ZASADY BEZPIECZEŃSTWA - PRZYPOMNIENIE

W trosce o bezpieczeństwo korzystania z bankowości elektronicznej i realizowanych transakcji przedstawiamy Państwu podstawowe zasady bezpieczeństwa i prosimy o ich stosowanie w praktyce.

I. Największy wpływ na bezpieczeństwo korzystania z bankowości elektronicznej i realizacji transakcji ma sam Klient i wykorzystywane przez Niego urządzenie.

II. Przystępując do logowania ZAWSZE:

1. sprawdź czy adres strony do logowania rozpoczyna się od https://.
2. sprawdź czy połączenie z Bankiem jest szyfrowane (zielona część paska adresu z nazwą naszego Banku); obok paska adresowego lub w prawym dolnym rogu okna przeglądarki (pasek statusu) musi być widoczny symbol zamkniętej kłódki.
3. zweryfikuj certyfikat bezpieczeństwa Banku (dla kogo został wystawiony), którego szczegóły są dostępne poprzez kliknięcie na symbol kłódki w oknie przeglądarki.

III. W trakcie logowania należy pamiętać, że:

1. Bank nigdy nie prosi o podanie hasła SMS lub hasła z listy jednorazowej w trakcie logowania.
2. po prawidłowym podaniu identyfikatora i hasła logowania system powinien przejść do pulpitu użytkownika.

IV. Należy zwracać uwagę na niestandardowy wygląd lub działanie systemu, w szczególności:

- niezgodną z Państwa wolą zamianą danych w przelewach.
- nieuzasadnione komunikaty, w tym z prośbą o podanie kodu jednorazowego.
- żądanie podania dodatkowych informacji, w tym pojawianiem się dodatkowych pól, w których należy wpisać hasła jednorazowe lub hasła z wiadomości SMS.
- zmieniony adres systemu lub niewłaściwy certyfikat bezpieczeństwa (brak symbolu kłódki lub koloru zielonego w pasku adresu).

V. Należy dbać aby:

1. każdorazowo przed podpisaniem oraz wysłaniem przelewu sprawdzać poprawność numeru rachunku (tzw. NRB) odbiorcy porównując go z dokumentem źródłowym.
2. unikać korzystania z bankowości elektronicznej na nieznanych komputerach lub takich, do których dostęp mają również inne osoby (np. w kawiarenkach internetowych, u znajomych, itp.).

3. korzystać wyłącznie z legalnego i często aktualizowanego oprogramowania antywirusowego – regularnie skanować swój komputer oraz urządzenia mobilne.
4. regularnie zmieniać swoje hasło logowania. W celu zapewnienia bezpieczeństwa hasło musi spełniać minimalne wymogi określone przez Bank.
5. natychmiast zmienić swoje hasło logowania, jeśli zaistnieje podejrzenie, że ktoś mógł je poznać.
6. nie używać do logowania adresu ani linku otrzymanego przez e-mail lub komunikator internetowy.

   Bank nigdy nie wysyła takich wiadomości. Takiego rodzaju korespondencję należy traktować jako próbę oszustwa polegającego na wyłudzeniu poufnych danych przez osoby podszywające się pod instytucję finansową.
7. nie odpowiadać na żadne e-maile dotyczące weryfikacji danych dostępowych (np. identyfikatora, hasła) lub innych ważnych informacji.

   Bank nigdy nie prosi o potwierdzanie haseł stałych, hasła tokena, podanie numeru telefonu komórkowego, jego marki i modelu lub zainstalowanie na nim certyfikatu bezpieczeństwa.
8. nie otwierać podejrzanych i niespodziewanych załączników z poczty e-mail od nieznanych nadawców.
9. uważać na nietypowe informacje nadesłane w imieniu Banku, nie wykonywać podejrzanych poleceń, a w szczególności nie instalować oprogramowania z niezaufanego źródła.

   Bank nie wysyła drogą e-mailową linków do stron Banku oraz do serwisu transakcyjnego lub serwisu mobilnego oraz wszelkich stron, gdzie rzekomo ma nastąpić weryfikacja klienta czy też aktualizacja danych.
10. nie zezwalać przeglądarce na zapisywanie haseł i nazw użytkownika w formularzach.
11. nie przechowywać nazwy użytkownika i haseł w tym samym miejscu oraz nie udostępniać ich innym osobom.
12. dbać o to, aby użytkowana przeglądarka internetowa była zawsze aktualna.
13. zawsze kończąc pracę korzystać z polecenia **„Wyloguj”.**

VI. W przypadku wystąpienia jakiejkolwiek nieprawidłowości i/lub wątpliwości należy przerwać logowanie i niezwłocznie skontaktować się z Bankiem.

<u>UWAGA !</u>

Zachęcamy do zapoznania się z informacjami na temat bezpieczeństwa bankowości elektronicznej udostępnionymi na stronie internetowej Banku w zakładce „Bankowość elektroniczna” → „Bezpieczeństwo”.