Ministerstwo Spraw Wewnętrznych i Administracji

Data publikacji 09.02.2016

9 lutego – dzień bezpiecznego internetu

Jak korzystać z Internetu, aby nie stać się ofiarą przestępstwa? Co znaczą słowa „phishing" i „pharming"? 9 lutego po raz dwunasty obchodzony jest DBI, czyli „Dzień Bezpiecznego Internetu". W tym roku odbywa się pod hasłem: „Lepszy internet zależy od Ciebie".

Internet to nie tylko źródło ciekawych informacji czy sposób na załatwienie ważnych spraw, ale także – niestety – potencjalna pułapka, gdyż nieznajomość metod stosowanych przez internetowych przestępców może narazić użytkownika sieci na utratę danych lub pieniędzy. W tym roku po raz dwunasty obchodzimy w Polsce „Dzień bezpiecznego Internetu".

Chociaż „Dzień bezpiecznego Internetu" został zainicjowany przez Komisję Europejską i ma zwrócić uwagę na kwestię bezpiecznego dostępu dzieci i młodzieży do sieci, to przestrzeganie zasad bezpieczeństwa podczas korzystania z Internetu obowiązuje wszystkich, bez względu na wiek.

Przestępcy działający w sieci często posługują się metodą tzw. phishingu. Phisher rozsyła pocztą elektroniczną wiadomości, które łudząco przypominają oficjalną korespondencję z banku, serwisu aukcyjnego lub innych portali. Zazwyczaj informują one o konieczności ponownego reaktywowania konta. W mailu znajduje się odnośnik do strony, na której można dokonać ponownej aktywacji konta. Pomimo że witryna z wyglądu przypomina prawdziwą stronę, w rzeczywistości jest to przygotowana przez przestępcę pułapka. Niczego nieświadomi użytkownicy ujawniają swoje dane uwierzytelniające (kody pin, identyfikatory i hasła).

„Robaki" i pharming

Innym sposobem działania cyberprzestępców jest wykorzystywanie złośliwego oprogramowania, zwanego w zależności od swojej formy: robakami, końmi 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.

Pamiętaj, że...

- nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila;

- trzeba regularnie uaktualniać system i oprogramowanie;
- warto zaopatrzyć swój komputer w program antywirusowy, który ostrzeże nas przed niebezpieczeństwem;
- 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;
- jeśli podejrzewasz, że odwiedzana przez Ciebie witryna jest fałszywa, natychmiast zawiadom policję lub pracowników danego banku odpowiedzialnych za jego funkcjonowanie w sieci.

Pilnuj swoich haseł

Jedną z podstawowych zasad, jakich należy przestrzegać, aby zabezpieczyć swoje dane, jest używanie haseł składających się z małych i wielkich liter, cyfr i znaków specjalnych, o długości powyżej 8 – 10 znaków. Warto również zmieniać je co pewien czas, zwłaszcza po wykryciu przez program antywirusowy złośliwego oprogramowania. Nie należy zapisywać haseł i pinów w nieszyfrowanych plikach tekstowych na twardym dysku. Jeżeli korzystamy w domu z sieci bezprzewodowej (WiFi), odpowiednio skonfigurujmy router. Przy kupnie routera sugerujmy się nie tyle ceną, co możliwością szyfrowania WPA czy WPA2.

Zakupy w sieci

Zdarza się, że zamiast zamówionego na portalu aukcyjno-ogłoszeniowym towaru, w paczce niepełnowartościowe lub inne przedmioty. Jeśli ktoś otrzymał zapłatę za towar i nie wysłał go zamawiającemu, popełnił wyłudzenie, czyli nic innego jak oszustwo. Za taki czyn kodeks karny przewiduję karę nawet do 8 lat pozbawienia wolności.

Co powinno obudzić naszą czujność? Przede wszystkim niska cena, a także negatywne komentarze na temat sprzedającego. Ważne jest także to, od kiedy sprzedawca jest zalogowany w serwisie i ile osób korzystało z jego usług. Jeśli sprzedającym jest firma, warto sprawdzić, czy rzeczywiście istnieje. Potwierdzajmy wygranie licytacji, ale z wpłatą pieniędzy poczekajmy kilka dni, żeby upewnić się, czy wszystko jest w porządku. Opóźni to czas dostawy, ale w przypadku gdy konto firmy na portalu aukcyjnym zostało przejęte przez osobę podszywającą się, zmniejszamy ryzyko. W ciągu tych kilku dni prawdziwy właściciel zorientuje się i powiadomi portal aukcyjny, a oni nas. Koniecznie gromadźmy też całą korespondencję ze sprzedającym. Nie zajmuje wiele miejsca, a jest bezcennym dowodem kontaktów ze sprzedającym.

Dziecko w sieci

Rodzicu -

- rozmawiaj z dzieckiem, omawiaj kwestie bezpiecznego korzystania z sieci;
- kontroluj, co dziecko robi w sieci, jakie strony odwiedza;
- zapytaj informatyka o możliwość blokady niektórych stron.

Poradnik młodego internauty

- pamiętaj, że przyjaciele poznani w Internecie mogą nie być tymi, za których się podają – w rzeczywistości możesz rozmawiać z osobą, która ma wobec Ciebie złe zamiary;

- nie podawaj w internecie swojego nazwiska, wieku, numeru telefonu – posługuj się nickiem;
- nie umawiaj się z osobami poznanymi przez Internet;
- uważaj na e-maile otrzymane od nieznajomych, nigdy nie otwieraj podejrzanych załączników ani linków przesłanych Ci przez nieznaną osobę;
- pokaż rodzicom swoje ulubione strony, opowiedz o „wirtualnych” znajomych;

3 główne zasady bezpieczeństwa

- używajmy programów antywirusowych, które uchronią nas przed niepożądanymi wirusami i innymi niebezpieczeństwami. Nie zapomnijmy o systematycznej aktualizacji;
- uważajmy na e-maile niewiadomego pochodzenia, które zawierają podejrzane załączniki; nigdy ich nie otwierajmy;
- nie odpisujmy na spamy, ponieważ nasz e-mail zostanie uznany za aktywny i będą do nas przysyłane kolejne wiadomości z podejrzaną treścią.