

Wydawnictwo Helion ul. Kościuszki 1c 44-100 Gliwice tel. 032 230 98 63 e-mail: helion@helion.pl



Zagrożenia w internecie. Chroń swoje dziecko

Autor: John Lenardon Tłumaczenie: Julia Szajkowska ISBN: 978-83-246-0914-7 Tytuł oryginału: <u>Protect Your Child</u> <u>on the Internet: A Parents Toolkit</u> Format: A5, stron: 200

ionn



Niezbędny poradnik dla odpowiedzialnych rodziców

- Na jakie zagrożenia trzeba zwrócić szczególną uwagę?
- Jak sprawdzić, czym dziecko zajmuje się w internecie?
- · Jakich programów używać, aby zapewnić bezpieczeństwo w sieci?

Internet to wspaniałe narzędzie do wyszukiwania informacji, nawiązywania nowych znajomości czy szybkiego i wygodnego komunikowania się z przyjaciółmi. Jednak łatwość dostępu do sieci powoduje, że wiele osób wykorzystuje ją do nieetycznych celów lub publikuje witryny WWW, których nigdy nie udostępniłbyś swoim dzieciom. Zagrożenia czyhające w internecie, takie jak oszustwa i wyłudzenia czy łatwy dostęp do treści pornograficznych oraz gier hazardowych, są obecnie dość dobrze znane opinii publicznej. Gorzej jest ze znajomością skutecznych narzędzi do ochrony użytkowników sieci, dlatego wiele osób niepotrzebnie ogranicza dostęp do tego niezwykle przydatnego medium.

"Zagrożenia w internecie. Chroń swoje dziecko" to doskonały poradnik dla wszystkich rodziców, którzy chcą lepiej poznać problemy związane z korzystaniem z internetu oraz techniki ochrony swoich dzieci przed niebezpieczeństwami. Czytając tę książkę, dowiesz się, co grozi Twoim pociechom w trakcie korzystania z internetu oraz nauczysz się, jak przekazać im tę wiedzę i uwrażliwić je na zagrożenia. Poznasz sposoby monitorowania pracy swych dzieci w sieci, a także zaczniesz używać skutecznych narzędzi do zapewniania im bezpieczeństwa.

- · Elementy internetu i jego funkcjonowanie
- Zagrożenia związane z korzystaniem z sieci
- · Komunikowanie się z dziećmi i rozmowy o pracy w internecie
- Monitorowanie i kontrolowanie korzystania z sieci
- Stosowanie narzędzi zapewniających bezpieczeństwo

Śpij spokojnie i pozwól swym dzieciom bezpiecznie korzystać z dobrodziejstw ery internetu

Spis treści

NOTA OD WYDAWCY 9 WSTĘP 11

- 1. ZROZUMIEĆ INTERNET 13
- 2. ZAGROŻENIA ONLINE 25
- 3. POROZUMIEWANIE SIĘ, NAUKA I OBSERWACJE 65
- 4. ŚLEDZTWO 77
- 5. ROZWIĄZANIA ZAPOBIEGANIE I OCHRONA 105 DODATKI
- 1. POROZUMIENIE W SPRAWIE KORZYSTANIA Z INTERNETU 153
- 2. PRZEWODNIK PO POTRZEBNYM CI OPROGRAMOWANIU 157
- 3. SKRÓTY STOSOWANE W POKOJACH ROZMÓW 163
- 4. FORMULARZE DO WYPEŁNIENIA 179

SKOROWIDZ 191

Rozdział

4

ŚLEDZTWO

Za każdym razem, kiedy Twoje dziecko — czy ktokolwiek inny, jeśli chodzi o ścisłość — odwiedza stronę internetową, wchodzi do pokoju rozmów czy korzysta z komunikatora, zostawia za sobą ślad. Żeby sprawdzić, czy dziecko przestrzega zasad bezpieczeństwa w Sieci, wystarczy, że przejrzysz oprogramowanie, którego używa, w poszukiwaniu tych śladów.

W tym rozdziale postaram się wyjaśnić, jak przeprowadzić odpowiednie "śledztwo" w najczęściej używanych programach. Opiszę każdy z nich i powiem dokładnie, czego szukać i czego znalezienie powinno Cię zaniepokoić.

Koszmarem każdego rodzica jest odkrycie, że jego dziecko padło ofiarą ataków lub molestowania. W większości przypadków Twoje śledztwo nie wykaże niczego niezwykłego. Jeśli 78

jednak odnajdziesz coś niepokojącego, to z tego rozdziału dowiesz się, gdzie się zgłosić i w jaki sposób poinformować o zaistniałej sytuacji.

Być może nie zechcesz powiadamiać dziecka, że prowadzisz takie badania. To już pozostawiam Twojej osobistej decyzji. Jeśli jednak nie wtajemniczysz dziecka w swoje poczynania na samym początku, to potem, gdy odkryjesz, że dziecko złamało ustanowione reguły, możesz mieć poważne problemy z poruszeniem tego tematu. Zaufanie działa w obie strony, zatem dziecko może silniej zareagować na to, co rodzice zrobili, niż na to, co mówią.

Jeśli masz problemy z przeprowadzeniem rozmowy z dzieckiem, to może warto udać się po radę do szkolnego pedagoga. Poszukaj też w internecie — czasami można znaleźć tam ciekawe pomysły. Przeszukanie Sieci pod kątem wyrażenia "rozmowa z dzieckiem" za pomocą wyszukiwarki, np. Google, daje ciekawe wyniki. Na wyszukanych stronach znajdziesz porady dotyczące tematu rozmów z dzieckiem. W pobliskiej księgarni znajdziesz zapewne pomocną lekturę.

Jeżeli nie jesteś doświadczonym użytkownikiem komputera, to może powinieneś poprosić o pomoc w swoim śledztwie kogoś, kto ma w tej dziedzinie jakąś praktykę. Powinien być to zawodowy informatyk z wieloletnim doświadczeniem. Uważaj w tej mierze na przyjaciół i znajomych, którzy od lat pracują z komputerami i mają się za prawdziwe alfy i omegi — mogą niechcący przegapić ważne szczegóły. Poinformuj osobę, która będzie Ci pomagać, że nadzorujesz działania dziecka, ponieważ chcesz je chronić. Poproś swojego doradcę o zachowanie ścisłej tajemnicy.

Swoje badania przeprowadzaj okresowo. Wraz ze wzrostem wiedzy i obycia dziecka w internecie wzrastają zagrożenia, na jakie może się potencjalnie natknąć.

ŚLEDZENIE DZIAŁAŃ W PRZEGLĄDARCE

Sprawdzanie działań dziecka w internecie najłatwiej jest rozpocząć od uważnego przejrzenia danych przeglądarki, z której korzysta dziecko. Rzut oka na jej historię ujawni ślady:

- stron, które dziecko ostatnio odwiedziło,
- blogów, które być może prowadzi,
- "czatów", na których się udziela,
- jego ulubionych gier komputerowych,
- pobrań plików, jakich ostatnio dokonało.

Sprawdzenie przeglądarki może również dostarczyć dowodów hakerstwa.

Należy sprawdzać *Historię*, *Ulubione* i *Zakładki* przeglądarki, której używa dziecko. Znajdziesz tam wszelkie ślady użytkownika — miejsca on-line, w których bywało.

Obecnie mamy do wyboru kilka, a może nawet kilkanaście przeglądarek internetowych. Opiszę, jak przeprowadzić poszukiwania w najbardziej popularnych. W swoich poszukiwaniach nie skupiaj się tylko na jednej — przeglądaj dane zapisane w każdej przeglądarce zainstalowanej na komputerze; wszak dziecko może korzystać z kilku z nich. Jednej może używać do odrabiania lekcji czy grania, ale nie poinformuje Cię, że za pomocą innej przegląda nieodpowiednie dla niego strony internetowe

W tabeli 4.1 znajdziesz listę najbardziej popularnych przeglądarek i ikony, jakie im odpowiadają.

Ikony te pojawiają się, obok sporej liczby innych, na pulpicie. Są też widoczne razem z nazwami programów w menu *Start*, w opcji *Programy*. Pamiętaj jednak, że znający się na rzeczy użytkownik może podmienić ikony, żeby utrudnić odnalezienie programu. Jeśli zobaczysz ikonę, której nie rozpoznajesz, uruchom program, żeby sprawdzić, czy kryje się pod nią przeglądarka internetowa.

Nazwa przeglądarki	Ikona
Internet Explorer	Internet Explorer
Firefox	Mozilla Firefox
Netscape Browser	Netscape Browser
Opera	Opera

Tabela 4.1. Ikony najpopularniejszych przeglądarek internetowych

Przestrzegając zaleceń podanych w tym rozdziale, będziesz w stanie sprawdzać, w jakim celu Twoje dziecko używa komputera. Zakładam oczywiście, że masz prawo prowadzić takie działania na wspomnianym komputerze. Jeśli Twoje dziecko jest niepełnoletnie, a komputer jest Twoją własnością, to masz prawo przeprowadzać podobne badania zawsze, gdy przyjdzie Ci na to ochota. Jeżeli jednak dziecko jest już pełnoletnie i posiada własny komputer, to raczej nikt nie przyzna Ci prawa do przeprowadzenia na nim przeszukania bez zgody dziecka. Aby uzyskać pewność co do przysługujących Ci praw, skontaktuj się z odpowiednimi władzami — zapytaj na komisariacie policji, do czego masz prawo.

Plik z historią

Domyślne ustawienia przeglądarek internetowych sprawiają, że programy te trzymają dane na temat każdej odwiedzanej strony. Jeśli musisz powrócić do strony, którą oglądałeś ostatnio, możesz dostać się do niej poprzez plik *Historia* dostępny w każdej przeglądarce. Oznacza to, że nie musisz martwić się zapamiętywaniem adresu strony.

Jeżeli chcesz sprawdzić, jakie strony przeglądało ostatnimi czasy Twoje dziecko — włączając w to strony czatów, blogów i gier internetowych — wystarczy że przejrzysz plik z historią połączeń. Zobaczysz w nim listę wszystkich odwiedzanych stron, a żeby się dowiedzieć, czemu poświęcona jest konkretna witryna, wystarczy kliknąć jej adres. Oto jak się do tego zabrać.

Microsoft Internet Explorer

Jeżeli korzystasz z domyślnej przeglądarki systemu Windows i chcesz poznać historię wizyt w internecie, musisz wykonać następujące czynności.

1. Z menu *Widok* wybierz *Pasek eksploratora*, a z niego pozycję *Historia*.

about:blank - Microsoft Internet Explorer	×
Plik Edycja Widok Ulubione Narzędzia	Pomoc
→ Paski narzędzi Pasek stanu	Wyszukaj 👷 Ulubione 🚱 🔗 🖉 📄 🔝 🥸
Adres 💣 abox Pasek eksploratora	Wyszukaj Ctrl+E 💽 🚽 Przejdź Łącza 🎽
Przejdź do Zatrzymaj Esc Odśwież F5	Ulubione Ctrl+I Historia Ctrl+H Foldery
Rozmiar tekstu Kodowanie	Porada dnia Dyskusja
Źródło Report o prywatności Petry ekran E11	
	-
Pokazuje pasek Historia.	×

2. Kliknij dowolny odnośnik, aby zobaczyć zawartość strony odwiedzanej przez użytkownika.



Mozilla Firefox

82

Jeśli natomiast korzystasz z przeglądarki Firefox, wykonaj, co następuje.

1. Z menu Historia wybierz opcję Wyświetl w panelu bocznym.



2. Historia odwiedzin pojawia się w nowym oknie po lewej stronie.



3. Kliknij odnośnik, aby odwiedzić wybraną stronę.

Netscape Browser

W przypadku korzystania z przeglądarki Netscape Browser:

1. Historia pojawi się, gdy wybierzesz zakładkę *History* (jeśli nie widzisz bocznego menu, udaj się do menu *View* i wybierz opcję *My Sidebar*).



2. Kliknij odnośnik, aby obejrzeć żądaną stronę.

Opera

Korzystając z Opery, postępuj zgodnie ze wskazówkami:

1. Z menu Narzędzia wybierz opcję Historia.



2. Pojawi się historia oglądanych stron. Kliknij dwukrotnie dowolny odnośnik, aby udać się na wybrana stronę.

()Historia - Opera				
Plik Edycja Widok Zekładki	Widżety Narzędzia Pomoc			
Nowa GGooge	🗙 💭 Historia	×		-
🕑 Otwórz 👻 Usuń 🍪 Widok 🖲 🔍 Znajdź				
Nazwa	*Adres	Odwiedzono	Popularność	
🕆 🧰 Dzisiaj				
* apple.com.pl/				
🖸 Apple IMC Poland	http://www.apple.com.pl/quickti	2006-12-13 10:43:23	1	
Apple - iPod + iTunes	http://www.apple.com.pl/itunes	2006-12-13 10:43:21	1	
Apple IMC Poland	http://www.apple.com.pl/	2006-12-13 10:43:17	1	
apple.com/				
🚺 Apple - QuickTime	http://www.apple.com/guicktime/	2006-12-13 10:43:26	1	
▼嶺 gadu-gadu.pl/				
读 Gadu-Gadu.pl - Pols	http://www.gadu-gadu.pl/	2006-12-13 10:43:52	1	
▼G google.pl/				
G napster - Szukaj w	http://www.google.pl/search?hl	2006-12-13 10:43:36	1	
G Google	http://www.google.pl/	2006-12-13 10:44:00	1	
mapster.com/				
Napster	http://www.napster.com/	2006-12-13 10:43:39	1	
Oportal.opera.com/				
redir.opera.com/				
Image: Searchportal.informatio				
🗀 Wczoraj				
Wcześniej w tym tygodniu				
Wcześniej w tym miesiacu				
Dawpiej				

84

Czego szukać?

Będąc już w pliku z historią działań w internecie, szukaj stron o tematyce dla dorosłych, witryn pobierania, witryn poświęconych hakerstwu, a także zwracaj uwagę na wszystkie strony, które wydadzą Ci się nieodpowiednie dla Twojego dziecka. Jeśli w czasie przeglądania historii odwiedzanych stron poczujesz co do którejś wątpliwości, pamiętaj, że klikając jej nazwę, możesz z łatwością obejrzeć zawartość.

Podczas swojego śledztwa możesz natknąć się na strony pornograficzne czy inne zawierające równie nieodpowiednią treść. Pamiętaj jednak, że dziecko nie musiało odwiedzać ich celowo. Mogło zostać skłonione do wizyty na nich podstępem — wystarczyło, że kliknęło hiperłącze w poczcie elektronicznej. Wiadomość e-mail mogła zawierać obietnicę pobrania darmowej muzyki ze wspomnianej strony. Dziecko, po kliknięciu odnośnika, znajduje się nagle na nieodpowiedniej dla niego stronie. Poza tym wyszukiwarka może zwracać niepoprawne wyniki wyszukiwania, ponieważ właściciele witryn umieszczają w kodzie niewłaściwe słowa kluczowe (o silnikach wyszukiwarek pisałem więcej w rozdziale 2.).

Badając historię działalności dziecka w Sieci, powinieneś raczej szukać pewnych powtarzających się wzorów zachowań niż pojedynczych objawów. Jeżeli dziecko powraca na daną stronę, to może to być powód, aby poważnie z nim porozmawiać.

Musisz też mieć na uwadze fakt, że niektóre dzieci wiedzą, w jaki sposób czyścić historię połączeń internetowych. Na przykład w przeglądarce Internet Explorer można wykonać tę operację, wybierając z menu *Narzędzia* opcję *Opcje internetowe...* Po jej wybraniu ukaże się okno dialogowe z przyciskiem *Wyczyść historię*. Po jego kliknięciu wszystkie wpisy w pliku z historią zostaną wyczyszczone. Twoje dziecko może znać tę funkcję i czyścić historię połączeń za każdym razem, gdy korzysta z internetu. Jeżeli wiesz, że dziecko całe godziny spędziło w Sieci, ale po sprawdzeniu historia połączeń okazuje się pusta, to zapytaj dziecko, z jakich powodów ją opróżniło. Pamiętaj też, że istnieje możliwość usuwania jej pojedynczych wpisów. Dziecko może, przykładowo, wyrzucać wpisy dotyczące stron dla dorosłych, które ostatnio odwiedziło. (Sugerowane działania, jakie możesz podjąć, jeżeli podejrzewasz, że dziecko usuwa wpisy z historii, znajdziesz w rozdziale 5., w opisie oprogramowania śledzącego użytkowników w Sieci).

Sprawdzanie Ulubionych i Zakładek

86

Większość przeglądarek internetowych daje Ci możliwość stworzenia listy stron często odwiedzanych. Jest to tak zwana lista *Ulubionych* lub *Zakładek*. Posiadanie takiej listy pozwala odwiedzać ulubione strony bez wpisywania ich pełnego adresu w przeglądarce. W zamian wybierasz stronę z menu *Ulubione,* które znajduje się na górze okna przeglądarki, klikasz ją i już jesteś na miejscu.

Dodawanie strony do listy ulubionych jest banalnie proste. Załóżmy, że jesteś na stronie Polskiej Agencji Prasowej. Jeżeli zechcesz do niej powracać, ale nie chcesz za każdym razem wpisywać jej adresu, to możesz dodać ją do *Ulubionych*:

- 1. Uruchom stronę PAP w przeglądarce (w opisywanym przykładzie jest to Internet Explorer).
- 2. Kliknij menu Ulubione na górze okna przeglądarki.
- 3. Następnie wybierz opcję *Dodaj do ulubionych*... i potwierdź swój wybór, wciskając przycisk *OK* w oknie, które się pojawi.

Bardzo możliwe, że Twoje dziecko stworzyło listę ulubionych stron. Jeżeli często odwiedza swój blog, to zapewne dodało go do tej listy, aby ułatwić sobie dostęp do tej strony. Mogą się na niej również znaleźć wszelkie pokoje rozmów, w których często się pojawia, a także jego ulubione strony internetowe.

Dostęp do list w przeglądarce Internet Explorer uzyskasz, wybierając menu *Ulubione*. Przeglądarki Firefox, Netscape i Opera pokazują ją po wybraniu menu *Zakładki*¹.

Jeśli któryś z elementów listy budzi Twój niepokój, to kliknij jego nazwę, a przeniesiesz się na stronę, która została zapisana na liście.

Oczywiście możesz nie znaleźć żadnych elementów Zakładek czy Ulubionych, co może oznaczać, że dziecko żadnych nie utworzyło. Jeśli wie o tym, jak działają, powinieneś je zapytać, dlaczego z nich nie korzysta.

Pamiętaj też o tym, że można zmieniać nazwy i etykiety witryn w liście ulubionych stron. Kiedy dodajesz stronę do listy, to w okienku dialogowym *Dodaj do ulubionych* czy *Dodaj do zakładek* pojawi się pole z sugerowaną nazwą strony. Możesz ją oczywiście zmienić zgodnie z własnymi upodobaniami. Znaczy to mniej więcej tyle, że Twoje dziecko może zmienić nazwę strony hazardowej na bardziej niewinną, choćby "Disney". Jedynym sposobem na to, żeby się dowiedzieć, jakie strony naprawdę kryją się na liście ulubionych, jest ich otwieranie.

WYKRYWANIE PROGRAMÓW TYPU SPYWARE I ADWARE

Stwierdzenie, czy na komputerze znajdują się programy typu *spyware* i *adware*, nie należy do prostych zadań. Chociaż większość z nich instaluje się na komputerze w wyniku przeglądania stron internetowych, to w samych przeglądarkach programy te nie pozostawiają żadnych śladów. Pewność dadzą Ci

¹ Bookmarks w przeglądarce Netscape — przyp. tłum.

jedynie programy antywirusowe (które, jak pisałem już w rozdziale 2., nie zawsze są skuteczne). Jednak zawsze pojawiają się pewne charakterystyczne znaki zainfekowania komputera. Oto lista najczęściej spotykanych:

- w przeglądarce pojawia się nagle nowy, nieinstalowany przez Ciebie pasek zadań,
- jesteś ciągle zasypywany gradem wyskakujących okienek reklamowych,
- wpisujesz w przeglądarce nazwę jednej witryny, a Internet Explorer otwiera zupełnie inną,
- strona domowa zdefiniowana w przeglądarce nagle zostaje zastąpiona inną,
- komputer zaczyna pracować bardzo wolno,
- na pasku systemowym (prawy dolny róg ekranu) pojawiają się nowe ikony,
- niektóre klawisze nie działają tak, jak powinny (np. *Tab* może nie przenosić kursora do kolejnego pola).

W rozdziale 5. pokażę, jak wykrywać i usuwać programy szpiegujące i reklamowe. Poza tym udzielę w nim kilku rad dotyczących sposobów ich unikania.

ŚLEDZENIE PRACY KAMER INTERNETOWYCH

Wydawałoby się, że nie ma prostszej rzeczy niż stwierdzenie, czy dziecko korzysta z kamery internetowej — przecież widać ją, gdy jest podłączona do komputera. Jednak niektóre dzieci ukrywają kamery przed swoimi rodzicami.

Aby kamera internetowa działała, niezbędne jest zainstalowanie specjalnego oprogramowania. Zatem jeśli chcesz sprawdzić, czy dziecko z niej korzysta, musisz szukać tego oprogramowania.

88

Programy do obsługi kamer internetowych mają z reguły w nazwie słowa takie jak "Webcam", "Quickcam", "Camera" czy "Kamera", więc powinny być łatwe do znalezienia. Ich ikony, znajdujące się na pulpicie, mają najczęściej kształt małej kamerki. Podobna kamerka powinna się pojawić również w prawym dolnym rogu ekranu.

Jednak ikony i nazwy plików zmienia się łatwo, więc może się zdarzyć, że będzie trzeba wnikliwie przeszukać cały komputer. W takiej sytuacji możesz potrzebować pomocy doświadczonego użytkownika komputera.

Jeżeli się okaże, że Twoje dziecko ukrywa przed Tobą kamerę internetową, to porozmawiaj z nim o przyczynach takiego postępowania.

ŚLEDZENIE KOMUNIKATORÓW

Powinieneś wiedzieć, z kim Twoje dziecko rozmawia poprzez komunikator. Każdy z programów tego typu przechowuje listę kontaktów. Większość z nich posiada również archiwum przeprowadzonych rozmów, ale tę ich funkcję dziecko może wyłączyć, kiedy tylko zechce.

Aby przejrzeć listę kontaktów w Gadu-Gadu, kliknij dwukrotnie jego ikonę znajdującą się w prawym dolnym rogu ekranu (pasek systemowy):



Pojawi się okienko wyglądające tak:



Jeśli znajdziesz nieznane Ci imiona, zapytaj dziecko, kim są ci ludzie i w jaki sposób ich poznało.

ŚLEDZENIE WIADOMOŚCI POCZTY ELEKTRONICZNEJ

Poczta elektroniczna jest bardzo rozpowszechniona wśród młodych ludzi, a wiadomości, jakie wymieniają między sobą, mogą Ci wiele powiedzieć. Wiadomości e-mail powiedzą Ci, czy dziecko padło ofiarą prześladowania przez internet lub czy napastuje w ten sposób innych. Poza tym możesz sprawdzić, czy dziecko nie utrzymuje kontaktów z pedofilem. Przeglądanie poczty dziecka będzie dla Ciebie nieocenionym źródłem informacji. Na rynku dostępne są różne programy pozwalające odbierać pocztę, ale największą popularnością cieszą się Microsoft Outlook i Microsoft Outlook Express. Program Outlook Express instaluje się automatycznie wraz z systemem Windows, natomiast Microsoft Outlook jest częścią pakietu Microsoft Office.

Uruchomienie tych programów polega na podwójnym kliknięciu jednej z ikonek pokazanych w poniższej tabeli.

Klient poczty elektronicznej	lkona
Microsoft Outlook	Microsoft Outlook
Microsoft Outlook Express	Dutlook Express

Po uruchomieniu któregoś z nich zobaczysz po lewej stronie okna listę folderów. Kliknij dowolny z nich, a pokażą Ci się wiadomości w nim zapisane.

Do wysyłania i odbierania poczty dziecko może także korzystać z interfejsu WWW. Wiele portali pozwala zakładać darmowe konta poczty elektronicznej — usługę taką często określa się angielskim słowem *webmail*². Dziecko musi jedynie założyć konto pocztowe — co jest bardzo proste — i przez stronę WWW może wymieniać listy z dowolną osobą na świecie.

W Polsce usługi tego typu świadczy kilka wielkich portali internetowych. Jednym z popularniejszych jest Onet, który pod adresem *http://poczta.onet.pl* pozwala założyć darmowe konto pocztowe. Żeby wymieniać listy e-mail, dziecko musi jedynie wypełnić krótki formularz. Potem może się już zalogować na swoje konto i rozpocząć korespondencję. Poczta *webmail* działa

² Poczta internetowa — *przyp. tłum.*

prawie tak samo jak program Microsoft Outlook, ale jest uruchamiana w przeglądarce internetowej. Poniżej zamieszczam zrzut z ekranu panelu logowania poczty portalu Onet:



W przeglądarce pozostaną ślady korzystania z poczty w serwisie internetowym. W pliku z historią połączeń znajdziesz adres witryny, która udostępnia takie usługi, a dziecko najprawdopodobniej doda go do listy ulubionych stron.

Jeśli odkryjesz, że dziecko korzysta z poczty na witrynie WWW, to będzie Ci potrzebny jego login (nazwa użytkownika) i hasło, aby uzyskać dostęp do jego konta. Strony te zapewniają ochronę haseł, więc odnośniki z pliku z historią nie zadziałają. Niezbędne informacje możesz uzyskać od dziecka, ale możesz też zainstalować program śledzący działalność w Sieci (takie programy omówię szczegółowo w rozdziale 5.).

Niezależnie od tego, czy dziecko korzysta z poczty internetowej czy też z klienta poczty, jak Outlook, musisz mieć świadomość, że każda z wiadomości w nich zawartych może zostać usunięta. Jeżeli wiesz, że dziecko używa poczty elektronicznej, a w skrzynce odbiorczej nie znajdujesz żadnych wiadomości, powinieneś natychmiast zapytać je, dlaczego wszystkie usunęło.

ŚLEDZENIE DZIAŁALNOŚCI NA GRUPACH DYSKUSYJNYCH

Dzieci, dzięki grupom dyskusyjnym, mają kontakt z ludźmi w dowolnym wieku, żyjącymi na całym świecie. Grupy prowadzą rozmowy na każdy temat, jaki możesz sobie wymyślić, oferując tym samym możliwość zgłębienia wiedzy, z której chętnie korzystają dzieci. Niestety, niektóre z nich mogą zawierać informacje, które uznasz za nieodpowiednie dla Twojego dziecka.

Żeby uczestniczyć w życiu grupy, trzeba mieć program, który pozwoli odczytać wiadomości na nią wysyłane. Istnieje wiele programów posiadających takie funkcje, ale największą popularnością cieszy się Microsoft Outlook, ten sam program, który instaluje się z systemem Windows. Przeprowadzenie inspekcji działalności dziecka w grupie dyskusyjnej nie nastręcza wielu problemów, ponieważ musi ono subskrybować każdą grupę, więc wszystkie wiadomości będą widoczne w programie. Oczywiście dziecko ma możliwość usunięcia subskrypcji.

Ponieważ wiadomości grup dyskusyjnych odczytuje się najczęściej w programie Outlook Express, będę dalej mówić właśnie o nim. Uruchom go, klikając dwukrotnie jego ikonę, albo uruchom go z menu startowego *Start/Programy/Outlook Express*.

Otrzymasz ekran zbliżony do pokazanego na następnej stronie.

Aby zbadać zawartość wiadomości grupy dyskusyjnej, przejrzyj wszystkie subskrybowane grupy umieszczone w lewej kolumnie. Ich nazwy powinny wskazywać na tematykę, której są poświęcone, ale jeżeli chcesz sprawdzić jej zawartość, kliknij dowolną z nich. Po kliknięciu wybranej nazwy w środkowej



kolumnie pojawią się wiadomości (posty) wysyłane na tę grupę. Przy niektórych pojawi się znak "+". Kliknij go, aby odkryć odpowiedzi wysyłane na dany post. Kliknięcie nagłówka w środkowej kolumnie spowoduje wyświetlenie treści wiadomości w kolumnie po prawej stronie okna.

W internecie można znaleźć wiele darmowych "czytników" wiadomości grup dyskusyjnych — slrn-pl, 40tude, NNR, OE. Przeszukanie dysku pod kątem takich programów pozwoli Ci odkryć, które z grup subskrybuje Twoje dziecko.

Jeśli podczas swoich poszukiwań natrafisz na grupę, która według Ciebie nie jest dla dziecka odpowiednia, to porozmawiaj z nim o tym problemie.

WYKRYWANIE PROGRAMÓW CHRONIĄCYCH PRYWATNOŚĆ

Istnieją specjalne programy zaprojektowane w celu wykrywania i usuwania śladów wszelkiej działalności użytkownika komputera w internecie. Usuwają na przykład ślady bytności w Sieci, kasując wpisy z historii i inne pliki. Mogą też usunąć informacje o pobraniach z sieci *peer-to-peer*, rozmowach w pokojach rozmów i wiele innych. Niektóre z nich potrafią czyścić historię wszystkich plików otwieranych ostatnio w edytorze tekstu czy przeglądarce obrazów. Co więcej, potrafią też usuwać historię wystąpień na grupach dyskusyjnych. Jeżeli dziecko korzysta z jakiegoś programu tego typu, to na komputerze nie pozostaną ślady jego działań.

Programy takie kosztują około 150 złotych za licencję, ale w Sieci można oczywiście znaleźć ich darmowe odpowiedniki. W ich nazwach pojawiają się często słowa "wipe³" czy "scrub⁴".

Skoro oprogramowanie tego typu wymazuje wszelkie ślady aktywności użytkownika komputera, to jego użycie staje się widoczne w oczywisty sposób. Jeżeli Twoje dziecko właśnie spędziło sześć godzin w internecie, a Ty nie odnajdziesz żadnych śladów jego działań w *Historii* przeglądarki, to spokojnie możesz założyć, że korzysta ono z takiego programu albo ręcznie usuwa wszystkie wpisy.

Jest to poważny powód do obaw. Dziecko może oglądać strony pornograficzne albo ściągać nielegalnie muzykę z internetu.

Samo usunięcie programu czyszczącego nie rozwiąże problemu. Przecież dziecko może później zainstalować inny produkt tego typu. Najlepszym rozwiązaniem wydaje się w tym przypadku rozmowa z dzieckiem o tym, dlaczego ukrywa ślady swojej pracy. Możesz też rozważyć użycie programu śledzącego aktywność w internecie — programy takie nie podlegają działaniu programów czyszczących (więcej informacji na ich temat znajdziesz w rozdziale 5.).

³ Ang. wycierać — *przyp. tłum.*

⁴ Ang. szorować — *przyp. tłum.*

MYŚLĘ, ŻE MOJE DZIECKO JEST HAKEREM

Swego czasu w gazetach było głośno o włamaniach do systemów komputerowych znanych firm i o tym, że ich sprawcami były dzieci. W większości przypadków ich rodzice nie mieli najmniejszego pojęcia o tym, co robią ich pociechy.

Niektóre zachowania mogą wskazywać na to, że dziecko próbuje swoich sił w hakerstwie. Jednak równie dobrze mogą one wskazywać na silne zainteresowanie komputerami i chęć zwiększenia swojej wiedzy w tej dziedzinie. Jak już wspominałem w rozdziale 3., rozmowa z dzieckiem stanowi Twoją pierwszą linię obrony. Upewnij się, że zna ono prawne konsekwencje hakowania.

Pamiętaj, że poza specyficznym zachowaniem będą też inne wskazówki świadczące o tym, że masz w domu hakera.

Hakowanie trwa

Opanowanie technik hakowania zajmuje dużo czasu. Poza tym młody człowiek musi jeszcze wyszukać odpowiednie narzędzia i porozumieć się z innymi znającymi ten temat. Dziecko może spędzać coraz więcej czasu przed ekranem monitora z wielu uzasadnionych powodów, jednak powinieneś sprawdzić, dlaczego nagle zmieniło swoje nawyki. Jeśli przyczyną jest zainteresowanie hakerstwem, to musisz poszukać zainstalowanych programów służących temu celowi — takich jak te opisane w kolejnym punkcie.

Hakowanie wymaga odpowiednich narzędzi

Zaatakowanie systemu komputerowego wymaga potężnego zestawu narzędzi. Jeśli w systemie dziecka pojawią się nowe programy, spróbuj je uruchomić. Bardzo możliwe, że już ich nazwa będzie wskazywała, do czego służą. Jako przykład podam tu nazwy dwóch popularnych programów hakerskich — *John the Ripper*, program do łamania haseł, i *NetSlayer*, służący do przejmowania kontroli nad cudzym komputerem.

Dzięki nim można zaatakować inny komputer w Sieci, ale mogą też służyć one do nauki. Musisz jednak sprawić, żeby dziecko zrozumiało, że nie istnieją żadne dozwolone przez prawo powody, dla których można choćby próbować zaatakować cudzy komputer. Wyjaśnij że, takie działania są nielegalne i dziecko może z ich powodu trafić do więzienia, jeśli zostanie złapane.

Jeśli nie masz pewności, które programy mogą być wykorzystane do włamań, to poproś o radę profesjonalistę.

Hakowanie wymaga badań

Samo pobranie oprogramowania nie wystarcza. Poza tym trzeba się dowiedzieć, jak go właściwie używać. Szukaj czasopism, które specjalizują się w zagadnieniach hakerskich, jak *Hakin9*, czy też kultowy już kwartalnik wydawany w USA: 2600: The Hacker Quarterly, czy książek poświęconych ochronie komputera. Sprawdzaj też listę ulubionych stron dziecka i subskrybowane grupy dyskusyjne pod kątem zagadnień dotyczących włamań do systemów.

Hakowanie wymaga sprzętu

Jeżeli dziecko domaga się coraz lepszego sprzętu komputerowego, musisz się upewnić, że faktyczne potrzebuje go do gier, a nie do zaawansowanego włamywania się. Niektóre formy ataku wymagają szybszego łącza internetowego lub szybszego sprzętu. Dziecko może prosić Cię o lepszy komputer tylko po to, żeby przechwalać się nim w szkole, ale może warto się temu lepiej przyjrzeć. 98

Prawdziwy haker musi również znać system operacyjny UNIX lub jego odmianę — Linux. Wielkie korporacje korzystają raczej z różnych odmian systemu UNIX niż z systemów Microsoft Windows czy Macintosh. Jeśli odkryjesz w komputerze jeden z tych systemów, powinieneś zapytać dziecko, dlaczego się nim zainteresowało. Pamiętaj, że głęboka znajomość wielu systemów komputerowych stanowi dobre podwaliny pod karierę i wcale nie musi świadczyć o tym, że dziecko czy nastolatek uczy się hakować.

Hakowanie wymaga znajomości technik socjologicznych

Jednym z najprostszych sposobów włamywania się do systemów komputerowych jest manipulowanie ludźmi, którzy w wyniku działań hakera ujawniają informacje o systemie. Umiejętność tego typu nazywa się **socjotechniką**. Prosty przykład z życia dziecko może podejrzeć przez ramię rodzica hasło dostępowe do systemu. Może też zajrzeć do szuflady, żeby sprawdzić, czy ktoś nie zapisał go na skrawku papieru. Jeżeli dziecko zechce włamać się do systemu operacyjnego w szkole, to może zadawać nauczycielom pytania w stylu: jakim systemem dysponuje szkoła, jak wykonywane są kopie zapasowe danych i gdzie są przechowywane nośniki z nimi. Wielu nauczycieli przypisze takie zachowania głodowi wiedzy, a nie przygotowaniom do włamania. Dziecko może wykorzystać tu przewagę, jaką daje mu niewinny wygląd, i w ten sposób uzyskać cenne informacje, zadając pytania czy obserwując czyjąś pracę na komputerze.

Jeśli dziecko próbuje podejrzeć hasło lub dopytuje się o nie, to wytłumacz mu, jak ważne jest utrzymywanie go w tajemnicy przed wszystkimi. Naucz je, żeby prosiło innych ludzi o oddalenie się od klawiatury, gdy wpisuje swoje hasło. Powiedz mu, że nigdy nie wolno mu zdradzić go ani przyjaciołom, ani krewnym, niezależnie od powodów. Jeżeli podejrzewasz dziecko o hakerstwo, to porozmawiaj z nim o tym natychmiast. Przede wszystkim wyjaśnij, że same próby włamania do systemu są nielegalne. Dziecko może dostać karę więzienia za te próby albo zostać zawieszonym w prawach ucznia czy nawet powtarzać rok.

Poinformuj je również, że większość prób włamań da się wyśledzić, co nieuchronnie prowadzi do komputera, z którego zostały one podjęte. Niewielu jest na świecie hakerów, którzy nigdy nie zostali złapani, niezależnie od tego, jak byliby dobrzy.

Jeśli dziecko podejmie próbę włamania do komputerów szkolnych czy jakiejś firmy, może zostać obciążone kosztami działań mających zapobiec atakowi czy prowadzących do odzyskania uszkodzonych danych. W przypadku gdy dziecko jest niepełnoletnie, to Ty zostaniesz obciążony kosztami.

Wreszcie porozmawiaj z dzieckiem o moralnych i etycznych implikacjach hakowania. Jest to naruszenie cudzej prywatności, nawet jeżeli sprawa dotyczy włamania do systemu firmy. Włamania do systemów powinny być traktowane jako bardzo poważne wykroczenia i nigdy nie należy podejmować się takich działań.

CO MOŻESZ ZROBIĆ?

Jeśli w czasie swoich badań napotkasz któryś z opisanych tu problemów, zapewne będziesz chciał go zgłosić odpowiednim władzom. Jednak sprawa wyboru odpowiednich ku temu osób nie jest oczywista. Na przykład jeśli dziecko padło ofiarą prześladowania przez sieć, to policja może uznać, że nie zostało popełnione przestępstwo, i nie będzie chciała interweniować.

Poniżej znajdziesz listę problemów, jakie możesz napotkać podczas prywatnego śledztwa, i kilka rad, jak sobie z nimi radzić.

Pornografia i przemoc w Sieci

100

Jeżeli dziecko ogląda strony z materiałami pornograficznymi lub zawierającymi sceny przemocy, to raczej nie masz możliwości zamknięcia witryny powodującej kłopoty. Witryny mogą być zarejestrowane w dowolnym kraju na świecie, a to, co jest nielegalne w jednym państwie, wcale nie musi kłócić się z prawem innego. Najlepszym rozwiązaniem w takim przypadku wydaje się przeprowadzenie z dzieckiem szczerej rozmowy oraz, jeżeli uznasz to za stosowne, instalacja specjalnego oprogramowania, które zablokuje niechciane strony. Oprogramowanie takie (znane jako programy kontroli rodzicielskiej) zostanie szerzej omówione w rozdziale 5.

Pornografia i przemoc na grupach dyskusyjnych

Zdjęcia pornograficzne i zawierające obrazy pełne przemocy są szeroko dostępne na grupach dyskusyjnych. Gdy się zorientujesz, że dziecko jest członkiem grupy, która nie jest dla niego odpowiednia, możesz poprosić swojego dostawcę usług internetowych o usunięcie takiej grupy. Jeżeli jego reakcja nie będzie zadowalająca, zawsze możesz zmienić usługodawcę.

Nękanie

Policja zainteresuje się sprawą nękania właściwie dopiero wtedy, gdy dojdzie do naruszenia nietykalności osobistej.

Samo powiedzenie dziecku "broń się przed łobuzem" też nie rozwiązuje problemu. Dziecko zapewne szuka u Ciebie wsparcia i bardzo ważne jest, by czuło, że ma w Tobie oparcie niezależnie od zaistniałych okoliczności.

Jeżeli czujesz, że samodzielnie nie sprostasz problemowi prześladowania dziecka, spróbuj znaleźć w Sieci hasła "nękanie

dzieci" czy "prześladowanie dzieci" — na pewno znajdziesz pomocne strony. Możesz też porozmawiać z dyrektorem szkoły, do której uczęszcza dziecko, czy pedagogiem szkolnym i poprosić ich o pomoc. Należałoby również poinformować o fakcie rodziców nękającego.

Groźby w wiadomościach e-mail

Ustanowiono wiele praw, zgodnie z którymi rozsyłanie niechcianej poczty (spamu) jest nielegalne. Jednakże ich egzekucja nastręcza problemy, jako że spam może pochodzić z dowolnego kraju świata.

W takiej sytuacji możesz na pewno złożyć skargę u dostawcy internetu. Jeżeli mieszkasz w Polsce, możesz skontaktować się także z Urzędem Ochrony Konkurencji i Konsumentów. Obecnie zapowiada się, że walka z wiadomościami o nieodpowiedniej treści będzie długa i żmudna. Najlepszą obroną przed nimi wydaje się zainstalowanie odpowiedniego oprogramowania chroniącego przed spamem.

Prześladowanie i nękanie w pokojach rozmów

W sytuacji, w której dziecko miało złe doświadczenia "na czacie", mogę zaproponować Ci kilka rozwiązań problemu. Niektóre z pokoi rozmów są nadzorowane przez dorosłych. Jeśli tak jest w Twoim przypadku, to skontaktuj się z moderatorem pokoju i zgłoś mu całe zajście. Gdy w pokoju nikt nie prowadzi nadzoru, spróbuj przekonać dziecko do jego zmiany na inny.

Gdy odniesiesz wrażenie, że którykolwiek z bywalców pokoju próbuje namówić Twoje dziecko na spotkanie, powinieneś natychmiast powiadomić o tym lokalną policję. Upewnij się, że masz zapisy rozmów przeprowadzonych na czacie, które mogłyby być pomocne w śledztwie.

Pornografia i prześladowanie przy użyciu kamer internetowych

To, gdzie zgłosisz fakt, że Twoje dziecko ogląda materiały pornograficzne emitowane przez kamerę internetową, zależy od okoliczności całego zdarzenia. Jeśli na przykład w sposób według Ciebie niewłaściwy zachowuje się przyjaciel dziecka, to najpierw skontaktuj się z jego rodzicami. Jeżeli dziecko utrzymuje tego typu kontakty z osobą dorosłą, nie pozostaje Ci nic innego, jak zawiadomić policję.

Jeśli to Twoje dziecko zachowuje się nieodpowiednio przed kamerą internetową, musisz natychmiast z nim porozmawiać na ten temat. Wyjaśnij mu, że wszystko, co przed nią robi, może zostać nagrane i wysłane w wiadomościach grup dyskusyjnych czy umieszczone na stronach internetowych, a to z kolei prowadzi do wielu sytuacji wprawiających dziecko w zakłopotanie teraz i w życiu późniejszym.

Hakerstwo

Gdy dziecko rozpoczyna eksperymenty z hakerstwem, koniecznie musisz mu wyjaśnić, że jest to proceder nielegalny i że może skończyć się dla dziecka aresztem. W sytuacjach ekstremalnych niektórzy rodzice decydują się na powiadomienie policji. Takie działanie może jednak prowadzić do aresztowania dziecka. Hakerstwo jest poważnym przestępstwem i jest to podstawowa rzecz, którą dziecko musi zrozumieć.

Programy typu spyware i adware oraz niewłaściwe formy reklamy

Nie istnieją żadne władze, którym można zgłaszać ogólnie rozumiany problem z oprogramowaniem szpiegującym i reklamującym. Pomimo to, jeśli strona adresowana do dzieci umieszcza nieodpowiednie dla nich reklamy, należy skontaktować się bezpośrednio z firmą, która jest jej właścicielem. Załóżmy, że Twoje dziecko odwiedza stronę sprzedającą dzieciom muzykę, ale wyskakujące na niej okienka reklamują strony dla dorosłych. W takiej sytuacji spróbuj nawiązać kontakt z webmasterem strony i poproś o zaprzestanie wyświetlania takich reklam. Na stronie znajduje się z reguły formularz kontaktowy lub adres e-mail, pod który można pisać.

Hazard

Gdy odkryjesz, że Twoje dziecko korzysta z usług oferowanych przez stronę hazardową, skontaktuj się z jej właścicielem i poinformuj go, że jeden z użytkowników jest niepełnoletni. Strony takie unikają młodych użytkowników, więc konto dziecka zostanie szybko zlikwidowane.

Informacje osobiste

Zdarzały się przypadki, w których ktoś tworzył drzewo genealogiczne swojej rodziny i umieszczał je na stronie internetowej. Niestety, drzewo zawierało imiona i nazwiska oraz nazwy miast, z których pochodzili członkowie danej rodziny. Również wiele szkół umieszczało dane swoich uczniów na stronach internetowych.

Żadne ze wspomnianych informacji nie powinny były znaleźć się w Sieci, ponieważ dzięki nim ludzie mogą się dowiedzieć, kim jest i gdzie mieszka Twoje dziecko. Jeżeli ktokolwiek opublikował w internecie informacje mogące pomóc w identyfikacji Twojego dziecka, skontaktuj się z tą osobą i poproś o ich natychmiastowe usunięcie.