**<http://www.niedziela.pl/artykul/89629/nd/Pozyskiwanie-poufnych-informacji>**

**"Phishing"** - celowo błędny zapis słowa fishing (z ang. łowienie ryb) - polega na pozyskiwaniu poufnych informacji osobistych. Jest kilka teorii na temat tego, skąd wzięło się to określenie. Jedna z nich mówi, że zostało wymyślone w latach 90. przez tzw. crackerów (od angielskiego słowa crack, czyli łamać) próbujących wykraść konta jednego z największych amerykańskich portali internetowych.

Według drugiej, termin ten pochodzi od nazwiska Briana Phisha, który miał być pierwszą osobą stosującą techniki psychologiczne do wykradania numerów kart kredytowych. Częstym celem tzw. phisherów są banki czy aukcje internetowe. **Internetowi przestępcy** rozsyłają pocztą elektroniczną specjalnie przygotowane wiadomości, które udają oficjalną korespondencję z banku, serwisu aukcyjnego lub innych portali.

Zazwyczaj zawierają one informację o rzekomej deaktywacji konta i konieczności ponownej aktywacji. W e-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 przestępców pułapka. W ten sposób nieostrożni i nieświadomi użytkownicy ujawniają swoje dane uwierzytelniające (kody PIN, identyfikatory i hasła).

Zdarza się też, że przestępcy posługują się prostszymi metodami, które polegają na wysłaniu maila z prośbą, czy żądaniem, podania danych służących do logowania na konto i jego autoryzacji.

Innym sposobem działania cyberprzestępców jest wykorzystywanie oprogramowania, zwanego w zależności od swojej formy: robakami, koniami trojańskimi lub wirusami. Takiego **"robaka"** można ściągnąć korzystając z zainfekowanych witryn internetowych.

Niebezpieczną oraz trudną do wykrycia formą "phishingu" jest tzw. pharming. Zamiast wysyłania fałszywych wiadomości e-mail, przestępcy przekierowują użytkowników wpisujących prawidłowe adresy banku, którego są klientami na fałszywe strony internetowe.

W takich sytuacjach należy pamiętać o tym, że legalne serwisy nie wysyłają maili z prośbą o odwiedzenie i zalogowanie się na stronie. Nie należy też otwierać łączy bezpośrednio z otrzymanego e-maila oraz warto też uaktualniać system i oprogramowanie.

Banki i instytucje finansowe stosują protokół bezpieczeństwa typu HTTPS. Adres tak zabezpieczonej strony **WWW** rozpoczyna się 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 - przestrzega policja.