



DEZINFORMACJA I OSZUSTWA W SIECI  
**NIE DAJ SIĘ NABRAĆ!**



KOMITET  
DO SPRAW  
POŻYTKU  
PUBLICZNEGO



Moc Małych  
Społeczności





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

# DZIEŃ DOBRY!



**dobreprogramy**

- Kłaniają się Państwu:
  - Leszek Kędzior
  - Kamil Cybulski
  - Krzysztof Fiedor
- Fundacja e-nergia powstała z pasji do cyfrowych technologii, potrzeby dzielenia się wiedzą oraz chęci wspierania Tych, którzy są przytłoczeni rewolucją cyfrową i nie potrafią się w niej odnaleźć.
- Mamy za sobą ponad 23 lata doświadczenia w edukacji cyfrowej i integracji społecznej. Z informatyką jesteśmy związani od dziecka.
- Już w 2002 r. założyliśmy portal [dobreprogramy.pl](http://dobreprogramy.pl) i propagowaliśmy m.in. zasady bezpieczeństwa w sieci.



# PLAN SPOTKANIA

- 1. Dezinformacja
- 2. Bezpieczeństwo w sieci
- 3. Poradnik
- 4. Pytania
- 5. Podsumowanie





# **CZĘŚĆ 1**

# **DEZINFORMACJA**



12

WYDANIE SPECJALNE

WARSZAWA

OSINY

• NA ŻYWO



REPUBLIKA1KLIK.PL

PILNE

W OSINACH NA LUBELSZCZYZNIE SPADŁ I EKSPLODOWAŁ OBIEKT LOTNICZY

POTRZEBUJEMY 700 000 zł  
NA ORGANIZACJĘ I TRANSMISJĘ  
SZCZYTU TRANSATLANTYCKIEGO

23%



KOSINIAK-KAMYSZ: JEBŁO TO JEBŁO. PO CO DRAŻYĆ TEMAT?

16:33

W POD WNIOSKIEM O REFERENDUM WS. NIELEGALNEJ MIGRACJI PRZEZ CAŁY SIERPIEŃ OD 12-TEJ DO 1



- To był przykład dezinformacji, na którą nabrał się nawet jeden z posłów...
- Film do dziś można obejrzeć w serwisie X (dawny Twitter). Nikt go nie usunął.
- Tylko ten jeden post ma blisko pół miliona (!) wyświetleń





**Dezinformacja to celowe publikowanie fałszywych informacji. Jest szkodliwa i niebezpieczna.**

**Może wywoływać strach, panikę, wrogość do różnych grup społecznych i narodowościowych, osłabiać instytucje publiczne, czy wpływać na wynik wyborów...**





# CELE DEZINFORMACJI

- Wpływ na opinię publiczną:  
manipulacje wyborcze, podważanie zaufania do instytucji.
- Wywoływanie niepokojów społecznych:  
podsycanie agresji, polaryzacja społeczeństwa.
- Korzyści ekonomiczne:  
promowanie fałszywych produktów, oszustwa finansowe.
- Osłabianie przeciwników:  
dyskredytacja, destabilizacja.



# DEZINFORMACJA TO BROŃ NASZYCH CZASÓW...

Rosja wydaje na ten cel nawet 2 mld dolarów, a w niektórych szacunkach mówi się nawet o 4 mld dolarów rocznie (na dezinformację i propagandę). W pierwszym kwartale 2022 r. wydatki na propagandowe media wzrosły trzykrotnie (r/r), co pokazuje, że wysiłki Kremla na rzecz utrzymania swojej narracji, szczególnie w kontekście pełnoskalowej agresji na Ukrainę, stale rosną.

Źródło: Raport częściowy Zespołu ds. Dezinformacji Komisji do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024 (str. 16).



# DLACZEGO WŁAŚNIE TERAZ?

- Dezinformacja nie jest zjawiskiem nowym, jest tak stara jak początki zdolności komunikacyjnych człowieka.
- W XX wieku pojawiły się media masowe, które umożliwiały docieranie z przekazem do dużych grup ludzi, ale ich wykorzystywanie dla potrzeb dezinformacji nie było tak łatwe i skuteczne jak obecnie.
- Mechanizmy rządzące Internetem umożliwiają docieranie z dezinformacją na niespotykaną wcześniej skalę i z niespotykaną wcześniej skutecznością.



PRZYKŁAD Z 1900 R.



KANAŁIZACYA  
MIASTA WARSZAWY

JAKO NARZĘDZIE

JUDAIZMU I SZARLATANERYI

W CELU

ZNISZCZENIA ROLNICTWA POLSKIEGO

ORAZ

WYTEPIENIA LUDNOŚCI SŁOWIAŃSKIEJ NAD WISŁĄ

NAPISAŁ

F. R.

ROLNIK NADWISŁAŃSKI.



KRAKÓW

SKŁAD W KSIĘGARNI G. GEBETHNERA I SPÓŁKI.

1900



# TYPOWE NARZĘDZIA DEZINFORMACJI

- Fałszywe wiadomości (fake news), celowo stworzone, aby wprowadzać w błąd.
- Fałszywe nagrania wideo lub audio (deepfakes), które wyglądają i brzmią realistycznie
- Fałszywe obrazy - wygenerowane w całości przez sztuczną inteligencję lub przerobione autentyczne zdjęcia, w celu wprowadzenia w błąd.
- Komentarze np. w mediach społecznościowych



# PRZYKŁADY DEZINFORMACJI





Zbigniew Jakubowski

August 26 at 12:30 PM · 🎵 Wódko wódeczko - Extended · THR!LL, BOYS · 🌐

Zaczęły pojawiać się informacje o bezrobociu w Polsce przypominę 68% wyborców pis nie pracuje.



MANIPULACJA

## 68% wyborców PiS nie pracuje? To manipulacja

19 września, 2025 Magdalena Grochocka

W sieci krążą wpisy, według których aż 68% wyborców PiS „nie pracuje”. Teza szybko podzieliła internautów – jedni uznali ją za trafną obserwację, inni za manipulowanie danymi. Jak jest naprawdę? Sięgamy do oficjalnych danych.

OSTATNIE WPISY



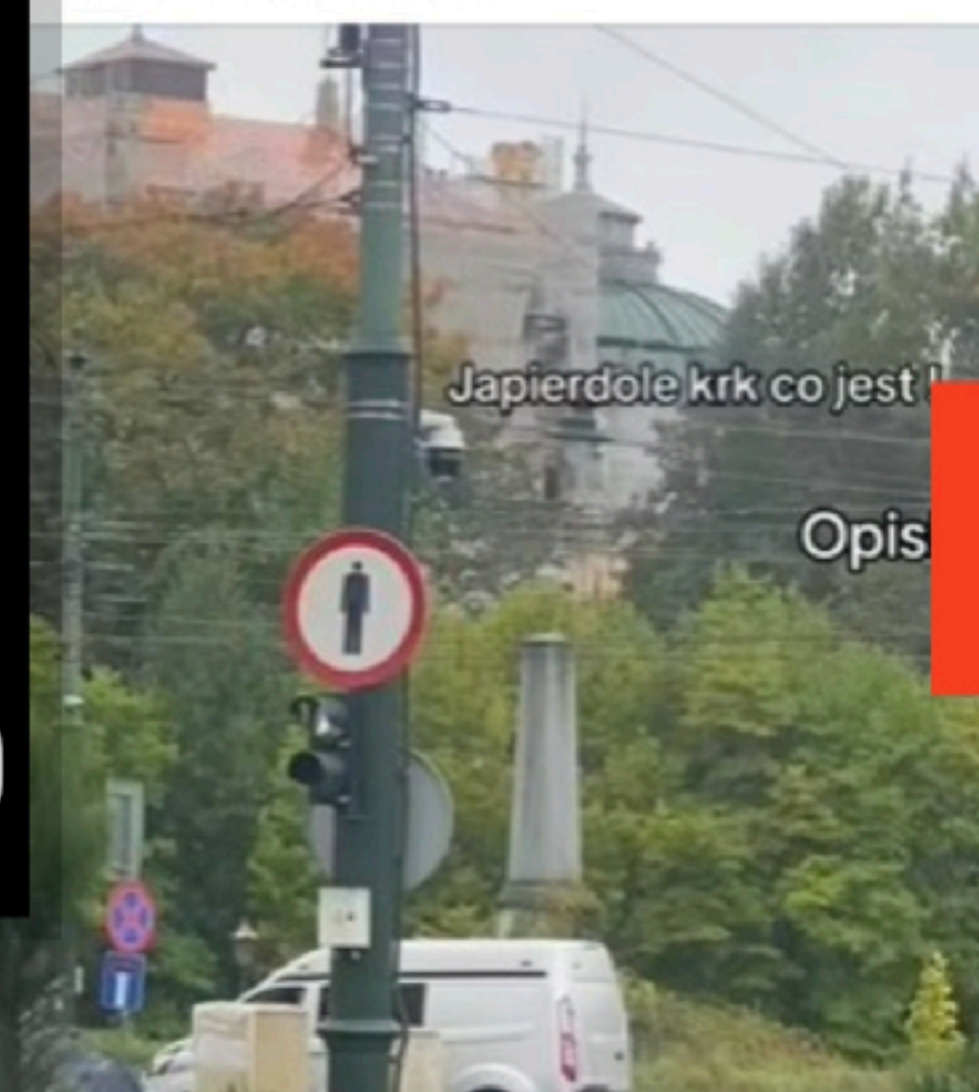


Wojna w Ukrainie

Udostępnij:   

**W Krakowie  
Ukrainiec  
zastrzelił trzy  
młode osoby?**

Jak do nosi prokuratura mężczyzna pochodzi z Ukrainy. Mężczyzna został aresztowany i postawiono mu zarzuty- morderstwo ze szczególnym okrucieństwem, brak wízy i przemoc psychiczna nad osobami trzecimi. Tego typu zarzuty są uznawane za najgorsze i są oznaczane jako



**FAŁSZ**

AFP

**Nie, w Krakowie nie doszło do „potrójnego morderstwa”  
dokonanego przez Ukraińca**



Skopiuj link



Drukuj



Udostępnij



Strona główna > Fake News > Ukraińcy okradają ...

01.10.2024 godz.10:58 • 9 min czytania

Fake News ⓘ

# Ukraińcy okradają powodzian? Tragedia użyta do dezinformacji

UKRAINA

FAKE NEWS

KLIMAT

Czy uzbrojeni Ukraińcy szabrują domy, magazyny i napadają na transporty żywności dla powodzian z Kotliny Kłodzkiej? Z naszej analizy dowiesz się, czy rzeczywiście doszło do takich wydarzeń.



fot. Tiktok / Pexels / Modyfikacje: Demagog



POLECANE DLA CIEBIE

Artykuł

ZDROWIE

Antyszczepionkowy wykład Piotra Witczaka w domu kultury. Instytucja umywa ręce

Artykuł

POLITYKA KRAJOWA

Postowie łamią prawo i zastaniają się immunitetem. A mogą po prostu przyjąć mandat

Podcast

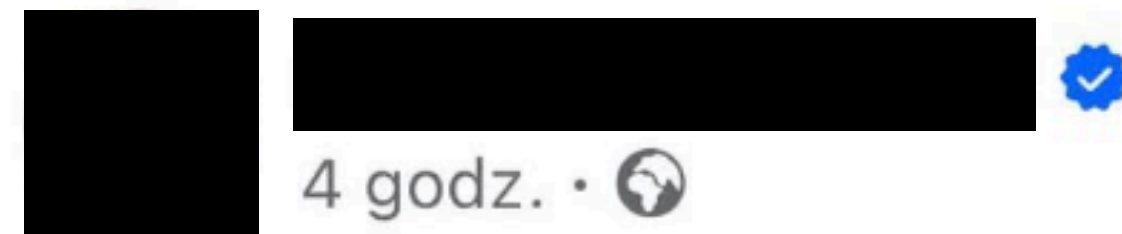


Czy warto korzystać z chatbota do nauki?

Rozmowa z prof. Aleksandrą Przegalińską

25.09.2025





4 godz. • 🌐

Chiny zbudowały działo, które strzela 7 razy szybciej niż dźwięk. A my? My w Unii mamy nakrętki, imigrantów i małżeństwa jednopłciowe. 🙄



DEZINFORMACJA



Skomentuj jako Fundacja e-nergia

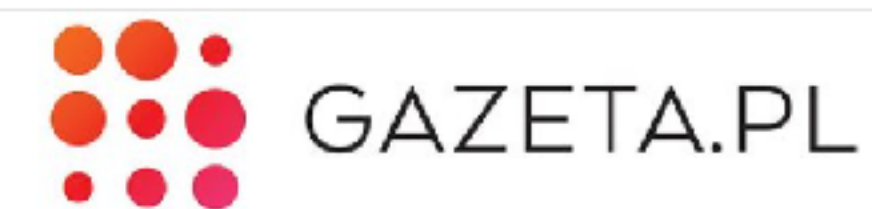






### Bjogo-3

Dlaczego idol tłumów milczał przez 20 lat? Tajemnica, przez którą zatrzymane go godzinę po szokującym wyznaniu



**CAŁY KRAJ JEST W SZOKU PO W CZORAJSZEJ WIADOMOŚCI. JUREK OWSIAK POŻEGNAŁ SIĘ ZE SWOIM DOTYCHCZASOWYM ŻYCIEM.**

AMAZON.PL

## Skandal wstrząsnął Polską: oświadczenie Owsiaaka wysadziło internet, a władze natychmiast wtrąciły go za kratki. „Teraz...

**Dowiedz się więcej**

🤔👍👎 27

11 komentarzy

## Sponsorowane



**Kurs maturalny z Informatyki z 20% rabatem!**  
maturalnesos.pl



 **LIMITED TIME  
OFFER | 60% OFF**  
landing.pcloud.com

## Urodziny

## Kontakty



Meta AI 



<  Życzenia na każdy dzień – 😊 ...  
cudownie. · [Obserwuj](#)  
3 godz. · 🌐

Mój tata nie chciał, żebym publikowała jego prace, ale są piękne i chciałam, żeby wszyscy zobaczyli, że ma talent. ❤️ 😊 😊



 **Boże błogosławieństwo i miłość ·** ...  
[Obserwuj](#)  
30 gru 2024 · 🌐

Nikt się ze mną nie przywita, ponieważ pochodzę ze wsi.





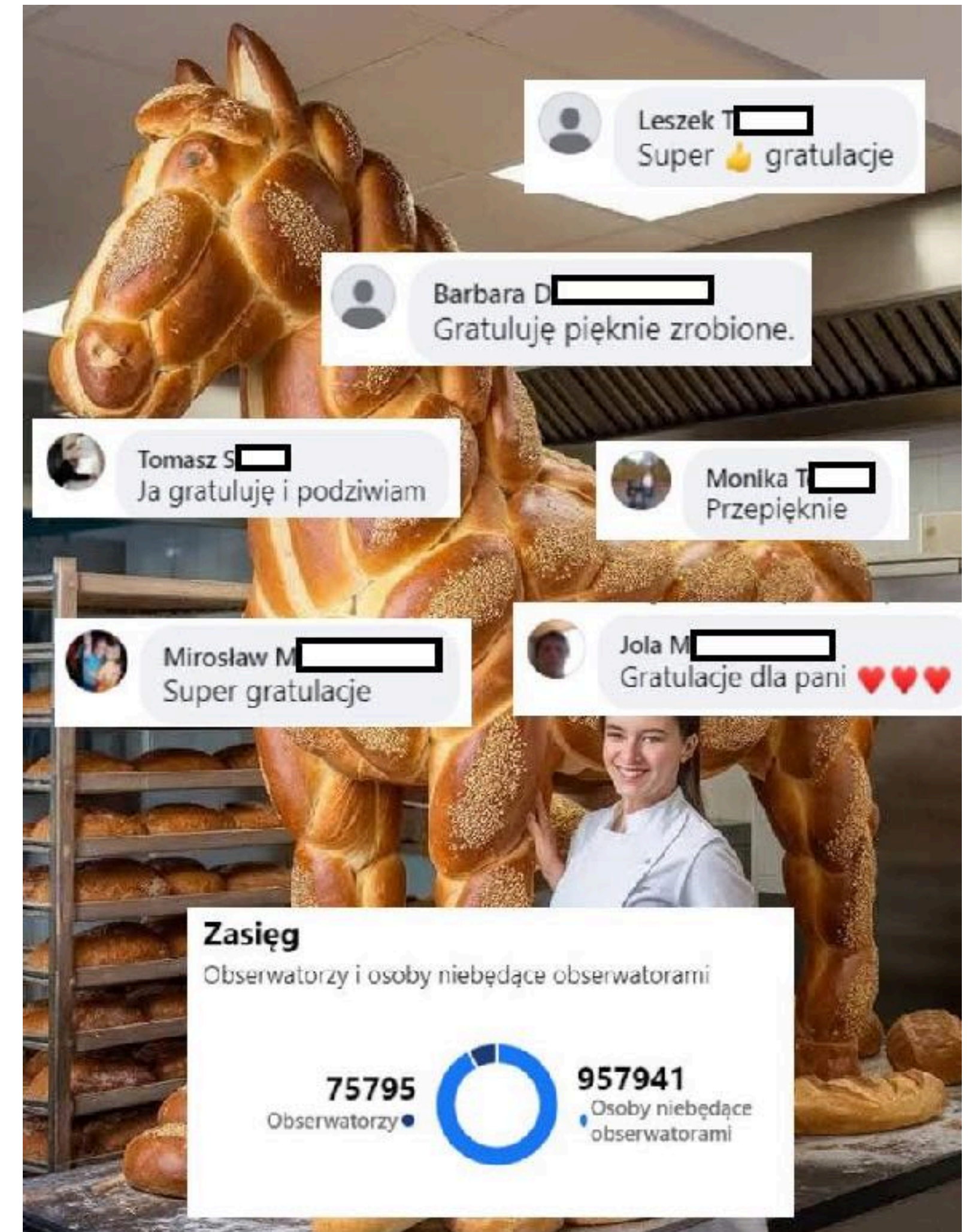


Polska w dużych dawkach

7 stycznia · 🌐



Ta kobieta upiekła chałkonia ale nikt jej nie pogratulował



👍😂❤️ 11 tys.

1448 komentarzy 312 udostępnień



Kacperek ma 13 lat. Słoneczny chłopiec, który walczy o życie... 🙏

Nie wiemy, ile jeszcze ma czasu, ale wiemy jedno — zasługuje na szansę.

Kacperek pilnie potrzebuje pomocy. Każdy dzień ma znaczenie. 💔

📢 Prosimy, udostępnij ten post.

Twoje jedno kliknięcie może dotrzeć do osoby, która zmieni jego los.

Nie przewijaj w ciszy — Twoje serce może uratować jego przyszłość.

🔄 Pomóż nam roznieść wołanie o życie.

Razem możemy więcej. ❤️ 🙏



🗣️ W sieci krąży „poruszająca” historia „Pana Janusza” – starszego rzemieślnika, który po wojennych przejściach tworzy lampki w kształcie psów i mimo hejtu nie przestaje działać.

💡 Cała historia to jednak oszustwo – postać stworzono przy użyciu AI, a sprzedawane lampy są tanim produktem z Chin oferowanym po zawyżonej cenie. Jako pierwsza o sprawie poinformowała [Eko. Paulina Górską](#) ostrzegając na TikToku przed oszustwem i pokazując, jak się przed nim chronić.

⚠️ Aby sprawdzić autentyczność aukcji, skorzystaj z lupy Google – łatwo przekonasz się, czy dany produkt nie jest dostępny taniej gdzie indziej. Zwróć też uwagę na brak danych kontaktowych oraz długi czas dostawy – to kolejne sygnały ostrzegawcze.

🔍 Przeczytaj artykuł: <https://bit.ly/LampkiPanaJanusza>





**JAK NIE DAĆ SIĘ NABRAĆ  
NA DEZINFORMACJĘ?**



# 1. SPRAWDZAJ ŹRÓDŁO

Nie każda informacja w internecie jest prawdziwa!

- Upewnij się, że informacja pochodzi z **oficjalnego źródła** (np. komunikatu policji, urzędu, znanych mediów).
- Zwróć uwagę na adres strony internetowej – fałszywe strony często korzystają z podobnie wyglądających adresów np. **facebo0k.com** zamiast **facebook.com**
- Zwróć uwagę, czy **strona ma dane kontaktowe** i inne informacje.
- **Nie ufaj anonimowym profilom** w mediach społecznościowych, które nie mają historii, zdjęć, ani wiarygodnych treści.





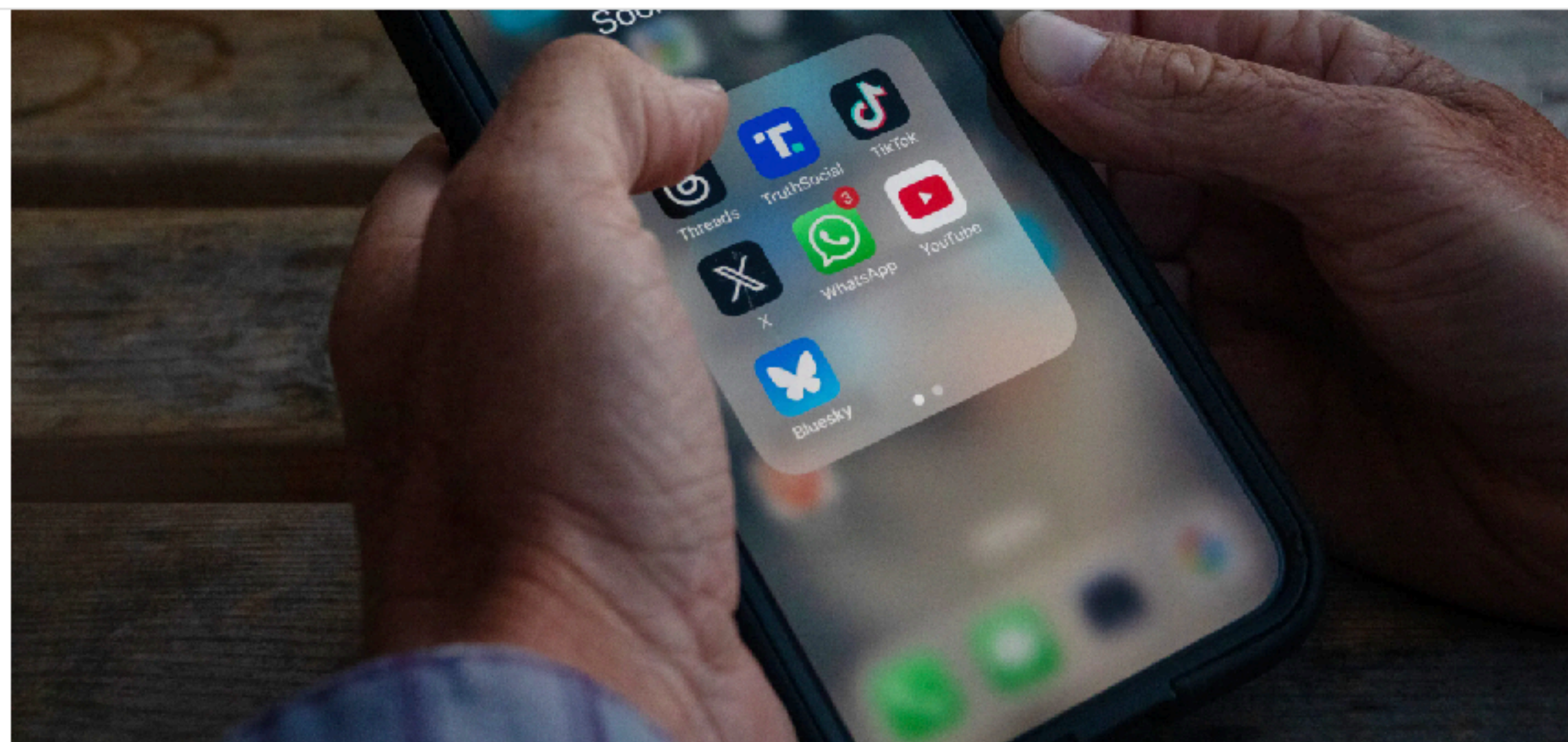
## 2. WERYFIKUJ

Potwierdź informację w innych miejscach.

- Sprawdź **inne źródła informacji** (np. znane portale, strony instytucji państwowych).
- Jeżeli w innych miejscach nie ma takiej informacji, **może być ona fałszywa**.
- Zwróć uwagę, **czy informacja jest aktualna**.
- Nie zamykaj się w tzw. **bańce informacyjnej**.







Social media has become rife with financial scams, and MEPs were determined to hold both Big Tech and banks liable during legislative negotiations. | Matt Cardy/Getty Images

NOVEMBER 27, 2025 2:55 PM CET

BY GIOVANNA FAGGIONATO AND ELIZA GKRTSI

BRUSSELS — Platforms including Meta and TikTok will be held liable for financial fraud for the first time under new rules agreed by EU lawmakers in the early hours of Thursday.

The Parliament and Council agreed on the package of rules after eight hours of negotiations to strengthen safeguards against payment fraud. The deal adds another layer of EU regulatory risk for U.S. tech giants, which have lobbied the White House to confront Brussels' anti-monopoly and content moderation rules.

“This is a big win. A big, big step forward. We are coming from a reality where platforms are not liable under any law,” Morten Løkkegaard, the Danish Renew MEP who shepherded part of the package through Parliament, told POLITICO. “It is a historical moment.”

Advertisement



DYGRESJA



# 3. UWAŻAJ NA EMOCJE

To częsty podstęp dezinformatorów!

- Uważaj na krzykliwe nagłówki i agresywne słowa.
- Mają na celu wywołanie złości, strachu i innych skrajnych emocji.
- Zatrzymaj się i **zastanów**: czy to może być manipulacja?
- Emocje to najprostsza droga, by ktoś **wywołał Twoją reakcję**.





# 4. NIE UFAJ ZDJĘCIOM I FILMOM

Obraz może być zmanipulowany...

- W dobie sztucznej inteligencji (AI) zdjęcia, a nawet filmy (zarówno obraz i głos) można **łatwo zmanipulować**.
- **Przyjrzyj się dokładnie**, czy wszystkie elementy na zdjęciu bądź filmie są realne.
- Zwróć uwagę na nienaturalne cienie, rozmazane dłonie, błędne napisy, dziwne tło i inne szczegóły (np. logo **Sora** oznacza narzędzie do generowania fałszywych filmów).





# 5. NIE DZIAŁAJ POCHOPNIE

Poczekaj zanim zareagujesz!

- **Absolutnie każda reakcja** tj. komentarz, udostępnienie, a nawet emotka (np. polubienie, serduszko, złość) **zwiększa zasięg informacji**, która może być fałszywa.
- Nawet jeśli tylko chcesz „ostrzec innych” – jednocześnie pomagasz w jej rozpowszechnianiu.
- Najpierw sprawdź, potem działaj.





# 6. ZASTANÓW SIĘ

Rozsądek przede wszystkim!

- **Zachowaj rozsądek i bądź krytyczny** wobec informacji, szczególnie tych emocjonalnych.
- Zadaaj sobie pytanie „**kto na tym zyskuje?**”.
- **Dezinformacja ma zwykle konkretny cel** - np. skłócenie społeczeństwa, wywołanie strachu, czy wrogości do różnych grup społecznych i narodowościowych itd.





# 7. SIĘGAJ PO POMOC

Nie musisz samodzielnie weryfikować wszystkiego

- Istnieją organizacje i **specjalne strony weryfikujące informacje**.
- Możesz do nich także **wysłać konkretną informację** w celu weryfikacji.
- Korzystaj z pomocy ekspertów - to nic nie kosztuje, a może **uchronić Cię przed manipulacją**.





# **CZĘŚĆ 2**

# **BEZPIECZEŃSTWO W SIECI**



**NASK**

U W A G A O S Z U S T W O

Przykłady matexrjñü  
**mnnyojtn**

**OdcD S**



- **To były przykłady manipulacji wykorzystujących tzw. deepfake, czyli wygenerowane lub zmanipulowane przez sztuczną inteligencję (AI) materiały wideo, audio i obrazy, które udają prawdziwe osoby, miejsca, zdarzenia.**
- **Oszuści bardzo często podszywają się pod osoby znane, wykorzystując takie sfabrykowane materiały, aby przekonać głównie do różnych „inwestycji”.**
- **Celem są oczywiście pieniądze osób, które dadzą się na to nabrać. „Inwestycje” to fikcja.**



# BEZPIECZEŃSTWO W INTERNECIE

- Internet to potężne narzędzie, ale poza dezinformacją, czyha tu nas wiele zagrożeń
- Codziennie narażeni jesteśmy na próby kradzieży danych, oszustwa i ataki.
- Dbanie o bezpieczeństwo w sieci chroni nas przed stratami finansowymi, utratą danych i naruszeniem prywatności.
- Świadomość i odpowiednie działania to klucz do bezpiecznego korzystania z sieci.



**Wraz z rozwojem cyfryzacji  
stale obserwujemy wzrost  
zagrożeń płynących z sieci.**

**Pojawiają się nowe i coraz  
bardziej przebiegłe metody  
oszustw, a ich ofiarami padają  
najczęściej osoby starsze.**

**CERT nieustannie donosi  
o takich zdarzeniach...**





# 600 000

**W 2024 R. CERT ODNOTOWAŁ REKORDOWY WZROST AKTYWNOŚCI CYBERPRZESTĘPCÓW.  
LICZBA ZGŁOSZEŃ WYNIOSŁA PONAD 600 000 (WZROST O 62% W PORÓWNANIU Z 2023).**



# GLÓWNE KAMPANIE CYBEROSZUSTW W POLSCE W 2024 R.

- **Oszustwo na dziecko przez WhatsApp**  
Podszywanie się pod dziecko, które „zmieniło numer telefonu” i prosiło rodziców lub innych członków rodziny o pilny przelew na nowy telefon.
- **Fałszywe wezwania od Policji**  
Podszywanie się pod organy ścigania z zarzutami przestępstw, grożące postępowaniem sądowym. Przestępcy oferowali polubowne „załatwienie sprawy” za opłatą.
- **Naruszenia praw autorskich**  
Maile sugerujące naruszenie własności intelektualnej, zawierające złośliwe pliki udające dokumenty prawne.
- **Fałszywe mandaty z kodami QR**  
Kartki imitujące wezwania do zapłaty umieszczane fizycznie na samochodach. Kody QR prowadziły do fałszywych stron płatności.

Źródło:

<https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku>



# INNE METODY OSZUSTW

- Phishing to najpopularniejsza metoda oszustw w sieci (i nie tylko w sieci).
- Phishing to próba wyłudzenia poufnych informacji (loginów, haseł, danych karty kredytowej) przez podszywanie się pod zaufane osoby lub instytucje.
- Ataki phishingowe często wykorzystują e-maile, wiadomości SMS lub fałszywe strony internetowe



# INNE METODY OSZUSTW

- Ransomware to cyfrowy szantaż w sieci.
- Ransomware to złośliwe oprogramowanie, które blokuje dostęp do danych i żąda okupu za ich odzyskanie.
- Ataki ransomware mogą dotyczyć zarówno plików osobistych, jak i danych firmowych.



# **PRZYKŁADY OSZUSTW W SIECI**

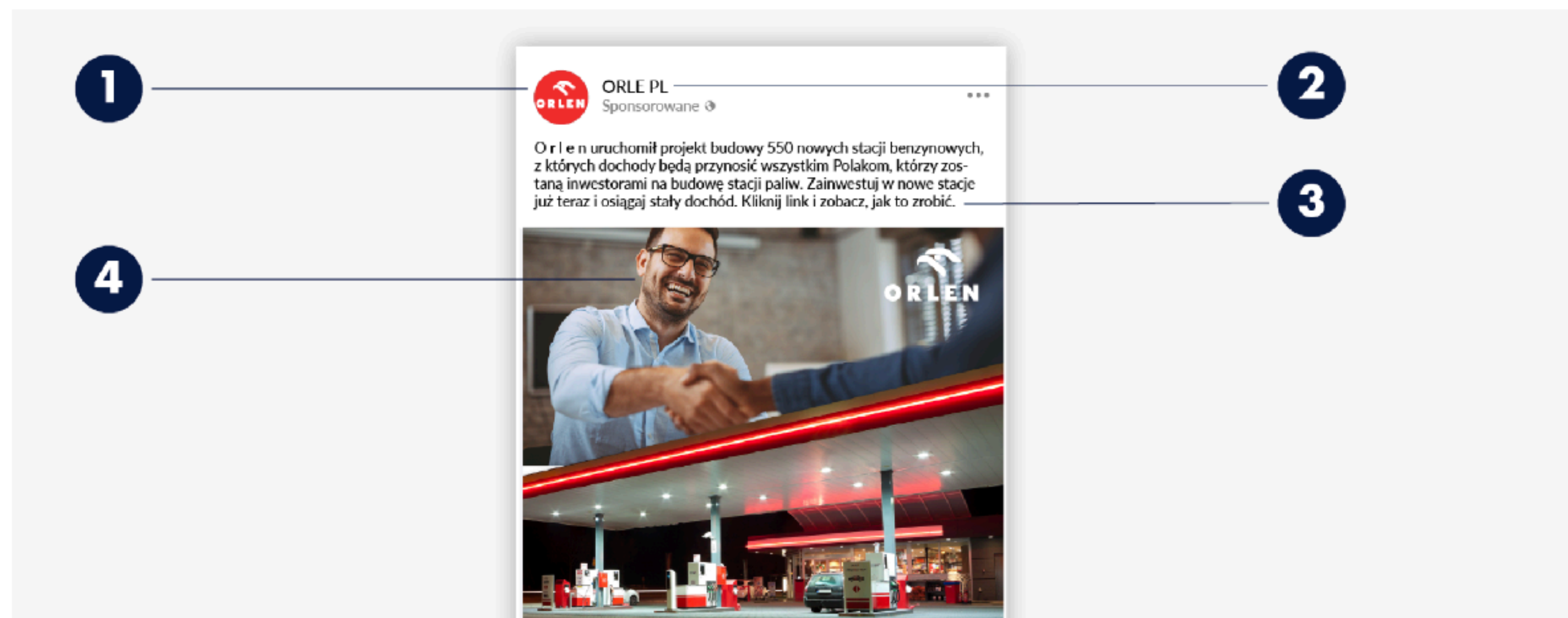


## ORLEN ostrzega przed pojawiającymi się w internecie oszustwami finansowymi podszywającymi się pod koncern.

Fałszywe ogłoszenia gwarantujące rzekome bardzo wysokie i pewne zyski pojawiają się przede wszystkim na portalach Facebook, YouTube, licznych stronach internetowych, w mailingach, esemesach czy reklamach internetowych. Fałszywe ogłoszenia zachęcają najczęściej do inwestowania w akcje spółek Grupy ORLEN oraz projekty inwestycyjne prowadzone przez Grupę. Ogłoszenia te wykorzystują bezprawnie nazwę i znaki firmowe instytucji państwowych, spółek skarbu państwa czy wizerunki powiązanych z nimi osób.

**Przypominamy:** ORLEN zachęca do inwestowania wyłącznie przez swoje oficjalne kanały, takie jak: orlen.pl, orlenwportfelu.pl lub oficjalne profile w mediach społecznościowych. Poniżej przedstawiliśmy, czym charakteryzuje się phishing w internecie, czyli próba podszycia się pod inną firmę w celu wyłudzenia pieniędzy.

### Jak rozpoznać próbę oszustwa





Skopiuj link



Drukuj



Udostępnij



Strona główna > Fake News > Deepfake z Rafate...

09.07.2024 godz.15:09 • 5 min czytania

Fake News ⓘ

# Deepfake z Rafałem Brzoską wykorzystany w oszustwie inwestycyjnym

FAKE NEWS CELEBRYCI OSZUSTWO

Wizerunek przedsiębiorcy po raz kolejny został wykorzystany do scamu.



fot. Facebook / Modyfikacje: Demagog

♥️ POLECANE DLA CIEBIE

Artykuł SZCZEPIONKI

Antyszczepionkowy wykład Piotra Witczaka w domu kultury. Instytucja umywa ręce

Artykuł POLITYKA KRAJOWA

Posłowie łamią prawo i zastaniają się immunitetem. A mogą po prostu przyjąć mandat

Podcast



Czy warto korzystać z chatbota do nauki?

Rozmowa z prof. Aleksandrą Przegalińską

25.09.2025







## Ostateczne przypomnienie Netflix. [DD-148591-D0676]



informacje rozliczeniowe &lt;info@reitcircles.com&gt;

Do

Odpowiedz

Odpowiedz wszystkim

Prześlij dalej



pon. 11.11.2024 11:03

W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją prawidłowo

**Zaktualizuj szczegóły płatności****Drogi kliencie**

Mamy problemy z Twoimi danymi rozliczeniowymi. Spróbujemy ponownie, ale może być konieczna aktualizacja danych rozliczeniowych.

**Kontynuuj**

Masz pytania? Zadzwoń pod numer 0800-768-07.  
Netflix International B.V.

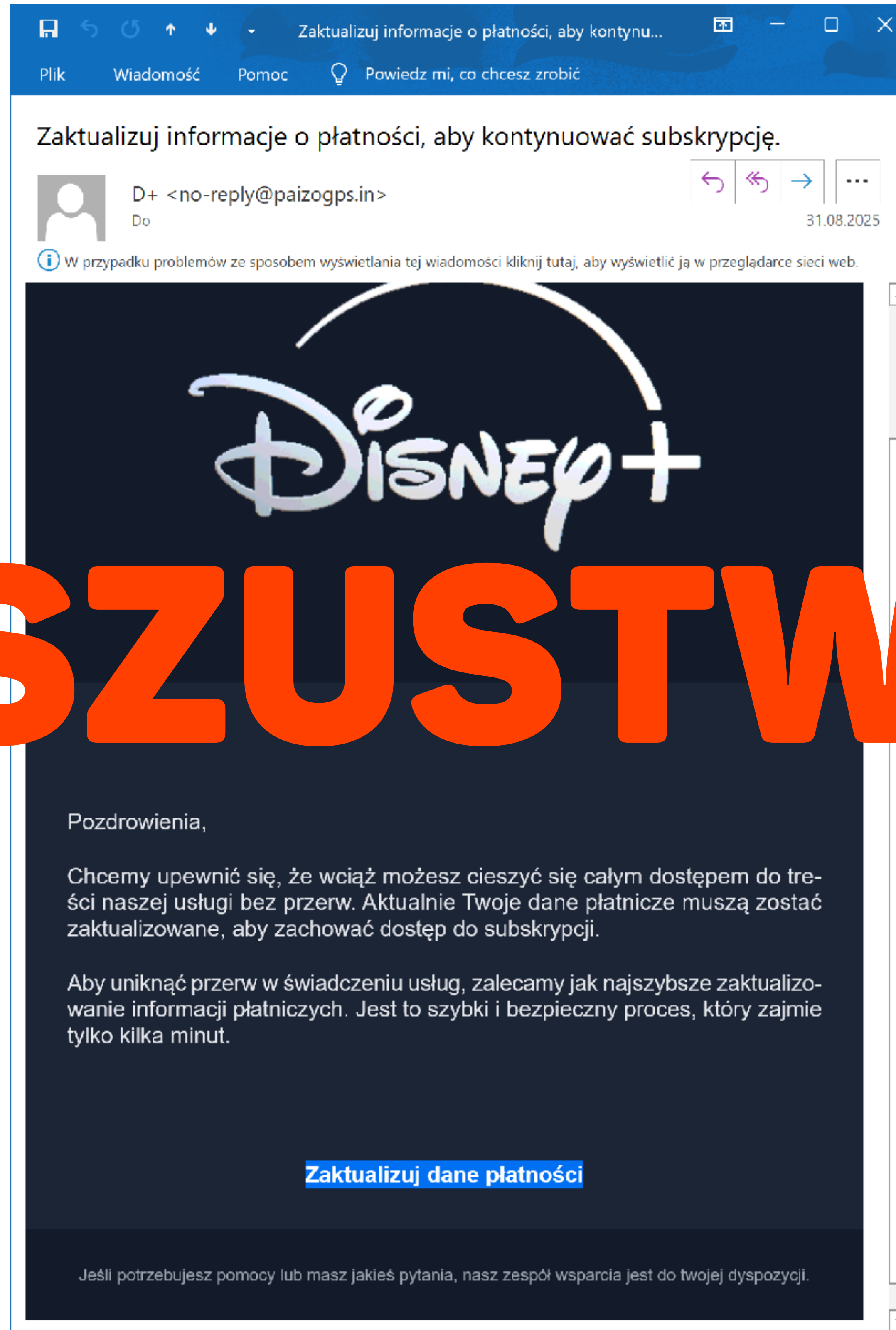
**Ustawienia komunikacji****Warunki użytkowania****Prywatność****Centrum pomocy**

Ta wiadomość jest wysyłana w ramach subskrypcji.  
SRC: 633B530F\_fc6c7b6e-6878-4e22-b19a-  
bf36cce91c11\_fr\_BE\_EVO





# OSZUSTWO







Plik

Wiadomość

Pomoc



Powiedz mi, co chcesz zrobić

845242 - Potwierdzenie operacji - 12/17/2024 2:09:47 PM



pko Bank Polski <pko7@labor-zahntechnik.de>

Do

← Odpowiedz

↶ Odpowiedz wszystkim

→ Prześlij dalej



wt. 17.12.2024 15:10



Ta wiadomość została wysłana z ważnością: Wysoki.

W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją w przeglądarce sieci web.

## PKO Bank Polski

**Dzień dobry,**

Proszę pobrać potwierdzenie transakcji skarbowej, która została zakończona z naszym bankiem.

**PKO\_0019928168615.PDF** (891.24K)

[Pobierz Załącznik](#)

© 2024 PKO Bank Polski S.A.

# OSZUSTWO



re. Pilne: blokada konta bez aktualizacji [G1-344696-D1464]



Netflix <client@osyris.tov.be>  
Do

Odpowiedz

Odpowiedz wszystkim

Prześlij dalej

pon. 11.08.2025 04:00



Twoja subskrypcja została zawieszona

# Ostatnie przypomnienie: kwestia płatności musi zostać rozwiązana dzisiaj

Witam,

Ostatnia chwila, by zaktualizować dane płatności i zapobiec zawieszeniu subskrypcji. Wierzymy, że nadal chcesz korzystać z naszej biblioteki filmów, seriali i gier. Jeśli jednak postanowisz zrezygnować — dziękujemy za wspólny czas i okazane zaufanie.

Aktualizacja

OSZUSTWO



29  
/ 10

## Komunikat z dnia 29.10.2025 roku o naruszeniu ochrony danych osobowych



### Komunikat z dnia 29.10.2025 roku o naruszeniu ochrony danych osobowych.

Zgodnie z art. 34 ust. 3 lit. c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), informujemy o naruszeniu poufności Państwa danych osobowych.

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Charakter naruszenia ochrony danych osobowych | <p>W dniu 22.10.2025 roku w związku z przygotowaniem przetargu na "Odbieranie i zagospodarowanie odpadów komunalnych z nieruchomości zamieszkałych z terenu gminy Wisznia Mała" znak sprawy RI.271.29.2025 na platformie E-PROPUBICO (służącej do publikacji postępowań przetargowych i zamówień publicznych), doszło do publikacji dokumentu w postaci załącznika nr 8 „Wykaz nieruchomości zamieszkujących”, zawierającego dane dotyczące mieszkańców gminy Wisznia Mała. W wyniku zamieszczenia dokumentu ujawniono nadmiarowe dane: imię i nazwisko osoby składającej deklarację, numer PESEL, numer telefonu, data urodzenia, NIP, ilość osób zamieszkujących domostwo, imiona i nazwiska mieszkańców. Plik został wygenerowany z systemu odpadowego EGRO SIGID, w celu przekazania potencjalnemu wykonawcy wykazu nieruchomości, z których będzie on zobowiązany odbierać odpady, podstawiać pojemniki i świadczyć inne usługi opisane w przedmiocie zamówienia do ww. postępowania. Pierwotnie dokument miał zawierać tylko dane w postaci: miejscowość, ulica i numer domu. W dniu 29.10.2025 roku ok. 8.45 natychmiast po otrzymaniu informacji o naruszeniu plik w formacie Excel usunięto z platformy. Naruszenie nie miało charakteru celowego a wynikało z błędu ludzkiego.</p> <p>Konsekwencje dla osób, których dane zostały ujawnione:</p> <p><b>Ryzyko kradzieży tożsamości</b> – udostępnienie imienia, nazwiska, PESEL-u, adresu zamieszkania i numeru telefonu umożliwia podszycie się pod daną osobę np. w celu zaciągnięcia zobowiązań finansowych, rejestracji usług lub wyludzeń.</p> <p><b>Narażenie na oszustwa i phishing</b> – osoby mogą otrzymywać fałszywe wiadomości lub telefony z próbami wyludzenia</p> |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



BIP



DZIENNIK  
USTAW



MONITOR  
POLSKI

### KALENDARIUM IMPREZ

● Październik 2025 ●

| Pn | Wt | Śr | Cz | Pt | So | N  |
|----|----|----|----|----|----|----|
| 29 | 30 | 1  | 2  | 3  | 4  | 5  |
| 6  | 7  | 8  | 9  | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | 31 | 1  | 2  |

Zobacz nadchodzące wydarzenia



**JAK ZADBAĆ O SWOJE  
BEZPIECZEŃSTWO W SIECI?**



# 1. CHROŃ SWOJE DANE

Pamiętaj: bank, policja, urząd nigdy nie prosi o Twoje hasło!

- Nigdy nikomu nie podawaj swoich **haseł**, numeru **PIN**, czy kodu **BLIK**.
- Zastrzeż swój **PESEL**:
  - w aplikacji mObywatel
  - na stronie gov.pl
  - w Urzędzie Gminy
  - w swoim banku.
- Uważaj z podawaniem numeru **dowodu osobistego**, czy numeru **karty bankowej**.





## 2. STOSUJ BEZPIECZNE HASŁA

Traktuj hasła jak klucze do swojego domu!

- Nie ustawiaj haseł, które łatwo odgadnąć np. 123456, data urodzin, imię dziecka.
- Kluczowe są: **konto e-mail, portale społecznościowe oraz bankowość elektroniczna.**
- Nie stosuj tego samego hasła w różnych miejscach.
- Korzystaj z tzw. **dwuetapowego uwierzytelniania (2FA)**:
  - Hasło + SMS
  - Hasło + aplikacja (np. Google Authenticator).





# 3. NIE KLIKAJ W OTRZYMANE LINKI

Oszuści często wysyłają wiadomości z fałszywymi linkami

- Nie otwieraj linków w wiadomościach SMS z nieznanymi numerów, czy w wiadomościach od nieznanymi osób.
- Jeśli wiadomość budzi emocje (np. „Twoje konto zostanie zablokowane!”) – to typowa próba oszustwa.
- Zawsze loguj się (np. do banku, sklepu) przez oficjalną stronę lub aplikację - nigdy z linku.
- Uważnie wpisuj adres strony, uważaj na literówki (np. „allegro0.pl” zamiast „allegro.pl”).
- Oszuści podrabiają wygląd prawdziwych stron.





# 4. ZACHOWAJ OSTROŻNOŚĆ

Oszuści podszywają się pod bank, policję, znajomych...

- Jeżeli ktoś kontaktuje się, podając za np. pracownika banku, urzędu, policjanta i prosi o Twoje hasła lub kody - **nie rób tego!**
- Natychmiast **przerwij rozmowę**, samodzielnie skontaktuj się z tą instytucją na numer z oficjalnej strony i powiadom ją o tym.
- Uważaj na próby podszywania się pod osoby z rodziny (tzw. **oszustwo na wnuczka**) lub kogoś rzekomo działającego w ich imieniu (np. przyjaciel, prawnik itd.)
- Uważaj na tzw. **ransomware** (np. załączniki w mailach).
- Regularnie **aktualizuj oprogramowanie** na komputerze i smartfonie oraz wykonuj **kopie bezpieczeństwa** (backupy).





# 5. „CO NAGLE TO PO DIABLE”

Oszuści wywierają presję żeby działać bez zastanowienia.

- Jeśli ktoś kontaktuje się i przekonuje, że „musisz natychmiast coś zrobić” (np. przesłać pieniądze BLIKiem) **to zapewne oszustwo!**
- **Nie wierz w wiadomości** o „awarii konta”, „problemie z przesyłką” czy „blokadzie konta na Facebooku”.
- Nie działaj pochopnie! **Grozi to kradzieżą tożsamości i pieniędzy.**





# 6. UWAŻAJ NA OKAZJE

W pogoni za okazyjnym zakupem łatwo stracić pieniądze...

- Zanim coś kupisz w sieci, sprawdź sklep – **zobacz opinie** w zewnętrznym miejscu (np. Ceneo, Opineo), zwróć uwagę na adres, numer kontaktowy, **regulamin**.
- Zbyt atrakcyjna cena (znacznie poniżej rynkowej) może oznaczać fałszywy sklep i **próbę wyłudzenia**.
- Nie płać przelewem z góry. Bezpieczniejsza jest karta płatnicza, która daje **możliwość odzyskania pieniędzy** w ramach procedury *Chargeback*.
- W przypadku zakupu od osób fizycznych kupuj z odbiorem osobistym, a wysyłkowo korzystając z płatności za pośrednictwem platform sprzedażowych (np. Allegro Lokalnie, OLX), które oferują **ochronę kupujących**.





# 7. ZGŁASZAJ PODEJRZANE SYTUACJE

Twoja reakcja może pomóc nie tylko Tobie, ale i innym.

- W przypadku podejrzenia oszustwa **skontaktuj się** z instytucją, pod którą ktoś próbuje się podszywać (np. bankiem) lub z policją.
- **Zawiadom CERT** (cert.pl), który działa w ramach krajowego systemu cyberbezpieczeństwa.
- Podejrzone wiadomości SMS możesz bezpośrednio przekazać na **bezpłatny nr 8080**.
- Numery i adresy znajdziesz w naszym **poradniku**.





**CZĘŚĆ 3**

**NASZ PORADNIK I GDZIE SZUKAĆ POMOCY**



## DOWIEDZ SIĘ WIĘCEJ

CERT Polska: [cert.pl](http://cert.pl)  
Bezpieczne Dane: [bezpiecznedane.gov.pl](http://bezpiecznedane.gov.pl)  
Aplikacja Cyberalerty



## WERYFIKACJA INFORMACJI

PAP: [pap.pl/fact-checking](http://pap.pl/fact-checking)  
AFP: [sprawdzam.afp.com](http://sprawdzam.afp.com)  
Stowarzyszenie Demagog: [demagog.org.pl](http://demagog.org.pl)  
Stowarzyszenie Pravda: [pravda.org.pl](http://pravda.org.pl)  
Fundacja Przeciwdziałamy Dezinformacji: [fakenews.pl](http://fakenews.pl)



## ZGŁASZANIE OSZUSTW W SIECI

CERT Polska: [incydent.cert.pl](http://incydent.cert.pl)  
Aplikacja mObywatel  
Policja (Centralne Biuro Zwalczania Cyberprzestępczości):  
tel. 47 72 136 99, [kontakt.bzc@cbzc.policja.gov.pl](mailto:kontakt.bzc@cbzc.policja.gov.pl)



[www.e-nergia.org](http://www.e-nergia.org)

DEZINFORMACJA I OSZUSTWA W SIECI  
**NIE DAJ SIĘ NABRAĆ!**

Wydawcą poradnika jest Fundacja e-nergia ul. Trzebnicka 10D 55-095 Domaszczyn KRS 0000882948



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

# PRAKTYCZNY PORADNIK

FUNDACJI E-NERGIA



# NIE DAJ SIĘ NABRAĆ NA DEZINFORMACJĘ



**Deinformacja** to celowe publikowanie fałszywych informacji. Jest szkodliwa i niebezpieczna. Może wywoływać strach, panikę, wrogość do grup społecznych i narodowościowych, osłabiać instytucje publiczne, czy wpływać na wynik wyborów...

## 1. SPRAWDZAJ ŹRÓDŁO

Upewnij się, że informacja pochodzi z **wiarygodnego źródła** np. komunikatu policji. Uważaj na fałszywe adresy (np. facebook.com).

## 2. WERYFIKUJ

Sprawdź **inne źródła informacji** (znane portale, strony instytucji państwowych). Sprawdź czy ktoś jeszcze o tym pisze. Jeżeli w innych miejscach **nie ma takiej informacji, może być ona fałszywa**.

## 3. UWAŻAJ NA EMOCJE

Krzykliwe nagłówki mające na celu wywołanie złości, strachu i innych skrajnych emocji. To częsty **podstęp dezinformatorów**.

## 4. NIE UFAJ ZDJĘCIOM I FILMOM

W dobie sztucznej inteligencji (AI) **zdjęcia, a nawet filmy** (obraz i głos) można **łatwo zmanipulować**. Przyjrzyj się dokładnie czy elementy na zdjęciu lub filmie są realne. Zwracaj uwagę na **szczegóły**.

## 5. NIE DZIAŁAJ POCHOPNIE

Udostępnienia, komentarze i reakcje (np. emotką pod wpisem na Facebooku) **zwiększają zasięg informacji, która może być fałszywa**.

## 6. ZASTANÓW SIĘ

Zachowaj rozsądek i bądź krytyczny wobec informacji, szczególnie tych emocjonalnych. Zadaj sobie pytanie „**kto na tym zyskuje?**”. Deinformacja ma zwykle konkretny cel - np. skłócenie społeczeństwa.

## 7. SIĘGAJ PO POMOC

Istnieją specjalne **strony weryfikujące informacje**. Możesz do nich także wystać konkretną informację w celu weryfikacji. Adresy znajdziesz na ostatniej stronie tego poradnika.

# DBAJ O SWOJE BEZPIECZEŃSTWO



## 1. CHROŃ SWOJE DANE

Nigdy nikomu nie podawaj swoich **hasel**, numeru **PIN**, czy kodu **BLIK**. Zastrzeż swój **PESEL** w aplikacji **mObywatel**. Uważaj z podawaniem numeru **dowodu osobistego**, czy numeru **karty bankowej**.

## 2. STOSUJ BEZPIECZNE HASŁA

Nie ustawiaj hasel, które łatwo odgadnąć. Kluczowe są: **e-mail**, **portale społecznościowe** oraz **bankowość elektroniczna**. Korzystaj z **dwuetapowego uwierzytelniania** np. hasło + SMS / aplikacja.

## 3. NIE KLIKAJ W OTRZYMANE LINKI

Zawsze loguj się (np. do banku) przez **oficjalną stronę** lub **aplikację**. Uważnie wpisuj adres strony, **uważaj na literówki** (np. „allegro.pl” zamiast „allegro.pl”). Oszuści podrabiają wygląd prawdziwych stron.

## 4. ZACHOWAJ OSTROŻNOŚĆ

Jeżeli ktoś kontaktuje się, podając za np. pracownika banku, urzędu, czy policjanta i **prosi o Twoje hasła lub kody** - nie rób tego! **Natychmiast przerwij rozmowę**, skontaktuj się z tą instytucją i powiadom ją o tym.

## 5. „CO NAGLE TO PO DIABLE”

Jeśli ktoś kontaktuje się i przekonuje, że „**musisz natychmiast coś zrobić**” (np. przestać pieniądze BLIKiem albo zweryfikować swoje konto na Facebooku) **to zapewne oszustwo!** Nie działaj pochopnie!

## 6. UWAŻAJ NA OKAZJE

Zanim coś kupisz, sprawdź sklep – zobacz opinie, adres i numer kontaktowy. **Zbyt atrakcyjna cena** (znacznie poniżej rynkowej) może oznaczać fałszywy sklep i **próbę wyłudzenia**.

## 7. ZGŁASZAJ PODEJRZANE SYTUACJE

Zgłaszaj podejrzone sytuacje. Skontaktuj się ze swoim bankiem, policją, lub zgłoś do CERT. Numery i adresy znajdziesz **na kolejnej stronie**.



\* \* \* \*



Wraz z rozwojem cyfryzacji stale obserwujemy **wzrost zagrożeń płynących z sieci**. Pojawiają się nowe i przebiegłe metody oszustw, a ich ofiarami padają najczęściej osoby starsze.







# Uważaj na fałszywe inwestycje w sieci

[Sprawdź](#)

Uważaj na fałszywe załączniki w mailach



Uważaj na fałszywe prośby o szybki przelew



Uważaj na fałszywe sklepy online

[>Aktualności](#)[> 15 października 2025](#) | [CERT Polska](#) | [#raport miesieczny](#) | [#csirt nask](#) | [#raport](#) |

## Dawka informacji o cyberzagrożeniach – premiera raportów miesięcznych CERT Polska

WRZESIEŃ 2025

Podsumowanie  
Miesiąca  
CERT POLSKA

Opublikowaliśmy właśnie pierwszy raport miesięczny, podsumowujący nasze działania i obserwacje za wrzesień 2025. To początek nowej formuły komunikacji – chcemy regularnie informować o najważniejszych incydentach, trendach i aktywnościach zespołu.

[Czytaj więcej](#)



## Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

 **Osoba fizyczna / inne podmioty**

 **Operator usług kluczowych**

 **Dostawca usługi cyfrowej**

 **Podmiot publiczny**

## Prosimy o wybranie odpowiedniej kategorii:

 **Złośliwa domena**

Domeny wyludzające dane osobowe lub środki finansowe

 **Podejrzana wiadomość SMS**

Treść wiadomości SMS

 **Podejrzana wiadomość e-mail**

Podejrzane załączniki, phishing, szantaż

**\$ Oszustwo**

Fałszywe sklepy internetowe i inne próby podszywania się

 **Ransomware**

Zaszyfrowane pliki z żądaniem okupu

 **Złośliwe oprogramowanie**

Próbki wirusów lub inne szkodliwe programy

 **Podejrzany telefon**

Namawianie do zainwestowania pieniędzy, zaciągnięty kredyt...

 **Atak DDoS**

Informacje dotyczące ataków DDoS

 **Podatności**

Błędy w oprogramowaniu lub aplikacjach internetowych

 **Nielegalne treści**

Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl

 **Dezinformacja**

Zgłoszenie treści o charakterze dezinformacyjnym

**Inne**

Wszystkie inne incydenty niepasujące do poprzednich kategorii



# **CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI**

**TEL. 47 72 136 99**

**KONTAKT.CBZC@CBZC.POLICJA.GOV.PL**





bezpiecznedane.gov.pl

Ostatnia aktualizacja danych: 19.09.2025 r.

Zaloguj się

# Sprawdź, czy Twoje dane są bezpieczne

Zaloguj się i sprawdź, czy Twoje dane nie zostały udostępnione w sieci!  
Korzystanie z naszej wyszukiwarki jest darmowe.

Sprawdź dane



## Przede wszystkim – bezpieczeństwo

Ministerstwo Cyfryzacji zainicjowało stworzenie tej strony, ponieważ w cyberprzestrzeni dochodzi do wycieków danych. Każdego dnia specjaliści z Naukowej i Akademickiej Sieci Komputerowej (NASK) pracują nad rozwiązaniami, które pomagają Ci kontrolować bezpieczeństwo Twoich danych.





# Usługi

Szukaj

[Dodaj ulubione](#)

## Ochrona danych



Bezpiecznie w sieci



Sprawdź dowód



Zastrzeż PESEL



Sprawdź PESEL



## Zdrowie



Recepty



Dokumenty



Usługi



Kod QR



Więcej

[< Usługi](#)

Bezpiecznie w sieci



## Zgłoś incydent w sieci

Dostajesz niepokojące wiadomości lub widzisz podejrzaną stronę? Zgłoś to!



Zgłoś incydent

Oszustwa, cyberataki lub nielegalne treści.



Baza wiedzy

Dowiedz się, jak chronić swoje dane i unikać zagrożeń w sieci.



Chcesz być na bieżąco z aktualnymi ostrzeżeniami o nadużyciach w sieci?

[Włącz powiadomienia](#)



Dokumenty



Usługi



Kod QR



Więcej



## Aktywne Alerty

Najnowsze powiadomienia o atakach

7 października 2025

Nowe

**Uwaga na e-maile od "GOV.PL"**



## Historia Alertów

Poprzednie powiadomienia o atakach

13 września 2025

Nowe

**Ogólnopolski problem z  
płatnościami kartą. Awaria te...**



4 lipca 2025

Nowe

**Uwaga na wiadomości od  
oszustów podszywających si...**



16 czerwca 2025

Nowe

**Nie lataj dronem na północy  
Polski!**



4 marca 2025

Nowe



Alerty



Wiadomości



Wiedza

7 października 2025

## ! Uwaga na e-maile od "GOV.PL"

Udostępnij

Otwórz w przeglądarce

Otrzymujemy masowe zgłoszenia o wiadomościach e-mail, w których oszuści podszywają się pod rządowy portal gov.pl. Oto jak wygląda fałszywa wiadomość:



Po czym możesz poznać, że to oszustwo?

Wiadomości **×** nie są wysyłane z adresu e-mail w domenie gov.pl. Nadawcą są różne e-maile, które tylko w opisie zawierają frazę "GOV.PL", np. "Gov.pl"

Na czym polega ten atak?









Zamknij ✕



Zaloguj się

Niższe  
cenę prądu  
w określonych  
godzinach dnia  
i w weekendy<sup>1</sup>

Niższe  
ceny prądu  
w określonych  
godzinach dnia  
i w weekendy<sup>1</sup>

Przełącz się na Nową Energię



# **CZĘŚĆ 4**

## **CZAS NA PYTANIA**



# **CZĘŚĆ 5**

## **PODSUMOWANIE**





F U N D A C J A  
**E-NERGIA**

Dziękujemy za uwagę!