Podstawowe zasady bezpieczeństwa

Pamiętaj!
Bezpieczeństwo transakcji zależy również od Ciebie - chroń dane dostępowe do bankowości internetowej przed kradzieżą lub dostępem osób niepowołanych.
Koniecznie przestrzegaj niniejszych zasad bezpieczeństwa oraz zasad przesyłanych w komunikatach w bankowości internetowej i umieszczanych na stronie banku.

- Nie udostępniaj nikomu loginu lub hasła do systemu bankowości elektronicznej, chroń swój telefon, token przed dostępem osób niepowołanych.
- Zweryfikuj (klikając dwukrotnie symbol kłódki w pasku adresu czy certyfikat jest ważny i czy został wystawiony dla Asseco Poland S.A. i adresu cbp.cui.pl przez firmę DigiCert Inc. Brak "zatrzaśniętej kłódki" oznacza, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane.
- Nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie.
- Nigdy nie używaj do logowania adresu lub linku przesłanego poprzez e-mail lub SMS.
- Podczas logowania wymagane jest wpisanie wyłącznie identyfikatora i hasła. Jeśli podczas logowania lub bezpośrednio po zalogowaniu pojawi się prośba o podanie innych danych zgłoś ten fakt do banku i zrezygnuj z dalszych działań.
- Regularnie zmieniaj hasło do systemu bankowości elektronicznej.
- Nie otwieraj podejrzanych linków w otrzymywanych wiadomościach e-mail i SMS.
- Zainstaluj i aktualizuj oprogramowanie antywirusowe.
- Aktualizuj system operacyjny, wersję przeglądarki oraz oprogramowanie urządzeń, przy użyciu których korzystasz z bankowości elektronicznej oraz regularnie skanuj każde urządzenie programem antywirusowym.
- Regularnie sprawdzaj, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie.
- W przypadku autoryzowania przelewów lub edycji szablonów zweryfikuj, czy kwota transakcji oraz numer konta odbiorcy są zgodne z wprowadzanymi przez Ciebie danymi.
- Przeglądaj historię rachunku pod kątem podejrzanych transakcji.
- Zwróć szczególną uwagę na poprawność numeru NRB po wklejeniu go ze schowka systemu. Najlepiej zrezygnuj z kopiowania NRB. Sprawdź poprawność numeru NRB przed i po podpisie przelewu.
- Nie korzystaj z bankowości elektronicznej za pośrednictwem niesprawdzonych połączeń (np. publicznej Wi-Fi).
- Jeżeli zaobserwujesz nietypowe lub podejrzane działania, niezwłocznie zgłoś ten fakt do banku.
- Ustal limity kwotowe operacji.
- **Pamiętaj, nigdy nie wysyłamy:**
  - Pytań dotyczących haseł lub innych poufnych danych, ani próśb o ich aktualizację,
  - Wiadomości zawierających linki do stron transakcyjnych (bankowość internetowa)

  Bezzwłocznie zawiadom nas w przypadku otrzymania listu, wiadomości e-mail, sms-a , telefonu w takich sprawach lub pojawienia się dodatkowych pól z pytaniem np. o hasła do autoryzacji podczas logowania – należy to traktować jako próbę wyłudzenia poufnych danych.

- 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.
- Bank nie wymaga potwierdzenia danych SMS-em lub mailem.
- Po zakończeniu pracy w bankowości elektronicznej wyloguj się używając przeznaczonej do tego opcji w aplikacji, gwarantuje to poprawne zamknięcie sesji przez użytkownika.
- Zawsze sprawdzaj na stronie logowania do bankowości elektronicznej aktualne zasady bezpiecznego korzystania z bankowości elektronicznej http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci
- Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia. Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie Twoich działań lub przejęcie kontroli nad urządzeniem.

Pamiętaj!
Jeśli zignorujesz powyższe zasady bezpieczeństwa zostajesz narażony na możliwość przejęcia kontroli nad Twoim rachunkiem przez osobę nieuprawnioną co prowadzić może do kradzieży danych osobowych kontrahentów oraz kradzieży środków pieniężnych zgromadzonych na rachunku.

Zobowiązuję się do stosowania zasad bezpiecznego korzystania z bankowości elektronicznej określonych przez Bank:

……
Data i podpisy Użytkowników

Podpisy złożono w mojej obecności

……
Data i podpis pracownika banku