
10 zasad
bezpieczeństwa
dla użytkowników
bankowości elektronicznej
#BankDobrychDecyzji

BNP PARIBAS

10 ZASAD BEZPIECZNEJ BANKOWOŚCI ELEKTRONICZNEJ

01 Sprawdzaj adres strony – szyfrowanie połączenia

Nie korzystaj z:

- linków w e-mailach lub SMS-ach niewiadomego pochodzenia oraz linków podanych na niezweryfikowanych stronach .www
- funkcji w przeglądarce takich jak: autouzupełnianie formularzy, zapamiętywanie haseł, zapamiętywanie sesji

Weryfikuj:

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

02 Czytaj komunikaty bezpieczeństwa

- Uważnie czytaj komunikaty dotyczące bezpieczeństwa umieszczone na stronie do logowania, ekrany widoczne po zalogowaniu oraz wiadomości w poczcie wewnętrznej. Znajdziesz tam informacje o aktualnych zagrożeniach czy możliwych próbach ataków socjotechnicznych.
- Podejrzane SMS-y zgłaszaj na ogólnokrajowy, całodobowy i bezpłatny numer **CERT 8080** - pozwoli to dodać podejrzane numery do bazy blokowanych połączeń.

03 Chroń prywatne dane

- Pracownicy banku nigdy nie proszą o: Twój login lub hasło do bankowości, instalację dodatkowego oprogramowania, uzyskanie zdalnego dostępu do komputera/telefonu, pełen numer karty i kod CVV/CVC, podanie kodu BLIK, wykonanie przelewu, wpłatę lub wypłatę pieniędzy w bankomacie czy oddziale banku.
- Zgłoś taki przypadek pod numerem telefonu czynnym 24/7:
  +48 22 548 29 40 (koszt połączenia wg stawki operatora).

04 Korzystaj z Ochrony Behawioralnej

- To nowoczesna, bezpłatna usługa, która dodatkowo zwiększa bezpieczeństwo Twoich środków na koncie. Aktywacja jest prosta, możliwa zarówno w GOonline jak i aplikacji GOmobile: *Ustawienia Profilu osobistego-> Sekcja bezpieczeństwo-> Ochrona behawioralna -> Zaakceptuj warunki.*

05 Dbaj o bezpieczeństwo Twojego komputera

- Korzystaj z oprogramowania antywirusowego lub antyspyware.
- Pamiętaj o poprawkach i aktualizacjach zalecanych przez producentów 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, np. na lotnisku czy w kawiarni.

06 Weryfikuj składane dyspozycje i korzystaj z limitów

- Zawsze sprawdzaj czy wiadomość SMS z kodem autoryzacyjnym zgadza się z wykonywaną przez Ciebie operacją (np. potwierdź z danymi z faktury - numer rachunku/kwotę operacji).
- W przypadku autoryzacji podpisem elektronicznym lub tokenem pamiętaj o weryfikacji szczegółów transakcji. Upewnij się, że są one zgodne z transakcją, którą realizujesz.
- Ustaw bezpieczne limity dziennych transakcji BLIK, kart płatniczych, wypłat gotówkowych, przelewów. Próby podejrzanych, dużych przelewów i wypłat nie zostaną wtedy zrealizowane.

07 Dbaj o bezpieczeństwo Twoich haseł

- Silne hasło: zawiera przynajmniej 15 znaków, wielkie i małe litery, znaki specjalne (@#ś&!), cyfry (1, 3, 7, 0). To może być równoważnik zdania lub zdanie.
- Hasło powinno być znane tylko użytkownikowi oraz bezpiecznie przechowywane.
- Pracownik banku nigdy nie prosi o podanie loginu lub hasła.
- Jeżeli logujesz się za pomocą hasła maskowanego pamiętaj, że bank nie potrzebuje Twojego pełnego hasła, poza operacją zmiany hasła na nowe. Podawaj tylko wybrane znaki z hasła podczas logowania.
- Jeżeli logujesz się za pomocą podpisu elektronicznego, nie udostępniaj nikomu nośnika kryptograficznego USB ani karty kryptograficznej, na której przechowywane są Twoje klucze oraz kodu PIN do nich.

08 Sprawdzaj dane logowania

- Sprawdzaj 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.

09 Korzystaj z powiadomień systemowych

- Ustaw automatyczne powiadamianie e-mail lub SMS o każdym udanym lub nieudanym logowaniu, zablokowaniu dostępu do systemu i obciążeniu rachunku powyżej zadeklarowanej kwoty. Dzięki takim powiadomieniom będziesz mieć kontrolę nad aktywnością w ramach swojego rachunku bankowego.

10 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.

Więcej informacji dotyczących bezpieczeństwa znajdziesz na naszej stronie
www.bnpparibas.pl/bezpieczenstwo