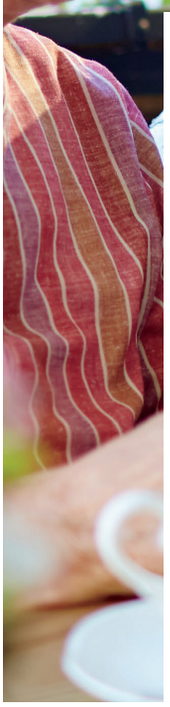


# BEZPIECZNY SMARTFON I KOMPUTER

Twój praktyczny przewodnik po cyfrowym bezpieczeństwie

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW
Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Rządowy Program Wsparcia Organizacji Pozarządowych
Moc Małych Społeczności

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW Narodowy Instytut Wolności Centrum Rozwoju Społeczeństwa Obywatelskiego

Rządowy Program Wsparcia Organizacji Pozarządowych Moc Małych Społeczności

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU WSPARCIA ORGANIZACJI POZARZĄDOWYCH MOC MAŁYCH SPOŁECZNOŚCI

# BEZPIECZNY SMARTFON I KOMPUTER

## TWÓJ PRAKTYCZNY PRZEWODNIK PO CYFROWYM BEZPIECZEŃSTWIE

**Opracowanie:** zespół Stowarzyszenia Wspierającego Inicjatywy Europejskie “**IMPET**”

**Redakcja i nadzór ekspercki:** Dariusz Stawik

**Oprawa wizulana**: Aleksandra Traczyk

Publikacja przygotowana z wykorzystaniem narzędzi AI, z zapewnieniem kontroli merytorycznej

W przedstawionych „historiach z życia” wszystkie osoby i dialogi są fikcyjne. Przykłady ilustrują typowe sytuacje, z jakimi spotykają się użytkownicy i mają charakter edukacyjny.

Sułków, 2025

# SPIS TREŚCI

# Witaj, drogi Czytelniku!

Trzymasz w ręku poradnik, który może uchronić cię przed wieloma kłopotami. Zanim pomyślisz: *„znowu to straszenie Internetem”* – daj nam szansę. Obiecujemy: to nie będzie nudna instrukcja pełna technicznych terminów!

**Po co powstał ten poradnik?**

Internet to wspaniały wynalazek. Dzięki niemu możesz m.in.:

- zobaczyć zdjęcia wnuków, nawet jeśli mieszkają za granicą,
- zrobić przelew bez stania w kolejce w banku,
- sprawdzić prognozę pogody,
- obejrzeć powtórkę ulubionego serialu.

**Ale...**

Tak jak w prawdziwym życiu spotykamy uczciwych ludzi, ale czasem trafiamy na kieszonkowców i naciągaczy, tak samo jest w Internecie. Z tą różnicą, że oszuści w sieci bywają jeszcze sprytniejsi – nie widzisz ich twarzy, nie słyszysz głosu, nie masz jak ocenić, że *„coś tu nie gra”*.

I właśnie dlatego powstał ten poradnik.

**Dla kogo jest ta publikacja?**

Dla każdego, kto:

- używa komputera czy smartfon, ale nie zawsze rozumie wszystkie ostrzeżenia,
- słyszał o oszustwach, ale nie wie dokładnie, jak się przed nimi chronić,
- chce nauczyć się czegoś nowego – niezależnie od wieku.

**Każdy ma prawo się uczyć. Teraz twoja kolej!**

# BEZPIECZNY SMARTFON

## Blokada telefonu – twoja pierwsza ochrona

Wyobraź sobie, że wychodzisz z domu i zostawiasz drzwi szeroko otwarte. Nierozsądne, prawda? A jednak wiele osób robi dokładnie to samo… ze swoim telefonem!

Telefon bez blokady to otwarty dostęp do:

- twoich zdjęć (w tym prywatnych),
- kontaktów do bliskich,
- aplikacji bankowych,
- wiadomości na Facebooku,
- poczty e-mail.

Jeśli zgubisz telefon w sklepie, autobusie albo ktoś ci go ukradnie, osoba, która go znajdzie, będzie miała dostęp do całego twojego cyfrowego życia.

# Jak zablokować telefon?

## OPCJA 1

**Kod cyfrowy:** 4 lub 6 cyfr do odblokowania telefonu.

**Jak ustawić:**
Wejdź w Ustawienia → Zabezpieczenia / Zabezpieczenia i prywatność → Blokada ekranu i wybierz PIN.

**Jaki PIN wybrać?**

- **Dobrze**: 284719, 837492 (brak oczywistego układu)
- Źle: 1111, 1234, data urodzenia, 0000

**Rada:**
Zapisz PIN w domu, w bezpiecznym miejscu, np. w szufladzie z dokumentami (nie w telefonie i nie w portfelu!).

## OPCJA 2

**Wzór:** odblokowanie telefonu poprzez narysowanie kształtu na ekranie.

**Jak ustawić:**
Wejdź w Ustawienia → Zabezpieczenia / Zabezpieczenia i prywatność → Blokada ekranu i wybierz Wzór

- Dobrze: skomplikowany kształt z zakrętami
- Źle: litera „L”, prosty kwadrat

**Uwaga:** To mniej bezpieczna metoda - na ekranie mogą pozostać ślady, po których ktoś domyśli się twojego wzoru.

# OPCJA 3

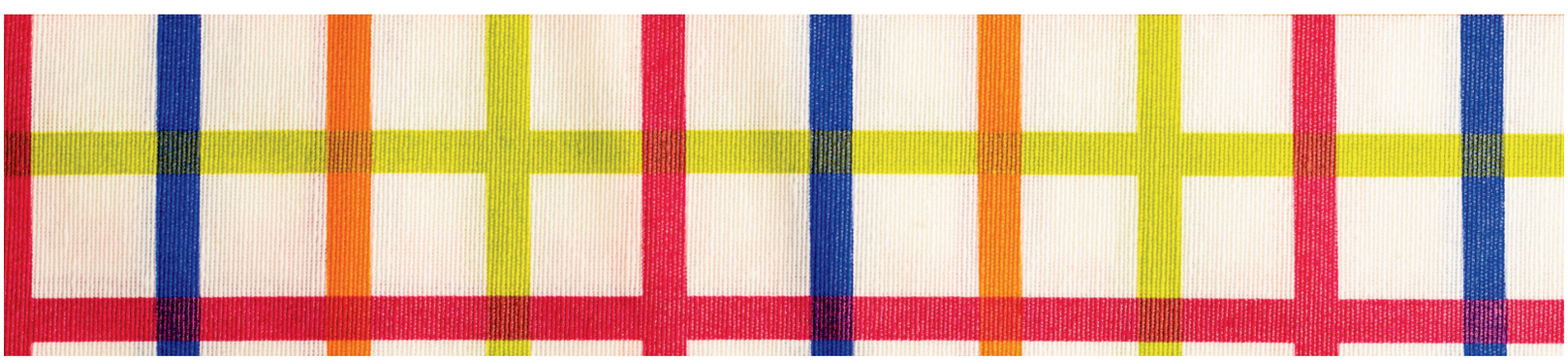
**Odcisk palca/rozpoznanie twarzy:** telefon rozpoznaje twój palec lub twarz.

**Dlaczego to dobre rozwiązanie?**

- szybkie,
- bezpieczne,
- nie musisz nic pamiętać.

**Jak ustawić:**
Wejdź w Ustawienia → Zabezpieczenia / Zabezpieczenia i prywatność → Blokada ekranu i wybierz Odcisk palca / Twarz

**Uwaga:** jeśli telefon nie rozpozna twarzy lub odcisku palca, poprosi o PIN. Dlatego warto mieć ustawiony.



**Historia z życia**
Pan Stanisław zgubił telefon na targu. Na szczęście miał ustawiony PIN. Ktoś znalazł telefon i oddał go do biura rzeczy znalezionych. Gdyby nie blokada, znalazca mógłby przejrzeć prywatne wiadomości, zdjęcia rodzinne, a nawet wejść na konto bankowe. Dzięki PIN-owi wszystko pozostało bezpieczne.

**Zapamiętaj**
**Blokada ekranu to jak zamek w drzwiach - absolutna podstawa. Jeśli jeszcze jej nie masz - ustaw ją dzisiaj.**

# MOCNE HASŁO – JAK JE STWORZYĆ I NIE ZWARIOWAĆ?

Hasła to klucze do twojego cyfrowego życia. Niestety wiele osób używa bardzo prostych haseł, które oszuści łamią w kilka sekund.
Hasło jest jak zamek: wolisz pancerny sejf czy kłódkę za złotówkę?

Masz wszędzie to samo hasło? – przegrywasz wszystko naraz.

## Dobre vs. złe hasła

| **Źle** | **Dobrze!** |
|---|---|
| kotek | K0t3k!JestPuszysty |
| jan123 | J4n_Ur0dz0ny#199 |
| data urodzenia | 50!06!15Ur |

To tylko przykłady — nie używaj ich dosłownie!

---

## 3 złote zasady tworzenia haseł

1. **Długość = siła**
Minimum 8 znaków, ale im dłuższe, tym lepsze!
słabe: kot (3 znaki – do złamania w sekundę)
**mocne**: MójKotLubiRyby!23 (17 znaków – bardzo trudne do złamania)

2. **Mieszaj składniki**
Dobre hasło to połączenie: dużych i małych liter, cyfr, znaków specjalnych (!, @, #).
**Przykład:**
AlaMaKota → Al4M@Kot@!7

3. **Inne hasło do każdego serwisu**
To naprawdę bardzo ważne! bank → jedno hasło ; poczta → inne
Facebook → inne.

# Jak to wszystko zapamiętać?

Na szczęście są proste sposoby.

**Sposób 1: zeszyt**

Możesz zapisać hasła w zeszycie.

**Zasady bezpieczeństwa:**

- trzymaj zeszyt w szufladzie z dokumentami,
- nie podpisuj go *„HASŁA”* — lepiej *„Notatki”* lub *„Ważne numery”*,

nigdy nie rób zdjęcia stron z hasłami.

**Dlaczego to bezpieczne?**

Bo złodziej musiałby włamać się do twojego domu i znaleźć ten zeszyt, a włamanie cyfrowe jest znacznie łatwiejsze.

---

**Sposób 2: metoda „zdania-hasła”**

Zamiast przypadkowych znaków, wykorzystaj zdanie, które łatwo **zapamiętasz:**

MójWnuczekMa5Lat!

---

**Sposób 3: menedżer haseł (dla chętnych)**

To specjalna aplikacja, która pamięta wszystkie hasła za ciebie. Ty pamiętasz tylko jedno - główne hasło.

**Jak działa?**

- zapisujesz hasła w programie (np. LastPass, Bitwarden),
- program je szyfruje,
- podczas logowania wpisuje je automatycznie.

**Zalety:** każde konto ma unikalne, mocne hasło oraz pamiętasz tylko jedno główne hasło.

**Wady:** wymaga krótkiej konfiguracji na początku.

**Dla kogo?**

Dla osób, które swobodniej korzystają ze smartfona lub mają kogoś, kto pomoże ustawić aplikację.

# Aplikacje: pobieraj tylko ze sklepu

Aplikacja to program w telefonie - może to być gra, prognoza pogody, aplikacja bankowa czy Facebook. Niestety, oszuści tworzą fałszywe aplikacje, które udają prawdziwe, a w rzeczywistości kradną dane lub pieniądze.

## Skąd bezpiecznie pobierać aplikacje?

| Typ telefonu | Sklep z aplikacjami | Ikona |
|---|---|---|
| Android | Google Play | |
| iPhone (Apple) | App Store | |

I to wszystko.
Jeśli ktoś proponuje inne miejsce — nie instaluj.

**Zapamiętaj**
Sklep z aplikacjami (Google Play / App Store) jest jak apteka - to, co tam znajdziesz, jest sprawdzone. Link z SMS-a to jak tabletki kupione na bazarze - nigdy nie wiesz, co dostajesz.

## Czego nigdy nie robić

Nie instaluj aplikacji z:

- SMS-ów lub e-maili z linkiem

Np.: *„Pobierz nową aplikację banku: www.jakistamlink.com”,*

- przypadkowych stron internetowych,
- jeśli ktoś przez telefon mówi, żeby wejść na stronę i coś pobrać - to oszustwo,
- instrukcji od *„pracownika banku”*

Bank nigdy nie prosi o instalację aplikacji przez telefon.


**Historia z życia**

Pani Krystyna dostała SMS-a:

*„Twoja przesyłka czeka. Zainstaluj aplikację do śledzenia paczek: [link]”.*

Zamiast kliknąć link, sama otworzyła Google Play, wpisała *„InPost”* i pobrała prawdziwą aplikację. To była świetna decyzja ponieważ SMS okazał się próbą oszustwa, a fałszywa aplikacja mogła przejąć jej konto bankowe.


# Aktualizacje: twoja cyfrowa tarcza

Czasem telefon wyświetla komunikat:
*„Dostępna jest aktualizacja systemu”*
I wielu z nas myśli: *„Zrobię to później…”* A potem odkłada to na kolejny dzień… i następny. Tymczasem unikanie aktualizacji, **to jeden z najczęstszych i najpoważniejszych błędów.**

## Co daje aktualizacja?

| Co się aktualizuje? | Co to daje? |
|---|---|
| Poprawki bezpieczeństwa | chronią telefon przed wirusami i włamaniami |
| Usprawnienia systemu | telefon działa sprawniej |
| Nowe funkcje | dodatkowe możliwości i ulepszenia |

**Zapamiętaj**
Aktualizacja to nie kłopot, tylko ochrona. To jak wymiana zamka w drzwiach na mocniejszy - robisz to, żeby czuć się bezpiecznie. Gdy telefon prosi o aktualizację - **zrób ją jak najszybciej.**

## Co to właściwie jest aktualizacja?

Wyobraź sobie, że twój telefon to dom. Aktualizacja to:

- załatanie dziur w ścianach,
- wymiana starego zamka na nowszy i mocniejszy,
- naprawa okien, które nie domykały się do końca.

Cyberprzestępcy szukają właśnie takich *„szczelin”.* Aktualizacja je zamyka, zanim ktoś zdąży je wykorzystać.

Dlaczego aktualizacje są takie ważne?
W 2025 roku wykryto poważne luki w systemie Android, które pozwalały hakerom przejąć telefon bez żadnego działania użytkownika — bez kliknięcia w link czy pobierania aplikacji. Osoby, które zainstalowały aktualizację, były bezpieczne. Ci, którzy ją zignorowali, mogli łatwo paść ofiarą oszustów.

## Jak zrobić aktualizację?

**Naładuj telefon**
minimum 50% baterii (najlepiej podłącz ładowarkę)

**Połącz się z Wi-Fi**
aktualizacje mogą sporo ważyć

**Kliknij „Zaktualizuj”**
gdy pojawi się komunikat

**Poczekaj**
telefon może się wyłączyć i włączyć ponownie
to normalne i zwykle trwa 10–20 minut

**Gotowe**
**wszystkie zdjęcia, kontakty i aplikacje zostają na miejscu**

# Wi-Fi: kiedy włączyć, a kiedy wyłączyć?

Wi-Fi to bardzo wygodny sposób łączenia się z Internetem. Warto jednak wiedzieć, kiedy korzystać z Wi-Fi, a kiedy lepiej przełączyć się na Internet mobilny.

## Co to jest Wi-Fi?

**Twój telefon może łączyć się z Internetem na dwa sposoby:**

- Wi-Fi – przez sieć bezprzewodową w domu lub w miejscach publicznych (np. kawiarnia, dworzec),

- Internet mobilny (4G/5G) – przez sieć komórkową (np. Plus, Orange, Play, T-Mobile).

Oba działają dobrze, ale różnią się poziomem bezpieczeństwa.

---

**Domowe Wi-Fi = bezpieczne**
Twoja domowa sieć ma hasło, które znasz ty i twoja rodzina. Możesz na niej bez obaw:

- logować się do banku,
- robić przelewy i zakupy online,
- wpisywać hasła,
- korzystać z poczty e-mail i mediów społecznościowych.

Na publicznym Wi-Fi **możesz:**

- oglądać filmiki,
- czytać portale,
- przeglądać Facebooka,
- sprawdzać pogodę, itp.

Na publicznym Wi-Fi **nie rób:**

- logowania do banku,
- płatności i zakupów online,
- wpisywania haseł.

**A co jeśli musisz sprawdzić konto w podróży?**
Użyj Internetu mobilnego (4G/5G) - jest bezpieczny, ponieważ połączenie jest szyfrowane przez operatora.
Ikonki na górze ekranu: 4G / LTE / 5G

**Jak włączyć Internet mobilny?**

- przeciągnij palcem z góry ekranu (otwórz szybkie ustawienia),
- wyłącz Wi-Fi,
- włącz dane komórkowe / Internet mobilny.

**Publiczne Wi-Fi znajdziesz m.in. w:**

- kawiarniach,
- hotelach,
- pociągach i autobusach,
- szpitalach, dworcach,
- *„darmowych sieciach miejskich”*.

**Dlaczego trzeba uważać?**
Bo nie wiesz, kto jeszcze jest w tej samej sieci. Oszuści mogą podglądać ruch w sieci i próbować przechwycić:

- hasła,
- dane karty płatniczej,
- loginy do poczty i banku.

To trochę tak, jakbyś wypowiadał na głos PIN do karty w zatłoczonym autobusie — ktoś może usłyszeć.


# Sprawdź, zanim klikniesz!

To jeden z najważniejszych rozdziałów w tym poradniku. Dlaczego? Bo większość oszustw i kradzieży pieniędzy zaczyna się od jednego kliknięcia w podejrzany link.

## Jak działa oszustwo?

**Oszust wysyła SMS lub e-mail z linkiem. Wiadomość wygląda *„prawie prawdziwie”*:**

*„Dzień dobry, twoja paczka czeka w magazynie. Dopłata 1,50 zł: www.jakis-dziwny-link.com”*

*Klikasz → otwiera się strona wyglądająca jak bank → wpisujesz login i hasło → oszust je przejmuje → tracisz pieniądze.*

## ZŁOTE ZASADY

1. Podejrzany SMS/e-mail? NIE KLIKAJ!
2. Sprawdź nadawcę i link – coś dziwnego? To oszustwo!
3. Zweryfikuj – zadzwoń do firmy/banku na znany Ci numer.
4. Wątpliwości? Skasuj i zapomnij.
5. Nie wstydź się zapytać kogoś młodszego: *"Zobacz, czy to nie oszustwo?".*

**Zapamiętaj:**
Kliknięcie w link trwa sekundę. Odzyskanie skradzionych pieniędzy może być niemożliwe. Zawsze lepiej 5 razy sprawdzić niż raz stracić!

**Historia z życia**
Pani Janina, 68 lat:
*„Dostałam SMS-a o dopłacie 1,80 zł do paczki. Już chciałam kliknąć, ale przypomniałam sobie radę ze szkolenia: sprawdź link. Zobaczyłam dziwny adres i zadzwoniłam do córki. Paczka już była na poczcie — żadnej dopłaty nie było. Gdybym kliknęła, mogłabym stracić pieniądze. Dobrze, że zatrzymałam się na chwilę!"*

**Co zrobić, zanim klikniesz?**

1. Zatrzymaj się.
2. Nie klikaj od razu.
3. Sprawdź podejrzane elementy.
4. Przejrzyj „7 czerwonych flag".
5. Zweryfikuj samodzielnie
    - **paczka** → sprawdź w aplikacji lub na oficjalnej stronie, wpisując adres ręcznie,
    - **bank** → zadzwoń na numer z karty lub wejdź do aplikacji,
    - **urząd** → zadzwoń lub sprawdź osobiście.
6. Skasuj wiadomość, jeśli masz pewność, że to oszustwo.
7. Ostrzeż bliskich.
8. Podziel się informacją — szczególnie z seniorami w rodzinie.

# Jak rozpoznać próbę oszustwa?

1. **Wiadomość o „dopłacie”**
**Przykłady:**

- *„Niedopłata 1,23 zł”*
- *„Dopłać 2 zł do przesyłki”*
- *„Opłata celna 3 zł”*

**Dlaczego to podejrzane?**
Prawdziwe firmy kurierskie nie proszą o drobne dopłaty przez SMS z linkiem.

---

2. **Straszenie blokadą**
Przykłady:

- *„Twoje konto zostanie zablokowane”*
- *„Podejrzana aktywność”*
- *„Potwierdź dane, aby nie zawiesić usług”*

**Ważne:** banki i urzędy nie każą klikać w link, żeby uniknąć blokady. Jeśli coś jest nie tak - zawsze sprawdzisz to po samodzielnym zalogowaniu do aplikacji lub kontaktując się z infolinią.

---

3. **Błędy językowe**
**Przykłady:**

- *„Twoja przesyłka czeka w magazyn”*
- *„Prosimy o klikniecie”*
- *„Twoj konto”*

Oszuści często korzystają z translatorów. Prawdziwe instytucje dbają o poprawność językową.

# Jak rozpoznać próbę oszustwa?

4. **„Za piękne, żeby było prawdziwe”**

**Przykłady:**

- *„Wygrałeś 50 000 zł!”*
- *„Zwrot podatku czeka!”*
- *„Gratulacje, zostałeś wybrany!”*

Jeśli nigdzie się nie zgłaszałeś i nic nie kupowałeś — nic nie wygrałeś.

---

5. **Dziwny lub bardzo długi link**

Prawidłowe adresy:

- www.pkobp.pl
- www.inpost.pl
- www.allegro.pl

Podejrzane adresy:

- www.pkobp-bezpieczne-klient-verify.xyz
- www.pko-bp.com.pl.verify-secure.ru
- bit.ly/abC12X (skrócone linki — nie widać dokąd prowadzą)

Jeżeli adres jest długi, dziwny, inny niż zwykle — nie klikaj.

---

6. **Presja czasu i prośba o dane**

**Przykłady:**

- *„Ostatnia szansa!”*
- *„Kliknij natychmiast!*
- *PESEL, numer karty, PIN, kod SMS-a.*

Oszust chce, żebyś działał w pośpiechu. Zasada nr 1: zatrzymaj się i pomyśl.

# BEZPIECZNY KOMPUTER

## Bezpieczeństwo to połączenie technologii i zdrowego rozsądku.

Wyobraź sobie, że twój komputer to dom. Masz w nim wszystko, co ważne: zdjęcia z rodzinnych uroczystości, dokumenty, dostęp do banku, wiadomości od bliskich.

Wirusy to cyfrowi włamywacze, którzy próbują dostać się do środka, żeby:

- ukraść hasła,
- wyłudzić pieniądze,
- zablokować komputer i żądać okupu,
- zniszczyć lub zaszyfrować pliki.

Antywirus to strażnik, który pilnuje wejścia i chroni twój komputer przed zagrożeniami.


## Co robi antywirus?

| Funkcja | Co to oznacza? |
| --- | --- |
| Wykrywa wirusy | skanuje i ostrzega pliki |
| Blokuje szkodliwe strony | antywirus pokaże komunikat o zagrożeniu. |
| Chroni przed szpiegowaniem | uniemożliwia śledzenie |
| Sprawdza e-maile | ostrzega gdy jest wirus |

---

**Jaki antywirus wybrać?**

Dobra wiadomość: jeśli używasz Windows 10 lub Windows 11, masz już antywirusa. Nazywa się Windows Defender (Windows Security) i jest darmowy. Dla większości użytkowników to wystarczająca ochrona.

**Zapamiętaj**

Antywirus jest jak strażnik przy bramie — pomaga chronić komputer przed zagrożeniami. Ale pamiętaj: jeśli sam *„wpuszczasz złodzieja”*, klikając w podejrzane linki, nawet najlepszy antywirus może nie pomóc

**Historia z życia**

**Pan Tadeusz, 72 lata:**

**Włączyłem komputer i wyskoczył napis: *„Komputer zablokowany! Zapłać 500 zł, aby odzyskać pliki. Zdenerwowałem się, ale zadzwoniłem do wnuka. Powiedział: ‘Dziadku, nic nie płać’. Przyjechał, włączył antywirusa i usunął wirusa. Oszuści mieliby moje dane.”***

**Skąd wiedzieć, że komputer może mieć wirusa?**

**Sygnały ostrzegawcze:**

- komputer działa nietypowo wolno,
- pojawiają się wyskakujące reklamy,
- pliki znikają lub mają dziwne nazwy,
- antywirus pokazuje częste alerty,
- widzisz programy, których nie instalowałeś.

---

**Złote zasady korzystania z antywirusa**

- zawsze miej włączony antywirus,
- regularnie aktualizuj Windows,
- jeśli antywirus ostrzega — zaufaj mu,
- nie instaluj kilku antywirusów naraz (mogą się „gryźć”),
- zielona tarcza = komputer bezpieczny.

# POCZTA E-MAIL: PUŁAPKI W SKRZYNCE

E-mail (poczta elektroniczna) to jedno z najczęściej używanych narzędzi przez oszustów. Dlaczego? Bo wysłanie tysięcy fałszywych wiadomości nic ich nie kosztuje. Oszust wysyła wiadomość, która udaje e-mail od banku, urzędu albo sklepu. To tzw. phishing (czyt. *„fiszing”*) — czyli *„łowienie”* ofiar w Internecie.

## Jak wygląda e-mail od oszusta?

*OD: Bank PKO BP <kontakt@pko-bezpieczenstwo.com>*
*TEMAT: PILNE! Zablokowanie konta*

*Szanowny Kliencie,*

*Wykryliśmy podejrzana aktywność na Twoim koncie.*
*Ktoś próbował wykonać przelew na kwotę 8000 zł.*

*Musisz natychmiast potwierdzić swoją tożsamość,*
*klikając w poniższy link:*

*[POTWIERDŹ TOŻSAMOŚĆ]*

*W przeciwnym razie Twoje konto zostanie*
*permanentnie zablokowane.*

*Z poważaniem,*
*Zespół Bezpieczeństwa PKO BP*

# Co jest nie tak z tym mailem?

**Adres nadawcy jest dziwny**
Zawsze sprawdź, kto naprawdę wysłał e-mail. Nazwy mogą być fałszywe - liczy się adres!

**Fałszywy:** kontakt@pko-bezpieczenstwo.com / kontakt@pkobp.pl / urzad.skarbowy@wp.pl / netflix.pomoc@outlook.com

**Jak sprawdzić?**
Kliknij lub dotknij nazwę nadawcy — zobaczysz pełny adres e-mail.

**Zapamiętaj:**
Banki i urzędy nie wysyłają ważnych wiadomości z prywatnych adresów (gmail, WP, Onet). Jeśli wygląda „urzędowo", a jest z darmowej poczty → uważaj!

---

**Podejrzany załącznik**
Uważaj na pliki typu:
.exe, .scr, .bat — mogą instalować wirusy
.zip z nieznanego źródła
Bezpieczniejsze rozszerzenia: .pdf, .jpg, .png, .docx — ale otwieraj tylko od znanych osób.

---

**Zapamiętaj:**
Fałszywy e-mail jest jak obca osoba pukająca do drzwi i mówiąca, że ma dla ciebie ważną przesyłkę. Nie otwierasz od razu — najpierw sprawdzasz, kto to. Tak samo rób z wiadomościami w Internecie.

# Co jest nie tak z tym mailem?

**Prosi o hasło, PIN lub dane karty**
ŻADNA firma, bank, urząd NIGDY nie poprosi mailowo o:

- Hasło
- PIN do karty
- Numer karty + CVV
- PESEL
- Numer dowodu

Jeśli mail o to prosi — to prawdopodobnie oszustwo.

---

**Straszy lub kusi**
Oszuści używają dwóch emocji:

**STRACH:**

- *"Twoje konto zostanie zablokowane!"*
- *"Grozi Ci kara!"*
- *"Ktoś się włamał na konto!"*

**ZACHŁANNOŚĆ:**

- *"Wygrałeś 10 000 zł!"*
- *"Zwrot podatku czeka!"*
- *"Ekskluzywna oferta dla Ciebie!"*

Prawdziwe firmy piszą spokojnie i rzeczowo.

---

**Błędy językowe**
Fałszywe wiadomości często zawierają literówki, brak polskich znaków lub dziwne sformułowania. Prawdziwe instytucje dbają o poprawność tekstów.

# BEZPIECZNE ZAKUPY W INTERNECIE

Zakupy online to ogromna wygoda — nie trzeba jechać do miasta, stać w kolejkach ani dźwigać ciężkich toreb. Kurier dostarcza paczkę prosto pod drzwi. Warto jednak znać kilka zasad, aby robić zakupy bezpiecznie.

## Gdzie robić bezpieczne zakupy?

W znanych sklepach internetowych, np.: Allegro, Zalando, Euro RTV AGD, Media Expert, Empik, oraz na oficjalnych stronach producentów (Samsung, Apple, Nike).
Na OLX zachowaj ostrożność — to platforma z ofertami od osób prywatnych.

## ZŁOTE ZASADY

- kupuj w znanych sklepach (Allegro, znane marki),
- sprawdzaj kłódkę w pasku adresu,
- czytaj opinie przed zakupem,
- jeśli cena jest za piękna – to pułapka!,
- unikaj przelewów na prywatne konta,
- wątpliwości? Zapytaj rodzinę przed zakupem.

**Czego unikać?**

- stron o dziwnych nazwach (np. super-tani-sklep-24h.xyz),
- sklepów bez opinii,
- „super promocji” (np. telewizor za 50 zł),
- podejrzanych reklam w Internecie, linków wysyłanych SMS-em.

**Zapamiętaj:**
Internet jest jak bazar: są uczciwi sprzedawcy z dobrym towarem, ale zdarzają się też naciągacze. Warto wybierać sprawdzone miejsca!

**Historia z życia:**
**Pani Elżbieta, 65 lat:**
***„Szukałam w Google nowego odkurzacza. Znalazłam stronę, gdzie kosztował 200 zł taniej niż wszędzie indziej. Pomyślałam: Świetna okazja!'. Ale córka powiedziała: 'Mamo, sprawdźmy najpierw opinie'. Wpisałyśmy nazwę sklepu w Google – wszystkie opinie krzyczały: OSZUSTWO!"***

**Jak rozpoznać fałszywy sklep?**

| **Sygnał** | **Co to oznacza?** |
|---|---|
| Cena bardzo niska | Telewizor za 100 zł? Podejrzane. |
| Brak opinii | Może być nowy… albo nieistniejący. |
| Błędy językowe | *„Kup teraz ofert"* — sygnał ostrzegawczy. |
| Brzydka, chaotyczna strona | Może być przygotowana szybko przez oszustów. |

# Jak sprawdzić, czy sklep jest bezpieczny?

**KROK 1: Sprawdź adres strony (HTTPS)**
Po kliknięciu w pasku adresu (na samej górze) sprawdź, od czego zaczyna się adres strony:

- *HTTPS://...* – Oznacza, że połączenie jest szyfrowane (nikt nie podgląda, co robisz).
- *HTTP://...* – Oznacza, że połączenie jest niezaszyfrowane. "Niezabezpieczona". Nigdy nie podawaj tu swoich danych!

**Wskazówka:** Jeśli widzisz przy adresie symbol kłódki (lub jeśli po kliknięciu w ikonę obok adresu pojawia się komunikat o bezpieczeństwie), to jest to dodatkowe potwierdzenie, że używany jest protokół HTTPS.

---

**Krok 3: Sprawdź dane kontaktowe**
Prawdziwy sklep powinien mieć: nazwę i adres firmy, NIP, numer telefonu, regulamin i politykę zwrotów.
Podejrzane sklepy:

- brak adresu, tylko e-mail (np. gmail),
- brak NIP, regulaminu i danych firmy.

Informacji szukaj w zakładkach *„Kontakt”* lub *„O nas”.*

---

**Krok 2: Sprawdź opinie**
Wpisz w Google: *„nazwa sklepu opinie”*
**Szukaj:**

- dużo pozytywnych opinii,
- komentarzy typu *„towar dotarł, wszystko OK”.*

**Unikaj stron, o których piszą:**

- *„oszustwo”, „nie dostałem towaru”, „brak kontaktu”.*


# WERYFIKACJA DWUSKŁADNIOWA (2FA) - TWÓJ „SPUER – ZAMEK”

To jedno z najlepszych zabezpieczeń, jakie możesz włączyć. Brzmi poważnie? *„Weryfikacja dwuskładnikowa”?* Spokojnie - to naprawdę proste.

## CO TO ZNACZY?

Wyobraź sobie, że twoje konto ma dwa zamki zamiast jednego:

- pierwszy zamek = twoje hasło,
- drugi zamek = kod wysłany SMS-em na telefon.

Żeby ktoś się zalogował, musi mieć oba *„klucze”.*

## DLACZEGO TO TAKIE WAŻNE?

**Gdy masz tylko hasło:**

- oszust zdobywa twoje hasło (np. z fałszywego e-maila),
- loguje się na konto,
- kradnie pieniądze.

**Gdy masz włączoną 2FA:**

- oszust wpisuje twoje hasło,
- system prosi o kod z SMS-a,
- oszust nie ma twojego telefonu → nie wejdzie na konto .

**Zapamiętaj**
Weryfikacja dwuskładnikowa to druga kłódka na bramie. Jedną można sforsować — dwie to już prawie niemożliwe. To jedna z najskuteczniejszych metod ochrony przed oszustami.

**Gdzie włączyć 2FA?**
**Włącz je wszędzie, gdzie to możliwe — szczególnie w:**

- **poczcie e-mail,**
- **banku,**
- **Facebooku i Messengerze,**
- **innych mediach społecznościowych.**

**Jak wygląda logowanie z 2FA?**

**Bez 2FA:**

- wpisujesz hasło,
- jesteś w środku.

**Z 2FA:**

- wpisujesz hasło,
- dostajesz SMS z kodem (np. „Twój kod: 472 839”),
- wpisujesz kod,
- dopiero wtedy się logujesz.

**To trwa kilka sekund, a daje ochronę jak dwa solidne zamki w drzwiach.**

# POPULARNE OSZUSTWA

**Bezpieczeństwo to połączenie technologii i zdrowego rozsądku.**

Popularne oszustwa wymierzone w seniorów najczęściej wykorzystują zaufanie, niewiedzę lub samotność osób starszych. Do najpowszechniejszych należą oszustwa *„na wnuczka”*, *„na policjanta”* lub *„na urzędnika”*, w których przestępcy podszywają się pod bliskich lub funkcjonariuszy i nakłaniają do przekazania pieniędzy. Seniorzy bywają też celem domokrążców oferujących podejrzane umowy lub usługi.

# Oszustwo „na wnuczka”

To jedno z najstarszych oszustw wymierzonych w seniorów. Oszust podaje się za wnuka lub inną bliską osobę, licząc na panikę i szybkie działanie.

## Jak wygląda taki telefon?

**Krok 1:** Telefon od *„wnuczka”*
**Głos:** *„Cześć babciu... (płacz)”*
**Ty:** *„Kto mówi?”*
**Głos:** *„No jak to kto... nie poznajesz mnie?”*
Oszust nie mówi imienia — czeka, aż sam/a je podasz:
**Ty:** *„Janek?”*
**Oszust:** *„Tak, babciu...”*
Od tego momentu gra trwa dalej.

**Krok 2:** Dramatyczna historia
**Przykłady:**

- *„Miałem wypadek, potrzebuję pieniędzy na operację!”*
- *„Jestem na policji, muszę zapłacić kaucję!”*
- *„Muszę wpłacić zadatek jeszcze dziś!”*

Oszust chce wzbudzić silne emocje - strach, współczucie, poczucie obowiązku.

**Krok 3:** Presja czasu i tajemnica

- *„Potrzebuję pieniędzy natychmiast.”*
- *„Proszę, nie mów nikomu - wstydzę się.”*

Celem jest, żebyś nie zdążył/a się zastanowić ani nikomu powiedzieć.

**Krok 4:** Odbiór pieniędzy przez *„znajomego”*

- *„Nie mogę podjechać. Przyjdzie kolega i odbierze pieniądze.”*

Po pieniądze przychodzi obca osoba - i znika.

**Historia z życia**
**Pani Władysława, 78 lat:**
***„Zadzwonił ktoś, płakał: ‘Babciu, to ja, Damian. Potrąciłem kogoś na pasach.’***
***Przeraziłam się. Oddałam 12 000 zł. Wieczorem zadzwoniłam do prawdziwego Damiana — był w pracy, nic mu się nie stało. Zrozumiałam, że padłam ofiarą oszustwa.”***

**Zapamiętaj**

- zawsze oddzwoń na znany numer,
- nie przekazuj pieniędzy obcym osobom,
- jeśli sytuacja wydaje się pilna i tajna - sprawdź ją dwa razy,
- lepiej zrobić jeden telefon kontrolny niż stracić oszczędności życia.


# Oszustwo „na policjanta”

Fałszywy policjant dzwoni z *„pilną"* informacją: twoje pieniądze są zagrożone. Ironia? To właśnie on stanowi największe zagrożenie - pod pretekstem ochrony chce wyłudzić twoje oszczędności.

## Jak wygląda taki schemat?

**Krok 1:** Telefon od „policji”
Na ekranie telefonu może pojawić się napis „POLICJA” lub numer 997.
*„Tu aspirant Kowalski. Pani konto jest zagrożone przez grupę przestępczą. Musi pani pomóc w tajnej operacji.”*

Oszust mówi poważnym, służbowym tonem, aby wzbudzić zaufanie i stres.

⬇

**Krok 2:** Polecenia
Oszust może poprosić o:
wypłacenie wszystkich oszczędności, przekazanie pieniędzy rzekomemu *„funkcjonariuszowi pod przykrywką”,* wykonanie przelewu na *„bezpieczne konto”.*

**Krok 3:** Tajemnica i presja
*„To tajna akcja. Nie może pani nikomu o tym mówić!”*
Celem jest, byś działał/a szybko i bez konsultacji z kimkolwiek.

**Prawdziwa policja nigdy:**

- nie prosi o wypłacenie pieniędzy,
- nie odbiera gotówki od obywateli,
- nie prowadzi „tajnych akcji” z twoimi oszczędnościami,
- nie prosi o przelew na „bezpieczne konto”,
- To wszystko są działania oszustów,
- Nie istnieje coś takiego jak „policyjne bezpieczne konto”.

**Co zrobić?**

- zachowaj spokój,
- powiedz: *„Oddzwonię na komisariat”*,
- samodzielnie zadzwoń na numer 112 lub na lokalny, komisariat, korzystając z oficjalnego numeru.

**Oszust zazwyczaj natychmiast się rozłącza.**


# Oszustwo „na pracownika banku”

**To jedno z najczęściej spotykanych oszustw w ostatnich latach.**

## Jak wygląda taki schemat?

**Krok 1:** Telefon z „banku”
Na ekranie może pojawić się nazwa banku lub prawdziwy numer, np. PKO BP.
*„Dzień dobry, dzwonię z banku. Wykryliśmy podejrzaną aktywność na koncie.”*

**Krok 2:** Prośba o dane
Oszust może poprosić o:

- numer karty i kod CVV,
- login i hasło do banku,
- kod z SMS-a (uwaga — kod potwierdza przelew!),
- wykonanie przelewu na *„konto techniczne”*.

**Krok 3:** Wywołanie strachu
Oszust brzmi profesjonalnie, używa oficjalnych sformułowań i może znać twoje imię i nazwisko. Często mówi:
*„Za chwilę straci pan wszystkie oszczędności."*
To ma sprawić, że zaczniesz działać w pośpiechu.

Historia z życia
Pan Marek, 69 lat:
*„Zadzwoniła osoba podająca się za pracownika banku. Znała moje dane i mówiła bardzo przekonująco. W panice przelałem 45 000 zł na 'konto zabezpieczone'. Po godzinie coś mnie tknęło. Zadzwoniłem do banku - okazało się, że padłem ofiarą oszustwa. Pieniędzy nie udało się odzyskać."*

**Prawdziwy pracownik banku nigdy nie poprosi o:**

- hasło do konta,
- PIN do karty,
- kod z SMS-a,
- numer pełnej karty i CVV,
- przelanie pieniędzy na *„konto techniczne"* lub *„konto bezpieczeństwa".*

Te prośby padają tylko od oszustów.
Nie istnieją *„konta techniczne"* służące do ochrony pieniędzy.

---

**Jak reagować?**

- nie podawaj żadnych danych,
- rozłącz się,
- zadzwoń samodzielnie do banku (na numer z oficjalnej strony lub z umowy, a nie z SMS-a).

# Oszustwo „na zdalny pulpit”

To jedno z najgroźniejszych oszustw. Po jego wykonaniu przestępca może mieć pełną kontrolę nad twoim komputerem.

## Jak przebiega oszustwo?

**Krok 1:** Telefon od „pomocy technicznej”
Oszust podaje się za pracownika Microsoftu, operatora Internetu lub serwisu technicznego:
*„Dzwonimy, bo komputer ma wirusa. Pomożemy zdalnie.”*

**Krok 2:** Prośba o instalację programu
Przestępca prosi o zainstalowanie programu do zdalnej obsługi, np.: AnyDesk, TeamViewer.

**Krok 3:** Podanie kodu
Po wpisaniu kodu oszust może: widzieć cały ekran komputera, poruszać myszką, wpisywać hasła itd.
Użytkownik widzi wszystko na ekranie, ale nie ma kontroli nad komputerem.

**Jak się bronić?**
nigdy nie instaluj programów na prośbę osoby dzwoniącej,
Microsoft ani operatorzy nie dzwonią, żeby prosić o instalowanie takich aplikacji,
jeśli ktoś mówi o *„wsparciu technicznym przez telefon”* — rozłącz się.

Historia z życia
Pan Andrzej, 75 lat:
*„Zainstalowałem AnyDesk, bo myślałem, że dzwonią z obsługi Internetu. Nagle myszka zaczęła poruszać się sama, a oszust otworzył bankowość. Szybko odłączyłem Internet - straciłem 2 000 zł, ale reszta pieniędzy została uratowana.”*

**Jeśli już zainstalowałeś program to zrób to natychmiast:**

1. Odłącz Internet
2. Wyłącz Wi-Fi lub wyjmij kabel.
3. Zadzwoń do banku i zablokuj dostęp do konta.
4. Poinformuj policję — numer 112.
5. Odinstaluj program (w razie potrzeby poproś rodzinę o pomoc).

Im szybciej zadziałasz, tym większa szansa, że pieniądze zostaną uratowane.

# Oszustwo „na dopłatę” (SMS)

To jedno z najczęstszych oszustw - proste i skuteczne, bo wygląda bardzo wiarygodnie.

## Jak wygląda taki SMS?

Przykład:
Twoja paczka czeka. Niedopłata 1,50 zł.
Opłać: http://inpo5t-paczka.com

## Co się stanie, jeśli klikniesz?

- **Fałszywa strona banku**

SMS prowadzi do podrobionej strony banku. Wpisujesz login i hasło → oszust je przejmuje → możesz stracić pieniądze.

- **Płatna subskrypcja SMS**

Link może uruchomić usługę Premium SMS, która pobiera opłaty z telefonu co tydzień.

**Jak rozpoznać podejrzany SMS?**

- prośba o dopłatę kilku złotych (1–3 zł),
- link do strony w SMS-ie,
- cyfry zamiast liter (np. „inpo5t”),
- dziwny adres strony (np. .xyz, paczka-track23.com),
- wiadomość sugeruje pośpiech.

Uwaga: prawdziwe firmy kurierskie nie wysyłają SMS-ów z linkiem do dopłaty.

**Co zrobić?**

- usuń wiadomość,
- sprawdź paczkę w aplikacji lub na oficjalnej stronie, (wpisz adres ręcznie, np. inpost.pl),
- w razie wątpliwości pokaż SMS bliskiej osobie.


**Zapamiętaj**

Dopłaty przez SMS to częsta metoda oszustów. Jeśli faktycznie istnieje dopłata do przesyłki, dowiesz się o niej w aplikacji lub przy odbiorze, a nie z podejrzanego linku.

# Fałszywe inwestycje i loterie

To oszustwa, które wykorzystują marzenie o szybkich i łatwych zarobkach.

## Oszustwo „na inwestycję”

Przykład komunikatu:
*„Zainwestuj 1000 zł, za miesiąc będziesz mieć 10 000 zł. Gwarantowany zysk!”.*
Jak to działa?

1. Wpłacasz pierwszą kwotę, np. 500 zł.
2. Po kilku dniach na ekranie widzisz „zysk” (np. 700 zł), ale nie możesz wypłacić pieniędzy.
3. Oszust prosi o kolejne wpłaty — „zabezpieczenie”, „opłatę techniczną”.
4. Po czasie kontakt znika, a środki przepadają.

**Pamiętaj:** prawdziwe inwestycje nigdy nie gwarantują wysokich i szybkich zysków.

# Oszustwo „na wygraną”

Przykład:
*„Wygrałeś 50 000 zł!”*
A potem pojawia się wymóg:
„Wpłać 200 zł opłaty manipulacyjnej, aby odebrać nagrodę.”
**Fakty:**
Jeśli nie brałeś udziału w konkursie, nie mogłeś wygrać.
Legalne loterie nie proszą o wpłaty przed wypłatą nagrody.

**Zapamiętaj**

- jeśli coś brzmi zbyt pięknie, by było prawdziwe. Zwykle nie jest prawdziwe.
- nikt nie daje pieniędzy za darmo.
- uważaj na obietnice szybkiego, pewnego i wysokiego zysku to najczęstsze *„czerwone flagi”*.

# Oszustwa na Facebooku i Messengerze

Coraz częściej oszuści przejmują konta na Facebooku lub Messengerze i piszą do znajomych, udając właściciela konta.

## Jak wygląda oszustwo?

Dostajesz wiadomość od znajomej osoby:
*„Cześć! Mam kłopot. Pożyczysz 500 zł? Oddam jutro.”*
W rzeczywistości:

- to nie znajoma osoba,
- oszust włamał się na jej konto i próbuje wyłudzić pieniądze.

## Uwaga na podejrzane linki od „znajomych”

Czasem oszust nie prosi od razu o pieniądze. Może wysłać krótki komunikat z linkiem, np.: *„Zobacz, czy to ty na tym filmie ”, „Masz tu swoje zdjęcia!”, „Pilne! Kliknij!”*

**Kliknięcie może spowodować:**
przejęcie twojego konta (oszust pozna hasło),
instalację niebezpiecznego oprogramowania,
przekierowanie do fałszywej strony banku lub płatności.

**Jak się upewnić, że to prawdziwa prośba?**
Zadzwoń na numer telefonu tej osoby
Nie ufaj wiadomościom tylko z Messengera

**Zapytaj:**
*„Czy naprawdę prosisz o pożyczkę?”*
W większości przypadków usłyszysz:
*„Nie, to nie ja — ktoś włamał się na moje konto.”*

**Zasada:**
Jeśli widzisz dziwny link od znajomego — zadzwoń do niego lub napisz SMS:
*„Czy to ty wysłałeś ten link?”*

**Jeśli odpowie:**
*„Nie wiem, o co chodzi”* — nie klikaj i poinformuj go, że konto mogło zostać przejęte.

**Uwaga na kody BLIK**

Częsty komunikat oszustów:
*„Mój BLIK nie działa — podaj swój kod, zaraz oddam.”*
Nigdy nie podawaj kodu BLIK.

Kod BLIK działa jak PIN do karty — służy do pobierania pieniędzy z twojego konta.

## Co zrobić, jeśli padłeś ofiarą?

Najważniejsze: nie wstydź się. Oszustwa są przygotowane profesjonalnie - każdy może się nabrać.

**Krok 1:** Skontaktuj się z bankiem.
Poproś o: blokadę BLIK / karty / konta, anulowanie transakcji (jeśli możliwe).

**Krok 2:** Zgłoś sprawę na policję.
Zgłoszenia pomagają namierzać oszustów.

**Krok 3**: Poinformuj rodzinę: otrzymasz wsparcie, inni będą czujni.

**Krok 4:** Ostrzeż znajomych:  możesz uratować czyjeś pieniądze.

**Czy można odzyskać pieniądze?**
To trudne, bo oszuści działają szybko.
Jednak:

- bank może zablokować transakcję, jeśli zadzwonisz szybko,
- policja czasem namierza sprawców,

Im szybciej zareagujesz, tym większa szansa.

**Zapamiętaj**
Sprawdzaj prośby o pieniądze telefonicznie, nie podawaj kodów BLIK, nie klikaj podejrzanych linków, działaj szybko i nie bój się prosić o pomoc.


# Dezinformacja, fake newsy i deepfake

## Dlaczego to ważne?

Kiedyś, aby oszukać ludzi, trzeba było przygotować fałszywe gazety lub ulotki. To było trudne i kosztowne.
Dziś sytuacja jest zupełnie inna - każdy może w kilka minut stworzyć fałszywą wiadomość i rozesłać ją do tysięcy osób. Często kosztuje to... nic.

**Dodatkowo rozwój sztucznej inteligencji (AI) sprawił, że niezwykle łatwo jest tworzyć:**

- fałszywe informacje,
- przerobione zdjęcia,
- podrobione nagrania wideo (deepfake).

Takie treści pojawiają się w Internecie codziennie - i jest ich coraz więcej.

**Po co ktoś tworzy fałszywe treści?**
Najczęstsze powody:
pieniądze - każde kliknięcie to zarobek z reklam,
manipulacja opinią - ktoś chce, abyś w coś uwierzył albo kogoś ocenił negatywnie,
wzbudzanie emocji - strach i sensacja przyciągają uwagę.

# Czym jest fake news?

**Fake news to fałszywa informacja,** która wygląda jak prawdziwy artykuł lub wiadomość.

**Charakterystyczne cechy:**

- sensacyjny tytuł,
- brak rzetelnych źródeł,
- fałszywe lub podejrzane strony internetowe.

**Przykład fake newsa:**

PILNE! Rząd wprowadza podatek od posiadania psa! 500 zł rocznie!

Źródło: *„Prawda24h.xyz”*

Brak autora, brak daty

**Jak poznać, że to fałsz?**

- nie ma podanych źródeł,
- nazwa strony jest podejrzana,
- tytuł wywołuje emocje i szok.

**Zapamiętaj**

**Emocje = sygnał ostrożności** (szok, strach, sensacja).
Zawsze sprawdzaj źródło informacji.
Nie udostępniaj niczego, czego nie jesteś pewien/pewna.

**Bezpieczna zasada:**

Zanim klikniesz *„Udostępnij”* - zatrzymaj się i sprawdź.

# Prawdziwy przykład dezinformacji

**Pandemia COVID-19**

**Fałszywa informacja:**
*„Bill Gates chce wszczepiać ludziom chipy przez szczepionki!”*

**Rzeczywistość:**

- to był fałszywy przekaz, powielany w Internecie,
- krążyły przerobione grafiki i materiały wideo,
- nie istniały żadne „chipy w szczepionkach”.

**Skutki:**

- wielu ludzi uwierzyło w fałszywe treści,
- część osób odmawiała szczepień,
- utrudniało to walkę z pandemią.

# Jak rozpoznać fake news?

**Zanim udostępnisz wiadomość, zadaj sobie trzy pytania:**

1. **Kto to napisał?**

**Dobrze:**

- znane, rzetelne media (np. TVP, Polsat, Onet, PAP),
- podany autor artykułu,
- strona ma zakładkę *„O nas”.*

**Źle:**

- podejrzana nazwa strony (np. *„prawda-24h.xyz”*),
- brak autora,
- mnóstwo reklam i wyskakujących okien.

---

2. **Kiedy to było?**

**Dobrze:**

- widoczna i aktualna data publikacji.

**Źle:**

- brak daty,
- bardzo stare informacje podawane jako nowe.
- uwaga: oszuści często wykorzystują stare artykuły, aby wywołać emocje,
- jeśli wydarzyło się coś ważnego, piszą o tym różne media, sprawdź inne źródła.

# Sztuczna inteligencja (AI): nowe zagrożenia i jak się przed nimi chronić

Sztuczna inteligencja (AI) bardzo przyspieszyła tworzenie fałszywych treści w internecie. Jeszcze kilka lat temu stworzenie fałszywego artykułu czy filmu wymagało umiejętności i czasu. Dziś może zrobić to każdy w kilka kliknięć.

**AI potrafi:**

- pisać fałszywe artykuły i wiadomości,
- tworzyć realistyczne zdjęcia, które nigdy nie istniały,
- tworzyć filmy i głosy przypominające prawdziwe osoby (tzw. deepfake).

Dlatego fałszywych treści jest coraz więcej i są coraz bardziej przekonujące.

# Fałszywe zdjęcia

AI może tworzyć obrazy, które wyglądają jak prawdziwe zdjęcia.

**Sposób 1: prawdziwe zdjęcia z fałszywym opisem**
Przykład:
Dołączone jest zdjęcie powodzi, a pod nim opis:
*„Powódź w Krakowie!”*
Prawda: to zdjęcie może pochodzić z innego kraju lub sprzed lat.

**Jak sprawdzić?**
Kliknij zdjęcie prawym przyciskiem i wybierz opcję wyszukiwania obrazu w Google.

---

**Sposób 2: zdjęcia stworzone przez AI**
AI potrafi wygenerować obraz, którego nigdy nie było.
Przykład: słynne zdjęcie *„papieża w puchowej kurtce”, które uwierzyły miliony osób”.*

**Jak rozpoznać fałszywe zdjęcie?**

- nienaturalne dłonie (AI często myli palce),
- dziwne cienie lub proporcje,
- zbyt „idealny”, nienaturalny wygląd.

Uwaga: AI rozwija się bardzo szybko - rozpoznawanie takich zdjęć będzie coraz trudniejsze. Dlatego zawsze sprawdzaj źródło.


## Czym jest deepfake?

Deepfake to film lub nagranie dźwiękowe stworzone przez AI, w którym wygląda (lub brzmi), jakby dana osoba coś powiedziała, choć tego nigdy nie zrobiła.

## Czym jest deepfake?

**Przykład: fałszywe przemówienie prezydenta Zełenskiego (2022)**

Stworzono film, w którym prezydent Ukrainy miał wzywać żołnierzy do poddania się. Film był fałszywy. Usta i mimika nie pasowały do dźwięku. Celem było wywołanie paniki i chaosu.

**Jak rozpoznać deepfake?**
Zwracaj uwagę na:
**Obraz**

- ruch ust nie pasuje do słów,
- rzadkie mruganie, nienaturalne spojrzenie,
- dziwne światło lub cienie.

**Głos**

- brzmi nienaturalnie i monotonnie,
- zdarzają się *„przeskoki”* lub przerwy.

**Najważniejsze: sprawdź źródło** wiadomości w telewizji i na oficjalnych kanałach — większa wiarygodność,

- film od *„znajomego”* na Messengerze lub TikToku — bądź ostrożny.

---

**Dlaczego to poważny problem?**
Kiedyś stworzenie deepfake’u wymagało specjalistów i sprzętu.  Dziś może to zrobić praktycznie każdy, za darmo.

**Efekt:**

- fałszywych filmów będzie coraz więcej,
- będą wyglądać coraz bardziej realistycznie,
- trudniej będzie odróżnić prawdę od fałszu.
- dlatego równie ważna jak technologia jest czujność użytkowników.

**Jak zachować bezpieczeństwo?**
Nie udostępniaj informacji, jeśli nie masz pewności, że są prawdziwe.

- sprawdź źródło,
- sprawdź datę,
- zobacz, czy inne media o tym piszą,
- w razie wątpliwości — poczekaj lub zapytaj bliskich.
- nie wierz w sensacyjne nagłówki,
- nie rozpowszechniaj ostrzeżeń z łańcuszków,
- nie przesyłaj dalej niesprawdzonych treści.

Lepiej nie udostępnić niczego niż udostępnić fałsz.

**Zapamiętaj**
AI jest potężnym narzędziem, zarówno dobrym, jak i niebezpiecznym. Możesz się chronić, stosując trzy proste pytania:
Kto to opublikował?
Kiedy to powstało?
Czy inne, wiarygodne źródła o tym mówią?

**To tylko minuta, a może uchronić cię przed manipulacją.**

# Stowarzyszenie Wspierające Inicjatywy Europejskie „IMPET”

## Więcej o nas ...

Stowarzyszenie Wspierające Inicjatywy Europejskie IMPET działa na terenie Sułkowa i okolic, realizując inicjatywy edukacyjne, społeczne i międzypokoleniowe. Współpracujemy z lokalnymi instytucjami, takimi jak OSP, szkoła czy świetlica, aby wzmacniać kompetencje mieszkańców i zwiększać ich odporność na współczesne wyzwania. Prowadzimy działania związane z bezpieczeństwem cyfrowym, obsługą urządzeń mobilnych, mediami społecznościowymi oraz wykorzystaniem narzędzi AI w życiu codziennym. Organizujemy warsztaty, szkolenia oraz punkt cyfrowego wsparcia.

Więcej informacji o naszych działaniach znajduje się na stronie internetowej Stowarzyszenia.

KOMITET DO SPRAW POŻYTKU PUBLICZNEGO

NIW Narodowy Instytut Wolności Centrum Rozwoju Społeczeństwa Obywatelskiego

Rządowy Program Wsparcia Organizacji Pozarządowych Moc Małych Społeczności

SFINANSOWANO ZE ŚRODKÓW NARODOWEGO INSTYTUTU WOLNOŚCI – CENTRUM ROZWOJU SPOŁECZEŃSTWA OBYWATELSKIEGO W RAMACH RZĄDOWEGO PROGRAMU WSPARCIA ORGANIZACJI POZARZĄDOWYCH MOC MAŁYCH SPOŁECZNOŚCI

Nr tel.: (+48) 784 677 614
Mail: biuro.impet@gmail.com