niestosowne, prowokujące lub mogące posłużyć do zidentyfikowania ich w realnym świecie. I często sprawdzaj te okna.

❖ Wypełnianie formularzy w sieci – przekazywanie danych osobowych

Wyczerpująco zajmuję się problemem prywatności w Internecie w rozdziale 4. Musisz mieć świadomość, że dzieci ciągle wypełniają

formularze, startując w licznych konkursach, rejestrują się w różnych miejscach, wysyłają wiadomości. Upewnij się, że nauczyłeś je, by najpierw uzgadniały wszystko z tobą, by wysyłały formularze tylko do określonych witryn, dbających o ochronę prywatności. Jeśli twoje dziecko nie ma 13 lat, nowe prawo wymaga od witryny, by uzyskała zgodę rodziców.

❖ Własne strony WWW dzieci

Wielu dostawców usług internetowych, wiele serwisów sieciowych i różne portale dają za darmo możliwość stworzenia strony WWW każdemu, kto chce. Dla dzieci to okazja do twórczej działalności i wyrażenia swoich opinii. Nauczyciele często zachęcają uczniów do tworzenia własnych stron WWW.

Jak to bywa nadużywane?

Dzieci zazwyczaj tworzą strony, które mówią o nich więcej niż należy. Wymieniają nazwy szkół, klubów sportowych, czasem nawet numery telefonów, fotografie i adresy. Prawie zawsze dołączają adres e-mail.

Jedyną pociechą pozostaje to, że osobiste strony są trudne do odszukania, bo normalnie nie są rejestrowane na wyszukiwarkach, czyli są zbyt zaciemnione, by je zlokalizować. A im trudniej tobie taką stronę odnaleźć, tym mniejsze prawdopodobieństwo, że uda się to innym.

Jeśli twoje dziecko tworzy własną stronę, obejrzyj ją – nie jako rodzic policjant, ale dlatego, że może ci to pokazać, jak twórcze jest twoje dziecko, może ci dużo o nim powiedzieć. Zobacz, czy nie ma tam jakichś niepotrzebnych informacji osobistych. A zwłaszcza, czy nie ma informacji umożliwiających osobisty kontakt. Jeśli treść strony nie daje możliwości ustalenia, kim jest dziecko i jak się z nim kontaktować, być może są tam fotografie? Innymi słowy, przeanalizuj stronę pod kątem zawartych informacji. Czy za ich pomocą można „namierzyć" dziecko w realnym świecie? Myśl naprawdę intensywnie. Czasem zostawiamy ślady, które po zsumowaniu mogą doprowadzić do nas.

Czy wiesz, jakie informacje naprawdę zostały przekazane i mogą zostać złożone razem? Oto, jak możesz to ustalić.

❖ Halo, informacja? Chcę się dowiedzieć, co wiecie o moim dziecku

Istnieje w sieci kilkanaście książek adresowych, które zawierają adresy e-mailowe i, w niektórych przypadkach, adresy domowe i numery telefonów. To tzw. białe strony. Informacje pochodzą z normalnych publicznych książek telefonicznych, z dobrowolnie tworzonych list i z wyszukujących je specjalnych programów. Jeśli dziecko chce, by każdy mógł z nim nawiązać kontakt, wpisuje e-mail albo adres domowy do którejś z tych książek.

Niektóre z bezpłatnych serwisów e-mailowych również tworzą książki adresowe członków, ale tam informacje mogą nie być tak bogate jak w książkach adresowych dostępnych poprzez wyszukiwarki. Książki adresowe ICQ i komunikatora internetowego mogą być zaskakująco niebezpieczne, bo zawierają wiele informacji, co do których dziecko może nawet nie wiedzieć, że stały się publiczne.

Mimo że w prawdziwym świecie dziecko może być ostrożne w udzielaniu osobistych informacji, w sieci są sposoby, by używając okruchów informacji, zdobyć więcej danych o określonej osobie. Na przykład, jeśli dziecko podało gdzieś numer telefonu, prawdopodobnie można odszukać adres na białych stronach. Czasem przy rejestracji w niektórych internetowych książkach adresowych adres e-mail jest podawany razem z innymi informacjami, np. z numerem telefonu. Jest kilkanaście witryn, które umożliwiają ustalenie innych danych osoby, której telefon znamy. Po prostu wpisuje się numer telefonu i wyskakuje nazwisko osoby i jej adres, z wygodnymi odsyłaczami do stron wyszukujących adres e-mail i pokazujących mapę z drogą dojścia do jej domu. Jeśli telefon jest zastrzeżony, prawdopodobieństwo, że coś takiego się zdarzy, jest mniejsze.

Istnieje także możliwość wyszukiwania w odwrotną stronę. Wprowadzasz adres e-mailowy interesującej cię osoby i otrzymujesz inne informacje o niej. (Szukaliśmy mnie, ale nic nie znaleźliśmy, więc może nie jest to na razie tak naprawdę poważny problem, bo przecież mój e-mail i służbowe telefony widnieją na setkach stron). Mimo wszystko uważam, że warto to sprawdzić. Jedna z witryn pozwala przeglądać kilkanaście baz danych jednocześnie. To dobre miejsce, żeby zacząć.

Co można na to poradzić?

Możesz sprawdzić i zobaczyć, czy twoje dziecko jest gdzieś wymienione i usunąć stamtąd informacje o nim.

Jeśli dziecko używa ICQ, sprawdź ich książki telefoniczne i profile pod adresem: www.icq.com.

Jeśli dzieci używają *instant messenger* w AOL lub innego serwisu typu komunikator czy darmowego konta e-mailowego, sprawdź odnośne listy klientów. I jeśli twój ISP udostępnia książki telefoniczne użytkowników lub profile, również tam poszukaj swojego dziecka, posługując się identyfikatorem (jego lub swoim) albo adresem e-mailowym.

W końcu powinieneś poszukać informacji o swoim dziecku, używając do tego wielkich wyszukiwarek, wprowadzając pełne imię i nazwisko w cudzysłowie. Jeśli ktoś publikuje coś o nich lub jeśli posługują się prawdziwym nazwiskiem w grupach dyskusyjnych, dowiesz się przeszukując Deja News (adres: www.dejanews.com), również umieszczając imię i nazwisko w cudzysłowie.

❖ WWW (The Wild Wild West – Najdzikszy Zachód Internetu): IRC, FTP, Usenet i grupy dyskusyjne

Niektóre miejsca w Internecie, np. IRC, FTP i Usenet, są bardziej otwarte dla wszystkich niż inne.

Usenet to ogólnoświatowy zbiór grup dyskusyjnych. Grupy te zajmują się określonymi tematami. Nie są ulokowane w sieci WWW. Tworzą oddzielną i znacznie starszą część Internetu, bez wyrafinowanej grafiki, dźwięku, animacji (innej niż żywa dyskusja członków grupy). Grupy dyskusyjne kolekcjonują artykuły, dokumentację dyskusji i inne wiadomości na określony temat, następnie publikują je lub udostępniają czytelnikom poprzez Internet. Niektóre grupy dyskusyjne są moderowane, co oznacza, że materiał przed opublikowaniem jest przeglądany przez moderatora. Większość grup jednak nie jest moderowanych.

W miarę rozwoju Internetu Usenet i grupy dyskusyjne stają się mniej popularną formą. Ale ponieważ ciągle mają liczną grupę oddanych fanów, prawdopodobnie znikną w najbliższej przyszłości. Będą nadal wspaniałą drogą poznawania ludzi o podobnych zainteresowaniach, a dla nastolatków dobrym źródłem wiedzy na określone tematy. Odszukiwanie grup jest bardzo proste: przeglądasz listę grup

i wybierasz taką, której temat ci odpowiada. Wysyłanie artykułów i wypowiedzi jest równie łatwe, wykonujesz tylko instrukcje zawarte na stronie Deja News.

Ale uczestnicy grup dyskusyjnych cieszą się też opinią wyjątkowo zajadłych dyskutantów, często stosujących słowne ataki na innych, posługujących się wulgarnym i obraźliwym językiem. Jest wiele świetnych grup dyskusyjnych, szczególnie dla rodziców dzieci specjalnej troski (sprawdź misc.kids), ale o wiele więcej jest takich, w których dominują chaos i niestosowne zachowania. Są nawet takie, gdzie handluje się nielegalnymi materiałami, np. pornografią dziecięcą.

IRC jest obszarem do rozmów stworzonym poza siecią WWW, gdzie tysiące kanałów czy tematów dają ludziom okazję do porozmawiania. Na IRC na ogół wymiana zdań przebiega spontanicznie, bez ściśle określonych reguł zachowania, jakie wprowadziły takie potęgi czatowe, jak AOL czy Talk City. To oznacza, że istnieje tam taka sama atmosfera niekontrolowanego Dzikiego Zachodu jak w grupach dyskusyjnych, tylko wszystko dzieje się na żywo. Wiele grup pedofilów z wyboru używa IRC jako miejsca wymiany poglądów. By ustrzec się przenikliwości rodziców i ukrytych agentów FBI, wprowadzają na swoich kanałach tryb „wstęp tylko za zaproszeniem".

FTP (*file transer protokol*) to metoda uzyskiwania dostępu do plików znajdujących się w komputerach podłączonych do Internetu. Najczęściej jest używana do wchodzenia w pliki zawierające gry, ale czasem w tych komputerach zgromadzone są materiały pornograficzne z udziałem dzieci, szerzące nienawiść i pedofilię i je też można za pomocą FTP oglądać.

Grupy dyskusyjne, FTP i IRC to dobre przykłady, że Internet może być zarówno źródłem pożytecznych informacji, miejscem ożywionych dyskusji, jak i poważnych zagrożeń dla naszych dzieci.

Co można na to poradzić?

Po prostu pamiętaj, że w związku z atmosferą Dzikiego Zachodu w wielu rozmowach na IRC i w licznych grupach dyskusyjnych dziecko biorące w nich udział powinno być troskliwie nadzorowane – albo też całkowicie od nich izolowane, dopóki nie osiągnie wieku, kiedy będzie w stanie zatroszczyć się o siebie. Należy też ostrzec dzieci, że powinny znać nie tylko zasady netykiety, ale i szczególne reguły obowiązujące na wybranym kanale IRC czy w grupie dyskusyjnej, zanim się do nich włączą. Nieznajomość tych reguł może sprowokować poważne i ostre skarcenie, „wykopanie" z kanału (czyli wyrzucenie na jakiś czas) lub „zabanowanie"(czyli stały zakaz wstępu na kanał).

Może będziesz zadowolony, gdy dowiesz się, że łatwiej jest utrzymać dziecko z dala od pewnych grup dyskusyjnych niż od wchodzenia na określone strony. Jeśli dziecko nie szuka informacji na jakiś zakazany temat, grupy dyskusyjne nie są dla niego specjalnie zajmujące (bo nie ma tam grafiki, dźwięku, animacji). Więc może wystarczy znaleźć ciekawe strony w sieci, by trzymać dziecko z dala od tych grup. Ponieważ wiele przyjaznych dzieciom miejsc do pogawędek jest łatwiejszych w obsłudze, a często i zabawniejszych niż dyskusje IRC, dzieci mogą bez oporu całkowicie zrezygnować z IRC.

Porozmawiaj z nimi o stronach FTP, na które wchodzą i co z nich ściągają. Upewnij się, że nie wchodzą na niebezpieczne tereny i że używają programów antywirusowych.

Na rynku jest wiele produktów filtrujących IRC, FTP i grupy dyskusyjne, podobnie jak i strony WWW. Niektóre są w stanie całkowicie zablokować dostęp do nich.

Rozdział 3

Ciemna strona Internetu

W Internecie jest wiele nieprzyzwoitych informacji, niezależnie od tego, jak zdefiniuje się słowo „nieprzyzwoity". Nie zapominajmy, że Internet to stwarzający okazje kusiciel. Ale ważne, byśmy widzieli rzeczy w odpowiednich proporcjach.

Jesteśmy przezornymi rodzicami... czy paranoicznymi zgredami?

Wszystko w życiu może być niebezpieczne. Pamiętam, jak wiele lat temu oglądałam z moimi dziećmi „Ulicę Sezamkową" i w pewnej scenie Grover bał się wszystkiego. Obawiał się nawet, że sufit się na niego zawali. Trzeba go było nauczyć, jak ma nabrać dystansu do swoich lęków (i do zagrożeń). To była świetna lekcja. Pokazała, że kiedy nie rozumiemy zagrożenia, nie wiemy, jak coś działa, czy jakie jest prawdopodobieństwo, że coś pójdzie źle, nawet sufit może budzić przerażenie.

Czasem dobrze jest wiedzieć, czym martwią się inni rodzice. Zgodnie z badaniami przeprowadzonymi przez Jupiter Communications 72% rodziców w 1998 roku martwiło się zagrożeniami płynącymi ze strony obcych poprzez e-mail i kawiarenki. Ta liczba w 1999 roku nieznacznie wzrosła – do 76%. Zagrożeń związanych z rozrywkami dla dorosłych obawiało się w 1998 roku 68% rodziców, a w 1999 roku – 75%. Problemem ochrony prywatności martwiło się w 1998 roku 55% rodziców, a w 1999 roku – 68%. Najbardziej wzrosło poczucie zagrożenia rodziców w związku z handlem internetowym. Reklamy skierowanej do dzieci obawiało się w 1998 roku 18% rodziców, a w 1999

roku – już 45% (różne ośrodki badawcze podają różne cyfry, ale wzrost poczucia zagrożenia w związku z reklamami i handlem odnotowują wszyscy). Takie opinie rodziców są rezultatem zarówno większej świadomości, jak częstszego używania Internetu.

Rodzicom, którzy nie znają Internetu, wszystko w nim wydaje się wyłącznie groźne i przerażające. Ale gdy dowiadują się więcej, umieją odróżnić zagrożenia rzeczywiste od wyimaginowanych.

❖ Nie wszystkie zagrożenia i niebezpieczeństwa w Internecie są równie realne

Częścią wyzwania, wobec którego stajemy, próbując zapewnić dzieciom bezpieczeństwo w sieci, jest konieczność odróżnienia tego, co jest tylko drażniące czy niesmaczne, od tego, co niebezpieczne lub nielegalne. Ale to my, rodzice, mamy prawo decydować o tym, co nasze dzieci mogą oglądać, a czego nie powinny. I musimy być realistami w ocenie zagrożeń. Jest wyraźna granica między sposobem myślenia ostrożnych rodziców a sposobem myślenia paranoicznych zgredów. Nie powinniśmy widzieć potworów pod każdym cyberłóżkiem i w każdej cyberszafie. Musimy umieć rozpoznać rzeczywiste zagrożenia i pamiętać, że niektóre rzeczy są tylko denerwujące, a nie groźne.

Wreszcie, w miarę dorastania naszych dzieci rośnie ich zdolność rozpoznawania i oceny, musimy więc podnosić szlaban wyżej, dając im więcej wolności i możliwości wyboru. Rodzicielstwo wymaga od nas nauczenia dzieci umiejętności formułowania samodzielnych sądów. Dodatkowe kółka trzeba czasem zdejmować.

Informacje nie ranią dzieci – robią to ludzie

Są dwa rodzaje zagrożeń, które nasze dzieci mogą spotkać w życiu. Jedne wiążą się z wrażliwością dzieci, ich stanem emocjonalnym i rozwojem intelektualnym. Drugie dotyczą fizycznego dobrostanu i bezpieczeństwa. Choć nikt nie chciałby, by uczucia jego dzieci zostały zranione ani by były one wystawione na okropne i niesmaczne informacje, sądzę, że gdyby to od nas zależało, wolelibyśmy taki rodzaj traumy niż molestowanie czy zranienie fizyczne. To ludzie, a nie informacje stanowią w cyberprzestrzeni największe zagroże-

nie dla naszych dzieci. Ale to nie oznacza, że informacje nie mogą być problemem.

Musimy pamiętać, że informacje, do których może dotrzeć dziecko, są różne: od takich, które uważamy za nieodpowiednie, wstrętne, a nawet niebezpieczne dla ich emocjonalnego rozwoju, do informacji dotyczących nabywania w sieci niebezpiecznych substancji czy broni.

Niektórzy rodzice uważają, że dzieci powinny mieć dostęp do wszelkich informacji, niezależnie od tego, jak bardzo wydają się nam odrażające. Wierzą, że to pomoże dzieciom radzić sobie z problemami, z którymi zetkną się w życiu, i że jest to sprawa wolności słowa i myśli. Inni rodzice sądzą, że powinni cenzurować wszystkie informacje docierające do ich dzieci, bo to rodzice są arbitrami w sprawie swobody intelektualnej dzieci. Nie ma właściwej odpowiedzi, dotyczącej wszystkich dzieci, istnieje tylko właściwa dla twojego dziecka.

Czy zdecydujesz, że twoje dziecko może mieć nieograniczony dostęp do wszystkich zasobów Internetu, ograniczony dostęp do wybranych zasobów, czy przyjmiesz jakieś pośrednie rozwiązanie, pamiętaj: to ma być twój wybór. To nie jest sprawa polityki rządowej, ale sposobu myślenia rodziców. A jedną z ich prerogatyw jest decydowanie, jakie informacje są odpowiednie dla dziecka.

O jakie zagrożenia chodzi?

W tym rozdziale będę mówiła o dwóch rodzajach zagrożeń: o takich, które inni stwarzają dla dzieci, i o takich, które dzieci stwarzają dla innych, także dla ciebie. (Rodzice doskonałych dzieci mogą opuścić ten rozdział, pod warunkiem że idealne dzieci mają też idealnych przyjaciół).

❖ Co grozi dzieciom?

Jest sześć rodzajów zagrożeń, które dzieci mogą napotkać w Internecie:

1. Mogą znaleźć informacje, które są dla nich nieodpowiednie. Chodzi o pornografię, nienawiść, nietolerancję, bigoterię, przemoc, oszustwa, informacje nieprawdziwe i przesadzone.

2. Mogą mieć dostęp do informacji, korzystać z usług i kupować przedmioty dla nich niebezpieczne. Istnieją strony instruujące, jak zbudować bombę, oferujące broń, alkohol, trucizny, tytoń i narkotyki oraz proponujące hazard w sieci.
3. Mogą być uwodzone czy niepokojone przez ludzi (często przez inne dzieci) wulgarnych, obrażających, rzucających groźby, podsyłających wirusy i włamujących się do komputera.
4. Mogą przekazać ważne osobiste informacje, wypełniając formularze, biorąc udział w konkursach i w rezultacie mogą stać się celem handlowców stosujących nieuczciwe techniki marketingowe.
5. Mogą być oszukane i wykorzystane, gdy coś kupują w sieci i ryzykują ujawnienie innym istotnych informacji finansowych, takich jak numery kart kredytowych, numery pin i hasła.
6. Mogą być uwodzone przez cybernapastników, którzy chcą spotkać się z nimi twarzą w twarz.

Gdy przejrzysz tę listę, zobaczysz, że dziecko nie ma wpływu tylko na dwa punkty spośród wymienionych. Oprócz sytuacji, gdy przez nieuwagę wejdzie w określone obszary (co omówiłam w poprzednim rozdziale), może odrzucić niestosowne i niebezpieczne informacje. Może również odmówić wypełniania formularzy i rejestrowania się w witrynie lub upewnić się, że informacje, które ma zamiar podać, są aprobowane przez rodziców i że zostaną odpowiednio potraktowane przez tych, którzy je zbierają.

Tylko działania cybernapastników i cyberuwodzicieli są poza ich kontrolą. Ale dopóki ktoś nie wymyśli technologii takiego zmniejszania naszych dzieci, by mogły przecisnąć się przez modem, one same muszą zgodzić się na spotkanie z kimś lub udzielić informacji, jak można je odszukać, przez co mogą znaleźć się w prawdziwym niebezpieczeństwie.

Mogę podać wskazówki, jak unikać zagrożeń, ale sami musicie poradzić sobie z tym, że dziecko czasem celowo wchodzi na niestosowne strony, robi niebezpieczne rzeczy i wystawia się na zagrożenia. Taka jest natura dzieci. (A zwłaszcza nastolatków!).

Ale nie martw się. Pomożemy ci zdobyć większą kontrolę nad tym, co twoje dziecko robi w sieci, i nauczymy cię, jak możesz pomóc dzie-

ciom krytycznie myśleć i dokonywać świadomych wyborów. Ale żebyś mógł nauczyć dziecko skutecznego unikania zagrożeń, najpierw sam musisz poznać te zagrożenia. (Spróbuję zrobić to tak bezboleśnie, jak się tylko da).

Niektóre z tych zagrożeń obejmują nielegalne działania. W dalszej części przedstawię krótkie omówienie prawa. Teraz skoncentrujemy się na tym, jak te zagrożenia powstają. Udzielę również kilku wskazówek, jak możesz radzić sobie z tymi zagrożeniami we własnym domu, używając technologii, stosując odpowiednie reguły postępowania i rozmawiając z dziećmi.

Wolisz, żeby twoje dzieci nie miały z tym do czynienia

Będziecie zadowoleni słysząc, że z mojego doświadczenia wynika, iż większość dzieci szybko nudzi się stronami dla dorosłych i innymi niestosownymi materiałami. Po pierwszej wycieczce w ciemną strefę, by sprawdzić, co ona zawiera, większość dzieci wraca stamtąd rozczarowana zawartością. (Co nie znaczy, że nie kursują tam i z powrotem przez jakiś czas, zwłaszcza gdy są w grupie i chcą zrobić wrażenie na innych, gdy wzrasta poziom hormonów albo gdy oglądają krwawe sceny). Ale ciemna strefa może zawierać coś więcej niż tylko nudne podniety dla mającego problemy dziecka czy nastolatka. Jednakże to ty musisz wiedzieć, czy dziecko ma problemy. Niektóre z moich podpowiedzi pomogą ci lepiej zrozumieć nawyki twojego dziecka w serfowaniu i mieć większą kontrolę nad jego aktywnością w Internecie, ale by pomóc dziecku czy nastolatkowi w poradzeniu sobie z bólem czy złością, potrzebne jest coś innego niż oprogramowanie filtrujące. Potrzebna jest pomoc profesjonalisty.

Ja mogę pomóc ci określić zagrożenia w sieci, ale to ty musisz mieć orientację w problemach swojego dziecka. (W rozdziale „Poznaj swoje dzieci i wypracujcie wasz własny kontrakt bezpiecznego serfowania" daję parę wskazówek dotyczących poznawania dziecka. Dołączyłam krótką listę wybranych rzeczy, które wszyscy powinniśmy o swoich dzieciach czy nastolatkach wiedzieć).

❖ Treści jawnie seksualne – pornografia dla dorosłych

„Gorące dziewczyny! Namiętne nastolatki i bombowe blondynki!" – wielu z nas natknęło się w Internecie na takie informacje. Nie ulega wątpliwości, że w sieci są setki tysięcy stron zawierających jawnie seksualne treści. Nic dziwnego, że internetowe strony poświęcone seksowi zdają się przyciągać więcej uwagi niż jakiekolwiek inne.

Te strony dla dorosłych są różne: od typu Playboy (wobec tych niektórzy rodzice mogą nie mieć większych zastrzeżeń) do eksponujących brutalnie dewiacje seksualne, których nawet najbardziej liberalni rodzice woleliby swoim dzieciom nie prezentować. Szczęśliwie wiele odpowiedzialnych witryn dla dorosłych stara się trzymać dzieci z daleka, żądając dowodu pełnoletności od wchodzących na ich strony.

Zawartość Internetu nie jest i nie powinna być ograniczona tylko do tego, co jest stosowne dla sześciolatków. Jest wiele rzeczy, które dorośli mogą legalnie robić, a które nie są odpowiednie dla dzieci. To nasze, dorosłych, prawo.

Ale niezależnie od tego, jaki jest nasz poziom tolerancji i czy coś jest legalne, czy nie, nie musimy pozwalać dzieciom oglądać tego, co my uważamy za nieodpowiednie dla nich. To nasze, rodziców, prawo decydować o tym, co jest dla nich odpowiednie, a co nie. Dlatego napisałam tę książkę.

Prawdziwe wyznania

Kiedy kilka lat temu robiłam program telewizyjny, pracowałam z grupą dzieci w wieku 8–10 lat z podmiejskiej szkoły. Pytałam je, co robią w Internecie takiego, o czym wiedzą, że rodzice by tego nie pochwalali. Jeden 9-latek nieśmiało podniósł rękę i zwierzył się nam (i ewentualnym telewidzom), że oglądał „nagich ludzi". Stopniowo pozostali uczniowie przyznali się, że oni także patrzyli na „rozebranych ludzi". Zażartowałem, że prawdopodobnie uczyli się biologii. Ale 9-latki (i młodsi) mogą oglądać „rozebranych ludzi" i znacznie więcej po prostu za jednym kliknięciem myszą.

Dzieci nie muszą szukać kioskarza, który zechce sprzedać im pisemka porno. Nie muszą wyciągać pieniędzy, by je kupić. Nie muszą przemycać ich z domu kolegi (czy z twojej łazienki). To, co mogą zo-

baczyć w sieci, jest dostarczone do domu, bezpłatne, bardzo łatwe do znalezienia (poprzez zwykłą wyszukiwarkę) i w wielu przypadkach – znacznie bogatsze graficznie niż to, co mogłyby dostać spod lady.

Choć wielu rodziców uważa, że obrazkowe treści seksualne nie są największym zagrożeniem, które nasze dzieci mogą spotkać w sieci, niewielu z nas chciałoby, by oglądały one obrazy bestialstwa, gwałtów czy sadomasochizmu.

Co można na to poradzić?

Mnóstwo! Wszystkie opcje wymienione w rozdziale 8 są wolne od obrazków o tematyce seksualnej (choć dzieci mogą się dowiedzieć więcej o rozmnażaniu się żółwia morskiego, niż sam chciałbyś wiedzieć). I wszystkie produkty, które testowaliśmy, zostały zaprogramowane tak, by wychwytywać głównie treści seksualne. To robią najskuteczniej.

Przede wszystkim jednak należy usiąść z dzieckiem i uświadomić mu, że choć może wykazywać normalną ciekawość wobec „rozebranych ludzi" (i innych rzeczy też), nie warto popadać w obsesję. Jest nadzieja, że po początkowym podnieceniu temat zacznie być nudny. To dobry moment, by przekazać mu swoje poglądy na sprawy seksu, pornografii, zniewolenia i wyjaśnić, dlaczego uważasz wpatrywanie się w to za stratę czasu.

Musisz stale dbać o poprawianie jakości wewnętrznego „programu filtrującego" swoich dzieci, czyli o zdolność krytycznego myślenia.

❖ Nienawiść, nietolerancja, bigoteria

Idee dla wielu ludzi odpychające znalazły w cyberprzestrzeni licznych odbiorców. Musimy upewnić się, że nasze dzieci są świadomymi, sceptycznymi i niechętnymi odbiorcami treści zawierających nienawiść, nietolerancję, bigoterię.

Zakres stron zawierających takie treści jest bardzo szeroki. Na wielu podaje się w wątpliwość istnienie Holocaustu. Na innych wykpiwa się mniejszości rasowe, grupy etniczne, religijne czy mające odmienne preferencje seksualne. Niektóre pośrednio zachęcają do nietolerancji, głosząc wyższość określonej rasy. Członkowie pewnych grup wyśmiewają tych, którzy do nich nie należą. Każdy, kto ma ochotę szerzyć nienawiść, może to robić w Internecie.

Niestety, trzeba było aż tragedii w Littleton, by ludzie uświadomili sobie, jak wiele nienawiści istnieje w świecie wirtualnym (i rzeczywistym). A większość jest zgodna z prawem. Prawo zakazujące szerzenia nienawiści dotyczy tylko wypowiedzi skierowanych do konkretnych osób lub grup, w określonym kontekście.

Ironią jest, że medium, które powinno promować równość i tolerancję, jest tak często wykorzystywane do promowania czegoś przeciwnego. Internet usuwa wszystkie przeszkody, więc cóż to za cudowna droga komunikowania swoich idei! Internet jest ślepy na płeć, wiek, fizyczne kalectwo, rasę, religię. Kiedy poznajesz ludzi w sieci, nie wiesz, ile mają lat, jaka jest ich płeć, kolor skóry, z jakim akcentem mówią czy jak się modlą. To najbardziej egalitarne środowisko na świecie. Nie ma granic geograficznych – nieprzerwana globalna komunikacja. Na tym polega piękno Internetu.

Jednak uprzedzenia są w Internecie nie mniej wyraźne. Na przykład ludzie są często zaskoczeni, dowiadując się, że jestem kobietą, bo mam nietypowe imię i jestem prawnikiem. Jestem rozbawiona, obserwując, jak zmienia się ich ton, gdy wychodzi na jaw moja płeć. Dlaczego tak się dzieje, zwłaszcza w dzisiejszych czasach, nie wiem. Ale wszyscy tak postępujemy. Wszyscy traktujemy ludzi różnie zależnie od ich płci, wieku, pochodzenia. To część naszego wychowania.

Jest wprawdzie kilkanaście witryn, które tropią nienawiść, bigoterię i nietolerancję w sieci. Jednakże mimo to nienawiść rozkwita w sieci, bo opętani nią bigoci i szaleńcy mogą czuć się bezpieczni, schowani za swoimi monitorami.

Co można na to poradzić?

Musimy uświadomić naszym dzieciom, że wielu ludzi spotkanych w Internecie ma uprzedzenia i przesądy, które są sprzeczne z naszym systemem wartości. To odpowiedni moment, by wyjaśnić, jakie wartości cenimy i czemu wierzymy w to, w co wierzymy. Gruntowne wyjaśnienia tego rodzaju stanowią najlepszą broń przed podejmowanymi przez innych próbami wpływania na przekonania twoich dzieci.

Kiedy dzieci spotykają się z fanatyzmem i nienawiścią w Internecie czy gdziekolwiek indziej, możemy pomóc im zrozumieć zagrożenia wynikające z takich uprzedzeń, znaczenie tolerancji i różnorodności. Im częściej mają one okazję rozmawiać i wymieniać

poglądy z innymi dziećmi, tym szybciej mogą dowiedzieć się, jak bardzo jesteśmy różni.

Mark Twain powiedział: „Podróże nie sprzyjają fanatyzmowi, uprzedzeniom i ograniczonemu myśleniu". Dzięki Internetowi nasze dzieci codziennie podróżują po całym świecie. Musimy upewnić się, czy naprawdę rozumieją, że są częścią globalnej społeczności. Musimy nauczyć je cenić różnice i różnorodność, jakie globalna społeczność reprezentuje, a nie drwić z nich.

Zapytaj dziecko, jak wyobraża sobie osobę, z którą ma kontakt poprzez sieć. Następnie podaj inne możliwe opisy, mówiąc, że ma lat 50, a nie 15, jest mężczyzną nie kobietą, przedstawicielem innej rasy i zapytaj, jaki to ma wpływ na odbiór tej osoby i dlaczego. To może być dobry sposób wykrywania uprzedzeń i stereotypów. Należy też rozmawiać o złych czy bolesnych sprawach, jeśli się zdarzą. Przy takiej okazji warto:

- Pokazać, jak bardzo boli dyskryminacja.
- Przypomnieć im, że gdy kogoś przezywamy czy mówimy, że nienawidzimy „takich" ludzi, to tym samym ich dyskryminujemy.
- Nauczyć je, by nigdy nie przymykały oczu na dyskryminację czy uprzedzenia, niezależnie od tego, gdzie się z nią spotykają: w szkole, w domu czy na ulicy.
- Uświadomić sobie, że nawet jeśli my nikogo nie dyskryminujemy, nasze dzieci mogą ulegać wpływom mediów czy innych ludzi, z którymi się stykają.
- Przekazać dzieciom, że zawsze powinny kwestionować utrwalone sposoby załatwiania spraw i próbować uczynić świat lepszym.

Kiedy dyskusja się już rozpocznie, bądź przygotowany na brutalne pytania i jeszcze brutalniejsze odpowiedzi.

Anti-Defamation League i National PTA przygotowały wspaniałe informacje o tym, jak możemy uczyć nasze dzieci reagowania na nienawiść, nietolerancję, fanatyzm. Centrum Szymona Wisenthala jest kolejnym źródłem informacji o tym, jak unikać nietolerancji i nienawiści. (Zajrzyj na ich strony, by dowiedzieć się czegoś więcej: www.afdl.org, www.pta.org i www.wiesenthal.org).

❖ Przemoc i krwawe sceny

Dzieci i nastolatki nie są tak bardzo zainteresowane stronami dotyczącymi seksu, jak się rodzicom wydaje. Są natomiast znacznie bardziej zaintrygowane stronami z krwawymi scenami, wypełnionymi amputowanymi częściami ciała, ludźmi zabijającymi maczugami małe foki i wyrzucone na plażę wieloryby – scenami, które dla nas byłyby jak senny koszmar. Dzieci traktują je jak horror filmowy, nie jak prawdziwe życie. Obawiam się, że najlepsze, co możemy w tej sprawie zrobić, to nie tracić nadziei, że kiedyś z tego wyrosną.

Pewien bardzo rozsądny specjalista od mediów pracujący w bibliotece powiedział mi, że gdy widzi gromadkę dzieci z nosami przylepionymi do monitora, wie, że oglądają strony z drastycznymi krwawymi scenami.

Nasze Teenangels (specjalna grupa nastolatek, z którą pracuję, wyspecjalizowana w sprawach bezpieczeństwa w Internecie) mówią, że ich przyjaciele zaglądają na takie strony, kiedy tylko mają okazję. Podały mi adresy stron, gdzie nieustannie pokazywane są ciała okaleczone w głośnych katastrofach. Nie rozumiem atrakcyjności takich obrazów, ale wygląda na to, że tego rodzaju fascynacje są powszechne wśród nastolatków. Zawartość witryn różni się – od prymitywnych do naprawdę niesmacznych. (Na niektórych można znaleźć ciała pocięte na kawałki, upozowane w nienaturalny sposób). Strony zawierające przemoc często również próbują prowokować przemoc. Ale od czasu tragedii w Littleton większość z nas wie, że należy je traktować jak strony szerzące nienawiść.

Co można na to poradzić?

Czasem skutkuje pouczenie dzieci, by „tam" nie zaglądały. (Choć niezbyt w to wierzę). Należy mówić im, że pokazywane tam sceny to nie jest horror filmowy, że zabijane kijami foki i wieloryby są prawdziwe, że ofiary wypadków to są bliskie komuś, realne osoby. Niektóre programy filtrujące mogą blokować także dostęp do stron z przemocą i drastycznymi obrazami. (Informacje na temat narzędzi filtrujących znajdziecie w rozdziale 8).

❖ Dezinformacja i naciąganie

Internet to tani i łatwy sposób rozpowszechniania informacji. Każdy może publikować, każdy może być ekspertem. Oddzielenie prawdy od fantazji w cyberprzestrzeni to jedno z najtrudniejszych zadań. Tak zwani artyści, fałszywi artyści, nawiedzeni i zwyczajni szaleńcy kwitną w tym nie krępującym swobody środowisku.

Jak odróżnić, co jest reklamowym chwytem, a co faktem? Które informacje są wiarygodne, a które są zwykłym bałamuctwem? Jak dzieci mają oddzielić fantazjowanie od profesjonalnych przemyśleń? A my sami? (Sądzę, że to materiał na kolejną książkę).

Robin Raskin, Internetowa Mama (Internet Mom), ocenia nieprawdziwe informacje jako wielki problem, na który technologia nie ma sposobu. „Większość narzędzi wspomagających rodzicielską kontrolę wspaniale blokuje materiały pornograficzne, nie jest jednak tak skuteczna w blokowaniu dziwacznych treści, piramid finansowych, rasizmu i kłamstwa. To są subtelności, których żadna technologia łatwo nie zablokuje". Obawiam się, że to oznacza, iż zadanie spada na nas.

Czy nam się to podoba, czy nie, to nasze, rodziców, zadanie nauczyć dzieci odróżniania nieprawdziwych informacji, koloryzowania od faktów. Musimy je także przekonać, że nie każdy jest tym, kim się wydaje. Większość nas już zaczęła to robić. Ale nasze dzieci muszą, niestety, wcześnie nauczyć się tych rzeczy.

Za każdym razem, gdy prowadziłam swoje dzieci do kasy w supermarkecie, widziałam przedziwne tytuły w brukowych gazetach: „Mężczyzna z Marsa jest ojcem dziecka w stanie Indiana", „400-letnia kobieta dzieli się sekretami długowieczności" itd. Kiedy dzieci już nauczyły się czytać, musiałam objaśniać im, co jest prawdą (choć rzadko potrafiłam to zrobić wystarczająco dobrze, bo mimo że jestem prawnikiem, nie jestem pewna, czy sama rozumiem, jak można wypisywać takie rzeczy).

Za każdym razem, gdy otrzymywały adresowany do nich list od jakiejś firmy, obwieszczający, że wygrały miliony dolarów, musiałam zwracać ich uwagę na napis u dołu drobnym drukiem. Ale czy to w supermarkecie, czy przy skrzynce pocztowej byłam obok, mogłam odpowiedzieć na każde pytanie. Tak samo ważne jest, byśmy byli blisko, gdy serfują po Internecie, szczególnie gdy dopiero zaczynają to robić. Ale to łatwiejsza część zadania. Musimy bowiem nauczyć je

także, jak mają odpowiadać na te pytania, kiedy serfują samodzielnie. A to jest znacznie trudniejsze.

Co można z tym zrobić?

Nauczmy je być bystrymi odbiorcami informacji. Spróbujmy zachęcić je do dzielenia się z nami informacjami, które znalazły w Internecie – wtedy możemy skonfrontować je z rzeczywistością. Spróbuj serfować razem z nimi, by pokazać im źródła, które należy traktować ze szczególnym sceptycyzmem.

Musimy nauczyć je także ćwiczenia własnego krytycyzmu. To najważniejsza rzecz, jakiej uczymy dzieci, ale szczególne znaczenie ma właśnie w odniesieniu do Internetu. Na czym, poza wyglądem strony, mają się opierać, oceniając jej wiarygodność? Zasłużone instytucje, jak American Library Association (ALA) i inne stworzyły listy polecanych bezpiecznych stron, ale w sumie nie obejmują one więcej niż 40 tysięcy stron (rozmiar typowej biblioteki w szkole średniej). Nie ma jeszcze czegoś takiego, jak świadectwo akceptacji dla stron internetowych.

A co z milionami pozostałych stron w sieci? Jak dzieci mają ocenić wiarygodność strony, jeśli dorośli mają z tym problemy? W co mają wierzyć? Członkowie grupy Teenangels mówili mi, że należy uczyć dzieci, by nigdy nie wierzyły niczemu, co widzą, słyszą lub czytają w Internecie. To może nieco zbyt radykalne podejście. Ale rzeczywiście musimy nauczyć je, by były sceptyczne.

Jak mamy uczyć dzieci oceniać wiarygodność strony? Jak mogą określić, kto za nią stoi? Czy prezentuje ona fakty, czy fikcję? Jak mamy wychować inteligentnych konsumentów internetowej informacji?

Zaufanie do marki

Zanim dzieci rozwiną stosowną zdolność krytycznego myślenia, najlepiej jest zdać się na sąd kogoś, komu ufamy. Można próbować zapoznać dziecko z listą stron zaaprobowanych przez szkołę i bibliotekę. Pomocne może być także posługiwanie się katalogami przy wyszukiwaniu informacji zamiast zwykłego użycia hasła. (Czy pamiętacie moje objaśnienia dotyczące działania wyszukiwarek?). Wyszkoleni sędziowie przeglądają każdą stronę i podejmują decyzję, czy włączyć ją do katalogu. Z tego względu sama często używam katalo-

gów Yahoo! i Lycos. Obie te firmy stosują wiele sit i filtrów i chciałabym, by tak było również w innych wyszukiwarkach.

Cenię też wysoko prowadzoną przez Lycos listę najlepszych stron w sieci – Top 5%. (Strona naszej firmy prawniczej została uhonorowana tą nagrodą kilka lat temu). Możesz nawet prowadzić wyszukiwanie tylko w obrębie nagrodzonych stron. Zaufanie do profesjonalistów ułatwia początki poznawania Internetu. (Upewnij się tylko, że podajesz przyjazny dzieciom temat wyszukiwania, bo w innym przypadku możesz znaleźć strony dobre, ale nie dla dzieci).

Czy posługujesz się katalogiem, czy listą bezpiecznych stron, by nie stykać się z wytworami dziwaków i szaleńców, polegasz na szanowanej firmie w znajdowaniu stron rzetelnych i wartościowych.

Możemy zachęcać dzieci, by rozmawiały z bibliotekarzami i nauczycielami o tym, jak oceniać wiarygodność informacji. To poprawi ich własną zdolność oceniania rzetelności informacji. Ale i wówczas, gdy polegają na zdaniu ekspertów (lub twoim), i wtedy, gdy wdrażają własne systemy oceny informacji, musimy uczyć je, by najpierw zastanowiły się nad pochodzeniem informacji i polegały na zdrowym rozsądku tak w świecie wirtualnym, jak i w rzeczywistym. Nasze dzieci mają stać się osobami krytycznie myślącymi.

❖ Cyberoszuści, plotki, miejskie legendy

Wszystkim nam nieobce są miejskie bajdy. Zwariowany podglądacz par w alei zakochanych. Mały aligator, przywieziony jako pamiątka z Florydy, wpadł do toalety i potem żył i polował w sieci kanalizacyjnej. Niektóre legendy przechodzą z pokolenia na pokolenie. (Czyż istnieją jeszcze aleje kochanków i czyż aligatory nie są chronionym gatunkiem, zagrożonym wymarciem?).

Pamiętacie opowieści o Mikeyu, dziecku, które nic nie jadło? Pamiętacie więc może i plotki (zupełnie niedorzeczne), które pojawiły się mniej więcej dwadzieścia lat temu, że Mikey zmarł, zjadłszy cukierka i napiwszy się wody mineralnej, bo od tego pękł mu żołądek? (Moja praca dyplomowa dotyczyła plotek w biznesie).

Plotki, zwłaszcza te brzmiące bardziej prawdopodobnie, przetrwały wieki. Nie inaczej dzieje się w cyberprzestrzeni. Tu nawet przenoszą się one łatwiej, niż kiedykolwiek mogły przenosić się w innych miejscach.

Ktoś poszedł do kina, usiadł na igle do zastrzyków podskórnych i zaraził się AIDS. Ktoś inny został uśpiony przez piękną kobietę, obudził się w wannie wypełnionej lodem i stwierdził, że nie ma jednej nerki. (Najwyraźniej została wyjęta i sprzedana komuś, kto potrzebował transplantacji). Prawda czy oszustwo? Sam musisz być sędzią.

Dobre plotki i oszustwa charakteryzują się trzema zasadniczymi cechami: mogły się zdarzyć, dotyczą czegoś, o czym wiemy lub sądzimy, że jest możliwe (ludzie mogą zarazić się wirusem HIV poprzez kontakt z zainfekowaną igłą, ludzie poszukują organów do transplantacji) i pożywką dla nich jest lęk (obawa przed zakażeniem HIV, przed uśpieniem przez nieznajomą osobę, przed seksem z nieznajomymi itp.). Różnica między plotką a oszustwem polega na tym, że oszustwo jest świadomie rozpowszechnianym kłamstwem, plotka może być rozpowszechniana z głębokim przekonaniem o jej prawdziwości. Ale jeśli oszustwo zostanie przekazane przez kogoś, kto w nie uwierzył, staje się plotką, więc co za różnica?

Plotki o wirusach komputerowych są po prostu ostatnim modnym oszustwem w cyberprzestrzeni

Codziennie znajduję w swojej e-mailowej skrzynce fałszywe ostrzeżenia przed nowymi wirusami. Kilka lat temu którejś nocy mój syn Michael przesłał mi listę prawdopodobnie zarażonych plików, którą ktoś przysłał jemu. Na liście umieszczono – oprócz innych mało prawdopodobnych nosicieli wirusów – uaktualnione programy dostępu do AOL. To przykład typowej mistyfikacji wirusowej, której celem jest przestraszenie ludzi, którzy właśnie zainstalowali sobie popularne programy. (Napomniałam Michaela, by przeczytał tę część, zanim prześle komuś e-mailem plotkę – a on zachęcił mnie do włączenia do książki tego rozdziału, by przestrzec innych). Jedną z najpopularniejszych plotek w Internecie w ostatnich latach była opowieść o wirusie Good Time, o którym mówiono, że może zainfekować komputer poprzez normalny e-mail. Doświadczeni użytkownicy komputerów i Internetu od razu ocenili te opowieści jako plotki, bo wiedzieli, że wirusem nie można zarazić się przy czytaniu wiadomości (ale może być przeniesiony poprzez wgranie plików dołączonych do e-mailu). Wiele mniej zorientowanych osób dało się nabrać. (Jednak trzeba wiedzieć, że ostatnio odkryte wirusy mogą zarazić komputer wtedy, gdy czytasz wiadomość).

Co można na to poradzić?

Na szczęście istnieje kilkanaście doskonałych witryn, do których możesz się udać, gdy następnym razem otrzymasz e-mail obwieszczający, że przybywa Armageddon czy inny najnowszy wirus. Tam znajdziesz wskazówki, którym wiadomościom przyjrzeć się uważnie, a które zignorować.

Zanim przekażesz dalej wiadomość o nowym wirusie, sprawdź ją. To jedna z zasad internetowej etykiety i dobry sposób na zachowanie wiarygodności w oczach innych. I jeśli wiesz o kimś, że rozpowszechnia cyberplotki, powiedz mu o tym. (Albo ignoruj wszystko, co ci przysyła, i poproś o usunięcie twojego adresu z listy osób, którym te wiadomości przesyła).

Największe zagrożenie: gdy dzieci robią coś ryzykownego lub kupują w Internecie nielegalne i niebezpieczne produkty

❖ Mamo, jak się robi bombę?

Jest w Internecie dostępnych wiele niewinnych książek, ale „The Big Book of Mischief" (Wielka księga psot) do nich nie należy. Niech cię nie zwiedzie niewinnie brzmiący tytuł – „psoty", o których traktuje, mogą doprowadzić do poważnych obrażeń i śmierci. Uczy przemocy i dostarcza dzieciom narzędzi potrzebnych do jej realizowania. Pewne wyobrażenie o jej zawartości daje podtytuł pierwszego rozdziału: „Poradnik terrorysty". Oczywiście umieszczono tam odpowiednie zastrzeżenie, że każda próba wykonania zawartych w książce przepisów może doprowadzić do poważnego uszkodzenia ciała lub śmierci. I że książka powstała głównie dla przyjemności poczytania. (Najwyraźniej wszyscy dzisiaj mają swoich prawników).

Dalej mamy „The Anarchist Cookbook" (Książkę kucharską anarchisty), traktującą o tym, że w pobliskim warzywniaku, sklepie żelaznym i sklepie z narzędziami rolniczymi można kupić wszystko, co jest potrzebne do produkcji bomby. (Jest tam nawet instrukcja wytwarzania nitrogliceryny).

A kim są ci terroryści uzbrojeni w śmiercionośne i łatwo dostępne informacje? Sądząc po ostatnich tragicznych wydarzeniach, mniej czy bardziej znanych, zaliczają się do nich nasze dzieci i ich szkolni koledzy.

Naprawdę przerażające jest to, co słyszałam od tysięcy dzieciaków, a mianowicie, że chciałyby zbudować bombę tylko po to, żeby zobaczyć, jak to działa. I mówią to chłopcy i dziewczynki z miast i z obszarów wiejskich. Więc nawet nasze dobre dziecko może łatwo stworzyć zagrożenie, gdy się będzie nudziło któregoś dnia.

Przed tragedią w Littleton ukazał się w „Ladie's Home Journal" artykuł o matce pewnego 13-latka, który doznał poparzeń 25% powierzchni ciała, gdy wraz z kolegą konstruował bombę według opisów, które obaj znaleźli w Internecie. Okazało się, że chłopiec nie miał w domu komputera, ale jego kolega miał zarówno komputer, jak i dostęp do Internetu i chłopcy serfowali po sieci bez żadnego nadzoru. Żeby dowiedzieć się, jak zbudować bombę, wystarczyło uruchomić ulubioną wyszukiwarkę i wystukać słowo „bomba" na klawiaturze. Początkowo (co można zrozumieć) Cheryl, matka chłopca, skierowała złość na Internet. Ale ta złość zelżała, gdy uświadomiła sobie, że jej syn równie łatwo mógł znaleźć informacje o konstruowaniu bomby w pobliskiej czytelni. (Choć nastolatki mówią mi, że nie zawracałyby sobie głowy chodzeniem do czytelni po takie informacje. To łatwość dostępu sprawia, że poszukiwanie takich informacji w Internecie jest atrakcyjne – i groźne).

Ale Cheryl się zreflektowała. Zrozumiała, jaką rolę odgrywa w życiu dziecka znajomość komputera, i postanowiła chronić syna i rodzinę przed skutkami analfabetyzmu komputerowego. W cztery miesiące po wypadku kupili komputer i podłączyli się do Internetu. Ale zarazem robili wszystko, by chronić siebie i syna.

Co konkretnie zrobili w tym celu? Postawili komputer we wspólnym pokoju, nie w sypialni Michaela. Ustalili dla niego również zasady korzystania: Michael mógł wchodzić do Internetu tylko w obecności rodziców. Monitorowali szczegółowo jego poczynania w sieci. Zdecydowali, że nie będą stosowali żadnego oprogramowania blokującego dostęp do określonych treści, tylko zaufają synowi, iż będzie przestrzegał ustalonych zasad. To jeden ze sposobów, jak rodzina może radzić sobie z zagrożeniami wynikającymi z Internetu, i jest to dobry sposób. Zaufaniem i edukacją można wiele zdziałać z niektórymi dziećmi.

Co można na to poradzić?

Podawanie większości wymienionych informacji jest absolutnie zgodne z prawem. Cóż więc można zrobić? Można przedsięwziąć określone kroki, by upewnić się, że dziecko rozumie zagrożenia. Uświadom mu, że przy montowaniu bomby może zostać okaleczone, stracić palce, ręce, nogi, a czasem i życie. Świadomość niebezpieczeństwa musi przeważyć dziecięcą ciekawość. Należy również zachować wrażliwość na sygnały wskazujące, że twoje dziecko być może pcha się w kłopoty. Jeśli rodzi się w nas podejrzenie, że dziecko może wziąć się do budowania bomby, należy zwrócić szczególną uwagę na takie rzeczy, jak wiadra lub pojemniki, butelki z wodą sodową lub wybielaczem, rurki, amoniak, gliceryna lub parafina. Niestety, przedmioty takie na ogół nie wzbudzają podejrzeń. To dlatego dzieciom tak łatwo zgromadzić wszystko, czego potrzebują do zrobienia bomby. Rodzice powinni również zainteresować się, gdy dziecko zbiera puste lub dziwnie wyglądające pojemniki, gwoździe lub ostre śruby, metalowe kulki i łuski po nabojach, z których usunięto proch. Gdy rodzice znajdą coś, co wygląda podejrzanie, nie powinni próbować samodzielnie rozbrajać takiego przedmiotu, ale jak najszybciej wezwać policję.

Oprócz edukowania i zwracania uwagi na podejrzane działania dzieci, także technologia pomaga rodzicom uzyskać pewność, że ich dzieci nie będą miały dostępu do nieodpowiednich informacji w sieci. Można filtrować i blokować nadchodzące wiadomości i strony WWW, zawierające określone słowa, np. słowo „bomba". Można również zablokować strony, które zakwalifikowano jako zawierające informacje pirotechniczne. Inną metodą jest umożliwienie dzieciom dostępu tylko do wybranych stron.

Informacje o konstruowaniu bomb i przemocy

Zainteresowanie dostępnymi w Interencie informacjami o budowaniu bomb szczególnie wzrosło po tragedii w Littleton. Odnotowałam dziesięciokrotny wzrost liczby zapytań od rodziców w sprawie oprogramowania filtrującego takie informacje. Podczas gdy sprawy seksu rzadko skłaniają rodziców do rozważania potrzeby posiadania takiego oprogramowania, budowanie bomb, przemoc i nienawiść wydają się przekraczać odporność wielu rodziców.

Ale programy filtrujące nie blokują tych stron tak skutecznie, jak stron z zawartością seksualną. (W kwestii oprogramowania filtrującego zob. rozdział 8 w części „Coś z kolumny A, coś z kolumny B"). Pamiętaj, że nawet gdy zdecydujesz się zastosować któreś z narzędzi filtrujących, twoje dzieci powinny wiedzieć, dlaczego niebezpieczne jest zajmowanie się produkcją bomb. Muszą być zdolne do samodzielnej oceny informacji.

❖ Narkotyki, alkohol, papierosy, broń i trucizny

Są dwa rodzaje witryn, poświęconych tym sprawom. Jedne zachęcają do używania wymienionych artykułów. Zagrożenie wynikające z ogłaszania takich materiałów w Internecie nie jest większe niż wtedy, gdy ktoś w inny sposób zachęca nieletnich do ich używania (choć być może więcej takich informacji jest łatwo dostępnych dla dzieci w sieci niż poza nią). Inne witryny to oferujące sprzedaż tego typu artykułów każdemu, kto chce je kupić, także dzieciom.

Witryny zachęcające do używania

Niektóre witryny dotyczące alkoholu, papierosów i broni zostały stworzone przez producentów tych dóbr; inne, promujące narkotyki i trucizny (na ogół dla celów samobójczych), tworzone są przez ludzi, którzy zachęcają do ich używania.

Wielu producentów stwierdza, że ich strony przeznaczone są dla dorosłych, którzy mogą legalnie używać ich produktów, a nie dla dzieci, ale musimy wiedzieć, że są one łatwo dostępne dla dzieci. (Niektóre z organizacji broniących praw dziecka uważają, że czasem koncerny wręcz kierują je do dzieci). Niezależnie od intencji producentów i dzieci powinny być świadome niebezpieczeństw związanych z alkoholem, tytoniem, truciznami, narkotykami i bronią.

Mam nadzieję, że przeprowadziliście już kilka rozmów na ten temat. Jeśli nie, to pora zacząć.

Co można na to poradzić?

Edukacja i poszanowanie zasad są zawsze najlepszą obroną przed tego rodzaju informacjami. Być może już przekazałeś dzieciom potrzebną wiedzę. Zapytaj je – będziesz zaskoczona, że wiedzą aż tyle. Jeśli uważasz, że poza edukacją potrzebna jest dodatkowa ochrona, to

większość programów filtrujących blokuje dostęp do stron związanych z alkoholem, papierosami i narkotykami.

Witryny sprzedające dzieciom te produkty

Istnieją tysiące witryn oferujących sprzedaż alkoholu w internecie. W wyszukiwarce, która nie filtruje wyszukiwanych stron ani nie jest przyjazna dzieciom, możesz szybko odnaleźć setki miejsc, które oferują sprzedaż win i innych alkoholi. Małe tłocznie win, które nie mogą sobie pozwolić na kosztowną sieć dystrybucji alkoholu, chętnie korzystają ze sprzedaży internetowej.

Trochę trudniej znaleźć witryny proponujące sprzedaż farmaceutyków (zazwyczaj oferują one środki sprzedawane na recepty, takie jak viagra, leki odchudzające, a czasem także inne medykamenty) lub broni. Jeszcze trudniej znaleźć miejsca sprzedające truciznę i zakazane narkotyki (choć strona zachęcająca do popełniania samobójstw oferowała sprzedaż cyjanku). Ale takie witryny istnieją i dzieci mające pieniądze lub karty kredytowe mogą kupić wszystko równie łatwo jak dorośli.

Kilka lat temu pewna matka otworzyła przesyłkę adresowaną do syna i odkryła, że zawiera ona półautomatyczny pistolet, który chłopiec zamówił przez Internet. Płatnością obciążył kartę kredytową rodziców. (Nie mam pojęcia, jak sobie wyobrażał moment, gdy odbiorą rachunek). Twoje dziecko może zrobić to samo.

Co można na to poradzić?

Musisz wiedzieć, że strony oferujące środki medyczne i alkohol, w przeciwieństwie do oferujących niebezpieczne materiały, nie są adresowane do dzieci. Są skierowane do dorosłych – koneserów wina, szukających małych i ciekawych winiarni, do mężczyzn mających problemy z erekcją lub z wagą, szukających dostępnych na receptę specyfików.

Dzieci nieczęsto kupują te artykuły. Papierosy i alkohol na ogół są w Internecie znacznie droższe niż w sklepie. Dzieci raczej więc kupują je w sklepie (oczywiście jeżeli znajdą mało skrupulatnego sprzedawcę albo namówią dorosłego, by je dla nich nabył).

Jeśli chcesz mieć pewność, że twoje dzieci niczego takiego nie kupują, musisz sprawdzać uważnie wyciągi bankowe i być przy otwieraniu przesyłek adresowanych do dzieci.

❖ Czy wychowujemy przyszłych cyberhazardzistów...

Nie ma wątpliwości, że za pośrednictwem Internetu można bez problemu zaspokajać swoje potrzeby związane z nałogami. Internet umożliwia też uprawianie hazardu, podobnie jak i innych nałogów. Tak naprawdę hazard rozkwita w sieci nawet wtedy, gdy gdzie indziej napotyka ostre rządowe restrykcje.

Większość stron hazardowych jest więc lokowana za granicą, co utrudnia zastosowanie regulacji prawnych. Witryny hazardowe żądają wniesienia opłat z góry, w formie obciążenia karty kredytowej lub debetowej albo przekazu gotówkowego. Zwykłe użycie wyszukiwarki wskaże tysiące miejsc, gdzie można uprawiać hazard. A pieniądze nastoletniego dziecka są tak samo dobre jak każde inne.

Byłam szczerze zaskoczona dowiadując się, że dzieci tak często odwiedzają strony hazardowe. Obecnie, gdy coraz więcej dzieci ma karty bankowe, umożliwiające im korzystanie z naszego konta w jakichś nieprzewidzianych okolicznościach, a także własne oszczędności z kieszonkowego czy prezentów urodzinowych, jest im łatwiej uprawiać hazard niż kiedykolwiek wcześniej. Czasem używają nawet naszych kart w nadziei, że nie skontrolujemy wyciągów bankowych. I często rzeczywiście nie kontrolujemy.

Co można na to poradzić?

Sprawdzaj kartę kredytową i wyciągi bankowe z rachunków własnych i dzieci. Ograniczając im korzystanie z karty kredytowej, utrudnisz uprawianie hazardu w sieci. (Niektóre programy filtrujące blokują możliwość wysłania określonych informacji, np. numeru karty). Ponadto, jeśli komputer jest ustawiony w centralnym miejscu domu pod twoim czujnym okiem, być może całkowicie ustrzeżesz je od hazardu.

Wyjaśnij też dzieciom, że jedynymi osobami odnoszącymi korzyść z hazardu są osoby oferujące hazard. (Kiedyś byłam prawnym reprezentantem kasyn i wiem, jak dochodowy jest hazard dla ich właścicieli). Wyjaśnij im też, że wiele witryn hazardowych to oszustwo, że wiele z nich, w świetle międzynarodowego prawa finansowego, może zatrzymać wygrane. Hazard w sieci jest grą bez możliwości wygrania, szczególnie dla dzieci i nastolatków.

Znieważanie, dokuczanie i nękanie

Czasem ludzie, czując się anonimowo (ukrywają się za ekranem komputera) i mając chłonną publiczność, mówią rzeczy, których nigdy nie odważyliby się powiedzieć komuś w bezpośrednim kontakcie. Także robią rzeczy, których nie odważyliby się zrobić w prawdziwym życiu. Kiedy tego rodzaju wypowiedzi skierowane są do dzieci, zrozumiałe jest nasze zaniepokojenie, bo ich uczucia mogą zostać głęboko zranione. Te wypowiedzi zmieniają się: od zniewag, przez budzące lęk (molestowanie), do wiarygodnych gróźb rzeczywistego wyrządzenia krzywdy w realnym życiu.

❖ Znieważanie

Zachodzi wtedy, gdy ludzie mówią przykre, ordynarne, obraźliwe lub prowokujące rzeczy do innych w sieci. Czasem są to po prostu wulgarni ludzie, czasem osoby, które chcą rozpętać kłótnię z innymi lub pomiędzy innymi. Niektórzy ludzie wysyłają obraźliwe lub prowokujące uwagi na temat jakiejś grupy, udając zarazem, że są członkami innej – wszystko po to, by rozpocząć wojnę.

Ciekawe, że wielu autorów takich wypowiedzi nigdy nie pozwoliłoby sobie na podobne zachowanie w rzeczywistości. Często uważają je za niewinną zabawę.

Co można na to poradzić?

Wielu rodziców, którzy dłużej mają do czynienia z Internetem, wypracowało różne metody radzenia sobie z wulgarnymi, obraźliwymi wiadomościami, wysyłanymi do ich dzieci. Jeden z tych rodziców, Bill Bickel, ma kilkanaście własnych stron, na których opowiada historie o swoich dzieciach. Wysłał wiadomość, którą zamieszczam poniżej, by pomóc innym rodzicom radzić sobie z wulgarnymi przesłaniami kierowanymi do ich dzieci. Bill wystosował ją, odnosząc się do wiadomości, które otrzymał w związku ze stroną WWW swoich dzieci, ale jego wypowiedź równie dobrze odnosi się do wszystkich wulgarnych zniewag, przekazywanych w e-mailach i czatach. Przedrukowałam ją za jego uprzejmym pozwoleniem. Są to dobre rady i zachęcam do stosowania ich (niezależnie od tego, czy twoje dzieci są adresatem, czy nadawcą obelg).

Czasem ludzie wysyłają naszym dzieciom niestosowne, wulgarne lub nawet obraźliwe wiadomości. Aaron otrzymał ich wiele. Rzecz jasna, wszyscy przeglądamy e-maile naszych dzieci, ale denerwujące jest to, że ktoś kieruje do naszego dziecka takie słowa. Myśl, że najpewniej robi to inne dziecko, nie jest wielką pociechą, bo nie fizycznych obrażeń się tutaj lękamy. (Obraźliwe e-maile Aaron otrzymał z Australii. My mieszkamy w New Jersey).

Moja rada jest taka: nie ignoruj takich wiadomości i nie czekaj, aż przyjdzie kolejna. Następną otrzyma pewnie inne dziecko. Tego rodzaju poczynania należy ukrócić natychmiast.

Wyślij kopię wiadomości do POSTMASTER@costam.com, dodając po prostu: proszę z tym coś zrobić. Ja zrobiłem tak dwukrotnie. I konto jednego z nadawców zostało zamknięte, a drugiego zawieszone (kochane dzieciaczki mające te konta robiły już wcześniej podobne rzeczy). Zgodnie z dobrym obyczajem wysłałem swoją wiadomość do właścicieli konta, nie wpisując tytułu, by dzieci jej nie przechwyciły. Tak samo zareagowałem na list do mnie, którego treść w większości była nieparlamentarna: przesłałem kopię do właściciela konta. W ciągu 24 godzin otrzymałem przeprosiny z zapewnieniem, że nastoletnia córka przez pewien czas ma zakaz korzystania z komputera.

Starsze dzieci i nastolatki należy poinstruować, by zgłaszały obelżywe listy pod wskazany adres lub zupełnie je ignorowały. Nie powinny angażować się w wojnę na wyzwiska, choć może się to wydawać pociągające. Eskalacja takich zachowań postępuje szybko, a one same szybko wymykają się spod kontroli. Nawet jeśli nie zareagujesz tak jak Bill Bickel, powinieneś próbować przeglądać e-maile, by przejąć wysyłane do dziecka obelgi.

Potem upewnij się, czy dziecko nie bierze sobie tych zniewag do serca. Uświadom mu, że nie warto poświęcać im uwagi. Nie jest to łatwe, ale musimy pomóc dzieciom jakoś się uodpornić, jeśli mamy pozwolić im na spędzanie czasu w sieci.

❖ Nękanie i prześladowanie

Są jednak osoby, które nie poprzestają na obrażaniu ciebie czy dzieci. Posuwają się one czasem do grożenia śmiercią, hakerowania czy przesyłania wirusów. Mogą śledzić dziecko w Internecie, używając listy kumpli i ICQ, mówić nieprzyjemne rzeczy o nim do innych w ka-

wiarenkach, do których dziecko wchodzi. Mogą wypisywać ohydne słowa w „książkach gości" na stronach WWW naszych dzieci. Mogą wreszcie podszywać się pod nasze dzieci, używając odpowiedzi na e-maile i tzw. technologii podstawiania i mówić oraz robić rzeczy, które mogą wpędzić nasze dzieci w kłopoty. Może to przybrać naprawdę okropne formy. Czasami musimy włączyć w sprawę dostawcę Internetu (ISP), czasem zaś trzeba rozważyć powiadomienie policji, zwłaszcza gdy w grę wchodzą pogróżki dotyczące realnego świata. Takich rzeczy nie wolno lekceważyć.

Co można na to poradzić?

Obszerną analizę cyberprześladowania i tego, co zrobić, gdy dziecko jest nękane czy śledzone, zawarłam w podrozdziale rozdziału 4 „Zostaw moje dziecko w spokoju!". Ale przestrzeganie przez dzieci zasad sieciowej etykiety i unikanie najbardziej swawolnych kawiarenek i grup dyskusyjnych powinno zapobiec większości tego rodzaju problemów. Dalszą pomocą może być zrezygnowanie z książki gości i z podawania informacji osobistych na własnych stronach WWW.

Należy też nauczyć dzieci, by nigdy nie reagowały na pogróżki czy zaczepki, które dostają w e-mailach. Ignorowanie jest często najlepszą metodą.

Można również używać programów filtrujących, by zablokować wiadomości nadchodzące od nieznanych nadawców czy od określonego nadawcy.

Wirtualni napastnicy

W dalszej części książki poświęcam cyberprześladowcom cały podrozdział. Musimy wiedzieć, jak oni działają, i nauczyć dzieci unikania ich pułapek. Tu przedstawiam tylko zarys. Ale trzeba zapoznać się z pełną wersją, by zdać egzamin, który muszą zdać wszyscy rodzice, by móc zapewnić bezpieczeństwo dzieciom.

Największy problem z wirtualnymi napastnikami wynika z faktu, że działają oni na terenie twojego domu. Ale zamontowanie systemu alarmowego i dodatkowych zamków nie zatrzyma ich w bezpiecznej odległości. Wchodzą do domu poprzez wasz komputer.

Twoje dziecko czuje się bezpiecznie, siedząc w kapciach i piżamie, gdy ty jesteś kilka kroków dalej, oglądając telewizję lub czytając. A ludzie, którzy rozmawiają z dzieckiem przebywającym w „bezpiecznej strefie", także czują się bezpieczni, jak zaproszeni do domu goście. Wirtualni napastnicy liczą na to, że to poczucie bezpieczeństwa uśpi czujność dzieci. Wykorzystują specyficzne poczucie intymności serfujących, by przekonać dziecko, że wcale nie są obcymi ludźmi.

Co można na to poradzić?

Twoim zadaniem jest nauczyć dzieci, że ci ludzie to obcy, niezależnie od tego, jak przyjaźni się wydają. Jeśli rodzice ustalili zasadę, że chcą znać wirtualnych kolegów swoich dzieci, i jeśli są blisko, gdy pojawia się problem, zadanie cyberprześladowcy będzie znacznie trudniejsze.

Chronienie dziecka w Internecie trochę przypomina montowanie blokad przeciwwłamaniowych w samochodzie. Choć nie może to całkiem zapobiec kradzieży samochodu, jeśli złodziej będzie tego naprawdę chciał, ale na tyle utrudni zadanie, że może on wybrać łatwiejszy obiekt. (Gdy wszyscy rodzice będą tak robili, napastnicy nigdzie nie będą mieli szczęścia).

Nasze dzieci zbyt często wierzą w to, co mówią im inni. A kiedy chcą coś sprawdzić, sprawdzają profile użytkowników tworzone przez samych cybernapastników. Jeśli oni kłamią, mogą sami własne kłamstwa potwierdzać. Musimy nauczyć dzieci, by nie ufały tak łatwo. To smutna, ale konieczna lekcja.

Wcześniej pewnie uczyliśmy dzieci zachowania wobec obcych, ale miłe osoby to przecież nie ci obcy. Dla dzieci przestrogi dotyczą tylko tych zarośniętych, brudnych i cuchnących osobników. Poproś dziecko, by opisało obcego, a przekonasz się, że mam rację. (Niestety, większość cybernapastników nie pasuje do wyobrażeń dzieci – często są to ludzie wykształceni, odnoszący sukcesy).

Zgłoś organom ścigania każdą próbę namawiania dziecka na spotkanie twarzą w twarz. Więcej informacji znajdziesz w podrozdziale „Komu zgłaszać problemy i przestępstwa w cyberprzestrzeni?" (rozdział 5). Możesz je również zgłosić do wydziału bezpieczeństwa swojego dostawcy Internetu (ISP).

❖ Wielka trójka

Problem cyberprześladowców i cybernapastników jest tak ważny, że poświęcam mu oddzielny rozdział (omawiamy w nim najważniejsze cechy ich metod działania, a także sposoby obrony). Poza tym istnieją dwa inne rodzaje zagrożeń, które także uważam za bardzo ważne i wymagające czegoś więcej niż tylko zdrowego rozsądku, by je w pełni zrozumieć. Chodzi o zagrożenie dla prywatności – co obejmuje też marketing, który wymaga od twoich dzieci ujawnienia danych osobowych ich lub rodziny – i o zagrożenia płynące z nieuczciwego marketingu i finansowych cyberoszustw. Te trzy sprawy omawiam w następnym rozdziale. Zanim jednak do nich przejdę, pomówmy o zagrożeniach dla komputera i o tych, które mogą stwarzać twoje dzieci dla ciebie i innych w sieci.

Zabezpieczenie komputera: hakerzy i wirusy

❖ Co to jest wirus?

Wirus to specjalny kod komputerowy, zawarty w programie komputerowym, który został stworzony w celu zainfekowania pliku i gdy zostanie uruchomiony, może przenosić się na kolejne pliki i spowodować uszkodzenie komputera. Komputer może nie dać się włączyć, można utracić pliki, cały twardy dysk może zostać wyczyszczony. Wirus może siać spustoszenie na różne sposoby.

Szansa złapania wirusa poprzez Internet jest mała, ale jeśli już się to zdarzy, zniszczenia mogą być duże. (Nie można złapać wirusa po prostu odwiedzając stronę WWW. Musisz coś wgrywać, by twój system uległ zainfekowaniu). Większość wirusów została zaprogramowana specjalnie po to, by niszczyły systemy komputerowe, i są w tym bardzo skuteczne. Niektóre mnożą się same, infekując plik za plikiem, gdy zagnieżdżą się w programie.

Dużo bardziej ryzykowne jest wymienianie się dyskietkami (coś, co dzieci robią stale i nieodmiennie) i używanie zakażonych programów. Kiedy powstała strona WWW mojej firmy prawniczej, pisaliśmy artykuły z domów i z naszego biura. Trzymaliśmy je na jednym dysku i przegrywaliśmy w różne strony, przenosząc z komputera na komputer. Pewnego ranka żadnego komputera nie dało się włączyć. Wirus był na dysku i zaraził wszystkie komputery, do których się dostał. Na szczęście zakupiliśmy właśnie program antywirusowy Norton AntiVirus i szybko go zainstalowaliśmy. Ten program i nasze modlitwy uratowały nasz system.

Oprócz wirusów istnieją aplikacje zwane „końmi trojańskimi". Konie trojańskie służą hakerom do infiltrowania twojego systemu. Koń trojański nie odtwarza się jak wirus. Otwiera „tylne drzwi" do twojego komputera, którymi haker może włamać się do systemu, gdy ty nie używasz komputera, i wykraść dowolne informacje (np. numery kart kredytowych i hasła).

Co można na to poradzić?

Aby uniknąć wirusów i koni trojańskich, stosuj zasady bezpiecznego używania komputera! Na szczęście jest wiele dobrych programów antywirusowych (chronią również przed końmi trojańskimi), które przeglądają zawartość komputera w poszukiwaniu wirusów i usuwają je. Najpopularniejsze to Norton AntiVirus i McAfee AntiVirus. Obydwa oczyszczają system z istniejących wirusów i stale go sprawdzają, szukając nowych, przyniesionych nieświadomie.

Programy takie są często uaktualniane, by wyłapywały również nowo pojawiające się wirusy. Aktualną wersję można ściągnąć za darmo z Internetu (program antywirusowy jest skuteczny tylko wtedy, gdy jest aktualny). Zarówno McAfee, jak i Norton pozwalają na darmowe użytkowanie swoich programów przez okres próbny. Wiedzą, że gdy je wypróbujesz, na pewno zechcesz je mieć.

Chcąc mieć pewność, że jestem zabezpieczona przed najnowszymi wersjami wirusów, zaczęłam ostatnio używać obydwu programów antywirusowych – i Nortona, i McAfee – czyli jak w starym powiedzeniu: i pasek, i szelki. Ale przezorności nigdy dość.

Rozważne i bezpieczne używanie komputera oznacza zachowanie przezorności. Lepiej zapobiegać niż leczyć. Jeśli będziesz przestrzegać następujących zasad, wszystko będzie w porządku:

- Zainstaluj dobry program antywirusowy i często go aktualizuj.
- Zainstaluj go tak, by włączał się automatycznie zawsze, gdy uruchamiasz komputer.
- Przepuszczaj każdy ściągany z Internetu program/dokument przez program antywirusowy, zanim go zainstalujesz.

- Sprawdzaj każdą dyskietkę za pomocą programu antywirusowego, zanim ją otworzysz.
- Nie otwieraj plików wysłanych przez kogoś, kogo nie znasz, a i wówczas dopiero po sprawdzeniu przez program antywirusowy (wirus Melisa działał tak, że wysyłał się jako e-mail do kogoś, kogo znasz. Używał książki adresowej w zainfekowanym komputerze, by przenosić się dalej).
- Regularnie sprawdzaj system na obecność wirusów.

Tych zasad muszą przestrzegać wszyscy użytkownicy – także dzieci.

Zagrożenia, jakie dzieci stwarzają dla innych – także dla ciebie

Nie możemy pominąć tu zagrożeń, jakie dla ciebie i dla innych mogą stwarzać twoje dzieci i ich koledzy. Mogą podać numery kart kredytowych, ujawnić osobiste informacje dotyczące ciebie i rodziny, pogwałcić prawa autorskie, popełniać przestępstwa komputerowe, zgubić lub zniszczyć twoje pliki. W niektórych przypadkach mogą nawet nie wiedzieć, że to robią, ale to nie zmniejsza ryzyka.

❖ Dlaczego dzieci odgrywają w Internecie fantazje przemocy? – „Bo mogę"

Wszystkie dzieci odgrywają w sieci różne fantazje, udając, że są kimś innym, niż są. Ale czasem odgrywają też fantazje przemocy.

Dwudziestu siódmoklasistów siedziało cicho w bibliotece, nie wiedząc do końca, kim jestem i dlaczego zostali tu przyprowadzeni. Popatrzyłam na grupę. To były typowe, dobrze wychowane dzieci ze spokojnej dzielnicy. Mieszkały w okolicy, gdzie są dobre szkoły, bezpieczne ulice. Nie oczekiwałam żadnych niespodzianek. (Rodzice i nauczyciele zapewne już wiedzą, co działo się potem).

Zapytałam je, jak często korzystają z Internetu i co tam robią. Wszyscy odpowiedzieli, że korzystają na co dzień. Większość powiedziała o czatach, słuchaniu muzyki, stronach sportowych i wysyłaniu wiadomości do przyjaciół za pomocą komunikatora i e-mailów. Niektórzy założyli sobie własne strony. Uzyskałam typowe odpowiedzi na typowe pytania.

Wówczas zadałam pytanie: co takiego robili w Internecie, o czym wiedzą, że ich rodzice by tego nie pochwalali. (Jestem zawsze zaskoczona tym, że dzieci zwierzają mi się z różnych skandalicznych rzeczy, tylko po to, żeby mi pomóc). Tu zaczęło być ciekawie. Kilkoro dzieci przyznało się do stworzenia strony, na której wyśmiewali się z otyłej koleżanki ze szkoły. Poinformowali innych o istnieniu tej strony. Dziewczynka była ogromnie zgnębiona. Podając się za nią, wysłali do AOL fałszywy jej profil. (Te dzieci miały zdecydowanie za dużo czasu dla siebie).

Kilkoro innych przyznało się do posługiwania się kartami kredytowymi rodziców, by wejść na strony dla dorosłych. (Wcale nie przyszło im do głowy, że kiedyś przyjdzie rachunek za serwis pornograficzny). Niektórzy zostali wyrzuceni z AOL za używanie wulgarnego języka lub prowokowanie kłótni.

Ale zawsze będę pamiętała jedną konkretną historię, opowiedzianą przez łagodnego, nieśmiałego, inteligentnego chłopca o płowych włosach. Miał świetne stopnie, był typem dziecka nigdy nie sprawiającego kłopotów. Podniósł rękę i powiedział, że wysyła e-maile, w których grozi odbiorcy śmiercią. To natychmiast wyostrzyło moją uwagę.

Porozmawialiśmy chwilę o jego życiu. Powiedział, że nie pcha się w kłopoty w „pż" (prawdziwym życiu – dla niewtajemniczonych). Odrabia lekcje, wraca ze szkoły prosto do domu i słucha rodziców. Ale w Internecie wysyła pogróżki. Kiedy drążyłam dalej, powiedział, że nigdy nie zrobiłby niczego złego, bo obawiałby się przyłapania i kłopotów. Lubi być „grzecznym dzieckiem". Sądzi, że to zabawne odgrywać swoje fantazje w wirtualnym świecie. Był też przekonany, że nie grozi mu przyłapanie. Gdy zapytałam go, dlaczego to robi, odpowiedział po prostu: „Bo mogę".

Ten chłopiec jest grzecznym dzieckiem, jakie najchętniej widzielibyśmy w roli przyjaciela naszego dziecka. Porównujemy do niego innych, pytając: „Czemu nie możesz być taki jak...". Zawsze pamięta powiedzieć „proszę" i „dziękuję". Nigdy nie groziłby nikomu w realnym życiu. Ale w Internecie nie jest dobrze wychowanym, wybitnym uczniem. Tu jest brutalnym i twardym typem, jakim zawsze chciał być. To internetowa wersja doktora Jekylla i pana Hyde'a. I robi to wszystko w zaciszu swego pokoju, wcześniej przykładnie odrobiwszy lekcje.

Tyle tylko, że kiedy ktoś odbiera taką pogróżkę, nie wie, że została wysłana przez niewinnego ucznia; traktuje ją jako śmiertelnie poważną groźbę. A okaże się także poważną dla ucznia, gdy policja, ustaliwszy jego adres, zapuka do drzwi.

❖ „Droga Jennifer, mam zamiar cię zabić"

W Cyberangels pomagamy ofiarom prześladowań znaleźć swoich prześladowców i oskarżyć ich. Zgłaszają się do nas po pomoc na ogół wówczas, gdy są już półżywe ze strachu. Jeden przypadek, gdy napastnik groził śmiercią matce i jej nastoletniej córce, stał się szczególną, osobistą krucjatą Kelley Beatty, naszej dyrektorki.

Matka przysłała do nas rozpaczliwy e-mail. Była tropiona w Internecie. Prześladowca groził śmiercią jej i jej córce. Znał ich pełne personalia, adres, prawdziwe nazwisko, numer telefonu. Zgłaszała to już w miejscowej policji, ale tam nie potraktowano jej obaw poważnie. Bała się o bezpieczeństwo swoje i dziecka. Nie była w stanie pracować, musiała brać leki w związku z silnym stresem.

Kelley nie potrzebowała wiele czasu, by ustalić, jak prześladowca wszedł w posiadanie danych personalnych matki. Sama umieściła je w swoim profilu w ICQ. Uzyskanie numeru telefonu wymagało tylko otwarcia białych stron w internetowej książce telefonicznej i odszukania nazwiska. W czasie pogawędek wspominała też o córce i prześladowca najwyraźniej zapamiętał tę informację. (Matka została natychmiast o tych ustaleniach poinformowana, doradziliśmy jej bezzwłoczne usunięcie danych personalnych i poinstruowaliśmy, jak serfować anonimowo).

Kiedy prześladowca ujawnia, że posiada o ofierze jakieś informacje dotyczące realnego świata, traktujemy sprawę bardzo serio. Równie poważnie traktują to organa ścigania. Kelley rozpoczęła śledztwo. Szczęśliwie prześladowca również zostawił swój ślad. To pozwoliło Kelley i jej zespołowi szybko go zidentyfikować i zaskoczyć informacją, że Cyberangels wiedzą, kim jest, i że to, co robi, jest przestępstwem. On mieszkał w Kanadzie, a ofiara – w USA. Ale napastowanie jest przestępstwem w obydwu tych krajach. (Ostrzegam rodziców przed samodzielnym wykonywaniem takich manewrów. Nie kontaktujcie się sami z prześladowcą. To prawie zawsze powoduje eskalację prześladowań. Skontaktujcie się z policją, z Cyberangels lub swoim dostawcą Internetu).

W opisywanym przypadku prześladowca natychmiast okazał skruchę. Przyznał, że jest nastolatkiem, i tylko się wygłupiał. Uważał, że to zabawne tak postraszyć ludzi, i nie miał zamiaru spełniać swoich pogróżek. Przyrzekał, że nigdy więcej tego nie zrobi. Kelley przekazała te informacje ofierze, która od razu zadzwoniła do domu chłopca (zawsze odradzam takie działania). Odebrała babcia i natychmiast zrozumiała, jak groźne były zachowania wnuka. Tak Kelley, jak i ofiara były przekonane, że sprawa zostanie należycie załatwiona i nie ma potrzeby podejmowania kroków prawnych.

❖ Kiedy dzieci stają się hakerami i popełniają inne przestępstwa komputerowe

Niektóre dzieci, wyposażone w dobre komputery, udowodniły, że są niezwykle sprawne w manipulowaniu systemami komputerowymi innych i w poruszaniu się w cyberprzestrzeni. Włamują się do cudzych systemów, wysyłają e-maile i udają, że zrobił to ktoś inny. Ponieważ robią to, siedząc we własnym domu, wydaje się im, że są anonimowe. Wiele z nich nie rozumie, jak poważne skutki mogą mieć takie działania.

Są dwa typy hakerów: ci, którzy to robią dla sławy i zabawy, i ci, którzy robią to dla korzyści materialnych albo chcąc wyrządzić szkodę innym. Większość dzieci to ta pierwsza kategoria. Są dumne, że potrafią włamać się do komputerów CIA albo przejąć stronę WWW „New York Timesa". Bycie znanym hakerem to w Internecie swoisty „krzyż walecznych".

Problem w tym, że hakerzy uznawani są za bohaterów nie tylko przez swoich rówieśników, ale także przez wielu dorosłych, którzy powinni mieć więcej zdrowego rozsądku. Według magazynu „Fortune" dyrektor firmy Panasonic powiedział, że hakowanie to szkoła komputerowych ekspertów. Fakt, że dorosły, który jest cenionym fachowcem, nazywa przestępstwo „niezwykłą i szaloną przygodą", to sedno problemu.

Dzieci nie rozumieją, że włamanie do komputera jest przestępstwem, i to poważnym. (Szczerze mówiąc, wielu dorosłych także nie. Kiedy mówiłam w telewizji o zatrzymaniu autora wirusa Melisa, wielu „zwykłych przechodniów" pytanych w tym samym czasie o zdanie uważało, że będzie niezwykle cennym pracownikiem dla każdej firmy komputerowej, gdy tylko zostanie zwolniony z więzienia).

Wysyłanie innym wirusów także uważane jest za rodzaj hakowania. Każdy, kto kiedykolwiek miał zainfekowany komputer, wie, jaką szkodą może być utrata dużej liczby informacji, ale wiele dzieci nie traktuje sprawy poważnie (dopóki same nie staną się ofiarami).

Niektóre dzieci posyłają sobie nawzajem wirusy na takiej zasadzie, na jakiej nasze pokolenie robiło sobie głupie kawały przez telefon. Na pierwszym spotkaniu w Białym Domu, poświęconym dzieciom i Internetowi, zebrano na scenie kilkanaścioro dzieci, by porozmawiać o tym, jak używają sieci. Pewien chłopiec powiedział m.in., że używa jej do wysyłania bomb e-mailowych (chodzi o tak dużą liczbę wiadomości napływających do danej skrzynki w jednym momencie, że system przestaje działać). Może dlatego, że niewiele osób zrozumiało, o co chodzi, słuchacze wybuchnęli śmiechem, zamiast zareagować bardziej właściwie.

Wprawdzie rzadko, ale zdarza się, że dzieci niszczą strony lub włamawszy się do systemu, popełniają przestępstwa finansowe. Mogą wcale nie myśleć o ryzyku związanym z włamywaniem się do cudzych komputerów, ale jest to poważne przestępstwo. FBI ocenia, że straty finansowe wynikające z tego rodzaju przestępstw przekraczają kwotę 10 miliardów dolarów rocznie. A co gorsza, wiele z nich pozostaje niewykrytych.

Kilka lat temu wprowadzono ustawę ułatwiającą oskarżanie hakerów. Coraz częściej grupy stojące na straży prawa na podstawie tej ustawy oskarżają dzieci o przestępstwa związane z Internetem.

Panowie w ciemnych garniturach

Pewna znajoma podzieliła się ze mną swymi przeżyciami sprzed kilku lat. Nieoczekiwanie w drzwiach jej domu zjawiło się kilku panów w ciemnych garniturach, pytając o jej syna. Okazało się, że był on jednym z pierwszych hakerów, który złamał kody zabezpieczające karty kredytowe. Nie postawiono mu nigdy żadnych zarzutów, on sam zawsze zaprzeczał niewłaściwemu użyciu stworzonego przez siebie programu, ale matce bardzo trudno było otrząsnąć się po wizycie tajnych agentów w jej domu. Dzisiaj się z tego śmieje, jej syn jest świetnie zarabiającym specjalistą komputerowym, ale wtedy nie było jej do śmiechu.

Dzieciom wydaje się, że nigdy nie zostaną złapane. To już nie jest prawda, choć wiele lat temu hakerzy rzeczywiście rzadko byli identyfikowani.

Co można na to poradzić?

Do ciebie należy nauczenie dziecka, by nie hakowało i nie popełniało innych przestępstw komputerowych. By zrozumiało, jakie mogą być konsekwencje takiego zachowania, musi identyfikować się z ofiarą, bo inaczej włamanie do cudzego systemu pozostanie dla niego nieszkodliwym, anonimowym działaniem. Jeśli przybliżysz problem, pokazując, jakie byłyby konsekwencje, gdyby ktoś włamał się do twojego służbowego komputera i zniszczył wykonaną przez ciebie pracę, albo co by było, gdyby ktoś włamał się do domowego komputera i usunął dzieciom ich ulubione gry i pliki, być może wtedy łatwiej pojmą powagę przestępstwa.

W ubiegłym roku, gdy prowadziłam pogadankę dla rodziców i dzieci, pewien piątoklasista opowiedział, jak utracił wszystkie gry i materiały do szkolnego referatu, gdy jego komputer został zarażony koniem trojańskim. Na wszystkich dzieciach historia zrobiła duże wrażenie. Nikt nie opowiadał dowcipów o wirusach i hakerach. To była najlepsza pogadanka, jaką kiedykolwiek miałam, właśnie dzięki temu uczniowi.

Musisz rozmawiać z dzieckiem o hakowaniu. Uświadom mu, jak poważna to sprawa. Niektóre szkoły zapraszają przedstawicieli policji i prokuratury do wygłaszania pogadanek o przestępstwach komputerowych. Sądzę, że powinny poza tym starać się zidentyfikować początkujących hakerów i przydzielać im bardziej konstruktywne zadania, w których mogliby się sprawdzić.

Rodzice muszą pamiętać, że każda forma wglądu w komputerową aktywność dzieci chociaż trochę utrudni im popełnianie przestępstw. Czasem więc zajrzyj im przez ramię i nie zgadzaj się na ustawienie komputera w ich pokoju. Ulokowanie sprzętu w miejscu dostępnym dla wszystkich to jedna z moich sprawdzonych rad. Jeśli dzieci, chichoczące przy komputerze, milkną nagle, gdy wchodzisz – uważaj!

Z drugiej strony...

Ale nie wszyscy hakerzy są źli. Grupa hakerów zwalczających pedofilię (Ethical Hackers Against Pedophilia – EHAP, www.ehap.com) to ludzie o wybitnych umiejętnościach, którzy swój czas poświęcają na odnajdowanie i zgłaszanie odpowiednim organom cyberprześladowców i pornografii dziecięcej, pojawiającej się w Internecie. Wiele dzieci, bardzo biegle korzystających z komputerów, włączyło się

do podobnych grup i wykorzystują swoje umiejętności, by pomagać, a nie szkodzić. Bywa, że to dzieci odkrywają słabe punkty w komputerowych systemach zabezpieczeń, czasem nawet pomagają szkołom w wykrywaniu włamań do sieci.

❖ Kije i kamienie – zniesławianie innych w sieci

Kije i kamienie mogą połamać kości, ale słowa nie zrobią krzywdy – prawda czy fałsz? Fałsz! Mimo że mamy prawo do swobody wypowiedzi, to jednak nie daje nam prawa do mówienia nieprawdziwych i przykrych rzeczy o innych. W pewnych konkretnych okolicznościach zniesławienie może być uznane za napastowanie, które zawsze jest uważane za przestępstwo.

Niestety, od czasu gdy powstał Internet, wiele dzieci właśnie tu wyjawia swoje żale. Tworzą zniesławiające strony i wysyłają zniesławiające komentarze. Na początku istnienia Internetu ofiary pomówień na ogół ignorowały takie zachowania, obecnie jednak coraz częściej podejmują jakieś kroki. Czasem włączają się w to nawet szkoły, nierzadko zresztą ze szkodą dla siebie.

Dzieci muszą wiedzieć, że operatorzy i dostawcy Internetu udostępnią ich dane personalne w przypadku postępowania sądowego. I że mogą zostać odszukane i osądzone za to, co powiedziały w sieci.

❖ Hola! To moje! O własności intelektualnej

Wielu ludzi zapomina, że prawo, które działa w realnym świecie, dotyczy też Internetu. Krajowe i międzynarodowe prawa i umowy dotyczące własności intelektualnej chronią prawa autorskie twórców. Nie trzeba zgłaszać dzieła do Copyright Office ani naklejać symbolu C, by podlegało ochronie. Jeśli coś napiszesz i opublikujesz, to zgodnie z prawem o własności intelektualnej, podlega to ochronie przed zawłaszczeniem. Ponieważ tak łatwo można zablokować, wyciąć czy wymazać wszystko z dowolnej strony WWW, a także przegrać i zapisać dokument czy obraz graficzny na swoim komputerze, ludzie często zapominają, że wszystkie działania nie mieszczące się w pojęciu legalności są przywłaszczeniem. Nasze dzieci muszą wiedzieć, że mogą korzystać z materiałów przez kogoś sporządzonych tylko dołączając odpowiednią bibliografię i że nie mogą „pożyczać" z cudzej pracy więcej niż jeden czy dwa cytaty.

Zgodnie z międzynarodowymi standardami prawnymi przejęcie własności intelektualnej jest przestępstwem także wtedy, gdy nie wiąże się z czerpaniem jakichkolwiek profitów. Wiele dzieci zamienia się dyskietkami, wymieniając kopię czegoś na kopię czegoś innego. Według obowiązującego prawa to przestępstwo. Choć jest mało prawdopodobne, by policja zaczęła masowo aresztować nasze dzieci, to teoretycznie takie zagrożenie istnieje.

W ostatnim czasie przemysły filmowy i muzyczny stały się bardzo aktywne, usiłując powstrzymać rzesze nastolatków dokonujących pirackich nagrań filmów i muzyki w Internecie. Ale w cyberprzestrzeni agresywne przymuszanie może dać zawstydzające efekty. Nasze dzieci stały się bardzo biegłe w używaniu nowoczesnej technologii do praktyk pirackich wobec mediów. I nie kończy się to na mediach. Dzieci cały czas robią pirackie kopie programów komputerowych, nie zastanawiając się nawet, że łamią prawo i kradną własność intelektualną.

Jeśli uświadomimy dzieciom, jak okropnie by się czuły, gdyby ktoś ukradł im projekt przez nie stworzony, być może będą robiły to rzadziej. (Ale gdy weźmie się pod uwagę liczbę studentów, o których mówi się, że kupują prace dyplomowe w Internecie, to może jest to beznadziejna propozycja. Musimy podjąć szybkie i zdecydowane działania, by wpoić zasady etycznego zachowania).

Ucz swoje dziecko, by szanowało własność innych, nawet gdy wydaje się, że wszyscy mogą z niej swobodnie korzystać. Internet istnieje, bo ludzie – dla wspólnej nauki i rozrywki – są skłonni publikować stanowiące ich własność informacje. Prawa tych ludzi muszą być chronione, w przeciwnym razie strumień informacji może osłabnąć – ze szkodą dla wszystkich.

Zagrożenia ze strony twoich dzieci i ich przyjaciół

Dotychczas koncentrowaliśmy się na chronieniu dzieci przed innymi w cyberprzestrzeni. Ale istnieją też zagrożenia dla ciebie i innych, spowodowane przez twoje dzieci i ich kolegów, specjalnie lub niechcący.

❖ Żarty, które mogą kosztować cię utratę konta internetowego

Wszyscy dostawcy Internetu i usług internetowych mają swoje zasady. Określa się je jako „zasady realizowania usług". Jest to kontrakt zawarty z tobą jako odbiorcą usługi. Jeśli ty sam lub ktoś używający twojego konta łamie zasady, jesteś narażony na utratę konta.

Ulubionym wybrykiem nastolatków jest wchodzenie do czyjegoś konta i tworzenie śmiesznego lub prowokującego profilu. Wielu z nich otwarcie wymienia się swoimi hasłami z przyjaciółmi. Jedna z dziewcząt ze śmiechem powiedziała mi, że użyła hasła przyjaciółki, żeby dostać się do jej konta, i zmieniła jej profil, podając, że nosi biustonosz D 4 i poszukuje chłopca. Koleżanka niczego nie spostrzegła, dopóki nie zaczęła otrzymywać lubieżnych listów od nieznajomych, którzy odwiedzili jej stronę. Dziewczyna musiała zmienić swój identyfikator, by uniknąć molestowania. Mam nadzieję, że to je obie czegoś nauczyło.

Uprzedź swoje dzieci, by nie powierzały nikomu swojego hasła. Uprzedź je również, by nie robiły nigdy podobnych kawałów, posługując się hasłem innej osoby. Gdyby ten wybryk został zgłoszony, dziewczynka straciłaby swoje (i pewnie rodziców) konto, a jej przyjaciółka mogła znaleźć się w bardzo poważnych kłopotach.

Jeśli uważasz, że twoje dzieci nie mogłyby tego zrobić, pamiętaj, że są jeszcze inne dzieci. Nawet jeśli ufasz, że twoje dzieci nie złamią zasad, czy możesz tak samo zaufać ich kolegom? Mogą oni używać twojego konta, gdy są w waszym domu – mogą nie znać twoich reguł albo mogą nie mieć ochoty ich przestrzegać. Żałuję, że sama o tym nie pomyślałam, zanim dostałam twardą lekcję.

Kiedy prowadziłam sesje forum prawniczego w AOL, miałam obowiązek regularnie gościć w Internecie, monitorując rozwój dyskusji. Któregoś wieczoru, gdy próbowałam się zalogować, dowiedziałam się, że moje konto zostało zamknięte. Powiedziano mi, że ktoś pogwałcił zasady korzystania z usług. Nie mogąc skontaktować się z nikim z administracji, musiałam otworzyć sobie inne konto, żeby w ogóle wejść do sieci. Nowe konto nie miało potrzebnych mi opcji narzędziowych, więc nie mogłam regulować pracy grup dyskusyjnych. Byłam zła, a i moja opinia ucierpiała. Trzeba było kilku dni, żeby wyjaśnić sprawę, a w tym czasie wszystkie e-maile odsyłano do nadawców.

Okazało się, że przyjaciele mojej córki wpadli do niej z wizytą i skorzystali z mego konta, by dostać się do sieci. Wdali się w pyskówkę w kawiarence dla nastolatków, ich zachowanie zostało zgłoszone do AOL, a administrator zamknął moje konto z powodu pogwałcenia zasad korzystania z sieci.

❖ Gdy dzieci używają naszych kart kredytowych i robią bez pozwolenia zakupy w sieci

Pewien mój przyjaciel, jeden z pierwszych prawników specjalizujących się w sprawach Internetu w Stanach Zjednoczonych, osoba bardzo biegła w zagadnieniach technicznych, zadzwonił do mnie, skarżąc się na swoje dzieci. Okazało się, że znalazły informacje o jego karcie kredytowej zapisane dla wygody w komputerze. Zwołali swoich kolegów i wspólnie zamówili wielkoekranowy telewizor w internetowym sklepie.

Na szczęście w AOL zauważono, że adres, pod który ma być dostarczony zakup, i adres karty nie zgadzają się (dzieci były dość sprytne, by zamówić dostawę do domu przyjaciół) i zadzwoniono, by uzyskać potwierdzenie zakupu. Kolega wycofał zamówienie, zanim stało się coś niedobrego.

To, że wiesz dużo o komputerach, nie zawsze przygotowuje cię na to, co twoje dzieci lub ich koledzy mogą wymyślić. Pamiętaj o tym. I kontroluj wyciągi bankowe, a ważnych informacji nie trzymaj w komputerze, gdzie mogą być łatwo znalezione (i wykorzystane) przez dzieci.

❖ Chroń swoją pracę: nie używaj służbowego konta internetowego na potrzeby rodziny

Ocenia się, że połowa ludzi korzystających z Internetu ma dostęp do niego poprzez swoją pracę. Skargi napływające do pracodawców w związku z niewłaściwym używaniem Internetu przez pracownika lub inne osoby, korzystające z konta pracownika, dotyczą: zniesławiania, pogwałcenia praw autorskich, zdrady tajemnic handlowych i informacji poufnych, molestowania, hakowania, szerzenia nienawiści.

Mimo że wejście do Internetu przy użyciu służbowego konta może się wydawać kusząco łatwe, nie rób tego z domowego komputera

i z dziećmi. Oszczędność paru groszy na opłacenie abonamentu nie jest warta ryzyka utraty pracy. Załóż sobie prywatne konto.

Ponieważ pracodawcy coraz częściej ponoszą odpowiedzialność w związku z poczynaniami pracowników w sieci, wielu z nich ustala sztywne zasady korzystania przez personel z dostępu do Internetu. Większość zakazuje korzystania z konta przez niezatrudnionych i znacząco ogranicza zakres działań dozwolonych w sieci.

Poza tym Wielki Brat stale patrzy. W wielu Stanach USA dopuszczalne jest kontrolowanie przez pracodawcę elektronicznej poczty pracowników, jeśli pracodawca dostarcza sprzęt i dostęp do Internetu albo gdy pracownicy wyrażą zgodę na taki monitoring. To oznacza, że pracodawcy mogą czytać twoją korespondencję i sprawdzać, jakie strony odwiedzasz (albo jakie odwiedzają twoje dzieci). Jeśli pracodawca wykryje niewłaściwe używanie konta, może cię ukarać, a nawet zwolnić z pracy. Więc bądź ostrożny.

Rozdział 4

A teraz naprawdę poważne sprawy

W następnych podrozdziałach omówimy dokładnie trzy główne zagrożenia dla naszych dzieci w sieci: niewłaściwe użycie danych personalnych (ich i twoich), zagrożenia finansowe i zagrożenia dla ich osobistego bezpieczeństwa.

Jak chronić prywatność swoją i dzieci

Ilu z was było członkami klubu obchodzących urodziny Howarda Johnsona? (Nie wstydźcie się, nikomu nie przekażę tych informacji). Ja byłam. Dzięki temu, idąc do restauracji Howarda Johnsona w urodziny, dostawałam za darmo lody i posiłek. (Do dzisiaj nie mogę jeść smażonych krewetek, nie mamrocząc: „wszystkiego dobrego z okazji urodzin").

Kiedy moja córka wchodzi do marketu, pierwszą rzeczą, jaką robi, jest wpisanie się do książki gości i umieszczenie swojego nazwiska na liście tych, którzy są zainteresowani otrzymywaniem wiadomości o wyprzedażach i promocjach. W ten sposób ustawicznie wyzbywamy się cząstek swojej prywatności, by złapać różnorodne „okazje": lody, smażone krewetki, specjalne katalogi wyprzedaży.

❖ Zaglądaj im przez ramię

Nie spodziewamy się jednakże, że ktoś będzie próbował zebrać różne dane personalne wprost od naszych dzieci. Przykłady, które wcześniej podałam, o urodzinach Howarda Johnsona i o mojej córce wy-

pełniającej formularze wszędzie, gdziekolwiek robi zakupy, są bardzo na temat. (Czyż to nie wspaniałe, że któraś z moich dygresji jest na temat?). Jednak dzieci nie chodzą do Howarda Johnsona. To może być raczej miejsce, gdzie chcieliby jeść rodzice, a nawet dziadkowie, ale niekoniecznie nastolatki. To oznacza, że rodzice zawsze byli przy stoliku, gdy wypełniałeś kartę członkowską klubu. Zazwyczaj też chodzimy na zakupy z dziećmi, gdy są małe. Upewniamy się, że sobie poradzą, zanim pozwolimy im robić zakupy samodzielnie. Do tego momentu dzieci powinny już wiedzieć o zaśmiecaniu skrzynki ulotkami reklamowymi i o bezpośredniej akwizycji przez telefon. To znaczy, że powinny już umieć porównać korzyści płynące z otrzymania notki o wyprzedaży z zagrożeniem wynikającym z przekazania komuś swoich danych.

Na szczęście moja córka jest ostrożna. Ale to nie jest dziełem przypadku: to ja nauczyłam ją ostrożności. Nigdy nie podaje swojego prawdziwego numeru telefonu. Zostawia pustą rubrykę lub – jeśli musi coś wpisać – podaje zmyślony numer lub telefon do mego biura prawnego. Jak uczyłam ją ostrożności? Kiedy zobaczyłam pierwszy raz, że wypełnia formularz zgłoszenia, podeszłam i zapytałam, dlaczego to robi, sprawdziłam też, o jakie informacje jest proszona i jakich udziela, i wyjaśniłam, jakie ryzyko może się z tym wiązać. Dopóki była nastoletnim dzieckiem, nalegałam, by zawsze najpierw pokazała mi formularz. Wspólnie ustalałyśmy też, którym marketom można zaufać, a którym lepiej nie. (To najwyraźniej rodzinna tradycja, bo moja mama też sprawdzała moje formularze w zamierzchłych czasach mojej młodości).

❖ Z Internetem jest inaczej

Być może nie przeszkadza ci, kiedy twoje dziecko udziela pewnych osobistych informacji w twojej obecności i za twoją zgodą w realnym świecie, w firmach, które darzysz zaufaniem, ale czy zgadzasz się, żeby twoje dziecko wypełniało w Internecie formularze, wymagające przekazywania danych osobowych? Jeśli nie ma cię przy tym, jak masz wiedzieć, kiedy pouczyć je o wiarygodności i zaufaniu? Albo kiedy doradzić zrezygnowanie z konkursu, bo darmowy bawełniany podkoszulek nie równoważy ryzyka utraty prywatności?

Skąd możemy wiedzieć, że ta witryna jest rzeczywiście tą, za którą się podaje? Że nie należy do oszusta, który chce wyciągnąć numer

karty kredytowej od niczego nie podejrzewających wirtualnych nabywców? W normalnym świecie możemy odwiedzić sklep. Ktoś płaci czynsz za miejsce, opłaca abonament telefoniczny, zatrudnia pracowników. Ale w Internecie fikcyjna firma może prezentować się tak samo imponująco jak IBM. To sprawa rozwiązań graficznych i jeszcze 50 dolarów miesięcznie za miejsce w sieci.

Poza tym zbieranie danych w Internecie różni się od „normalnego" zbierania danych. Informacje mogą być uzyskiwane w wielu miejscach i tak przetworzone, że bardzo szybko powstaje całkiem pojemne dossier dziecka. Technologia pozwala na zbieranie pewnych danych nawet bez twojej wiedzy, np. informacji o tym, w jakich miejscach lubisz serfować, gdzie mieszkasz, ile czasu spędzasz w określonych obszarach sieci. W kilka minut można użyć tych informacji, by spreparować reklamę czy ogłoszenie dokładnie „na miarę" twojego dziecka – nawet w czasie tej samej sesji internetowej.

❖ Czy to poważny problem?

Gdy wydano moją pierwszą książkę „A Parents' Guide to the Internet", jeden z recenzentów napisał, że więcej stron poświęciłam zagrożeniom handlowym niż pornografii. Choć nie wierzę, że ktoś liczył strony czy ilość czasu, jaką poświęciłam każdej z tych spraw, to jednak jego opinia odzwierciedla moje sądy o powadze zagrożeń, jakie każda z nich niesie. I najwyraźniej poglądy rodziców są podobne. Według badań rodzice postrzegają zbieranie informacji personalnych od dzieci jako najważniejszy problem.

- 68% pytanych rodziców odpowiedziało, że niedopuszczalne jest domaganie się od dzieci ich adresu e-mailowego w celu sporządzenia statystyk częstości odwiedzania witryny i określania rodzaju aktywności, które tam podejmują.
- 56% uważa za niedopuszczalne pytanie dzieci o adres e-mailowy, zainteresowania i ulubione zajęcia w sieci wówczas, gdy zbiera się informacje w celu ulepszenia produktu (oferty).
- 72% rodziców uważa za niedopuszczalne domaganie się od dziecka prawdziwego adresu i nazwiska, gdy chce ono coś zakupić przez Internet lub zarejestrować się jako użytkownik witryny, nawet wtedy, gdy informacja ma być wykorzystywana tylko wewnątrz firmy.

- 97% uważa za niedopuszczalne domaganie się od dziecka prawdziwego adresu i nazwiska, gdy ono coś kupuje w sieci lub chce się zarejestrować jako użytkownik strony, a następnie udostępnianie tej informacji innym firmom.

❖ Co wiedzą i jak to wykorzystują?

Informacje zbierane od nas i od naszych dzieci oraz sposób ich użytkowania można podzielić na trzy kategorie:

- Śledzenie indywidualnych zainteresowań. Operator strony śledzi twoje poczynania na danej stronie i preferencje dla wewnętrznych celów marketingowych (żeby wiedzieć, komu wysłać wiadomość o nowych grupach muzycznych, a komu o nowym programie komputerowym, a wszystko na podstawie znajomości stron, które najchętniej odwiedzasz), by tworzyć dostosowane do twoich zainteresowań reklamy i ogłoszenia.
- Określanie preferencji całych grup demograficznych. Operator określa preferencje poszczególnych osób (w tej witrynie dziewczęta wybierają muzykę, chłopcy wybierają gry) i informacje demograficzne o grupie jako całości (ile dziewcząt, ilu chłopców, ilu 13-latków, ilu z miasta, ilu z małych miejscowości, chłopcy preferują gry, dziewczynki muzykę itp.), a uzyskane w ten sposób informacje dzieli z osobami trzecimi, np. z ogłoszeniodawcami, nie identyfikując pojedynczych osób. To pozwala operatorom na pozyskanie właściwych reklamodawców, a reklamodawcom zapewnia udane promocje.
- Udzielanie informacji personalnych innym w formie pozwalającej na identyfikację poszczególnych osób. Operator strony lub ktoś zamieszczający reklamę zbiera informacje od klienta i dzieli się nimi z trzecią osobą (np. Robert Kowalski mieszka w Krakowie, ma lat 11, posiada komputer Pentium MMX300, korzysta z serwera XX i spędza 2 godziny dziennie w sekcji gier witryny xyz.com).

Baza danych zebranych w ten sposób pozwala specjalistom od reklamy „podejść" dziecko bardzo skutecznie, przyciągając jego uwa-

gę wykorzystaniem w reklamie dotyczących go informacji. Wszyscy znamy imiennie adresowane reklamy typu: „Dzień dobry, pani Kowalska. Wiemy, że ma pani problemy z wagą...". Ponieważ w sieci wysyła się przekazy interaktywne, mogą one być znacznie bardziej chwytliwe.

Wielka Firma Sprzedająca Artykuły Lubiane Przez Dzieci (będą ją nazywać w skrócie Wielką Firmą) skupuje od kilku niezbyt etycznych stron WWW informacje, które one wydobyły od swoich rejestrujących się członków – małolatów (nie martw się, żadna z dziecięcych witryn, które polecam w tej książce, nie robi podobnych rzeczy). Tym sposobem wie, że Jaś ma dwójkę rodzeństwa i psa myśliwskiego i mieszka w Montclair, New Yersey. Gra jako obrońca w miejscowym klubie piłkarskim i lubi zespół Backstreet Boys. Ma 11 lat. Teraz, kiedy Jaś zaloguje się na jedną z tych stron, gdzie przez Wielką Firmę identyfikowany jest jako „Jaś", mogą pojawić się tam dopasowane do jego osoby reklamy. Ogłoszeniu może towarzyszyć muzyka Backstreet Boys i może ono przedstawiać jedenastolatka w małym mieście z psem myśliwskim, noszącego buty produkowane przez Wielką Firmę. Wielka Firma może wykorzystać migawkę z graczami klubu sportowego, którzy zajadają się tym gatunkiem sera i makaronu, który chciałaby sprzedać Jasiowi. Albo znajdzie w swojej skrzynce taki e-mail: „Cześć, Jasiu. Pewnie masz dość dzielenia się wszystkim z rodzeństwem? Ta nowa gra komputerowa zapewni ci trochę prywatności. Nikt nie będzie mógł w nią grać oprócz ciebie. Wprowadzasz swoje hasło i nikt inny nie ma do niej dostępu. To ulubiona gra komputerowa zespołu Backstreet Boys. A możesz ją kupić w sklepie Wielkiej Firmy w Montclair".

Sam zdecyduj, czy uważasz za uczciwe zwiększanie skuteczności reklamy poprzez takie wykorzystanie informacji personalnych o dzieciach. Sam też musisz zdecydować, czy ufasz akwizytorom, mającym o was tyle informacji. Czy naprawdę chcesz, by aż tyle wiedzieli o twoim 11-latku? (Zwłaszcza gdy rodzice o tym nie wiedzą i nie wyrażają zgody. Ale o prawie za chwilę).

Nie ma tu dobrej odpowiedzi. Niektórzy rodzice nie chcą, by ich dzieci udzielały jakichkolwiek informacji personalnych w jakichkolwiek okolicznościach, podczas gdy innym może zupełnie nie przeszkadzać fakt, że firmy i specjaliści od reklamy gromadzą dane dotyczące dziecka, a nawet udostępniają je innym, pod warunkiem że w zamian dostarczają informacje o produktach i odpowiednią obsługę.

Ale to powinna być twoja decyzja. Powinieneś wiedzieć, jakie dane są gromadzone i po co, powinieneś móc ufać operatorowi strony, gdy mówi, że uszanuje twoje decyzje, zwłaszcza gdy chodzi o młodsze dzieci. Operatorzy stron i reklamodawcy powinni zrozumieć, że świadomy rodzic może stać się ich sprzymierzeńcem.

❖ Jak zbierają dane?

Są dwa sposoby utraty anonimowości w sieci: dobrowolny, gdy dostarczasz informacji, rejestrując się w jakiejś witrynie czy wypełniając formularze; mimowolny, nieświadomy – poprzez „ciasteczka" (*cookies*) lub inną podobną technologię.

Dobrowolne informowanie: „Tak, proszę pani..."

Wychowujemy grzeczne dzieci (nie mówię o grzecznych nastolatkach, tylko o grzecznych dzieciach). Gdy dzieci są małe (określenie to obejmuje wszystkie dzieci, które mają nie więcej niż 12 lat), nie rozumieją w pełni wagi poufności danych personalnych. Gdy w jakimś formularzu ktoś pyta o nazwisko, adres i telefon, podają bez większego zastanowienia. A gdy jeszcze dodatkowo błyśnie im na horyzoncie szansa wygrania w konkursie atrakcyjnej nagrody, wszystkie dzieci i nastolatki gotowe są sprzedać własne dusze, nie mówiąc o przekazaniu dowolnych informacji personalnych.

Z czego zrezygnują dla podkoszulka

Wiele witryn domaga się, by dzieci tam wchodzące rejestrowały się, jeśli chcą brać udział w niektórych proponowanych zajęciach. Często bywa, że samo wypełnienie formularza uprawnia dziecko do „nagrody" w postaci kubeczka czy podkoszulka. Na innych stronach zachętą do podzielenia się danymi osobowymi może być płyta kompaktowa czy zdjęcie idola z autografem. Dzieci postrzegają to jako „dostawanie czegoś za darmo". Nie przychodzi im do głowy, że płacą za te „nagrody", podając informacje o sobie i ułatwiając przez to specjalistom od reklamy wywieranie wpływu. Nie przychodzi im (i nam) do głowy, że rozległe bazy danych o naszych preferencjach są tworzone przez całe nasze życie – właśnie po to, żeby handlowcy mogli nam sprzedać „produkty".

Do niedawna różne witryny domagające się rejestracji żądały od dzieci podawania prawdziwego imienia i nazwiska, adresu, telefonu, płci, adresu e-mailowego, daty urodzenia, czasem informacji o rodzinie (czy masz rodzeństwo, czy masz zwierzaka domowego). Niektóre pytały nawet, jak rodzice gromadzą pieniądze na ich dalszą naukę. I operatorzy tych stron nie zachęcali swoich klientów, by pytali rodziców o zgodę na przekazywanie tych wszystkich informacji. Ale to się, na szczęście, zmienia.

❖ Używanie technologii do zbierania danych

Co to są „ciasteczka" (cookies)?

„Ciasteczka" to pliki tekstowe (po prostu informacje, nie programy), które serwer strony WWW przesyła do twojego komputera poprzez przeglądarkę. Są one zainstalowane w pliku „ciasteczka" na dysku twardym i zawierają określone informacje. Te informacje mogą na żądanie zostać przesłane z powrotem do serwera. Używając ciasteczek, operator może powiedzieć, które strony odwiedzasz i wiele innych rzeczy o tobie i komputerze.

Ciasteczka nie są jednak całkiem złe (zwłaszcza czekoladowe wafelki wedlowskie). Wykonują wiele pożytecznych zadań, np. ułatwiają nam wstęp na strony wymagające rejestracji. Gdy rejestrujesz się pierwszy raz, plik ciasteczka zachowuje informacje, które podajesz, i przywołuje je, gdy przy następnej wizycie wypiszesz swoje hasło. Gdyby nie ciasteczka, musiałbyś za każdym razem wypełniać formularz zgłoszeniowy.

Ciasteczka są też przydatne, gdy robisz zakupy w sieci i chcesz kupić więcej niż jeden artykuł. To one umożliwiają zebranie wszystkich zakupionych rzeczy i przesłanie ich w tym samym czasie do serwera (czyli pełnią funkcję cybersklepowego wózka). W przeciwnym razie musiałbyś wybierać i kupować każdą sztukę oddzielnie.

Administratorzy stron korzystają z ciasteczek, by śledzić, dokąd udajesz się w sieci i co tam robisz. Dzięki nim wiedzą, że lubisz strony muzyczne, z modą i komputerowe, i że spędzasz w sieci czas po lekcjach aż do piątej po południu. Wiedzą też, że jesteś 16-letnią dziewczyną, bo im to sama powiedziałaś, rejestrując się. To, że mają w pamięci twoje preferencje, pozwala im lepiej projektować swoje strony i poprawić poziom oferowanych ci usług.

Wiele serwisów posługuje się ciasteczkami, by dopasować swoją ofertę do klienta, także do ciebie. Jeśli regularnie kupujesz w jednej z większych księgarni internetowych powieści kryminalne, zachowują tę informację, by następnie powiadomić cię o ukazaniu się pozycji tego rodzaju. To tak jakbyś miał swojego sprzedawcę, który wie, co lubisz, jaki rozmiar nosisz i czego szukasz.

Wielki Brat

Prawie wszyscy twórcy ogłoszeń i reklam instalują ciasteczka w swoich ogłoszeniach i śledzą, dokąd się udajesz, „przeklikując" się na ich stronę (chodzi o sytuację, gdy internauta, zobaczywszy ogłoszenie, klika w takim miejscu, że przechodzi od razu na stronę właściciela ogłoszenia). Na podstawie specjalnych umów o wymianie informacji niektórzy reklamodawcy i właściciele stron udzielają innym tak uzyskane wiadomości o klientach. Tym sposobem kilkanaście firm może mieć sporo informacji o twoich nawykach w sieci – pewnie więcej niż mógłbyś sobie życzyć. Wiedzą, że odwiedzałeś strony sportowe poświęcone golfowi, potem kliknąłeś na ogłoszeniu o sprzedaży sportowych pojazdów, potem sprawdzałeś repertuar okolicznych kin, szukając, gdzie grają ostatni film Disneya, zamówiłeś tam 3 bilety na dzisiejszy wieczór. Następnie przejrzałeś lokalną gazetę (już wcześniej się tam zarejestrowałeś) i przeczytałeś w niej ogłoszenia samochodowe.

Czego się o tobie dowiedzieli na podstawie tej sesji serfowania? Wiedzą, że grasz w golfa, albo chciałbyś to robić, i że poszukujesz samochodu wyższej klasy. Wiedzą, że masz jedno lub dwoje małych dzieci. Wiedzą, że masz kartę American Express, bo nią płaciłeś za bilety do kina. Wiedzą, w jakiej okolicy mieszkasz. Dodają te informacje do zebranych wtedy, gdy rejestrowałeś się jako czytelnik gazety lokalnej (nazwisko, czasem adres, zawód, płeć, dochód).

Na podstawie adresu mogą ustalić, że mieszkasz w eleganckiej okolicy, gdzie domy kosztują majątek. Mieszkają tam głównie młodzi, dobrze wykształceni ludzie z dziećmi. Teraz zaczniesz otrzymywać duże ilości reklam dotyczących samochodów albo reklamy od innych firm, zainteresowanych złowieniem młodego, dobrze zarabiającego człowieka. Możesz też dostawać mnóstwo śmieciowej poczty (tradycyjnej, nie elektronicznej). Jeśli mają umowy o wymianie informacji z firmami prowadzącymi sprzedaż w tradycyjnych sklepach, mogą ustalić, że masz 36 lat, niebieskie oczy i ciemne włosy, ważysz 81 kilogramów i nosisz okulary. (Często informacje wypisane w prawie jazdy są dostępne dla sprzedawców).

To prawdziwe przykłady informacji gromadzonych na nasz temat i wymienianych pomiędzy różnymi firmami. Zastanów się, jak powinniśmy się czuć, wiedząc, że mogą one mieć takie informacje również o naszych dzieciach.

Będziemy musieli znaleźć jakiś złoty środek pomiędzy zgodą na to, by różne witryny mogły dostosowywać swoją ofertę do potrzeb naszych i naszych dzieci, a zgodą na to, by pozbawieni skrupułów operatorzy gwałcili naszą prywatność, gromadząc dla własnych celów informacje o nas. Gdy w grę wchodzą „ciasteczka", rozwiązanie sprowadza się do podjęcia decyzji o tym, kiedy dziecko powinno je zaakceptować, a kiedy nie.

Co „ciasteczka" mówią innym o tobie i co możesz na to poradzić?

Istnieją miejsca w sieci, gdzie można sprawdzić, jakie informacje są dostępne dla innych poprzez ciasteczka. Junkbusters (www.junkbusters.com) ma wspaniałą stronę o ciasteczkach i prywatności. Kiedy odwiedzisz tę stronę, dowiesz się, jakie informacje o tobie i twoim komputerze można uzyskać poprzez przeglądarkę. Możesz być niemile zaskoczony.

Możesz sprawdzić katalog przeglądarki internetowej na twardym dysku i prawdopodobnie znajdziesz tam kilkanaście ciasteczek. Większość z nich ma słowo „ciasteczko" w nazwie. Są sposoby na usunięcie ciasteczek i anonimowe serfowanie. Zanim jednak coś usuniesz, sprawdź, czy nie potrzebujesz tego, by wejść na jakieś strony, na których się zarejestrowałeś. Jeśli usuniesz takie ciasteczka, będziesz musiał ponownie się rejestrować.

Przeglądarki sieci WWW, wersja 4.0 i dalsze, pozwalają na odrzucenie wszystkich ciasteczek. Pozwalają także (podobnie jak starsza wersja 3,0) usuwać ciasteczka pojedynczo, gdy są oferowane. Dowiesz się, jak to zrobić, odwiedzając strony: www.netscape.com lub www.microsoft.com.

❖ Czy ta wiedza jest im rzeczywiście potrzebna, czy też są zachłanni?

Możemy cieszyć się, że dostajemy oferty dostosowane do naszych potrzeb i indywidualnych preferencji, ale czy operatorzy stron i twórcy reklam nie zbierają więcej informacji, niż muszą?

By śledzić twoją drogę w sieci, operator nie musi znać twojego prawdziwego nazwiska czy miejsca zamieszkania. Nie potrzebują twojego nazwiska i adresu, by przysłać ci e-mail donoszący o nowościach z zakresu, który cię interesuje. Twórcy reklam również nie potrzebują tak naprawdę twojego nazwiska, adresu, numeru telefonu, żeby wiedzieć, co ci się podoba. Wystarczy, że wiedzą, iż dziesięcioletniemu chłopcu, który mieszka w New Yersey, podobają się niebieskie trampki na grubej podeszwie, a dziesięcioletniemu chłopcu, który mieszka w Kansas, podobają się czarne trampki na cienkiej podeszwie. Niepotrzebna im wcale wiadomość, że dziesięciolatek, który nazywa się Kuba Malinowski i mieszka na ulicy Dzięcioła pod numerem 21, preferuje czarne trampki na cienkiej podeszwie.

Choć możemy chcieć, by twórcy reklam ulepszyli swoje produkty i oferowali usługi, które odpowiadałyby naszym potrzebom, nie musimy w tym celu ryzykować utraty prywatności. Możemy uświadomić im nasze gusta, nie podając adresu, numeru telefonu oraz pełnego imienia i nazwiska. To oznacza, że to oni muszą się poważnie zastanowić, jakich informacji rzeczywiście potrzebują i jak mogą je uczciwie uzyskać.

A operatorzy stron powinni stale przypominać dzieciom, że podając jakieś dane personalne, muszą zawsze uzyskać zgodę rodziców. Sprawdź, czy strony odwiedzane przez twoje dziecko robią to. Jeśli nie, poinformuj operatora, jak się w związku z tym czujesz.

❖ Federalna Komisja Handlu (FTC) przybywa na ratunek!

W Stanach Zjednoczonych Federalna Komisja Handlu jest instytucją odpowiedzialną za sprawy ochrony danych osobowych dzieci na stronach komercyjnych w Internecie. Jest jedną z agend rządowych najlepiej zorientowanych w sprawach Internetu i zajmuje się nimi od początku istnienia sieci. FTC przeprowadziła liczne kontrole witryn dla dzieci w ciągu kilku ostatnich lat. Stwierdziła, że wiele z nich nie informuje rodziców (ani dzieci), jakiego rodzaju informacje zbierają od dzieci ani w jaki sposób chcą je wykorzystywać. Poza tym, choć wiele wykorzystuje zebrane informacje tylko wewnątrz firmy, są też takie, które je sprzedają lub na innych zasadach udostępniają reklamodawcom i firmom sprzedaży bezpośredniej.

W ciągu ostatnich lat FTC błagała i prosiła, z niewielkim skutkiem, by gospodarka internetowa przyjęła jakieś autoregulacje. Niestety, mimo różnych deklaracji zawsze znalazło się kilka firm, które nie traktowały sprawy poważnie.

To dlatego w październiku 1998 roku została uchwalona ustawa o ochronie danych osobowych dzieci – Children's Privacy Protection Act (obowiązuje od kwietnia 2000). Prawo to odnosi się tylko do stron komercyjnych i zapewnia rodzicom wgląd w rodzaj informacji o dziecku, które są gromadzone przez daną witrynę, jeśli dziecko nie ma 13 lat. Daje to rodzicom prawo decydowania, jak te informacje mogą być wykorzystane i komu udostępnione. Ustawa dotyczy wyłącznie dzieci młodszych niż 13-letnie. Wymaga od operatora strony skontaktowania się z rodzicem i uzyskania jego potwierdzonej zgody (to coś więcej niż tylko odpowiedź na e-mail) na udział dziecka w pogaduszkach czy innym systemie kontaktu jeden na jednego lub w klubach korespondencyjnych przyjaciół. FTC uważa, że skoro to są zajęcia wiążące się z najwyższym ryzykiem, rodzice powinni wiedzieć, że dzieci w nich uczestniczą. Ja także się z tym zgadzam.

Operatorzy witryn muszą również uzyskać zgodę rodziców, zanim przystąpią do gromadzenia danych, które pozwolą zidentyfikować dziecko. Są to: adres e-mailowy, pełne nazwisko i adres zamieszkania. Rodzice mają prawo wglądu w informacje, które posiada operator, mogą też zażądać ich usunięcia.

Na stronie Cyberangels planujemy otwarcie sekcji, w której będziemy przestrzegali przed dziecięcymi witrynami nie stosującymi tego prawa. Będziemy je odwiedzali i próbowali zachęcać do poszanowania prawa. Jeśli nic innego nie przyniesie pożądanych skutków – przekażemy informacje do FTC.

❖ Komu wierzysz?

Niektóre miejsca w sieci są godne zaufania, ale nie wszystkie. Rodzice muszą zdecydować, czy witryna budzi zaufanie, czy nie. Ale to, że

ufasz witrynie, która ma dane personalne twojego dziecka, nie znaczy, że ufasz wszystkim reklamodawcom, z którymi podzieli się tymi informacjami. Więc sprawdź, jakie przyjęto w niej zasady ochrony danych. Jeśli nie ma żadnych albo są niejasne, nie pozwalaj dzieciom tam serfować, dopóki operatorzy czy właściciele nie ustalą czytelnych zasad ochrony danych.

A jeśli przedstawili politykę ochrony danych, to czy ujawnili, jakie wiadomości gromadzą i w jaki sposób je uzyskują? Czy zbierają więcej, niż potrzebują? Jeśli dzielą informacje z osobami trzecimi, czy robią to tylko w formie zbiorczej, tzn takiej, która nie pozwoli na zidentyfikowanie dziecka? Z kim dzielą te informacje? Z reklamodawcami czy nieokreślonymi trzecimi firmami? Kim są ci reklamodawcy, czy są godni zaufania, czy możesz ufać, iż nie zrobią złego użytku z danych twojego dziecka? Czy reklamodawcy przysłali informacje o własnych zasadach ochrony danych, powiadamiając cię, co robią z uzyskanymi na temat twojego dziecka informacjami? Jeśli nie, zapytaj ich o to. Daj im do zrozumienia, że ochrona prywatności twojego dziecka jest dla ciebie ważna.

Jeśli nie zamieścili na stronie informacji, jak można się z nimi skontaktować (jak żąda tego ustawa), wyślij e-mail do Webmastera, który powinien je dostarczyć.

Jak się bronić przed oszustwami i nieuczciwym marketingiem w sieci

❖ Cyberbrzdąc jako cel: internetowa reklama skierowana do dzieci

Ponieważ coraz więcej dzieci korzysta z Internetu, coraz więcej handlowców usiłuje tam sprzedać dzieciom różne rzeczy i poszukuje o nich i o tobie informacji, które ułatwią im to zadanie. Reklama internetowa, w porównaniu z reklamą telewizyjną, to ciągle Dziki Zachód; a jeśli chodzi o marketing skierowany do dzieci – to Dziki Zachód w pierwszych dniach gorączki złota.

Jak łakomym kąskiem jest rynek dziecięcy?

Mimo że reklama w sieci nie przyniosła aż takich dochodów, jakich reklamodawcy się spodziewali, wszyscy wiedzą, że tam jest przyszłość. Statystyki przemawiają do wyobraźni handlowców:

- Roczne wydatki w jakiś sposób związane z dziećmi to suma 150 miliardów.
- Na reklamy telewizyjne kierowane do dzieci wydaje się 700 milionów dolarów rocznie.
- Sprzedaż artykułów komputerowych dla dzieci przekracza 5 miliardów dolarów rocznie (1,6 mld sprzęt, a 3,5 mld oprogramowanie).

Dzwoni, dzwoni cały czas

By uświadomić sobie wpływ, jaki reklama może mieć na dzieci, wystarczy przypomnieć sobie, ile znają one tekstów reklamowych i jak małe były, gdy rozpoznawały reklamowane zabawki.

Dzieci są niesłychanie podatne na wpływ mediów.

Twoim zadaniem jest uczyć dzieci być bystrymi konsumentami – hasło „myślący nabywca" powinno być waszą maksymą. Być bystrym konsumentem w Internecie to dokładnie to samo co być nim w życiu, z jedną wszakże różnicą. Internetowe reklamy są bardzo zindywidualizowane. Opracowano je tak, by przemówiły do jednego konkretnego dziecka – mogą posługiwać się jego imieniem, imieniem jego zwierzaka czy nazwą miasta, by skuteczniej zadziałać. Ponadto są interaktywne i mogą działać jak hipnoza. Zadaniem rodziców jest pomóc dzieciom oddzielić reklamowe fakty od fikcji i ograniczyć liczbę reklam docierających do nich w sieci. Musimy nauczyć je odróżniać ziarno od plewy także wtedy, gdy ogłoszenie „jest dla nich". Nasze dzieci muszą umieć rozszyfrowywać reklamy.

Pomóżmy dzieciom zrozumieć, gdzie kończy się treść, a zaczyna reklama

Jedną z ważniejszych spraw w związku z reklamą skierowaną do dzieci jest konieczność uświadomienia im, w którym momencie kończy się program i zaczynają reklamy. Zastanawialiście się, czemu w trakcie dziecięcych programów słyszymy: „A teraz słowo od naszego spon-

sora...". Telewizyjne reklamy skierowane do dzieci są nadzorowane przez Federal Communications Commission od 1974 roku. W czasie programów dziecięcych reklamy mogą być nadawane dopiero po 5 sekundach przerwy po właściwym programie. Ta przerwa to znak, że program się skończył, a zaczyna reklama. Stąd i zapowiedzi.

Ponadto ustalono, że należy ograniczyć ilość czasu, który może być przeznaczony na reklamy w czasie bloku programów dziecięcych. Wprowadzono też różne inne restrykcje, by zapobiec zamianie kreskówek w niekończący się ciąg reklam. Reklama produktu nie może być integralną częścią pokazu filmowego, a jego bohaterowie nie mogą występować w reklamach nadawanych w czasie tego programu.

Ale w cyberprzestrzeni te restrykcje jeszcze nie obowiązują. Na razie nie ma szczególnych regulacji prawnych dotyczących internetowej reklamy skierowanej do dzieci, poza ogólną zasadą, że wszystkie reklamy i strony sponsorowane muszą być odpowiednio oznaczone.

Co zrobiono w związku obawami rodziców przed reklamą?

Robaczek Reklamowy

Bardzo popularna witryna dla dzieci poniżej 14 roku życia i jedna z pierwszych stworzonych z myślą o dzieciach – KidsCom, wysuwa się na czoło, jeśli chodzi o pomaganie dzieciom w identyfikowaniu reklam w sieci. Wprowadziła Robaczka Reklamowego (Ad Bug), bohatera kreskówek, który pokazuje reklamy i materiały promocyjne na stronach KidsCom.com i innych biorących udział w tej akcji. Dzięki uprzejmości KidsCom, WiredKids.org – witryna zajmująca się wszystkimi problemami dzieci w sieci (którą prowadzę) – będzie mogła zaoferować Robaczka także innym witrynom. Jest to pomysł szczególnie pomocny dla najmłodszych użytkowników, którzy nie potrafią jeszcze przeczytać słowa „reklama".

❖ Jak przemysł reklamowy próbuje regulować swoje działania?

W odpowiedzi na niepokoje rodziców w USA 25 lat temu powstała sekcja oceny reklamy dziecięcej Rady Biur Dobrego Biznesu, która stworzyła obowiązkowe standardy reklamy dziecięcej i wskazówki na temat gromadzenia danych i ochrony prywatności.

Podstawowa zasada brzmi: „Zawsze należy uprzedzić dzieci, że są poddawane oddziaływaniom mającym na celu sprzedanie im czegoś". W wytycznych zaleca się także reklamodawcom dołożenie właściwych starań w celu upewnienia się, że dzieci dokonują zakupów za zgodą rodziców. W przeciwnym wypadku rodzice powinni mieć prawo do zrezygnowania z zakupu i odzyskania całości kosztów. Reklamodawcy i ogłoszeniodawcy powinni też wiedzieć, że w świetle obowiązującego prawa rodzice mogą nie ponosić odpowiedzialności za kontrakty zakupu podpisane przez ich dzieci.

Handlowcy dostosowują się dobrowolnie do tych regulacji. Wielu z nich ma na względzie dobro dzieci. A wszyscy rozumieją, że jeśli firmy sprzedające w Internecie artykuły dla dzieci nie zaczną uwzględniać obaw rodziców dotyczących ochrony prywatności ich dzieci, to rodzice mogą spowodować pojawienie się twardych regulacji prawnych internetowego rynku reklam dla dzieci. Zresztą reklamodawca nic nie osiągnie, odsuwając rodziców. Najsprytniejsi to wiedzą. Daj znać operatorom tych stron, które wykonują dobrą robotę, zachowując umiar w reklamowaniu, że pochwalasz ich postępowanie. Na tych, którzy twoim zdaniem prowadzą nieodpowiedzialny marketing wobec dzieci, zgłaszaj skargi. Gdy zorientują się, że uczciwa postawa procentuje zwiększoną sprzedażą, bardzo szybko dostosują się do wymagań.

Więc powtarzajcie za mną: „Rodzice to potęga! Rodzice to potęga! Rodzice to potęga!".

❖ Wydawanie pieniędzy – czyli to, co dzieci i nastolatki robią najlepiej

Sumy, jakie dzieci i nastolatki wydają w sieci, rosną w postępie geometrycznym, a analizy dowodzą, że ta tendencja się utrzyma.

Dzieci i nastolatki mogą kupować w Internecie towary na trzy sposoby. (Mogą nawet sprzedawać i wymieniać rzeczy). Wielu znanych handlowców i producentów oferuje swoje wyroby w sieci. Są zaprojektowane specjalnie dla celów komercyjnych witryny, które umożliwiają dzieciom zakładanie własnych kont i kupowanie dowolnych towarów, uzgodnionych z rodzicami. Ostatnio mogą też kupować (i sprzedawać czy wstawiać w komis) rzeczy w witrynach aukcyjnych.

Nic za darmo: jak się płaci za zakupy w Internecie?

Najpierw pokrótce omówię sposoby płacenia za zakupy w Internecie, informując, na co należy uważać przy takich transakcjach.

Są zasadniczo cztery sposoby płacenia za rzeczy kupione w Internecie: czeki (wysłane faksem lub pocztą), karty kredytowe, karty debetowe i karty dostępu do elektronicznych pieniędzy. Zasady bezpieczeństwa w sieci są właściwie takie same jak te obowiązujące w realnym świecie (nie udzielaj innym informacji o swojej karcie kredytowej, upewnij się, że nikt nie ma dostępu do hasła karty debetowej, regularnie sprawdzaj wyciągi z kart kredytowych i debetowych, by wykryć bezprawne ich użycie). Istnieje jednak kilka zasad specyficznych tylko dla Internetu.

Przede wszystkim nigdy nie używaj czeków, gdy płacisz za coś w sieci. Ochrona nabywców płacących czekiem za zakupy w sieci nie jest wystarczająca. Jeśli sprzedawca domaga się czeku lub przesłania faksem dowodu wpłaty, zrób zakupy gdzie indziej. Jeśli dbasz o swoje bezpieczeństwo, używaj zawsze karty kredytowej, robiąc zakupy w Internecie.

Karty kredytowe mają określone procedury ochrony konsumenta, gwarantowane prawnie. Pozwala to, w większości wypadków, na odzyskanie pełnej kwoty, jeśli coś źle zadziała. Właśnie ze względu na wysoki poziom ochrony konsumenta, jeśli nie masz karty kredytowej, zorientuj się, czy nie możesz pożyczyć jej od znajomego. Karta debetowa nie gwarantuje konsumentowi takiego samego poziomu bezpieczeństwa, chociaż jeśli szybko zgłosisz nielegalne użycie karty debetowej, od tego momentu jesteś chroniony.

Karty o określonej wartości pozwalają na pewien poziom ochrony prywatności, ale mogą być równie niebezpieczne jak gotówka. Jeśli nie są częścią specjalnego systemu płatności, w przypadku gdy kartę zgubisz, to tak jakbyś utracił wszystko. Traktuj je jak karty telefoniczne – jeśli ktoś je znajdzie, może ich użyć tak jak gotówki.

Czy to jest bezpieczne?

Większość hakerów nie dba o informacje dotyczące twojej karty kredytowej. Im chodzi o pełną bazę danych o numerach kart kredytowych. Przechwytywanie pojedynczych e-mailów jest mało dochodowe, a bardzo męczące ze względu na metody przekazywania danych w sieci. (Większa informacja jest na czas przesyłania dzielona na

mniejsze kawałki, zwane „pakietami". Pakiety są przesyłane różnymi drogami internetowymi i składane na powrót w całość w miejscu docelowym – czyli w internetowym sklepie).

Dzieciom mogą się przydać informacje o twojej karcie, więc jeśli przechowujesz je w komputerze, zabezpiecz je hasłem.

Każdy, kto rozumie możliwe zagrożenia, wie, że transakcje z użyciem kart kredytowych w sieci są bezpieczne przynajmniej w takim samym stopniu jak poza siecią. (Czyż nie jesteś zaniepokojony, gdy kelner czy pracownik stacji benzynowej bierze twoją kartę i wczytuje ją gdzieś na zapleczu?). Ale są określone kroki zabezpieczające, które należy podejmować, by mieć pewność, że przeprowadzane przez ciebie transakcje są w miarę możliwości bezpieczne.

Zawsze używaj „bezpiecznego" serwera. Możesz też spojrzeć na adres strony WWW. Czy jest tam oznaczenie „http", jak przy większości stron, czy oznaczenie „https", co oznacza bezpieczny serwer? Przyjmujący płatności na ogół zamieszcza też na swojej stronie informacje o zabezpieczeniach i sposobie przekazywania informacji finansowych, takich jak numery kart kredytowych. Dowiedz się, jak zabezpieczają takie dane. Nigdy nie rób zakupów w miejscach, które nie podają żadnych informacji albo proponują niewystarczające zabezpieczenia.

Poza tym regularnie sprawdzaj wyciągi bankowe dotyczące kart i zachowuj kopie wszystkich zamówień składanych w Internecie. Jeśli stwierdzisz nieprawidłowości, natychmiast skontaktuj się z bankiem czy instytucją, która wydała kartę. Twoje prawa mogą zależeć od tego, jak szybko zgłosisz nieprawidłowości czy defraudację. Więc nie zwlekaj – zrób to natychmiast. I pamiętaj, że rozmowa telefoniczna może nie być wystarczającą formą zgłoszenia nieprawidłowości – może być wymagane wysłanie zgłoszenia listem poleconym.

Czy wiesz, z kim handlujesz w Internecie?

Sprawdź, kim jest sprzedający, zanim coś kupisz. Jeśli masz do czynienia ze znaną firmą, prawdopodobnie można wierzyć, że w sieci zachowuje ten sam poziom dbałości o klienta, jaki prezentuje w realnym świecie.

Istnieją także firmy mniej nam znane, bo prowadzące działalność wyłącznie w Internecie. Są na ogół także godne zaufania. Są poza tym firmy „wprowadzane" przez instytucje, którym ufasz, czy takie,

do których są odnośniki z twego portalu (czyli z miejsca, gdzie zaczynasz serfowanie).

Ale co myśleć o milionach innych firm działających w sieci? Tak jak sprawdzasz firmę wysyłkową, możesz sprawdzić firmę internetową w serwisach konsumenckich. Tam uzyskasz informacje o wcześniejszych zażaleniach konsumentów i stosownie ocenisz sprzedającego.

Nie prowadź transakcji z żadną określoną osobą, zanim nie ocenisz ryzyka. Większość praw chroniących konsumenta odnosi się do firm, nie do osób fizycznych. To oznacza, że będziesz zdany na własne siły w dochodzeniu swoich praw. Ponadto większość indywidualnych sprzedawców nie ma rachunków handlowych, które pozwalają przyjmować zapłatę kartami kredytowymi, więc klient zmuszony jest do płacenia czekami, gotówką lub przekazami. A to oznacza, że wtedy, gdy płatność zostaje zakwestionowana, poziom zabezpieczenia interesów kupującego jest nieporównywalnie niższy, niż w sytuacji, gdy używa karty kredytowej.

Witryny prowadzące aukcje stworzyły taki system zbierania opłat, w którym powiernik (za prowizję równą 5% wartości zakupu) przyjmuje od kupującego zapłatę, a od sprzedawcy towar, i kiedy wszystkie sprawy między kupującym a sprzedającym zostaną ustalone – przekazuje nabywcy towar, a sprzedającemu pieniądze. To może być bardzo wygodny system, gdy ma się do czynienia ze sprzedawcami będącymi osobami fizycznymi. Możesz zażyczyć sobie dostarczenia zakupu do skrytki pocztowej – tym sposobem nie ujawnisz nikomu swego prawdziwego adresu. Ale jeśli płacisz czekiem, twój adres jest wydrukowany w nagłówku, więc i tak jest już ujawniony.

Zawsze zgłaszaj wszelkie problemy, z jakimi się spotkasz. Im więcej swoich doświadczeń przekazujemy innym, tym szybciej będziemy w stanie ulepszyć internetowy handel i wyeliminować nieuczciwych.

❖ Zakupy w sklepie internetowym

Dokonując takich zakupów, zawsze sprawdź zasady ochrony prywatności i to, jak zarządzający witryną zamierzają traktować informacje uzyskane od klientów. Niektóre witryny oferują artykuły, które dzieci uwielbiają kupować. Możesz je kupować bezpośrednio w sieci, tak samo jak kupuje się w większości firm wysyłkowych na podstawie katalogu. To miejsca godne zaufania. Ale czy czujesz się całkiem bezpiecznie, jeśli dzieci mające dostęp do twojej karty kredytowej kuszone są zabawkami i modnymi ciuchami?

E-handel dla dzieci – gdzie mogą bezpiecznie robić zakupy?

Wielu rodziców nie chce, by dzieci używały ich kart kredytowych do robienia zakupów w sieci. Chcą też mieć pewność, że dzieci kupują w miejscach godnych zaufania. Dlatego powstał nowy model e-handlu. Witryny zajmujące się handlem artykułami dziecięcymi umożliwiają rodzicom założenie linii kredytowej dla dzieci. Dzięki temu unikalnemu systemowi (który pomagałam stworzyć) dzieci za wiedzą rodziców mogą oszczędzać, robić zakupy, tworzyć listy życzeń i wpłacać na organizacje charytatywne z bezpiecznego rachunku internetowego.

Wymóg rodzicielskiej zgody daje rodzicom pewność, że dzieci i nastolatki wydają pieniądze tylko w sposób wcześniej przez rodziców zaaprobowany. Kiedy np. dziadkowie chcą wiedzieć, co mała Zuzia chciałaby na urodziny, zaglądają do jej listy życzeń i po prostu wybierają jakąś rzecz, obciążając swój rachunek, a prezent jest odsyłany bezpośrednio do wnuczki. Rodzice mogą zlecić, żeby kieszonkowe dziecka było automatycznie dopisywane do jego rachunku.

Jest wiele różnych witryn zajmujących się handlem artykułami dziecięcymi i spodziewam się, że powstanie ich jeszcze więcej. Oceniając je, powinieneś wziąć pod uwagę następujące trzy rzeczy:

1. Czy przywiązują odpowiednią wagę do ochrony prywatności dziecka? Czy mówią, jakie informacje zbierają i jak je wykorzystają? Czy pytali o twoją zgodę na wstąpienie dziecka poniżej 13 roku życia?
2. Czy gwarantują, że sprzedawcy nie będą oferowali dzieciom artykułów dla dorosłych (np. Playboya na kasetach wideo)?
3. Czy żądają od sprzedawców podpisania zgody, że nie będą wykorzystywać danych kontaktowych do promocji, bezpośredniego marketingu, informowania o wyprzedażach? Czy sprawdzają przestrzeganie tych zasad przez sprzedawców?

Jeśli na któreś pytanie nie możesz odpowiedzieć „tak", raczej rób zakupy w innym miejscu. Dobrze jest mieć możliwość wyboru. I poinformuj ich, dlaczego zrezygnowałeś z ich usług, by mieli szansę wziąć pod uwagę twoje zastrzeżenia.

❖ Co należy wiedzieć o aukcjach w Internecie

Jeśli kochasz pchle targi, tandety, wyprzedaże, giełdy czy jarmarki, spodobają ci się internetowe aukcje. Możesz kupić wszystko, od nowych komputerów do fasoli w strąkach, często po okazyjnych cenach i nie zdejmując kapci i szlafroka. Włączasz się do licytacji i jeśli zalicytujesz najwyżej – wygrywasz!

W ten sposób sprzedaje się mnóstwo zbiorów kolekcjonerskich, sprzęt komputerowy, sporo nowych rzeczy i trochę śmieci (chyba że są to prawdziwe skarby, których zawsze poszukiwałeś). Jeśli się tam zapuścisz, na pewno coś kupisz, wierz mi.

Aukcje w sieci: po raz drugi... po raz trzeci... sprzedane!

Aukcje internetowe to wspaniałe miejsca dla amatorów okazji. Ale jeśli nie jesteś ostrożny, możesz dostać mniej, niż ci się wydawało. Klienci takich witryn najczęściej skarżą się, że towaru wcale nie dostarczono lub został uszkodzony w czasie transportu, albo okazał się niezupełnie tym, co klient licytował.

Oto lista rzeczy, które powinieneś zrobić, jeśli chcesz kupować w witrynach aukcyjnych:

- Upewnij się, że to wiarygodna witryna. Zażalenia na defraudację przy okazji aukcji były częstsze niż zażalenia na jakiekolwiek inne oszustwa, składane w Internecie. Sprawdź najpierw witrynę przy pomocy organizacji ochrony praw konsumenta. Jeśli uzyskane informacje budzą wątpliwości, idź w inne miejsce. Możesz także „popytać" w grupach dyskusyjnych czy poszukać aukcji polecanych przez witryny, którym ufasz.
- Dobrze zapoznaj się z witryną aukcyjną. Dowiedz się, jak pracuje, jakie obowiązują zasady reklamacji i zwrotu towarów (czy zwrot wiąże się z opłatami manipulacyjnymi?), kosztów przesyłki, ubezpieczenia, warunków gwarancji. Zwróć też uwagę na liczbę punktów świadczących usługi gwarancyjne i procedurę składania reklamacji.
- Unikaj indywidualnych sprzedawców (nie firm) i postaraj się poznać osobę, od której kupujesz. Jeśli koniecznie musisz mieć coś, co sprzedaje jakaś prywatna osoba, sprawdź

ją uważnie. Poproś o kontakt poza siecią i adres e-mail. Sprawdź, czy serwisy wyszukiwania ludzi w Internecie podadzą takie same informacje. Spróbuj ustalić telefon na podstawie posiadanego adresu e-mail i odwrotnie (czyli przeprowadź takie poszukiwania, jakie przedstawiłam w rozdziale 2). Jeśli witryna ma „książkę skarg i wniosków", sprawdź, co inni nabywcy mieli do powiedzenia na temat sprzedającego. Musisz też wiedzieć, że niektórzy handlowcy po prostu sami wypełniają takie książki pochwałami, by wzbudzić zaufanie ewentualnych nabywców. A konkurencja dla odmiany często umieszcza negatywne opinie, usiłując zniechęcić potencjalnych klientów. Więc wszelkie opinie traktuj raczej ostrożnie. Jeśli należysz do jakiejś grupy kolekcjonerskiej, możesz tam zapytać, czy ktoś nie został oszukany przez tego sprzedawcę albo czy nie zna kogoś bardziej godnego zaufania. Podziel się swoimi doświadczeniami, niezależnie od tego, czy będą one złe, czy dobre, by mogły posłużyć także innym.
- Upewnij się, że znasz warunki płatności, zanim przystąpisz do licytacji. Jeśli zgłosisz ofertę, akceptujesz podane warunki niezależnie od tego, czy są ci znane, czy nie. Nieznajomość tych warunków nie zwalnia z konieczności podporządkowania się im.
- Nie wierz we wszystko, co usłyszysz. Jeśli oferują ci kolekcjonerski rarytas, zdobądź rzetelną wycenę i kupuj tylko w miejscach godnych zaufania. Wielu sprzedających usiłuje wcisnąć arytykuły podrobione jako prawdziwe. Jeśli oferta wygląda na zbyt dobrą, żeby mogła być prawdziwa, prawdopodobnie nie jest prawdziwa. Nie trać zdrowego rozsądku tylko dlatego, że poruszasz się w sieci. Gdybyś nie zdecydował się na jakiś zakup w tradycyjnym sklepie, nie decyduj się na niego i tutaj. Nie ulegaj naciskom, że trzeba coś kupić „natychmiast".
- Nie kupuj przez Internet nielegalnych artykułów – łatwo możesz zostać „namierzony". Nawet jeśli nie będzie cię szukać policja, czy naprawdę chcesz, by ludzie trudniący się takim procederem mieli twój domowy adres, telefon i numer karty kredytowej? W Internecie ludzie sprzedają prace dyplomowe, fałszywe dowody tożsamości i właściwie prawie

wszystko, co można sobie wyobrazić. (Ostatnio znaleźliśmy kogoś, kto w jednej z aukcji sprzedawał coś, co mogło być pornografią dziecięcą. Prowadzący aukcję wycofał to ze sprzedaży natychmiast po uzyskaniu od nas wiadomości, ale to daje wyobrażenie o tym, jacy ludzie tam „bywają").

- Używaj bezpiecznej metody płacenia należności. Jeśli to możliwe, korzystaj z usług agenta powiernika i dostępnych zabezpieczeń. Niektóre witryny oferują nabywcom różne opcje, by uchronić ich przed drobnymi stratami.
- Planuj z wyprzedzeniem. Sprawdź ceny w innych miejscach, nie prowadzących aukcji. Zdecyduj, ile możesz wydać, i tego się trzymaj. Wiele nowych witryn aukcyjnych daje możliwość określenia z góry kwoty, do której licytujesz wybrany przedmiot. To dobry pomysł, bo wielu ludzi wpada w gorączkę i licytuje wyżej niż powinni. Jest to także ważne, gdyby naszym dzieciom zdarzyło się wejść na strony aukcyjne.

Krzywdziciele dzieci: cyberprześladowcy – prawdziwe zagrożenie w przestrzeni wirtualnej

❖ „Zostaw moje dziecko w spokoju!" – nękanie i napastowanie poprzez Internet

Cybernękanie to nie jest sytuacja, gdy dorosły usiłuje spotkać dziecko w realnym życiu, by je molestować. (To uwodzenie lub napastowanie). Cybernękanie to sytuacja, gdy ktoś kogoś dręczy i śledzi w sieci albo używa Internetu jako środka do sprowokowania prześladowań lub konfrontacji w realnym świecie.

Istnieją trzy rodzaje cybernękania:

1. Napastowanie, które odbywa się tylko w sieci.
2. Nękanie dziejące się głównie w sieci, ale wychodzące również poza sieć lub mające jakieś komponenty w realnym życiu.

3. Dręczenie i nękanie dziejące się w realnym świecie, które ma także jakieś komponenty w sieci.

Wszystko to są rzeczy przerażające, ale fizycznie groźne jest tylko dręczenie i nachodzenie, dziejące się w realnym świecie. (Jakikolwiek związek z realnym światem kwalifikuje sprawę jako prześladowanie w realnym świecie).

Najczęściej to kobieta jest nękana przez mężczyznę, choć celem ataków może być także dziecko. Znany jest przypadek nękania z udziałem dziecka, gdy sąsiedzi pokłócili się, a następnie jeden z nich przekazał w grupie dyskusyjnej wiadomość, że mała córka jego sąsiada bardzo interesuje się seksem. Podał jej adres i telefon. Ciągle natykamy się na imiona wypisane na ścianach toalet, ale w tym przypadku „ścianę toalety" w samych tylko Stanach ogląda 86 milionów ludzi. W rezultacie rodzina ta została zmuszona do zmiany miejsca zamieszkania. A wcześniej dowiedziała się, że nawet gdyby w tej sprawie wniosła oskarżenie, to przypadek byłby traktowany tylko jako wykroczenie.

Pod wpływem tego zdarzenia w USA powstało prawo chroniące dzieci przed napaściami dorosłych, jeśli zawarta jest w nich zachęta do działań seksualnych lub domniemanie aktywności seksualnej. Dorośli nękani w podobny sposób mają za sobą tylko stanowe prawo o cyberprześladowaniu.

Ostatnio pewna kobieta z Kalifornii była nękana przez Internet. Był to pierwszy przypadek postawienia kogoś w stan oskarżenia na podstawie nowego prawa dotyczącego cybernękania. Ofiara sama nigdy nie używała Internetu. Prześladowca wszedł do grupy dyskusyjnej zajmującej się tematem seksu i ogłosił, że ta kobieta zainteresowana jest grupowym seksem z mężczyznami. Podał jej adres. Ochotnicy zjawili się pod drzwiami. Na szczęście od razu zrozumieli, o co chodzi, i znikli, gdy ich o to poprosiła. Ale i tak było to przerażające. Internet może być potężnym narzędziem, gdy chodzi o skrzywdzenie kogoś.

Kim jest typowa ofiara?

Najczęściej ofiarą cybernękania jest początkujący internauta, nie znający zasad etykiety sieciowej. Na ogół napastnik czuje się silniejszy dzięki anonimowości w Internecie. Ma wrażenie, że może się bez-

piecznie ukrywać za swoim monitorem. Ale jeśli nie masz do czynienia z naprawdę chorym człowiekiem lub kimś, kto ma jakiś własny interes w nękaniu cię, większość szybko traci zainteresowanie zabawą, jeśli nie budzi reakcji, o jaką im chodziło.

Co z nękaniem w Internecie, które przenosi się do realnego świata?

Choć większość przypadków cybernękania zaczyna się i kończy w sieci, to jednak niektóre przenoszą się do realnego świata. Wtedy rzecz staje się bardzo niebezpieczna. Napastnicy odnajdują upatrzoną osobę w realnym świecie, używając wszystkich sposobów odszukiwania ludzi, które przedstawiłam w rozdziale 2. Są w stanie odnaleźć adres domowy, adres szkoły, do której chodzi dziecko, i numery telefonów. Grożą, używając telefonu lub zwykłej poczty, albo przekazują twoje dane kontaktowe innym w Internecie, zachęcając ich do nękania ciebie.

To bywa naprawdę groźne. Przedstawiałam już opowieść „Droga Jennifer, mam zamiar cię zabić", której bohaterka nie była w stanie opuścić domu, by pójść do pracy. Ostatnio zadzwoniła do mnie matka w panice: jej 14-letni syn otrzymywał w Internecie pogróżki, które przerodziły się w groźby przekazywane telefonicznie. Syn był przerażony, a ona miała zamiar trzymać go pod kluczem, dopóki prześladowca nie zostanie odnaleziony. Chciała także wzmocnić domowy system alarmowy, dodając kolejny alarm przeciwwłamaniowy.

Cyberprześladowca zdawał się wiedzieć o jej synu więcej, niż ktoś, kto mógłby go znać tylko z sieci. Przejrzałyśmy krok po kroku wszystkie ryzykowne miejsca. Zapytałam, czy syn umieścił w sieci swój profil. Okazało się, że tak. Ale powiedział, że podał tam tylko imię i wiek, nic nie mówiąc o miejscu zamieszkania czy szkole. Powiedział też, że nigdzie w sieci nie podawał takich informacji i że najczęściej gawędzi ze swoimi kolegami ze szkoły. Kolejna pogróżka pochodziła z pobliskiego automatu telefonicznego. Policja została włączona w sprawę i natychmiast zwróciła się do AOL o ustalenie tożsamości cyberprześladowcy. (AOL dostarcza takich informacji wyłącznie na wezwanie sądu lub w przypadku prowadzonego przez policję śledztwa, a i wtedy daje najpierw swemu klientowi szansę podjęcia zgodnych z prawem działań, blokujących ujawnienie). Gdy cyberprześladowca zaczyna działać także poza siecią, większość policjantów czuje się pewniej i chętniej podejmują śledztwo.

To przerażające być nękanym...

Nie należy czekać, aż nękanie przeniesie się poza sieć. Ale na tym wczesnym etapie może wcale nie być łatwo sprawić, by ktoś potraktował poważnie twoje lęki. Możesz słyszeć rady typu: „To niech pani wyłączy komputer", „To tylko słowa", „A czym się tu przejmować?" od ludzi, którzy sami nigdy nie byli celem podobnych ataków, którzy nie rozumieją przerażenia i terroru, w jakim żyją ofiary tych dręczycieli.

Każdy, kto był kiedykolwiek celem nękania w Internecie, powie ci, że jest ono równie przerażające jak nękanie poza siecią. Może być nawet odczuwane jako bardziej osobiste, gdyż prześladowca niejako „wchodzi" do wnętrza domu poprzez komputer.

W większości przypadków osobą nękającą twoje dziecko jest jakieś inne dziecko. Może to być również ktoś, kogo twoje dziecko uraziło, szukający sposobów zemsty. Ale ponieważ większość przypadków cybernękania pojawia się w związku z potrzebami seksualnymi czy odrzuconymi zalotami, cyberprześladowcy na ogół tracą zainteresowanie, odkrywając, że mają do czynienia z dzieckiem. Pedofile, którzy wyszukują nieletnie ofiary, nie stosują nękania i straszenia upatrzonych obiektów, raczej uwodzą je i mamią.

W miarę jak coraz więcej nastolatków angażuje się w zwykłe cyberflirty, wzrasta ryzyko, że staną się celem cybernękania. A procent dziewcząt, które angażują się w pogawędki zawierające seksualne aluzje, niestety co dzień wzrasta.

Większość cyberprześladowców rozgląda się za nowicjuszami w cyberprzestrzeni. W miejscach, gdzie najczęściej pojawiają się osoby niedoświadczone, najłatwiej natknąć się na agresorów. Starają się oni wybierać osoby, które dadzą się sterroryzować, osoby, które będą reagowały, gdy oni nacisną guzik. Przyglądanie się przerażeniu swoich ofiar jest celem życia wielu cyberprześladowców. Daje im poczucie siły.

Czasem motywem dręczenia jest zemsta, gdy coś, co zaczęło się w sieci jako pyskówka, przeradza się w nękanie i prześladowanie. Może też być tak, że ofiarą cyberprześladowcy zostaje ktoś ze względu na swoje przekonania religijne czy przynależność etniczną. Ofiara mogła nieświadomie zrobić coś, co sprowokowało zemstę. Znajo-

mość i przestrzeganie zasad netykiety może zmniejszyć prawdopodobieństwo zaistnienia takiej sytuacji.

Większość nastolatków mówiła nam, że w sieci robią rzeczy, których nigdy nie zrobiliby w realnym życiu, i że często znacznie mniej przejmują się odczuciami innych ludzi w sieci niż w życiu. Przyznają się do używania wulgarnego języka, którym normalnie się nie posługują, i do ordynarnego sposobu bycia, choć normalnie są uprzejmi. Z powodu mniejszych zahamowań, charakterystycznych dla wielu ludzi w wirtualnym świecie, większość nastolatków wyraża się w sposób znacznie bardziej wyzywający. Choć bywa to wyzwalające doświadczenie dla nastolatków rozwijających swoje cyberskrzydła, może zarazem prowokować nękanie i prześladowanie.

Musimy także uświadomić sobie, że większość cyberprześladowców nie ma nic przeciwko konkretnej ofierze. Każdy może się nią stać. Wybierają na ogół przypadkowe osoby, by zrobić na innych wrażenie swoją siłą i umiejętnościami komputerowymi. Taki rodzaj cyberdokuczania może równie dobrze prowadzić do hakerstwa.

Ignorowanie cybernapaści jest na ogół najlepszą metodą. To nie aż taka fajna zabawa prowokowanie kogoś, kto cię ignoruje.

Kelley, moja przyjaciółka i specjalistka od problemów cyberprześladowania, dyrektorka Cyberangels, radzi:

„Jeśli twoje dziecko zaczyna otrzymywać telefony od nieznanych ludzi, sprawia wrażenie zbyt przerażonego, by odbierać telefony, albo bywa bardzo zdenerwowane i poruszone po odebraniu telefonu, może być ofiarą cyberprześladowcy i nawet sobie tego nie uświadamiać.

Coś, co często zaczyna się jako «chodzenie ze sobą», może przerodzić się w walkę o władzę, w której ofiara czuje się bezradna i schwytana w pułapkę. Ofiara usiłuje przywrócić poprzedni kształt relacji albo sądzi, że «mój chłopiec jest po prostu zazdrosny».

Jako rodzic masz prawo i obowiązek ochraniać swoje dziecko. Jeśli podejrzewasz, że nastolatek jest nękany lub nachodzony w sieci, porozmawiaj z nią/nim o tym. Często dzieci za wszystko obwiniają siebie i dopóki sytuacja nie stanie się dramatyczna, nie przyjdą same ze skargą. Zapewnij je, że można przykrościom położyć kres. Jeśli trzeba, ponieś dodatkowe koszty i zmień swój adres e-mailowy, by uniemożliwić prześladowcy kontakt. Jeśli nękanie przeniosło się na telefon, możesz także zmienić numer telefonu. Jeśli pojawiają się groźby pod adresem dziecka, skontaktuj się z policją.

Nie zadowalaj się wyjaśnieniem, że to pewnie «tylko dziecinna zabawa». Nastolatki bardzo wierzą innym nastolatkom, ale my wiemy, że zaufanie jest często po prostu lokowane w nieodpowiednim miejscu – przez nas wszystkich. Powiedz im, że to nie jest ich wina i że czasem złe rzeczy przydarzają się bardzo porządnym ludziom".

Co można na to poradzić?

Nie bądź ofiarą i nie pozwól, by stało się nią twoje dziecko. Jeśli nabierzesz podejrzeń, że ktoś może próbować nękać kogoś z was w realnym życiu, natychmiast zawiadom policję. Zachowaj szczegółowy zapis wszystkich rozmów i upewnij się, że dziecko nie próbuje odpowiadać, nawet gdy pogróżek jest coraz więcej. To tylko podsyca pożar, a wielu prześladowców dąży właśnie do tego, by przerazić ciebie i dziecko. Nie dawaj im tej satysfakcji.

Więc jak możesz zabezpieczyć siebie i dziecko? Oto zasady bezpieczeństwa w sytuacji cybernękania:

- Nie odpowiadaj na prowokacje.
- Wybierz nieprowokujące, aseksualne imię, pod którym istniejesz w cyberprzestrzeni (nick, identyfikator).
- Nie flirtuj w sieci, jeśli nie jesteś gotowy na przyjęcie konsekwencji.
- Zachowaj obraźliwe wiadomości, które otrzymałaś, i prześlij je dostawcy Internetu.
- Jeśli znajdziesz się w sytuacji, która staje się nieprzyjemna – wyjdź z niej, wyloguj się całkowicie albo przejdź w inne miejsce.
- Zwróć się o pomoc do policji, gdy tylko pojawią się sygnały wskazujące na to, że prześladowca wie, gdzie mieszkasz, i grozi ci.

❖ Anatomia cybernapastnika: ochranianie dziecka przed molestowaniem w cyberprzestrzeni

Zdarzyło się ostatnio wiele przypadków, kiedy pedofile i inni dorośli namawiali dzieci na spotkanie w normalnym świecie i molestowali je. Na szczęście jest pewnie jeszcze więcej przypadków, kiedy ta-

kie usiłowania uwiedzenia dziecka zostały udaremnione przez grupy stojące na straży prawa. Zastanawiałam się, czy mówić o tych przypadkach, bo nie chciałabym robić z nich sensacji. Ale jeśli wyjaśnienie metod, jakimi posługują się przestępcy, sprawi, że rodzice będą bardziej świadomi, a ich dzieci bezpieczniejsze, warto to zrobić.

Cyberprześladowcy, tak jak ich odpowiedniki w realnym świecie, zazwyczaj nie są przerażającymi, owłosionymi potworami w długich płaszczach, które w wyobraźni widzimy przyczajone gdzieś w mrocznych zaułkach. Wielu z nich to osoby, które spokojnie mógłbyś zaprosić do swojego domu (i często to robisz). Mogą to być pediatrzy, ludzie prowadzący drużyny harcerskie, trenerzy, naukowcy itp. Prawie zawsze są to mężczyźni. (Czasem kobiety są współsprawcami, ale rzadko molestują). Często są to osoby wykształcone, ładnie się wysławiające. Mogą mieć różne sylwetki, cechy charakteru i kolor skóry, mogą być bogaci albo bezrobotni. Łączy ich jedno: ochota na twoje dziecko.

Większość z nas czuje się chora, myśląc o dorosłej osobie mającej seksualne kontakty z dzieckiem, ale jeśli mamy skutecznie chronić dzieci, musimy wejść w skórę prześladowcy.

Przede wszystkim napastnicy często wcale nie postrzegają siebie jako prześladowców. Widzą siebie jako kochających partnerów dzieci, które molestują. Dla nich to nie jest gwałt, to uwiedzenie. I jak każde uwodzenie, to proces powolny i pełen trudu. (Znani są napastnicy, którzy czekali dwa lata i dłużej, zbierając dane o konkretnym dziecku, zanim przypuścili szturm). To sprawia, że tak trudno ich wykryć. Nie wyglądają groźnie w oczach dziecka.

Agent FBI, który ostatnio brał wraz ze mną udział w dyskusji panelowej, ujął rzecz najtrafniej: „Przed erą Internetu ci ludzie musieli pojawić się fizycznie blisko dziecka. Musieli wałęsać się w okolicach szkół czy placów zabaw. Dzieci mogły ich zobaczyć. Dorośli mogli ich zobaczyć. To była dla nich niebezpieczna sytuacja, bo każdy mógł zauważyć dorosłego mężczyznę kręcącego się w pobliżu dzieci. Często musieli podejmować pracę albo być wolontariuszami i zdobyć pozycję osób, którym się ufa, by móc dosięgnąć swojej ofiary. Teraz jednak to ryzyko osobistego zagrożenia, jakie pedofil musiał podejmować, by być w miejscu uczęszczanym przez dzieci, zniknęło. Teraz może być «jednym z paczki» i plątać się z innymi w Internecie, nie wystawiając siebie na widok publiczny. Dopóki nie zrobi czy nie powie w publicznym miejscu czegoś podejrzanego, może sobie tam przebywać, ile chce, i spokojnie prowadzić obserwacje".

Wielu z nich tak robi. Wiadomo, że niektórzy stworzyli ogromne bazy danych dotyczące dzieci. Śledzą gusty dzieci, wiedzą, co które lubi, a czego nie. Wyszukują informacje o tym, czyi rodzice się rozwodzą, kto nie lubi nowej narzeczonej swojego tatusia czy narzeczonego mamusi, kto lubi gry komputerowe, a kto muzykę rockową. Dzieci często przekazują w profilach i w kawiarenkach informacje o swoim życiu osobistym. Choćby dlatego nie powinny tego robić.

Nie trzeba nawet siły, żeby wszystko z nich wydobyć

Oto fikcyjna rozmowa w kawiarence, która mnie i moim przyjaciołom wydaje się całkiem realistyczna. Wyobraź sobie przebiegłego pedofila, który siedzi sobie w młodzieżowej kawiarence i skrzętnie notuje w pamięci wszystkie szczegóły dotyczące jakiegoś dziecka, które potem pomogą mu w uwiedzeniu go. Czy dziecko pójdzie na ten lep? Większość, niestety, idzie.

Dziecko: Nie cierpię mojej mamy! Wiem, że to jej wina, że rodzice się rozwodzą.

Pedofil: Rozumiem cię. Moi rodzice też się rozwodzą.

Dziecko: I nigdy teraz nie mamy forsy. Za każdym razem, gdy czegoś potrzebuję, ona mówi „Nie możemy sobie na to pozwolić". Kiedy rodzice byli razem, mogłem sobie kupować różne rzeczy. Teraz nie.

Pedofil: Ja tak samo. Nienawidzę tego!

Dziecko: Pół roku czekałem, żeby się ukazała nowa gra komputerowa. Mama obiecała, że mi ją kupi, jak już się ukaże. Obiecała! Teraz gra już jest. Myślisz, że mogę ją kupić? Guzik! „Nie mamy tyle pieniędzy!". Nienawidzę matki!

Pedofil: Ojej, głupio mi, bo ja ją dostałem! Mam takiego naprawdę fajnego wujka, który mi stale kupuje różne rzeczy. On jest potwornie bogaty.

Dziecko: To masz szczęście. Chciałbym mieć bogatego wujka.

Pedofil: Mam pomysł! Zapytam mojego wujka, czy nie mógłby kupić tej gry także tobie! On jest naprawdę świetny. I mogę się założyć, że powie „Tak".

Dziecko: Naprawdę? Dzięki!!

Pedofil: BRB (w cyberżargonie: *be right back* – zaraz wracam)... Idę zadzwonić do wujka.

***

Pedofil: No i zgadnij, co powiedział? No, powiedział, że w porządku. Kupi ci tę grę!
Dziecko: O rany! Dzięki, nie mogę w to uwierzyć!!!
Pedofil: Gdzie ty mieszkasz?
Dziecko: Ja w Nowym Mieście. A ty?
Pedofil: Ja w Dużym Mieście. Mój wujek też. To niedaleko od Nowego Miasta.
Dziecko: Wspaniale!
Pedofil: Czy gdzieś blisko ciebie jest jakieś centrum handlowe? Moglibyśmy się tam spotkać.
Dziecko: Mieszkam koło centrum handlowego xyz.
Pedofil: Słyszałem o nim. Nie ma problemu. Co myślisz o sobocie?
Dziecko: Fajnie.
Pedofil: Możemy iść do McDonalda, jeśli będziesz chciał. Spotkamy się tam w południe.
Dziecko: Dobrze. Gdzie?
Pedofil: Przed wejściem do sklepu komputerowego. Mój wujek ma na imię George. Jest naprawdę fajny.
Dziecko: Cudownie... Dziękuję, jestem naprawdę wdzięczny. Masz szczęście, że masz takiego bogatego i fajnego wujka.

Nadchodzi sobota, dziecko idzie do centrum handlowego i spotyka dorosłego przed sklepem komputerowym. Dorosły przedstawia się jako „wujek George" i wyjaśnia, że jego siostrzeniec już czeka na nich w McDonaldzie. Dziecko jest skrępowane, ale wujek wchodzi do sklepu i kupuje grę za 100 dolarów. Wychodzi i wręcza ją dziecku, które od razu jest uspokojone i zachwycone.

Żadne alarmy typu „Uwaga, obcy!" nie działają tutaj. To nie jest obcy – to wujek George. A jeśli potrzebny jest jakiś dowód – oto on: gra za 100 dolarów. Więc dziecko bez oporów wsiada do samochodu, którym mają dojechać do kolegi, czekającego w McDonaldzie. Ciąg dalszy usłyszysz w dzienniku wieczornym.

To potworne. Mdli nas na myśl o tym, ale tak się dzieje. Niezbyt często, ale na tyle często, że wszystkich należy ostrzec. (Każdego roku kilkuset cyberuwodzicieli zostaje namierzonych i aresztowanych). Nawet jedno takie zdarzenie to byłoby za dużo, gdyby dotyczyło twojego dziecka. Wiedząc, jak działają i jakich „zawodowych" sztuczek używają, będziesz w stanie lepiej nauczyć dziecko, jak uniknąć bycia ofiarą.

Scenariusz działań pedofilów w sieci

Każdy przypadek jest inny, ale pedofile mają tendencję do używania zasadniczo takiej samej taktyki. Oprócz „kija i marchewki", jak przedstawiono wyżej, często starają się uwieść dziecko. Chcą, aby dziecko ich „chciało".

Zaczynają od nawiązania rozmowy, starając się stworzyć atmosferę zaufania i przyjaźni. Często udają innego nastolatka czy dziecko, zazwyczaj płci przeciwnej, chyba że dziecko zdradziło się z zainteresowaniami homoseksualnymi. (Dziecko może znać lub nie rzeczywisty wiek „uwodziciela" w chwili spotkania twarzą w twarz). W tym momencie zaczynają się telefony. Czasem dziecko zaczyna dostawać prezenty, np. aparat i film typu polaroid.

Gdy przełamali już bariery nieufności, stopniowo wprowadzają temat seksu, często, posiłkując się pornografią dziecięcą, by wywołać w ofierze wrażenie, że inne dzieci oddają się takim zajęciom regularnie. Potem zaczynają wprost nawiązywać do seksualności dziecka, wykorzystując jego ciekawość w tej mierze, zadając pytania i zalecając „zadania domowe", np. noszenie specjalnej bielizny, wysyłanie zdjęć o seksualnym charakterze do pedofila czy wykonywanie określonych działań seksualnych.

Te „zadania domowe" w jakimś momencie prowadzą do wymiany jawnie seksualnych zdjęć dziecka (zrobionych polaroidem) czy filmu wideo. W końcu pedofil dąży do zorganizowania spotkania twarzą w twarz. (Na tym etapie być może już przyznał się do swojego wieku lub podał zbliżony do prawdziwego).

Dlaczego to się udaje

Wszystkie nauki, jakie dawaliśmy dzieciom, gdy jeszcze były bardzo małe, na temat tego, by nie zadawały się z nieznajomymi, nie mają

zastosowania w wirtualnym świecie, gdzie każdy jest obcy. To część zabawy: rozmawiać z ludźmi, których się nigdy nie widziało. Poza tym wszystkie „zamontowane" przez nas alarmy nie włączają się, gdy w grę wchodzi inne dziecko. Ostrzeżenia odnoszą się tylko do nieznajomych dorosłych, nie do innych dzieci. Gdyby ktokolwiek z nas wszedł na plac zabaw i zaczął rozmowę, dzieci by go zignorowały i najpewniej uciekły. Ale gdyby na tym samym placu zabaw do jedenastolatka podszedł nieznajomy rówieśnik, po 10 sekundach pewnie zgodnie by się bawili. Właśnie tak pedofile wyłączają „radary" naszych dzieci – udają, że też są dziećmi.

A dzieci często wierzą w to, co słyszą czy co czytają. One „wiedzą" coś na temat „przyjaciela", bo wierzą w to, co on im powiedział. Wierzą też w to, co o nim przeczytały w „prezentacyjnym" profilu, w którym są oczywiście tylko rzeczy potwierdzające to, co już wcześniej zostało powiedziane. Więc dla dziecka to już nie tylko prawda, ale i udowodniona prawda.

Bystry rodzic może pokrzyżować plany pedofila na wielu etapach. Poza tym dzieci mające normalnych przyjaciół i silną, otwartą, opartą na zaufaniu relację z rodzicami mają mniejsze szanse stać się ofiarą pedofila spotkanego w sieci. Pedofile na ogół stawiają na dziecięce osamotnienie. Podsycają pretensje dziecka do rodziców i domowego życia, tworząc atmosferę „my przeciw nim". „Twoja mama jest taka niesprawiedliwa dla ciebie. Nie wiem, dlaczego nie pozwala ci..." (można wstawić dowolny zakaz: malować się, chodzić na koncerty rockowe, cokolwiek). Taka atmosfera powoduje dwie zmiany: tworzy dystans pomiędzy dzieckiem a rodzicami, a jednocześnie tworzy skryte, tajemnicze przymierze między dzieckiem a pedofilem. (Należy wiedzieć, że chłopcy padają ofiarą pedofilów prawie tak samo często jak dziewczynki).

Opis prawdziwego przypadku

Śledziłam wiele przypadków w ciągu kilku ostatnich lat. Do moich obowiązków szefa Cyberangels należało także przekazywanie niektórych z nich prokuraturze i wspieranie rodzin w niełatwym okresie śledztwa. Czasem po prostu pomagamy rodzinom pozbierać się po tym, co wyrządziło im molestowanie. (Dziecko nie jest jedyną ofiarą – całe rodziny cierpią na skutek molestowania. Rodzice czują się winni, że nie ochronili dziecka, rodzeństwo nie wie, jak traktować brata czy siostrę – ten ból często trwa przez całe życie).

Kiedy w grę wchodzą cyberłowcy, ściśle współpracuję z policją, zwłaszcza z jednostką specjalną. To właśnie ta jednostka jest odpowiedzią policji na pornografię dziecięcą i działalność pedofilów w Internecie. By znaleźć pedofila, pracownicy tej jednostki wykorzystują otrzymane od innych doniesienia, a niekiedy tajni agenci sami występują w sieci jako dzieci. Zwracają oni uwagę głównie na osoby gotowe podróżować, by spotkać „dziecko", z którym prowadzili pogawędki w kawiarenkach. Czasem podają się również za dorosłych zainteresowanych pornografią dziecięcą, a potem odnajdują i aresztują tych, którzy ją rozprowadzają.

Przypadek, z którym zetknęłam się kilka lat temu, dotyczył mieszkających w New Jersey nastolatki i dorosłego uwodziciela. Był to jeden z pierwszych zgłoszonych przypadków takiego zachowania w Internecie. Na szczęście romans został wykryty, zanim dziewczynka spotkała się z tym mężczyzną twarzą w twarz. Ale to trwało ponad półtora roku, zanim matka odkryła romans. Zapoznając się ze szczegółami, zastanów się, co można było zrobić, by wykryć sytuację wcześniej i jak możesz skorzystać z tego ostrzeżenia, by lepiej chronić swoje dziecko.

Paul Brown był bezrobotny, ważył prawie 200 kilogramów i mieszkał w suterenie. Miał konta internetowe. Mary miała 12 lat, gdy mama, nauczycielka, kupiła jej komputer, bo Mary miała kłopoty w nawiązywaniu kontaktów z rówieśnikami. Mary wysłała poprzez Internet wiadomość, że poszukuje korespondencyjnego przyjaciela. Opisała siebie jako nastoletnią dziewczynę. Paul napisał do niej, używając swojego prawdziwego nazwiska (to coś, co robią zadziwiająco często), ale podając się za 15-letniego chłopca.

Paul i Mary przez kilkanaście miesięcy podtrzymywali e-mailowy i telefoniczny kontakt. W miarę rozwoju związku zaczęli pisać listy, a Mary wysłała mu swoją fotografię. On opowiedział jej, że mieszka ze swoją matką w domku i że chciałby znaleźć dziewczynę. W którymś momencie Paul Brown poprosił Mary o „przysługę": „Jeśli wyślę ci rolkę filmu, czy mogłabyś poprosić jakąś koleżankę, żeby zrobiła ci zdjęcia w różnych strojach i różnych uczesaniach? I z makijażem, jeśli jakiś stosujesz, i w różnych pozach. Niektóre mogłyby być seksy, jeśli to możliwe. Proszę. Bądź tak dobra. Dziękuję ci. Jesteś cudowna. Całuję".

Mary zgodziła się. Przez następne osiem miesięcy nadal prowadzili rozmowy i korespondowali, a Mary dołączała swoje fotografie.

Brown zachęcał ją, używając w swoich listach okrzyków: „Stale robisz postępy!". W maju 1996 Brown skierował do Mary miłosne wyznanie: „Gdybym powiedział, że cię kocham, to byłoby za mało. W wieku 14 lat zawojowałaś moje serce i sprawiłaś, że mam ochotę śpiewać. Kocham wszystko, co ma związek z tobą...".

Niedługo potem Brown przyznał się, że ma dwadzieścia kilka lat. Zasugerował też, by Mary nagrała siebie na kasecie wideo w seksualnie prowokacyjnych pozach. Zrobiła to. Brown, otrzymawszy kasetę, zwrócił ją Mary z instrukcjami, jak ma poprawić niektóre fragmenty, by widoczne były piersi i genitalia. Potem wyznał, że jest rozwiedziony i ma ponad 30 lat.

Od czasu do czasu wysyłał jej drobne prezenty. Kilka miesięcy później, gdy Brown obiecał, że przekaże kopie kaset wideo czterem członkom ulubionego zespołu muzycznego Mary, dziewczynka posłała mu dodatkowe kasety. (Brown twierdził, że bardzo dobrze zna członków tego zespołu). Każda kaseta wysłana przez Mary była przeznaczona dla innego członka zespołu i zawierała otwarcie seksualne ujęcia. Brown wysłał jej też swoje slipki numer 48. Kiedy matka je odkryła, zawiadomiła policję. Zatrzymując Browna, agenci FBI znaleźli kasety wideo Mary i dziesięciu innych dziewczyn z różnych części kraju.

Mary miała 14 lat, kiedy cała sprawa się wydała. Brown został uznany za winnego nakłaniania nieletnich do robienia filmów i zdjęć jawnie seksualnych i został skazany na prawie 5 lat więzienia (maksymalna kara za przestępstwo tego typu popełniane po raz pierwszy). Po tym wszystkim Mary napisała do Browna: „Ufałam ci. Myślałam, że jesteś moim przyjacielem".

Jest w tym przypadku kilka rzeczy szczególnych. Po pierwsze, Mary prowadziła rozmowy międzymiastowe. Rodzice zawsze powinni zainteresować się rachunkami za budzące wątpliwości rozmowy międzymiastowe. Po drugie, Mary była samotna. Takie dzieci są często bardzo bezbronne. Rodzice powinni być zorientowani w ich sieciowych przyjaźniach i monitorować ich wirtualne życie. I po trzecie, choć trudno wiedzieć, co twoje dzieci robią, kiedy ciebie nie ma w domu, zwłaszcza gdy jesteś samotnym rodzicem, półtora roku to zbyt długi czas, by taka relacja rozwijała się niezauważona. Musisz znaleźć czas na to, by poznać przyjaciół dziecka, zarówno z prawdziwego, jak i z wirtualnego świata.

Gdy dziecko jest samotne i ma problemy w nawiązywaniu kontaktów z rówieśnikami, to zawsze oznacza, że może stać się łupem pedofila czy cybernapastnika. Prześladowcy potrafią wyszukiwać osamotnione dzieci. Potrafią także „namierzać" dzieci, które są początkującymi internautami i nie znają obowiązujących zasad. Większość pytanych nastolatków przyznaje się, że otrzymywały w sieci różne propozycje. Ale to, co jest oczywiste dla dziecka dobrze zorientowanego w cyberświatku, może nie być oczywiste dla nowicjusza.

Pedofile mogą być przyjacielscy wobec takich dzieci i cierpliwie budować zaufanie i więź z nimi w nadziei, że któregoś dnia spotkają się twarzą w twarz.

Zachęcaj swoje dziecko do nawiązywania kontaktów w Internecie, ale postaw komputer w centralnym, dla wszystkich dostępnym miejscu w domu i interesuj się nowymi znajomościami, by takie sekretne związki nie mogły się zrodzić. Edukacja jest też istotnym elementem unikania zagrożeń. (Gdyby Mary była zawczasu ostrzeżona i poinformowana o tym, jak działają pedofile, być może zauważyłaby, jaki stary głos miał Brown przez telefon, i łatwiej rozpoznałaby klasyczne chwyty). Inne ważne elementy to kontrola wiadomości odbieranych i wysyłanych przez młodsze dzieci, używanie filtrów, urządzeń blokujących i monitorujących. Można by uniknąć sytuacji w rodzaju tej, która przydarzyła się Mary, gdyby rodzice pomyśleli o różnych rzeczach zawczasu, gdyby rozmawiali z dziećmi, informowali je i mieli oczy szeroko otwarte.

Zmylenie twoich straży: nawet gdy czuwasz, złe rzeczy mogą się zdarzyć

Już w swojej pierwszej książce „A Parent's Guide to the Internet" omówiłam przypadek Paula Browna (został skazany w 1997 roku, kiedy pisałam książkę), włączyłam go, bo to dobry przykład typowych działań cybernapastników. Wydawało mi się, że sugerował, że gdyby matka była nieco uważniejsza, być może sprawa wyszłaby na jaw wcześniej. Miałam rację co do metod działania cybernapastników. Myliłam się, sądząc, że uwaga matki może zapobiec wykorzystaniu seksualnemu. Potrzeba czegoś więcej. Potrzebna jest i uwaga matki, i ostrożność dziecka, które powinno wiedzieć o sposobach działania pedofilów.

W 1998 roku spotkałam matkę, która zrobiła wszystko, co należało. Była uważna i kontrolowała wirtualne znajomości córki. Zadawała właściwe pytania. Miała dobry kontakt ze swoją córką, a mimo to

Charles Hatch, pedofil ze stanu Utah, zmylił wszystkie straże i wykorzystał seksualnie jej 13-letnią córkę.

Jennifer miała jedenaście i pół roku, kiedy po raz pierwszy spotkała w sieci „Charliego". Sądziła, że jest starszy od niej o kilka lat, i imponowała jej przyjaźń starszego chłopca. Jennifer była świetną uczennicą i choć była w szkole średniej, już uczęszczała na niektóre zajęcia do college'u. Mieszkała w miłym domu, z kochającymi rodzicami. Miała też rodzeństwo i przyrodnie rodzeństwo z pierwszego małżeństwa ojca. Wszyscy byli ze sobą bardzo związani.

Matka Jennifer, Sharry, rozmawiała z dziewczynką o jej wirtualnym przyjacielu, Charliem. Stanowczo chciała rozmawiać z Charliem przez telefon, gdy Jennifer i Charlie zaczęli do siebie dzwonić. Zdał ten egzamin i Sharry była przekonana, że to rzeczywiście nastoletni chłopiec, tak jak się przedstawiał. Albo tak dobrze modulował głos, albo znalazł kogoś młodszego, kto wykonał ten telefon. Charlie dzwonił nawet do braci Jennifer, mówiąc, że któregoś dnia zostanie ich szwagrem, gdy Jennifer i on się pobiorą. Błagał, by Jennifer przyjechała odwiedzić go w Utah. Wówczas Sharry zaprosiła jego w odwiedziny. Ale Charlie zawsze miał jakiś powód, dla którego nie mógł przyjechać.

W miarę trwania znajomości Sharry zaczęła nalegać na to, by porozmawiać z matką Charliego. Najpierw odmawiał, mówiąc, że matka jest chora, później, że jej choroba to rak, z powodu którego na koniec zmarła. Rodzina połknęła ten haczyk. Większość troskliwych rodzin by uwierzyła.

Choć „związek" rozwijał się od prawie dwóch lat, był względnie powściągliwy. Charlie był raczej romantyczny niż nalegający, przysyłał kosztowne prezenty, w tym aparat polaroid. (Pamiętacie polaroid wysłany przez Paula Browna?).

Jennifer nie miała doświadczenia w umawianiu się z chłopcami, a Charlie zdawał się wiedzieć, że nie należy jej zbyt popędzać. Po około półtorarocznej znajomości Charlie przysłał jej swoje jawnie seksualne fotografie od szyi w dół. Dziewczyna poczuła się bardzo skrępowana i wyraźnie zdystansowała się. Jednakże w tym czasie w jej życiu zdarzyło się kilka tragedii, które uczyniły z niej łatwiejszy łup. Jej ojciec trafił do szpitala z powodu poważnej choroby, a starszy przyrodni brat zmarł na wylew. Charlie, jak wszyscy napastnicy, wiedział, kiedy uderzyć. Powiedział Jennifer, że jest mu winna swoje seksualne zdjęcia, bo on wysłał jej swoje. Kiedy odmówiła, powiedział, że zostanie sama, bo jej rodzina umiera, a on ją zostawi. Z oporami, po wewnętrznej walce, zgodziła się wysłać mu swoje zdjęcia w seksualnych pozach.

Kiedy Sharry sprzątała pokój Jennifer, znalazła list, w którym Charlie precyzował, w jakich pozach Jennifer ma być na tych zdjęciach. Sharry napisała do niego, grożąc, że poinformuje policję, jeśli jeszcze raz spróbuje skontaktować się z jej córką. Nigdy nie odpisał, a Jennifer zakazano używania Internetu.

Pewnego dnia, kiedy Jennifer i Sharry sądziły, że cała sprawa się skończyła, odezwał się telefon. Dzwonił detektyw z Utah, informując, że współpracownik Hatcha znalazł zdjęcia Jennifer w jego kalendarzu. Charlie nie miał szesnastu lat, ale trzydzieści sześć. Był kiedyś nauczycielem i został zwolniony z pracy, gdy jedna z uczennic oskarżyła go o wykorzystywanie seksualne. (Szkoła nie podjęła żadnych działań). Aktualnie pracował w biurze pomocy społecznej, miał żonę i dzieci własne oraz przysposobione.

Kilka miesięcy później Charles Hatch został skazany przez sąd federalny w Utah za wykorzystywanie seksualne. Otrzymał wyrok sześciu i pół roku więzienia i zakaz korzystania z Internetu.

Matka Jennifer stała się moją przyjaciółką, gdy szukała w Cyberangels wsparcia w doprowadzeniu do końca tej sprawy. Jest wspaniałą i troskliwą matką, a sprawa jej córki wiele nas wszystkich nauczyła. Oto okazuje się, że niektórzy napastnicy (określani przez policję jako „podróżnicy") wyszukują dobre, inteligentne, grzeczne dzieci, nie znające ciemnych stron życia, pochodzące z podmiejskich czy wiejskich rodzin.

Wystąpienie matki w związku ze skazaniem prześladowcy córki

Wystąpienie to zostało odczytane w sądzie przez adwokata w czasie procesu Charlesa Hatcha. Sharry była zbyt zdenerwowana, by je osobiście przeczytać w zatłoczonej sali sądowej. Historia ta równie dobrze mogłaby dotyczyć córki czy syna każdego z nas. Powinniśmy posłuchać, co Sharry ma do powiedzenia, i uświadomić naszym dzieciom, że nie wszyscy ludzie są tymi, za których się podają w cyberprzestrzeni. Przytul mocno swoje dziecko dziś wieczorem i z ulgą pomyśl, że ten mężczyzna jest w więzieniu.

Jak określiła to Sharry, wystąpienie jest obroną jej córki i wszystkich innych dzieci:

„Nigdy nie sądziłam, że życie może tak nieodwracalnie się zmienić, aż do chwili, gdy przypadkiem znalazłam list do mojej córki napisany przez Charlesa Hatcha. Uświadomiłam sobie, że on jest oszustem, a nie 16-letnim chłopcem, którego matka zmarła na raka, za jakiego się podawał. W tym momencie wszystkie brakujące cząstki internetowej przyjaźni między nim a moją córką i resztą naszej rodziny złożyły się w całość. W końcu zobaczyłam, że od ponad roku moja córka była nękana i stopniowo manipulowana przez niego. W końcu została wykorzystana akurat wtedy, gdy mój mąż leżał ciężko chory i gdy straciliśmy jedno z naszych dzieci. On czekał i czaił się przez ponad rok, a uderzył, gdy rodzina przeżywała trudne chwile.

Byłam oddana swoim dzieciom od chwili, gdy wiedziałam o ich poczęciu, i pracowałam ciężej niż ktokolwiek, kogo znam, by wyplenić źdźbła nienawiści zasiewane w ich sercach. Te źdźbła są unoszone przez społeczne prądy i mogą łatwo wylądować w dowolnym miejscu. Po latach, gdy zapuszczą korzenie, widzimy ich owoce: przemoc, wojnę, biedę, apatię, strach i wzajemną nienawiść.

Działania podjęte przez Charlesa Hatcha zniweczyły moje wysiłki i poniżyły moją rodzinę i mnie.

Muszę powstrzymać instynktowną chęć zadania ciosu, jeśli mam nadal zostać wierna zasadom moralnym, które wpajałam swoim dzieciom. Ale jako człowiek nadal cierpię, czuję się przytłoczona tym, co może w przyszłości spotkać inne dzieci, bo niektórzy z nas wydają się nie być w stanie stawić czoła nieodpartej chęci schwytania i zniewolenia innych, wykorzystania słabszych, młodszych, niewinnych.

To są te ziarna, które przynoszą owoce i przenoszą zło z pokolenia na pokolenie. Choć próbuję jak mogę zapomnieć o całej sprawie, nie potrafię. To nie chce minąć. Nadal prześladuje mnie na jawie i we śnie. W sennych koszmarach on przychodzi do mojego domu, by zabrać moją córkę, i rzuca ją kilka godzin później... zupełnie inną... a ja jestem jak sparaliżowana i nie mogę interweniować.

To nadal prześladuje moją córkę. Nawet w tym tygodniu opowiedziała mi o koszmarze sennym, gdy została wyciągnięta z domu przez «Charliego» – ale on jej nie przyprowadził z powrotem. Wolę koszmary w snach, niż na jawie, dlatego ona nie pojawi się tu dzisiaj. Stara się prowadzić w miarę możliwości normalne życie.

O marzeniach mojej jedynej córki nie umiem nic powiedzieć.

Ciągle ujawniają się nowe skutki tego incydentu. Widzę, że to dziecko, które z wyróżnieniem zaliczało kolejne klasy, ma coraz gorsze stopnie i traci nadzieję na stypendium. Mała dziewczynka, która kiedyś beztrosko i chętnie bawiła się z koleżankami, jest coraz bardziej wyobcowana ze swojej grupy rówieśniczej.

Przed tym zdarzeniem była bardzo otwarta. Teraz ma coraz gorsze stopnie, bo trudno jej głośno mówić i nawiązywać kontakt wzrokowy podczas odpowiedzi. Teraz nie ufa nikomu. Stała się mniej pewna siebie, bardziej zależna ode mnie. I choć powtarzam jej, że nie zrobiła niczego złego, tylko popełniła błąd, ona przepuszcza to przez pryzmat swoich doświadczeń.

Jej młodszy brat jest otwarcie zły za zdradę, której doświadczył. Jej ojciec, wściekły za gwałt na niewinnym dziecku, był gotów szukać tego człowieka i zniszczyć go. Ja sama jestem zarazem poruszona i bardziej niż dotknięta czymś, z czego Charles Hatch i jemu podobni nigdy się nie wyleczą. Ciągle na nowo dochodzę do tego samego wniosku: to my musimy wziąć odpowiedzialność za tych, którzy sami nie potrafią być odpowiedzialni. Musimy chronić nasze dzieci i izolować ludzi, którzy polują na innych pod wpływem przymusu i nieuleczalnej choroby. Nie mamy innego wyboru.

Charles Hatch będzie w taki czy inny sposób cierpiał. Jego problem jest natury psychicznej, a my nie umiemy go wyleczyć. Współczuję jemu i innym dotkniętym jego czynami. Być może to jedyna okazja, bym została usłyszana, a statystyki mówią, że jest na świecie ogromna liczba matek i córek, i rodzin, które nigdy nie miały tej szansy, by ich głos był słyszany, mimo że ich życie zostało złamane przez dorosłego, który śledził i polował na dzieci.

Zgodnie z danymi opublikowanymi na stronie Cyberangels istnieje 21 317 stron pedofilskich, umieszczonych w sieci WWW. Według innych danych codziennie jeden napastnik udaje się w podróż, by spotkać się twarzą w twarz ze swoją ofiarą. Według lokalnych agencji – nawet więcej.

Mam taką prośbę, by Charles Hatch został odizolowany od dzieci na tak długo, jak to możliwe, i by był pociągnięty do odpowiedzialności za swoje czyny. W tym wypadku uwięzienie go jest jedynym sposobem obrony. Moja córka i ja wyrażamy nasze współczucie jego rodzinie i dzieciom. Nie wiem już, co jest słuszne. Ciągle jeszcze mogą pojawić się różne skutki, o których w tej chwili nie wiem. Wiem tylko, czego wymaga od nas odpowiedzialność. Proszę, błagam: chrońmy dzieci".

Nie mogę sobie wyobrazić lepszego zakończenia tego rozdziału niż to zaczerpnięte z przemówienia Sharry: proszę, chrońmy nasze dzieci.

Rozdział 5

A teraz o tym, co naprawdę nudne: prawo

Ponieważ wielu czytelników pyta, czy w Internecie obowiązuje jakieś prawo i jak odróżnić to, co po prostu przeszkadza i denerwuje, od tego, co nielegalne – musiałam włączyć ten rozdział. Jeśli znajomość prawa nie jest dla ciebie ważna – pomiń go. Nie martw się, nie utrudni to zrozumienia tego, co najważniejsze w tej książce. Niektóre rzeczy jednak są bardziej zrozumiałe, jeśli się wie, co może podlegać regulacjom prawnym, a co nie.

Choć starałam się pisać tę książkę nie jak prawnik, to w tym rozdziale fakt, że jestem prawnikiem, bardzo ułatwił mi sprawę. Postaram się nie zanudzić was, ale trudno jest uczynić prawo czymś podniecającym. Jeśli masz skłonność do łatwego zasypiania, proponuję opuszczenie tego rozdziału. Ale jeśli cierpisz na bezsenność – nawet lekarz nie zaleciłby niczego lepszego.

Globalny dostęp oznacza konieczność znalezienia globalnych rozwiązań

Pamiętaj, że Internet nie ma właściciela, nie jest przez nikogo kontrolowany i nie istnieje w realnej przestrzeni. Więc zanim zaczniemy omawiać prawo, musimy rozumieć, jak jest ono ograniczone, gdy chodzi o regulowanie całego Internetu.

Internet jest globalny. Wszystko, co nadasz w Kapuściakach, jest natychmiast dostępne w każdym miejscu na świecie. To oznacza, że aby kontrolować to, co jest dostępne w Internecie, musimy regulować go globalnie. Z tego wynika potrzeba ustalenia globalnych standardów i możliwości egzekwowania prawa na terenie całego globu. Ale największym problemem w ogólnoświatowych wysiłkach są różnice w prawie i standardach. To, co jest dopuszczalne i legalne w Stanach, może być nielegalne w innym miejscu. I wiele rzeczy legalnych w jednym kraju, jest zakazanych w innym.

Prawdopodobnie największe różnice dotyczą pornografii dziecięcej i norm prawnych odnoszących się do seksualnego wykorzystywania dzieci. Na przykład, japońskie prawo do niedawna zakazywało tylko pornografii ukazującej owłosienie genitalne. Ponieważ młodsze dzieci nie mają jeszcze takiego owłosienia, pornografia dziecięca mogła uchodzić za legalną. Wielu producentów pornografii dziecięcej wykorzystało tę lukę prawną, umieszczając swoje strony na serwerach w Japonii, by obejść prawo własnego kraju. Ostatnio Japonia przyjęła prawo, które zamyka te możliwości. To powinno bardzo pomóc w zwalczaniu pornografii dziecięcej.

Problem nie ogranicza się do Dalekiego Wschodu. To, co w USA jest uznawane za pornografię dziecięcą, jest legalne w wielu krajach europejskich. To powoduje poważne problemy, gdy chodzi o zamykanie stron pornograficznych.

Nawet w krajach, które rozpoznają pornografię dziecięcą, ustalenia dotyczące wieku mogą się istotnie różnić. W USA trzeba mieć poniżej 18 lat, by być uznanym za dziecko w świetle ustaw o pornografii, a w innych krajach ustawodawstwo takie może dotyczyć tylko dzieci poniżej 13 roku życia. Więc nic nie możemy zrobić przeciwko witrynom umieszczonym w tych krajach, chyba że wiek dziecka jest niższy niż dopuszczalny.

Zaczynasz rozumieć, jakie to wszystko skomplikowane. Jeśli strona jest założona na serwerze w kraju, który nie uważa za nielegalne określonych treści czy zachowań, czyje prawo ma wówczas zastosowanie? Czy prawo kraju, w którym znajduje się serwer? Czy prawo kraju zamieszkania osoby oglądającej? To niektóre z pytań, które rodzi globalny charakter Internetu. I są to pytania, na które trzeba w najbliższych latach odpowiedzieć, jeśli mamy znaleźć wspólne rozwiązania.

❖ Co na to ONZ?

Dotychczas nie było ogólnoświatowych prób ścigania przestępstw przeciwko dzieciom w cyberprzestrzeni. Ale obecnie Organizacja Narodów Zjednoczonych zaczyna je podejmować.

UNESCO zajmuje się problemem Internetu z ramienia ONZ. W styczniu 1999 roku zorganizowało konferencję ekspertów na temat pedofilii i pornografii dziecięcej w Internecie. W efekcie tej konferencji (na której prezentowałam referat o ustalaniu zasad) UNESCO stworzyło program „Innocence in Danger – Children Online". W Stanach Zjednoczonych połączyłam go z naszą własną akcją „Wired Kids".

Program „Innocence in Danger" (Niewinność w niebezpieczeństwie) ma szanse tylko wtedy, gdy eksperci z różnych stron świata włączą się do pracy nad zapewnieniem dzieciom bezpieczeństwa w poruszaniu się po Internecie. Homayra Sellier, obrończyni praw dzieci, matka, została wyznaczona przez UNESCO do stworzenia tego programu i uruchomienia go. Zachęciła wiele osób w różnych częściach świata, by poświęciły swój czas tej wspaniałej sprawie. (Wiem, wszak zachęciła i mnie).

Zgodnie z jej planem każde państwo powinno stworzyć krajowy komitet, który określi podstawowe dla danego kraju sprawy w zakresie bezpieczeństwa dzieci w Internecie. Następnie podejmie działania, by rozwiązać te problemy w swoim kraju. Potem narodowe komitety podejmą wspólną pracę w celu znalezienia i wdrożenia rozwiązań ogólnoświatowych. Amerykański komitet działa w ramach organizacji non profit Wired Kids, która ma szersze cele niż zakreślone przez UNESCO i będzie się koncentrowała na wyrównaniu szans dostępu do Internetu, bezpieczeństwie i udzielaniu pomocy nauczycielom i szkołom w efektywnym wykorzystaniu Internetu.

To nie jest teren zupełnego bezprawia – tak się tylko wydaje

Choć przestrzeń wirtualna jest globalna i trudno ją regulować, nie należy wyciągać wniosku, że nie działa tam żadne prawo. Zbyt wielu ludzi sądzi, że jest to miejsce, gdzie prawo nie obowiązuje i gdzie każdy może robić, co mu się podoba, i nie będzie za swoje działania odpowiadał. Ale nie mają racji. Większość praw obowiązuje tak w sieci, jak i poza nią. Poza kilkoma wyjątkami to, co jest przestępstwem w realnym świecie, jest nim też w Internecie. A ludzie, którzy stoją na straży prawa w realnej rzeczywistości, robią to też w wirtualnej.

❖ Ojcowie założyciele i prawo

Każda dyskusja o pornografii musi zacząć się od konstytucji i stwierdzenia, że większość jawnie seksualnych treści, które spotykamy w Internecie, jest przez nią chroniona. To oznacza, że nie możemy zabronić innym oglądania tych treści w jakimkolwiek medium, dlatego że się nam nie podobają, że uważamy je za niesmaczne i niestosowne dla naszych dzieci. Oznacza to również, że jeśli chcemy ochronić nasze dzieci przed kontaktem z takimi treściami, to do nas, rodziców, należy kontrola dostępu dzieci do tych treści. Z tego powodu wszystko, co rząd usiłowałby zrobić w kierunku cenzurowania jakichś informacji, będzie uznane za niekonstytucyjne i pozostanie stratą ich i naszego czasu.

❖ Co naprawdę wiemy o wolności słowa?

Często odwołujemy się do konstytucyjnego prawa do wolności słowa. Ale wielu ludzi nie wie, co to naprawdę oznacza. Sąd Najwyższy jasno określił, że Internet zasługuje na największą możliwą ochronę wolności słowa.

Konstytucja amerykańska daje każdemu w Stanach Zjednoczonych prawo do swobody wypowiedzi, niecenzurowanej przez rząd (z kilkoma ściśle określonymi wyjątkami). Nie daje prawa do powiedzenia wszystkiego, co się chce, w każdym miejscu i czasie. Nie zabrania także pozarządowym instytucjom i jednostkom, takim jak choćby rodzice, kontrolować to, co mówią ich dzieci i do czego mają dostęp. (Wolność słowa działa w dwie strony, daje ci prawo powiedzenia tego, co chcesz, i słuchania tego, co inni mają do powiedzenia).

Jawnie seksualne informacje ogólnie mogą być chronione, ale określone typy takich jawnie seksualnych treści (określane jako „obsceniczne") nie są chronione. Określa się to jako „wypowiedzi nie podlegające ochronie". Jeśli coś jest obsceniczne, rząd może się tym zająć i używanie tego, produkcję i dystrybucję traktować jako przestępstwo, natomiast jeżeli jest to określane jako „nieprzyzwoite" – nie może takich działań podjąć, bo nieprzyzwoitość, w przeciwieństwie do obsceniczności, jest chroniona przez prawo.

Choć wielu ludziom może się wydawać, że to to samo, jest wielka różnica między „nieprzyzwoity" a „obsceniczny" w sensie prawnym. (Trzeba wiedzieć, że prawnicy nigdy nie mówią takim językiem jak

zwykli ludzie. Gdyby tak było, nie byliby potrzebni i wszyscy musieliby pisać książki o bezpieczeństwie w sieci, żeby zarobić na życie).

Kongres także stale myli obsceniczne z nieprzyzwoitym. To jedna z przyczyn, dla których wszelkie jego usiłowania poddania kontroli zawartości Internetu zawodzą. W każdym przypadku sąd określił projekty ustaw jako niezgodne z konstytucją. (Jak to się ma do mojej tezy, że prawnicy mówią innym językiem niż wszyscy inni, skoro większość kongresmanów to prawnicy!). Te rozstrzygnięcia znajdują aplauz u obrońców wolności słowa, ale często jeszcze bardziej gmatwają sprawy w oczach rodziców i nauczycieli. Jeśli prawo nie może chronić ich dzieci przed zalewem określonych informacji, to jakie opcje mają do dyspozycji? Co jest nielegalne? Czy nie ma żadnych praw, które pomagałyby rodzicom?

❖ Pornografia dziecięca – to nie tylko okropne, ale i nielegalne!

Pornografia dziecięca została niemal zlikwidowana w Stanach Zjednoczonych mniej więcej dziesięć lat temu, pozostały głównie obrazki wyprodukowane wcześniej. Ale od nadejścia ery Internetu i popularności sieci WWW dziecięca pornografia odżyła, stała się kwitnącym biznesem, którego produkcja i dystrybucja osiągnęła rozmiary przemysłowe, nawet w Stanach Zjednoczonych. A do tej produkcji wykorzystywane są nasze dzieci.

Pornografia dziecięca to nie pornografia, która jest przeznaczona dla dzieci. To pornografia, która używa dzieci (lub wydaje się używać) do aktów seksualnych lub scen lubieżnych. Jest nielegalna w całych Stanach Zjednoczonych i w wielu innych krajach na świecie. Wydaje się, że dziecięcą pornografię uznano za oddzielną kategorię, niechronioną przez prawo. Zamiast konieczności zdecydowania, czy pornografia dziecięca jest „obsceniczna", sąd może po prostu skupić się na określeniu:

- Czy obraz koncentruje się na okolicy narządów płciowych dziecka?
- Czy obraz jest seksualnie sugestywny?
- Czy, biorąc pod uwagę wiek dziecka, można uznać pozę, w jakiej dziecko jest pokazywane, za nienaturalną?

- Czy dziecko jest częściowo lub całkiem nagie?
- Czy obraz ma na celu wzbudzenie reakcji seksualnej?

Teraz, gdy ujawniłam test, oczekuję więcej informacji od rodziców, którzy znajdą lub będą sądzili, że znaleźli dziecięcą pornografię w Internecie.

Muszę was jednak ostrzec, że reklamy, które otrzymujecie, obiecujące pikanterię w postaci „nastolatków uprawiających seks", tak naprawdę pokazują 18-latków uprawiających seks, nie młodsze dzieci. Dziecięca pornografia jest zbyt surowo ścigana, by mogła być wszędzie reklamowana. To tak jakby handlarz narkotyków umieścił ogłoszenie w „Panoramie firm". (Odbieram mniej więcej dwadzieścia listów dziennie od rodziców zadających jakieś pytania lub zgłaszających regularne strony dla dorosłych jako strony z pornografią dziecięcą na podstawie zamieszczanych ogłoszeń. Ale ogłaszanie, że oferujesz pornografię dziecięcą, nawet jeśli jej nie oferujesz, także jest nielegalne).

Powinieneś także wiedzieć, że nie jest nielegalne robienie czy rozpowszechnianie zdjęć nagich dzieci, jeśli nie są ustawione w takich pozach, że budzi to skojarzenia seksualne. Szczegółowe regulacje mogą być różne, ale ogólnie w Ameryce zdjęcie nagiego dziecka, bez żadnych innych charakterystyk, nie jest nielegalne.

❖ Akty prawne chroniące dziecko przed seksualnymi napastnikami w cyberprzestrzeni

W Stanach Zjednoczonych zakazane jest, zarówno w cyberprzestrzeni, jak i w realnej rzeczywistości:

- zachęcanie lub zmuszanie nieletniego do jawnie seksualnych zachowań,
- importowanie i transportowanie materiałów obscenicznych,
- świadome zbieranie pornografii dziecięcej,
- reklamowanie pornografii dziecięcej,
- przedstawianie nieletnich zaangażowanych w seksualne zachowania,
- przedstawianie kogoś, kto wygląda jak dziecko, zaangażowanego w jawnie seksualne zachowania,

- reklamowanie i promowanie zachowań jawnie seksualnych, gdy tworzy się wrażenie, że w takie zachowania zaangażowane są osoby nieletnie.

Prawo chroni też dzieci przed wabieniem lub usiłowaniem zwabienia ich na spotkanie twarzą w twarz w celu dokonania nielegalnych aktów seksualnych lub zmuszanie ich do dostarczania swoich jawnie seksualnych zdjęć.

To jeden z największych problemów z napastnikami w sieci. Zanim namówią twoje dziecko do spotkania twarzą w twarz, zmuszają je do zrobienia i wysłania im jawnie seksualnych zdjęć, a jeszcze częściej posyłają dzieciom własne jawnie seksualne zdjęcia. (Kiedy cybernapastnik nakłania dziecko do sfotografowania się w jawnie seksualnej pozie, łamie prawo).

Wykorzystywanie seksualne zawsze było bardzo poważnym przestępstwem, ale w przeszłości kary za nie nie były tak surowe, jak powinny być. Na szczęście ostatnio Kongres zatwierdził ustawy zwiększające kary za zachowania związane z seksualnym krzywdzeniem dzieci i pornografią dziecięcą.

❖ Cybernękanie dzieci

Kilka lat temu pewien dorosły mieszkaniec Illinois, który kłócił się z sąsiadem, zamieścił w Internecie ogłoszenie, że młoda córka sąsiada jest chętna do seksualnych zabaw. Podał jej nazwisko, adres, telefon. Telefony zaczęły się natychmiast, nawet w środku nocy, od obcych poszukujących młodej i chętnej partnerki seksualnej. Wszyscy byli zdziwieni, gdy okazało się, że to haniebne zachowanie według prawodawstwa Illinois jest tylko wykroczeniem, a prawo federalne w ogóle nie ma tu zastosowania.

Poruszony tym koszmarnym zdarzeniem, Kongres ustanowił prawo zakazujące celowego rozpowszechniania nazwiska, adresu, numeru telefonu czy adresu e-mailowego dziecka poniżej 16 roku życia w celu zachęcania, wywołania lub ułatwienia nielegalnej aktywności seksualnej (taką jest każda aktywność seksualna wobec osoby nieletniej). Gdyby ten straszny sąsiad popełnił swój czyn obecnie, mógłby być skazany zgodnie z nowym prawem.

Innymi słowy cybernękanie jest zazwyczaj tylko wykroczeniem (zagrożonym maksymalną karą roku więzienia). Prawo większości

stanów wymaga, by najpierw zaistniała „wiarygodna groźba", zanim akt stanie się w oczach prawa karalny. Więc jeśli cyberprześladowca nie grozi ci czymś w realnym świecie, nie ujawnia, że zna twój adres i śledzi cię, większość organów ścigania nawet nie zacznie postępowania w sprawie. (Na ich obronę mogę powiedzieć, że nie zawsze łatwo jest odróżnić kogoś, kto po prostu blefuje, od kogoś rzeczywiście polującego).

❖ Co ze stronami zachęcającymi do seksualnego wykorzystywania dzieci?

Niestety, w Stanach Zjednoczonych witryny, które propagują czy zachęcają do seksu między dorosłym a dzieckiem, także te, które zawierają nieprowokujące zdjęcia nagich dzieci, zazwyczaj nie są nielegalne.

Rozmaite organizacje i Cyberangels stworzyły listy stron, które zachęcają do pedofilii lub wspierają grupy pedofilów. W sierpniu 1999 roku lista ta zawierała ponad 30 tys. stron WWW. By uzyskać więcej informacji na jej temat, odwiedź www.cyberangels.org/kidlist.html. Jest dostępna bez opłat dla organów ścigania i za opłatą licencyjną dla firm produkujących oprogramowanie filtrujące.

Prawo wobec handlu narkotykami, alkoholem, bronią i papierosami

Broń, alkohol, papierosy

Sprzedaż tych artykułów już od dawna obwarowana jest różnymi aktami prawnymi, regulującymi minimalny wiek nabywcy, posiadanie licencji przez sprzedawcę albo obie te sprawy.

Przede wszystkim alkohol i broń mogą być sprzedawane tylko przez licencjonowanych sprzedawców. Fakt, że są one sprzedawane przez Internet, w większości przypadków dla prawa nie różni się od sytuacji, gdy są one sprzedawane na zamówienie listowne lub telefoniczne. Inny wielki problem dotyczący sprzedaży tych artykułów powstaje w związku z tym, że prawo wymaga dowodu pełnoletności

nabywcy. Ale jak ktoś ma udowodnić w Internecie swój wiek? Jeśli za dowód wieku uznamy kartę kredytową, każde dziecko uzbrojone w karty rodziców może tam uchodzić za osobę dorosłą.

Broń na ogół nie może być sprzedana osobie, która nie ukończyła 21 lat. Sprzedawca może sprawdzić dowód pełnoletności, może też kierować się zdrowym rozsądkiem, oceniając wiek nabywcy, ale te metody nie sprawdzają się w sieci. Toteż sprzedawcy muszą być szczególnie ostrożni, gdy mają do czynienia z klientami internetowymi. Podejrzewam, że większość przypadków sprzedaży broni nieletnim jest raczej wynikiem nieuwagi sprzedawców niż celowego działania. Ale jest kilka luk, które pozwalają oferującym broń w Internecie ominąć restrykcje dotyczące sprzedaży nieletnim. Problem pojawia się, gdy prezentacja broni w Internecie dokonywana jest tak, że pozwala na bezpośrednie skontaktowanie osoby prowadzącej w Internecie sprzedaż z osobą dokonującą zakupu, a ta osoba może nie spełniać kryterium wieku wymaganego do zakupu broni. Bez odpowiedzialnego pośrednika (takiego jak organizator wystawy broni w Internecie) mało skrupulatni sprzedawcy mogą nie zwracać należytej uwagi na wiek kupujących.

To nowa sprawa i nie ma jeszcze prawa zapobiegającego udostępnianiu informacji o sprzedawcach na stronie wystawowej. Ostatnio pojawiła się propozycja uchwały zabraniającej witrynom prezentującym broń publikowania w ogólnodostępnej witrynie informacji o sprzedawcach. Wydaje mi się ona rozsądnia.

Z alkoholem sprawa wygląda podobnie. Tak naprawdę próby prawnego uregulowania jego sprzedaży nie są podejmowane dlatego, że dzieci kupują alkohol w sieci. To inicjatywa hurtowni alkoholu, obawiających się zmniejszenia obrotów na rzecz sprzedawców internetowych, oraz władz lokalnych, obawiających się utraty wpływów z podatków za odnawianie licencji na sprzedaż spirytualiów.

Co ze sprzedażą nielegalnych substancji trujących i narkotyków

Takie rzeczy są nielegalne niezależnie od tego, gdzie się odbywają. Szczególne zasady mają zastosowanie wtedy, gdy rzeczy są sprzedawane legalnie, ale stają się nielegalne, gdy są kupowane. Zazwyczaj są to sprawy leżące w gestii urzędu celnego, bo chodzi o dobra przywiezione przez kupującego czy wysłane na zamówienie internetowe.

❖ Moje prawnicze zastrzeżenie

Ostrzegałam, że prawne rozważania mogą być bardzo nudne, ale tak wiele osób prosiło o umieszczenie tych informacji, że zdecydowałam się złamać swoje postanowienie, by nie mówić jak prawnik. Jeśli nie śpicie, mam jeszcze parę aktów prawnych do omówienia. Przedstawione regulacje obowiązują w tej chwili i są tylko małym wycinkiem prawa dotyczącego pornografii dziecięcej, wykorzystywania dzieci i Internetu. Poza tym mogą się one zmienić, a może już się zmieniły, zanim książka trafi na półki księgarskie. Musicie wreszcie pamiętać, że przedstawione omówienie nie może być traktowane jak porada prawna. Gdy potrzebujecie takiej porady – zwróćcie się do prawnika.

Cybergliny: kto czuwa nad przestrzeganiem prawa w cyberprzestrzeni?

Czy pamiętacie, że wszystko, co jest przestępstwem w realnym świecie, jest nim również w cyberprzestrzeni? Niektóre amerykańskie organy stojące na straży prawa zostały wyznaczone jako pierwsza linia obrony w przypadkach tych przestępstw w Internecie, gdzie ma zastosowanie prawo amerykańskie, ale nie ma stróżów prawa specjalnie dla cyberprzestrzeni.

Kilka lat temu, gdy pisałam swoją pierwszą książkę, mało kto zajmował się próbami egzekwowania prawa w cyberprzestrzeni. FBI miało swoją specjalną grupę, Federalna Komisja Handlu (FTC) regulowała kwestie związane z internetowymi reklamami kierowanymi do dzieci i zbieraniem danych od dzieci, a w Urzędzie Celnym USA istniał Wydział Cyberprzemytu. Dziś, po kilku latach, te trzy komórki są nadal głównymi instytucjami zajmującymi się przestępstwami w cyberprzestrzeni i wprowadzaniem prawa w Internecie. Choć w ciągu ostatnich kilku lat powstało kilkanaście wydziałów policji do spraw przestępstw w cyberprzestrzeni, a niektóre z nich zdobyły powszechne uznanie w całym kraju, gruntowna wiedza o tym, jak wykrywać i zwalczać przestępstwa w cyberprzestrzeni, jest ciągle raczej wyjątkiem niż regułą.

Problem egzekucji prawa w Internecie po części wiąże się z brakiem nawyków i funduszy dla organów ścigania, które mają dość za-

jęć z wykrywaniem i chwytaniem przestępców podlegających miejscowej jurysdykcji – cóż tu mówić o operatorach stron WWW czy cybernapastnikach, którzy mogą mieszkać w dowolnym miejscu na świecie.

Na szczęście wraz z rozwojem Internetu nasilały się też starania o to, by obowiązywało tam prawo. Departament Sprawiedliwości powołał specjalne regionalne grupy zadaniowe zajmujące się tym problemem, szkolące specjalistów. Zwykły policjant, który zajmował się nieco Internetem i na tej podstawie uchodził w komendzie za eksperta, ustępuje powoli miejsca nowym kadrom, o wysokim poziomie przygotowania specjalistycznego. Jednak ograniczenia budżetowe, brak sprzętu odpowiedniej klasy i konieczność stałego kształcenia sprawiają, że utrzymanie tych komórek wymaga ogromnego wysiłku.

Specjalna jednostka FBI jest najstarszą grupą śledczą, obarczoną zadaniem znajdowania prześladowców z cyberprzestrzeni. Choć okazjonalnie zajmuje się przypadkami pornografii dziecięcej, głównym jej zadaniem jest wykrywanie ludzi, którzy w Internecie uwodzą i seksualnie wykorzystują dzieci. Jednostka została utworzona w 1993 roku w odpowiedzi na pierwsze zgłoszone do prokuratury cyberprzestępstwo – molestowanie małego chłopca z Marylandu.

Wydział Cyberprzemytu, jednostka do zadań specjalnych działająca w ramach Urzędu Celnego USA, został powołany do zajmowania się przypadkami pornografii dziecięcej pojawiającymi się w Internecie. W ostatnim czasie został zreorganizowany jako samodzielna jednostka urzędu. Choć zajmuje się także przypadkami napastników, które wiążą się z dochodzeniami w sprawach pornografii dziecięcej, jego podstawowe zainteresowania ograniczają się do pornografii dziecięcej. Jednostka ta ma duże znaczenie w działaniach o zasięgu ogólnoświatowym, bo Urząd Celny ma więcej agentów pracujących poza granicami USA niż większość pozostałych instytucji stojących na straży prawa. Zespół pracuje niezmordowanie, pomagając chronić dzieci i likwidować pornografię.

Federalna Komisja Handlu (Federal Trade Commission) jest agencją, która zajmuje się problemami reklamy, zbierania danych i oszustw wobec konsumentów. Interesuje się zarówno przypadkami, które zdarzają się w Internecie, jak i tymi w realnym świecie, i należy do bardziej zasłużonych instytucji. Myślę, że to ludzie tam zatrudnieni sprawiają, że jest to tak szczególna instytucja. Nie znam żadnej innej agendy federalnej, która ramię w ramię z przemysłem

próbuje poprawić świat dla przyszłych pokoleń. Im naprawdę zależy na dzieciach i na Internecie.

Jednak nawet tak elitarne agendy same nie poradzą sobie z problemem. Przestępcy spędzają dwadzieścia cztery godziny na dobę, siedem dni w tygodni, próbując wykorzystać system do znalezienia nowych sposobów uwiedzenia dziecka, oszukania emeryta czy przywłaszczenia sobie czegoś, co do nich nie należy. Typowy policjant pracuje osiem godzin dziennie, pięć dni w tygodniu. Więc kto ma przewagę w grze w policjantów i złodziei? Łatwo policzyć.

Oto dlaczego gliny potrzebują naszej pomocy – rodzice, nauczyciele i grupy obrony praw dziecka mogą pomóc w wyrównaniu sił na boisku. Każdy z nas może wziąć część odpowiedzialności za usunięcie nielegalnych stron i powstrzymanie zakazanych praktyk, choćby zgłaszając je odpowiednim władzom, gdy się na nie natknie.

❖ Jak oni odnajdują ludzi w sieci?

Ludzie błędnie sądzą, że Internet zapewnia anonimowość. Jednakże za każdym razem, gdy wchodzą do sieci, zostawiają elektroniczny ślad, jakby okruszki chleba, w miejscach, w których byli. Za każdym razem, gdy serfujesz, jesteś identyfikowany przez numer IP (Internet Protocol). Jeśli używasz własnego serwera lub określonego serwera dostawcy usług internetowych, masz numer statyczny IP. Jest to numer na stałe przydzielony tobie, jeżeli używasz tego samego komputera i tego samego dostawcy Internetu. Śledzenie osoby sprowadza się zatem do śledzenia adresu IP. Jeśli używasz AOL lub innego serwisu, by dostać się do Internetu, otrzymujesz dynamiczny adres IP, co oznacza, że jest on ci przydzielony na jakiś czas, na zasadzie losowej, z puli adresów IP, jaką dysponuje serwer. Aby można go było połączyć z osobą, trzeba wiedzieć, kiedy był przydzielony. Do tego konieczna jest współpraca dostawców usług internetowych lub serwisów sieciowych, którzy muszą przejrzeć własne zapisy, by połączyć konkretny IP z określonym klientem.

Problem powstaje, gdy organy ścigania potrzebują zapisów dotyczących IP, a one nie są już przechowywane przez dostawców Internetu czy usług internetowych, którzy na ogół przechowują je przez tydzień albo jeszcze krócej. Jeśli napastnik czy twórca pornografii nie zostaną szybko zidentyfikowani, zniknie ważne ogniwo, które łączy podejrzanego z przestępstwem.

Obrońcy prawa starają się doprowadzić do wydłużenia okresu obowiązkowego zachowywania tych danych, a dostawcy Internetu bronią się przed zwiększonymi kosztami przechowywania olbrzymiej bazy danych przez długi czas. Możemy tylko mieć nadzieję, że kiedyś wypracują jakieś rozwiązanie, które zadowoli wszystkich. Są np. sytuacje, w których policja i prokuratura mogą prosić dostawców Internetu o zachowanie danych określonego użytkownika przez 90 dni, z możliwością przedłużenia tego okresu – w razie potrzeby – o dodatkowe 90 dni.

Wielu ludziom wydaje się też, że wymazanie danych we własnym komputerze sprowadza się do przyciśnięcia przycisku *delete*. Ale tym sposobem usuwa się dane tylko ze swojego pola widzenia. Twój komputer wie, że te dane są, i przy użyciu odpowiednich programów potrafi je odszukać. Jedynym sposobem faktycznego usunięcia informacji jest przeformatowanie twardego dysku. Wtedy na miejscu starych informacji zapisujesz coś innego (to jak nagrywanie nowych rzeczy na taśmie magnetofonowej lub wideo). Jednakże specjaliści są w stanie odtworzyć zawartość dysku nawet po przeformatowaniu.

Ponadto twoja przeglądarka zachowuje zapis miejsc, które odwiedzałeś. Nazywa się te pliki *cache* lub historia. Jeśli je przejrzysz, dowiesz się, gdzie bywały twoje dzieci.

❖ Komu zgłaszać problemy i przestępstwa w cyberprzestrzeni?

Upowszechnienie wiedzy o tym, gdzie należy zgłaszać cyberprzestępstwa i dokąd zwrócić się, gdy potrzebujemy pomocy w sieci, jest kluczem do oczyszczenia Internetu.

Jedną z najlepszych linii informacyjnych na świecie jest National Center for Missing and Exploited Children's CyberTipline (CyberLinia Zgłoszeniowa Krajowego Centrum Dzieci Zaginionych i Wykorzystywanych), powołana przez Kongres amerykański.

Linie zgłoszeniowe, istniejące w innych częściach świata, wzorowały się na CyberLinii Krajowego Centrum. Ośrodek ten nie byłby tym, czym jest, gdyby nie Ernie Allen, wizjoner, gdy chodzi o sprawy bezpieczeństwa dzieci. Ale cały personel stanowią pełni poświęcenia, świetnie przygotowani specjaliści.

Sprawą bezpieczeństwa dzieci w cyberprzestrzeni zajęło się również kilkanaście organizacji non profit. Te, które opisuję, posiadają linie zgłoszeniowe i ściśle współpracują z organami ścigania. Są one szczególnie godne uwagi, a ponadto niektóre z nich mają też świetne strony WWW poświęcone sprawom bezpieczeństwa dzieci.

Nie będę zapewne obiektywna, ale organizacja Cyberangels pomaga ludziom, którzy potrzebują pomocy w sieci od ponad czterech lat. Została stworzona przez Curtisa Sliwę. (Kieruję Cyberangels od czerwca 1995 roku). To największa z grup zajmujących się sprawami bezpieczeństwa w Internecie. Otrzymuje dziennie setki doniesień o cyberprzestępstwach, od pornografii dziecięcej do przypadków nękania, oszukiwania, uwodzenia i wykorzystywania seksualnego dzieci.

Jedną z najstarszych grup chroniących dzieci przed cybernapastnikami jest SOC-UM (Safeguarding Our Children – United Mathers, www.soc-um.org), grupa kierowana przez kobietę, którą niezmiernie cenię, Debbie Mahoney. Debbie jest matką młodego człowieka, który jako dziecko był seksualnie molestowany przez zaprzyjaźnionego sąsiada, jednego z pierwszych ekspertów w sprawach komputerów i Internetu. Choć jej syn nie został uwiedziony poprzez sieć, Debbie uświadomiła sobie, jak łatwo wykorzystać Internet do wyszukania i omamienia ofiary. Od tego momentu postanowiła poświęcić swoje życie temu, by dzieci mogły bezpieczniej poruszać się w Internecie. Jej działania wyprzedziły nawet powstanie sieci WWW, bo pojawiły się wówczas, gdy powstawały grupy dyskusyjne tworzone przez pedofilów. Debbie pracuje też w programie Wired Kids. Przyjmują zgłoszenia przypadków pornografii dziecięcej, zaginięć dzieci, wykorzystywania seksualnego i uwodzenia.

EHAP (Ethical Hackers Against Pedophilia, www.ehap.org) to elitarna grupa ekspertów komputerowych, którzy połączyli siły, by zwalczać istniejącą w sieci pornografię dziecięcą i tropić cybernapastników. W czerwcu 1999 roku grupa liczyła tylko 17 osób. Ale ich dokonania, sukcesy i pomoc, jakiej udzielili różnym organom ścigania, są niewspółmierne do ich liczby. Wbrew nazwie, nie są hakerami łamiącymi prawo. Używają swoich zdolności i umiejętności, współpracując z organami ścigania, by odnajdować przestępców. Szykanowanie, nękanie i włamania do komputera powinny być zgłaszane dostawcy usług Internetowych (ISP), którego używa obwiniany.

Co możemy zrobić sami?

My, rodzice, jesteśmy naprawdę potężną grupą. Gdybyśmy działali razem, moglibyśmy wiele zmienić. A instytucje stojące na straży prawa potrzebują naszej pomocy.

❖ Zgłoś swoje odkrycia

Nawet jeśli nie chcesz włączać w sprawę organów ścigania, powinieneś poinformować ISP, gdy któryś z jego klientów usiłuje nawiązać niestosowny kontakt z twoim dzieckiem. Pracownicy FBI mówią, że gdy przeglądają komputer używany przez napastnika, nieodmiennie znajdują w nim e-maile od rodziców oskarżających go o próby uwodzenia ich dziecka. Gdyby ci rodzice zrobili coś więcej niż tylko złożenie skargi na ręce uwodziciela, być może czyjeś inne dziecko uniknęłoby molestowania. Musimy zacząć budować coś na kształt systemu pomocy sąsiedzkiej.

Gdy natkniesz się na stronę wzbudzającą zastrzeżenia, poinformuj o niej firmy produkujące oprogramowanie blokujące i filtrujące. Jeśli odwiedzasz jakąś stronę, która ci się bardzo podoba, zasugeruj jej właścicielom, by uczestniczyli w ratingu dokonywanym w standardach PICS (standardy ratingu stron WWW dokonywane przez specjalne agencje na podstawie zawartości treściowej). Poza tym, gdy znajdziesz stronę, która ci się podoba, przekaż informacje o niej do witryn prowadzących listy dobrych stron, by można było ją zrecenzować i ewentualnie umieścić w wykazach.

Jeśli dowiesz się o stronie uczniowskiej, na której grozi się innym przemocą, poinformuj szkołę i lokalną policję. Więcej na ten temat podaję w rozdziale „Internet w szkołach".

To nie jest system doskonały, ale zawsze mały krok do przodu. I sądzę, że w ciągu kilku lat z pomocą zainteresowanych rodziców wiele zmienimy. (Nawet jeśli jesteś przeciwna filtrowaniu, to ocenianie stron internetowych i zbieranie dobrych stron dla dzieci są najlepszymi sposobami obrony przed próbami ograniczania wolności słowa w Internecie).

❖ Ofiaruj swój czas

Możesz również ochotniczo przyłączyć się do którejś z grup zajmujących się sprawami bezpieczeństwa w Internecie. Cyberangels

(www.cyberangels.org) i SOC-UM (www.soc-um.org.) prowadzą nabór w sieci i umożliwiają ochotnikom pracę wtedy, gdy korzystają z Internetu. (To oznacza, że możesz być wolontariuszem po pracy, w godzinach nocnych, gdy dzieci śpią, i że możesz pracować w piżamie i szlafroku).

Zajrzyj na te strony, by dowiedzieć się więcej o tym, co robią wolontariusze i ile czasu należy poświęcić. Obydwie grupy prowadzą szkolenia dla ochotników.

Jeśli nie jesteś zainteresowany pracą w jakiejś większej grupie, możesz pomóc, edukując dzieci w pobliskiej szkole w kwestiach bezpiecznego serfowania. Możesz zaoferować swoją pomoc w bibliotece.

Możesz stworzyć własną stronę WWW lub lokalny biuletyn informacyjny zawierający wiadomości na temat bezpieczeństwa w sieci i ewentualnie umieścić odnośniki do innych stron związanych z tym problemem. Możesz też oceniać strony dla agencji zajmujących się ich klasyfikacją albo zbierać fundusze dla grup obrony praw dziecka. Formy pomocy mogą być najrozmaitsze. Ich granice w istocie wyznacza jedynie wyobraźnia i zaangażowanie.

Ja z kolei interesuję się tym, co robią rodzice. W Wired Kids chcemy przedstawiać inicjatywy rodzicielskie i podawać odnośniki do tych stron, które uważamy za pożyteczne.

Na pomoc! Co robić, jeśli zdarzy się to najgorsze

Mam nadzieję, że nigdy nie będą wam potrzebne informacje zawarte w tej części. Ale straszne rzeczy czasem jednak się zdarzają i wiedza o tym, jak się zachować, co zrobić, a czego nie robić, gotowy plan działania miejscowej społeczności może nieraz przyczynić się do tego, że dziecko wróci bezpiecznie do domu.

❖ Co robić, gdy dziecko zaginie i podejrzewasz, że ma to związek z cybernapastnikiem

- Nie wpadaj w panikę. Wiem, że to bardzo trudne, ale musisz myśleć jasno, by pomóc organom ścigania. Nie dotykaj

komputera i nikomu nie pozwól tego robić. Także sąsiadowi, który uważa się za eksperta, nie pozwól na poszukiwanie dowodów. Zostaw to profesjonalistom.

- Najpierw zadzwoń do miejscowej policji. Oni najlepiej znają okolice i są pod ręką. Jednak nie pozwól im dotykać komputera, jeśli w ekipie nie ma specjalisty od cyberprzestępstw.
- Zbierz wszystkie informacje, których mogą potrzebować. Wyszukaj ostatnie zdjęcia dziecka, porozmawiaj z jego kolegami i koleżankami, być może oni coś wiedzą. Sprawdź, czy masz hasło do konta e-mailowego i czy wiesz, kto jest twoim dostawcą Internetu i usług e-mailowych. Jeśli dziecko ma konto e-mailowe w szkole, zbierz tam te same informacje. Czy dziecko miało konto ICQ? Jeśli tak, znajdź numer i hasło. Czy używasz produktów filtrujących lub monitorujących? Odszukaj instrukcje i sprawdź, czy masz pod ręką hasło.

Organa ścigania dysponują metodami szybkiego dostępu do informacji posiadanych przez dostawcę usług Internetowych (ISP). Mają też na ogół dobre relacje ze specjalistami do spraw bezpieczeństwa pracującymi w ISP, bo często są to byli funkcjonariusze FBI czy policji. Wyszkolony zespół specjalistów od cyberprzestępstw potrafi dziś wyśledzić w Internecie prawie wszystko.

❖ Reakcja otoczenia

Debbie Mahoney, założycielka SOC-UM, jest ogromnie oddana sprawie zaginionych dzieci. Stworzyła instrukcję do opracowywania planu reakcji na zagrożenie, wykorzystując doświadczenia nabyte podczas akcji poszukiwania dziecka porwanego w Kalifornii w 1994 roku. Choć dziecko nie było ofiarą cybernapastnika, poradnik sprawdza się tak samo dobrze w różnych sytuacjach. Bezpieczny powrót dziecka do domu Debbie przypisuje niezwykłemu zaangażowaniu miejscowej ludności. Upewnij się, że gdy zdarzy się coś niedobrego, społeczność lokalna pośpieszy z pomocą z podobnym entuzjazmem. I sprawdź, czy jest przygotowana do takiego działania.

Każda szkoła i społeczność lokalna powinny mieć swój plan reakcji na zagrożenie. Zazwyczaj zarząd miasta, działając w porozumieniu z organami ścigania, wyznacza grupę zadaniową. Kiedy s[illegible] jakoś wiąże się z Internetem, ważne jest, by do grupy zadaniowej włączona była komórka cyberprzestępstw w policji.

Debbie zaleca, by grupa zadaniowa, która opracowuje plan reakcji na zagrożenie, pomyślała o następujących sprawach:

- Obecność łącznika policji w ochotniczym centrum.
- Przygotowanie pomieszczeń dla centrum ochotniczego.
- Przygotowanie planów miasta i okolic.
- Umowa z telekomunikacją, że podłączy centrum ochotnicze do sieci telefonicznej natychmiast po otrzymaniu zgłoszenia.
- Obmyślenie szybkich sposobów powielania i rozprowadzania materiałów informacyjnych.

Ja dodałam kilka jeszcze sugestii, odnoszących się głównie do sytuacji, gdy w grę wchodzi cyberuwodzenie lub porwanie, czy też sprawa w jakiś inny sposób ma związek z Internetem:

- Lokalna policja powinna zawczasu zapewnić numery awaryjnych kontaktów z najpopularniejszymi dostawcami Internetu i usług sieciowych. Nie może być tak, że w trakcie akcji policja odkrywa, że nie może skontaktować się z nikim w wydziale bezpieczeństwa, bo to dzień wolny od pracy.
- Organa ścigania na szczeblu lokalnym powinny przygotować listę największych firm produkujących oprogramowanie filtrujące i kontakty dla ich wydziałów ochrony. Jeśli rodzice używali oprogramowania filtrującego, być może jego producenci będą w stanie odczytać informacje dla innych niedostępne.
- Specjaliści informatycy z miejscowej biblioteki i szkoły powinni skontaktować się z policją i przedstawić używane systemy oraz podać zakres informacji, którymi dysponują. Czy szkoła używa systemów filtrowania? Jeśli tak, co wie o praktykach serfowania? Czy jest system e-mail i ICQ? Co ze stronami tworzonymi przez uczniów – jakie informacje szkoła ma na ten temat?

Wcześniejsze przygotowanie się do ewentualnych kryzysów może wiele zmienić. Gdy chodzi o poszukiwanie zaginionych dzieci i chwytanie przestępców, czas jest najistotniejszym elementem. Więc bardzo ważne jest posiadanie planów działania, które zapewnią uzyskanie najlepszych rezultatów.

Rozdział 6

Internet w szkołach

Szkoły w sieci

Zgodnie z ostatnimi badaniami rządowymi, w 1998 roku 89% szkół publicznych w Stanach Zjednoczonych miało dostęp do Internetu, choć 51% szkół publicznych miało dostęp do Internetu tylko w jednej klasie. Wiele szkół miało podłączenie jedynie w bibliotece lub pracowni technicznej. Mimo to bardzo wielu rodziców, z którymi rozmawiałam, i większość tych, którzy odpowiedzieli na naszą ankietę, stwierdziło, że nie ma pojęcia o tym, jak ich dzieci korzystają z Internetu w szkole ani co robią w sieci.

W ciągu kilku najbliższych lat wszystkie szkoły uzyskają dostęp do Internetu. Szkoły powinny więc nauczyć się współpracować z rodzicami. A jeśli rodzice nie mają dostatecznego rozeznania w tej kwestii, powinni zadawać pytania, oferować swoją pomoc i wsparcie. To jedyna droga, byśmy mieli pewność, że nasze dzieci korzystają w pełni – i bezpiecznie – z tego, co oferuje Internet.

Musimy jednak pamiętać, że szkoły także nie dysponują cudownym rozwiązaniem. Zmagają się z problemami bezpieczeństwa, z niedostatkiem funduszy, brakiem dostępu do najlepszych szkoleń i zmieniającą się technologią. Każdy okręg szkolny radzi sobie ze sprawami bezpieczeństwa na swój sposób. Niektóre używają oprogramowania filtrującego. (Obecnie prawo uzależnia przydział funduszy federalnych szkołom od stosowania przez nie oprogramowania filtrującego). Inne wysyłają rodzicom informacje i ustalają zasady bezpiecznego korzystania z Internetu.

Wiele szkół przejęło regulaminy, które rodzice i uczniowie muszą podpisać, zanim uczniom wolno będzie korzystać z Internetu w szkole. Rozwiązania trzeba dopasowywać do warunków, biorąc pod uwa-

gę technologię, której szkoła używa, personel, poziom zaangażowania rodziców, potrzeby i zachowanie uczniów, społecznie akceptowany system wartości.

❖ Jak szkoły korzystają z Internetu?

Najczęściej pierwszym miejscem, w którym szkoła instaluje dostęp do Internetu, jest biblioteka lub pracownia techniczna. Dzieci zbierają w sieci materiały do szkolnych zadań, często też używają Internetu do zabawy: wysyłają e-maile, grają w gry, gadają. Wiele szkół wyeliminowało możliwość pogaduszek, gdy okazało się, że stwarza to więcej zagrożeń niż ma walorów edukacyjnych.

Bibliotekarze lub biblioteczni specjaliści od mediów na ogół nadzorują serfujące dzieci. Monitory są często ustawione tak, że bibliotekarz zza biurka może je obserwować, co pomaga dzieciom trzymać się ustalonych reguł. Jednak w typowej dużej szkole średniej w bibliotece może przebywać 150 uczniów, a 40 jednocześnie może używać komputerów z dostępem do Internetu. To uniemożliwia bezpośredni dozór. Z tego powodu wiele szkół wprowadziło oprogramowanie filtrujące jako dodatek do regulaminów korzystania z bibliotecznych komputerów.

W niektórych szkołach również w klasach są komputery podłączone do Internetu. Kiedyś korzystanie z nich było nagrodą dla uczniów, którzy pierwsi skończyli pracę. Jednak w miarę jak pojawiają się nowe programy edukacyjne, Internet staje się elementem normalnej pracy szkolnej.

❖ Czy Internet podnosi poziom nauczania, czy jest tylko kolejną zabawką?

Zbyt często ludzie nie wiedzą, że istnieją dowody, iż korzystanie z Internetu i komputerów poprawia umiejętność uczenia się i podnosi wyniki uzyskiwane w testach. Oto przykład: klasy trzecie w szkole podstawowej w Logan w okręgu Baltimore, zostały wytypowane do udziału w specjalnym programie.

Zakładał on dostarczenie dzieciom do domów komputerów i szybkich linii dostępu do Internetu oraz takich samych komputerów i połączeń nauczycielom. Do momentu instalacji szybkich linii telefonicznych wiele dzieci nie miało nawet telefonów w domach. (W miasteczku był wysoki odsetek rodzin o niskich dochodach, bo w okolicy zlikwidowano wiele zakładów. Większość rodzin objętych programem żyła poniżej poziomu ubóstwa, mając dochody nie przekraczające 10 tys. dolarów rocznie).

Przed wprowadzeniem programu tylko 20% dzieci z klas trzecich opanowało umiejętność czytania na poziomie odpowiednim lub wyższym. Po roku okazało się, że 80% czyta na stosownym lub wyższym poziomie. A to dopiero początek postępów.

Standaryzowane testy wykazały, że w ciągu roku przeciętny uczeń poprawił swoje wyniki w zakresie czytania tak, że osiągnął postęp przewidziany na rok i pięć miesięcy. Podobnie w matematyce.

Interesującym skutkiem ubocznym programu było to, że dzieci miały w stu procentach odrobione prace domowe. (Mnie nigdy nie udało się nawet zbliżyć do takiego poziomu). Uczniowie biorący udział w programie mieli także mniej nieobecności w szkole. Dodatkowo program stał się cennym źródłem internetowej edukacji rodziców.

Ale historia ma smutny epilog, bo mimo dowodów na edukacyjne dobrodziejstwa płynące z udziału w programie, nowa szkoła, do której dzieci trafiły, nie była zainteresowana jego kontynuacją. Mimo to firma Bell Atlantic zasłużyła na medal za to, co zrobiła dla tych dzieci.

❖ Jak wykorzystać Internet do realizacji nowatorskich programów edukacyjnych w nauczaniu dzieci trudnych?

To prawdziwa opowieść o specjalnym programie dla szczególnych dzieci, prowadzonym przez niezwykłą kobietę, którą znam i uwielbiam, Susan M. Condrey. Susan pracuje w Wydziale Oświaty w okręgu Orange i w 1997 roku otrzymała grant w wysokości 500 tys. dolarów na realizację swego programu „Jedna płeć". Dzięki temu programowi przełamała tradycję szkół publicznych, tworząc szkołę niekoedukacyjną. Była jej dyrektorką.

Program w dużym stopniu opiera się na wykorzystaniu nowych technologii i Internetu. Susan opowiadała o nim tak:

„W określonym czasie przychodzili do szkoły na zmianę, dziewczynki lub chłopcy. Mieli tych samych nauczycieli, otoczenie, program, ale nie byli razem w klasie. Program «Jedna płeć» w Fountain

Valley w Kalifornii wystartował w ramach 2-letniego grantu badawczego, w celu sprawdzenia, czy segregacja płciowa uczniów wpływa pozytywnie na poziom ich osiągnięć szkolnych, zmniejsza absencję, liczbę aktów przemocy i innych przestępstw.

W szkole w Fountain Valey znalazły się dzieci przeniesione ze swoich szkół rejonowych, gdyż były zagrożone wyrzuceniem, chronicznie wagarowały, nie robiły postępów w nauce albo dlatego, że były bardzo opóźnione w realizowaniu programu po pobycie w ośrodkach karnych. Pochodziły z okolicznych miejscowości, w 85% ze szkół o najniższym poziomie, z rejonów o wysokim wskaźniku przestępczości, z dzielnic, w których wiele rodzin zamieszkuje w jednym domu czy mieszkaniu.

Uczniowie posiadali niewątpliwie «mądrość ulicy», ale mieli braki w wykształceniu. Nie podróżowali ani nie czytali. Niektórzy nigdy nie byli na plaży, odległej o dwadzieścia kilometrów, ani w górach – o godzinę jazdy samochodem. Ogólnie można powiedzieć, że byli sfustrowani, pełni złości i raczej nie mieli specjalnych nadziei na zrealizowanie wielkiego amerykańskiego marzenia.

Nasza szkoła była inna. Oprócz tego, że chłopcy byli odseparowani od dziewcząt, strategie nauczania oparliśmy na użyciu nowych technologii. Były listy lektur, nie było tekstów. Uczniowie spędzali dwie godziny dziennie, pracując samodzielnie nad indywidualnie zadanymi lekcjami, następnie przechodzili do związanych z programem zajęć edukacyjnych, które wprowadzały ich w społeczeństwo, najpierw wirtualnie, a potem realnie. Uczyli się myśleć. Najpierw prowadzili poszukiwania w Internecie, potem w życiu. Uczyli się znajdować informacje, nadawać im sens, prezentować je. Regularnie brali udział w wideokonferencjach z udziałem ekspertów i uczniów z różnych szkół w całym kraju. Nauczyciele rozpoczęli monitorowany program, w ramach którego każdemu uczniowi przydzielono dorosłego wolontariusza. Dawało to okazję nie tylko do przeprowadzenia zaplanowanych zajęć, ale pozwalało też na utrzymywanie indywidualnej e-mailowej korespondencji. Internet otworzył okno na świat całym klasom szkolnym i poszczególnym uczniom.

John mieszkał w motelu z młodszą siostrą i matką, która została zastrzelona, kiedy on miał 12 lat. Ojciec był w więzieniu. Następnych kilka lat John spędził, tułając się między ośrodkami wychowawczymi, domami dziecka, zmieniając dla rozrywki swój wygląd, z punka stając się skinheadem. Lydia zaś była po prostu znudzona. Znudzona szkołą, obijała się po centrach handlowych albo zostawała w domu i oglądała telewizję tak długo, aż było za późno na wyjście do szkoły. Straciła większość czasu w klasach 7 i 8. Obydwoje byli zdolnymi dziećmi, ale zapóźnionymi w realizacji programu, gdy wyrokiem sądowym zostali umieszczeni w naszej szkole. Żadne nie widziało dla siebie takiej przyszłości, do której warto było się wyrywać.

Szkoła niekoedukacyjna zapewnia określony poziom spokoju, pozwala uczniom swobodniej się wypowiadać, ułatwia zaryzykowanie błędu, koncentrację na nauce. Internet dostarczył im podniet i doświadczeń wcześniej niedostępnych. Dzięki tej technologii uczniowie zaczynali odkrywać nowe możliwości, porozumiewać się, dorastać i uczyć się. John skończył szkołę, pracuje jako operator kamer wideo, ma nadzieję kontynuować naukę i być może znaleźć pracę w przemyśle rozrywkowym. Lydia radzi sobie dobrze i w tym roku wróci do swojej macierzystej szkoły. Oszczędza pieniądze, pracując w czasie wakacji, żeby sobie kupić komputer. Na twarzach obojga wyraźnie widoczna jest świeżo zdobyta wiara w siebie".

❖ Koty w Indiach

Nauczyciele to naprawdę nietuzinkowi ludzie. Ale nawet najlepsi nauczyciele mogą się czasem czegoś nauczyć od swoich pupilów.

Art Wolinsky to człowiek niezwykły, nawet wśród nauczycieli. Kieruje grupą Nauczyciele XXI wieku w stanie New Jersey (powstała ona w ramach programu przygotowanego przez Biały Dom, którego celem jest przygotowanie nauczycieli do korzystania w procesie dydaktycznym z technologii XXI wieku). Ale trzydzieści lat temu, kiedy zaczynał uczyć, dopiero wprowadzał swoje niezwykłe pomysły w klasie.

Art zastępował nauczyciela, który zostawił mu konspekt lekcji. Należało porównać telekomunikację, opiekę zdrowotną, transport, edukcję i infrastrukturę komunikacyjną Stanów Zjednoczonych i krajów rozwijających się. Art zdecydował, że przeprowadzi temat po swojemu. Poprosił więc uczniów o przeprowadzenie porównania, jak ich zdaniem poradziłyby sobie Stany Zjednoczone i Indie z epidemią, która w przeciągu jednej nocy zabiłaby wszystkie koty w kraju.

Ręce natychmiast podniosły się do góry. W Stanach Zjednoczonych – mówiły dzieci – prezydent ogłosiłby w telewizji, co robić, a czego nie robić, a przedtem przeprowadziłby narady z ekspertami od spraw zdrowia. Następnie przedstawiono by zalecenia dotyczące zbierania i usuwania ciał zmarłych zwierząt, by nie stwarzały dalszego

zagrożenia dla życia. Ludzi pouczono by, jak uniknąć kolejnej epidemii. Z kraju wolnego od choroby sprowadzono by koty. Powstałyby też ośrodki wspierające osoby, które nie mogą pogodzić się ze stratą pupilków, i wszystko wróciłoby do normy.

Indie, według oceny uczniów, nie poradziłyby sobie tak dobrze. Brak infrastruktury uczyniłby z tego zdarzenia klęskę narodową. Kocie zwłoki rozkładałyby się na ulicach, powodując rozszerzanie się epidemii na ludzi. Brak ogólnokrajowego systemu przekazywania informacji uniemożliwiłby mieszkańcom wsi zrozumienie tego, co się dzieje, i mogłoby to doprowadzić do niepokojów społecznych. W Indiach wszystko potoczyłoby się źle.

Art używał tego schematu w ciągu następnych trzydziestu lat nauczania. I przez trzydzieści lat uczniowie nieodmiennie dochodzili do tych samych wniosków – że Indie nie poradzą sobie z sytuacją tak dobrze jak Stany Zjednoczone. Ale w ostatnim roku, z powodu Internetu, jeden z uczniów odpowiedział inaczej.

Gdy Art zadał swoje stare jak świat pytanie i poprosił o podniesienie ręki tych, którzy sądzą, że lepiej poradzą sobie Stany Zjednoczone – podniosły się wszystkie oprócz jednej. Kiedy z kolei zapytał, kto sądzi, że lepiej ze sprawą poradzą sobie Indie – podniosła się jedna ręka. Art zaczął inteligentnie indagować ucznia. „Więc sądzisz, że Indie poradzą sobie z sytuacją lepiej?" – powiedział najbardziej sceptycznym belferskim tonem. „Opisz więc i porównaj transport, media, opiekę zdrowotną w obu krajach, proszę". Uczeń przedstawił wszystko należycie. „Więc czemu sądzisz, że Indie poradzą sobie lepiej niż Stany Zjednoczone?". Uczeń odpowiedział po prostu: „Bo, według artykułu, który znalazłem w Internecie, w Bombaju nie ma wcale kotów".

Internet pomógł wielu uczniom stawiać nauczycieli w trudnej sytuacji. I dobrzy nauczyciele są tym zachwyceni. Bo to oznacza, że uczniowie poszukują informacji i lubią dowiadywać się czegoś, zamiast wkuwać na pamięć podane formuły i daty. Dzięki Internetowi Art znalazł kolejne rozwijające się państwo z dużą populacją kotów.

Problemy z Internetem w szkołach

Mimo że Internet jest wspaniałym narzędziem edukacyjnym, posługiwanie się nim w szkole nasuwa pewne problemy. Oprócz takich samych trudności, z jakimi borykają się rodzice dzieci mających dostęp do Internetu w domu, jest kilka specyficznych dla szkół. Chodzi tu o informacje na temat uczniów, jakie szkoła może udostępniać na własnej stronie WWW, o używanie własności intelektualnej uczniów i innych osób, o ocenę wiarygodności źródeł. Nie można też zapominać o hakerach, plagiatach i trudnościach, jakie ma szkoła w kontrolowaniu tego, co uczniowie piszą na własnych stronach internetowych, tworzonych i wysyłanych w domu. Wreszcie łańcuszki listowe, krążące między uczniami – mogą one zapchać cały system szkolny.

❖ Zdjęcia dzieci i informacje o nich

Wszyscy niecierpliwie oczekujemy momentu, kiedy możemy wysłać babci zdjęcie naszego dziecka wygrywającego zawody sportowe czy uzyskującego nagrodę w konkursie. Okupione ciężką pracą dziecka wzmianki o nim i migawki w lokalnej gazecie pieczołowicie wycinamy i wklejamy do albumu, by pokazać babci. Cóż więc złego w publikowaniu tych samych zdjęć na szkolnej stronie WWW?

Przede wszystkim strona WWW nie jest gazetą lokalną. Jest dostępna dla ponad 84 milionów ludzi w samych Stanach Zjednoczonych. Również dla ludzi, którzy mogą wykorzystać te informacje, by dotrzeć do naszych dzieci, i to nie są nasi sąsiedzi, powodowani troską o nie. To będą ludzie obcy twojej rodzinie i społeczności. (Jedna z ofiar, Polly Klaas, została wybrana z listy stworzonej na potrzeby marketingu skierowanego do nastolatek w pewnym obwodzie pocztowym. Jej zabójca kupił listę dziewczynek w określonym wieku i przypadkowo ją wylosował z listy. Lista zawierała adres, nazwisko i wiek).

Chociaż FBI nie donosiło jeszcze o przypadku molestowania dziecka, które byłoby znalezione poprzez szkolną stronę WWW, policjanci obawiają się (a ja także), że w którymś momencie ktoś wykorzysta publikowane tam informacje, by „namierzyć" jakieś dziecko. Pomyślcie chwilę. Dzieci, które figurują na szkolnych stronach WWW, są w szkole codziennie między ósmą a trzecią. Łatwo je tam znaleźć, można je śledzić, gdy idą do domu, zwłaszcza gdy ma się w ręku fotografię i zna się imię. „Agatko, czy mogę chwilę z tobą porozmawiać?". Jak wiele z naszych dzieci nie odpowie komuś, kto zwróci się do nich po imieniu?

Uważam za wskazane, by szkoły zamieszczały zdjęcia dzieci dopiero po uzyskaniu zgody rodziców i tylko w grupach co najmniej pięcioosobowych. Proponuję też, by nie wymieniano dzieci z imion

i nazwisk, ale określano je ogólnie, np. „Klasa trzecia pani Kowalskiej", „Drużyna siatkarek" itp.

Po zastanowieniu się przyznacie, że mam rację. Sądzę, że nigdy nie zgodzilibyśmy się, żeby ktoś umieścił zdjęcie naszego dziecka na wielkiej tablicy przy autostradzie. Pomyślmy o Internecie jak o gigantycznej tablicy ogłoszeń, ustawionej przy największej superautostradzie świata. Jeśli nie chcielibyśmy widzieć zdjęcia swojego dziecka w takim miejscu, nie umieszczajmy go w sieci.

W ubiegłym roku miałam pogadankę dla grupy rodziców w pewnym technikum. Podczas spotkania uświadomiłam sobie, że nawet mądrzy i pełni dobrych chęci nauczyciele nie myślą o zagrożeniach związanych z publikowaniem w Internecie informacji, umożliwiających identyfikację uczniów i kontakt z nimi. Kiedy jak zwykle mówiłam o tym, dlaczego nie należy pozwalać, by dzieci zamieszczały umożliwiające kontakt informacje o sobie na własnych stronach WWW lub wysyłały profile, jeden z rodziców nieśmiało podniósł rękę. „Czy to oznacza, że naszym dzieciom nie powinno się dawać pracy domowej, polegającej na zbudowaniu autobiograficznej strony WWW, zawierającej adres e-mailowy, zdjęcie i opis zainteresowań?". Najwyraźniej nauczyciel zalecił uczniom standardowe zadanie w postaci stworzenia własnej strony WWW. Nie miał pojęcia o zagrożeniach, jakie się z tym mogą wiązać, i natychmiast zmienił zadanie domowe, polecając stworzenie strony autobiograficznej, nie zawierającej informacji umożliwiających kontakt. Było to dla dzieci równie kształcące, a znacznie bezpieczniejsze.

Ostatnio zadzwoniła do mego biura bardzo zdenerwowana matka. Jej syn, uczeń szkoły podstawowej na Florydzie, chciał wziąć udział w szkolnym konkursie na najlepszy projekt autobiograficznej strony WWW. Matka nie chciała się zgodzić, by umieścił tam swój adres e-mailowy. Ponieważ nauczyciel wymagał, by adres był zamieszczony (żeby ludzie mogli bezpośrednio kontaktować się z dzieckiem), chłopiec został wykluczony z udziału w konkursie. Matka w trosce o bezpieczeństwo syna i jego kolegów szkolnych próbowała rozmawiać z nauczycielem i dyrektorem, ale nie znalazła większego zrozumienia. Kiedy ja sama zadzwoniłam do dyrektora, też nie spotkałam się ze szczególnie ciepłym przyjęciem. (Wiem, jestem prawnikiem, a żaden dyrektor nie ucieszy się z telefonu od prawnika w piątkowe popołudnie). Ale choć chłodne powitanie nie zrobiło na mnie większego wrażenia, to odpowiedź na moje ostrzeżenia o potencjalnym zagrożeniu

– tak. Zapytał, czy mogę przedstawić dowody na to, że jakieś dziecko było molestowane przez kogoś, kto znalazł je poprzez szkolną stronę WWW. Zapytałam wtedy, czy jest gotów zgodzić się na to, by jeden z jego uczniów był pierwszym takim dzieckiem? W tym momencie rozmowa urwała się, ale obiecał zastanowić się nad sprawą.

Ostatnią rzeczą, jaką ma się ochotę robić w piątek po południu, jest rozzłoszczenie dyrektora szkoły. (Są oni jedynymi istotami groźniejszymi niż rozjuszony byk – w każdym razie ja tak pamiętam dyrektora swojej szkoły). Ale to naprawdę ważne, by nauczyciele i dyrektorzy byli wyczuleni na zagrożenia związane z ujawnianiem informacji ułatwiających kontakt z dzieckiem na szkolnych stronach. Wszyscy mamy ten sam cel. I wspólny priorytet – dobro dzieci.

❖ Twórczość dzieci

Większość z nas miała ten luksus, że mogliśmy wystawiać prace artystyczne naszych dzieci, poczynając od pierwszych bazgrot, na drzwiach naszych lodówek. Gdy dzieci przechodziły od prostych wierszyków w klasach początkowych do kompozycji orkiestralnych w ostatnich, każdy z nas sądził, że wychowuje następcę Pavarottiego, Picassa i Longfellowa w jednej osobie. Pewnie nie byliśmy bezstronni – nasze pociechy jakoś nie zostały dostrzeżone w konkursach młodych talentów – ale ich twórczość, nawet najprostsza i najmniej porywająca, jest ich własnością. Należy do nich tak samo mocno, jak gdyby była chroniona przez prawo autorskie.

Szkoły powinny uzyskać zgodę ucznia i jego rodziców na publikowanie twórczości dziecka. (Tak samo jak wszystkie inne strony publikujące czyjąś twórczość. Kto wie, może kiedyś zostaną odkryci i wesprą nas na stare lata?).

❖ Plagiaty

Dzieci zawsze były pomysłowe, gdy idzie o unikanie prac domowych. Potrafią marnować całe godziny na miganie się od zajęć, których wykonanie zabierze im kilkanaście minut. My mogliśmy co najwyżej liczyć na mądrzejszego starszego brata czy kolegę, że pomogą nam odrobić lekcje (albo – najlepiej – odrobią je za nas), nasze cyberdzieci mogą serfować po setkach stron, które sprzedają nastolatkom gotowe wypracowania czy zadania z innych przedmiotów. I nawet nie mu-

szą ich przepisywać – tylko ściągają plik, napisany, zaopatrzony w wykresy, gotowy do oddania. Wielu znanych mi sprytnych nauczycieli zaznaczyło sobie te strony i rutynowo porównują prace dostarczone przez uczniów z tymi dostępnymi w Internecie. Ponieważ takie prace pobiera się po uiszczeniu opłaty, sprawdź wyciągi bankowe z karty kredytowej – może się okazać, że finansujesz ściąganie uprawiane przez twoje dziecko.

❖ Pozaszkolne strony WWW

Od pokoleń dzieci opowiadały sobie dowcipy o nauczycielach. Rysowały ich karykatury. Pokolenie cyberdzieci też to robi, ale one używają do tego potęgi Internetu, gdzie każdy może taką stronę obejrzeć. Dzieci podają kolegom adres strony, by ci mogli podziwiać ich twórczość. Często adresy trafiają do rąk nauczyciela. Nauczyciele i pracownicy administracji, którzy stali się obiektem opisów tam zawartych, grożą dyrekcji powiadomieniem policji lub wszczęciem postępowania sądowego. Szkoła czuje się wtedy w obowiązku coś zrobić. Na ogół dziecko zostaje zawieszone w obowiązkach ucznia lub usunięte ze szkoły, ewentualnie traci stypendium.

Pewien nastolatek, zezłościwszy się na niektórych nauczycieli i pracowników administracji, zemścił się, umieszczając parę wulgarnych i obraźliwych słów na ich temat na stronie WWW. Stronę napisał w domu i stamtąd przesłał ją do sieci. Nie była umieszczona na szkolnym serwerze, ale była dostępna dla każdego, kto korzystał z Internetu. Adres szybko upowszechnił się wśród uczniów i wielu z nich wchodziło tam, korzystając ze szkolnych komputerów. Kiedy wiadomość o tym dotarła do zainteresowanych nauczycieli i innych pracowników, wpadli w furię – trudno się temu dziwić. Zwrócili się o pomoc do policji, która groziła oskarżeniem ucznia o prześladowanie (ale nie była w stanie tego zrobić). Zdawało się, że wszyscy zaangażowani potracili głowy, ale kierownik – nie. Stwierdził, że nie jest to sprawa szkoły, ale rodziców. Wezwał rodziców, którzy się zjawili i potraktowali sprawę tak poważnie, jak na to zasługiwała. Razem wypracowali stosowną formułę przeprosin i taki sposób załatwienia sprawy, by jej nadmiernie nie rozdmuchiwać. Prasa nie doczekała się sensacji. Kierownik dzielnie wytrzymał wściekłość i presję nauczycieli. Miał rację.

Kilka miesięcy później opowiedział mi ciąg dalszy. Powiedział, że spotkał tego nastolatka na jakiejś szkolnej uroczystości i że uczeń

znowu usprawiedliwiał się i przepraszał za swój wyczyn. Podziękował kierownikowi za godne załatwienie sprawy. Chłopiec działał w złości i nie pomyślał o konsekwencjach. Po jakimś czasie nauczyciele także przyznali mu rację. Zaczęłam żałować, że moje dzieci są już dorosłe i nie mogą chodzić do szkoły kierowanej przez kogoś tak spokojnego i mądrego – na pewno skorzystałyby na tym. Szkoda, że nie wszyscy są tacy.

❖ Odsyłacze do innych stron

Jeśli szkoła tworzy odsyłacze do stron innych niż szkolne, powinna je sprawdzać, by mieć pewność, że są odpowiednie dla uczniów. Wiele witryn dla dzieci używa teraz stron pomostowych, by zaznaczyć przejście z bezpiecznego środowiska do sieci WWW. Jak taka strona może wyglądać? Zasadniczo przekazuje się tam komunikat: „Teraz wychodzisz z naszej witryny. Choć zapewniamy połączenie z różnymi stronami, o których sądzimy, że mogą cię zainteresować, zanim tam wejdziesz, powinieneś wiedzieć, że te strony nie są przez nas prowadzone, mogą nie zapewniać należytej ochrony danych osobowych, które im przekażesz, i mogły zmienić się pod względem zawartości od czasu, kiedy je recenzowaliśmy. Kiedy zdecydujesz się tam przejść, musisz polegać na własnej ocenie. Serfuj więc uważnie". (Oczywiście prezentują to na ogół w bardziej wyszukanej formie, ale sens jest taki).

Nawet jeśli szkoła twojego dziecka zdecydowała, że nie będzie tworzyć strony pomostowej, powinna poinformować rodziców, że dzieci mogą wchodzić na inne niż szkolne strony i mimo że ich zawartość była recenzowana w momencie tworzenia połączenia, od tego czasu mogły zostać zmienione lub usunięte, a szkoła nie może stale kontrolować tego, co się na nich dzieje. Szkoła musi poinformować rodziców i uczniów, że korzystają z tych stron na własną odpowiedzialność. Z tych powodów może lepiej nie tworzyć połączeń do stron pozaszkolnych, jeśli szkoła nie ma zamiaru regularnie ich kontrolować.

❖ Grożenie śmiercią i bombami

Grożenia bombą nie wymyślono w Littleton. Pomysłowe dzieci wywoływały szkolne alarmy bombowe od lat, zwłaszcza gdy była dobra pogoda albo gdy były nieprzygotowane do klasówek. (Kiedy ja byłam mała, mieliśmy zwyczaj wyznaczać kogoś do włączenia alarmu poża-

rowego). Ale od czasu tragedii w Littleton liczba szkolnych alarmów bombowych wzrosła dramatycznie.

W pewnym okręgu w Marylandzie plaga alarmów bombowych pojawiła się następnego dnia po zdarzeniach w Littleton. Dziennikarze uparcie dzwonili do mnie z zapytaniem, jak znaleźć w sieci pogróżki o bombie, które dotyczą określonej szkoły czy okolicy. Liczba ostrzeżeń wzrosła w okresie zwyczajowego przeprowadzania testów (jednak te dzieci nie różnią się od nas aż tak bardzo). W końcu alarmy, początkowo występujące tylko w Marylandzie, jak huraganowy ogień rozprzestrzeniły się po całym kraju, dotykając nawet te szkoły, w których testy przeprowadzano w innym terminie. (Zabawa w głupi telefon może być szczególnie groźna w Internecie, bo tam plotki rozchodzą się bardzo szybko, strasząc niepotrzebnie wielu ludzi).

Obecnie wiele szkół ma własną ochronę, która zajmuje się zapewnianiem bezpieczeństwa, bronią przynoszoną do szkoły, gangami, brutalnymi uczniami, różnymi formami protestów. Niektóre szkoły używają też filtrującego oprogramowania, które jest umieszczone poza szkołą, na jakimś serwerze zastępczym. Dzięki temu oprogramowaniu szkoła dysponuje miesięcznym rejestrem zablokowanych stron, na które uczniowie usiłowali wchodzić.

Na ogół strony zablokowane to również takie, na których można znaleźć instrukcje konstruowania bomb. Ale żadna ze szkół, z którymi miałam kontakt, nie przegląda swoich rejestrów i nie przekazuje ich ochronie. A tak łatwo można to zrobić i porównać z informacjami zebranymi przez ochronę w inny sposób. Szkoła powinna wiedzieć, kto uparcie szuka instrukcji budowy bomb, i wykorzystać tę wiedzę do lepszego rozwiązywania problemów bezpieczeństwa. Mają już te informacje, ale nikt z nich nie korzysta.

Rejestry mogłyby być wykorzystane w jeszcze inny sposób. Jednym z problemów, z którymi szkoły się borykają, jest brak wiedzy o groźbach, które uczniowie wysyłają za pośrednictwem sieci WWW. Uczniowskie strony nie są na ogół dostrzegane przez wyszukiwarki, a znalezienie strony, która nie jest skatalogowana w wyszukiwarce, jeśli nie zna się nazwy domeny, jest jak szukanie igły w wirtualnym stogu siana. Kiedy uczeń tworzy kontrowersyjną czy prowokacyjną stronę WWW, zazwyczaj jedynymi osobami, które o tym wiedzą, są koledzy, używający szkolnych komputerów, by wejść na tę stronę. A zatem rejestry odwiedzanych stron powiedzą nam o nagłej popularności pewnych adresów. Dlatego należy je przeglądać. Można w ten sposób szybko odnaleźć uczniowskie strony.

Jest to również dla władz szkoły rzadka okazja spożytkowania informacji, by zapobiec przemocy. Informacje te pozwalają wyłowić uczniów, którzy wołają o pomoc.

Szkoły mogą też ustanawiać własne linie zgłoszeniowe albo poinformować dzieci, że takie linie istnieją w innych miejscach. To podstawa.

❖ Ograniczanie wypowiedzi niezwiązanych z programem nauczania

Szkoły mają dużą swobodę w wybieraniu materiałów, lektur, podręczników i programów nauczania. Mają też prawo do selekcji materiałów i ograniczania wolności słowa w sprawach niezwiązanych z programem. Prawo daje szkołom rozległe uprawnienia do blokowania i cenzurowania wypowiedzi, jeśli jest to uzasadnione bezpieczeństwem i dobrem uczniów. Ale jeśli szkoła tworzy otwarte forum, takie jak wydawnictwo lub strona WWW, i pozwala członkom społeczności na przekazywanie komentarzy, nie może później cenzurować poglądów, które się jej nie podobają. Forum może być albo zamknięte – i wtedy łatwo podlega ograniczeniom, albo otwarte – i szkoła już nie ma możliwości oddziaływania.

Szkoły muszą zastanowić się nad ograniczeniem otwartych form wypowiedzi, dostępnych społeczności uczniowskiej, jeśli chcą zachować prawo do kontroli zawartości szkolnych stron WWW.

❖ Programy korespondencyjnych przyjaźni

Jedną ze wspanialszych dróg poznawania dzieci z całego świata jest znajdowanie w Internecie korespondencyjnych przyjaciół. Programy współpracy na poziomie międzyszkolnym są najbezpieczniejszą drogą komunikacji z nieznajomymi. Potrzebujemy więcej takich programów, miejmy więc nadzieję, że szkoła twojego dziecka włączy się w ich tworzenie.

Jeśli szkoła nie współpracuje z innymi wybranymi szkołami w programie szukania przyjaciół, rodzice powinni być o tym poinformowani w ulotce o zasadach korzystania z Internetu i wyrazić zgodę na

ewentualny udział dziecka w innych tego rodzaju programach. Z udziałem dziecka w programie szukania przyjaciół, który nie ma gwarancji szkoły, wiąże się wiele zagrożeń, które omówiłam w rozdziale 2.

❖ Ocena wiarygodności źródeł: jak uczyć dzieci krytycznego myślenia i umiejętnego korzystania z mediów

Wydanie książki jest kosztowne. Zrobienie programu w telewizji zwykłej i kablowej nawet jeszcze bardziej. Gazety starannie sprawdzają fakty, a ośrodki naukowe korzystają z opinii recenzentów dla upewnienia się, że to, co ma zostać opublikowane, jest rzetelne i wiarygodne. Ale stronę WWW każdy może opublikować w ciągu paru godzin i ogłosić tam wszystko, co zechce – nieraz bez rzetelnych podstaw. (Ja często utrzymuję, że jestem wysoka, szczupła, mam blond włosy i jestem przystojna. Bo nikt nie powiedział, że myślenie życzeniowe jest w Internecie zakazane).

Zostawiając na boku rozmiary mojej garderoby, skąd można wiedzieć, kiedy ma się do czynienia z wiarygodną informacją, a kiedy z czyjąś bufonadą? Nie jest to łatwe. Nie ma w Internecie stempla kontroli jakości. Strona opublikowana przez grupę antysemitów, którzy utrzymują, że Holocaust wcale się nie zdarzył, może wyglądać poważnie i brzmieć jak uczona dysertacja. I kiedy nasze dzieci się na nią natkną, mogą potraktować ją jak materiał źródłowy do pracy o II wojnie światowej. Ostatnio szkoły spotykają się z tym problemem dość często. Trzeba więc nauczyć dzieci, jak mają oceniać wiarygodność stron WWW, by Internet mógł stać się pomocą w kształceniu. Dzieci muszą stać się krytycznymi konsumentami informacji.

Kiedy natykamy się na jakąś stronę, powinniśmy zastanowić się, jaki cel mógł przyświecać jej autorowi. Czy została zaprojektowana, żeby coś sprzedać? Jeśli jest własnością kogoś, kto coś sprzedaje, można domyślać się, że zaprojektowano ją, by choćby pośrednio promować jakiś produkt czy usługę. Każda strona stworzona po to, by coś sprzedać, powinna być oceniana tak samo krytycznie jak wszelkie promocje czy reklamy w realnym świecie.

Gdy już znamy punkt widzenia twórcy, możemy lepiej ocenić to, co nam przekazuje. Nawet młodsze dzieci miały okazję przekonać

się, że batony i hamburgery naprawdę nie są tak duże i smaczne, jak wydawały się w telewizji. Zetknęły się z byle jak wykonanymi zabawkami czy z grami komputerowymi, do których potrzebne było dodatkowe oprzyrządowanie za dodatkowe pieniądze, żeby w ogóle działały, choć wcześniej o tym nie wspominano. Łatwo więc będzie zachęcić je do krytycznego myślenia podczas oglądania stron internetowych.

Informacje przedstawiane na stronie WWW powinny być dokładne i aktualne. Jeśli prezentuje się tam określony punkt widzenia – powinno to być jasno powiedziane, a kwalifikacje autorów – rzeczowo określone.

Oglądając jakąś stronę, dzieci poszukujące materiałów do prac szkolnych muszą zwrócić uwagę na kilka rzeczy:

- **Kto jest autorem lub twórcą strony, jakie ma kwalifikacje i dorobek?** Czy napisał ją laureat Nagrody Nobla, czy Jaś Nawiedzony? Choć niewielu autorów jest skłonnych przyznać, że nie mają podstaw do wygłaszania stwierdzeń, które wygłaszają, zostawiają różne demaskujące ich wskazówki.
  Dzieci powinny najpierw zajrzeć do referencji wystawionych autorom. Jeśli ktoś podaje, że jest profesorem Uniwersytetu Południowej Laponii, powinny być odsyłacze do stron Uniwersytetu. Czy autor wymienia posiadane nagrody? Jeśli tak, to czy zamieszcza odnośniki do miejsc, gdzie można znaleźć potwierdzenie tych faktów? Czy autor coś opublikował? Jeśli tak, to czy znane witryny księgarskie mają jego książki?
  Poszukaj innych stron z ewentualnymi referencjami tej osoby. Nie każdy musi być profesorem uhonorowanym nagrodami czy znanym autorem, ale większość dobrych materiałów jest cytowana w innych miejscach w sieci.
- **Jaka jest orientacja strony? Jakiego punktu widzenia nie uwzględnia?** Posiadanie określonej orientacji niekoniecznie jest złą rzeczą, pod warunkiem że czytelnik jest tego świadomy. Nie zapominajmy, że wszyscy mają jakieś nastawienia, ale niektóre bywają szczególnie znaczące. Czy jest to materiał reklamowy, przedstawiający „bezstronne" poglądy ogłoszeniodawcy? Czy ten fakt jest podany do wiado-

mości czytelnika? Czy jest to strona prezentująca organizację non profit, realizującą określoną misję lub cel? Gdzie utworzono stronę? Czy należy do międzynarodowej grupy, która może mieć jakieś uprzedzenia wobec jakiejś kultury lub wobec jakiegoś narodu?
Często, uważnie czytając, można odkryć nastawienie autora. Zastanów się nad tym, przez kogo zostało to napisane, jaki punkt widzenia przedstawiono, a jakie poglądy pominięto? Uczniowie i studenci powinni starać się uwzględnić różne orientacje i punkty widzenia, gdy poszukują materiałów do prac.

- **Jak dalece aktualne są informacje?** Czy strona zawiera informację o ostatnim „uaktualnianiu"? Wiele stron, które studiowałam, pisząc tę książkę, także te poświęcone wyszukiwaniu rzetelnych źródeł, ostatnio uaktualniano w 1996 r. Kiedy je czytałam, miałam to na uwadze. Niektóre rzeczy nie uległy zmianom, ale inne – jak choćby lista akceptowanych stron czy rola szkół – zmieniły się ogromnie. Strona, na którą zajrzałam w poszukiwaniu aktualnych informacji, była uaktualniana kilka miesięcy wcześniej i ta data widniała na samym wierzchu. Jeśli nie ma takiej daty, zobacz, czy jest rubryka „ostatnie doniesienia" albo „co nowego" i jak często ten fragment jest zmieniany. Dobra strona jest „odnawiana" regularnie przynajmniej raz w miesiącu, a strony z nowinkami i modnymi tematami – częściej.
- **Czy podawane informacje są spójne?** Czy informacje podane na stronie nie są sprzeczne? Czy wszystkie są na temat? A może autorzy proponują cenzurowanie w jednym zdaniu, a swobodę wypowiedzi w drugim? Czy to jedyna strona, gdzie wyraża się takie poglądy, czy też są inne, które te poglądy wspierają? Czy porównałeś jej zawartość z uznanymi źródłami? Często strona, która wygląda zbyt dobrze, żeby mogła być prawdziwa, nie jest prawdziwa. Większość wartościowych stron, przedstawiających dobrze ugruntowane poglądy, znajduje uznanie u innych.
- **Do jakich stron ma odnośniki?** Czy są aktywne? Czy są przejścia do wiarygodnych stron oraz czy rzetelne i wiarygodne strony mają odnośniki do omawianej? Czy odsyłacze są prawidłowo oznaczone? Czy są aktualne? Jakie jeszcze strony umieściły odnośniki do oglądanej? Czy odnośniki faktycznie działają, czy też prowadzą donikąd?

Bezpieczne korzystanie z Internetu w szkole

❖ Udział rodziców

Najlepszym sposobem, który szkoła może zastosować, by włączyć rodziców, jest poinformowanie ich o tym, co się dzieje. Każda ankieta, którą przeprowadzam wśród rodziców, ujawnia jedno: nie wiedzą oni, jak w szkole dziecka korzysta się z Internetu, a wielu z nich nie wie również, co to jest Internet i jak działa. Wszystkie szkoły ubolewają nad faktem, że rodzice są mało zaangażowani, podczas gdy rodzice narzekają, że są ignorowani.

Informacja i świadoma zgoda

Najprostszą drogą zaangażowania rodziców jest poinformowanie ich o tym, co szkoła robi (nazywam to „zasadą informowania"), uzyskanie ich zgody na wszystko, co wiąże się z podwyższonym ryzykiem (nazywam to „zasadą świadomej zgody") i edukacja, by mogli uczestniczyć w podejmowaniu decyzji i rozwiązywaniu problemów.

Szkoły powinny poinformować rodziców, jak korzysta się z Internetu na terenie szkoły, jakie zagrożenia istnieją w sieci i jak sobie z nimi radzić. Informacja musi być jasna i wyczerpująca, wszystkie istotne sprawy tak przedstawione, by zrozumieli nawet ci najmniej zorientowani w komputerach rodzice. I powinna być dołączona do regulaminu korzystania z Internetu, który szkoła przygotowuje i wręcza uczniom oraz rodzicom.

Każda szkoła powinna opracować regulamin korzystania z Internetu, niezależnie od tego, czy stosuje oprogramowanie filtrujące, czy nie. Ma to być zbiór zasad, których dzieci (i nie tylko one) muszą przestrzegać, korzystając z Internetu. Niektóre szkoły formalizują tryb przyjmowania regulaminu (staje się on przedmiotem decyzji rady pedagogicznej), inne wprowadzają go zwyczajnie, jak wiele obowiązujących w szkole zasad (choćby zakaz biegania po korytarzach czy pa-

lenia papierosów na terenie szkoły). Ale każda szkoła powinna mieć regulamin internetowy.

Byłam zadziwiona, dowiadując się, że tak niewiele szkół przyjęło jakiś regulamin korzystania z Internetu. Niedawno występowałam przed grupą dyrektorów szkół w jednym z większych miast w Stanach Zjednoczonych. Byłam zaszokowana, gdy powiedzieli mi, że od dwóch lat rozważają przyjęcie regulaminu właściwego korzystania z Internetu, ale dotychczas żadnego nie przyjęli. W ten sposób szkoła naraża się na odpowiedzialność prawną. Czekać dwa lata, by ustalić zasady dotyczące tego, co dzieciom wolno, a czego nie wolno robić, gdy włączają się do sieci? Dlaczego? Rozumiejąc zagrożenia, szkoły powinny szybko ustalić zasady bezpieczeństwa i uzyskać aprobatę rodziców. Jeśli formalne ustalenia trwałyby za długo, lepiej to zrobić mniej formalnie i po prostu wręczyć rodzicom i uczniom zbiór zasad.

Tworzenie takich regulaminów to nic nadzwyczajnego. Przez lata robiłam to na użytek wielkich korporacji, a szkoły są czymś podobnym. I choć my, prawnicy internetowi, mamy nadzieję, że wynajmiecie nas do tej pracy, żebyśmy mogli wykarmić nasze dzieci i opłacić im czesne, tak naprawdę prawnik nie jest do tego potrzebny. Regulamin musi jasno przedstawiać dzieciom i rodzicom, co im wolno, a czego nie, i jakie będą konsekwencje złamania zasad. Wiele szkół nieodpłatnie udostępnia swoje regulaminy, więc można zapoznać się z kilkoma i wybrać z nich to, co odpowiada waszym potrzebom. W aneksie załączyłam dwa przykładowe regulaminy.

Ustalanie reguł

Oto co należy wziąć pod uwagę, opracowując zasady korzystania z Internetu:

- Gdzie w szkole jest dostęp do Internetu? Czy tylko w bibliotece? W klasach?
- Kto nadzoruje korzystanie z Internetu?
- Jakie są szczególne warunki korzystania z Internetu w różnych miejscach na terenie szkoły?
- Co uznajemy za zagrożenie? Łańcuszki e-mailowe? Korzystanie z programów typu komunikator? Wchodzenie na nieodpowiednie strony? Przekazywanie danych osobowych? Wysyłanie obraźliwych wypowiedzi o innych? Łamanie praw autorskich? Piractwo? Pogróżki użycia przemocy? Grożenie bombą? Korzystanie z płatnych serwisów?
- Czy korzysta się z serwisów lub oprogramowania filtrującego? Jak to działa? Czy istnieje ryzyko nadmiernego filtrowania (gdy niewinne strony zostają zablokowane) lub niedostatecznego filtrowania (gdy niestosowne strony będą dostępne)? Co należy zrobić, jeśli uczeń potrzebuje dostać się na stronę, do której dostęp jest zablokowany? Czy są sposoby ominięcia blokady? Czy lista stron blokowanych może być modyfikowana? Czy można z niej usuwać strony i dodawać nowe?
- Jakie są zasady dotyczące ściągania plików? Czy uczniowie zostali poinformowani o wirusach i hakerach?
- Czy na szkolnej stronie WWW umieszczona jest wewnętrzna książka adresowa z numerami telefonów, imionami dzieci i rodziców? Plany lekcji? Nazwiska członków drużyn sportowych?
- Czy uczniowie mogą być ukarani za publikowanie zniesławiających lub prowokujących informacji o szkole i personelu na stronach WWW, które tworzą poza szkołą?
- Gdzie uczniowie mogą zgłaszać strony, w których grozi się przemocą? Czy istnieje anonimowa linia zgłoszeniowa, z której mogą korzystać?
- Czy szkoła publikuje dane osobowe uczniów w sieci? Czy podaje adresy e-mailowe? Czy zamieszcza zdjęcia? Indywidualne czy grupowe? Czy można zidentyfikować uczniów na tych zdjęciach? Jak?
- Jakie informacje na temat aktywności uczniów w Internecie szkoła gromadzi? Komu mogą być udostępnione? Czy są dostępne dla rodziców na ich życzenie?
- Co się stanie, jeśli uczeń złamie reguły? Czy dostanie naganę? Zostanie zawieszony?

Gdy szkoła już ustali, jak ma wyglądać regulamin, powinna przedstawić go uczniom i rodzicom (pamiętając, że nie wszyscy rodzice muszą wiedzieć cokolwiek o Internecie, więc należy używać możliwie przystępnego języka). Trzeba poinformować dzieci, co im wolno robić, a czego nie, uświadomić konsekwencje grożące za nieprzestrze-

ganie zasad. Następnie trzeba omówić zagrożenia i uzyskać zgodę rodziców na wprowadzenie ustalonych zasad.

Wyjaśnianie wyborów dokonanych przez szkołę

Jeśli szkoła postanawia nie korzystać z oprogramowania filtrującego, należy wyjaśnić, dlaczego taka decyzja została podjęta, jakie wybrano lepsze sposoby zapewnienia bezpieczeństwa. Oto przykład, jak można to zrobić:

„Szkoła Monroe Middle ma jedną z najlepszych pracowni informatycznych w Middletown. Pani Richards, bibliotekarka specjalista od mediów, właśnie przejrzała dostępne produkty filtrujące. Doszła do wniosku, że blokują one więcej stron niż trzeba, a zarazem wiele nieodpowiednich stron nie jest blokowanych, opracowała więc specjalny system tylko dla Monroe.

Począwszy od tej jesieni, pani Richards będzie uczyła zasad bezpiecznego korzystania z Internetu, a na lekcjach wychowania społecznego uczniowie będą pracowali nad projektem strony WWW o bezpiecznym serfowaniu i będą gromadzili pomysły na ten temat. Biorąc pod uwagę liczbę uczniów i personelu kontrolującego, wierzymy, że połączenie edukacji dotyczącej bezpieczeństwa w sieci i ścisłej kontroli nad uczniami korzystającymi z Internetu najbardziej odpowiada naszym potrzebom.

Ponadto każdy uczeń otrzyma regulamin korzystania z Internetu, w którym wyjaśniamy, co wolno, a czego nie wolno robić w szkolnym systemie komputerowym. Regulamin ten wyślemy rodzicom każdego dziecka. Muszą się z nim zapoznać. Pani Richard będzie odpowiadać na wszystkie pytania uczniów i rodziców, a odpowiedzi na najczęściej zadawane pytania zostaną umieszczone na szkolnej stronie WWW.

Zanim uczeń będzie mógł korzystać w szkole z dostępu do Internetu, pani Richards musi otrzymać od rodziców podpisany egzemplarz regulaminu. To oznacza, że rodzice także są odpowiedzialni za zachowanie ich dzieci w Internecie, tak w domu, jak i w szkole".

A gdy szkoła zdecyduje się na oprogramowanie filtrujące:

„Szkoła Monroe Middle ma jedną z najnowocześniejszych pracowni komputerowych w Middletown. Pani Richards, bibliotekarka specjalista od mediów, zakończyła właśnie sprawdzanie dostępnych produktów filtrujących i wybrała najlepiej odpowiadający potrzebom

szkoły. Ten system został już wybrany przez pięć tysięcy szkół w naszym stanie. Jest jednym z najwyżej cenionych przez szkoły. Na rynku istnieje od 1996 roku. Zapoznaliśmy się z badaniami efektywności blokowania i doszliśmy do wniosku, że program ten lepiej niż inne filtruje treści skażone nienawiścią, przemocą i inne, które uważamy za nieodpowiednie dla naszych uczniów.

Trzeba jednak wiedzieć, że każdy program filtrujący może blokować strony najzupełniej niewinne, a przepuszczać nieco takich, których zawartość jest szkodliwa. Z tego powodu chcemy dołożyć starań, by nasze dzieci rozumiały, na czym polegają zagrożenia, i wiedziały, jak korzystać z Internetu efektywnie i bezpiecznie.

Począwszy od tej jesieni, pani Richards będzie prowadziła lekcje poświęcone problemom bezpieczeństwa w sieci, a na lekcjach wychowania obywatelskiego dzieci będą pracowały nad projektem strony WWW, dotyczącej bezpiecznego serfowania. Biorąc pod uwagę stosunek liczby uczniów do liczby personelu, mogącego sprawować nadzór, uważamy, że oprogramowanie filtrujące jest istotną częścią naszego planu bezpieczeństwa i będzie używane razem z edukowaniem uczniów i dokładnym sprawdzaniem ich poczynań przy komputerach.

Poza tym każdy uczeń otrzyma regulamin korzystania z Internetu, w którym określono, co dziecko może, a czego nie może robić, używając szkolnego systemu komputerowego. Regulamin wyślemy rodzicom, którzy muszą się z nim zapoznać. Pani Richards będzie odpowiadać na wszystkie pytania uczniów i rodziców, a listę najczęściej zadawanych pytań umieści również na szkolnej stronie WWW.

Żaden uczeń nie będzie mógł korzystać ze szkolnego systemu, dopóki pani Richards nie otrzyma od jego rodziców podpisanego egzemplarza regulaminu korzystania z Internetu. Oznacza to, że rodzice także biorą odpowiedzialność za zachowanie dziecka w sieci, w domu i w szkole".

Jeśli rodzice są poinformowani, mogą zdecydować, jakiego rodzaju zagrożenia są w stanie zaakceptować. Jeśli szkoła wysyła rodzicom do podpisania tylko formularz zgody bez odpowiedniego omówienia problemu, to taki formularz zgody nie jest wart papieru, na którym go wydrukowano. Każda zgoda, żeby była znacząca, musi być zgodą świadomą, czyli podjętą wtedy, gdy posiada się potrzebne informacje.

Bywa, że dziecko spędza czas w witrynach aukcyjnych, gdzie wydaje duże sumy. Szkoły chciałyby, żeby to rodzice, a nie szkoły, odpo-

wiadali za to. To kolejny powód, dla którego szkoły powinny zadbać o stworzenie regulaminu korzystania z Internetu i o uzyskanie świadomej zgody rodziców na proponowane warunki.

A jeśli rodzice nie podpiszą zgody, szkoła musi dopilnować, by dziecko rzeczywiście nie miało dostępu do Internetu ze szkolnego systemu. W innym przypadku szkoła może ponosić odpowiedzialność.

Niech zdecydują rodzice

Rodzice, uzbrojeni w odpowiednio dokładne informacje, są osobami najbardziej uprawnionymi do podejmowania decyzji tyczących bezpieczeństwa ich dziecka. Toczy się dyskusja na temat zamieszczania fotografii uczniów na szkolnych stronach WWW? Niech zdecydują rodzice. Powiedz im, na czym polega kontrowersja – jedni rodzice chcą sławy i splendoru dla dziecka, inni natomiast obawiają się, że zdjęcie może pobudzić pedofilów do podejmowania prób kontaktu. Wyłóż wszystko uczciwie. A wybór należy do nich.

Jeśli szkoła chce mieć pewność, że jest rozgrzeszona z odpowiedzialności i wolna od ewentualnych roszczeń, jedyną drogą jest uzyskanie poręczenia od rodziców. Jednakże kiedy rodzice zgodzą się zwolnić szkołę od odpowiedzialności, oni ponoszą ryzyko, że mogą być pociągnięci do odpowiedzialności przez swoje dzieci po osiągnięciu przez nie pełnoletności.

Na przykład:

„Jesteśmy dumni z naszych uczniów. I gdy mamy okazję uczcić ich sukcesy i osiągnięcia sportowe, publikujemy ich zdjęcia i opisy dokonań w naszej szkolnej gazetce. Te same materiały pojawiają się też w lokalnej gazecie. Naturalne byłoby zamieszczenie tych artykułów i zdjęć także na naszej szkolnej stronie WWW.

Ale wielu ekspertów od spraw bezpieczeństwa przestrzega przed zamieszczaniem w Internecie zdjęć nieletnich. Uważają, że ktoś może użyć tych informacji, by odszukać i ewentualnie skrzywdzić dziecko. Eksperci podkreślają, że opublikowanie tych informacji na stronie WWW to zupełnie inna sprawa niż umieszczenie ich w szkolnej gazetce czy gazecie lokalnej, przede wszystkim dlatego, że Internet ma w samych tylko Stanach Zjednoczonych ponad 84 miliony użytkowników, znacznie więc więcej niż możliwa liczba czytelników szkolnej gazetki czy lokalnej gazety. Podkreślają też, że ludźmi, do których te informacje mogą trafić, nie są sąsiedzi, którym leży na sercu dobro naszych dzieci, ale obcy, którzy nie czują żadnej więzi z naszą społecznością.

Policja podaje, że dotychczas nie natrafiono na ślad żadnego przypadku molestowania czy krzywdzenia dziecka, do którego doszło za sprawą opublikowania informacji o uczniu na szkolnej stronie WWW. Z tego powodu uznaliśmy, że decyzja należy do rodziców. Nasza szkoła z zasady publikuje tylko grupowe zdjęcia dzieci, z podpisem określającym całą grupę, bez imion poszczególnych osób, rodzice mogą przedstawić na piśmie zalecenie umieszczenia w Internecie zdjęcia ich dziecka podpisanego imieniem i nazwiskiem, jeśli takie zdjęcie pojawi się w gazetce szkolnej. Odpowiedni formularz będzie dostępny na każde żądanie. Rodzice muszą zapewnić, że rozumieją zagrożenia i że przyjmują odpowiedzialność za wszelkie negatywne skutki swoich decyzji. Formularz zawiera stwierdzenie, że rodzice przejmują wszelkie ryzyko i zwalniają szkołę i dyrekcję szkoły od jakichkolwiek roszczeń związanych z opublikowaniem zdjęcia i nazwiska.

Chcielibyśmy, by rodzice podzielili się z nami swoimi uwagami na ten i inne tematy. Proszę zwracać się do pani Richards ze wszystkimi pytaniami, możecie też odwiedzić szkolną stronę WWW. Nasza szkoła jest niezwykła właśnie dzięki temu, że mamy stałe, robocze kontakty z rodzicami naszych uczniów i całą społecznością. Razem sprostamy tym trudnym i ekscytującym czasom".

Jak mogą się włączyć rodzice?

❖ Dobrzy rodzice to poinformowani rodzice

W grudniu 1997 na pierwszej zorganizowanej przez Biały Dom konferencji poświęconej sprawom bezpieczeństwa dzieci w Internecie, gdzie podpisywałam swoją poprzednią książkę, nieśmiało podeszła do mnie wysoka, smukła i bardzo atrakcyjna kobieta. (Rzecz jasna, znienawidziłam ją od pierwszego wejrzenia!). Przedstawiła się jako Della Curtis, bibliotekarka, specjalista od mediów i szef Biura Techniki Informatycznej Szkół Publicznych okręgu Baltimore. Następnie wręczyła mi swoją książkę – opasły tom poświęcony ustalaniu przez szkoły regulaminów dostępu do Internetu, gdzie uwzględniono me-

tody przeciwdziałania nękaniu seksualnemu, zasady zalecane przez szkołę przy tworzeniu i publikowaniu stron WWW, zasady korzystania z Internetu i wiele, wiele innych spraw. Wyjaśniła, że zajmuje się problemem nowoczesnych technologii i opracowuje zasady, dzięki którym szkoły mogłyby przeciwdziałać zagrożeniom związanym z Internetem, i że będzie zaszczycona, jeśli rzucę okiem na jej pracę.

Wzięła podpisany egzemplarz mojej książki, uścisnęła mi rękę i odeszła. Za dwie godziny wróciła. Przez ten czas przeczytałam jej książkę, a ona moją, od deski do deski. (Nie na darmo była bibliotekarką! Nikt nie czyta tak szybko jak bibliotekarze). Zbliżając się do końca jej książki, wiedziałam, że chcę pracować z tą niezwykle utalentowaną kobietą. Muszę! Była zbyt wielkim odkryciem, bym miała pozwolić jej odejść. Na szczęście ona miała podobne wrażenia na mój temat. (Teraz jest jedną z moich najlepszych przyjaciółek i kieruje w Wired Kids zespołem doradców dla szkół, bibliotek i innych miejsc publicznych oferujących dostęp do Internetu).

Wraz z grupą równie świetnych specjalistów od mediów bibliotecznych z okręgu Baltimore stworzyliśmy program dla rodziców pod nazwą Internetowa Edukacja Rodziców. Obejmował on godzinny blok w telewizji kablowej, który prowadziłam i w ramach którego była dyskusja panelowa i pokaz korzystania z Internetu. Ale prawdziwą perełką programu były lekcje dla rodziców, odbywające się w szkołach, do których chodziły ich dzieci. Okazało się, że to najlepszy i najskuteczniejszy program przybliżający rodzicom Internet w kraju (a pewnie i na świecie).

❖ Tworzenie zespołów złożonych z rodziców, bibliotekarzy i nauczycieli

W miarę jak coraz więcej szkół i bibliotek uzyskuje dostęp do Internetu, nauczyciele i bibliotekarze stają się internautami. (Nie chodzi o to, że robią coś, czego nie powinni, tylko o to, że stają się użytkownikami sieci). Zawsze są oni sprzymierzeńcami rodziców. Znają nasze dzieci i dzieci naszych sąsiadów, wiedzą, co dzieci robią, kiedy rodzice są w pracy, i wiedzą też, jakie niezwykłe możliwości tkwią w sieci.

Poproś ich o skonstruowanie programu zachęcającego rodziców do współpracy. Zrób, co zdołasz, by im pomóc. Zasługują na nasze

wsparcie i podziw. (Już to chyba mówiłam wcześniej – bibliotekarze są naszym najbardziej niedocenionym bogactwem naturalnym. A ja mam to szczęście, że znam wielu naprawdę nadzwyczajnych). To skarbnica różnych źródeł i wskazówek. Na przykład Amerykańskie Stowarzyszenie Bibliotekarzy stworzyło wspaniałą stronę nazwaną KidsConnect, która jest prowadzona przez bibliotekarzy szkolnych. Poprzez e-maile wysłane na adres strony dzieci zadają bibliotekarzom pytania, a po kilku dniach uzyskają odpowiedź, gdzie znajdą materiały na poruszany temat. Wtedy mogą zwrócić się po pomoc do bibliotekarza we własnej szkole.

Jeśli zechcesz pomóc, gdy już skończysz czytać tę książkę i masz chwilę, by swobodnie poserfować, masz szansę wesprzeć plan włączania szkół i bibliotek do sieci. Podziel się bogactwem. Pokaż innym, co umiesz, i pozwól, by oni nauczyli cię tego, co umieją.

Rzuć okiem na proponowane przez szkołę regulaminy korzystania z Internetu i zobacz, czy nie możesz zaproponować jakichś ulepszeń. Zgłoś się na ochotnika, by nauczyć innych rodziców tego, co sam umiesz, podziel się wiedzą o dobrych i ciekawych stronach, które znalazłeś.

Zrealizowanie skutecznej ochrony naszych dzieci w Internecie wymaga powstania zespołu, w którym współdziałać będą rodzice, bibliotekarze i nauczyciele.

❖ Wskazówki dotyczące tworzenia zespołu

Jeśli zastanawiasz się, w czym możesz pomóc i jak przystąpić do tworzenia takiego zespołu, oto kilka spraw, od których można zacząć:

- Co inne dzieci robią w Internecie?
- Ile inni rodzice wiedzą o Internecie?
- Jakie przyjęto regulaminy korzystania z dostępu do Internetu?
- Porozum się z innymi rodzicami i ustalcie wspólnie zasady postępowania w sytuacjach, gdy dzieci korzystają z Internetu w domu swoich kolegów.
- Przestrzegaj wspólnie ustalonych zasad i szanuj wartości uznawane przez innych rodziców.
- Przekazuj innym adresy nowych, ciekawych stron, na które się natkniesz.

- Czy inni rodzice używają oprogramowania filtrującego? Jeśli tak, jakiego?
- Co jest najlepsze spośród tego, co oni wybrali?
- Zaplanuj kilka lokalnych inicjatyw, choćby coś w rodzaju cyberzabawy w ciepło-zimno.
- Korzystaj z możliwości technicznych, jakie ma biblioteka.
- Koniecznie włącz do zespołu bibliotekarza i specjalistę od mediów.

Najlepsze instrukcje bezpiecznego korzystania z Internetu, na jakie się natknęłam, pochodziły z bibliotek, a sama śmietanka – z bibliotek szkolnych. Sprawdź, z jakich korzystają w twojej bibliotece szkolnej.

Uwagi autorki

Stale otrzymuję e-maile od nauczycieli. Chcą, bym rekomendowała materiały edukacyjne i programy dotyczące bezpieczeństwa w Internecie. Proszą mnie o opinie na temat oprogramowania filtrującego, zamkniętych systemów i zasad bezpiecznego korzystania z sieci. Ale najczęściej chcą wiedzieć, jaka odpowiedzialność im grozi, jeśli dzieci wpadną w kłopoty, korzystając z Internetu pod ich nadzorem.

Jakie to smutne, że nauczyciele, którzy są przepracowani, mają niskie zarobki i są niedostatecznie wspierani przez nas, rodziców – dodatkowo czują się zagrożeni sankcjami prawnymi z powodu informacji, na jakie mogą natknąć się dzieci w Internecie! Wszystkie te lęki mogą wynikać z postaw, jakie szkoły prezentują wobec problemów związanych z dostępem do Internetu.

Zachowanie bezpieczeństwa naszych dzieci wymaga wspólnego działania. Szkoły, bibliotekarze i rodzice muszą połączyć siły, jeśli mamy zyskać pewność, że wszystkie dzieci mogą w pełni bezpiecznie korzystać z dobrodziejstw Internetu. Ale wiele szkół lekceważy sprawę, przyjmując, że samo oprogramowanie filtrujące wszystko załatwi, i podejmując decyzje za zamkniętymi drzwiami. To problem wspólny i każdy musi się włączyć i wiedzieć, co szkoły robią w sieci.

Kiedy nauczyciel ma 25–30 dzieci w klasie i jeszcze ktoś instaluje mu w klasie komputer, co on ma zrobić? Kto ma go wyszkolić? Jak używać komputera – do nauki czy do zabawy? Kto ma go zrepe-

rować, gdy się zepsuje? (Większość szkół polega wyłącznie na zdolnych uczniach).

Odpowiedzi na wszystkie te pytania nie pojawią się od razu. Nie ma rozwiązań dobrych dla wszystkich szkół i klas. Wypracowanie ich wymaga czasu, cierpliwości i elastyczności, tak ze strony nauczycieli, jak i rodziców. Władze szkoły muszą rozmawiać z rodzicami i nauczycielami, by opracować program, który będzie dla wszystkich dobry.

Nauczyciele powinni móc spokojnie spać w nocy i nie zamartwiać się tym, że zirytowani rodzice mogą zaskarżyć ich w związku z poczynaniami dzieci w Internecie. (Właśnie dowiedziałam się o takim przypadku).

Upewnijmy się, że nauczyciele nie obawiają się korzystania z nowej, wspaniałej technologii. Wesprzyjmy ich, by mogli wprowadzić nasze dzieci w nowe tysiąclecie.

Rozdział 7

Ucz swoje dzieci dobrze

Ze wszystkich narzędzi i wskazówek dbania o bezpieczeństwo, które wam przedstawiłam, najważniejsze jest stwierdzenie, że najlepszą obroną jest edukacja internetowa. Musisz nauczyć dzieci, by były uważne i ostrożne w cyberprzestrzeni.

Nawet gdy używasz wszystkich dostępnych zabezpieczeń technicznych, jeśli dzieci nie wiedzą, co im grozi i jak reagować, gdy zetkną się w sieci z czymś dalekim od ideału – są mimo wszystko zagrożone.

Nie da się filtrować życia. Będą więc dobrze uzbrojone, gdy będą dobrze przygotowane.

Kto kogo uczy?

❖ Pozwólcie, by dzieci was uczyły: niełatwo jest słuchać

Przez całe życie dzieci są uczone i instruowane przez dorosłych. Wszyscy – nauczyciele, rodzice, członkowie rodziny – wiedzą więcej i stale to podkreślają. Wiecie co? Większość naszych dzieci wie dużo więcej o komputerach niż my. Są biegłe w strategicznych grach komputerowych, które nas przerażają; godzinami ćwiczą swoje umiejętności. Niewielu dorosłych ma koordynację wzrokowo-ruchową potrzebną do tego, żeby zabić potwory i dostać się do skarbu. A nasze dzieci robią to z łatwością.

Dajcie im szansę zmiany stron na boisku. Uzbrojeni w wiedzę zawartą w tej książce, byście nie wyglądali na kompletnych ignorantów, usiądźcie w wygodnym fotelu i poproście dzieci, by zademonstrowały wam wasz domowy komputer.

Jeśli już korzystacie z sieci, poproście je, by pokazały wam swoje ulubione strony, kawiarenki i grupy dyskusyjne. Przyjrzyjcie się im. To nie tylko okazja lepszego poznania dziecka, ciekawa wędrówka po wirtualnym świecie, ale być może szansa odkrycia, jak pogodzić wasze zasady i potrzeby dzieci.

Nawet jeśli jesteście doświadczonymi użytkownikami Internetu, pozwólcie dziecku być „przewodnikiem" w tej wycieczce. Niech dla odmiany ono mówi i poucza. Zróbcie z tego rodzinne popołudnie czy wieczór. To doświadczenie pozwoli wam popatrzeć na komputer jak na coś, co was łączy, nie dzieli.

Zainteresujcie się najnowszą grą komputerową. (Wielu z nas, tak czy owak, marzy o tym, by w nią zagrać, więc skorzystajcie z okazji. A gdy okaże się, że już dwadzieścia godzin gracie w grę piłkarską, całą winą możecie obciążyć mnie i tę książkę).

Będziecie zachwyceni umiejętnościami waszych dzieci. Choć jest wiele gier sportowych będących czystą rozrywką, znacznie więcej jest gier strategicznych, w których gracz musi rozwiązywać kolejne problemy i odkrywać wskazówki, by przejść na kolejne poziomy.

Weźcie joystick, kiedy go wam oferują. To będzie gra, w której nie trzeba dawać dzieciom forów. Nie mamy szans w rywalizacji z pokoleniem znawców komputerów, które wychowujemy. Kiedy popatrzycie na twarze dzieci, gdy one was uczą, i zauważycie ich nadzwyczajną cierpliwość wobec waszego analfabetyzmu, zrozumiecie, dlaczego proponuję ten eksperyment.

I jeszcze jedno: jeśli używacie jakichś programów wspomagających rodzicielską kontrolę, a dzieci chciałyby odwiedzić strony zablokowane przez program, nie żałujcie czasu, zajrzyjcie tam z nimi. To pomaga budować wzajemne zaufanie.

Uświadom dzieciom niebezpieczeństwa cyberprzestrzeni

Tu kończy się zabawa. Nauczenie dzieci, by były ostrożne i uważne w cyberprzestrzeni, ma większe znaczenie niż jakiekolwiek oprogra-

mowanie, które można kupić. Ale jakoś tak się dzieje, że w momencie gdy tylko ktoś wypowie słowo „komputer" albo „Internet", wszyscy wpadają w panikę. Nie wiem czemu. Wszystkie wypróbowane dobre rady mają zastosowanie także w cyberprzestrzeni. Ucz swoje dzieci tego, czego rodzice uczyli ciebie... a czego ich rodzice...

Należy trzymać się podstawowych reguł i przekładać je na język cybernetyczny.

Pozwólcie, że pokażę, jakie to łatwe.

❖ Stara zawartość – w nowym i udoskonalonym opakowaniu

- Nie rozmawiaj z obcymi i niczego od nich nie przyjmuj. (Widzicie? Skąd my to znamy?).
- Muszę znać twoich przyjaciół.
- Wracaj prosto do domu.
- Nie mów nieładnie o innych ludziach.
- Nie bierz rzeczy, które nie należą do ciebie.
- Bądź miły i odnoś się do innych z szacunkiem.
- Nie przekazuj innym informacji o sobie.
- Nie przekazuj innym informacji o swojej rodzinie.

Mówiłam wam, że wszystko już wiecie, potrzebujecie tylko kogoś, kto przełoży to na żargon cybernetyczny. Oto tłumaczenie:

❑ **Nie rozmawiaj z obcymi i niczego od nich nie przyjmuj.** Kto jest obcy w sieci? Wszyscy! A mimo to stale rozmawiamy w kawiarenkach i grupach dyskusyjnych. To jedna z bardziej ekscytujących rzeczy, jakie możemy robić dzięki Internetowi. Więc jak ta rada ma działać? Ucz swoje dzieci, że każda osoba, której nie znają w realnym świecie, jest obca. Można z nią rozmawiać, ale nigdy nie należy mówić jej rzeczy, które można powiedzieć przyjacielowi. Pamiętaj – rozmawiaj z innymi, ale się im nie zwierzaj. Rozmawiaj o muzyce, filmach, sporcie – ale nie o sprawach osobistych. Pewna nastolatka ujęła to bardzo trafnie: „Pamiętajmy, że ludzie, z którymi gadamy w sieci, to nie są nasi przyjaciele, tylko ludzie, z którymi gadamy w sieci". Naszym dzieciom trudno jest to zapamiętać. Jak powiedziałam wcześniej, najgorsze jest to, że cyberprześladowcy działają w naszym domu. Dzieci czują się bezpieczne, bo siedzimy blisko, więc „radar" ostrzegający przed obcymi nie działa.

Sieć zapewnia specyficzne poczucie intymności, na które liczą cybernetyczni przestępcy. Próbują przekonać dziecko, że wcale nie są obcy. Mają nadzieję, że przekonają je, że zwykłe zasady ich nie dotyczą. A rodzice muszą przypominać dzieciom, że ci ludzie są obcymi i że zwykłe zasady zawsze obowiązują.

❑ **Muszę znać twoich przyjaciół.** Wszyscy słyszeliśmy to od swoich rodziców i mówiliśmy to samo własnym dzieciom. Nigdy nie pozwolilibyście dzieciom w realnym świecie przebywać z kolegami, których nie znacie. Dlaczego w wirtualnej przestrzeni miałoby być inaczej? Powinniście poznać ludzi, z którymi wasze dziecko często rozmawia. Nie ma powodu, by znać każdego, z kim dziecko się zetknęło w Internecie, ale trzeba wiedzieć, z kim utrzymuje regularne kontakty.

Jest kilka powodów, dla których trzeba poznać sieciowych przyjaciół; powodów, których nie ma w przypadku znajomości w realnym życiu. W realnym świecie dziecko widzi, kto jest dorosły. W cyberprzestrzeni nie. Większość napastników, którzy usiłują naprawdę spotkać się z naszym dzieckiem – i którzy mają w planach trochę inne rzeczy niż przyjaźń – udaje, że są dziećmi, by nie wzbudzić podejrzeń. (Więcej o tym, jak oni działają, możesz znaleźć w rozdziale 4). Czasem rodzice lepiej niż dziecko „wyczują" dorosłą osobę i mogą rozpoznać dorosłego udającego nastolatka, by wprowadzić dziecko w błąd.

❑ **Wracaj prosto do domu.** Kiedy byłam mała, znana byłam z wałęsania się po lekcjach. Albo przyjaciele zapraszali mnie do siebie, albo coś ciekawego się gdzieś działo. Moja mama wpadała w panikę i codziennie powtarzała mi to samo: „Wracaj prosto do domu".

Bezcelowe włóczenie się po Internecie niczym nie różni się od mojego wałęsania się po okolicy. Moja mama chciała wiedzieć, że jestem bezpieczna i że robię coś pożytecznego, np. odrabiam lekcje. Zezwalanie na to, by dzieci spędzały nieograniczopną ilość czasu w sieci, serfując bez celu, to szukanie kłopotów.

Miejcie pewność, że serfują w jakimś celu. Jeśli serfują „tak sobie", by poserfować, ustalcie limity czasowe. Mają wrócić do normalnego świata, do ludzkich relacji i rodzinnych zajęć w określonym czasie (i do odrabiania pracy domowej).

❑ **Nie mów nieładnie o innych ludziach.** Mówienie obraźliwych rzeczy o innych w cyberprzestrzeni określane jest słowem *flaming*.

Często wiąże się z pogwałceniem warunków korzystania z sieci, ustalonych przez dostawcę usług internetowych, na pewno spotka się też z reakcją innych ludzi. Pyskówki często przybierają charakter długich i rozległych batali, które szybko przenoszą się z kawiarenek czy grup dyskusyjnych do poczty elektronicznej. Jeśli dziecko uważa, że ktoś mu ubliża, powinno od razu powiadomić rodziców, operatora systemu lub moderatora grupy.

❑ **Nie bierz rzeczy, które nie należą do ciebie.** Dzieci serfują i odrabiają lekcje. Serfują i tworzą swoje własne strony WWW. Serfując, często „pożyczają" sobie rzeczy, które inni napisali, zdjęcia i grafiki należące do innych osób. Najczęściej łamią wówczas prawo. Kradną czyjąś własność. Wielu ludzi sądzi, że gdy się coś kopiuje, to wystarczy podać źródło. Nie mają racji. Istnieje coś, co określa się jako „uczciwe użytkowanie" (*fair use*). Wykorzystanie na swojej stronie czyjejś grafiki, całego poematu czy opowiadania nie jest „uczciwym użytkowaniem". Jest mało prawdopodobne, by ktokolwiek oskarżył dziecko o pogwałcenie w szkolnym wypracowaniu czyichś praw autorskich, ale coraz więcej ludzi oskarżanych jest przez przedstawicieli przemysłu rozrywkowego o wykorzystywanie ich własności intelektualnej na stronach WWW.

❑ **Bądź miły i odnoś się do innych z szacunkiem.** Wszędzie obowiązują jakieś zasady zachowania się. Świat wirtualny nie stanowi tu wyjątku. Wiele miejsc w sieci ma własne reguły poprawnego zachowania. Najpierw poznaj te zasady. Każda kawiarenka też ma swoje reguły. Nie wpadaj i nie zaczynaj rozmowy, zanim nie zorientujesz się, o czym się mówi. Przez chwilę poczytaj, zamiast pytać innych, o czym dyskutują. I szanuj ludzi oraz ich poglądy. Nie przesyłaj tej samej wiadomości w kółko. Czas innych ludzi jest cenny i nie muszą mieć ochoty na przedzieranie się przez te same wiadomości zamieszczone w różnych miejscach. Jeśli ktoś ci pomaga, podziękuj. Grzeczność w cyberprzestrzeni popłaca. Wszystko to składa się na szacunek dla innych.

❑ **Nie przekazuj innym informacji o sobie i swojej rodzinie.** Nigdy naprawdę nie wiesz, z kim rozmawiasz. W kawiarence mogą być obce osoby, obserwujące, czytające, których obecności nie jesteś świadomy. Nie zamieszczasz osobistego pamiętnika na kartce pocztowej. Przekazywanie jakichś informacji personalnych może być szczególnie groźne dla dzieci. Upewnijcie się, że dzieci wiedzą, co macie na myśli, mówiąc o danych osobistych, i że akceptują nieujawnianie ich tak w Internecie, jak i poza nim. Przećwiczcie pytania, z jakimi mogą zetknąć się na czatach. Uczymy nasze dzieci, by były grzeczne, by nie ignorowały innych ludzi, nie odpowiadały „to nie twoja sprawa". Mówimy im też, by nie rozmawiały z obcymi. To czasem rodzi w dziecku niepewność, która może wystawić je na niebezpieczeństwo. Gdy dzieci nie rozumieją zasad, mogą je odrzucić. Nie byłoby dobrze, gdyby tak się stało z zasadą nieprzekazywania informacji osobistych.

Przygotuj dziecko na przykre niespodzianki – i na ludzi, którym niekoniecznie jego dobro leży na sercu

Większość dzieci od najmłodszych lat wie, kiedy zadzwonić pod 997 i jakie informacje podać. Uczymy je, by szukały policjanta, gdy potrzebują pomocy. Uczymy je nazwiska, imienia i adresu, gdy tylko potrafią mówić, na wypadek gdyby się gdzieś zgubiły. Większość dzieci wie, co można powiedzieć przez telefon, a czego powiedzieć nie wolno, gdy zadzwoni ktoś obcy. Uczymy je, by nigdy nie mówiły, że nikogo dorosłego nie ma w domu. Nalegamy, by mówiły, że dorosły w tej chwili nie może podejść do telefonu. Ćwiczymy to z nimi tak długo, aż wiedzą, jak się zachować. Wiemy, że trening czyni mistrza, a chcemy, by nasze dzieci po mistrzowsku dbały o swoje bezpieczeństwo.

Ale czy równie dobrze uczymy je, jak mają radzić sobie z różnymi groźnymi sytuacjami w sieci? Chyba nie. Niektórzy z nas czują się niezręcznie, rozmawiając z dziećmi o pedofilii. Niełatwo jest mówić o dobrym i niedobrym dotykaniu, jednak zalecałabym, by wszyscy rodzice omówili to z dziećmi. Informowanie dzieci, że mogą być obiektem seksualnego pożądania pewnych chorych czy opętanych dorosłych, też nie będzie miłym tematem popołudniowej rozmowy. Na szczęście pewien 6-latek, którego spotkałam, mówiąc o sprawach bezpieczeństwa, podsunął sprytne rozwiązanie tego problemu. Kiedy spytałam o jakieś podpowiedzi, tyczące bezpieczeństwa, podniósł rękę i szybko poinformował mnie, że nigdy nie powinnam przekazywać swoich danych innym w sieci. Gdy zapytałam dlaczego, uśmiechnął się z wyższością i powiedział, że złodzieje stale polują na takie informacje, żeby przyjść do naszego domu i nas okraść. Jakkolwiek okrop-

nie brzmi słowo włamywacz, to pedofil brzmi o wiele gorzej. I łatwiej poradzić sobie z sytuacją, gdy celem przestępstwa jest dom i rzeczy materialne, niż z sytuacją, gdy celem przestępstwa jest samo dziecko. A poza tym to przemawia do dzieci!

Więc jak mamy je uczyć? Omawiamy możliwe scenariusze rozwoju sytuacji w Internecie. Ćwiczymy z nimi według schematu: „ty powiedziałeś/ on powiedział", „a co powiesz, jeśli on powie...?". Następnie trzeba przećwiczyć to z nimi w sieci. Wejdź do Internetu z pracy czy innego miejsca i odwiedź kawiarenkę, w której bywa twoje dziecko (uprzedź je, że to zrobisz – zaufanie jest tutaj bardzo ważne). Prowadź rozmowę, zadając różne pytania, gdy wydaje ci się, że traci czujność. Zobaczysz, jak sobie radzi. Powtarzaj to od czasu do czasu, ale zawsze uprzedź, że masz taki zamiar. Zrób z tego rodzaj rywalizacji. Zobacz, czy uda ci się je zaskoczyć, czy też jest zbyt mądre, by się dać zaskoczyć. Dzieci uwielbiają wygrywać w zabawie ze swymi rodzicami – więc zrób z tego grę. (Najlepiej się to sprawdza z dziećmi poniżej dwunastu lat).

Spotkania w realnym świecie z cyberznajomymi

Przede wszystkim musisz zrozumieć, że jedyny sposób, by pozostać naprawdę bezpiecznym, spotykając kogoś w realnym świecie, polega na tym, by nikogo nie spotykać. Kropka. Nigdy tego nie rób i nie pozwól na to dzieciom. Celowo umieściłam ten rozdział po rozdziale o cyberprześladowcach, mając nadzieję, że będziecie ciągle zbyt przerażeni, by pozwolić nastolatkom spotkać się z kimś w realnym świecie.

Nawet nastolatki zdają sobie sprawę z niebezpieczeństwa, które tu może czyhać. Niby to wiedzą, ale w którymś momencie romantyzm bierze górę nad rozsądkiem. Często uważają, że „mnie się to nie może zdarzyć" i niepotrzebnie ryzykują. Nie każde spotkanie kończy się nieszczęściem, ale wiele kończy się rozczarowaniem, a wystarczająco dużo kończy się nieszczęściem, by nasze nastolatki były ostrożne i nie podejmowały niepotrzebnego ryzyka.

Nastolatki, które pracowały ze mną, tworząc wskazówki służące zapewnieniu bezpieczeństwa młodszych dzieci, zalecały, by dziecko poniżej jedenastego roku życia nigdy nie spotykało się w prawdziwym życiu z osobami, które poznało w sieci, nawet w obecności rodziców. Były nieco mniej rygorystyczne, gdy chodziło o nastolatków, ale rozumiały powagę sytuacji.

Jednak nastolatki to nastolatki, a to oznacza, że ich główną życiową pasją będzie łamanie ustaleń i podejmowanie ryzyka. Oto kilka podstawowych zasad, które przydają się wtedy, gdy macie zamiar pozwolić swoim nastoletnim dzieciom na spotkania w prawdziwym życiu z osobami poznanymi w sieci, jak i wtedy, gdy wiecie, że one tak czy owak zignorują zakaz spotkań. (Jedna z moich Teenangels pełni w realnym świecie rolę „przyzwoitki" swojej koleżanki, która regularnie spotyka się z osobami, które poznała w Internecie. Najgorsze, co im się do tej pory zdarzyło, to spotkanie z mężczyzną udającym szkockiego żołnierza, którym wyraźnie nie był, ale za to miał liczne tatuaże i ogólnie wydawał się „trochę dziwaczny".) Pomyśl jednak o tym i niech twoje nastoletnie dziecko również poważnie się zastanowi. To są sytuacje, gdy naprawdę coś złego może się zdarzyć.

Pamiętacie moje motto? Informacje nie zabijają ludzi, to ludzie zabijają ludzi. Tylko w jedyny sposób ludzie mogą naprawdę skrzywdzić twoje dziecko – spotykając się z nim oko w oko. Wiem, że wielu nastolatków zignoruje mnie, i choć nie wycofuję się z twardej zasady: nigdy tego nie rób, przedstawię kilka wskazówek, które pozwalają ograniczyć ryzyko, choć go nie eliminują! (Te wskazówki przydadzą się także rodzicom, którzy sami rozważają umawianie się na randki ze znajomymi z cyberprzestrzeni).

Spotkanie z cyberznajomymi (zwłaszcza gdy w grę wchodzą jakieś romantyczne motywy, a jak mówimy o nastolatkach, to na ogół wchodzą) jest czymś nieco innym, niż normalne pierwsze spotkanie z nieznajomą osobą. Gdy widzisz wirtualnego znajomego pierwszy raz, masz wrażenie, że znasz go od dawna – zwykła ostrożność, obecna w nas w kontakcie z nieznajomą osobą, gdzieś ulatuje. Wiemy przecież, kto jest jego ulubionym autorem, jakiej muzyki słucha, jakim sportem się interesuje, co lubi jeść. Dzieci nie uświadamiają sobie, że to tylko im się wydaje, że wiedzą coś o tej osobie – a w rzeczywistości wiedzą to, co im powiedziano. Tak naprawdę nie znają tej osoby, znają tylko jej wypowiedzi. Uświadom więc nastolatkom, że znajomi z Internetu powinni być traktowani jak osoby obce i powinny ich dotyczyć wszystkie normalne w takich okolicznościach środki ostrożności.

Poza tym ludzie nie zawsze są prawdomówni w sieci, nawet jeśli nie mają zamiaru celowo wprowadzić innych w błąd. Tam możesz być,

kim chcesz – nieśmiały nastolatek może być lwem salonowym, grubas może twierdzić, że jest szczupły, sportowcy mogą podawać się za naukowców, a naukowcy za sportowców. Dorosłe kobiety często kłamią na temat swojego wieku i wagi, a mężczyźni mają zwyczaj kłamać na temat swoich dochodów, łysiny i sprawności fizycznej. Nastolatki udają, że są starsze niż są, czasem podają się za osobę przeciwnej płci. Można być pewnym jedynie tego, że każdy trochę kłamie. (A niektórzy nawet całkiem sporo!). Więc miej oczy otwarte i przygotuj nastolatka na szok i zadziwienie, gdy porówna rzeczywistość z fantazją.

Zdjęcia, które ktoś przysyła nastoletnim dzieciom, mogą być stare albo bardzo podretuszowane. Mogą pochodzić z czasów, gdy nadawca był nastolatkiem, ważył mniej i miał gładszą skórę, ale mogą być też zdjęciami całkiem innej osoby. Najlepsza rzecz w Internecie jest także najniebezpieczniejszą jego właściwością: tu może się wyraźnie ujawnić osobowość człowieka – to, czym jesteś w środku, ma szansę błyszczeć nieprzyćmione tym, czym jesteś na zewnątrz. Ale dodatkowe wskazówki, które w realnym życiu pomagają nam ustalić prawdę, takie jak język ciała, ubiór, higiena osobista, ton głosu – nie istnieją w cyberprzestrzeni.

Nie pozwól więc, proszę, nastoletniemu dziecku spieszyć się z bezpośrednim spotkaniem. Jak powiedziałam, sugerowałabym, by w ogóle tego nie robiły. Jeśli masz zamiar pozwolić im na zignorowanie moich zaleceń, upewnij się, że są w stanie myśleć i zachować ostrożność! Oto kilka rzeczy, które trzeba im przypomnieć:

1. Nie wierz we wszystko, co przeczytasz na ekranie.

W Internecie możesz być tym, kim masz ochotę być. Ja uparcie staram się przekonać ludzi, że jestem wysoką, atrakcyjną blondynką (jak na razie brak wierzących). Ten fajny szesnastoletni brunet może nie być brunetem, a co ważniejsze – może nie mieć szesnastu lat.

2. Nie śpiesz się, nie podejmuj pochopnych decyzji i skorzystaj z pomocy przyjaciół.

Daj sobie czas, by najpierw lepiej poznać tę osobę w sieci. Każdy może się ładnie zaprezentować w kilku pierwszych e-mailach. Ale podtrzymywać spójny obraz przez dłuższy czas jest trudniej. Trzymaj stare e-maile, by porównać zawarte w nich informacje. Być może w jednym pisał, że pracuje na poczcie, a w innym, że jest studentem. Może studiuje wieczorowo, ale może po prostu kłamie. Trzeba być

wyczulonym na wszelkie niespójności. Zaufaj swojej intuicji: jeśli zaczynasz się czuć jakoś nieswojo z informacjami, które otrzymujesz, to na ogół masz rację.

Nie daj popędzać siebie i nie poganiaj innych. Pozwól, by relacja rozwijała się w sieci tak długo, jak długo jest ci to potrzebne. Nie śpiesz się.

Poproś przyjaciół, by spojrzeli na te e-maile. Czasem oni, nie mając twoich różowych okularów, mogą inaczej zinterpretować coś, co ty interpretujesz optymistycznie. Gdy jesteśmy samotni, jeśli wcześniej nas zraniono, chcemy wierzyć, że teraz znaleźliśmy kogoś, kto ma wszystkie cechy idealnego partnera (które mogą być odwrotnością cech ostatniego partnera). Kiedy widzimy te cechy w jakiejś osobie, popadamy w taki zachwyt, że nie dostrzegamy, że ma również i inne cechy. Satysfakcjonujące odpowiedzi na pytania: „ile masz wzrostu, gdzie mieszkasz, jakiej muzyki słuchasz, jak się ubierasz, jakim sportem się interesujesz, czy lubisz MTV i filmy o miłości" to za mało, by poznać człowieka. Trzeba poznać system wartości, doświadczenia, bagaż emocjonalny (tak, i nastolatki dźwigają emocjonalny bagaż), a to wymaga czasu. Więc powoli.

3. Uczciwość to najlepsza zasada.

Być może nie jesteś tak wysoka, szczupła czy sprawna, jak byś chciała być. Może nie należałaś do klasowej czołówki. Może obawiasz się, że gdy powiesz prawdę o sobie, nikt nie będzie cię chciał.

Ale jeśli zaczynasz od kłamstwa, w końcu na czymś się wsypiesz. Jeśli chcesz ukryć kilka kilogramów czy posłużyć się podretuszowanym zdjęciem, trudno. Ale nie ukrywaj prawdy, gdy zaczynasz myśleć, że to może być coś więcej niż znajomość, która skończy się na kilku e-mailach. Nie kręć i nie klucz – to najlepsza droga, by zakończyć potencjalną przyjaźń czy rodzący się romans.

4. Zacznij od rozmowy telefonicznej.

Należałoby przejść od e-mailów i rozmów w sieci do rozmów telefonicznych, zanim zdecydujemy się na spotkanie twarzą w twarz. Najbezpieczniej byłoby rozmawiać z telefonu publicznego. Ustal czas rozmowy i podaj tej osobie numer automatu. Gdy poczujecie się pewniej, możecie wymienić prawdziwe numery telefonów.

Radziłabym, byś raczej wzięła numer telefonu tej drugiej osoby i zadzwoniła do niej, ale używając takiej opcji, by zablokować dostęp

do numeru twojego telefonu. Gdy mamy czyjś numer, w sieci można zebrać wiele informacji o tym człowieku.

Ale jeśli ta druga osoba też przeczytała moją książkę i wie, że nie należy podawać numeru swojego telefonu? Ktoś musi być pierwszy. Więc jeśli musisz, podaj swój telefon, ale tylko wtedy, gdy znasz tożsamość drugiej osoby. Jeśli sprawy rozwiną się niepomyślnie, możesz zablokować rozmowy.

5. Kiedy macie się spotkać, bądź z grupą przyjaciół albo najlepiej z rodzicami i tylko w miejscach publicznych.

Kiedy macie się spotkać pierwszy raz, weź ze sobą paru przyjaciół. (Wolałabym, żebyś poszła z rodzicami, ale staram się być realistką). Spotkajcie się w barze czy w centrum handlowym, niezbyt blisko domu. Uprzedź, że spotkanie będzie krótkie – kawa lub woda mineralna. Jeśli internetowi znajomi upierają się, że ma to być spotkanie bez osób trzecich – nie chodź.

Następnie przypomnij sobie to, co ta osoba mówiła o sobie w sieci. Czy to odpowiada rzeczywistości? Jeśli rzeczywistość jest inna – daj sobie spokój. Myśl. Nieważne, że czujesz się samotna – najważniejsze jest bezpieczeństwo.

6. Powiedz komuś, zostaw wiadomość.

Musisz upewnić się, że ktoś jeszcze wie, z kim masz zamiar się spotkać i gdzie, kiedy masz zamiar wrócić (ktoś inny niż osoba, z którą masz zamiar się spotkać). Zachowuj wszystkie e-maile i powiedz przyjaciołom, gdzie je znaleźć. Jeśli zdarzy się coś złego, te listy będą źródłem informacji pomocnych w zidentyfikowaniu osoby, z którą się spotykasz. Pewna matka przekazała mi swój sposób: kiedy jej dorosły syn ma się w realnym świecie spotkać z dorosłą kobietą (w każdym razie on ma nadzieję, że z kobietą), którą poznał w Internecie, zostawia w kopercie wszystkie dane i wręcza kopertę matce, na wypadek gdyby coś złego się zdarzyło. Tym sposobem, jeśli wszystko dzieje się normalnie, jego prywatne sprawy pozostają prywatne. A jeśli nie – ona szybko będzie miała dostęp do informacji, których potrzebuje, by zgłosić sprawę policji.

7. Nigdy nie wychodźcie razem ani nie zapraszaj go do domu.

Nawet jeśli spotkanie trwa dłużej, niż było to planowane, nie opuszczaj miejsc publicznych. Publiczne to tutaj kluczowe słowo. Pa-

miętacie, jak matka ostrzegała, by nigdy nie wsiadać z niezn
mi do samochodu? Nie wsiadaj do samochodu, nie wchodź do dom
czy do innego odosobnionego miejsca. Jeśli następuje zmiana planów, skontaktuj się z osobami, które wiedzą o spotkaniu, i powiedz im o zmianie. Jeśli to randka, nie działaj pochopnie, nawet jeśli nie masz zwyczaju zachowywać się ostrożnie na randkach – ta sytuacja jest inna. Nie wychodźcie razem z lokalu, upewnij się, że nikt za tobą nie idzie, nie śledzi cię w drodze do domu. Nie wracaj prosto do domu, odwiedź kogoś po drodze.

8. Zgłaszaj policji każdy atak czy groźbę ataku.

Jeśli zdarzy się coś złego, niezależnie od tego. czy stosujesz się do moich zasad, czy nie, nie wstydź się pójść na policję. Podaj wszystkie fakty. Jeśli tego nie zrobisz, istnieje prawdopodobieństwo, że ta osoba nadal będzie tak postępować. Masz prawo powiedzieć „nie" i oczekiwać, że to będzie respektowane. Jeśli dzieje się coś złego, pamiętaj, to nie jest twoja wina!

9. Nie wstydź się upierać przy swoich zasadach.

Twoje bezpieczeństwo jest najważniejszą sprawą. Każdy, komu na tobie zależy, będzie cię szanował za zachowanie ostrożności. To jak rozważne prowadzenie pojazdu. Nawet jeśli jesteś najlepszym kierowcą świata, są na świecie inni kierowcy, których trzeba brać pod uwagę. To po prostu zdrowy rozsądek!

10. Nie zachowuj się prowokująco w Internecie – to może wywołać różne zaskakujące reakcje.

Staraj się nie robić w sieci prowokacyjnych komentarzy. Cyberflirty szybko się rozwijają i później trudno jest wrócić na poziom mniej romantyczny. Jeśli czyjeś zachowanie krępuje cię – powiedz o tym. Zrób kopię e-mailu i trzymaj kopie wszystkiego, co uważasz za obraźliwe, by można to było sprawdzić.

11. Jeśli osoby, z którymi postanawiasz nie mieć więcej kontaktów, nękają cię czy napastują, zwróć się o pomoc.

Nie próbuj samodzielnie radzić sobie z cybernapastnikiem. Nie odpowiadaj, gdy prześladowca kontaktuje się z tobą. Po prostu ignoruj go, w większości przypadków daje to dobre skutki. Nigdy nie dawaj swojego zdjęcia komuś w sieci, jeśli nie chcesz dać go 200 milionom

ludzi. Często cyberflirty kończą się tym, że jedna strona prześladuje drugą i publikuje w Internecie osobiste informacje i fotografie z seksualnymi sugestiami, typu „Jennifer ma ochotę na gorącą noc".

Nie dawaj im żadnej amunicji. Stare „Chcesz miło spędzić czas, zadzwoń do Ani", umieszczone na ścianie w toalecie, może dać straszne efekty, a co dopiero gdy zostanie to umieszczone na internetowej cyberścianie grup dyskusyjnych zainteresowanych seksem. Może się to stać bardzo, bardzo niebezpieczne.

Tropy, które zostawiamy – Shannon, obecnie znana jako Tiffany

Większość dzieci wie, że nie należy przekazywać informacji osobistych w Internecie – ale niektóre informacje „wydostają" się jakoś niechcący w czasie rozmowy; informacje, które same w sobie nie są groźne, zebrane razem pozwalają zidentyfikować i odszukać dziecko.

Wiadomo, że dzieci nie zastanawiają się zbyt długo, udzielając różnych informacji. Najlepszy przykład zawarty jest w pewnym opowiadaniu, które znalazłam w Internecie. Natknęłam się na nie kilka lat temu na stronie, która wzięła je z innego źródła. Opowiadanie to najwyraźniej krążyło w sieci przez trzy lub cztery ostatnie lata, wysyłane e-mailem przez jednego nastolatka innemu i publikowane na wielu personalnych stronach WWW.

Ponieważ nie zdołałam odkryć, do kogo powinnam zwrócić się o pozwolenie na ponowne opublikowanie go, musiałam napisać własną wersję. Oto ona:

> Tiffany Peterson złapała swój leżący na ławce plecak, wrzuciła do niego rękawiczki, odwróciła się i pomachała koleżankom z drużyny. Pobiegła, mając nadzieję, że złapie Timbo5, zanim ten wyloguje się, by iść na obiad. Przekręciła klucz w zamku i weszła, zatrzaskując za sobą drzwi. „Mama! Jestem już w domu!" – wykrzyknęła, wbiegając na schody. Miała tylko pięć minut, zanim on, jak wiedziała, wyjdzie z sieci. Jeszcze chwila i zarejestrowała się jako „Shortstopteen" – znalazła go! Był tam – w ich ulubionej kawiarence Sport dla Nastolatków.

***

Shortstopteen: Cześć, Timbo. Wiesz co? Wygraliśmy!
Timbo5: Cześć Shortstop. Jaki był wynik?
Shortstopteen: 9 do 7! Złapałam ostatnią piłkę! To nam umożliwi dodatkowe rozgrywki.
Timbo5: Ciągle grasz na drugiej bazie?
Shortstopteen: Nie. Przekonałam trenera, by pozwolił mi grać na środkowym polu.;-) (Zrozumiecie ten kod po przeczytaniu rozdziału o netykiecie).
Timbo5: Co się stało z poprzednią osobą ze środkowego pola?
Shortstopteen: Przeniosła się do Teksasu. A trener powiedział, że wszystkie jego najlepsze środkowe obrończynie były blondynkami. Więc wybrał mnie!;-)
Timbo5: Świetnie! Gratuluję. Muszę iść. Mama woła mnie na obiad. Do zobaczenia jutro.
Shortstopteen: Dobrze, do zobaczenia jutro.

Tiffany pogawędziła chwilę z innymi znajomymi i wylogowała się. Timbo5 był jej ulubionym wirtualnym kolegą. Miał 14 lat, tak jak Tiffany, i mieszkał w Wirginii. Też grał w baseball. Ale on grał na pierwszej bazie. Chciałby grać w największych zespołach ligowych, gdy dorośnie. Tiffany miała nadzieję, że do czasu, gdy ona będzie dorosła, kobiety także będą mogły grać w głównej lidze.

Chociaż nie znała nawet jego prawdziwego imienia, a on nie znał jej imienia, wiedziała o nim dużo. Był znacznie zabawniejszy niż większość innych dzieci z kawiarenki. O baseballu wiedział wszystko. Wolałaby, żeby mieszkał gdzieś bliżej New Jersey, mogliby chodzić razem na mecze.

A Timbo5 naprawdę troszczył się o nią, zawsze ostrzegał ją, by nie podawała nikomu swojego prawdziwego nazwiska czy adresu. To miło, że się tak troszczył, ale Tiffany już wiedziała o tym, że nie należy podawać żadnych danych osobistych. Rodzice i nauczyciele omówili to z nią wyczerpująco. Była bardzo ostrożna i nie dawała żadnych wskazówek, które pomogłyby komuś znaleźć ją w realnym życiu.

Mama ją zawołała, więc zbiegła na dół na obiad, by podzielić się z rodziną dobrymi wiadomościami dotyczącymi dodatkowych rozgrywek i jej sukcesu.

W następnym tygodniu Tiffany codziennie miała treningi. Coś jednak było nie w porządku. Wydawało jej się, że ktoś ją śledzi. Oglądała się za siebie, idąc do domu o zmroku. Stwierdziła, że przyspiesza kroku. Otworzyła drzwi szybko i rozejrzała się jeszcze raz. Mimo że nikogo nie zobaczyła, była niespokojna. Nie zawołała nawet „Cześć" do mamy, tylko pobiegła na górę do swojego komputera.

Shortstopteen: Cześć, Timbo...
Timbo5: Cześć Shortstopteen, co słychać?
Shortstopteen: Jestem zdenerwowana. Pewnie trema przed meczem. Myślałam, że ktoś mnie śledzi w drodze do domu.
Timbo5: Czy widziałaś kogoś idącego za tobą?
Shortstopteen: Nie. Ale czułam się dziwnie. Jakbym wyczuwała czyjąś obecność... ale gdy się oglądałam, to nikogo tam nie było.
Timbo5: Czy rodzice są w domu?
Shortstopteen: Tak. Już w porządku. Pewnie przedmeczowe strachy.
Timbo5: Nie podałaś nikomu w sieci swojego adresu ani prawdziwego nazwiska?
Shortstopteen: Wiesz, że jestem bardzo ostrożna. Pouczasz mnie cały czas! Zaczynasz mówić jak moi rodzice!;->
Timbo5: No nie, przestań!

Tiffany zapomniała o swoim lęku i gawędziła sobie aż do obiadu.

Następnego dnia był mecz. Tiffany grała bardzo dobrze, jej zespół wygrał, przechodząc do finału. Kiedy wróciła do domu, zalogowała się i opowiedziała Timbo5 o swoim wielkim zwycięstwie i poskarżyła się, że jutro znowu ma trening.

Kiedy następnego dnia podczas treningu rozgrzewała się, kozłując piłkę dookoła boiska, spojrzała na trybuny i zobaczyła mężczyznę, który patrzył wprost na nią. Poczuła ten sam lęk i niepokój, jaki czuła kilka dni temu, wracając do

domu. Spoglądała na niego od czasu do czasu, ale w końcu zapomniała o nim i zajęła się grą. Po treningu przypomniała sobie o obcym mężczyźnie, ale na trybunach już nikogo nie było. Wzięła głęboki oddech i ruszyła do domu.

Tym razem była pewna, że ktoś za nią idzie. Rozglądała się wokół i choć nikogo nie widziała, była porządnie przestraszona. Wybrała dłuższą, ale lepiej oświetloną i bardziej ruchliwą drogę. Gdy w którymś momencie spojrzała w okno wystawowe, zobaczyła odbicie kogoś, kto mógł być mężczyzną z trybuny, ale kiedy się odwróciła – nikogo nie zobaczyła. Była jednak pewna, że go rozpoznała. Potem słyszała nawet kroki.

Kiedy zbliżała się do domu, zaczęła biec. Miała wrażenie, że słyszy, jak tamte kroki też nabierają prędkości. Wpadła do domu, zatrzaskując za sobą drzwi. Mama, zaalarmowana hałasem, weszła do pokoju, pytając: „Czy wszystko w porządku, Tiffany? Wyglądasz na zdenerwowaną". Tiffany wstrzymała oddech i powiedziała, że po prostu spieszyła się do domu.

Tym razem powoli wchodziła na schody. Musi porozmawiać z Timbo5. Była naprawdę przestraszona. Ale kiedy się zalogowała, okazało się, że Timbo5 nie ma w kawiarence. Wysłała mu ICQ i stwierdziła, że nie ma go w sieci. Akurat wtedy, gdy ona najbardziej go potrzebuje!

Zadzwonił dzwonek u drzwi. Słyszała, że mama otworzyła, potem usłyszała męski głos. Kilka minut później rodzice poprosili ją do pokoju. Ciągle zastanawiała się, jak ma powiedzieć im o swoich lękach, nie wywołując w nich paniki. Tak bardzo martwiła się, że zabiorą jej komputer, jeśli pomyślą, że podała komuś dane personalne.

Rodzice siedzieli w pokoju z jakimś mężczyzną – tym, którego widziała podczas treningu. Zaniepokoiła się. „Tiffany, siadaj, proszę. To jest sierżant Thompson z policji stanowej" – Tiffany popatrzyła na zatroskane twarze rodziców.

„Cześć, Shortstopteen", powiedział sierżant. Tiffany nie mogła pojąć, w jaki sposób poznał jej imię z kawiarenki. „Jestem Timbo5", dodał. Nie wierzyła własnym uszom. Timbo5? Ten policjant? Timbo5 ma przecież 14 lat i mieszka w Wirginii!

„Pozwól mi to wyjaśnić", powiedział i zaczął jej opowiadać, że pracował w „przebraniu" w kawiarenkach, próbując chronić dzieci przed napastnikami działającymi w sieci. „Ale jak mnie pan odnalazł? Ja nigdy nie podawałam swojego prawdziwego nazwiska ani innych informacji". „Wprawdzie nigdy nie dałaś mi swojego nazwiska tak dosłownie, ale dałaś mi wiele innych informacji o sobie. Podałaś mi nazwę zespołu, w którym grasz. Reszta była już naprawdę łatwa – sprawdzić, który stan ma mistrzowską drużynę w baseballu, noszącą nazwę Tygrysy z Randolph Township. Potem zadzwoniłem do szkoły Randolph Township i zapytałem, która drużyna gra w tym tygodniu w dodatkowych rozgrywkach. W lokalnej gazecie sprawdziłem nazwisko środkowego obrońcy w tej drużynie. Potem w elektronicznej książce telefonicznej sprawdziłem wszystkich Petersonów i znalazłem twój adres i telefon. Zadzwoniłem do twoich rodziców i powiedziałem im, co się stało".

Tiffany była oszołomiona. Jak ten czterdziestoletni mężczyzna siedzący przed nią może być jej przyjacielem Timbo5? Poza tym ten policjant mówi, że też jest z New Jersey. Jak to możliwe, skoro Timbo5 mówił, że jest z Wirginii?

Wiedziała, kim jest Timbo5, bo on jej mówił różne rzeczy o sobie. A ona nie uwierzyła tak od razu jego słowom, wszystko sprawdziła. Miał swój profil w sieci, który sprawdziła. Tam też była informacja, że kocha baseball, ma 14 lat i mieszka w Wirginii. Miała więc dowód na piśmie!

Zaczęła jednak słuchać uważniej, gdy sierżant Thompson wyjaśnił, że stworzył ten profil tylko po to, by przekonać ją do swojej fałszywej tożsamości. Potem wyjaśnił, że szedł za nią do domu, gdy ją już zidentyfikował na boisku jako jasnowłosą środkową obrończynię.

„Zrobiłem to, żeby ci pomóc – powiedział. – Mój przyjaciel miał czternastoletnią córkę. Przekazała zbyt wiele informacji nieznajomemu, który pewnego dnia pojawił się w jej domu i zabił ją. Od tej pory robię wszystko, by nauczyć dzieci, jak mają sprawdzić, że nie przekazują nieświadomie istotnych informacji o sobie".

Tiffany teraz wreszcie zrozumiała, że wpadła w tę samą pułapkę co córka przyjaciela sierżanta Thompsona. Pomyślała o tych wszystkich drobnych szczegółach, które podała, a które pomogły komuś ją znaleźć. Sierżant Thompson popatrzył na nią. „Czy pomożesz mi i przekażesz innym dzieciom to, czego się właśnie dowiedziałaś?". Tiffany przyrzekła, że pomoże. I Tiffany, i jej rodzice byli przejęci głęboką wdzięcznością, że zdołali uniknąć tragedii i zdobyć mądrość w taki „łatwy" sposób.

Używanie pseudonimów: uczymy dzieci chronić siebie czy kłamać?

Aby uniknąć ujawniania przez dzieci danych osobowych, radziłam rodzicom, by uczyli je posługiwania się w sieci jakimś pseudonimem czy imieniem innym niż prawdziwe. Żadne dziecko na świecie (i dorosły też) nie uważa, że rodzice dali mu odpowiednie imię. Alicje wolałyby być Renatami, a Renaty chciałyby być Wandami. To sytuacja z góry przegrana dla rodziców. Pozwalając dzieciom wybrać sobie „specjalne" imię internetowe, dajemy im szanse naprawienia „błędu" rodziców: pozwalamy im nazwać siebie tak, jak my powinniśmy byli je nazwać.

Wiele dzieci kreuje całą fałszywą osobowość, wymyślając szkołę, adres domowy, drużynę sportową. Te informacje podają także w profilu. Dzięki temu, gdy ktoś pyta o jakieś dane, nie zastanawiają się, czy powiedzieć, że „nie mogą tego mówić" (i tym samym przyznać, że nie kontrolują w pełni swojego życia), czy też że nie udzielają podobnych informacji, i zaryzykować, że wydadzą się komuś niegrzeczni. Po prostu podają swoje przybrane imię. Dlatego zawsze mogą odróżnić przyjaciół z realnego świata od przyjaciół internetowych, bo ci ostatni nie znają ich prawdziwego imienia.

Moi współpracownicy z grupy Teenangels nie godzą się w tej kwestii ze mną. Twierdzą, że jest to uczenie dzieci kłamstwa i może prowadzić do pomyłek. A że z powodu zmieszania dzieci mogą ujawnić różne dane, w ostatecznym rachunku może to być raczej szkodliwe. Sami się zastanówcie, co będzie dobre dla waszych dzieci, i tego się trzymajcie. Podoba mi się idea zmyślonego imienia, ale tworzenie całej osoby i życiorysu może jest przesadą.

Dzieci to tylko dzieci: jak uczyć je odpowiedzialności

Naturalnym dalszym ciągiem dyskusji o pseudonimach będzie przypomnienie dzieciom o odpowiedzialności za to, co robią. Czy fakt, że ludzie w sieci mogą być, kim chcą, zmienia ich poczucie odpowiedzialności?

Gdybyś mógł robić wszystko, co chcesz, i nie obawiać się, że zostaniesz przyłapany, czy złamałbyś prawo? Nawymyślał teściowej? Oszukiwał na podatkach? Zjadł podwójny deser? To z tym problemem stykają się nasze dzieci, wchodząc do Internetu. Wydaje im się, że są anonimowe i nie mogą zostać złapane.

❖ Co dzieci mówią o udawaniu kogoś innego

Przytaczam odpowiedzi nastolatek na pytanie, czy zdarzyło się, że udawały w sieci kogoś innego. Oto ich słowa:

„Udawałam różne ważne osoby i ludzie się na to nabierali, ale w końcu przyznawałam się, że nie jestem prawdziwym ważniakiem, bo dziewczyny stawały się zbyt ufne i zaczynały przekazywać różne osobiste informacje. Powinny być zadowolone, że ja sobie tylko żartowałam, że nie jestem psychopatą o morderczych instynktach. O rany, niektóre dziewczyny potrafią być strasznie głupie, kiedy mówią tyle o sobie".

„Tak, rozmawiałam z wieloma ludźmi z różnych stron świata i ja, tak jak wiele innych osób, stworzyłam kilka miłych historyjek na «swój» temat. Chodziło np. o takie rzeczy, że mieszkam na Hawajach, jestem modelką, jestem wysoka, szczupła i mam piękne, długie włosy. Tak bym chciała, żeby to była prawda! Łatwo udawać przez pewien czas kogoś innego. Przyznaję to! Czasem jest to też zabawne. Trzeba tylko uważać, żeby nie wdepnąć w kłopoty. Wszystko sprowadza się do korzystania z komputera, który Pan Bóg umieścił w naszych głowach".

„Na ogół zmieniałam osobowość, wchodząc do Internetu. Nie wiedziałam, kim wewnątrz jestem, i to wywoływało we mnie niepokój. Zazwyczaj udawałam, że jestem doskonała i że mam wszędzie przyjaciół. To sprawiało, że czułam się lepiej. Internet to dla

mnie cudowne miejsce do życia i chętnie wyłączam się z normalnego świata".

„Tak, zawsze udawałam, że mam osiemnaście lat, 170 cm wzrostu i ważę 55 kilogramów, bo to cudownie być szczupłą".

„Tak, udawałam, że jestem starsza i ładniejsza".

„Wymyśliłam sobie całkiem nowe życie – gdzie mieszkam, ile mam lat, jak wyglądam, jaki mam charakter".

„Tak, udawałam strasznie puszczalską. Nie mam chłopca, więc opowiadałam co innego i ciągle flirtowałam, i mówiłam o seksie".

„Nie, zawsze jestem sobą. Sądzę, że jeśli ludzie nie lubią mnie takiej, jaka jestem, to nie warto z nimi rozmawiać!".

„Oczywiście, że udawałam. Każdy udaje. Udaje się, że ma się więcej lat, albo udaje się chłopca albo kogokolwiek".

„Tak, udawałam, że jestem kimś, kim nie byłam, bo chciałam, żeby ludzie inaczej na mnie reagowali. To pozwalało mi zobaczyć siebie taką, jaką chciałam być, ale robiąc to, zobaczyłam, że wcale nie chcę taka być i że chcę być sobą".

„Nie udawałam. Lubię być sobą – taką, jaka naprawdę jestem. W domu i w szkole nikt mnie naprawdę nie zna, bo muszę udawać kogoś innego. Swobodniej się czuję, rozmawiając z ludźmi w Internecie. Oni znają mnie prawdziwą i nie oceniają mnie po wyglądzie".

„Nie, nie lubię ukrywać swojej osobowości. Myślę, że to ważne, byśmy byli sobą".

„Tak, jeśli jestem w kawiarence, zawsze zmyślam. Dlatego uważam, że nikomu nie można wierzyć, bo wszyscy robią to samo".

„Ponieważ wygląda na to, że nikt nie ma ochoty rozmawiać z piętnastolatką, zawsze udaję, że mam 18 lat. Ale to czasem wywołuje głupie uwagi chłopców".

❖ Nikt mnie nie znajdzie w sieci...

Po części problem polega na tym, że dzieci nie rozumieją, że w sieci nie są anonimowe. Nawet posługując się pseudonimami, zostawiają ścieżkę elektronicznych śladów wszędzie, gdzie serfują.

Mówiłam już o groźbach podłożenia bomby czy zabójstwa wysyłanych przez dzieci. Czy to naprawdę aż tak się różni od tego, co my robiliśmy, będąc w ich wieku? Kiedy ja byłam młoda, robiliśmy inne rzeczy, przez które wpada się w tarapaty, toteż stale mieliśmy kłopoty.

Moi koledzy i ja dzwoniliśmy do pobliskiej pizzerii i zamawialiśmy pizzę z podwójną porcją anchois (to była najokropniejsza rzecz, jaką zdołaliśmy wymyślić) dla zwariowanej starszej pani z naszej ulicy, która stale krzyczała na nas, że wchodzimy na jej trawnik i robimy za dużo hałasu. Potem siedzieliśmy w ciemnościach, patrząc przez szparę w firance, jak podjeżdża pojazd dostawczy i stara kobieta kłóci się z chłopcem, który przywiózł pizzę. Mogliśmy śmiać się histerycznie i czuć się bezpiecznie, a zarazem mieć słodką świadomość, że zemsta się udała. (Teraz mogę się do tego przyznać, bo jako prawnik wiem, że upłynęło już tyle czasu, że moje młodzieńcze przestępstwo uległo przedawnieniu – choć dostałam solidną burę od mamy, gdy kilka lat temu dowiedziała się o całej sprawie. Na szczęście moje dzieci nie mogą robić takich kawałów, bo teraz nie przyjmuje się już anonimowych zamówień).

Wielu z nas, pamiętając podobne psikusy, które robiliśmy jako dzieci, może wszystko zbyć wzruszeniem ramion, mówiąc „dzieci to dzieci". Ale trzeba zdać sobie sprawę z tego, że groźby zabójstwa zamieszczane przez nastolatka w Internecie brzmią dokładnie tak samo, jak wysyłane przez szalonego dorosłego opętanego zamiarem zamordowania kogoś. To są pogróżki, którym się wierzy, i my, rodzice i nauczyciele, rozumiemy, jak są poważne.

To dobry moment, żeby porozmawiać o odpowiedzialności. Nasze dzieci muszą wziąć odpowiedzialność za swoje działania. A w związku z ostatnimi tragediami i masowymi zabójstwami w szkołach obowiązuje zasada zerowej tolerancji wobec wysyłania gróźb za pośrednictwem Internetu.

Odróżnianie głupich żartów od poważnych gróźb

Po tragedii w Littleton problem odróżniania poważnych gróźb od głupich żartów nabrał całkiem innego znaczenia. Pojawiły się setki stron WWW bliźniaczo podobnych do tej z Littleton. Słowa związane z tragicznym zdarzeniem, takie jak „mafia w trenczach" i inne, niezwykle często zaczęły pojawiać się w wyszukiwarkach i profilach. Uczniowie z Karoliny Północnej zamieścili szczegółową mapę szkoły, zaznaczając miejsca, w których umieszczą bomby. Inni wygłaszali ostrzeżenia o bombach w grupach dyskusyjnych. Piątoklasista z New Jersey wysłał do wszystkich kolegów z klasy e-mail z pogróżkami. Szkoły od lat otrzymują informacje o bombach. (Niestety, od lat też uczniowie popełniają w szkołach morderstwa. Ale problem dzieci dokonujących masowych zabójstw dzieci jest nowy). Oznacza to, że dzieci nie korzystają już dłużej z luksusu „bycia tylko dziećmi" i nie mogą wysyłać głupich i pustych gróźb, nie narażając się na konsekwencje.

Jak uczymy nasze dzieci odpowiedzialności?

Kiedy mój syn był mały i miał kłopoty w szkole, mógł liczyć, że przyjdę do szkoły, gotowa go bronić. Ale kiedy ja byłam mała, moja matka przyszłaby w takiej samej sytuacji do tej samej szkoły gotowa mnie zabić. Myślę, że zwracając coraz więcej uwagi na odczucia naszych dzieci, zapomnieliśmy, że muszą one także uczyć się odpowiedzialności za swoje czyny i ponosić ich konsekwencje. Powinniśmy być wobec nich bardziej konsekwentni i stanowić lepszy wzór do naśladowania. Kiedy dzieci najbardziej nas potrzebowały, my, dorośli, do których tradycyjnie mogły się zwrócić o wsparcie, zawiedliśmy je. Brakowało nam czasu i nie potrafiliśmy nauczyć ich odpowiedzialności za własne czyny. A inni dorośli, których dzieci mogą potraktować jako wzorce, nie stanowią wzorca takiego rodzaju, jakiego dzisiaj dzieci potrzebują.

Tradycyjna rodzina jest obecnie wyjątkiem, nie regułą. Po rozwodzie rodzice bardzo często zapominają, że rozwiedli się ze swoim partnerem, ale nie z dziećmi. Sądy zawalone są sprawami rodziców, którzy odmawiają wypełniania swoich obowiązków i zajmowania się dziećmi. Rodziny zaniedbują swoich starzejących się krewnych, którzy żyją w samotności i zapomnieniu.

A gwiazdy sportu, kina, telewizji, muzycy rockowi, wybierani przywódcy polityczni są niezwykle dalecy od ideału, znacznie częściej są znani ze swoich potknięć. Narkotyki, alkohol, przemoc, lekceważenie prawdy i moralności to terminy, którymi można opisać bardzo wiele osobistości dzisiejszego świata.

Co zatem mamy zrobić, kiedy nasze dzieci poszukują wzorca i nie znajdują go? Dobre wzory niełatwo dziś znaleźć. Czy mówimy to naszym dzieciom? Mam nadzieję, że nie.

Sami musimy spróbować stać się dla nich wzorcem, przykładem i musimy pomóc im znaleźć innych godnych naśladowania. Musimy dostrzegać bohaterów wśród zwykłych ludzi, takich, którzy robią coś dla swojej społeczności; którzy rozumieją odpowiedzialność związaną z własnym zawodem, stanowiskiem, pozycją społeczną; którzy żyją według najlepszych zasad; którzy pokażą naszym dzieciom, jak można odnieść sukces, nie przestając być „porządnym człowiekiem".

Miejmy nadzieję, że nauczymy je, że mogą i powinny oczekiwać więcej od nas i od innych, a my możemy i powinniśmy oczekiwać więcej od nich.

❖ Nie dajmy się wciągnąć do polowań na czarownice

Musimy znaleźć jakiś złoty środek i próbując nauczyć dzieci odpowiedzialności za własne działania, pozwolić im zarazem być dziećmi. Ale co robić z groźbami wysyłanymi przez dzieci? Biorąc pod uwagę fakt, że niektóre dzieci dopuszczają się gwałtownych czynów po stworzeniu strony WWW, na której grożą takimi czynami, nikt nie odważy się ignorować podobnych obwieszczeń. Granica między czujnością a polowaniem na czarownice jest wyraźna. Musimy uważać, by jej nie przekroczyć.

Po tragedii w Littleton i podobnych wydawało się, że wszyscy podzielili się na dwa obozy: jedni domagali się zamykania stron zawierających instrukcje budowania bomb i cenzurowania tworzonych przez dzieci stron rozpowszechniających nienawiść lub przemoc, inni domagali się tolerancji i ignorowania treści dotyczących przemocy czy gróźb wysyłanych przez dzieci. Ale żadna skrajność się nie sprawdza.

Musimy zrobić dwie rzeczy: uświadomić naszym dzieciom, że odpowiadają za swoje działania, i jednocześnie słuchać uważniej i stworzyć takie miejsca, gdzie dzieci bez lęku przed karą mogłyby mówić o sytuacjach, które w ich przekonaniu są groźne.

❖ Czy dobrze jest skarżyć?

Kiedy zdarzyła się masakra w Littleton, rodzice i dyrektorzy szkół zastanawiali się, co zrobić, żeby w przyszłości nie dopuścić do podobnej sytuacji. Przede wszystkim trzeba rozmawiać z dziećmi. One zawsze wiedzą, kto w ich grupie jest inny, trudny, a co ważniejsze – kto może być groźny dla siebie i innych. Mogą nawet poważnie obawiać się niektórych kolegów, ale nie mają ochoty o tym opowiadać.

Dzieci i nastolatki mówią mi, że nie lubią „skarżyć", ale zrobiłyby to w przypadku potencjalnie groźnych sytuacji, gdyby mogły zrobić to anonimowo. Boją się represji, czują się bardzo źle, rozmawiając na taki temat z władzami szkoły czy nauczycielami. Niektórzy sądzą, że anonimowa linia byłaby najlepszym wyjściem.

Linia zgłoszeniowa: początki

Tuż po tragedii w Littleton udzielałam wywiadu gazecie „Wall Street Journal". Powiedziałam, że gdybyśmy przejrzeli wszystkie strony WWW napisane przez dzieci i poważnie potraktowali wszystkie pogróżki, które tam znajdziemy, połowa dzieci korzystających z sieci wylądowałaby w więzieniu. Zapewniałam, że dzieci często odgrywają w Internecie swoje fantazje i że to jedna z najlepszych rzeczy, jakie Internet nam zapewnia: możliwość odgrywania.

Artykuł ukazał się następnego dnia, a ja nie mogłam spać. Ktoś musi coś zrobić. Jeśli Cyberangels mówią, że nie mogą pomóc w tej sytuacji, to kto może? Czy mamy zlekceważyć nasz obowiązek udzielenia pomocy innym w sieci? Czy jest sposób na to, by zachowując prawo do prywatności i wolności słowa, odnaleźć dzieci z zaburzeniami, które z wyprzedzeniem zapowiadają wyładowanie swojej złości na sobie lub innych?

Czułam, że muszę coś wymyślić i wtedy narodziła się idea dziecięcej linii zgłoszeniowej – KIDReportline. Powstała, by dzieci miały gdzie zgłaszać groźby, które uważają za poważne, nie skazując się zarazem na lęk przed zemstą.

Jak to działa?

Byśmy mogli w linii zgłoszeniowej przyjąć jakieś zgłoszenie, muszą być spełnione pewne istotne warunki. Osobą zgłaszającą musi być dziecko. Doniesienie ma dotyczyć strony WWW stworzonej przez kolegę z klasy, który musi być przez osobę zgłaszającą uważany za zagrażającego sobie lub innym. Wreszcie strona WWW musi mówić o jakimś rodzaju przemocy lub zawierać groźby. Oto nasze zasady:

- Przyjmujemy zgłoszenia tylko od kolegów szkolnych uczniów, których strony budzą podejrzenie. Dorośli, rodzice lub nauczyciele, mogą zgłaszać swoje podejrzenia szkole, rodzinie albo organom ścigania. Koledzy szkolni często odnoszą wrażenie, że nie mają do kogo się zwrócić. Unikają informowania władz szkoły. Mogą obawiać się reprymendy albo wstydzić się „donoszenia". Ale koledzy klasowi to często jedyne osoby, które doceniają zagrożenia stwarzane przez rówieśników. Na ogół są też jedynymi osobami, które wiedzą o stronach należących do kolegów.
- Przyjmujemy tylko zgłoszenia odnoszące się do stron WWW tworzonych przez uczniów. Jeśli uczeń grozi przemocą, używając innego niż Internet medium, radzimy dziecku przysyłającemu nam zgłoszenie, by powiedziało o sprawie władzom szkolnym, rodzicom lub komuś innemu. Nasze doświadczenie dotyczy Internetu. Strony WWW umiemy ocenić natychmiast. Inne sytuacje muszą być rozwikłane przez inne agendy. Cyberangels mogą zajmować się tylko zagrożeniami jakoś wiążącymi się z Internetem. Cyberangels nie tworzą żadnej bazy danych ani nie stosują żadnego sposobu ich rejestracji. W dozwolonym prawem stopniu utrzymujemy tożsamość osoby zgłaszającej w tajemnicy. Czasem wysyłający zgłoszenie uczeń po prostu potrzebuje kogoś, kto porozmawia z nim o jego lękach i obawach. Staramy się być tym kimś.

Staramy się też wybierać kroki jak najmniej brutalne z tych, które uważamy za wskazane. Kiedy ktoś przysyła nam zgłoszenie strony zawierającej coś, co uznamy za rzeczywiste groźby użycia przemocy wobec osoby, która stworzyła stronę, lub wobec innych, zgłaszamy to szkole i policji. Czasem kontaktujemy się z uczniem, który stworzył stronę, oferując pomoc.

Dlaczego to robimy?

Bo to jedyna droga pozwalająca na zachowanie równowagi między prawem do wolności słowa a naszym pragnieniem zapobieżenia kolejnej tragedii, która może się zdarzyć dlatego, że nikt nie słuchał groźnych zapowiedzi. Przede wszystkim zaś mamy nadzieję stać się miejscem, gdzie dzieci znajdą kogoś, kto wsłucha się w ich lęki i problemy.

Mamy nadzieję, że korzystając z popularności strony Cyberangels, rozreklamujemy to przedsięwzięcie. Mamy rozległe doświadczenie w ocenie wiarygodności wypowiedzi internetowych i dobre kontakty ze społecznościami sieciowymi. Sądzimy, że dzięki temu zdołamy stworzyć instytucję, która skutecznie udzieli pomocy, nie stosując gestapowskich metod.

Sami nie poszukujemy żadnych stron i reagujemy tylko na wiarygodne zgłoszenia, przysłane przez kolegów szkolnych i dotyczące stron WWW. To nasz sposób, żeby robić coś więcej niż tylko gadać.

Wiele szkół kontaktowało się z nami, pytając, czy mogą podawać uczniom adres naszej strony i e-mailu. Inni utrzymywali, że mają zamiar podjąć podobne działania na własną rękę.

Im więcej szkoły robią, by ułatwić dzieciom mówienie o ich problemach, i im bardziej szkoły i rodzice słuchają tego, co mówią dzieci, tym lepiej dla nas wszystkich. To jedna z naszych innowacji, co do której mamy nadzieję, że będzie naśladowana przez wszystkich, którym leży na sercu dobro dziecka.

Rozsądne rodzicielstwo: zapobieganie problemom

❖ Ostrzeżony – to lepiej uzbrojony: przykazania dla rodziców

Kiedy dzieci nauczyły się dekodować hasła, przeglądać nasze pliki i znajdować informacje o naszych kartach kredytowych w komputerze, trudno je kontrolować. A jeszcze trudniej zgadnąć, jakie będzie ich następne posunięcie, co musimy wiedzieć, jeśli chcemy być o krok przed nimi.

Ale czy ktoś powiedział, że rodzicielstwo to łatwa sprawa? Rodzicielstwo to uczenie się w mgnieniu oka, konieczność reagowania na niespodzianki, dzieci zostawiające w upalny dzień nadgryzioną czekoladkę na jasnej kanapie czy wycierające brudne łapki o twój kostium właśnie wtedy, gdy wychodzisz spóźniona do pracy. Czemu więc komputerowa aktywność dzieci miałaby być czymś z innej bajki?

Już mówiłam o zagrożeniach i niebezpieczeństwach. Oto kilka dodatkowych spraw, które należy przemyśleć, jeśli nie chcemy być zaskoczeni:

- **Hasło.** Nie podawaj swojego hasła innym ani nie przechowuj go w miejscu, gdzie ktoś je może znaleźć. W końcu to ci, co znają hasła, kontrolują świat. Wybierz hasło, które łatwo ci będzie zapamiętać, ale zarazem takie, którego twoje dzieci łatwo nie odgadną. Często je zmieniaj. Kiedy je wpisujesz, nie pozwól, by ktoś ci zaglądał przez ramię. Nigdy nie przechowuj hasła na twardym dysku.
  Musisz też pamiętać, że niektórzy dostawcy usług internetowych mają taki system, który umożliwia obciążanie twojego konta określonymi zakupami dokonanymi w sieci. Opłaty za posiadanie konta i dokonane zakupy odciągane są automatycznie z karty kredytowej. Robienie zakupów jest więc bardzo wygodne, bo nie trzeba za każdym razem wystukiwać numeru karty. Ale to jeszcze jeden powód, by dobrze strzec hasła, bo to ono identyfikuje posiadacza konta.
- **Ochraniaj dzieci, gdy są poza domem.** Uzgodnij z rodzicami przyjaciół swoich dzieci jakąś formę monitorowania poczynań pociech przy komputerze i stosowanie podobnego oprogramowania blokującego. W przeciwnym razie obchodzenie twoich zakazów może się zdarzać za każdym razem, gdy dzieci wybiorą się na „buszowanie" po Internecie do swoich kolegów. Jeśli nie uda się uzgodnić jednolitego podejścia, to przynajmniej upewnij się, że inni rodzice respektują twoje życzenia i nie godzą się, by twoje dzieci korzystały z komputera w ich domach.
- **Zabezpiecz ważne pliki hasłem lub wykonaj dodatkową ich kopię.** Nie zostawiaj ważnych plików bez dodatkowych zabezpieczeń, jeśli dzieci bez nadzoru używają komputera. Nawet najbardziej niewinni i wprawni użytkownicy komputera mogą wcisnąć nieodpowiedni klawisz w niewłaściwym momencie. Sama robiłam to znacznie częściej, niż mam odwagę przyznać. Jedno niepotrzebne kliknięcie i można stracić ważne artykuły czy wystąpienia. Szkic mojej pierwszej książki, pracowicie przygotowany na nowym laptopie, w czasie podróży do Moskwy uległ zniszczeniu. Komputer bez powodu wyłączył się (przysięgam, że nic nie zrobiłam), automatyczne zapisywanie nie zadziałało. Zestresowana lotem, zmęczona, musiałam zaczynać wszystko od początku. Więc jeśli masz jakieś ważne pliki, zrób kopie na dyskietkach. Albo jeszcze lepiej, zabezpiecz pliki hasłem, a oprócz tego stwórz kopie. Wtedy mniejsze będzie prawdopodobieństwo, że dzieci będą grzebały w twoich plikach. Wiele programów pozwala na zabezpieczanie hasłem określonych informacji. Może ci to oszczędzić wielu problemów.
- **Karty kredytowe.** Nie przechowuj w swoim komputerze informacji o kartach kredytowych. Niewygoda, związana z koniecznością wyszukiwania tych danych gdzie indziej, może zniechęcić bardzo biegłe w obsłudze komputera dzieci i ich przyjaciół.
- **Ustaw komputer w centralnym miejscu domu, nigdy w pokoju dziecka.** Komputer podłączony do Internetu powinien być umieszczony w takim miejscu, gdzie przebywają różni członkowie rodziny. Dzieci rzadziej pakują się w kłopoty tuż pod naszym nosem (choć nie jest to niemożliwe). Koledzy dziecka, którzy mogą być inicjatorami takich działań, też będą mniej skłonni do prowokacji w twojej obecności, bo prowokacja angażuje zbyt duże ilości energii, by odbyła się po cichu. Coś możesz zauważyć. To zalecenie powtarzam najczęściej.
- **Wyjaśnij swoim dzieciom, że ludzie często nie są tacy, jacy się wydają.** Pamiętam zabawny skecz, w którym brzuchaty mężczyzna w kalesonach udawał, że jest młodą nastoletnią dziewczyną, gawędząc w Internecie z nastoletnim kibicem piłki nożnej, który był z kolei matroną w średnim wieku, z lokówkami i w podomce. Poza tym, że moje dzieci śmiały się z tego skeczu, posłużył mi on do przedstawienia rodzinie problemu. Ludzie nie zawsze są tymi, za których się podają w sieci. Wielu dorosłych uwodzi dzieci, udając, że są dziećmi. Choć utrata złudzeń bywa bolesna, ta wiedza może uchronić dziecko od ewentualnych kłopotów w przyszłości.
- **Musisz mieć pewność, że widzisz, co się dzieje na ekranie.** Uprzedź dzieci, że od czasu do czasu zerkasz na monitor. Pod naszym nosem dzieci mogą popaść w kłopoty, ale świadomość, że gdy przyjdzie ci ochota, możesz spojrzeć na to, co

robią, ułatwia im przestrzeganie reguł. Pewna matka na jakimś spotkaniu zapytała mnie, jakże ma spoglądać na to, co się dzieje na ekranie komputera, jeśli dzieci wyłączają go, gdy ona zjawia się na horyzoncie. Jeśli twoje dziecko chowa coś, gdy wchodzisz do pokoju, co ty, rodzic, robisz? Zaglądasz do szuflady, gdzie to coś zostało ukryte, tak? Z komputerem jest tak samo. Nadal jesteś rodzicem. Musisz nauczyć się, jak odtworzyć to, co było na ekranie i zostało wyłączone (przycisk: historia), ale radzę, byście usiedli obok i porozmawiali z dzieckiem. Kiedy wszystko zawodzi, rozmowa nie zaszkodzi.

- **Sprawdzaj od czasu do czasu twardy dysk i dyskietki.** Szukaj przegranych zdjęć lub grafik przechowywanych na twardym dysku lub na dyskietkach. Łatwo je znaleźć, bo na ogół w nazwie mają rozszerzenie „.jpg" lub „.gif". Uprzedź dzieci, że będziesz kontrolować zawartość dysku i dyskietek.
- **Uważaj na swoje własne wędrówki.** Jeśli odwiedzasz strony, na które wolałbyś swoich dzieci nie kierować, sprawdź twardy dysk w poszukiwaniu zapomnianych obrazków. I upewnij się, że nie zostawiasz zakładek, które mogą do tych stron doprowadzić. Dzięki prawu do wolności słowa możesz oglądać to, na co masz ochotę, nie zastanawiając się, czy jest to stosowne dla twoich dzieci. Ale uważaj nadając nazwy zakładkom i nie przechowuj na dysku nic, czego nie chciałbyś pokazywać swoim dzieciom.
- **Nie wymuszaj samodzielności dzieci, dopóki one nie są do niej przygotowane.** Kontroluj e-maile i siedź razem z dziećmi, dopóki są małe i są w niemoderowanej kawiarence. Sprawdź, czy znają obowiązujące tam reguły, czy wiedzą, gdzie zgłaszać przypadki niestosownego zachowania i łamania reguł. Znajomość podstawowych zasad umożliwi im bezpieczniejsze serfowanie. Jak pamiętasz, jedno z moich ostrzeżeń brzmi: „Informacja nie rani dzieci – robią to inni ludzie". Zatem dwie najważniejsze w moim przekonaniu reguły to:

1. Twoje dzieci wiedzą, jakie informacje mogą, a jakich nie powinny przekazywać innym ludziom w Internecie. Nigdy nie podają danych, które umożliwiłyby obcym osobom odnalezienie ich w realnym świecie.
2. Twoje dzieci wiedzą, że nie wolno im spotykać się twarzą w twarz z wirtualnymi „przyjaciółmi".

- **Staraj się grać aktywną i ważną rolę w życiu wirtualnym swojego dziecka i nie wpadaj w panikę bez powodu.** Poznaj wirtualnych przyjaciół i znajomych dziecka. Dziecko nie powinno obawiać się opowiadania ci o wszystkim, więc nie krytykuj go, gdy coś się nie uda. Zachęcaj dziecko, by zwracało się do ciebie zawsze, gdy otrzyma wiadomość, z którą czuje się źle, która jest sprzeczna z twoimi zasadami. Sekrety mogą być groźne. Bądź osobą, z którą dziecko dzieli swoje sekrety, i zasłuż na jego zaufanie. Nie ufaj nadmiernie, że oprogramowanie blokujące uchroni dzieci przed kłopotami. Nawet gdy zainstalujemy wszystkie dostępne obecnie narzędzia kontroli, obeznane z informatyką dziecko znajdzie sposób, by je oszukać i wpakować się w kłopoty. Nie ma narzędzi doskonałych. Niektóre programy przepuszczają strony, które chciałbyś zablokować. Inne nie blokują wysyłania różnych informacji przez dziecko. Nie polegaj na technice, nie łudź się, że ochroni ona twoje dziecko. To twoje zadanie.
- **Musisz wiedzieć, czy możesz ufać swoim dzieciom, czy zastosują się do ustalonych zasad i nie skrzywdzą innych.** Uświadom im ryzyko związane z hakowaniem i innymi wykroczeniami. Naucz je netykiety. A jeśli nadal nie można im ufać, zamknij komputer i zabierz ze sobą klucz. To może być jedyny sposób na uchronienie ich przed kłopotami.

Podstawowe zasady: szybko i prosto

Oto twoja rodzicielska ściągawka – niektóre podstawowe zasady, o których powinieneś pamiętać. (Napisałam je w takiej formie, by mieściły się na wewnętrznej stronie dłoni, na wypadek gdybyś chciał rozmawiać z dziećmi i miał kłopoty z zapamiętaniem tych zasad. Podstawowa różnica między rodzicem a uczniem polega na tym, że jako rodzic możesz używać ściągawki i nikt cię nie zdyskwalifikuje).

- Nie pozwól dziecku spędzać zbyt dużo czasu przy komputerze.
- Ludzie, nie komputery, mają być ich przyjaciółmi i kolegami.
- Postaw komputer we wspólnym pokoju, w kuchni lub salonie, nie w pokoju dziecka.

- Naucz się o komputerach tyle, byś mógł dzielić z dziećmi ich fascynacje.
- Pilnuj dzieci, gdy wchodzą do Internetu, i sprawdzaj, dokąd się udają.
- Zadbaj, by dzieci czuły się swobodnie, przychodząc do ciebie ze swoimi problemami i pytaniami.
- Zaleć dzieciom unikanie niemoderowanych kawiarenek i kanałów IRC.
- Często rozmawiaj z dziećmi o tym, co lubią robić w Internecie.
- Pomóż im zachować rozsądne proporcje między czasem spędzanym przy komputerze a czasem przeznaczonym na inne zajęcia.
- Poznaj ich przyjaciół i znajomych wirtualnych, tak jak poznajesz ich przyjaciół i kolegów z realnego świata.
- Ostrzeż je, że ludzie w Internecie mogą wcale nie być tymi, za których się podają.
- Zachęć je do kierowania się zdrowym rozsądkiem podczas serfowania w cyberprzestrzeni, tak jak robią to w życiu.
- Nie wpadaj w panikę, gdy przychodzą do ciebie z problemami, z którymi zetknęły się w sieci. Masz je zachęcić do mówienia wszystkiego, a nie przerażać.
- Omów te zasady z dziećmi, skłoń je do akceptacji i przyklej listę gdzieś blisko komputera.
- Pamiętaj o sprawdzaniu, czy stosują się do tych zasad, zwłaszcza gdy chodzi o ilość czasu spędzanego przed komputerem.

Poznaj swoje dzieci i wypracujcie wasz własny „kontrakt bezpiecznego serfowania"

❖ Co naprawdę wiemy o naszych dzieciach?

Rozwiąż poniższy kwiz. Założę się, że będziesz zdziwiony, że tak mało wiesz o swoich dzieciach.

Jak się nazywa najlepszy przyjaciel dziecka? Pełne nazwisko i imię.

Numer telefonu najlepszego kolegi?

Jaki program telewizyjny twoje dziecko lubi najbardziej? Jaki film? Jaką grupę muzyczną? Stację radiową? Czasopismo?

Jak nazywają się nauczyciele twojego dziecka?

Jakich przedmiotów uczy się w szkole?

Jakie przedmioty lubi najbardziej?

Którego nauczyciela najbardziej lubi?

Czy jest w szkole jakiś chuligan, którego się obawia?

Czy należy do jakiejś paczki? Czy walczą z inną grupą?

Jaka jest jego ulubiona książka? Ulubiony autor? Ulubiony gatunek literacki?

Czy prowadzi dziennik lub pamiętnik?

Jeśli nie jesteś wyjątkiem, nie będziesz w stanie odpowiedzieć na jedno, kilka lub na wszystkie pytania. Potraktuj to jak okazję do lepszego poznania swojego dziecka. Dowiedz się, jakie są jego zainteresowania, co czyta, co ogląda, jakie strony w sieci odwiedza. Zbyt często mówimy *o* dzieciach zamiast *ich* słuchać. A one mają wspaniałe rzeczy do powiedzenia, jeśli tylko słuchamy, jeśli naprawdę słuchamy.

Poproś, by dziecko pokazało ci kawałek Internetu. Razem z nim odwiedź jego ulubione strony. Nie zadawaj podchwytliwych pytań i nie stwarzaj wrażenia, że szpiegujesz. Wykorzystaj tę okazję, by poznać niektóre jego rozrywki. Możesz być przyjemnie zaskoczony, poznając interesujące go rzeczy. Na przykład, jak znajduje drogę w Internecie? Czy używa odsyłaczy, czy wyszukiwarek? Jeśli tak, których? Zapytaj, dlaczego preferuje określone wyszukiwarki i jak definiuje poszukiwane hasła. Gdy będziesz mieć lepsze wyobrażenie o tym, jak dziecko korzysta z Internetu, możesz zacząć myśleć o ustaleniu zasad regulujących zachowanie w sieci i zapewniających poruszanie się po bezpiecznych obszarach. Twoje zasady mają służyć temu, by lepiej poznało netykietę, by wiedziało, czego spodziewać się od innych ludzi, by wiedziało, jak się zachować w nieoczekiwanych sytuacjach i jak chronić siebie przed zranieniem w cyberprzestrzeni. To jest właśnie „kontrakt bezpiecznego serfowania".

Mają to być wspólnie ustalone zasady, stworzone przy udziale i rodziców, i dzieci. Nie powinny być siłą narzucane dzieciom. Ich skuteczność po części opiera się na porozumieniu między rodzicami a dzieckiem przy ich tworzeniu. Niektóre dzieci dobrze reagują na

spisane zasady, parafowane przez obydwoje rodziców i samo dziecko; inne będą wolały, by lista została umieszczona gdzieś w pobliżu komputera, jako przypomnienie. Powinieneś zrobić to, co im bardziej odpowiada. W końcu to ty znasz je najlepiej.

❖ Co wziąć pod uwagę, szkicując własny kontrakt i ustalając zasady bezpiecznego serfowania

Podałam kilka podstawowych zasad, byś mógł opracować własne. Masz pełną swobodę w dobieraniu i zmienianiu ich, tak aby najlepiej odpowiadały potrzebom waszej rodziny. W liście zamieszczonej poniżej staram się podsumować to, o czym nie wolno zapominać. Traktuj ją jak ściągawkę w rozmowach z dzieckiem.

- Ludzie w Internecie mogą udawać każdego, kogo chcą. Nie pozwól, by ktoś zrobił z ciebie durnia.
- Nie używaj brzydkich słów.
- Nie wdawaj się w kłótnie ani nie odpowiadaj osobom, które posługują się wulgarnym językiem.
- Nie odpowiadaj, jeśli ktoś powie coś takiego, co sprawia, że czujesz się nieswojo, albo coś, co uważasz za złe.
- Jeśli ktoś robi coś takiego, że czujesz się nieswojo, od razu powiedz o tym rodzicom. Ale nie wyłączaj komputera ani nie wychodź z tego obszaru, gdzie ktoś robi coś niewłaściwego, by dorośli mogli odszukać tę osobę i zgłosić jej poczynania jako pogwałcenie zasad korzystania z serwisu.
- Kiedy jesteś w Internecie, używaj pseudonimu, nigdy prawdziwego nazwiska (nie używaj nawet prawdziwego imienia ani prowokujących określeń, typu „nastolatka").
- Nie spędzaj całego wolnego czasu przy komputerze.
- Nigdy nie podawaj prawdziwego nazwiska, adresu, numeru telefonu, nazwy szkoły, miejsca pracy rodziców, nazwisk kolegów, nazwy klubu sportowego, niczyjego adresu e-mailowego żadnej osobie w Internecie.
- Jeśli ktoś prosi cię o te informacje, nie odpowiadaj, tylko powiedz rodzicom lub innej dorosłej osobie.
- Nigdy nie rozmawiaj przez telefon z osobą, którą znasz z Internetu, nie wysyłaj jej nic ani nie przyjmuj od niej przesyłek. Nie zgadzaj się na spotkanie.

- Nie umieszczaj swojego zdjęcia w Internecie ani nie wysyłaj go nikomu bez zgody rodziców.
- Bez zgody rodziców nie umieszczaj żadnych prawdziwych informacji o sobie w profilu użytkownika. Nie umieszczaj tam słów, które mogą sprawić przykrość innym czy sprowokować niedobre reakcje.
- Istnieją w Internecie miejsca, gdzie ludzie dyskutują czy oglądają rzeczy, które my uważamy za niewłaściwe. Jeśli natkniesz się na takie miejsce, wciśnij przycisk „wstecz", a następnie powiedz o tym rodzicom.
- Nie rób w Internecie niczego, co wymaga wnoszenia opłat, jeśli nie uzgodnisz tego z rodzicami.
- Nie podawaj innym – nawet najlepszym kolegom – swojego hasła.
- Nigdy nie podawaj informacji dotyczących karty kredytowej twojej lub rodziców.
- Nie kopiuj materiałów innych osób i nie udawaj, że są twoje.
- W ważnych sprawach nie polegaj na radach obcych, których spotykasz w kawiarence.

❖ Formalizowanie umów

W załączniku nr 3 zamieściłam przykład kontraktu bezpiecznego serfowania. Powiem wam, co mówię swoim klientom w kancelarii prawnej, kiedy pytają mnie, czy powinni używać takiego formularza zgody. Jeśli odpowiada to twoim potrzebom, możesz go używać. Jeśli nie, możesz potraktować go jako ściągawkę przy tworzeniu własnego. Niekiedy rodzice myślą, że jestem przesadnie legalistyczna, sugerując przedstawienie zasad na piśmie. To nie jest prawnie zobowiązujący kontrakt, to zbiór wytycznych. Jeśli omówisz te sprawy z dziećmi, może okazać się, że wcale nie trzeba będzie ich spisywać. Musisz tylko mieć pewność, że na pewno omówiliście każdy punkt, że dzieci zrozumiały, o co chodzi, i że zgodziły się przestrzegać reguł. Gdy to zostanie zrobione – nie ma potrzeby spisywania zasad.

To dzieci często lubią to robić, czują się wtedy bardziej odpowiedzialne za podejmowane decyzje. Pamiętaj, że tu chodzi o porozumienie między wami, nie o możliwość oskarżania dzieci o złamanie kontraktu.

Netykieta: nauczmy dzieci odpowiedniego zachowania w cyberprzestrzeni

❖ Pochodzenie netykiety

Żeby zrozumieć netykietę, trzeba najpierw zrozumieć sieć. Sieć była początkowo zaludniona przez informatyków wierzących w wolność słowa, w zasady i ideały (tak przynajmniej mówili). Komercjalizm był zawsze źle widziany (i tak naprawdę jest złamaniem zasad używania pierwotnej sieci Internet, stworzonej przez National Science Fundation). Ale mimo zmian, które komercja wprowadziła do Internetu, niektóre stare zasady nadal obowiązują. Określa się je jako netykietę (czyli etykietę dla Internetu). Zawsze lepiej jest znać zasady, zanim człowiek znajdzie się w nowym środowisku, a sieć jest takim najnowszym środowiskiem. Pamiętajmy, że oprócz zasad obowiązujących w wirtualnym świecie istnieją różne zasady dla różnych ludzi w realnym świecie. Poprzez Internet ludzie z różnych stron świata będą wymieniali poglądy i to, co dla nich jest normalne, dla ciebie może być dziwne. Ale w tej zabawie obowiązuje jeszcze jedna zasada: szacunek.

Wiele się trzeba nauczyć, ale nie musimy uczyć się wszystkiego od razu. Wszyscy byliśmy kiedyś nowicjuszami w Internecie, a już niedługo będziemy weteranami, zaśmiewającymi się z sieciowych kawałów.

❖ Zasady poprawnego zachowania w Internecie według pani Parry

Wszyscy uczymy dzieci poprawnego zachowania. Choć sami rzadko możemy to stwierdzić, zdarza się, że słyszymy od innych, że one są naprawdę grzeczne. Maniery w Internecie to nic innego. Są to zasady poprawnego zachowania w sieci, zwane netykietą. I dobrze, że istnieją, bo niektórzy ludzie robią rzeczy oburzające, gdy usiądą przy klawiaturze – rzeczy, których by nie zrobili w realnej przestrzeni. Nie wiem, czy to dlatego, że sądzą, iż są anonimowi, czy dlatego, że Internet robi z nas śmiałków. Ale nie pozwólmy dzieciom wpaść w pułapkę mówienia i robienia rzeczy, o których wiedzą, że nie powinny ich

robić czy mówić. Musimy je uprzedzić, że można je odszukać i że tak naprawdę nic w sieci nie jest anonimowe. Wszystko, co mówią, musi być mówione ze świadomością, że wcześniej czy później inni dowiedzą się, co zostało powiedziane.

Oto kilka podstawowych wskazówek, które powinieneś znać i przekazać swoim dzieciom, jeśli mają one stać się prawdziwymi „obywatelami" wirtualnego świata:

- **Poznaj zasady, zanim coś zrobisz czy powiesz w sieci.** Niektóre kluby dyskusyjne i kawiarenki mają własne, szczególne zasady dotyczące tego, co można powiedzieć czy zrobić. Ponieważ ludzie często potrafią być bardzo krytyczni wobec tych, którzy łamią zasady, znajomość tych zasad może zaoszczędzić tobie i dziecku niepotrzebnych przykrości.
- **Pomyśl, zanim coś napiszesz.** Pomyśl, czy to, co chcesz powiedzieć, jest stosowne, czy nie sprowokuje kłótni i wyzwisk. Możesz być pewien, że wszystko, co powiesz, wróci i będzie cię nękać.
- **Nie krytykuj innych, szczególnie początkujących, nawet jeśli łamią zasady.** Jeśli chcesz komuś pomóc lub go poprawić, zrób to e-mailem, nie w publicznym miejscu, takim jak kawiarenka czy grupa dyskusyjna.
- **Nie marnuj czasu innych i przepustowości łączy.** Nie przesyłaj „łańcuszków" e-mailowych, plotek czy głupich żartów. Nie przesyłaj wszystkim kopii czegoś tylko dlatego, że możesz to zrobić. Wysyłaj je tylko tym, którzy ich potrzebują.
- **Szanuj prywatność innych.** Nie podawaj publicznie niczyjego e-mailu bez pozwolenia zainteresowanej osoby. Nie używaj niczyjego hasła bez jego zgody.
- **Nie bierz niczego, nie płacąc za to.**

Zgodnie z netykietą niedopuszczalne jest też:

- Używanie drukowanych liter – jest to traktowane jak krzyk i jest przykre dla oczu.
- Rozpoczynanie lub prowokowanie kłótni.
- Rozpowszechnianie nieprawdy i mówienie niegrzecznie o innych.
- Przesyłanie dużych załączników bez uprzedzenia.

- Zwracanie się do kogoś prawdziwym imieniem w kawiarence czy innym miejscu publicznym.
- Wysyłanie e-mailów do ludzi, których nie znasz, reklamowanie czegoś.
- Mówienie o czymś niezwiązanym z tematem w kawiarence tematycznej.
- Nierespektowanie kolejności mówienia czy szczególnych zasad obowiązujących w kawiarence.

To są zasady, od których nie ma odstępstw. To, że jesteś ukryty za ekranem komputera, nie zwalnia od obowiązku przestrzegania zasad dobrego wychowania.

❖ Uśmieszki: emocje w cyberprzestrzeni

Niektórzy z was być może są weteranami sieciowymi, ale część niewiele wie o Internecie i istniejących tam serwisach. By wam pomóc, przygotowałam listę ikon oznaczających emocje, czasem nazywanych „uśmiechami", które są skrótami pozwalającymi czytelnikowi lepiej uchwycić subtelności przekazu internetowego. To mała próbka, więcej znajdziesz w: www.familyguidebook.com i www.cnet.com.

Ponieważ za pomocą klawiatury nie można przekazywać sarkazmu, humoru, kpiny czy innych emocji towarzyszących wypowiedziom (w końcu pisanie jest pisaniem), ludzie, którzy korzystają z Internetu, wprowadzili umowne oznaczniki emocji. Nazywa się je „uśmiechami":

<g>	szeroki uśmiech
<G>	bardzo szeroki uśmiech
:-)	uśmiechnięta twarz
:->	bardzo uśmiechnięta twarz
;-) lub;->	mrugnięcie
:-(	zmarszczenie brwi
:-P	pokazanie języka
@——>—	cyberróża
<):-)	klown
(:-O	ktoś, kto jest zdziwiony
:D	szczęśliwy i hałaśliwy
:ox	szaaa! to tajemnica!

Jeśli nie rozumiesz, czemu te znaczki oznaczają to, co mówię, że oznaczają, to obróć tę książkę o 90 stopni w prawo. (Jeśli dalej nie rozumiesz, to obróć ją jeszcze raz. <G>).

Co za dużo...

Jednym z większych wyzwań, przed jakimi stają rodzice, jest dbanie o to, by ich dzieci nie zostały całkowicie pochłonięte przez komputery i Internet.Wszyscy jesteśmy świadomi dobrodziejstw wynikających z umiejętności posługiwania się komputerami, ale musimy też dostrzegać zagrożenia związane z tym, że dzieci spędzają każdą wolną chwilę ukryte za ekranem komputera. Cyberprzyjaciel to marna namiastka prawdziwego przyjaciela z krwi i kości. A ręce usprawniane tylko stukaniem w klawiaturę nigdy nie dorównają tym sprawnym dzięki grze w piłkę czy ćwiczeniu palcówek na pianinie. Prawdziwe chmury na niebie wyglądają inaczej niż chmury na obrazku otwierającym system Windows '95. Wszyscy rodzice, którzy stanęli wobec niemożliwego wprost zadania oderwania od ekranu dzieci zajętych grami wideo, wiedzą, jak uzależniająca może być interaktywna rzeczywistość. A jednocześnie znajomość komputera i cyberprzestrzeni jest częścią rozwoju naszych dzieci. Jak mamy pomóc dzieciom w zachowaniu umiaru?

Ustalmy, jak często i jak długo dzieci mogą siedzieć przy komputerze. Moi współpracownicy z grupy Teenangels mówią, że trzeba elastycznie ustalać limity czasu, bo niekiedy wykonanie pracy domowej wymaga dłuższego przeglądania źródeł. Jako ogólną zasadę zgodziliśmy się przyjąć czas 1,5 godziny dziennie – przy założeniu, że nie mają akurat jakiejś pracy domowej zmuszającej do dłuższego siedzenia przy komputerze.

Choć powinniśmy dążyć do tego, by nasze dzieci same pilnowały przestrzegania uzgodnionych limitów czasowych, może warto wiedzieć, że są programy komputerowe ograniczające czas korzystania z komputera. Można nawet ustalić godziny, kiedy komputer będzie używany i kiedy można włączyć się do Internetu. (Można tych programów użyć, by ograniczyć czas spędzany na grach komputerowych). Niektórzy rodzice, szczególnie ci biegli w informatyce, próbują „wpadać" z biurowych komputerów do ulubionych kawiarenek swoich dzieci, by sprawdzić, czy one tam są. To cybernetyczny odpowiednik

pukania do drzwi pokoju z przypomnieniem, by kończyły rozmowę telefoniczną i odrobiły pracę domową.

Kiedy dziecko jest na tyle duże, by korzystać z komputera?

Bardzo często rodzice dają się złapać w pułapkę porównywania swoich dzieci z innymi: które pierwsze zaczęło mówić, chodzić, wyrosło z pieluchy. Często zwracają się do mnie z pytaniem, kiedy dziecko powinno zacząć poznawać komputer i po czym poznać, że jest do tego gotowe. Zawsze udzielam takiej samej wykrętnej odpowiedzi: „To zależy". Zależy od ciebie i od twego dziecka.

Większość dzieci zapoznaje się z komputerem siedząc na naszych kolanach, obserwując, jak się nim „bawimy". Moja siostrzenica Danielle brała zapasową klawiaturę, gdy miała dziesięć miesięcy. Stukała sobie spokojnie, w dużej odległości od komputera. Gdy była troszkę starsza, od czasu do czasu podchodziła do monitora, by zerknąć na migające kolory i dźwięki. Jeśli rodzice zbyt długo zapominali o niej, zajęci komputerem, wdrapywała się im na kolana, chcąc znowu znaleźć się w centrum uwagi. Kiedyś przy takiej okazji jej ręce natrafiły na mysz i szybko skojarzyła, że poruszenie myszą powoduje ruch kursora. Zaśmiewała się, gdy kursor dziko tańczył po całym ekranie.

Są programy dla małych dzieci, powodujące powstawanie dźwięków za każdym razem, gdy dziecko wciśnie jakiś klawisz. Danielle uczyła się, że komputer może być dla niej tak samo interesujący jak dla jej rodziców. Gdy miała dwa i pół roku potrafiła bawić się swoim ulubionym programem, ciągle ucząc się kontroli ruchów kursora. Mając trzy lata znakomicie panowała nad ruchami kursora. Gdy dostała nowy CD-ROM, przedstawiający jej ulubionego bohatera, Artura, zaskoczyła wszystkich. Moja siostra, rozmawiając przez telefon, usłyszała szum uruchamianego komputera. Danielle siedziała przed komputerem i załadowawszy nowy CD-ROM, zaczęła odtwarzać program. Wtedy po raz pierwszy sama używała komputera.

Czy wszystkie dzieci są w stanie samodzielnie używać komputera w wieku trzech lat? Oczywiście, że nie. (Niektóre zaczynają w wieku 2 lat!). To zależy od otoczenia, od tego, jak często dziecko widzi innych członków rodziny używających komputera, i od samego dziecka. Kiedy rodzice uprawiają sporty, dziecko interesuje się sportem. Kiedy rodzice gotują, dziecko lubi gotować. Kiedy rodzice spędzają dużo czasu przy komputerze – dziecko naśladuje ich, zainteresowane tym, co ich interesuje.

Pozwólmy więc dzieciom siadać na naszych kolanach i dotykać myszy i klawiatury. (Nazywa się to serfowaniem z kolan). Znajdź programy z ulubionymi bohaterami, odszukaj też strony WWW, gdzie są prezentowane postacie z bajek. Często interaktywne programy można połączyć z książkami, co pobudza do czytania, a zarazem oswaja z komputerem. (Odwiedź Kid-Space, świetną witrynę dla małych dzieci – www.kid-space.org – dzieci mogą tam tworzyć muzykę, zanim jeszcze potrafią czytać).

Prowadź je za rączkę, gdy używają akcesoriów dostosowanych do rozmiarów dorosłej ręki. Sprawdź, czy do twojego komputera są akcesoria w mniejszym rozmiarze. Byłam zaskoczona, że tak niewiele różnych komputerowych gadżetów istnieje w wersji dla dzieci. Łatwiej jest używać przyrządów dostosowanych rozmiarem, są też one na ogół bardziej kolorowe.

Mimo że byłam zachwycona, iż moja genialna siostrzenica kontynuowała rodzinne tradycje techniczne, radziłam, by nie zostawiano jej bez nadzoru z kosztownym Power Mac mojej siostry. Akurat gdy pisałam moją poprzednią książkę, odkryliśmy, że nasz cherubinek zdołał usunąć z komputera mojej siostry wszystkie pliki, ponieważ odkryła, że można przenosić pliki i wrzucać je do kosza, a za każdym razem, gdy się to zrobi, pojawia się Oskar Grouch.

Dzieci powinny zacząć używać komputera, gdy chcą, i powinny uczyć się tego we własnym tempie. Pamiętajmy, że to nie są zawody.

Aktywność w sieci jest mniej ciekawa dla małych dzieci, bardziej dla tych, które potrafią czytać i pisać, i potrafią stosować się do podawanych instrukcji – czyli na ogół dla siedmiolatków i starszych. Nawet i wtedy witryny WWW dla rodzin i dla dzieci powinny być odwiedzane tylko z rodzicami czy innym dorosłym. To wspaniały sposób wspólnego spędzania czasu, okazja do porozmawiania o zasadach, systemie wartości, podzielenia się przemyśleniami.

Dzieci nie powinny używać Internetu bez nadzoru, dopóki nie masz pewności, że rozumieją ustalone przez ciebie reguły i będą się do nich stosować. Wymyślne programy nie zastąpią rodzicielskiej kontroli.

A zatem, kiedy dziecko jest gotowe do korzystania z komputera? Gdy oblatany w Internecie rodzic tak uważa.

Rozdział 8

Dokonywanie wyborów i ich realizacja

W poszukiwaniu rozwiązania dobrego dla ciebie i twoich dzieci

Teraz znasz już zagrożenia. Podpowiedziałam nawet, jak uczyć dzieci, żeby były mądrymi konsumentami informacji. I co dalej? Dokąd się udasz? Co zrobisz? Czy będziesz opierać się na zaufaniu i edukacji? Czy skorzystasz z pomocy programów filtrujących? Wybór należy do ciebie. Ale zanim dokonasz tego wyboru, podzielę się z tobą wiedzą o tym, jak postępują inne rodziny.

❖ Jak radzą sobie inni?

AOL podaje, że 80% rodziców młodszych dzieci używa oferowanych przez nich programów, wspierających rodzicielską kontrolę.

Ogólnokrajowe badania rodziców dotyczące komputerów domowych przeprowadził Uniwersytet Pensylwania. Rezultaty opublikowano w maju 1999. Były to niewielkie badania na 1100 rodzinach z dziećmi w wieku 8–17 lat, które miały komputer w domu. Około 60% tych gospodarstw domowych miało też dostęp do Internetu. Badania wykazały, że mniej więcej jedna trzecia z nich używa jakiegoś rodzaju narzędzi filtrujących (to znacznie wyższy wskaźnik niż moje mniej metodyczne badania rodziców i dzieci podczas spotkań z nimi). Badania wykazały też, że rodzice mieli niejednoznaczne postawy, jeśli chodzi o Internet. Większość, 78%, stwierdziła, że są „bardzo" albo „w pewnym stopniu" zmartwieni tym, że dzieci mogą ujawnić dane osobowe w Internecie i że mogą oglądać materiały jawnie seksualne. Spora grupa, 59%, miała zarazem przekonanie, że dzieci pozbawione dostępu do Internetu są w mniej korzystnej sytuacji w porównaniu z rówieśnikami, a więcej niż 70% uważało, że Internet pozwala dzieciom odkrywać fascynujące, pożyteczne rzeczy i pomaga w odrabianiu lekcji. Joseph Turow, który przedstawił wyniki badania, ujął to tak: „Rodzice widzą Internet jako marzenie i jako koszmar zarazem". Sądzę, że badania są bardzo użyteczne dzięki temu, że pokazują, co robią rodzice, mający w domu dostęp do Internetu. Przytłaczająca większość badanych stwierdziła, że ustalają zasady korzystania przez dziecko z Internetu i „mają oko" na to, co ich dzieci robią w sieci. A dokładniej z badań wynika, że w odniesieniu do dzieci w wieku 8–12 lat:

- 84% rodziców ustala, które miejsca w sieci dziecko może odwiedzać.
- 84% rodziców określa porę dnia czy nocy, kiedy dzieciom wolno korzystać z Internetu.
- 78% rodziców określa, co dzieciom wolno robić w sieci.
- 63% rodziców określa, ile czasu dziecku wolno spędzić w sieci.
- 73% rodziców ustaliło zasadę, że dziecko może korzystać z Internetu tylko w towarzystwie osoby dorosłej, tak w domu, jak i poza domem.
- 49% rodziców przyjęło zasadę, że dziecko może korzystać z Internetu wyłącznie w domu.
- 30% rodziców przyjęło zasadę, że dziecko może korzystać z Internetu tylko wtedy, gdy ma to związek z odrabianiem lekcji.

Gdy dzieci podrastają, zasady stają się mniej rygorystyczne. Dla nastolatków między 13 a 17 rokiem życia:

- 71% rodziców ustala zasady dotyczące miejsc w sieci, które wolno dzieciom odwiedzać.
- 68% rodziców ustala porę dnia czy nocy, kiedy dzieci mogą korzystać z Internetu.
- 70% rodziców ustala zasady dotyczące tego, co dziecko może robić w sieci.
- 55% rodziców określa, ile czasu dziecko może spędzać przed komputerem.

- 29% rodziców przyjmuje zasadę, że dziecko może wchodzić do Internetu tylko w obecności osoby dorosłej, w domu i poza domem.
- 35% rodziców przyjmuje zasadę, że dzieci mogą korzystać z Internetu tylko w domu.
- 21% rodziców przyjmuje zasadę, że dzieci mogą korzystać z Internetu tylko w związku z lekcjami.

Rodzice, którzy mają w domu dostęp do Internetu używają następujących sposobów, by trzymać dzieci z dala od kłopotów w cyberprzestrzeni:

- 86% rodziców dzieci między 8 a 12 rokiem życia i 80% rodziców nastolatków ustala zasady, których ich dzieci mają przestrzegać.
- 88% rodziców młodszych dzieci i 73% rodziców nastolatków kontroluje to, co ich dzieci robią przy komputerze.
- 67% rodziców dzieci młodszych i 29% rodziców nastolatków nie pozwala dzieciom korzystać z Internetu, gdy dorosłych nie ma w domu.
- 35% rodziców dzieci między 8 a 12 rokiem życia i 27% rodziców nastolatków stosuje oprogramowanie blokujące dostęp do określonych stron.
- 24% rodziców młodszych dzieci i 17% rodziców nastolatków zakazuje dzieciom korzystania z Internetu w domu.

Teraz już się domyślacie, co mam zamiar powiedzieć: choć dobrze jest wiedzieć, jak radzą sobie inni, nie ma to tak naprawdę wielkiego znaczenia, kiedy trzeba ustalić zasady odpowiednie dla waszej rodziny.

❖ Jakie są możliwości?

Kiedy dwa lata temu pisałam swój przewodnik po Internecie dla rodziców, niewiele mieli oni do dyspozycji poza wielofunkcyjnym tradycyjnym oprogramowaniem filtrującym i blokującym. Od tego czasu powstało wiele typów programów monitorujących. Ale najbardziej ekscytująca zmiana dokonała się w zakresie budowania tzw. bezpiecznych przystani – zamkniętych lub półzamkniętych środowisk tworzonych dla dzieci i nastolatków. Rodzice uwielbiają te miejsca, a co ważniejsze – dzieci je lubią!

Podczas gdy niektórzy rodzice chcieliby, by dzieci były odgrodzone od wszystkiego, co budzi ich sprzeciw, inni chcą, by ich dzieci miały kontakt ze wszystkim i ze wszystkiego mogły się uczyć. Niektórzy wcale nie zawracają sobie głowy blokowaniem określonych stron, inni znów sądzą, że bez blokujących programów zupełnie sobie nie poradzą. Niektórzy chcą używać przyjaznych dzieciom wyszukiwarek, ale żadnego poza tym urządzenia filtrującego. To wasze rodzicielskie prawo – ustalać zasady dla waszej rodziny. Możecie karmić swoje dzieci kiełkami i serem tofu albo zabierać je co dzień do McDonalda. Podobnie to wy decydujecie, co dzieci powinny robić w sieci i dokąd wolno im pójść.

Aby dokonać wyboru, musisz jednak wiedzieć, co tam jest. A jest wiele wspaniałych, bezpiecznych i zabawnych stron dla dzieci i nastolatków. Większość serwisów jest bezpłatna, niektóre wymagają niewielkiego miesięcznego abonamentu. Są filtrujące wyszukiwarki, przyjazne dzieciom przeglądarki i wiele list bezpiecznych stron.

Jednak nawet wtedy, gdy wybierzesz korzystanie z narzędzi filtrujących i blokujących, zarejestrujesz się w przyjaznych dzieciom serwisach, polegasz na bezpłatnych „bezpiecznych przystaniach" lub korzystasz ze wszystkich tych opcji, pamiętaj, że edukacja twoich dzieci w zakresie bezpieczeństwa w Internecie jest podstawową metodą obrony. Nie powierzaj żadnemu produktowi ani żadnej witrynie sprawy bezpieczeństwa twego dziecka. Korzystanie z techniki jest jak używanie pasów bezpieczeństwa i poduszek powietrznych w samochodzie. Pierwszą i zasadniczą obroną jest rozsądne prowadzenie samochodu. Poduszki i pasy poprawiają bezpieczeństwo, gdy dzieje się coś nieoczekiwanego lub gdy inny kierowca nie jest dostatecznie uważny.

Dzieci należy nauczyć, jak mają radzić sobie z różnymi treściami i z różnymi sytuacjami, jak oceniać wiarygodność osób i informacji, jak decydować, co jest warte ich czasu i uwagi. Tylko poprzez edukację można to osiągnąć. Dzieci muszą rozumieć zasady i wartości wyznawane przez rodzinę, by takie sądy wydawać. Tylko rodzice mogą przekazać dziecku zasady i wartości wyznawane w rodzinie. Programy filtrujące mogą być pewną pomocą, zwłaszcza gdy dzieci są młodsze. Ale nie da się przecież filtrować życia.

Jeśli jesteś zainteresowany narzędziami technicznymi ułatwiającymi wprowadzenie dokonanych przez siebie wyborów, to powiem, że

jest ponad sto różnych programów, które dokonują oceny treści zawartych na określonych stronach po to, by blokować dostęp do nich. Wiele filtruje informacje wysyłane i otrzymywane. Choć niektórzy uważają je za pomocne, nie można ich traktować jak zastępczych rodziców. Mogą być stosowane, ale nie mniej ważny jest dobry kontakt z dzieckiem i stałe rozwijanie jego zdolności myślenia.

Tak, Wirginio... Internet ma dobre strony!

Akurat wtedy, gdy mieliście zamiar dać sobie z tym wszystkim spokój, mając „po uszy" paskudnych rzeczy w Internecie i jego ciemnych stron – bach! Panie i panowie, witajcie w lepszej stronie Internetu!

Kilka lat temu rodzice, którzy chcieli ograniczyć kontakt swoich dzieci z niestosownymi treściami w sieci, nie mieli wielkiego wyboru. Ale przemysł odpowiedział na ich potrzeby i powstało wiele wartościowych i zabawnych portali wyłącznie dla dzieci. A im więcej będzie ciekawych witryn dla dzieci, tym mniejsze prawdopodobieństwo, że będą one zaglądały w nieodpowiednie miejsca.

Teraz mamy do wyboru szeroki zakres zabawnych, ciekawych i wartościowych treści – a wszystko to jest zarazem bezpieczne! Istnieją przyjazne dzieciom wyszukiwarki, listy dobrych stron sporządzone przez nauczycieli i bibliotekarzy, wyposażone w odnośniki, wspaniałe witryny dla dzieci w różnym wieku, „bezpieczne przystanie", zaprojektowane dla dzieci (wirtualne odpowiedniki bezpiecznych placów zabaw) i kluby zrzeszające dzieci. Omówię tu kilka z nich, ale stale sprawdzaj, czy nie pojawiły się nowe. Ta dziedzina rozwija się dynamicznie, firmy prześcigają się w tworzeniu materiałów służących edukacji i rozrywce. Przemysł wreszcie odkrył, że dostarczanie tego, co jest potrzebne rodzicom, to dobry interes.

❖ Wyszukiwanie przyjaznej dzieciom zawartości

Filtrujące wyszukiwarki

Są dwa rodzaje filtrujących wyszukiwarek: takie, które były od podstaw tworzone jako przyjazne dzieciom, i takie, które filtrują rezultaty poszukiwań przeprowadzanych przez główną wyszukiwarkę. Większość dużych wyszukiwarek posiada teraz opcję wyszukiwania

„czystych stron", co pozwala na przeszukiwanie i wybieranie tylko tych stron, które zawierają treści odpowiednie dla dzieci. Każdy, kto próbował szukać hasła „dziewczynki" i „zabawki" i znalazł znacznie więcej, niż oczekiwał, doceni filtrujące wyszukiwarki.

Przedstawiam poniżej moje ulubione. Wszystkie je wypróbowałam i mam pewność, że dobrze wypełniają swoje zadanie, polegające na odsiewaniu stron i blokowaniu reklam niestosownych dla dzieci. Jeśli zdecydujesz się na używanie innych, najpierw je wypróbuj.

Przyjazne dzieciom wyszukiwarki

Przy użyciu tych wyszukiwarek możesz przeprowadzić bezpieczne i przyjazne dzieciom poszukiwania, gdy tylko je wybierzesz – żadna rejestracja nie jest potrzebna:

AOL's NetFind Kids Only
www.aol.com/netfind/kids
Ask Jeeves for Kids!
www.ajkids.com

Ask Jeeves for Kids! jest potomkiem bardzo popularnej wyszukiwarki, Ask Jeeves. Ask Jeeves for Kids! działa inaczej niż inne wyszukiwarki, bo zamiast podawania haseł (słowa połączone znakami+ lub –) można zadawać proste pytania. Więc zamiast poszukiwać niebo+niebieskie+dlaczego, można zaprogramować wyszukiwanie „dlaczego niebo jest niebieskie". Ta wyszukiwarka ma też bardzo użyteczną opcję, służącą wyłapywaniu prostych błędów w pisaniu. Pokazuje ponadto poszukiwania prowadzone przez inne dzieci, podając wzór pytań, które można zadawać.

DIG
www.dig.com

Disneyowska przyjazna dzieciom wyszukiwarka przegląda tylko strony portalu Disney, ale jest tam tyle wspaniałych gier, historyjek, że twoje dzieci mogą nie mieć ochoty oglądać całej reszty Internetu.

KidsClick
http://sunsite.berkeley.edu/KidsClick

KidsClick to wyszukiwarka stworzona specjalnie dla dzieci przez bibliotekarzy z Ramapo Catskill Library System w Nowym Jorku. Zaczęli od stworzenia razem z Amerykańskim Towarzystwem Bibliotekarskim listy godnych polecenia stron dla dzieci, a potem rozwijali ten pomysł.

Yahooligans!
www.yahooligans.com

Yahooligans! była pierwszą przyjazną wyszukiwarką dla dzieci, stworzoną kilkanaście lat temu. Jest to specjalny serwis, oferowany przez Yahoo!, jedną z najpopularniejszych wyszukiwarek. Zawiera wiele doskonałych witryn i serwisów dla dzieci. To coś więcej niż zminiaturyzowana wersja Yahoo! – proponuje mnóstwo ciekawych zajęć dla dzieci, jak np. ich „stronę z plikami do kopiowania", z dźwiękami, filmami i obrazami. Dzieci uwielbiają zamieszczać je w swoich pracach domowych i na swoich stronach WWW. Yahooligans! ma też opcję wyboru, pozwalającą na serfowanie wyłącznie po stronach przyjaznych dzieciom.

Zwykłe wyszukiwarki, posiadające opcje „przyjaznego dzieciom wyszukiwania"

Posługując się tymi wyszukiwarkami, najpierw wchodzisz w normalną jej stronę, potem wybierasz filtry, które służą do bezpiecznego serfowania.

Family Filter w Altavista
http://image.altavista.com/cgi-bin/globalff

Filtr rodzinny Altavista pozwala odcedzić obrazki, filmy i pliki dźwiękowe. Pozwala na filtrowanie wszystkich poszukiwań, w tym przeszukiwań stron WWW. Ustawienia filtrów można dowolnie zaprogramować, a następnie wybrane ustawienie zabezpieczyć hasłem, dzięki czemu za każdym razem, gdy dzieci korzystają z Altavista, wyszukiwanie będzie filtrowane.

SearchGuard wyszukiwarki Lycos
http://my.lycos.com/safetynet/safetynet.asp

SearchGuard jest opcją bezpiecznego serfowania, dostępną w witrynie Lycos, która filtruje wyszukiwane strony, odrzucając te szerzące nienawiść, rasizm oraz strony dla dorosłych. Zarejestrowani użytkownicy mogą łatwo włączać i wyłączać opcję, wprowadzając hasło. SearchGuard pozwala też rodzicom zablokować dostęp do kawiarenek, poczty elektronicznej i list dyskusyjnych.

❖ Listy zaakceptowanych stron

Zbyt często koncentrujemy się na zakazach. Robimy dzieciom wykłady na temat miejsc w sieci, do których nie powinny się udawać.

Mówimy im, czego nie robić. Ale powróćmy pamięcią do okresu, gdy były nieco mniejsze. Za każdym razem, gdy mówiliśmy im „nie" i nie dawaliśmy jednocześnie jakiejś pozytywnej propozycji, czegoś na „tak", to za chwilę były dokładnie tam, gdzie miały się nie pokazywać. Więc listy akceptowanych stron to wspaniała rzecz na początek.

Amerykańskie Towarzystwo Biblioteczne

Amerykańskie Towarzystwo Biblioteczne ma kilkanaście wspaniałych list „dobrych stron". Jeśli chodzi o Internet, nikt nie rozumie go lepiej i nie potrafi lepiej poprowadzić dzieci niż bibliotekarze i biblioteczni specjaliści od mediów.

ALA's (American Library Association) dobre miejsca dla dzieci
http://www.ala.org/alsc/children-links.html

ALA's 700+ Wspaniałych stron: Zabawne, niezwykłe, tajemnicze, wspaniałe strony WWW dla dzieci i dla dorosłych, którym na dzieciach zależy.
http://www.ala.org/parentspage/greatsites/

ALA's Internetowy przewodnik dla nastolatków
http://www.ala8.ala.org/teenhoopla/links.html

Cyberangels

Wiem, że nie jestem obiektywna, ale grupa matek wolontariuszek naszych Cyberangels odnalazła setki wartościowych i bezpiecznych stron dla dzieci w różnych kategoriach, jak np. nauka i ściągawki do pracy domowej. Uzyskały one nasz „dyplom uznania". Dokonując oceny tych stron, zwracaliśmy również uwagę na to, czy podają swoje zasady ochrony prywatności. Tym sposobem pomogliśmy wielu wspaniałym witrynom stworzyć odpowiednie zasady, a także zasady bezpiecznego serfowania, żeby mogły zakwalifikować się do naszej listy. Chcecie nam pomóc? Dyrektor zespołu sprawdzania witryn zawsze chętnie skorzysta z pomocy każdej zainteresowanej, wrażliwej osoby. Wystarczy wysłać e-mail: CAST@cyberangels.org. albo Cybermoms@cyberangels.org.

Lista witryn zaaprobowanych przez Cyberangels' Cybermoms':
http://www.cyberangels.org/cybermoms/links.htm

Przewodnictwo i wsparcie

Kiedy poszukiwałam jakiegoś przewodnictwa i wsparcia w sprawie ochrony dziecka, znalazłam cudownych, wrażliwych i mądrych ludzi w Towarzystwie Przyjaciół Dzieci. Laurie Lipper i Wendy Lazarus to naprawdę niezwykli ludzie, którzy dobro dzieci stawiają najwyżej. Oni pierwsi zwrócili uwagę na problem bezpieczeństwa dzieci w Internecie. Poza tym są orędownikami równego dostępu dzieci do edukacji i osiągnięć technicznych. Wypowiadają się w sieci także w sprawach zdrowia dzieci. Ich witryna jest kopalnią informacji. Jest tam Centrum Informacyjne dla rodziców w językach angielskim i hiszpańskim, niezwykły Przewodnik dla rodziców po informatycznej superautostradzie i Bezpieczeństwo dzieci w sieci: rady i pomoce dla rodziców. (Mam ten zaszczyt, że moja pierwsza książka wymieniona została w obu tych przewodnikach).

http://www.childrenspartnership.org

Inne listy polecanych stron, przygotowane przez cenione firmy

SurfMonkey kanał dla dzieci: lista ciekawych stron:
http://www.surfmonkey.com/directory/Coolsites/default.asp
Yahooligans! Przewodnik po sieci WWW dla dzieci:
http://www.yahooligans.com/
Spis internetowych stron dla dzieci przygotowany przez Lycos:
http://www.lycos.com/Home/Kids/
Webcrawler Kanał dla Dzieci i Rodzin, z telewizyjnymi warsztatami i przewodnikiem po stronach WWW:
http:// www.webcrawler.com/ctw/
Informator dla dzieci firmy Netscape:
http://www.directory.netscape.com/Home/Kids/

❖ Zaufaj znanym i wypróbowanym firmom

Istnieją instytucje, którym zawsze ufaliśmy w sprawach naszych dzieci. Mam tu na myśli Childrens Television Workshop, Public Broadcasting Service, Disney, Nickelodeon, „Sports Illustrated for Kids", „Time for Kids", „National Geographic", „The Discovery Channel" i inne. Wszystkie one przełożyły swoje rozrywkowe czy edukacyjne materiały na język nowego medium, jakim jest Internet. A treść nie tylko nie ucierpiała na tym, ale nawet stała się zabawniejsza dla dzieci, włączonych w interaktywne formy prezentacji.

Oto adresy: The Children's Television Workshop – www.ctw.org
Public Broadcasting System's Kids Online – www.pbs.org/kids
Disney – www.disney.com
Nickelodeon – www.nick.com
Sports Illustrated for Kids – www.sikids.com
Time for Kids – www.pathfinder.com/TFK/
National Geografic for Kids – www.nationalgeografic.com/kids/
The Discovery Channel for Kids – www.discoverykids.com

Także wiele znanych korporacji, które nie mają związku z mediami czy rozrywką, postanowiło wsiąść do pociągu: „Internet dla dzieci". Chodzi mi o witryny stworzone przez firmy cieszące się wysokim poważaniem w realnym świecie, ceniące swoje dobre imię.

Fleet

Fleet Kids (zbudowane we współpracy z Headbone, jedną z głównych witryn dla dzieci i młodzieży): http:/fleetkids.com

Fleet Kids zostało stworzone, by ułatwiać dzieciom poznawanie spraw związanych z finansami, pracą zespołową i aktywnością obywatelską. Tak naprawdę zostało to potraktowane przez firmę jako rodzaj służby publicznej: nie ma tam odsyłacza do najbliższej filii firmy Fleet. Jeśli chcecie wiedzieć, czego uczą nasze dzieci, sprawdźcie: www.fleet.com/fleetkids.

Chevron

http://www.chevronkids.com/

To wspaniała witryna. Mimo że pojawiają się tam samochody, nie jest to reklama firmy. Promuje się tu raczej to, co dzieci uwielbiają. Mają wiele darmowych programów i gier, zabawy, a dodatkowo – świetnie opracowane zasady ochrony bezpieczeństwa i prywatności w Internecie, które są wykorzystywane jako wzorzec przez wiele grup przemysłowych.

Każdy z nas powinien wyrazić im uznanie za starania i wysiłek włożony w stworzenie ciekawej i wartościowej witryny dla dzieci. Inaczej niż firmy, które mają bezpośredni interes w tworzeniu podobnych stron, Chevron robi to z dobrej woli.

❖ Bezpieczne przystanie w sieci

Wiele najnowszych witryn dla dzieci zaspokaja wymagania rodziców w zakresie jakości prezentowanych treści, ale ważniejsze jest to, że zaspokaja też zapotrzebowanie dzieci na zabawne i ciekawe materia-

ły. Ich nazwy obce są rodzicom, którzy nie są blisko Internetu, ale to te firmy kontrolują rynek dziecięcy w sieci. Są one szczególnie atrakcyjne dla dzieci nieco starszych, które są za duże na dziecięce witryny, a za małe na zawartość Internetu dla dorosłych. Oto niektóre moje i dzieci ulubione witryny:

Bonus (www.bonus.com) jest witryną stworzoną dla dzieci w wieku 3–13 lat. Opisywana jest jako tematyczny park dla dzieci z bezpiecznymi zjeżdżalniami i innymi atrakcjami. I tak ją widzą dzieci. Bonus nie ma kawiarenki, ale ma całe mnóstwo gier. Są też sekcje dla rodziców i nauczycieli. Aktywnie popiera pomysł programu Wired Kids, przedstawiając gry i zagadki dotyczące bezpieczeństwa i opisując zachowania dzieci w Internecie.

Freezone (www.freezone.com) jest witryną zaprogramowaną dla dzieci w wieku 8–14 lat. Zapewniono tam wszelkie warunki do tego, by nastolatki mogły budować własną społeczność. Jest tam bezpieczna i monitorowana kawiarenka, są kluby dyskusyjne, kartki pocztowe. Często jest wymieniana jako ulubione miejsce pogawędek. Ponadto ma wiele najbardziej wszechstronnych procedur służących zapewnieniu bezpieczeństwa. Rodzice mogą odbyć przeglądową wycieczkę, by zorientować się, co dzieci będą tam robić.

Headbone (www.headbone.com) jest wirtualnym światem, stworzonym dla dzieci w wieku 8–14 lat. Przedstawia bardzo dużo oryginalnych treści i pomysłów. Headbone ma własne profile, listy kumpli i kawiarenki, wszystkie monitorowane i dostępne dla dzieci poniżej 13 lat tylko za zgodą rodziców. Sprawy bezpieczeństwa traktowane są tu bardzo poważnie. W planie jest też partnerstwo, które być może zapewni przeniesienie zawartości Headbone do telewizji i gazet na całym świecie.

KidsCom (www.kidscom.com) to jedno z ciekawszych miejsc dla dzieci, istniejące od 1995 roku, przeznaczone dla użytkowników w wieku 4–15 lat. Są tam monitorowane kawiarenki, międzynarodowe programy nawiązywania korespondencyjnych znajomości i liczne gry. Dzieci uwielbiają tę witrynę, ale o niepowtarzalności KidsCom decyduje opcja ParentTalk, czyli rodzaj grupy dyskusyjnej dla rodziców, w której dowiadują się oni, czego powinni nauczyć swoje pociechy na temat Internetu i jak mają dotrzymywać im kroku w serfowaniu.

Lycos Zone (www.lycoszone.com) jest bezpiecznym rajem w sieci stron WWW, zaprogramowanym dla dzieci od wieku przedszkolnego. Jest tam strefa „gier i zabaw" dla różnych grup wiekowych, obszar

poświęcony odrabianiu lekcji i wreszcie miejsce na sprawy „nowe i ciekawe". Jest nawet kącik dla rodziców i nauczycieli. Witryna posiada odsyłacze do innych doskonałych miejsc dla dzieci. Kiedy dziecko odwiedza stronę, automatycznie jest uruchamiany filtr gwarantujący bezpieczne wyszukiwanie.

Mamamedia (www.mamamedia.com) to witryna stworzona nie przez ekspertów od spraw mediów i rozrywki, ale przez nauczycieli. Adresowana jest do dzieci w wieku 5–12 lat. Podczas gdy inne witryny prezentują jakieś materiały i zostawiają miejsce na budowanie „wspólnoty bywalców", Mamamedia dąży do tego, by dzieci same tworzyły zawartość witryny, podejmując różne zajęcia w sieci. Wszystko podporządkowano misji, której celem jest nauczenie dzieci, jak poznawać i wyrażać siebie oraz jak wymieniać poglądy z innymi ludźmi. Są tam unikalne narzędzia, które pomagają dzieciom tworzyć opowieści, z własnymi bohaterami i fabułą. Mamamedia jest ciągle oceniana przez nauczycieli jako jedna z najwartościowszych witryn dla dzieci.

Zeeks (www.zeeks.com) to nowicjusz wsród witryn dziecięcych. Są tam także gry, bezpłatny e-mail i kawiarenka (obecnie przeniesiona do Freezone). Jest też niemało oryginalnych treści, wiele zajęć i pomysłowych propozycji dla dzieci, które chciałyby tworzyć własne strony. Witryna przeznaczona dla dzieci w wieku 6–13 lat. Oferuje również bezpłatne oprogramowanie filtrujące ZeekSafe, które może współpracować z przeglądarką stron WWW.

Wkrótce powinna być już dostępna kolejna witryna, stworzona przez ludzi, którym ufam i których uwielbiam, więc warta wzmianki. SurfMonkey tworzy serwis dla dzieci, pod następującym adresem: www.surfmonkey.com

❖ Specjalne serwisy dla dzieci i młodzieży

Wielu rodziców nie chce, by ich dzieci same buszowały po całym Internecie. Chcieliby za to, by dziecko mogło udać się w bezpieczne miejsce w sieci, bez możliwości przejścia w inne. Nazywam takie miejsca klubami dziecięcymi lub portami docelowymi. Dziecko łączy się z nimi telefonicznie, tak jak my z AOL, i może bezpiecznie serfować po całym wirtualnym ogrodzie zabaw, należącym do nich. Nie ma zagrożenia, że przejdzie na inne strony. Rodzice gotowi są wnosić opłaty, by dzieci mogły korzystać z takich miejsc.

Junior Net

Junior Net to oparty na subskrypcji członkowskiej serwis wyłącznie dla dzieci w wieku 3–12 lat. Kosztuje 9,95 dolarów miesięcznie i nie ma w nim reklam. Często mówi się o nim „dziecięcy Internet". Twórcy gazet i czasopism dla dzieci współpracują z Junior Net i zezwalają na używanie swoich materiałów w zamkniętym środowisku. Junior Net wzbogaca formami interaktywnymi znane i wypróbowane materiały, jak np. ukryte obrazki. Rozbudowuje także własną, specyficzną zawartość, trzymając dzieci z dala od właściwego Internetu, w wydzielonym, bezpiecznym środowisku.

Disney Club Blast (www.disneyblast.com)

Disney Club Blast to specjalny serwis dla subskrybentów w ramach sieci Disney.com, który dostarcza rodzinom najlepszej jakości zawartość w cieszącej się uznaniem formie. Członkowie mogą korzystać z szerokiej gamy aktywności, włączając w to serwis pocztowy D-Mail (czyli disneyowski system przekazywania wiadomości), zamkniętą kawiarenkę dla członków, biuletyny informacyjne, kluby i spotkania ze sławnymi ludźmi przyjaznymi dzieciom. Znajdziecie tam ponad sto interaktywnych gier, powieści, komiksów, gry zespołowe, w których może uczestniczyć jednocześnie do 24 graczy. Dodatkowo Disney Club Blast dostarcza oprogramowanie, które pozwala rodzicom kontrolować komunikację internetową ich dzieci. Karta członkowska w Disney Club Blast kosztuje 5,95 dolarów miesięcznie lub 39, 95 rocznie (członkowie mają też prawo do 10% zniżki przy zakupach w Disney Store).

A kolejne się pojawią...

Cyberspace Kids (www.cyberspacekids.com) to nowo powstały zamknięty system, który posługuje się przeglądarką dla dzieci Crayon Crawler. Noodles (www.noodles.com) i Nickelodeon (www.nick.com) również tworzą zamknięte, bezpłatne przystanie dla dzieci i młodszych nastolatków. Gdy to piszę, te przystanie nie były jeszcze gotowe. Ale ludzie, którzy je tworzą, gwarantują, że będą ciekawe dla dzieci i wartościowe dla rodziców.

Coś z kolumny A, coś z kolumny B

❖ Technologia wspomagająca decyzje rodziców

Obecnie istnieje kilkanaście metod pozwalających rodzicom kontrolować dostęp dzieci do określonych informacji czy miejsc w Internecie. Rodzice mogą zablokować dostęp do konkretnych niestosownych stron czy treści. Mogą też blokować informacje otrzymywane i wysyłane, a także ograniczyć filtrowanie i blokowanie do określonych kategorii treściowych, jak np. narkotyki, alkohol, seks, nienawiść, przemoc i inne, które uznają za szkodliwe dla dzieci. Narzędzia blokujące mogą też zablokować strony, o których z recenzji wiadomo, że zawierają niestosowne treści, podobnie jak mogą zablokować nadchodzące e-maile, krótkie wiadomości i załączniki, a także określone serwisy w Internecie, np. grupy dyskusyjne.

Rodzice mogą używać specjalnego oprogramowania lub narzędzi wspomagających kontrolę rodzicielską, dostarczanych przez dostawców Internetu. Mogą korzystać z rankingu stron WWW tworzonego przez specjalne grupy. Mogą zapisać się na dostawę Internetu filtrowanego w całości lub w określonym zakresie.

Technologia pozwala śledzić drogę dziecka w sieci. Można nawet zapisać każde słowo wysłane lub otrzymane. Istnieją narzędzia ograniczające pole serfowania do sprawdzonych, bezpiecznych obszarów Internetu. Rodzice mogą używać jednego lub wielu tych narzędzi w różnych kombinacjach, by mieć pewność, że znaleźli najlepszy sposób ochrony swego dziecka.

Filtrować czy nie filtrować – oto jest pytanie

Kilka lat temu rodzice mieli do wyboru dwa sposoby posłużenia się technologią, by mieć kontrolę nad tym, gdzie dzieci serfują. Mogli używać oprogramowania filtrującego/blokującego albo mogli wyłączyć komputer. Teraz wszystko jest inaczej.

W ciągu kilku ostatnich lat powstało wiele nowych produktów i serwisów, które mają zwiększyć techniczny arsenał dostępny dla rodziców, dbających o bezpieczeństwo dzieci korzystających z Internetu. Jest obecnie kilka wielozadaniowych programów filtrujących i blokujących. Możesz korzystać ze wszystkich oferowanych przez nie

opcji albo tylko z niektórych. Są programy, które monitorują poczynania i wypowiedzi dziecka w sieci, a następnie dają dokładne sprawozdanie, minuta po minucie, albo tylko uogólniony raport. Inne produkty pozwalają na stworzenie dzieciom pulpitu dostosowanego do ich potrzeb, który może blokować określone funkcje, jak e-mail, i filtruje dostęp do Internetu. Są nawet takie programy do stosowania w domu, które – wykorzystując inteligentne karty – umożliwiają jednemu dziecku dostęp do Internetu, a drugiemu nie. Najważniejsze jednak jest to, że jeśli nie znajdziesz produktu, który by zaspokajał wszystkie twoje potrzeby, możesz wziąć po trosze z wielu, by stworzyć coś naprawdę na własną miarę. (Tylko upewnij się, czy programy, które wybierasz, mogą ze sobą współistnieć). Ale pamiętaj – jeszcze zanim zaczniesz rozglądać się za technologicznymi pomocnikami, naucz swoje dziecko zasad bezpiecznego poruszania się po Internecie i krytycznego myślenia. Wtedy poradzi sobie z treściami, które prześlizną się przez filtry.

Być może zdecydujesz, że technologiczne propozycje to nie jest to, co ci odpowiada i czym chciałbyś się posługiwać. Aby dokonać świadomego wyboru, musisz poznać możliwości tych programów.

Kontrowersje

Posługiwanie się technologią dla obrony dziecka przed nadużywaniem technologii – brzmi jak horror o robotach, które się zbuntowały. I wielu ludzi postrzega posługiwanie się technologią w celu kontrolowania dostępu dzieci do sieci jako rodzaj horroru.

Byłam zaskoczona poziomem kontrowersji wzbudzanych przez sprawę posługiwania się przez rodziców oprogramowaniem filtrującym, które ma wspomagać ich decyzje dotyczące miejsc odwiedzanych aktualnie przez ich dzieci. Nie mogę tego pojąć.

Przeciw korzystaniu z oprogramowania wysuwa się następujące argumenty:

- Programy te nadmiernie blokują, zamykając dostęp do wielu najzupełniej niewinnych stron.
- Programy te niewystarczająco blokują, przepuszczając wiele niestosownych stron.
- Dzieci należy nauczyć, jak radzić sobie z informacjami, a nie nakładać im „klapki na oczy".

- Rodzice nadmiernie polegają na tych narzędziach, zaniedbując inne środki ostrożności, bo sądzą, że to jedyne rozwiązanie.
- Ludzie decydujący o kryteriach blokowania mają swoje uprzedzenia, co odbija się na wyborach, których dokonują.
- Te uprzedzenia mogą nie być jasne dla klientów posługujących się programami czy serwisami.
- Ludzie wybierający strony, które powinny być zablokowane, nie są szkoleni ani nie podlegają nadzorowi, mogą więc niewłaściwie wykonywać swoją pracę.
- Określone treści, dotyczące np. nadużywania alkoholu czy narkotyków przez rodziców albo kazirodztwa, powinny być dostępne dla dzieci bez wiedzy rodziców.
- Dzieci łatwo potrafią „obejść" programy filtrujące.
- Dzieci powinny mieć nieograniczony dostęp do wszystkich legalnie dostępnych informacji – one też mają prawo wolności słowa.
- Kiedy raz dopuścimy używanie jakiegoś rodzaju filtrów, wejdziemy na śliską ścieżkę, która może doprowadzić do państwowej cenzury.

Po pierwsze, należy wiedzieć, że dzieci nie mogą „obejść" oprogramowania filtrującego najnowszej generacji. Zdolny haker poradzi sobie z tym zadaniem, ale na ogół umie on znacznie więcej niż nastoletnie dziecko. Jednak większość programów, jeśli ktoś zaczyna przy nich majstrować, protestuje, wydając informatyczny odpowiednik ostatniego tchnienia, czyli powoduje migotanie ekranu lub wręcz zamknięcie systemu.

Zdolny programista może zrobić prawie wszystko z każdym programem. Ale powiem wam, że zaoferowałam grupom uzdolnionych komputerowo niby-hakerów w trzech szkołach średnich 100 dolarów za złamanie czterech dużych programów filtrujących. I nikt nie wygrał centa. Jeśli chodzi o mnie, to uważam to za przekonujący dowód. (Udowodniono naukowo, że nastolatki zrobią wszystko, co w ich mocy, by zarobić 100 dolarów). Więc jeśli nie chcesz używać żadnych technologicznych narzędzi rodzicielskiej kontroli, dlatego że dzieci łatwo sobie z nimi poradzą, możesz być spokojny. To już nie jest prawda.

Pozostałe zastrzeżenia ciągle są aktualne. Musimy być krytyczni wobec wyrobów, które nie zapewniają tego, co obiecują. Musimy też

być pewni, że rodzice są świadomi mocnych i słabych stron poszczególnych produktów. Mając w głowie te zastrzeżenia, dokonujemy oceny „wielkiej czwórki". Gdy przejdę do podrozdziału poświęconego samym programom, przedstawię pytania, jakie należy zadać, jeśli chce się świadomie wybrać produkt o określonych właściwościach.

Zgadzam się (i sądzę, że większość czytelników się ze mną zgodzi), że zawsze musimy być wyczuleni na cenzorskie zakusy rządu i wszędzie musimy bronić wolności słowa. Ale decyzje rodziców o tym, co ich dziecko może, a czego nie może oglądać, nie mają nic wspólnego z wolnością słowa. To sprawa wychowania.

Te produkty są bez wątpienia bardzo przydatne dla rodziców, którzy potrzebują dodatkowej pomocy, i dla tych, którzy w innym przypadku całkowicie zakazaliby dziecku dostępu do Internetu.

Ale filtrowanie to wybór inny w przypadku każdej rodziny. To także inny wybór w przypadku każdego dziecka. Co jest dobre dla jednego dziecka w rodzinie, może nie być odpowiednie dla pozostałych. To decyzja i wybór rodziców, a nie grup agitujących na rzecz wolności słowa i nie decyzja rządu. Nikt nie powinien czuć się zmuszany do filtrowania lub niefiltrowania. Jednak niektórzy rodzice czują się w jakiś sposób poddani presji.

Pamiętajmy też, że to wybór, który musi być dostosowany do konkretnego dziecka. To co jest dobre dla młodszego dziecka w rodzinie, łamiącego wszelkie zasady, może nie być odpowiednie dla starszego, spokojnego, które nigdy w życiu nie złamało żadnego zakazu. Ale niektóre programy można dostosować do potrzeb więcej niż jednego użytkownika, dzięki czemu można inaczej traktować sześciolatka, a inaczej szesnastolatka.

Napisałam tę książkę, by was, rodziców, wesprzeć. Nie musicie tłumaczyć się innym ze swoich rodzicielskich decyzji. Nikt nie ma nic do powiedzenia na temat tego, jak ubieracie swoje dzieci czy jak je odżywiacie (w każdym razie nie w oczy). Sami musicie dokonywać takich wyborów, jakie uznacie za stosowne.

Programy wzmacniające kontrolę rodzicielską: dodatkowa ochrona

Programy komputerowe służące zapewnieniu bezpieczeństwa dzieciom w Internecie można podzielić na kilka kategorii. Do jednej należą te, które blokują dostęp do „złych stron" albo pozwalają na

otwieranie tylko „dobrych" stron. Określa się je jako oprogramowanie filtrujące i blokujące. Do tej kategorii należą popularne Net Nanny i Cyber Patrol. Ale nowsze typy programów wyposażają dzieci w specjalne, przyjazne pulpity, które mogą więcej niż tylko kontrolować, dokąd dziecko serfuje. Do tej grupy należą Edmark's KidDesk i SurfMonkey. Niektóre programy są darmowe, za inne trzeba zapłacić, ale na ogół nie są to sumy wygórowane

Jakie są możliwości narzędzi technologicznych?

Krótki przegląd właściwości

Większość produktów blokujących pracuje na tej zasadzie, że klasyfikują strony. Dokonują recenzji stron i umieszczają je na liście stron białych/czystych (zawierającej strony przyjazne dzieciom) albo na liście stron czarnych/zakazanych (uznanych za nieodpowiednie dla dzieci na podstawie określonych kryteriów). Program albo pozwala wchodzić tylko na białe strony, albo nie pozwala wchodzić na czarne strony. Ale ponieważ Internet rozrasta się w tempie 200 tysięcy zarejestrowanych stron miesięcznie, nie ma nadziei, że jakaś lista będzie długo aktualna. Z tego powodu większość produktów cenzuruje także słowa lub zwroty, a niektóre nawet filtrują kontekst tych słów, by nie blokować niewinnych zwrotów. (Różnica między filtrowaniem a blokowaniem polega na tym, że blokowane strony są przeglądane i kategoryzowane wcześniej, a filtrowane – w chwili gdy są otwierane). Gdy dzieci próbują wejść na stronę, która jest blokowana lub filtrowana, nie mogą jej otworzyć. Niektóre programy informują, dlaczego nie można jej otworzyć. Na ekranie wówczas pojawia się komunikat, że „strona jest zablokowana przez... (nazwa programu)". Inne pracują w trybie utajnionym (tzn. nie informują, że coś jest blokowane. Dziecko może nawet nie wiedzieć, że taki program jest zainstalowany). Na ekranie pojawia się wiadomość, że wystąpił błąd, uniemożliwiający otwarcie strony.

Wiele programów rejestruje kroki dziecka w wirtualnej przestrzeni: gdzie dziecko było, jak długo, co tam robiło (niektóre zachowują wygląd ekranu w określonych odstępach czasu, inne rejestrują dokładnie, słowo po słowie, co dziecko napisało i otrzymało). Określone produkty mogą też kontrolować, ile godzin (i w jakiej porze dnia) spędza dziecko przy komputerze, nie wchodząc do Inter-

netu. Mogą one też uniemożliwiać korzystanie z pewnych programów (np. gier).

Niektórzy dostawcy usług internetowych oferują własne zastrzeżone produkty, które działają tylko w obrębie ich systemu. Są one bezpłatne.

Istnieją też programy pozwalające na całkowite zablokowanie jakichś typów nadchodzących informacji (takich jak e-maile czy ICQ), na ich filtrowanie (by zablokować spam, zawierający odnośniki do stron porno), wreszcie uniemożliwiające wysyłanie określonych informacji (takich jak adres, imię, nazwisko, numer telefonu). Można też zablokować poszukiwania w Internecie albo ograniczyć je do stron wybranych przez przyjazne dzieciom wyszukiwarki.

Te programy są w określony sposób ustawione przez producenta albo mogą być dopasowane do potrzeb klienta. Im bardziej można je dostosować do indywidualnych życzeń, tym dłuższe i trudniejsze jest instalowanie i uruchamianie ich. Niektóre pozwalają na wybranie różnych poziomów ochrony dla różnych dzieci.

Filtrowanie, blokowanie i monitorowanie – o rany!

Poniżej zamieszczam szczegółowy opis dostępnych obecnie typów zabezpieczeń technologicznych. W dalszej części rozdziału porównuję właściwości najpopularniejszych programów, które sprawdzaliśmy i podaję nasze oceny (zob. tabela). Przedstawiam też rezultaty testów, którym poddaliśmy te programy, używając każdego zgodnie z instrukcją.

❖ Jak one działają

Listy złych stron

Są programy, które blokują dostęp do stron określonych (przez producenta albo przez rodziców) jako niepożądane. Tego rodzaju programy mają listy „złych stron" (regularnie uaktualniane), sporządzone przez producenta, i dostęp do każdej strony wymienionej na liście jest automatycznie blokowany. Niektóre programy pozwalają na dodawanie lub usuwanie stron z listy. Trzeba jednak wiedzieć, że większość producentów oprogramowania nie daje wglądu w swoje listy stron zablokowanych. Net Nanny zasługuje tu na specjalną wzmiankę, bo ujawnia, co blokuje, i pozwala, by klient wprowadził własne modyfikacje. To oznacza, że ty decydujesz, co twoje dziecko może oglądać, nie firma produkująca oprogramowanie filtrujące. Kupując produkt, na ogół dostaje się na jakiś czas prawo do bezpłatnej aktualizacji listy. Koszty uaktualniania po upływie tego okresu są różne, podobnie jak i częstotliwość uaktualniania oraz łatwość instalowania znowelizowanych wersji. Biorąc pod uwagę gwałtowne tempo przyrostu nowych stron (200 tysięcy w ciągu miesiąca) – im częstsze są uaktualnienia, tym lepiej. (Nie trzeba dodawać, że lepiej mieć coś za darmo niż za pieniądze).

Zanim jednak zdecydujesz się skorzystać z tego rozwiązania, musisz wiedzieć, że istniała swego czasu poważna kontrowersja na temat tego, jak „złe strony" są selekcjonowane. Niespójne kryteria, nieodpowiednio wyszkolony – lub wcale nieszkolony – personel recenzujący, brak autentycznej kontroli jakości pracy – może w efekcie prowadzić do tworzenia niewiarygodnych list, zawierających zbyt mało lub zbyt dużo stron. Niektórzy producenci oprogramowania używają najpierw narzędzi technologicznych do przeglądania stron w poszukiwaniu wulgarnego języka, a następnie tak wyselekcjonowane strony są czytane przez człowieka, który ostatecznie decyduje, czy należy je zablokować, czy nie. Ale mimo to wiele najzupełniej niewinnych stron jest blokowanych, celowo lub przypadkowo.

Zwróć się do firmy, której produkt masz zamiar kupić, z prośbą o udostępnienie kryteriów, jakimi posługują się tworząc listy „złych" i „dobrych" stron. Musisz mieć pewność, że zgadzasz się z tymi kryteriami, bo gdy kupujesz produkt blokujący złe strony, to tak naprawdę kupujesz czyjś sąd. Firma, która wybiera treści dla twojego dziecka, powinna wyznawać system wartości podobny do twojego. Mając listę zablokowanych stron, spróbuj do nich dotrzeć i sprawdzić, czy zgadzasz się z klasyfikacją, której dokonała firma. Jeśli się nie zgadzasz, dowiedz się, czy można zmieniać zawartość listy.

Może się zdarzyć, że dziecko, by odrobić lekcje, potrzebuje otworzyć jakąś stronę, a jest ona zablokowana. Wygodniej byłoby mieć produkt, który pozwala na odblokowanie strony, jeśli uznasz, że nie jest szkodliwa dla twoich dzieci. W przeciwnym razie trzeba by zupełnie wyłączyć program filtrujący, aby dziecko mogło dostać się na zablokowaną stronę.

Popatrz na listę zablokowanych stron w poszukiwaniu takich, które sam możesz uznać za wartościowe, np. dotyczących planowania rodziny, AIDS, strony organizacji kobiecych. Listy mogą być obszerne, ale przekopanie się przez nie da ci pojęcia o programie blokującym i jego „skrzywieniach". Nie ma dobrych i złych kryteriów wyboru stron do zablokowania, są tylko kryteria, z którymi się zgadzasz, i takie, z którymi się nie zgadzasz.

Oto kilka pytań, które warto sobie postawić, oglądając listę „złych stron" blokowanych przez program:

- Ile stron jest na liście?
- Jak je wybrano? Według jakich kryteriów? Kto przeglądał te strony? Jaki rodzaj wyszkolenia mają te osoby? Czy istnieje kontrola jakości, jak działa?
- Czy klient ma dostęp do listy? Czy może dodawać lub usuwać z niej strony? Czy zdarza się blokowanie niewinnych stron tylko dlatego, że mogą być kontrowersyjne?
- Czy możesz chcieć, by określone kategorie zostały zablokowane lub odblokowane?
- Jak często uaktualniana jest lista?
- Jak długi jest okres bezpłatnego uaktualniania?

Dostęp tylko do zaaprobowanych „dobrych" stron

Niektórzy producenci, rozumiejąc, że nie są w stanie nadążyć za obecnym tempem tworzenia nowych stron, opowiadają się za listami stron przejrzanych, sprawdzonych i uznanych za przyjazne dzieciom. Każdy producent, dokonując ocen, używa własnych kryteriów, więc strony umieszczone na jednej liście, mogą nie występować na innej.

Stosując listy zaakceptowanych stron, można uniknąć problemów związanych z blokowaniem złych stron, ale jednocześnie niemożność dotarcia do stron, które nie znalazły się na liście, bo nie zdążyły, uniemożliwia dzieciom korzystanie z dobrych nowych witryn. Obecnie jest to może mniejszy problem niż niegdyś, bo listy zaakceptowanych stron rozrosły się i teraz obejmują tysiące wspaniałych i ciekawych miejsc. Ta opcja ma sens zwłaszcza w stosunku do młodszych dzieci, poniżej 10 roku życia.

Ważną cechą list „dobrych" stron w niektórych programach jest możliwość dodania całych list stron „czystych" czy „białych". Producenci również proponują uaktualnianie list przez pewien okres bezpłatnie, później odpłatnie. Problem kontroli jakości doboru stron do listy „dobrych" istnieje tak samo jak w przypadku „złych" stron.

Dokonując wyboru programu zawierającego listę odpowiednich stron, należy postawić sobie podobne pytania, jak wobec list złych stron. W tej opcji szczególnie ważna jest liczba stron na liście, jeśli dziecko ma być ograniczone do korzystania tylko z nich. Nie mniej ważne są kryteria wpisywania na listę. Upewnij się, czy nie wchodzą w grę ukryte motywy polityczne.

Strony oceniane

Listy dobrych i złych stron powstają w wyniku przypisania stronie oceny „odpowiednia" lub „nieodpowiednia" dla dzieci. Ale istnieją też instytucje recenzujące, które dokonują ocen stron, posługując się większą liczbą kryteriów. Dzięki temu oceny mogą być stopniowane oraz zróżnicowane w różnych kategoriach. Odpowiedniość może uwzględniać np. wiek dziecka lub rodzaj zawartości.

Witryny są oceniane przez niezależną instytucję albo dokonują same oceny na podstawie wcześniej ustalonych kryteriów. Od tego momentu strona zyskuje specjalny kod elektroniczny, niewidoczny dla nas, ale odczytywany przez przeglądarkę, która otwiera stronę lub zabrania dostępu do niej, zależnie od wcześniej ustalonych kryteriów selekcji.

System oceniania pozwala na otwieranie dostępu do stron uzyskujących dobre oceny i blokowanie dostępu do otrzymujących złe (na poziomie, który ustawisz na swojej przeglądarce). Dostęp do systemu ocen PICS jest bezpłatny.

Niestety, blokowanie stron „dla dorosłych" czy innych niestosownych nie sprawdza się, bo bardzo niewiele stron „dla dorosłych" i innych niewłaściwych podlega w ogóle jakiemukolwiek systemowi oceny. Jedyną drogą prowadzącą do tego, by przeglądarka wybierała strony wysoko oceniane, jest zablokowanie dostępu do wszystkich stron nieocenianych i do tych spośród ocenianych, które nie uzyskały ustalonego przez rodziców poziomu ocen. A to oznacza, że dzieci miałyby dostęp tylko do dobrych spośród ocenianych stron. Ponieważ obecnie tylko 12 tys. stron jest ocenianych przez RSACi, to posługiwanie się wyłącznie nimi wydaje się nadmiernym ograniczaniem dostępu dziecka do zawartości Internetu.

Dopóki nie będzie tak, że więcej stron będzie podlegało ocenie w tym systemie PICS, zalecamy posługiwanie się innymi narzędziami kontroli rodzicielskiej.

Kluczowe słowa i zwroty

Okazuje się, że pewne słowa i zwroty zazwyczaj występują w większości stron zawierających treści, które chcesz blokować czy przesiewać. Technologia pozwala na zablokowanie dostępu do każdej strony, na której pojawiają się te kluczowe słowa. (Niektóre programy pozwalają na dodawanie lub wymazywanie wyrazów z listy słów kluczowych).

Jednym z większych problemów związanych z filtrowaniem jest to, że niewinne strony mogą zostać niepotrzebnie zablokowane, bo zawierają kluczowe słowa. Dlatego niektóre programy odsiewają tylko strony, na których kluczowe słowa występują w określonym kontekście lub w połączeniu z innymi kluczowymi słowami.

W programach blokujących określone słowa zazwyczaj jako kluczowe wybierane są następujące wyrazy: „tytoń", „palenie", „wino", „narkotyki", „seks", „piersi", różne wulgaryzmy, terminy opisowe i żargonowe na określenie aktywności seksualnej i organów płciowych. Jeśli program nie jest ustawiony tak, by blokować te słowa tylko wtedy, gdy występują w określonym kontekście, może się okazać, że blokuje niepotrzebnie ogromną liczbę stron.

Jednak należy też wiedzieć, że witryny dla dorosłych, wiedząc, jak działa funkcja blokowania, zaczęły pisać z błędami słowa zazwyczaj powodujące zablokowanie strony. Może pojawić się np. penus zamiast penis czy dodatkowa litera na końcu słowa. Trudno uwierzyć, że operatorzy takich stron nie polują też na młodszą publiczność, gdy robią takie rzeczy. Choć, być może, po prostu nie znają ortografii...

Filtrowanie grafiki, niejednokrotnie części przekazu najbardziej nieodpowiedniej dla dzieci, nie jest łatwe. Jeśli na stronie nie występują zarazem jakieś filtrowane słowa, to witryny z naprawdę odrażającymi obrazami, jak np. pornografia dziecięca, zupełnie nie są odsiewane. Choć firmy produkujące oprogramowanie filtrujące pracują nad tym, na razie nie mają zbyt wielkich osiągnięć. To kolejny powód, by uczyć dzieci, co mogą oglądać, a czego nie.

Ostrzeganie

Niektóre programy sygnalizują, że działają, wysyłając informacje, że blokują stronę. Inne blokują dostęp, ale nie dają informacji o przyczynach braku dostępu. Sama nie lubię takiego „utajnionego" stylu działania.

Musisz mieć pewność, że dziecko wie, jakie zabezpieczenia zostały zainstalowane. Internet jest ciągle zbyt nieznanym zjawiskiem, by użytkownicy wiedzieli, że gdy nie mogą załadować jakiegoś pliku, jest to raczej sprawa oprogramowania niż samej sieci. Dzieci mogą strawić wiele czasu, usiłując usunąć problem. Po co je niepotrzebnie frustrować? Poza tym to okazja do porozmawiania o tym, jakie treści mogą być blokowane i dlaczego (znowu można porozmawiać o wartościach). Jeśli mimo to chciałyby obejrzeć coś, co zostało zablokowane, najpierw obejrzyj to sam i jeśli uznasz, że nie ma tam nic złego – również im otwórz dostęp.

Monitorowanie drogi z blokowaniem dostępu lub nie

Niektóre programy z tej grupy zachowują ślad drogi przebytej przez dziecko. Zdają „raport" na temat odwiedzonych stron (niektóre mogą zarazem blokować dostęp). To ta „czapka niewidka", jaka się zawsze rodzicom marzyła. Niektóre produkty zapisują wszystko, zachowując szczegółowy opis nieodpowiedniego języka i odwiedzanych nieodpowiednich stron. Inne wykonują co pewien czas zdjęcie ekranu.

Znowu przypomnienie: dzieci powinny wiedzieć, że są kontrolowane. To sprawa szacunku dla nich i podstawa zdobywania ich zaufania.

Programy, które współdziałają z określonymi serwisami internetowymi

Niektóre programy blokujące pracują tylko w określonych serwisach internetowych, podczas gdy inne pracują we wszystkich. Wprawdzie najpopularniejsi dostawcy usług sieciowych mają własne zestawy narzędzi rodzicielskiej kontroli (większość posługuje się lub opiera na technologii Cyber Patrol), ale możesz chcieć bardziej dopasować te narzędzia do swoich potrzeb niż standardowa oferta. Jeśli korzystasz z bezpośredniego dostępu do Internetu, ta możliwość nie ma dla ciebie znaczenia.

Programy, które mają ograniczać korzystanie z komputera i/lub dostęp do Internetu

Istnieją programy kontrolujące ilość czasu i godziny dnia, w jakich dziecko wchodzi do Internetu. Pozwalają też często na limitowanie czasu i określenie godzin, w jakich dziecko może grać w gry komputerowe, wchodzić w określone pliki czy uruchamiać jakiś napęd. Może to być darem niebios dla pracujących rodziców, którzy nie mają opieki do dziecka po jego powrocie ze szkoły. Program taki trzyma je z dala od sieci do powrotu rodziców do domu. Pomoże też trzymać je z dala od finansowych i innych ważnych plików.

Programy, które można dostosować do potrzeb więcej niż jednego dziecka w tym samym czasie

Niektóre programy pozwalają na wprowadzenie różnych ustawień dla różnych dzieci w domu. Inaczej rodzice byliby zmuszeni do używania programów, które czternastolatka skazują na taki sam poziom kontroli jak sześciolatka. Kluczem do sukcesów w stosowaniu narzędzi kontroli rodzicielskiej jest dopasowywanie ich do konkretnego dziecka. Jeśli masz więcej niż jedno dziecko, zaopatrz się w produkt, który pozwala na wprowadzenie różnych ustawień dla różnych dzieci.

Przesiewanie przychodzących wiadomości

To bardzo istotna cecha. Wiele zagrożeń w dzisiejszych czasach dostarcza się nam wprost do domu. E-maile mogą zawierać kody HTML, które łączą bezpośrednio ze stronami dla dorosłych. Ludzie, z którymi dziecko nie powinno się kontaktować, mogą je złapać e-mailem i przysyłać mu wiadomości, których nie powinno odbierać. Przesiewanie nadchodzących wiadomości filtruje wszystkie e-maile, ISQ i inne wiadomości wysyłane w czasie rzeczywistym. Gdy dzieci używają już e-mailu na własny rachunek, może to być ważne narzędzie ułatwiające zatrzymanie niepożądanych informacji, jak reklamy, czy zablokowanie konkretnych nadawców lub wiadomości.

Przesiewanie wysyłanych wiadomości

Gdybym miała wybrać pojedynczą opcję, która jest najważniejsza dla bezpieczeństwa dziecka korzystającego z sieci, byłaby to właśnie ta. Przesiewanie wychodzących wiadomości zapobiega temu, by dziecko przekazało komuś numer telefonu, adres czy inne poufne dane. Jest to szczególnie pomocne w przypadku młodszych dzieci, które łatwo można namówić do wyjawienia personalnych informacji, których obiecały nie ujawniać. Nie pozwala im to też na wypełnianie większości formularzy subskrypcyjnych, wymaganych przez niektóre witryny dla dzieci. Będą potrzebowały pomocy rodzica, żeby to zrobić, więc będziesz wiedział, jakie informacje na temat dziecka i rodziny mają te witryny.

Opcja ta funkcjonuje tak, że dodajesz informacje personalne do listy słów kluczowych, które powodują blokowanie. Musisz jednak być dość sprytny i podać te informacje w kilku możliwych wersjach, np. numer telefonu może być 826-66-66, ale równie dobrze dziecko może napisać go w sposób następujący: 0- 4812-826-6666 albo (48)12 8266666. Choć musisz też wiedzieć, że gdy dziecko chce przekazać jakieś informacje, może obejść blokadę, umawiając się z kimś z czatów, że gdy używa numeru 6 – chodzi o 1, a gdy 4 – chodzi o 8 i zapisać numer umówionym „szyfrem". Jeśli sądzisz, że twoje dziecko mogłoby chcieć coś podobnego zrobić – rozważ nabycie oprogramowania takiego jak Cyber Snoop lub Disk Tracy, które pozwala monitorować wszystko, co dziecko mówi, gdy jest w Internecie.

❖ Blokowanie na poziomie serwera

Blokowanie lub filtrowanie przez serwer ma miejsce wtedy, gdy narzędzia kontroli rodzicielskiej zainstalowane są w serwerze dostawcy dostępu do Internetu (ISP) lub usług internetowych, nie w twoim komputerze. Tym sposobem blokowanie zachodzi u źródła. Rodzice nie muszą się martwić o uaktualnianie list czy instalowanie programów. Ale programy te nie będą dopasowane do potrzeb indywidualnego klienta.

Bess

Bess to program filtrujący instalowany na serwerze dostawcy Internetu. Podobno jest używany przez szkoły częściej niż jakiekolwiek

inne narzędzie filtrujące. Bess jest kupowany przez dostawcę Internetu i następnie oferowany jako narzędzie kontroli rodzicielskiej albo sprzedawany szkołom lub publicznym lokalnym centrom internetowym, które oferują dostęp do sieci przez serwery, na których zainstalowany jest Bess. Nie wymaga to instalowania niczego, ale nie może być dopasowywane do potrzeb rodziców. Bess filtruje przychodzące i wychodzące e-maile i materiały z grup dyskusyjnych oraz uniemożliwia dostęp do jakichkolwiek kawiarenek. Jest łatwy w użyciu, bo, jak inne narzędzia rodzicielskiej kontroli w AOL, trzeba go tylko włączyć i już działa. Nic nie trzeba konfigurować. Poza tym Bess jest automatycznie uaktualniany.

Filtrowany dostęp do Internetu

Niektórzy dostawcy usług internetowych oferują tylko dostęp jakoś filtrowany. Chodzi najczęściej o dostęp do sieci oferowany przez grupy religijne lub inne o szczególnych zainteresowaniach. Jest to w porządku, jeśli klient zna ich nastawienie i stosowane kryteria filtrowania.

❖ Narzędzia kontroli rodzicielskiej dostarczane w serwisach sieciowych

Każdy z dostawców usług internetowych oferuje jakiś rodzaj narzędzi rodzicielskiej kontroli bez żadnych dodatkowych opłat. Charakteryzują się one różnym poziomem restrykcyjności, od takich, które umożliwiają dostęp tylko do obszarów dla dzieci i nastolatków, przez blokujące e-maile i wiadomości wysyłane w systemach IM. A niektórzy ISP dostarczają nawet Cyber Patrol (lub jego pochodne) do użytku abonentów.

❖ Kilka słów o specjalnych ofertach

Dokładnie przeanalizowaliśmy cztery najbardziej popularne na rynku programy pełniące rolę narzędzi kontroli rodzicielskiej: Cyber Patrol, CYBERsitter, Net Nanny i SerfWatch. Oddzielnie omawiamy też kilka innych produktów, a mianowicie te, które tylko monitorują aktywność w sieci, przeglądarki i specjalne pulpity dla dzieci, które odsiewają zawartość lub ograniczają dostęp do określonych stron.

KidDesk Internet Safe

Edmark to główna firma produkująca programy edukacyjne. KidDesk to specjalny pulpit, do zaprogramowania którego spożytkowano całe doświadczenie, jakie firma Edmark może zaoferować dzieciom. Dzieci mogą wysyłać e-maile tylko w swoim domu – do rodzeństwa, rodziców. Mogą też wybierać wygląd pulpitu. Rodzice mogą umożliwić dzieciom odwiedzanie zrecenzowanych i zaaprobowanych wcześniej stron i mogą dodawać nowe strony do swojej listy. Dzieci lubią ten program, a rodzice mu ufają. To doskonała kombinacja. Istnieje też uboższa, darmowa wersja KidDesk. Możesz ją odnaleźć pod adresem: www.edmark.com/prod/kids/download.

Surf Monkey

Uwielbiam Surf Monkey i dzieci też uwielbiają. Ma specjalną opcję pozwalającą, by rodzice przeglądali każdy e-mail, zanim zostanie przekazany dzieciom. Umożliwia zablokowanie wszystkiego, oprócz określonych wcześniej stron. Młodsze dzieci szczególnie lubią Surf Monkey, animowaną postać, która czyta głośno ich e-maile, jeśli same nie mogą lub nie chcą ich czytać.

Na początku były pewne problemy z tym programem, bo za bardzo wyprzedzał swoją epokę. By korzystać z niego bez trudności, potrzebny jest odpowiedni sprzęt – producent zaleca procesor Pentium 133, ja zalecałabym przynajmniej Pentium 200 MMX lub lepszy. Ale jeśli dysponujesz odpowiednim sprzętem, niewiele jest równie dobrych programów. Oto opinie kilku użytkowników:

Chłopiec, lat 10 i pół: „Lubię używać Surf Monkey. Mam dzięki temu swój własny adres e-mailowy. Podoba mi się to, że można głosować na ulubione zabawy. W tym tygodniu trzeba było wybierać ulubionego Pokemona. Mogę oglądać mnóstwo fajnych stron dzięki temu programowi".

Chłopiec 7 i pół roku: „Podoba mi się, jak małpa do mnie mówi. Podpowiada mi, co robić. Mogę znaleźć dużo ciekawych miejsc i zabawnych rzeczy dzięki temu".

Dziewczynka, lat 9: „Uwielbiam małpkę. Ona nawet może czytać mi moje e-maile. Mam swój własny obrazek na ekranie, bardzo fajny. Mogę też chodzić na pogawędki, a mama i tata pozwalają mi tam być. Ale prawdziwy powód, że to lubię, to ten, że to jest właśnie dla mnie, akurat mój styl i typ, i rodzice pozwalają mi robić tam wszystko, co chcę".

Matka: „Ta przeglądarka jest bardzo dobra dla młodych ludzi, takich, którzy dopiero uczą się poruszania się po sieci. Surf Monkey pomaga dzieciom nauczyć się korzystać z Internetu, a Cybot – pomaga rodzicom w sprawowaniu kontroli. Przeglądarka oferuje mnóstwo ciekawych zabaw dla dzieci, oprócz tego dziecko może dostać własny adres e-mail. Wychodzące i przychodzące wiadomości są przesiewane pod kątem zawartości wulgaryzmów. Rodzice mogą zdecydować, czy dziecko będzie miało dostęp do e-mailu i czatów, czy nie. Ten program na pewno pozostanie w moim komputerze, dopóki moje najmłodsze dziecko nie będzie na tyle duże, by posługiwać się normalną przeglądarką".

Co jeszcze można dodać? Tylko dwie rzeczy. Można przegrać produkt pod adresem www.surfmonkey.com i – wierzcie lub nie – jest on bezpłatny! Surf Monkey ma też nową wersję mniej wymagającą. Nazywa się Sufr Monkey Bar, i podobnie jak Surf Monkey jest bezpłatna i dostępna w Internecie. To raczej pasek narzędzi niż pulpit czy przeglądarka. Wymaga mniej pamięci niż normalna wersja programu. I współpracuje z Microsoft Internet Explorer 5.0. Poza tym ściąga się go w ciągu kilku minut, co potrafią docenić ci, którzy wiedzą, jak to jest, gdy ściąganie pliku trwa całą wieczność. Masz go stale na pulpicie i ustawiasz tak, by używał go każdy lub tylko dzieci. Czy wybierzesz przeglądarkę, czy pasek narzędzi, powiem tylko jedno: spróbuj, a polubisz ten program.

ZeekSafe

ZeekSafe ma również wersję w postaci paska narzędzi. Jest na pulpicie i filtruje nieodpowiednie strony, używając firmowego programu. ZeekSafe blokuje około 100 tys. stron. Jest on również bezpłatny i łatwy do zainstalowania. Można go pobrać pod adresem: www.zeeks.com.

Oferta firmy ClickChoice: myFilter

ClickChoice oferuje nowy produkt – myFilter – służący do filtrowania. Ten program do darmowego używania podobno monitoruje 100 milionów stron WWW i kategoryzuje je jako stosowne dla dzieci (do lat 12), dla nastolatków (do 17 lat) i dla dorosłych.

ClickChoice przesiewa strony WWW, używając technologii filtrowania, by wykryć te, które zawierają terminy nie do przyjęcia. Następnie recenzenci stron (których wedle firmy są tysiące) przeglądają zakwestionowane i sprawdzają, czy ich zawartość słusznie budzi sprzeciw.

ClickChoice, oceniając strony, bierze pod uwagę następujące kategorie treściowe: pornografia, bluźnierstwo, pirotechnika, wypowiedzi szerzące nienawiść lub zachęcające do nienawiści, alkohol, tytoń, narkotyki, hazard, gwałt. Program można załadować za darmo (po udzieleniu kilku informacji) pod adresem www.clickchoice.com.

Co się pojawia nowego?

W czasie pisania tej książki pojawiły się nowe bezpłatne programy filtrujące. Wydaje się nam, że obiecująco wygląda Crayon Crawler, który można za darmo pobrać pod adresem www.crayoncrawler.com.

❖ Czapka niewidka: programy monitorujące

Disk Tracy, Kids Cam i Cyber Snoop

Te trzy programy monitorują wszystko, co twoje dziecko powie w Internecie. Podczas gdy Net Nanny i CYBERsitter dają sprawozdanie ze stron, które dziecko odwiedzało, programy wymienione tutaj zapisują każde słowo dziecka. Disk Tracy i Cyber Snoop mają też inne możliwości, takie jak blokowanie i filtrowanie.

Kids Cam działa nieco inaczej. Utrwala obraz ekranu w określonych interwałach czasowych, udostępniając go następnie rodzicom.

Choć te programy mogą przekazać ci informacje o wypowiedziach twojego dziecka, większość osób, z którymi rozmawiałam, odbiera je jako zdecydowanie zbyt dużą ingerencję.

❖ Waga ciężka: wielka czwórka

Porównanie produktów

Te cztery wielkie programy to Cyber Patrol, CYBERsitter, Net Nanny i SurfWatch. Sądzimy, że wiedza o tym, czym te produkty różnią się od siebie i jak wypadły w naszych testach, może się czytelnikom przydać.

Jak prowadziliśmy nasz przegląd i testy programów

Próbowałam w tej książce nie wyrażać się jak prawnik, ale niestety, muszę na chwilę przywdziać swoją togę. Chcę, żeby czytelnik wiedział, co nasze badanie odzwierciedla, a czego nie. Żeby to pokazać, opisałam warunki przeprowadzania testów i sposób uzyskiwania wyników. Twoje doświadczenia mogą być inne niż nasze.

	Program	Cyber Patrol 4	CYBERsitter 99	Net Nanny 4	SurfWatch 3,0
Uaktualnienie programu	Częstotliwość	Co tydzień	Co tydzień	Codziennie	Codziennie
	Łatwość obsługi	automatycznie	automatycznie	automatycznie	Przycisnąć jeden przycisk
	Koszty	3 m-ce za darmo	darmowo	zawsze bezpłatnie	6 m-cy bezpłatnie
Program	Zabezpieczenia	podwójne hasło	podwójne hasło	potrójne hasło	jedno hasło
	Tryby pracy	niejawnie lub jawnie	tylko niejawnie	niejawnie lub jawnie	tylko jawnie
	Liczba różnych użytkowników	9	1	12	1
Zakres filtrowania	Kategorie tematyczne	• Alkohol, papierosy i hazard • Edukacja seksualna Terroryzm/ ekstremizm • Narkotyki/ kult narkotyków • Satanizm/kult • Przemoc/ bluźnierstwa • Częściowa nagość • Pełna nagość • Akty seksualne tekst i grafiki • Wulgarne powiększenia organów płciowych • Nietolerancja	• Dla dorosłych/ seksualnie zorientowane • Zaznaczone przez PICS jako dla dorosłych/ przemoc • Nienawiść/ nietolerancja • Papierosy/ alkohol • Broń/ przemoc • Kulty/ okultyzm • Homoseksualizm • Gry oparte na przemocy • Hazard • Zakazane działania/ narkotyki *CYBERsitter oferuje też do wyboru filtrowanie 14 innych dziedzin*	• Dla dorosłych • Hazard • Narkotyki/ alkohol • Przemoc • Nienawiść • Akty kryminalne • Pedofilia • Pornografia dziecięca	• Narkotyki/ alkohol/ tytoń • Hazard • Nienawiść • Seks • Przemoc *SurfWatch oferuje także dodatkowo filtrowanie w zakresie wybranych 15 kategorii*

Blokuje i filtruje	Informacje wychodzące	✓	✓	✓	✗
	Strony WWW/URL/IP	✓	✓	✓	✓
	Kluczowe słowa/zdania	✗	✓	✓	✓
	Związki frazeologiczne	✗	✓	✓	✓
	Wyszukiwarka	✓	✓	✓	✓
	Grupy dyskusyjne	✓	✓	✓	✓
	Aplikacje do czatów	✗ (oprócz IRC)	✓	✓	✓
	Obsługuje system ocen PICS	✓	✓	✓	✓
	ICQ/IM	✗	✓ Filtruje słownictwo albo blokuje całą aplikację	✓ Filtruje język albo blokuje w całości	✗
	E-mail	✗	✓ Filtruje wszystkie wiadomości tekstowe	✓ Filtruje wszystkie wiadomości tekstowe	✗
Inne	Monitorowanie dziecka	✗	✓	✓	✗
	Kontrola czasu	Trwanie i oznaczone godziny	Trwanie i oznaczone godziny	Trwanie i określone godziny	✗

Jakie programy wybraliśmy do różnych testów

Wybraliśmy cztery różne marki programów do sprawdzenia funkcji blokowania stron oraz pełnego testowania własności: Cyber Patrol (wersja 4.0), CYBERsitter 99, Net Nanny (wersja 4.0) i SurfWatch (wersja 3.0). Wszystkie inne produkty wymienione w tej książce zostały sprawdzone w zakresie, o jakim wspomniano w książce (np. jeśli mówimy, że jakiś program monitoruje korzystanie z Internetu, to ta cecha była sprawdzana).

Staraliśmy się wybrać najczęściej nabywane programy, ale wiele firm odmówiło ujawnienia danych na temat rocznej sprzedaży lub

sprzedaży do chwili zbierania danych. Wydaje się, że wybrana czwórka należy do najpopularniejszych programów. Sposród nich Net Nanny jest na rynku najdłużej. Pierwsza wersja została wprowadzona w 1995 roku. SurfWatch wypuścił swój pierwszy produkt kilka miesięcy później. SurfWatch podaje, że ma największą liczbę użytkowników (mniej więcej trzy i pół razy więcej niż najbliższy rywal). Cyber Patrol wydaje się zdobywać rynek usług, wchodząc nań z określonymi ISP. SurfWatch wydaje się robić to samo w odniesieniu do rynku dziecięcego – filtrowane wyszukiwarki, bezpieczne porty i zamknięte systemy. Nowy produkt Net Nanny dopiero wejdzie na rynek, na potrzeby tej książki testowaliśmy go przed oficjalnym rozpoczęciem sprzedaży. Jest o tyle lepszy od swojej poprzedniej wersji, iż spodziewam się, że nastąpi znaczący wzrost sprzedaży i przejęcie części rynku Cyber Patrol i SurfWatch.

Jak przeprowadzaliśmy testy

By przetestować każdy z programów, instalowaliśmy je zgodnie z instrukcją producenta i używaliśmy ustawień standardowych (takich, jakie ustawił producent). Każdy był sprawdzany na tym samym komputerze Pentium 200 MMX, z 32 MB pamięci RAM i modemem 28.8 kbps (niektóre były sprawdzane dodatkowo na sprzęcie Pentium 133, 24 MB RAM z modemem 28.8 kbps). Systemem operacyjnym komputerów był Windows 95. Programy instalowano po jednym w danym czasie i usuwano po zakończeniu testów, przed instalacją kolejnego programu. Wszystkie testy prowadziła ta sama osoba, z wyjątkiem „przepuszczania" przez listy stron, by sprawdzić, które z nich program blokuje, których nie. Każdy program był sprawdzany na stronach wybranych losowo, sklasyfikowanych na podstawie zawartości. Wyłoniono osiem kategorii stron, wśród nich szereg dobrych stron, zawierających określone hasła, takie jak „seks", „narkotyki", i siedem kategorii o problematycznej zawartości, np. budowanie bomb, alkohol, tytoń, nienawiść, przemoc, seks, satanizm, sekty. (Lista stron użytych w testach została przekazana producentom programów, by mogli je zrecenzować i podjąć stosowne działania).

Dodatkowo przy pomocy każdego programu przeprowadziliśmy test poszukiwania szkodliwych stron, związanych z innymi niż seks tematami, które miały być blokowane lub filtrowane przy ustawieniach standardowych (np. alkohol, narkotyki).

Serfowaliśmy, korzystając z każdego z programów, sprawdzając jego skuteczność w odniesieniu do testowanych witryn i połączonych z nimi miejsc, ale w ocenie skuteczności wzięliśmy pod uwagę tylko testowane strony.

Orkiestra, tusz! Wyniki testu: jak spisała się wielka czwórka

Programy filtrujące najczęściej krytykuje się z tego powodu, że blokują nadmiernie, tzn. blokują niewinne strony. Testowaliśmy programy na listach „dobrych" stron, by sprawdzić, jak często blokowały niewinne strony. Wszystkie aplikacje wypadły zaskakująco dobrze. Niektóre nie zablokowały żadnej niewinnej strony. Cyber Patrol zablokował cztery, dwie z nich to strony Uniwersytetu Columbia, polecane przez Amerykańskie Towarzystwo Bibliotekarskie, ale przez innych uznawane za kontrowersyjne ze względu na język i sposób przedstawiania tematów: seks i używanie narkotyków.

Dla mnie samej rezultaty były zaskoczeniem, bo gdy testowałam te produkty dwa lata wcześniej (inne wersje oczywiście), blokowały niepotrzebnie znacznie więcej stron.

Z czterech testowanych programów najlepiej wypadły w tym zakresie Net Nanny i SurfWatch, bo nie zablokowały żadnej z „dobrych" stron. CYBERsitter plasuje się na następnym miejscu, zablokowawszy tylko jedną stronę (dotyczącą edukacji narkotykowej). Cyber Patrol zablokował cztery, trzy dotyczące edukacji zdrowotnej i jedną – narkotyków. Ale z czterdziestu pięciu testowanych stron to niewiele.

Sądzę, że poziom doskonałości programu zależy od czasu jego obecności na rynku i zakresu zebranych w związku z tym doświadczeń. Im dłużej programy są na rynku, tym wyższy poziom osiągnęli ich producenci. Mieli więcej okazji do wymiany doświadczeń ze szkołami, bibliotekami i rodzicami, więc dzisiejsza zdolność do nieblokowania stron niewinnych jest efektem wielu prób. Kiedy chodzi o blokowanie i filtrowanie, to w mniejszym stopniu jest to sprawa technologii, w większym – doświadczenia. A testowane przez nas programy to najdłużej udoskonalane produkty.

Ponadto sprawdzaliśmy, czy wymienione programy blokują „złe strony" należące do różnych kategorii. Sprawdzaliśmy je na stronach zawierających informacje o budowaniu bomb, alkoholu i papierosach, szerzących nienawiść, przemoc, zawierających jawnie seksualne tre-

ści i propagujących satanizm. W tabeli przedstawione są wyniki tego testowania w różnych kategoriach:

	CYBERsitter 99	Cyber Patrol 4.0	Net Nanny 4.0	SurfWatch 3.0
Budowa bomb	5 z 20	12 z 20	7 z 20	12 z 20
Alkohol	0 z 18	15 z 18	0 z 18	17 z 18
Tytoń	2 z 18	2 z 18	0 z 18	10 z 18
Nienawiść	6 z 18	12 z 18	11 z 18	13 z 18
Przemoc	4 z 12	4 z 12	6 z 12	5 z 12
Treści jawnie seksualne	18 z 19	17 z 19	17 z 19	15 z 19
Satanizm i inne kulty	5 z 14	4 z 14	7 z 14	4 z 14

Jak to interpretować?

Mieliśmy bardzo mały zbiór stron, na których testowaliśmy produkty. Początkowo po dwadzieścia stron w każdej kategorii, ale niektóre były niedostępne lub zostały zlikwidowane w okresie między kompletowaniem listy a przeprowadzaniem testu. Takie warunki badania nie pozwalają przewidzieć, jak zachowa się program wobec rozległej bazy internetowej, ale wiemy, jaki rodzaj treści niepożądanych blokuje najlepiej. SufrWatch blokował najwięcej stron w największej liczbie kategorii. (Ciekawe, że dwa lata temu również SurfWatch najlepiej wypadł w naszych testach).

Te nasze testy były przeprowadzane na małej próbce i wyniki mogą nie być miarodajne w odniesieniu do dużej liczby stron. Inne grupy także przeprowadzały badania i możesz zapoznać się z ich wynikami. Cyberangels mają listę aprobowanych programów filtrujących i własne oceny tych programów na swojej stronie www.cyberangels.org. Publikujemy również bardzo obszerną listę programów i ich recenzje w www.familyguidebook.com i www.wiredkids.org.

Nie podejmuj jednakże decyzji wyłącznie na podstawie naszych ocen. Wszystkie firmy dostarczają wersji demo programu. Możesz je samodzielnie wypróbować i podjąć własne decyzje. Ale bądź ostrożny, bo Cyber Patrol i CYBERsitter poinformowały nas, że ich programy nie pracują prawidłowo, jeśli zainstaluje się je na komputerze, na którym już są inne programy filtrujące, nawet jeśli aktywny

jest tylko jeden. (W instrukcji dołączonej do programu nie ma wzmianki o tych problemach. Sugerowałam, by dołączyli takie ostrzeżenie). To dlatego instalowaliśmy programy jeden po drugim. Proponujemy, by czytelnicy tak samo testowali wersje demo różnych programów.

❖ Wybierz własną drogę

W tym rozdziale przedstawiłam możliwości, które rodzice mają do dyspozycji, od czystych działań wychowawczych do technologicznych zabezpieczeń, z całą gamą rozwiązań pośrednich. Przeprowadziłam krótki przegląd metod ochrony, jakie rodzice mogą zastosować, od opierania się na zaufaniu do dziecka i edukowania go, do całkowitego zakazu korzystania z komputera. Musimy mieć świadomość, że wprowadzając większą kontrolę, bardziej ograniczamy zakres informacji dobrych i złych, do których dziecko może się dostać, mniej opieramy się na zaufaniu do niego. Ponadto im bardziej ograniczamy dostęp do różnych miejsc i usług, tym więcej wyborów pozostawiamy w rękach osób trzecich. (Dlatego ważne jest, byśmy zgadzali się z dokonanymi przez nich wyborami). Każdy musi sam wyważyć te sprawy. To ma być twój wybór. Ale trzeba pamiętać, że nie jest on dokonany raz na zawsze – możesz i powinieneś wprowadzać zmiany, w miarę jak dzieci dorastają, zdobywają twoje zaufanie i rośnie ich potrzeba dostępu do szerszego zakresu treści.

Oto, w dużym skrócie, te wybory:

Poziomy kontroli i zabezpieczenia

(w porządku wzrastającym)

- Zaufanie i edukacja.
- Domowy kontrakt bezpiecznego serfowania (patrz załącznik nr 3).
- Zachęcanie do korzystania z przyjaznych dzieciom witryn, nadzorowanie serfowania.
- Oprogramowanie zapisujące długość serfowania i odwiedzane strony.
- Filtrujące wyszukiwarki.
- Filtrowanie i blokowanie na pulpicie.

- Blokowanie na poziomie serwera, narzędzia rodzicielskiej kontroli na poziomie serwisów sieciowych lub filtrowany przez ISP dostęp do Internetu.
- Dostęp wyłącznie do przyjaznych dzieciom „placów zabaw" w sieci.
- Dostęp wyłącznie do przyjaznych dzieciom serwisów subskrybowanych (dla członków).
- Zamykanie komputera (lub zastosowanie programu uniemożliwiającego dostęp do Internetu) na czas nieobecności rodziców w domu.
- Zamieszkanie w wolnym od komputerów środowisku.

Zauważ, że nie ma sposobu, by mieć pewność, że dziecko jest w stu procentach bezpieczne – jeśli nie mieszka się w miejscu, gdzie komputerów nie ma ani w szkole, ani w bibliotece, ani u kolegów. Ponieważ jest to prawie nieprawdopodobne, a jeszcze bardziej niepożądane, każdy musi zaakceptować pewien poziom odpowiedzialności za przebywanie w wirtualnej przestrzeni i za to, że mogą zdarzyć się rzeczy, których nie chcemy. Musimy nauczyć się żyć z tym ryzykiem. Próbujemy je minimalizować, ale w jakimś stopniu musimy zaakceptować.

Rozdział 9

A teraz słowo od prawdziwych ekspertów – dzieci i nastolatków

Od trzech lat co tydzień spotykam się z grupami uczniów. Myślę, że rodzice i nauczyciele potwierdzą, że ilekroć rozmawiamy z dziećmi (i słuchamy ich), mamy szansę czegoś się dowiedzieć. Czasem nawet można się nauczyć czegoś pożytecznego.

Włączyłam ten rozdział do książki, by podzielić się tym, czego nauczyłam się od dzieci i nastolatków. Być może usłyszysz tu echo wypowiedzi swojego dziecka lub jego przyjaciół. By znaleźć rozwiązanie problemu bezpieczeństwa w sieci dla swojej rodziny, musisz wiedzieć, co myślą dzieci. Najlepszą drogą jest rozmawianie z nimi. Wspólne przeczytanie tego rozdziału może pomóc im otworzyć się.

Rozdział składa się z czterech części. W pierwszej, „Zasady? – to nie dla mnie!", przekazuję, co dzieci powiedziały nam o swoich zachowaniach w Internecie i ryzyku, które podejmują. Wypowiedzi pochodzą z ankiety, którą przeprowadziliśmy razem z internetową edycją pisma „Seventeen Magazine", uzyskując odpowiedzi od prawie 11 tysięcy nastoletnich dziewcząt. Potem następuje część „Mogłyby napisać tę książkę za mnie". Podaję w niej pomysły dotyczące sposobów zachowania bezpieczeństwa, przekazane przez same respondentki. Trzecia część „Szanowny Panie Prezydencie" to sądy i spostrzeżenia dotyczące Internetu, przemocy w szkołach i mediach, jakimi podzielili się ze mną uczniowie śródmiejskich szkół średnich. Mogą wielu zaskoczyć – mnie zaskoczyły. Ostatnia część, moja ulubiona, „Teenangels", dotyczy moich Teenangels, specjalnej grupy na-

stolatek, które zostały wyszkolone w kwestiach bezpieczeństwa w sieci i teraz działają w szkołach w całym kraju jako rzeczniczki idei bezpiecznego serfowania, inicjując tworzenie programów i ucząc innych nastolatków roli szkolnych ekspertów w sprawach bezpieczeństwa w sieci. Dzielą się własnymi przemyśleniami i pomysłami na zachowanie bezpieczeństwa z innymi nastolatkami, z dziećmi poniżej dziesiątego roku życia i z rodzicami. Kilka naszych szkolących się „aniołków" spisało własne porady dla rodziców – przytaczam je dosłownie, z oryginalną pisownią i gramatyką.

„Zasady? – to nie dla mnie!"

Nasze pierwsze ankiety skierowaliśmy do około sześciu tysięcy rodzin w okręgu Baltimore. Potem przeprowadzaliśmy badania uczniów szkół średnich, prosząc ich o przedstawienie swojej wiedzy na temat zasad zachowania bezpieczeństwa w sieci, a także o opisanie własnych zachowań w Internecie. Prosiliśmy ich również o podanie trzech wskazówek dotyczących bezpieczeństwa, które przekazaliby swoim przyjaciołom zaczynającym korzystać z Internetu. Wyniki były intrygujące, bo porównując odpowiedzi na te pytania, doszliśmy do wniosku, że młodzież ustala inne zasady dla siebie, a inne dla kolegów. Szczególnie jedna odpowiedź zawsze przychodzi mi na myśl. Uczniów poproszono o napisanie eseju wyjaśniającego młodszym kolegom podstawowe zasady bezpiecznego korzystania z Internetu. Większość napisała, że bardzo ważne jest nieujawnianie własnego nazwiska, adresu, telefonu. Pewna siódmoklasistka napisała:

„Sądzę, że musisz pamiętać o kilku zasadach:

1. Kiedy wchodzisz do kawiarenki, nigdy nie podawaj obecnym tam osobom swojego nazwiska, adresu lub numeru telefonu, *chyba że czujesz się bezpiecznie.*
2. Nigdy nie zgadzaj się na spotkanie z kimś, *chyba że znasz jego życiorys.*
3. Nigdy nie jedź *poza miasto* z osobą, z którą nie czujesz się bezpiecznie".

Moje podkreślenia pokazują, jak dzieci poszukują luk i wyjątków (sądzę, że wszystkie zostaną prawnikami). Być może zainteresuje was,

że ta konkretna siódmoklasistka przyznała się, że przekazała komuś w sieci swoje nazwisko, imię, adres i numer telefonu.

❖ Bez nich nie byłoby tych badań

Pod koniec 1998 roku spotkałam (tak naprawdę było to spotkanie wirtualne) dwoje znanych naukowców z Uniwersytetu Południowej Florydy, dr. Michaela Bersona i dr Ilene Berson. Oni również są ekspertami w kwestiach bezpieczeństwa, napisali wiele prac na ten temat. Zdecydowaliśmy się podjąć współpracę. Na początek postanowiliśmy przeprowadzić badania polegające na zebraniu własnych ocen nastolatków, a internetowa edycja młodzieżowego pisma „Seventeen Magazine" udostępniła swoje łamy dla naszych ankiet. Wyniki były zastanawiające, choć potwierdzały to, co słyszałam przez lata przy okazji spotkań i pogadanek.

❖ Ankieta w „Seventeen Magazine"

Mniej więcej połowa badanych dziewcząt podała, że ma 14 lub 15 lat. Następne 32% stanowiły osoby, które zadeklarowały, że mają 13 lub 16 lat. Wszystkie badane osoby oświadczyły, że są płci żeńskiej. Oto czego się dowiedzieliśmy:

- 60% respondentek wypełniało w Internecie kwestionariusze lub formularze, które zawierały pytania o dane osobowe, takie jak: nazwisko, adres, data urodzenia, telefon, nazwa szkoły.
- 12% wyraziło zgodę na osobiste spotkanie z kimś, kogo poznały w sieci.
- 45% przekazało komuś, kogo poznały w Internecie, dane osobowe, takie jak prawdziwe nazwisko, wiek lub data urodzenia, adres, telefon lub nazwa szkoły.
- 61% otrzymało zdjęcia od kogoś poprzez Internet.
- 23% wysyłało zdjęcia do kogoś, kogo poznały w cyberprzestrzeni.
- 15% otrzymało e-maile z sugerującymi coś lub grożącymi czymś komunikatami, z którymi nie czuły się dobrze.
- 3% wysyłało podobne wiadomości.
- 30% bywało w takich kawiarenkach, w których dyskusja sprawiała, że czuły się źle.

- 2% wertowało strony poświęcone budowaniu bomb.
- 30% czytało w Internecie treści pełne nienawiści.
- 15% zetknęło się w Internecie z groźbami przemocy.

Znaczna większość (70%) stwierdziła, że rodzice rozmawiali z nimi o sprawach bezpieczeństwa w Internecie, duża grupa podała, że rozmawiali z nimi nauczyciele (35%). Mniej więcej połowa powiedziała, że rodzice od czasu do czasu siadają z nimi przy komputerze, gdy one serfują, i zerkają na ekran czasami lub stale, by wiedzieć, gdzie serfują. Około 60% nastolatek podaje, że rodzice, nauczyciele lub opiekunowie rozmawiają z nimi o zajęciach w Internecie regularnie lub czasami. Jedna z ciekawszych zależności, którą odkryliśmy, polega na tym, że nastolatki, których rodzice serfują z nimi, nie angażują się w cyberseks, podczas gdy prawie 60% ogółu dziewcząt podaje, że angażują się w cyberseks (nie definiując, co to oznacza). Poza tym 65% nastolatek twierdzi, że ich rodzice nie zainstalowali żadnego oprogramowania filtrującego, a kolejne 20% nie wie, czy rodzice zainstalowali coś takiego, czy nie. Ponad 70% stwierdza, że rodzice korzystają w domu z Internetu. Wiele nastolatek podaje, że korzystają głównie z programów natychmiastowego przekazywania wiadomości, a następną najbardziej popularną aktywnością jest serfowanie w poszukiwaniu nowości. (Tylko 1,5% podało, że gra głównie w gry, ale badanie grupy chłopców dałoby pewnie inny obraz zainteresowania grami).

Kiedy pytaliśmy, czy zrobiły w cyberprzestrzeni coś takiego, czego nie zrobiłyby w kontakcie osobistym, uzyskaliśmy m.in. takie odpowiedzi:

„Tak, wyraźnie ludzie są śmielsi i bardziej otwarci w Internecie, kiedy nie muszą ponosić konsekwencji swoich działań".

„Oczywiście! Wszyscy to robią. Komputer podłączony do linii telefonicznej jest jak maska wobec całego świata. Możesz zrobić czy powiedzieć wszystko, bo nigdy nie spotkasz się z tą osobą. Na przykład mój brat ma 13 lat, a wszystkim mówi, że ma 16 albo więcej. On jest fajnym facetem i normalnie bardzo szanuje kobiety. W Internecie jednak mówi okropne lub dwuznaczne rzeczy do nich i o nich. Zachowuje się jak potwór. To okropne... i trochę przerażające".

„Tak, jasne... nasze normalne granice i osobiste zahamowania zostają zniesione i możemy reagować beztrosko i swobodnie, jeśli mamy ochotę. Przynajmniej ja... inne może zachowują się jak boginie".

„Ja obraziłam wielu ludzi. Kiedy moi kumple przychodzili do mnie, razem wchodziliśmy do miejsc takich jak kawiarenki dla Afroamerykanów i krzyczeliśmy «Ku-Klux-Klan górą!», albo do żydowskich, żeby zawołać: «Heil Hitler», ale teraz już tego nie robię, od kiedy znowu zaczęłam chodzić do kościoła i zostałam ocalona przez Jezusa Chrystusa. Po prostu żartowaliśmy, nie byliśmy naprawdę rasistami".

„Tak, ale wolałabym nie opisywać, co robiłam. Zamiast tego raczej powiem, że w cyberświecie możesz być absolutnie każdym, kim chcesz być. Z tego powodu wiele ludzi robi rzeczy, których normalnie by nie robili. W realnym życiu ludzie wszędzie oceniają cię na podstawie wyglądu, zachowania i nie wiadomo czego jeszcze, ale w Internecie tym, co się naprawdę liczy, jest twoja osobowość i postawa".

„No cóż, próbowałam cyberseksu wcześniej i nigdy nie zrobiłabym tego w realnym życiu. Nie popieram seksu przedmałżeńskiego. Myślę, że to wielki dar, który dajesz swojemu mężowi. Kiedyś zbeształam kogoś, kto zachowywał się perwersyjnie i mówił mi rzeczy, których nie miałam ochoty słuchać".

„Więc kiedyś powiedziałam facetowi, którego poznałam na czacie, wszystko o sobie, to znaczy telefon i te rzeczy. Teraz wiem, że to było głupie z mojej strony i nigdy już nie zrobiłabym czegoś podobnego, bo choć to mało prawdopodobne, to on mógł być psychicznie chory albo coś takiego".

„Czuję, że mogę swobodniej rozmawiać o swoich sprawach z kimś z sieci, bo ten ktoś nie chodzi do mojej szkoły, a nawet nie mieszka w tym samym mieście. Mogę zapytać ich o radę i prawdopodobnie udzielą mi najlepszej, bo nie działają na niczyją korzyść. Mogę przedstawić siebie i poznawać nowych ludzi, bo nie jest to tak krępujące, jak patrzeć komuś w oczy, i jeśli naprawdę czuję się źle w ich towarzystwie, mogę ich zablokować albo wylogować się".

„Uprawiałam cyberseks... to coś, czego bym nigdy nie zrobiła i nie zrobię w normalnym życiu, dopóki nie wyjdę za mąż".

„Jestem znacznie bardziej odważna w Internecie niż w normalnym życiu. Jestem BARDZO nieśmiała, a w Internecie mówię rzeczy, których normalnie nie powiedziałabym publicznie".

„Kłamałam bez żadnych właściwie powodów. Powiedziałam kiedyś chłopcu, że nie mogę mu dać mojego numeru telefonu, bo mama nie zgadza się, żeby chłopcy do mnie dzwonili w ciągu roku szkolnego. Moja matka tak naprawdę ma w nosie, kto do mnie dzwoni. Po prostu nie wiedziałam, co powiedzieć".

„Tak, nie flirtowałabym z ludźmi, których właśnie poznałam. Zupełnie inaczej w Internecie".

„Łatwiej jest flirtować, mówić różne rzeczy. Nie jakieś złe, po prostu bardziej szczere".

„Tak, bo to znacznie łatwiej rozmawiać i poznać kogoś w sieci, bo nie widzi się niczyjej twarzy. Nigdy nie zrobiłam niczego złego, ale jestem znacznie swobodniejsza w tym, co mówię w cyberświecie, niż w życiowych sytuacjach. I w jakiś sposób to sprawia, że też w życiu łatwiej mi się rozmawia z nowo poznanymi chłopcami".

„Tak, prawdę mówiąc. Uprawiałam cyberseks! Nigdy nie zdecyduję się na prawdziwy seks przed wyjściem za mąż, po tym doświadczeniu w cyberrzeczywistości. Czułam się okropnie, jakbym wiedziała, że robię coś złego! Nie popełnię tego błędu więcej!".

Kiedy pytaliśmy je, czy kiedykolwiek udawały kogoś innego, odpowiedziały (ich własne słowa):

„Oczywiście, że udawałam. Każdy to robi. Udajesz, że jesteś starsza, albo udajesz, że jesteś facetem albo kimkolwiek, kim chcesz być".

„Tak, zamieniałam się w kogoś, kim nie jestem, bo chciałam wzbudzać inne reakcje ludzi. To pozwalało mi zobaczyć siebie jako kogoś,

kim chciałabym być, a robiąc to, uświadomiłam sobie, że to nie to, że wcale taka nie chcę być i że chcę być sobą".

„Tak, jeśli jestem na czacie, zawsze zmyślam różne rzeczy na swój temat. To dlatego mówię, że nie można ufać nikomu w Internecie, bo wszyscy tak robią".

„Ponieważ wydaje się, że nikt nie ma ochoty rozmawiać z 15-latką, zawsze udawałam, że jestem 18-letnią kobietą. To jednak czasem prowokowało niełądne uwagi ze strony facetów".

„Tak. Udawałam prawie każdego, od Leonarda DiCaprio do seryjnego mordercy".

„Kiedyś udawałam, że jestem 16-latką. Rozmawiałam ze swoim chłopcem, żeby zobaczyć, czy zgodzi się z nią spotkać twarzą w twarz. Zgodził się i wtedy powiedziałam mu, kim jestem naprawdę i zerwaliśmy ze sobą".

„Tak, udawałam różne osoby. To zabawne i niczym nie grozi, bo nikt nie wie, kim naprawdę jesteś".

„Cóż, wszyscy udajemy, że jesteśmy starsi czy mamy inne imiona. Kto tego nie robi? To część zabawy związanej z byciem w sieci, że możesz być każdym przez chwilę".

„Tak, udawałam, że jestem kimś, kim chciałabym być, kimś bardzo popularnym".

„Nie udawałam, że jestem kimś innym, ale udawałam, że jestem o kilka lat starsza, bo nie ma w Internecie wielu ludzi w moim wieku, z którymi można pogadać, a jeśli są, to muszą kłamać na temat swojego wieku".

„Nie, bo uważam, że to źle kłamać innym na temat tego, kim się jest. Nie chciałabym, żeby ktoś zrobił to mnie, i dlatego nie robię tak innym".

Na pytanie, czy znalazły się kiedykolwiek w Internecie w sytuacji, która je przerażała, odpowiedzi były takie:

„Moja przyjaciółka zgodziła się na spotkanie z facetem, którego poznała w Internecie, gdy on przyjechał do naszego miasta, i chciała, żeby ktoś jeszcze z nią był. Powiedziałam moim rodzicom i randka z chłopcem nie doszła do skutku. Nie poszłabym i nie mogłam popierać jej decyzji spotkania z kimś w realnym świecie. Ona poczuła się w jakimś sensie zdradzona, ale przynajmniej jest żywa".

„Kiedyś się przeraziłam, bo taki facet mówił mi ciągle różne rzeczy o mnie, moje nazwisko, adres, nazwiska przyjaciół, powiedział, że wie, gdzie mieszkam, i żebym lepiej uważała. Na koniec okazało się, że to żart kolegi mojego kolegi, ale ja się dalej bałam i byłam bardzo zła na kolegę, że przekazał komuś moje dane tylko po to, żeby mnie przestraszyć. To nie było śmieszne".

„Kiedyś prowadziłam z przyjaciółmi rozmowę w ICQ, kiedy jeden z chłopców, z którymi gadałam, przysłał mi plik. Automatycznie otworzyłam go i uświadomiłam sobie, że ta osoba wdarła się do mojego systemu. Nagle napęd CD-ROM zaczął się włączać i wyłączać i na ekranie zaczęły pojawiać się denerwujące (ale niegroźne) wiadomości. Niebawem mysz przestała działać. Właśnie kończyłam dużą pracę i bałam się, że haker może coś zrobić, by ją zniszczyć. Zamknęłam komputer i to było wszystko, co z tą sprawą zrobiłam. Jedna z moich przyjaciółek miała podobne doświadczenie, tylko u niej komunikaty na ekranie były przerażające i groźne. Kiedy haker włamał się do systemu, na ekranie zaczęły pojawiać się szczątki zmasakrowanej dziewczyny z jej twarzą, a do tego groźby i przerażające odgłosy".

„Ja wiem, że to normalne, naprawdę wcale mnie nie przeraziło, po prostu się śmiałam. Większość dzieci jest ciągle narażona na takie rzeczy nie tylko w Internecie, więc co za sprawa, czasem przez to jest nawet ciekawiej. Ale kiedyś ten mieszczuch naprawdę się wściekł na mnie, a wiedział, że moi rodzice wyjechali, i mógł zadzwonić do któregoś z moich kolegów i wziąć mój adres, ale zamiast tego dzwonił do mnie co pięć minut...".

„Kiedyś weszłam do Internetu tylko po to, żeby sprawdzić pocztę. Ale wpadłam do swojej ulubionej kawiarenki, a kiedy już tam byłam, to jakiś typ od razu zaczął podawać moje dane personalne. Nie wiem, skąd wiedział cokolwiek o mnie, ale opowiadał wszystkim o różnych strasznych rzeczach, które zdarzyły mi się w dzieciństwie. Nawet moja najlepsza przyjaciółka nie wie o tym, co mi zrobiono, gdy byłam mała. Zdołałam tylko zaprzeczyć wszystkiemu i wylogowałam się. Płakałam cały tydzień".

„Ten facet przysyłał mnie i mojej najlepszej przyjaciółce ICQ i wiedział to wszystko o nas... a my z nim nawet nie rozmawiałyśmy wcześniej. On wiedział, kim jesteśmy, gdzie mieszkamy, i bawił się nami, wmawiając nam, że to my zaczęłyśmy wysyłać wiadomości do niego Powiedziałam o tym moim rodzicom, ale oni się nie przejęli. I tak to trwało przez półtorej godziny. Prosiłam kolegów, by coś z nim zrobili. Powiedział nam, gdzie pracuje, i nastawał, żebyśmy z nim chodziły w różne miejsca, na ciastka albo na obiad, i że on nam kupi prezenty gwiazdkowe i urodzinowe, choć nigdy go nie widziałyśmy. Zostawi je dla nas w samochodzie w pracy, żebyśmy przyszły i wzięły, możemy je wziąć i rzucić na ziemię... gdyby dopiął swego. Był przekonany, że umówi się z moją najlepszą przyjaciółką, ale ja się zjawiłam i wszystko się skończyło. Nikt nie mógł zastopować tego faceta. Zmieniałyśmy wiele razy nasze identyfikatory, ale on już się włamał do naszej skrzynki i zawsze mógł nas znaleźć. W grudniu zmieniliśmy komputer i obie zmieniłyśmy swoje identyfikatory i od tego czasu nie mógł nas odnaleźć".

„Mniej więcej rok temu poznałam w Internecie chłopca, któremu podałam swój numer telefonu, i okazało się, że on mieszka jakieś pięć minut drogi ode mnie. Gadaliśmy przez tydzień, a potem on zaproponował, żebyśmy się spotkali i ja się zgodziłam. Spotkaliśmy się w centrum handlowym i on okazał się zupełnie normalnym 15-latkiem. Nie był wariatem ani nikim takim. Ale miałam mnóstwo przykrości od swoich rodziców i nigdy więcej nie przekażę żadnych danych personalnych. To nie jest bezpieczne i w ogóle to głupi pomysł. Jeśli ktokolwiek, kto to czyta, rozważa podanie komuś w Internecie jakichś informacji o sobie, niech tego nie robi, bo może wpaść w kłopoty".

„Otrzymałam od kogoś e-mail z pogróżkami. Natychmiast zmieniłam hasło i sprawdziłam, czy nie podałam jakichś danych personalnych w moim profilu. Nie odpowiedziałam tej osobie, bo wtedy wiedziałaby, że konto jest nadal aktywne, i mogłaby szukać innych

informacji o mnie. Potem postanowiłam już wcale nie otwierać swojej skrzynki i założyć nową".

„Byłam w kawiarence i ta osoba groziła, że się zabije, a dla mnie to brzmiało przerażająco. Więc wysłałam jej wiadomość, żeby tego nie robiła, i gadałam z nią trochę, żeby poczuła się lepiej i żeby obiecała, że nie zrobi sobie nic złego. I ona obiecała".

„Powiedziałam tym ludziom, żeby zostawili w spokoju tego cudzoziemca, bo oni się z niego śmieli. Przezywali go i wyśmiewali wszystko, co powiedział. I oni powiedzieli, żebym się nie wtrącała, bo zaraz mogą się dowiedzieć, gdzie mieszkam. Wtedy uciekłam".

Warto byłoby posłuchać odpowiedzi twojego dziecka na takie pytania. Mógłbyś wówczas dowiedzieć się o nim wielu rzeczy...

Mogłyby napisać tę książkę za mnie...

Większość nastolatków, a nawet młodsze dzieci, znają prawie wszystkie zasady dbania o bezpieczeństwo. Oto lista stworzona przez moje małe szkolące się anioły, dziewięcio- i dziesięcioletnie, Alyssę, Lauren i Maggie.

Rady, dotyczące zachowania bezpieczeństwa Alyssy, Lauren i Maggie (wyrażone ich własnymi słowami):

1. Zawsze pytaj rodziców o zgodę, zanim wejdziesz do Internetu.
2. Nigdy nie przekazuj informacji o sobie – nazwiska, adresu, numeru telefonu, nazwy szkoły czy imion rodziców.
3. Nigdy nie kłam na temat swojego wieku, żeby się dostać na jakąś stronę.
4. Nie kupuj nic bez zgody rodziców.
5. Nie używaj wulgarnego języka, bo możesz zostać wyrzucony z Internetu i nie dostaniesz się tam z powrotem.
6. Nie otwieraj e-mailów od nieznanych osób.
7. Nigdy nie wysyłaj przez Internet zdjęcia osobie, której nie znasz.
8. Nigdy nie proś osoby poznanej w Internecie o spotkanie w realnym życiu.

9. Jeśli ktoś mówi, że jest dyrektorem Optimusa i że dostałeś darmowe bilety, i żebyś podpisał różne formularze, i pyta, czy chcesz, powiedz „nie", bo to może być kłamstwo albo on może być oszustem.
10. Jeśli ktoś mówi, że jest wyprzedaż i że potrzebują twojego numeru telefonu, zawsze odmawiaj.
11. Uważaj na złych ludzi w Internecie, bo możesz zostać skrzywdzony.
12. Jeśli ktoś nie przestrzega zasad, ignoruj go!
13. Nigdy nie wierz nikomu, kto ci mówi, ile ma lat. Nawet jeśli zadajesz takie pytania, na które twoim zdaniem tylko dziecko może znać odpowiedź, to nie jest dowód, że masz do czynienia z dzieckiem.
14. Powiedz rodzicom, jeśli coś złego się zdarzy.

❖ Rady Maggie

Maggie chciała, by rodzice wiedzieli, jak ona się czuje, kiedy oni zaglądają do jej poczty i depczą jej prywatność.

1. Choć znacie hasło do skrzynki swojego dziecka, nie grzebcie w jego e-mailach.
2. Jeśli chcecie sprawdzać korespondencję swoich dzieci, róbcie to razem z nimi.

Napisała też w imieniu wszystkich dzieci list do rodziców:

Droga mamo, drogi tato!

Wiem wszystko o zasadach dbania o bezpieczeństwo w Internecie. Wiem, że są na świecie ludzie, którzy mogliby chcieć mnie zranić. Ale nie martwcie się, nie zaskoczą mnie. Bezpieczeństwo jest ważne, ale nie czuję się dobrze, gdy czytacie moje listy, nie uprzedzając mnie o tym. Chciałabym też, żebyście wiedzieli, że znam wszystkie zasady bezpieczeństwa w Internecie. To niektóre rady, których mogłabym udzielić koledze, który nigdy nie korzystał z Internetu: nie rozmawiaj z nieznajomymi. Nie ściągaj żadnych plików bez zgody rodziców, bo mogą zawierać wirusy. Na szczęście możecie mi teraz ufać. Całuję.

Wasz syn/córka

Nie tylko moje Teenangels znają zasady. Nastolatki odpowiadające na ankietę w „Seventeen Magazine" także je znały. Kiedy popro-

siliśmy je, by podały kilka rad, jakich chciałyby udzielić koledze, który nigdy nie był w Internecie, odpowiedzi były takie:

- Nigdy nie udostępniaj NIKOMU w sieci informacji takich jak: nazwisko, adres, numer telefonu, adres e-mail, hasło, nazwa szkoły.
- Jeśli ktoś sprawia, że czujesz się niezręcznie, nie rozmawiaj z nim.
- Nie spotykaj się z nikim, kogo poznasz w cyberświecie, chyba że będziesz z przyjaciółmi czy rodzicami. Jeśli będziesz sam, a osoba, z którą się spotkasz, okaże się złym człowiekiem, nie będzie nikogo, kto mógłby ci pomóc.
- Bądź ostrożny. Nigdy nie wiadomo, kto jest po drugiej stronie.
- To pewne, że jest mnóstwo miłych ludzi w sieci, ale jest też wielu zaburzonych. Po co ryzykować? Gdy igra się z ogniem, można ulec poparzeniu. To dotyczy wszystkich, ale zwłaszcza nastoletnich dziewcząt.
- Nie rób tego, czego nie należy.
- Ludzie nie zawsze są tymi, którymi wydają się być.
- Nie traktuj poważnie wszystkiego, co ludzie ci mówią.
- Nie otwieraj e-mailów, jeśli nie znasz nadawcy.
- Powiedziałabym im, żeby nigdy nie godzili się na spotkanie z kimś, a jeśli czują się pod presją, zagrożeni lub skrępowani czymś, co ktoś im mówi, powinni przestać rozmawiać z tą osobą, nawet przerwać na jakiś czas połączenie z Internetem. Jeśli ta osoba nadal ich prześladuje, należy ją zablokować. (Niektórzy dostawcy usług internetowych mogą to zrobić na życzenie klienta). Powiedziałabym im to wszystko, żeby byli bezpieczni, nie zostali porwani czy skrzywdzeni w inny sposób.
- Nigdy nie dawaj nikomu swojego adresu, bo nie wiesz na pewno, że osoba, z którą rozmawiasz, jest rzeczywiście wyśnionym 18-latkiem, a nie seryjnym gwałcicielem, polującym na kolejną ofiarę.
- Nie obawiaj się umieszczania kogoś na liście osób, które mają być ignorowane.
- Uważaj na to, co mówisz, bo może to do ciebie wrócić.
- Nie wysyłaj nikomu swoich zdjęć przez Internet, bo on może je łatwo przesłać innym.

- Nie przekazuj informacji, których nie opublikowałabyś w ogólnokrajowej gazecie.
- Uważaj na to, o czym mówisz, kiedy rozmawiasz z kimś, kogo nigdy nie widziałaś.
- Nie udzielaj zbyt wielu informacji. To zaskakujące, jak łatwo można człowieka znaleźć.
- Usuwaj obraźliwe wiadomości.
- Dobrze się baw i nie traktuj zbyt poważnie niczego oprócz pogróżek, o których sądzisz, że mogą być poważne.
- Powiedziałabym, by blokowali kontakt z osobami, które zachowują się podejrzanie, i by nie przekazywali zbyt wielu informacji o sobie.
- Ściągaj pliki na dyskietkę, nie na dysk, chyba że masz pewność, że są bezpieczne i nie zawierają wirusów.
- Bądź ostrożny z wchodzeniem do miejsc i kupowaniem rzeczy za pieniądze. Czytaj to, co napisane drobnym drukiem, i nie zgadzaj się, dopóki nie wiesz wszystkiego. Niektóre witryny domagają się opłat od odwiedzających je, więc sprawdź.
- Trzymaj się z dala od ludzi, którzy mają nazwy alkoholi czy narkotyków w swoich pseudonimach, bo oni są tym na ogół zainteresowani.
- Najlepiej wcale nie wchodź do kawiarenek, bo nigdy nie wiesz, co się tam może zdarzyć. To pochlebiające, gdy chłopiec mówi ci, że cię kocha, ale on nawet cię nie zna. Większość z nich ma w głowie tylko cyberseks.
- Nie otwieraj żadnych plików dołączonych do wiadomości, bo to może być pornografia lub wirus.
- Baw się, ale nie popadaj w obsesję.
- Nie szukaj kłopotów!

Widzicie? Mówiłam, że mogłyby napisać za mnie tę książkę!

„Szanowny Panie Prezydencie!"

Krótko po tragedii w Littleton spędziłam kilka dni, rozmawiając z uczniami szkoły na Manhattanie. Kilku uczniów biorących udział w sesjach korzystało z Internetu, ale posiadanie w domu komputera z dostępem do Internetu było wśród nich wielką rzadkością.

Grupy liczyły 10–150 uczniów na sesji. Oceniam, że w rozmowie wzięło udział około sześciuset uczniów w wieku 15–18 lat. Grupy były bardzo różne, niektóre złożone głównie z mniejszości narodowych, mniej więcej równa liczba przedstawicieli każdej płci. Niektóre osoby były bardziej skłonne do rozmowy niż inne, ale większość mówiła, co myślą o Littleton, o mediach, o proponowanych rozwiązaniach i odpowiedzialności za własne czyny.

Byłam zaskoczona tym, jak bardzo przemyślane były ich opinie. Wiele wypowiedzi, zwłaszcza dotyczących sprawy konstruowania bomb, filtrowania i przymusowego oceniania filmów, zachwyciło mnie. Byłam pod wrażeniem tego, co mieli do powiedzenia i jak dobrze potrafili to zrobić. Nasza przyszłość jest w dobrych rękach. Oto co chcieliby przekazać prezydentowi w związku ze spotkaniem poświęconym przemocy, które miało się odbyć w związku z Littleton. Choć jest to napisane moimi słowami, idee pochodzą od nich:

Mamy przekonanie, że nie ma żadnej osoby odpowiedzialnej za to, co stało się w Littleton. Lepsze porozumiewanie się, troskliwsze wychowanie, więcej zrozumienia i tolerancji ze strony kolegów z klasy i trudniejszy dostęp do informacji o konstruowaniu bomb być może sprawiłyby, że byłoby to mniej prawdopodobne, ale nikogo nie można obwiniać. Strzelający sami są odpowiedzialni za swoje działania.

Obawiamy się, że zainteresowanie sprawą przemocy w szkołach będzie krótkotrwałe. Po głośnych tragediach w szkołach specjaliści zajmują się bezpieczeństwem uczniów i tworzą programy zapobiegania przemocy. Ale po paru miesiącach wszystko wraca do stanu wyjściowego. Chcielibyśmy mieć pewność, że ten problem będzie dłużej budził zainteresowanie i że więcej żadne dziecko nie będzie musiało umrzeć, zanim znajdziemy rozwiązanie. Musimy próbować różnych strategii, zanim wypracujemy taką, która będzie skuteczna.

To smutne, że kiedy mówi się o problemach przemocy w szkole, wielu ludzi myśli jedynie o uczniach szkół w centrach miast. Nasze szkoły wyposażone są w wykrywacze metalu, mają uzbrojoną ochronę. A przecież tragedie i masowe zabójstwa w szkołach zaczęły się nie w szkołach śródmiejskich, ale w szkołach na przedmieściach i terenach wiejskich. Sądzimy, że należy wyjaśnić, dlaczego młodzież, która jest zagrożona, nie jest pod obserwacją z powodu lokalizacji szkoły, choć my jesteśmy. Uważamy, że takie rzeczy zdarzają się częściej na przedmieściach i na obszarach wiejskich i nie mogłyby zdarzyć się w centrum miasta, bo my mamy mnóstwo innych zajęć. Taki scenariusz najczęściej zdarza się wtedy, gdy nastolatki zbyt dużo czasu spędzają bezczynnie.

Uważamy, że wszystkie szkoły powinny dysponować wykrywaczami metalu i uzbrojoną ochroną. Choć nie uwolni to szkół od przemocy, ale umożliwi wykrycie uzbrojonego ucznia. Jednak głównym punktem kampanii przeciw przemocy powinno być zapewnienie uczniom pomocy w kontrolowaniu złości i odnalezieniu alternatywy dla przemocy. Uczniowie powinni wiedzieć, że życzliwi terapeuci są na miejscu, że wysłuchają i pomogą zranionym czy zaburzonym dzieciom. Należy więcej środków skierować na rozwój poradnictwa, by mogło obejmować nie tylko tych, którzy sami zgłaszają się po pomoc. Trzeba też aktywnie poszukiwać osób potrzebujących pomocy.

Wydaje się nam, że lepiej niż władze szkolne wiemy, kto w naszej szkole może być skłonny do gwałtownych zachowań. Ale nawet my nie umiemy odróżnić pustych pogróżek od naprawdę niebezpiecznych. Wielu z nas sądzi, że ustanowienie gorącej linii mogłoby pomóc, większość jednak wie, że wcale nie używalibyśmy jej. Większość z nas w przypadku poważnych gróźb zwróciłaby się raczej do władz szkolnych lub policji, nie do rodziców. Moglibyśmy zgłaszać przypadki potencjalnej przemocy i gróźb tylko wtedy, gdybyśmy robili to anonimowo. Obawiamy się kary. Boimy się też, że nasze słowa nie będą traktowane poważnie.

Niektórzy z nas korzystają z Internetu, wielu gra w gry komputerowe, wszyscy chodzimy do kina i oglądamy telewizję. Sądzimy, że publikowanie informacji o konstruowaniu bomb na stronach WWW powinno być zakazane. Nie widzimy powodu, by takie informacje były łatwo dostępne. Gdybyśmy je mieli pod ręką, moglibyśmy spróbować zrobić bombę tylko po to, żeby sprawdzić, czy potrafimy. Zgadzamy się, że te wiadomości można znaleźć też w bibliotece, i nie uważamy, że książki zawierające je powinny być zakazane. Wątpimy natomiast, czy wielu nastolatków zadałoby sobie trud wyszukiwania ich w bibliotece. To naprawdę łatwość dostępu tworzy problem. Niepokoimy się też, że nasze młodsze rodzeństwo ogląda strony WWW z seksem dla dorosłych. Część z nas uważa, że strony dla dorosłych powinny być strzeżone hasłem. Doceniamy wagę wolności słowa, jednak uważamy, że niektóre rzeczy muszą podlegać kontroli.

Sądzimy, że selekcja zawartości treściowej może być dokonywana przez rodziców lub szkoły, nie przez rząd. Godzimy się na to, by

nasi rodzice instalowali oprogramowanie wspomagające rodzicielską kontrolę czy filtrujące. Nie popieramy jednak oprogramowania monitorującego, które umożliwia wejście na każdą stronę, ale potem przekazuje informacje o naszym serfowaniu rodzicom. Odbieramy to jako pogwałcenie naszej prywatności. Jednak oprogramowanie takie może być pożyteczne w przypadku młodszych dzieci.

Gier komputerowych używamy dla zabawy. Fakt, że celem jest człowiek, nie ma żadnego znaczenia. Każdy cel byłby taki sam. Nie wydaje się nam, że to znieczula nas na zabijanie ludzi. Nie sądzimy, by gry komputerowe czy telewizyjne mogły skutecznie zachęcić do stosowania przemocy starsze dzieci czy nastolatków. Część z nas (zwłaszcza dziewczęta) uważa jednak, że młodsze dzieci mogą nauczyć się brutalnych zachowań pod wpływem tych gier. Obawiamy się, że wielu rodziców po prostu nie interesuje się tym, jakie gry mają ich dzieci, i tym sposobem gry przeznaczone dla starszych mogą trafić do młodszych. Uważamy, że gry zawierające przemoc nie powinny być adresowane do młodszych dzieci. Część z nas sądzi, że rodzice i uczniowie powinni mieć obowiązek podpisania oświadczeń, że wiedzą, iż gra, którą kupują, zawiera dużo przemocy i powinna być przeznaczona dla użytkowników szesnastoletnich lub starszych.

Nie wierzymy, że filmy promują brutalne zachowania. Ale jesteśmy zadowoleni, że filmy są oceniane i sądzimy, że te brutalne nie powinny być dozwolone dla osób młodszych niż 16 czy 18 lat.

Naszym zdaniem nie jest prawdą, że filmy zachęcają do agresji. Ale jesteśmy zadowoleni, że filmy podlegają ocenie. Tylko że najwyraźniej nikt tych ocen nie traktuje poważnie. Bardzo rzadko ktoś z nas bywa proszony o udowodnienie, ile mamy lat, gdy kupujemy bilety na film przeznaczony dla dorosłych. Uważamy, że to powinno być skrupulatnie przestrzegane. Ciekawe, że od tych z nas, którzy wybrali się do kina na film „Matrix" po zdarzeniach w Littleton, żądano okazania dokumentów. Może to dobry znak.

Nie uważamy, że telewizja jest brutalna.

Sądzimy, że rodzice poświęcają dzieciom zbyt mało uwagi i nie udzielają wsparcia. Rodzice zbyt często chcą być nie rodzicami, ale kolegami swoich dzieci. My potrzebujemy i chcemy przewodnictwa naszych rodziców i traktujemy ich z szacunkiem. Akceptujemy restrykcje i ograniczenia naszych działań, gdy są wprowadzane konsekwentnie. Jeśli się z tym czeka do momentu, gdy mamy 16 lat lub więcej, to wtedy jest za późno.

Niektórzy z nas mieli to szczęście, że otrzymali od swoich rodziców wiele miłości. Dostarczali nam też „stresów", ale w ten sposób wiele się od nich uczymy. Rodzice powinni nauczyć nas odróżniać dobro od zła. Ale i ci z nas, którzy nie mieli dobrych relacji ze swoimi rodzicami, nie mają podstaw, by obwiniać matkę czy ojca o swoje niewłaściwe czyny.

Złościmy się, ale zrobiliśmy postęp w panowaniu nad swoją złością. Pomagają nam w tym przyjaciele, słuchamy muzyki, idziemy pod prysznic, płaczemy, uprawiamy sporty, czasem wyładowujemy złość na kolegach. Choć niektórzy z nas zachowują się niekiedy impulsywnie, na ogół nie przychodzi nam do głowy, żeby strzelać do kolegów z klasy. Wiele razy przeżywaliśmy wielką złość, ale nie wybieraliśmy naprawdę poważnych form przemocy, bo to nie jest „nasz sposób". Chcielibyśmy, by było więcej programów, które uczyłyby nas kontrolować złość, lepiej się porozumiewać i znaleźć jakieś alternatywy dla przemocy.

Uważamy, że powinna istnieć skuteczniejsza kontrola sprzedaży broni. Uważamy też, że dorośli powinni częściej słuchać tego, co mamy do powiedzenia.

I wreszcie niektórzy z nas nie są w stanie zrozumieć, jak młodzież, która mieszka w dobrych dzielnicach, jeździ dobrymi samochodami i dostaje wszystko, na co ma ochotę, może być aż tak niezadowolona z życia. Zaczynamy myśleć, że może pieniądze i przywileje nie są źródłem szczęścia.

Wiemy, że jest pan bardzo zajęty, ale mamy nadzieję, że znajdzie pan kilka minut, by wysłuchać, co mamy do powiedzenia. Być może wspólnie znajdziemy jakieś rozwiązania.

Podpis: Nastolatki

Teenangels

Teenangels powstały na skutek programu, który zrobiłam dla telewizji ABC w kwietniu 1999 roku. Program dotyczył bezpieczeństwa nastoletnich dziewcząt, ja występowałam jako ekspert od spraw bezpieczeństwa w Internecie. Częścią tego programu było spotkanie z dziewczętami w jednej z nowojorskich szkół. Dziewczynki ustawiły się w kolejce do mikrofonu i zasypały mnie pytaniami. Wtedy po raz pierwszy uświadomiłam sobie, że te nastolatki naprawdę martwią się o bezpieczeństwo w sieci młodszego rodzeństwa, kuzynów, sąsiadów.

Byłam zachwycona tym, że przedstawiam sprawy grupie, która naprawdę rozumie zagrożenia i potrafi odróżnić rzeczy niebezpieczne od po prostu denerwujących.

Pięć spośród uczennic zostało wydelegowanych przez swoje szkoły do współpracy ze mną w przygotowaniu pierwszego programu bezpieczeństwa internetowego w ramach projektu Wired Kids. Dziewczyny miały 15–17 lat i na cześć Cyberangels nazwały siebie Teenangels. Potem rozpoczęło się szkolenie. Podczas wakacji, rezygnując z plaży w upalne dni i z wakacyjnych prac zarobkowych, poświęcały swój czas tej misji, pracując wraz ze mną, by poznać problemy istotne dla bezpieczeństwa w Internecie. Siedziały w moim pokoju konferencyjnym i przyswajały sobie reguły bezpieczeństwa. Dla mnie było to największe wyzwanie w mojej karierze – kwestionowały, że określone rzeczy są rzeczywiście niebezpieczne, i koniecznie chciały wiedzieć, jak bardzo niebezpieczne. Były nastawione na znajdowanie rozwiązań, a jednocześnie chodziło im o to, by każde dziecko miało dostęp do komputera. Pytane, czemu tak wiele czasu poświęcają tej sprawie, jednogłośnie odpowiadały, że po to, by rodzice nie obawiali się pozwolić swoim dzieciom na korzystanie z Internetu. Jedna z nich powiedziała, że kiedyś dostęp do Internetu dawał człowiekowi pewną przewagę, a dzisiaj brak dostępu to bardzo poważne obciążenie.

Spotkały się i pracowały z oficerem oddziału FBI Gordonem Rossem, detektywem z policji stanowej New Jersey, który przyczynił się do schwytania osoby odpowiedzialnej za stworzenie wirusa Melissa, i z twórcą Net Nanny. W programie szkolenia jest współpraca z innymi jeszcze wybitnymi ekspertami w dziedzinie bezpieczeństwa w Internecie.

Po zakończeniu wstępnej części szkolenia same napisały kilka zestawów porad dotyczących bezpieczeństwa w sieci, adresowanych do różnych grup wiekowych: do dzieci do 10 roku życia, do nastolatków i do rodziców. Jest to ich własna praca. Za każdym razem, gdy dowiedziały się czegoś nowego, zmieniały zestawy. Wreszcie stworzyły zbiór, który je usatysfakcjonował. Mnie też.

Ta lista porad będzie pierwszym z wielu kroków podjętych z myślą o zapoznaniu dzieci, nastolatków i rodziców o zagrożeniach i pożytkach korzystania z Internetu, o sposobach radzenia sobie z zagrożeniami. Zostanie wydrukowana i będzie bezpłatnie rozprowadzona w szkołach i na imprezach sponsorowanych. Będzie również dostępna w sklepach ze sprzętem komputerowym i artykułami dla dzieci.

Drugą częścią ich programu będzie film wideo. W tym filmie będziemy uczyć dzieci i nastolatki zasad bezpieczeństwa w sieci, powiemy, jak unikać największych zagrożeń w cyberprzestrzeni (cybernapastników).

Teenangels podejmą swoją misję, ucząc kolejne grupy nastolatków, jak informować innych o zagrożeniach w sieci. Jako ambasadorowie idei bezpieczeństwa, te dziewczyny pomogą osobom odpowiedzialnym w szkołach za bezpieczeństwo korzystania z sieci stworzyć liczniejszą grupę wyszkolonych dzieci, które z kolei przekażą swoją wiedzę innym. W przyszłości powstanie także serwis internetowy, który umożliwi dzieciom zainteresowanym włączeniem się do pracy nad poprawieniem bezpieczeństwa w sieci przechodzenie kursów bezpiecznego serfowania od razu na tej stronie. Będziemy zachęcać szkoły w całym kraju do udziału w programie podnoszenia bezpieczeństwa w Internecie. Mamy nadzieję, że program będzie się stale powiększał, jak śnieżna kula.

Z ust nastolatków (prawdziwych ekspertów)... Rady Teenangels dla rodziców, dzieci i młodzieży

Rady dla rodziców:

1. Sprawdźcie, czy wasze dziecko nie spędza zbyt dużo czasu w Internecie /przy komputerze. Posłużcie się zdrowym rozsądkiem, ustalając normy. Nie da się określić dokładnie ilości czasu, jaki można spędzać przy komputerze. Zależnie od dnia (dzień powszedni czy weekend), wieku dziecka i sposobu korzystania z Internetu, limity czasu będą różne. Średnio 1–2 godziny wydaje się najodpowiedniejszą ilością czasu. Ale zawsze będą wyjątki. Korzystajcie z własnego osądu, decydując, co jest najlepsze dla dziecka.

2. Ludzie, a nie komputery, powinni być najlepszymi przyjaciółmi dziecka. Pomóżcie waszemu dziecku zachować równowagę między zainteresowaniem komputerami a zaangażowaniem w inne formy aktywności.

3. Ustawcie komputer we wspólnym pokoju, nie w sypialni dziecka. Od czasu do czasu rzućcie okiem na ekran, by sprawdzić, co dzieci oglądają. Jednak musicie też starać się budować zaufanie w stosunkach z dziećmi, mając nadzieję, że wystarczy im zdrowego rozsądku, by odróżnić dobre od złego.

4. Poznajcie komputer tak dobrze, by bawić się nim razem z dziećmi. Nie obawiajcie się nauczyć się czegoś od swoich dzieci. Jednak

to wy jesteście rodzicami i musicie też czegoś nauczyć swoje dzieci. To musi być ruch w obu kierunkach. Poznajcie wiedzę swoich dzieci o komputerach, zorientujcie się, co wiedzą o Internecie. Być może będziecie zaskoczeni tym, ile wiedzą i ile mogą was nauczyć.

5. Sprawdźcie, jakie strony odwiedzają wasze dzieci i w jakich kawiarenkach bywają. W miarę ich dorastania powinno też wzrastać wzajemne zaufanie. Zachęcajcie dzieci do rozmów o tym, co lubią robić w cyberświecie. Zawsze bądźcie otwarci. Nie spieszcie się z ocenami, odwiedźcie razem niektóre z tych miejsc (jeśli dzieci są młodsze).

6. Musicie zrobić wszystko, by dzieci nie obawiały się zwracać się do was z pytaniami. Jeśli zdarzy się coś złego, nie reagujcie nerwowo. Powiedzcie im, że to nie ich wina. Wy też musicie wiedzieć, co robić, gdy zdarzy się coś złego.

7. IRC to system, który nie ma zasad dostarczania usług, więc ludzie mogą mówić wszystko, na co mają ochotę, i na ogół nie spotykają ich za to restrykcje. To jest i dobre, i złe. Dobre, bo użytkownicy mogą swobodnie wypowiadać się na każdy temat. Złe, bo dzieci nie są chronione przed obscenicznymi wypowiedziami i pedofilami. Klienci AOL mogą spotkać się z zawieszeniem lub wykluczeniem za używanie wulgarnego języka, obrażanie innych, dokuczanie, ale użytkownicy IRC – nie. Niektóre kanały IRC mają jakieś swoje reguły, ale zdarza się to raczej rzadko. Dlatego zaleca się, by rodzice nie pozwalali swoim dzieciom korzystać z IRC, chyba że pod czujnym okiem.

8. Nie zapomnijcie sprawdzić, czy i w jakim stopniu dziecko dostosowuje się do ustalonych reguł, zwłaszcza gdy chodzi o ilość czasu spędzanego przy komputerze. Wyraźnie określcie swoje zasady. Gdy już omówicie je z dziećmi, dobrze jest spisać je i listę przykleić do komputera czy gdzieś w pobliżu, by można je było przeczytać, serfując. To ułatwi ich zapamiętanie.

9. Poznajcie wirtualnych „przyjaciół" swoich dzieci, tak jak poznajecie wszystkich innych przyjaciół i kolegów. Zapytajcie, kto jest na ich liście kumpli, z kim najczęściej rozmawiają.

10. Ostrzeżcie swoje dzieci, że ludzie nie zawsze są tymi, za których się podają. Porozmawiajcie o tym otwarcie. I dzieci, i rodzice mogą tu być nauczycielami. Prowadząc otwarte rozmowy o sprawach bezpieczeństwa, zagrożeniach, korzyściach i stratach, macie szansę stale uczyć się od siebie nawzajem.

11. Uczcie swoje dzieci, by kierowały się zdrowym rozsądkiem w cyberprzestrzeni, tak jak to robią w realnym życiu. To jak z rozpoczynaniem nauki w szkole. Rodzice nie mogą być tam stale z dzieckiem. Ale mogą trzymać je za rękę w drodze do szkoły. To samo odnosi się do sieci. Wesprzyjcie dziecko poprzez edukację, otwarte rozmowy, budowanie zaufania i najważniejsze – uczenie samodzielności.

12. Nie zakazujcie dzieciom korzystania z Internetu. Poznajcie jego zalety i omówcie je z dzieckiem. Kiedyś było tak, że dzieci posiadające komputer i dostęp do Internetu miały pewną przewagę nad pozostałymi. Teraz ci, którzy nie mają komputera i dostępu do Internetu, są w znacząco gorszej sytuacji.

13. By uchronić twardy dysk przed zniszczeniem, należy zainstalować oprogramowanie antywirusowe. Wirusy pojawiają się praktycznie każdego dnia, toteż program antywirusowy należy często uaktualniać. Dobrymi programami są McAfee i Norton Antivirus.

Pamiętajmy, że rodzice nie są złymi rodzicami dlatego, że nie wiedzą wszystkiego o komputerach, ale że stają się lepszymi, nie zaniedbując żadnej możliwości porozumiewania się z dziećmi, a to czasem oznacza uczenie się od nich.

Rady Teenangels dla nastolatków

1. Nigdy nie przekazuj nikomu swojego hasła. Jeśli ktoś je pozna, może otwierać twoją skrzynkę pocztową, kupować różne rzeczy na twoją kartę kredytową i zdobyć dane osobowe, pozwalające na zidentyfikowanie ciebie. Może zmienić twój profil, robić głupie kawały, udając ciebie, i może doprowadzić do tego, że zostaniesz pozbawiony dostępu do Internetu. Może też zmienić twoje hasło i odciąć cię od twojej własnej skrzynki. Wybierz hasło łatwe do zapamiętania, ale takie, które nie będzie łatwe do odgadnięcia. Zmieniaj je często, przynajmniej raz na miesiąc (ale gdzieś zapisz, żeby nie zapomnieć). Bądź ostrożny, jeśli ktoś przygląda się, gdy wprowadzasz hasło – może je odczytać. Kto zna hasło, ten kontroluje wszystko.

2. Nie udzielaj nigdy takich informacji, które umożliwiłyby komuś zidentyfikowanie cię w realnym świecie. Informacje, takie jak numer szkoły, do której chodzisz, zespół, do którego należysz, adres, numer telefonu czy szczegółowy opis, zawierający inne dane, może umożliwić komuś, kto się bardzo stara, znalezienie ciebie. Sprawdź, czy w jakichś miejscach dostępnych dla wszystkich, takich jak szkolna strona WWW

czy twoja własna, nie ma informacji, które umożliwiłyby odnalezienie cię poza siecią. Nie używaj prawdziwego imienia i nazwiska.

3. Wybierając identyfikator, zwróć uwagę, by nie zawierał części czy całości prawdziwego nazwiska. Nie wybieraj takiego, który jest wulgarny, prowokujący. Wybierz łatwy do zapamiętania.

4. Miej zawsze program antywirusowy. Jego skuteczność zależy od tego, czy jest odpowiednio często uaktualniany, bo każdego dnia powstają nowe wirusy. Dobrze jest też mieć program pierwszej pomocy, który sprawdza wszystkie pliki w poszukiwaniu błędów lub wirusów. Uważaj, by przypadkowo nie usunąć żadnych potrzebnych plików czy programów.

5. Nigdy w realnym życiu nie spotykaj się z ludźmi, których poznasz w sieci. Jeśli koniecznie chcesz złamać tę zasadę, powiedz komuś, komu ufasz, z kim się spotkasz, gdzie i kiedy. Jeśli nie chcesz przekazywać nikomu personaliów tej osoby, możesz je umieścić w zaklejonej kopercie i powiedzieć komuś, by otworzył ją tylko wtedy, gdy nie wrócisz do domu o określonej godzinie. Zanim się spotkasz, porozmawiaj z tą osobą przez telefon i może niech twoi rodzice porozmawiają z jej rodzicami. Dzwoń z budki telefonicznej, by nie dało się ustalić numeru twojego telefonu domowego. Umów się w jakimś uczęszczanym miejscu. Przyjdź z inną osobą, najlepiej z kimś dorosłym. Pierwsze spotkania nie powinny być długie. Po spotkaniu nie wracaj prosto do domu, najpierw wstąp do jakiegoś publicznego miejsca i upewnij się, że nikt nie idzie za tobą. Nie wstydź się i nie bój się powiedzieć „nie".

6. Nigdy nie otwieraj załączników do e-mailu od nadawcy, którego nie znasz. Mogą zawierać wirus, który zniszczy ci komputer. Nigdy nie przegrywaj niczego od kogoś, kogo nie znasz, czy ze źródła nie budzącego zaufania. Jeśli otrzymasz załącznik od kogoś, kogo znasz, najpierw sprawdź go za pomocą programu antywirusowego. Jeśli otrzymujesz normalny e-mail od kogoś, kogo nie znasz, po prostu usuń go, nie odpowiadaj na niego, bo może to być sztuczka hakera. Usuwaj listowe „łańcuszki" i reklamy. Nie przesyłaj „łańcuszków"dalej.

7. Nie bądź głupi. Używaj zdrowego rozsądku. Nie trać czujności i nie zadurzaj się w ludziach poznanych w Internecie. Dla nikogo nie łam zasad. Jeśli coś wydaje się zbyt piękne, żeby było prawdziwe, to na ogół tak właśnie jest. Nie trać kontroli nad sytuacją.

8. Jeśli sądzisz, że jesteś nękany czy prześladowany, nigdy nie odpowiadaj prześladowcy. Poinformuj dorosłą osobę o tym, co się dzieje. Jeśli naprawdę się obawiasz, zawiadom policję.

9. To, że ktoś wysyła ci e-mail czy podaje swoje dane personalne, nie oznacza, że musisz mu odpowiadać czy podać takie same informacje. Ty o tym decydujesz. Jeśli ktoś ci przeszkadza, po prostu wyloguj się. Nie musisz z nikim rozmawiać, jeśli nie masz ochoty.

10. Łatwo jest popaść w obsesję czy uzależnić się od komputera i Internetu, gdy spędza się zbyt dużo czasu w wirtualnym świecie. Próbuj zachować zdrową równowagę pomiędzy światem wirtualnym a realnym. Internet to wspaniałe miejsce do nauki, do rozmów z ludźmi, ale życie społeczne nastolatka nie powinno obracać się wokół komputera.

11. Przestrzegaj zasad czatów. Dowiedz się czegoś o kawiarence, zanim tam wejdziesz (czy jest moderowana, jaki jest temat, jakie obowiązują zasady uczestnictwa). Ustal, pod jakim adresem można zgłaszać ewentualne wykroczenia. Jeśli korzystasz z IRC, upewnij się, czy korzystasz z bezpiecznego kanału i bezpiecznych tematów. Poznaj i przestrzegaj zasad internetowego dobrego wychowania. Nie używaj wulgarnego języka. Nie daj się wciągać w kłótnie. Jeśli nie czujesz się dobrze w jakimś miejscu, opuść je. Jeśli ktoś robi coś niestosownego, zachowaj tekst i wyślij go do dostawcy Internetu. Jeśli złamiesz zasady, przygotuj się na konsekwencje.

12. Kieruj się zdrowym rozsądkiem i ufaj swojej intuicji. Jeśli słyszysz pogróżki, wzmianki o bombach i broni, ZAWSZE zachowaj takie wiadomości i przekaż je niezwłocznie komuś dorosłemu.

13. Jeśli znasz osoby, które stanowią zagrożenie dla siebie samych lub dla kogoś innego, powiedz o tym komuś. Każdy potrzebuje kogoś, do kogo może się zwrócić. Jeśli nie chcesz pójść do pedagoga, powinieneś porozmawiać z kimś, komu ufasz. Choć możesz mieć ambicję, by samodzielnie porozmawiać z zaburzoną osobą i pomóc jej, nie zapominaj, że jesteś tylko nastolatkiem i samodzielnie nie udźwigniesz ciężaru cudzych problemów.

14. Nie wierz we wszystko, co czytasz, widzisz i słyszysz w Internecie. Ogłoszenia mogą być zwodnicze. Nigdy nie wiesz, z kim rozmawiasz ani czy ktoś mówi ci prawdę. Zawsze pamiętaj, że znasz tylko imię na ekranie. Nie znasz osoby przy klawiaturze drugiego komputera. Tak jak ludzie bywają nieuczciwi w normalnym życiu, mogą być też nieuczciwi w cyberświecie. Na stronach WWW można powiedzieć wszystko, także kłamstwo, i niełatwo jest odróżnić prawdę od nieprawdy. Można tam rozpowszechniać fałszywe lub tendencyjne informacje. Więc używaj w Internecie zdolności krytycznego myślenia. To twoje najlepsze narzędzie do odróżniania prawdy od fałszu.

15. Jeśli dostajesz pogróżki od hakera, wyłącz komputer i odczekaj trochę, zanim ponownie włączysz się do Internetu. Uważaj, z kim przyjaźnisz się w Internecie. Jeśli przyjaźnisz się z hakerem, bądź szczególnie ostrożny, bo oni potrafią zrobić duże szkody w komputerze, jak wpadną w złość. Nie ufaj zbytnio nikomu i nie zdradzaj innym swoich personaliów, zwłaszcza hasła, bo ludzie, którzy wydają ci się przyjaciółmi, mogą użyć tego przeciwko tobie.

16. Bądź mądrym użytkownikiem Internetu. Choć kupowanie i sprzedawanie w sieci może wyglądać na najłatwiejszy w świecie sposób robienia zakupów, musisz przedsięwziąć środki ostrożności, posługując się kartą kredytową. Upewnij się, że masz do czynienia z rzetelnym i wiarygodnym sprzedawcą. Nigdy nie podawaj numerów kart kredytowych w witrynach, które nie mają odpowiednich zabezpieczeń, gdzie twoje informacje mogą być dostępne dla niepowołanych osób trzecich. Jeśli to możliwe, kupuj tylko w sklepach znanych firm.

Porady Teenangels dla dzieci (do lat 10)

1. Rodzice stale ci powtarzają: „Nie rozmawiaj z obcymi". Ta sama zasada obowiązuje, gdy jesteś w Internecie. Nie rozmawiaj z ludźmi, których nie znasz. Pamiętaj, ludzie z Internetu to nie twoi przyjaciele, tylko osoby, z którymi rozmawiasz.

2. Rodzice ostrzegają dzieci przed spędzaniem zbyt dużej ilości czasu przed telewizorem. Przy komputerze też nie należy spędzać zbyt wiele czasu. Dzieciom potrzeba ruchu i ćwiczeń do prawidłowego rozwoju. Musisz mieć czas na zabawy z kolegami. Nie możesz spędzać za dużo czasu w Internecie, to nie może też przeszkadzać ci w innych zajęciach. Popatrz raczej na prawdziwe chmury niż na te z obrazka otwierającego system Windows.

3. Jeśli na ulicy podejdzie do ciebie ktoś nieznajomy i zacznie cię pytać o różne dane personalne, na pewno mu ich nie podasz. Reaguj tak samo, gdy jesteś w Internecie. Nie ujawniaj żadnych informacji o sobie, ani żadnych danych, które pozwoliłyby cię zidentyfikować. Nie polecamy także wysyłania profilów. Nie podawaj nikomu nazwiska, adresu, numeru telefonu, nazwy szkoły czy drużyny sportowej. Pamiętaj, nie potrzeba wielu informacji, by dowiedzieć się wszystkiego o tobie. Także kiedy wypełniasz formularze, uważaj, by nie podawać zbyt wielu informacji o sobie.

4. Nie musisz rozmawiać ani odpowiadać każdemu, kto przyśle ci e-mail czy *instant message*. Nie myśl, że ignorowanie jest niegrzecznością. Jeśli otrzymujesz wiadomości, które sprawiają, że czujesz się nieswojo, powiedz o tym komuś, a jeśli jesteś w kawiarence – wyjdź natychmiast. Jeśli otrzymujesz niepokojące e-maile czy IM, wydrukuj je, zachowaj kopię na dysku i powiedz rodzicom lub nauczycielowi. Pamiętaj, że to nie twoja wina, że ktoś przysyła ci takie listy, ty nie zrobiłeś nic złego, by je otrzymywać.

5. Tak jak należy w określony sposób zachowywać się przy stole, tak samo trzeba w odpowiedni sposób zachowywać się w Internecie. Dobre wychowanie w cyberprzestrzeni polega na przyswojeniu zasad netykiety i postępowaniu zgodnie z nimi. Poznaj zasady obowiązujące w miejscach, w które chcesz się udać, i przestrzegaj ich. Nie bądź niegrzeczny dla innych ludzi w cyberprzestrzeni, nie pisz drukowanymi literami (to odpowiednik krzyku), nie wysyłaj ciągle tej samej wiadomości, nie wdawaj się w kłótnie i obrzucanie wyzwiskami. Ludzie zawsze powinni szanować innych. Nie mów w Internecie rzeczy, których nie powiedziałbyś w realnym świecie. Nie traktuj różnych napaści personalnie – ludzie mówią niemiłe rzeczy i najlepiej to ignorować.

6. Czy otworzysz list, który nie jest do ciebie adresowany albo jest wysłany przez kogoś, kogo nie znasz? Nawet jeśli list z nieznanego źródła jest adresowany do ciebie, osoba wysyłająca go mogła nie wiedzieć nic a tobie, także o tym, ile masz lat. Być może to jakaś reklama, której nie masz ochoty oglądać. Nie otwieraj e-mailów ani nie ściągaj plików od osób, których nie znasz, bo mogą zawierać wirusy. A one mogą poważnie uszkodzić komputer. Zapytaj rodziców, zanim cokolwiek skopiujesz. Nigdy nie odpowiadaj na listy od nieznanego nadawcy. Nie rozmawiasz z nieznajomymi, więc czemu masz czytać e-maile od nich?

7. Nigdy nie podawaj swojego hasła nikomu (oprócz rodziców), nawet najlepszemu przyjacielowi. Każdy, kto zna twoje hasło, może zmienić twój profil, twoje konto, hasło itp. Może tym sposobem wejść w posiadanie różnych danych, takich jak nazwisko, adres, numer telefonu.

8. Na pewno wymieniasz się kartkami czy plakietkami z kolegami, chodzisz z rodzicami na zakupy do supermarketu. Na ogół nie sprzedajesz ani nie kupujesz niczego od kogoś, kogo nie znasz, prawdopodobnie w ogóle nie robisz zakupów bez zgody rodziców. Podobnie w Internecie – dzieci nie powinny kupować ani sprzedawać niczego, nawet jeśli towar wygląda bardzo dobrze i oferta wydaje się

korzystna, ponieważ nie wiadomo, czy ta osoba nie kłamie, czy naprawdę ma rzecz, którą ty chcesz kupić. Bez zgody rodziców nie rób niczego i nie klikaj na niczym, co wymaga pieniędzy. Nigdy nie podawaj informacji dotyczących kart kredytowych rodziców.

9. Jeśli powiem, że niebo jest zielone, pieniądze rosną na drzewach, a ja jestem Elvisem Presleyem, czy mi uwierzycie? Założę się, że macie dość rozsądku, by uznać, że kłamię, i ignorować mnie. Czasem jednak nie jest tak łatwo powiedzieć, czy ktoś kłamie, czy nie. Dlatego nie wierz we wszystko, co usłyszysz, przeczytasz czy zobaczysz w Internecie. Ogłoszenia mogą nie być prawdziwe. Łatwo jest zaprojektować stronę WWW tak, by cię zwieść – informacje mogą być nieprawdziwe lub przesadzone. Nie wiesz, z kim rozmawiasz ani czy ten ktoś mówi prawdę. Pamiętaj, widzisz tylko imię na ekranie – nie widzisz osoby za komputerem na drugim końcu. Tak jak ludzie bywają nieuczciwi w realnym życiu, tak samo bywają nieuczciwi w Internecie.

10. Na pewno słyszeliście o strzelaninie w Colorado i o zamachach bombowych w Oklahoma City. Choć może sądzicie, że wam nigdy nic takiego się nie zdarzy, tak naprawdę może to spotkać każdego. To możliwe, że otrzymacie przerażające pogróżki o bombach, broni czy samobójstwie. Nigdy nie traktujcie takich rzeczy jak żartu. Mogą one być bardzo poważne! Jeśli spotkacie się z kimś wysyłającym pogróżki lub grożącym samobójstwem albo mówiącym o bombach czy broni, natychmiast powiedzcie o tym rodzicom lub nauczycielom. Możecie ocalić czyjeś życie!

11. Nie powinniście wpisywać się na listy klientów ani rejestrować się gdziekolwiek bez zgody rodziców. Jeśli wpiszecie się na listę i proszą was o adres i numer telefonu, podajcie zmyślony. Nie ma powodu, by znali wszystkie dane, przecież wszystko wysyłają przez Internet. Jeśli będą potrzebowali skontaktować się z tobą, mogą wysłać e-mail.

12. Kiedy jesteście wściekli na swoich rodziców, czujecie się nieszczęśliwi w rodzinie, źli na szkołę, na cały świat, pokłócicie się z kolegą, pogadajcie ze starszym rodzeństwem, przyjacielem, kimś z rodziny. Internet nie jest dobrym miejscem do rozładowywania takich uczuć. Istnieją telefony zaufania, do których można zadzwonić i porozmawiać o poważnych problemach.

13. Jeśli ktoś prosi was o zdjęcie, po prostu powiedzcie, że nie macie skanera lub zdjęcia. Nie należy wysyłać zdjęć poprzez Internet.

Wnioski

Sądzę, że pozwolę Teenangels zamknąć dyskusję. Oto co one chciałyby powiedzieć rodzicom, nastolatkom i młodszym dzieciom.

Rodzice...

Nie obawiajcie się Internetu. To ogromnie użyteczne narzędzie i nie może być odrzucane dlatego, że jest nowe i nieznane. Internet może być dla was i waszych dzieci wspaniałą pomocą w budowaniu więzi i rozwijaniu wspólnych zainteresowań. Bądźcie szczerzy ze swymi dziećmi i włączcie się w ich świat. A przede wszystkim przekażcie im to, co wiecie o zachowaniu bezpieczeństwa i o korzystaniu z niezliczonych możliwości Internetu. Powiedzcie dzieciom, by nie obawiały się przyjść do was z jakimikolwiek problemami.

Nastolatki...

Internet to wspaniały sposób poznawania ludzi, wyszukiwania informacji i prowadzenia pogawędek z przyjaciółmi, ale wiążą się z nim pewne zagrożenia. Bądźcie świadomi tych zagrożeń. Zawsze kierujcie się zdrowym rozsądkiem. Choć może się wam wydawać, że was nie spotka nic złego, to jednak złe rzeczy zdarzają się. Bądźcie szczerzy ze swoimi rodzicami, mówcie o tym, co robicie w wirtualnym świecie. Nie wyrzucajcie ze swojego życia realnych ludzi, otwierając drzwi znajomym z ceberprzestrzeni. Nie spędzajcie za wiele czasu w Internecie. Wyjdźcie na zewnątrz i cieszcie się życiem.

Dzieci...

Choć fajnie jest pogadać z kolegami w przyjaznym dzieciom miejscu, musicie więcej czasu spędzać z kolegami z realnego świata. Szkoła, rodzina, przyjaciele są ważniejsi od Internetu. Zawsze mówcie rodzicom o tym, co robicie w sieci. Pozwólcie im usiąść obok i nauczcie ich wszystkiego, co sami wiecie o Internecie. Nie złośćcie się na nich. Musicie wiedzieć, że oni się niepokoją o was i nie chcą, byście w jakikolwiek sposób zostali zranieni. Nie zapominajcie, że ludzie w sieci nie zawsze mówią prawdę. Nie przekazujcie informacji o sobie. Jeśli w Internecie przydarzy się coś złego, zawsze powiedzcie o tym rodzicom lub innej dorosłej osobie, której ufacie. Pamiętajcie, że to nigdy nie jest wasza wina.

Amen!

Załącznik 1

Regulamin korzystania z urządzeń telekomunikacyjnych przez uczniów szkół publicznych okręgu Baltimore

Cel instalacji urządzeń telekomunikacyjnych

Dzięki urządzeniom telekomunikacyjnym klasa wychodzi poza budynek szkolny, uzyskując dostęp do informacji zgromadzonych w lokalnych, stanowych i międzynarodowych sieciach elektronicznych, takich jak Internet. Uczniowie szkół publicznych w okręgu Baltimore uzyskują dostęp do zainstalowanych tu urządzeń telekomunikacyjnych w celach edukacyjnych, takich jak poszukiwanie informacji związanych z programem nauki, przekazywanie wiadomości i wprowadzanie nowoczesnych technik uczenia się. Umiejętność korzystania z zasobów Internetu i komunikowania się za pomocą nowych mediów to podstawowe umiejętności w erze informatycznej, służące osiąganiu lepszych wyników w szkole i sukcesów w XXI wieku.

Dostępne źrodła informacji:

- rządowe publikacje i bazy danych,
- muzea i galerie sztuki,
- mapy i inne pomoce geograficzne,
- encyklopedie i słowniki,
- gazety i czasopisma,
- katalogi biblioteczne i informatory.

Bezpieczeństwo korzystania z urządzeń telekomunikacyjnych

Podejmuje się kroki zmierzające do uczynienia z Internetu bezpiecznego źródła wiedzy. Uczniowie korzystający z Internetu będą pod opieką, zostaną także zapoznani z zasadami odpowiedniego i bezpiecznego korzystania, wybierania i oceniania informacji. Na komputerach używanych przez uczniów będzie także zainstalowane oprogramowanie filtrujące, które powinno blokować dostęp do określonych budzących sprzeciw treści.

Warunki i zasady korzystania z urządzeń

Uczniowie powinni:

- Używać urządzeń telekomunikacyjnych wyłącznie do celów edukacyjnych.
- Porozumiewać się z innymi w kulturalny i grzeczny sposób.
- Zachowywać w tajemnicy własne nazwisko, adres, numer telefonu, hasło, a także szanować poufność tych danych w odniesieniu do innych osób.
- Korzystać tylko z kont pocztowych i haseł zapewnianych przez szkołę.
- Zgłaszać każdy przypadek napastowania sprawującemu opiekę pracownikowi.
- Respektować prawa autorskie i prawo do własności intelektualnej.

Uczniom nie wolno:

- Świadomie bez pozwolenia wchodzić do sieci komputerowej w celu wykorzystania lub zniszczenia danych.
- Odszukiwać lub rozsyłać materiały obraźliwe, obsceniczne, pornograficzne, zagrażające lub zakazane na innej podstawie.
- Instalować prywatne oprogramowanie na szkolnych komputerach.
- Używać urządzeń telekomunikacyjnych do celów komercyjnych lub do działalności niezgodnej z prawem.

Ostrzeżenie

Nie bierzemy odpowiedzialności za jakość informacji. Szkoły publiczne okręgu Baltimore nie biorą odpowiedzialności za żadne informacje, które mogą zostać utracone, zniszczone lub niedostępne z powodu trudności technicznych lub innych.

Kary

Nieprzestrzeganie zasad korzystania z urządzeń telekomunikacyjnych może stanowić pogwałcenie prawa cywilnego lub uchwał rady szkoły. Skutkiem takiego zachowania może być pozbawienie prawa do korzystania z urządzeń telekomunikacyjnych, działania dyscyplinarne ze strony szkoły lub postępowanie sądowe.

Szanowni rodzice/opiekunowie

Prosimy o waszą zgodę na korzystanie przez dziecko z Internetu w szkole. Dokładnie informujemy rodziców i dzieci o ustalonych zasadach korzystania z Internetu. Przed podpisaniem dokumentu proszę przeczytać informacje na odwrocie. Zachęcamy do przedyskutowania z dzieckiem wszystkich zagadnień.

Zgoda ucznia użytkownika

Musi być podpisane przez każdego ucznia.

Niniejszym zgadzam się przestrzegać zasad korzystania z Internetu w szkole. Przyjmuję do wiadomości, że złamanie regulaminu może być zarazem przekroczeniem prawa lub uchwał rady szkoły. W przypadku naruszenia przeze mnie regulaminu mogę zostać pozbawiony prawa korzystania z urządzeń telekomunikacyjnych na terenie szkoły, mogę narazić się na działania dyscyplinarne szkoły i/lub postępowanie karne.

Podpis ucznia Data

Odpowiedź rodziców/opiekunów

Należy wypełnić, jeśli dziecko nie ukończyło 18 lat.

Przeczytałem i zrozumiałem regulamin korzystania z urządzeń telekomunikacyjnych, obowiązujący w szkołach publicznych okręgu Baltimore. Jako rodzic/opiekun ww. ucznia wyrażam zgodę, by moje dziecko korzystało pod opieką nauczyciela z dostępu do urządzeń telekomunikacyjnych.

Przeczytałem i zrozumiałem zasady korzystania z urządzeń telekomunikacyjnych. Zdecydowałem, że moje dziecko nie będzie korzystało z dostępu do tych urządzeń w szkole. Moje dziecko wypełni zadania szkolne, korzystając z innych źródeł.

Załącznik 2

Regulamin korzystania z sieci TrevorNet w Trevor Day School

Zasady i wskazówki dotyczące korzystania ze szkolnej sieci przez całą społeczność szkolną.

Wprowadzenie

W Trevor Day School istnieje sieć komputerowa TrevorNet, która ma ułatwić komunikację wewnątrz społeczności szkolnej i pomiędzy tą społecznością a społecznością globalną. Stały dostęp do źródeł informacji poprawia poziom osiągnięć szkolnych. Wymiana informacji i komunikacja w obrębie szkoły i z innymi ośrodkami naukowymi wzbogaca możliwości uczenia się.

Możliwości sieci

TrevorNet posiada te same aplikacje, które są zainstalowane na laptopach uczniów i wykładowców: Microsoft Office, notatnik itp. TrevorNet zapewnia też dostęp do katalogów bibliotecznych, poczty elektronicznej, edytorów tekstów, a co najważniejsze – uczniowie, wykładowcy i wszyscy pracownicy poprzez TrevorNet mają dostęp do Internetu.

Internet

Kilkanaście milionów komputerów na całym świecie jest ze sobą połączonych przez cyfrową superautostradę, zwaną Internetem. Każda osoba używająca któregoś z tych połączonych komputerów może porozumiewać się z innymi i przekazywać informacje. W ciągu ostat-

nich 20 lat Internet stał się powszechnie wykorzystywaną przechowalnią dla plików tekstowych, dźwiękowych i filmowych. Sieć stron WWW, narzędzie umożliwiające odszukanie informacji w Internecie, ułatwiła korzystanie z Internetu. Sieć WWW uczyniła też z Internetu nowe medium komunikacyjne. Każda osoba mająca komputer, odpowiednie oprogramowanie i dostęp do Internetu może opublikować wszelkie informacje do ogólnoświatowego użytku.

Wskazówki korzystania z TrevorNet i Internetu

Sieć TrevorNet powstała dla dobra uczniów i nauczycieli w celach akademickich. Wprowadzono następujące zalecenia, by wszyscy mogli korzystać z niej bezpiecznie, swobodnie i efektywnie.

Korzystanie z zasobów sieci

Wzajemny szacunek i odpowiedzialność za konsekwencje własnych działań obowiązują w sieci TrevorNet tak samo jak w całej szkole. Komputery, podobnie jak inne zasoby szkolne, są wspólne; priorytet zawsze mają prace szkolne, a uzgodnienia dotyczące dostępu do urządzeń muszą być prowadzone uczciwie. Nie przeszkadzajcie w pracy innym. Nie używajcie języka nieodpowiedniego do szkolnego otoczenia.

Ponieważ szkolne komputery współpracują w TrevorNet w niewidoczny, ale dokładnie zaprogramowany sposób, możliwe jest nieświadome spowodowanie zniszczeń. Nie należy wprowadzać żadnych zmian na twardym dysku jakiegokolwiek szkolnego komputera: zmieniać ustawień, dodawać, usuwać lub uruchamiać programy bez wiedzy i zgody sekcji technicznej.

TrevorNet, zarówno w szkole, jak i poza nią, jest rozległym forum dyskusyjnym. Jego wartość leży w możliwości wymiany różnych poglądów. Kłótnie i ataki personalne nie mieszczą się w zakresie dopuszczanego użycia TrevorNet.

Hasła

Przestrzegajcie poufności hasła. Nie podejmujcie prób wpisywania się jako ktoś inny. Nie podawajcie nikomu swojego hasła ani nie pytajcie o cudze hasło. Zmieńcie hasło, gdy sądzicie, że ktoś może je znać.

E-mail

Te same zasady kultury mówienia i pisania odnoszą się do poczty elektronicznej. Język niestosowny w środowisku szkolnym jest też niedozwolony w TrevorNet. Zanim wyślesz wiadomość, sprawdź, czy zachowuje taki sens i ton, jaki chciałbyś przekazać adresatowi. Nie wysyłaj niepotrzebnych listów, które marnują czas adresata, i nie drukuj wiadomości, jeśli nie są ci potrzebne do prac szkolnych.

Prywatność

Prawo do prywatności jest wysoko cenione i szanowane w Trevor Day School. Jednak pamięć w sieci TrevorNet jest jak szatnia szkolna, w tym sensie, że szkoła ma prawo sprawdzać jej zawartość, by zapewnić poprawne funkcjonowanie systemu i wymóc odpowiedzialne korzystanie z sieci. Aby zachęcić do twórczego myślenia, niezależności i rozwoju intelektualnego, szkoła będzie sprawdzała pliki tylko wtedy, gdy poważnie uzasadnione podejrzenie, że w sieci pojawiły się treści lub działania sprzeczne z regulaminem szkolnym lub z prawem. Włączamy w to zachowania przestępcze, polegające na rozpowszechnianiu treści obscenicznych, brutalnych lub zachęcających do przemocy, plagiaty, pogwałcenie praw autorskich, działania, które zagrażają, obrażają lub zniesławiają osobę lub osoby i materiały, które oczerniają ludzi na podstawie płci, rasy, pochodzenia etnicznego, poziomu sprawności, wierzeń religijnych czy tożsamości seksualnej.

Prawo autorskie i plagiaty

Odpowiedzialni użytkownicy informacji zawsze odnotowują źródła, z których korzystają. Używaj informacji znalezionych w Internecie w taki sam sposób, w jaki używasz informacji z innych publicznych źródeł: zaznacz, skąd materiał pochodzi, by pokazać, że jest wiarygodny. Listy elektroniczne są prywatne i nie powinny być cytowane lub wysyłane do innej osoby bez zgody nadawcy. Plagiat – używanie cudzych słów lub pomysłów jakby były nasze własne – jest zawsze naganny, a może też być złamaniem prawa.

Dostęp do Internetu

Trevor Day School zapewnia dostęp do informacji istniejących w TrevorNet i w Internecie jako sposób edukacji. Te źródła, jeśli są mądrze wykorzystywane, mogą znacząco wzbogacić i zmienić sposób uczenia się. Swoboda dostępu do źródeł istniejących w Internecie równoważy ryzyko napotkania materiałów, których wartość jest wątpliwa. Każdy użytkownik Internetu musi wziąć odpowiedzialność za tę swobodę dostępu.

Bezpieczeństwo

Komunikacja poprzez Internet może mieć o wiele większy zasięg niż obszar, w którym normalnie poruszają się uczniowie Trevor Day School. Nikomu w Internecie nie przekazuj nazwiska, adresu, zdjęć, numeru telefonu. Powiadom nauczyciela lub administrację, jeśli ktoś, kogo znasz wyłącznie z Internetu, prosi cię o dane personalne lub proponuje spotkanie.

Ostrzeżenie

Rodzice, nauczyciele, uczniowie i pracownicy administracji muszą być świadomi, że Trevor Day School nie ma kontroli nad zawartością informacji zgromadzonych w innych połączonych z Internetem komputerach ani nie kontroluje tożsamości osób mających dostęp do Internetu. Uprzedzamy, że w tych komputerach mogą być materiały, które są nielegalne, obsceniczne, obraźliwe, krzywdzące, rasistowskie czy budzące sprzeciw z innych powodów. Administracja i pracownicy nie zezwalają na posiadanie, używanie czy oglądanie podobnych materiałów. Zakazuje się przynoszenia takich materiałów na teren szkoły.

Podpis pracownika Data

Obowiązki uczniów i rodziców/opiekunów

Wszyscy uczniowie używający TrevorNet lub korzystający za jej pośrednictwem z Internetu muszą potwierdzić pisemnie, że oni i ich rodzice lub opiekunowie przyjmują odpowiedzialność związaną z korzystaniem z dostępu do sieci.

Przeczytałem zasady korzystania z sieci TrevorNet i Internetu i przyjmuję do wiadomości, że niestosowanie się do nich może spowodować utratę prawa dostępu do sieci i ewentualne dalsze decyzje dyscyplinarne.

Podpis ucznia Data

Ja również zapoznałem się z zasadami i przyjmuję do wiadomości konsekwencje nieprzestrzegania ich przez moje dziecko.

Podpis rodzica (jeśli uczeń nie ma 18 lat) Data

Załącznik 3

Kontrakt bezpiecznego serfowania

Umowa dotycząca korzystania z Internetu

Chcę korzystać z naszego komputera i z Internetu. Wiem, że istnieją pewne zasady dotyczące właściwego sposobu zachowywania się. Zgadzam się przestrzegać tych zasad, a moi rodzice zgadzają się pomagać mi w tym.

1. Nie podam swojego nazwiska, adresu, numeru telefonu, szkoły ani nazwisk rodziców, ich adresów, numerów telefonów, ani żadnych innych danych, które mogą umożliwić znalezienie mnie komuś, kogo poznam w sieci.

2. Rozumiem, że niektórzy ludzie w Internecie udają, że są kimś innym, niż są naprawdę. Czasem udają, że są dziećmi, gdy w rzeczywistości są dorosłymi. Opowiem rodzicom o wszystkich ludziach, których poznam w Internecie. Powiem również rodzicom o listach, które otrzymam, zanim na nie odpowiem lub zanim wyślę list do nowego znajomego.

3. Nie będę kupować ani zamawiać niczego w Internecie, ani podawać żadnych danych dotyczących karty kredytowej bez zgody rodziców.

4. Nie będę wypełniać w sieci żadnych formularzy, wymagających podania danych personalnych dotyczących mnie lub rodziny bez zapytania najpierw rodziców o zgodę. Chodzi zarówno o formularze związane z udziałem w konkursach, jak i o rejestrowanie się w jakichś witrynach. Zawsze też sprawdzę, jakie zasady ochrony danych obowiązują w danej witrynie. Jeśli nie zapewniają, że moje dane będą chronione, nie przekażę im żadnych danych.

5. Nie będę wdawać się w kłótnie i wojny w Internecie. Jeśli ktoś będzie próbował zacząć kłótnię ze mną, nie będę odpowiadać i powiadomię rodziców.

6. Jeśli zobaczę coś, co mi się nie spodoba lub co sprawi, że poczuję się nieswojo, lub coś, o czym wiem, że rodzice nie pozwoliliby mi oglądać, kliknę na przycisk „wstecz" albo wyloguję się.

7. Jeśli spotkam w Internecie ludzi, którzy robią lub mówią do innych dzieci coś, czego mówić lub robić nie powinni, poinformuję rodziców.

8. Nie będę miał internetowych tajemnic przed rodzicami.

9. Jeśli ktoś przyśle mi obrazki, odsyłacze do stron, o których wiem, że nie powinienem do nich zaglądać, albo listy napisane wulgarnym językiem, powiem o tym rodzicom.

10. Jeśli ktoś poprosi mnie o zrobienie czegoś, czego nie powinienem robić, powiem o tym rodzicom.

11. Nie będę dzwonić do nikogo, kogo poznam w sieci, jeśli rodzice nie wyrażą na to zgody.

12. Nie spotkam się osobiście z nikim, kogo poznam w Internecie, jeśli moi rodzice nie wyrażą na to zgody.

13. Nie wyślę niczego do kogoś poznanego w Internecie, jeśli rodzice nie wyrażą na to zgody.

14. Jeśli ktoś poznany w sieci przyśle mi coś, powiem o tym rodzicom.

15. Nie będę posługiwać się materiałami znalezionymi w Internecie, udając, że są moje.

16. Nie będę mówić złych rzeczy o ludziach i będę przestrzegać zasad netykiety.

17. Nie będę używać wulgarnych słów ani grozić nikomu, nawet w żartach.

18. Wiem, że rodzice chcą mieć pewność, że jestem bezpieczny, i obiecuję słuchać ich, gdy będą mi czegoś zakazywali.

19. Pomogę rodzicom dowiedzieć się czegoś więcej o komputerach i Internecie.

20. Będę dbać o bezpieczne używanie komputera i zawsze sprawdzę, czy nie ma wirusów na pożyczonych od kogoś dyskietkach lub w plikach ściąganych z Internetu.

21. Powiem rodzicom, jeśli zdarzy się coś złego, a oni obiecują, że nie wpadną w panikę w takiej sytuacji.

Przyrzekam stosować się do tych zasad (podpis dziecka).

Przyrzekam pomóc mojemu dziecku w stosowaniu się do tych zasad i nie reagować paniką, jeśli zdarzy się coś złego w cyberprzestrzeni (podpisy rodziców).

Słowniczek terminów

Applet – mały program w języku Java, istniejący wewnątrz strony WWW.
Bajt – jednostka miary informacji równa 8 bitom.
Biuletyn informacyjny (BBS – *bulletin board system*) – komputerowy system „spotkań" i ogłoszeń, który pozwala ludziom prowadzić dyskusje, wymieniać się plikami i ogłaszać wypowiedzi, także wtedy, gdy nie są w tym samym czasie podłączeni do komputera.
Bps – bity na sekundę – *bites per second* – miara szybkości przekazywania danych z jednego modemu do drugiego. Modem 28,8 może przekazać 28 800 bitów na sekundę.
Brama (*gateway*) – ogólnie każdy mechanizm, który zapewnia dostęp do innego systemu, np. telekomunikacja, może być nazwana bramą do Internetu.
Cache (bufor podręczny) – urządzenie do tymczasowego przechowywania danych. Oszczędza czas, pozwala na przechowywanie w pamięci podręcznej przeglądarki ostatnio odwiedzanych stron, dzięki czemu można szybko do nich wrócić.
CD-ROM (*compact disk-read only memory*) – dysk służący tylko do odczytywania, tzn. dane nie mogą być zmieniane lub usuwane.
Ciasteczka (*cookies*) – pliki, które zapamiętują, co użytkownik robił w serwisie, pomaga to spersonalizować serwisy.
CPU (*central processing unit*) – centralna jednostka obliczeniowa komputera, oznacza po prostu procesor (lub procesory).
Cyberprzestrzeń – termin ukuty przez Wiliama Gibsona w powieści „Neuromancer", obecnie używany do opisania różnorodnych źródeł informacji, dostępnych poprzez sieć komputerową.
Daemon – małe programy, które wykonują specjalne zadania. Na przykład program, który sygnalizuje dostarczenie wiadomości.
Domena – ostatnia część internetowego adresu.
Dyskietka (*floppy disk*) – wykonany z plastiku nośnik danych odczytywanych przez komputer.
E-mail (*electronic mail*) – wiadomości, zazwyczaj tekstowe, przesyłane przez komputer.
Ethernet – bardzo powszechna metoda łączenia komputerów w sieć.
FAQ (*frequently asked questions*) – często zadawane pytania. Dokumenty, które wymieniają często zadawane pytania na popularne tematy i zamieszczają odpowiedzi na nie.
Flaming – kierowanie obraźliwych lub obelżywych komentarzy do kogoś poprzez e-mail, grupy dyskusyjne lub czaty.
FTP (*file transfer protocol*) – sposób kopiowania lub przesyłania plików w Internecie. Pliki mogą zawierać programy lub dokumenty.
Gopher – metoda udostępniania materiałów w Internecie. Choć Gopher był szeroko używany na świecie jeszcze kilka lat temu, został w dużym stopniu zastąpiony przez sieć WWW.
Gospodarz (*host*) – każdy komputer w sieci, który wysyła informacje do innych komputerów.
Grupy dyskusyjne (*newsgroups*) – tworzą sieć zwaną Usenetem.
Home page – zazwyczaj pierwsza strona witryny WWW. Z niej rozpoczyna się interaktywna podróż po witrynie.

HTML (*hypertext markup language*) – język przeznaczony do tworzenia stron WWW.
HTTP (*hypertext transport protocol*) – protokół (zestaw instrukcji) przesyłania plików w Internecie. HTTP jest najważniejszym protokołem używanym w Internecie.
Internet – rozległy zbiór połączonych sieci, z których wszystkie używają protokołów TCP/IP, które ewoluowały z ARPANET-u w latach sześćdziesiątych i na początku siedemdziesiątych XX w.
IRC (*internet relay chat*) – usługa umożliwiająca wielu użytkownikom Internetu pogaduszki w czasie rzeczywistym.
ISDN (*integrated services digital network*) – międzynarodowy standard przesyłania danych poprzez linie telefoniczne. Może zapewnić prędkość transmisji do 128 000 bitów na sekundę.
ISP (*internet service provider*) – dostawca usług internetowych, instytucja zapewniająca odpłatnie dostęp do Internetu.
Java – język programowania, który pozwala na wgrywanie programów bezpośrednio poprzez Internet.
Kawiarenka (*chatroom*) – wirtualny pokój, gdzie użytkownicy mogą „rozmawiać" ze sobą, pisząc na klawiaturze.
Kilobajt – 1024 bitów.
Klient – przeglądarka komputera, która „prosi" o informacje. Jeden komputer może być w tym samym czasie klientem i gospodarzem.
Macintosh – komputery produkowane przez firmę Apple Computer.
Modem (*modulator demodulator*) – urządzenie, które umożliwia komputerowi komunikować się poprzez linię telefoniczną z innym komputerem lub siecią.
Napęd dyskietek (*floppy disk*) – urządzenie do odczytu i zapisu informacji na dyskietkach.
Netykieta – etykieta internetowa.
Odsyłacz (*link*) – odpowiednio wyszczególnione miejsce w tekście, jego kliknięcie łączy użytkownika z innym dokumentem, który programista HTML chciałby mu pokazać.
Odsyłacz hypertekstowy – ikony lub słowa na stronie WWW, które łączą z inną stroną poprzez kliknięcie na nich.
Oprogramowanie blokujące – specjalny program, który pozwala blokować dostęp do określonych stron i informacji w Internecie.
PICS (*Platform for Internet Content Selection*) – standaryzowany format systemów rankingowych. PICS sam nie jest systemem rankingowym. Używa się PICS, oceniając strony WWW pod kątem zawartości pornografii, przemocy, seksu.
Plik – zbiór informacji przechowywany w komputerze jako jedna jednostka.
Plug-in – program, który jest rozszerzeniem innego programu. Plug-in zazwyczaj nie może być używany samodzielnie.
POP (*points of presence*) – punkty kontaktowe. Lokalny numer telefonu, pod który dzwoni się w celu uzyskania połączenia z dostawcą usług internetowych.
Procesor – urządzenie chipowe, które przyjmuje dane, wykonuje operacje i podaje rezultaty.
Program – zestaw instrukcji, które należy spełnić, by jakieś zadanie zostało wykonane.
Protokół – zestaw zasad, które przeglądarka stosuje, by zlokalizować i wydostać pliki.
Przeglądarka – program, taki jak Netscape Navigator lub Microsoft Internet Explorer, który umożliwia przeglądanie sieci WWW i czytanie stron.
Przepustowość (*bandwidth*) – szybkość, z jaką informacje mogą przechodzić do twego komputera. Zazwyczaj mierzona w bitach na sekundę. Cała strona tekstu w języ-

ku angielskim to około 16 000 bitów. Szybki modem może przekazać około 30 000 bitów na sekundę.

RAM (*random access memory*) – pamięć używana, by utrzymać programy otwarte i w ruchu.

Serwer – komputer lub pakiet programów, który zapewnia specjalne usługi programom klienta umieszczonym na innych komputerach.

Słowo kluczowe (*keyword*) – słowo, które wpisuje się do wyszukiwarki, by znaleźć informacje na określony temat.

Spamming – niewłaściwe użycie list adresowych, polegające na wysyłaniu tej samej wiadomości do dużej liczby ludzi.

System operacyjny – program, który uruchamia komputer oraz porządkuje i kontroluje pliki, dyski, pamięć itp.

URL (*uniform resource locator*) – adres, który umożliwia przeglądarce znalezienie strony WWW.

Uśmieszki (*emoticons*) – komputerowa nazwa „ikon" oznaczających emocje, ton, język ciała itp.

WWW (*World Wide Web*) – ogół połączonych dokumentów w Internecie, tworzących spójny system, który można oglądać za pomocą przeglądarki.

Wyszukiwarka (*search engine*) – program, który pozwala użytkownikowi wyszukiwać dane z zastosowaniem słów kluczowych.

Tworzenie zakładki – pozwala zachować adres strony w przeglądarce, dzięki czemu w przyszłości może odnaleźć stronę natychmiast.

Zakładka – adres strony WWW zachowany w przeglądarce komputera.

Internet jest niezwykłym miejscem. Pozwala na jednoczesne porozumiewanie się, uczenie i zabawę. Coraz więcej dzieci ma do niego dostęp, i to zjawisko jest ze wszech miar korzystne. Jednak wielu rodziców i opiekunów dzieci dostrzega również ciemne strony Internetu, na przykład wchodzenie na niewłaściwe dla nieletnich strony internetowe lub kontakty z nieznanymi osobami. Parry Aftab ostrzega przed niebezpieczeństwami, które czyhają na dzieci w Internecie, przedstawia kompletny program, umożliwiający korzystanie z bogactw Internetu przy jednoczesnym unikaniu jego zagrożeń. Uczy, jak nadzorować dzieci korzystające z komputera oraz jak posługiwać się programami filtrującymi w celu unikania oszustw i niebezpiecznych reklam.

PATRONAT

Cena 29 zł

Bibl. Nauk Humanistycznych i Społ. UZ
nr inw.: ks 2 - 176807
II 176807/II

Informacje o naszych książkach
można znaleźć w witrynie intern
www.proszynski.pl