Auret Bank

Zasady bezpiecznego korzystania z usług bankowych w systemie bankowości elektronicznej

AURET BANK Spółdzielczy zapewnia wysoki poziom bezpieczeństwa m.in. dzięki wykorzystaniu szyfrowania protokołem SSL oraz stosowaniu haseł jednorazowych przekazywanych za pomocą wiadomości SMS i certyfikatów kwalifikowanych.

Sprawdź adres strony:

- Do logowania do bankowości internetowej nigdy nie używaj linków przesyłanych w korespondencji e-mail lub wiadomości przesłanych za pomocą komunikatorów internetowych. Zawsze korzystaj z przycisku "Zaloguj się" na stronie naszego Banku (https://www.auretbank.pl);
- Sprawdź, czy adres na stronie logowania zaczyna się od przedrostka **https**, oznaczającego protokół, odpowiadający za bezpieczeństwo połączenia (https://online.auretbank.pl/).

Sprawdź certyfikat:

- Sprawdź, czy w obrębie okna przeglądarki internetowej znajduje się symbol zamkniętej kłódki, który gwarantuje szyfrowanie sesji specjalnym protokołem TLS, pozwalającym na bezpieczną komunikację;
- Kliknij w kłódkę, aby sprawdzić, czy wyświetlany certyfikat jest ważny i został wydany dla AURET BANK.

Uwierzytelnij się:

- Ustaw hasło do logowania bankowości elektronicznej;
- Ustaw PIN do autoryzacji;
- Weryfikuj dokładnie, czy informacje otrzymane za pomocą wiadomości SMS zgadzają się z wykonywaną w chwili obecnej czynnością.

Ustaw silne hasło:

- Hasło musi mieć długość od 8 do 18 znaków i zawierać co najmniej jedną wielką literę, jedną małą literę, jedną cyfrę, jeden znak specjalny;
- Ustalając hasło używaj kombinacji dopuszczalnych znaków. Unikaj używania łatwych haseł (jak np. własnego imienia), stosuj za to hasła trudne do rozszyfrowania;
- Specjaliści ds. cyberbezpieczeństwa zalecają, aby hasła tworzyć przy użyciu trzech/czterech losowych słów. Po prostu je połączysz, na przykład: Kawatramwajryba; ścianacienkuLa; uzywambardzosilnegohasla;
- Dodatkowo możesz skorzystać z poniższych reguł, żeby je odpowiednio zmodyfikować np.:
  - zamień a na @
  - zamień małe „o” na 0
  - zamień s na $
  - zamień i na !

  np. kawapieswoda można zapisać: k@wapie$w0da
- ze względów bezpieczeństwa po 3 próbach wprowadzenia nieprawidłowego hasła dostęp do systemu zostanie automatycznie zablokowany. W takim przypadku możesz zgłosić dyspozycję odblokowania telefonicznie do pracownika Banku bądź poprzez zgłoszenie się do dowolnej placówki Banku.

Chroń swoje dane:

- Nie ujawniaj nikomu loginu, hasła, kodu PIN czy kodów autoryzacyjnych;
- Regularnie zmieniaj swoje hasło do logowania;
- Nie odchodź od komputera, podczas gdy jesteś zalogowany do systemu;
- Nie przechowuj swoich haseł razem z loginem;
- Wpisując login i hasło upewnij się, że inne osoby nie mogą ich przechwycić lub podejrzeć.

Korzystaj z zaufanej sieci:

- Nie korzystaj z usług bankowości internetowej na ogólnie dostępnych komputerach, w kawiarenkach internetowych;
- Nie korzystaj z usług bankowości internetowej używając nieznanych sieci Wifi;
- Nie dodawaj do zaufanych urządzeń przeglądarek, z których nie korzystasz na co dzień;
- Zadbaj aby Twoje urządzenia służące do połączenia z Internetem w domu było zabezpieczone w odpowiedni sposób.

Wyloguj się:

- Po zakończeniu korzystania z bankowości elektronicznej użyj przycisku Wyloguj i zamknij przeglądarkę;
- Nigdy nie zamykaj strony poprzez „x";
- W systemie bankowości internetowej jest ustawiony czas automatycznego wylogowania (w przypadku braku aktywności), aby zapewnić komfort pracy przy zachowaniu rozsądnego poziomu bezpieczeństwa.

Pamiętaj: Bezpieczeństwo bankowości internetowej zależy także od Ciebie !

- Zablokuj dostęp do bankowości elektronicznej, jeśli podejrzewasz kradzież danych;
- Zadzwoń do Banku jeśli wygląd strony logowania do bankowości wzbudza Twój niepokój;
- Nie realizuj transakcji jeśli po zalogowaniu do systemu bankowości elektronicznej cokolwiek wzbudzi Twoje podejrzenie.