

**Jak na co dzień dbać o bezpieczeństwo pieniędzy?
Zawsze przestrzegaj podstawowych zasad bezpieczeństwa**

Korzystając z bankowości internetowej lub aplikacji mobilnej zawsze przestrzegaj podstawowych zasad bezpieczeństwa. Oszuści próbują wykorzystać Twoje roztargnienie i nieostrożność. Nie daj się zaskoczyć!

Jak na co dzień dbać o bezpieczeństwo pieniędzy?

Korzystając z bankowości internetowej lub aplikacji mobilnej zawsze przestrzegaj podstawowych zasad bezpieczeństwa. Oszuści próbują wykorzystać Twoje roztargnienie i nieostrożność. Nie daj się zaskoczyć!

- Korzystaj zawsze z aktualnego systemu operacyjnego oraz z aktualnych aplikacji. Zabezpiecz swój komputer aktualnym oprogramowaniem antywirusowym.
- Korzystaj z poprawnych, czyli trudnych do rozszyfrowania haseł do komputera i do bankowości internetowej. Silne hasło powinno składać się z co najmniej 8 znaków, zawierać wielkie i małe litery, cyfry oraz znaki specjalne. Nie zapisuj haseł ani ich nie przekazuj innym osobom.
- Ustal bezpieczne limity przelewów internetowych i płatności kartą. Łatwo je zmienisz w bankowości elektronicznej.
- Korzystaj z bankowości elektronicznej na własnym sprzęcie i w miejscu z zaufanym Internetem. Unikaj logowania w miejscach typu kino, kawiarnia, publiczne hot-spoty.
- Zawsze po zakończeniu korzystania z bankowości internetowej klikaj w przycisk „Wyloguj”.
- Logując się na stronę bankowości internetowej, sprawdź poprawność adresu i szyfrowanie połączenia (adres powinien zaczynać się od <https://>... a obok powinien być widoczny symbol zamkniętej kłódki).
- Zawsze zwracaj uwagę na komunikaty o błędach certyfikatów wyświetlane przez przeglądarkę internetową. Zrezygnuj z transakcji, jeśli cokolwiek wzbudzi Twoje wątpliwości.
- Nie instaluj na swoim komputerze programów z nieznanymi źródłami.
- Na komputerze korzystaj z klawiatury ekranowej wprowadzając hasło.
- Czytaj nasze komunikaty na temat bezpieczeństwa – bądź na bieżąco!
- Śledź informacje oraz komunikaty przesyłane na Twoją skrzynkę w systemie bankowości elektronicznej

Zgłaszaj na Infolinię Banku próby podszywania się pod bank nie tylko Bank BPS, ale również innych instytucji

Złodzieje mogą podjąć próbę włamania do Twojego komputera lub telefonu także wtedy, kiedy Ty nie jesteś zalogowany do banku, a np. sprawdzasz swoje maile lub przeglądasz strony internetowe.

Dlatego:

- Nie otwieraj maili od nieznanych nadawców, nie klikaj w załączniki do wiadomości czy smsów, które wydają Ci się podejrzane (np. pochodzą od firmy kurierskiej, chociaż niczego nie zamawiałeś w sklepach internetowych albo od dostawcy energii, z którym nie masz podpisanej umowy).
- Nie klikaj w linki prowadzące do stron rzekomo aktualizujących Twoje certyfikaty bezpieczeństwa lub system transakcyjny – bank NIGDY o to nie prosi w mailach.
- Uważaj na wiadomości, w których ktoś prosi Cię o dopłatę do jakiejś transakcji – upewnij się, najlepiej dzwoniąc do danej osoby lub firmy, czy prośba jest prawdziwa.

Nie wysyłaj kodów BLIK nawet osobom znajomym, które proszą Cię o to przez Facebooka, messengera lub inny serwis społecznościowy, najlepiej zadzwoń i zapytaj, czy rzeczywiście ktoś miał do Ciebie taką prośbę.

Jeśli ktoś dzwoni do Ciebie podając się za pracownika banku, jeśli otrzymujesz wiadomości, których nadawcy podszywają się pod bank lub po prostu coś Cię zaniepokoiło w związku z przelewami, zadzwoń na naszą Infolinię