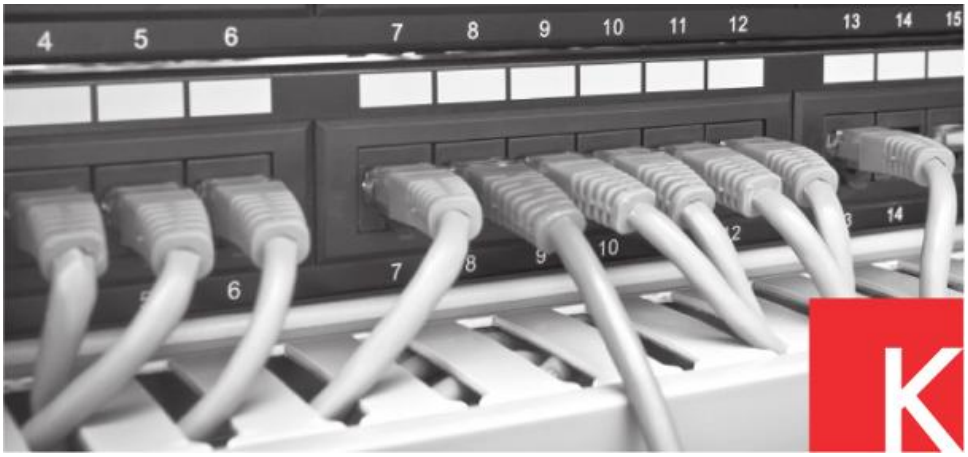
2012

Kompendium bezpiecznego korzystania z Internetu

veracity

Niniejsze kompendium jest przeznaczone dla osób, które chcą dowiedzieć się jak bezpiecznie korzystać z Internetu. Dostarcza ono spójnych i rzetelnych informacji na temat zagrożeń płynących z sieci i sposobów zabezpieczenia się przed nimi.



Autor
Fundacja Veracity
2012-06-01

Spis treści

Wprowadzenie

Celem niniejszego kompendium jest zaprezentowanie czytelnikowi zagrożeń płynących z sieci i sposobów zabezpieczenia się przed nimi. Przewodnik został podzielony na trzy rozdziały:

- Bezpieczeństwo w Internecie
- Główne zagrożenia dla użytkowników Internetu
- Zalecenia fundacji Veracity dotyczące bezpiecznego korzystania z Internetu

W pierwszej części kompendium opisano skalę i trendy w zakresie zagrożeń płynących z Internetu. W rozdziale tym można znaleźć streszczenie i wnioski z raportów dotyczących bezpieczeństwa w Internecie wydawanych przez najważniejsze instytucje i firmy zajmujące się tą tematyką.

Druga część kompendium zawiera opis i przykłady siedmiu najważniejszych rodzajów zagrożeń, na jakie narażeni są Internauci. Opisano w niej współczesne rodzaje oszustw i przestępstw Internetowych stosowanych przez cyberprzestępców.

Trzecia część kompendium zawiera zestaw 18 zaleceń fundacji Veracity w zakresie bezpiecznego korzystania z Internetu. W tej części zawarto zasady, opisy, konkretne wskazówki i przykłady działań, jakie powinien stosować każdy użytkownik Internetu, któremu zależy na bezpieczeństwie.

Zapraszamy do lektury.

Bezpieczeństwo w Internecie

Każdego roku liczba zagrożeń Internetowych rośnie w bardzo szybkim tempie. Dowodzą tego m.in. eksperci ds. bezpieczeństwa międzynarodowej firmy Symantec w swoim corocznym raporcie „INTERNET SECURITY THREAT REPORT". W badaniach prezentują oni statystyki dotyczące zmiany liczby szkodliwych programów (tzw. Malware), ataków hakerskich oraz działań phisingowych w ostatnich latach. Wyniki są niepokojące. Na przykład w 2011 roku liczba niebezpiecznych programów internetowych wzrosła o 36% w stosunku do 2010 roku [z 286mln do 403mln]. Częstotliwości i siły nabierają także ataki hakerskie i phishingowe. Wskazano, że w głównej mierze narażeni na nie są Internauci, którzy nie przestrzegają podstawowych zasad bezpieczeństwa podczas korzystania z Internetu.

Ponadto, z raportów badawczych CERT Polska wynika, że cyberprzestępcy stają się coraz ostrożniejsi i wykorzystują coraz nowsze sposoby kradzieży danych należących do użytkowników Internetu. Z drugiej strony rośnie ilość darmowych narzędzi dla domorosłych hakerów – niewymagających specjalistycznej wiedzy, a umożliwiających przechwycenie danych z niezabezpieczonych komputerów. To sprawia, że nie trzeba być informatykiem ani programistą, żeby stać się cyberprzestępcą.

Poziom wykrywalności cyberprzestępstw jest bardzo niski, ponieważ nie istnieją w Polsce wystarczająco silne organy rządowe, które z problemem cyberprzestępczości potrafiłyby sobie poradzić. To w gestii i obowiązku Internautów leży stosowanie wszelkich dostępnych zabezpieczeń, żeby zapobiegać przestępstwom internetowym. Należy przy tym pamiętać, że instalacja oprogramowania antywirusowego nie zapewnia pełnej ochrony przed zagrożeniami z sieci.

Badania G Data Security Survey wskazują, że komputery zwykłych internautów są bardziej narażone na ryzyko włamania aniżeli te, które znajdują się w firmach i korporacjach. Powód jest prosty – dużo łatwiej jest zainfekować komputer, który nie jest wystarczająco chroniony. Niestosowanie podstawowych zabezpieczeń przez Internautów jest równoznaczne z zaproszeniem cyberprzestępców do ataku na ich komputery.

Przykładem rosnącej ilości zagrożeń jest także raport Ministerstwa Spraw Wewnętrznych opisujący skalę problemu różnego rodzaju oszustw Internetowych. Wynika z niego, że co roku do prokuratur sądowych wpływa coraz większa ilość zawiadomień o dokonaniu przestępstw przez Internet. Wśród nich szczególnie popularnymi są wyłudzenia pieniężne, sprzedaż podrobionych towarów oraz kradzież i handel danymi osobowymi.

Polska w zestawieniu krajów narażonych na cyberprzestępczość zajmuje wysokie miejsce. Z raportu Norton Cybercrime Report 2011 wynika, że jest to miejsce znacznie powyżej średniej światowej. Ponadto specjaliści z PandaLabs, uplasowali Polskę na siódmym miejscu wśród najbardziej zainfekowanych krajów. Według nich 40% komputerów w Polsce jest zainfekowanych.

Trendy nie pozostawiają złudzeń. Wraz z rozwojem Internetu ilość zagrożeń będzie rosła, nie tylko ze strony szkodliwego oprogramowania, phisingu czy ataków hakerskich, ale także ze strony zwykłych oszustów wykorzystujących niewiedzę i zbytnią ufność Internautów. To właśnie niewystarczająca świadomość użytkowników Internetu na temat sposobów zabezpieczenia się przed zagrożeniami płynącymi z sieci jest główną przyczyną, dla której padają oni ofiarą cyberprzestępców.

Główne zagrożenia dla użytkowników Internetu

Badania przeprowadzone przez ekspertów G Data wśród 16 tys. użytkowników Internetu w 11 krajach wykazały następujący fakt: Internauci myślą o bezpieczeństwie w sieci, ale ich wiedza jest już nieaktualna, albo całkowicie nieprawdziwa. Tylko kilka procent Internautów zna naturę współczesnych zagrożeń Internetowych i potrafi efektywnie bronić się przed nimi. Dla wszystkich osób, które chcą uzupełnić swoją wiedzę na ten temat fundacja Veracity przygotowała listę najważniejszych współczesnych zagrożeń płynących z Internetu. Charakter zagrożeń nie zmienia się od dawna. Wśród nich znajdują się oszustwa, kradzieże i wyłudzenia. W praktyce zmieniają się przede wszystkim metody stosowane przez cyberprzestępców w celu ich dokonania. Zapraszamy do zapoznania się z najważniejszymi z nich.

Kradzież danych osobowych i haseł

Kradzież danych oraz haseł jest najpopularniejszym rodzajem przestępstwa Internetowego. Wirtualny świat niczym nie różni się od rzeczywistego. Najczęściej celem cyberprzestępców jest osiągnięcie korzyści finansowych poprzez nielegalne wykorzystanie skradzionych danych osobowych, haseł, adresów e-mail, kodów dostępów, numerów kont, PINów itp. Skradzione dane mogą zostać wykorzystane na wiele różnych sposobów np.:

- włamanie na konto ofiary (np. e-mail, konto bankowe, serwis społecznościowy, forum, komunikator, konto w grze)
- kradzież poufnych informacji,
- kradzież środków pieniężnych,
- odsprzedaż zdobytych informacji,
- szantaż,
- ośmieszenie,
- zszarganie wizerunku,
- podszycie się pod osobę przy wykonywaniu nielegalnych operacji,

- wyprodukowanie fałszywych dowodów tożsamości,
- założenie kont bankowych na fałszywe dane,
- wyłudzenie kredytów,
- założenie fałszywego konta na portalu internetowym i handlowanie różnymi rzeczami w czyimś imieniu.

Jak wykazano, cyberprzestępcy mogą wykorzystywać skradzione dane osobowe na bardzo wiele różnych sposobów – zawsze nieprzyjemnych lub szkodliwych dla ofiary.

Aby ustrzec się przed zagrożeniem utraty danych należy mieć świadomość współczesnych metod stosowanych przez cyberprzestępców do ich pozyskiwania.

Wśród popularnych metod stosowanych przez cyberprzestępców do zdobycia poufnych informacji można wyróżnić m. in. phishing (opisany poniżej), wykorzystanie szkodliwego oprogramowania (tzw. malware), a także zwykłe oszustwa bazujące na zbytniej ufności Internautów – np.:

- fałszywe oferty pracy, w których cyberprzestępcy proszą o przesłanie CV i ksero dowodu osobistego,
- fałszywe informacje o wygranych w konkursach, w których do potwierdzenia wygranej trzeba podać dane osobowe,
- fałszywe sondaże i ankiety Internetowe.

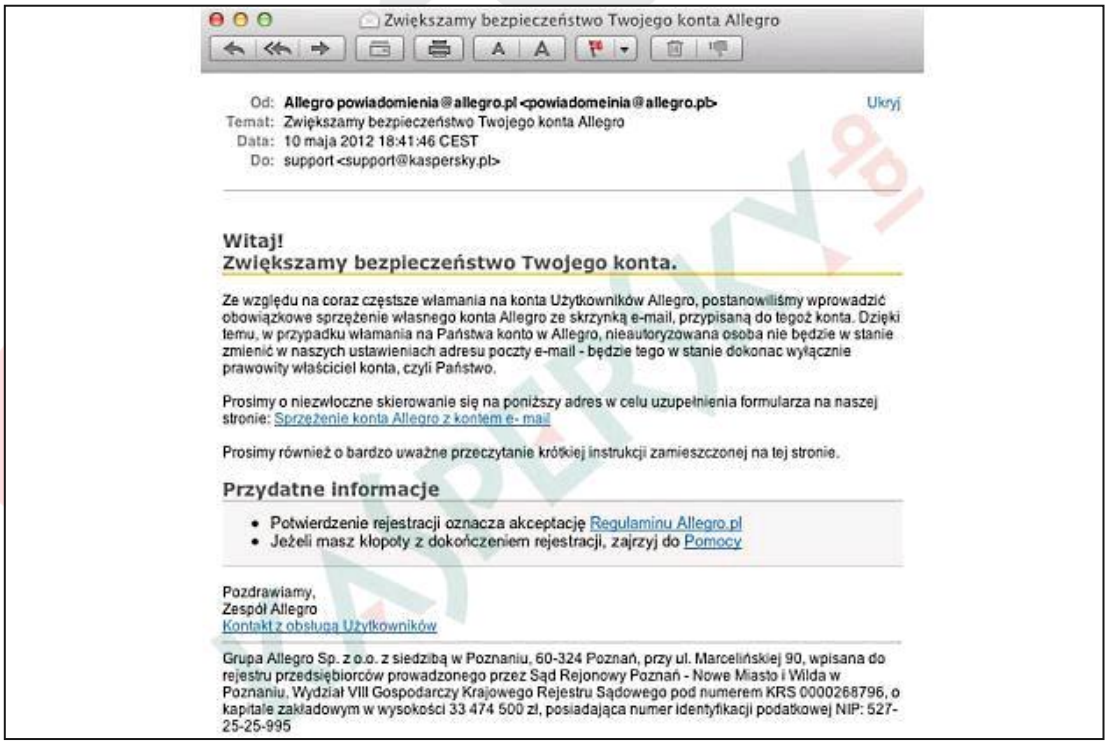
Podane powyżej przykłady odzwierciedlają tylko niektóre z działań stosowanych przez cyberprzestępców. W rzeczywistości ich pomysłowość nie zna granic, dlatego należy być szczególnie ostrożnym przy korzystaniu z Internetu.

Phishing

Phishing polega na wyłudzaniu przez cyberprzestępców prywatnych danych m. in. haseł i loginów, numerów kart kredytowych poprzez e-mail, który do złudzenia przypomina oryginał pochodzący od prawdziwego dostawcy usług. Najczęściej cyberprzestępcy próbują skusić odbiorców do podania swoich danych na spreparowanych stronach podszywających się pod witryny banków i sklepów internetowych.

Wiadomości phishingowe są bardzo profesjonalne i na pierwszy rzut oka wyglądają na prawdziwe, co ilustrują poniższe przykłady.

Przykład 1. Facebook w swoich wiadomościach używa domeny 'facebook.com', a nie 'facebookmail.com



Przykład 2. Nadawca używa fałszywego konta powiadomeinia@allegro.pl (zdjęcie Kaspersky Lab)

Jak można zauważyć, nadawca wiadomości wykorzystał nazwę konta, do złudzenia przypominającą prawdziwą. Adres e-mail, z którego wysłano wiadomość różni się od prawdziwego tylko przestawionymi literami. W ten sposób bardzo często postępują cyberprzestępcy – wykorzystują nieuwagę swoich ofiar, żeby zdobyć dostęp do ich danych i kont, a w przypadku banków do pieniędzy.

Oszustwa i wyłudzenia pieniężne

Oszustwa i wyłudzenia pieniężne następują dopiero po uzyskaniu przez cyberprzestępców danych osobowych ofiary. Jednak nie zawsze jest to konieczne. Szczególnym przypadkiem wyłudzeń pieniężnych, które nie wymagają wcześniejszego zdobycia informacji osobowych są te, które bazują na ludzkiej naiwności. Wśród nich można wyróżnić:

- oferty gwarantujące Internautom osiągnięcie wysokich zarobków w krótkim czasie – poprzez wykupienie specjalnych poradników, zestawów lub narzędzi komputerowych, które w rzeczywistości nie mają żadnej wartości (np. internetowe maszynki do robienia pieniędzy),
- prośba o pomoc polegającą na wpłaceniu dowolnych środków pieniężnych na fałszywe konto fundacji/stowarzyszenia charytatywnego lub osoby „potrzebującej" często wysyłana jako spam, a nawet przez nieświadomych znajomych za pośrednictwem e-mail, komunikatorów lub portali społecznościowych w formie „łańcuszków", w rzeczywistości przekazane pieniądze trafiają na konto oszustów,
- zakup towarów, przedmiotów, biletów po bardzo atrakcyjnych cenach – w rzeczywistości nieistniejących, fałszywych lub wadliwych.

Warto wiedzieć, że 40% wszystkich oszustw Internetowych odbywa się za pośrednictwem portali aukcyjnych (raport MSW). Niezwykle ważna jest tutaj znajomość zasad i reguł bezpiecznego postępowania przy wyborze dostawcy towarów i usług, które zamierzamy kupić.

Szkodliwe oprogramowanie (Malware)

Malware jest skrótem od malicious software – z angielskiego złośliwe oprogramowanie.

Szkodliwe oprogramowanie może występować m. in. w postaci wirusów i oprogramowania szpiegującego (spyware), które instaluje się na komputerze, telefonie lub tablecie bez wiedzy użytkownika. Form złośliwego oprogramowania jest znacznie więcej – w tym np. trojany, keyloggery, rootkity, dialery, itd. Nie sposób jest wymienić i opisać wszystkie z nich. Należy pamiętać, że tego typu programy mogą powodować uszkodzenia sprzętu bądź danych. Złośliwe oprogramowanie w wielu przypadkach wykorzystywane jest do śledzenia i kontrolowania aktywności Internautów w sieci. Cyberprzestępcy wykorzystują złośliwe oprogramowanie przede wszystkim w celu kradzieży informacji osobistych, wysyłania spamu a także do oszustw i innego rodzaju przestępstw Internetowych np. ataków hakerskich przy wykorzystaniu zainfekowanych komputerów – tzw. komputerów zombie.

Szkodliwe oprogramowanie bardzo często jest wprowadzane do komputerów na życzenie Internautów – poprzez ściągnięcie na dysk zainfekowanych aplikacji, filmów, gier, utworów muzycznych, wygaszaczy ekranów itp., pochodzących z niepewnych źródeł (torrenty, serwisy typu rapidshare). Innym źródłem pochodzenia szkodliwego oprogramowania mogą być zarażone komputery połączone w tej samej sieci oraz załączniki wiadomości e-mail pochodzących z nieznanych źródeł.

Niestety, coraz częściej do zainfekowania komputera wystarczy najzwyklejsza wizyta na pozornie bezpiecznej stronie Internetowej. Wszystko za sprawą ataków driver -by download.

Drive-by download

Drive-by download jest jedną z najbardziej popularnych metod stosowanych przez cyberprzestępców, gdyż do sprowadzenia złośliwego oprogramowania na komputer Internauty, wystarczy jego wizyta na zarażonej stronie. Ataki typu Drive-by download są szczególnie niebezpieczne, gdyż ich wykrycie jest praktycznie niemożliwe nawet dla bardzo doświadczonych użytkowników Internetu.

Z technicznego punktu widzenia ataki typu drive-by download występują wtedy, gdy użytkownik trafi na witrynę, aplikację lub inny element przeglądarki internetowej, który został zmodyfikowany poprzez dodanie złośliwego kodu przez cyberprzestępców (najczęściej wykorzystują oni luki w oprogramowaniu). W momencie załadowania się zarażonej strony równolegle następuje niewidoczne przekierowanie do szkodliwego adresu, a następnie pobranie i instalacja szkodliwego oprogramowania. Cały proces jest dla użytkownika niewidoczny i nie wymaga żadnej interakcji, ponieważ nie zostają wyświetlone żadne okienka, zapytania czy ostrzeżenia.

Bardzo często Internautów zachęca się do odwiedzania zainfekowanych stron za pośrednictwem linków znajdujących się w spamie rozsyłanym drogą elektroniczną, na forach internetowych oraz na portalach społecznościowych. Warto tutaj dodać, że większość ataków typu drive-by download jest przeprowadzana przez osoby niemające dużej wiedzy i umiejętności informatycznych. Osoby te po prostu zakupują lub pobierają z Internetu gotowe zestawy narzędzi przeznaczonych do tego typu ataków. W praktyce na ataki tego typu najbardziej narażone są osoby, które mają nieaktualne wersje systemów operacyjnych, oprogramowania, a w szczególności przeglądarek Internetowych.

Ponadto, według specjalistów SkanSafe, ataki typu drive-by download w ponad połowie przypadków są przeprowadzane za pośrednictwem legalnych stron internetowych, w których cyberprzestępcy znaleźli i wykorzystali luki w zabezpieczeniach. Należy pamiętać, że nie ma możliwości uniknięcia tego typu zagrożeń bez stosowania odpowiednich zabezpieczeń i praktyk.

Warto także wiedzieć, że popularną metodą stosowaną przy kierowaniu użytkowników na zainfekowane strony Internetowe jest tzw. typosquatting, który polega na wykorzystaniu przez cyberprzestępców adresów zbliżonych do popularnych serwisów. Typosquatting bazuje na wykorzystaniu błędów literowych popełnianych przez Internautów, podczas wpisywania z ręki adresu strony Internetowej w przeglądarce internetowej – przykład: superbank.pl, a suprbank.pl. Internauta, który popełni literówkę we wpisywanym adresie Internetowym może trafić na strony z reklamami, strony zainfekowane, a w najgorszym przypadku na stronę phishingową do złudzenia przypominające tą, na którą w rzeczywistości zamierzał wejść – np. fałszywą stronę banku.

Ataki hakerskie

Ataki hakerskie są zjawiskiem polegającym na obejściu przez cyberprzestępców zabezpieczeń systemów, witryn i portali Internetowych w celu m. in.:

- uzyskania chronionych informacji – w tym najczęściej baz danych; w Polsce wiele popularnych serwisów miało już problem z wyciekami danych – wśród nich między innymi Allegro, Nasza Klasa, Wykop.pl, Filmweb; na świecie najbardziej znanym jest przypadek Playstation Network, w którym wyciekły dane milionów użytkowników na całym świecie w tym 400 tys. Polaków,
- kradzieży baz danych oraz informacji stanowiących własności użytkowników indywidualnych, jak również stanowiących tajemnicę firm i instytucji,

- kasowania danych znajdujących się na dyskach twardych komputerów,
- unieruchomienia komputerów podłączonych do sieci lub też łączy internetowych
- włamania do kont pocztowych – serwerów pocztowych,
- włamania do komputerów indywidualnych użytkowników oraz komputerów będący własnością firm i instytucji.

Należy pamiętać, że cyberprzestępcy mogą wykorzystać skradzione dane na niekorzyść użytkowników Internetu, stąd tak ważne jest stosowanie zaleceń fundacji Veracity, które zostały opisane w kolejnym rozdziale.

Utrata prywatności

Gwałtowny rozwój sieci społecznościowych oraz malejąca grupa osób dbających o swoją prywatność stała się wymarzoną perspektywą dla cyberprzestępców, a także okazją do wymyślenia i stosowania przez nich nowych metod prowadzenia ataków na użytkowników. Praktycznie, co kilka dni pojawiają się nowe zagrożenia dla użytkowników portali społecznościowych, w formie profili i aplikacji zarażających nieostrożnych internautów szkodliwym oprogramowaniem. Na przykład eksperci z firmy Trend Micro wykryli oszustów na Facebooku, którzy zachęcali do stosowania walentynkowych motywów na profilach. Aplikacja ta zawierała złośliwy kod, który uruchamiał skrypt wyświetlający reklamy i próbujący wykraść numer telefonu komórkowego.

Innym przykładem zagrożeń społecznościowych są tak zwane farmy fanów. Polega to na przyciągnięciu do strony o popularnej tematyce możliwie jak największej liczby zainteresowanych/fanów, którzy dołączają do grupy lub wciskają popularny w ostatnim czasie przyciski „lubię to”. Następnie powstałą w ten sposób liczną bazę użytkowników cyberprzestępcy odsprzedają za pośrednictwem Internetu.

Innym, ale bardzo popularnym sposobem zarażenia komputerów Internautów złośliwym oprogramowaniem jest sposób polegający na utworzeniu przez cyberprzestępcę zarażonej strony z ciekawą informacją, zdjęciem lub filmem i udostępnieniu odnośnika do tej strony na portalu społecznościowym. Nieostrożni użytkownicy wciskając odnośniki narażają się na atak typu drive-by download.

Ponadto, należy pamiętać, że samo założenie konta w portalu społecznościowym wiąże się z udostępnieniem w sieci informacji, które zostaną tam na zawsze. Wśród nich można wyróżnić:

- imię i nazwisko,
- datę urodzenia/wiek,
- numery komunikatorów,
- numer telefonu komórkowego,
- zdjęcia, filmy,
- adres e-mail,
- miejsca nauki/pracy,
- wykształcenie
- listę znajomych/członków rodziny.

Nawiązując do początku rozdziału, cyberprzestępcy znają bardzo dużo sposobów na wykorzystanie tego typu informacji.

Oprócz wymienionych wcześniej zagrożeń można wyróżnić jeszcze cyberstalking, czyli zjawisko powtarzającego się uporczywego nękania osoby poprzez różne formy naruszenia wolności osobistej i prywatności. Najbardziej narażone na tę formę cyberprzestępstwa są kobiety. Według badań, to one stanowią ponad 70% ofiar prześladowców. Cyberstalking to natrętne wirtualne próby komunikowania się z drugą osobą wbrew jej woli poprzez uporczywe nękanie, wykorzystujące wiadomości e-mail, komunikatory, fora internetowe oraz portale społecznościowe.

Zalecenia fundacji Veracity dotyczące bezpiecznego korzystania z Internetu

W tym rozdziale przedstawiono zestaw zaleceń i dobrych praktyk fundacji Veracity, które zapewnią Internautom bezpieczne korzystanie z Internetu. **Stosowanie się do zaleceń:**

- chroni przed utratą danych osobowych i haseł,
- ogranicza do minimum ryzyko utraty prywatności,
- pozwala uniknąć oszustw internetowych,
- pozwala skutecznie zabezpieczyć komputery przed szkodliwym oprogramowaniem.

1. Ostrożne korzystanie z portali społecznościowych

Wszystkie informacje, które zostają opublikowane w Internecie (zdjęcia, obrazy, komentarze, rozmowy) mogą zostać tam na zawsze. Całkowite usunięcie ich z sieci jest niemożliwe, ponieważ w każdej chwili ktoś inny może je skopiować i udostępnić w innej lokalizacji. Ponadto, właściciele portali takich jak Facebook gromadzą informacje w swoich archiwach, nawet, jeśli zostały one usunięte przez użytkownika. Nie należy podawać informacji, poprzez które można zostać zidentyfikowanym przez niechciane osoby.

Oto lista zaleceń fundacji Veracity:

- modyfikacja listy ustawień dotyczących prywatności i bezpieczeństwa (najczęściej w menu „opcje" lub „ustawienia" w zakładce „bezpieczeństwo"),
- ograniczenie dostępu do publikowanych i udostępnianych informacji tylko dla użytkowników, którzy powinni je widzieć,
- uruchomienie szyfrowania połączeń:
    - przykład:

      Facebook: konto -> ustawienia konta -> bezpieczeństwo -> zaznacz opcje: bezpieczne przeglądanie -> zapisz zmiany

- wyłączenie usług wykorzystujących dane osobowe:
    - przykład:

Reklamy na Facebooku: konto -> ustawienia konta -> reklama na facebooku -> zaznacz opcje: nikt

- niepublikowanie numeru telefonu, adresu zamieszkania, adresu e-mail, adresu miejsca pracy itp. (jeśli znajomi użytkownika będą potrzebować takich danych, mogą o nie poprosić),
- unikanie aplikacji zbierających dane o użytkowniku, w szczególności:
  - aplikacji udostępniających zawartość dopiero po ujawnieniu swoich danych osobowych,
    - przykład:

      Facebook – mój kalendarz,
  - podejrzanych ofert i konkursów pochodzących również od znajomych,
    - przykład:

      fałszywa promocja na Facebooku – obietnica otrzymania darmowej bluzy z logiem Facebooka dla pierwszych 300 tysięcy użytkowników, którzy „polubią promocję", na promocję nabrało się ponad 100 tysięcy osób automatycznie udostępniających swoje dane osobowe,
- nie wciskanie podejrzanych linków pochodzących od nieznajomych (patrz drive by download),
- wylogowywanie się przed odejściem od komputera, zapewniające brak dostępu niepowołanym osobom do prywatnej korespondencji.

2. Unikanie sond, kwestionariuszy, konkursów wzbudzających niepewność

„Jeśli coś jest zbyt piękne, żeby było prawdziwe, to prawdziwe nie jest" – należy postępować zgodnie z tą zasadą. Popularnym procederem występującym w sieci jest wprowadzanie użytkowników Internetu w błąd lub ukrywanie istotnych informacji, dlatego:

- należy czytać regulaminy – oszuści Internetowi w celu uniknięcia konsekwencji za swoje czyny stosują odpowiednio spreparowane regulaminy zwalniające ich z jakiejkolwiek prawnej odpowiedzialności za treści publikowane na stronach internetowych,
  - przykład:

  Domowy system zarabiania – strona oferująca narzędzie do zarabiania pieniędzy przez Internet opisująca przykłady ludzi, którzy odnieśli sukces (cytat z regulaminu: „informacje zawarte na stronie DomowySystemZarabiania.pl są wyłącznie do celów rozrywkowych")

- przykład:

  konkursy Premium SMS – wysyłka pierwszego darmowego SMSa jest jednoznaczna z akceptują regulaminu obejmującego płatne SMSy zwrotne,

- należy czytać polityki prywatności – tylko tak dowiemy się, w jaki sposób dostawca usług będzie mógł wykorzystać udostępnione mu dane osobowe,
- należy unikać konkursów, sondaży i ankiet nie zawierających:
  - informacji na temat danych adresowych i kontaktowych z właścicielem lub podmiotem odpowiedzialnym za realizację usług (sam formularz zgłoszeniowy nie jest wystarczający),
  - regulaminów,
  - polityk prywatności.

3. Bezpieczne korzystanie z poczty e-mail

Wiadomości e-mail wysyłane przez cyberprzestępców mogą przybierać formę i treść łudząco podobną do prawdziwych wiadomości wysyłanych przez zaufanych adresatów. Ataki przy wykorzystaniu odpowiednio spreparowanych wiadomości należą do najczęstszych w sieci. Dlatego przy korzystaniu ze skrzynki e-mail należy stosować się do poniższych wskazówek:

- nie należy odpowiadać na wiadomości e-mail pochodzące z niepewnych źródeł,
- nie należy sprawdzać linków zawartych w ww. wiadomościach – wiadomości mogą wydawać się wiarygodne, ale gdy treść w nich zawarta dotyczy np. prośby o zmianę hasła do konta bankowego należy dokładnie sprawdzić kim jest nadawca (np. zadzwonić do obsługi banku),

Jak rozpoznać fałszywe maile:

- fałszywe maile występują najczęściej w formie bezosobowej, ponieważ wysyłane są masowo do dużej ilości adresatów – banki kierują korespondencję bezpośrednio do zainteresowanej osoby,
- w temacie fałszywej wiadomości mogą pojawić się słowa, które wyglądają, jakby popełniono w nich przypadkowe błędy: cyfry zamiast liter, wielkie litery w środku wyrazu, błędy ortograficzne i gramatyczne, wszystko to, ma na celu ominięcie filtrów antyspamowych,
- w treści fałszywej wiadomości najczęściej znajduje się link lub załącznik, oraz prośba do skorzystania z niego w ramach dokonania, np. aktualizacji swoich danych, zmiany hasła itp.

4. Instalacja i odpowiednia konfiguracja oprogramowania antywirusowego

Dobry program antywirusowy jest niezbędny do zabezpieczenia komputera przed złośliwym oprogramowaniem rozsyłanym za pośrednictwem Internetu. Przy tym należy pamiętać, że programy tego typu nigdy nie dadzą pełnej gwarancji bezpieczeństwa, ponieważ to od zachowania użytkownika Internetu zależy jego bezpieczeństwo. Aby maksymalnie zwiększyć ochronę komputera należy zainstalować program antywirusowy. Na rynku dostępnych jest wiele bezpłatnych narzędzi antywirusowych. Płatne zapewniają dodatkowe funkcjonalności. Warto pamiętać, że wersje płatne zapewniają większe bezpieczeństwo użytkownikom poprzez zestaw dodatkowych narzędzi badających zawartość strony docelowej, zanim użytkownik zostanie na nią przekierowany.

Przykłady darmowego oprogramowania antywirusowego:

- avast! Free Antivirus http://www.avast.com/pl-pl/free-antivirus-download
- AVG Anti-Virus Free http://free.avg.com/pl-pl/strona-glowna
- Avira Free Antivirus http://www.avira.com/en/avira-free-antivirus
- Panda Cloud Antivirus http://www.cloudantivirus.com/en/

Oprócz wyboru i instalacji odpowiedniego programu antywirusowego konieczna jest jego konfiguracja, przy tym należy pamiętać o:

- włączeniu ochrony w czasie rzeczywistym – opcja ta zapewnia stałą ochronę komputera dzięki sprawdzaniu obecności wirusów i innych zagrożeń bezpieczeństwa na komputerze, zapewnia również zaawansowaną ochronę, aktywnie wykrywając nieznane zagrożenia bezpieczeństwa na komputerze,
- regularnym skanowaniu komputera – sama instalacja oprogramowania antywirusowego – szczególnie wersji darmowej nie zapewnia bezpieczeństwa systemu jeśli nie będziemy go regularnie skanowali. Jak wspomniano wcześniej, popularnym sposobem zarażania komputerów złośliwym oprogramowaniem są ataki typu drive by download, niemożliwe do wykrycia „gołym okiem”, tylko regularne skany mogą wykryć zagrożenia,
- stworzeniu harmonogramu regularnych skanów całego systemu
    - przykład: Avast: skanuj komputer -> skanuj natychmiast -> pełne skanowanie systemu (ustawienia) -> harmonogram

5. Ignorowanie fałszywych powiadomień antywirusowych

Jak unikać fałszywego oprogramowania antywirusowego (ang. scareware):

- pobieraj programy antywirusowe bezpośrednio ze stron producentów lub z dużych i sprawdzonych portali (np. dobre programy.pl),
- nie wierz komunikatom informującym o infekcji systemu i jednocześnie konieczności instalacji dodatkowych programów antywirusowych.

Fałszywe programy antywirusowe nie posiadają konkretnej marki czy nazwy, z którą można by je kojarzyć. Zamiast tego w ich nazwach stosowane są popularne słowa kluczowe jak: Antivirus2012, Security, SpyGuard.

6. Instalacja zapory ogniowej (tzw. Firewall)

Zapora ogniowa filtruje połączenia zarówno przychodzące, jak i wychodzące z komputera oraz blokuje potencjalnie niebezpieczne aplikacje. Na komputerach z systemami operacyjnymi Windows zapora taka jest domyślnie zainstalowana i włączona. Ponadto, niektóre z pakietów antywirusowych zawierają firewalla. W sytuacji braku zapory ogniowej należy ją koniecznie zainstalować.

- Przykłady zapór sieciowych:
  - Comodo Personal Firewall
  - PC Tools Firewall Plus
  - ZoneAlarm PRO

7. Regularne aktualizacje systemu i oprogramowania

Internauci posiadający na komputerze nieaktualne oprogramowanie są dużo bardziej narażeni na ataki z sieci niż internauci, którzy aktualizują programy i system regularnie. Wynika to z faktu, że im dużej dana wersja oprogramowania jest dostępna w sieci, tym większe prawdopodobieństwo, że crackerzy znajdą luki w zabezpieczeniach i wykorzystają je. W tym celu przeglądarki Internetowe bardzo często wypuszczają nowe łatki aktualizacyjne.

- Szczególnie należy dbać o aktualizację systemu operacyjnego, przeglądarki, wtyczek przeglądarkowych, plug-inów – Java, Flash i AdobeAcrobat.

Najskuteczniejszym sposobem posiadania najnowszej i aktualnej wersji oprogramowania i systemu operacyjnego jest uruchomienie automatycznych aktualizacji – pozwala to uniknąć zaniedbań w tej kwestii – aczkolwiek nie każdy program i sterowniki można aktualizować automatycznie. Można to obejść na dwa sposoby:

- poprzez pobranie oprogramowania służącego sprawdzaniu dostępności aktualizacji i automatycznej ich instalacji
    - przykład:
        - program „secunia”
- poprzez dokonywanie instalacji ręcznych, przy czym należy pamiętać, że najpewniejszym źródłem, z którego należy pobierać aktualizacje oprogramowania jest jego producent. Nie należy pobierać uaktualnień systemu i programów z innych stron, gdyż mogą być one już nieaktualne, uszkodzone albo zarażone.

8. Utworzenie i synchronizacja kopii zapasowej danych

Utrata danych, które są przechowywane na komputerze z reguły występuje w najmniej oczekiwanym momencie, dlatego należy w regularnych odstępach czasu tworzyć kopię zapasową danych, które są dla nas ważne i wartościowe. W ramach tworzenia kopii danych należy:

- ustalić harmonogram aktualizacji kopii zapasowej – np. co miesiąc lub częściej,
- wybrać formę zapisu danych:
    - dysk zewnętrzny (urządzenie przenośne),
    - serwer (w chmurze),
- dokonywać regularnych aktualizacji kopii zapasowej.

W przypadku użytkowania systemu Windows warto skorzystać z Centrum synchronizacji.

Podczas każdej synchronizacji plików pomiędzy lokalizacjami (na przykład pomiędzy komputerem i urządzeniem przenośnym) w Centrum synchronizacji porównywane są pliki w obu lokalizacjach, w celu uaktualnienia wprowadzonych zmian – w ten sposób zawartość danych na urządzeniu przenośnym będzie taka sama jak na dysku sieciowym. W systemach Windows synchronizacji można dokonać:

- Windows 7: Start -> Wszystkie programy-> Akcesoria-> Centrum synchronizacji
- Windows Xp: Start -> Wszystkie programy-> Akcesoria-> synchronizuj

9. Ostrożność przy pobieraniu plików

Pliki pobierane do komputera z niepewnych źródeł internetowych mogą zawierać bardzo niebezpieczne dla komputera złośliwe oprogramowanie. Należy zachować szczególną ostrożność i środki bezpieczeństwa przy pobieraniu plików. W tym celu zaleca się:

- pobieranie plików z pewnych źródeł, m. in.
  - strony producentów,
  - specjalistyczne duże portale Internetowe,
- ostrożność przy ściąganiu plików z torrentów, forów i serwisów typu „rapidshare" gdyż zdarza się, że zawierają one ukryte złośliwe oprogramowanie (najnowsze filmy, gry, programy, sterowniki – często zawierają złośliwy kod i infekują komputery), pobrane z takich źródeł pliki należy skanować w programie antywirusowym przed rozpakowaniem, otwarciem lub instalacją ich zawartości

10.Weryfikacja certyfikatów

Sprawdzanie ważności i rzetelności certyfikatów stron internetowych (szczególnie banków) pozwala uniknąć nieprzyjemnych zdarzeń i oszustw. Należy pamiętać, że fałszywe strony Internetowe bardzo często nie posiadają żadnych certyfikatów. Dlatego przed zalogowaniem do banku internetowego należy kliknąć na symbol zamkniętej kłódki na pasku przeglądarki, a następnie zweryfikować:

- czy nazwa właściciela serwera jest poprawna,
- czy certyfikat został wydany przez znane centrum,
- czy przeglądarka nie zgłasza jakichkolwiek zastrzeżeń do certyfikatu (np. utrata ważności).

11.Unikanie typosquattingu

Aby uniknąć zjawiska typosquattingu (oszustwo wykorzystujące typowe błędy literowe popełniane w trakcie wpisywania adresów internetowych) szczególnie ważna jest ostrożność przy wpisywaniu adresu

Internetowego. Każda pomyłka w nazwie popularnych stron internetowych (portali informacyjnych, banków, wyszukiwarek) może spowodować otwarcie niechcianych stron Internetowych, a w gorszym przypadku ściągnięcia z nich szkodliwego oprogramowania.

12.Stosowanie silnych haseł

Silne hasła są bardzo ważne do poprawnego zabezpieczenia danych, które chronią. Jeśli hasło jest zbyt proste cyberprzestępcy mogą je po prostu odgadnąć lub skorzystać z listy najczęściej stosowanych haseł, do których należą: „qwerty", „haslo", „imię dziewczyny", „imię psa", itp. W Internecie istnieją także narzędzia do łamania prostych haseł. Niewiele trzeba żeby złamać proste hasło, dlatego należy pamiętać o tym, że hasło:

- powinno składać się z minimum 8 znaków,
- nie może być związane z datą urodzenia użytkownika, jego imieniem, nazwiskiem, numerem telefonu, bądź innymi słowami bezpośrednio kojarzącymi się z użytkownikiem,
- nie powinno być wyrazem występującym w słownikach, zarówno polskich, jak i w językach obcych
- nie powinno być również nazwiskiem lub pseudonimem znanej osoby, nazwą grupy muzycznej, tytułem filmu czy piosenki,
- nie powinno składać się z ciągu tych samych cyfr czy liter lub sekwencji znaków występujących obok siebie na klawiaturze komputera.

Należy mieć na uwadze, że tworzenie długiego hasła zwiększa jego bezpieczeństwo, jednak bardziej istotną kwestią jest stopień skomplikowania sekwencji. W tym celu powinno się:

- używać kombinacji WIELKICH i małych liter,
- w treść hasła stosować cyfry,
- stosować znaki specjalne (?/;:"{}-+!@#),
- stosować polskie znaki (ą, ę, Ś, Ź, Ż),
- zastępować litery znakami specjalnymi bądź cyframi z nimi kojarzonymi.

Etapy postępowania	Przykłady	
Proste zdanie łatwe do zapamiętania	W 2012 roku byłem na wakacjach w Chorwacji	Majowie przepowiedzieli koniec świata pod koniec 2012 roku
Ciąg znaków przy użyciu pierwszych liter wyrazów	W2012rbnwwC	Mpkśpk2012r
Zmiana wielkości liter w stworzonej sekwencji	w2012RBNwwc	MPKśpK2012R
Zamiana liter na cyfry i znaki specjalne	\/\/dzjdR8Nww<	MPKśpKZOIIIR

Ważne jest także:

- **stosowanie różnych haseł w różnych miejscach** – należy stosować różne hasła do różnych serwisów, w których posiadamy konta; stosowanie takiego zabezpieczenia pozwala ograniczyć ryzyko przejęcia dostępu do różnych konta przez osoby niepożądane w przypadku przejęcia hasła do jednego z nich. Jest to niezwykle istotny aspekt; szczególnie należy pamiętać o różnych hasłach do: poczty e-mail, konta w banku, konta na portalach społecznościowych, konta na portalach aukcyjnych,
- **zmiana haseł w regularnych odstępach czasu** – im częściej zmieniane jest hasło tym lepiej, natomiast nie należy popadać w skrajność, zaleca się ustalenie harmonogramu zmiany haseł co miesiąc,
- **modyfikacja haseł** – modyfikacja nie powinna polegać na przekształceniu bądź dopisaniu kolejnej cyfry bądź innego znaku np. (hasło, hasło1, hasło1234), tylko w minimalnym stopniu zwiększa to efektywność zabezpieczeń,
- w przypadku długich, bezpiecznych haseł dozwolone jest stosowanie niezmiennej „bazy” czyli stałej części hasła oraz części ulegającej zmianie, jednak w bardziej zaawansowanej formie niż opisana powyżej.

13. Szyfrowanie danych (ssl)

Szyfrowanie jest kluczem do zapewnienia bezpieczeństwa prywatnych danych użytkownika Internetu. Wysyłanie wiadomości e-mail, dzielenie się zdjęciami i filmami, używanie sieci społecznościowych, logowanie do konta bankowego to czynności, które wymagają przesyłania dużej ilości informacji osobistych przez Internet. Informacje te są przechowywane na serwerze – komputerze, który gromadzi przesyłane treści. Wiele stron internetowych, takich jak strony logowania banków, używa szyfrowania aby chronić informacje, które „podróżują" z komputera użytkownika do ich serwera. Tylko strony szyfrowane zapewniają, że dane te nie zostaną przechwycone.

Aby rozpoznać czy strona jest szyfrowana, należy spojrzeć na adres strony Internetowej. Jeśli zaczyna się on od „https" to znaczy że strona jest zaszyfrowana (s to skrót od secure).

Aby wymusisz stosowanie szyfrowania ssl na stronach internetowych można używać pluginów przeglądarkowych, które zmuszają przeglądarkę internetową do szyfrowania informacji na popularnych stronach internetowych, które często nie są szyfrowane. Jednakże należy pamiętać, że pluginy te nie chronią użytkowników na wszystkich stronach Internetowych

- Przykłady pluginów:
  - Force-TLS
  - HTTPS-Everywhere

14. Bezpieczne korzystanie z publicznych hot-spotów

Kafejki Internetowe, czytelnie, uczelnie, dworce, hotele, lotniska, punkty ksero i inne miejsca publiczne oferują wygodny dostęp do Internetu za pośrednictwem bezpłatnego WI-FI z tzw. hotspotów. Niestety prawie zawsze sieci te są niezabezpieczone i narażają użytkowników na niebezpieczeństwo przechwycenia poufnych informacji, haseł i loginów. Dowiedli tego dziennikarze BBC, którzy za pomocą bezpłatnych narzędzi dostępnych w Internecie bez najmniejszych problemów przechwycili hasła i loginy pocztowe osób korzystających z bezpłatnych hot-spotów w miejscach publicznych. Dlatego przy częstym korzystaniu z niezabezpieczonych sieci publicznych należy:

- unikać logowania do portali społecznościowych, do kont bankowych, do skrzynki mailowej,
- korzystać z szyfrowania *ssl przy konieczności wykonania powyższych operacji,

- wyłączyć udostępnianie plików podczas korzystania z publicznego punktu dostępu bezprzewodowego (udostępnianie plików można wyłączyć w menu ustawień sieciowych systemu operacyjnego),
- ograniczyć ilość poufnych danych osobistych przechowywanych w komputerach i urządzeniach przenośnych lub zabezpieczyć odpowiednie pliki hasłem.

15. Zabezpieczenie urządzeń mobilnych

Telefony komórkowe i tablety coraz częściej stają się obiektem ataków cyberprzestępców, o czym świadczy rosnąca ilość szkodliwego oprogramowania typu malware skierowanego właśnie do użytkowników tych urządzeń. Niestety, pomimo dużego zagrożenia zaledwie jedna czwarta telefonów komórkowych i tabletów jest odpowiednio chroniona.

Należy przestrzegać zaleceń Veracity również przy korzystaniu z tego typu urządzeń. W tym szczególnie ważne są:

- Regularne aktualizacje oprogramowania i systemu operacyjnego
- Instalacja i odpowiednia konfiguracja programu antywirusowego i firewalla
- korzystanie z zaufanych źródeł do pobierania plików

16. Ograniczenie zaufania

Należy pamiętać, że nie każdy w Internecie jest tym, za kogo się podaje. Dlatego w przypadku wątpliwości, co do wiarygodności drugiej strony (np. sklepu Internetowego) należy weryfikować ją poprzez:

- sprawdzenie aktualności uzyskanych certyfikatów,
- przeszukanie katalogów firm w których dany podmiot może figurować,
- wyszukiwarki internetowe,
- serwisy z opiniami,
- fora internetowe

17. Dodatkowe formy zabezpieczenia kont bankowych

Wśród opcjonalnych form zabezpieczenia kont bankowych w Polsce można wskazać m. in.:

- karty kodów jednorazowych
- hasła SMS
- TOKENY

W zależności od banku możliwości zabezpieczenia kont są różne. Należy koniecznie sprawdzić jakie możliwości oferuje bank na jego stronie Internetowej lub poprzez infolinię i maksymalnie wzmocnić zabezpieczenie konta.

18. Blokowanie popupów i wyskakujących reklam

Wszystkie popularne przeglądarki internetowe umożliwiają blokowanie wyskakujących okienek – tzw. Pop-upów. Aby tego dokonać należy włączyć w przeglądarce blokowanie wyskakujących okienek.

- Przykład:
  - Mozilla: narzędzia -> opcje -> treść -> zablokuj wyskakujące okienka
  - Explorer: narzędzia -> opcje Internetowe -> prywatność -> włącz blokowanie wyskakujących okienek.
- Aby ograniczyć ilość okienek i reklam wyświetlanych podczas przeglądania Internetu można zainstalować także darmową wtyczkę przeglądarkową „Adblock Plus" dostępną na stronie producenta

Podsumowanie

Na podstawie danych statystycznych i najnowszych trendów w obszarze cyberprzestępczości można spodziewać się, że Internet będzie miejscem stwarzającym coraz większą ilość zagrożeń dla użytkowników sieci. Na niebezpieczeństwo są narażone przede wszystkim osoby nieświadome zagrożeń płynących z Internetu i nieznające sposobów zabezpieczenia się przed nimi. To najczęściej one padają ofiarą cyberprzestępców. Dlatego tak ważna jest znajomość zagrożeń i zaleceń Veracity przygotowanych w niniejszym kompendium. Zagrożeń jest wiele, stąd niezwykle ważne jest zachowanie ostrożności w wirtualnym świecie. Bo tak, jak w rzeczywistości również w Internecie można paść ofiarą przestępców.

Odesłania

- Internet Security Threat Report: http://aa-download.avg.com/filedir/news/2011_09_09_Future%20Poll_Cybercrime_Futures.pdf
- Raport Cybercrime Futures: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf -
- Raporty dot. obszarów bezpieczeństwa G-Data: http://www.gdata-software.com/security-labs/information/whitepaper.html -
- Global IT security Risks: http://www.kaspersky.com/images/kaspersky_global_it_security_risks_survey-10-100468.pdf -
- Raport o stanie bezpieczeństwa w Polsce w 2010 roku: http://www.bip.ms.gov.pl/pl/dzialalnosc/statystyki/download,33,0.html
- Phishing as Tragedy of the Commons: http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf -
- Data breach security Report: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf