Nowe metody cyberprzestępców - chrońmy swoje pieniądze w sieci

Data publikacji: 18.08.2014 7:30

Kilkukrotnie ostrzegaliśmy już przed cyberprzestępcami. Wyłudzanie danych do internetowych kont bankowych staje się coraz popularniejsze. Chrońmy więc swoje dane i do operacji finansowych przeprowadzanych drogą internetową podchodźmy z ograniczonym zaufaniem. Niestety, w sieci podobnie jak w życiu, najsłabszy jest czynnik ludzki?

Przed bezpieczeństwem w sieci w 100% nie ochroni nas żaden program antywirusowy połączony z najnowszym i zaktualizowanym firewallem. Większość ataków internetowych wykorzystuje często niewiedzę i naiwność samego użytkownika.

Fałszywe e-maile

Jak informuje śląska policja w ostatnim czasie ponownie uaktywnili się oszuści internetowi. OSTRZEGAMY przed e-mailami, które sugerują, że zostały wysłane z banków. Zawarte w nich dyspozycje podania danych koniecznych do zalogowania i kodów jednorazowych, bez wątpienia zakończą się „wyczyszczeniem" konta bankowego nierozważnego internauty.

Na setki tysięcy rozesłanych przez oszustów e-maili, w wielu przypadkach zdarza się, że list trafi do adresata mającego elektroniczne konto bankowe właśnie w banku, pod jaki poszywają się przestępcy. To często usypia czujność odbiorców. Należy bezwzględnie pamiętać, że banki NIGDY nie żądają od swoich klientów podania w kierowanej do nich korespondencji kodów jednorazowych i danych dostępowych do konta. Kody umożliwiające przeprowadzenie transakcji, wymagane są wyłącznie do zatwierdzenia operacji, już po zalogowaniu na stronie banku. Tworzone przez przestępców strony internetowe banków są bardzo często łudząco podobne do oryginalnych. W wielu przypadkach różnią się jednak adresem internetowym. Wtedy porównanie z oryginalnym często demaskuje już przestępców na tym etapie.

Do sfałszowanych stron prowadzą odnośniki, zamieszczone w treści wysyłanej przez oszustów korespondencji.

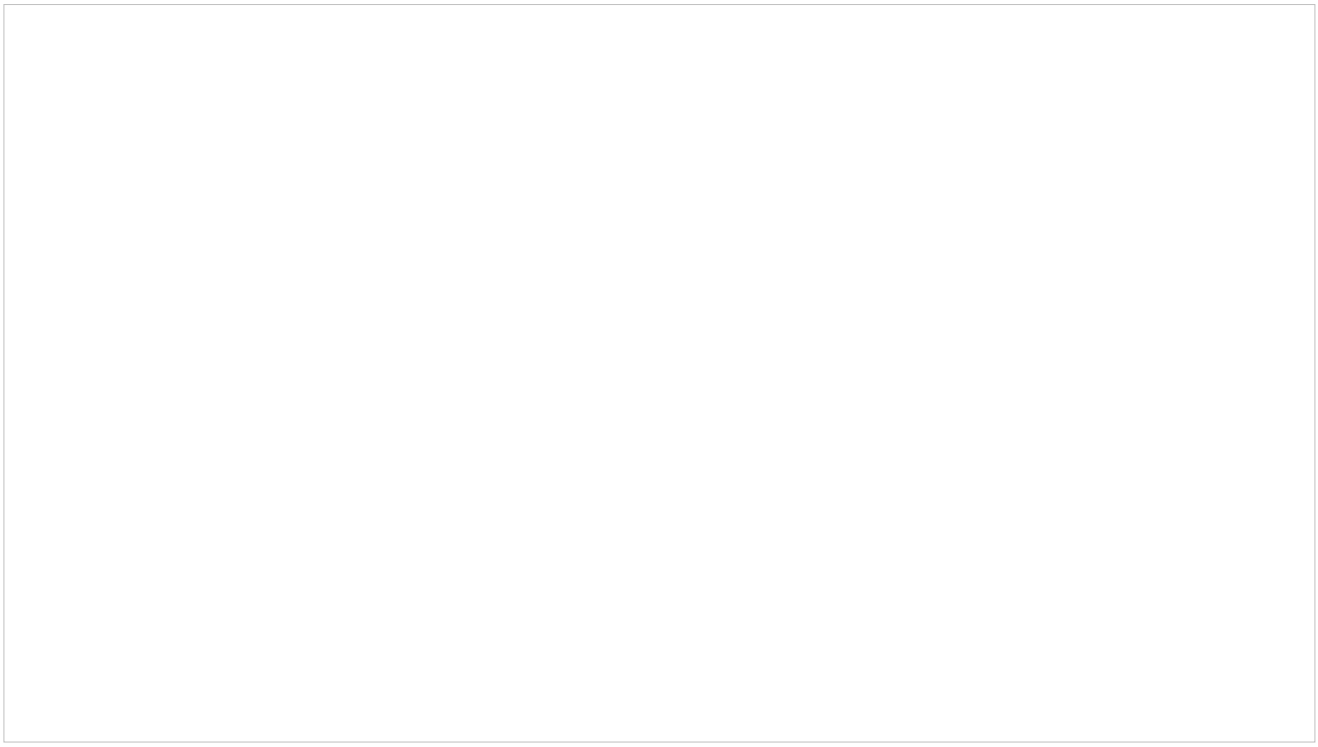
Po zalogowaniu się na podrobionej stronie www przestępcy poznają login i hasło klienta. Następne polecenie wprowadzenia kodu jednorazowego, umożliwia im wykonanie przelewu do swojego banku i często całkowite „wyczyszczenie" konta nierozważnego internauty.

Nowa metoda oszustów

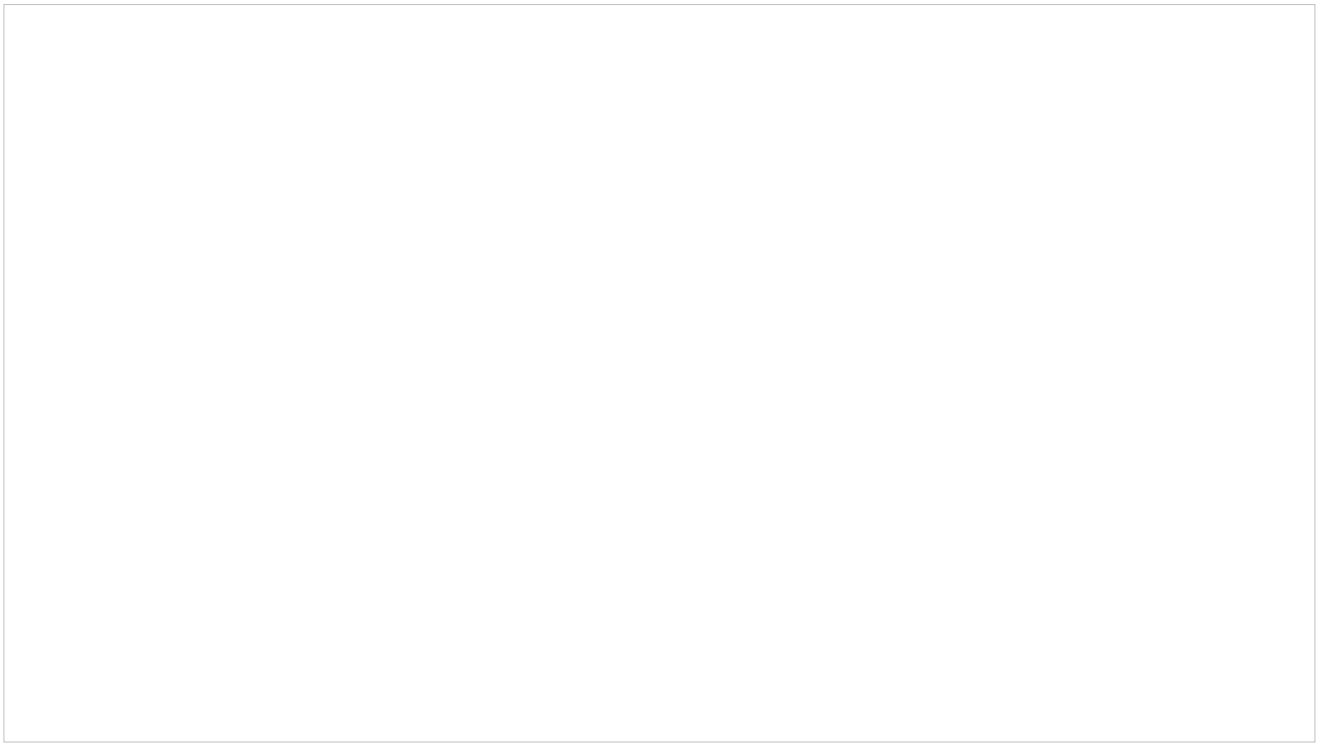
NOWĄ METODĄ oszustów jest sposób na uzyskanie kodów jednorazowych od klientów otrzymujących je za pośrednictwem SMS-ów. Na fałszywej stronie banku jest wyświetlana informacja, zachęcająca użytkownika do zabezpieczenia swojego telefonu specjalnym oprogramowaniem. Temu, kto ją zaakceptuje, zostaje wysłany 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.

Należy więc bezwzględnie unikać wchodzenia na stronę swojego banku poprzez linki otrzymane z nieznanych źródeł, nawet tych sugerujących „pewnego" nadawcę.

Przeprowadzając transakcję elektroniczne najlepiej uruchamiać stronę zapamiętaną w swojej przeglądarce. Nim zostanie ona umieszczona w „ulubionych", należy jednak dokładnie sprawdzić, czy jest to „prawdziwa" strona banku. Trzeba pamiętać, że bankowe strony logowania funkcjonują w trybie bezpiecznego połączenia szyfrowanego. Jest to doskonale widoczne w pasku adresu przeglądarki.



Po „kliknięciu” w pole tuż przed adresem banku można wyświetlić informację, czy rzeczywiście połączenie odbywa się w tym trybie (1). Możliwe jest tam również sprawdzenie tożsamości witryny (2) i szczegółów certyfikatu (3), który potwierdza, czy jest to oryginalna strona banku.



Tak „prześwietloną” stronę można dodać do „ulubionych” w używanej przeglądarce internetowej i korzystać wyłącznie z niej. Dla pewności warto jednak każdorazowo sprawdzić, czy nie nastąpiło przekierowanie i czy zgadza się adres banku oraz tożsamość witryny, potwierdzona odpowiednim certyfikatem.

Oczywiście nie należy zapominać o bezpieczeństwie samego komputera przed hakerami. Ważne jest, aby posiadać zainstalowane najnowsze oprogramowanie antywirusowe z aktualizowaną na bieżąco bazą wirusów. Spełnia ono należycie swoje funkcje jednak tylko wtedy, jeśli działa w trybie pełnej aktywności i kontroluje wszystkie pliki kopiowane i otwierane, nie tylko z nośników takich, jak dyskietki, dyski twarde, płyty cd/dvd, pamięci flash itp., ale także nadzorując dostęp do komputera poprzez sieć internetową.

Sam system operacyjny musi posiadać natomiast wszystkie zalecane przez producenta poprawki do wykrytych w nim „dziur” podatnych na ataki. W praktyce wymóg ten jest realizowany przez włączenie funkcji automatycznej instalacji aktualizacji, w miarę jak te udostępniane są przez producenta systemu operacyjnego.

Świadomość, że cyberprzestępcy bezustannie wymyślają nowe sposoby na wzbogacenie się, powinna spowodować u wszystkich internautów dalece posuniętą ostrożność przy wykonywaniu jakichkolwiek operacji finansowych drogą elektroniczną. - *podkreślają policjanci*

(red/KPP Śląsk)