Zasady bezpiecznego korzystania z Bankowości Internetowej

Drodzy Klienci,

przypominamy o podstawowych zasadach bezpiecznego korzystania z Bankowości Internetowej:

Usługa Bankowości Internetowej dostępna jest na stronie głównej Banku https://bspoddebice.pl po kliknięciu na ikonę *Logowanie eB@nkowość lub bezpośrednio pod adresem https://ibs.bspoddebice.pl*

Wszystkie operacje po zalogowaniu się do usługi, są automatycznie zabezpieczone protokołem SSL. Sygnalizowane jest to symbolem kłódki w oknie przeglądarki (najczęściej na górnym pasku adresu lub dolnym pasku stanu, zależnie od rodzaju przeglądarki i jej wersji), co oznacza, że strona jest szyfrowana i bezpieczna. Po dwukrotnym kliknięciu na symbol kłódki powinna pojawić się informacja, o szczegółach certyfikatu.

Identyfikator

Identyfikator jest unikalnym kodem użytkownika usługi.

Alias

To alternatywny/dodatkowy Identyfikator użytkownika usługi.

Hasło

Pierwsze hasło jest nadawane przez Bank i wysyłane na numer autoryzacyjny Użytkownika po wprowadzeniu Identyfikatora i wciśnięciu "Dalej". Kolejne logowania odbywają się z użyciem hasła ustalonego przez użytkownika.
Hasło logowania winno być złożone (zawierać minimum 8 znaków, w tym małą literę, wielką literę, cyfrę, znak specjalny).

Hasło maskowane

Wymaga wprowadzenia przez użytkownika wybranych znaków wchodzących w skład hasła, nie wymaga podawania hasła w całości.

Autoryzacja operacji

System umożliwia autoryzację:

- hasłami jednorazowymi SMS
  Jednorazowe hasło wysyłane jest na wskazany w Banku numer telefonu komórkowego użytkownika usługi.
  Wysłanie hasła SMS następuje automatycznie po kliknięciu na „Autoryzuj i wyślij".
- kodami wygenerowanymi w aplikacji EBO Token PRO
  Autoryzacja następuje po zalogowaniu do aplikacji EBO Token w której wyświetlone zostanie powiadomienie ze wszystkimi szczegółami zlecenia, które zatwierdzamy.

Zwróć uwagę w przypadku otrzymania wiadomość tekstowej SMS z kodem jednorazowym, mimo nie wykonywania operacji. Sprawdź zgodność treści wiadomości z kodem jednorazowym: Czy numer rachunku i kwota są zgodne ze zlecaną przez Ciebie w serwisie transakcyjnym operacją. Sprawdź zgodność wprowadzonych danych w ostatnim kroku wykonywania operacji.

Blokowanie

Trzykrotne błędne podanie hasła podczas logowania powoduje zablokowanie dostępu. Odblokowanie dostępu możliwe jest po skontaktowaniu się z infolinią Banku lub poprzez złożenie formularza odblokowania w dowolnej placówce Banku Spółdzielczego w Poddębicach.

Wygasanie sesji

Jeżeli po zalogowaniu do usługi, użytkownik nie będzie wykazywał żadnej aktywności przez 5 minut - zostanie automatycznie wylogowany.

Pamiętaj, iż bezpieczeństwo korzystania z usług bankowości internetowej zależy nie tylko od rozwiązań stosowanych przez Bank, ale przede wszystkim od samych użytkowników usługi, którzy winni zadbać o zabezpieczenie własnego urządzenia (komputera, tabletu, telefonu) i przestrzeganie podstawowych zasad bezpieczeństwa.

1. **Przy każdym logowaniu do Bankowości Internetowej, sprawdź:**
   - Czy używasz szyfrowanego połączenia?
   - Czy adres strony rozpoczyna się od https://?
   - Czy w oknie przeglądarki widoczna jest ikona kłódki oznaczająca połączenie szyfrowane?
   - Certyfikat strony (np. klikając dwukrotnie na symbolu kłódki).
   - Czy certyfikat ostał wystawiony dla właściwej domeny?
   - Czy certyfikat jest ważny?
2. **Nie odpowiadaj na e-maile zachęcające do ujawnienia danych i haseł.** ***Bank Spółdzielczy w Poddębicach:***

- nie wysyła e-maili wymagających podania danych osobowych Klientów lub też Identyfikatora, Hasła dostępu, haseł jednorazowych,
- nie wysyła e-maili z linkami do stron Banku oraz do usług bankowości elektronicznej oraz wszelkich stron, gdzie rzekomo ma nastąpić weryfikacja czy aktualizacja danych Klientów,
- nie prosi o podanie Identyfikatora, Hasła dostępu lub haseł jednorazowych w rozmowie telefonicznej z Klientem,
- nie przyjmuje drogą e-mailową zleceń wykonania transakcji finansowych.

3. **Twórz „silne" hasło do konta**.

   Hasło musi być unikalne, możliwie skomplikowane, ale dające się zapamiętać.
   Pamiętaj, aby go nikomu nie udostępniać. Zmieniaj je natychmiast, jeśli tylko stwierdzisz, że ktoś mógł je podejrzeć.

4. **Nie podawaj danych logowania (identyfikator, hasło) na stronie bez certyfikatu.**

5. **Nie przechowuj Identyfikatora z Hasłem dostępu razem. Nie przechowuj haseł w jawnej postaci.**

   Jeśli masz zapisane hasło w notatniku czy komputerze, to spróbuj je zapisać w taki sposób, aby trudno było je skojarzyć z bankowością internetową.

6. **Korzystaj z serwisu transakcyjnego wyłącznie na zaufanych komputerach.**

   Nie korzystaj z otwartych sieci WIFI. Dostęp do sieci WIFI w galeriach handlowych, dworcach, lotniskach jest przeważnie darmowy, ale korzystanie z tego typu sieci do prowadzenia operacji bankowych jest ryzykowne i nieodpowiedzialne. Korzystaj z sieci WIFI, tylko wtedy, gdy gwarantują one odpowiedni poziom bezpieczeństwa.

7. **Unikaj przeklejania numerów rachunków**.

   Zalecane jest ręczne wpisywanie numerów rachunków do zleceń w systemie bankowości internetowej albo uważne kontrolowanie wklejanego numeru i porównanie tego numeru z oryginalnym.

8. **Weryfikuj kody wysyłane przez SMS.**

   Pamiętaj, aby dokładnie czytać takie SMS, zawsze sprawdzaj, czy zgadza się numer rachunku odbiorcy oraz kwota operacji.

9. **Zadbaj o zabezpieczenie urządzenia, z którego korzystasz *(komputera, tabletu, telefonu).***

   - Korzystaj z aktualnych wersji systemu operacyjnego, przeglądarki internetowej, oprogramowania antywirusowego, personal firewall, oprogramowania zabezpieczającego przed spy-ware i ad-ware.
   - Nie instaluj oprogramowania pochodzącego z nieznanych/ niezaufanych źródeł.
   - Nie klikaj w linki niewiadomego pochodzenia.
   - Aktualizuj systematycznie system operacyjny, przeglądarkę internetową, oprogramowanie antywirusowe i bazy wirusów.
   - Pamiętaj, że korzystanie z oprogramowania P2P (np. eMule, Bearshare, eDonkey2000, KaZaA) związane jest z ryzykiem obniżenia bezpieczeństwa Twojego komputera.

10. **Opuszczaj serwis transakcyjny z użyciem funkcji WYLOGUJ.**

    Nie zostawiaj komputera zalogowanego do systemu bankowości internetowej bez kontroli.

11. **W przypadku stwierdzenia nieprawidłowości lub wątpliwości skontaktuj się z infolinią Banku lub prześlij wiadomość na adres: pomoc@bspoddebice.pl**