

Zasady bezpieczeństwa korzystania z bankowości internetowej

1. Ogólne zasady bezpieczeństwa.

- Do pracy w bankowości elektronicznej, wybieraj tylko zaufane urządzenia dostępne, posiadające legalne oprogramowanie oraz program antywirusowy.
- Ograniczaj logowanie do bankowości internetowej z obcych komputerów, tabletów i telefonów; jeżeli jest to możliwe, nie korzystaj z takich urządzeń.
- Regularnie (zgodnie z zaleceniami producentów) aktualizuj posiadane oprogramowanie: system operacyjny, przeglądarkę internetową i oprogramowanie antywirusowe.
- Regularnie skanuj zawartość dysków swojego urządzenia.
- Nie otwieraj podejrzanych maili oraz załączników. Fałszywe wiadomości e-mail są jedną z najczęściej wykorzystywanych metod infekowania komputerów użytkowników złośliwym oprogramowaniem.

2. Zasady bezpiecznego logowania.

- Do bankowości internetowej loguj się wyłącznie ze strony www.bschodziez.pl lub wpisując adres online.bschodziez.pl w linii adresowej przeglądarki.
- Nigdy nie używaj do logowania adresu lub linku otrzymanego w wiadomości e-mail lub wskazanego przez wyszukiwarkę.
- Przed zalogowaniem zawsze sprawdzaj czy strona bankowości internetowej zabezpieczona jest certyfikatem bezpieczeństwa a połączenie jest szyfrowane (adres strony rozpoczyna się od https:// oraz w obrębie okna przeglądarki widoczna jest ikona zamkniętej kłódki).
- Sprawdzaj poprawność certyfikatu bezpieczeństwa. W tym celu dwukrotnie kliknij na ikonę zamkniętej kłódki i sprawdź czy wyświetlany certyfikat jest ważny i czy został

wydany dla Banku Spółdzielczego w Chodzieży oraz zweryfikowany/wydany przez firmę Unizeto Technologies S.A.

- Chroń swoje dane do logowania (Identyfikator, hasło). Nigdy nie udostępniaj danych do logowania do serwisu bankowości internetowej.
- Nie zezwalaj przeglądarce na zapisywanie haseł i nazw użytkownika w formularzach. Poniżej instrukcje jak wyłączyć tę funkcjonalność w poszczególnych przeglądarkach:

- **Firefox**

Menu „Narzędzia” » „Opcje” » „Bezpieczeństwo” » „Hasła” » odznacz pole „Pamiętaj hasła do witryn”,

- **Opera**

Menu „Ustawienia”, zakładka „Preferencje...” » zakładka „Formularze”, odznacz pole „Włącz menedżera haseł”,

- **Internet Explorer**

Menu „Narzędzia” » „Opcje Internetowe” » zakładka „Zawartość” » część „Autouzupełnianie” » „Ustawienia” - odznacz pola „Nazwy użytkowników i hasła w formularzach”,

- **Google Chrome**

Menu „Ustawienia Google Chrome” » „Ustawienia” » „Prywatność” » „Hasła i formularze” – odznacz pole „Proponuj zapisywanie haseł podawanych w internecie”.

- Pamiętaj, Bank nigdy nie będzie wymagał od Ciebie podania kodu jednorazowego podczas logowania do bankowości internetowej lub bezpośrednio po zalogowaniu się do niej.

3. Zasady bezpiecznego korzystania z usługi Internet Banking

- Zawsze przed potwierdzeniem wykonania transakcji kodem autoryzacyjnym, sprawdzaj zgodność numeru rachunku odbiorcy oraz kwotę. Upewnij się, czy powyższe dane nie uległ podmanie.

- Jeżeli do autoryzacji transakcji wykorzystujesz kody SMS, zawsze przed wprowadzeniem kodu autoryzacyjnego, uważnie przeczytaj treść otrzymanego SMSa i upewnij się, że dotyczy on właściwej, zleconej przez Ciebie operacji. W przypadku stwierdzenia niezgodności nie wprowadzaj kodu jednorazowego i niezwłocznie skontaktuj się z Bankiem.
- Pamiętaj, że hasła jednorazowe służą wyłącznie do potwierdzenia realizacji dyspozycji. Nigdy nie przekazuj hasła w innych celach.
- Systematycznie sprawdzaj historię operacji wykonanych z Twojego rachunku – jeżeli zauważysz niezgodność, niezwłocznie zgłoś ją do Banku.
- Zawsze kończąc pracę korzystaj z polecenia [Wyloguj].
- Uważnie czytaj komunikaty Banku dotyczące bezpieczeństwa.

PAMIĘTAJ

Jeżeli masz jakieś wątpliwości lub jakieś podejrzenia dotyczące bezpieczeństwa korzystania z Internet Bankingu skontaktuj się z pracownikiem Banku pod numerem telefonu: 67 281 06 00.

Jeśli obawiasz się że Twoje dane logowania do bankowości elektronicznej mogły zostać skradzione lub w jakikolwiek sposób ujawnione osobom niepowołanym możesz je również zablokować wysyłając wiadomość SMS na numer telefonu komórkowego: 662 213 713 o treści – BI#identyfikator, gdzie identyfikator to login do Internet Bankingu (program zweryfikuje, czy podany identyfikator jest powiązany z numerem telefonu) lub BI#identyfikator#PESEL – gdzie identyfikator to login do Internet Bankingu; SMS blokuje dostęp z dowolnego telefonu. Po dokonaniu blokady przez system otrzymasz informację SMS-em o dokonaniu blokady. Jest to standardowa wiadomość SMS, a koszt uzależniony jest od cennika Twojego operatora komórkowego.