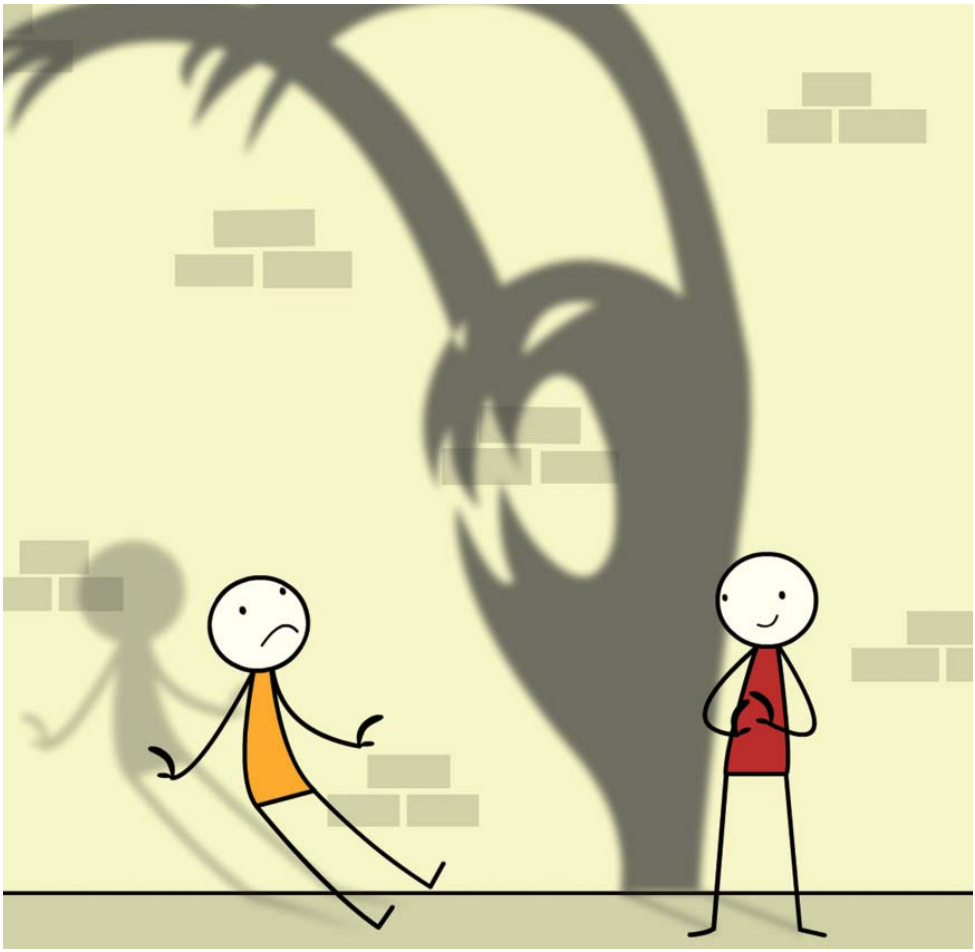
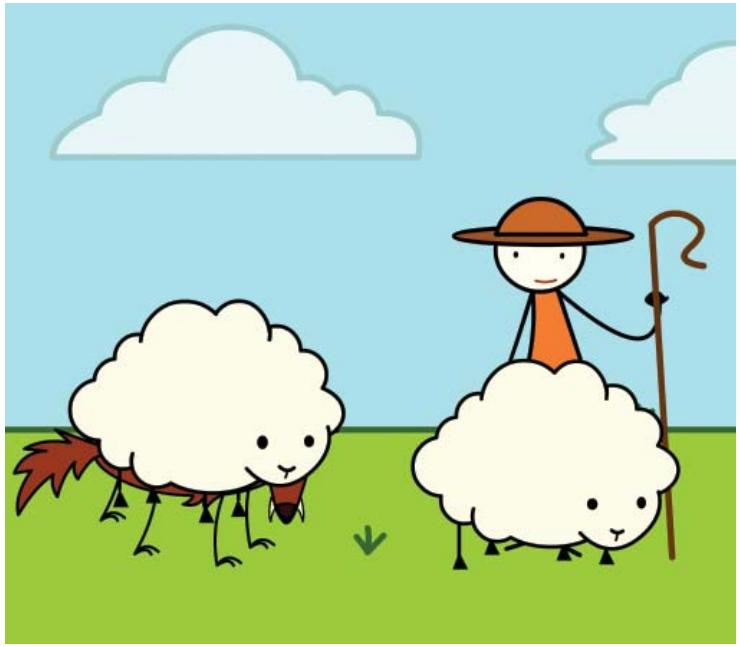


Bezpieczeństwo w Internecie

Chroń swoją tożsamość, dane osobowe i rodzinę.

bezpieczeństwo • łatwa obsługa • przejdź dosecure.org



Phishing

Czym jest phishing?

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

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

Działanie takich oszustów najczęściej polega na wysyłaniu 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 atrakcyjną nagrodę, 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, podszywając się pod daną osobę w celu wypłacenia pieniędzy z jej konta lub dokonania zakupów w Internecie. Twoje cenne dane mogą też po prostu zostać sprzedane innym.

Jak poznać próbę phishingu?

Zaufaj intuicji. Jeśli e-mail wygląda podejrzanie, od razu go usuń. Jeśli przesłana oferta wydaje się zbyt atrakcyjna, to najczęściej tak właśnie 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 ceniony Kliencie”

„Kliknij poniższe łącze, by zalogować się do swojego konta”

Jak mogę 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 nieoczekiwanie wyświetlonej witryny.

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

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

Korzystaj z aktualnego oprogramowania antywirusowego i antyszpiegowskiego, by zabezpieczyć się przed niepożądanym i niebezpiecznym oprogramowaniem. Przeglądarka z filtrem phishingowym umożliwi wykrycie znanych fałszywych witryn i uchroni 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 podszywał się oszust, korzystając z innego środka łączności, na przykład innego komputera bądź 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

Serwisy społecznościowe

Czym są serwisy społecznościowe?

Serwisy społecznościowe służą tworzeniu i rozwijaniu internetowych społeczności znajomych.

Serwisy Bebo, Facebook, Nimble i inne przyciągają tysiące internautów ze wszystkich grup wiekowych, umożliwiając użytkownikom internetowy kontakt ze znajomymi, a często również z osobami dotąd nieznanymi. W zależności od charakteru danego serwisu użytkownicy mogą się dzielić różnorodnymi zainteresowaniami, a za pośrednictwem funkcji serwisu rozmawiać, wysyłać wiadomości tekstowe i e-maile, wysyłać i pobierać zdjęcia i filmy, tworzyć i czytać blogi oraz omawiać i publikować informacje.

Bebo to popularny w Irlandii serwis społecznościowy dla użytkowników w wieku 13-24 lat. Trzeba mieć co najmniej 13 lat, by założyć w nim konto.

Facebook to serwis społecznościowy popularny przede wszystkim wśród użytkowników powyżej 25 roku życia, choć minimalny wiek wymagany do rejestracji to 13 lat.

Nimble to irlandzki serwis społecznościowy.

Blog to inaczej dziennik internetowy (od „web log"). Blog może być pamiętnikiem, miejscem debaty politycznej, źródłem najnowszych wiadomości lub zbiorem polecanych łączy. Najogólniej ujmując, blog to witryna internetowa, w której regularnie publikowane są nowe informacje.

Na czym to polega?

Tworząc profil w serwisie społecznościowym, najczęściej trzeba podać pewne podstawowe informacje o sobie, na przykład wybrać swoją nazwę użytkownika, podać kraj lub miasto pochodzenia i określić swoje gusty muzyczne czy inne zainteresowania. Następnie można zdecydować, czy profil ma być prywatny czy publiczny. Jeśli ustawisz swój profil jako „prywatny", Twoje informacje powinny być widoczne wyłącznie dla użytkowników, których dodasz do swojej listy znajomych.

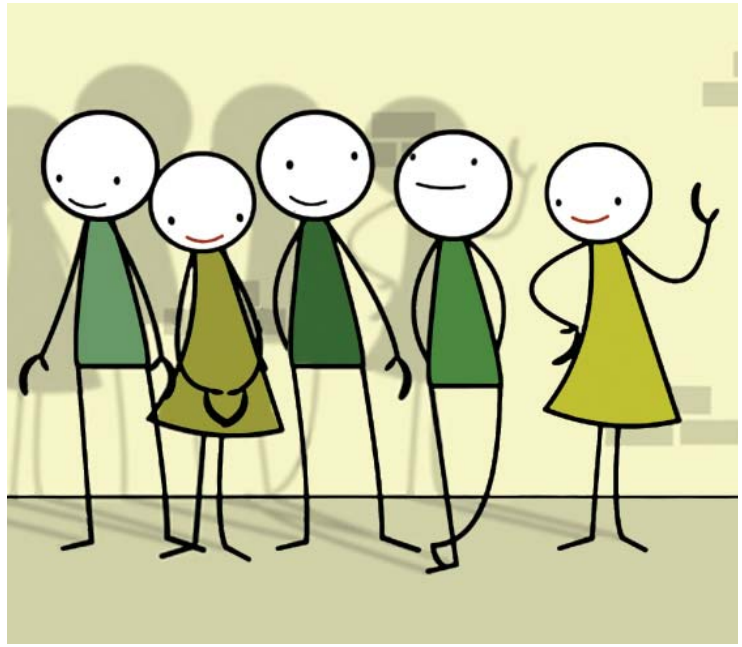
Na czym polegają zagrożenia?

Funkcjonowanie serwisów społecznościowych wiąże się z publikowaniem pewnej ilości danych o użytkowniku. Istnieje zagrożenie, że decydując o informacjach udostępnianych na swój temat, użytkownicy nie zawsze będą zachowywać taką samą ostrożność, jak podczas kontaktów osobistych. Na przykład nie należy publikować swojego adresu domowego ani numeru telefonu, a profil powinien być zawsze ustawiony jako „prywatny", by zawsze było wiadomo, z kim się kontaktujesz.

Jak się zabezpieczyć?

Uważaj, ile informacji personalnych udostępniasz w Internecie. Pamiętaj, że jest to zasób dostępny dla wszystkich. Publikuj wyłącznie takie informacje, które można bezpiecznie pokazać każdemu i chroń się przed kradzieżą tożsamości, ograniczając ilość danych udostępnionych w Internecie.

Jak mogę chronić swoje dziecko?



Korzystanie z serwisów społecznościowych może być dobrą, kształcącą zabawą, pod warunkiem że dziecko będzie uważać na to, jakie informacje o sobie ujawnia w Internecie.

Naucz dziecko, by nie wierzyło wszystkiemu, co wyczyta, gdyż zdarza się, że ludzie podają fałszywą tożsamość.

Przypominaj dziecku, by nigdy nie spotykało się z osobami znanymi wyłącznie z Internetu, jeśli nie będzie przy tym obecna zaufana osoba dorosła.

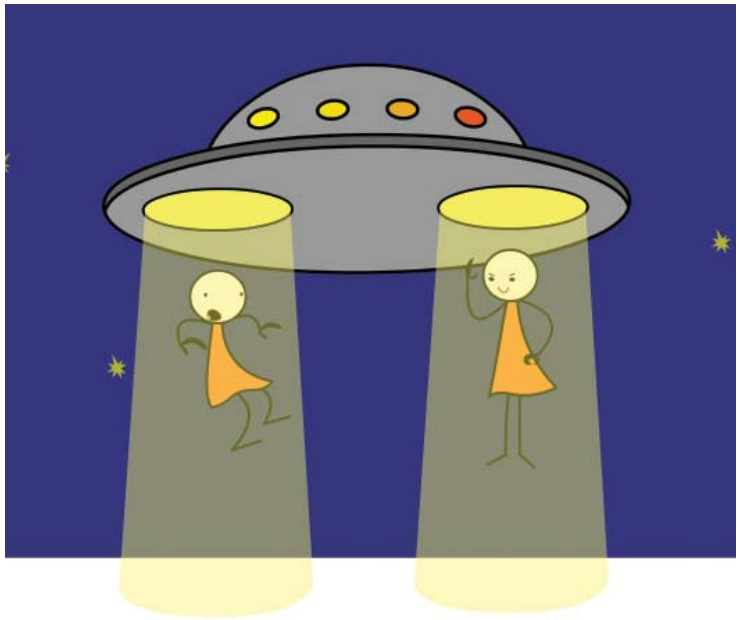
Samo ostrzeżenie przed spotykaniem się z nieznajomymi może nie wystarczyć, gdyż dziecko może nie uważać osoby znanej z internetowych rozmów za nieznajomego.

Zapoznaj się z programami i serwisami, z których korzysta Twoje dziecko, aby móc z nim swobodnie rozmawiać o Internecie. Pamiętaj, że strony internetowe są obecnie dostępne nie tylko w domu, ale i z telefonów komórkowych.

Dowiedz się, jakie witryny odwiedza Twoje dziecko i czy są one dla niego odpowiednie.

Większość współczesnych przeglądarek internetowych ma funkcje kontroli rodzicielskiej, które ograniczają zakres treści internetowych dostępnych dla Twojego dziecka. Warto zapoznać się z tymi zabezpieczeniami i odpowiednio je stosować.

Więcej informacji można znaleźć pod adresem www.makeITsecure.org/socialnetworking



Kradzież tożsamości

Czym jest kradzież tożsamości?

Kradzież tożsamości ma miejsce wtedy, gdy przestępca podszywa się pod daną osobę, wykorzystując jej skradzione dane do pobrania pieniędzy z jej konta lub zapłacenia za zakupy internetowe. Może też dodatkowo zarobić, sprzedając te dane innym.

Jak ją rozpoznać?

Niestety, rozpoznanie kradzieży tożsamości 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 wynajętego mieszkania, podjętej pracy lub kupionego domu.

Co robić, jeśli padnę ofiarą kradzieży tożsamości?

Natychmiast zadzwoń na policję (An Garda Síochána lub PSNI) i zgłoś przypadek kradzieży tożsamości.

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 kradzież tożsamości.

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

Jak mogę się zabezpieczyć przed kradzieżą tożsamości?

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 wyświetlona ikona kłódki, a adres strony powinien się zaczynać od znaków https://, a nie http://.

Sprawdzaj dostępność 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 zmienić ten adres, będzie to mniej kłopotliwe niż zmiana głównego adresu używanego do korespondencji.

Więcej informacji: www.makeITsecure.org/identitytheft

http:// i **https://** to ciągi znaków umieszczone 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 urządzenie i znacznie ograniczyć ryzyko utraty danych.

Zawsze korzystaj z aktualnego oprogramowania antywirusowego i antyszpiegowskiego

Wirusy komputerowe to małe programy, które dołączają się do większych 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.

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").

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

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 zabezpieczające tego typu umożliwiają automatyczną aktualizację przez Internet.

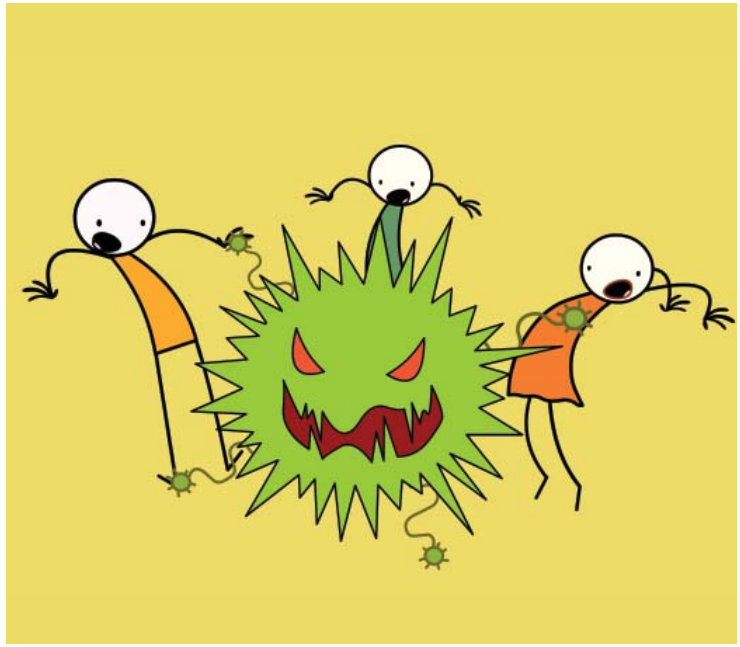
Zawsze instaluj aktualizacje zaufanych aplikacji

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

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 zapora sieciowa) pełni funkcję sieciowego odźwiernego. Na bieżąco filtruje dane przesyłane między Internetem a Twoim komputerem i zezwala na przyjęcie lub wysłanie tylko tych danych, które zostały przez Ciebie dopuszczone. Większość 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.

Wskazówki

Zawsze używaj aktualnego oprogramowania antywirusowego i antyszpiegowskiego oraz zapory (firewall).

Nigdy nie otwieraj podejrzanie wyglądających załączników do wiadomości e-mail.

Zawsze wyrażaj zgodę na instalowanie najnowszych oficjalnych aktualizacji zabezpieczeń, by chronić komputer przed wirusami i oszustami wyłudzającymi dane.

Nigdy nie podawaj nikomu swojego hasła

Zawsze upewnij się, że korzystasz z bezpiecznego połączenia internetowego, gdy podajesz dane personalne — szukaj ikony kłódki.

Zawsze wykonuj kopie zapasowe danych i przechowuj je w bezpiecznym miejscu.

Nigdy nie przesyłaj w wiadomości e-mail danych swojego rachunku bankowego ani karty kredytowej.

Zawsze ustawiaj swój profil w serwisach społecznościowych jako prywatny.

Nigdy nie pozwalaj dzieciom na spotkanie z osobą, którą znają tylko z Internetu, bez Twojego towarzystwa lub innej zaufanej osoby dorosłej. Nie każdy w Internecie jest tym, za kogo się podaje — ludzie często kłamią.

Zawsze zalecaj dzieciom ostrożność przy poznawaniu nowych osób w Internecie — jeśli czują, że coś jest nie w porządku, powinny o tym opowiedzieć Tobie lub innej zaufanej osobie dorosłej.

bezpieczeństwo • łatwa obsługa • makeITsecure.org

Department of Communications, Energy and Natural Resources
Roinn Cumarsáide, Fuinnimh agus Acmhainní Nádúrtha

Microsoft · Symantec · Three.ie · ibf Irish Banking Federation · BT · eircom · O2 · vodafone · Commission for Communications Regulation