



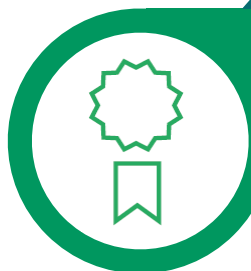
BNP PARIBAS

**10 zasad
bezpiecznej
bankowości elektronicznej
dla firm**

#BANKDOBRYCHDECYZJI

10 ZASAD

BEZPIECZNEJ BANKOWOŚCI ELEKTRONICZNEJ



01

Stosuj dwuetapowe logowanie

- Dzięki włączeniu dwuetapowego logowania, nawet jeśli ktoś pozna Twoje hasło, nie będzie w stanie uzyskać dostępu do konta bez drugiego czynnika uwierzytelniającego – czyli hasła SMS.



02

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).
- Podejrzane SMS-y zgłaszaj na ogólnokrajowy, całodobowy i bezpłatny numer **CERT 8080** - pozwoli to dodać podejrzane numery do bazy blokowanych połączeń.



03

Czytaj komunikaty bezpieczeństwa

- Zwracaj uwagę na komunikaty na temat bezpieczeństwa, które pojawiają się przed i po logowaniu do bankowości online oraz na stronie internetowej banku. Znajdziesz tam informacje o aktualnych zagrożeniach czy możliwych próbach ataków.

04

Dbaj o bezpieczeństwo Twoich haseł



- Silne hasło: zawiera przynajmniej 15 znaków, wielkie i małe litery, znaki specjalne (@#&!), cyfry (1, 3, 7, 0). Może być równoważnikiem zdania lub zdaniem.
- Hasło powinno być znane tylko użytkownikowi oraz bezpiecznie przechowywane.
- Jeśli 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.
- Jeśli 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.

05

Dbaj o bezpieczeństwo Twojego komputera



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

06

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



07

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 / kwotą 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 przelewów, kart płatniczych, wypłat gotówkowych. Próby podejrzanych, dużych przelewów i wypłat nie zostaną wtedy zrealizowane.



08

Sprawdzaj dane logowania

- Sprawdzaj daty ostatniego logowania, zarówno udanego, jak i nieudanego. Daty te powinny odpowiadać Twojej aktywności, w przeciwnym razie może to oznaczać, że osoba niepowołana uzyskała dostęp do Twojej bankowości. W przypadku wątpliwości zgłoś zaistniałą sytuację na Infolinię banku.



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 kończ aktywność w systemie bankowości elektronicznej poprzez wylogowanie. Kliknij ikonę "Wyloguj" w prawym górnym rogu serwisu. Nie zamykaj okna przeglądarki lub aplikacji bez wylogowania.

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