Uważaj z kontem internetowym!

Data publikacji: 22.02.2011 11:05

Masz konto internetowe? Przelewy są na nim potwierdzone SMS-ami? Uważaj na złodziei!

Użytkownicy bankowości internetowych powinni zwiększyć czujność - pojawiła się nowa forma kradzieży pieniędzy z internetowych kont bankowych. Złodzieje tworzą fałszywe strony banków i dzięki temu przejmują dane, które pozwalają im wejść na konto ofiary. Następnie za pomocą oprogramowania, kóre nieświadomy użytkownik banku zainstalował na komórce, przechwytują kody autoryzacyjne, które SMS-em bank wysyła do klienta. To nowa formę phishingu, czyli wyłudzania poufnych danych.

Atak na użytkownika konta odbywa się etapami: w pierwszej kolejności komputer zostaje zarażony złośliwym oprogramowaniem (dzieje się tak podczas odwiedzin podejrzanych stron internetowych). Kiedy klient chce wejść na swoje konto bankowe, zostaje przekierowany na łudząco podobną do oryginalnej, fałszywą stronę banku. I w ten sposób, logując się na konto, użytkownik podaje swoje dane (login, hasło itp.) złodziejom. To jednak w większości nie wystarcza, by ukraść pieniądze, ponieważ banki stosują system autoryzacji transakcji za pomocą SMS-a. Jednak i na to przestępcy znaleźli sposób.

Na fałszywej stronie banku pojawiają się bowiem informacje zachęcające do zainstalowania na telefonie specjalnego oprogramowania, kóre ma rzekomo zabezpieczać telefon, a w rzeczywistości umożliwia złodziejom dostęp do kodów autoryzujących, które użytkownicy bankowości elektronicznej otrzymują od banku w SMS-ach.

Jak ustrzec się przed przestępcami? Policja radzi, by nie odwiedzać „podejrzanych" witryn internetowych (są to np. witryny pornograficzne lub oferujące nielegalne oprogramowanie) i nie używać pojawiających się tam linków. Należy używać tylko autoryzowanego, oryginalnego i aktualizowanego na bieżąco oprogramowania.

Bardzo istotne jest również weryfikowanie, czy połączenie z bankiem odbywa się z wykorzystaniem protokołu bezpieczeństwa SSL (w większości przeglądarek sygnalizuje to pojawienie się „kłódki", a początek adresu powinien rozpoczynać się od ciągu znaków https://).

Ponad to powinniśmy pamiętać, że banki nie poproszą nas o aktualizację oprogramowania telefonu i nie wyślą SMS-a zawierającego link do jego ściągnięcia – pod żadnym pozorem nie wolno otwierać takiego hiperłącza.