



Pamiętaj, że Bank nigdy nie prosi o:

- instalację certyfikatów na komputerach i telefonach komórkowych
- podanie danych kart płatniczych i kredytowych (numer karty, kod PIN) oraz danych dotyczących Twojego telefonu (numer i model)
- udział w testowaniu nowych funkcjonalności serwisu transakcyjnego
- wykonanie przelewów testowych ani zwrot środków na rachunki innych Klientów

Jeżeli zaobserwujesz podejrzane działania lub wiadomości, prosimy zgłoś to natychmiast, dzwoniąc na numer infolinii Twojego Banku.

Zapraszamy do placówek Banku BPS. Nasi doradcy udzielą szczegółowych informacji dotyczących produktu.



Znajdź nas na Facebooku!
[facebook.com/TwojBPS](https://www.facebook.com/TwojBPS)



Bezpieczeństwo korzystania z **BANKOWOŚCI INTERNETOWEJ**



www.bankbps.pl



Infolinia: 801 321 456 | 86 215 50 00



www.facebook.com/TwojBPS



Bank BPS
Grupa BPS

Zadbaj o swoje bezpieczeństwo podczas korzystania z bankowości internetowej!

Poświęć parę chwil na zapoznanie się z informacjami, które mogą ułatwić Ci **bezpieczne korzystanie z bankowości internetowej**



Ważne wskazówki:

- zabezpiecz swój komputer aktualnym **oprogramowaniem antywirusowym** oraz **blokującym niepowołany dostęp do komputera** (firewall)
- regularnie **aktualizuj** system operacyjny, wersje przeglądarki oraz oprogramowanie na komputerze, z którego korzystasz z bankowości elektronicznej
- używaj **oprogramowania z legalnego źródła** - oprogramowanie ściągane z Internetu może być zmodyfikowane przez hakerów! Legalne systemy są na bieżąco aktualizowane i usuwane są luki w ich zabezpieczeniach
- **poprawnie twórz i regularnie zmieniaj swoje hasło dostępu:**
 - hasło powinno być trudne do rozszyfrowania, nie powinno zawierać imion, nazwisk, dat urodzenia, ani innych danych łatwych do odgadnięcia
 - powinno składać się z co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne
 - hasło powinien znać wyłącznie jego właściciel
- **zawsze sprawdzaj numer rachunku odbiorcy**, gdy kopiujesz dane do przelewu. Złośliwe oprogramowanie może spowodować, że wkleisz numer rachunku przestępcy - najlepiej, aby numer rachunku bankowego był **wprowadzany ręcznie**
- ustal **bezpieczne limity transakcyjne** dla przelewów internetowych
- korzystaj z **bankowości internetowej w domu i na własnym sprzęcie komputerowym**. Korzystając z bankowości internetowej, unikaj miejsc z niezabezpieczonymi sieciami Wi-Fi, do których dostęp ma wiele osób (np. kawiarenki internetowe, kina, restauracje, punkty publicznego dostępu tzw. hot-spoty).
- zawsze **kończ pracę** z systemem bankowości internetowej na komputerze, **korzystając z polecenia "Wyloguj"**
- **nie otwieraj wiadomości i załączników nieznanego pochodzenia** - mogą one zawierać wirusy i złośliwe oprogramowanie pozwalające przestępcom na szpiegowanie Twoich działań
- logując się na stronę bankowości internetowej, **weryfikuj poprawność adresu** oraz sprawdź czy połączenie jest szyfrowane (świadczy o tym adres witryny rozpoczynający się od „https://” oraz symbol zamkniętej kłódki)
- zawsze **zwracaj uwagę na komunikaty o błędach certyfikatów** wyświetlane przez przeglądarkę - zrezygnuj z autoryzacji transakcji, gdy masz jakiegokolwiek podejrzenia
- **bądź na czasie!** Śledź komunikaty Banku dot. najnowszych zabezpieczeń przed atakiem złośliwego oprogramowania

