Bank Nowy BFG S.A.

Zasady bezpiecznego korzystania z usługi bankowości elektronicznej PBSbank24

BEZPIECZNE LOGOWANIE

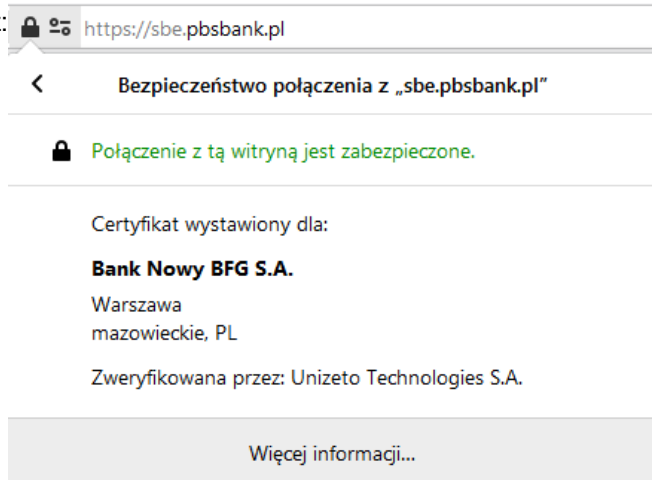
1. Zawsze korzystaj z przycisku „Zaloguj się" na stronie głównej Banku https://www.pbsbank.pl. Nigdy do logowania się do Banku nie używaj linków przesłanych w wiadomościach e-mail.
2. Sprawdź, czy adres na stronie logowania rozpoczyna się od ciągu znaków **https** (za bezpieczeństwo odpowiada protokół https).

3. Sprawdź, czy w oknie przeglądarki widoczny jest symbol kłódki, który gwarantuje szyfrowanie połączenia specjalnym, bezpiecznym protokołem SSL/TLS. W zależności od przeglądarki kłódka może znajdować się w pasku adresu lub w pasku stanu w dolnej części ekranu

4. Kliknięcie w kłódkę wyświetli szczegółowe informacje dotyczące certyfikatu. **Certyfikat SSL** służy do poświadczania autentyczności serwera, z którym komunikuje się dany komputer. Sprawdzenie szczegółów certyfikatu **przed zalogowaniem do serwisu** pozwala się upewnić, że strona, z którą nawiązane jest połączenie, to rzeczywiście strona PBSbank.

Prawidłowy certyfikat Banku powinien zawierać informacje:

- wystawiony dla: sbe.pbsbank.pl,wystawiony przez: Certum Extender Validation CA SHA2,
- ważny od: 15 czerwca 2020,
- ważny do: 15 czerwca 2021,
- numer seryjny: 02:D3:E4:30:87:BC:37:91:D5:FD:67:19:75:34:EB:83
- odcisk SHA-256: D3:EC:E9:4C:6A:22:2D:03:00:FE:59:4E:14:37:F0:87:B2:50:42:FF:AC:60:EE:2D:58:4D:2C:00:10:3E:6B:B3
- odcisk SHA1: 44:57:33:1F:81:E2:BC:87:34:D6:01:43:BA:B0:94:C1:31:03:06:7A



Uwaga!

Jeśli przy wejściu na stronę Banku przeglądarka wyświetli jakikolwiek komunikat ostrzegawczy dotyczący certyfikatu, skontaktuj się z infolinią Banku pod numerem 0 801 372 772 lub +48 13 46 55 750 (koszt wg taryfy operatora).

BEZPIECZNE URZĄDZENIE

Jak właściwie zabezpieczyć swój komputer:

1. Do obsługi PBSbank24 korzystaj z urządzeń z zainstalowanym system operacyjny dla którego producent zapewnia aktualizacje i są one instalowane. Bezwzględnie unikaj korzystania z systemów, dla których producent nie zapewnia wsparcia w postaci aktualizacji bezpieczeństwa, m. in. Windows XP, Me, 2000, 98, 95, Mac OS X 10.4 i starsze.
2. Korzystaj tylko z zaufanych urządzeń. Nie loguj się do usługi bankowości elektronicznej PBSbank24 z komputerów w ogólnodostępnych miejscach (np. kafejkach internetowych). Istnieje prawdopodobieństwo, że na takich komputerach będzie zainstalowane oprogramowanie przechwytujące dane do logowania.
3. Do obsługi PBSbank24 zalecane jest korzystanie z aktualnych wersji przeglądarek internetowych: Internet Explorer, Firefox, Opera, Safari, Google Chrome.
4. Urządzenie do obsługi PBSbank24 musi być skutecznie zabezpieczone przed zagrożeniami m.in. poprzez zainstalowanie aktualnego oprogramowania antywirusowego.
5. Używaj zapory sieciowej (firewall), która pomaga chronić komputer przed atakami z sieci.
6. Oprogramowanie antywirusowe musi skanować Twoje urządzenie w sposób aktywny.
7. Pamiętaj o regularnych aktualizacjach systemu operacyjnego oraz zainstalowanego na nim oprogramowania, w tym w szczególności oprogramowania antywirusowego. Aktualny system i oprogramowanie gwarantuje większe bezpieczeństwo.
8. Instaluj jedynie programy, do których masz zaufanie. Nie instaluj, ani nie korzystaj z programów pochodzących z nielegalnych lub niepewnych źródeł - mogą one być zainfekowane szkodliwym oprogramowaniem szpiegującym użytkownika.
9. Chroń swoją pocztę przed niechcianą korespondencją (spamem), korzystając z oprogramowania antyspamowego renomowanych producentów. Bardzo często szkodliwe oprogramowanie wykorzystuje do infekcji kolejnych komputerów pocztę e-mail. Zawsze ostrożnie podchodź do załączników i linków od nieznanych osób lub takich, których nie oczekiwałeś otrzymać.
10. Regularnie wykonuj skanowanie systemu, aby wykryć potencjalne zagrożenia.

Jak właściwie zabezpieczyć swoje urządzenie mobilne:

1. Upewnij się, że Twój telefon/tablet posiada aktualny system operacyjny dostarczony przez producenta i pamiętaj, aby regularnie go aktualizować.
2. Urządzenie, z którego korzystasz do obsługi Bankowości Internetowej musi być skutecznie zabezpieczone przed zagrożeniami poprzez zainstalowanie aktualnego oprogramowania antywirusowego.
3. Aplikacje PBSbank24 mobile oraz PBSToken instaluj wyłącznie z oficjalnych sklepów z aplikacjami (Google Play, Apple App Store, Sklep Windows).
4. Na bieżąco aktualizuj do najnowszych wersji aplikacje PBSbank24 mobile oraz PBSToken.
5. Zabezpiecz dostęp do swojego urządzenia mobilnego trudnym do odgadnięcia kodem lub hasłem.
6. Nie udostępniaj swojego urządzenia osobom trzecim.

BEZPIECZNE TRANSAKCJE

1. Stosuj dobre praktyki bezpieczeństwa:

- zwracaj uwagę na komunikaty przeglądarki,
- chroń swój login i hasło przed niepowołanymi osobami,
- podczas wpisywania loginu i hasła / PINu zwracaj uwagę, czy nikt nie podgląda wpisywanych danych,
- używaj zawsze funkcji **wyloguj** po zakończeniu pracy,
- zamykaj wszystkie okna przeglądarki przed odejściem od komputera,

- logując się do Bankowości Internetowej nie korzystaj z funkcji: autouzupełniania formularzy, zapamiętywania haseł, zapamiętywania sesji przeglądarki,
- powyższe ustawienia są praktyczne, jednak niosą za sobą ryzyko dostępu do Twojego rachunku przez innych użytkowników komputera bez Twojej wiedzy.

2. Używając tokena programowego:

- ustaw PIN do tokena / aplikacji mobilnej inny niż PIN do telefonu,
- zawsze sprawdzaj, czy informacje o transakcji wyświetlone przez token są zgodne z operacją, jaką zamierzasz wykonać,
- nie udostępniaj nikomu tokena,
- nie odblokowuj systemu operacyjnego swojego urządzenia mobilnego (tzn. rooting, jailbreak),
- w wypadku utraty - niezwłocznie zgłoś to w placówce banku lub telefoniczne.

3. Używając metody autoryzacji SMS:

W przypadku korzystania z metody autoryzacji SMS, bank wysyła kody do zalogowania, dane do autoryzacji płatności, składanych wniosków, zmiany ustawień własnych użytkownika to pod warunkiem podania przez użytkownika odpowiednich danych.

- zawsze sprawdzaj, czy informacje o transakcji przesłane w treści SMS są zgodne z operacją, jaką zamierzasz wykonać,
- nie otwieraj nieznanych linków przesyłanych SMS-ami/e-mail,
- Bank nigdy nie prosi w wiadomościach email/SMS o: instalowanie dodatkowego oprogramowania, certyfikatów bezpieczeństwa, podawanie danych dotyczących Twojego telefonu: numeru i modelu, aktualizację oprogramowania telefonu, potwierdzenie lub przekazanie jakichkolwiek danych dotyczących usługi PBSbank24 w szczególności danych do logowania lub wykonania transakcji,
- nie korzystaj z przesyłanych za pośrednictwem email/SMS lub umieszczonych na portalach społecznościowych linków do stron, z których można zainstalować dodatkowe oprogramowanie/certyfikaty bezpieczeństwa lub pobrać aktualizację posiadanego oprogramowania,
- jeżeli otrzymasz SMS/e-mail lub wiadomość za pośrednictwem portalu społecznościowego, z prośbą o podanie nr telefonu lub modelu, z prośbą o instalację na telefonie lub komputerze dodatkowego oprogramowania (certyfikatów bezpieczeństwa) względnie aktualizację posiadanego oprogramowania albo o podanie jakichkolwiek informacji o usłudze bankowości elektronicznej PBSbank24, w szczególności danych do logowania lub wykonania transakcji nie odpowiadaj na takie wiadomości i niezwłocznie powiadom Bank.
- w przypadku utraty telefonu, na który wysyłane są SMS-y służące do autoryzacji transakcji – niezwłocznie zgłoś ten fakt w placówce lub telefonicznie.

4. Używając telekodu/ Hasła maskowanego:

- nie podawaj nikomu nadanego telekodu /hasła,
- w przypadku podejrzenia dostania się telekodu/hasła w ręce osoby trzeciej natychmiast skontaktuj się z placówką Banku w celu jego zmiany.

5. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

6. Ustaw w usłudze bankowości elektronicznej PBSbank24 limity jednorazowe, dzienne, miesięczne dla transakcji na rachunku.

7. Uważaj na phishing.

Sprawdź, czy po zalogowaniu widzisz zdefiniowany przez Ciebie obrazek antyphishingowy.

Phishing jest szczególną formą przestępstwa informatycznego polegającego na podszyciu się pod znaną użytkownikowi instytucję np. bank i skłonieniu w ten sposób użytkowników komputerów do ujawnienia swoich danych (nazwa użytkownika, hasło, numer PIN lub inne informacje o dostępach), a następnie wykorzystaniu tych informacji. Phishing jest szczególnie groźny dla użytkowników bankowości internetowej. Wiadomości phishingowe przesyłane przez e-mail/SMS, a także umieszczane na portalach społecznościowych, wysyłane do potencjalnych ofiar kierują na strony, które podszywają się

pod stronę bankowości internetowej. Typowe sposoby poławiania poufnych informacji to:

- informowanie o rzekomym dezaktywowaniu konta i konieczności ponownej aktywacji z podaniem wszelkich poufnych informacji; strona przechwytująca informacje jest wówczas łudząco podobna do prawdziwej,
- informowaniu o potrzebie podania kolejnych danych wymaganych do zalogowania się do usługi lub wykonania transakcji,
- tworzenie fałszywych stron serwisów z adresami bardzo przypominającymi oryginalne, a więc łatwymi do przeoczenia dla osób niedoświadczonych w obsłudze przeglądarki internetowej,
- informowanie rzekomo w imieniu Banku o konieczności instalacji dodatkowego oprogramowania/certyfikatów bezpieczeństwa lub konieczności aktualizacji posiadanego oprogramowania, z przesłaniem takiego oprogramowania lub linku do strony, z której takie oprogramowanie można pobrać,
- informowanie rzekomo w imieniu Banku o konieczności przesłanie SMS-em lub na e-mail lub za pośrednictwem portalu społecznościowego, informacji o numerze telefonu, modelu telefonu lub też danych dotyczących usługi bankowości elektronicznej PBSbank24, w szczególności danych do logowania lub danych koniecznych do realizacji transakcji.

Pamiętaj!

- Bank nie podaje w wiadomościach e-mail/SMS, ani za pośrednictwem portali społecznościowych odsyłaczy do strony logowania do usługi bankowości elektronicznej PBSbank24, mogą się one znajdować jedynie na stronie Banku https://www.pbsbank.pl. W przypadku otrzymania takich wiadomości e-mail/SMS, należy je niezwłocznie usunąć.
- Wszystkie wiadomości e-mail lub SMS, a także wiadomości przesyłane za pośrednictwem portali społecznościowych, zawierające prośbę o zalogowanie się lub podanie jakichkolwiek informacji dotyczących usługi PBSbank24, w szczególności danych koniecznych do zalogowania lub wykonania transakcji - są podejrzane!

- Nie korzystaj z przesyłanych za pośrednictwem email/SMS lub umieszczonych na portalach społecznościowych linków do stron, z których można zainstalować dodatkowe oprogramowanie/certyfikaty bezpieczeństwa lub pobrać aktualizację posiadanego oprogramowania.
- Nie instaluj przesyłanych w załączeniu do wiadomości e-mail lub SMS programów.
- Jeżeli otrzymasz SMS/e-mail lub wiadomość na portalu społecznościowym, z prośbą o:

  1) podanie numeru telefonu lub modelu, lub

  2) z prośbą o instalację na telefonie lub komputerze dodatkowego oprogramowania (certyfikatów bezpieczeństwa), względnie aktualizację posiadanego oprogramowania,

  3) podanie jakichkolwiek informacji dotyczących usługi bankowości elektronicznej PBSbank24 w szczególności danych do logowania lub do realizacji płatności,

  - nie odpowiadaj na takie wiadomości i niezwłocznie powiadom Bank.

W przypadku jakichkolwiek podejrzeń co do autentyczności strony przed zalogowaniem prosimy o kontakt z infolinią Banku pod numerem 0 801 372 772 lub +48 13 46 55 750 (koszt wg taryfy operatora).

8. Nie odpowiadaj na e-maile lub SMS-y lub wiadomości przesyłane za pośrednictwem portali społecznościowych, z prośbą o weryfikację danych w szczególności danych składających się na podpis elektroniczny.

Bank nie inicjuje rozmów telefonicznych, nie wysyła wiadomości email/SMS, w których prosiłby Użytkownika o podawanie danych do logowania, tj. hasła oraz danych składających się na podpis elektroniczny, jak również nie inicjuje rozmów, podczas których mogłoby dojść do odblokowania usługi PBSbank24.

9. Uważaj na nietypowe działanie usługi bankowości elektronicznej PBSbank24 podczas logowania.

Jeżeli zauważysz nietypowe działanie usługi bankowości elektronicznej PBSbank24, a w szczególności wyświetlenia się komunikatu wskazującego na podanie podczas logowania nieprawidłowych danych, należy mieć świadomość, że może to być wynikiem podania przez Ciebie błędnych danych lub też zainfekowania sprzętu komputerowego złośliwym oprogramowaniem.

Jeżeli wprowadzone podczas logowania dane Użytkownika, hasła i/lub podpisu elektronicznego były poprawne, należy

bezwzględnie skontaktować z infolinią Banku pod numerem 0 801 372 772 lub +48 13 46 55 750 (koszt wg taryfy operatora) lub najbliższą placówką celem ustalenia przyczyn niemożności zalogowania, a do czasu uzyskania potwierdzenia z BOK nie podejmować kolejnych prób logowania do Usługi. Jeżeli wprowadzone dane do logowania były błędne, a dotychczas nie podejmowałeś i nie podejmujesz żadnych sprzecznych działań
z zasadami bezpieczeństwa usługi bankowości elektronicznej PBSbank24, określonymi w Regulaminie, Podręczniku użytkownika usługi bankowości elektronicznej PBSbank24 oraz w niniejszych Zasadach bezpiecznego korzystania z usługi bankowości elektronicznej PBSbank24, możesz podjąć ponowną próbę zalogowania, na innym sprzęcie komputerowym niż ten użyty przy poprzedniej nieudanej próbie logowania.

W przypadku kolejnej nieudanej próby logowania bez względu na wyświetlany komunikat nie należy podejmować dalszych prób logowania się do usługi bankowości elektronicznej PBSbank24, czy złożenia zlecenia **- niezwłocznie zaniechaj wszelkich czynności, nie podejmuj kolejnych prób logowania oraz natychmiast skontaktuj się z infolinią Banku** pod numerem 0 801 372 772 lub +48 13 46 55 750 (koszt wg taryfy operatora) lub najbliższa placówką, celem ustalenia przyczyn niemożności zalogowania się.

Czytaj informacje o pracach technicznych – Bank poinformuje Cię o nich z odpowiednim wyprzedzeniem na stronie www.pbsbank.pl.