Vademecum dla rodziców

Komputer i Internet w domu

Publikacja przygotowana przez

Departament ds. Kobiet, Rodziny i Przeciwdziałania Dyskyminacji
w Ministerstwie Pracy i Polityki Społecznej

oraz

Biuro Rzecznika Praw Dziecka

Opracowanie:
Bogdan Kaniuk – Biuro Rzecznika Praw Dziecka
Rafał Lew-Starowicz – Ministerstwo Pracy i Polityki Społecznej

Warszawa 2007

Spis treści

1. Warto wiedzieć

Skąd się wziął Internet.

Nie po raz pierwszy w historii technologia zaprojektowana na potrzeby wojska okazała się niezwykle przydatna w życiu codziennym. Pierwowzorem Internetu była, bowiem sieć Arpanet, która powstała pod koniec lat 60-tych i miała służyć armii amerykańskiej. Rząd amerykański obawiał się, że w przypadku wojny atomowej mogą zostać zniszczone tradycyjne środki komunikacji, nie będzie można kontrolować poczynań wojska i nastąpi decyzyjny paraliż. Zaradzić temu miało stworzenie sieci między komputerami, która miałaby charakter zdecentralizowany, mający wiele równoległych połączeń, które nie można byłoby zniszczyć w ataku rakietowym. Miało to pozwolić na zachowanie systemu wydawania rozkazów, sprawowania kontroli i porozumiewania się podczas globalnego konfliktu. Najprawdopodobniej niewielu naukowców pracujących nad zbudowaniem Arpanetu zdawało sobie sprawę jak ten wynalazek wpłynie na życie zwykłych ludzi już w niedalekiej przyszłości.

• Internet jest młody

Internet upowszechnił się dopiero kilkanaście lat temu. Stało się to możliwe, kiedy do powszechnego użytku weszły modemy telefoniczne, a później stałe łącza szerokopasmowe. W Polsce usługa anonimowego dostępu do Internetu została uruchomiona dopiero w 1996 r. przez TP S.A. W tym samym czasie firma Polbox zaoferowała pierwsze darmowe konta e-mail.

• Co to jest ISP?

ISP to skrót od angielskiej nazwy Internet Service Provider – czyli dostawca usługi internetowej. Dostęp do Internetu możemy uzyskać: za pomocą kabla telewizyjnego (taką usługę oferują operatorzy telewizji kablowej np. Astercity, UPC, itp.) za pomocą kabla telefonicznego i świadczą ją operatorzy telekomunikacyjni np.: Telekomunikacja Polska - Neostrada, Tele2, Netia, itp. Możliwe są też połączenia satelitarne, radiowe, za pomocą sieci telefonii komórkowej, a nawet sieci energetycznej.

Umowy mogą być skomplikowane

Umowy o świadczenie usługi dostępu do Internetu mogą być skomplikowane. Wiele istotnych postanowień znajduje się w dołączonym do umowy regulaminie, który powinien być nam doręczony najpóźniej w momencie zawierania umowy. Nie bójmy się zwrócić na to uwagę podczas rozmowy ze sprzedawcą.
Kiedy otrzymamy kompletną umowę wraz z regulaminem i wszystkimi załącznikami (cennikami, tabelami opłata itp.) nie spieszmy się z podpisywaniem. Spokojnie, bez pośpiechu przeanalizujmy wszystkie postanowienia zwracając szczególną uwagę na takie kwestie jak:

1. rozpoczęcie świadczenia usługi

Należy zwrócić uwagę na to, w jakim czasie ISP jest zobowiązany udostępnić nam usługę, jakie My musimy spełnić warunki oraz jakie są konsekwencje niedopełnienia ww. obowiązków. Należy pamiętać, iż w przypadku takich łączy jak radiowe, satelitarne, telefonii komórkowej może się zdarzyć, że w niektórych pomieszczeniach w domu Internet może nie działać. Częstym błędem konsumentów zamawiających taką usługę jest pochopne podpisywanie umowy bez sprawdzenia poziomu sygnału w pomieszczeniach. Później jest niezwykle trudno od umowy odstąpić bez konieczności poniesienia kosztów.

2. zmiany w regulaminie

ISP może jednostronnie zmienić regulamin w przypadku zaistnienia określonych okoliczności. Niezwykle istotne jest, aby te okoliczności były precyzyjnie ujęte w umowie lub regulaminie. Dostawca Internetu powinien również zapewnić nam odpowiedni czas do namysłu, czy przyjmujemy nowe warunki, czy nie.

3. rozwiązanie umowy

Niezwykle istotną częścią umowy są postanowienia dotyczące rozwiązania umowy. Pamiętajmy, że nie ma nic za darmo. Każda promocja ma swoją „ciemną stronę", którą przeważnie są poważne ograniczenia w możliwości odstąpienia od umowy lub jej wypowiedzenia przed upływem okresu, na jaki została zawarta.

4. obowiązki stron dotyczące eksploatacji sprzętu oraz jego zwrotu po zakończeniu umowy

Generalnie, należy zwrócić uwagę na warunki korzystania z usługi, a w szczególności na warunki eksploatacji użyczonego nam sprzętu służącego do odbioru Internetu oraz obowiązki ciążące na obu stronach w przypadku stwierdzenia wady lub uszkodzenia. Na tym tle bardzo często dochodzi do konfliktów na linii dostawca – odbiorca Internetu.

Należy również pamiętać, iż nie zawsze zakup całego pakietu usług (telewizja kablowa, Internet, telefon) będzie korzystny. Należy dokładnie przeanalizować cenniki (najlepiej kilku przedsiębiorców) porównać i dokonać optymalnego wyboru.

2. Kontrola dostępu i administrowanie

Nie pozwalasz swojemu dziecku chodzić w niektóre miejsca? Nie chcesz, aby Twoje dziecko wracało do domu po 21? Musisz wiedzieć, że podobne granice musisz wytyczyć, jeśli chodzi o korzystanie z komputera.

Zacznij od zaplanowania, gdzie w Twoim domu będzie stał komputer.

Powinien być on w takim miejscu, aby Twoje dziecko korzystając z niego nie było całkowicie wyizolowane. Umieść go w pokoju przechodnim, bądź w miejscu, w którym często przebywasz. Dziecko będzie odczuwało Twoją obecności i jeśli będzie potrzebowało pomocy, czy wyjaśnienia, istnieje większe prawdopodobieństwo, że najpierw poprosi Ciebie.

Zawrzyj ze swoim dzieckiem umowę dotyczącą czasu i sposobu korzystania z komputera.

Taka umowa powinna zawierać nie tylko obowiązki dziecka, ale również Twoje. Nie powinien być to jedynie zbiór zakazów.

Możesz skorzystać z gotowych wzorów dostępnych w Internecie pod adresami np.:

www.dzieckowsieci/images/stories/pliki/umowa1.pdf

www.dzieckowsieci/images/stories/pliki/umowa2.pdf

Poniżej zamieściliśmy również naszą propozycję.

Oczywiście w zależności od potrzeb i wieku dziecka umowę można modyfikować. Ważne jest jednak, aby od razu, na początku, zostały ustalone i przestrzegane pewne zasady korzystania z komputera. Później ich wprowadzenie będzie o wiele trudniejsze ze względu na konieczność przełamywania określonych przyzwyczajeń.

Przedyskutuj z dzieckiem znaczenie postanowień zawieranej umowy.

UMOWA DOTYCZĄCA KORZYSTANIA Z KOMPUTERA I INTERNETU

Dziecko:

Jestem świadomy/ma, że korzystanie z komputera oraz Internetu daje dużo przyjemności, rozrywki, pomaga w poznawaniu świata i kontaktach z innymi ludźmi. Internet jest dobry i pożyteczny, ale są osoby, które używają go, aby krzywdzić innych. Dlatego też, będę mieć ograniczone zaufanie do osób poznanych w Internecie tak samo, jak do osób nowopoznanych w świecie rzeczywistym.

Będę przestrzegał/ła zasad, które wspólnie z rodzicami ustaliliśmy:

1. Będę starał się sprawdzić każdą informację znalezioną w Internecie również w innych miejscach (np. na innych stronach internetowych, w bibliotece, zapytam rodziców)
2. Będę informował rodziców o każdym przypadku, kiedy ktoś poznany w Internecie będzie próbował dręczyć, obrażać, wyzywać, zmuszać do czegoś mnie lub inne osoby.
3. Będę informował rodziców o każdym przypadku, kiedy ktoś poznany w Internecie będzie chciał się ze mną spotkać
4. Będę informował rodziców o każdym przypadku, kiedy zauważę, że z moim komputerem dzieje się coś dziwnego
5. W sposób miły i grzeczny będę odnosił się do innych użytkowników Internetu. Nie będę odpowiadać na zaczepki słowne, ani używać wulgarnego języka
6. Będę prosił rodziców o zgodę i pomoc podczas instalacji nowych programów oraz pomagał rodzicom w obsłudze nowych programów, gier, jeśli rodzice będą chcieli je poznać
7. Będę chronił swoje dane (nazwisko, adres, nr. telefonu) i pod żadnym pozorem nie udostępnię ich nikomu poznanemu przez Internet
8. Nie będę przeglądać stron zawierających treści przeznaczone dla dorosłych
9. Nie będę zaniedbywać swoich obowiązków w szkole i w domu z powodu korzystania z komputera
10. Będę korzystał z komputera nie dłużej niż .... godzin dziennie

W przypadku złamania powyższych zasad zobowiązuje się do: .....

.....

Podpis: .....

Rodzice:

My - rodzice jesteśmy świadomi, iż komputer i Internet mogą stanowić źródło rozrywki oraz mogą pomagać w poszerzaniu wiedzy naszego dziecka oraz ułatwiać kontakt z rówieśnikami. Naszym zadaniem jest pomóc naszemu dziecku, aby korzystanie z niego było pożyteczne i bezpieczne.

Będziemy:

1. Starać się udzielać wszelkiej pomocy we właściwym i bezpiecznym korzystaniu z komputera
2. Starać się poznać nowe programy i gry instalowane przez nasze dziecko
3. Wyjaśniać kwestie związane z bezpieczeństwem komputera
4. Udzielać pomocy w sytuacji, kiedy nasze dziecko poczuje się dręczone, nękane przez innych użytkowników Internetu
5. Zgłaszać administratorom stron internetowych oraz odpowiednim organom przypadki znalezienia treści niezgodnych z prawem
6. Szanować prywatność naszego dziecka
7. Administrować „domowym systemem komputerowym”

Ustalmy, iż komputer będzie stał .....

.....

W przypadku złamania powyższych zasad zobowiązujemy się do: .....

.....

Podpisy:

Mama : ..... Tata: .....

Skonfiguruj system w komputerze

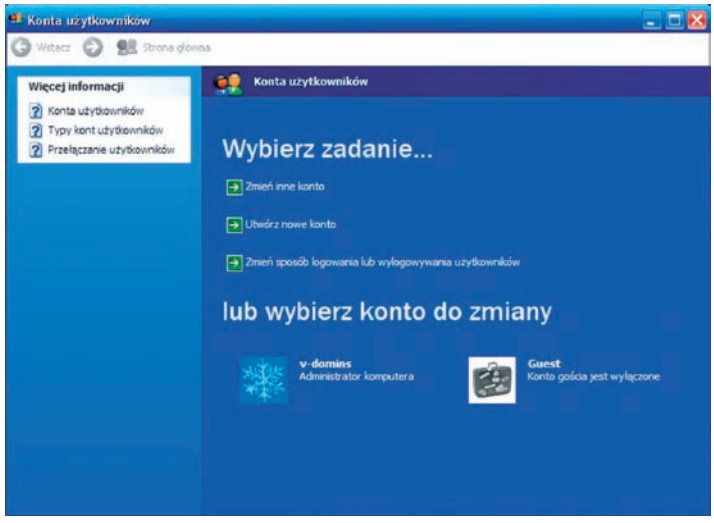
Pewnie wielokrotnie spotkałeś/łaś się z napisem „nieupoważnionym wstęp wzbroniony”. Musisz wiedzieć, że niektóre funkcje komputera powinny być zastrzeżone wyłącznie dla administratora – czyli Ciebie. Dziecko nie powinno mieć do nich dostępu. Dlatego też, niezbędna jest konfiguracja kont użytkowników.

Poniżej przedstawiamy instrukcję krok po kroku opracowaną przez Pana Dominika Sołtysika z firmy Microsoft - jak tworzyć profile użytkowników oraz jakie inne przydatne funkcje posiadają systemy operacyjne Microsoft Windows XP oraz Microsoft Windows Vista.

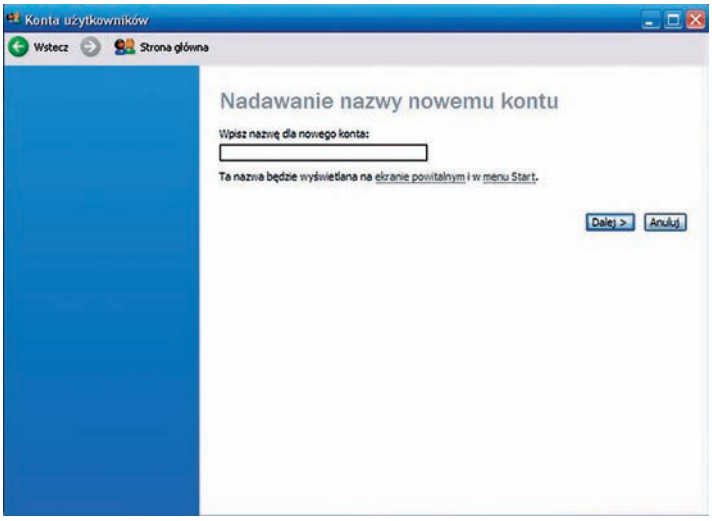
Aby utworzyć nowy profil użytkownika, osoba zalogowana w danym momencie na komputerze, musi posiadać uprawnienia administratora. Jest to konto, które powstaje domyślnie, zaraz po zakończeniu instalacji systemu operacyjnego

Windows XP

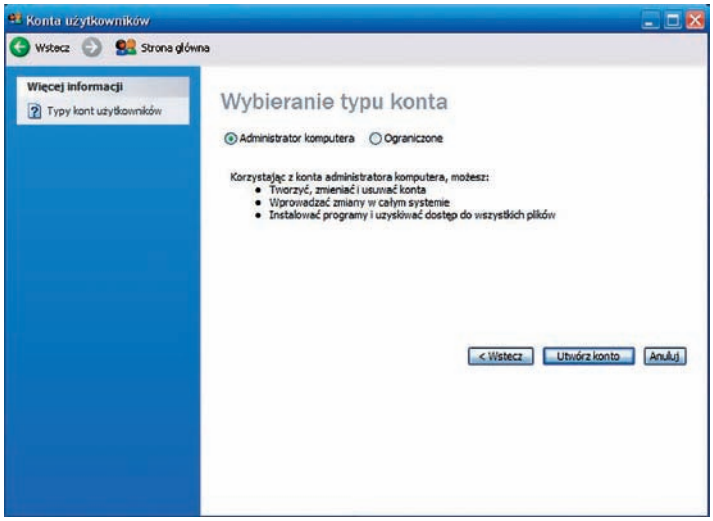
1 Kliknij Start, a następnie wybierz Panel Sterowania. W nowo otwartym oknie kliknij ikonkę konta użytkowników. Uruchamia się Kreator służący do zakładania kont użytkowników. Kliknij opcję „Utwórz nowe konto".



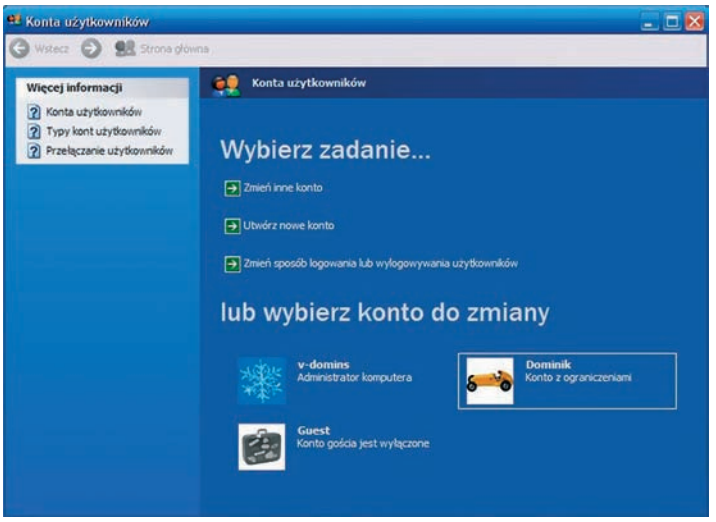
Kolejny monit poprosi o podanie nowej nazwy użytkownika.



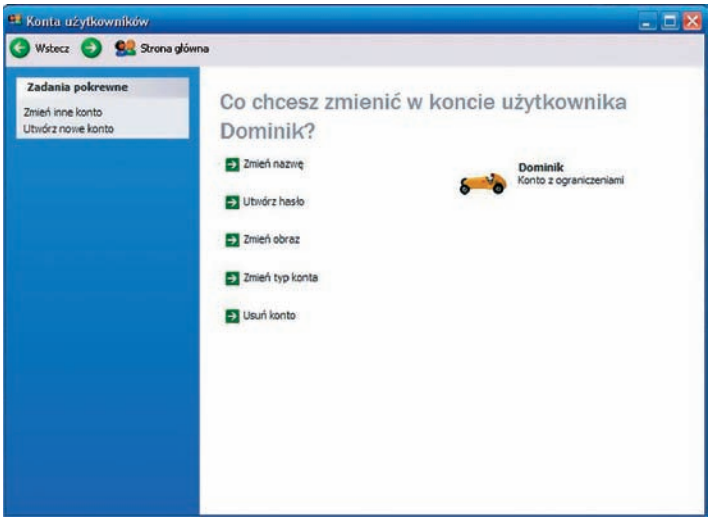
W następnym etapie wybieramy typ konta i wybieramy „Ograniczone", a następnie klikamy „Utwórz konto".



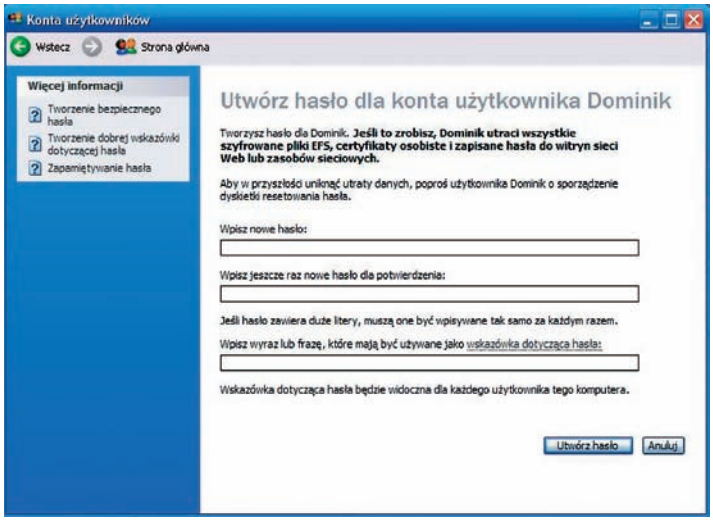
Wracamy do ekranu kreatora, w którym widać, że zostało utworzone nowe konto o nazwie np.: „Dominik".



W następnym kroku klikamy na nowo utworzony profil i wybieramy opcję „Utwórz hasło".



Teraz uzgodniwszy wcześniej z dzieckiem wpisujemy hasło użytkownika i potwierdzamy poprawne wpisanie hasła.

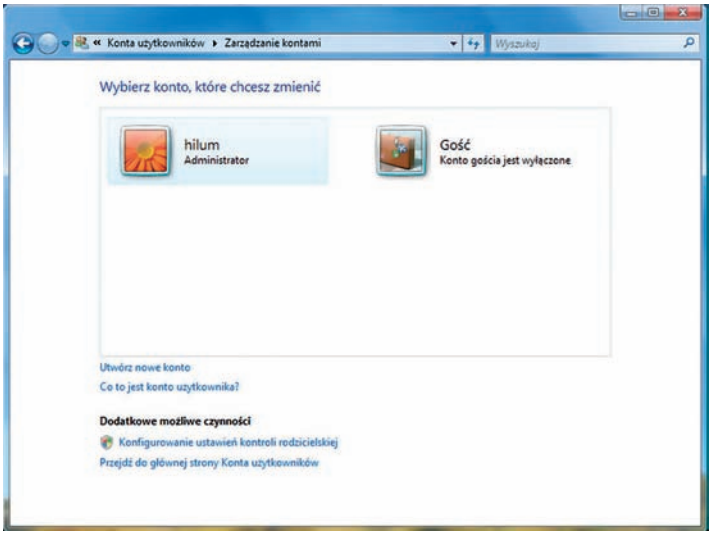


- Aby zabezpieczenie komputera miało sens, powinniśmy w ten sam sposób zabezpieczyć hasłem konto administratora.

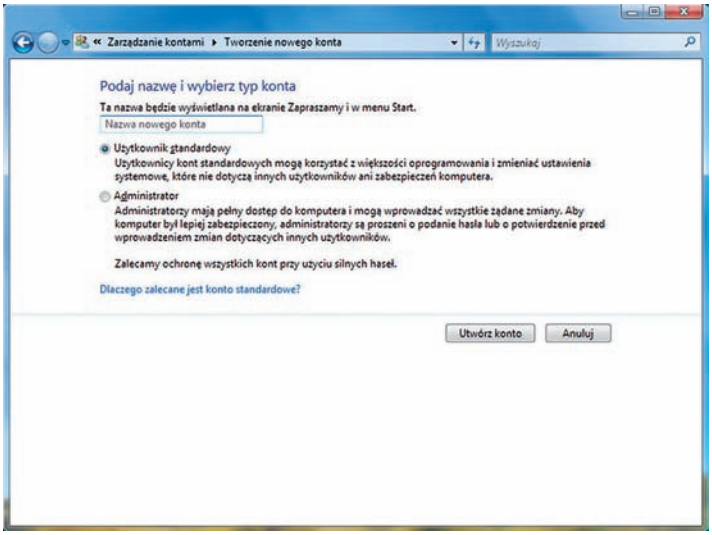
- Tworzenie takiego profilu użytkownika zabezpieczy przede wszystkim sam system operacyjny przed kasowaniem ważnych informacji znajdujących się na danym komputerze.

- W Microsoft Windows Vista, zarządzanie kontami użytkowników jest rozwiązane w znacznie bardziej przejrzysty i czytelny sposób. Możliwości konfiguracyjne są również większe w związku z modułem kontroli rodzicielskiej, jaki znajduje się bezpośrednio w systemie operacyjnym.

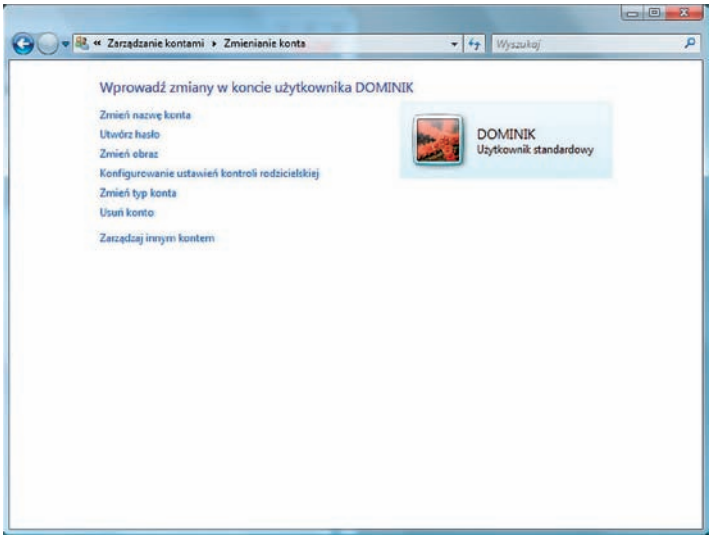
Aby w Windows Vista skonfigurować konta użytkowników, klikamy Start i wybieramy Panel sterowania. W Panelu sterowania odszukujemy i klikamy w ikonę „Konta użytkowników". W uruchomionym kreatorze klikamy opcję „Utwórz nowe konto":



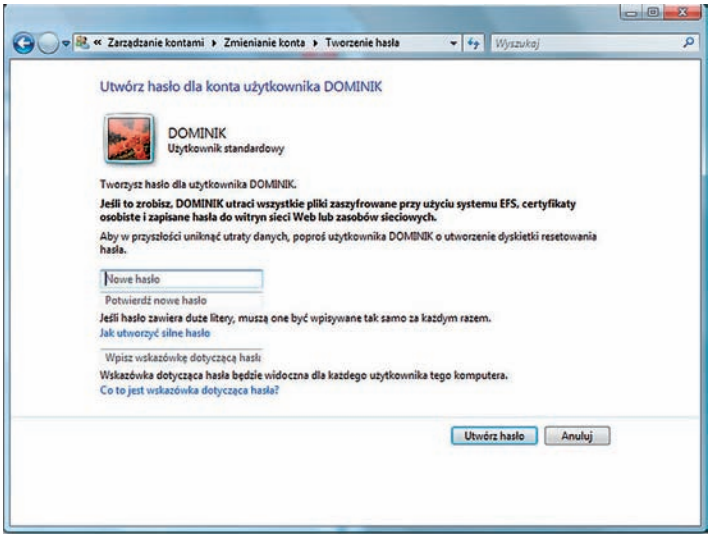
Następnie wpisujemy nazwę nowego konta użytkownika i wybieramy opcję „Użytkownika standardowego”.



W następnym kroku wracamy do ekranu, w którym widać wszystkich użytkowników, także i tego nowo utworzonego o nazwie „DOMINIK”. Aby dokończyć konfigurację, powinniśmy nadać hasło, zarówno użytkownikowi DOMINIK jak i administratorowi.
Klikamy na ikonę użytkownika DOMINIK i wybieramy opcję „Utwórz hasło”



W następnym kroku wpisujemy i potwierdzamy hasło dla nowego użytkownika.

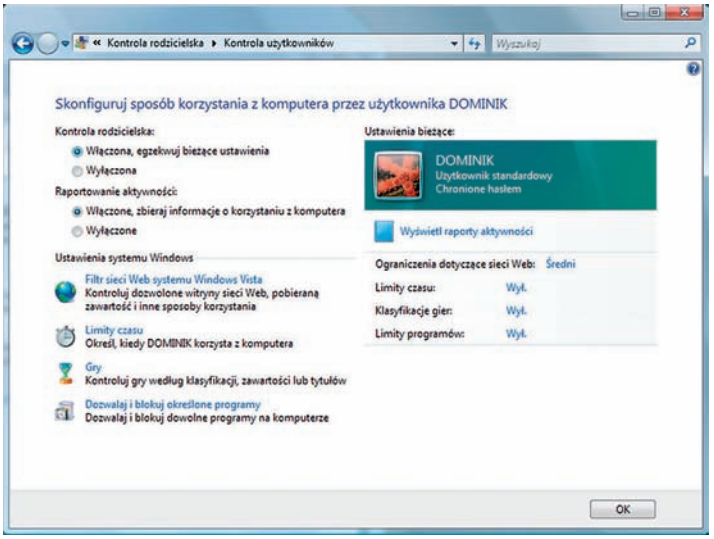


Użytkownik DOMINIK posiada już hasło, pozostało zabezpieczyć hasłem konto administratora.

W tym celu klikamy na jego ikonkę i powtarzamy całą procedurę nadając nowe hasło dla konta administratora.

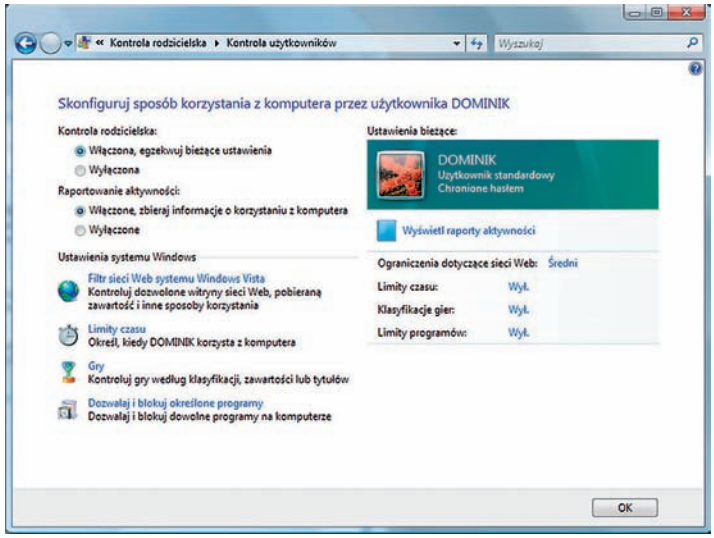
Tak skonfigurowany komputer jest bezpieczny, ale należy pójść o krok dalej i użyć ustawień kontroli rodzicielskiej. W tym celu w klikamy „Opcje bezpieczeństwa rodzinnego" w lewej części okna. W nowo otwartym oknie wybieramy DOMINIKA jako użytkownika, dla którego chcemy ustawić kontrolę rodzicielską.

W następnym ekranie wybieramy następujące opcje:
Kontrola rodzicielska:
Włączona, egzekwuj bieżące ustawienia
Raportowanie aktywności:
Włączone, zbieraj informacje o korzystaniu z komputera.

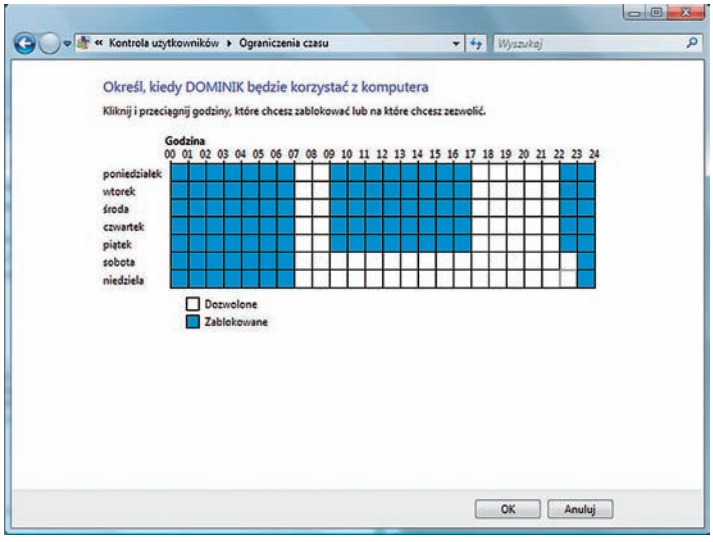


W następnej części ustawimy opcje związane z filtrowaniem sieci Web, limity czasu, ustawienia gier i programów.

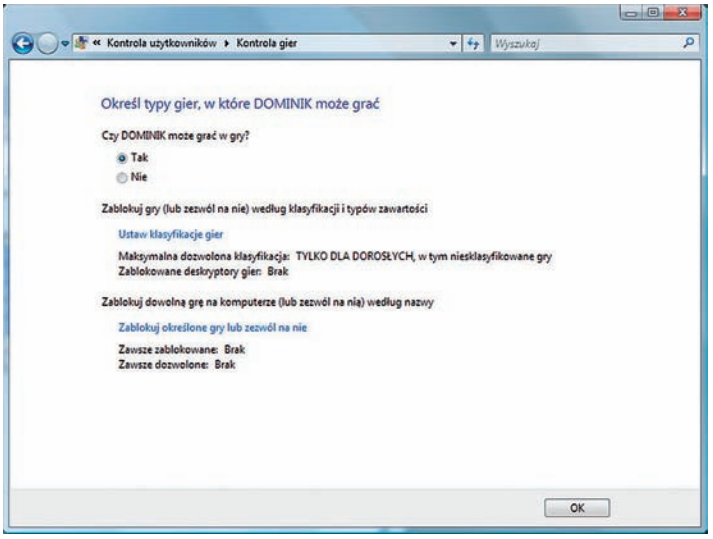
Zacznijmy od filtrów sieci Web, klikamy i przenosimy się do nowego ekranu konfiguracyjnego, w którym możemy zabezpieczyć komputer na dwa sposoby. Pierwszy z nich polega na ustawieniu poziomu filtrowania sieci Web, a drugi na stworzeniu listy dozwolonych i zablokowanych witryn internetowych. Jeśli poświęcimy więcej czasu i stworzymy taką listę, będzie to najpełniejszy sposób zabezpieczenia. W tym ekranie warto również zaznaczyć opcję „Zablokuj pobieranie plików", która uniemożliwi dziecku pobieranie niebezpiecznych plików i dokumentów.



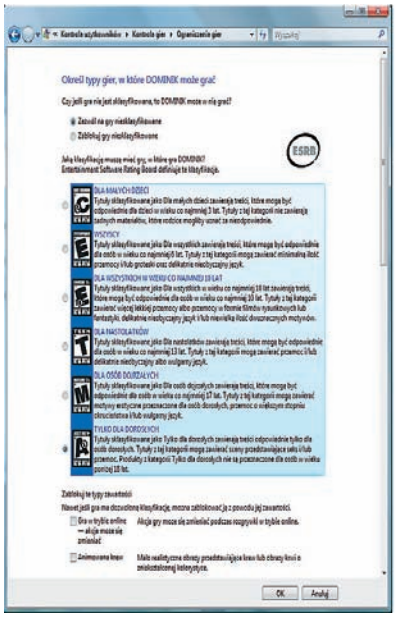
Zatwierdzamy wprowadzone informacje i przechodzimy do ustawień limitów czasowych na korzystanie z komputera. Za pomocą prostej tabeli określamy godziny dozwolone i zablokowane, w określonych dniach tygodnia.

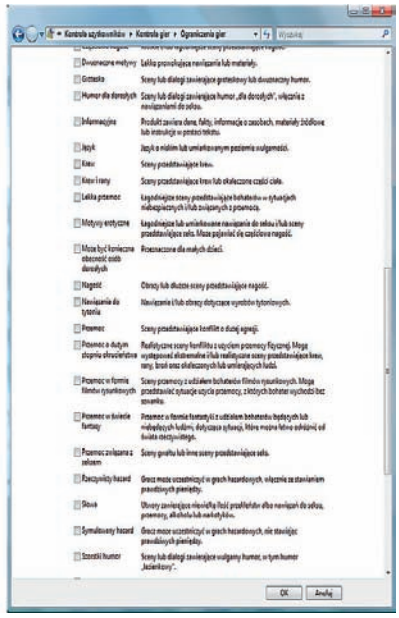


Zatwierdzamy wprowadzone zmiany i przechodzimy do ustawień gier. Na początek odpowiadamy na proste pytanie, czy Dominik może grać w gry? Jeśli tak, to klikamy w opcję „Ustaw klasyfikacje gier".

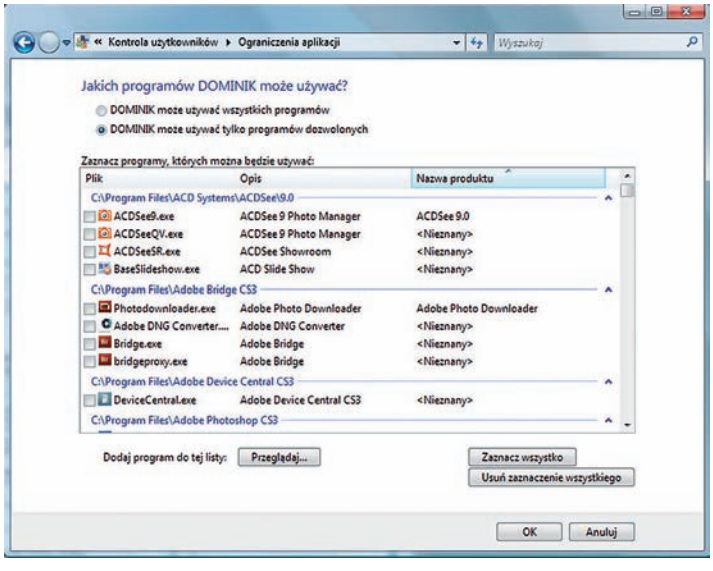


W powyższym ekranie możemy dokładnie określić, w jakie gry. Według klasyfikacji ESRB, DOMINIK może grać lub też, jakich elementów w grach dziecko nie powinno oglądać. Możemy tu wybierać z dość bogatej listy niebezpiecznych elementów.



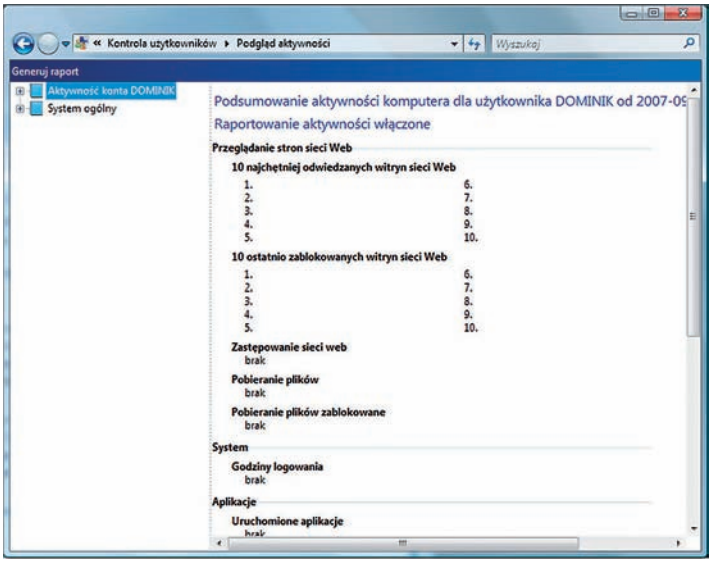


Zatwierdzamy zmiany i przechodzimy do ostatniego już kryterium – dozwolonych aplikacji. Na tym etapie możemy dokładnie określić, z jakich aplikacji zainstalowanych na komputerze aplikacji DOMINIK może korzystać, a z jakich nie.



Po zakończeniu konfiguracji DOMINIK może rozpocząć korzystanie z komputera. Jako Administrator możemy zawsze obejrzeć raport aktywności (dostępny w podstawowym ekranie ustawień kontroli rodzicielskiej) na tym komputerze i zobaczyć, co DOMINIK zrobił podczas korzystania z komputera. Dostępne są następujące informacje:

- **10 najchętniej odwiedzanych witryn sieci Web**
- **10 ostatnio zablokowanych witryn sieci Web**
- **Informacje o pobieranych plikach**
- **Godziny korzystania z komputera**
- **Uruchamiane aplikacje**
- **Uruchamiane pliki multimedialne**
- **Otrzymywane wiadomości e-mail**
- **Otrzymywane wiadomości błyskawiczne w komunikatorach internetowych**



Należy pamiętać, że Ochrona rodzicielska to tylko narzędzie dające rodzicom pewne możliwości. Staje się ono jednak bezużyteczne bez poświęcania uwagi samemu dziecku i braku zainteresowania sposobami korzystania z komputera.

• Używaj oprogramowania filtrującego oraz zabezpieczenia antywirusowego.

Należy pamiętać, że podstawą funkcjonowania w wirtualnym świecie musi być dbałość o zapewnienie właściwej ochrony danych znajdujących się w komputerze oraz bezpieczeństwo. Można porównać to do solidnego zamka w drzwiach, czy alarmu w samochodzie. Przestępstwa „wirtualne" są nie mniej groźne od tych popełnianych w realnym świecie. Mogą dotknąć zarówno Ciebie jak i Twoje dziecko.

Trzeba przyznać, iż zapewnienie bezpiecznego funkcjonowania domowego komputera nie jest łatwe. To duże wyzwanie wymagające często specjalistycznej wiedzy. Niniejsze opracowanie, mamy nadzieję, pomoże Ci sprostać temu zadaniu.

Co może grozić Twojemu komputerowi?

Twój komputer narażony jest na działanie złośliwego oprogramowania rozpowszechnianego m. in. przez Internet – malware:

✔ **Wirusy** – są to złośliwe programy infekujące system komputerowy, przeważnie nastawione na niszczenie danych. Wymagają nosiciela tzn. pliku, programu, pod który są podczepione - dzięki niemu dostają się do systemu komputerowego i powielają się. W przeszłości rozprzestrzeniały się poprzez dyskietki komputerowe, obecnie poprzez Internetowe sieci Peer-2-Peer, pocztę elektroniczną. Znane są również wirusy atakujące telefony komórkowe.

✔ **Robaki (Worms)** – złośliwe programy infekujące system komputerowy i powodujące skutki podobne do działań wirusa. Mogą jednak działać samodzielnie, nie potrzebują „ nosiciela", wykorzystują luki w systemie. Najczęściej atakują za pośrednictwem sieci Peer-2-Peer, poczty elektronicznej, a nawet sieci IRC.

✔ **Trojan** – program działający na tej samej zasadzie jak mitologiczny koń trojański. Zainstalowany w naszym systemie (najczęściej podstępnie, pod postacią użytecznego oprogramowania) znajduje lub powoduje lukę w zabezpieczeniach, dzięki której przestępcy mogą przejąć kontrolę nad komputerem i przekształcić go w zombie[1]. Zaatakowany komputer może służyć do rozsyłania spamu, ataków DOS/DDOS.

[1] Określenie to oddaje w pełni to, co się dzieje po zainfekowaniu z naszym komputerem – staje się on bezwolnym narzędziem w rękach przestępców.

✔ **Spyware** – (z angl. programy szpiegujące) - mają za zadanie, śledzić każdy nasz ruch, zapisują, jakie strony odwiedzaliśmy, jakie mamy zainstalowane programy. Niekiedy również zapamiętują, jakie wpisywaliśmy hasła. Zebrane informacje przesyłane są następnie do nieuczciwych firm zajmujących się marketingiem bądź reklamą. Mogą również służyć przestępcom specjalizującym się w kradzieży haseł i numerów kart kredytowych. Spyware dostają się do naszego systemu komputerowego podstępnie, bardzo często wykorzystując naszą nieuwagę. Instalują się wraz z „darmową" grą, programami typu p2p, dodatkami do przeglądarek internetowych, itp. W wielu przypadkach jesteśmy pytani wprost, czy zgadzamy się na umieszczenie w naszym systemie „dodatkowego programu dla celów marketingowych". Lekkomyślnie klikamy OK, a potem pojawiają się kłopoty. Oznaką funkcjonowania programu spyware może być dziwna aktywność łącza internetowego oraz spowolnienie systemu.

✔ **Rootkit** – program, który wnika bardzo głęboko w ustawienia systemu (nawet te dostępne jedynie dla fachowców). Powoduje ukrycie i zamaskowanie złośliwego oprogramowania (np. spyware, wirusów, robaków lub trojana). Rootkit jest w stanie kontrolować pracę programów antywirusowych i oszukiwać je tak, by błędnie informowały, że system jest czysty. Użytkownik jest zupełnie nieświadomy, że jego komputerem steruje inna osoba używając go do rozsyłania spamu, wirusów oraz ataków na strony internetowe oraz skrzynki pocztowe. Zdarzają się przypadki, że działalność rootkita wykrywana jest dopiero, kiedy naszym komputera zainteresuje się dostawca Internetu, lub Policja.

✔ **Adware** – programy, które instalują się na komputerze bez naszej wiedzy i zgody. Nie są przeważnie groźne dla systemu komputerowego mogą jednak powodować jego spowolnienie, przeciążenie łącza internetowego oraz zajmują miejsce na dysku twardym. Najczęściej są to reklamy, dodatki do przeglądarek internetowych itp.

W październiku br. najgroźniejszymi programami były według www.viruslist.pl[2]:

1. Najbardziej pazerny trojan atakujący banki: tytuł ten przypadł modyfikacji trojana *Trojan-Spy.Win32.Banker.ezn*, który atakuje 45 banków. Jest to dość "skromny" wynik w porównaniu z poprzednim miesiącem, gdy zwycięzca w tej kategorii miał na swym celowniku 134 banki.
2. Najbardziej pazerny trojan atakujący systemy płatności online: *Backdoor.Win32.Xhaker.c* pokazał, że jest sprawiedliwy - atakuje trzy elektroniczne systemy płatności oraz trzy systemy kart płatniczych.
3. Najbardziej pazerny trojan atakujący karty płatnicze: patrz wyżej.
4. Najbardziej ukradkowy program październikowy zwycięzca *Backdoor.Win32.Hupigon.mrv*, podobnie jak wrześniowy, został spakowany przy pomocy dziesięciu różnych pakerów.
5. Najmniejszy szkodliwy program: Mimo niewielkiego rozmiaru - zaledwie 17 bajtów - *Trojan.BAT.DeltreeY.a* ma silny cios.

[2] *Źródło:* www.viruslist.pl, http://www.viruslist.pl/weblog.html

6. Największy szkodliwy program: Po raz kolejny w kategorii tej rządzi rodzina Haradong - w październiku na miano to zasłużył sobie *Trojan.Win32.Haradong.ct* o rozmiarze 244MB, nieco większy niż jego bliski krewny i poprzedni zwycięzca z tej kategorii, Haradong.bj.
7. Najbardziej szkodliwy program: *Backdoor.Win32.Rbot.ejs,* jak wielu poprzednich zwycięzców w tej kategorii, wyłącza rozwiązania bezpieczeństwa poprzez usuwanie ich z pamięci oraz rejestru.
8. Najbardziej rozpowszechniony szkodliwy program w ruchu pocztowym: trzeci miesiąc z rzędu w kategorii tej wygrywa *Email-Worm.Netsky.q*, który w październiku stanowił 20,11% wszystkich szkodliwych programów w ruchu pocztowym.
9. Najbardziej rozpowszechniona rodzina trojanów: w kategorii tej zwyciężył *Trojan-Spy. Win32.Banker* posiadający 563 modyfikacji, o 100 mniej niż wrześniowy zwycięzca.
10. Najbardziej rozpowszechniona rodzina wirusów/robaków: drugi miesiąc z rzędu w kategorii tej prowadzi *Email-Worm.Win32.Zhelatin* (a.k.a Storm), który w październiku posiadał 38 modyfikacji.

● Pozbycie się ww. programów jest niezwykle trudne. Przede wszystkim wymaga zainstalowania antidotum – programu antywirusowego, bądź dodatkowo programu wykrywającego adware. Tego typu aplikacji jest bardzo wiele dostępnych na rynku. Niestety przeważnie są one płatne.

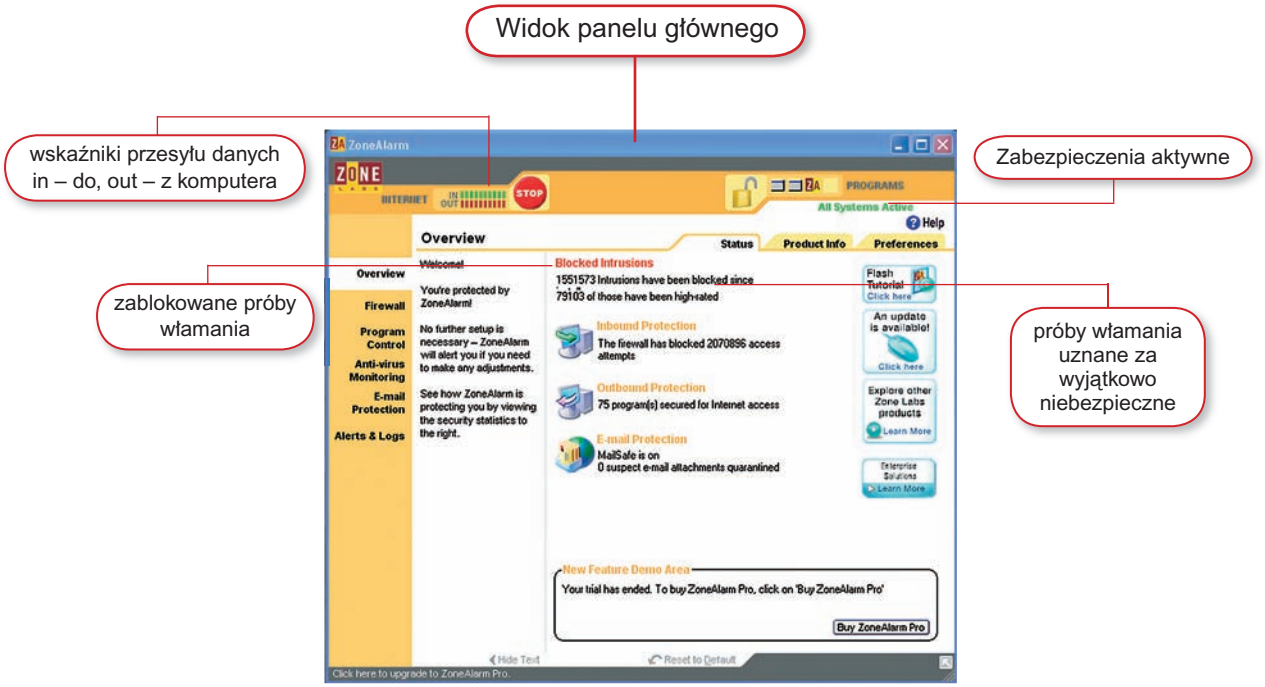
● Bardzo często po usunięciu złośliwego oprogramowania system jest nieodwracalnie uszkodzony i działa niestabilnie. Jedynym ratunkiem może okazać się wtedy jego całkowite przeinstalowanie, które jest procesem żmudnym i czasochłonnym. Dlatego też, niezwykle istotna jest profilaktyka – niedopuszczenie do zainfekowania naszego komputera. Pierwszą i najważniejszą ochroną domowego komputera powinien być zdrowy rozsądek (nieotwieranie nieznanej poczty, nieinstalowanie nieznanych programów itp.) w drugiej kolejności program typu firewall – zapora ogniowa, który chroni komputer przed dostaniem się złośliwego oprogramowania do systemu (działa na styku łącze internetowe – komputer).

● Podobnie jak w przypadku programów antywirusowych mamy bardzo wiele zapór dostępnych na rynku. Najczęściej są one płatne (z niewielkimi wyjątkami). Programy firewall są, co do zasady, bardzo skomplikowane w użytkowaniu. Ich skonfigurowanie oraz poznanie funkcjonowania to nie lada wyzwanie. Niestety dla własnego bezpieczeństwa oraz bezpieczeństwa dzieci trzeba to wyzwanie podjąć. Bez zapory ogniowej nasz komputer jest zupełnie bezbronny, wystawiony na ataki z zewnątrz.

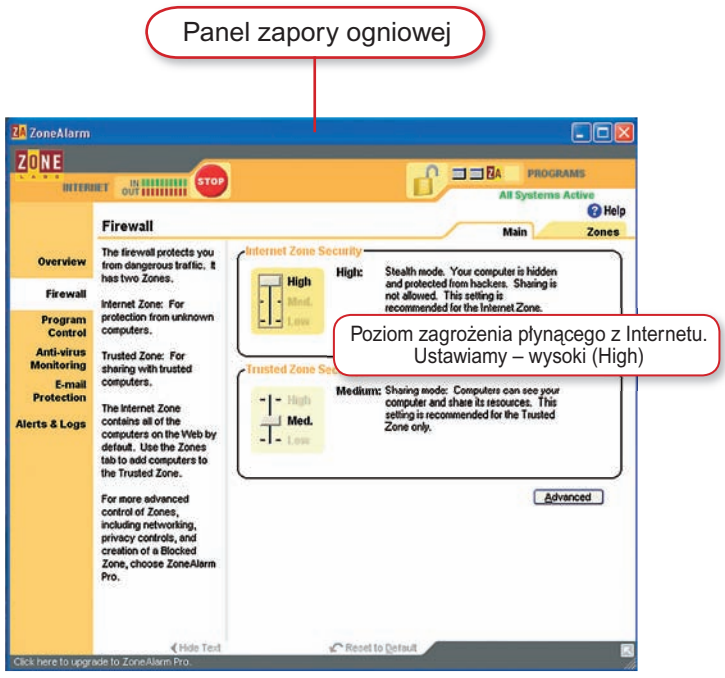
● Do pomocy przy instalacji oraz konfiguracji firewall'a można poprosić kogoś z rodziny - kto jest informatykiem. Można spróbować również znaleźć schematy ustawień programu na formach internetowych. W niniejszym opracowaniu przedstawiamy opis konfiguracji firewall'a na przykładzie jednego z najpopularniejszych darmowych programów tego typu – programu Zone Alarm.

Konfiguracja programu Zone Alarm[3]

Po zainstalowaniu programu Zone Alarm i uruchomieniu pojawi się panel główny (zdjęcie poniżej). Znajdują się na nim podstawowe informacje dotyczące Internetu, dostępu, przesyłu danych oraz ilości prób nieautoryzowanego dostępu do naszego komputera. Należy zwrócić szczególną uwagę na zielony napis w prawym górnym rogu „All systems active" oznacza on, że nasza zapora działa prawidłowo. Z prawej strony widzimy zakładki do poszczególnych funkcji programu.

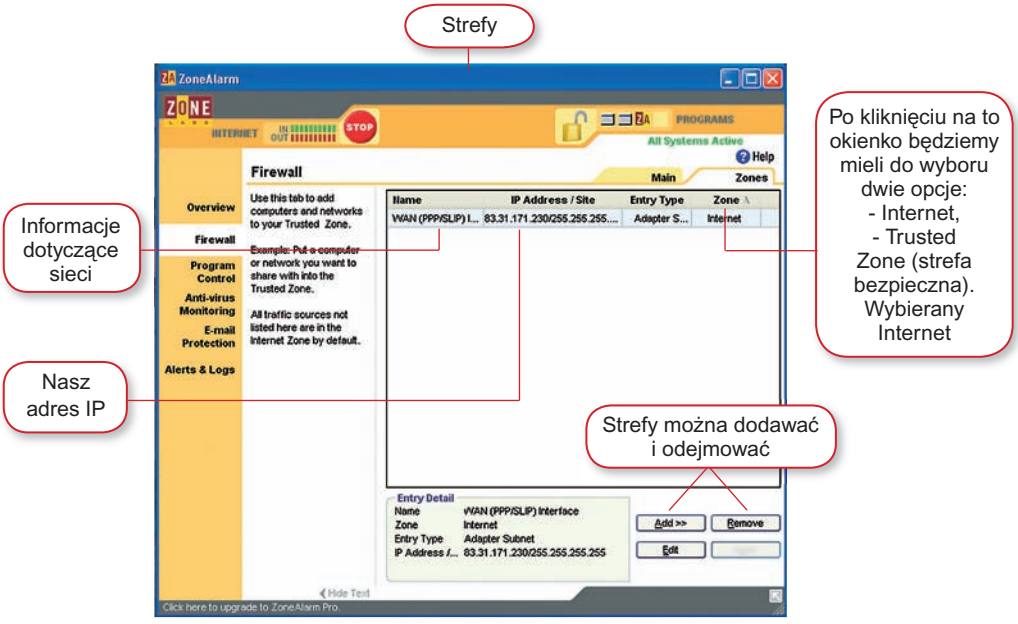


[3] Opracowano korzystając m. in. z publikacji:
- Dariusz Rzeźnicki - *Uszczelnianie Okien*, PC World Online <http://www.pcworld.pl/artykuly/42209_3.html>
- Opis programu Zone Alarm w wersji polskiej, forum IDG <http://forum.idg.pl/index.php?showtopic=4270>



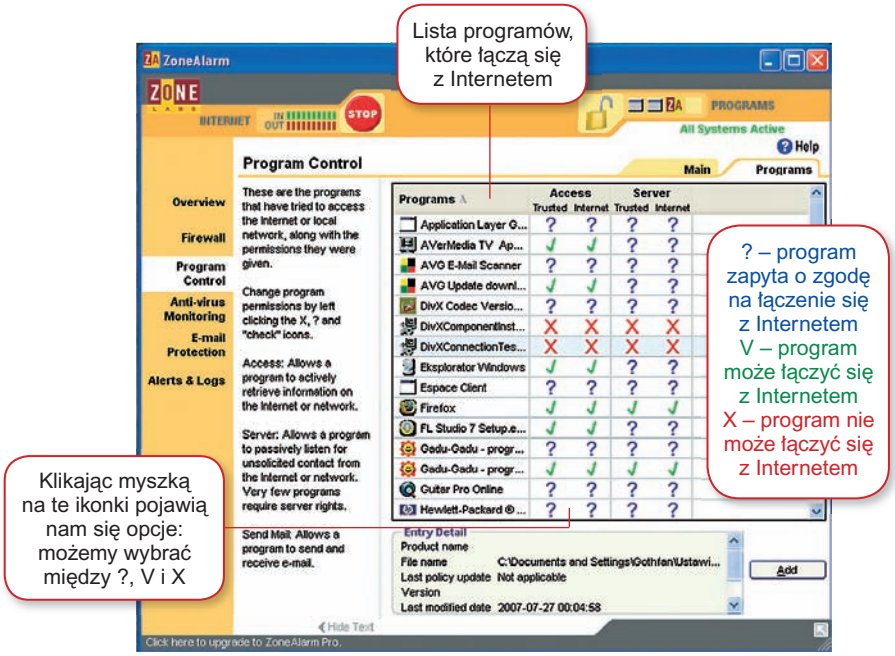
Zakładka „Firewall" i zakładka „Main" to panel naszej zapory ogniowej. Poziom zabezpieczenia obszaru Internetu ustawiamy przesuwając suwakiem na wysoki – „High".

Poniżej przedstawiamy obraz zakładki „Firewall" - „Zones" – strefy. Widzimy podstawowe informacje dotyczące stref zewnętrznych, do jakich połączony jest nasz komputer w tym, strefy Internet.



Zone Alarm przechwytuje żądania dostępu do Internetu wszelkich programów i usług, a następnie prosi użytkownika o decyzję w sprawie zezwolenia na połączenie poszczególnych chętnych. Zgoda bądź odmowa może być udzielona jednorazowo (tylko na konkretny moment) albo na stałe. To, jaką decyzję podejmiemy zależy od nas (i naszej znajomości zainstalowanych na komputerze programów). Możemy również skorzystać z usług wbudowanego do programu doradcy (Advisor), który zasugeruje nam, czy udzielić zgody, czy nie. Z doświadczenia wiemy jednak, że oddanie spraw bezpieczeństwa komputerowemu doradcy nie jest całkowicie dobrym rozwiązaniem. Zdecydowanie lepiej jest poświęcić nieco czasu i uwagi naszemu domowemu systemowi, aby móc samemu podejmować decyzje. W razie wątpliwości możemy spojrzeć na to, co radzi nam nasz doradca lub nie dopuścić do połączenia.

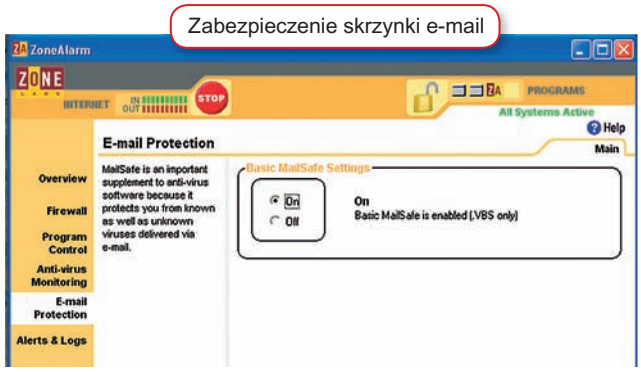
Kontrola programów jest jedną z najważniejszych funkcji programu Zone Alarm. Poniżej przedstawiamy obraz zakładki „Program Control" – „Main". Zawiera on opcje kontroli programów. Sugerujemy wybranie poziomu średniego „Medium" wtedy będziemy mieli pełną kontrolę nad zainstalowanymi na komputerze programami. Można również wybrać opcję „High" - zdajemy się wtedy na doradcę Zone Alarm, o którym była mowa powyżej.



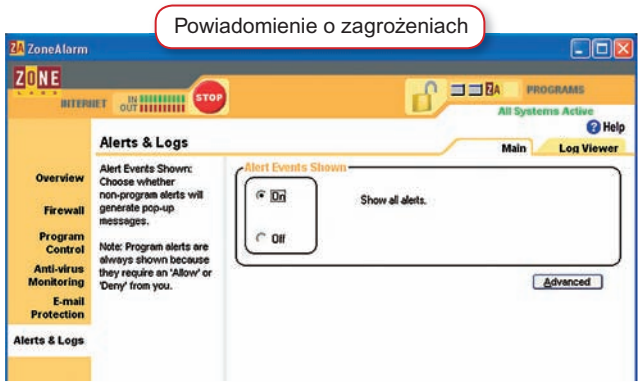
Screen powyżej pokazuje widok zakładki „Program Control" – „Programs" pokazującej, jakie programy zostały wykryte przez Zone Alarm jako łączące się z Internetem. W środkowym dużym oknie widzimy, jakie opcje zostały przydzielone poszczególnym programom:

? – program potrzebuje naszej zgody na połączenie z Internetem
✓ – program nie potrzebuje naszej zgody (jest bezpieczny)
✗ – odmówiliśmy zgody na połączenie programu z Internetem

Każdą z ww. opcji możemy dowolnie modyfikować klikając myszką na wybrany „znaczek". Jest to nasze „centrum dowodzenia" na granicy komputer-Internet. Kolejne ważne zakładki to: ochrona skrzynki e-mail (E-mail protection) i powiadomienia (Alerts & Logs) – poniżej:



Status zabezpieczenia naszej skrzynki e-mail – uruchamiamy wybierając **ON**

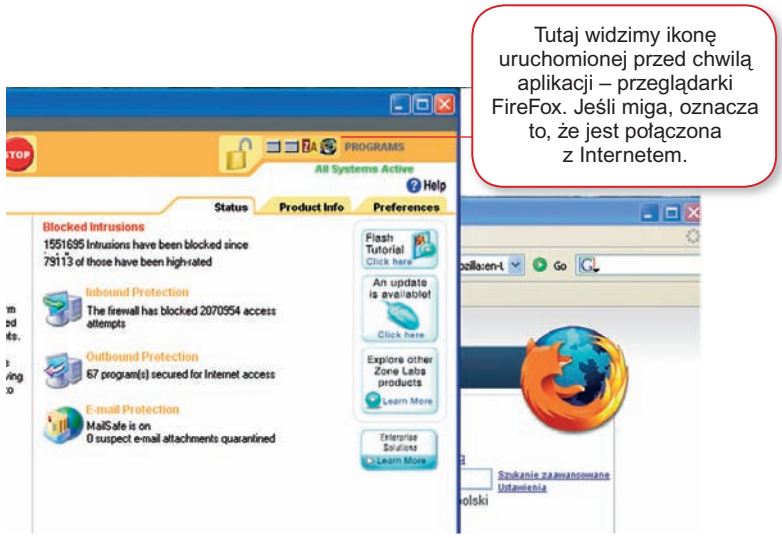


Powiadomienie o zagrożeniach – uruchamiamy wybierając **ON**

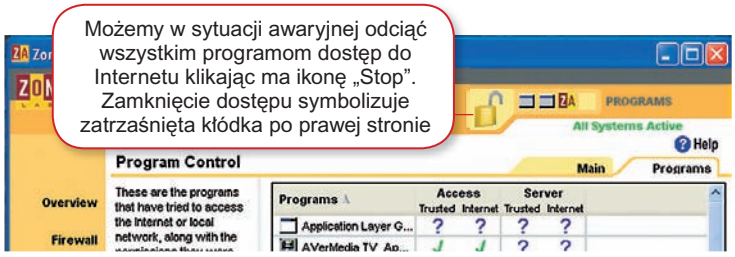
Obok widzimy ikonę powiadomienia o programie, który właśnie próbuje połączyć się z Internetem. Jeśli jest to program nam znany (tak jak w tym przypadku: program Windows Media Player) wybieramy opcję „Zezwalaj" – „Yes". Jeśli klikniemy ikonę „No" – odmowa dostępu program - Zone Alarm zablokuje dostęp do Internetu. Zaznaczając opcję „Remember this answer" firewall zapamięta nasze ustawienie i nie będzie pytał ponownie.

W zakładce Program Control (screen na str. 12) na liście programów pojawi się informacja – Windows Media Player - ? ✓ ?? I ???? (✓ – oznacza, że odblokowano dostęp - „Access"). Klikając myszką na ✓ możemy zmienić status dostępu i wybrać ? (zapytaj przy łączeniu) lub ✘ (nie zezwalaj na połączenie).

Poniżej inny przykład. Uruchamiamy przeglądarkę FireFox. Jeśli chcemy sprawdzić, czy jest uruchomiona i objęta ochroną Zone Alarm patrzymy na ikonki pojawiające się obok kłódki (uruchomione programy wykryte przez Zone Alarm). Widzimy dwa procesy związane (akurat w tym przypadku) z oprogramowaniem Neostrady, Zone Alarm oraz właśnie Fire Fox. Jeśli program pobiera lub odbiera dane z Internetu ikonka będzie pulsować.



Jeśli zaobserwujemy, że nasz komputer zachowuje się dziwnie i mamy podejrzenia, że może być to spowodowane przez połączenie do sieci możemy w prosty sposób zablokować do niej dostęp klikając ikonę „Stop". Kłódka na górze ekranu się zamknie – dostęp do Internetu został zablokowany (obraz poniżej).



W dolnym, prawym rogu widzimy ikonkę „Flash tutorial, Click here" – jest to prezentacja konfiguracji i opcji programu Zone Alarm niestety w języku angielskim.

✔ **Jeśli, chcesz w sposób zaawansowany blokować swojemu dziecku dostęp do Internetu - tylko do niektórych treści, jakie można znaleźć w sieci, możesz skorzystać z jednego z wielu dostępnych na rynku programów filtrujących (zarówno płatnych jak i darmowych). Zespół CERT działający przy NASK przeprowadził testy kilkudziesięciu takich programów. Zachęcamy do zapoznania się z wynikami ww. badania zanim zdecydujemy się na kupno takiego programu. (link do strony badań).**

Zagrożenia związane ze spamem

Spam są to niechciane wiadomości rozsyłane najczęściej drogą e-mailową lub za pomocą komunikatorów internetowych. Mają przeważnie charakter komercyjny – reklamowy. Dużą grupę spamu stanowią również tzw. „łańcuszki szczęścia" oraz wiadomości pozornie niewinne, zawierające w załączniku złośliwe oprogramowanie. Poprzez spam mogą być również rozsyłane treści o charakterze pornograficznym. Dlatego też podejrzaną pocztę należy kasować bez zapoznawania się z jej treścią.

Spam jest zakazany w większości krajów (również w Polsce). Walczą z tym zjawiskiem zarówno organy ścigania jak i instytucje zajmujące się ochroną konsumentów. Niestety bardzo ciężko dotrzeć do rzeczywistego nadawcy spamu. Dlatego też najlepszym sposobem na ograniczenie niechcianej korespondencji w naszej skrzynce mailowej jest dbałość o anonimowość w sieci i ograniczone zaufanie do wiadomości, które przesyła nam nieznana osoba (częstym nośnikiem złośliwego oprogramowania są fałszywe listy miłosne, informacje o wygranej, fałszywe listy wzbudzające współczucie, itp.). Nie ma w 100% skutecznego sposobu zabezpieczenia się przed spamem. Można go ograniczyć poprzez:

- **korzystanie z filtrów antyspamowych (bardzo często takie filtry są wbudowane w skrzynkę e-mail wymagają jedynie, odpowiedniej konfiguracji),**
- **niepodawanie swojego adresu e-mail nieznanym osobom w Internecie (często wymagany jest w procesie logowania do różnego rodzaju portali, lub aby móc skorzystać z darmowego oprogramowania),**
- **nieotwieranie załączników przesłanych przez nieznane osoby,**
- **nieuczestniczenie w „łańcuszkach szczęścia".**

• Omów ze swoim dzieckiem kwestie bezpiecznego korzystania z komputera i Internetu

Jest niezwykle istotne, aby korzystając z komputera mieć świadomość zarówno jego zalet jak i wad. Rozmowa z dzieckiem na ten temat to przede wszystkim Twoje zadanie.

W niniejszym poradniku skupiliśmy się przede wszystkim na kwestiach technicznego ograniczenia zagrożenia związanego z korzystaniem z Internetu. Pozostaje cała grupa problemów związanych z ryzykownym zachowaniem w Internecie i w relacjach z innymi użytkownikami.
Nie powinieneś/powinnaś skupiać się wyłącznie na zagrożeniach, aby nie wywoływać u swojego dziecka uczucia lęku niemniej jednak, należy uświadomić mu, iż:

➡ nieograniczone korzystanie z komputera może doprowadzić do uzależnień oraz zaburzyć relacje Twojego dziecka z rówieśnikami w realnym świecie

➡ w Internecie można znaleźć nieodpowiednie treści (np. pornografia, rasizm, ksenofobia, propaganda niewłaściwych postaw życiowych)

➡ istnieje możliwość kontaktu z przestępcami (szczególnie istotna jest kwestia ograniczonego zaufania do innych użytkowników – nie przekazywanie prawdziwych danych o sobie, nie spotykanie się z osobami poznanymi w sieci)

➡ w Internecie występują takie negatywne zjawiska jak dręczenie, nękanie, pomawianie innych osób (cyberstalking, cyberbulling[4] to zjawiska, których skala wciąż rośnie, a przed którym nie można zabezpieczyć się tylko za pomocą środków technicznych)

➡ za pomocą Internetu przestępcy mogą wedrzeć się do naszego systemu komputerowego, dokonać zniszczenia danych lub narazić nas na straty finansowe.

➡ ściąganie i wysyłanie muzyki, filmów od użytkowników sieci Peer-2-Peer jest łamaniem prawa autorskiego.

Niniejszy poradnik nie jest jedynym, z którego można czerpać wiedze na temat zagrożeń w Internecie. Istnieją całe programy edukacyjne skierowane zarówno do dzieci, jak i dorosłych, które skupiają się na różnych zagrożeniach.

[4] *Patrz:* Słowniczek

W przygotowaniu tematów do takiej rozmowy pomogą Ci również strony

www.dzieckowsieci.pl
www.sieciaki.pl
www.saferinternet.pl

Szczera rozmowa z dzieckiem na ww. tematy ma również tę zaletę, iż dzięki niej Twoje dziecko zrozumie, dlaczego stawiasz mu pewne ograniczenia związane z korzystaniem z komputera i Internetu.

• Nie bądź bierny, jeśli zauważysz w Internecie nielegalne treści

To, czy Internet będzie bezpiecznym miejsce zależy również od Ciebie. Jeśli zauważysz w sieci treści mające charakter nielegalny – propagowanie faszyzmu lub komunizmu, ksenofobia, rasizm i dziecięca pornografia nie odwracaj głowy. Możesz zgłosić anonimowe zgłoszenie do zespołu dyzurnet.pl lub poinformować Policję. Należy również zauważyć, iż zgodnie z art. 14 ustawy o świadczeniu usług drogą elektroniczną, właściciele serwisów są zobowiązani do reagowania na wiarygodny sygnał pojawienia się w serwisie treści niezgodnej z prawem. Możesz zatem zgłosić sprawę bezpośrednio do administratora serwisu.

Zgłaszaj również przypadki publikowania pornografii na serwisach odwiedzanych przez dzieci lub w przypadku kiedy mogą być prezentowane osobom, które sobie tego nie życzą. Sama pornografia nie jest zakazana ale niektóre formy jej prezentowania mogą być sprzeczne z prawem.

3. Co Twoje dziecko robi w Internecie?

Dzieci stykają się z nowymi technologiami na każdym kroku – nowy telefon komórkowy, nowy aparat cyfrowy, wreszcie nowy program w komputerze. Obsługę nowości technicznych dzieci poznają niejako mimochodem, podczas kiedy my-dorośli musimy spędzić wiele godzin, aby zrozumieć funkcjonowanie najprostszych urządzeń. Dlatego też, niezwykle istotne jest, abyśmy interesowali się „nową zabawką" naszego dziecka nawet, jeśli jest to skomplikowana gra, czy też nowy, trudny program komputerowy. Spróbujmy zrozumieć jego funkcjonowanie, a wtedy będziemy mogli sami ocenić, czy może nieść ze sobą zagrożenie.

Poniżej znajdują się wskazówki, jak bezpiecznie korzystać z Internetu razem z dzieckiem:

1. **Bierz udział w procesie instalacji oprogramowania (nie pozwalać dziecku na samodzielne instalowanie programów).**
2. **Czytaj uważnie umieszczone na produkcie ostrzeżenia oraz warunki eksploatacji,**
3. **Zwróć uwagę, czy dany program pochodzi z legalnego źródła.**
4. **Spróbuj poznać jego funkcjonowanie.**
5. **Jeśli nie jesteśmy w stanie sami poznać działania danego programu lub funkcjonowania portalu internetowego (w szczególności rozbudowanych portali społecznościowych) – nie wstydźmy się poprosić o pomoc nasze dziecko.**
6. **Nie bój się zadawać pytań, nawet takich, które z punktu widzenia dziecka wydają się oczywiste.**
7. **Powstrzymaj się z pochopnymi ocenami dotyczącymi przydatności określonych programów, gier itp. do czasu aż poznasz ich funkcjonowanie. Skup się na wskazaniu dziecku ewentualnych zagrożeń.**
8. **Unikaj argumentowania swoich decyzji dotyczących zablokowania dziecku dostępu do niektórych programów słowami: „strata czasu", „nic ci to nie da", „grą się nie najesz" itp.**

Dzieci przeważnie chętnie opowiadają swoim rodzicom o nowo nabytych umiejętnościach. Nie inaczej jest podczas obsługi komputera. Twoje dziecko chce, abyś był z nim i cieszył się z jego nowych osiągnięć w tej dziedzinie.

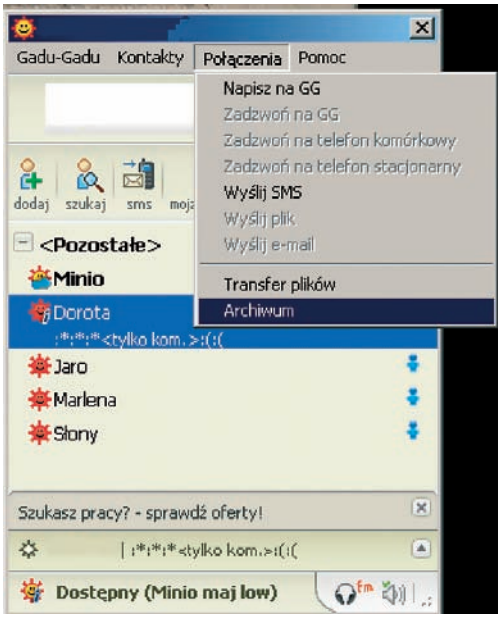
Pamiętaj, że Twoje dziecko wraz z wiekiem coraz bardziej zaczyna cenić swoją prywatność. Kiedy przychodzi okres zainteresowania płcią przeciwną „sprawy sercowe", ploteczki z koleżankami i kolegami stają się najpilniej strzeżoną tajemnicą. Pamiętasz jak zamykałeś/łaś się na wiele godzin w pokoju z dala od rodziców, aby w tajemnicy porozmawiać przez telefon? Dzisiaj możliwość dyskretnego, w tajemnicy przed rodzicami, komunikowania się z rówieśnikami daje pokaźną liczba różnych komunikatorów internetowych oraz chatów. Jeśli Twoje dziecko ma swoje „internetowe" tajemnice nie należy wyciągać pochopnych wniosków i próbować za wszelką ceną sprawdzić, co robiło w Internecie. Możesz w ten sposób na długo zerwać nić zaufania i spowodować, że dziecko ze swoimi problemami skryje się jeszcze głębiej. Przede wszystkim porozmawiaj ze swoim dzieckiem.

Co zrobić jednak, jeśli niepokojące zjawiska nasilają się i podejrzewamy, że ich źródło tkwi w Internecie?

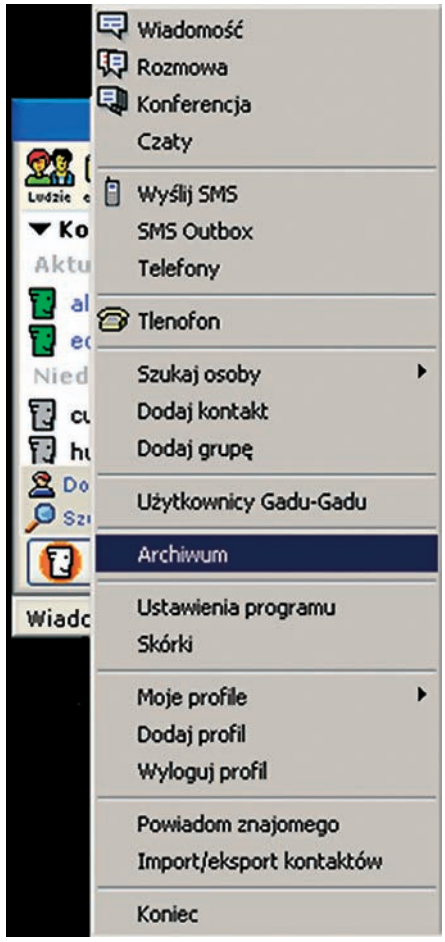
Jeśli sytuacja wydaje się być bardzo groźna i musisz koniecznie wiedzieć, z kim Twoje dziecko się kontaktuje jest na to kilka prostych sposobów. Pamiętaj jednak, że takie działania to ostateczność.

Komunikatory:

- najpopularniejsze komunikatory takie jak Gadu Gadu i Tlen posiadają archiwum rozmów. Jeśli dostęp do komunikatora nie jest zabezpieczony hasłem, a Twoje dziecko nie kasuje regularnie swojego archiwum jest szansa, że znajdziesz tam odpowiedzi na swoje pytania.



komunikator Gadu-Gadu



komunikator Tlen

Portale społecznościowe:

● Jeśli wiesz, pod jakim pseudonimem Twoje dziecko loguje się do portalu możesz sprawdzić, z kim się komunikuje oraz jaką ma grupę znajomych. Nie dotrzesz do konkretnych wiadomości tekstowych, ale możesz zaobserwować, czy wśród znajomych Twojego dziecka nie ma osób wzbudzających podejrzenie (np. osób dużo starszych)

● Portale takie jak grono.net, myspace.com, znajomi.interia wyświetlają zdjęcia i krótkie opisy „przyjaciół" Twojego dziecka, które może obejrzeć każda osoba po wejściu na profil. Ty też możesz mieć swój profil na takim portalu i możesz dzięki niemu obserwować swoje dziecko, jeśli zostaniesz dodany/na do jego listy „przyjaciół". W brew pozorom dzieci (a niekiedy również dorośli) przywiązują duża wagę do tego, kto jest na ich internetowej liście przyjaciół. Fenomen portali społecznościowych polega, bowiem m. in. na możliwości surfowania po profilach swoich przyjaciół, przyjaciół swoich przyjaciół etc. Jeśli wśród nich są rodzice stanowi to wyraz zaufania i silnych więzi rodzinnych.

Przeglądarki Internetowe:

- przeglądarki internetowe zapisują w plikach cookie adresy odwiedzanych stron Internetowych. W przypadku najpopularniejszego Internet Explorera znajduję się tutaj: C:\Documents and Settings\NazwaUżytkownika\Cookies, lub C:\Documents and Settings\NazwaUżytkownika\Temporary Internet Files. Jeśli w ww. plikach znajdują się adresy stron z pornografią jest to znak, że taka strona została wyświetlona na naszym komputerze. Byłby to z pewnością sygnał, że nasze dziecko może przeglądać strony z pornografią. Należy jednak pamiętać, iż taka strona mogła otworzyć się również zupełnie przypadkowo. Niektóre strony WWW (np. udostępniających darmowe programy, gry, tapety, dzwonki itp.) celowo przekierowują odwiedzające osoby na strony z pornografią. Wyjaśnij tę kwestię ze swoim dzieckiem.

Jeśli wyniki Twojego „śledztwa" nie uspokoją Cię nie wahaj się poprosić o pomoc specjalistów z Biura Rzecznika Praw Dziecka, Fundacji Kidprotect, Fundacji Dzieci Niczyje. www.brpd.gov.pl, www.kidprotect.pl, www.fdn.pl, www.helpline.org.pl a w przypadkach podejrzenia przestępstwa – zespołu www.dyzurnet.pl oraz Policji.

4. Gry

Co zrobić, żeby wybrać odpowiednią grę komputerową dla swojego dziecka?

- **Przede wszystkim należy zdecydować jakiego typu ma być to gra oraz czy jest ona odpowiednia do wieku dziecka.**

- **Trzeba pamiętać, iż gry to nie tylko zabawa, rozwijają wyobraźnię, edukują a nawet pomagają w leczeniu i rekonwalescencji pacjentów. Z drugiej strony gry pełne przemocy, mogą wpłynąć negatywnie na psychikę dziecka, od grania na komputerze można się także uzależnić.**

- **W Polsce w gry komputerowe grają coraz młodsze dzieci, dlatego tak ważnym jest wybór odpowiedniej gry, podobnie jak wybór odpowiedniej zabawki dla dzieci.**

Jest wiele kategorii gier komputerowych, najczęściej występujące to:

- **Gry zręcznościowe**, w których na przykład bohater musi zbierać różne przedmioty, pokonywać różne przeszkody.
- **Gry logiczne** – które uczą logicznego myślenia polegając na rozwiązywaniu rozmaitych zadań.
- **Gry sportowe** – zwykle są to gry imitujące konkurencje sportowe takie jak wyścigi czy koszykówka.
- **Gry przygodowe** – w których bohater musi przejść przez szereg plansz, na których natrafia na rozmaite przeszkody do pokonania, odkrywa nowe światy..
- **Gry bijatyki** (zawierają zwykle dużą dawkę przemocy) – często zawierają elementy rozmaitych sztuk walki.
- **Gry strzelaniny** – w których gracz musi używając broni jak największą liczbę razy najcelniej trafić do celu.
- **Gry symulacyjne** – na przykład lot samolotem lub jazdę samochodem.
- **Gry erotyczne** – gry zawierające dużą dawkę erotyki.
- **Gry edukacyjne** – gry służące do pozyskiwania nowych wiadomości z różnych dziedzin nauki i życia codziennego.
- **Gry platformowe** – gry zręcznościowe, w których postać bohatera musi skakać na rozmaite platformy i zbierać różne przedmioty.
- **Gry strategiczne** – gry, które często odwzorowują bitwy mające miejsce w historii oraz polegają na umiejętnym operowaniu oddziałami wojska.
- **RPG** – role playing game w tej kategorii gier, uczestnicy sami tworzą swój świat i zasady w nim obowiązujące.

W dużą ilość gier można grać równocześnie z innymi użytkownikami komputerów w sieci tj. za pomocą internetu jest to zjawisko zwane grą „on line". Taka forma grania niesie ze sobą niebezpieczeństwo powodowane możliwością bezpośredniego komunikowania się ze sobą graczy. Czasem towarzyszy temu wulgarny język a czasem nawet może służyć pedofilom do zdobywania informacji o dziecku. Należy przestrzec dziecko, aby nie podawało nigdy swoich danych osobowych ani informacji mogących być wykorzystanych ze szkodą dla niego.

Należy zwracać uwagę czy gra jest odpowiednia dla wieku dziecka przed jej zakupem.

Takiej informacji udzielą nam istniejące systemy klasyfikacji gier.

W Polsce mamy do czynienia głównie z ogólnoeuropejskim systemem oznaczeń gier PEGI.

Producenci stosujący system oznaczeń PEGI, zamieszczają na opakowaniach gier informację o treściach zawartych w grze za pomocą następujących znaków graficznych:

Ten znak oznacza, iż w grze znajdują się elementy przemocy.

Ten znak świadczy o występowaniu w grze wulgarnego języka

Ten znak ostrzega o występowaniu w grze treści o charakterze dyskryminującym ze względu na rasę, religię etc.

Ten znak ostrzega, iż w fabule gry występują narkotyki.

Ten znak ostrzega, iż treść gry może wywoływać uczucie strachu.

Ten znak mówi o tym, iż w grze występuje element hazardu.

Taki znak informuje o występowaniu w grze treści erotycznych.

Oraz wiek dziecka, od którego może ono mieć bezpieczny kontakt z daną grą:

Gra z takim oznaczeniem nie powinna być udostępniana dzieciom poniżej trzeciego roku życia.

Tak oznaczona gra nie powinna być udostępniana dziecku poniżej siódmego roku życia.

Gra z takim oznaczeniem nie jest przeznaczona dla dzieci poniżej dwunastego roku życia.

Gra z takim oznaczeniem zawiera elementy, które nie powinny mieć styczności dzieci poniżej szesnastego roku życia.

W grze z takim oznaczeniem są elementy, które sprawiają iż jest ona przeznaczona tylko dla osób dorosłych.

Źródło: www.pegi.info

Kontynuacją systemu PEGI w internecie jest projekt PEGI on line, który ma na celu ochronę dzieci i młodzieży przed nieodpowiednimi dla nich treściami w sieci.

PEGI Online opiera się na czterech filarach:

- Kodeksie bezpieczeństwa PEGI Online (PEGI Online Safety Code) i Umowie ramowej podpisywanej przez wszystkich uczestników;
- Logo PEGI Online eksponowanym przez licencjobiorców;
  specjalnej witrynie internetowej dla wnioskodawców i wszystkich użytkowników;
  procesie niezależnej administracji, poradnictwa i rozstrzygania sporów.
  Licencji na eksponowanie Logo PEGI Online udziela Administrator PEGI Online każdemu dostawcy gier, który spełnia wymagania określone w Kodeksie bezpieczeństwa PEGI Online (POSC). Wymagania te obejmują zobowiązanie do ochrony witryny przed niezgodnymi z prawem i obraźliwymi treściami tworzonymi przez użytkowników oraz niepożądanymi linkami, a także środki ochrony młodzieży i jej prywatności podczas udziału w grach internetowych.
- Logo PEGI Online jest umieszczane na opakowaniach gier sprzedawanych w postaci CD/DVD lub w samej witrynie internetowej. Logo wskazuje, czy w daną grę można grać w Internecie i czy dana gra lub witryna jest kontrolowana przez operatora dbającego o ochronę młodzieży.

- Gry, w które nie gra się w Internecie, lecz na konsolach albo komputerach osobistych, będą w dalszym ciągu oznaczane zgodnie z aktualnym systemem PEGI lub innymi funkcjonującymi, uznanymi europejskimi systemami oceny.

Źródło:
www.pegionline.eu

W amerykańskim systemie ESRB oznaczenia przedstawiają się następująco: (zdjęcie)

Tylko dla osób dorosłych

Dla wszystkich

Dla wszystkich powyżej 10 roku życia

Dla małych dzieci

Dla nastolatków powyżej 17 roku życia

To oznaczenie pojawia się na reklamach, zwiastunach gry gdy gra oczekuje na oficjalne oznaczenie.

Dla nastolatków

Źródło: www.esrb.org

Oprócz powyższych oznaczeń występuje na opakowaniu opis w języku angielskim treści zawartych w grze.

5. Słowniczek

➜ **ADSL** – Asymetric Digital Subscriber Line – Asymetryczne, szerokopasmowe łącze internetowe. Przesyłanie danych do użytkownika (z Internetu) jest szybsze od odwrotnego transferu. Technologia ta stworzona została z myślą o użytkownikach częściej odbierających dane (np. ze stron internetowych, programów p2p) niż wysyłających dane. Przykładem łącza ADSL może być np. neostrada.

➜ **Aplikacja** – inaczej program komputerowy lub użyteczny element oprogramowania.

➜ **Aukcja internetowa** - rodzaj aukcji przeprowadzanej za pośrednictwem Internetu. W ramach internetowego serwisu aukcyjnego internauci składają kolejne oferty kupna. Aukcję wygrywa ta osoba, która zaproponuje najwyższą cenę. Z punktu widzenia prawnego aukcje internetowe mają taką samą wagę jak te tradycyjne.

➜ **Admin** – popularne w środowisku internetowym określenie administratora – osoby odpowiedzialnej za przestrzeganie zasad panujących w danym serwisie/portalu/stronie internetowej. Adminowi przysługuje prawo banowania użytkowników (od angl. ban – zakazywać), czyli uniemożliwienia ponownego wejścia na dany serwis/portal/stronę internetową bądź wypowiadania się w określonym temacie na forum internetowym. Pomocą administratorowi mogą służyć ustanowieni przez niego moderatorzy, którzy obserwują, co robią inni użytkownicy.

➜ **Atak DOS/DDOS** – Denial Of Service/Distributed Denial Of Service – Przeciążenie systemu ofiary. W wersji DDOS polega na tym, iż na sygnał, z dużej ilości komputerów, w tym samym czasie, wysyłana jest prośba do systemu ofiary o skorzystania z usług, jakie oferuje. Dla każdej takiej prośby atakowany komputer musi przydzielić pewne zasoby (pamięć, zasoby procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań, z którymi ofiara nie może sobie poradzić, prowadzi do przerwy w działaniu lub nawet zawieszenia systemu.

➜ **Awatar** – obrazek umieszczany przez użytkowników forów internetowych, portali społecznościowych, itp. w swoim profilu, w pobliżu internetowego pseudonimu. Pojawia się wszędzie tam gdzie dany użytkownik się wypowiada. Jest ilustracją, dodatkową informacją na temat użytkownika, jest jego „witualną twarzą". Awatarem może być zdjęcie internauty, logo lub jakakolwiek grafika.

➜ **Blog** – rodzaj pamiętnika, bądź dziennika prowadzonego w Internecie, w formie strony internetowej. Na blogu oprócz tekstu mogą znajdować się również zdjęcia i klipy filmowe.

➜ **Botnet** – sieć komputerów zainfekowanych przez wirusa (komputerów zombie), pozostająca pod kontrolą innych osób, może służyć do popełniania przestępstw.

➜ **Cyberstalking** – anonimowe dręczenie innych osób za pomocą Internetu.

➜ **Cyberbulling** – prześladowanie, poniżanie i nękanie za pomocą Internetu.

➜ **Czat** – serwis internetowy służący do komunikacji pomiędzy wieloma użytkownikami Internetu. Na czacie prowadzi się rozmowę w czasie rzeczywistym, poprzez wpisywanie kolejno wiadomości tekstowych, które następnie wyświetlają się na monitorach rozmówców. Zwykle istnieją dwa rodzaje rozmowy – prywatna, której przebieg mogą śledzić tylko dwie osoby, oraz publiczna, dostępna dla wszystkich zalogowanych użytkowników (źródło Wikipedia – pl.wikipedia.org). Internauci przeważnie występują pod pseudonimami, które niekiedy mogą stanowić pewne źródło informacji niestety bardzo mało wiarygodne (np. pseudonim Jacek34 - prawdopodobnie oznacza, iż użytkownik ma na imię Jacek i ma 34 lata). W części czatów dostępne są również graficzne emotikony, stworzone dla ułatwienia ekspresji emocji

➜ **DSL** – Digital Subscriber Line – inaczej szerokopasmowe łącze internetowe

➜ **E-mail** – poczta elektroniczna – usługa polegająca na przesyłaniu wiadomości tekstowych (listów) z jednego komputera do drugiego za pomocą Internetu.

➜ **Emotikony** – graficzne znaki obrazujące emocje (np. uśmiech, zdenerwowanie, szczęście, łzy itp.) wykorzystywane przez internautów podczas rozmów. Używanie emotikonów podczas internetowych rozmów stało się do tego stopnia popularne, że pewne sekwencje znaków powodujące wyświetlenie się emotikonu używane są przez młodzież również podczas pisania sms-ów oraz tradycyjnych listów. Przykłady takich sekwencji to: **;)** – uśmiech z przymrużeniem oka, **:)** – normalny uśmiech, **:(** - smutek, **;(** - płacz, **:D** – uśmiech „pełną gębą”, **:P** – wystawia język, **:/** - krzywi się, **:|** - zmartwiony, **:]** – krzywy uśmiech, **:O** – zdziwiony, **:>** – spogląda z niedowierzaniem.

➜ **ESRB** – jeden z systemów klasyfikacji gier

➜ **FAQ** – Frequently Asked Questions – z angl. „najczęściej zadawane pytania”, najważniejsze informacje dotyczące korzystania z określonego programu/serwisu itp., rodzaj „instrukcji obsługi”.

➜ **Firewall** – patrz. zapora ogniowa

➜ **Forum dyskusyjne** – zorganizowane w ramach strony lub portalu internetowego miejsce wymiany poglądów przez użytkowników. Na niektórych forach możliwe jest dołączanie do tekstu emotikonów, zdjęć, a nawet filmów.

➜ **Grooming** – zjawisko uwodzenia dzieci za pomocą Internetu w celu wykorzystania seksualnego, przez osoby, które mogą mieć skłonności pedofilskie.

➜ **Hacker** – osoba szukająca i wykorzystująca luki w zabezpieczeniach systemu komputerowego.

➜ **IMHO** – In My Humble Opinion – zwrot używany podczas rozmów internetowych oznacza: „moim zdaniem”.

➜ **IP** – Internet Protocol Adress – unikatowy numer przyporządkowany urządzeniom podłączonym do sieci Internetowej. Adres IP jest przyznawany każdemu użytkownikowi przez jego dostawcę Internetu (ISP)

➜ **ISP** – Internet Service Provider – dostawca usługi internetowej np. Telekomunikacja Polska, Tele2, Netia.

➜ **Komunikator internetowy** – oprogramowanie służące do kontaktu między użytkownikami Internetu

➜ **Login** – od angielskich słów log in (zalogować), ciąg znaków identyfikujący użytkownika, podawany przez niego w procesie rejestracji konta np. na portalu społecznościowym, w serwisie mailowym, czy też w systemie operacyjnym. Bez znajomości loginu i hasła nie uzyskamy dostępu do konta użytkownika.

➜ **LOL** – Lot Of Laugh – zwrot używany podczas rozmów przez społeczność internetową, oznacza: „dużo śmiechu".

➜ **P2P – Peer-2-Peer** – model komunikacji umożliwiający jednoczesny, wzajemny odbiór i przesył danych z dwóch lub większej ilości komputerów. Technologia P2P wykorzystywana jest przez różnego rodzaju programy służące do wymiany danych (obrazów, muzyki, filmów) między użytkownikami Internetu. Najpopularniejsze z nich to: eMule/eDonkey, Soulseek, Bitorrent, WinMX, Kazaa, eMesh, Bearshare i inne. Korzystanie z sieci P2P umożliwia pobieranie danych i to praktycznie za darmo ale niejako „w zamian" wymusza udostępnianie zgromadzonych na komputerze zasobów. P2P działa na zasadzie „bierzesz to dawaj". Z punktu widzenia prawnego możemy mieć do czynienia z naruszaniem praw autorskich, jeśli użytkownik pobiera bądź udostępnia dane chronione prawem.

➜ **PEGI** – Pan European Game Information – jeden z systemów klasyfikacji gier, najpopularniejszy w Europie.

➜ **Portal internetowy** - rodzaj serwisu informacyjnego, dla którego nośnikiem jest Internet. Cechą charakterystyczną portalu jest zgromadzenie w jednym miejscu dostępu do różnorodnych usług, co ma zachęcać użytkownika do ustawienia adresu portalu jako strony startowej w przeglądarce www i traktowania go jako bramy do Internetu. Zazwyczaj portal zawiera informacje będące przedmiotem zainteresowania szerokiego grona odbiorców takie jak: aktualne wiadomości, prognoza pogody, katalog stron WWW, chat, forum dyskusyjne wyszukiwarka internetowa. W celu przyciągnięcia większej ilości użytkowników portale mogą oferować darmowe konta poczty elektronicznej, miejsce na strony WWW i dostęp do innych usług (np. multimedia, pobieranie plików, grupy dyskusyjne). Dla zarejestrowanych użytkowników mogą być dostępne dodatkowe usługi lub usługi o wyższej jakości niż dla użytkowników nierejestrowanych (źródło: Wikipedia – pl.wikipedia.org). Najpopularniejsze polskie portale internetowe to: Onet, Interia, Wirtualna Polska, o2.

➜ **Portale społecznościowe** – portale internetowe nastawione na interakcję miedzy użytkownikami Internetu. W przeciwieństwie do tradycyjnego portalu przepływ informacji odbywa się nie według modelu twórca portalu à użytkownik ale przede wszystkim użytkownik à użytkownik. Sam portal pełni rolę klamry spajającej społeczność, która powstała w jego ramach. Ważną cechą portalu społecznościowego jest to, że użytkownicy są jednocześnie jego współtwórcami. Kreują i decydują o tym, co się na nim dzieje. W przeciwieństwie do stron WWW i tradycyjnych portali, które są „odgórnie" stworzo-

ne przez właściciela i mogą być w zasadzie jedynie przeglądane, portale społecznościowe istnieją przede wszystkim dzięki aktywności swoich użytkowników. Najpopularniejsze portale społecznołciowe to: grono.net, epuls.pl, znajomi.interia.pl, fotka.pl, myspace.com, youtube.com. Na temat bezpieczeństwa portali społecznościowych powstał w Biurze Rzecznika Praw Dziecka raport „Internetowe portale społecznościowe a bezpieczeństwo dzieci" dostępny pod adresem: www.brpd.gov.pl/uploadfiles/publikacje/Raport.doc.

➜ **Profil użytkownika** – jest istotną częścią każdego portalu/serwisu społecznościowego, pokazuje kim jest użytkownik. Często zawiera, opis jego zainteresowań, poglądów, itp. Niekiedy w profilu użytkownika znajdziemy informacje na temat internetowych przyjaciół użytkownika, a nawet będziemy mogli odsłuchać jego ulubione piosenki, lub obejrzeć klip filmowy (umożliwiają to portale np.: www.youtube.com, www.myspace.com lub polski www.wrzuta.pl). Jeśli użytkownikiem jest dziecko, to ww. informacje mogą być wykorzystane przez osoby o skłonnościach pedofilskich, w procesie uwodzenia dziecka. Dlatego też, część portali społecznościowych umożliwia zamaskowanie części danych znajdujących się w profilu i udostępnienie ich wyłącznie osobom, które użytkownik oznaczy jako zaufane.

➜ **Screen** – inaczej obraz ekranu komputera.

➜ **Spam** – niechciane wiadomości rozsyłane najczęściej drogą e-mailową lub za pomocą komunikatorów internetowych. Mają przeważnie charakter komercyjny – reklamowy. Dużą grupę spamu stanowią również tzw. „łańcuszki szczęścia" oraz wiadomości pozornie niewinne, zawierające w załączniku złośliwe oprogramowanie.

➜ **Surfowanie** – popularne określenie oznaczające przeglądanie stron internetowych, poszukiwanie informacji w Internecie itp.

➜ **System operacyjny** – OS - program komputerowy bądź zbiór programów, który zarządza sprzętem oraz aplikacjami komputera (źródło Wikipedia - pl.wikipedia.org), jest bazą, podstawą do działania innych programów komputerowych. Najpopularniejszymi programami operacyjnymi są Windows, Linux, MacOS.

➜ **Wortal** – portal wertykalny – portal internetowy specjalizujący się w określonej dziedzinie np. edukacja, medycyna, gry komputerowe. W odróżnieniu od portalu internetowego, który stara się połączyć informacje z różnych dziedzin i jest „wszystkim w jednym" wortal skupia się na konkretnym zagadnieniu.

➜ **Zapora ogniowa** – oprogramowanie służące do ochrony systemu komputerowego przed zagrożeniem z zewnątrz np. z Internetu. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz odmawianie żądań dostępu pochodzących ze źródeł uznanych za niebezpieczne.