



CYBERNIEBEZPIECZEŃSTWA PORADNIK DLA RODZICÓW



CYBERNIEBEZPIECZEŃSTWA

PORADNIK DLA RODZICÓW



Szczecin 2009

Opracowanie:

asp. sztab. Andrzej Szrajber –
Sekcja Prewencji Komendy Miejskiej Policji w Szczecinie,
Zespół ds. Prewencji Kryminalnej, Profilaktyki Społecznej,
Nieletnich i Patologii

Konsultacje:

asp. sztab. Piotr Mazur –
Sekcja dw. z Przystępczością Gospodarczą
Komendy Miejskiej Policji w Szczecinie,
specjalista w zakresie przystępczości internetowej

Wydawca:

Grapus Sp. z o.o., Szczecin

Wydano nakładem:

Fundacja „Razem Bezpieczniej”
www.razembezpieczniej.pl

Skład komputerowy i druk:

Grapus Sp. z o.o., Szczecin
tel. 091 485 35 65, www.grapus.pl

ISBN 978-83-61096-68-9

Nakład 2.000 egz.



PUBLIKACJĘ SFINANSOWANO Z BUDŻETU WOJEWODY
ZACHODNIOPOMORSKIEGO W RAMACH RZĄDOWEGO
PROGRAMU ZAPOBIEGANIA PRZESTĘPCZOŚCI
I ASPOŁECZNYM ZACHOWANIOM „RAZEM BEZPIECZNIEJ”

SPIS TREŚCI

Wstęp.....	5
Błądzenie we mgle	
<i>Precyzyjne wyszukiwanie informacji</i>	<i>8</i>
Wilk i Czerwony Kapturek	
<i>Jak rozmawiać w Internecie</i>	<i>13</i>
Znalezione – niekradzione	
<i>Pobieranie i wymiana plików</i>	<i>27</i>
Wyspy gier i prawo pięści	
<i>Spędzanie czasu bez agresji.....</i>	<i>32</i>
Tu się kupuje, tu się sprzedaje	
<i>Jak nie dać się oszukać</i>	<i>35</i>
Prześladować czy chronić?	
<i>Kilka cennych wskazówek</i>	<i>41</i>

Angażując się w działania na rzecz bezpiecznego korzystania z Internetu oddajemy w Państwa ręce kolejny material edukacyjny z serii „Biblioteki bezpiecznej Szkoły”. Tym razem poradnik adresowany jest do rodziców i poświęcony niebezpieczeństwom czyhającym na użytkowników Internetu, szczególnie tych młodych, nieświadomych zagrożeń. Poradnik ma na celu krok po kroku zapoznać rodziców ze światem, który dla naszych dzieci jest codziennością. Mamy nadzieję, że przedstawione Państwu informacje uświadomią nam wszystkich na ten poważny problem i pozwolą skuteczniej przeciwdziałać „cyberniebezpieczeństwom”.

Serdecznie zapraszamy do lektury.

w imieniu Zarządu Fundacji „Razem Bezpieczniej”

Marzena Maćkowiak-Pluta

Waldemar Palejko

WSTĘP

Szanowni pedagodzy, rodzice, opiekunowie

Czy wiecie, że dziecko samotnie korzystając z Internetu w swoim pokoju, znajduje się w towarzystwie setek, tysięcy, a może nawet milionów różnych osób? Czy wiecie, że siedząc przed komputerem podłączonym do sieci, dziecko może nawiązywać relacje społeczne, które nie różnią się niczym od tych nawiązywanych na ulicy? Czy pozwolilibyście dziecku znaleźć się w wielotysięcznym tłumie nieznanych osób bez waszego nadzoru? Tak właśnie wygląda Internet. Jego rozwój z każdym rokiem jest coraz bardziej dynamiczny. Staje się podstawowym źródłem informacji dla dzieci, młodzieży oraz dorosłych. Ogromne zasoby wiedzy, jaką można znaleźć w sieci oraz łatwy dostęp do niej, zachęcają do korzystania z tej formy rozwoju zainteresowań i nauki. Różnorodność programów edukacyjnych ułatwiających zrozumienie określonych zjawisk powoduje, że niemal w każdym uczniowskim pokoju jest komputer podłączony do sieci.

Internet to nie tylko baza danych, ale także potencjał komunikacyjny. Szeroki zakres możliwości nawiązywania łączności w sieci przy jednocześnie niskich kosztach wzbudza coraz większe zainteresowanie. Dostępne, bezpłatne komunikatory ułatwiają intensywne kontakty bez ograniczenia czasu spędzonego w sieci. Pozwalają nie tylko podtrzymywać nawiązane w sposób bezpośredni kontakty społeczne, ale wykorzystywane są też do nawiązywania nowych relacji.

W Internecie istnieją portale, dzięki którym użytkownicy sieci mają możliwość odnowienia znajomości z koleżankami i kolegami z czasów szkolnych. Nie zawsze jednak możliwości oferowane przez autora strony są wykorzystywane zgodnie z założeniami. Często zdarza się, że do publicznej wiadomości przekazywane są informacje, które powinny być przeznaczone tylko dla ściśle określonej grupy osób.

Zastosowań Internetu jest wiele i właśnie dlatego różne warstwy społeczne z niego korzystają. Sposób wykorzystania jest także zróżnicowany. Jedni znają Internet na tyle, że potrafią poruszać się w nim płynnie i unikać zagrożeń, inni potrafią wskazać pod-

stawowe funkcje, a jeszcze inni nie znają Internetu wcale. O ile w sytuacji, w której nie korzysta się z sieci można sobie pozwolić na jej nieznaną, o tyle bycie rodzicem lub opiekunem małoletniego użytkownika Internetu obciąża do poznania jego struktury, dobrodziejstw i zagrożeń.

Dzieci i młodzież nie mają trudności z poruszaniem się w Internecie, co często sprawia kłopot ich rodzicom i opiekunom, którzy spędzają znacznie mniej czasu przy komputerze. Okoliczności te inicjują sytuację, w której opiekunowie tracą zdolności kontrolno-wychowawcze nad swoimi dziećmi. Brak wiedzy i doświadczenia rodziców nie pozwala sprawdzać wirtualnych środowisk, w których przebywają ich dzieci. Te z kolei, bez właściwego nadzoru oraz edukacji ze strony rodziców, mogą znaleźć się w sytuacjach, w których sobie nie poradzą. Brak znajomości zagrożeń uniemożliwia skuteczną ochronę przed nimi. Niebezpieczeństwa, o których mowa, stanowią zagrożenie dla młodych użytkowników. Nie zapominajmy jednak o tym, że dzieci same inicjują sytuację, w których narażają siebie lub swoją rodzinę na przykre skutki. Tak się dzieje np. wtedy, kiedy dziecko przekazuje nieupoważnionym internautom informacje dotyczące danych osobowych, jak: adres zamieszkania, wiek, hasła dostępu, piny itd.

Nie bez znaczenia pozostaje też kwestia niskiego poziomu świadomości na temat odpowiedzialności karnej za przestępstwa popełnione z wykorzystaniem Internetu, zarówno po stronie rodziców i opiekunów, jak i młodzieży. Użytkownicy Internetu nie zawsze wiedzą, że przekaz określonych treści czy określone zachowania mogą nosić znamiona przestępstwa.

Program **CYBERDŻUNGLA** powstał po to, byście szanowni pedagodzy, rodzice i opiekunowie wiedzieli, że dziecko, które spędza czas korzystając z Internetu nie jest zupełnie bezpieczne, a to, że przebywa w swoim pokoju nie oznacza, że jest odizolowane od świata zewnętrznego. Program umożliwi poznanie podstawowej struktury Internetu, zagrożeń płynących z poszczególnych form korzystania z sieci oraz naukę unikania sytuacji, w których rodzice i dzieci mogą być zagrożeni działaniem innych użytkowników Internetu (oszuści, pedofile etc.).

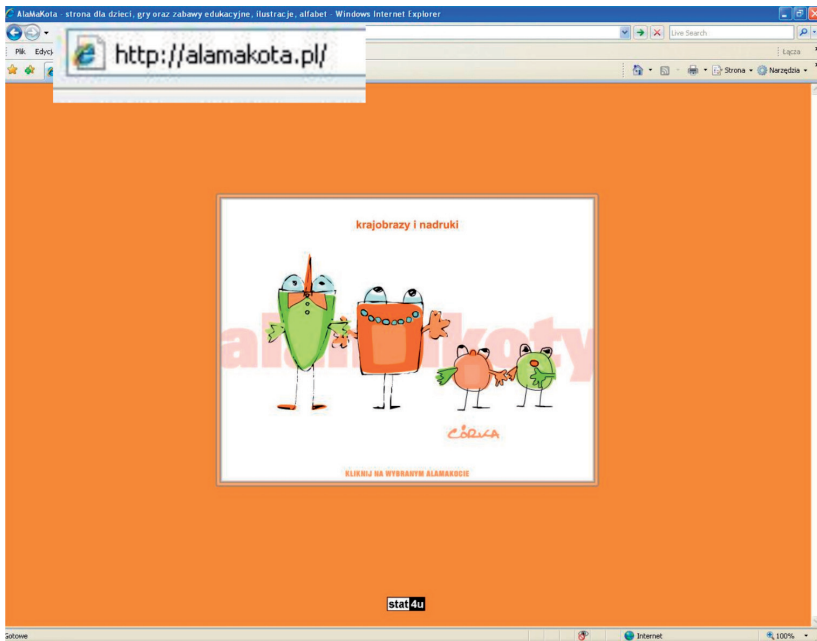
Innym elementem jest uaktywnienie waszej czujności nad dziećmi korzystającymi z zasobów Internetu oraz pomoc w wypracowaniu mechanizmu pozwalającego na jednoczesne, wspólne korzystanie z Internetu dzieci z opiekunami w określonych zakresach, szczególnie na płaszczyźnie rozrywki.

Przekazywane treści są dostosowane do możliwości dydaktycznych odbiorców i podane w formie przykładów opisujących sytuacje społeczne (np. kradzieże w sklepach, zachowania chuligańskie na ulicy) z przeniesieniem na grunt wirtualnej rzeczywistości.

Żeby dokładnie zrozumieć zagrożenia, na jakie narażone są dzieci korzystające z Internetu, należy prześledzić środowiska, z jakich korzystają najczęściej. Zacznijmy zatem od początku.

Błądzenie we mgle

Często młodzi internauci rozpoczynają swoją wędrówkę w sieci, wiedząc czego szukają i znając dokładnie adres strony, którą chcą odwiedzić, np. www.alamakota.pl. Wpisują go więc w odpowiednie pole i strona zostaje otwarta.



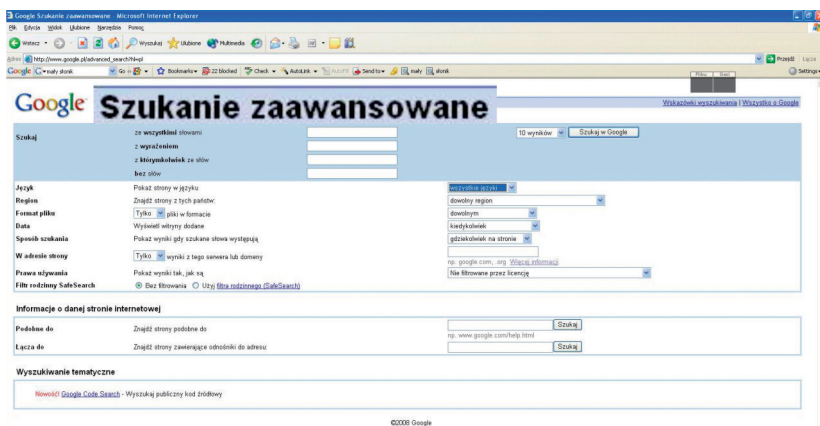
Rys. 1. Zrzut ekranu strony www.alamakota.pl

Jednak zdarza się, że najpierw korzystają z „wyszukiwarki”, czyli aplikacji pozwalającej znaleźć adresy stron zawierających interesującą ich tematykę. Najczęściej korzysta się w tym momencie ze strony www.google.pl wpisując wyraz, na podstawie którego wyszukiwane są strony zawierające go, np. lalka Barbie, mały słow-

[illegible]

[illegible]

Sytuacji tej można jednak uniknąć poprzez umiejętne, precyzyjne wyszukiwanie treści. Należy w ustawieniach zaawansowanych wyszukiwarki wskazać szczegółowe kryteria i zakres treści, jakiej poszukujemy. Wykonuje się to poprzez wskazanie miejsca wyszukiwania danych oraz ich formy. Opcja ta zawęży zbiór stron przedstawionych jako te, których szukamy, jednocześnie zmniejszając prawdopodobieństwo otwarcia strony niepożądanej.



Rys. 4. Zrzut ekranu strony www.google.pl – szukanie zaawansowane

Podobnie można uczynić, korzystając z aplikacji, które nazywamy kontrolą rodzicielską. W programach tych istnieje możliwość zablokowania stron zawierających niepożądane treści poprzez hasłowe określenie ich rodzaju, np.: pornografia, przemoc, filmy, narkotyki, sekty etc. To pozwoli wyeliminować strony, które chcemy ominąć i uchroni nasze dziecko przed wdepnięciem w „wirtualne błoto”. O aplikacjach tych dowiemy się więcej w dalszej części. Zanim jednak zaczniemy z dzieckiem naukę precyzyjnego wyszukiwania danych, sprawdźmy historię odwiedzanych stron. Wykonuje się to najczęściej poprzez naciśnięcie klawiszy **ctrl H** (klawisz znajduje się z prawej i lewej strony klawisza spacji), by upewnić się, że nie miało ono już kontaktu ze stronami o treści niepożądanej. Można to także wykonać poprzez naciśnięcie ikonki, która otworzy nam historię odwiedzanych stron. Na rysunku 5 można zobaczyć, jak to wykonać i co się w ten sposób uzyskuje.



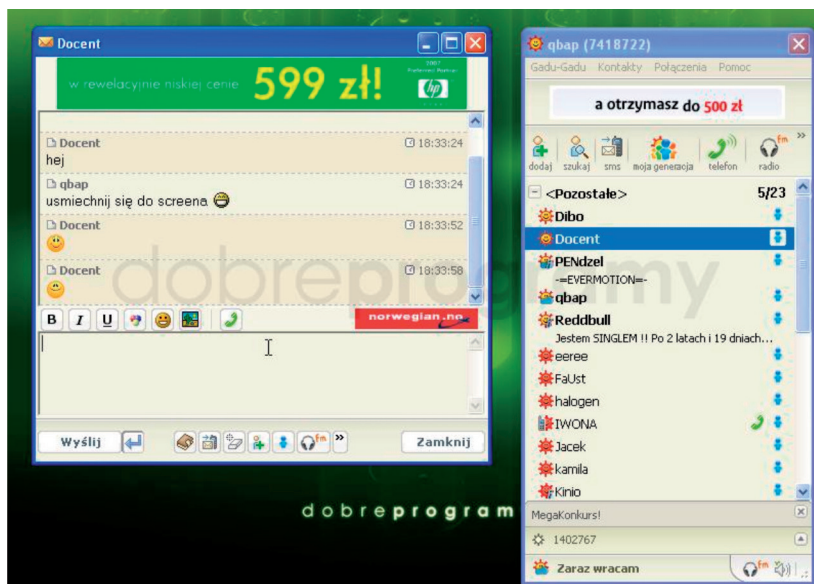
Rys. 5. Zrzut ekranu strony www.kmp.szczecin.pl – z otwartym oknem historii

Czynność ta pozwoli nam także uzyskać wiedzę na temat tego, czym interesuje się nasze dziecko i jakich w Internecie szuka informacji. Być może wtedy sami będziemy mogli przeprowadzić rozmowę, która zaspokoi głód wiedzy, a tym samym umocni relację z dzieckiem.

Wilk i Czerwony Kapturek

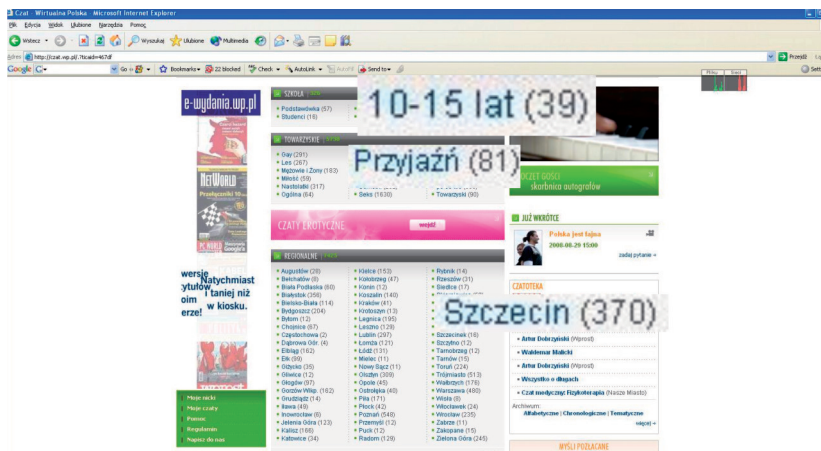
W czasach współczesnych Internet w szerokim zakresie jest wykorzystywany do komunikowania się. Użytkownicy sieci tworzą wirtualne społeczności, w których panują określone relacje. Wymieniają się informacjami, spostrzeżeniami, etc. Coraz częściej o określonej porze do komputerów zasiadają szkolni koledzy, którzy tworząc kilkusobową grupę, rozmawiają na różne tematy. Do kontaktów wykorzystują programy zwane komunikatorami.

Najpopularniejsze z nich, to: GG, Tlen, Skype. Wszystkie wyglądają bardzo podobnie do wskazanego na rysunku 6.



Rys. 6. Zrzut ekranu komunikatora GaduGadu

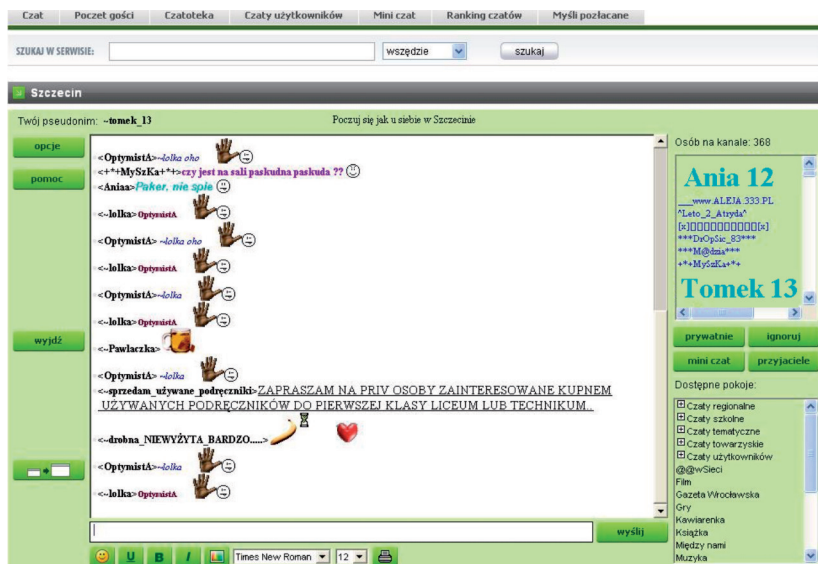
W tym celu wykorzystuje się także czaty, na których można dobierać rozmówców na podstawie miejsca zamieszkania, wieku lub zainteresowań.



Rys. 7. Zrzut ekranu strony www.wp.pl – zakładka czat

Wystarczy wprowadzić Nick (internetowe imię, pseudonim, np. Ania 12 czy Tomek 13) i można nawiązywać nowe znajomości. Czaty różnią się od komunikatorów tym, że nie trzeba się w nich rejestrować. Rejestracja polega na określeniu swojej osoby poprzez podanie wieku, płci, imienia itd. Po wykonaniu tego, system nadaje nam numer (można go porównać z numerem telefonu), który umożliwi innym użytkownikom wywoływać nas właśnie przy jego wykorzystaniu.

Czat pozwala na używanie dowolnie wybranego i często zmienianego Nicku podczas każdej z rozmów. Jest to element zwiększający poczucie anonimowości w sieci.



Rys. 8. Zrzut ekranu strony *www.wp.pl* – główne okno komunikacyjne czata



Pamiętaj. Nigdy nie wiesz, kto jest po drugiej stronie!!!

Niektóre aplikacje pozwalają prowadzić rozmowę przy użyciu mikrofonu oraz kamer internetowych. Wtedy rozmówcy widzą i słyszą się wzajemnie. Często jednak komunikacja odbywa się za pomocą klawiatury – w tej sytuacji obie strony pozostają dla siebie zupełnie anonimowe. Zarówno jedna, jak i druga forma stwarza określone zagrożenia, zwłaszcza dla dzieci niezdolnych do weryfikowania i selekcji informacji, które można przekazać swojemu rozmówcy. Dzieci oraz dorośli, zasiadając do komunikatora zapominają o tym, że po drugiej stronie może znajdować się każdy, począwszy od ucznia, poprzez „normalnego” internautę, aż po oszusta, włamywacza czy pedofila.

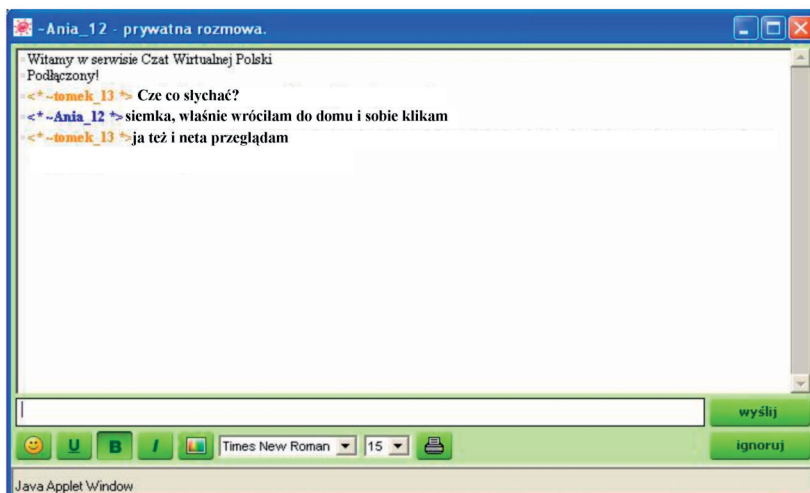
W przypadku używania komunikatora głosowego rozpoznanie faktycznej tożsamości rozmówcy nie stanowi problemu, szcze-

gólnie wtedy, kiedy używa on kamery internetowej. Słyszając głos i widząc twarz „wirtualnego towarzysza rozmowy”, mamy możliwość oceny, czy jest to rozmówca, z którym nasze dziecko może swobodnie konwersować. Jeśli nie jest to rówieśnik lub osoba znana rodzicom albo opiekunom, rozmowę należałoby przerwać. To jednak nie wszystko. Pamiętać należy o tym, że kamera, którą wykorzystujemy w rozmowach, nawet z kolegą z klasy, przekazuje szereg informacji do sieci, a tym samym do wielu setek użytkowników Internetu. Każdy ma możliwość obejrzenia wyposażenia mieszkania i na tej podstawie ocenienia zasobności portfela mieszkańców. Dzieci chętnie chwalą się tym, co rodzice posiadają w domu. To stwarza zagrożenie, że potencjalny oszust lub włamywacz nawiąże kontakt z naszym dzieckiem, używając np. Nicku (imienia używanego w Internecie) **Tomek 13**. Nie widząc go i nie słysząc, nasze dziecko nie ma możliwości oceny, czy rozmówca jest tym, za kogo się podaje.

Jeśli **Tomek 13** jest oszustem lub włamywaczem, będzie dążył do zdobycia informacji na temat wyposażenia mieszkania, struktury i stylu życia rodziny, miejsca zatrudnienia rodziców i zabezpieczenia mieszkania. Wiedza taka jest mu niezbędna do oceny ryzyka przy ewentualnym włamaniu, oszacowania ewentualnego zysku, zaplanowania włamania etc. Jeśli zaś okaże się pedofilem, będzie usiłował dowiedzieć się czegoś o zainteresowaniach dziecka, ulubionych bajkach, filmach, bohaterach, zwierzętach. Informacje te posłużą mu do zdobycia zaufania dziecka. W obu przypadkach rozmowa będzie prowadzona w sposób, który na pierwszy rzut oka nie wzbudzi podejrzeń. Jednak przy głębszej analizie można ocenić faktyczny zamiar rozmówcy i zakres informacji przekazanych mu przez nasze dziecko, odpowiadające na pozornie banalne pytania. Zobaczmy, jak może to wyglądać w praktyce. W tym celu wykreujemy sytuację, która może zaistnieć w każdym domu, w którym dziecko korzysta z Internetu.

Ania, która ma 12 lat zalogowała się w wybranym komunikatorze z zamiarem nawiązania rozmowy. Po pewnym czasie nawiązuje z nią kontakt internauta, który podaje się za **Tomka**.

Rozmowa przebiegać może np. w sposób podany poniżej.



Rys. 9. Zrzut ekranu okna komunikacyjnego

Tomek 13: *Cze co slychać?*

Ania 12: *Siemka, właśnie wróciłam do domu i sobie klikam.*

Tomek: *13 Ja też i neta przeglądam. Chyba zaraz się pokręcę po osiedlu.*

Gdyby dialog **Ani** i **Tomka** przez cały czas utrzymał się w podobnym tonie, nie budziłby żadnych zastrzeżeń. Niestety, dalsza rozmowa może być próbą „spychania” **Ani** na zupełnie inną płaszczyznę lub też może zmierzać do uzyskania różnych informacji bez wykraczania poza „bezpieczny temat”. Zatem może wyglądać w sposób wskazany poniżej. Pogrubionym drukiem zaznaczone zostały kwestie, które zasługują na szczególną analizę, ponieważ są „atakami” ze strony **Tomka** i oznaką nieuwagi **Ani**, która przekazuje cenne (dla przestępców) informacje.

Ania 12: *Tak? A na jakim mieszkasz?*

Tomek 13: *Na Majowym, a Ty?*

Ania 12: *Ja w domku.*

Tomek 13: *Często sobie klikasz?*

Ania 12: *To zależy.*

Tomek 13: Moi rodzice późno wracają z pracy, więc zawsze popołudniu tu jestem.

Ania 12: U mnie jest inaczej. Tata wyjechał za granicę, mama pracuje w biurze do godz. 16.00 i zawsze popołudniu jest w domu.

Tomek 13: Ja większość czasu spędzam z bratem. Ciągłe się z nim kłócę.

Ania 12: Ja jestem jedynaczką, więc kiedy wracam ze szkoły, jestem sama do czasu powrotu mamy.

Wskazaną techniką rozmówca uzyskuje informację (na razie dość ogólną) na temat rejonu zamieszkania **Ani**, organizacji dnia i ilości osób mogących przebywać w domu **Ani** o określonej porze. W czasie dalszej rozmowy będzie zadawał kolejne pytania, a udzielone odpowiedzi dostarczą mu o wiele więcej wiedzy, niż chciałaby tego **Ania**. Pamiętajmy o tym, że każda rozmowa przebiega inaczej, w zależności od rozmówców, ich faktycznego wieku, zainteresowań, intelektu etc. Podane przykłady szkicują jednak mechanizmy wykorzystywane podczas takich rozmów, sposoby zadawania pytań i analizy zebranych danych. Sprawdźmy, jakie to mogą być pytania i czego dowie się Tomek.

Pytanie Tomka 13

W co najczęściej
grasz na komputerze?

Możliwe
odpowiedzi
jakich udzieli
Ania:

- Lubię grać w...
- Nie lubię grać na komputerze.
- Nie mam czasu na gry.
- Rodzice nie pozwalają mi spędzać czasu przy grach.
- Zamiast grać na komputerze wolę...

Każda odpowiedź **Ani** zawiera określona informację.

Odpowiedź
zawiera
wiedzę
na temat:

- Wiek dziecka i jego płci, ponieważ określi to rodzaj wskazanej gry, która jest w zainteresowaniu określonej grupy osób.
- Zainteresowań i aktywności w ich rozwijaniu – wskaże to odpowiedź Ani, zarówno określającą ulubioną grę, jak i informującą o braku zainteresowania nimi. Rozmówca Ani określi obszar tematyczny pozostający w zainteresowaniu Ani i będzie miał możliwość poruszania tematów, które pozwolą na zacieśnianie znajomości.
- Klasy komputera, a więc poziomu życia rodziny - wynika to z wymagań sprzętowych wskazanej gry. Jeśli będzie to nowość o wysokich wymaganiach, oznaczać to będzie, że Ania ma w domu komputer wysokiej klasy, a jej rodzice są dobrze sytuowani.
- Jakości sprawowanego nadzoru rodzicielskiego i stosunku opiekunów do wybieranych przez dziecko form spędzania czasu w Internecie, a więc czujności rodzicielskiej. Jeśli Ania wskaże gry, które nie są przeznaczone dla dzieci w jej wieku (np. o wysokim poziomie agresji), oznaczać to może, że jej rodzice nie interesują się, w jaki sposób spędza czas przy komputerze, a więc też tym, z kim rozmawia i o czym oraz jakie nawiązuje znajomości. Taka sytuacja ułatwi więc rozmówcy nawiązanie z nią relacji, która nie będzie zakłócana nadzorem rodzicielskim.

Zadając jedno pytanie, **Tomek** uzyskuje tyle informacji, ile uzyskałby, zadając kilka kolejnych, ale to mogłoby wzbudzić podejrzenia **Ani** lub jej rodziców, zatem posługuje się techniką pozwalającą kontynuować rozmowę bez żadnych podejrzeń, przynajmniej ze strony **Ani**.

Innym przykładem tej techniki jest krótka informacja o sobie, swoich obowiązkach lub zainteresowaniach, przenosząca jednocześnie rozmowę na inny temat. W ten sposób **Tomek 13** „bada teren”, tzn. ustala, jaki temat rozmowy pochłonie **Anię** tak, by straciła samokontrolę. Temat ten musi ją zainteresować w sposób szczególny. Rozmowa może przebiegać następująco:

Tomek 13:

Mój pies Rocki zaczyna się denerwować,
muszę z nim iść na spacer, a strasznie tego
nie lubię. Mówię Ci, to masakra.

Możliwe
odpowiedzi
jakich udzieli
Ania:

- Wiem, co to znaczy, też mam psa yorka, wabi się Kulka, chodzę z nim do parku koło domu.
- Współczuję Ci, ja na szczęście nie mam psa.
- Zawsze marzyłam o tym, by mieć psa, ale rodzice nie chcą.
- Lubię psy, ale nie chciałbym mieć takiego w domu.

Odpowiedź
powoduje,
że:

- Tomek dowiaduje się, że Ania wychodzi z psem do parku, gdzie można ją spotkać o określonej porze, wie już, że powinien to być park w pobliżu domków jednorodzinnych – pozna ją po rasie psa. Wie też, jak pies się wabi, więc jeśli byłby to włamywacz, ma sposób na uciszenie szczekającego zwierzaka.
- Jeśli Ania cieszy się, że nie ma psa, to rozmówca tym bardziej będzie udawał zniechęcenie do spacerów, by w jak najszerszym zakresie wykazać podobieństwo zainteresowań z Anią.
- Jeśli Ania mówi, że zawsze marzyła o psie, to znaczy, że lubi też spacerować z nimi, co w przyszłości daje możliwość zaproszenia ją na taki. Tomek dowiaduje się też, że w domu Ani nie ma psa, więc w przypadku chęci dokonania włamania nie będzie ryzyka hałasu. Może się też dowiedzieć, że Ania nie jest zadowolona z zakazu rodziców w zakresie posiadania psa. Element osłabiający relację z rodzicami może wykorzystać do umacniania relacji ze sobą.

Takich pytań Tomek 13 może zadawać więcej i w ten sposób będzie zdobywał kolejne informacje, które nie powinny wydostać się na zewnątrz. Może poruszyć temat ulubionych filmów DVD, muzyki itd., pamiętając oczywiście o narzędziach, czyli odtwarzaczu DVD, wieży HI-FI czy telewizorze.

Wszystkie te informacje będą zbędne Tomkowi 13, jeśli faktycznie będzie nim trzynastoletni chłopiec (być może nawet o imieniu Tomek). Jeżeli jednak będzie to oszust, włamywacz lub pedofil, będzie wiedział o Ani zdecydowanie za dużo. Jeśli korespondencja naszego dziecka wzbudzi w nas jakiś niepokój, musimy upewnić się, z kim naprawdę mamy do czynienia.

W tym celu, zgodnie z porzekadłem „Kto mieczem wojuje, ten od miecza ginie”, musimy zastosować odpowiednią technikę rozmowy, by ustalić tożsamość rozmówcy. Polega ona na uspieniu jego czujności i przekonaniu go, że w dalszym ciągu rozmawia tylko z 12-letnią dziewczynką. Tak więc rozmawiamy dalej z Tomkiem 13, odpowiadając na jego pytania (oczywiście z zachowaniem zdrowego rozsądku), tak, by nie wzbudzić w nim podejrzeń. Swoimi odpowiedziami przekonujemy go, że całkowicie ufamy, że jest tym, za kogo się podaje. I po krótkiej chwili przechodzimy do „ataku”, np. według poniższego schematu.

Ania 12: Wiesz Tomku, miałam wczoraj paskudny dzień, moja koleżanka się na mnie obraziła i w dodatku dostałam pałę z klasówki z matmy.

Tomek odpowie prawdopodobnie, że mu przykro i że wszystko będzie w porządku po to, by w dalszym ciągu dążyć do nawiązania jak najlepszego kontaktu z Anią i wskazać, że stara się jej pomóc.

Tomek 13: Też nie cierpię matmy, nie kumam jej i obrywam pały, nie przejmuj się, jakoś je kiedyś poprawimy.

Tymczasem należy kontynuować „natarcie”.

Ania 12: Ja też za nic w świecie nie mogę skumać tej matmy, mam wrażenie, że matematyka się na mnie uwzięła, a co Ty teraz przerabiasz?

W tym momencie, jeśli rozmówca ma faktycznie 13 lat, odpowie bez wahania, podając aktualny temat z matematyki. Falszywy Tomek 13 uniknie odpowiedzi lub udzieli jej po długim czasie. Oczywiście nie można też wykluczyć, że rozmówca, chociaż falszywy, będzie dobrze zorientowany w programie nauczania matematyki uczniów 13-letnich. Dlatego nawet po uzyskaniu szybkiej odpowiedzi, zawierającej konkretną informację, powinniśmy drążyć dalej. Zadając kilka banalnych pytań na temat pogody, koleżanek, kolegów – w ramach „usypiania”, należy przejść do kolejnego „ataku”.

Ania 12: Fajnie się z Tobą klika.

Tomek 13: Z Tobą też.

Ania 12: Ale muszę zaraz kończyć.

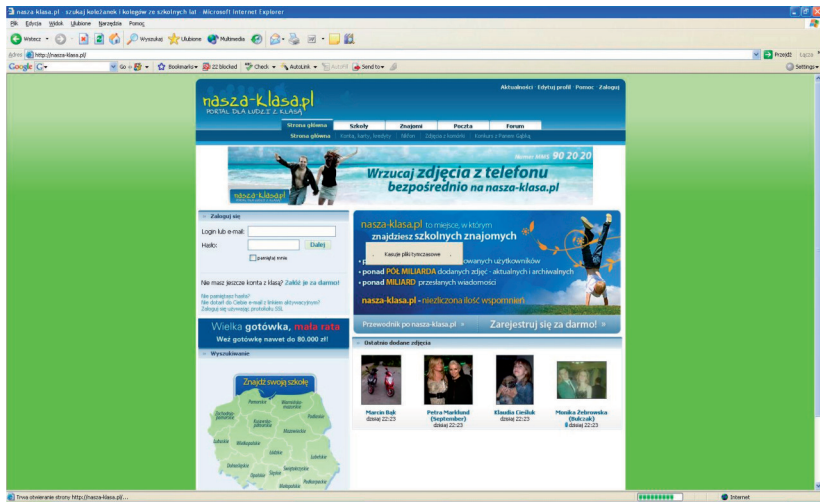
Tomek 13: Dlaczego? Przecież odrobiłaś lekcje. Mama wraca?

Ania 12: Za 3 dni muszę mieć przeczytaną lekturę na polaka, a to 120 stron. Książka tak gruba, że można jej używać zamiast stolka. Jaką wy teraz przerabiacie lekturę?

Sytuacja została powtórzona. Na podstawie tego, co odpowie Tomek i w jakim czasie, będziemy mogli wnioskować, z kim naprawdę mamy do czynienia. Jeśli nasze wątpliwości nadal nie zostaną rozwiązane, „atak” należy powtórzyć jeszcze kilkakrotnie, odwołując się do środowisk najbardziej adekwatnych dziecku – w tym przypadku 12-letniej Ani (szkoły, zainteresowań, umiejętności, muzyki). Jednak aby je znać, trzeba znać własne dziecko, a to wymaga czasu spędzonego wspólnie, także w Internecie. Najważniejsze jest to, by dziecko wiedziało, że w Internecie może natknąć się na różne niebezpieczeństwa i umiało sobie z nimi poradzić.

Nie tylko komunikatory stwarzają możliwości niekontrolowanego przekazywania wiedzy o sobie, rodzinie i bliskich do Internetu. Często odbywa się to przy wykorzystaniu portali społecznościowych, jak: nasza klasa, fotka czy sympatia oraz blogów (pamiętników internetowych). Oczywiście w sieci jest ich bardzo wiele. Ilustracje przedstawiają jedynie wybrane, najpopularniejsze wśród użytkowników strony.

- www.nasza-klasa.pl



Rys. 10. Zrzut ekranu strony www.nasza-klasa.pl

- www.fotka.pl



Rys. 11. Zrzut ekranu strony www.fotka.pl

- www.sympatia.pl



Rys. 12. Zrzut ekranu strony www.sympatia.pl

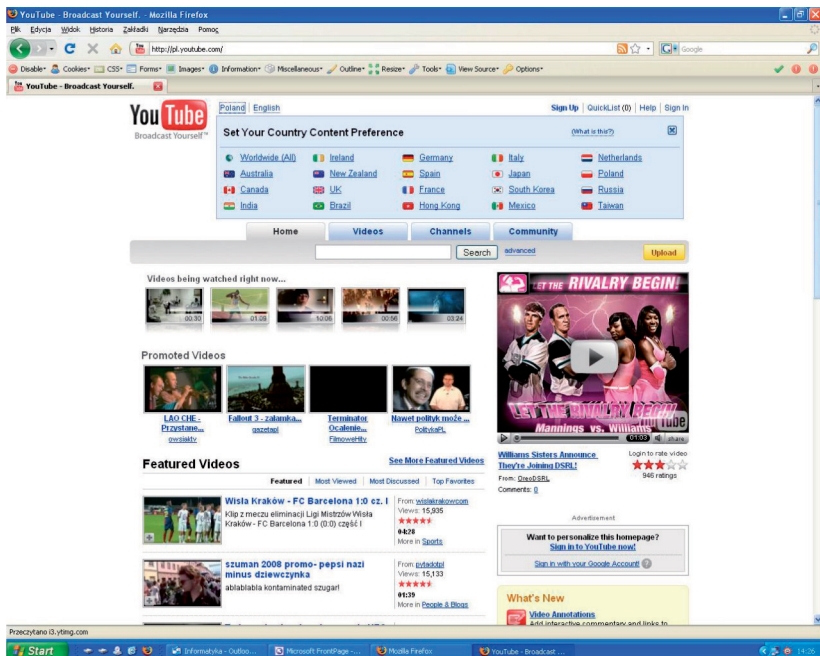
Umieszczane są w nich wizerunki wraz z opisem, zainteresowaniami itd. Często robią to młode dziewczyny, przybierające niewybredne pozy w kolorowych, nie zawsze obszernych ubiorach, które mogą być potem obiektem ataków różnych dewiantów. O ile można zrozumieć młodzieńczą lekkomyślność, o tyle ciężko pogodzić się z brakiem wyobraźni dorosłych, którzy, gdyby mogli, umieszciliby na portalu www.nasza-klasa.pl kserokopię wyciągów ze swoich kont bankowych (oby bez numerów i kodów dostępu), by móc pochwalić się kolegom z klasy swoim nowym życiem. Profile zaopatrzone w setki zdjęć domów, samochodów i innych dóbr materialnych w połączeniu z numerem telefonu komórkowego oraz numerem GaduGadu, stanowią mapę przestępczą dla oszustów, włamywaczy, pedofili etc., którzy mają także możliwość nawiązania kontaktu z wybranymi osobami przy wykorzystaniu komunikatorów, jak: GG, Tlen, Skype itp. Koło się zamyka.

Portal ten, jeśli nie jest właściwie skonfigurowany, obnaża także użytkownika, wskazując wszystkim powiązania, relacje oraz

zdjęcia i dane osobowe osób, które przyjęte zostały do kręgu znajomych.

Innym portalem, na którym możemy znaleźć wizerunki osób oraz informacje o nich, jest www.youtube.pl. Problem polega na tym, że wizerunki te są umieszczane często bez wiedzy lub zgody osób, które zostały sfotografowane. Niepokojące jest to, że treści te umieszczane są przez uczniów, którzy nagrywają filmy telefonami komórkowymi i zamieszczają je w portalu, który działa raczej demoralizująco niż wychowawczo. Nawet jeśli dziecko użytkownika nie umieszcza tam treści samodzielnie wykonanych w postaci zdjęć lub filmów, to nie oznacza, że poprawne jest śledzenie treści zawartych w www.youtube.pl. Zdarza się, że rodzice pozwalają swoim dzieciom oglądać na tym portalu filmy lub bajki, których emisja w telewizji została zakończona. Nie ma w tym nic złego, kiedy dziecko wpisuje tytuł bajki, którą po chwili może już obejrzeć. Niestety, „pomysłowi” internauci zamieszczają na portalu bajki z własną wersją tłumaczenia (dubbingiem), która bogata jest w wulgaryzmy i nadaje oglądanemu filmowi charakter pornograficzny. Zatem nie wystarczy pozwolić dziecku na oglądanie bajki, ale trzeba też sprawdzić, czy znaleziony film jest tym, którego dziecko szuka. Jeśli nie mamy możliwości, by murem stać nad dzieckiem, to przynajmniej w pierwszej fazie oglądania, nawet jeśli jesteśmy w innym pomieszczeniu, postarajmy się wsłuchiwać w dialogi płynące z komputera. Taki sposób, przynajmniej w pewnym stopniu, pozwoli na sprawowanie nadzoru nad młodym internautą.

Należy też dodać, że pojawiły się tzw. podróbki strony, które wyglądają niemal identycznie, łącznie z zachowaniem dostępnych funkcji, które występują na stronie oryginalnej. Niestety, korzystanie z tej podróbki naraża nas na zainstalowanie w naszym komputerze złośliwego oprogramowania, które ułatwia włamanie do niego, zdobywanie haseł itd.

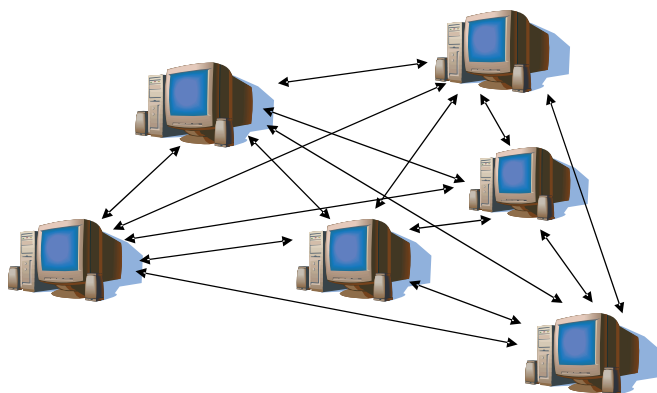


Rys. 13. Zrzut ekranu strony www.youtube.pl

Zrzut strony został przedstawiony celowo, by wykazać, że tak jak wiele innych stron, na pierwszy rzut oka nie budzi ona zastrzeżeń, jednak zawartość może zagrażać dziecku.

Znalezione – niekradzione

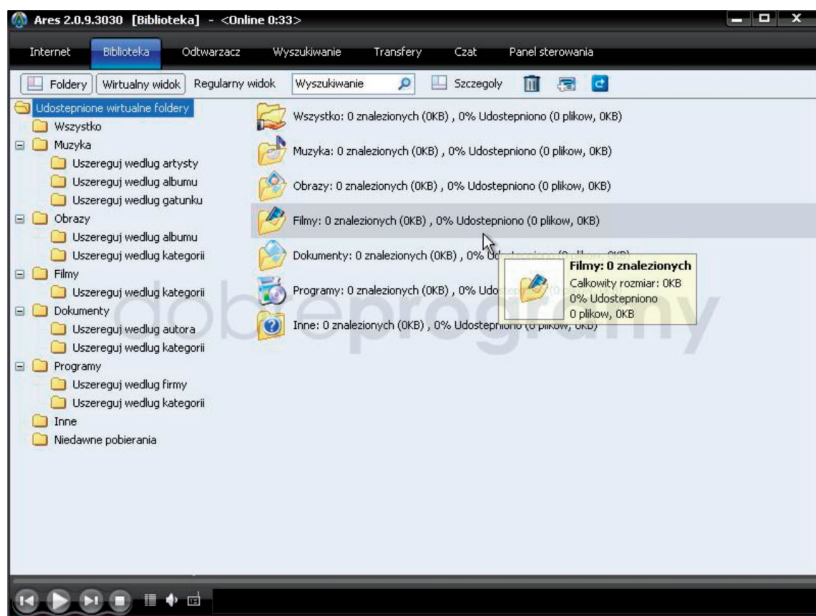
Mówiąc o zagrożeniach związanych z Internetem, nie można skupić się jedynie na tych, na które narażone są nasze dzieci. Nie można zapominać o takich, które one same stwarzają dla siebie i innych, nie wyłączając rodziców i opiekunów. Jak wspomniałem na początku, Internet to sieć połączonych ze sobą komputerów zawierających mnóstwo informacji, programów, plików, dokumentów etc.



Rys. 14. Schemat sieci służącej do wymiany plików pomiędzy użytkownikami

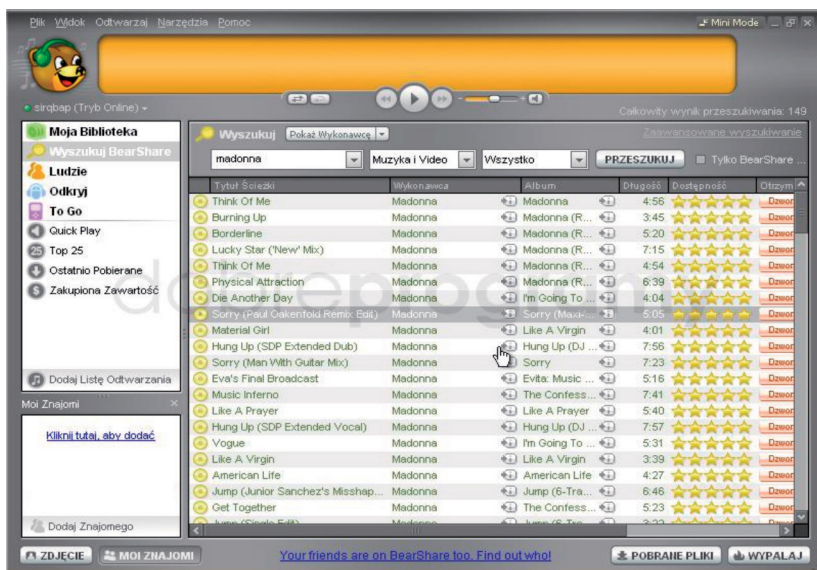
Wśród tysięcy użytkowników spotkać można takich, którzy mają podobne zainteresowania, a co za tym idzie – określone potrzeby związane z ich rozwojem. Przekłada się to na „głód” informacji, które są nieustannie poszukiwane. W celu ułatwienia ich zdobycia powstały programy, które nazywamy Peer to Peer (P2P). Pozwalają one na znalezienie w sieci danych przechowywanych w komputerach użytkowników i wymianę pomiędzy nimi. Tak więc **Ania** udostępnia swoje wiersze innym i ma możliwość pobierania wierszy udostępnionych przez kogoś. **Tomek** udostępnia swoją grafikę innym internautom i jednocześnie ma możliwość

pobierania obrazków stworzonych przez nich. Do takiej wymiany wykorzystuje się aplikacje takie, jak: „Kaaza”, „Emule”, „Bearshare”, „Ares” itd.

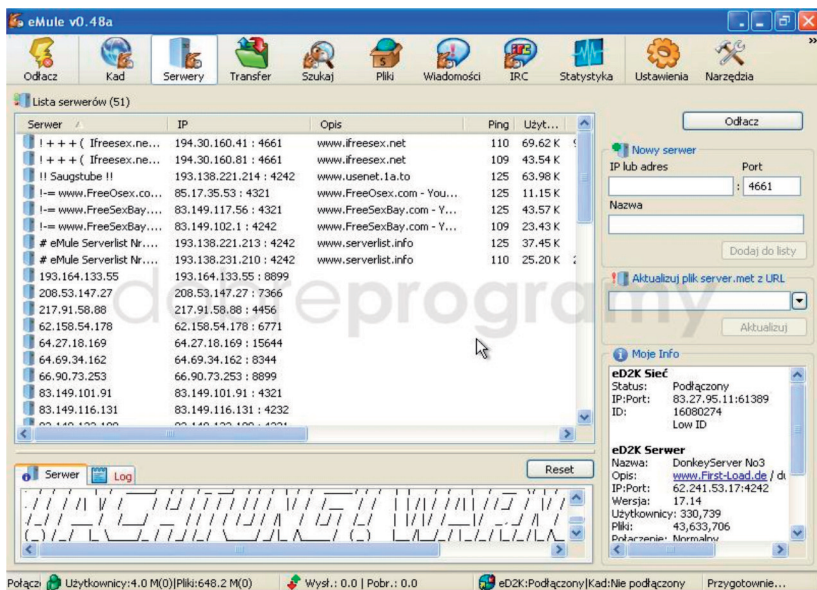


Rys. 15. Zrzut ekranu programu Ares

Wskazane ilustracje przedstawiają jedynie wybrane aplikacje, które są wykorzystywane do pobierania danych. W Internecie jest dostępnych wiele podobnych programów.



Rys. 16. Zrzut ekranu programu BearShare



Rys. 17. Zrzut programu Emule

Problem pojawia się w momencie, kiedy użytkownicy zaczynają się wymieniać plikami, które nie należą do nich, jak pliki muzyczne czy filmowe. Podczas zajęć prowadzonych w szkole uczniowie nie mogą zrozumieć, dlaczego nie wolno ściągać i wymieniać się muzyką czy filmami. Można to wyjaśnić w prosty sposób – podejść do jednego z nich i zabrać z biurka książkę, tłumacząc, że właśnie doszło do ściągnięcia pliku z jego komputera. Następnie dać książkę komuś innemu, zabierając w zamian np. piórnik i przenosząc go w inne miejsce. Kiedy uczniowie widzą, że wymiana oparta jest na dysponowaniu cudzym mieniem, podobnie jak w Internecie, wtedy rozumieją naganność pobierania i wymiany plików, których nie są właścicielami.



Nieznajomość prawa szkodzi!!!

Niektórzy próbują bronić się i oświadczają, że ściągają muzykę i filmy tylko dla siebie, a to nie jest przestępstwo. Rzeczywistość jest jednak inna. Zgodnie z art. 116 ust. 1 ustawy z dnia 4 lutego 1994 r. o prawach autorskich i prawach pokrewnych, *kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonania, fonogram, wideogram lub nadanie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Zgodnie z ust. 2 przytoczonej ustawy, jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3, przy czym należy pamiętać, że fakt, iż osoba posiadała grę bez uiszczenia opłaty, traktowany jest jako rzekome osiągnięcie korzyści majątkowej, więc ściągnięcie nawet tylko dla siebie jest osiągnięciem korzyści majątkowej. Przepis w ust. 3 wskazuje dalej, że jeżeli sprawca uczynił sobie z popełnienia przestępstwa określonego w ust. 1 stale źródło dochodu albo działalność przestępczą, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5. Nie pomoże w tej sytuacji tłumaczenie: „Nie*

wiedziałem”, ponieważ niezajomość prawa nie zwalnia z odpowiedzialności.

Ważne jest, by wszyscy wiedzieli, że rozpowszechnianie zaczyna się z chwilą rozpoczęcia ściągania pliku z Internetu, nawet jeśli użytkownik ma zamiar ściągnąć go tylko dla siebie. Jest to spowodowane konstrukcją programu, który w chwili rozpoczęcia operacji udostępnia plik innym internautom, mogącym pobrać go od użytkownika, który rozpoczął ściąganie – to jest właśnie rozpowszechnianie.

W taki właśnie sposób dzieci same narażają siebie lub rodziców na konsekwencje prawne i jest to jedno z niebezpieczeństw stwarzanych przez nich samych. Należy też dodać, że w poszukiwaniu plików (nawet tych, których pobranie jest dopuszczalne) posługują się określonymi nazwami, a to z kolei inicjuje sytuację, którą wskazywałem wcześniej, opisując mechanizmy precyzyjnego wyszukiwania informacji. Innymi słowy, pod określonymi nazwami mogą znajdować się pliki o treści, która nie jest przeznaczona dla dzieci lub młodzieży.

Wyspy gier i prawo pięści

W sieci można zagrać praktycznie we wszystko i to bez konieczności ściągnięcia gry do komputera. Można to zrobić ON-LINE, czyli w czasie połączenia z Internetem. Wachlarz ofert z zakresu rozrywki jest szeroki: od strategii, przez logikę, po „zręcznościówki”. Można się rzucać bananami, budować mosty albo urywać głowy.



Rys. 18. Zrzut strony *www.wyspagier.pl*

Jak świat światem, nic tak nie przykuwa uwagi, jak: krew, cierpienie, zemsta, przewaga, władza i zwycięstwo. Jeżeli ktoś miał okazję obserwować swoje dziecko podczas gry, w której należy pokonać innych, wie doskonale, jak bardzo zabawa ta wciągnęła młodego gracza. I nie ma w tym nic złego, kwestia tylko, w jaki sposób odnosi się zwycięstwo – sprytem, inteligencją, wiedzą czy siłą, agresją i hektolitrami przelanej krwi. Bez właściwej kontroli dzieci cały czas przy komputerze strzelałyby do przeciwników,

rozwiązując jednym wybuchem „100” problemów. Często z pokoju dziecka dochodzą głosy trzaskającej klawiatury i okrzyki złości lub euforii, ale dopóki malec „dobrze się bawi”, większość rodziców nie raczy nawet spojrzeć w ekran monitora. Tymczasem młody gracz uczy się, jak zabić, gdzie podłożyć bombę, w jaki sposób ukraść samochód, dowiaduje się też, że najwięcej punktów zdobywa się, zadając ciosy dziecku bawiącemu się w piaskownicy lub strzelając do policjanta. To tylko fabuły wybranych gier, które zostały sprawdzone. Pytanie, skąd i gdzie ich szukać? Odpowiedź jest bardzo prosta: podczas zajęć z policjantami uczniowie drugiej klasy szkoły podstawowej wskazali nazwy gier, ich adresy oraz zasady w zarysie.

Niektórzy pochwalili się też, że takie gry dostają od rodziców – tylko pogratulować tym, którzy uczą swoje dzieci, że sposobem na problemy jest agresja, przemoc, nienawiść, wrogość...



**Sprawdź, czy wybrana gra
jest odpowiednia dla Twojego dziecka!!!**

Problem nie wynika z tego, że rodzice chcą, by ich dzieci grały w te gry, ale z tego, że nie sprawdzają, co kupują. Nie zapytają sprzedawcy o fabułę, nie sprawdzą w Internecie jej opisu, w końcu – ceniąc sobie ponad wszystko chwilę spokoju i relaksu – nie zagrają z dzieckiem, by przekonać się osobiście, czy jest to gra właściwa. Wystarczy rzucić okiem na opakowanie gry, na którym są oznaczenia wieku gracza, poziomu przemocy, rodzaju gry.

Dowodów na taką postawę nie trzeba szukać daleko – można je znaleźć w najbliższym otoczeniu. Na jednej z imprez, zorganizowanej z okazji urodzin syna, w wyznaczonej „bawialni” pojawiła się grupa zaproszonych kolegów. Dodam, że panowie mieli po 6 lat. Kiedy spotkali się w sali, ujrzeni kilka wolnych stanowisk do gier video, oczywiście przepelnionych wojną, krwią, zabijaniem etc. Natychmiast poproszono obsługę o wyłączenie komputerów, co zostało uczynione. Dzieci rozbiegły się i zaczęły się ba-

wić, rozwijając się fizycznie i społecznie. Wprawdzie wymagało to zwiększonego nadzoru ze strony rodziców, ale i tak wszyscy byli zadowoleni z takiego obrotu sprawy. Radość jednak nie trwała długo. Równolegle na sali przebywała inna grupa dzieci (goście innego jubilata), których rodzice zażyczyli sobie włączenia gier video. W jednej chwili wszystkie dzieci, ściśnięte, stały przy stanowisku, przy którym rozgrywała się krwawa akcja. Rodzice mogli spokojnie plotkować o „rzeczach najważniejszych na świecie”, a dzieci bez nadzoru przeniosły się w wirtualny świat, w którym obowiązuje prawo silniejszego. Dopiero informacja o torcie spowodowała, że „młody tłum” się rozszedł.

Tu się kupuje, tu się sprzedaje

Coraz większym zainteresowaniem cieszy się Internet w sferze zakupów. Można w nim znaleźć wiele sklepów internetowych, które oferują różnorodny asortyment towarów. Niższe ceny oraz możliwość łatwego wyszukania konkretnego przedmiotu przyciągają internautów. Zakupu dokonuje się w różny sposób. Czasem wystarczy kliknąć na ikonkę z napisem „Włóż do koszyka” – w przypadku sklepów internetowych, innym razem należy wziąć udział w licytacji, jak to ma miejsce np. w portalu www.allegro.pl, w którym dodatkowo należy być zarejestrowanym.



Rys. 19. Zrzut strony www.allegro.pl

Rejestracji dokonuje się poprzez wypełnienie odpowiedniego formularza (poprzez Internet), podając swoje dane łącznie z adresem. Wtedy tradycyjną pocztą wysyłany jest na adres osoby rejestrującej się tzw. kod aktywacyjny, którego wprowadzenie uprawnia do licytowania i kupowania wybranego towaru. Takie

ułatwienie powoduje, że nie wychodząc z domu, w ciągu zaledwie godziny, możemy kupić tyle, ile w tradycyjny sposób w ciągu kilku dni.

Zakupy takie są zatem łatwe i przyjemne, ale nie zawsze bezpieczne. Na portalu www.allegro.pl napotkać można zwyczajnych oszustów, którzy zarejestrowali się, podając fałszywe dane osobowe. Po otrzymaniu kodu aktywacyjnego rozpoczynają swoją działalność przestępczą. Oszust taki w poczuciu anonimowości oferuje do sprzedaży atrakcyjne przedmioty w jeszcze bardziej atrakcyjnych cenach. Jednak po przelaniu określonej kwoty na wskazany przez niego rachunek bankowy (założony także na podstawie fałszywych dokumentów), nie wysyła zakupionego przedmiotu albo wysyła „towar zastępczy” w postaci cegły, pudełka ze szmatkami, kilogramowej paczki cukru etc. Przed takim zachowaniem można się jednak zabezpieczyć. Każdy zarejestrowany „allegrowicz” ma swoje konto, na którym zbiera oceny od swoich kontrahentów, niezależnie czy jest sprzedającym, czy kupującym. Wygląda to tak, że obie osoby po zakończonej transakcji wystawiają sobie tzw. komentarze z krótkim opisem. Może to być ocena pozytywna, negatywna lub neutralna. Wszystko zależy od stopnia zadowolenia wystawiającego. Zatem, zanim coś kupimy od „allegrowicza”, zapoznajmy się z komentarzami, jakie zostały mu wystawione. Ocenimy wtedy stopień ryzyka. Poza tym, często mamy możliwość wybrania formy płatności, która pozwala nam na uiszczenie ustalonej kwoty po otrzymaniu i sprawdzeniu przesyłki.



Nie kupuj pochopnie!!!

Należy pamiętać, żeby pochopnie nie przystępować do licytacji oraz aby nie klikać ikonki „Włóż do koszyka” bez zastanowienia. Operacja ta jest zawarciem umowy cywilnej, w konsekwencji której będziemy musieli zapłacić za wybrany towar, jeśli kontrahent nie wyrazi zgody na odstąpienie od niej. Często zdarza się, że dzieci, korzystając z kont rodziców, popełniają takie błędy, za

które konsekwencje ponoszą ci drudzy. Nastoletni użytkownicy Internetu, dokonując zakupów, niejednokrotnie posługują się kartą bankową swoich rodziców, co w myśl przepisów jest przestępstwem. Określa to ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych, która w art. 16 wskazuje obowiązki posiadacza karty, w szczególności polegające na tym, że nie może on udostępniać karty oraz kodów identyfikujących osobom nieuprawnionym. Artykuł 17 tejże ustawy mówi, że właścicielem karty jest wydawca, a więc bank, zatem należy stosować się do regulaminów i wewnętrznych przepisów. Przytoczony akt prawny w artykule 20 wskazuje wyraźnie, że karta może być wykorzystywana jedynie przez osobę, której dane widnieją na niej. Dotyczy to także kart płatniczych, tak więc nawet małżonkowie nie mogą dokonywać zakupów, płacąc kartą współmałżonka. Dotyczy to również dzieci wysyłanych po zakupy. Najistotniejsze jest to, że zgodnie z art. 28 ustawy, posiadacza karty obciążają operacje dokonane przez osoby, którym kartę udostępnił lub ujawnił kod identyfikacyjny. Rodzice nie będą więc mogli ubiegać się o cofnięcie transakcji dokonanych przez dzieci, argumentując to niekontrolowanym udostępnieniem karty.

Dodatkowym zagrożeniem jest podawanie numerów kart bankowych podczas transakcji, ponieważ mogą one dostać się w niepowołane ręce, a wtedy „życzliwy” internauta może pozbawić nas oszczędności zgromadzonych na rachunku bankowym. Znaczna część społeczeństwa, korzystając z dobrodziejstwa techniki, a w szczególności Internetu, korzysta z tzw. internetowych kont bankowych. To nic innego, jak dostęp do rachunku bankowego bez konieczności wychodzenia z domu. Nie trzeba stać w gigantycznych kolejkach do okienek bankowych, by dokonać przelewu, wypłaty lub założyć lokatę. Nie trzeba też tracić czasu w następnej kolejce w urzędzie pocztowym, by zapłacić rachunki i dokonać innych opłat. W dobie Internetu możemy dokonać tego szybciej, taniej i bez konieczności opuszczania mieszkania. Jednak taka wygoda może nieuważnych wiele kosztować. Od pewnego czasu w sieci napotkać można tzw. Phishing (password harvesting fishing – łowienie haseł). Narażeni na skutki tego zjawiska są wła-

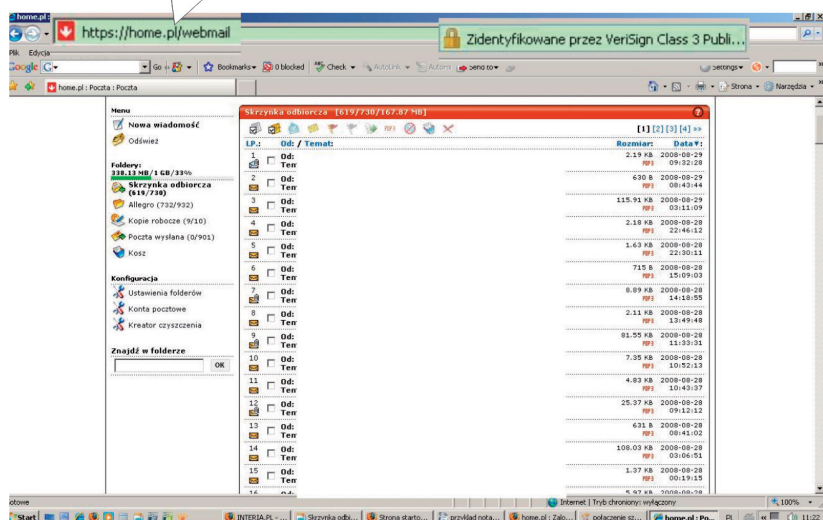
śnie posiadacze internetowych kont bankowych typu np. Inteli-go. Łowienie, podobnie do tradycyjnego, polega na zarzucaniu przynęty i czekaniu, aż ofiara połknie haczyk. W tym przypadku ofiarą będzie nieuważny internauta, haczyk wygląda identycznie, jak strona banku, którą chcemy otworzyć. W praktyce wygląda to tak, że użytkownik loguje się na stronie banku, w którym posiada rachunek. Otwiera się strona, która do złudzenia przypomina tę, którą chcemy otworzyć. Różni się jednak zamieszczonymi komunikatami i informacjami, które nakazują nam wykonanie określonych czynności, których dotąd nie trzeba było wykonywać, logując się. Sprowadzają się one najczęściej do podania numeru karty, hasła lub kilku kolejnych kodów z kart tzw. zdrapek, które wykorzystujemy przy wykonywaniu operacji (przelewów itp.). W ten sposób hakerzy zdobywają numer klienta, hasło oraz kody potrzebne do dokonania przelewów. Ważne jest, by wiedzieć, że bank nigdy nie żąda podania tych danych w sytuacji innej, niż identyfikacja użytkownika, czyli podczas logowania. Jeśli coś wzbudzi podejrzenia, należy, bez podawania żądanych informacji, natychmiast wyłączyć stronę i skontaktować się z bankiem w celu ustalenia, czy zaszły jakieś zmiany w sposobie logowania. Takie zachowanie jest przestępstwem, ściganiem którego zajmują się wyspecjalizowani policjanci.

Następnie należy zmienić hasło, ponieważ dotychczasowe jest w posiadaniu hakerów. Niezbędne może okazać się też „wyczyszczenie” systemu operacyjnego i zainstalowanie właściwych programów, uniemożliwiających dostęp do informacji zawartych w komputerze użytkownika. Decydując się na wybór przeglądarki internetowej (*podstawowego programu zainstalowanego w komputerze, który pozwala korzystać z Internetu*), należy wziąć pod uwagę opisane zagrożenia. Obecnie na rynku jest kilka pozycji:

- Opera
- Mozilla
- Internet Explorer 7
- Safari
- Google Chrome
- Firefox 3

Otwierając stronę banku, korzystamy z tzw. połączenia szyfrowanego (https). W przypadku obu przeglądarek Internet Explorer 7 i Firefox 3 jego prawidłowość oznaczona jest kolorem zielonym. Użytkownik wie wówczas, że połączenie jest bezpieczne. Gdyby pojawiło się jakiegokolwiek zagrożenie, kolor zielony zmieniłby się na czerwony. Dodatkowo przeglądarka Internet Explorer wyświetla informację o podmiocie, a Firefox wyświetla informację, dla kogo certyfikat został wystawiony (np. nazwa banku lub firmy), a po najechaniu myszką na to pole dowiemy się, kto wystawił certyfikat.

W tym miejscu wskazany jest adres strony, którą otworzyliśmy. Powinna to być strona wskazana przez bank.



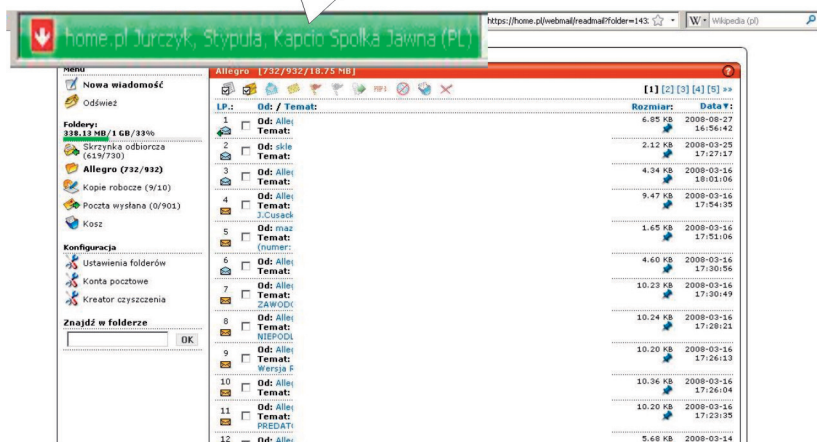
Rys. 20. Zrzut przeglądarki Internet Explorer 7

Tak więc, po otwarciu strony należy zawsze upewnić się, czy wszystko jest w porządku, zgodnie ze wskazówkami opisanymi powyżej.

Sytuacja wygląda nieco inaczej, jeśli użytkownik korzysta

z przeglądarki Firefox 3. Wskazane jest także korzystanie z oprogramowania chroniącego przed wirusami oraz atakami. Są to antywirusy i tzw. programy firewall, uniemożliwiające dostęp do naszego komputera innym użytkownikom sieci. Jeśli instalujemy je w pakiecie (wszystkie pochodzące od jednego producenta) działają one wówczas optymalnie.

W tym miejscu wskazany jest podmiot, dla którego certyfikat został wystawiony.
Po najechaniu myszką na to pole uzyskamy informację o wystawcy certyfikatu.



Rys. 21. Zrzut przeglądarki Firefox

Osoby bez doświadczenia w zakresie zabezpieczeń powinny zwrócić się o pomoc do osoby zaufanej.

Prześladować, czy chronić?

Kontrola nad dzieckiem służy temu, by uchronić je przed wszystkimi zagrożeniami, jakie zostały opisane do tej pory. Można ją sprawować na wiele sposobów, np. poprzez:

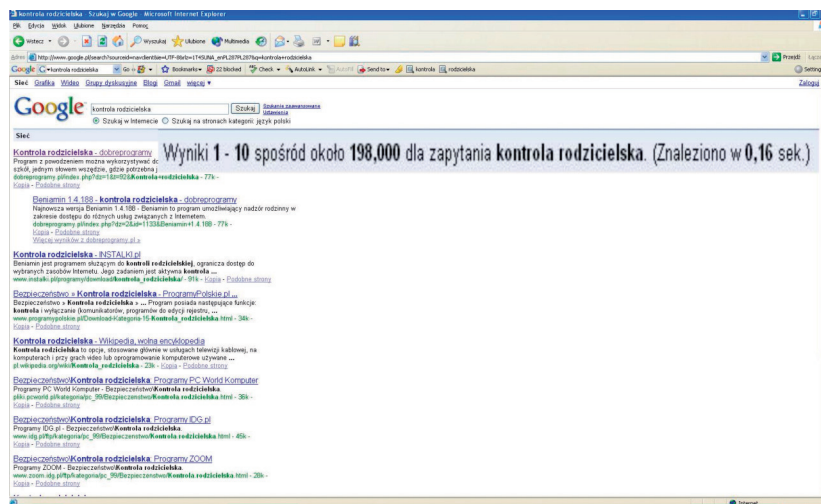
- wspólne spędzanie czasu w Internecie
- wyjaśnienie zagrożeń i omówienie sposobów ich unikania
- sprawdzanie historii odwiedzanych stron
- ograniczanie czasu spędzonego przy komputerze
- stosowanie programów wspomagających sprawowanie nadzoru nad dzieckiem.



Ufaj i sprawdzaj!!!

Ważne jest, by dziecko miało świadomość, że kontrola to nie to samo, co prześladowanie, a jej sprawowanie ma na celu dobro jego samego. Formę kontroli można omówić i wspólnie ustalić zakres oraz zasady korzystania z Internetu. Poprawia to relacje oraz buduje zaufanie. Jednak należy zostawić sobie niewielką rezerwę i dbając o bezpieczeństwo dzieci, uaktywnić blokadę niektórych stron oraz dozować czas spędzony przy komputerze. Nie zawsze jednak rodzice mają możliwość osobistego kontrolowania czasu spędzonego przed komputerem przez dziecko. Dzieje się tak np. wtedy, kiedy są jeszcze w pracy, a młody użytkownik Internetu po zakończonych lekcjach nudzi się w domu. Wtedy rodzice potrzebują pomocy programów, które nazywane są kontrolą rodzicielską. Można je znaleźć w Internecie jako freeware, czyli aplikację dostępną nieodpłatnie. Są to dość proste programy, których obsługa nie powinna sprawiać nikomu kłopotu. Można je odszukać w sposób, jaki opisany został wcześniej, wykorzystując wyszukiwarkę Google i wpisując słowa kluczowe: kontrola rodzicielska. Pojawi nam się kilka tysięcy propozycji, z których należy wybrać najbardziej odpowiednią, tzn. taki program, który spełni oczekiwania użytkownika i nie będzie sprawiał trudności w obsłudze.

Można też zakupić rozbudowane aplikacje, dające wiele możliwości ustawień, ale to polecam zaawansowanym użytkownikom. W funkcję kontroli rodzicielskiej wyposażone są także niektóre systemy operacyjne, np.: MS Windows Vista.

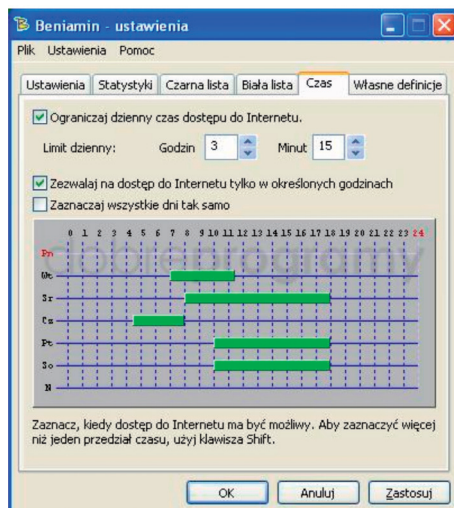


Rys. 22. Zrzut ekranu strony www.google.pl – słowa kluczowe – kontrola rodzicielska

Stosowanie tych programów budzi kontrowersje. Niektórzy twierdzą, że służą do prześladowania dzieci, inni, że pomagają rodzicom. Obie strony można pogodzić poprzez właściwą konfigurację programu. Jeżeli nastawimy się jedynie na sprawdzanie zawartości historii, tzn. wykazu tych stron, które odwiedziło nasze dziecko i czynność tę będziemy powtarzać kilkakrotnie, to istotnie może ona przypominać prześladowanie, a poza tym jedynie w niewielkim stopniu przyczyni się do zwiększenia ochrony. Należy zatem korzystać z możliwości konfigurowania programu w taki sposób, by nie było konieczności ciągłego sprawdzania otwieranych wcześniej stron.

Do najpopularniejszych należą:

- Beniamin



Rys. 23. Zrzut programu Beniamin

- Strażnik ucznia



Rys. 24. Zrzut programu Strażnik ucznia

- Opiekun Dziecka w Internecie



Rys. 25. Zrzut programu *Opiekun Dziecka w Internecie*

Więcej uwagi należy poświęcić innej funkcji zawartej we wspomnianych programach. Pozwala ona na wskazanie konkretnych stron, które nie powinny być otwierane – z podaniem określonego adresu lub też tematyki. Po tej czynności młody internauta, nawet podczas nieudolnego wyszukiwania stron, nie będzie narażony na kontakt z pornografią, przemocą itd. Program samodzielnie zablokuje stronę, jeśli jej zawartość będzie wskazana jako niedozwolona.

Inną, bardzo przydatną funkcją jest możliwość kontrolowania czasu spędzonego przez dziecko w Internecie. W tym celu w ustawieniach programu należy wskazać dzień tygodnia oraz godziny, w których (we wskazanym dniu) dziecko może korzystać z komputera. Funkcja ta graficznie przypomina plan lekcji, pozwalając w czytelny sposób określić czas przeznaczony dla dziecka. Można także skorelować ten czas z planem zajęć dziecka w szkole. Zatem możliwe jest ustawienie czasu dla Ani, np.: w środę od godz. 13.00 do 14.00. W efekcie Ania, po powrocie ze szkoły o godz. 12.45, nie zaloguje się w systemie (nie włączy komputera i nie będzie mogła z niego korzystać). Będzie to mogła zrobić, kiedy mi-

nie godz. 13.00. Czas korzystania będzie jednak ograniczony do godz. 14.00, a kiedy minie, system automatycznie wyloguje Anię (uniemożliwi jej dalsze korzystanie z komputera). W ten sposób można precyzyjnie zaplanować każdy dzień tygodnia, wybierając czas korzystania z komputera i blokując wybrane przez nas strony. Ania będzie miała jedynie możliwość podglądu, na co zezwolili jej rodzice. Jednak lepiej będzie omówić to z nią osobiście. Wtedy będzie wiedziała, że nie jest prześladowana, a ochraniana.

* * *

Internet to wielkie dobrodziejstwo, nieskończenie wielka kopalnia wiedzy, która jest, niestety, systematycznie zaśmiecana. Dżungla, w której znajdują się ścieżki proste oraz zawile, bezpieczne i mniej bezpieczne. Zagrożenia te nie powinny jednak powodować, że zrezygnujemy z Internetu. Wręcz przeciwnie, korzystajmy z niego jak najwięcej, cóż bowiem może być przyjemniejszego od zdobywania wiedzy. Trzeba jedynie pamiętać o kilku zasadach bezpieczeństwa, które zostały zawarte w tym poradniku. Mają one posłużyć nam oraz naszym dzieciom, które należy przygotować do wędrówki w sieci. To tak, jak pozwolić samodzielnie poruszać się w mieście. Bez odpowiedniej wiedzy i zasad bezpieczeństwa łatwo o kłopoty. Korzystajmy zatem z Internetu, ale mądrze. Nauczmy się w nim poruszać, byśmy mogli sprawować nadzór nad naszymi dziećmi. Tak jak w życiu – najpierw sami się czegoś nauczyliśmy, by potem móc uczyć dzieci i sprawować nad nimi nadzór, dbając o ich bezpieczeństwo.

Mam nadzieję, że w prosty i czytelny sposób przekazałem kilka rad i wskazówek, które pozwolą rodzicom i ich dzieciom bezpiecznie kroczyć przez wirtualny świat. Jeśli jednak zdarzy się przykra niespodzianka, zawsze można przywołać kogoś do pomocy. Można ją znaleźć m.in. na stronach: www.kmp.szczecin.pl oraz prewencja@kmp.szczecin.pl. Wystarczy opisać sytuację i zadać pytanie.

Program CYBERDŻUNGLA powstał dzięki zaangażowaniu rodziców, uczniów i nauczycieli, którzy czuli potrzebę poznania Internetu i jego zagrożeń.

Andrzej Szrajber



ISBN 978-83-61096-68-9