

Internetowe finanse bez stresu i zagrożeń

Korzystanie z bankowości internetowej i mobilnej staje się codziennością. Dzięki niej możemy sprawdzać saldo, opłacać rachunki i zarządzać finansami bez wychodzenia z domu. Niestety – z wygodą idą w parze zagrożenia. Oto, jak **bezpiecznie korzystać z bankowości elektronicznej**.

Zasady bezpiecznego logowania

- **zawsze wpisuj adres banku ręcznie** w przeglądarce (np. www.nazwabanku.pl) – **nie klikaj w linki z SMS-ów czy e-maili**.
- **nie loguj się do banku w miejscach publicznych** (np. na dworcu) oraz z **publicznego Wi-Fi** – to ryzyko przechwycenia danych.
- **nie zapisuj loginów i haseł** w zeszycie ani na kartce przy komputerze.

Ustal silne hasło i regularnie je zmieniaj

Silne hasło powinno zawierać: małe i wielkie litery, cyfry, znaki specjalne (np. ! @#). **Nie używaj daty urodzenia ani imienia!**

Przykład silnego hasła: **Zima!2025#konto**

Sprawdzaj, czy strona banku jest bezpieczna

Przed zalogowaniem upewnij się, że:

- adres zaczyna się od **https://** a obok adresu widnieje **kłódka**.
- jeśli widzisz „ostrzeżenie o niezabezpieczonym połączeniu”- **nie loguj się!**

Rozpoznawanie oszustw i podejrzanych wiadomości

Uważaj na:

- e-maile i SMS-y „z banku”, które proszą o dane logowania.
- wiadomości z informacją o „problemie z kontem” – bank **nigdy nie prosi o dane przez SMS!**
- aplikacje bankowe pobieraj tylko ze strony banku.
- jeśli masz wątpliwości – **zadzwoń na infolinię swojego banku**, zanim klikniesz w link!

Bezpieczne korzystanie z aplikacji mobilnych

- korzystaj **tylko z oficjalnej aplikacji banku**.
- nie instaluj „dodatkowych aplikacji do bankowości” – mogą być szkodliwe!
- włącz **biometrię lub kod PIN**, aby zabezpieczyć dostęp do aplikacji.
- po użyciu – **wyloguj się**, nie zostawiaj aplikacji otwartej w tle.

Podejrzane telefony z „banku” – jak rozpoznać oszusta?

Oszuści coraz częściej **podszycują się pod pracowników banków**, dzwoniąc do Klientów i twierdząc, że:

- ktoś próbuje włamać się na Twoje konto,
- trzeba natychmiast zablokować kartę lub konto,
- musisz zainstalować „aplikację bezpieczeństwa”,
- potrzebne są Twoje dane do logowania lub kod z SMS-a.

To najczęściej oszustwo!

Jak odróżnić prawdziwy telefon z banku od fałszywego?

Bank tak NIE robi	Oszust najczęściej robi
Nie poprosi o login, hasło, numer PIN	Pyta o dane logowania
Nie poprosi o kod SMS (chyba że Ty sam coś zlecasz)	Prosi o przepisanie kodu z SMS – twierdzi, że „to do weryfikacji”
Nie każe instalować aplikacji z linku przez telefon	Każe wejść na stronę i zainstalować „aplikację ochronną”
Dzwoni tylko z oficjalnych numerów – możesz je sprawdzić na stronie banku	Może dzwonić z numeru, który wygląda jak prawdziwy (tzw. spoofing)
Nie wywiera presji, nie straszy	Straszy: „jeśli szybko nie zareagujesz, stracisz swoje pieniądze!”

Materiał z serii **Notatki z wykładu** powstał w ramach zadania realizowanego przez Stowarzyszenie Wspierania Aktywności Obywatelskiej CIVIS SUM, finansowane ze środków przekazanych przez Powiat Zielonogórski na podstawie umowy o powierzenie realizacji zadania publicznego pn. „Powierzenie prowadzenia w 2025 r. jednego punktu nieodpłatnej pomocy prawnej i jednego punktu nieodpłatnego poradnictwa obywatelskiego na terenie Powiatu Zielonogórskiego”.