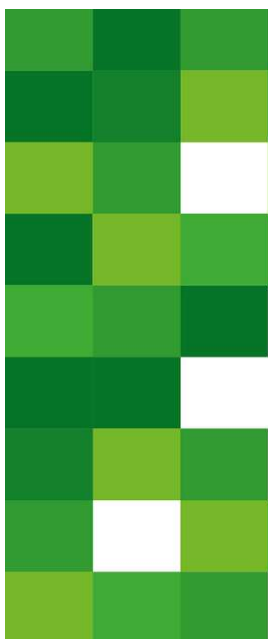


PIERWSZE LOGOWANIE DO BANKOWOŚCI INTERNETOWEJ SGB24 Z WYKORZYSTANIEM APLIKACJI MOBILNEJ TOKEN SGB


1. W pierwszym kroku należy zainstalować na urządzeniu aplikację mobilną **Token SGB** ze **Sklepu Play** lub **Apple Store**.
2. Wchodzimy na stronę internetową Banku: www.bsnowe.com.pl.
3. Wybieramy opcję 'Bankowość internetowa' lub wchodzimy bezpośrednio na stronę internetową <https://sgb24.pl>
4. Wpisujemy Identyfikator otrzymany z Banku rozpoczynający się od **NO.....**




Logowanie
Zaloguj się do bankowości internetowej

Identyfikator

DALEJ

PL  **KOMUNIKATY BEZPIECZEŃSTWA
BEZPIECZNE ZAKUPIY W INTERNECIE**



Bankowość w wersji mobilnej w aplikacji **SGB Mobile!**

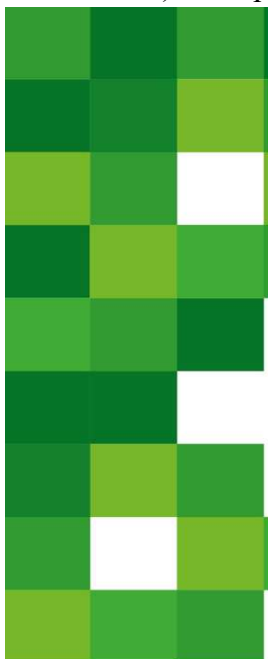
Pamiętaj o zasadach bezpieczeństwa.

- 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. Wpisujemy tymczasowe hasło do logowania (ośmioznakowe hasło otrzymane wiadomością SMS. Hasło zostanie wysłane SMS-em dopiero po wpisaniu identyfikatora i po kliknięciu 'DALEJ'). Po wpisaniu hasła klikamy **ZALOGUJ**.



Logowanie
Zaloguj się do bankowości internetowej




Hasło

ZALOGUJ

COFNUJ

**KOMUNIKATY BEZPIECZEŃSTWA
BEZPIECZNE ZAKUPIY 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)

Następnie system poprosi o wprowadzenie nowego hasła, które będzie służyło do kolejnych logowań.

Polityka bezpieczeństwa banku wymaga zmiany hasła.

Identyfikator użytkownika
NOS

Nowe hasło

Powtórz nowe hasło

DALEJ

COFNIJ



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

Zasady budowy hasel 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

Jeżeli hasło zostało wprowadzone poprawnie w obu polach, naciskamy DALEJ. Na nowo otwartej stronie pojawi okno, w którym widnieje prośba o wpisanie nazwy urządzenia, na którym będziemy instalować aplikację Token SGB.

Nazwa ta jest wykorzystywana tylko dla nas samych, np. celem identyfikacji urządzeń, które są podpisane pod bankowość elektroniczną. Możemy tu wpisać np. **Telefon, tablet, Samsung itp.**



Urządzenie autoryzujące

Nazwa urządzenia

DALEJ

COFNIJ



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

Po wpisaniu nazwy urządzenia klikamy ZALOGUJ. System wygeneruje kod aktywacyjny, który następnie wpisujemy w aplikacji mobilnej Token SGB.

The image shows two parts of the SGB activation process. On the left is a page titled "Urządzenie autoryzujące" (Authorizing device). It asks for an activation code, shows a blurred code "4 000 J", and provides instructions: "W celu dokończenia procesu aktywacji zainstaluj na urządzeniu mobilnym aplikację Token SGB, pobierając ją ze sklepu Google Play (Android) lub App Store (iOS), a następnie wprowadź powyższy kod w urządzeniu autoryzującym: telefon". It also mentions that during activation, the user will be asked for a verification code sent via SMS to the number "64*****". At the bottom, it says "Parowanie urządzenia autoryzującego w toku." and "Kod jest ważny 5 minut" with an "OK" button.

On the right is a security page titled "Pamiętaj o zasadach bezpieczeństwa." (Remember the security rules). It lists three points: 1. Use the login address for SGB Internet Banking or the official bank website, not search engines. 2. Always check the website address (https://) and domain (sgb24.pl). 3. Never log in via links from emails or SMS. A yellow box at the bottom says "Pamiętaj! Bank nie wymaga potwierdzenia danych SMS-em lub mail-em oraz instalacji jakichkolwiek aplikacji na komputerach użytkowników. W przypadku wystąpienia nieprawidłowości niezwłocznie skontaktuj się z Doradcą Infolinii Banku".

Powiązanie aplikacji mobilnej Token SGB z bankowością internetową SGB24

W pierwszym kroku po uruchomieniu aplikacji należy nacisnąć klawisz 'REJESTRACJA URZĄDZENIA' i wprowadzić kod aktywacyjny wygenerowany w przeglądarce internetowej.

The image shows the "REJESTRACJA URZĄDZENIA" (Device Registration) screen in the SGB mobile app. The left side has a green background with a monitor icon and text: "Skorzystanie z aplikacji mobilnej wymaga aktywacji aplikacji. W tym celu należy zalogować się do bankowości internetowej i zarejestrować urządzenie". At the bottom is a button "REJESTRACJA URZĄDZENIA".

The right side has a white background with a monitor icon and text: "Przepisz kod aktywacyjny wyświetlony w bankowości internetowej". Below this is a text input field "Wprowadź kod aktywacyjny". Underneath is a numeric keypad with digits 1-9, 0, and a delete icon (X). At the bottom is a button "DALEJ".

W następnym kroku w celu identyfikacji, należy wprowadzić kod weryfikacyjny, który został wysłany SMS-em.

The image displays two screenshots of the SGB mobile application registration process. Both screens feature the SGB logo and the text 'Banki Spółdzielcze' at the top. The left screen is titled '← REJESTRACJA URZĄDZENIA' and contains the instruction: 'W celu identyfikacji konieczne jest podanie kodu weryfikacyjnego, który zostanie przesłany za pomocą SMS'. Below this is a text input field labeled 'Wprowadź kod weryfikacyjny' and a 3x3 numeric keypad with digits 1-9, 0, and a delete key (⊗). The right screen is also titled '← REJESTRACJA URZĄDZENIA' and contains the instruction: 'Wprowadź PIN, który będzie służył do logowania do aplikacji'. Below this is a text input field labeled 'Wprowadź PIN' with a question mark icon, and a 3x3 numeric keypad with digits 1-9, 0, and a delete key (⊗). At the bottom of both screens are green buttons with a right arrow and the text 'DALEJ'.

Następnie w polu należy wprowadzić kod PIN, który będzie służył do logowania w aplikacji Token SGB. Nadawany nr PIN musi posiadać następujące właściwości:

- musi zawierać od 5 do 8 cyfr,
- nie może zawierać podobnych cyfr lub wg kolejności (1111, 2222, 123123, 12345)

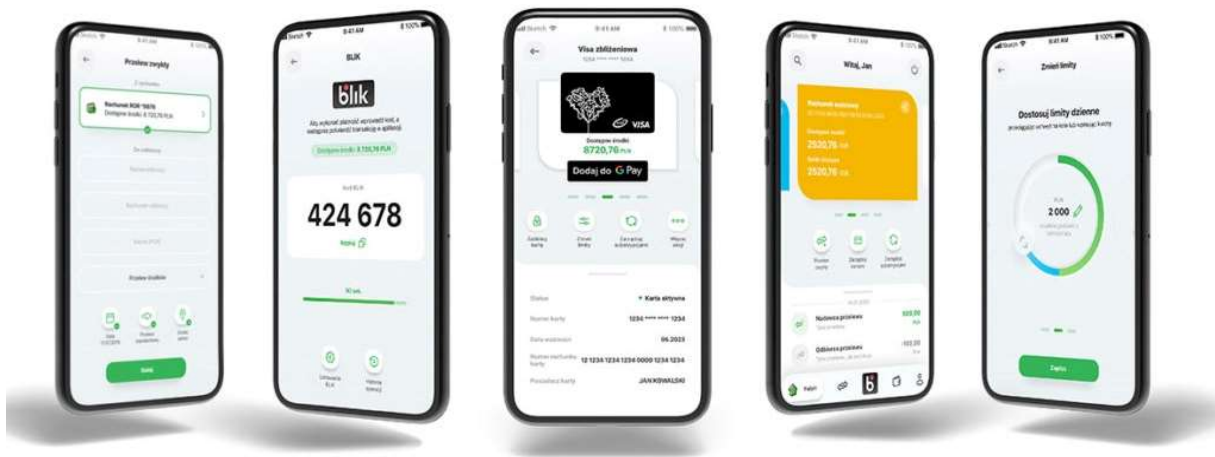
W ostatnim kroku należy ponownie wprowadzić kod PIN i wcisnąć klawisz DALEJ.

Podczas kolejnych logowań za pośrednictwem komputera, w przeglądarce należy wprowadzić Identyfikator, następnie hasło a następnie należy zalogować się do aplikacji mobilnej **Token SGB** ustalonym kodem PIN i uwierzytelnić klikając „akceptuj”.

Filmy instruktażowe

W portalu **YouTube** zostały opublikowane filmy dotyczące powyższych czynności. Filmy można otworzyć skanując poniższe kody QR za pomocą aparatu telefonu.





Aplikacja Token SGB służy tylko do autoryzacji dyspozycji dlatego też gorąco zachęcamy do korzystania z Aplikacji mobilnej SGB Mobile (dostępna w sklepach **Google Play** i **App Store**). Co daje SGB Mobile ?

masz dostęp do wszystkich swoich rachunków i kart bankomatowych

- możesz sprawdzić stan konta, historię wydatków i wpływów, historię transakcji kartowych, transakcji **BLIK**
- szczegółowe informacje o koncie.

realizujesz przelewy w dowolnym momencie

- łatwo i bezpiecznie zrealizujesz przelew
- z funkcją "Ponów" wszystkie dane wypełnią się automatycznie

korzystasz z **AutoPay**

- Stanie w kolejce do bramki na autostradzie to nie jest Twoje ulubione zajęcie? Uruchom usługę automatycznych przejazdów przez autostrady w SGB Mobile i sam decyduj kiedy się zatrzymasz

korzystasz z portfeli cyfrowych i **BLIKA**

- szybko aktywujesz usługę **BLIK**
- dodasz swoją kartę do portfela cyfrowego **Google Pay** lub **Apple Pay**.
- możesz zablokować karty w portfelach cyfrowych na wszystkich urządzeniach mobilnych

zarządzasz subskrypcjami

- sprawdzisz w jakich sklepach internetowych zarejestrowana jest Twoja karta
- możesz zablokować płatności takich usług jak np. **Netflix, Spotify, Tidal** i innych

zmieniasz limity

- limity kart bankomatowych, limity transakcji BLIK, zmiana PIN-u do karty,

potwierdzasz transakcje 3D Secure w SGB Mobile

Zachęcamy do ustawienia potwierdzania transakcji internetowych 3D Secure właśnie w SGB Mobile – nie wymaga to żadnego dodatkowego kontaktu z Bankiem, a samo potwierdzanie transakcji jest szybsze i wygodniejsze niż alternatywna forma.

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.
- 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.