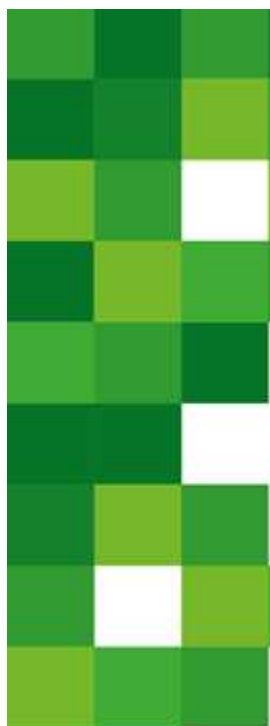


PIERWSZE LOGOWANIE DO BANKOWOŚCI INTERNETOWEJ SGB24 Z WYKORZYSTANIEM KODÓW SMS

1. W pierwszym kroku należy wejść na stronę internetową Banku: www.bsnowe.com.pl.
2. Wybieramy opcję 'Bankowość internetowa' lub wchodzimy bezpośrednio na stronę internetową <https://sgb24.pl>
3. Wpisujemy identyfikator otrzymany z Banku rozpoczynający się od NO.....



Logowanie


Zaloguj się do bankowości internetowej

Identyfikator

DALEJ

PL

KOMUNIKATY BEZPIECZEŃSTWA
BEZPIECZNE ZAKUPY W INTERNECIE



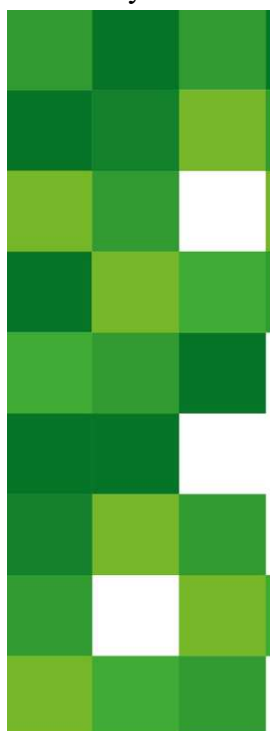
Pamiętaj o zasadach bezpieczeństwa.

- Wpisuj adres strony logowania do Bankowości Internetowej SGB24 lub korzystaj z oficjalnej strony Banku - nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce. Adres strony logowania rozpoczyna się od https:// (adres strony logowania rozpoczyna się od https://adresu instrukcyjnego bezpiecznego połączenia internetowego).
- Zawsze sprawdzaj adres strony www, na której się logujesz. Adres rozpoczyna się od https:// (w adresie strony widnieje wyłącznie domena sgb24.pl). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla sgb24.pl przez firmę Digicert. Możesz to sprawdzić, klikając w kłódkę.
- Nigdy nie loguj się do Bankowości Internetowej za pośrednictwem linku otrzymanego w wiadomości e-mail/ sms lub będącego wynikiem wyszukiwania w przeglądarce.

Pamiętaj!
Bank nie wymaga potwierdzenia danych SMS-em lub mailem oraz instalacji jakichkolwiek aplikacji na komputerach użytkowników. W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolinii Banku.

- 800 88 88 88
- (+48) 61 647 28 46 (dla połączeń komórkowych oraz z zagranicy)

4. Wpisujemy ośmioznakowe hasło otrzymane wiadomością SMS (hasło zostanie wysłane SMS-em dopiero w po wpisaniu identyfikatora i po kliknięciu 'DALEJ'). Po wpisaniu hasła naciskamy ZALOGUJ.



Logowanie

Zaloguj się do bankowości internetowej




Hasło

ZALOGUJ

COFNIJ

KOMUNIKATY BEZPIECZEŃSTWA
BEZPIECZNE ZAKUPY W INTERNECIE



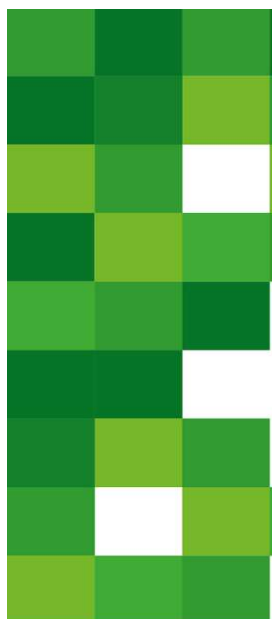
Pamiętaj o zasadach bezpieczeństwa.

- Wpisuj adres strony logowania do Bankowości Internetowej SGB24 lub korzystaj z oficjalnej strony Banku - nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce. Adres strony logowania rozpoczyna się od https:// (adres strony logowania rozpoczyna się od https://adresu instrukcyjnego bezpiecznego połączenia internetowego).
- Zawsze sprawdzaj adres strony www, na której się logujesz. Adres rozpoczyna się od https:// (w adresie strony widnieje wyłącznie domena sgb24.pl). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla sgb24.pl przez firmę Digicert. Możesz to sprawdzić, klikając w kłódkę.
- Nigdy nie loguj się do Bankowości Internetowej za pośrednictwem linku otrzymanego w wiadomości e-mail/ sms lub będącego wynikiem wyszukiwania w przeglądarce.

Pamiętaj!
Bank nie wymaga potwierdzenia danych SMS-em lub mailem oraz instalacji jakichkolwiek aplikacji na komputerach użytkowników. W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolinii Banku.

- 800 88 88 88
- (+48) 61 647 28 46 (dla połączeń komórkowych oraz z zagranicy)

4. Przepisujemy kod logowania który został wysłany SMS-em a następnie klikamy 'ZALOGUJ'.



Logowanie
Zaloguj się do bankowości internetowej

Hasło
.....

Kod SMS
Wpisz kod SMS

ZALOGUJ

COFNUJ

KOMUNIKATY BEZPIECZEŃSTWA
BEZPIECZNE ZAKUPY W INTERNecie

Bankowość w wersji mobilnej w aplikacji SGB Mobile!

Pamiętaj o zasadach bezpieczeństwa.

- Wpisuj adres strony logowania do Bankowości Internetowej SGB24 lub korzystaj z oficjalnej strony Banku – nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce. Adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe).
- Zawsze sprawdzaj adres strony www, na której się logujesz. Adres rozpoczyna się od https:// (w adresie strony widnieje wyłącznie domena sgb24.pl). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla sgb24.pl przez firmę DigiCert. Możesz to sprawdzić, klikając w kłódkę.
- Nigdy nie loguj się do Bankowości Internetowej za pośrednictwem linku otrzymanego w wiadomości e-mail/ sms lub będącego wynikiem wyszukiwania w przeglądarce.

Pamiętaj!
Bank nie wymaga potwierdzenia danych SMS-em lub mailem oraz instalacji jakichkolwiek aplikacji na komputerach użytkowników. W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolinii Banku

- 800 88 88 88
- (+48) 61 647 28 46 (dla połączeń komórkowych oraz z zagranicy)

5. Ostatnią czynnością jest stworzenie własnego hasła do logowania. Po wpisaniu hasła użytkownik może zaznaczyć opcję „Użyj tego samego hasła do autoryzacji” dzięki czemu wpisane hasło automatycznie stanie się również PIN-em do podpisywania autoryzacji.

Zasady budowy haseł są następujące:

- musi składać się z 8-20 znaków
- musi zawierać przynajmniej jedną wielką literę
- musi zawierać przynajmniej jedną małą literę
- musi zawierać przynajmniej jedną cyfrę



Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika
NOOI

Nowe hasło
Wpisz hasło

Powtórz nowe hasło
Wpisz ponownie nowe hasło

Użyj tego samego hasła do autoryzacji

ZAPISZ I ZALOGUJ

COFNUJ

Bankowość w wersji mobilnej w aplikacji SGB Mobile!

Pamiętaj o zasadach bezpieczeństwa.

- Wpisuj adres strony logowania do Bankowości Internetowej SGB24 lub korzystaj z oficjalnej strony Banku – nie korzystaj ze stron pojawiających się w wynikach wyszukiwania w przeglądarce. Adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe).
- Zawsze sprawdzaj adres strony www, na której się logujesz. Adres rozpoczyna się od https:// (w adresie strony widnieje wyłącznie domena sgb24.pl). Pamiętaj również o weryfikacji ważności certyfikatu wystawionego dla sgb24.pl przez firmę DigiCert. Możesz to sprawdzić, klikając w kłódkę.
- Nigdy nie loguj się do Bankowości Internetowej za pośrednictwem linku otrzymanego w wiadomości e-mail/ sms lub będącego wynikiem wyszukiwania w przeglądarce.

Pamiętaj!
Bank nie wymaga potwierdzenia danych SMS-em lub mailem oraz instalacji jakichkolwiek aplikacji na komputerach użytkowników. W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolinii Banku

Po wpisaniu hasła klikamy 'ZAPISZ I ZALOGUJ' a w przeglądarce uruchomi się strona główna bankowości internetowej SGB24.

AUTORYZACJA DYSPOZYCJI

A) Podczas pierwszego logowania nie zaznaczono „Użyj tego samego hasła do autoryzacji”

1. Przy wykonywaniu przelewu należy w polu (1) ‘Podaj hasło’ wpisać swoje hasło do logowania.
2. W polu (2) ‘Podaj kod SMS’ wpisujemy kod z SMS-a wysłanego na nr tel. kom.

Nadawca:	BARTC JEV 86-176
Odbiorca:	Legia Legia Bał
Rachunek odbiorcy:	33 1090 1678 000 Santander Bank Polska S.A. 1 o. w Grudziądzu
Kwota:	1,00 PLN
Tytułem:	wpłata
Data realizacji:	Dzisiaj
Rodzaj przelewu:	Elixir i wewnętrzny
UKRYJ DODATKOWE INFORMACJE	
Data dostarczenia:	Dzisiaj, 1
Opłaty:	1,00 PLN - Przelewy Elixir
1	<input type="password" value="Podaj hasło :"/>
2	<input type="password" value="Podaj kod SMS:"/>
Operacja nr _____ z dnia 06	
AKCEPTUJ	

3. Po uzupełnieniu danych klikamy w przycisk ‘AKCEPTUJ’.

B) Podczas pierwszego logowania nie zaznaczono „Użyj tego samego hasła do autoryzacji”

1. Przy wykonywaniu przelewu system poinformuje że konieczne jest ustawienie swojego hasła do autoryzacji i poprosi o przejście do ustawień.
2. Po przejściu do ustawień zostanie wyświetlone okno:

[i](#) [x](#)

Zmiana hasła do autoryzacji

Pamiętaj!
Jeżeli wykonałeś reset hasła to w polu „Obecne hasło” podaj tymczasowe hasło otrzymane SMS-em.

1	Obecne hasło	<input type="password" value="Wpisz obecne hasło"/>
2	Nowe hasło	<input type="password" value="Wpisz nowe hasło"/>
3	Powtórz nowe hasło	<input type="password" value="Powtórz nowe hasło"/>

ZATWIERDŹ

Zadbaj o zachowanie poufności swojego hasła.

- Nie udostępniaj hasła innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na żądania otrzymane od pracowników banku.
- Definiując swoje hasło pamiętaj o zachowaniu zasad bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

3. W polu (1) obecne hasło wpisujemy hasło tymczasowej do autoryzacji wysłane SMS-em.
4. W Polu (2) i (3) wymyślamy i wpisujemy nowe wymyślane hasło służące do autoryzacji.
5. Po wpisaniu wszystkich danych klikamy 'ZATWIERDŹ' a następnie wracamy do pulpitu i ponownie wprowadzamy przelew.
6. Od teraz przy wykonywaniu przelewu należy w polu (1) 'Podaj hasło' wpisywać swoje hasło (które wymyśliliśmy w pkt. 4).
7. W polu (2) 'Podaj kod SMS' wpisujemy kod z SMS-a wysłanego na nr tel. kom.

Nadawca:	BARTC JEV 86-170
Odbiorca:	Legia Legia Bai
Rachunek odbiorcy:	33 1090 1678 000 Santander Bank Polska S.A. 1 o. w Grudziądzu
Kwota:	1,00 PLN
Tytułem:	wpłata
Data realizacji:	Dzisiaj
Rodzaj przelewu:	Elixir i wewnętrzny
UKRYJ DODATKOWE INFORMACJE	
Data dostarczenia:	Dzisiaj, 1
Opłaty:	1,00 PLN - Przelewy Elixir
1	<input type="password" value="Podaj hasło :"/>
2	<input type="password" value="Podaj kod SMS:"/>
Operacja nr z dnia 06	
AKCEPTUJ	

8. Po uzupełnieniu danych klikamy w przycisk 'AKCEPTUJ'.

Bezpieczeństwo w Internecie

Poznaj najważniejsze zasady bezpieczeństwa w Internecie.

Pamiętaj! Jeśli coś budzi Twoją wątpliwość lub nie działa tak jak powinno, jak najszybciej skontaktuj się z infolinią banku. Czytaj komunikaty bezpieczeństwa, które regularnie zamieszczamy na stronie www.sgb.pl/komunikaty-o-bezpieczenstwie/

Bankowość internetowa

- Nigdy nie loguj się do bankowości internetowej z linku, który przyszedł do Ciebie mailem lub SMS-em, ani poprzez link z wyszukiwarki. Wpisuj adres strony logowania ręcznie lub korzystaj z przycisku logowania na oficjalnej stronie banku.
- Nie udostępniaj hasła innym osobom, na żadnych stronach internetowych, pocztą elektroniczną, wiadomością SMS lub w odpowiedzi na żądania otrzymane od pracowników banku.
- Sprawdzaj adresy stron www, na których się logujesz, oraz ważność ich certyfikatów. Adres strony logowania powinien zaczynać się od **https**

- Zadbaj o skomplikowane hasła, unikatowe i trudne do odgadnięcia przez postronne osoby.
- Nie używaj tego samego hasła do różnych kont.
- Nie zapisuj haseł na kartkach ani w plikach na komputerze.
- Login i hasło do bankowości oraz numery kart to dane, które powinny być znane tylko Tobie. Nigdy nie podawaj ich innym.
- Nie loguj się przez publiczną, niezabezpieczoną sieć wi-fi lub hotspot do bankowości internetowej czy aplikacji mobilnej.
- Nie loguj się do bankowości na urządzeniach publicznie dostępnych, np. w kafejkach czy w hotelach.
- Pamiętaj aby po każdej sesji wylogować się z bankowości internetowej.
- Ustaw bezpieczne limity operacji dla przelewów, płatności kartami i wypłat gotówki.

Komputer i telefon

- Regularnie aktualizuj oprogramowanie na komputerze i telefonie (system, aplikacje, przeglądarkę, antywirusy).
- Używaj zapory sieciowej (firewall) i systematycznie skanuj komputer programem antywirusowym.
- Nie instaluj na komputerze i smartfonie oprogramowania z nieznanego źródła.
- Nie podłączaj zewnętrznych nośników danych (np. pendrive) do swojego komputera, jeśli nie masz pewności co do ich bezpieczeństwa. Podobnie z podłączaniem telefonu do komputera.
- Pobieraj aplikację mobilną banku i jej aktualizacje wyłącznie z autoryzowanych sklepów: Google Play i App Store.
- Zawsze blokuj dostęp do telefonu i komputera. Zabezpiecz telefon hasłem, wzorem, odciskiem palca lub Face ID.
- W razie utraty karty lub telefonu z aktywną aplikacją – od razu je zablokuj. Kartę możesz zablokować przez bankowość internetową lub mobilną, a aplikację przez infolinię banku.

Podejrzany kontakt

- Zastanawia Cię wiadomość o dziwnym zamówieniu lub zaległej płatności? Przed podjęciem czynności w niej wskazanej skontaktuj się z biurem obsługi klienta firmy, która wysłała tę wiadomość.
- Nie otwieraj załączników w niespodziewanych mailach, jeśli nie wiesz co może w nich być.
- Nie klikaj w linki i nie pobieraj żadnych aplikacji, jeśli nie znasz nadawcy wiadomości.
- Dokładnie czytaj powiadomienia o transakcjach, w tym SMS-y – jeśli coś się nie zgadza, nie zatwierdzaj operacji.
- Jeżeli dzwoni do Ciebie przedstawiciel banku, ale nie masz pewności, że nim jest – zerwij połączenie. Potem samodzielnie zadzwoń na naszą infolinię.
- Nie przekazuj kodu BLIK nikomu, nawet znajomemu.
- Kupujesz w nowym sklepie? Poszukaj opinii na jego temat (z różnych źródeł)
- Nie podawaj PIN-u do karty podczas zakupów w Internecie. Do potwierdzenia transakcji kartą w Internecie nigdy nie jest wymagane podanie PIN.