WYMAGANIA SYSTEMOWE I ZASADY BEZPIECZEŃSTWA
Korzystania z systemu eBankNet w Banku Spółdzielczym w Brańsku

1. Minimalne wymagania systemowe

System operacyjny - Windows 10/11, macOS w aktualnie wspieranych wersjach, Linux w aktualnie wspieranych dystrybucjach
Przeglądarka - Google Chrome, Microsoft Edge, Mozilla Firefox, Safari
Wersja przeglądarki - Aktualna lub poprzednia stabilna wersja
Połączenie internetowe - Dostęp do Internetu
Protokół komunikacji - HTTPS, TLS 1.2 lub nowszy
Rozdzielczość ekranu - Minimum 1024 × 768 pikseli, zalecana 1366 × 768 lub wyższa
Obsługa JavaScript - Włączona
Pliki cookies - Włączona obsługa plików cookies
Certyfikaty - Obsługa certyfikatów cyfrowych i połączeń TLS

2. Zalecane zabezpieczenia urządzenia

Użytkownik powinien:
- korzystać z systemu operacyjnego posiadającego wsparcie producenta;
- instalować aktualizacje bezpieczeństwa systemu i przeglądarki;
- używać aktualnego oprogramowania antywirusowego;
- mieć włączoną zaporę sieciową;
- nie korzystać z urządzeń zainfekowanych lub niezaufanych;
- nie używać przeglądarek z dodatkami mogącymi przechwytywać dane lub modyfikować treść stron.

3. Zalecenia zwiększające bezpieczeństwo wykonywania transakcji

W celu zapewnienia maksymalnego bezpieczeństwa podczas korzystania z bankowości elektronicznej zaleca się przestrzeganie następujących zasad:

- Korzystanie z zaufanego urządzenia – wykonywanie operacji bankowych wyłącznie na własnym komputerze lub urządzeniu mobilnym, do którego użytkownik ma wyłączny dostęp.
- Aktualizowanie oprogramowania – regularne instalowanie aktualizacji systemu operacyjnego, przeglądarki internetowej oraz oprogramowania zabezpieczającego.
- Ochrona antywirusowa – korzystanie z aktualnego oprogramowania antywirusowego oraz zapory sieciowej.
- Bezpieczne połączenie internetowe – unikanie korzystania z publicznych, niezabezpieczonych sieci Wi-Fi podczas logowania i wykonywania transakcji.

- Weryfikacja adresu strony banku – każdorazowe sprawdzanie poprawności adresu strony internetowej banku oraz upewnianie się, że połączenie jest szyfrowane (HTTPS).
- Ochrona danych logowania – nieudostępnianie identyfikatora, hasła, kodów autoryzacyjnych ani innych danych umożliwiających dostęp do bankowości elektronicznej.
- Weryfikacja transakcji – przed zatwierdzeniem przelewu należy dokładnie sprawdzić numer rachunku odbiorcy, kwotę oraz pozostałe dane transakcji.
- Ochrona kodów autoryzacyjnych – zatwierdzanie wyłącznie tych operacji, które użytkownik samodzielnie zainicjował. Należy zwracać uwagę na treść komunikatów autoryzacyjnych.
- Wylogowywanie się z systemu – po zakończeniu pracy należy zawsze prawidłowo wylogować się z bankowości elektronicznej i zamknąć przeglądarkę.
- Ostrożność wobec podejrzanych wiadomości – nieotwieranie podejrzanych załączników i linków otrzymanych w wiadomościach SMS, e-mail lub komunikatorach, nawet jeśli pozornie pochodzą od banku.
- Monitorowanie rachunku – regularne sprawdzanie historii operacji i niezwłoczne zgłaszanie bankowi wszelkich nieautoryzowanych lub podejrzanych transakcji.
- Nieinstalowanie nieznanego oprogramowania – nieinstalowanie aplikacji ani narzędzi do zdalnego dostępu na polecenie osób podających się za pracowników banku lub konsultantów technicznych.

4. Bezpieczeństwo systemu bankowości elektronicznej eBankNet

Bank Spółdzielczy w Brańsku, w trosce o bezpieczeństwo środków finansowych i danych swoich Klientów, stosuje w systemie bankowości elektronicznej eBankNet mechanizmy zabezpieczające dostęp do rachunków, ochronę danych oraz autoryzację operacji bankowych.

4.1. Zabezpieczenia dostępu do systemu

1. Indywidualny identyfikator użytkownika – każdy użytkownik posiada indywidualny identyfikator umożliwiający dostęp do systemu bankowości elektronicznej.
2. Hasło dostępu – logowanie do systemu wymaga podania indywidualnego hasła użytkownika. Hasło powinno być poufne i znane wyłącznie użytkownikowi.
3. Szyfrowanie transmisji danych – komunikacja pomiędzy przeglądarką internetową Klienta a systemem bankowości elektronicznej odbywa się z wykorzystaniem szyfrowanego połączenia HTTPS.
4. Ochrona przed nieuprawnionym dostępem – system stosuje mechanizmy kontroli poprawności danych logowania oraz zabezpieczenia przed wielokrotnymi próbami nieprawidłowego logowania.
5. Automatyczne zakończenie sesji – po określonym czasie bezczynności system automatycznie

kończy sesję użytkownika, ograniczając ryzyko wykorzystania pozostawionego bez nadzoru konta.

4.2. Zabezpieczenia wykonywania transakcji

1. Dodatkowa autoryzacja operacji – wykonywanie operacji wymagających autoryzacji jest zabezpieczone dodatkowym potwierdzeniem przez użytkownika, z wykorzystaniem metod udostępnionych przez Bank.
2. Autoryzacja mobilna – w przypadku korzystania z tej metody potwierdzanie operacji odbywa się za pośrednictwem aplikacji mobilnej powiązanej z użytkownikiem.
3. Kody jednorazowe SMS – w przypadku korzystania z autoryzacji SMS potwierdzenie operacji wymaga podania jednorazowego kodu otrzymanego na zarejestrowany numer telefonu.
4. Weryfikacja danych transakcji – przed zatwierdzeniem operacji użytkownik powinien zweryfikować prezentowane dane, w szczególności rachunek odbiorcy i kwotę przelewu.
5. Limity transakcyjne – system umożliwia określanie limitów operacji, w tym limitów kwotowych, ograniczających potencjalne skutki nieuprawnionego dostępu.
6. Kontrola autoryzacji – operacje wymagające potwierdzenia nie powinny być realizowane bez prawidłowego zakończenia procesu autoryzacji.

4.3. Funkcje bezpieczeństwa dostępne dla użytkownika

W systemie eBankNet użytkownik może korzystać z funkcji związanych z bezpieczeństwem rachunku i dostępu do bankowości elektronicznej, w szczególności:
1. Zmiana hasła – możliwość zmiany hasła dostępu do systemu.
2. Zarządzanie limitami – możliwość sprawdzenia i zmiany dostępnych limitów transakcyjnych, zgodnie z uprawnieniami i zasadami określonymi przez Bank.
3. Powiadomienia SMS – możliwość korzystania z powiadomień o określonych zdarzeniach i operacjach na rachunku.
4. Mobilna autoryzacja – możliwość korzystania z aplikacji mobilnej do zatwierdzania operacji bankowych, jeżeli metoda została aktywowana.
5. Ustawienia bezpieczeństwa – dostęp do funkcji związanych z zabezpieczeniem konta użytkownika.
6. Historia operacji – możliwość przeglądania wykonanych operacji i kontrolowania aktywności na rachunku.

4.4. Ochrona użytkownika przed oszustwami

Bank zaleca zachowanie szczególnej ostrożności podczas korzystania z bankowości elektronicznej.
- Bank nigdy nie prosi o przekazanie hasła do bankowości elektronicznej, kodów SMS ani danych autoryzacyjnych.

- Bank nie wymaga instalowania programów do zdalnego dostępu do komputera lub telefonu w celu zabezpieczenia rachunku.
- Użytkownik powinien zatwierdzać wyłącznie operacje, które samodzielnie zainicjował.
- W przypadku otrzymania kodu autoryzacyjnego do operacji, której użytkownik nie wykonywał, nie należy go wykorzystywać ani przekazywać innym osobom.
- W przypadku podejrzenia przejęcia danych logowania należy niezwłocznie skontaktować się z Bankiem.
- Należy regularnie kontrolować historię rachunku i zgłaszać Bankowi wszelkie nieznane operacje.

4.5. Odpowiedzialność użytkownika

Bezpieczeństwo korzystania z systemu bankowości elektronicznej zależy zarówno od zabezpieczeń stosowanych przez Bank, jak i od przestrzegania zasad bezpieczeństwa przez użytkownika.
Klient zobowiązany jest do ochrony danych uwierzytelniających, zachowania poufności haseł i kodów autoryzacyjnych oraz niezwłocznego informowania Banku o podejrzeniu nieuprawnionego dostępu do rachunku.