ŻYJ BEZPIECZNIE

http://zyjbezpiecznie.policja.pl/zb/finanse-i-dokumenty/47375,Skimming-i-phishing.html
2018-04-24, 12:27

SKIMMING I PHISHING

Rozwój technologiczny i - co za tym idzie - wprowadzenie elektronicznych form płatniczych pociągnęły za sobą wykształcenie i rozwój nowych form przestępczości bankowej. Okradanie kont bankowych to metoda stosowana także przez złodziei w Polsce. Najpopularniejsze i najpoważniejsze przestępstwa tego typu to "skimming" i "phishing". Co oznaczają te obco brzmiące nazwy? Skąd się wzięły? Jak się zabezpieczać przed tego typu przestępstwami?

Oba określenia pochodzą z języka angielskiego. "Skimming" to przestępstwo, które polega na bezprawnym skopiowaniu zawartości paska magnetycznego karty bankowej (bankomatowej, kredytowej itp.) w celu wytworzenia duplikatu oryginalnej karty. Taka zduplikowana karta działa tak samo jak oryginalna, a transakcje nią dokonane obciążają prawowitego właściciela.

Karty mogą być kopiowane w sklepach, restauracjach, na stacjach benzynowych, w zasadzie w każdym punkcie, gdzie można dokonywać płatności kartami. Karta jest kopiowana przez sprzedawcę, który współpracuje z przestępcami lub sam jest przestępcą. Ponieważ zazwyczaj jest ona w posiadaniu przestępcy krótko, nie zawsze ma on okazję poznać jej kod PIN. Dlatego najczęściej kopiowane są karty, które nie wymagają autoryzacji przy pomocy PIN-u. Do kopiowania służy małe urządzenie, zawierające czytnik kart oraz pamięć pozwalającą na zapisywanie zawartości pasków magnetycznych. Urządzenie to podłącza się następnie do komputera i kopiuje zawartość sczytanych pasków magnetycznych.

Znacznie groźniejszą odmianą "skimmingu" jest "skimming bankomatowy". Przestępcy instalują specjalistyczne urządzenia, służące do pozyskiwania zarówno danych paska magnetycznego kart, jak i kodów PIN. Urządzenia mogą być montowane na bankomatach oraz w ich wnętrzu. Zazwyczaj złodzieje instalują komplet nakładek na bankomat (jedna część montowana jest w miejscu, gdzie wsuwa się kartę do bankomatu, druga - z zainstalowaną kamerą, jako dodatkowy baner świetlny - podwieszana jest w górnej części urządzenia). Taki zestaw rejestruje dane zawarte na pasku magnetycznym naszej karty, a za pomocą kamery odczytuje wprowadzany PIN.

Jak chronić swoją kartę, jak zapobiegać skimmingowi? Wystarczy przestrzegać kilku wskazówek. Po pierwsze musimy uzmysłowić sobie skalę zagrożenia i nabrać pewnej nieufności do urządzenia, jakim jest bankomat. W obecnej sytuacji najczęściej bezrefleksyjnie obdarzamy bankomat całkowitym zaufaniem, podczas gdy przecież może on służyć przestępcom. Zanim dokonamy transakcji w bankomacie, należy sprawdzić, czy:

• czytnik kart nie wygląda podejrzanie;
• klawiatura bankomatu jest równa lub lekko obniżona w stosunku do poziomu obudowy;
• czy do bankomatu nie są przymocowane podejrzane urządzenia - odstające elementy.

Pamiętajmy również, aby na bieżąco sprawdzać saldo naszego rachunku oraz wyciągi z kart i kont.

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 wzieło to określenie. Jedna z nich mówi, że zostało wymyślone w latach dziewięćdziesiątych przez przez crackerów próbujących wykraść konta jednego z największych amerykańskich portali. Druga mówi, że termin pochodzi od nazwiska Briana Phisha, który miał być pierwszą osobą stosującą techniki psychologiczne do wykradania numerów kart kredytowych.

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.