Zasady bezpiecznego korzystania z bankowości elektronicznej

1. Bank nigdy nie wysyła wiadomości e-mail do Klientów. (Jeśli klient otrzymał wiadomość od banku to jest to wiadomość fałszywa i może zawierać wirusy. Najczęściej złośliwe oprogramowanie znajduje się w załączniku lub w linku zachęcanym do kliknięcia. Po otrzymaniu takiej fałszywej wiadomości nie wolno pobierać załączników ani klikać w reklamowany link, należy całą wiadomość niezwłocznie skasować.)
2. Zawsze sprawdzaj na stronie logowania bankowości elektronicznej aktualne zasady bezpiecznego korzystania z bankowości elektronicznej.
3. Szczegółowe informacje o zagrożeniach dla użytkowników bankowości elektronicznej należy weryfikować na stronie Związku Banków Polskich: http://zbp.pl/dlakonsumentow/bezpieczny-bank/aktualnosci (link znajduje się na stronie logowania bankowości elektronicznej).
4. Jeśli otrzymasz komunikat o przerwie konserwacyjnej podczas logowania lub realizacji przelewu, koniecznie zrezygnuj z dalszej pracy w bankowości elektronicznej i skontaktuj się z Bankiem.
5. Zabezpiecz komputer aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall).
6. Regularnie aktualizuj system operacyjny, wersję przeglądarki oraz oprogramowanie na stacji roboczej, przy użyciu której korzystasz z bankowości elektronicznej.
7. Uważaj na nietypowe informacje z banku, nie wykonuj podejrzanych poleceń a w szczególności nie instaluj oprogramowania z niezaufanego źródła, zarówno na stacji roboczej, przy użyciu której korzystasz z bankowości elektronicznej, jak i w telefonie komórkowym.
8. Po zakończeniu pracy w bankowości elektronicznej wyloguj się używając przeznaczonej do tego opcji w aplikacji, gwarantuje to poprawne zamknięcie sesji przez użytkownika.
9. Nie instaluj oprogramowania, jeżeli instrukcja instalacji zawiera zalecenie rezygnacji ze skanowania aplikacji oprogramowaniem antywirusowym.
10. Chroń dane dostępowe do bankowości elektronicznej.
11. Nie loguj się i nie dokonuj płatności w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hot-spotach.
12. Zweryfikuj czy certyfikat jest wystawiony dla „Bank Spółdzielczy w Kruszwicy” przez firmę Unizeto Technologies S.A. (kliknięcie na "zatrzaśniętą kłódkę" w pasku przeglądarki). Brak "zatrzaśniętej kłódki" oznacza, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane.
13. Sprawdź poprawność numeru NRB przed i po podpisie przelewu.
14. Zwróć szczególną uwagę na poprawność numeru NRB po wklejeniu go ze schowka systemu. Najlepiej zrezygnuj z kopiowania NRB.
15. Nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie.
16. Jeśli otrzymasz komunikat o przerwie konserwacyjnej podczas realizacji przelewu, zrezygnuj z dalszej realizacji przelewu i skontaktuj się z Bankiem.
17. Ustal limity operacji dla przelewów.

Zachowania użytkownika, a ryzyko wykonywania operacji finansowych przez Internet

Bankowość elektroniczna jest wygodną i bezpieczną formą korzystania z usług bankowych, w tym składania zleceń finansowych. W ostatnim czasie nasiliły się ataki na Klientów bankowości elektronicznej. Przestępcy nie mogąc złamać zabezpieczeń infrastruktury dostawców bankowości elektronicznej (Banków, dostawców technologii i usług), skupili się na łamaniu zabezpieczeń infrastruktury Klientów i bazowaniu na wzorcach ich zachowań. W czasach globalizacji, szalonego rozwoju usług mobilnych, coraz wyższych wymagań użytkowników co do ergonomii łatwo zapomnieć użytkownikowi o przestrzeganiu podstawowych zasad bezpieczeństwa, co przestępcy, stosując coraz bardziej wyrafinowane metody ataku, mogą wykorzystać.

Szanowny użytkowniku, bezwzględnie stosuj się do zasad bezpieczeństwa jakie publikuje Bank, w przeciwnym razie, Twoja twierdza, jaką jest bankowość elektroniczna, ma zostawione otwarte wrota.

Bank ze swojej strony dokłada starań aby nieustannie rozwijać technologie i usługi, które będą wspierać użytkownika w wygodnym i bezpiecznym korzystaniu z bankowości elektronicznej.