

JAK DBAĆ O BEZPIECZEŃSTWO SWOICH PIENIĘDZY?!



- **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 do BANKU !!!

Korzystając z bankowości internetowej lub aplikacji mobilnej zawsze przestrzegaj podstawowych zasad bezpieczeństwa:

- **NIGDY** nie podawaj nikomu przez Internet lub telefon swoich danych osobowych, identyfikatorów ani haseł !
- **Nie instaluj** oprogramowania i nie ściągaaj aplikacji pochodzących z nieznanymi źródłami!
- **Nie otwieraj** maili od nieznanymi nadawcami, 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!

- 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). Sprawdź także dokładnie poprawność adresu URL pod kątem literówek i niestandardowych znaków, które bardzo często nie są widoczne na pierwszy rzut oka.
- 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 nieznanego źródła.
- Na komputerze korzystaj z klawiatury ekranowej wprowadzając hasło.
- Śledź informacje oraz komunikaty publikowane na stronie Banku oraz przesyłane na Twoją skrzynkę w systemie bankowości elektronicznej.

PAMIĘTAJ w przypadku czasowej niedostępności Twojej bankowości elektronicznej zachowaj spokój i nie ulegaj panice.

Taki jest właśnie cel cyberprzestępców – wywołanie paniki, strachu i chaosu.

Nie wspieraj ich w tym.

Nie kieruj się również anonimowymi opiniami czy komentarzami np. z mediów społecznościowych czy forów internetowych. Upewnij się, że to wiarygodne informacje a nie „fake newsy”.