

Przewodnik dla Klienta Instrukcja uruchomienia bankowości internetowej

Szanowny Kliencie !

Dziękujemy za skorzystanie z naszej usługi dostępu do bankowości internetowej.

Niniejszy przewodnik ma na celu poprowadzenie Państwa przez proces uruchomienia bankowości internetowej. Mamy nadzieję, iż opisane tu etapy działania pozwolą Państwu na bezproblemowe uruchomienie usługi.

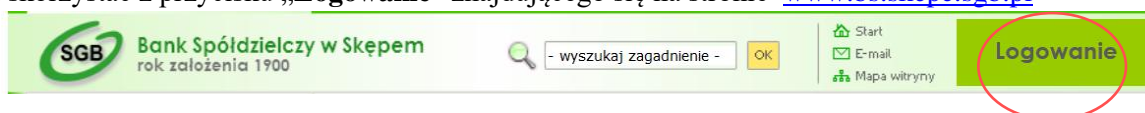
KROK 1

PIERWSZE LOGOWANIE DO SYSTEMU

Uruchomić przeglądarkę internetową, np. Microsoft Internet Explorer

Wpisać adres strony <https://bsskepe.ebp.cui.pl>

można też skorzystać z przycisku „Logowanie” znajdującego się na stronie www.bs.skepe.sgb.pl



Po uruchomieniu aplikacji zostaje wyświetlone okno LOGOWANIA.

W polu „Login” wpisujemy nazwę użytkownika nadaną przez Bank – „Login”.

The image shows the login page of the SGB Bank Spółdzielczy w Skępem. It features the bank's logo and name at the top. Below that, the text 'Zaloguj się do bankowości internetowej' is displayed. Underneath is a text input field labeled 'Login'. Below the input field is a green button labeled 'DALEJ'. At the bottom of the page, there are links for 'ZASADY BEZPIECZEŃSTWA', 'BEZPIECZNE ZAKUPY W INTERNECIE', and a language dropdown menu set to 'Polski'.

Następnym krokiem autoryzacji jest wprowadzenie w polu „HASŁO” otrzymanego z Banku w formie komunikatu SMS Tymczasowego KODU DOSTĘPU.

The image shows the password page of the SGB Bank Spółdzielczy w Skępem. It features the bank's logo and name at the top. Below that, the text 'Zaloguj się do bankowości internetowej' is displayed. Underneath is a text input field labeled 'HASŁO'. Below the input field is a green button labeled 'ZALOGUJ'. At the bottom of the page, there are links for 'ZASADY BEZPIECZEŃSTWA', 'BEZPIECZNE ZAKUPY W INTERNECIE', and a language dropdown menu set to 'Polski'.

Po wprowadzeniu tymczasowego KODU DOSTĘPU należy wprowadzić otrzymany w wiadomości SMS „Logowanie do Bankowości Internetowej” KOD.

Przykład wiadomości SMS:

Logowanie do Bankowości Internetowej


nr 1 w dniu 2020-08-18

Kod: 944969

DZIĘKUJEMY



Po kliknięciu przycisku **ZALOGUJ** pojawi się okno o nadanie nowego hasła dostępu



Należy wprowadzić własne hasło dostępu i zatwierdzić przyciskiem **ZAPISZ I ZALOGUJ**

Uwaga:

Definiując swoje hasło dostępu pamiętaj o zachowaniu podstawowych zasad bezpieczeństwa:

- musi składać się z 10-24 znaków
- musi zawierać przynajmniej jeden znak specjalny
- musi zawierać przynajmniej jedną wielką
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jedną cyfrę
- dozwolone znaki: 0123456789abcdefghijklmnopqrstuvwxzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#\$%^&*()-_+=+[{]}|;: ",<.>/?

Prosimy pamiętać, że hasło dostępu jest poufne. W związku z tym nie powinno być ujawniane osobom trzecim.

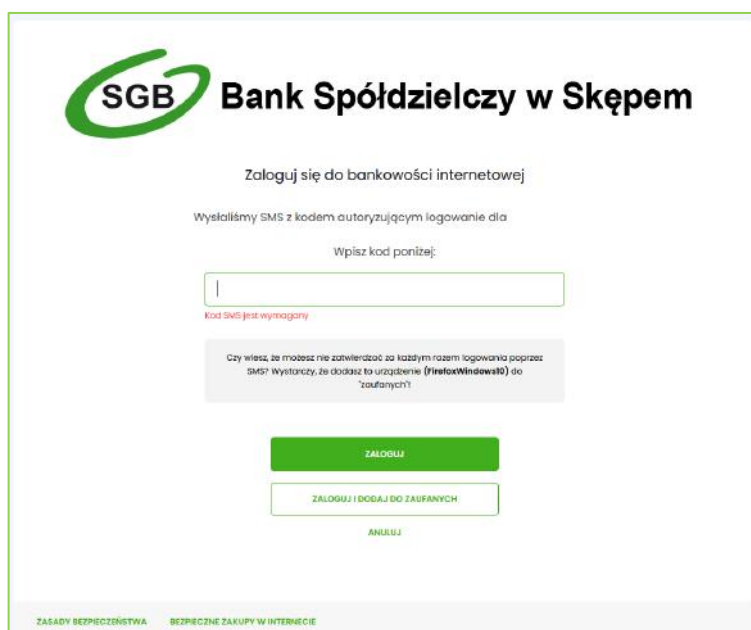
Następnie wprowadzamy otrzymany w wiadomości SMS kod SMS i klikamy na przycisk **ZALOGUJ**

Podczas kolejnego logowania w pole „Kod dostępu” wpisujemy tylko losowo wskazane w białych polach znaki z naszego nowo nadanego hasła, tak jak na poniższym przykładzie.

dla przykładowego hasła: **Mojehas%01**
będą to znaki:



Następnie wpisujemy otrzymany w wiadomości SMS Kod SMS



KROK 2

AUTORYZACJA ZLECEŃ

Przed dokonaniem autoryzacji zlecenia należy nadać sobie własny **PIN do autoryzacji**.
W tym celu przechodzimy do zakładki **USTAWIENIA** wybieramy **Zmiana hasła**
oraz następnie **Zmiana PIN do autoryzacji**

W polu **Obecny PIN** należy wpisać otrzymany w wiadomości SMS: **Tymczasowy PIN do autoryzacji**
W polach **Nowy PIN** oraz **Powtórz nowy PIN** należy wpisać własny PIN, pamiętając o zachowaniu wymienionych poniżej zasad budowy PIN.

<

Zmiana PIN do autoryzacji

Obecny PIN

Nowy PIN

Powtórz nowy PIN

ZATWIERDŹ

Zadbaj o zachowanie poufności swojego PIN.

- Nie udostępniaj PIN innym osobom, na żadnych stronach internetowych, poczty elektronicznej, wiadomością SMS lub w odpowiedzi na zgłoszenia otrzymane od pracowników banku.
- Definiuj swój PIN pamiętając o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Zasady budowy PIN są następujące:

- musi składać się z 4-8 znaków
- może zawierać wyłącznie znaki ze zbioru: **0123456789**

INSTRUKCJE

Zachęcamy Państwa do obejrzenia krótkich filmów instruktażowych prezentujących zakres usług świadczonych przez nasz Bank: <http://www.bs.skepe.sgb.pl>
(zakres prezentowanych usług w filmach instruktażowych może różnić się od tych świadczonych przez nasz Bank)

BEZPIECZEŃSTWO USŁUGI

Przypominamy o stosowaniu zasad, które pomogą w bezpiecznym korzystaniu z bankowości elektronicznej:

- Zanim wprowadzisz na stronie swój Identyfikator użytkownika i Kod Dostępu sprawdź, czy adres strony logowania rozpoczyna się od https (oznacza bezpieczne połączenie internetowe)
- Sprawdź czy w pasku adresu lub na pasku stanu w dolnej części ekranu przeglądarki widoczna jest zamknięta kłódka
- Sprawdź czy certyfikat jest wystawiony dla Bank Spółdzielczy w Skępem przez firmę Unizeto Technologies S.A.
- Pamiętaj: Bank nie wymaga potwierdzenia danych SMS-em lub mailem.
- Aktualizuj wersję przeglądarki
- Zabezpiecz swoje urządzenie (komputer, tablet, smartphome) aktualnym oprogramowaniem antywirusowym
- Regularnie aktualizuj system operacyjny
- Chronić telefon i tablet logując się do bankowości elektronicznej
- Kopiując do schowka systemu operacyjnego numer NRB, po wklejeniu sprawdź jego poprawność. Najlepiej zrezygnuj z kopiowania NRB.
- Przed podpisem przelewu, sprawdź poprawność numeru NRB.
- System automatycznie zablokuje dostęp do systemu po 5 nieudanych próbach logowania/autoryzacji.

Aktualne informacje o zagrożeniach można sprawdzić na stronie Związku Banków Polskich: <http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci>

LISTA OPERACJI WYMAGAJĄCYCH SILNEGO UWIERZYTELNIANIA ORAZ WYJĄTKI

Silne uwierzytelnianie - Sprawdzenie tożsamości użytkownika i jego prawa dostępu do rachunku za pomocą elektronicznych kanałów dostępu oparte jest na czymś CO ZNASZ (identyfikator ID i hasło, hasło stałe) oraz na tym CO MASZ (Karta mikroprocesorowa, Kod SMS).

Wszystkie operacje wykonywane w bankowości internetowej wymagają silnego uwierzytelnienia. Wyjątkiem od zastosowania silnego uwierzytelnienia jest dodanie urządzenia, z którego następuje logowanie do urządzeń zaufanych. Wyjątkiem od stosowania silnego uwierzytelnienia jest również wykonywanie przelewów z szablonów uprzednio dodanych do zaufanych.

KONTAKT Z BANKIEM

Bank Spółdzielczy w Skępem
ul. Sierpecka 72
87-630 Skępe
tel. 54 287-70-77 w dni robocze w godz. 8⁰⁰ do 15⁰⁰
e-mail: centrala@bsskepe.sgb.pl