ŻYJ BEZPIECZNIE

https://www.zyjbezpiecznie.policja.pl/zb/komputer-i-internet/47343,Phishing.html
2020-09-23, 12:20

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.

Ocena: 5/5 (4)

Tweet

komputery włamania kradzieże oszustwa internet phishing