

# Poradnik bezpieczeństwa



# Zagrożenia



## Internet – puszka Pandory.

Sieć Internetowa jest coraz częściej obecna i wykorzystywana w życiu codziennym każdego człowieka. Jej cechą jest wiele zalet takich jak np. ciągły postęp i rozwój, powszechny dostęp do informacji, komunikacja o skali globalnej, wygoda użytkownika czy też możliwość dokonywania płatności online. Oprócz tych zalet są jednak także wady i zagrożenia, którymi są chociażby wirusy dla których Internet jest nośnikiem. Coraz częściej z sieci korzystają także najmłodszy, którzy są najłatwiejszą grupą docelową dla ataków cyberprzestępców. Bezpieczeństwo komputerów powoli staje się więc sprawą absolutnie podstawową zarówno dla firm i przedsiębiorstw jak i dla użytkowników domowych i ich rodzin.

## Sytuacja na froncie walki z cyberprzestępczością.

Wirusy i złośliwe oprogramowanie nie są już niestety domeną filmów science-fiction. Już dawno stały się one codziennym zagrożeniem dla wszystkich nas korzystających z komputerów osobistych. Z najnowszych badań wynika, że codziennie w Internecie powstaje ok. 40 mutacji wirusów, których istnieje już ponad milion. Codziennie w Internecie pojawia się ok. 150 fałszywych stron wyłudających dane osobiste lub konta bankowe użytkowników. Podobnie z bardzo popularnymi ostatnio programami szpiegowskimi, których dziennie powstaje ok. 500. Jeśli dodamy do tego rootkity, trojany i spam, które są wyjaśnione poniżej to możemy mieć wstępne wyobrażenie o tym jak bardzo jest zagrożony nasz komputer osobisty oraz jego użytkownicy.

## Zagrożenia.

Istnieje wiele zagrożeń, które czyhają na użytkowników Internetu. Często nie jesteśmy świadomi tego, że nasz komputer jest atakowany w momencie kiedy przeglądamy strony Internetowe, robimy zakupy przez Internet lub odbieramy pocztę elektroniczną. Zagrożenia i złośliwe oprogramowanie ciągle ewoluuje i zmienia się wykorzystując nowe sposoby i techniki ataków. Poniżej znajdziesz informacje na temat podstawowych rodzajów zagrożeń oraz sposobów walki z nimi.

## Wirusy komputerowe

Wirus komputerowy to najczęściej dość prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirus komputerowy w przeciwieństwie do robaka komputerowego do swojej działalności wymaga nośnika w postaci programu komputerowego, poczty elektronicznej, przenośnego nośnika danych (USB, płyty CD) itp. Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i bez troskę użytkowników.

Często wirusami komputerowymi mylnie nazywane są wszystkie złośliwe programy co nie jest prawdą.

Wirusy mają rozmaite zastosowanie utrudniające lub wręcz uniemożliwiające użytkownikowi pracę z komputerem. Głównym celem wirusów jest zarażanie coraz większej ilości komputerów i użytkowników. Coraz częściej wirusy stają się źródłem zarobku dla ich twórców w rozmaity sposób wymuszając dane i pieniądze

# Zagrożenia



nieświadomego użytkownika komputera, którego zabezpieczenia są niewystarczające do odparcia ataku. Wirusy atakują także hardware czyli sprzęt komputerowy użytkownika, spowalniając go lub czyniąc bezużytecznym.

## Zapora internetowa – Firewall

Tarcza internetowa umożliwia bezpieczne korzystanie z zasobów Internetu, a jednocześnie blokuje dostęp do potencjalnie niebezpiecznych stron. Zabezpiecza komputer przed atakami włamywaczy i złośliwymi programami, takimi jak wirusy, robaki i trojany. Bardzo ważne jest korzystanie ze sprawdzonych i szczelnych zapór Internetowych oferowanych przez uznane firmy zajmujące się zabezpieczeniami na rynku.

Jeżeli nie jesteś zaawansowanym użytkownikiem staraj się korzystać z domyślnych ustawień zapory internetowej dostępnej w ramach Twojego oprogramowania zabezpieczającego.

## Po czym poznać że komputer jest zakażony wirusem?

Symptomów zakażenia komputera wirusem jest wiele, poniżej znajdziesz najczęstsze z nich:

- ▶ komunikat o wykrytym zagrożeniu wysyłany do użytkownika przez oprogramowanie antywirusowe. W takich wypadkach postępuj zgodnie z zaleceniami oprogramowania, dystrybutora.
- ▶ wolniejsze i mniej sprawne działanie systemu operacyjnego
- ▶ zwiększona liczba reklam wyświetlających się na stronach przy przeglądaniu zasobów Internetu
- ▶ zmiany w działaniu przeglądarki internetowej
- ▶ problemy w działaniu niektórych programów

### Wskazówki:

- ▶ korzystaj zawsze z aktualnego i uznanego na rynku oprogramowania antywirusowego. Używanie darmowych programów ochronnych i antywirusowych jest lepsze niż brak ochrony ale pamiętaj, że nie chronią Cię one w tak wysokim stopniu jak oprogramowanie komercyjne.
- ▶ korzystaj z wysokiej jakości zapór internetowych typu firewall, które gwarantują kontrolę ruchu Internetowego i zabezpieczają Cię przed szkodliwym oprogramowaniem z sieci.
- ▶ korzystaj z legalnego oprogramowania. Legalne oprogramowanie upoważnia Cię do bieżących aktualizacji, które często w znaczny sposób przyczyniają się do bezpieczeństwa Twojego komputera. Aktualizacje systemu operacyjnego i jego dodatków, a także przeglądarek Internetowych czy też np. komunikatorów internetowych są wyjątkowo istotną kwestią dla Twojego bezpieczeństwa.
- ▶ pobierając oprogramowanie z Internetu staraj się by źródło było zaufane i wiarygodne. Nie instaluj programów pobranych z Internetu co do których nie masz zaufania.
- ▶ nie otwieraj załączników poczty elektronicznej od nieznanomych adresów.

# Zagrożenia



## Programy szpiegujące – Spyware

Programy szpiegujące (ang. spyware) to programy komputerowe, których celem jest szpiegowanie działań użytkownika. Programy te zazwyczaj rozpowszechniają się podobnie jak wirusy czyli drogą internetową.

Programy te gromadzą informacje o użytkowniku i wysyłają je często bez jego wiedzy i zgody autorowi programu.

Za pomocą programów szpiegujących **mogą zostać wykradzione następujące dane:**

- ▶ adresy www stron internetowych odwiedzanych przez użytkownika
- ▶ dane osobowe
- ▶ numery kart płatniczych
- ▶ hasła i loginy
- ▶ zainteresowania użytkownika (np. na podstawie wpisywanych słów w oknie wyszukiwarki)
- ▶ adresy poczty elektronicznej
- ▶ archiwum korespondencji

**Programy typu spyware mogą także wyświetlać niechciane reklamy lub rozsyłać spam.**

Sposób dostania się oprogramowania spyware na komputer klienta może być różny. Są to np. okna pop-up z informacjami o atrakcyjnej promocji czy też wygraniu nagrody, które mają skłonić użytkownika do odwiedzenia specjalnie spreparowanych stron, skąd przemycane są do komputera ofiary naprawdę groźne narzędzia spyware. Niekiedy wystarczy otwarcie spreparowanej strony, aby w tle rozpoczęło się pobieranie i instalacja niebezpiecznej aplikacji. Tego typu działanie jest szczególnie niebezpieczne, ponieważ nie wymaga od użytkownika żadnej interakcji – trudno więc bronić się przed takim atakiem. Programy spyware ukrywają także umożliwiające ich automatyczne uruchamianie wpisy w Rejestrze.

## Po czym poznać, że na komputerze zainstalowane jest oprogramowanie szpiegujskie?

Jeżeli Twój komputer nagle zaczyna dziwnie się zachowywać i da się zaobserwować któreś z poniższych symptomów to zachodzi możliwość, że masz zainstalowane oprogramowanie szpiegujskie (spyware) na swoim twardym dysku:

**Ciągle otwierają się okienka pop-up z niechcianymi reklamami.**

Niektóre rodzaje złośliwego oprogramowania mogą bombardować Twój komputer niechcianymi reklamami w okienkach pop-up, które nie mają żadnego związku ze stronami www, które akurat odwiedzasz. Bardzo często są to reklamy produktów na potencje czy też stron erotycznych. Jeżeli takie okienka pojawiają się praktycznie od razu po uruchomieniu komputera lub nawet wtedy, gdy akurat w ogóle nie surfujesz po Internecie może to oznaczać, że masz na swoim komputerze zainstalowane oprogramowanie szpiegujskie (spyware)

# Zagrożenia



**Dotychczasowe ustawienia zostały zmienione i nie ma możliwości ich przywrócenia.**

Niektóre rodzaje złośliwego kodu potrafią zmieniać ustawienia Twojej „strony domowej” (home page) lub ustawień domyślnych wyszukiwarki, z której korzystasz. Oznacza to, że strona startowa, która normalnie pojawia się, gdy uruchamiasz swoją przeglądarkę internetową, lub, gdy próbujesz uruchomić stronę wyszukiwania w Internecie zostały podmienione na zupełnie inne – takie, z których w ogóle nie miałeś zamiaru skorzystać. Nawet, jeżeli udaje Ci się wrócić do pierwotnych ustawień to i tak po ponownym restarcie Twojego komputera te podstawione strony pojawiają się ponownie.

**Przeglądarka internetowa zawiera dodatkowe komponenty, które nie były instalowane przez użytkownika.**

Oprogramowanie szpiegujskie i inne złośliwe programy potrafią dodawać dodatkowe paski narzędzi czy dodatkowe, niechciane opcje do Twojej przeglądarki. Nawet, jeżeli potrafisz je samodzielnie usunąć mogą one pojawiać się ponownie po restarcie komputera.

**Komputer zaczął działać bardzo powoli.**

Oprogramowanie szpiegujskie i inne złośliwe programy nie zostały napisane w taki sposób, aby działały efektywnie minimalnie obciążając procesor Twojego komputera. Praktycznie bez przerwy śledzą one Twoje działania i dostarczają niechciane reklamy. Dodatkowo często zawierają w sobie błędy, które mogą spowodować nawet zawieszanie się całego systemu. Jeżeli zauważysz, że Twój komputer nagle zaczął działać wolniej niż wcześniej przy wykonywaniu podobnych działań, lub nagle, praktycznie bez powodu się zawiesza, to możliwe, że masz zainstalowane na swoim dysku oprogramowanie szpiegujskie (spyware) lub inny złośliwy program.

### Wskazówki:

- ▶ świadomie wybieraj i konfiguruj swoją przeglądarkę internetową. Popularne przeglądarki Internetowe takie jak Mozilla Firefox, Opera czy Internet Explorer posiadają możliwość nałożenia specjalnych filtrów chroniących przed wyludzeniem poufnych danych
- ▶ korzystaj zawsze z aktualnego i uznanego na rynku oprogramowania antywirusowego i antyspyware. Używanie darmowych programów ochronnych i antywirusowych jest lepsze aniżeli brak ochrony ale pamiętaj, że nie chronią Cię one w tak wysokim stopniu jak oprogramowanie komercyjne.
- ▶ staraj się unikać stron o podejrzanej treści
- ▶ nie otwieraj reklam, okien pop-up, wiadomości e-mail o podejrzanej treści

# Zagrożenia



## Rootkity i keyloggery.

Działanie oprogramowania szpiegowskiego i innych zagrożeń często jest wspierane przez inne oprogramowanie, którego jedyną rolą jest ukrywanie obecności głównego zagrożenia czyli np. wirusów lub szpiegów. Profesjonalni hakerzy zatrudniani przez grupy przestępcze stosują kombinacje spyware'u i rootkitów. Rootkity to narzędzia służące do kamuflażu, które potrafią ukryć działanie wybranych programów – dzięki temu osoba przeglądająca komputer nie dostrzeże żadnego zagrożenia.

Rootkity najczęściej znajdują dla siebie miejsce w plikach systemu operacyjnego i starają się ukrywać działania innego złośliwego oprogramowania.

Innym rodzajem zagrożenia są keyloggery. Te programy, pracując w tle, rejestrują wszystkie znaki wprowadzane za pomocą klawiatury. Ponadto mogą rejestrować np. wszystkie odwiedzone witryny i uruchamiane programy, co pozwala bez problemu gromadzić wszelkie informacje o operacjach, jakie przeprowadzamy np. na naszym koncie bankowym lub chociażby w sklepach internetowych. Keylogger może otworzyć port i przetransmitować zgromadzone dane do hakera lub, posługując się innymi mechanizmami, przekazać dane za pośrednictwem emaila.

### Wskazówki:

- ▶ korzystaj zawsze z aktualnego i uznanego na rynku oprogramowania antywirusowego i antyspaware. Używanie darmowych programów ochronnych i antywirusowych jest lepsze niżeli brak ochrony ale pamiętaj, że nie chronią Cię one w tak wysokim stopniu jak oprogramowanie komercyjne.
- ▶ używaj tylko legalnego oprogramowania i pobieraj bieżące aktualizacje
- ▶ korzystaj z wysokiej jakości zapór internetowych typu firewall, które gwarantują kontrolę ruchu Internetowego i zabezpieczają Cię przed szkodliwym oprogramowaniem z sieci.

## Poczta elektroniczna i spam.

Poczta elektroniczna jest jedną z najchętniej i najpowszechniej wykorzystywanych możliwości jakie niesie ze sobą Internet. Daje ona bardzo szerokie możliwości kontaktu i komunikacji bez względu na zasięg i miejsce w którym przebywa odbiorca. Poczta elektroniczna jest wykorzystywana w stopniu masowym, także przez dzieci i młodzież korzystającą z Internetu.

Niestety podobnie jak Internet niesie ona ze sobą także wiele zagrożeń. Między innymi jest ona popularnym nośnikiem wirusów i innych zagrożeń, takich jak np. spam.

# Zagrożenia



## Spam – czyli niechciane wiadomości.

Popularnie nazywany spam jest w większości przypadków niczym innym jak niechcianą i nie zamawianą przez użytkownika korespondencją wysłaną masowo. Nierzadko też taka korespondencja zawiera elementy złośliwego kodu lub wręcz wirusy komputerowe. W tym wypadku poczta elektroniczna jest wykorzystywana jako nośnik do rozprzestrzeniania się różnego rodzaju zagrożeń.

## Szkodliwość spamu.

Spam jest szkodliwy z wielu przyczyn, poniżej znajdziesz kilka z nich:

- ▶ spam jest często nosicielem wirusów, szpiegów i innego złośliwego oprogramowania
- ▶ może spowodować zatykanie się łącza i zajmowanie przestrzeni na koncie pocztowym
- ▶ może powodować wolniejsze działanie serwerów pocztowych
- ▶ często narusza prywatność użytkowników, gdyż zawiera treści, których nie życzą sobie oni oglądać (pornograficzne, obraźliwe, nie odpowiednie dla dzieci)

### Wskazówki:

- ▶ nie otwieraj wiadomości, które budzą Twoje podejrzania, najlepiej od razu je usuwaj.
- ▶ korzystaj z aktualnego i uznanego na rynku oprogramowania Antyspam, które pozwoli Ci zapomnieć o spamie.
- ▶ wszelkie wiadomości e-mail od nieznanych nadawców czy też w obcym języku są potencjalnie niebezpieczne. Zwracaj na nie szczególną uwagę.
- ▶ nigdy nie klikaj w linki ani nie otwieraj załączników w podejrzanych wiadomościach e-mail. To one najczęściej są źródłem rozprzestrzeniania się wirusów drogą e-mail.
- ▶ nie daj się łatwo nabrać na to, że wygrałeś jakąś sumę pieniędzy czy wycieczkę do dalekiego kraju. To najprostszy sposób aby wyłudzić od Ciebie Twoje prywatne dane, takie jak: numer karty kredytowej, numer dowodu osobistego, PESEL czy też numer konta bankowego. Zawsze staraj się sprawdzić dostawcę takich wiadomości lub jeśli nie jesteś pewien dostawcy, nie podejmuj żadnych działań usuwając tą korespondencję do kosza.

# Dziecko w sieci



## Jak uchronić dziecko przed zagrożeniami płynącymi z sieci?

Internet może być dla dzieci doskonałym miejscem do nauki, rozrywki, rozmów z przyjaciółmi ze szkoły oraz odpoczynku i rozwijania zainteresowań. Jednak podobnie jak w realnym świecie, również w Internecie na dzieci mogą czyhać różne zagrożenia.

Dzieci są grupą wyjątkowo podatną na ataki cyberprzestępców. Ze względu na swój młody wiek i częsty brak różnicowania treści odpowiednich od nieodpowiednich są wyjątkowo narażone na rozmaite ataki za pomocą sieci Internet.

Zagrożenia czyhające na dzieci w Internecie to m.in.:

- ▶ strony z nieodpowiednią treścią, na które może trafić Twoje dziecko przeglądając zasoby sieci Internet.
- ▶ wyłudzenia informacji od dzieci i młodzieży dotyczące ich danych lub danych ich rodziców przez aplikacje szpiegujące lub osoby kontaktujące się z dzieckiem przez sieć Internet i działające w złej wierze.
- ▶ podszywanie się osób o złych zamiarach pod rówieśników, kolegów lub koleżanki Twojego dziecka. Ten typ zagrożeń jest wyjątkowo groźny gdyż takiego działania dokonują osoby planujące konkretne niebezpieczne działania w stosunku do Twojego dziecka.

Zanim pozwolisz dziecku korzystać z Internetu bez nadzoru, uzgodnij z nim zasady, którymi powinno się kierować.

Jeśli nie wiesz, od czego zacząć, skorzystaj z poniższych wskazówek w zakresie zagadnień, które należy omówić z dzieckiem, aby korzystało z Internetu bezpiecznie.

### Wskazówki:

- ▶ Zachęcaj dzieci do opowiadania o swoich doświadczeniach związanych z korzystaniem z Internetu. Korzystaj z Internetu razem z dziećmi. Usiądź przy dziecku wtedy gdy korzysta ono z komputera – to także świetna okazja do rozmowy.
- ▶ Naucz dzieci ufać ich intuicji. Jeśli znajdują w Internecie coś, co wywołuje ich niepokój, powinny Ci o tym powiedzieć. Nie lekceważ żadnych informacji, które otrzymujesz od dziecka.
- ▶ Jeśli dzieci odwiedzają pokoje rozmów, korzystają z komunikatorów internetowych takich jak GaduGadu, Tlen czy Skype, gier internetowych lub wykonują w Internecie inne czynności wymagające zalogowania się w celu identyfikacji użytkownika, pomóż im wybrać odpowiednią nazwę i dopilnuj, aby nie zdradzała ona żadnych informacji osobistych o dziecku.

# Dziecko w sieci



- ▶ Przy korzystaniu z komunikatorów Internetowych uczul też dziecko aby nie korespondowało ono z osobami nieznanymi, które nie są obecne na jej liście kontaktów.
- ▶ Wyraźnie podkreśl, że dzieciom nigdy nie wolno podawać adresu, numeru telefonu ani innych informacji osobistych, takich jak nazwa szkoły czy miejsce zabaw.
- ▶ Naucz dzieci, że różnica między dobrem a złem jest taka sama w Internecie, jak w prawdziwym świecie.
- ▶ Pokaż dzieciom, jak okazywać szacunek innym internautom. Dopilnuj, aby dzieci przestrzegały zasad dobrego wychowania korzystając z komputera.
- ▶ Wymagaj, aby dzieci przestrzegały praw własności innych internautów. Wyjaśnij, że nielegalne kopiowanie efektów pracy innych ludzi — muzyki, filmów, gier wideo i innych programów — to kradzież.
- ▶ Powiedz dzieciom, że nie należy spotykać się z osobami poznanymi w Internecie. Wyjaśnij, że internetowi przyjaciele nie zawsze są tymi, za których się podają.
- ▶ Naucz dzieci, że nie wszystko, co przeczytają lub zobaczą w Internecie, jest prawdą. Zachęcaj je do zadawania pytań, jeśli nie są czegoś pewne.
- ▶ Korzystaj z nowoczesnego oprogramowania do kontrolowania aktywności dziecka w Internecie. Funkcja kontroli rodzicielskiej pozwala zablokować dostęp do nieodpowiednich witryn, monitorować odwiedzane przez dzieci witryny i sprawdzać, co dzieci tam robią a nawet ograniczać czas spędzony przez dziecko w Internecie.

# Pomoc w przypadku problemów



## Reaguj na zagrożenie!

Jeżeli stałeś się ofiarą ataku cyberprzestępcy **poinformuj o tym odpowiednie służby**.

Pierwszą instancją pomocy jest Twój operator telekomunikacyjny lub dostawca usług antywirusowych lub też bank, jeżeli zagrożenie dotyczy Twoich finansów i płatności online.

**Jeżeli zagrożenie jest poważne** zawsze należy powiadomić o tym Policję oraz odpowiednie organizacje zajmujące się wsparciem użytkowników Internetu w sytuacjach zagrożenia. Często szkodliwe oprogramowanie i działania cyberprzestępców łamie Twoje podstawowe prawa – możesz wtedy zgłosić się do Rzecznika Praw Obywatelskich. Więcej informacji znajdziesz pod adresem: [www.rpo.gov.pl/index.php?s=1](http://www.rpo.gov.pl/index.php?s=1)

Jeżeli uważasz, że Twoje dziecko jest zagrożone, możesz zwrócić się do Fundacji Kidprotect.pl ([www.kidprotect.pl](http://www.kidprotect.pl)), która od 2002 roku prowadzi hotline „StopPedofilom!” ([www.StopPedofilom.pl](http://www.StopPedofilom.pl)). Hotline umożliwia internautom anonimowe zgłaszanie wszelkich incydentów związanych z pornografią dziecięcą i nagabywaniem seksualnym dzieci, tak on-line jak i poza siecią. Hotline współpracuje z polską policją, w razie potrzeby przekazuje informacje do organizacji w innych krajach. Adres kontaktowy do Fundacji to: [fundacja@kidprotect.pl](mailto:fundacja@kidprotect.pl).

Jeżeli w czasie surfowania po Internecie, odnajdziesz treści niezgodne z prawem lub szkodliwe dla użytkowników, możesz to zgłosić pod adresem: [www.dyzurnet.pl/](http://www.dyzurnet.pl/)

**Jeżeli zagrożone jest Twoje dziecko** możesz zgłosić się do Helpline. Helpline jest projektem polegającym na świadczeniu pomocy w sytuacjach zagrożenia dzieci i młodzieży w Internecie: [helpline.org.pl/](http://helpline.org.pl/)

**Jeżeli jesteś klientem Netii** to specjalnie dla Ciebie uruchomiliśmy dedykowaną skrzynkę poczty elektronicznej pod adresem: [helpdesk@netia.pl](mailto:helpdesk@netia.pl)

Pod tym adresem możesz zasięgnąć większej ilości informacji i uzyskać wsparcie w sprawach związanych z Twoim bezpieczeństwem w Internecie.