
Bankowość
Elektroniczna
Bezpieczeństwo
transakcji
bankowych
w Internecie
BOŚ
BANK

RODZAJE RYZYK ZWIĄZANYCH Z KORZYSTANIEM Z USŁUG BANKOWOŚCI ELEKTRONICZNEJ – BEZPIECZEŃSTWO TRANSAKCJI BANKOWYCH W INTERNECIE

Podstawowym ryzykiem związanym z korzystaniem z kanału bankowości internetowej jest możliwość utraty danych oraz środków na skutek działania szkodliwego oprogramowania oraz osób trzecich.

Do utraty danych może dojść w sytuacji, gdy:

- Padniemy ofiarą phishingu – phishing polega na podszywaniu się przestępcy pod bank w celu wyłudzenia od konkretnej osoby pożądanych informacji lub skłonienia jej do określonych działań. Przestępcy wysyłają klientom banków fałszywe maile lub dzwonią do ofiary podszywając się pod pracownika banku – pod pretekstem większego bezpieczeństwa proszą nas o podanie danych do bankowości elektronicznej czy też kliknięcia w link podany w e-mailu. Czasami przestępcy podmieniają na komputerze, z którego stronę internetową banku na podobnie wyglądającą, dzięki której można wyłudzić dane logowania klienta. Jeśli będziemy nieostrożni i damy się wciągnąć w pułapkę, utracimy login i hasło do konta, co może skutkować utratą środków z rachunku.
- Padniemy ofiarą złośliwego oprogramowania – wobec silnych zabezpieczeń stosowanych przez banki hakerzy szukają innych sposobów na pozyskanie danych do naszych rachunków. Jednym z nich jest zainstalowanie na komputerze wirusów czy programów szpiegujących, które śledzą informacje pojawiające się na ekranie komputera, sczytują znaki wprowadzane na klawiaturze, a nawet przejmują kontrolę nad urządzeniem. Wirusy mogą np. podmienić numer konta adresata przelewu na inny w momencie wypełniania formatki wysyłania przelewu. Jak możemy się zarazić takim wirusem? Zwykle przestępcy wysyłają do klientów banków fałszywe e-maile, które zawierają załącznik ze złośliwym oprogramowaniem. Jeśli nasz komputer nie jest odpowiednio zabezpieczony, a my otworzymy taką wiadomość z załącznikiem, narażamy się na ogromne niebezpieczeństwo utraty dostępu nie tylko do komputera, ale też do bankowości elektronicznej.

Jak ustrzec się przed utratą danych oraz środków?

1. **Pamiętaj, żaden Bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.**
   Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować, jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się z Infolinią lub Oddziałem Banku i poinformuj o zdarzeniu.
2. **Sprawdź na stronie Twojego Banku, jakie zabezpieczenia stosowane są w serwisie internetowym.**
   Przy każdym logowaniu bezwzględnie stosuj się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem Infolinii lub Oddziału Banku.
3. **Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.**
   Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.
4. **Dokonuj płatności internetowych tylko z wykorzystaniem „pewnych komputerów".**
   Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych, np. w kawiarenkach internetowych lub na uczelni.
5. **Skontaktuj się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on z bezpiecznych kanałów dystrybucji tej usługi.**
   Zwracaj szczególną uwagę, na jakość i bezpieczeństwo usług internetowych dostarczanych przez Twojego dostawcę. Jeśli masz jakieś wątpliwości w tym zakresie zawsze masz prawo zapytać się dostawcy, o jakość bezpieczeństwa oferowanego przez niego.
6. **Instaluj na swoim komputerze tylko legalne oprogramowanie.**
   Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.
7. **Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.**
   Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.
8. **Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje, np. przeglądarki internetowe.**
   Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty", których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.
9. **Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia.**
   Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań.

10. **Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje.**
    Szczególnie niebezpieczne mogą być strony internetowe zawierające treści pornograficzne. Ponadto z pozoru niewinne strony zawierające programy typu „freeware" również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.
11. **Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.**
12. **Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego Banku.**
13. **Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing).**
    Używaj do tego celu adresu podanego Ci przez bank, z którym podpisał(aś/eś) umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek" (Firefox) lub „adresów Ulubionych" (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.
14. **Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony logowania Twojego Banku.**
    Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.
15. **Przed zalogowaniem sprawdź, czy połączenie z bankiem jest bezpieczne.**
    Adres witryny internetowej Twojego Banku powinien rozpoczynać się od skrótu: "https://", a nie "http://". Brak litery "s" w skrócie "http" oznacza brak szyfrowania, czyli, że Twoje dane są transmitowane przez Internet tekstem jawnym, co naraża Cię na ogromne niebezpieczeństwo.
16. **Sprawdzaj prawidłowość certyfikatu.**
    Zanim wpiszesz identyfikator bądź login i hasło sprawdź, czy połączenie z bankiem odbywa się z wykorzystaniem szyfrowania. Jeżeli znajdziesz symbol kłódki, kliknij na niego dwa razy, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla Twojego Banku. Jeśli certyfikat utracił ważność lub nie został wystawiony dla Twojego Banku albo nie można go zweryfikować zrezygnuj z połączenia.
17. **Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu.**
    Identyfikator jest poufnym numerem nadawanym przez Bank, nie możesz go zmienić.
18. **Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie.**
    Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego na Tobie nie wymusi zmieniaj je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.
19. **Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.**
20. **Korzystaj z infolinii udostępnionej przez Twój bank.**
    Zawsze masz prawo skorzystać z Infolinii swojego Banku, jeśli masz wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem Internetu.
21. **Odwiedzaj regularnie Portal „Bezpieczny Bank" na stronie internetowej ZBP –** www.zbp.pl
    Jeśli chcesz wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową, regularnie odwiedzaj ten Portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.