ATAK PHISHINGOWY NA KLIENTÓW BANKÓW

FUNDACJA ROZWOJU I OCHRONY FORCE KOMUNIKACJI ELEKTRONICZNEJ

Phishing to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań („fishing" - wędkowanie i „phreaking" - oszukiwanie systemów telekomunikacyjnych).

Cechy charakterystyczne wiadomości phishingowej

Wiadomości starają się wywołać wrażenie pewnego zagrożenia związanego z kontem. Pojawia się informacja, że potrzebna jest pilne zalogowanie się na konto bankowe

Wiadomość zachęca użytkownika do kliknięcia linku, po czym zostaje on przekierowany na stronę banku, na której musi wprowadzić poufne dane (login, hasło, pesel), aby na przykład dokonać ich potwierdzenia, ponownie aktywować konto itp.

Link zawarty w wiadomości nie przekierowuje na stronę banku, ale na fałszywą stronę opracowaną przez oszustów. Strona przypomina wyglądem stronę banku, posiada jego logo, a wyświetlany adres www zawiera nazwę jego instytucji. Użytkownik zazwyczaj na pierwszy „rzut oka" nie podejrzewa oszustwa.

Jak nie dać się złapać?

Uważaj na e-maile od instytucji, które proszą o **aktualizację danych**

Uważaj na e-maile, w których jesteś proszony o **podanie danych osobowych**

Nie klikaj w link podany w e-mailu przekierowujący na stronę banku. Najlepszym rozwiązaniem jest wpisanie adresu strony banku bezpośrednio do przeglądarki internetowej

https

Zawsze sprawdź czy w pasku adresu banku znajduje się kłódka i bezpieczny protokół (**https://**, a nie http://).

Pamiętaj o **oprogramowaniu antywirusowym** i aktualizacji przeglądarki internetowej

Czy wiesz, że najczęstsze próby phishingowe odbywają się za pomocą maila w postaci spamu?
Pomóż Fundacji FORCE w Badaniu zjawiska spamu w Polsce 2016

WYPEŁNIJ ANKIETĘ