



Bezpieczeństwo w Internecie

Chroń swój to samo ,
dane osobowe i rodzin .

bezpieczeństwo • łatwa obsługa • przejdź dosecure.org

Słowo wstępne od Ministra Komunikacji, Energii i Zasobów Naturalnych

Z wielką przyjemnością ci przedstawiam Państwu naszą trzecią ogólnokrajową kampanię na rzecz wiadomości o bezpieczeństwie komputerowego: **makeITsecure** 2008.



Ponieważ obecna kampania będzie po raz pierwszy prowadzona w całej Irlandii, chcę serdecznie podziękować deputowanemu Peterowi Robinsonowi. Dzięki jego zaangażowaniu tegoroczna kampania obejmie również Irlandię Północną.

Dziękuję naszym sponsorom za ich udział w naszej ogólnokrajowej kampanii. Chcę też serdecznie powitać nowych partnerów: firmy 3 i O₂.

Celem kampanii jest zapewnienie skutecznego i bezpiecznego korzystania z komputerów i szerokopasmowego dostępu do Internetu dzięki podaniu podstawowych informacji o zagrożeniach, które dotyczą wszystkich użytkowników.

W celu uzyskania dodatkowych informacji zapraszamy Cię do serwisu www.makeITsecure.org.

Powitanie od Petera Robinsona, deputowanego Parlamentu i Zgromadzenia Ustawodawczego, Ministra ds. Finansów i Personelu

Niezmiernie się cieszę, że Department of Finance and Personnel (DFP) może wspierać tak niezwykle i ważny program, jak **makeITsecure**.

Pomimo niezaprzeczalnej przydatności nowych technologii i usług internetowych wszyscy powinni mieć wiadomość istniejących zagrożeń. Ciągła popularyzacja tej wiedzy jest niezwykle istotna, dlatego właśnie zorganizowano tę kampanię.

W obliczu prowadzonej przez DFP polityki poszerzania dostępu do elektronicznej, w pełni ceniąc i wspierając popularność szerokopasmowego dostępu do Internetu w Irlandii Północnej, mamy obowiązek nie tylko przypominać obywatelom o korzyściach związanych z Internetem. Musimy również ostrzegać, oraz informować o prostych i skutecznych metodach zapewnienia bezpieczeństwa.

Dzięki tej kampanii wszyscy będziemy wiedzieli nie tylko, jak cieszyć się korzyściami techniki komputerowej i dostępu do Internetu, lecz także, jak zapewnić przy tym bezpieczeństwo sobie i naszym bliskim.

Rozważaj i w pełni wykorzystuj możliwości Internetu

Internet stał się nieodłączną częścią życia, jest niezbędny w pracy i w domu.

Internet nie tylko ułatwia zakupy i korzystanie z usług bankowych, ale również umożliwia wszystkim czerpanie z bogatych zasobów informacji. Ogólnie wiadomo, że to również ogromna społeczność użytkowników, którzy codziennie kontaktują się i udostępniają sobie nawzajem pewne dane.

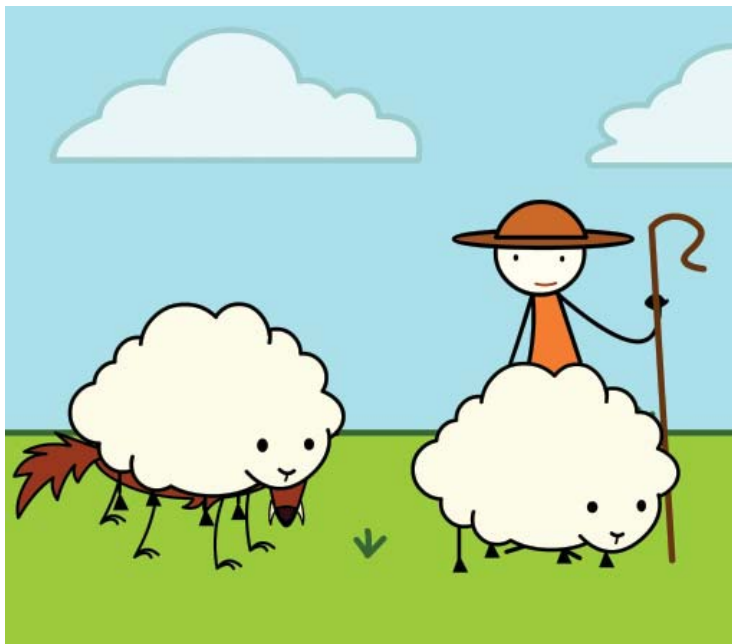
Choć przeglądanie stron internetowych i transakcje elektroniczne są niewątpliwie wygodne i ciekawe, trzeba mieć świadomość potencjalnych zagrożeń.

Należy zadbać o zabezpieczenie komputera i zachować ostrożność podczas udostępniania swoich danych osobowych w Internecie.

Niniejsza broszura oraz witryna **makeITsecure** powstały, aby pomóc użytkownikom i ich rodzinom bezpiecznie korzystać z Internetu.

Broszura opisuje typowe zagrożenia związane z przeglądaniem stron internetowych i transakcjami w Internecie. Wskazuje też, jak unikać zagrożeń, by wszyscy mogli z satysfakcją i bezpiecznie z niego korzystać.

bezpieczeństwo • łatwa obsługa • [makeITsecure.org](http://www.makeITsecure.org)



Phishing

Czym jest phishing?

Phishing, czyli wyludzanie danych, polega na tym, że oszuści internetowi (phisherzy) podszycia się pod prawdziwe instytucje (takie jak banki i operatorzy kart kredytowych), aby wyludzić od użytkowników poufne informacje, na przykład numery kont bankowych lub numery PIN.

Działanie takich oszustów najczęściej polega na wysłaniu wiadomości e-mail, w których proszą o „weryfikację” lub „ponowne przekazanie” poufnych danych.

Zdarza się też, że proszą o wypełnienie formularza na stronie internetowej, w zamian oferując atrakcyjne nagrody, na przykład pieniądze lub wakacje.

Trzeba być nieufnym wobec każdego, kto prosi o przekazanie danych bankowych, numerów kart kredytowych, haseł, numerów PIN, numeru PPS lub numeru ubezpieczenia społecznego.

Oszuści mogą wykorzystać uzyskane w ten sposób informacje, podszycia się pod daną osobę w celu wypłacenia pieniędzy z jej konta lub dokonania zakupów w Internecie. Twoje cenne dane mogą po prostu zostać sprzedane innym.

Phisher to przestępca, który podszycia się pod istniejącą firmę lub instytucję w celu wyludzenia od użytkowników poufnych danych.

Jak poznać prób phishingu?

Zaufaj intuicji. Jeśli e-mail wywołuje podejrzenie, od razu go usuń. Jeśli przesłana oferta wydaje się zbyt atrakcyjna, to najprawdopodobniej nie jest. Jeśli wiadomość wygląda, jak wysłana z Twojego banku lub przez operatora kart kredytowych, natychmiast skontaktuj się z działem obsługi klienta odpowiedniej instytucji.

Oto typowe sformułowania spotykane w wiadomościach phishingowych:

„Zweryfikuj swoje konto”

„Odpowiedz w ciągu 48 godzin, by zapobiec zablokowaniu konta”

„Szanowny Panie/Ki Panie”

„Kliknij poniżej, by zalogować się do swojego konta”

Jak możesz się zabezpieczyć przed phishingiem?

Zaufaj intuicji. Pamiętaj, że żadna szanująca się firma nigdy nie poprosi klientów o przesyłanie poufnych danych pocztą e-mail.

Nigdy nie podawaj swoich danych osobowych w wiadomości e-mail, faksem ani w formularzach otwartych z reklamy wyskakującej lub nieoczekiwanej wyświetlonej witryny.

Zawsze sprawdzaj, czy wyciągi z kart kredytowych i rachunku bankowego nie zawierają nieprawidłowości.

Korzystaj z aktualnego oprogramowania antywirusowego i antyśpiegowskiego, by zabezpieczyć się przed niepożądanym i niebezpiecznym oprogramowaniem. Przeglądarka z filtrem phishingowym umożliwi wykrycie znanych fałszywych witryn i ochroni przed oszustwami internetowymi poprzez zablokowanie takich stron lub wyświetlenie ostrzeżenia.

Co robić, jeśli Ci się wydaje, że jesteś ofiarą phishingu?

Jeśli podejrzewasz, że jesteś ofiarą oszustwa phishingowego, powiadom o tym firmę, pod którą podszycia się oszust, korzystając z innego rodzaju łączności, na przykład innego komputera lub telefonu stacjonarnego lub komórkowego. Następnie skontaktuj się z najbliższym posterunkiem policji (Garda), a w Irlandii Północnej zadzwoń pod numer informacyjny służby policyjnej PSNI: 0845 600 8000.

Więcej informacji: www.makeITsecure.org/phishing

Reklamy wyskakujące to reklamy internetowe, które „wyskakują” w nowym oknie przeglądarki.

Serwisy społeczno ciowe

Czym s serwisy społeczno ciowe?

Serwisy społeczno ciowe słu tworzeniu i rozwijaniu internetowych społeczno ci znajomych.

Bebo to popularny w Irlandii serwis społeczno ciowy dla u ytkowników w wieku 13-24 lat. Trzeba mie co najmniej 13 lat, by zało y w nim konto.

Facebook to serwis społeczno ciowy popularny przede wszystkim w ród u ytkowników powy ej 25 roku ycia, cho minimalny wiek wymagany do rejestracji to 13 lat.

Nimble to irlandzki serwis społeczno ciowy.

Blog to inaczej dziennik internetowy (od „web log”). Blog mo e by pami tnikiem, miejscem debaty politycznej, ródlem najnowszych wiadomo ci lub zbiorem polecanych t czy. Najogólniej ujmuj c, blog to witryna internetowa, w której regularnie publikowane s nowe informacje.

Serwisy Bebo, Facebook, Nimble i inne przyci gaj ty si ce internautów ze wszystkich grup wiekowych, umo liwiaj c u ytkownikom internetowy kontakt ze znajomymi, a cz sto równie z osobami dot d nieznanymi. W zale no ci od charakteru danego serwisu u ytkownicy mog si dzieli ró norodnymi zainteresowaniami, a za po rednictwem funkcji serwisu rozmawia y, wysyła wiadomo ci tekstowe i e-maile, wysyła i pobiera zdj cia i filmy, tworzy i czyta blogi oraz omawia i publikowa informacje.

Na czym to polega?

Tworz c profil w serwisie społeczno ciowym, najcz ciej trzeba poda pewne podstawowe informacje o sobie, na przykład wybra swoj nazw u ytkownika, poda kraj lub miasto pochodzenia i okre li swoje gusty muzyczne czy inne zainteresowania. Nast pnie mo na zdecydowa y, czy profil ma by prywatny czy publiczny. Je li ustawisz swoj profil jako „prywatny”, Twoje informacje powinny by widoczne wył cznie dla u ytkowników, których dodasz do swojej listy znajomych.

Na czym polegaj zagro enia?

Funkcjonowanie serwisów społeczno ciowych wi e si z publikowaniem pewnej ilo ci danych o u ytkownika. Istnieje zagro enie, e decyduj c o informacjach udost pnianych na swój temat, u ytkownicy nie zawsze b d zachowywa tak sam ostro no y, jak podczas kontaktów osobistych. Na przykład nie nale y publikowa swojego adresu domowego ani numeru telefonu, a profil powinien by zawsze ustawiony jako „prywatny”, by zawsze było wiadomo, z kim si kontaktujesz.

Jak si zabezpieczy ?

Uwa aj, ile informacji personalnych udost pniasz w Internecie. Pami taj, e jest to zasób dost pny dla wszystkich. Publikuj wył cznie takie informacje, które mo na bezpiecznie pokaza ka demu i chro si przed kradzie to samo ci, ograniczaj c ilo danych udost pnionych w Internecie.

Jak mog chroni swoje dziecko?

Korzystanie z serwis ów społeczno ciowy ch mo e by dobr y, kształc c zabaw y, pod warunkiem e dziecko b dzie uwa a na to, jakie informacje o sobie ujawnia w Internecie.

Naucz dziecko, by nie wierzyło wszystkiemu, co wyczyta y, e ludzie podaj fałszyw to samo y.

Przypominaj dziecku, by nigdy nie spotykało si z osobami znanymi wył cznie z Internetu, je li nie b dzie przy tym obecna zaufana osoba dorosła.

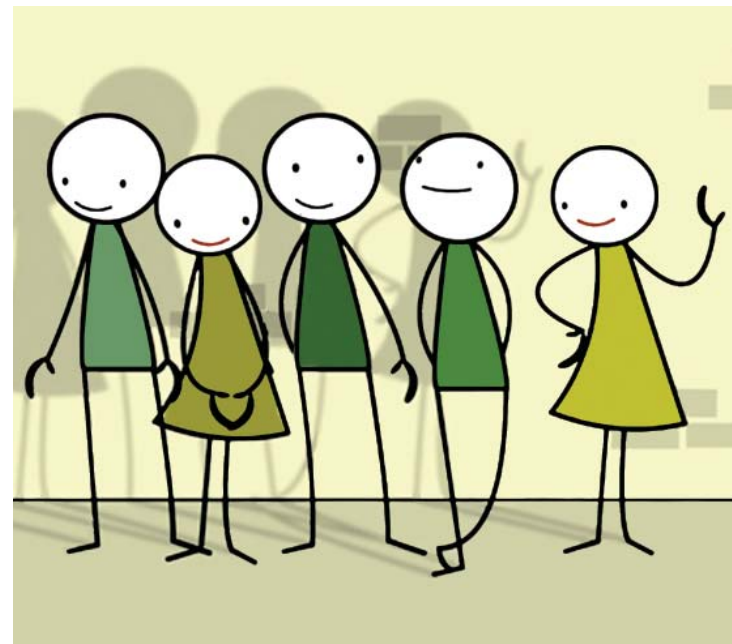
Samo ostrze enie przed spotykaniem si z nieznanymi mo e nie wystarczy y, gdy dziecko mo e nie uwa a osoby znanej z internetowych rozmów za nieznanego.

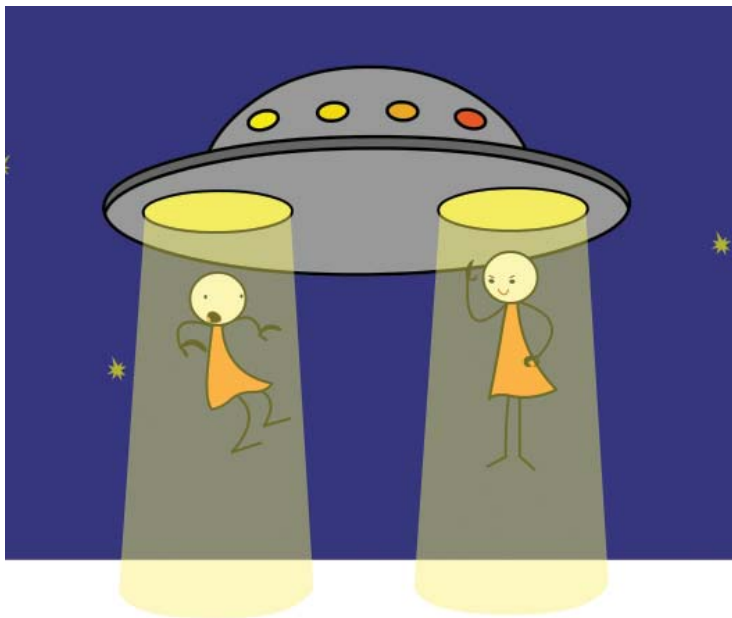
Zapoznaj si z programami i serwisami, z których korzysta Twoje dziecko, aby móc z nim swobodnie rozmawia o Internecie. Pami taj, e strony internetowe s obecnie dost pne nie tylko w domu, ale i z telefonów komórkowych.

Dowiedz si y, jakie witryny odwiedza Twoje dziecko i czy s one dla niego odpowiednie.

Wi kszo współczesnych przegl darek internetowych ma funkcje kontroli rodzicielskiej, które ograniczaj zakres tre ci internetowych dost pnych dla Twojego dziecka. Warto zapozna si z tymi zabezpieczeniami i odpowiednio je stosowa y.

Wi cej informacji mo na znale pod adresem www.makeITsecure.org/socialnetworking





Kradzie to samo ci

Czym jest kradzie to samo ci?

Kradzie to samo ci ma miejsce wtedy, gdy przestępca podszywa się pod daną osobę, wykorzystując jej skradzione dane do pobrania pieniędzy z jej konta lub zapłaceniu za zakupy internetowe. Może to dodatkowo zarobić, sprzedając te dane innym.

Jak ją rozpoznać?

Niestety, rozpoznanie kradzie to samo ci najczęściej oznacza, że już jesteś jej ofiarą. Oto typowe objawy:

- Odrzucone wnioski o kredyt lub pożyczkę.
- Firmy windykacyjne zgłaszające się w celu egzekucji długów, których dana osoba nie zaciągała.
- Otrzymanie informacji na temat rzekomo wynajmowanego mieszkania, podjętej pracy lub kupionego domu.

Co robić, jeśli padniesz ofiarą kradzie to samo ci?

Natychmiast zadzwoń na policję (An Garda Síochána lub PSNI) i zgłoś przypadek kradzie to samo ci.

Powiadom telefonicznie i pisemnie odpowiedni bank lub inne instytucje finansowe, u których masz rachunki lub z którymi się kontaktujesz.

Powiadom pisemnie instytucję lub serwis internetowy, gdzie nastąpiła kradzie to samo ci.

Anuluj wszelkie karty i zamknij wszelkie konta, co do których masz dowody lub podejrzenia nieuprawnionego dostępu.

Jak możesz się zabezpieczyć przed kradzie to samo ci?

Zachowaj ostrożność podczas podawania danych osobowych przez Internet.

Jeśli robisz zakupy w Internecie, upewnij się, że połączenie jest zabezpieczone. Na pasku stanu przeglądarki powinna być włączona ikona kłódki, a adres strony powinien się zaczynać od znaków `https://`, a nie `http://`.

Sprawdź dostępną i treść publikowanej przez firmy polityki poufności i bezpieczeństwa.

Korzystaj z silnego hasła i nikomu go nie udostępniaj. Idealne hasło to losowa kombinacja cyfr, liter i znaków interpunkcyjnych o długości co najmniej 8 znaków.

Załóż osobne konto e-mail do zakupów i grup dyskusyjnych. Jeśli trzeba, będzie zmienił ten adres, będzie to mniej kłopotliwe niż zmiana głównego adresu używanego do korespondencji.

Więcej informacji: www.makeITsecure.org/identitytheft



`http://` i `https://` to ciąg znaków umieszczony na początku adresu internetowego. Jeśli podajesz dane swojej karty kredytowej przez Internet, upewnij się, że witryna jest bezpieczna, czyli jej adres zaczyna się od `https://`.

Zabezpieczenie dostępu do Internetu

Choć korzystanie z Internetu nigdy nie jest całkowicie bezpieczne, wystarczy kilka prostych kroków, by zabezpieczyć swój komputer lub inne używane urządzenia i znacznie ograniczyć ryzyko utraty danych.

Zawsze korzystaj z aktualnego oprogramowania antywirusowego i antyszpiegowskiego

Wirusy komputerowe to małe programy, które dołączają się do innych aplikacji, na przykład edytorów tekstu czy programów pocztowych. Mogą one wyrządzić wiele szkód poprzez zniszczenie, skopiowanie lub kradzież danych. Mogą się też replikować i zarażać komputery innych użytkowników.

Spyware to oprogramowanie szpiegujące, które bez Twojej wiedzy zbiera i wysyła przez Internet informacje na Twój temat.

Program antywirusowy to oprogramowanie instalowane na komputerze, które szuka wirusów we wszystkich plikach i programach, a w razie ich wykrycia usuwa infekcję.

Systemy operacyjne to oprogramowanie, na bazie którego działają wszystkie inne programy. Przykładowe systemy operacyjne to Microsoft® Windows, Linux i Mac OS.

Oprogramowanie szpiegujące („spyware”) to ogólne określenie małych programów, które są pobierane do systemu bez wiedzy użytkownika. Mogą one zbierać informacje personalne i przesyłać je przez Internet swojemu twórcy.

Wirusy i programy szpiegujące są ogólnie nazywane oprogramowaniem złośliwym lub niebezpiecznym („malware”).

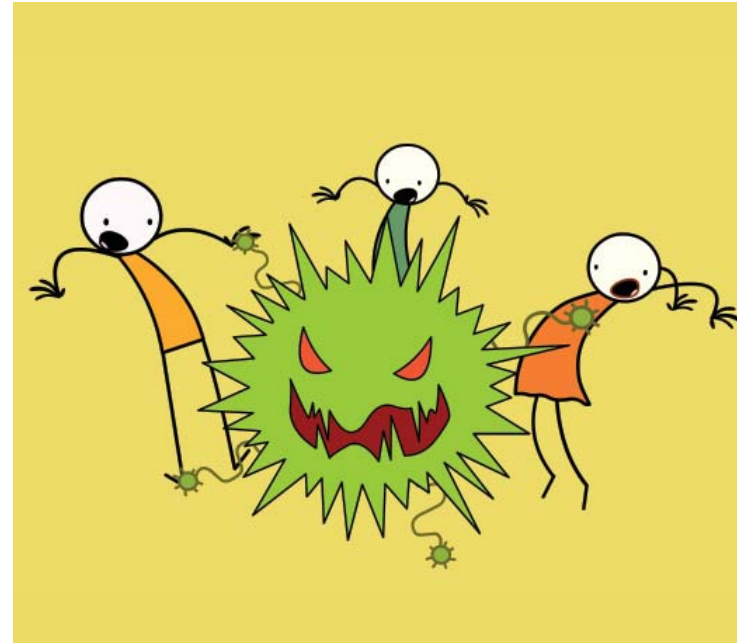
Oprogramowanie antywirusowe i antyszpiegowskie wykrywa niebezpieczne programy i usuwa je z systemu. Ponieważ wirusy i programy szpiegujące ulegają ciągłym zmianom, trzeba zawsze dbać o bieżące aktualizowanie oprogramowania antywirusowego i antyszpiegowskiego. Wszystkie aplikacje zabezpieczaj tego typu umożliwiają automatyczną aktualizację przez Internet.

Zawsze instaluj aktualizacje zaufanych aplikacji

Na każdym komputerze lub podobnym urządzeniu zainstalowanych jest wiele programów, w tym najważniejszy program: system operacyjny. Stanowi on platformę, na której działają inne aplikacje, takie jak edytory tekstu, gry i przeglądarki internetowe.

Ponieważ oprogramowanie złośliwe wciąż ewoluuje, stwarzając coraz to nowe zagrożenia, twórcy aplikacji nieustannie opracowują aktualizacje zabezpieczeń, by zapobiegać infekcjom.

Dlatego należy zawsze instalować wszystkie aktualizacje zabezpieczeń udostępniane przez producentów posiadanego oprogramowania, by mieć pewność, że system jest w pełni aktualny.



Zawsze korzystaj z zapory (firewall)

Firewall (inaczej zaporę sieciową) pełni funkcję sieciowego odwiernika. Na bieżąco filtruje dane przesyłane między Internetem a Twoim komputerem i zezwala na przyjęcie lub wysłanie tylko tych danych, które zostały przez Ciebie dopuszczone. W przypadku współczesnych systemów operacyjnych i pakietów zabezpieczeń zawiera oprogramowanie zapory. Gdy korzystasz z Internetu, zawsze upewnij się, że jest ono włączone.

Zapora (firewall) to urządzenie lub program, którego zadaniem jest blokowanie nieautoryzowanego dostępu do Twojego komputera podczas połączenia z Internetem.

