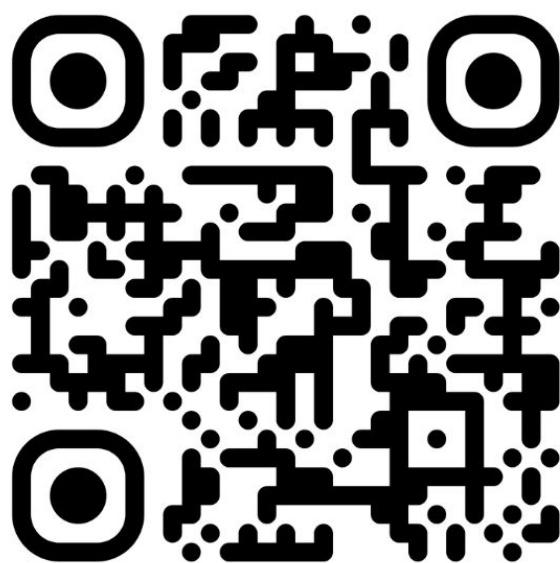




**Internet to okno na świat.
Otwieraj go bezpiecznie!**



Technologia jest dla ludzi.

Wystarczy odrobina ostrożności, by cieszyć się nią bez obaw!



Dofinansowane przez
Unię Europejską

most
STOWARZYSZENIE

KS
Ostrava



W sieci stosuj zasadę ograniczonego zaufania

Uważaj na "pilne" sprawy

Oszuści wymuszają pośpiech, by wyłączyć Twoje logiczne myślenie. Czujesz presję czasu? Zatrzymaj się. Ta krótka pauza to Twoja najlepsza tarcza przed stratą pieniędzy lub kradzieżą danych.

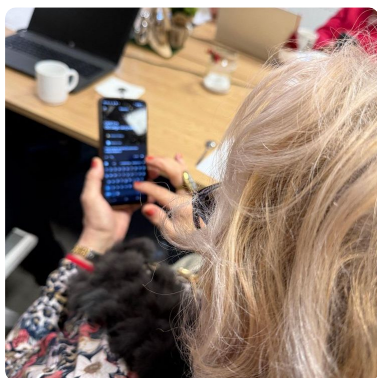
Typowe przykłady oszustw:

"Twoje konto zostanie zablokowane!"

"Masz nieopłaconą paczkę!"

"Dopłać 2 zł do rachunku za prąd!"

Najczęstsze metody oszustw



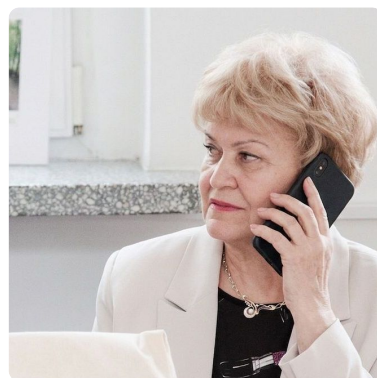
Phishing

Oszuści wysyłają fałszywe wiadomości e-mail lub SMS, podszywając się pod banki, urzędy czy firmy kurierskie. Ich celem jest wyłudzenie Twoich danych osobowych i haseł.



Spoofing

Przestępcy fałszują numer telefonu, z którego dzwonią — tak, by wyglądał jak numer Twojego banku, policji lub innej zaufanej instytucji. Nie daj się nabrać!



Metoda „na wnuczkę"

Dzwoniący podaje się za bliską osobę lub urzędnika i prosi o pilny przelew lub gotówkę. Zawsze weryfikuj tożsamość rozmówcy, dzwoniąc bezpośrednio do rodziny.

Pamiętaj: Żaden bank, urząd ani policja nie zadzwoni do Ciebie z prośbą o podanie hasła, numeru PIN, przekazanie gotówki, ani zainstalowanie "aplikacji do ochrony pieniędzy"!

W razie wątpliwości zawsze dzwoń na oficjalną infolinię instytucji, sprawdzając numer w umowie lub na stronie internetowej.

Jak chronić siebie i swoje dane?

Bezpieczeństwo w Internecie zaczyna się od prostych nawyków. Te trzy proste zasady to fundament Twojego bezpieczeństwa w sieci.



Silne hasła to podstawa

Najlepsze hasło to takie, które łatwo zapamiętać, ale trudno zgadnąć. **Użyj długiego zdania, które ma dla Ciebie sens.**

Przykład:

ZimaToMojaUlubionaPor Roku1961!

To bezpieczniejsze niż krótkie hasła typu Kasia123.

Pamiętaj! Warto zmieniać swoje hasła co kilka miesięcy.



Nie klikaj w ciemno

Dostałeś link w wiadomości od nieznanego nadawcy? **Nie klikaj.** Zamiast tego zadzwoń bezpośrednio do instytucji, od której rzekomo przyszła wiadomość.

Sprawdź numer na oficjalnej stronie, **zadzwoń i zweryfikuj** — ten jeden telefon może uchronić Cię przed zagrożeniem.



Weryfikuj prośby o pieniądze

Ktoś pisze do Ciebie na komunikatorze (np. WhatsApp, Facebook Messenger), podając się za córkę lub syna, i prosi o szybki przelew, bo "zgubił telefon" lub "ma nagłą sytuację"?

Zanim cokolwiek zrobisz — zadzwoń i zweryfikuj na jej znany Ci numer. Twoi bliscy zrozumieją tę ostrożność.



Chroń swoje dane osobowe

Nigdy nie podawaj przez telefon ani w podejrzanych wiadomościach: numeru PESEL, numeru karty płatniczej, hasła do konta bankowego ani kodu PIN. Żadna prawdziwa instytucja nigdy o to nie prosi.



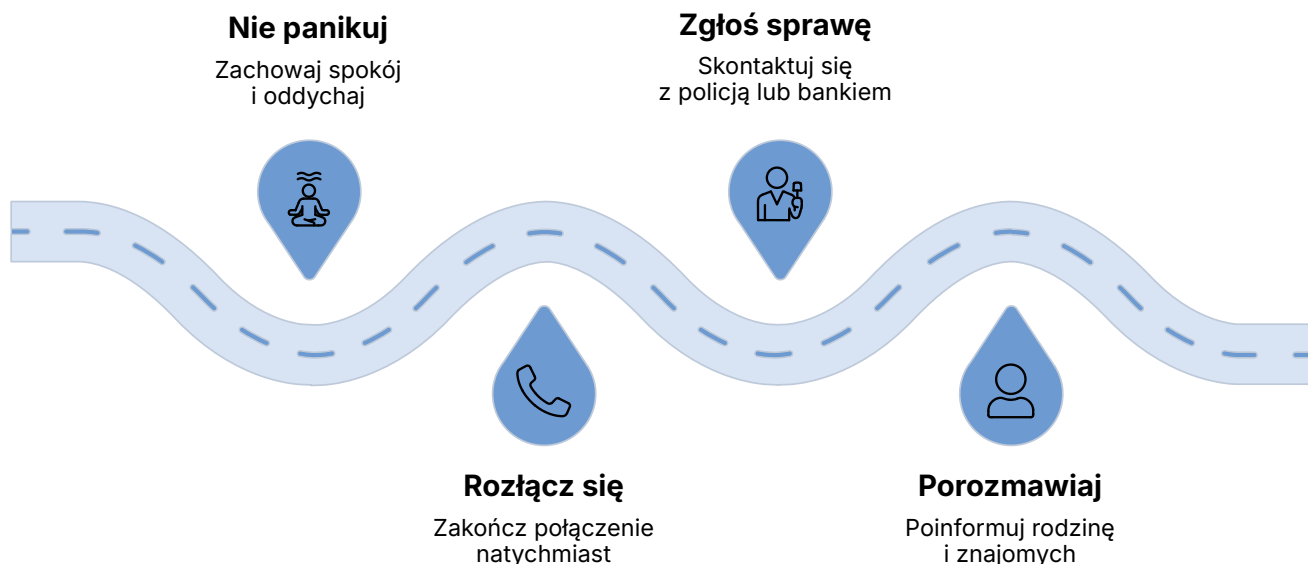
Aktualizuj oprogramowanie

Regularne aktualizacje systemu, przeglądarki i aplikacji to **najlepsza tarcza** przed nowymi zagrożeniami. Gdy telefon lub komputer prosi o aktualizację — **nie odkładaj jej na później.**

Pamiętaj, nie jesteś sam!

Jeśli podejrzewasz, że ktoś próbował Cię oszukać, lub kliknąłeś w dziwny link – nie wpadaj w panikę. To zdarza się nawet ekspertom od technologii. Ważne, żebyś wiedział, jak reagować i do kogo się zwrócić o pomoc.

Co robić gdy coś Cię zaniepokoiło?



Nie panikuj!

Oszuści celowo wywołują presję czasu i strach. Weź głęboki oddech — **spokój to Twoja przewaga**.



Rozłącz się!

Jeśli podejrzewasz oszustwo, **natychmiast zakończ rozmowę**. Nie musisz być grzeczny wobec oszusta.



Zgłoś!

Zadzwoń na **Policję (112)**. Jeśli doszło do transakcji — natychmiast powiadom swój bank.



Porozmawiaj z bliskimi!

Dziel się swoimi obawami z rodziną lub przyjaciółmi. Razem łatwiej rozpoznać zagrożenie i znaleźć pomoc.

Ważne numery:

- Policja: **112**
- Twój bank: **numer podany na odwrocie karty płatniczej**

Twoje bezpieczeństwo jest ważne! Dziel się tą wiedzą z sąsiadami, przyjaciółmi i rodziną. Razem możemy skuteczniej chronić się przed oszustami. Bądź czujny — i ciesz się Internetem bez strachu!