



BGZ BNP PARIBAS

10 zasad bezpieczeństwa

dla użytkowników Bankowości Internetowej



www.bgzbnpparibas.pl/bezpieczenstwo



1 Sprawdzaj adres strony - szyfrowanie połączenia (https)

Nie korzystaj z:

- odnośników w wiadomościach pocztowych, bądź na innych stronach,
- funkcji w przeglądarce - autouzupełniania formularzy,
- funkcji w przeglądarce - zapamiętywania haseł,
- funkcji w przeglądarce - zapamiętywania sesji przeglądarki.

2 Sprawdzaj certyfikat strony

- Weryfikuj certyfikat przed każdą próbą logowania do systemu, pozwoli to sprawdzić autentyczność serwera.

3 Uważaj na e-maile z prośbą o podanie czy weryfikację poufnych danych np. haseł do bankowości elektronicznej

- Uważaj, Bank nigdy nie prosi o takie dane. Zgłoś taki przypadek na numer infolinii 801 321 123 / +48 22 566 99 99 (z za granicy) Infolinia czynna jest 24/7.



4 Dbaj o bezpieczeństwo swojego komputera

- Korzystaj z oprogramowania lub urządzeń typu firewall jak również oprogramowania antywirusowego czy antyspyware.
- Pamiętaj o poprawkach i aktualizacjach zalecanych przez producentów używanego oprogramowania w tym systemu i oprogramowania zabezpieczającego Twój komputer.
- Instaluj legalne oprogramowanie ze sprawdzonych źródeł.
- Nie używaj publicznych, otwartych sieci WiFi. Unikaj logowania do systemów bankowości internetowej z publicznie dostępnych komputerów, na przykład w kafejkach internetowych.



5 Weryfikuj składane dyspozycje przed zatwierdzeniem

- Zawsze sprawdzaj czy wiadomość SMS z kodem autoryzacyjnym jest zgodna z wykonywaną przez Ciebie operacją (np. potwierdź z danymi z faktury - numer rachunku / kwotę operacji).
- W przypadku autoryzacji podpisem elektronicznym lub tokenem pamiętaj o konieczności weryfikacji szczegółów transakcji. Upewnij się, że są one zgodne z transakcją, którą zamierzasz zrealizować (np. potwierdź dane z faktury).



6 Dbaj o bezpieczeństwo Twoich haseł

- Bank nigdy nie potrzebuje Twojego pełnego hasła, poza operacją zmiany hasła na nowe Token - nie udostępniaj nikomu nośnika kryptograficznego ani hasła.
- Podpis elektroniczny - nie udostępniaj nikomu nośnika kryptograficznego USB ani karty kryptograficznej, na której przechowywane są Twoje klucze, ani też kodu PIN do nich.



7 Sprawdzaj dane logowania

- Sprawdź daty ostatniego logowania, zarówno udanego jak i nieudanego. Jeśli daty te nie odpowiadają Twojej aktywności, powinno Cię to zaniepokoić, może to oznaczać, że ktoś inny uzyskał dostęp do Twojego konta.



8 Zmień obrazek

- Zapamiętaj domyślnie wybrany obrazek lub zmień na inny, wybrany ze zbioru dostępnych w systemie. W tym celu wybierz funkcję 'Mój profil' -> 'Ustawienia ogólne'.



9 Wyloguj się z serwisu

- Zawsze wyloguj się z serwisu. W tym celu kliknij ikonę „wyloguj” w prawym górnym rogu. Nie zamykaj okna przeglądarki bez wylogowania z serwisu bankowości elektronicznej.



10 Korzystaj z powiadomień dotyczących Twojej aktywności w systemie

- Ustaw automatyczne powiadamianie e-mailem lub SMS'em o każdym udanym lub nieudanym logowaniu, zablokowaniu dostępu do systemu i obciążeniu rachunku powyżej zadeklarowanej kwoty. (W systemie Pl@net automatyczne powiadomienia ustawia się po wejściu w Mój Profil na górnej belce, a następnie klikając w ikonkę Powiadomienia).