Bezpieczna bankowość internetowa

Kategoria: Styl życia
Opublikowano: sobota, 19, marzec 2011 00:00
Rafał Rudka
Odsłony: 3400

Unikaj ryzyka kradzieży tożsamości i chroń swoje dane bankowe (przede wszystkim login i hasło do konta). Bankowość internetowa jest bardzo wygodna i bezpieczna, ale tylko wtedy gdy przestrzegamy obowiązujących zasad i dbamy o solidne zabezpieczenie swojego komputera.

Pamiętaj, że samo uzywanie zabezpieczonej witryny banku prawie nigdy nie stwarza zagrożenia. Niebezpieczeństwo sporwadzasz na siebie sam lub też dajesz się zwieść cyberprzestępcom.

Dane dostępowe do kont bankowych wyciekają zazwyczaj z winy użytkownika. Pierwszym powodem jest źle zabezpieczony lub zainfekowany komputer (program szpiegujący lub przechwytujący znaki wpisywane na klawiaturze). Drugim powodem jest logowanie się na spreparowanej stronie banku, stworzonej przez przestępców w celu wyłudzania danych dostępowych. Nigdy nie loguj się na podejrzanej witrynie

Zagrożenia

- Phishing to wyłudzanie haseł i danych przez przestępców działających w Internecie. Polegaja to na tym, że przestępcy kierują użytkowników do fałszywego serwisu internetowego w nadziei, że ujawnią prywatne informacje, takie jak loginy i hasła
- Kradzież tożsamości odbywa się za pośrednictwem wirusów (Kod napisany z zamiarem wywołania jego samoistnego powielania. Wirus próbuje przenosić się z komputera do komputera, zarażając inny plik /zwykle program wykonywalny/. Poza samym rozprzestrzenianiem wirusy mogą służyć do wyrządzania szkód lub działalności przestępczej) lub programów szpiegowskich (and. spyware - niechciane oprogramowanie, które potajemnie monitoruje zachowanie użytkownika, skanuje w poszukiwaniu prywatnych informacji lub pozwala osobom z zewnątrz przejąć kontrolę nad komputerem), które umożliwiają przestępcom uzyskanie dostępu do Twojego konta bankowego i innych danych osobowych przechowywanych na Twoim komputerze.

Nie daj się zwieść oszustom

Jednym z największych zagrożeń w przypadku bankowości internetowej jest kradzież tożsamości. Oszuści rozsyłają e-maile, które swym wyglądem przypominają wiadomości przesyłane przez bank (lub inne zaufane organizacje) i które zawierają łącza do fałszywych stron internetowych, również przypominających swym wyglądem te prawdziwe. Phishing przypomina podstawianie na ulicy fałszywego bankomatu, który wygląda jak prawdziwy.

- Wystrzegaj się e-maili przysyłanych w ramach phishingu. Mogą one do złudzenia przypominać wiadomości przysyłane przez bank, ale w rzeczywistości pochodzą od przestępców, którzy próbują zwabić Cię na fałszywą stronę internetową w celu uzyskania Twoich danych osobowych.
- Banki nigdy nie przysyłają wiadomości e-mail z prośbą o ujawnienie czy podanie numeru PIN, hasła lub innych danych osobowych ani z łączami do stron wymagających podania takich informacji. Zazwyczaj też w wiadomościach e-mail banki podają Twoje pełne imię i nazwisko, nie stosując zwrotów bezosobowych w rodzaju "Szanowni Państwo", a także ujmują w ich treści możliwe do zweryfikowania informacje, na przykład część Twojego numeru rachunku bankowego lub adres. Jeśli klikniesz znajdujące się w fałszywej wiadomości łącze, które przekieruje Cię do strony wymagającej podania hasła lub danych osobowych, narazisz się na niebezpieczeństwo wyłudzenia i kradzieży danych.

- Zawsze upewniaj się, że w celu połączenia się z bankiem internetowym korzystasz z bezpiecznego połączenia internetowego. Sprawdzaj, czy na początku adresu znajduje się fragment "https" i czy połączenie jest oznaczone symbolem kłódki (zobacz Informacje o bezpiecznych stronach internetowych).
- Mimo że wiele zaufanych organizacji faktycznie przysyła wiadomości e-mail zawierające wiarygodne łącza (na przykład do stron internetowych z dalszymi informacjami na dany temat), zawsze uważaj, gdy z nich korzystasz. Lepiej wprowadzić adres swojego banku bezpośrednio w polu adresu przeglądarki internetowej lub skorzystać z zakładki utworzonej na podstawie właściwego adresu.
- Jeśli uznasz, że Twoje dane są w jakikolwiek sposób zagrożone, zawsze skontaktuj się z bankiem.

Upewnij się, że Twój komputer jest bezpieczny

Ponieważ przestępcy mogą wejść w posiadanie Twoich haseł i danych osobowych, korzystając z wirusów lub programów szpiegowskich, ważne jest zapewnienie jak najwyższego poziomu zabezpieczeń swojemu komputerowi. Zastosuj się do poniższych rad, a w szczególności:

- Zainstaluj oprogramowanie antywirusowe.
- Zablokuj programy szpiegowskie.
- Włącz zaporę sieciową.
- Pobierz najnowsze aktualizacje systemu Windows.

Słuchaj głosu rozsądku

- Jeśli nie masz pewności, czy e-mail, którego nadawcą wydaje się Twój bank, jest autentyczny, skontaktuj się z bankiem inną drogą w celu rozwiania wątpliwości.
- Naucz się na pamięć swojego hasła i numeru PIN. Nie zapisuj ich, a wszelkie istniejące ich zapisy jak najszybciej zniszcz.
- Stosuj różne hasła dla stron banku i kart kredytowych. Nie używaj tego samego hasła dla każdej strony.
- Używaj silnych haseł.
- Zachowaj ostrożność podczas korzystania z komputerów publicznych w celu uzyskania dostępu do konta (patrz Bezpieczne korzystanie z komputerów publicznych).
- Wystrzegaj się osób, które zaglądają Ci przez ramię podczas wprowadzania danych i logowania się w różnych serwisach.
- Nigdy nie ujawniaj swych osobistych danych zabezpieczających, takich jak numer konta lub numer PIN, osobom, którym nie ufasz.
- Nie daj się nabrać na oszustwa związane z praniem brudnych pieniędzy. Wystrzegaj się wszelkich "możliwości zarobkowych", które wiążą się z otrzymywaniem pieniędzy od lub przechowywaniem ich dla osób nieznajomych.
- Strona internetowa Twojego banku może być dobrym źródłem dalszych informacji, również na temat popularnych rodzajów oszustw.

Kontroluj swoje rachunki

- Jeśli na wyciągu ze swojego rachunku zauważysz jakiekolwiek podejrzane transakcje, zgłoś je niezwłocznie.

Bezpieczna bankowość internetowa

Kategoria: Styl życia
Opublikowano: sobota, 19, marzec 2011 00:00
Rafał Rudka
Odsłony: 3400

Źródło: bezpieczniejwsieci.org