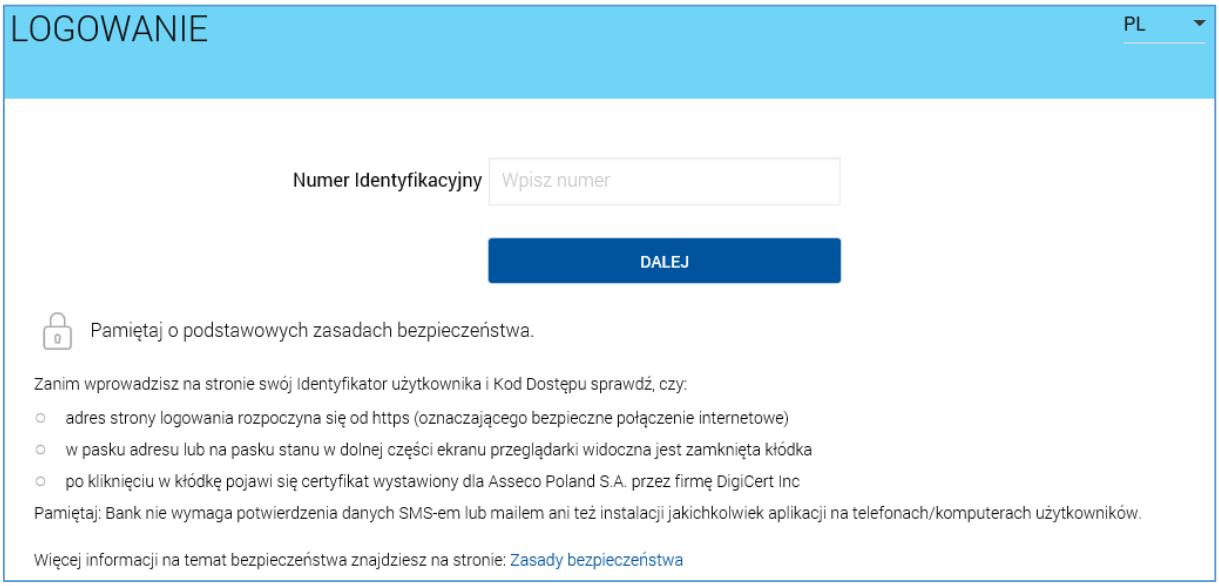
Gospodarczy Bank Spółdzielczy w Mosinie
Spółdzielcza Grupa Bankowa

Skrócona instrukcja logowania do bankowości internetowej

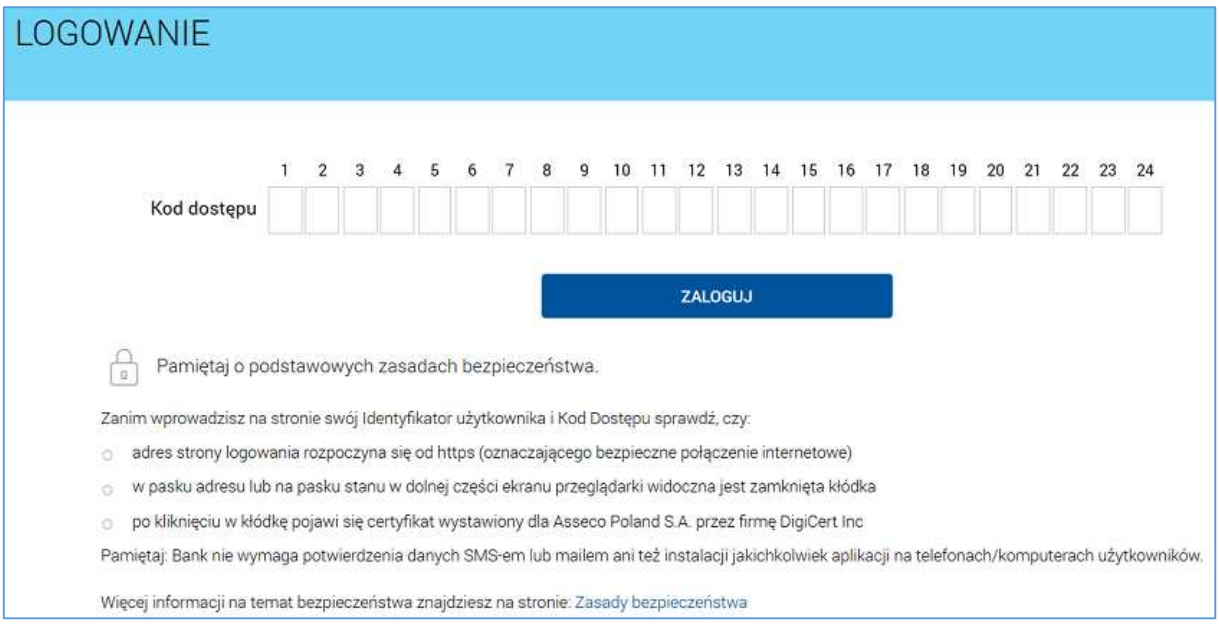
w Gospodarczym Banku Spółdzielczym w Mosinie
(dotyczy klientów indywidualnych / detalicznych)

Pierwsze logowanie za pomocą hasła maskowalnego.

1. Uruchom przeglądarkę internetową i przejdź do witryny ***www.gbsmosina.pl***.
2. Po wczytaniu witryny Gospodarczego Banku Spółdzielczego w Mosinie kliknij (po prawej stronie) w link ***„Bank dla klienta indywidualnego”***.
3. W nowo otwartym oknie przeglądarki w polu ***„Numer Identyfikacyjny”*** podaj ciąg 9 znaków (identyfikator użytkownika) otrzymany z banku i kliknij przycisk ***„DALEJ”***.



4. W kolejnym etapie w polu ***„Kod dostępu”*** podaj wszystkie litery/cyfry występujące w haśle otrzymanym z banku, a następnie kliknij ***„ZALOGUJ”***. Każde ponumerowane pole „Kodu dostępu” odpowiada jednemu znakowi występującemu w haśle. Jeśli hasło składa się z 8 znaków, to należy je wpisać w pierwsze 8 ponumerowanych pól (pozostałe pola pozostaw puste).



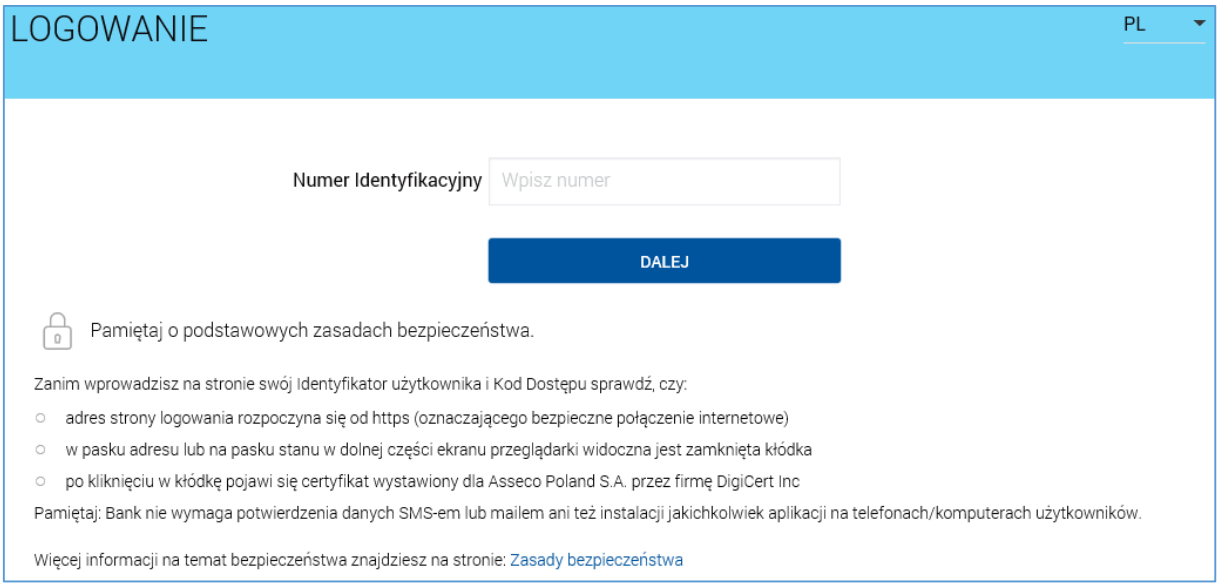
5. Po podaniu wszystkich liter/cyfr występujących w haśle otrzymanym z banku, kliknij ***„ZALOGUJ”***.

6. W kolejnym etapie wprowadź własne hasło maskowalne.
   Własne hasło maskowalne musi mieć długość minimum 10 znaków, a maksymalnie może zawierać 24 znaki. We własnym haśle maskowalnym nie należy używać polskich znaków.

   Po pomyślnym wpisaniu i zatwierdzeniu własnego hasła maskowalnego, od tego momentu logowanie do konta internetowego będzie wymagało podania kodu dostępu w postaci:
   losowo wybranych znaków z własnego hasła maskowalnego*.*

Drugie i kolejne logowanie za pomocą hasła maskowalnego.

1. Uruchom przeglądarkę internetową i przejdź do witryny ***www.gbsmosina.pl***.
2. Po wczytaniu witryny Gospodarczego Banku Spółdzielczego w Mosinie kliknij (po prawej stronie) w link ***„Bank dla klienta indywidualnego”***.
3. W nowo otwartym oknie przeglądarki w polu ***„Numer Identyfikacyjny”*** podaj ciąg 9 znaków (identyfikator użytkownika) otrzymany z banku i kliknij przycisk ***„DALEJ”***.



4. W kolejnym etapie w polu ***„Kod dostępu”*** podaj losowo wybrane znaki z własnego hasła maskowalnego, a następnie kliknij ***„ZALOGUJ”***. W poniższym przykładzie należy podać pierwszy, trzeci, czwarty, szósty, siódmy i ósmy znak własnego hasła maskowalnego. Każde ponumerowane pole „Kodu dostępu” odpowiada jednemu znakowi występującemu w haśle maskowalnym.

… UWAGA …

Po 10 nieudanych próbach zalogowania się do konta internetowego (za pomocą hasła maskowalnego), dostęp zostanie automatycznie zablokowany na okres 6 godzin. Po 6 godzinach dostęp do konta internetowego zostanie automatycznie odblokowany. Jeżeli użytkownik będzie miał potrzebę szybszego odblokowania dostępu do konta internetowego, w takim przypadku należy skontaktować się z działem obsługi bankowości internetowej w celu odblokowania dostępu do konta internetowego (tel. **+48 61 81 97 708** lub **+48 61 81 97 728**, od **poniedziałku** do **piątku** w godz. **8:00** - **18:00**). Po odblokowaniu w/w dostępu, logowanie do konta internetowego przebiega podobnie jak przy pierwszym logowaniu za pomocą hasła maskowalnego – różnica polega na tym, że klient otrzymuje „Kod dostępu" w postaci wiadomości SMS na swój numer telefonu komórkowego.

… BEZPIECZEŃSTWO …

1. Zawsze sprawdzaj adres internetowy strony logowania do bankowości internetowej. W przypadku Gospodarczego Banku Spółdzielczego w Mosinie, adres internetowy strony logowania do bankowości internetowej to „**https://cbp.cui.pl**" lub „**cbp.cui.pl**" („Bank dla klienta indywidualnego").
2. Zawsze sprawdzaj czy połączenie z bankowością internetową jest szyfrowane - na pasku adresu lub obok paska adresowego (w którym dla Gospodarczego Banku Spółdzielczego w Mosinie musi widnieć adres „**https://cbp.cui.pl**" lub „**cbp.cui.pl**") musi być widoczny symbol „***zatrzaśniętej kłódki***". Współczesne przeglądarki internetowe sygnalizują połączenie szyfrowane znakiem ***zielonej*** „***zatrzaśniętej kłódki***" na pasku adresu. Brak „zatrzaśniętej kłódki" lub „kłódka przekreślona" oznaczają, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane. W takim przypadku prosimy o zaprzestanie używania wyświetlonej strony internetowej i kontakt z działem obsługi bankowości internetowej banku.
3. Nigdy nie ignoruj ostrzeżeń przeglądarek internetowych o błędnych certyfikatach na stronach bankowości internetowej.
4. Nie wchodź w linki do bankowości internetowej przesyłane w mailach.
5. Uważaj na fałszywe e-maile od nieznanych osób i załączniki dołączane do e-maili - szczególnie dotyczące rzekomych przesyłek, ciekawych artykułów, wezwań do zapłaty, faktur do opłacenia, itp. Zawsze sprawdzaj adres, z którego została przesłana wiadomość, a w przypadku wątpliwości skontaktuj się telefonicznie z firmą, od której rzekomo pochodzi.
6. Zadbaj o regularną zmianę hasła do bankowości internetowej. Nie powinno być ono zbyt proste. Nie zapisuj danych logowania w przeglądarkach internetowych i/lub na dyskach twardych komputerów.
7. Chroń dane do logowania do bankowości internetowej - nie przekazuj ich nawet najbliższym osobom. Jeśli chcesz, aby powyższe osoby mogły korzystać z Twojego konta w bankowości internetowej, możesz ustanowić dla nich w banku stosowne pełnomocnictwo.
8. Po zakończeniu pracy w bankowości internetowej wyloguj się używając przeznaczonej do tego opcji, gwarantuje to poprawne zamknięcie sesji przez użytkownika.
9. Nie loguj się do bankowości internetowej z ogólnodostępnych komputerów i nie korzystaj z bankowości internetowej poprzez nieznane Tobie, niezabezpieczone sieci wifi (np. w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hot-spotach).
10. Aktualizuj na bieżąco system operacyjny komputera i przeglądarki internetowe z których korzystasz.
11. Na komputerach na których korzystasz z bankowości internetowej używaj aktualizowanego na bieżąco programu antywirusowego.
12. Czytaj dokładnie treść SMS'ów autoryzacyjnych - treść powinna dokładnie zgadzać się z transakcją, którą zlecasz w serwisie bankowości internetowej.
13. Sprawdzaj poprawność numeru NRB odbiorcy przed i po zatwierdzeniu przelewu do dyspozycji w bankowości internetowej.

14. Jeśli otrzymasz komunikat o przerwie konserwacyjnej bankowości internetowej podczas realizacji przelewu, zrezygnuj z dalszej realizacji przelewu i skontaktuj się z działem obsługi bankowości internetowej banku.