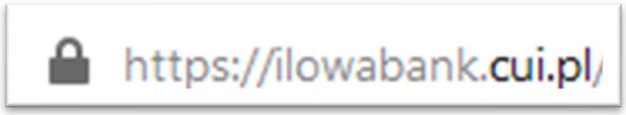
Bank Spółdzielczy w Iłowej
Grupa BPS

Przewodnik bezpiecznego korzystania z bankowości internetowej w Banku Spółdzielczym w Iłowej – autoryzacja KOD SMS

1. Przed zalogowaniem:

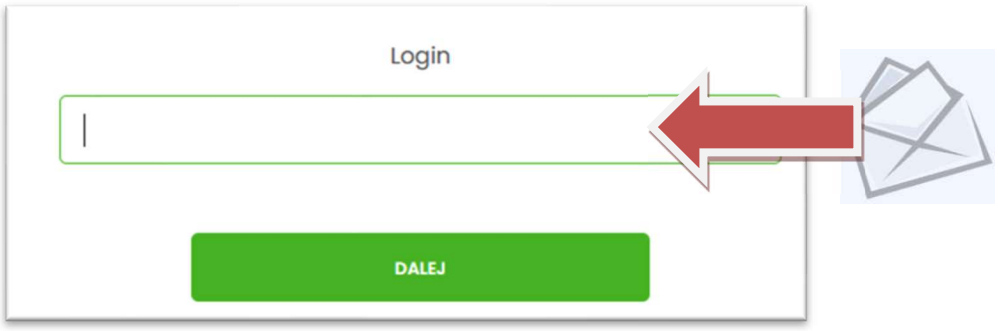
- wpisz poprawny adres internetowy i zweryfikuj certyfikat banku:



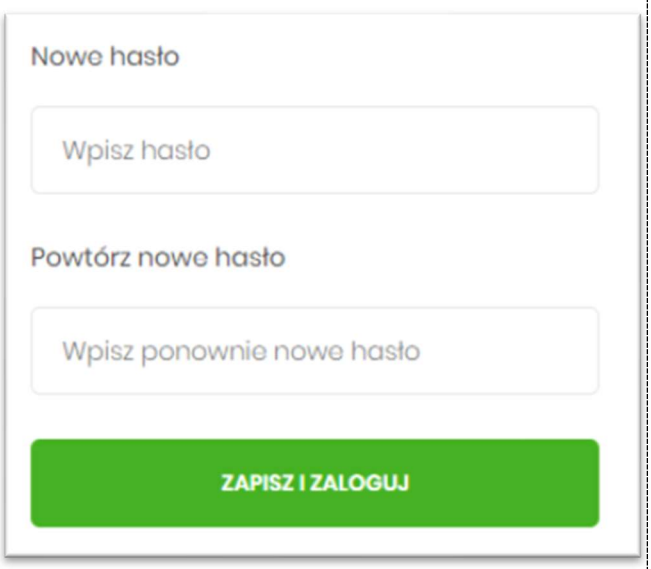
- wystawiony dla Bank Spółdzielczy w Iłowej

2. Pierwsze logowanie:

- wpisz identyfikator użytkownika nadany przez Bank w kopercie



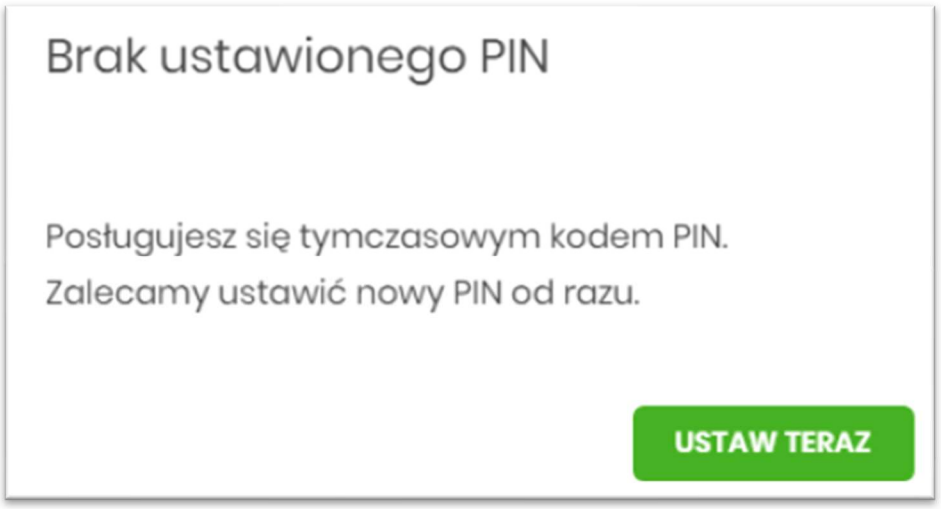
- wpisz dostarczony SMSem pierwszy kod dostępu i nadaj swoje hasło do kolejnych logowań



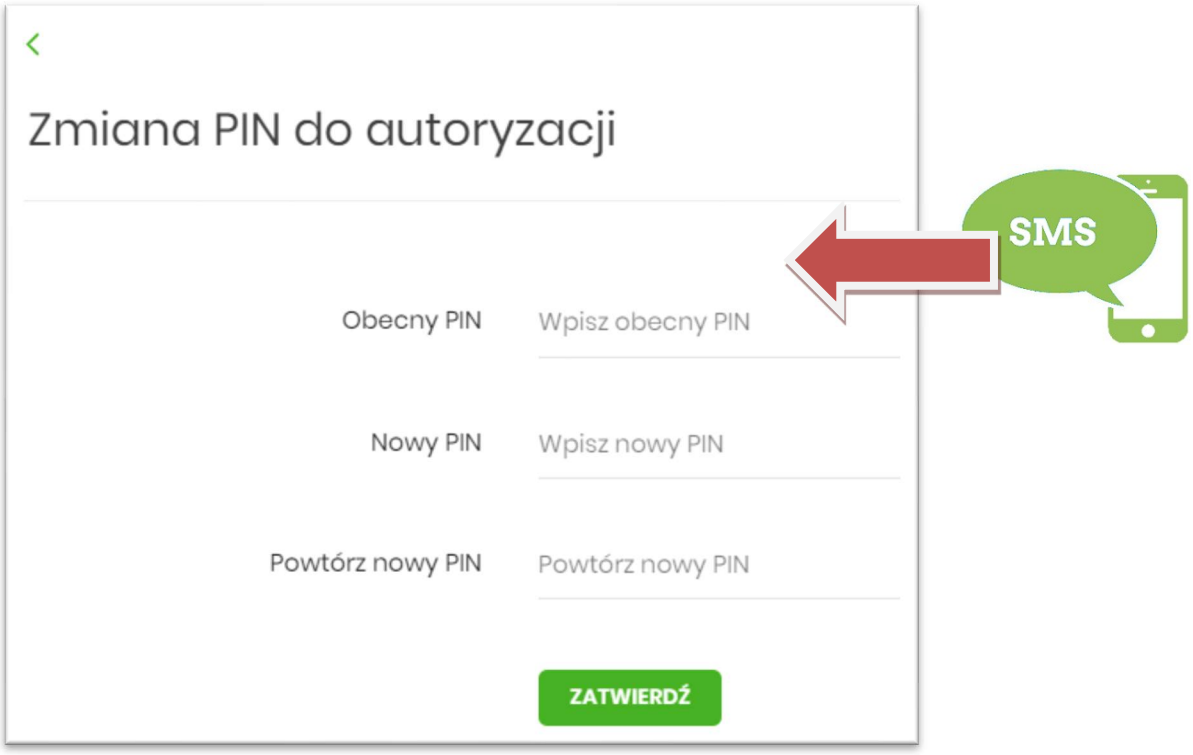
To klucz do Twojego konta (zapamiętaj je!) – hasło powinno być trudne do zgadnięcia dla innych i skutecznie chronione! Hasło powinno mieć długość minimum 10 znaków, zawierać małe i duże litery, znaki specjalne (np. ! #) i cyfry.

3. Ustawienie kodu PIN do potwierdzania dyspozycji

- Po pierwszym zalogowaniu system zaprezentuje komunikat zalecający ustawienie kodu PIN do autoryzacji przez wybranie przycisku [USTAW TERAZ]



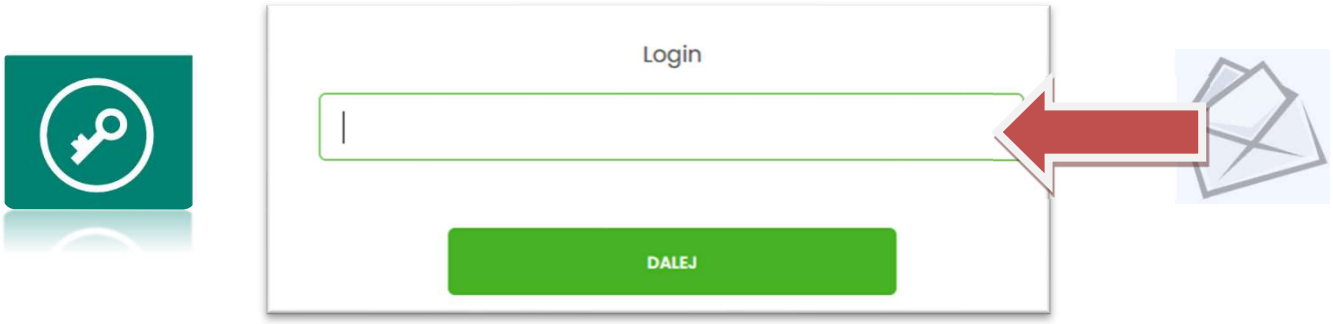
- Użytkownik musi wpisać obecny PIN tymczasowy, który otrzymał za pomocą SMS oraz wpisać i powtórzyć nowy własny PIN, a następnie kliknąć przycisk [ZATWIERDŹ].



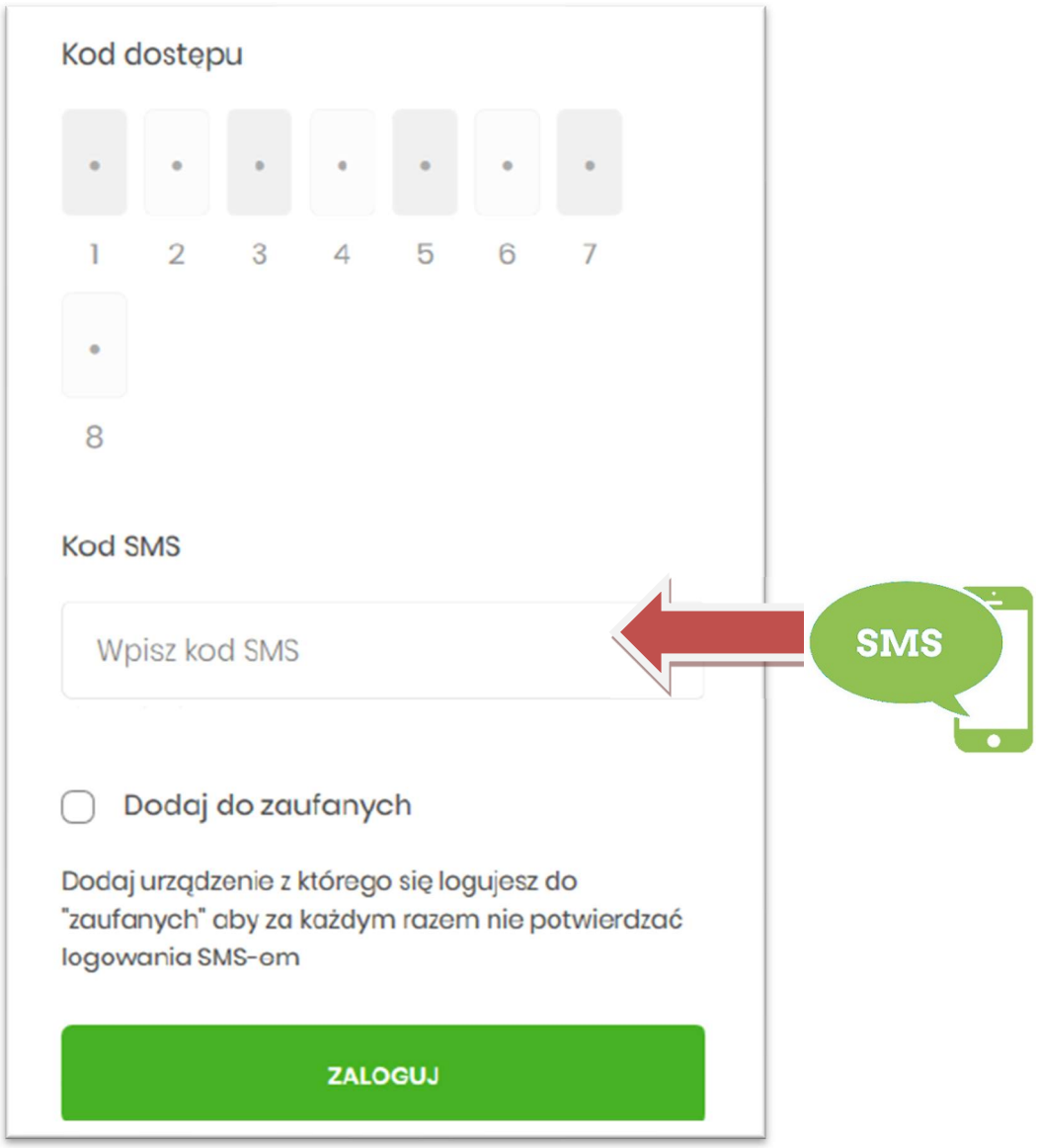
Zapamiętaj nowy (własny) PIN - będzie on wymagany do potwierdzania operacji np. przelewu.

4. Kolejne logowania do bankowości internetowej za pomocą hasła maskowanego:

- wpisz identyfikator użytkownika nadany przez Bank



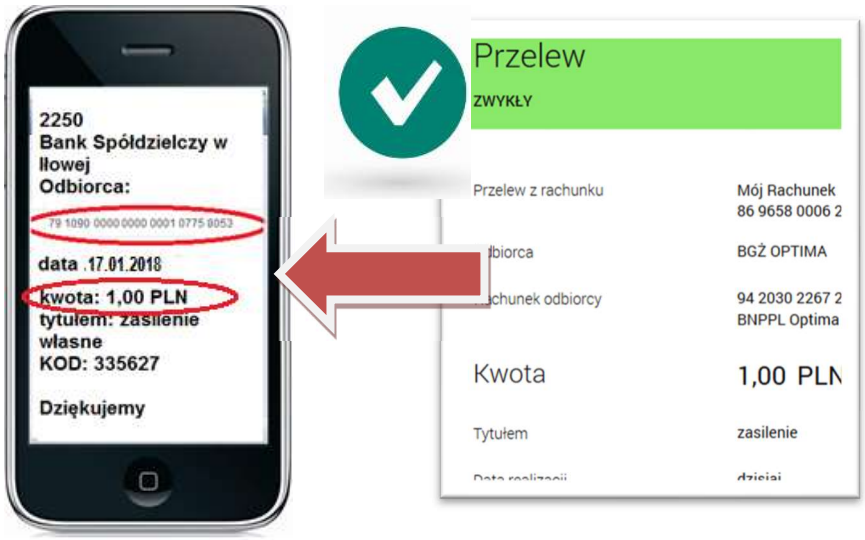
- wpisz losowo wybrane przez system pozycje ze swojego hasła, które zostało nadane przy pierwszym logowaniu w polu kod dostępu



- po poprawnym wpisaniu hasła należy wpisać aktualny kod SMS i kliknąć przycisk [ZALOGUJ]

5. Potwierdzanie operacji np. przelewu

Kolejna autoryzacja np. przelewu będzie wymagała wpisania otrzymanego kodu SMS oraz zdefiniowanego wcześniej własnego kodu PIN (w punkcie 3).



Przed wpisaniem kodu autoryzacyjnego SMS i PIN porównaj kwotę oraz numer rachunku odbiorcy z treścią SMSa!

6. Ważne informacje

- Gdy widzisz nietypowe zachowanie strony bankowości internetowej np. żądanie podania dodatkowych informacji weryfikacyjnych, po wpisaniu danych autoryzacyjnych informacja o aktualizowaniu, „proszę czekać" itp. – **traktuj to jako próbę oszustwa za pomocą złośliwego oprogramowania i natychmiast skontaktuj się z bankiem.**
- Wszelkie emaile, wiadomości i telefony w których jesteś proszony o dane autoryzacyjne typu hasła, kod sms **traktuj jako próbę oszustwa i natychmiast zgłaszaj do Banku!**

Stosuj się do poniższych zaleceń:

1. Zabezpiecz komputer i telefon aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall).
2. Regularnie aktualizuj system operacyjny, wersję przeglądarki oraz oprogramowanie na komputerze i telefonie.
3. Uważaj na nietypowe informacje z banku, nie wykonuj podejrzanych poleceń, a w szczególności nie instaluj oprogramowania z niezaufanego źródła.
4. Po zakończeniu pracy w bankowości elektronicznej wyloguj się.
5. Nie instaluj oprogramowania jeżeli instrukcja instalacji zawiera zalecenie rezygnacji ze skanowania aplikacji oprogramowaniem antywirusowym.
6. Chroń dane dostępowe do bankowości elektronicznej.
7. Nie loguj się i nie dokonuj płatności w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hot-spotach i niezabezpieczonych sieciach WIFI.
8. Sprawdź poprawność numeru rachunku przed i po podpisie przelewu.
9. Zwróć szczególną uwagę na poprawność numeru rachunku po wklejeniu go ze schowka systemu.
10. Nie otwieraj załączników email pochodzących z nieznanego źródła – może to być złośliwe oprogramowanie służące do kradzieży.

Aktualności, zagrożenia oraz szczegółowe informacje znajdują się na stronie Banku pod adresem www.bsilowa.pl