KOMENDA POWIATOWA POLICJI W BRZEZINACH

http://brzeziny.policja.gov.pl/ebr/prewencja/bezpieczne-porady/bezpieczny-komputer-i-i/3807,Bezpieczny-komputer-i-internet.html
2023-06-10, 17:19

BEZPIECZNY KOMPUTER I INTERNET

Zabezpiecz swój komputer

Czysto informacyjne i rozrywkowe wykorzystanie Internetu to już przeszłość. Dziś za pomocą sieci dokonuje się skomplikowanych transakcji finansowych, kupuje w wirtualnych sklepach i obsługuje konta bankowe. Niestety, zawsze tam, gdzie są pieniądze, są i oszuści. Dlatego policja radzi jak zabezpieczyć swój komputer, by korzystanie z Internetu było możliwie jak najbezpieczniejsze.

* Surfując po Internecie zachowujmy daleko posuniętą czujność i ostrożność. Na niektórych stronach, zwłaszcza pornograficznych i hakerskich, bardzo często znajdują się złośliwe programy, które możemy nieświadomie zainstalować na komputerze. Mogą one sparaliżować jego pracę bądź wyciągając z niego poufne dane,
* Korzystajmy z legalnego systemu operacyjnego. Pirackie oprogramowania są nie tylko nielegalne, ale mogą zawierać też programy szpiegujące, które bez naszej wiedzy zainstalują się w komputerze. Będą podglądały wszystko, co wpisujemy na klawiaturze i przekazywały tę wiedzę niepożądanym osobom. W ten sposób możemy utracić kody dostępu do naszych kont internetowych, poczty i autoryzowanych stron,
* Zainstalujmy program antywirusowy i antyszpiegowski - darmowe wersje takich programów można znaleźć w Internecie i legalnie je ściągnąć. Programy te uchronią nasz komputer przed wirusami i programami hakerskimi,
* Warto też zaopatrzyć się w tzw. firewall (dosł. ścianę ogniową), która zablokuje próby włamania się z sieci do naszego komputera. Z internetu możemy pobrać darmowe oprogramowanie tego typu,
* Regularnie aktualizujmy: system operacyjny, oprogramowanie antywirusowe i antyszpiegowskie i inne programy, których używamy podczas łączenia się Internetem. Luki w oprogramowaniu mogą posłużyć do włamania się do komputera,
* Dokładnie przyglądajmy się stronom banków, z których korzystamy za pośrednictwem Internetu. Oszuści często podszywają się pod pracowników banku i proszą nas o podawanie numerów kart płatniczych oraz kodów PIN. Nie odpowiadajmy na takie prośby, ale zgłośmy to obsłudze naszego banku. Można także zainstalować tzw. oprogramowanie antyphishingowe, które wychwytuje takie fałszywe strony,
* Korzystając z konta internetowego wpisujmy sami adres strony, nie posiłkujmy się linkami rozsyłanymi przez kogokolwiek. Mogą one kierować do "fałszywej strony banku", której autorami są oszuści,
* Nie otwierajmy maili od nieznanych adresatów i nie używajmy linków rozsyłanych w niechcianej poczcie (tzw. spamie) oraz przez komunikatory. Mogą prowadzić do niebezpiecznych stron lub programów. Użycie oprogramowania antyspamowego znacznie ogranicza ilość niechcianej poczty,
* Komunikatory internetowe (np. Tlen, Gadu-Gadu) są bezpieczne pod warunkiem, że rozmawiamy tylko ze znanymi nam osobami i nie korzystamy z linków oraz plików przesyłanych przez niewiadomych nadawców,
* W przeglądarkach internetowych można ustawić opcję filtru rodzinnego lub zainstalować na komputerze oprogramowanie, które uniemożliwi młodszym członkom rodziny korzystanie z niepożądanych stron.

Jak chronić komputer przed spamem

Prawie każdy korzysta z poczty elektronicznej i prawie każdy użytkownik irytuje się ilością otrzymywanego spamu. Spam to elektroniczne wiadomości masowo rozsyłane do osób, które ich nie oczekują. Poniżej przedstawiamy kilka porad jak uchronić się przed niechcianą pocztą.

Od 10 marca 2003 roku w Polsce obowiązuje zakaz spamowania. Reguluje to Ustawa z dnia 18 lipca 2002 roku o świadczeniu "usług drogą elektroniczną. Ustawa ta reguluje obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną oraz zasady ochrony danych osobowych osób korzystających z tych usług. Nakazuje wyodrębniać i oznaczać w sposób nie budzący wątpliwości informację handlową. Przesyłanie nie zamówionej informacji handlowej skierowanej do oznaczonego odbiorcy drogą mailową jest zakazane. Jej wysyłanie jest możliwe tylko wtedy, gdy

odbiorca wyrazi zgodę, w szczególności przez podanie swojego adresu mailowego. Wysyłanie tej informacji bez zgody odbiorcy jest traktowane jako nieuczciwa konkurencja. Osoba, która otrzyma nie zamówioną informację handlową może wystąpić z wnioskiem o ściganie tego wykroczenia" (portal - forum dyskusyjne pt. Prawo Komputerowe) .
W przypadku otrzymywania niechcianej poczty można sprawdzić czy jest to wiadomość przesłana za zgodą używanego portalu obsługującego naszą skrzynkę pocztową. Przeważnie jest tak, że użytkownik korzystający z usług portalu pocztowego wyraża zgodę na otrzymywanie tzw. ofert reklamowych. Należy pamiętać, że warunkiem korzystania z ofert niektórych darmowych serwisów pocztowych jest również otrzymywanie takich wiadomości, które są traktowane przez nas jako niechciana poczta.
Wyjściem z tego typu problemu jest założenie płatnej skrzynki pocztowej, wolnej od reklam, a także nie wyrażanie zgody na serwisach internetowych na przetwarzanie naszego adresu e-mail w celach marketingowych. Czasami dobrze jest używać ustawień antyspamowych, które w ustawieniach oferują portale pocztowe. Można także wykorzystać programy, które zabezpieczają komputer przed rozsyłaniem niechcianej poczty. W takich programach można samemu zdefiniować adresy, których nie życzymy sobie otrzymywać w przyszłości.
Własny adres e-mailowy, który zamierzamy wstawić na stronach internetowych, blogach czy forach dyskusyjnych można zakodować. Dzięki temu adres wyświetli się internautom, a boty zbierające adresy e-mail nie wychwycą go i w rezultacie nie przechwycą go spamerzy.
Podstawową metodą zabezpieczenia się przed spamem jest używanie legalnych kopii systemu i zainstalowanego w nim oprogramowania oraz bieżące ich aktualizowanie.

Bezpieczne zakupy w sieci

Polacy coraz chętniej kupują w Internecie. To wygodne, gdyż, nie ruszając się sprzed monitora, można zamówić dowolny produkt z dostawą do domu. W sieci nie ma kolejek, godzin spędzonych na chodzeniu między półkami... Niestety, tak jak w realnym świecie, tak i w wirtualnym możemy paść ofiarą oszusta lub złodzieja. Policja radzi, co zrobić, by dokonanie zakupu było możliwie bezpieczne.
Kilka zasad, jak bezpiecznie kupować w sieci:
• Przede wszystkim pamiętajmy, by zawsze kierować się ograniczonym zaufaniem do sprzedającego,
• Nigdy nie kupujmy w sieci korzystając z komputera stojącego w kafejce internetowej. Tam najłatwiej o utratę poufnych danych. Używajmy tylko komputera domowego i zachowujmy całą korespondencję ze sprzedawcą. Jeśli nas oszuka, pozwoli to policji szybko go ująć,
• Korzystajmy tylko ze znanych i sprawdzonych portali internetowych,
• Przed zakupem w wirtualnym sklepie zasięgnijmy opinii o nim i sprawdźmy jego rzetelność. Można to zrobić u znajomych lub na forach internetowych. Zwracajmy też uwagę, czy sklep podaje swój adres i numer telefonu. Wtedy, w razie jakichkolwiek wątpliwości, możemy tam zadzwonić,
• Przy płaceniu kartą kredytową zwracajmy uwagę, czy połączenie internetowe jest bezpieczne i czy przesyłane przez nas dane nie zostaną wykorzystane przez osoby nieuprawnione. Na dole strony powinien pojawić się symbol zamkniętej kłódki, a na końcu adresu – literki "https". Zazwyczaj można też zamówić towar z opcją płatności przy odbiorze,
• Gdy kupujemy na aukcji internetowej, przeczytajmy komentarze o sprzedającym. Brak komentarzy pozytywnych lub ich niewielka liczba powinny wzbudzić naszą szczególną czujność,
• Otrzymując ofertę e-mailem nie korzystajmy z linków, na stronę sklepu wejdźmy wpisując adres w oknie przeglądarki, unikniemy w ten sposób stron podszywających się pod legalnie działające sklepy,
• Zamawiając sprzęt zapytajmy, czy sprzedawca dołącza oryginalne oprogramowanie na płytach i instrukcję obsługi,
• Kupując telefon komórkowy zapytajmy o ładowarkę i dowód zakupu, telefony kradzione sprzedawane są bez ładowarki i "dokumentacji",
• Jeśli, mimo zachowania zasad ostrożności, dostaniemy zamiast zamówionego produktu puste pudełko, natychmiast zadzwońmy na Policję. Wtedy zapisana korespondencja i przesłana przez oszusta paczka będą stanowiły dowód przestępstwa.

Jak chronić dziecko w sieci

10 rad dla rodziców dotyczących bezpiecznego korzystania z Internetu przez dzieci.
1. Odkrywaj Internet razem z dzieckiem.
Bądź pierwszą osobą, która zapozna dziecko z Internetem. Odkrywajcie wspólnie jego zasoby. Spróbujcie znaleźć strony, które mogą zainteresować Wasze pociechy, a następnie zróbcie listę przyjaznych im stron Jeśli Wasze dziecko

sprawniej niż Wy porusza się po Sieci, nie zrażajcie się – poproście, by było Waszym przewodnikiem po wirtualnym świecie.

2. Naucz dziecko podstawowych zasad bezpieczeństwa w Internecie.

Uczul dziecko na niebezpieczeństwa związane z nawiązywaniem nowych znajomości w Internecie. Podkreśl, że nie można ufać osobom poznanym w Sieci, ani też wierzyć we wszystko co o sobie mówią. Ostrzeż dziecko przed ludźmi, którzy mogą chcieć zrobić im krzywdę. Rozmawiaj z dzieckiem o zagrożeniach czyhających w Internecie i sposobach ich unikania.

3. Rozmawiaj z dziećmi o ryzyku umawiania się na spotkania z osobami poznanymi w Sieci.

Dorośli powinni zrozumieć, że dzięki Internetowi dzieci mogą nawiązywać przyjaźnie. Jednakże spotykanie się z nieznajomymi poznanymi w Sieci może okazać się bardzo niebezpieczne. Dzieci muszą mieć świadomość, że mogą spotykać się z nieznajomymi wyłącznie po uzyskanej zgodzie rodziców i zawsze w towarzystwie dorosłych lub przyjaciół.

4. Naucz swoje dziecko ostrożności przy podawaniu swoich prywatnych danych.

Dostęp do wielu stron internetowych przeznaczonych dla najmłodszych wymaga podania prywatnych danych. Ważne jest, aby dziecko wiedziało, że podając takie informacje, zawsze musi zapytać o zgodę swoich rodziców. Dziecko powinno zdawać sobie sprawę z niebezpieczeństw, jakie może przynieść podanie swoich danych osobowych. Ustal z nim, żeby nigdy nie podawało przypadkowym osobom swojego imienia, nazwiska, adresu i numeru telefonu.

5. Naucz dziecko krytycznego podejścia do informacji przeczytanych w Sieci.

Wiele dzieci używa Internetu w celu rozwinięcia swoich zainteresowań i rozszerzenia wiedzy potrzebnej w szkole. Mali internauci powinni być jednak świadomi, że nie wszystkie znalezione w Sieci informacje są wiarygodne. Naucz dziecko, że trzeba weryfikować znalezione w Internecie treści, korzystając z innych dostępnych źródeł (encyklopedie, książki, słowniki).

6. Bądź wyrozumiały dla swojego dziecka.

Często zdarza się, że dzieci przypadkowo znajdują się na stronach adresowanych do dorosłych. Bywa, że w obawie przed karą, boją się do tego przyznać. Ważne jest, żeby dziecko Ci ufało i mówiło o tego typu sytuacjach; by wiedziało, że zawsze kiedy poczuje się niezręcznie,coś je zawstydzi lub przestraszy, może się do Ciebie zwrócić.

7. Zgłaszaj nielegalne i szkodliwe treści.

Wszyscy musimy wziąć odpowiedzialność za niewłaściwe czy nielegalne treści w Internecie. Nasze działania w tym względzie pomogą likwidować np. zjawisko pornografii dziecięcej szerzące się przy użyciu stron internetowych, chatów, e-maila itp. Nielegalne treści można zgłaszać na policję lub do współpracującego z nią punktu kontaktowego ds. zwalczania nielegalnych treści w Internecie – Hotline'u (www.dyzurnet.pl). Hotline kooperuje również z operatorami telekomunikacyjnymi i serwisami internetowymi w celu doprowadzenia do usunięcia nielegalnych materiałów z Sieci.

8. Zapoznaj dziecko z NETYKIETĄ - Kodeksem Dobrego Zachowania w Internecie.

Przypominaj dzieciom o zasadach dobrego wychowania. W każdej dziedzinie naszego życia, podobnie więc w Internecie obowiązują takie reguły: powinno się być miłym, używać odpowiedniego słownictwa itp. (zasady Netykiety znajdziesz na stronie www.sieciaki.pl) Twoje dzieci powinny je poznać (nie wolno czytać nie swoich e-maili, kopiować zastrzeżonych materiałów, itp.).

9. Poznaj sposoby korzystania z Internetu przez Twoje dziecko.

Przyjrzyj się, jak Twoje dziecko korzysta z Internetu, jakie strony lubi oglądać i jak zachowuje się w Sieci. Staraj się poznać znajomych, z którymi dziecko koresponduje za pośrednictwem Internetu. Ustalcie zasady korzystania z Sieci oraz sposoby postępowania w razie nietypowych sytuacji.

10. Pamiętaj, że pozytywne strony Internetu przeważają nad jego negatywnymi stronami.

Internet jest doskonałym źródłem wiedzy, jak również dostarczycielem rozrywki. Pozwól swojemu dziecku w świadomy i bezpieczny sposób w pełni korzystać z oferowanego przez Sieć bogactwa.źródło: www.dzieckowsieci.pl

Phishing

Phishing - celowo błędny zapis słowa "fishing" (łowienie ryb) - to, najkrócej mówiąc, pozyskanie poufnej informacji osobistej. Phisherzy wykorzystują w tym celu mechanizmy socjotechniczne. Krąży kilka teorii na temat tego skąd się wzięło to określenie. Jedna z nich mówi, że zostało wymyślone w latach dziewięćdziesiątych przez przez crackerów próbujących wykraść konta jednego z największych amerykańskich portali.

Popularnym celem phisherów są banki czy aukcje internetowe. Phisher przeważnie rozpoczyna atak od rozesłania

pocztą elektroniczną odpowiednio przygotowanych wiadomości, które udają oficjalną korespondencję z banku, serwisu aukcyjnego lub innych portali. Zazwyczaj zawierają one informację o rzekomym zdezaktywowaniu konta i konieczności jego ponownego reaktywowania. W mailu znajduje się odnośnik do strony, na której można dokonać ponownej aktywacji konta. Pomimo że witryna z wyglądu przypomina stronę prawdziwą, w rzeczywistości jest to przygotowana przez przestępcę pułapka. Nieostrożni i nieświadomi użytkownicy ujawniają swoje dane uwierzytelniające (kody pin, identyfikatory i hasła). Bywa również, że przestępcy posługują się prostszymi metodami, które polegają na wysłaniu maila z prośbą, czasem wręcz żądaniem, podania danych służących do logowania na konto i jego autoryzacji.
Innym sposobem działania cyberprzestępców, który ma doprowadzić do poznania poufnych danych, jest wykorzystywanie złośliwego oprogramowania, zwanego w zależności od swojej formy: robakami, koniami trojańskimi (trojanami) lub wirusami. Takiego "robaka" można ściągnąć korzystając z zainfekowanych witryn internetowych.
Bardziej zaawansowaną, a co za tym idzie niebezpieczniejszą dla użytkownika oraz trudniejszą do wykrycia, formą phishingu jest tzw. pharming. Zamiast wysyłania fałszywych wiadomości e-mail, przestępcy przekierowują użytkowników wpisujących prawidłowe adresy np. swojego banku na fałszywe strony internetowe.
Każdy internauta powinien mieć świadomość zagrożeń, jakie wiążą się z pobieraniem z sieci oprogramowania z niepewnych serwerów czy odpowiadaniem na podejrzaną pocztę elektroniczną. Pamiętajmy, że:
• serwisy nie wysyłają e-maili z prośbą o odwiedzenie i zalogowanie się na stronie,
• nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila,
• należy regularnie uaktualniać system i oprogramowanie,
• nie wolno przesyłać mailem żadnych danych osobistych - w żadnym wypadku nie wypełniajmy danymi osobistymi formularzy zawartych w wiadomości e-mail,
• zastanówmy się nad napisaniem wiadomości e-mail zwykłym tekstem zamiast HTML,
• banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. Adres strony WWW rozpoczyna się wtedy od wyrażenia 'https://', a nie 'http://'. Jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to osobom z banku i nie podawać na niej żadnych danych.
Każde podejrzenia co do sfingowanych witryn należy jak najszybciej przekazać policjantom lub pracownikom danego banku odpowiedzialnym za jego funkcjonowanie w sieci.

"Nigeryjski szwindel"

Zwykle zaczyna się podobnie. Autor przesłanego do nas maila informuje, że możemy otrzymać olbrzymie pieniądze, a fortuna jest dosłownie na wyciągnięcie ręki. Musimy tylko dopełnić kilku formalności i dokonać opłat manipulacyjnych. Te kwoty, w porównaniu z gotówką, jaką mamy dostać, wydają się jednak niewielkie. Dopiero po jakimś czasie okazuje się, że nie czeka na nas żaden spadek ani wygrana, ale padliśmy ofiarą oszustów.
"Oszustwo nigeryjskie" lub "nigeryjski szwindel" – tym terminem policjanci określają specyficzny i stosunkowo nowy rodzaj oszustw. Ten przestępczy proceder najczęściej rozpoczyna się od kontaktu, który przestępcy nawiązują z pokrzywdzonymi za pośrednictwem poczty elektronicznej. Polega on na wciągnięciu ofiary w grę psychologiczną. Jej fabuła oparta jest na fikcyjnym transferze dużej kwoty pieniędzy z jednego z krajów afrykańskich, zwykle Nigerii. W rzeczywistości chodzi po prostu o wyłudzenie od ofiar pieniędzy dzięki wykorzystaniu wymyślonej historii. Ofiarami wcześniej padali przypadkowi właściciele skrzynek mailowych. Teraz coraz częściej przestępcy starannie dobierają tych, których chcą oszukać.
Na arenie międzynarodowej przypadki takie bada U. S. Secret Service, ale nawet ta służba stoi na stanowisku, że odzyskanie pieniędzy utraconych w wyniku „oszustwa nigeryjskiego” jest praktycznie niemożliwe. Aby móc skutecznie bronić się przed oszustami warto wiedzieć, jakimi metodami się oni posługują.
"Na uchodźcę politycznego z czarnego lądu"
Przestępca kontaktuje się z ofiarą najczęściej wykorzystując do tego pocztę elektroniczną, rzadziej telefon. W korespondencji pada propozycja otrzymania ogromniej kwoty pieniędzy. Chodzi o części fortuny, jaką oszust posiada (odziedziczył), ale której sam nie może podjąć z banku z różnych przyczyn. Niekiedy oszust podaje się za uchodźcę politycznego, dziedzica fortuny zgromadzonej przez jednego z przywódców któregoś z państw afrykańskich obalonego w trakcie przewrotu politycznego. Chodzi zwykle o bardzo duże sumy, 20 – 30 mln USD, a oszust w zamian za pomoc w jej odzyskaniu oferuje nawet połowę tej kwoty.
„Pomoc” ta wymaga jednak od ofiary finansowania kolejnych kroków, jakie oszust musi czynić by sfinalizować przelew majątku na konto wskazane przez ofiarę. W cyklicznie otrzymywanej korespondencji ofiara dowiaduje się, że oszust musi np. zarejestrować działalność gospodarczą, posłużyć się kilkoma łapówkami by przekupić bankierów, skorumpowanych policjantów lub innych urzędników państwowych w jego kraju lub musi opłacić procedurę wystawienia

certyfikatów przez bank, poświadczających, że pieniądze nie pochodzą z nielegalnego źródła (np. z działalności terrorystycznej lub handlu narkotykami). Ofiara, która już widzi siebie jako milionera, pokrywa kolejne koszty związane z finalizacją całej operacji. Pieniądze przejmuje oszust, który od czasu do czasu uwiarygodnia historię przesyłając pocztą elektroniczną spreparowane certyfikaty, kopie potwierdzeń przelewów, itp. W tym momencie rozpoczyna się gra, która ma na celu jak najdłuższe zwodzenie ofiary i wyłudzenie jak największej ilości pieniędzy. Zazwyczaj ofiara na tym etapie zaczyna podejrzewać oszustwo i w pewnym momencie przestaje płacić. Oszust jednak osiągnął zamierzony cel – praktycznie już po otrzymaniu pierwszej wpłaty. Gdy ofiara przerywa „finansowanie operacji" często dochodzi do gróźb lub zmiany fabuły gry. Oszust teraz może podawać się za inną osobę, ale są to tylko próby wyłudzenia kolejnych sum.

Na "inwestora"

Przestępca kontaktuje się z ofiarą najczęściej wykorzystując do tego wyłącznie pocztę elektroniczną. Oszust podaje się za młodego, wykształconego człowieka, któremu udało się „wybić" w jego rodzinnym kraju (młody prawnik, student, modelka). Jego ojciec lub przyjaciel posiada ogromny majątek, który chce korzystnie zainwestować. Ofiara ma pomóc w inwestowaniu pieniędzy w swoim rodzimym kraju. Dalszy ciąg jest analogiczny do poprzedniej metody.

Na "wygraną na loterii"

Potencjalna ofiara otrzymuje pocztą elektroniczną spreparowaną wiadomość o wygranej dużej sumy pieniędzy w jednej z (narodowych) loterii jakiegoś europejskiego kraju. Ostatnio oszuści najczęściej podszywali się pod organizatorów loterii hiszpańskich. Wraz z informacją otrzymujemy certyfikat uprawdopodobniający wygraną oraz istnienie samej loterii. Kwoty, jakie mamy otrzymać są zwykle znacznie niższe niż w klasycznym „oszustwie nigeryjskim", Oszust, by rozwiać wszelkie podejrzenia ofiary, twierdzi, że nagrodę można odebrać osobiście, podając dokładny adres i telefony kontaktowe. Mało kto jednak decyduje się na precyzyjne sprawdzenie tych danych. Zwykle pokrzywdzeni deklarują, że chcą otrzymać wygraną w formie międzynarodowego przelewu bankowego. Tu pojawiają się pierwsze opłaty, które ofiara zobowiązana jest uiścić by móc odebrać nagrodę – opłata dla prawnika, opłata za wystawienie kilku nieznanego pochodzenia wewnętrznych dokumentów banku i certyfikatów, do opłacenia podatku od wzbogacenia włącznie. Jak w każdym z omawianych przypadków żadna wygrana nie istnieje, a oszust podtrzymuje kontakt tak długo, jak długo ofiara dokonuje kolejnych wpłat. Niekiedy ofiara informuje, że posiada połowę żądanej przez oszusta kwoty, na co oszust odpowiada, że drugą część pokryje on ze środków własnych, które później ofiara mu zwróci. Wszystko ma służyć temu, by nie wstrzymywać całej procedury. Wreszcie oszust wysyła pocztą tradycyjną, nie tylko elektroniczną, kolorowe certyfikaty i potwierdzenia przyjęcia przez różne instytucje i banki opłat od ofiary. Zaś pieniądze z wygranej giną gdzieś na „czarnym lądzie"...

Na "konta w banku bez właściciela"

Przestępca, udając najczęściej pracownika banku, kontaktuje się z ofiarą za pośrednictwem poczty elektronicznej. Potencjalna ofiara jest informowana, że klient banku zmarł lub zginął w tragicznym wypadku i zostawił po sobie konto z ogromną sumą pieniędzy. Nie wskazał jednocześnie żadnych spadkobierców, a bank nie mógł ustalić żadnego członka jego rodziny. Po odczekaniu kilku lub nawet kilkunastu lat bank zamierza zlikwidować martwe konto i szuka kogoś, kto przejmie jego zawartość.

Kiedy ofiara wyrazi zainteresowanie, oszust przysyła wiadomość ze szczegółami historii. Często załącza dokumenty (wątpliwej jakości) potwierdzające istnienie przedmiotowego konta, należącego do zmarłego milionera. Czasami oszuści decydują się również na kontakt telefoniczny. Z ofiarą kontaktują się kolejne osoby - dyrektor banku, prawnik lub inny urzędnik, który jest władny wystawiać lub uwiarygodniać dokumenty - które mają uwiarygodnić całą historię. Wtedy też pojawiają się pierwsze informacje, że ofiara będzie musiała sfinansować kilka przedsięwzięć, by w końcu móc cieszyć się milionami. Okazuje się, że ma ponieść opłaty za wystawienie przez bank lub inne urzędy certyfikatów, poświadczających, że pieniądze pochodzą z legalnego źródła, za usługi prawników oraz koszty operacyjne w banku. Oszust podtrzymuje korespondencję prosząc o kolejne wpłaty tak długo jak na to pozwala naiwność ofiary oszustwa.

Pozostawione miliony na koncie są oczywiście fikcją, jak również to, że informacja pochodzi z banku. Nazwiska pracowników banku mogą być prawdziwe, gdyż przeważnie są to dane ogólnie dostępne w Internecie. Należy jednak zwrócić uwagę na numery telefonów, których nie znajdziemy w informacjach kontaktowych rzeczywiście istniejącego banku, a adresy e-mail używane przez oszustów często należą do puli adresów serwerów oferujących bezpłatną rejestrację konta poczty elektronicznej, (np. Yahoo, Google Gmail).

Na "aukcje internetową"

Ofiara jest wyszukiwana na portalu aukcyjnym, gdzie wystawia jakiś wartościowy sprzęt elektroniczny, np. laptop lub sprzęt fotograficzny. Kontakt za pośrednictwem poczty elektronicznej nawiązuje oszust, który sprawia wrażenie bardzo zainteresowanego zakupem oferowanego towaru. Wartościowy przedmiot ma najczęściej stanowić prezent dla bliskiej osoby, przebywającej w innym kraju niż oszust. Oszustowi bardzo zależy na czasie wysyłki, który ma być jak najkrótszy, więc sprzedaż musi się odbyć poza aukcją, jeżeli aukcji nie można zakończyć z opcją „kup teraz". Oszust takie niedogodności jest gotów wynagrodzić oferując nawet dwukrotnie wyższą kwotę niż żąda sprzedający.

Wielu sprzedających zgadza się wysłać towar, oczywiście po otrzymaniu zapłaty. Tu pojawia się charakterystyczny dla tego oszustwa sposób działania sprawcy. Po zakończeniu transakcji, najczęściej drogą elektroniczną, ofiara otrzymuje spreparowany skan potwierdzenia dokonania wpłaty pieniędzy, wraz z komentarzem, iż przelew pieniędzy z Afryki trwa kilka dni, a prezent musi być dostarczony niezwłocznie. Często wpłata ma odbywać się za pośrednictwem takich systemów płatności, jak Bidpay, Money Gram, Western Union. Oszust prosi, by ofiara wysłała towar przed otrzymaniem wpłaty na konto. Ma przecież potwierdzenie dokonania wpłaty w postaci zeskanowanego dokumentu. Zazwyczaj sprzedający godzi się na to. Jeżeli natomiast nie wyraża zgody, jest straszony złamaniem umowy, oskarżany o oszustwo, a w skrajnych przypadkach straszony nawet zgłoszeniem sprawy do Interpolu. W konsekwencji sprzedający wysyła towar, ale nigdy nie otrzymuje za niego pieniędzy.

Na "spadek"

Pierwszy kontakt z wytypowaną ofiarą ma wyglądać na zupełnie przypadkowy. Może to być „przypadkowe" spotkanie z osobą, która twierdzi, że nosi takie same nazwisko jak ofiara (bądź nazwisko panieńskie matki ofiary), lub zna kogoś kto mógł należeć do rodziny ofiary. Scenariuszy może być wiele. Chodzi tylko o to, by w pamięci ofiary utkwił fakt, że gdzieś za granicą żyje ktoś, kto należy do jej rodziny, wie o istnieniu ofiary, mimo że nie utrzymuje stałego kontaktu. Przestępcy śledzą wszystkie informacje, które mogą świadczyć o nagłej śmierci (katastrofa komunikacyjna, pożar lub trzęsienie ziemi) osoby o takim samym nazwisku jak potencjalna ofiara. Następnie kontaktują się z ofiarą najczęściej wykorzystując do tego pocztę elektroniczną, rzadziej telefon. W korespondencji informują potencjalną ofiarę, że jest jedynym żyjącym spadkobiercą dalekiego krewnego, który niedawno stracił życie, np. w katastrofie lotniczej (dane najczęściej są ogólnie dostępne w Internecie) i nie pozostawił potomstwa, a w testamencie swój ogromny majątek postanowił przekazać jedynemu znanemu krewnemu, czyli wytypowanej potencjalnej ofierze oszustwa. Odziedziczoną fortunę ofiara może podjąć z banku po dopełnieniu kilku formalności i opłaceniu należności. Ofiara ‚na polecenie oszusta podającego się za prawnika bądź bankiera, zaczyna finansować kolejne wydatki. Jak w przypadku innych oszustw nigeryjskich, oszuści uwiarygodniają całą historię przesyłając pocztą elektroniczną spreparowane certyfikaty, kopie potwierdzeń przelewów, itp. Również w tym przypadku, rozpoczyna się gra na zwłokę, która ma na celu jak najdłuższe zwodzenie ofiary i wyłudzenie jak największej kwoty pieniędzy.

By nie paść ofiarą oszustwa zachowajmy rozwagę i rozsądek!

Pamiętajmy:

1. Jeżeli zostaliśmy wybrani na pomocnika w odzyskaniu pieniędzy przez uchodźcę politycznego z czarnego lądu i za to mamy otrzymać np. 12 milionów dolarów, możemy być pewni, że jest to oszustwo.
2. Jeżeli otrzymamy e-mail z informacją, że zostaliśmy zwycięzcami zagranicznej loterii, w której nie braliśmy udziału, to śmiało możemy potraktować tą informację jako spam i od razu przekierować ją do kosza.
3. Jeżeli otrzymamy niespodziewanie miliony dolarów w spadku po krewnym, o którego istnieniu nie mieliśmy pojęcia, a warunkiem otrzymania fortuny jest dokonanie określonych wpłat, możemy być niemal pewni, że ktoś próbuje nas oszukać,
4. Uważajmy, jeżeli ktoś za przekazanie nam ogromnej kwoty pieniędzy żąda opłat manipulacyjnych (opłacania prawników, certyfikatów),
5. Pamiętajmy, że certyfikaty wystawiane przez różne instytucje, to dokumenty, które tak jak dokumenty identyfikacyjne, papiery wartościowe i banknoty, mają odpowiednie zabezpieczenia - hologramy, recto-verso, czy mikrodruk, które po wykonaniu skanowania (digitalizacji obrazu), tracą swoje właściwości, a tym samym przesłany nam skan certyfikatu nie ma żadnej wartości i wagi prawnej.
6. Po zakończeniu transakcji z opcją „wpłata na konto bankowe" należy trzymać się sztywno podstawowej zasady – towar wysyła się wyłącznie dopiero po zaksięgowaniu pełnej kwoty na koncie bankowym.

Materiały: Biuro Kryminalne KGP (Jak uniknąć "oszustwa nigeryjskiego" - http://www.policja.pl/portal/pol/154/39219/Jak_uniknac_quotoszustwa_nigeryjskiegoquot.html)

Być świadomym i bezpiecznym użytkownikiem Internetu

Internet jest alternatywnym światem, platformą wymiany informacji, zawiązywania znajomości, miejscem zabawy, nauki i pracy. I tak jak świat rzeczywisty, sieć ma swoje dobre i złe strony, ponieważ wszystkie zachowania ludzkie mają także tu swoje odzwierciedlenie. Aby nie paść ofiarą internetowych przestępców, należy zachować ostrożność i pamiętać o paru zasadach.

Zagadnienie bezpieczeństwa w sieci jest złożonym problemem, jednak ogólnie można podzielić je na dwa obszary. Pierwszym jest bezpieczeństwo realizowane przez właściwe zabezpieczenie komputera, zarówno programowe, jak i fizyczne, natomiast drugim jest zabezpieczenie osobiste użytkownika, realizowane przez informacje dobrowolnie umieszczane w sieci. Mówiąc o bezpieczeństwie w sieci, należy wiedzieć, że oba te elementy wspólnie zabezpieczają użytkownika przed konsekwencjami spotkania się z „ciemną stroną" Internetu.

Zabezpieczenie komputera, jako urządzenia realizującego aktywność użytkownika w sieci, powinno być pierwszym etapem w polityce bezpieczeństwa sieciowego. Niewłaściwe zabezpieczenie komputera może skutkować zarówno wymiernymi stratami finansowymi, jak i przejęciem władzy nad komputerem przez osoby niepowołane. Każde urządzenie informatyczne podłączone do globalnej sieci jest narażone na ataki przeprowadzane przez osoby wykorzystujące zarówno słabości systemów operacyjnych, jak i słabą wiedzę oraz brak świadomości użytkownika.

Sieciowi agresorzy, czyli hakerzy, atakują komputery w sieci w celu nielegalnego uzyskania poufnych danych znajdujących się w zasobach dyskowych bądź w celu nieautoryzowanego wykorzystania mocy obliczeniowej atakowanych urządzeń. Niezabezpieczony użytkownik może nieświadomie pobrać z sieci i zainstalować oprogramowanie, które może wykraść i wysłać hakerowi osobiste i newralgiczne dane, zniszczyć je, bądź uszkodzić system. Programy zbierające informacje z zainfekowanych komputerów nazywa się w gwarze informatycznej „robakami". Ich zadaniem jest wyciągnięcie danych znajdujących się w plikach atakowanego systemu, takich jak loginy i hasła do kont pocztowych i bankowych, dane logowań do zastrzeżonych obszarów sieci wykorzystywanych przez użytkownika (fora, portale społecznościowe), dane ze stworzonych przez użytkownika plików. Bardzo często „robaki" mają funkcje destrukcyjne, mające na celu zamaskowanie swojej działalności, bądź po prostu jedyną ich funkcją jest niszczenie plików i danych. Ponadto, wykorzystując słabości systemu i potencjalny brak zabezpieczeń, rozmnażają się, kopiują, podłączając się do wiadomości e-mail czy wymiennych nośników danych, infekując kolejne maszyny. „Robaki" mogą również otwierać ukryte połączenia, udostępniając hakerom furtkę do zarażonego systemu, umożliwiając tym samym przejęcie nad nim kontroli. Uzyskanie dostępu do zasobów komputera umożliwia wykorzystanie go, bez wiedzy użytkownika, do zmasowanego ataku na wskazane przez hakera cele. Użytkownik taki staje się bez swojej wiedzy i woli agresorem, z którego komputera dokonywany jest atak na np. serwery rządowe czy bankowe.

Cechą charakterystyczną „robaków" jest to, że są autonomicznymi programami. Z kolei programy posiadające ww. cechy, ale potrzebujące do rozprzestrzeniania się programu-żywiciela to „wirusy". Rozpowszechniają się przez infekcję programów użytkowych. Nieświadomy użytkownik komputera pobiera z sieci program, który ma mu pomóc lub uprzyjemnić czas spędzany przed monitorem, i dostaje program, który oprócz oczekiwanej funkcjonalności posiada w sobie złośliwy kod, będący szkodliwy dla użytkownika.

Wykradzenie danych dot. logowań do portali bądź usług sieciowych może skutkować przejęciem przez hakera kontroli nad pocztą e-mail, kontem bankowym, komunikatorami, tożsamościami w portalach społecznościowych. I wtedy haker może nam poważnie zaszkodzić. Nasze adresy e-mail czy nasze wirtualne tożsamości są swoistym gwarantem tego, że nasi znajomi przez komunikację z nimi kontaktują się z nami. I kiedy z konta na Facebooku czy Naszej Klasie rozesłana zostanie kompromitująca bądź obraźliwa wiadomość, znajomi użytkownika odbiorą ją jako informację od niego. Przejmując konto pocztowe i wykorzystując życzliwość znajomych ofiary, przestępca może próbować wyłudzić pieniądze, np. pisząc prośby o pomoc w imieniu ofiary. Przejęcie konta w serwisie aukcyjnym może spowodować utratę kontroli nad kontem, powiązanym z nami fizycznie, i w rezultacie konto takie może być wykorzystane do dokonywania oszustw. Działalność taka bezpośrednio godzi zarówno w wiarygodność użytkownika i jego dobre imię, jak i bezpośrednio w bezpieczeństwo finansowe oraz naraża na problemy z organami ścigania.

Należy również wspomnieć o ryzyku uzyskania przez hakera dostępu do internetowego konta bankowego. Z uwagi na zaimplementowane przez banki systemy zabezpieczeń i autentykacji użytkownika oraz wykonywanych operacji, przejęcie kontroli nad środkami zgromadzonymi na koncie jest co prawda trudne, jednak nie jest niemożliwe. Dlatego wszelkie operacje na kontach bankowych należy traktować jako szczególnie wrażliwe.

Mając powyższe na uwadze, należy zabezpieczyć swój sprzęt komputerowy przed działaniami hakerów. Podstawową zasadą bezpieczeństwa jest, po pierwsze, aktualizowanie systemu. Programiści, znajdując w systemie bądź programie funkcję mogącą stanowić zagrożenie dla komputera, zgłaszają ten fakt do producenta systemu. Producent publikuje aktualizację, tzw. łatkę, która ma na celu zabezpieczenie systemu przed atakiem wykorzystującym zdiagnozowaną słabość.

Ponadto, obowiązkowym jest zainstalowanie skutecznego oprogramowania antywirusowego. Dostępne aktualnie pakiety antywirusowe oferują w swojej funkcjonalności sprawdzanie wszystkich plików na podłączonych dyskach pod kątem wystąpienia infekcji, sprawdzanie otwieranych wiadomości pocztowych, zawartości przeglądanych stron internetowych, pobieranych i otwieranych plików. Ważna jest też aktualizacja tego oprogramowania - zarówno bazy wirusów, jak i samego programu. Zasadą również powinno być niepobieranie żadnych plików z niezaufanych źródeł. Ponadto, każdy pobrany plik powinien być sprawdzony przez uaktualniony program antywirusowy. Jest to o tyle ważne, że każdy plik, nie tylko wykonywalny (*.exe), może być potencjalnym nośnikiem złośliwego oprogramowania. Wirusy mogą być ukryte w plikach filmowych, graficznych, muzycznych itp.

Niezbędne jest również zainstalowania tzw. firewalla - zapory sieciowej, czyli oprogramowania sprawującego kontrolę nad połączeniami komputera z Internetem. W pierwszym etapie konfiguracji takiego oprogramowania należy zablokować wszystkie połączenia, a następnie dodać wyjątki - zezwolić jedynie na połączenia niezbędne do komfortowej pracy w sieci. Złośliwe oprogramowanie, nawiązując połączenia zewnętrzne, zazwyczaj próbuje nawiązać odrębne połączenie - na odrębnym porcie komunikacyjnym. Zastosowanie wyżej opisanej reguły firewalla będzie skutkować natychmiastowym powiadomieniem użytkownika o niezidentyfikowanym połączeniu i pytaniem, czy dane połączenie ma być zrealizowane. W razie jakichkolwiek wątpliwości należy podejrzane połączenie zablokować, gdyż może być to próba ataku.

Dodatkowo zaleca się, aby do operacji mających duże znaczenie dla użytkownika, wykorzystywać systemy operacyjne w wersji tzw. live, tzn. wczytywane do pamięci nie z dysku twardego, ale ze startowej płyty CD/DVD. Posiadając taki system, można bezpiecznie korzystać z Internetu, ponieważ żadne dane nie są pobierane z dysku twardego komputera, więc nawet może być on zawirusowany. Po prostu dysk twardy wraz z ewentualnie znajdującymi się na nim wirusami/robakami nie będzie odczytywany. Uzyskuje się w ten sposób sterylny kanał komunikacyjny do operacji szczególnie wrażliwych, takich jak np. operacje bankowe.

Z zagadnieniem bezpieczeństwa w sieci nierozerwalne jest też fizyczne bezpieczeństwo użytkownika. Należy mieć na uwadze, że publikowanie w Internecie dane przeglądane są przez różnych ludzi. Użytkownicy serwisów i portali społecznościowych, prowadzący blogi czy prywatne strony internetowe, publikują informacje o sobie, nie zastanawiając się nad tym, kto może stać się odbiorcą tych danych. Z sieci korzystają zarówno uczciwi, serdeczni ludzie, ale również przestępcy, dla których takie zapisy są kopalnią informacji o statusie majątkowym użytkownika, miejscu zamieszkania czy nawet terminach planowanych urlopów. Posiadając tego typu wiedzę, bardzo łatwo przestępcy zaplanować np. włamanie. Dlatego każda osoba powinna mieć to na uwadze, zamieszczając dane o sobie, takie jak np. zdjęcia swojego nowego domu, samochodu czy sprzętu RTV, a także dane planowanych wyjazdów.

Należy też mieć na uwadze inne niebezpieczeństwa związane z publikacją osobistych informacji. Osobie postronnej posiadającej wiedzę o problemach, troskach, zmartwieniach czy radościach użytkownika łatwo jest nawiązać w sieci relację, w której wyda się pożądaną, interesującą osobowością. Znając problemy użytkownika, łatwo jest wykorzystać tę wiedzę do zbudowania zaufania, co – przy wirtualnym charakterze znajomości – nie musi być niebezpieczne. Dużą ostrożność należy jednak zachować w momencie, kiedy wirtualna znajomość zmienia się w realne spotkania. Nigdy nie wiadomo do końca, kto jest tym znajomym. Jeśli jest osobą taką, jaką dał się poznać - to nie ma powodu do obaw, w przeciwnym wypadku najlepsze jest przerwanie wszelkich kontaktów. Należy zwrócić szczególną uwagę i zachować wyjątkową ostrożność w momencie, kiedy dziecko zawiera jakiekolwiek znajomości przez Internet, a następnie przenosi je w świat rzeczywisty. Dziecko z natury rzeczy jest podatne na manipulację, co może być wykorzystane przez przestępców. W tym momencie pojawia się ważne zadanie dla rodziców i opiekunów dzieci - w porę zobaczyć zagrożenie i w odpowiedni sposób przeciwdziałać ewentualnym skutkom.

Należy mieć również na uwadze, że zamieszczone w sieci informacje, zdjęcia, mogą zostać łatwo przekształcone i zmanipulowane, co przyczynić się może do problemów towarzyskich również w świecie rzeczywistym. Przyjmuje się, że każda działalność w Internecie, na skutek której użytkownik czuje się zagrożony czy ośmieszony - słowem niekomfortowo, jest tzw. cyberprzemocą. Cyberprzemoc jest skodyfikowana w przepisach karnych i użytkownik uważający, że jest jej ofiarą może zgłosić ten fakt w każdej jednostce Policji (art. 190a § 2, art. 267 § 1 i 2, art. 268 § 2, art. 269 § 1 i 2, art. 278, art. 286, art. 287, art. 293 Kodeksu Karnego).

Podsumowując, globalna sieć komputerowa (Internet), jest wspaniałym tworem, platformą wymiany informacji, zawiązywania znajomości, miejscem relaksu, zabawy, nauki, pracy, czyli jest alternatywnym światem, istniejącym w gąszczu przewodów, wśród migających światełek modemów. I tak jak świat rzeczywisty, ma swoje dobre i złe strony.

Wszystkie zachowania ludzkie mają swoje odzwierciedlenie w sieci. Zachowując ostrożność, tak jak w świecie rzeczywistym, świat wirtualny pokaże swoje piękno. I od jego użytkowników zależy, czy stać się ofiarą jego „ciemnej strony".

Opracował:
asp. Tomasz Zachmacz
Wydział Wsparcia Zwalczania Cyberprzestępczości
Biura Kryminalnego KGP