OSTRZEGAMY PRZED NOWĄ FORMĄ PHISHINGU!

Data publikacji 21.02.2011

Jeśli korzystasz z bankowości elektronicznej, jeśli autoryzacja operacji na twoim koncie jest potwierdzana SMS-ami – bądź ostrożny! Odnotowano nowy sposób kradzieży pieniędzy z internetowych kont bankowych. Przestępcy, korzystając ze stworzonych przez siebie fałszywych stron banków, są w stanie nie tylko przejąć dane pozwalające wejść na konto internetowe, ale też dotrzeć do kodów autoryzujących transakcje, które są przesyłane w SMS-ach na telefony komórkowe. Aby nie dać się oszukać, należy pamiętać o paru prostych zasadach!

Do policjantów dotarły sygnały o nowej formie cyberataku na klientów banków, którzy w celu autoryzacji transakcji otrzymują jednorazowe SMS-y. W pierwszej fazie ataku komputer użytkownika zostaje zarażony złośliwym oprogramowaniem – najprawdopodobniej podczas odwiedzin „podejrzanych" witryn internetowych. Następnie, kiedy ofiara chce wejść na stronę internetową swojego banku, oprogramowanie to uaktywnia się, kierując najczęściej użytkownika do fałszywej strony banku, która jest łudząco podobna do prawdziwej. Klient banku, przeświadczony, że to właściwa strona, chcąc wejść na swoje konto, podaje dane potrzebne do zalogowania się. W konsekwencji sprawcy zdobywają poufne informacje – m.in. nazwę użytkownika, hasło, numer telefonu.

Dodatkowo, i to jest nowość, na fałszywej stronie banku jest wyświetlana informacja zachęcająca użytkownika do zabezpieczenia swojego telefonu specjalnym oprogramowaniem. Temu, kto ją zaakceptuje, zostaje wysłany SMS z linkiem do pobrania programu. Po kliknięciu na link i ściągnięciu oprogramowania telefon zostaje zainfekowany, a przestępcy otrzymują dostęp do kodów autoryzujących operacje bankowe, które są przesyłane przez bank w SMS-ach.

Co zrobić, by nie paść ofiarą przestępców? Musimy w tym przypadku pamiętać o paru prostych zasadach:

- nie wolno odwiedzać „podejrzanych" witryn internetowych (są to np. witryny pornograficzne lub oferujące nielegalne oprogramowanie) i używać pojawiających się tam linków;
- należy używać tylko autoryzowanego, oryginalnego i aktualizowanego na bieżąco oprogramowania;
- niezbędne jest 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://);
- musimy 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;
- należy stale podnosić świadomość dotyczącą bezpieczeństwa teleinformatycznego;
- jeśli podejrzewasz, że padłeś ofiarą oszustów, natychmiast skontaktuj się ze swoim bankiem i zgłoś do

najbliższej jednostki Policji.

Mariusz Góra