Socjotechnika w praktyce

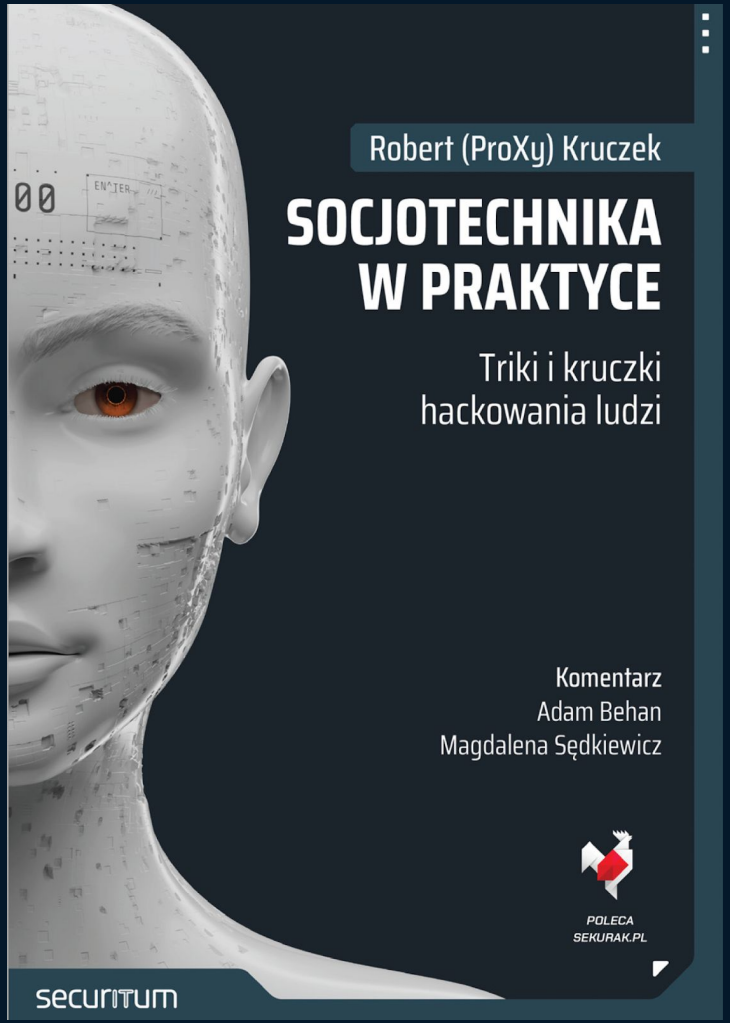
Jak nas atakują i jak możemy się bronić?

O mnie

- Psycholog, Cyberpsycholog
- Programistka + AppSec
- NTHW - “Herbatka ze smokiem”

- Fanka F1 i szydełkowania

https://www.linkedin.com/in/lenasedkiewicz/
https://lenasedkiewicz.com/


Robert (ProXy) Kruczek
SOCJOTECHNIKA W PRAKTYCE
Triki i kruczki hackowania ludzi
Komentarz
Adam Behan
Magdalena Sędkiewicz
POLECA SEKURAK.PL
securitum

Disclaimer

Prezentacja wyłącznie do celów edukacyjnych!

I do refleksji, czy jesteśmy gotowi na taki atak?

Geneza kłamstwa

kłamstwo

=

półprawda pozwalająca przetrwać

kłamstwo

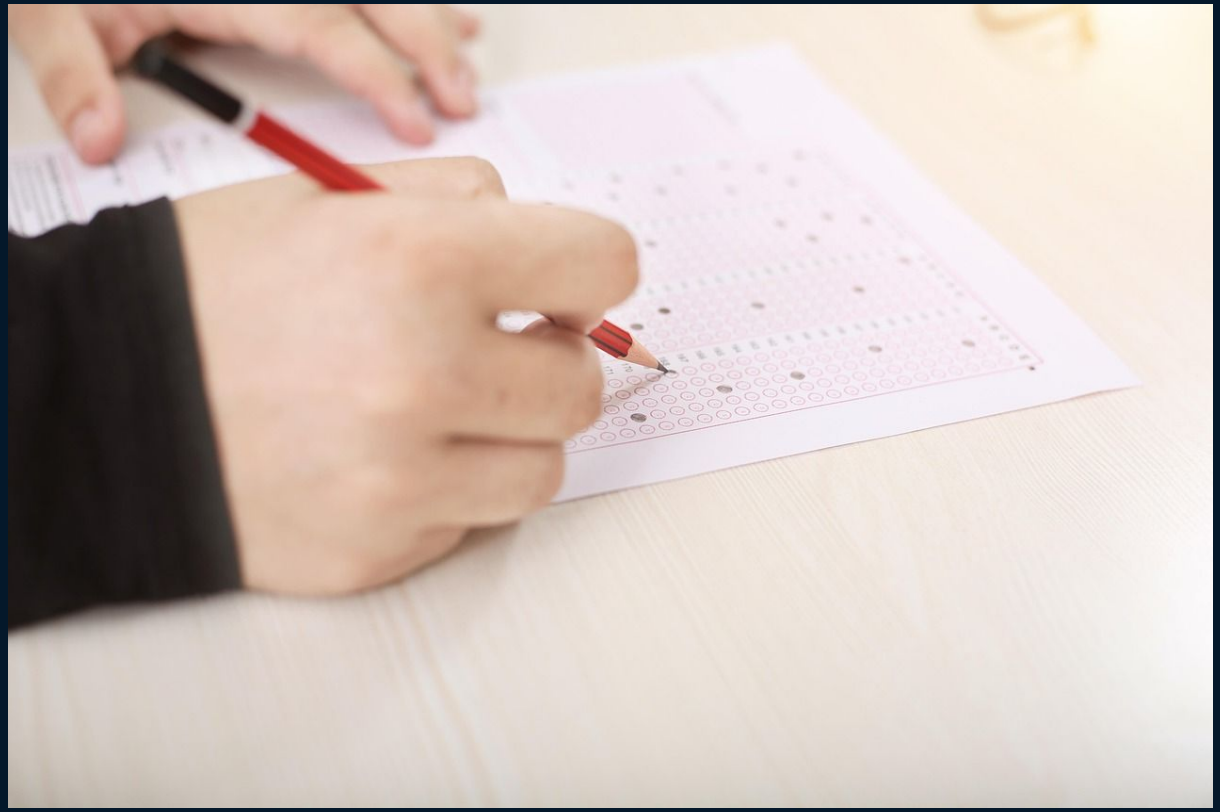
=

białe kłamstwo (dla dobra np. relacji)

kłamstwo
=
samooszukiwanie się
(ewolucja)

“Od jednego nie przytyję”

“Tak, pyszne, wezmę dokładkę”



“Tak tak, nauczył_m się!”

“Wyglądasz wspaniale w tej sukience”

“Zaraz”

Efekt?
Przyzwyczajamy się...

Promocja!

... albo przekraczamy kolejne granice.

A świat na to...


ONLINE
MARKETING
S.E.O
Content
Lists
Links
Titles
Blogs
Sales

Marketing...


ONLINE
MARKETING
S.E.O
Content
Lists
Links
Titles
Blogs
Sales

Marketing...

Oszustwa finansowe...

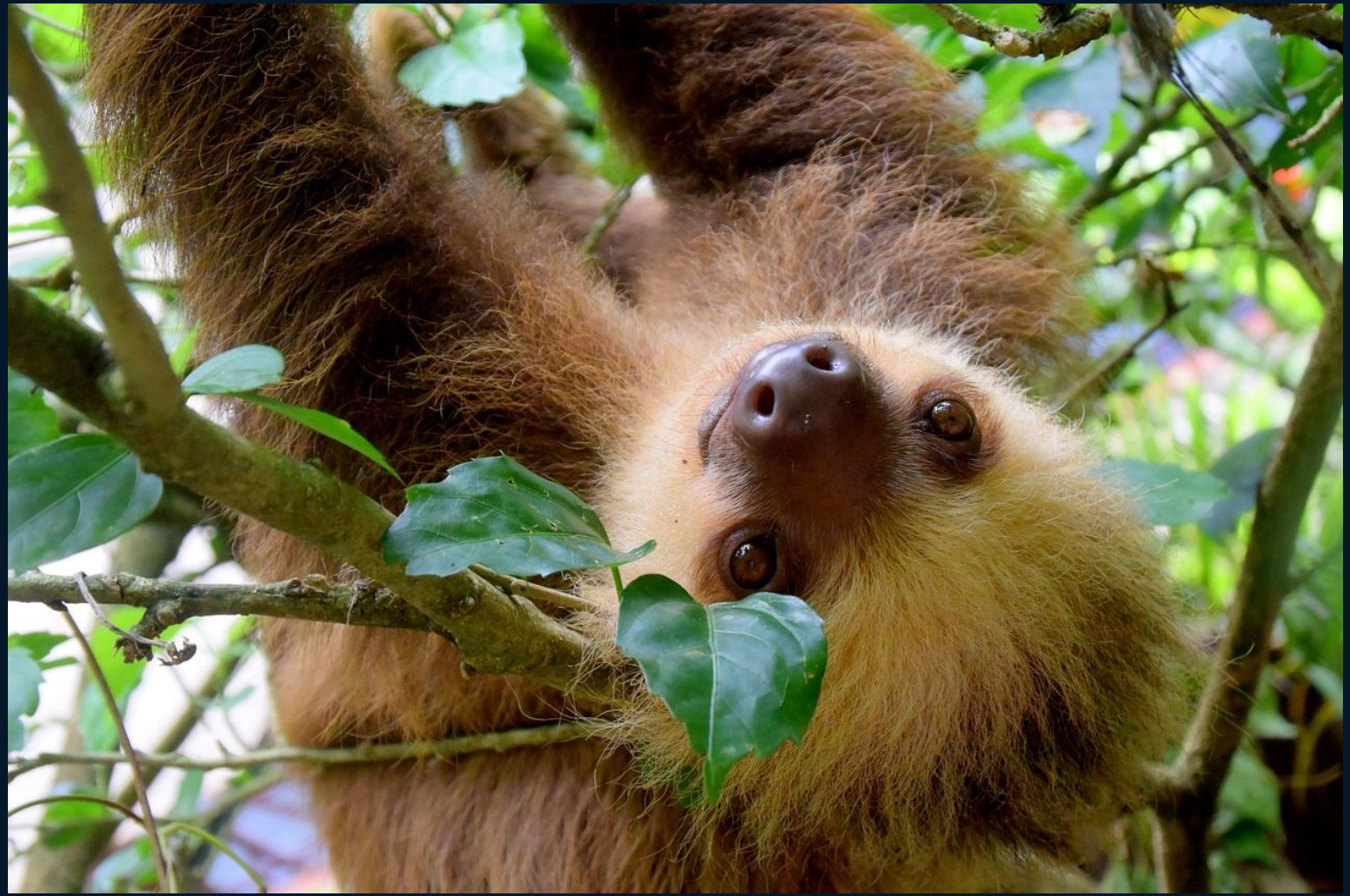
Polityka...

Ludzie nie powinni wiedzieć, jak się robi kiełbasę i politykę.

Bismark

Polityka...

Socjotechnika



Socjotechnika

...to czynność wywierania wpływu na ludzi poprzez praktyczne zastosowanie podstępu wykorzystującego uniwersalne mechanizmy reakcji psychologicznych.

Celem takiego działania jest nieautoryzowane pozyskanie poufnych lub niedostępnych w inny sposób informacji. [za: Urząd komisji nadzoru finansowego]

https://cebrf.knf.gov.pl/component/content/article/socjotechnika?catid=26&Itemid=101, dostęp: 30.11.2025

Socjotechnika

… jak, wykorzystując naturalne podatności Twojej głowy, namówić Cię do zrobienia czegoś, w wyniku czego stracisz coś dla Ciebie ważnego (dane, pieniądze, etc.), często nawet tego nie zauważając…

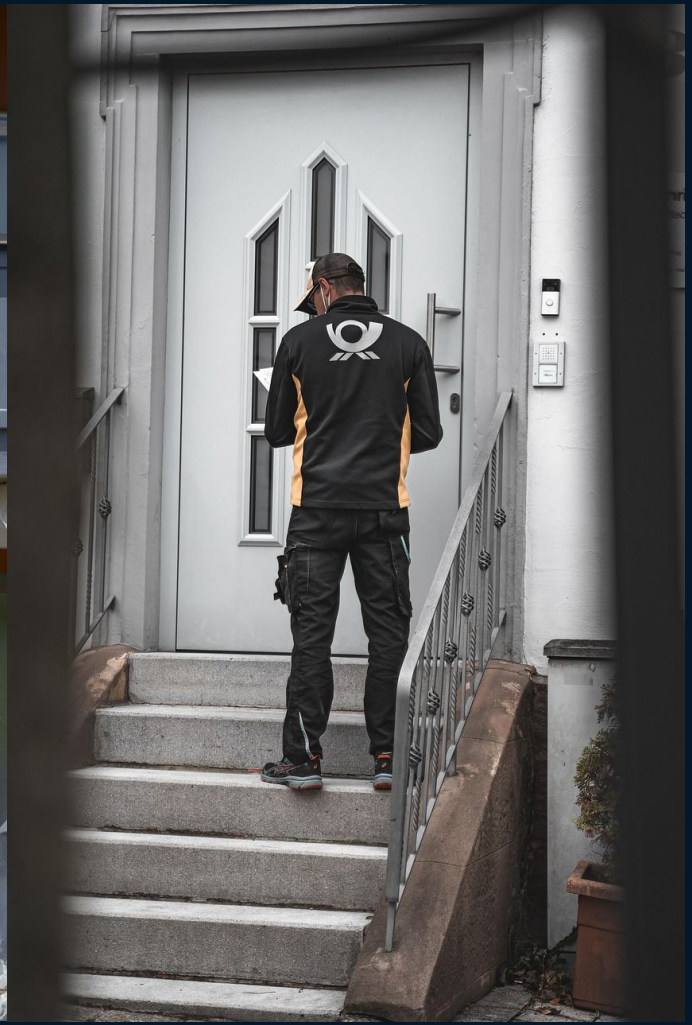
Co może zostać wykorzystane?

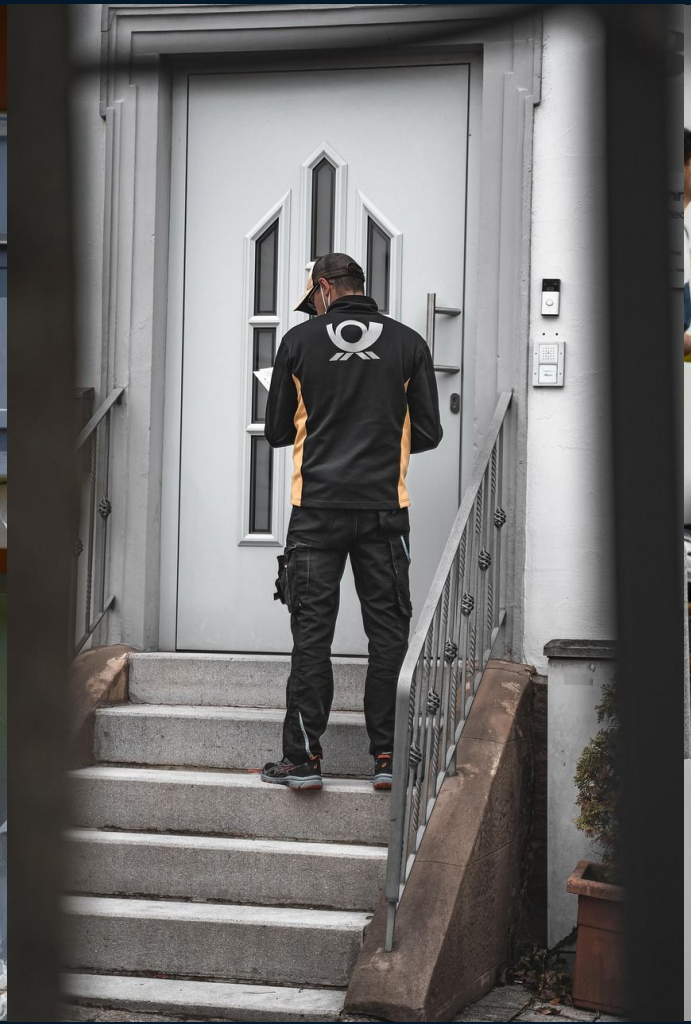
reakcja walka - ucieczka - zamrożenie

konieczność działania pod presją (np. czasu)

wpływ czyjegoś autorytetu na decyzje

Ignorowanie “szumu” w tle (cel: wtopienie się w tłum)



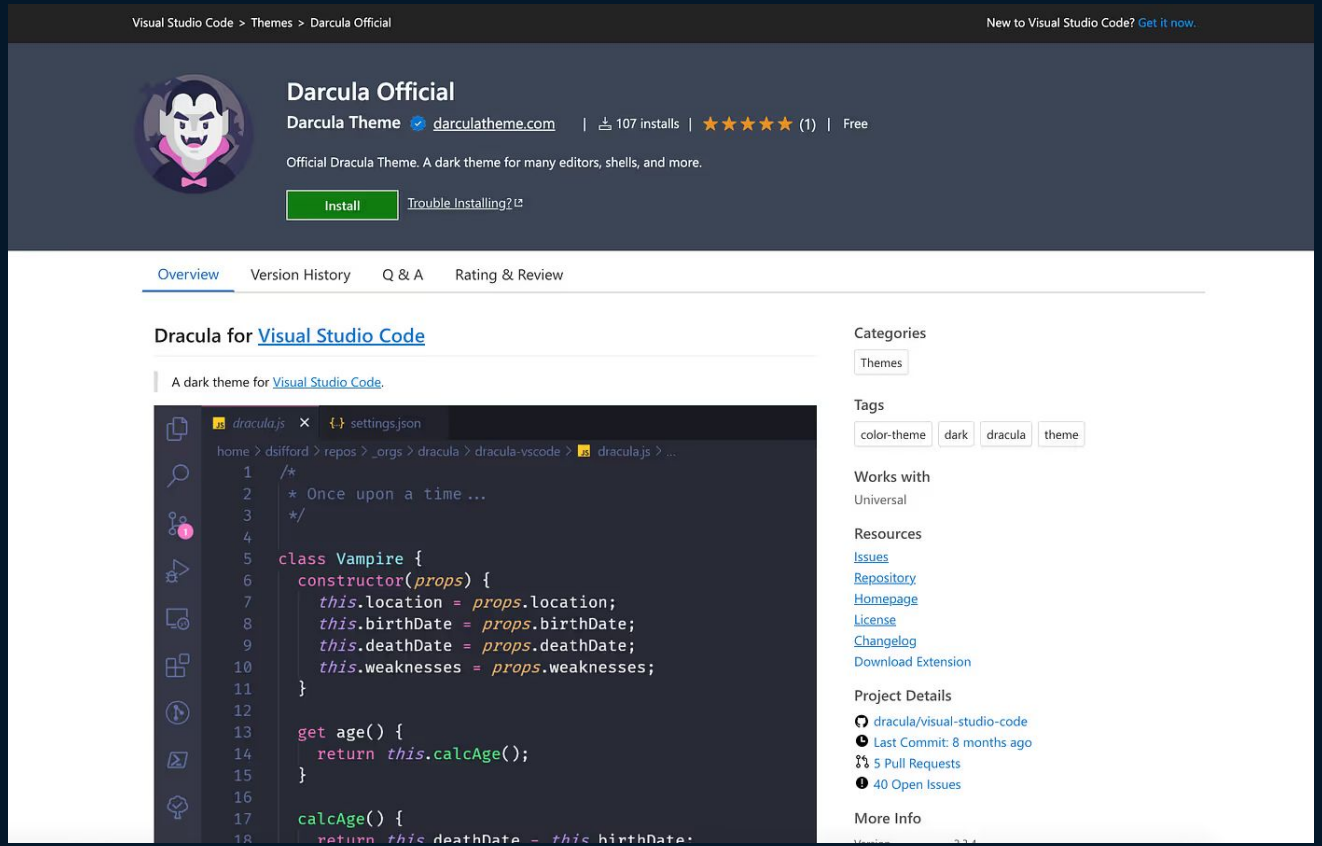


Empatia i chęć pomocy

“automatyzmy”

Na pograniczu socjotechniki

Typosquatting

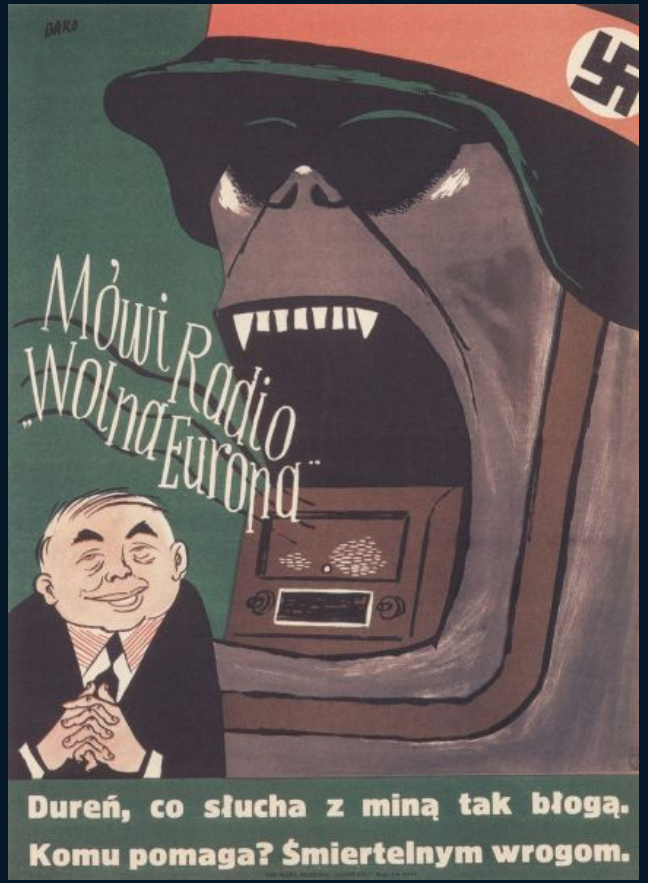


Źródło: https://www.koi.ai/blog/1-6-how-we-hacked-multi-billion-dollar-companies-in-30-minutes-using-a-fake-vscode-extension, dostęp: 30.11.2025
dodatkowe źródło: https://sekurak.pl/badacze-potwierdzaja-sciezke-ataku-na-developerow-za-pomoca-instalacji-falszywej-skorki-do-visual-studio-code/

https://www.matemaks.pl/zludzenia-optyczne.html, dostęp: 25.11.2025

Propaganda

https://przystanekprl.pl/wp-content/uploads/2024/01/151.jpg



https://histmag.org/Najciekawsze-plakaty-propagandowe-PRL-Galeria-15486

Źródło: https://wielkahistoria.pl/bitwa-pod-kadesz-jedna-z-najbardziej-przelomowych-batalii-epoki-starozytnej , dostęp: 30.11.2025

Fake news

Donald Trump

This article is more than 7 years old

Trump accuses CNN of 'fake news' over reported Celebrity Apprentice plans

President-elect denies reports he plans to remain an executive producer amid widespread concern over spread of fake news on social media

Martin Pengelly *and agencies*

Sat 10 Dec 2016 14.54 CET

Share

Donald Trump has denied reports he plans to remain an executive producer of The Celebrity Apprentice. Photograph: Shannon Stapleton/Reuters

President-elect Donald Trump has accused CNN of reporting "fake news" regarding his reported intention to maintain an executive producer credit on The Celebrity Apprentice after moving into the White House.

He would not be working on the series at all, he said in two tweets sent before dawn on Saturday, "even part time".

Most viewed

When will we k result of the US election?

US election resu Donald Trump a Harris vie to be

Live

US election 202 updates: voting in most states a Trump hope to presidency

Here is what my data says about presidential ele John Zogby

First US election three-all tie bet and Harris

https://www.theguardian.com/us-news/2016/dec/10/trump-celebrity-apprentice-cnn-fake-news

“Misinformation”

https://aszdziennik.pl/151379,sinica-nas-zachwyca-kampania-polskich-jezior-zaprasza-do-plazowania , dostęp: 2024 rok

Crossweb.pl
1 203 obserwujących
5 h •

Cześć 👋

Jak się macie w Cyber Monday? 😄

W tym tygodniu czeka nas m.in.:
📌 Start jedynych w swoim rodzaju kalendarzy adwentowych - #Cyberadvent by Beata Zalewa z m.in. Grzegorz Sztandera, ⚔️ Lena Sędkiewicz i Heartless Adham oraz Świąteczny Kalendarz Programisty by Radek Wojtysiak z m.in. Rita Łyczywek (Małgorzata), 🐉 Katarzyna Brzozowska czy Cezary Sanecki
📌 Agile Warsaw #335 z Krzysztof Niewiński
📌 Oh My Hack pod patronatem Crossweb i prelekcje m.in. Grzegorz Tworek, 🔥 Jakub Mrugalski czy Michał Kłaput
📌 WordUp Warszawa z Karolina Tanona i Karol Sawka
📌 3 duże wydarzenia w Warszawie - Python Summit, YavaConf i DevAI by Data Science Summit i prelekcje min. Katarzyna Leszczyńska-Bohdan, Piotr Stapp czy Mateusz Chrzonstowski
📌 Xmas Party 2025! organizowane przez Kraków Miastem Startupów
📌 BeefUp #11
📌 UXberries UX Unpacked #1: UX Researcher 2.0 - Badania UX w nowym świetle Weronika Pielech - są jeszcze wolne miejsca! Zapisy na Crossweb 😉
📌 HackNation PL z m.in. Sebastian Małyska, Arek (Arkadiusz) Radek czy Dawid Perdek
📌 ... i więcej ➡️ https://lnkd.in/g-sssFH

Crossweb.pl
1 203 obserwujących
5 h •

Cześć 👋

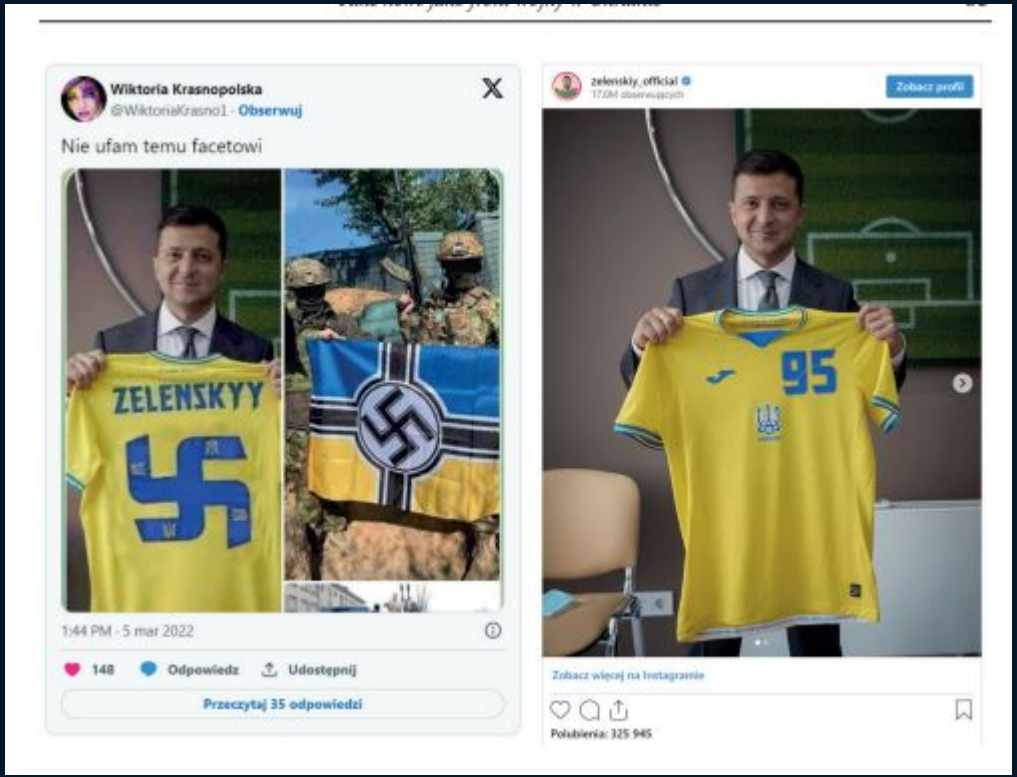
Jak się macie w Cyber Monday? 😄

W tym tygodniu czeka nas m.in.:
🪓 Start jedynych w swoim rodzaju kalendarzy adwentowych - #Cyberadvent by Beata Zalewa z m.in. Grzegorz Sztandera, ⚔️ Lena Sędkiewicz i Heartless Adham oraz Świąteczny Kalendarz Programisty by Radek Wojtysiak z m.in. Rita Łyczywek (Małgorzata), 🐉 Katarzyna Brzozowska czy Cezary Sanecki
🪓 Agile Warsaw #335 z Krzysztof Niewiński
🪓 Oh My Hack pod patronatem Crossweb i prelekcje m.in. Grzegorz Tworek, 🔥 Jakub Mrugalski czy Michał Kłaput
🪓 WordUp Warszawa z Karolina Tanona i Karol Sawka
🪓 3 duże wydarzenia w Warszawie - Python Summit, YavaConf i DevAI by Data Science Summit i prelekcje min. Katarzyna Leszczyńska-Bohdan, Piotr Stapp czy Mateusz Chrzonstowski
🪓 Xmas Party 2025! organizowane przez Kraków Miastem Startupów
🪓 BeefUp #11
🪓 UXberries UX Unpacked #1: UX Researcher 2.0 - Badania UX w nowym świetle Weronika Pielech - są jeszcze wolne miejsca! Zapisy na Crossweb 😉
🪓 HackNation PL z m.in. Sebastian Małyska, Arek (Arkadiusz) Radek czy Dawid Perdek
🪓 ... i więcej ➡️ https://lnkd.in/g-sssFH

Dezinformacja

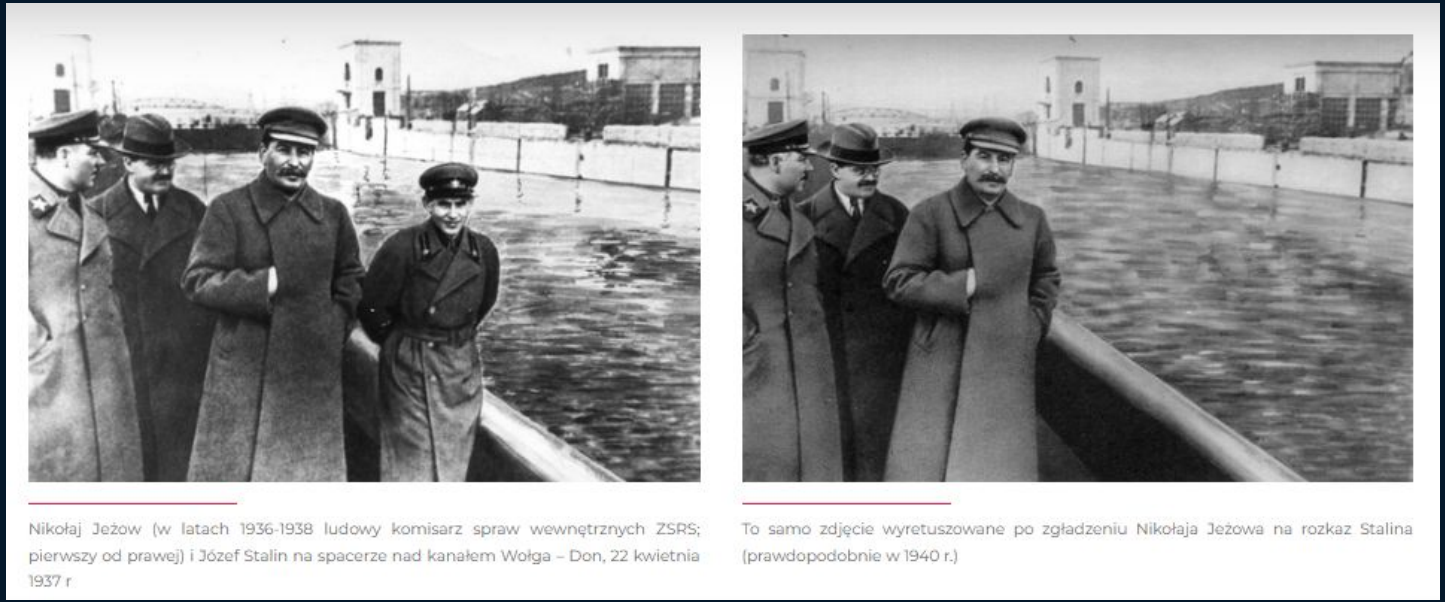
Wojna na Ukrainie?

Wojna na Ukrainie?



https://pressto.amu.edu.pl/index.php/sup/article/download/42242/35439/95328

Manipulacja źródłami fotograficznymi ("nowy" typ fake news")



Nikołaj Jeżow (w latach 1936-1938 ludowy komisarz spraw wewnętrznych ZSRS; pierwszy od prawej) i Józef Stalin na spacerze nad kanałem Wołga – Don, 22 kwietnia 1937 r

To samo zdjęcie wyretuszowane po zgładzeniu Nikołaja Jeżowa na rozkaz Stalina (prawdopodobnie w 1940 r.)

https://przystanekhistoria.pl/pa2/tematy/propaganda/103975,Dawne-techniki-retuszu-fotografii.html, dostęp: 2024 rok

Deepfake

https://news.sky.com/story/fake-ai-images-keep-going-viral-here-are-eight-that-have-caught-people-out-13028547, dostęp: 2024 rok

https://www.nask.pl/media/2025/10/Handbook-Przewodnik-Cyberbezpieczenstwo-i-AI-dla-Mediow-i-Tworcow.pdf

- **Fałszywe reklamy promujące przede wszystkim nieistniejące produkty finansowe** – platformy inwestycyjne, aplikacje do szybkiego zarabiania pieniędzy, rzekome rabaty, dopłaty rządowe, programy państwowe, a także niesprawdzone lub fikcyjne środki medyczne i terapie. Czasami odnoszą się także do rzekomych zmian prawnych lub edukacyjnych bądź wprowadzania nowych zakazów. Często wykorzystują wizerunki polityków, dziennikarzy, ekspertów w danej dziedzinie, celebrytów, a nawet duchownych, by nadać przekazowi autorytet i zwiększyć jego wiarygodność.
- **Manipulacja treścią przemówień politycznych** – zmiana wypowiedzi znanych osób w celu szerzenia dezinformacji lub wzbudzenia kontrowersji.
- **Syntetyczne materiały audio i video do wyłudzania danych** – voice cloning i podszywanie się pod znajomych w komunikatorach („na wnuczka", „na policjanta", a teraz też „na przyjaciela").
- **Materiały o charakterze dyskredytacyjnym i kompromitującym** – przedstawiające ludzi w stanie upojenia, w sytuacjach o zabarwieniu erotycznym/pornograficznym (tzw. deepnude) czy jako ofiary przemocy.

Granice się zacierają...

Skala zagrożenia?

Skala zagrożenia?

Socjotechnika – zagrożenie, które ewoluuje

Jak wynika z raportu ENISA „Threat Landscape 2024", inżynieria społeczna uplasowała się na trzecim miejscu wśród najpoważniejszych cyberzagrożeń, zaraz po atakach ransomware i złośliwym oprogramowaniu.

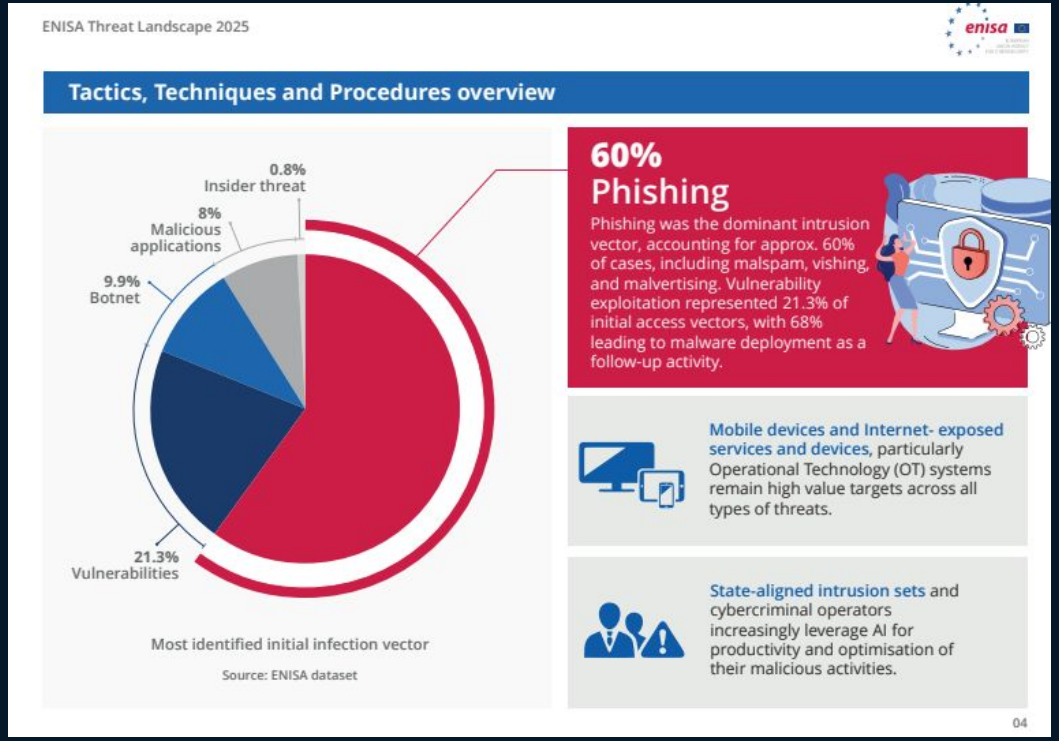
https://www.nask.pl/aktualnosci/socjotechniki-to-jedno-z-najpowazniejszych-cyberzagrozen-jak-nie-dac-sie-zmanipulowac-o-tym-ecsm-2024, dostęp: 30.11.2025 r.

Skala zagrożenia?

Phishing remains the dominant intrusion vector (60%) and is evolving through techniques used in large-scale campaigns. The availability of phishing-as-a-service platforms demonstrates the industrialisation of phishing operations, enabling adversaries of all skill levels to launch complex campaigns. Abuse of cyber dependencies have also intensified, as shown by compromises in open-source repositories, malicious browser extensions and breaches of service providers, amplifying risk throughout interconnected digital ecosystems.

https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf , dostęp: 01.12.2025 r.

Skala zagrożenia?



https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf , dostęp: 01.12.2025 r.

Czy firmy się przyznają?

6.1 PHISHING INCIDENTS REMAIN A MOST IMPORTANT INITIAL VECTOR

Phishing and pretexting via email continue to be the leading cause of cybersecurity incidents. According to Verizon, phishing and pretexting accounts for 73% of breaches of social engineering incidents. Business email compromise, which falls under pretexting in the Verizon statistics, continues to have an important financial impact. While the median transaction remained stable, it still accounts for 50K USD in losses. An important addition in this report is that, of all the victims who reached out to law enforcement, they were able to get back 79% of their losses in half of the cases.[300]. The FBI reports that, in 2023, they received more than 22,000 complaints relating to Business Email compromise with adjusted losses of over 2.9

[300] 2024 Data breach Investigations Report – Verizon.

https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

Kogo lubią (udawać) atakujący?

Check Point Research identified the following top spoofed brands based on their overall appearance in brand phishing events during Q4 2023: Microsoft (33%), Amazon (9%), Google (8%), Apple (4%), Wells Fargo (3%)[308]. For Q1 2024 we mainly saw an increase for Microsoft and LinkedIn: Microsoft (38%), Google (11%), LinkedIn (11%), Apple (5%), DHL (5%)[309].

IBM reports similar data, although not identical. For 2023, the most spoofed brands included Google, Telegram, Microsoft, Visa and Apple[310].

https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

Kto przoduje w atakach z wykorzystaniem socjotechniki?

6.4 SCATTERED SPIDER TARGETED BY LAW ENFORCEMENT

In June 2024, a 22-year-old man from the UK was arrested in Spain for allegedly being part of the cybercriminal group known as Gold Harvest, also referred to as Scattered Spider. This operation is said to be a joint operation between the FBI and the Spanish Police[315] [316].

Scattered Spider stands out for its social engineering attacks and distinctive composition compared to typical cybercriminal organisations. Throughout 2023, the group used SMS phishing (smishing), voice phishing (vishing) to harvest credentials, and phone calls towards helpdesks to manipulate support staff into resetting passwords or multi-factor authentication (MFA) for targeted accounts. They also used previous intrusions at telecom companies to perform SIM swaps, enabling interception of one-time password (OTP) codes. The group targeted IT and INFOSEC employees, presumably because of their access to security applications and documentation that facilitate lateral movement and further account compromises. A smaller number of attacks focused on employees with access to financial resources[317] [318].

https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

Jak nas atakują i jak się bronić?

phishing

smishing

vishing

pretexting

spoofing

BEC

phishing
(mail, strona)
\+ spear phishing (targetowany)

smishing
(SMS)

vishing
(telefon)

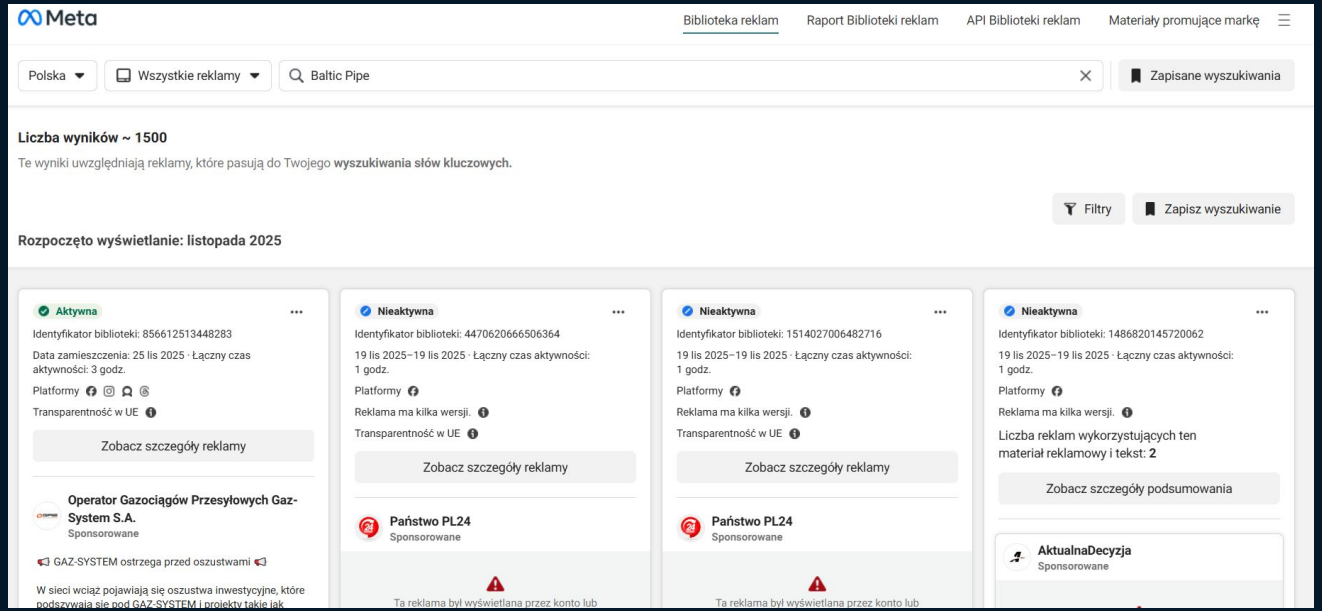
pretexting
(fałszywa historia, podszycie się pod kogoś)

spoofing
(podszycie się, np. pod numer tel)

Business Email Compromise

Przykłady - użytkownik

Zbyt dobre, by było prawdziwe



https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=PL&is_targeted_country=false&media_type=all&q=Baltic%20Pipe&search_type=keyword_unordered, dostęp: 25.11.2025

https://demagog.org.pl/fake_news/zostan-inwestorem-projektu-baltic-pipe-uwaga-na-scam/ , dostęp: 2024 rok

DEMAGOG Menu Wypowiedzi Fake newsy Zgłoś do weryfikacji Wesprzyj nas

Skopiuj link

Drukuj

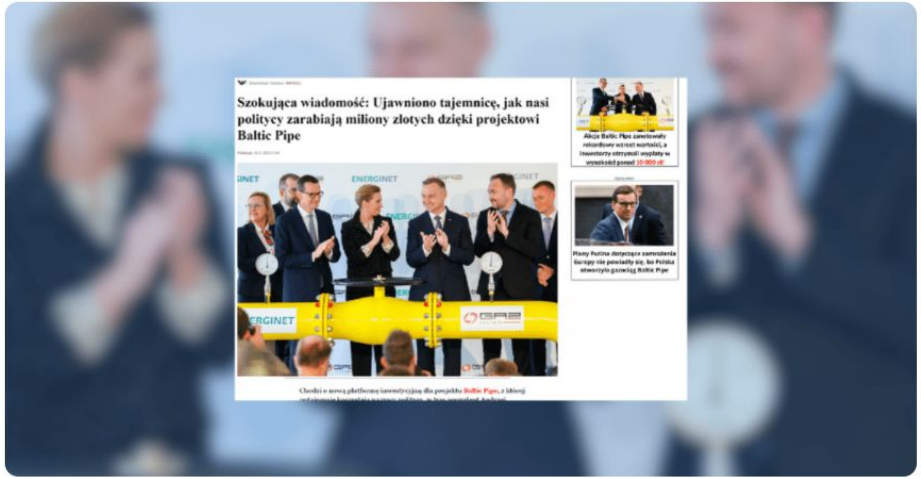
Udostępnij

Fake News

Nowa platforma inwestycyjna Baltic Pipe? To kolejne oszustwo

FAKE NEWS OSZUSTWO

Wizerunek prezydenta Andrzeja Dudy użyty w celach oszustwa.



POLECANE DLA CIEB

EKOLOGIA

Chcemy coraz więcej mat
Ale zapasy kurczą się nie
powodu

Artykuł OSINT

OSINT gospodarczy. Jak
spółki i ich wiarygodność

Podcast

Czy DSA ogranicz
słowa w interneci
Rozmowa z dr Dor
Głowacką

28.10.2025

https://demagog.org.pl/fake_news/nowa-platforma-inwestycyjna-baltic-pipe-to-kolejne-oszustwo/?gad_source=1&gad_campaignid=23150820387&gbraid=0AAAACdXq8DsOdQlB3cHLqwModAUFVScN&gclid=Cj0KCQiAxJXJBhD_ARIsAH_JGjiB_xeYvBuA0lh5lUnCnClOqvWZTJ8HffETGp_pkzuc-4s-EwHrA8waAqCOEALw_wcB, dostęp: 25.11.2025

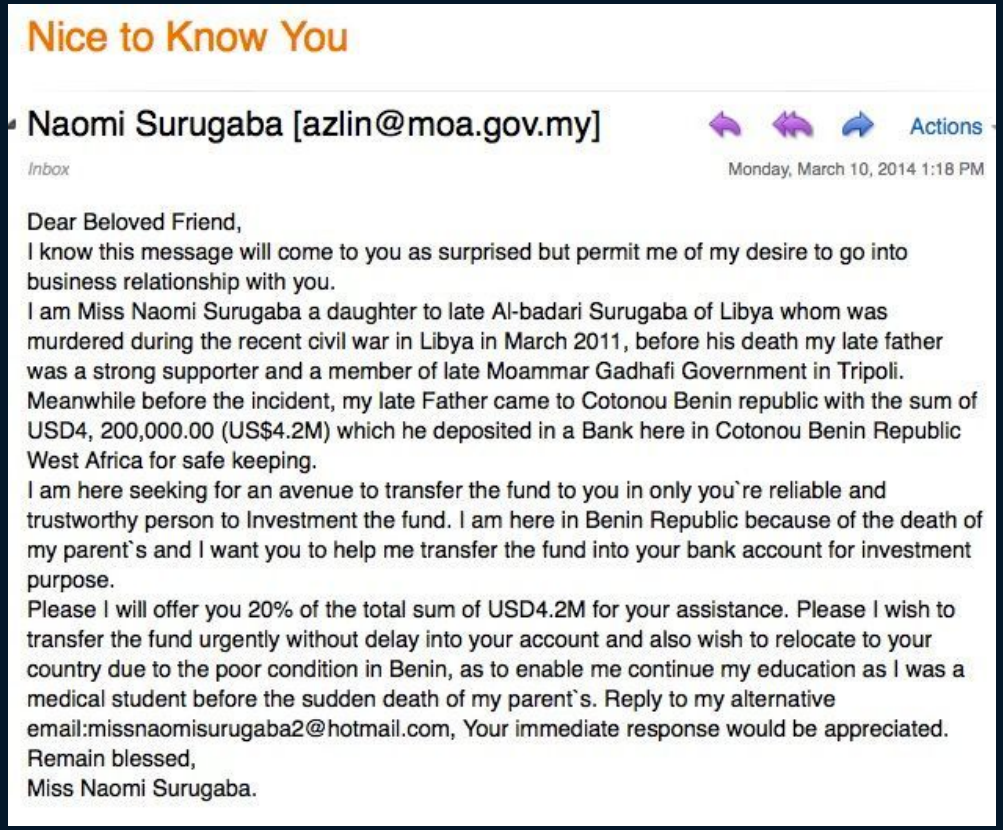
UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Dodatkowo, w październiku 2025 roku analitycy CSIRT KNF zgł e wrześniu'25), które publikowały reklamy fałszywych inwestycji. W scenariuszu znanym pod nazwą „fraud inwestycyjny" cyberprzestępcy podszywają się pod znane osoby lub instytucje, celem nakłonienia potencjalnej ofiary do zainwestowania środków i otrzymania wysokiej stopy zwrotu. W rzeczywistości prowadzą grę psychologiczną, mającą na celu narażanie ofiary na wysokie starty finansowe.

Fałszywe oferty (zarówno w postaci nagrań video, jak i statycznych reklam) dystrybuowane są poprzez reklamy na platformie Facebook (rys. 1).

Rysunek 1 Fałszywe inwestycje – reklamy na platformie Facebook

https://cebrf.knf.gov.pl/component/content/article/przeglad-wybranych-oszustw-internetowych-pazdziernik-2025?catid=14:ostrzezenia-csirt&Itemid=101, dostęp: 25.11.2025



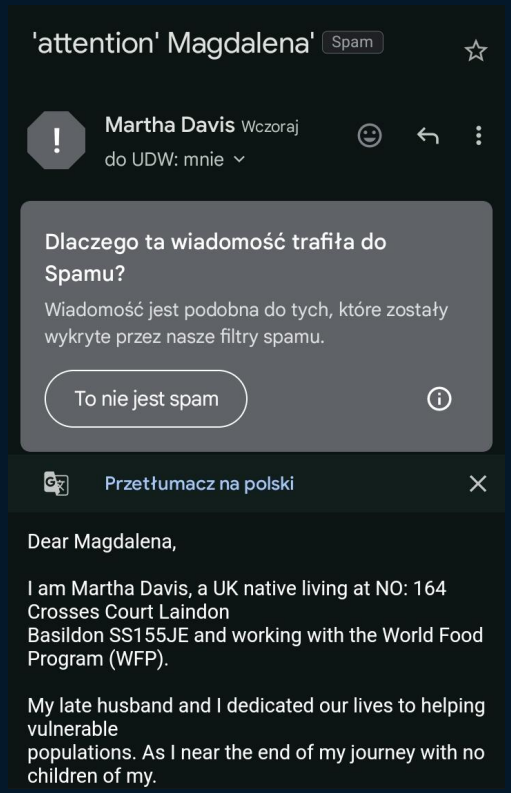
Nice to Know You

Naomi Surugaba [azlin@moa.gov.my] Actions

Inbox Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

https://publicystyka.ngo.pl/afrykanski-ksiaze-i-worki-ze-zlotem-oszustwa-internetowe-cz-2, dostęp: 30.11.2025



children of my.
I am reaching out to ensure our mission lives on.

Having found your email in the WFP database, I am asking if you would
be willing to accept my entire savings of $1,200,000.00 USD for
charitable purposes, specifically to assist orphanages in your
country. I suggest allocating 40% towards your business endeavors and
60% towards supporting orphanages and empowering widows, in the name
of God and for my peace of mind. With a stage 4 cancer diagnosis, I am
facing surgery with a 50/50 chance of success.

I am not looking for a hero or a saint, but someone who will use these
funds to uphold our shared values of empowering widows and supporting
orphanages.

orphanages.

If you are willing to accept this proposal, I would be grateful. If
not, I completely understand and wish you the best.

Sincerely,
Mrs. Martha Davis

Rada nr 1.0:

pieniądze niestety nie spadają z nieba...

Rada nr 1.0:

pieniądze niestety nie spadają z nieba...

(umiejętności z kursu za 10 k również...)

Rada nr 1.0:

pieniądze niestety nie spadają z nieba…

(umiejętności z kursu za 10 k również…)

Ani cudowne oferty pracy, w których zarobimy miliony…
(przynajmniej nie każdemu).

Rada nr 1.0:

Życie jest ciężkie!

6.5 SOCIAL ENGINEERING THROUGH JOB SEARCH PLATFORMS

Social engineering attacks are increasingly targeting job listing platforms, exploiting the trust inherent in recruitment processes. Cybercriminals and nation-state actors use advanced social engineering tactics to deceive both job seekers and employers, resulting in financial loss, espionage and compromised security.

https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, dostęp: 1.12.2025

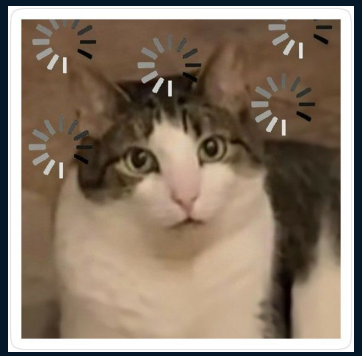
Rada nr 1.1:

Zanim zainwestujesz w coś / coś kupisz - daj sobie 24h na przemyślenie + dowiedz się więcej

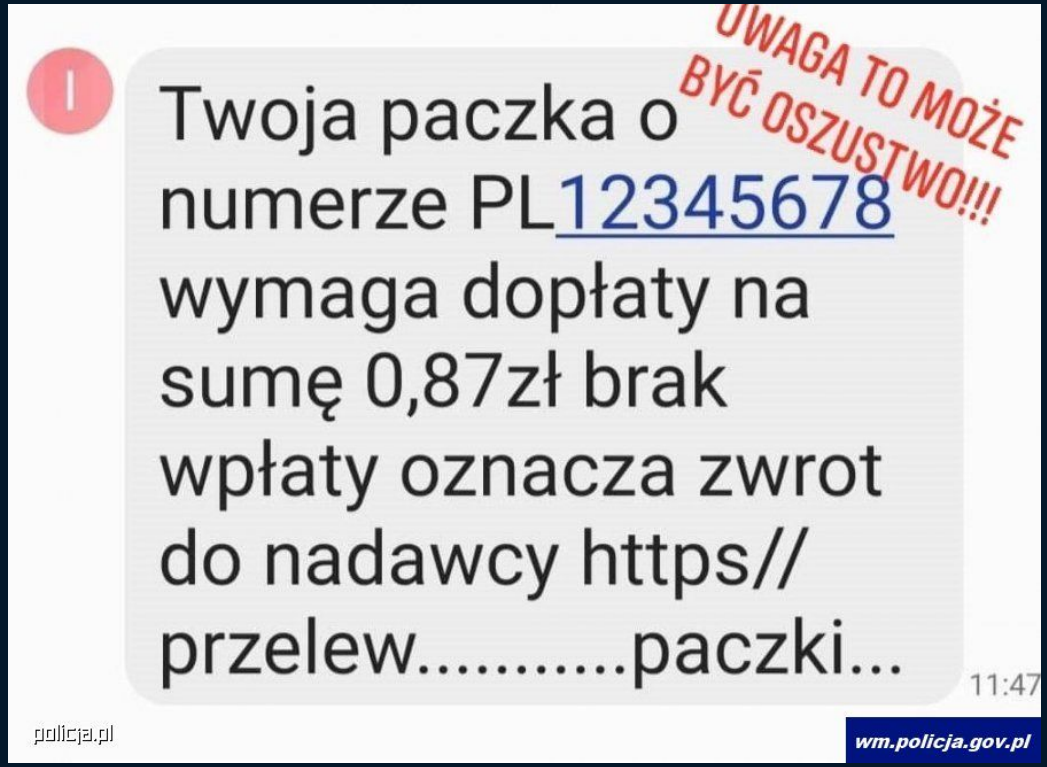
(wyjście z pętli presji czasu)

Rada nr 1.1:

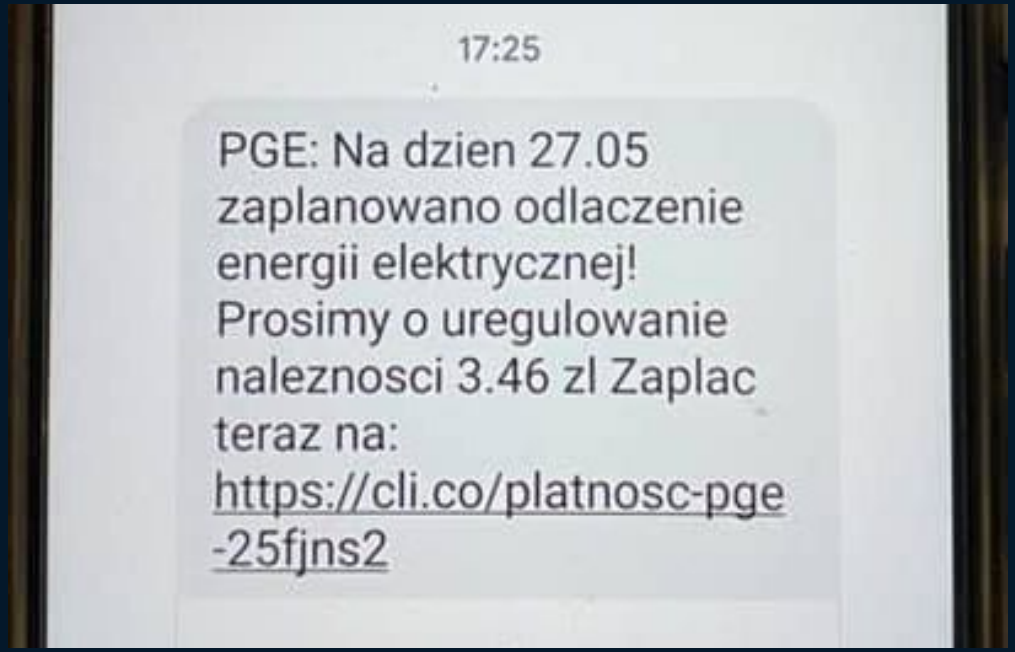
Dajmy sobie czas, by nasz gadzi mózg się uspokoił ;)



Scam z huśtawką emocjonalną w tle



https://warminsko-mazurska.policja.gov.pl/ol/aktualnosci/75555,Dostales-SMS-a-z-prosba-o-doplate-do-przesylki-Uwazaj-to-moze-byc-oszustwo.html, dostęp: 30.11.2025



https://lubelska.policja.gov.pl/lub/aktualnosci/119808,Oszustwo-na-doplate-do-rachunku-za-prad.html , dostęp: 30.11.2025

https://cbzc.policja.gov.pl/dokumenty/zalaczniki/442/442-657.png, dostęp: 30.11.2025

Rada nr 2.0:

Przerwij połączenie i oddzwoń!

Rada nr 2.1:

Nie klikaj w linki z smsów!

(W mailach zanim klikniesz podejrzyj, gdzie dany link prowadzi…)

Rada nr 2.2:

Wejdź na stronę dostawcy + miej managera haseł

LUB

Zadzwoń na oficjalną infolinię i spytaj!

Rada nr 2.3:

Uważność = umiejętność jutra

CoGUI

A new phishing kit named 'CoGUI' sent over 580 million emails to targets between January and April 2025, aiming to steal account credentials and payment data.

The messages impersonate major brands like Amazon, Rakuten, PayPal, Apple, tax agencies, and banks.

The activity culminated in January 2025, where 170 campaigns sent 172,000,000 phishing messages to targets, but the following months maintained equally impressive volumes.

https://www.bleepingcomputer.com/news/security/cogui-phishing-platform-sent-580-million-emails-to-steal-credentials/, dostęp: 30.11.2025

CoGUI

CoGUI attack chain

The attack starts with a phishing email impersonating a trusted brand, often having urgent subject lines requiring the recipient's action.

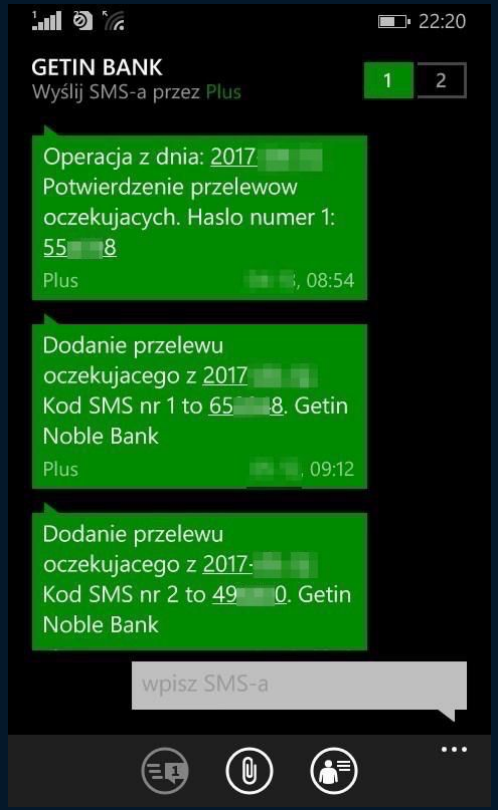
The messages include a URL that redirects to a phishing website hosted on the CoGUI phishing platform, but the link only resolves if the target meets specific criteria pre-defined by the attackers.

These criteria include their IP address (location), browser language, operating system, screen resolution, and device type (mobile or desktop).

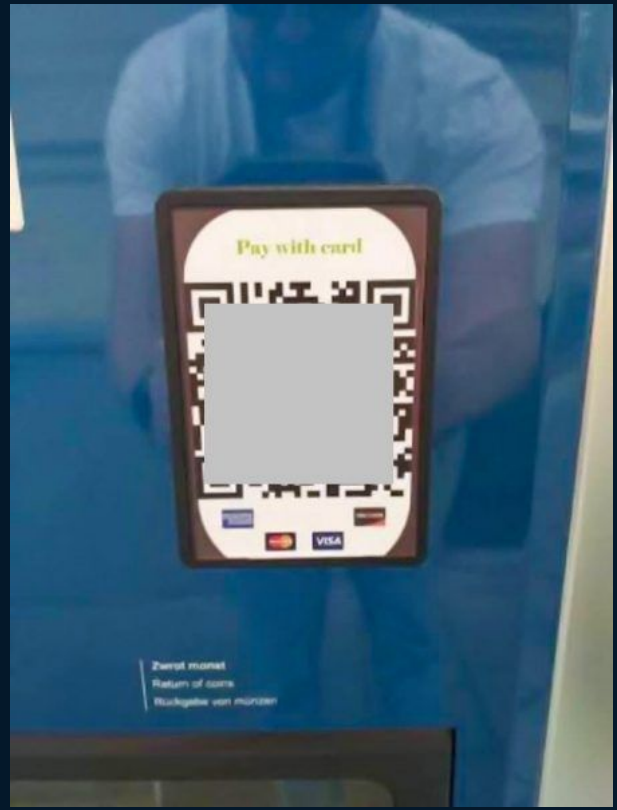
If the criteria aren't met, victims are redirected to the brand's legitimate site that was impersonated to reduce suspicion.

Valid targets are redirected to a phishing page featuring a fake login form that mimics the design of the real brand, tricking victims into entering their sensitive information.

https://www.bleepingcomputer.com/news/security/cogui-phishing-platform-sent-580-million-emails-to-steal-credentials/, dostęp: 30.11.2025



Chwila nieuwagi



https://niebezpiecznik.pl/post/autoryzacja-mobilna-aplikacja-bank-przelewy/, dostęp: 30.11.2025

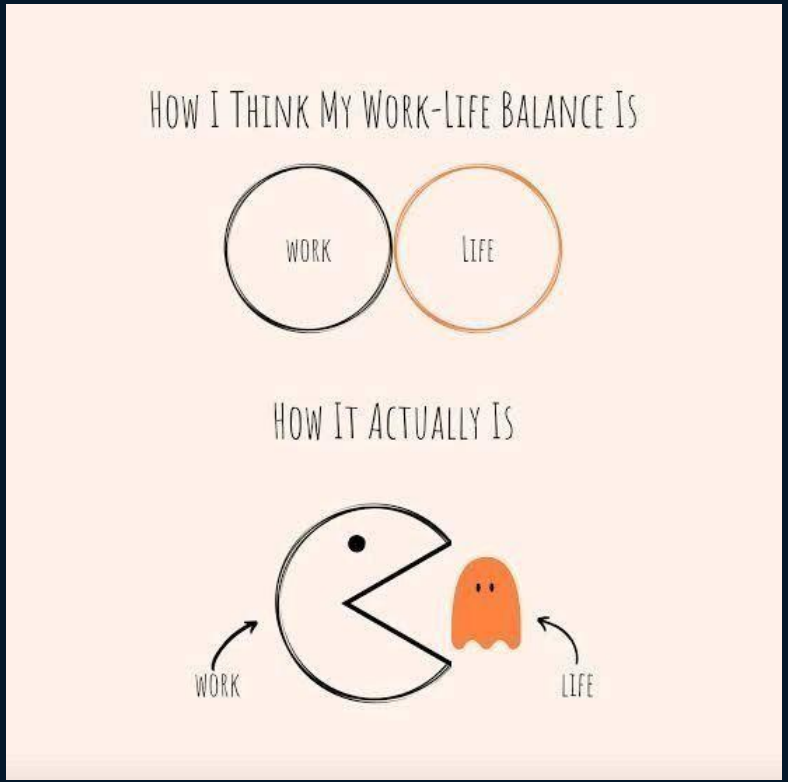
https://sekurak.pl/w-krakowie-na-parkingach-pojawily-sie-falszywe-kody-qr-uwazajcie-na-zawartosc-swojego-konta-bankowego/ , dostęp: 30.11.2025

Rada nr 3.0:

Czytamy uważnie + dwa razy

Rada nr 3.1:

Warto dbać o work - life wellness…



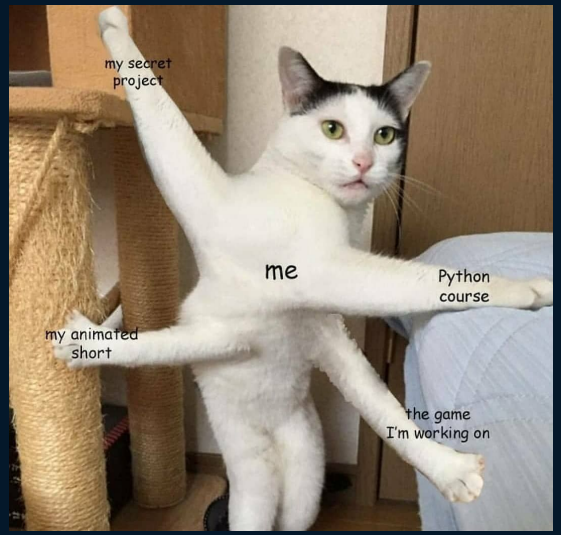
https://pl.pinterest.com/pin/redes-in-2025--438819557468962090/

Rada nr 3.2:

Multitasking się nie sprawdza ;)

Rada nr 3.2:

Jakiekolwiek przeciążenie się nie sprawdza…

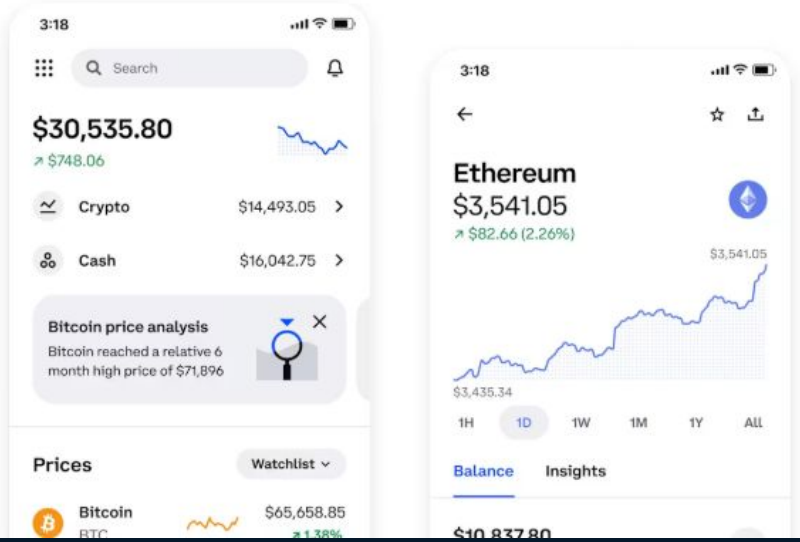


https://www.facebook.com/BIBMsia/photos/a.558759790926935/2180113268791571/?id=419381398198109

Przykłady - firma

Cryptocurrencies Individuals Businesses Institutions Developers Company

Sign in Sign up



The future of money is here

We're the most trusted place for people and businesses to buy, sell, and manage crypto.

Insider’s threat

What happened

Criminals targeted our customer support agents overseas. They used cash offers to convince a small group of insiders to copy data in our customer support tools for less than 1% of Coinbase monthly transacting users. Their aim was to gather a customer list they could contact while pretending to be Coinbase—tricking people into handing over their crypto. They then tried to extort Coinbase for $20 million to cover this up. **We said no.**

https://www.coinbase.com/pl/blog/protecting-our-customers-standing-up-to-extortionists, dostęp: 30.11.2025

Rada nr 4

Użycie narzędzi adekwatnych do zagrożenia

1. **Malicious Insiders**: Individuals who intentionally misuse their access for personal gain, revenge, or other harmful purposes
2. **Negligent Insiders**: Employees who unintentionally expose data or systems through carelessness or lack of security awareness
3. **Compromised Insiders**: Legitimate users whose credentials have been stolen or who are being manipulated through social engineering

https://gurucul.com/cybersecurity-101/what-is-insider-threat-prevention/

Timeline of Events

M&S

The breach appears to have originated through a third-party supplier. M&S's IT helpdesk is run by Tata Consultancy Services (TCS), and executives later admitted that the hackers first compromised this contractor. In practice, the attackers used **social engineering** to trick helpdesk staff into handing over access: they rang support desks posing as internal IT, obtained credentials or password resets, and then infiltrated the M&S network. CEO Stuart Machin bluntly **told** reporters M&S was simply "unlucky … through human error" – the malicious calls fooled staff despite the company's security investments. In other words, the attackers rang M&S suppliers and employees, exploiting trust and the fact that their callers were native English speakers. Once inside, the hackers deployed the DragonForce ransomware to encrypt data and steal customer records.

https://www.blackfog.com/marks-and-spencer-ransomware-attack/, dostęp: 30.11.2025

Rada nr 5 - nauka na czyichś błędach

1. **Strong Multi-Factor Authentication.** All remote-access tools and employee accounts should have strong MFA. If the supplier helpdesk had required a second factor for password resets or admin logins, the simple phone-based breach might not have succeeded.
2. **Third-Party Risk Management.** Vendors and MSPs should be tightly controlled. Best practice is to give external contractors only the minimum privileges they need, and to segment their access from core systems. In this case, isolating the helpdesk environment (or using just-in-time virtual machines) could have prevented attackers from pivoting into M&S's main network.
3. **Employee Training and Verification.** Because the intrusion began with social engineering calls, security awareness would have been useful. Regular drills and strict procedures (e.g. requiring call-back verification or helpdesk ticket tracking) can ensure that support staff never blindly follow an unscheduled phone request. Employees must be trained to question unexpected requests for credentials or system changes.

https://www.blackfog.com/marks-and-spencer-ransomware-attack/, dostęp: 30.11.2025

4. **Email and Network Defenses.** A layered email security stack and phishing simulations are important. Advanced malware scanning, anomaly detection and network segmentation (so that one host compromise cannot encrypt all systems) are also needed. M&S has since said it is accelerating its multi-year tech upgrade into just a few months.
5. **Backups and Incident Plans.** A tried-and-true defense against ransomware is to maintain offline or immutable backups of all data and system images. If M&S had air-gapped backups, it could have restored systems without paying ransom. Likewise, a rehearsed incident response plan (from the UK's NCSC or CISA playbooks) enables faster recovery.

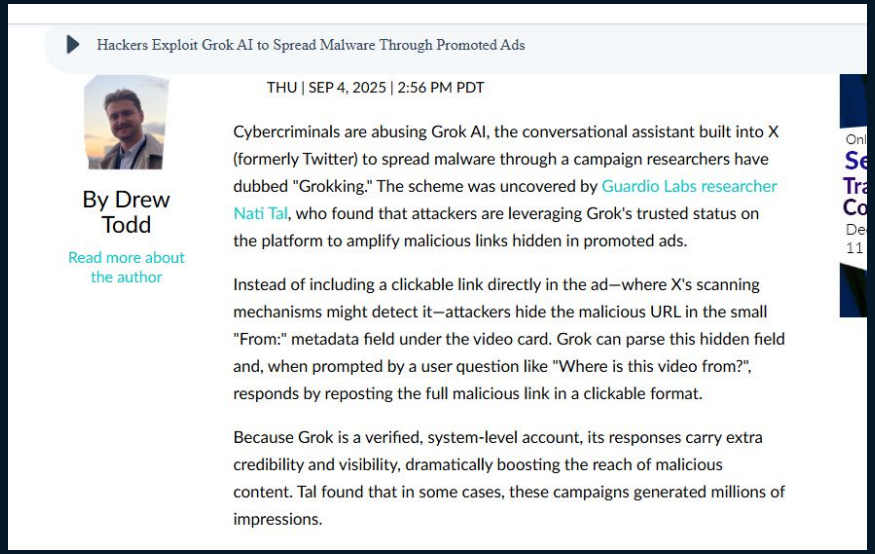
https://www.blackfog.com/marks-and-spencer-ransomware-attack/, dostęp: 30.11.2025

Nie zapominajmy o AI...

Artificial intelligence has become a defining element of the threat landscape. By early 2025, AI-supported phishing campaigns reportedly represented more than 80 percent of observed social engineering activity worldwide, with adversaries leveraging jailbroken models, synthetic media and model poisoning techniques to enhance their operational effectiveness.

https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf , dostęp: 01.12.2025 r.

Nie zapominajmy o AI...



Hackers Exploit Grok AI to Spread Malware Through Promoted Ads

THU | SEP 4, 2025 | 2:56 PM PDT

By Drew Todd

Read more about the author

Cybercriminals are abusing Grok AI, the conversational assistant built into X (formerly Twitter) to spread malware through a campaign researchers have dubbed "Grokking." The scheme was uncovered by Guardio Labs researcher Nati Tal, who found that attackers are leveraging Grok's trusted status on the platform to amplify malicious links hidden in promoted ads.

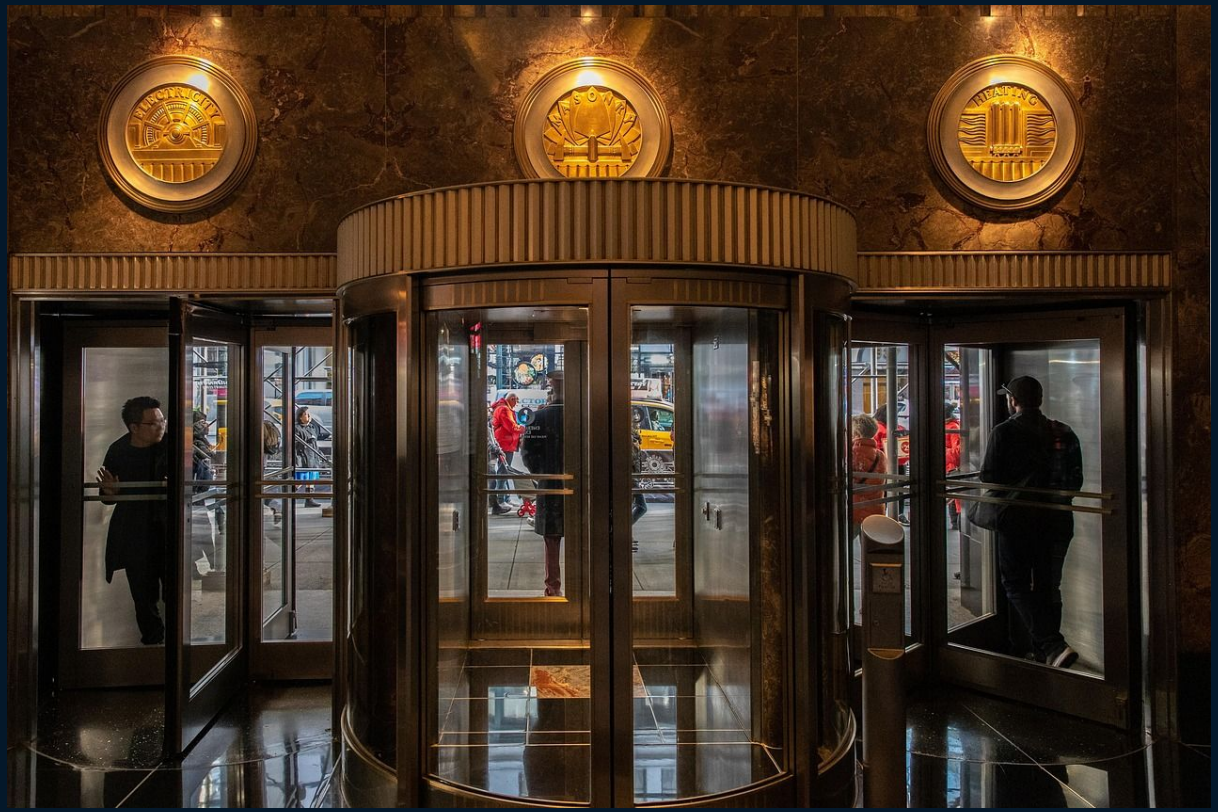
Instead of including a clickable link directly in the ad—where X's scanning mechanisms might detect it—attackers hide the malicious URL in the small "From:" metadata field under the video card. Grok can parse this hidden field and, when prompted by a user question like "Where is this video from?", responds by reposting the full malicious link in a clickable format.

Because Grok is a verified, system-level account, its responses carry extra credibility and visibility, dramatically boosting the reach of malicious content. Tal found that in some cases, these campaigns generated millions of impressions.

https://www.secureworld.io/industry-news/hackers-exploit-grok-ai-malware , dostęp: 01.12.2025 r.

Krok przed nami...

Gruntowne przygotowania



Spójna historia

dodatkowy składnik, który pomaga hackerom…

Przekonanie o nietykalności

https://www.imdb.com/title/tt0083271/mediaviewer/rm36390401/

https://lenasedkiewicz.com/pl/resources/cybersecurity/

Podsumowanie

100% obrona nie zawsze jest możliwa.

Można jednak być nieco lepiej przygotowanym.

Na co jeszcze warto zwrócić uwagę?

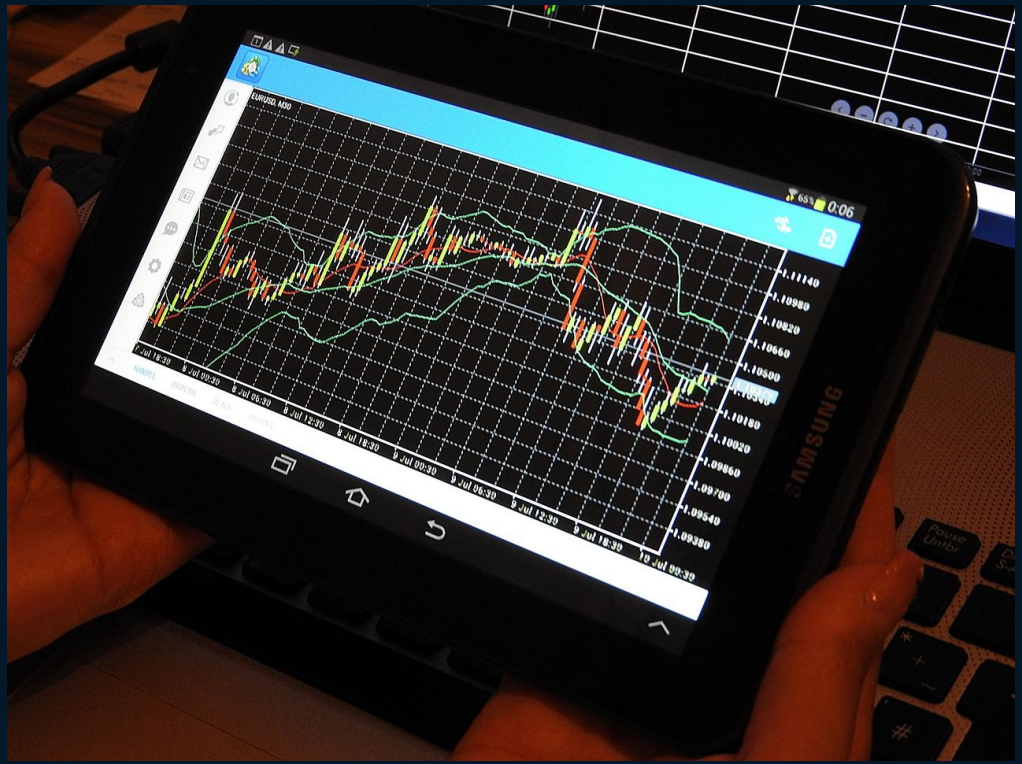
Analiza udostępnianych informacji

Zasada ograniczonego zaufania

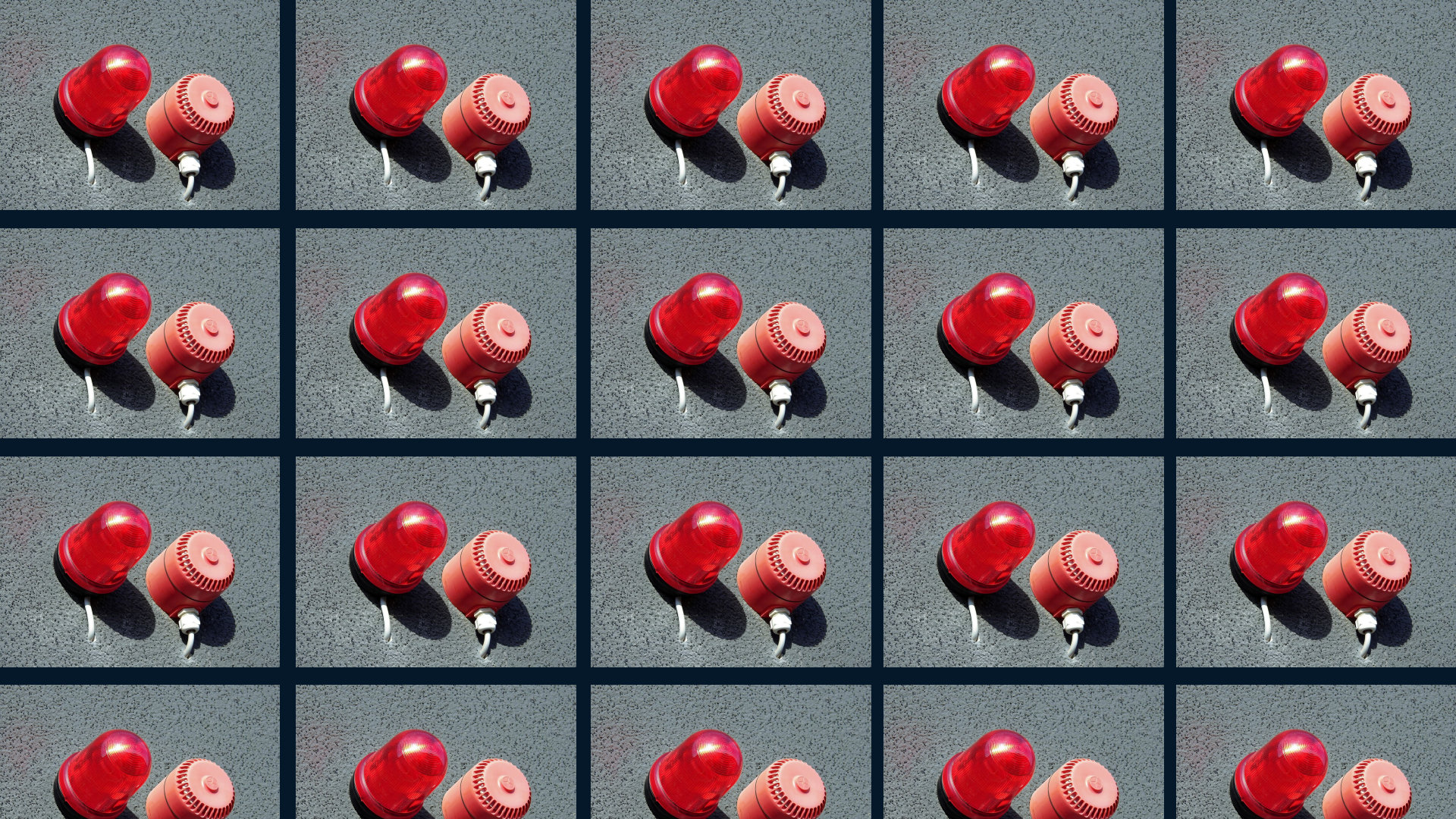
Oddech

Szkolenie pracowników

Dobre procedury

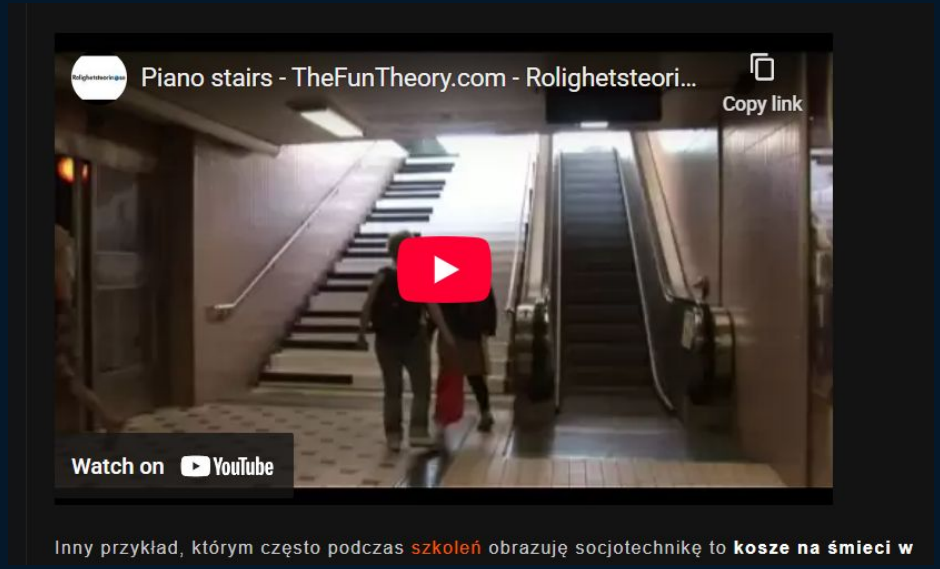


Przeciwdziałanie zmęczeniu bezpieczeństwem



https://lenasedkiewicz.com/pl/resources/digitalhygene/

PS: Nie każda socjotechnika jest zła ;)



https://niebezpiecznik.pl/post/socjotechnika/, dostęp: 30.11.2025

Q&A

https://lenasedkiewicz.com/pl/resources/cybersecurity/