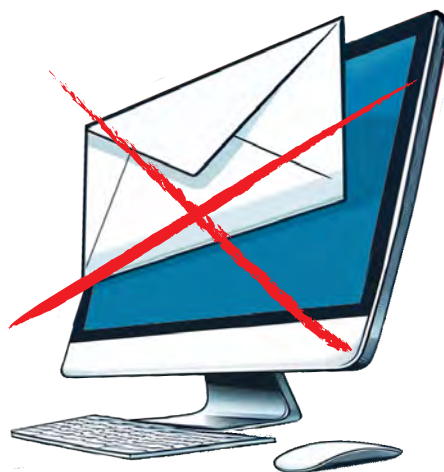


## Pamiętaj o podstawach bezpieczeństwa!

- Podczas zakupów w nowych sklepach internetowych zapoznaj się z regulaminem!  
Uchroni Cię to przed niechcianą subskrypcją i utratą oszczędności.
- Nie przekazuj nikomu swoich
  - danych osobowych,
  - danych kart płatniczych,
  - danych dostępowych do kont bankowych,
  - loginów i haseł do poczty e-mail, mediów społecznościowych,
  - nie podawaj informacji na temat swoich oszczędności.
- Aplikacje, z których korzystasz, pobieraj tylko z oficjalnych sklepów Google Play (Android) i App Store (iOS)!
- Nie klikaj w reklamy, podejrzone artykuły, post sponsorowane w mediach społecznościowych!
- Uważaj na oferty loterii i konkursów z atrakcyjnymi nagrodami!

## Nie daj się phishingowi!



## Weryfikuj wiadomości e-mail!

- Porównaj wyświetlaną nazwę z rzeczywistym adresem e-mail!  
Oszuści często podszywają się pod inne osoby.
- Uważaj na ogólne lub bezosobowe pozdrowienia, np. „Drogi Kliencie”, „Drogi przyjacielu”!
- Traktuj z podejrzliwością prośby o dokonanie przelewu w wiadomości e-mail!
- Uważaj na prośby o podanie danych osobowych!
- Zawsze sprawdzaj łącze, najężdżając na nie kursorem!  
Jeśli masz wątpliwości – nie klikaj!

## Poznaj zasady bezpieczeństwa i nie daj się oszukać!



## Podejrzone rozmowy telefoniczne

Zachowaj czujność podczas rozmów telefonicznych, gdy:

- ktoś podaje się za członka rodziny lub bliską Ci osobę i prosi o pieniądze,
- ktoś podaje się za policjanta lub pracownika banku i informuje, że Twoje oszczędności są zagrożone i musisz szybko podjąć działania,
- otrzymujesz telefon z informacją, że ktoś z Twoich bliskich potrzebuje pomocy (np. uczestniczył w wypadku) i musisz przekazać pieniądze na operację lub pomoc prawną,
- nie masz pewności z kim rozmawiasz.

## Co zrobić, gdy odbierzesz telefon?

- Jeśli dzwoni ktoś, kto podaje się za pracownika banku lub innej instytucji, a rozmowa wydaje Ci się podejrzana - rozłącz się!
- Nie daj się wciągnąć w rozmowę jeśli nie masz pewności kto jest po drugiej stronie!
- Zweryfikuj rozmówcę dzwoniąc na znany numer instytucji lub udaj się do placówki!
- Nigdy nie oddzwaniaj na nieznany numer - może to być numer zagraniczny i narazisz się na wysokie koszty!
- Zablokuj niechciane połączenia!

## Pamiętaj!

- Nigdy nie podejmuj działań pod wpływem emocji i presji czasu!
- Policja, prokuratura, pracownicy służb medycznych lub innych instytucji nigdy nie proszą o przekazanie pieniędzy.
- Pracownik banku lub innej instytucji nigdy nie poprosi Cię o podanie danych do logowania na konta ani danych karty płatniczej.
- Zawsze weryfikuj swojego rozmówcę! Zadzwoń do kogoś z rodziny i sprawdź, czy przedstawiona historia jest prawdziwa!

**Odwiedź naszą stronę internetową, aby dowiedzieć się więcej!**



[https://online.banknowy.pl/porta1\\_online/bezpieczenstwo](https://online.banknowy.pl/porta1_online/bezpieczenstwo)

## W jaki sposób oszuści mogą Tobą manipulować?

- Wywierają nacisk, aby szybko podjąć działania i pilnie przekazać pieniądze.
- Wzbudzają lęk i niepokój np. mówiąc, że ktoś włamał się na Twoje konto bankowe i próbuje Cię okraść.
- Proszą, aby dla dobra sprawy nikomu nie mówić o rozmowie.
- Wykonują kilka telefonów w krótkich odstępach czasu - aby uniemożliwić zweryfikowanie sprawy.
- Wysyłają wiadomości SMS, aby uwiarygodnić prowadzoną rozmowę.
- Nakłaniają do instalowania aplikacji na telefonie lub komputerze.
- Informują, że zaufana osoba przyjdzie i odbierze pieniądze.

