(CYBER)SZKOLENIA

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Phishing, oszustwa w sieci i ransomware.

Najpowszechniejsze cyberzagrożenia – jak rozpoznać, jak zapobiegać

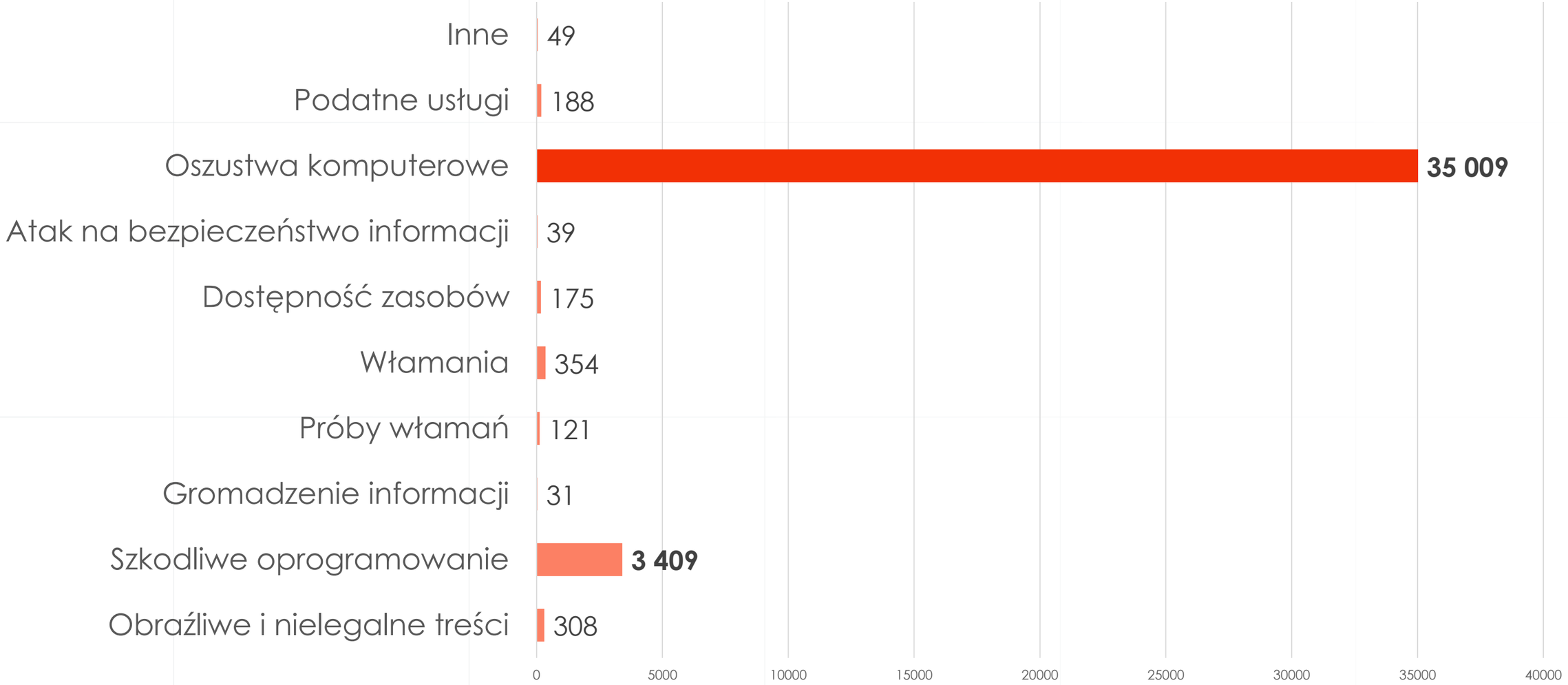
Ministerstwo Cyfryzacji

NASK

Plan części pierwszej

- Rodzaje i charakterystyka cyberzagrożeń
- Rozpoznawanie
- Reagowanie i zapobieganie
- Zgłaszanie incydentów

Incydenty zarejestrowane przez CERT Polska w 2022 roku



Oszustwa komputerowe

- Ataki wykorzystujące **socjotechnikę.**

- **Przeważnie podszywanie się pod inne osoby bądź instytucje.**

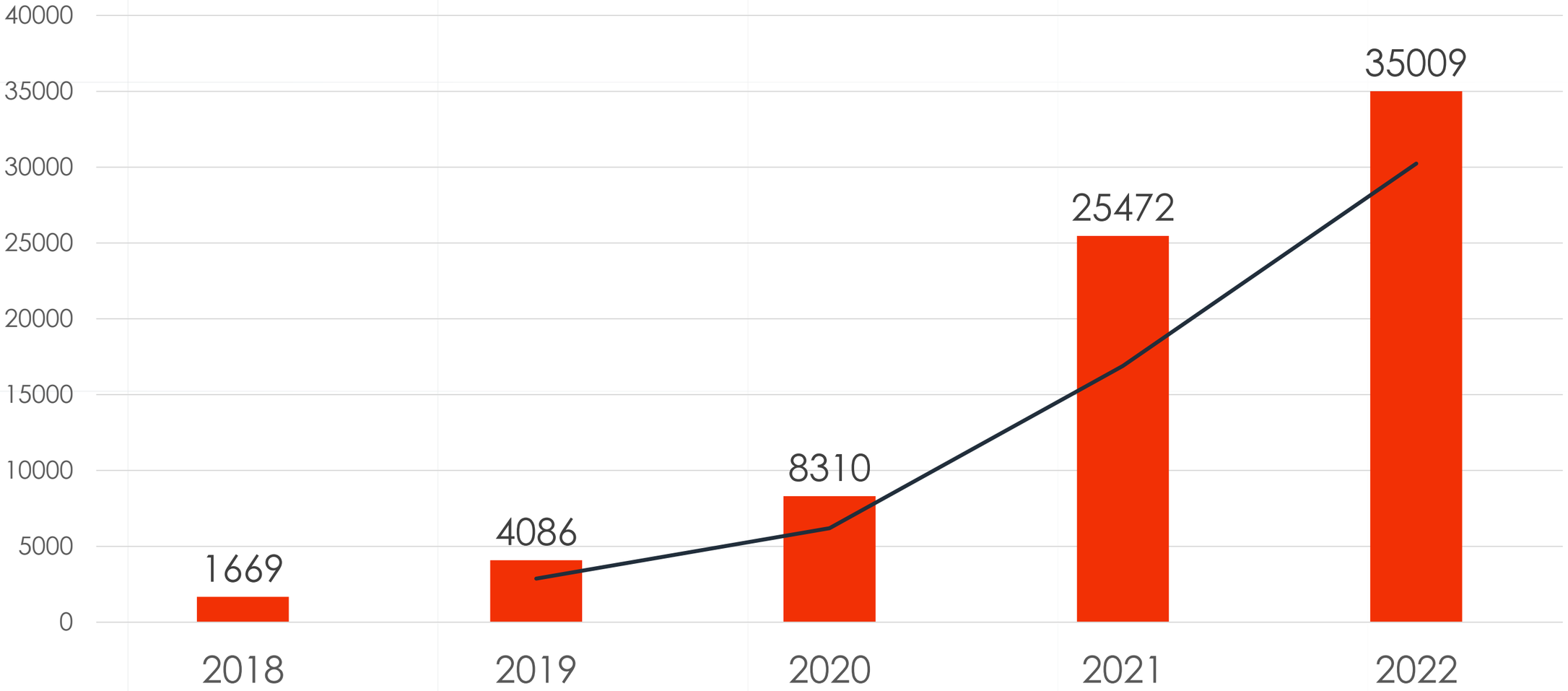
- Cel: **osiągnięcie korzyści majątkowej lub wyrządzenie innej osobie szkody.**

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Oszustwa zarejestrowane przez CERT Polska w latach 2018-2022



Phishing

czyli o metodach ataku i socjotechnice

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Phishing

Manipulacja, podstęp, perswazja + proste rozwiązania techniczne.

Podszywanie się pod zaufany podmiot lub osobę + wiadomości i fałszywe strony czy programy.

Nakłanianie do:

- ujawnienia poufnych danych,
- przekazania pieniędzy,
- instalacji złośliwego oprogramowania.

Rodzaje phishingu

mailowy

SMShing

Vishing

w reklamach,
ogłoszeniach,
w mediach itp.

masowy

spersonalizowany

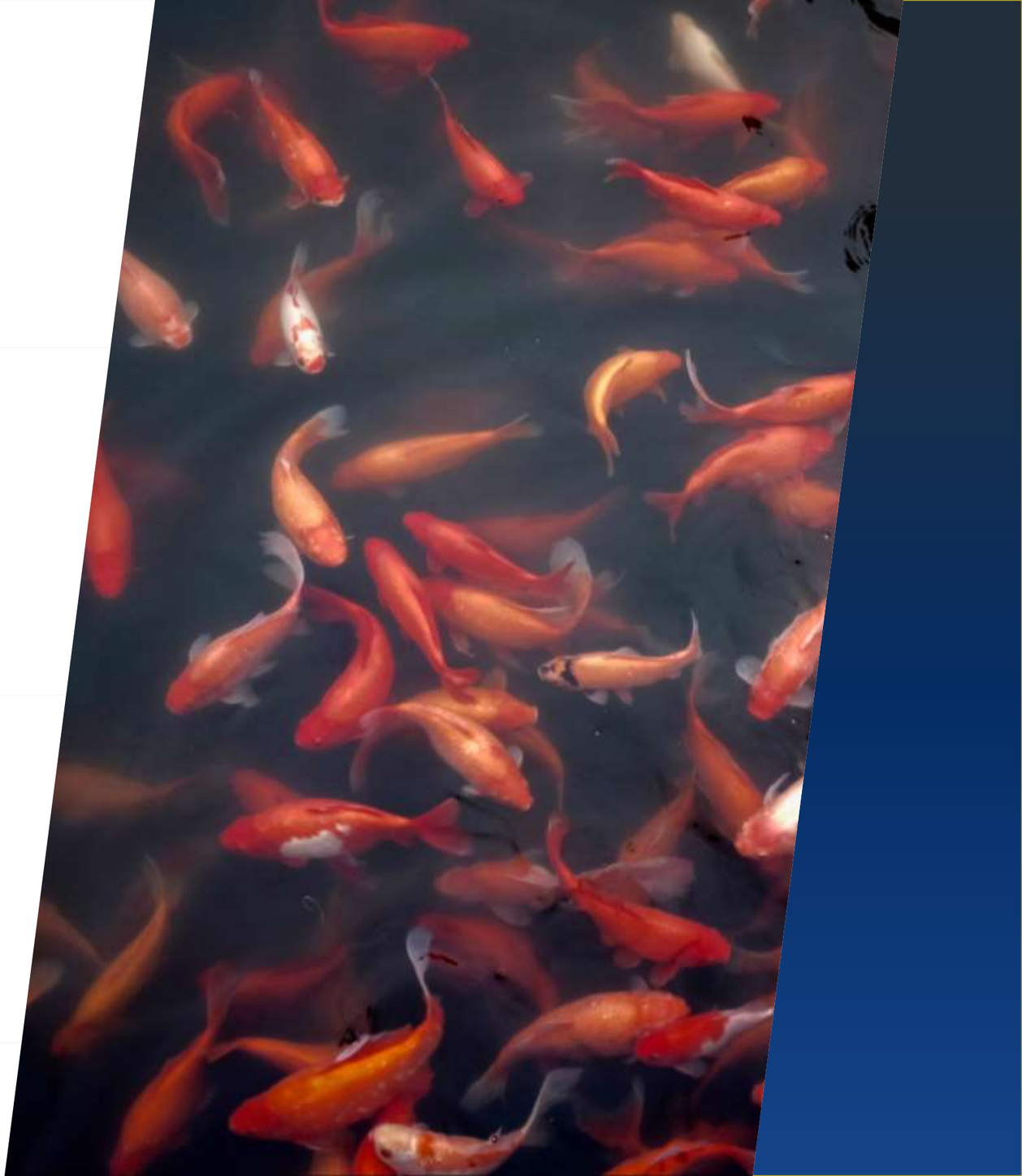
(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Phishing masowy

Wysyłka masowa, malspam.

Nastawiony na odsetek użytkowników, który statystycznie *kliknie;* mniejsza zdobycz, ale na masową skalę.

Uniwersalny pretekst i historia – może dotyczyć każdego.



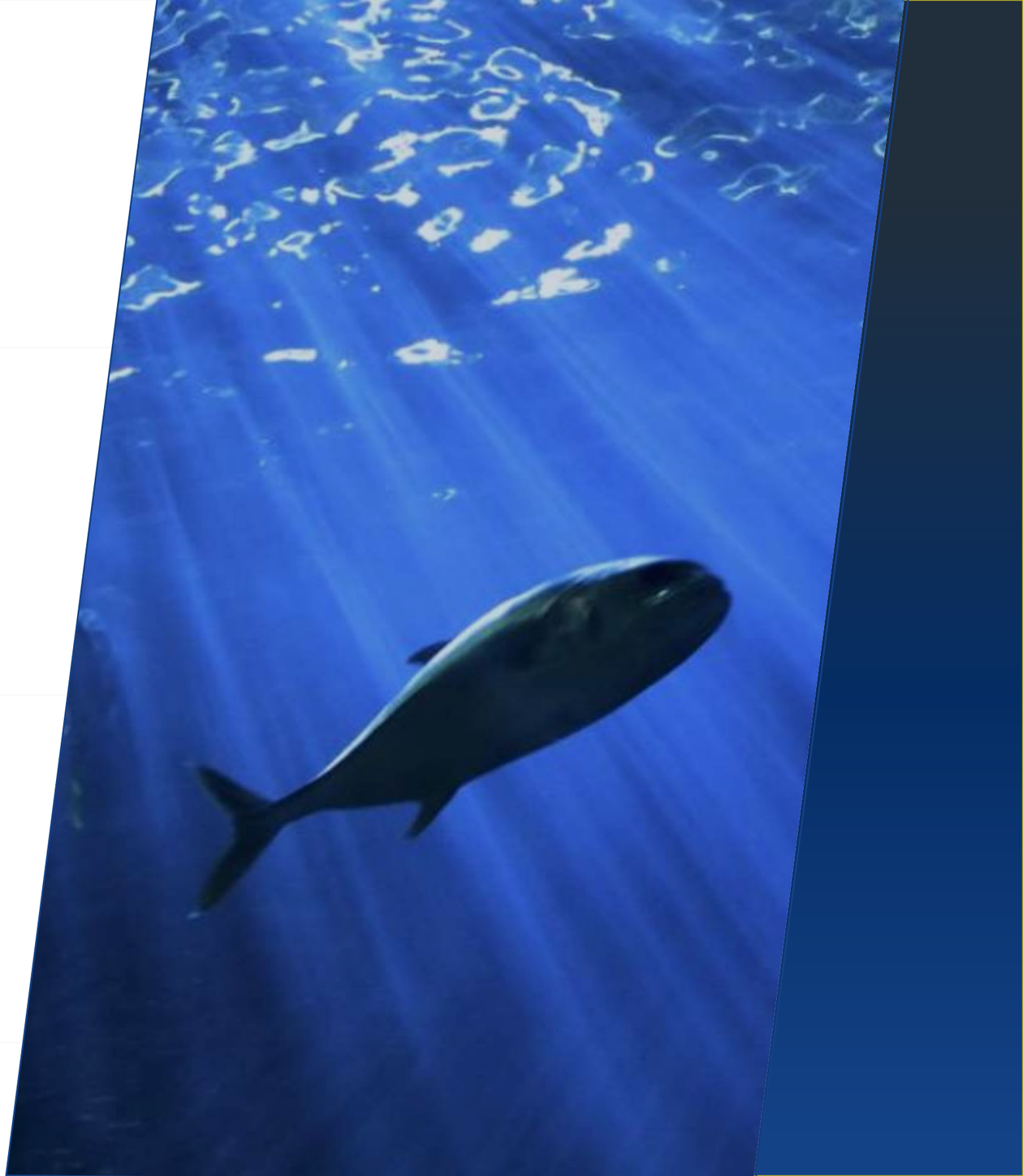
Phishing spersonalizowany, celowany

(ang. Spear phishing, whaling)

Precyzyjnie wybrany cel – osoba lub grupa; duży jednorazowy zysk.

Rozpoznanie celu i jego otoczenia; często atak na cele pośrednie.

Pretekst i historia ataku specjalnie przygotowane pod cel.



Manipulacja – wywoływanie silnych emocji

- Twoje konto zostało zablokowane!
- Musisz natychmiast dokonać opłaty!
- Potrzebna jest twoja pomoc!
- Twoim bliskim grozi niebezpieczeństwo!
- Kompromitujące cię materiały zostaną opublikowane!
- Wygrałaś na loterii!
- Okazja! Zyskasz dużo pieniędzy nie wychodząc z domu!




Co zrobić po otrzymaniu **każdej** wiadomości?

Zatrzymaj się.

Daj sobie czas na reakcję…

Oceń sytuację.

1. Kontekst wiadomości

Czy nakłania do podjęcia szybkich działań i wzbudza emocje?

2. Język wiadomości

Błędy gramatyczne, nietypowe sformułowania, literówki, akcent

3. Szata graficzna i „profesjonalne” zwroty

Nie daj się zwieść – logo, stopkę, format i kolorystykę łatwo podrobić!

4. Adres/numer nadawcy

Zwracaj szczególną uwagę na nazwę domenową. Uważaj na **spoofing !**

Podejmij decyzję, co zrobić.

Jeżeli masz wątpliwości, coś budzi Twoje podejrzenia:

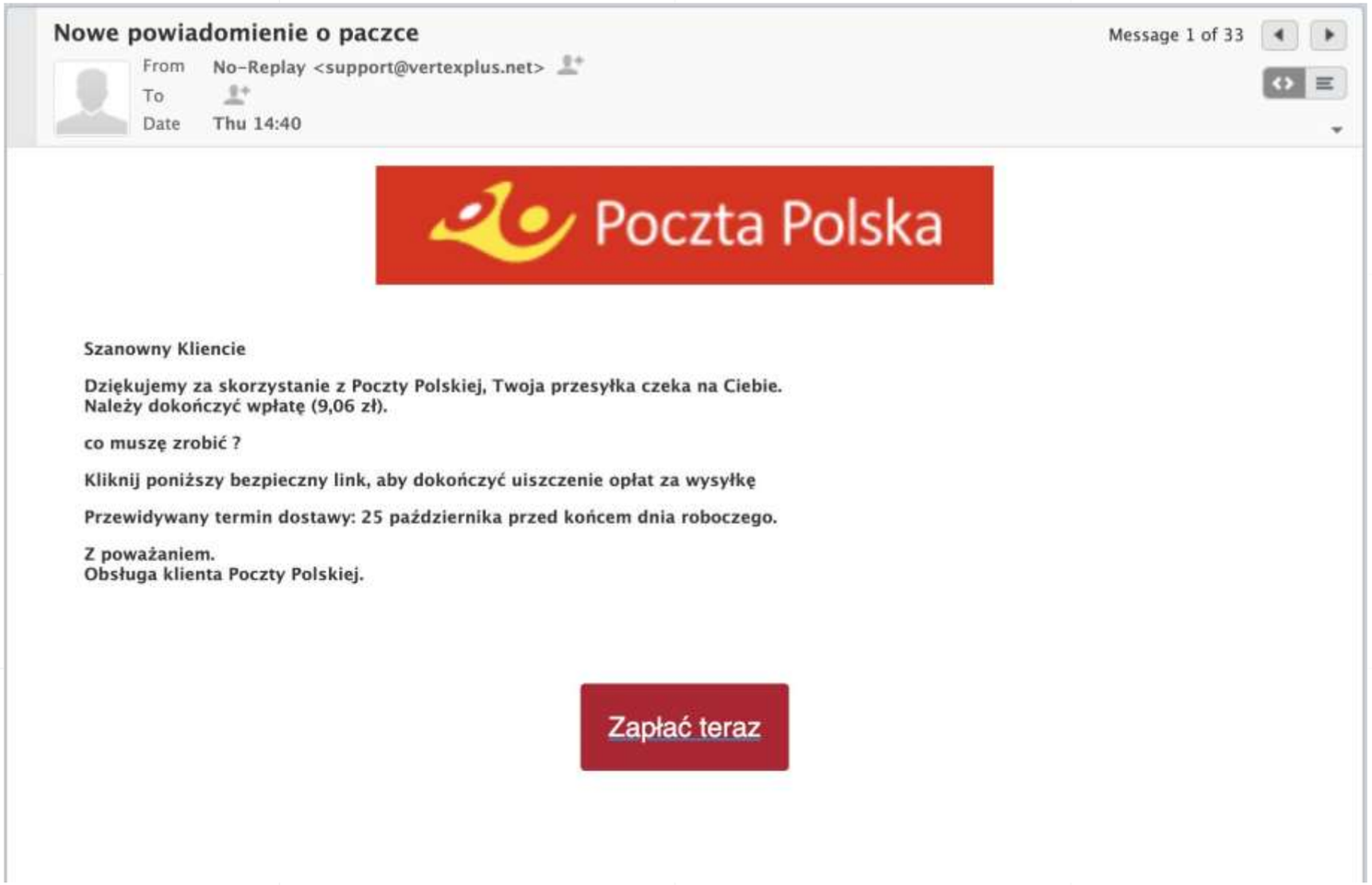
nie klikaj w linki.

nie pobieraj (i nie otwieraj!) załączników.

nie wdawaj się w dyskusję.

Phishing masowy

przykłady maili i SMSów phishingowych



- Uniwersalny pretekst
- „Zaufany nadawca”
- Czynnik wzbudzający emocje
- Link do strony

Co tu nie gra?

mBank

Dzień dobry,

z uwagi na brak spłaty kredytu nr 843843841 otrzymujesz odsetki karne.

Aby rozwiązać problem z odestkami zaloguj sie do banku.

Zaloguj się

W czasie braku spłaty nadal pobieramy odsetki karne za usługi dodatkowe z nim związane (zgodnie z taryfą prowizji i opłat).

Jeśli na rachunku masz Dopuszczalne Saldo Debetowe, które odnawia się w czasie wypowiedzenia, aby uniknąć opłaty za odnowienie, złóż dyspozycję rezygnacji.
Możesz to zrobić w dowolnej placówce.

Tę wiadomość wysłaliśmy automatycznie, prosimy nie odpowiadaj na nią.
Jeśli masz pytania, skontaktuj się z doradcą w placówce, Ekspertem online lub konsultantem mLinii.
Z pozdrowieniami,

zespół mBanku

Skontaktuj się z nami
Kliknij i zobacz, jak możesz to zrobić

Dbamy o Twoje bezpieczeństwo, dlatego część wysyłanych załączników zabezpieczamy hasłem.

czw. 08.12.2022 23:28

InPost <inpost605000716521@pl-e.jp>

Konieczne działanie ze względu na nieprawidłowy adres

Do

InPost .pl

Drogi Odbiorco,

Niniejszym chcielibyśmy poinformować, że nie udało nam się dzisiaj dostarczyć paczki nr 873234989001340872938732. Ponieważ była to ostatnia próba, paczka została zwrócona do głównego magazynu.

Przyczyną nieudanej próby dostarczenia jest:
Nieudane dostarczenie: brak danych adresowych

Korzystając z linku poniżej, możesz zgłosić kolejną próbę dostarczenia:

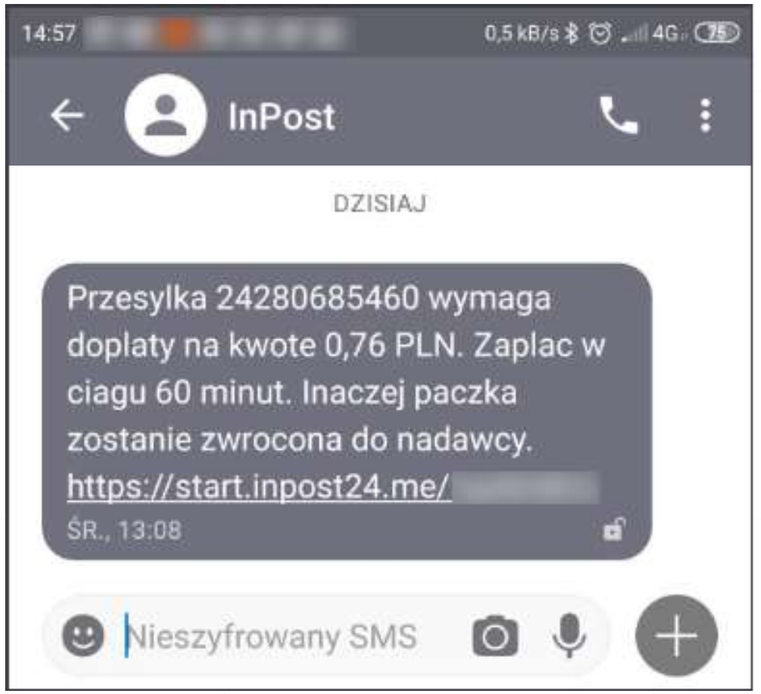
Zmiana adresu dostawy

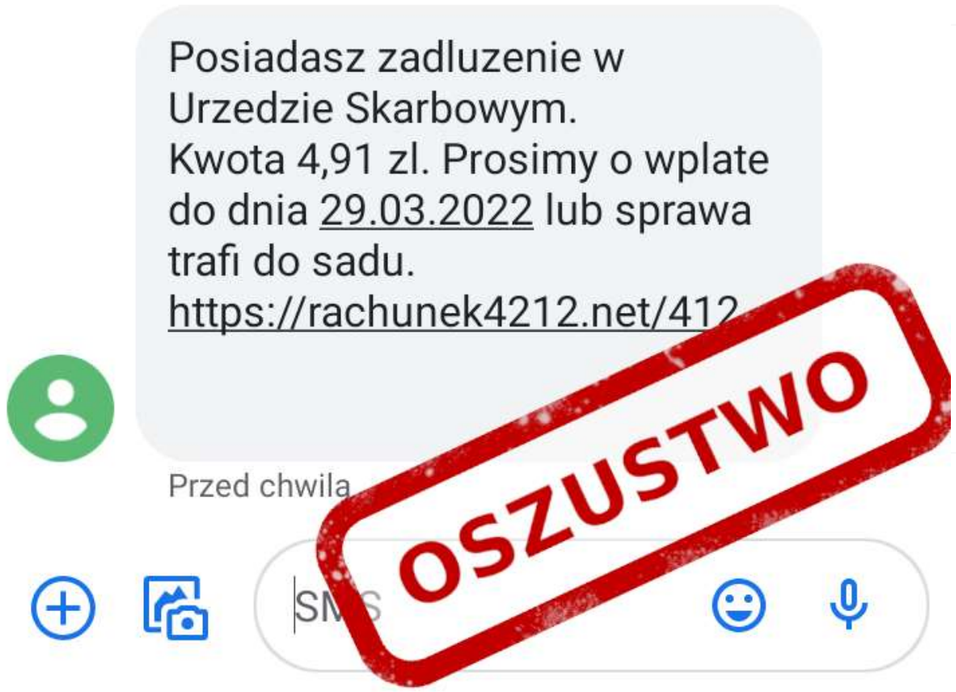
Pamiętaj, że pierwsza i druga próba dostarczenia były bezpłatne.
Za ponowne dostarczenie będą obowiązywać dodatkowe opłaty.
Możesz też wybrać odbiór osobisty z naszego magazynu do 09.12.2022.

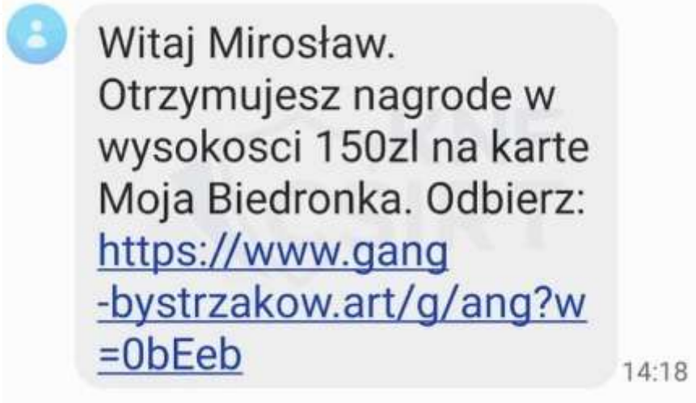
Jeśli potrzebujesz dalszej pomocy, skontaktuj się z nami za pomocą formularza kontaktowego na naszej stronie internetowej.
Jeśli nie powiadomisz nas o swojej decyzji, Twoja paczka zostanie zwrócona do nadawcy za dwa dni.

Jest to wiadomość automatyczna. Prosimy na nią nie odpowiadać.

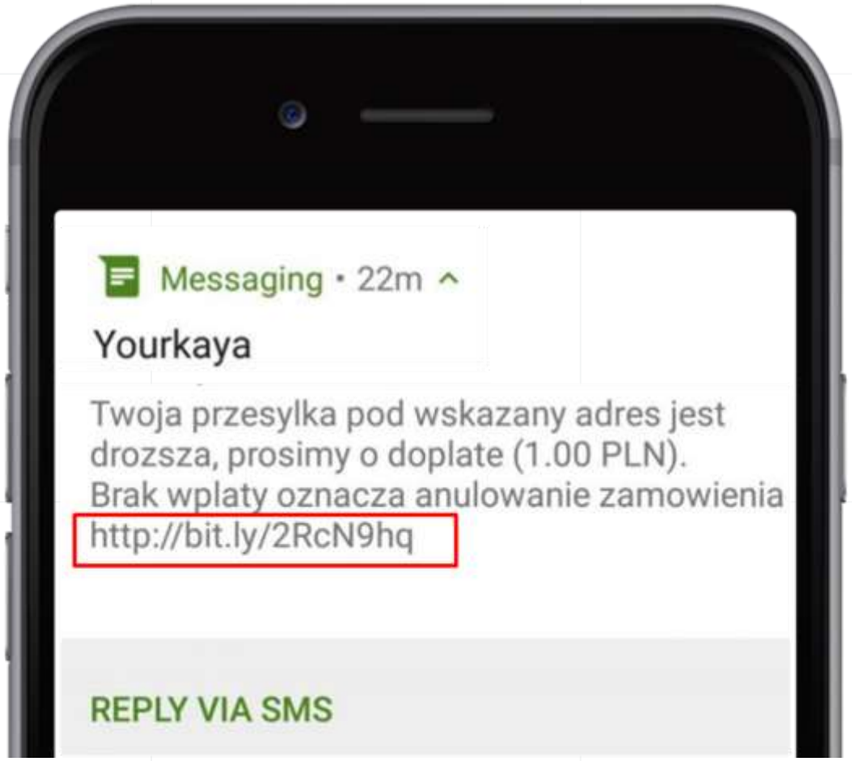
Pozdrawiamy,
InPost

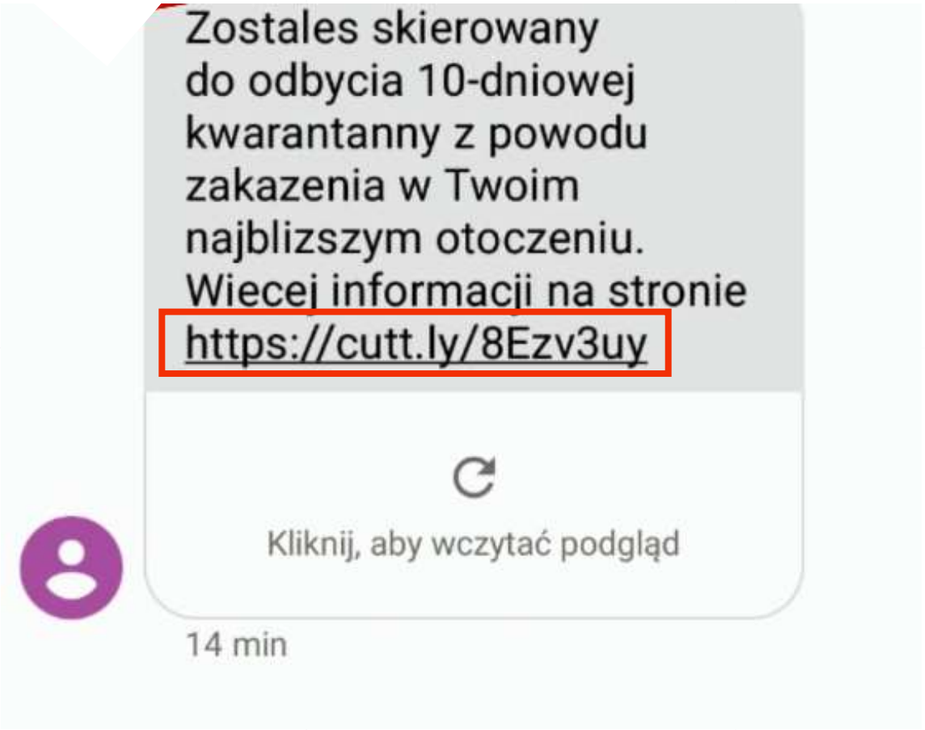



Posiadasz zadluzenie w Urzedzie Skarbowym. Kwota 4,91 zl. Prosimy o wplate do dnia 29.03.2022 lub sprawa trafi do sadu. https://rachunek4212.net/412
Przed chwila
SMS
OSZUSTWO

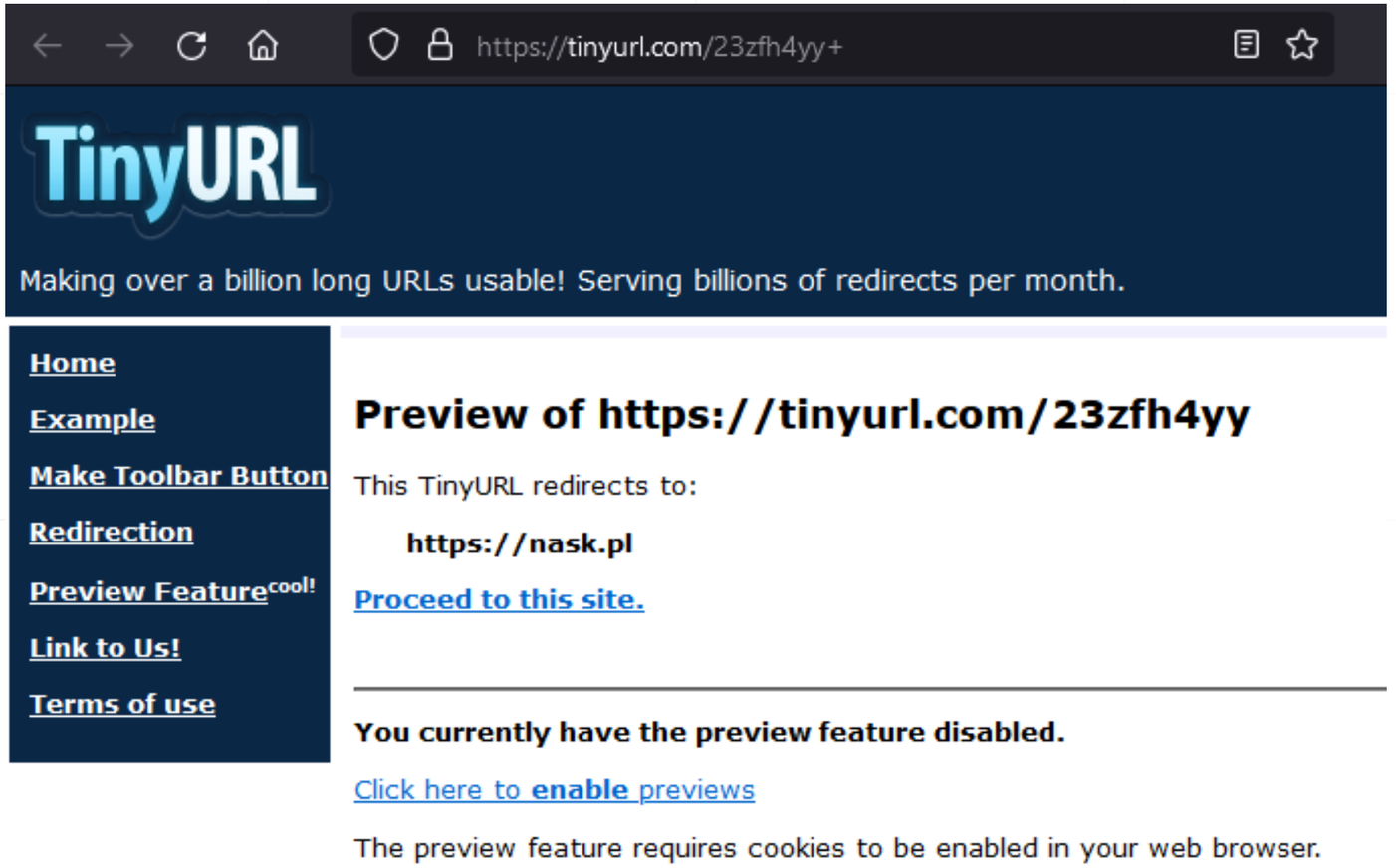

Witaj Mirosław. Otrzymujesz nagrode w wysokosci 150zl na karte Moja Biedronka. Odbierz: https://www.gang-bystrzakow.art/g/ang?w=0bEeb
14:18

Skracarki linków





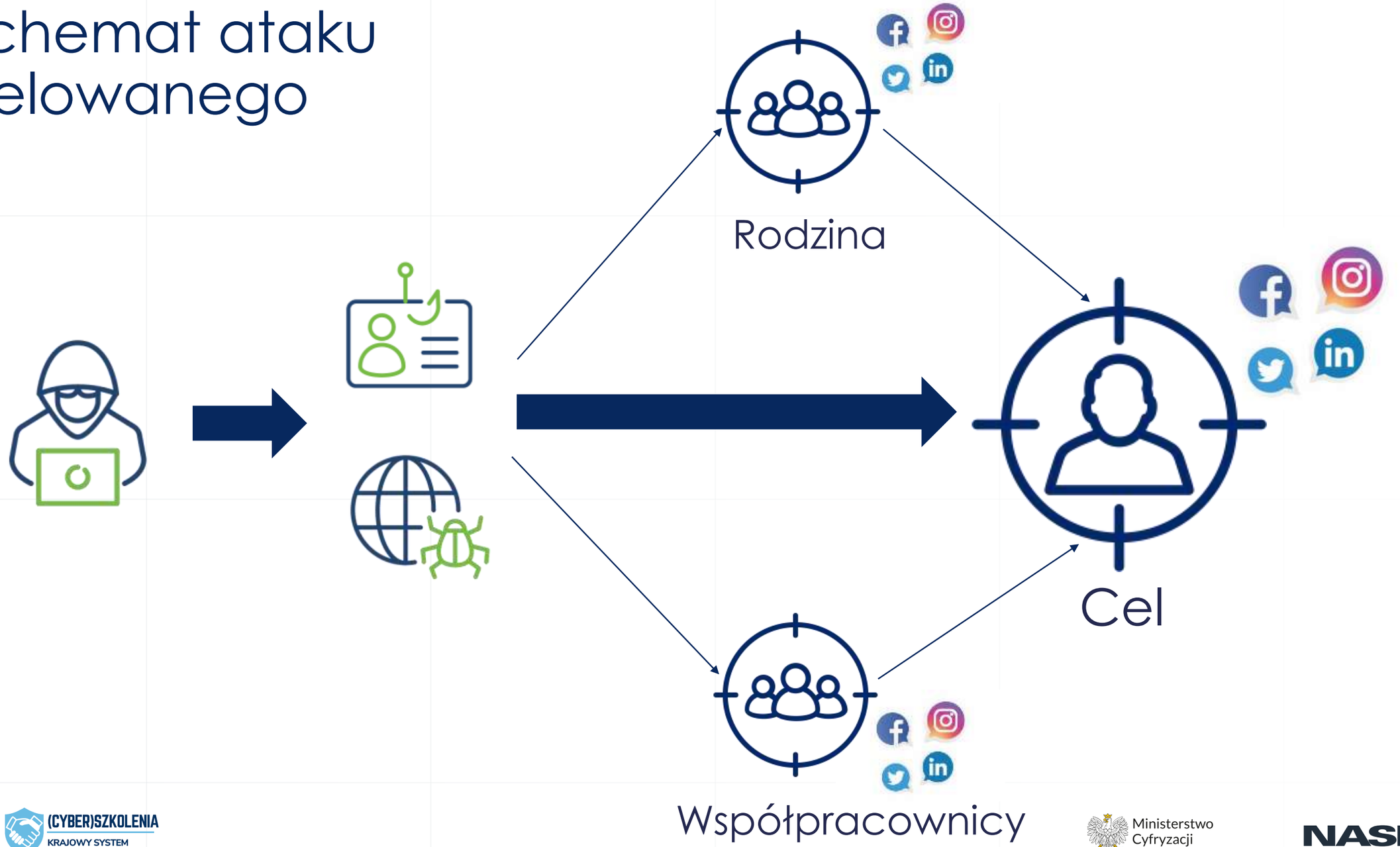
Sprawdzenie miejsca docelowego linku jest możliwe,
ale „uciążliwe”, szczególnie na telefonie.



Phishing spersonalizowany

spear phishing, czyli oszustwo szyte na miarę

Schemat ataku celowanego



Ataki na przedsiębiorstwa i korporacje

Wchodząca w skład Polskiej Grupy Zbrojeniowej, handlująca bronią spółka Cenzin, ofiarą międzynarodowego oszustwa. Jak dowiedzieli się reporterzy śledczy RMF FM, straty wynoszą około 4 milionów złotych.

W kilku transzach przelano na fałszywe konto 4 miliony złotych (zdj. ilustracyjne) /Pixabay

Spółka Cenzin - jak ustalili dziennikarze RMF FM - padła ofiarą tzw. phishingu. Do firmy przyszło kilka e-maili od osoby lub osób podszywających się pod czeskiego dostawcę broni.

polsatnews.pl » Polska

"Wydarzenia": oszuści okradli LOT. Przewoźnik przelał na ich konto 2,6 mln zł raty za samoloty

14.06.2019, 19:14 | Polska

Intermarche oszukane na 15 mln euro. Pieniądze trafiły na polskie konto

Sieć supermarketów Intermarche utraciła 15 mln euro na rzecz grupy oszustów, która przekonała jednego z pracowników firmy do przelania gigantycznej kwoty na konto, które miało rzekomo należeć do dyrektora generalnego Intermarche. Co ciekawe, pieniądze trafiły na konto w polskim banku - donosi "Retail Detail".

Ataki socjotechniczne na samorządy

Gmina padła ofiarą oszustwa, sprawę bada prokuratura

15-07-2021

Gmina Konstancin-Jeziorna w procesie lokowania wolnych środków finansowych na bankowej lokacie terminowej padła ofiarą oszustwa na kwotę 5 mln zł.

https://www.konstancinjeziorna.pl/news/gmina-padla-ofiara-oszustwa-sprawe-bada-prokuratura

Gmina oszukana na 5 milionów złotych

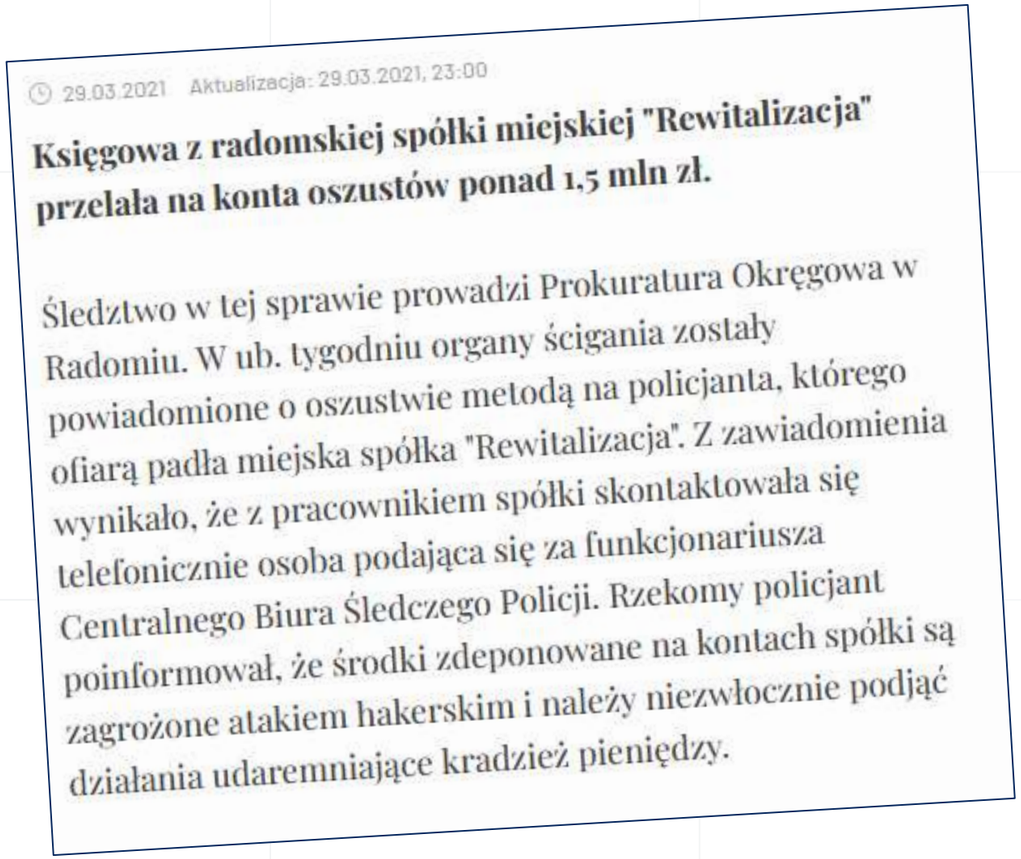
Przez **Redakcja** 7 maja 2021

Skarbnik Urzędu Gminy Rząśnia padła ofiarą oszustwa. Z gminnej kasy wyparowało 5 milionów złotych.

Prokuratura Rejonowa w Wieluniu prowadzi śledztwo w sprawie zuchwałego oszustwa, do jakiego doszło w Urzędzie Gminy w Rząśni. Z nieoficjalnych ustaleń wynika, że ze skarbnik Urzędu Gminy w Rząśni mieli kontaktować się oszuści, którzy skutecznie nakłonili ją do przelania na ich konto zawrotnej kwoty 5 milionów złotych.

https://twojepajeczno.pl/wiadomosci/powiat/gmina-oszukana-na-5-milionow-zlotych/

Ataki na organizacje



29.03.2021 Aktualizacja: 29.03.2021, 23:00

Księgowa z radomskiej spółki miejskiej "Rewitalizacja" przelała na konta oszustów ponad 1,5 mln zł.

Śledztwo w tej sprawie prowadzi Prokuratura Okręgowa w Radomiu. W ub. tygodniu organy ścigania zostały powiadomione o oszustwie metodą na policjanta, którego ofiarą padła miejska spółka "Rewitalizacja". Z zawiadomienia wynikało, że z pracownikiem spółki skontaktowała się telefonicznie osoba podająca się za funkcjonariusza Centralnego Biura Śledczego Policji. Rzekomy policjant poinformował, że środki zdeponowane na kontach spółki są zagrożone atakiem hakerskim i należy niezwłocznie podjąć działania udaremniające kradzież pieniędzy.

https://samorzad.pap.pl/kategoria/aktualnosci/prezes-oszukanej-spolki-miejskiej-twierdzi-ze-ksiegowa-robila-przelewy-bez

Cecha wspólna:

Działania niezgodne z wewnętrznymi procedurami

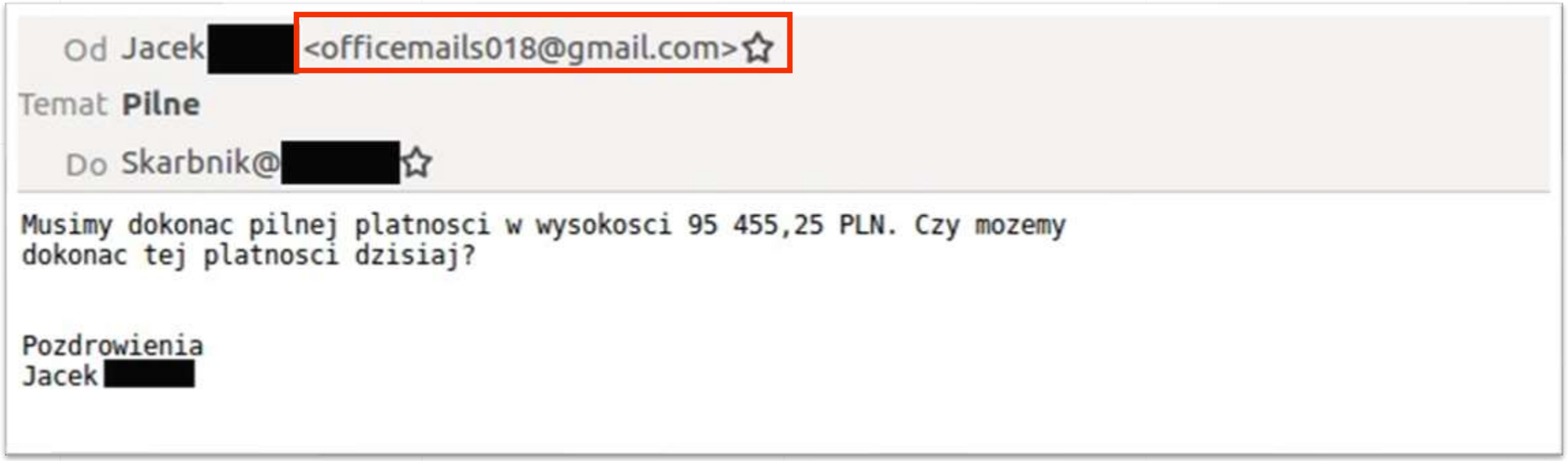
Konsekwencje:

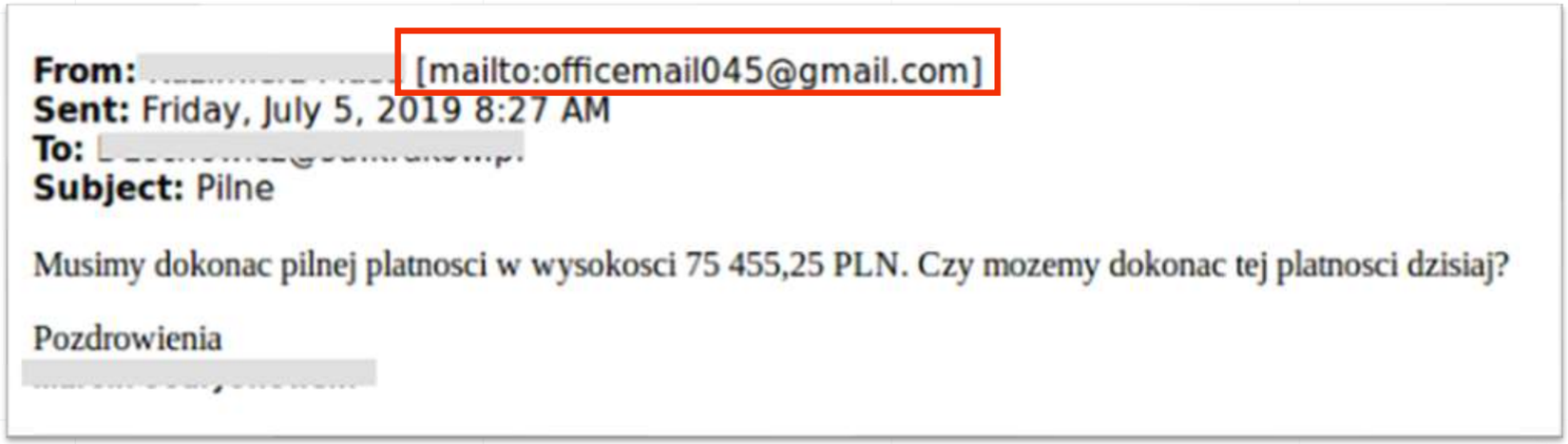
Narażenie organizacji na utratę pieniędzy

Pociągnięcie do odpowiedzialności, w tym zwolnienia dyscyplinarne.

Oszustwo „na dyrektora” / atak *BEC*

ang. Business E-mail Compromise

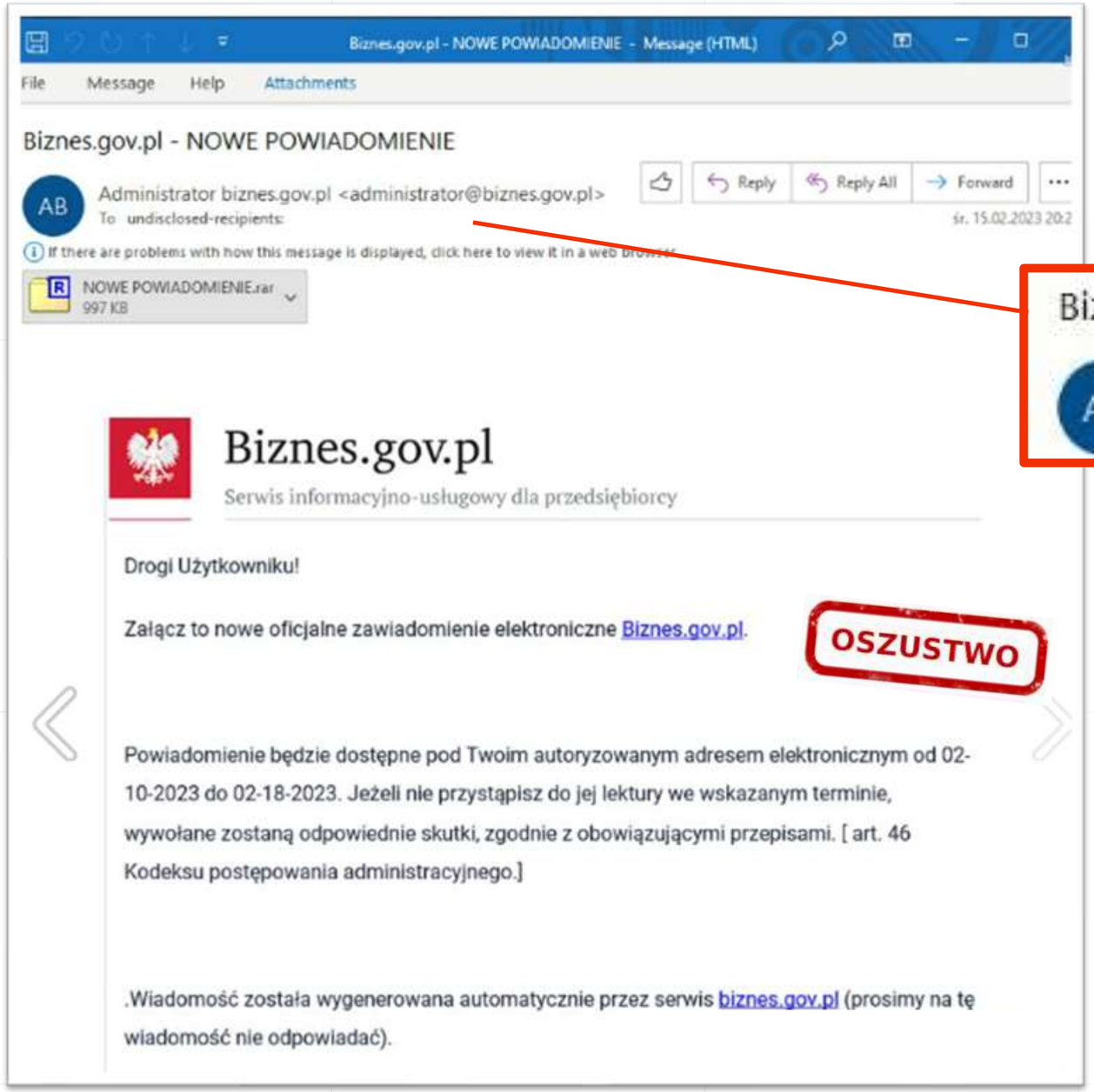




Spoofing
– podstawiony numer lub nazwa nadawcy

Znajomo wyglądający, poprawny numer telefonu, nazwa (nadpis) czy adres nadawcy – **może być sfałszowany**.

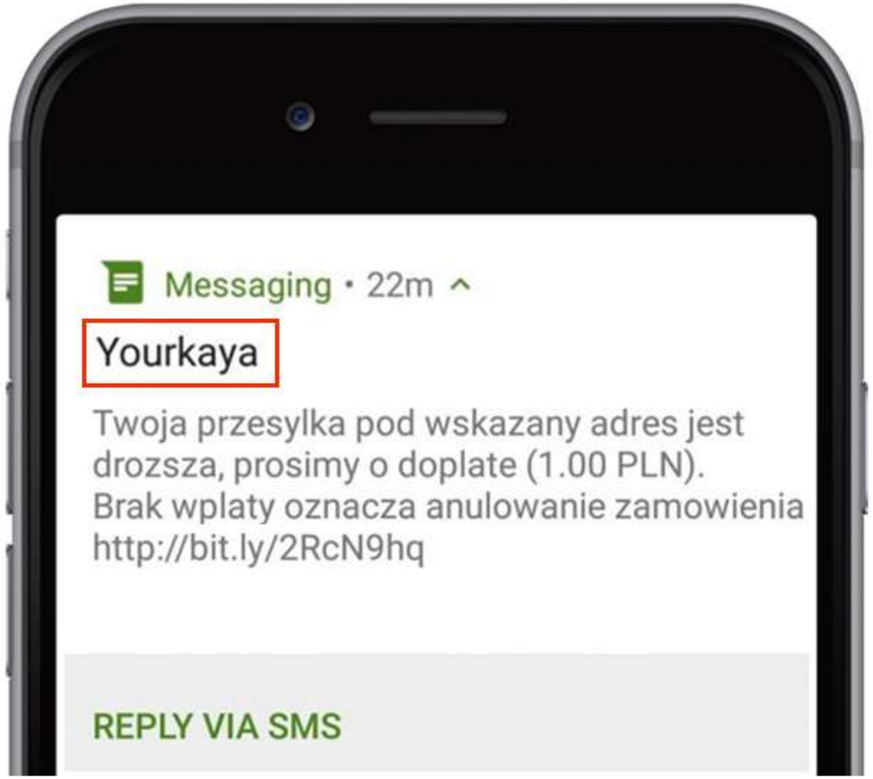
Spoofing mailowy



- Stosunkowo rzadko występuje, dzięki odpowiedniej konfiguracji usług pocztowych.
- Czasem przestępcy zamiast spoofingu korzystają z przejętych kont mailowych.

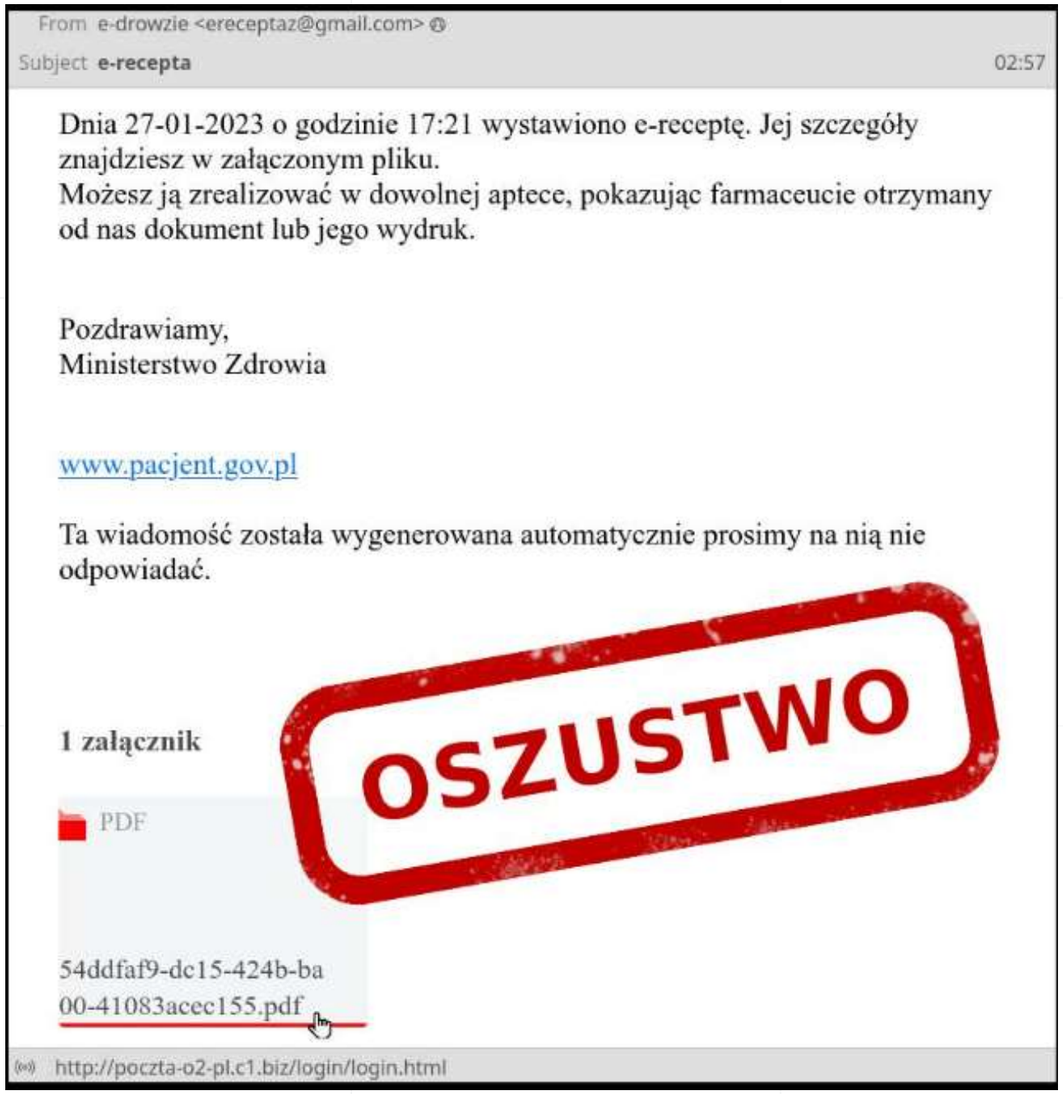
Spoofing telefoniczny

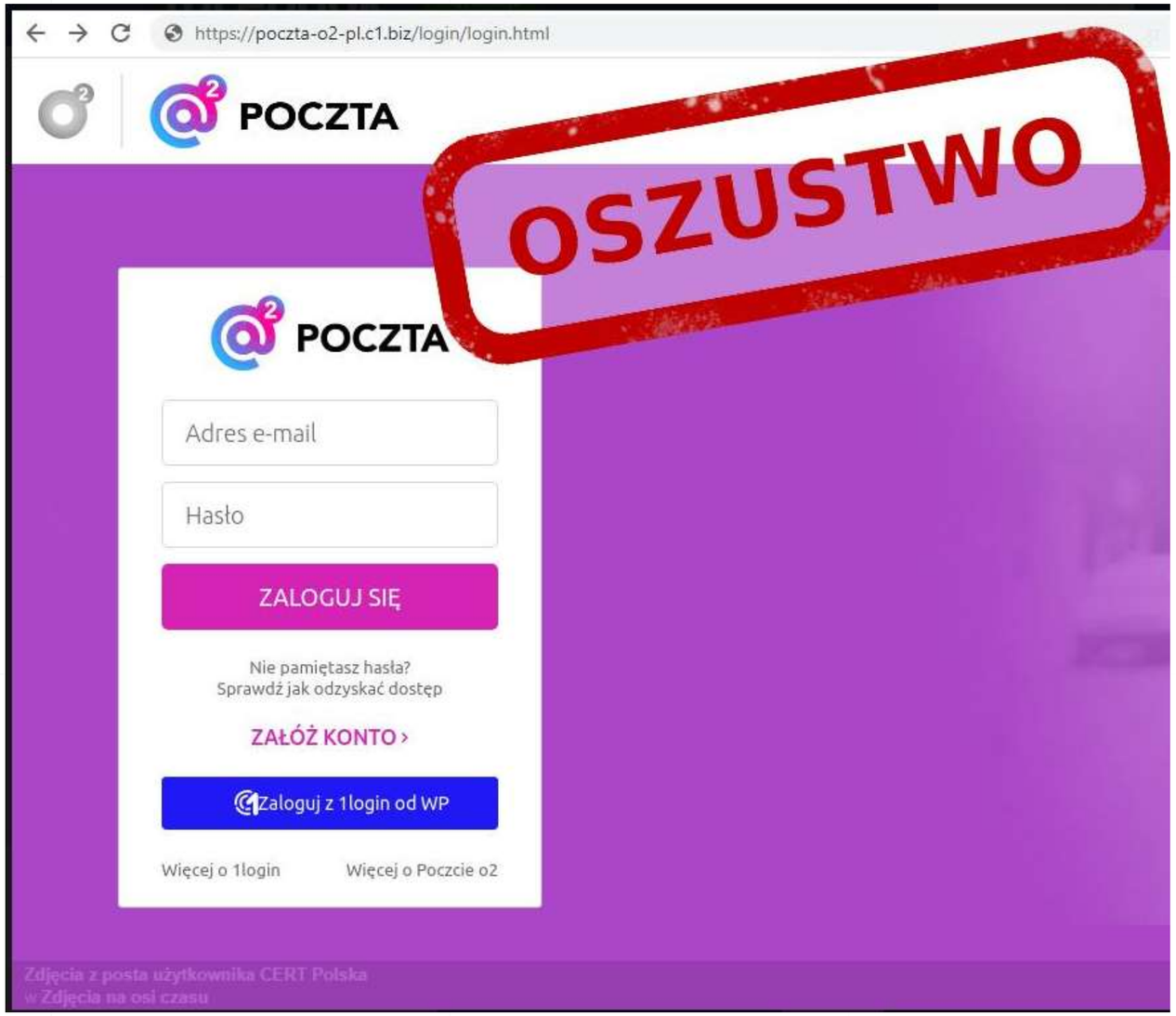
Występuje często!



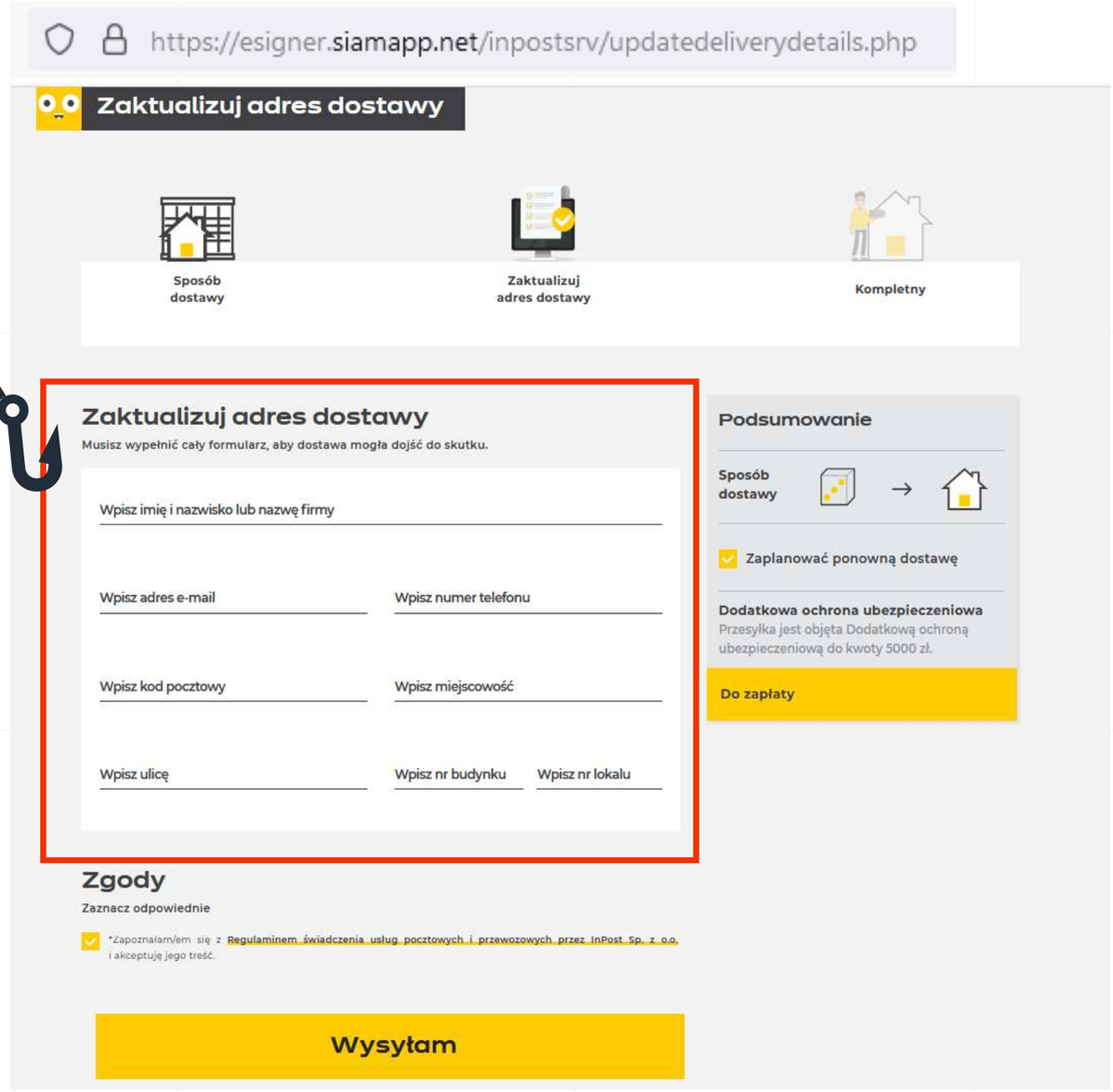
Co jeśli dasz się złapać?

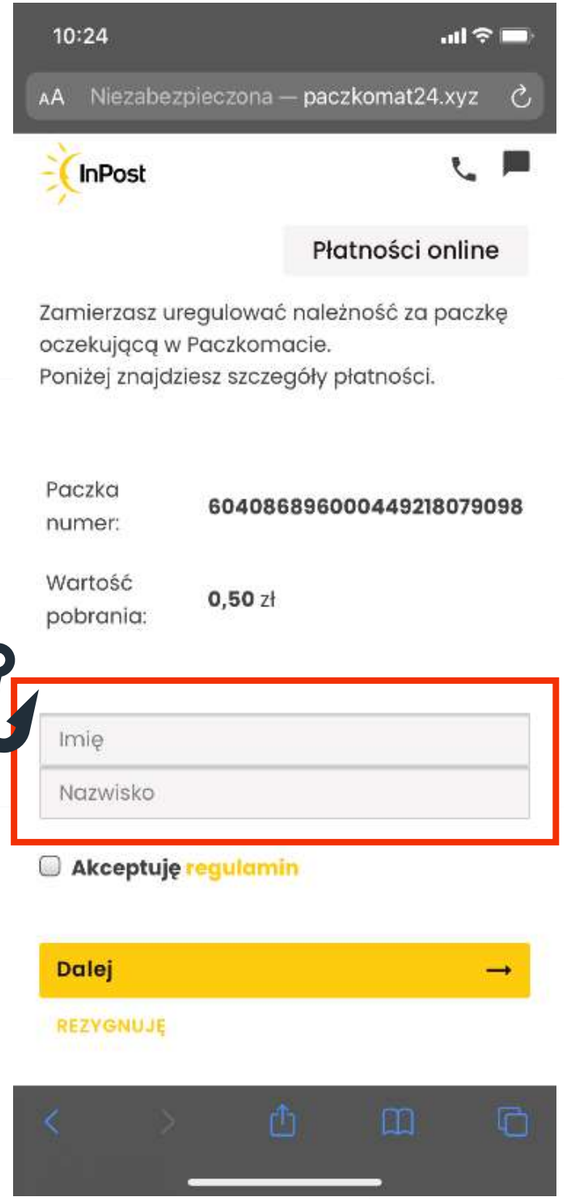
Phishing masowy – o co tak naprawdę chodzi…

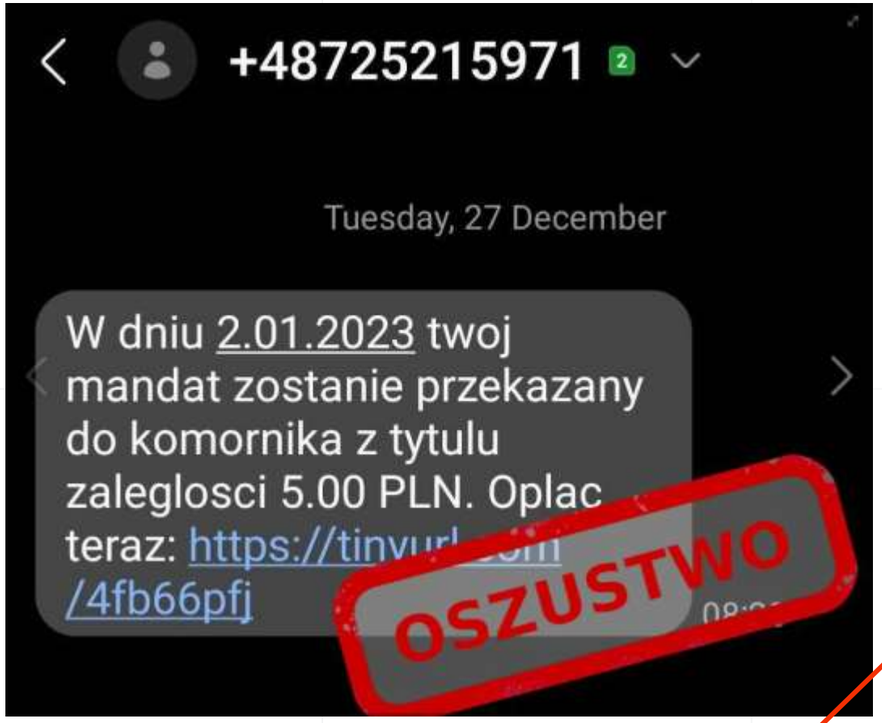

From e-drowzie <ereceptaz@gmail.com>
Subject e-recepta
02:57
Dnia 27-01-2023 o godzinie 17:21 wystawiono e-receptę. Jej szczegóły znajdziesz w załączonym pliku.
Możesz ją zrealizować w dowolnej aptece, pokazując farmaceucie otrzymany od nas dokument lub jego wydruk.
Pozdrawiamy,
Ministerstwo Zdrowia
www.pacjent.gov.pl
Ta wiadomość została wygenerowana automatycznie prosimy na nią nie odpowiadać.
1 załącznik
PDF
54ddfaf9-dc15-424b-ba00-41083acec155.pdf
http://poczta-o2-pl.c1.biz/login/login.html
OSZUSTWO

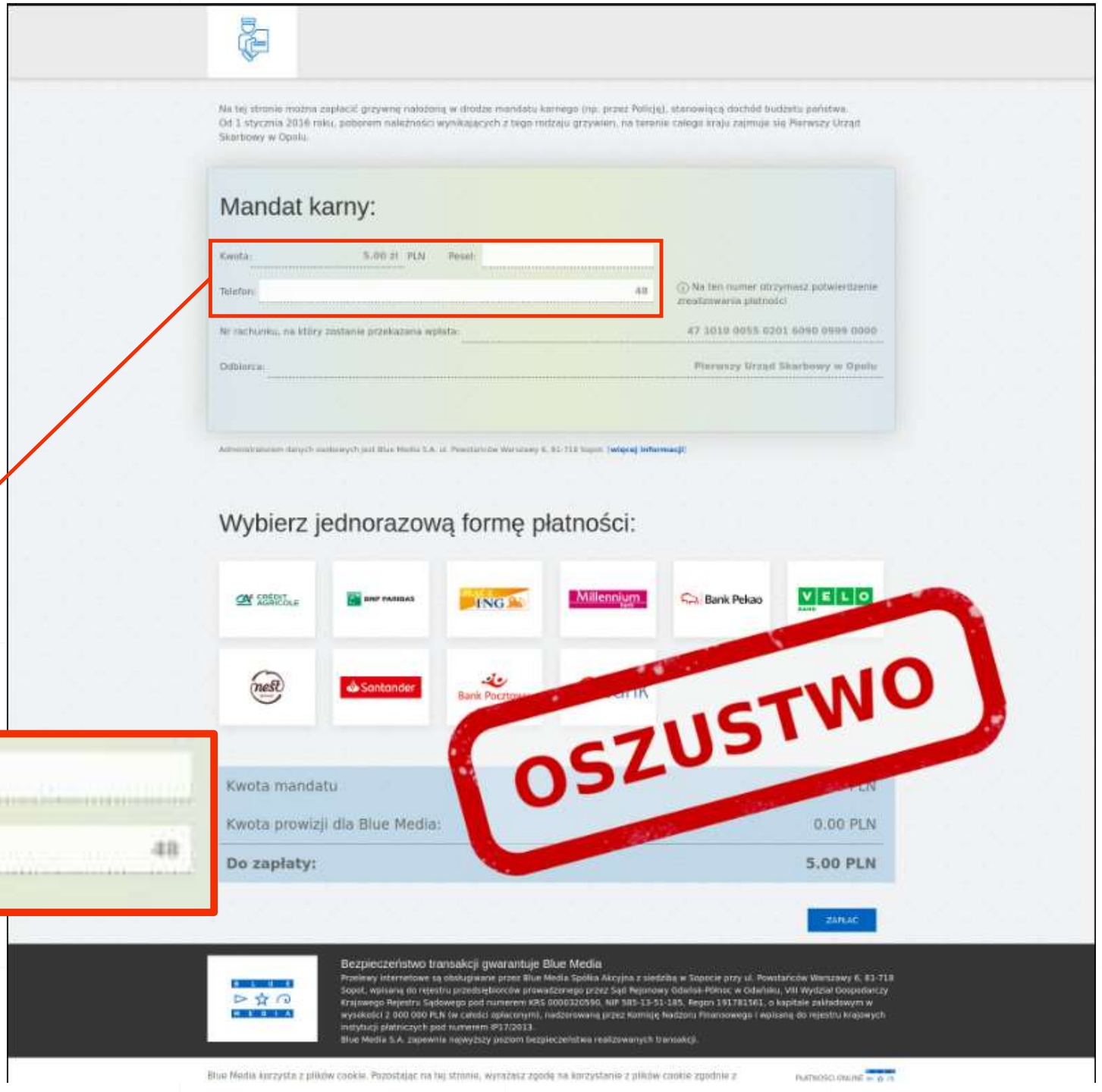

https://poczta-o2-pl.c1.biz/login/login.html
POCZTA
POCZTA
Adres e-mail
Hasło
ZALOGUJ SIĘ
Nie pamiętasz hasła?
Sprawdź jak odzyskać dostęp
ZAŁÓŻ KONTO ›
Zaloguj z 1login od WP
Więcej o 1login
Więcej o Poczcie o2
Zdjęcia z posta użytkownika CERT Polska
w Zdjęcia na osi czasu
OSZUSTWO

adamek**********@o2.pl	no**********
adam*********@o2.pl	12********
adame**********@o2.pl	me**********
adame***********@o2.pl	ad********
adamekwitk***********@o2.pl	fb**********
adame********@o2.pl	la**********
adamia**********@o2.pl	ku**********
adamia********@o2.pl	ly********


https://esigner.siamapp.net/inpostsrv/updatedeliverydetails.php
Zaktualizuj adres dostawy
Sposób dostawy
Zaktualizuj adres dostawy
Kompletny
Zaktualizuj adres dostawy
Musisz wypełnić cały formularz, aby dostawa mogła dojść do skutku.
Wpisz imię i nazwisko lub nazwę firmy
Wpisz adres e-mail
Wpisz numer telefonu
Wpisz kod pocztowy
Wpisz miejscowość
Wpisz ulicę
Wpisz nr budynku
Wpisz nr lokalu
Podsumowanie
Sposób dostawy
Zaplanować ponowną dostawę
Dodatkowa ochrona ubezpieczeniowa
Przesyłka jest objęta Dodatkową ochroną ubezpieczeniową do kwoty 5000 zł.
Do zapłaty
Zgody
Zaznacz odpowiednie
*Zapoznałam/em się z Regulaminem świadczenia usług pocztowych i przewozowych przez InPost Sp. z o.o. i akceptuję jego treść.
Wysyłam


10:24
AA Niezabezpieczona — paczkomat24.xyz
InPost
Płatności online
Zamierzasz uregulować należność za paczkę oczekującą w Paczkomacie.
Poniżej znajdziesz szczegóły płatności.
Paczka numer:
604086896000449218079098
Wartość pobrania:
0,50 zł
Imię
Nazwisko
Akceptuję regulamin
Dalej
REZYGNUJĘ

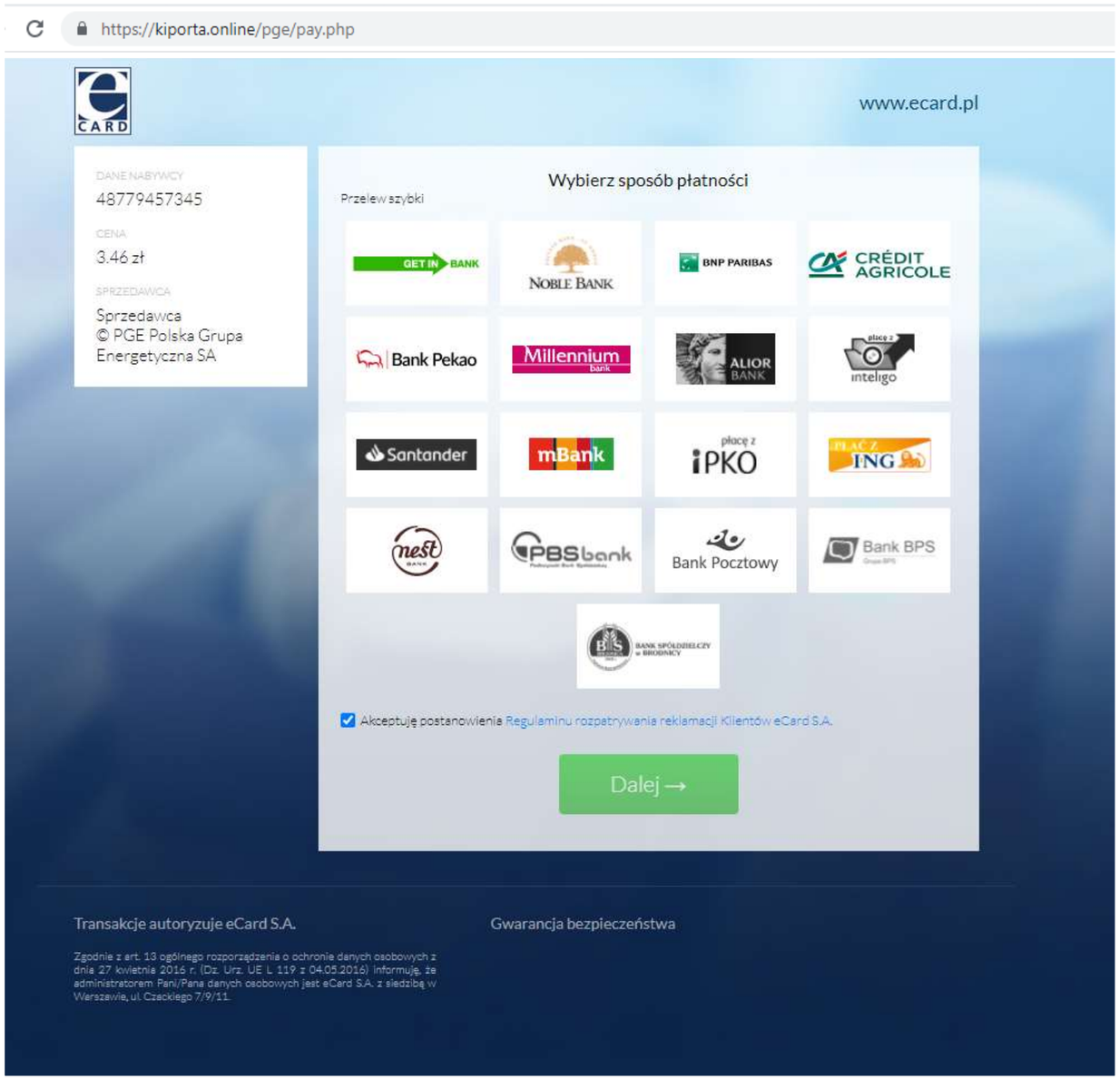


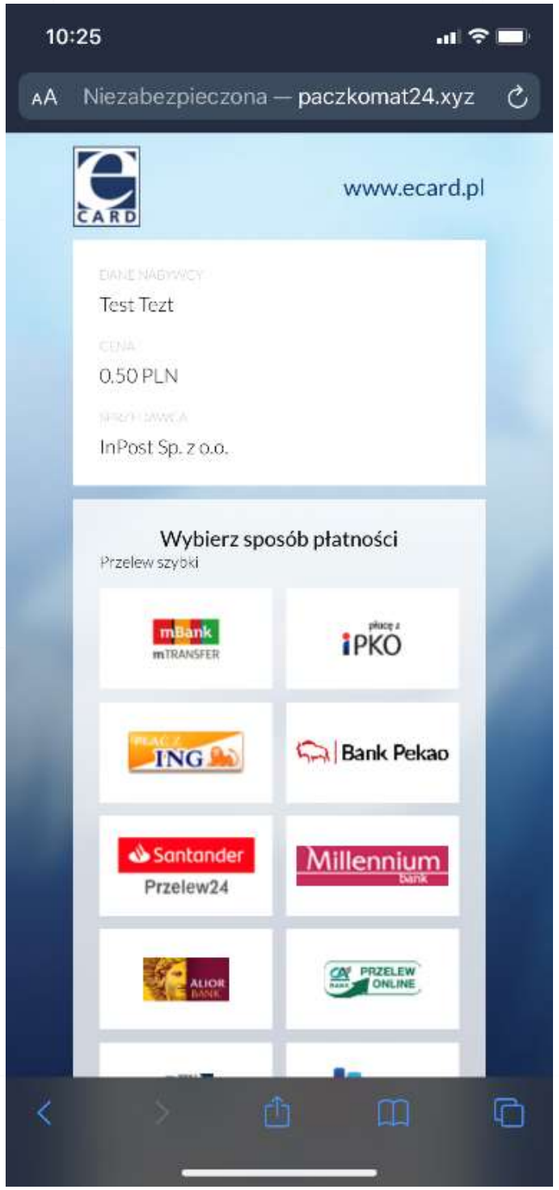


(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

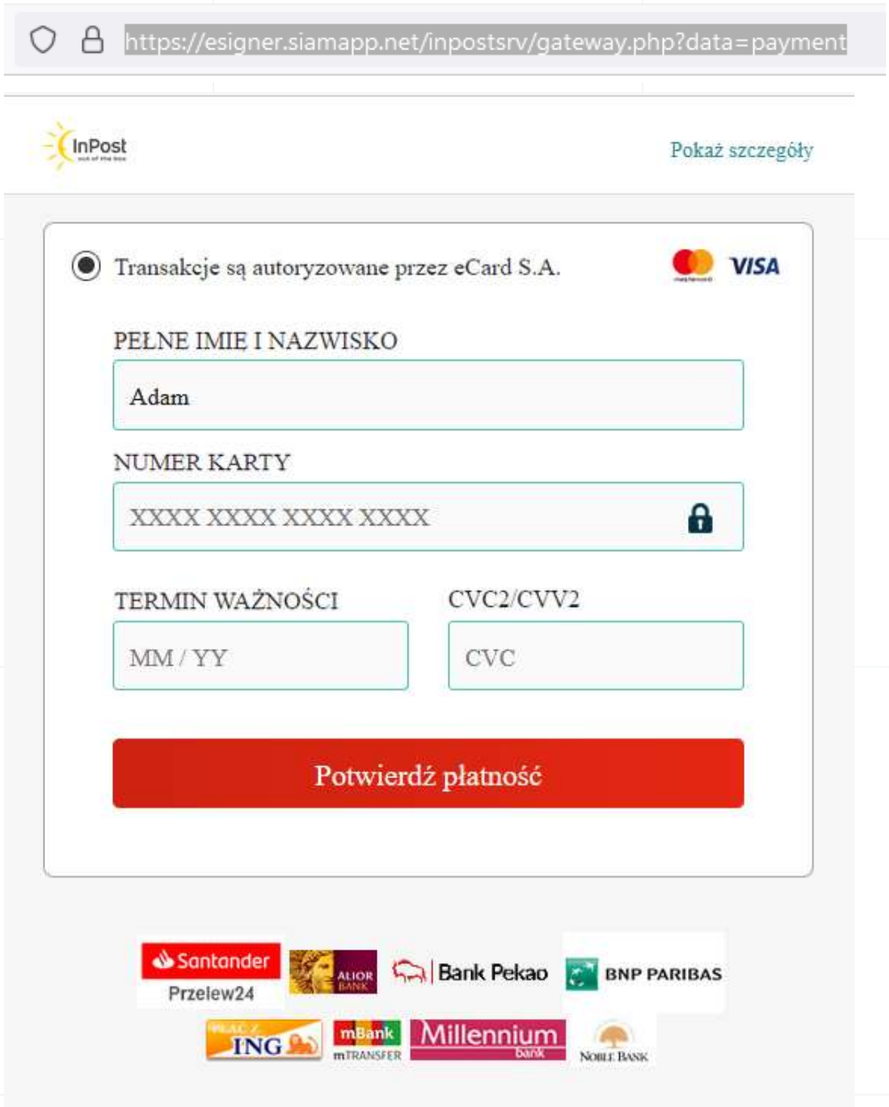
Fałszywe bramki e-płatności

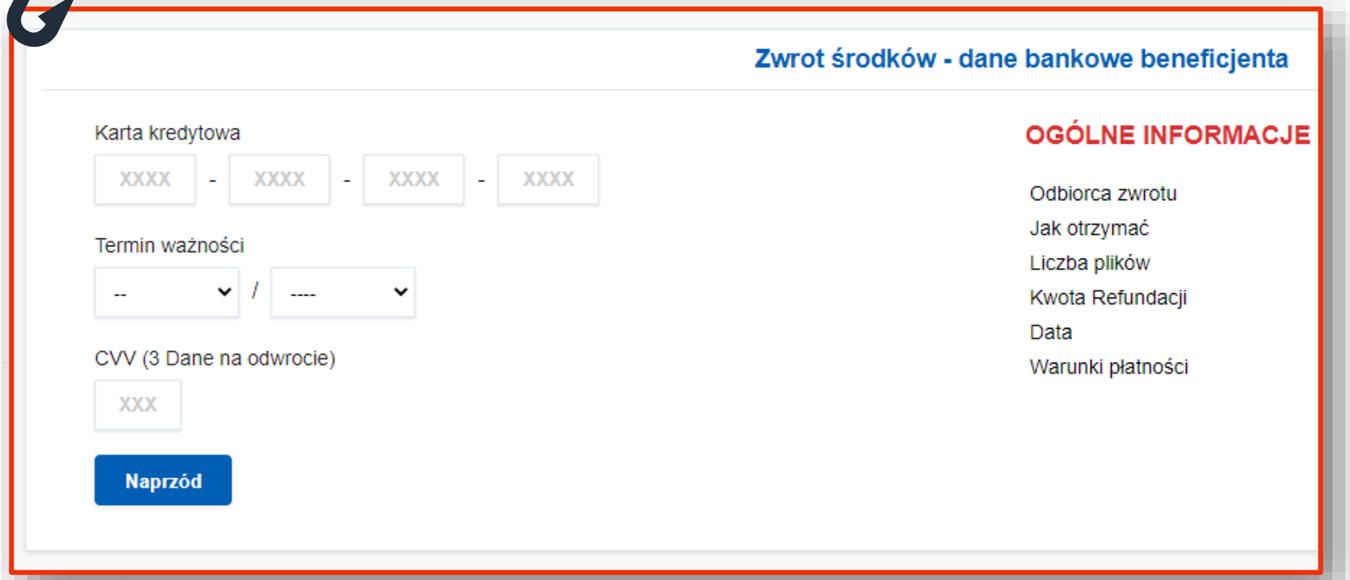
https://pay.ecard.pl/payment/choice





Fałszywe panele płatności kartą

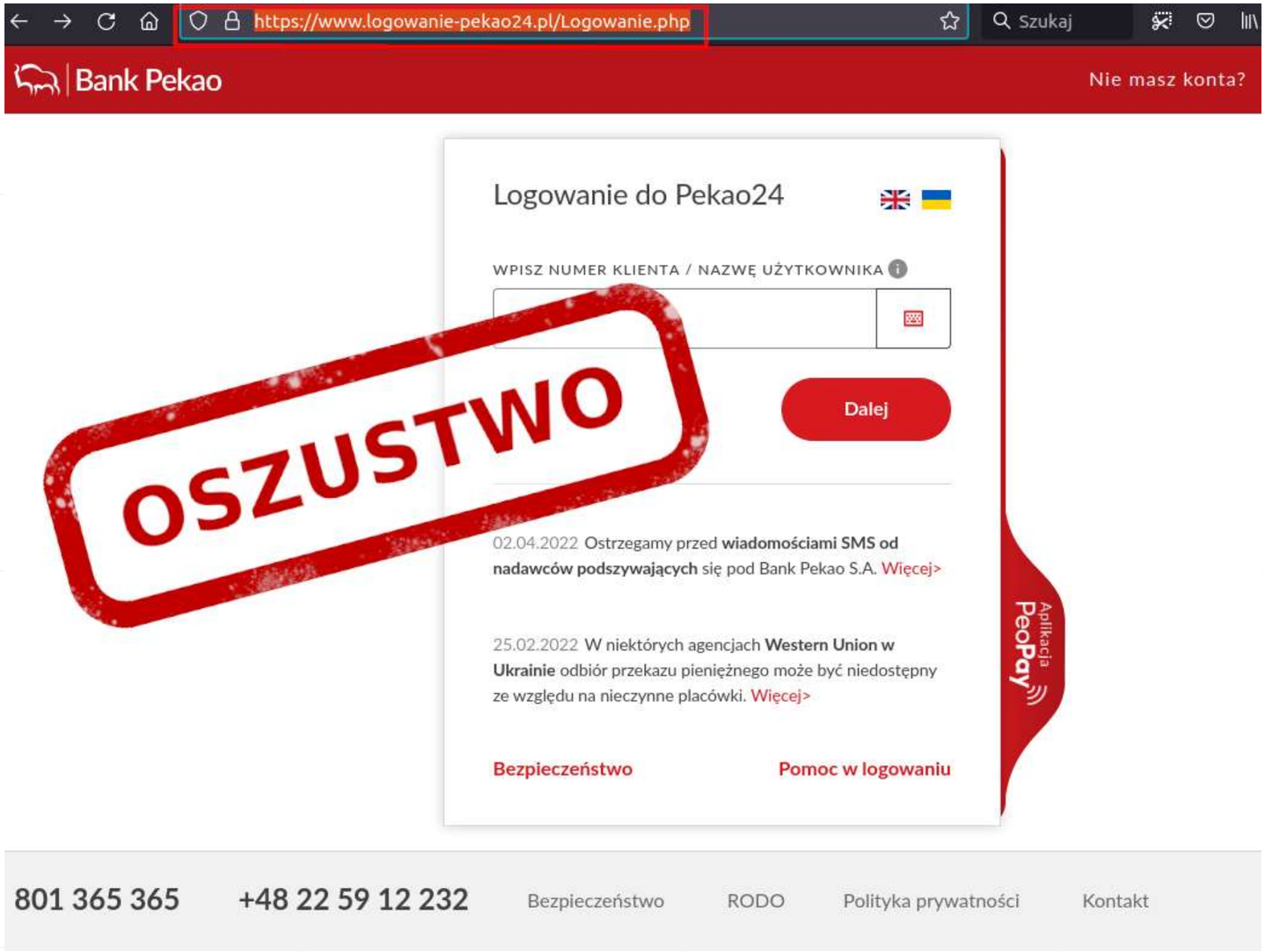


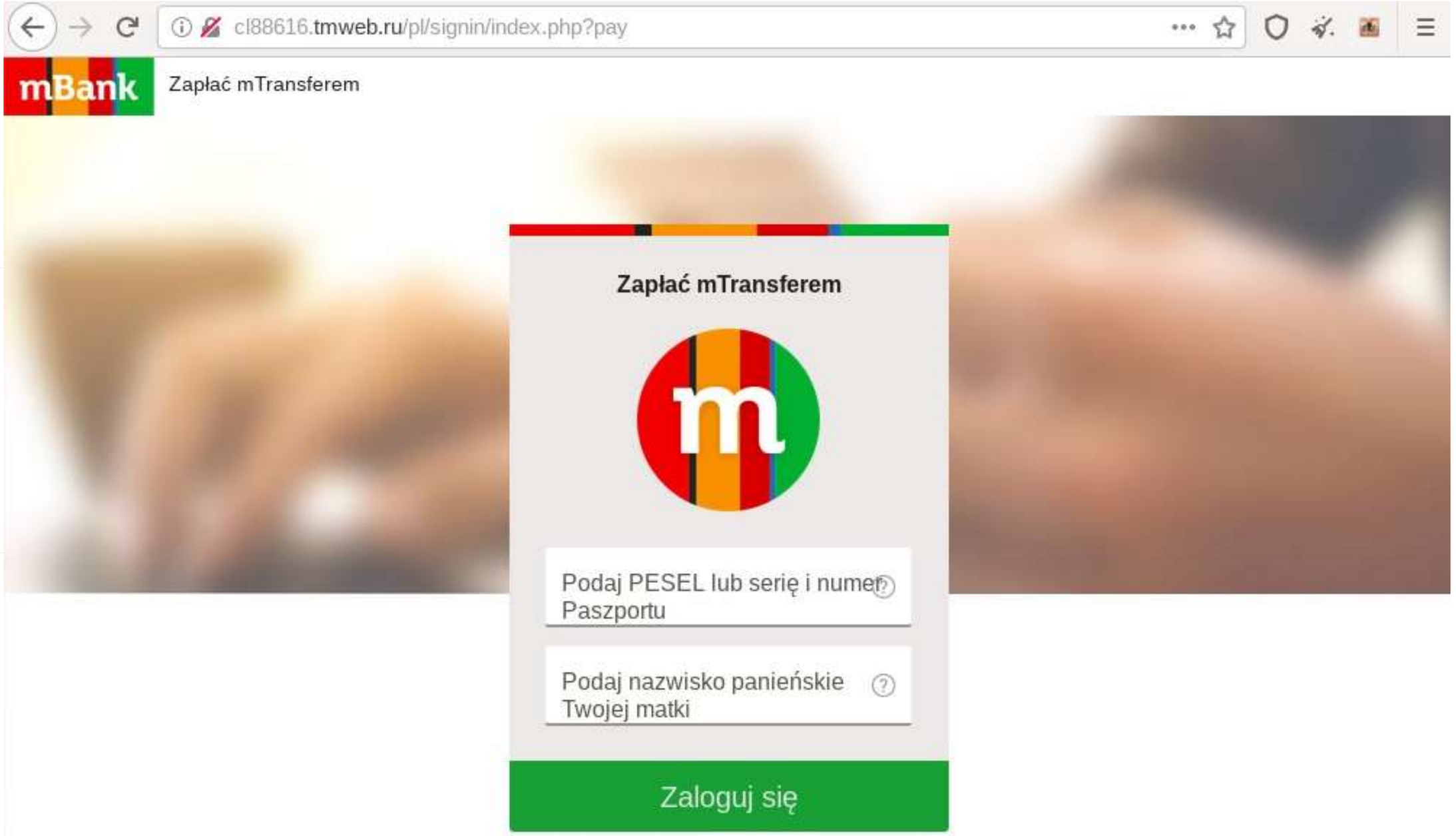


Paczka danych z kart płatniczych do kupienia od przestępców

Base	BIN	EXP	Info	zip	State	City	Country	Price
[03.07.2022] dispute MIX Refundable CVR 41%	557423	03/2024		34236	SA	Fl	Poland	10.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	557511	01/2024		UNKNOWN	NA	Zwoler...Bljh	Poland	16.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	516931	04/2026		84-200	UNKNOWN	Wejherowo	Poland	16.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	535473	07/2024		UNKNOWN	UNKNOWN	Torun	Poland	16.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	516745	01/2024		58-300	WA	Wa\U0142Brzych	Poland	16.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	557506	11/2022		UNKNOWN	UNKNOWN	UNKNOWN	Poland	16.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	435044	11/2024		34190	UNKNOWN	Saint-Bauzille-De-Putois	Poland	10.00 $
[03.07.2022] dispute MIX Refundable CVR 41%	442470	10/2024		60-819	NA	UNKNOWN	Poland	12.80 $
[03.07.2022] dispute MIX Refundable CVR 41%	424671	11/2024		24-100	PU	UNKNOWN	Poland	16.00 $
[12.06.2022] slogan MIX Refundable CVR 50%	535470	08/2024		62-065	ST	Grodzisk Wielkopolski	Poland	6.40 $
[12.06.2022] slogan MIX Refundable CVR 50%	435044	08/2025		43-300	UNKNOWN	Bielskobiaa	Poland	4.00 $
[12.06.2022] slogan MIX Refundable CVR 50%	516931	10/2022		UNKNOWN	UNKNOWN	UNKNOWN	Poland	6.40 $

Fałszywe panele logowania do banku




cl88616.tmweb.ru/pl/signin/index.php?pay
mBank
Zapłać mTransferem
Zapłać mTransferem
Podaj PESEL lub serię i numer Paszportu
Podaj nazwisko panieńskie Twojej matki
Zaloguj się

https://milenniumpl.com

Oszuści podszywają się pod Bank Millennium i informują o nowych "zabezpieczeniach" - nie klikaj w link i nie podawaj danych

KLIENCI INDYWIDUALNI PRESTIGE BANKOWOŚĆ PRYWATNA FIRMY PRZEDSIĘBIORSTWA

A A

Millennium bank

Wpisz, czego szukasz

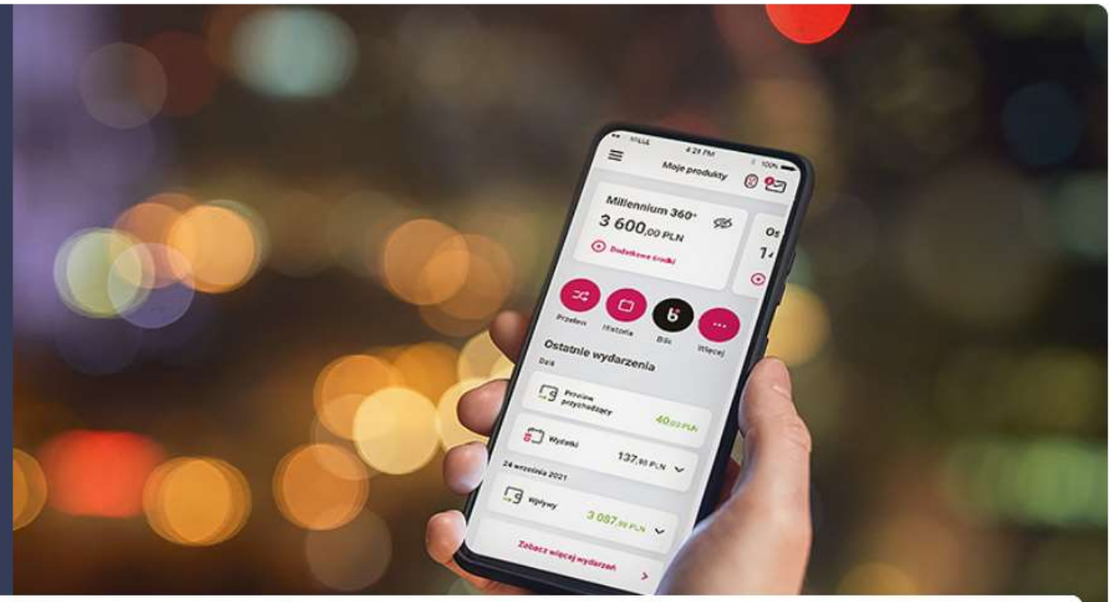
POŻYCZ GOTÓWKĘ ZAŁÓŻ KONTO LOGOWANIE

Konta Karty Kredyty Oszczędności Inwestycje Ubezpieczenia Bankowość elektroniczna Wsparcie Kontakt

Otwórz się na **nowe możliwości**

Wybierz konto Millennium 360° z innowacyjną aplikacją

ZAŁÓŻ TERAZ DOWIEDZ SIĘ WIĘCEJ Nota prawna



MILLENNIUM 360°

Prowadzone zawsze za 0 zł

KARTA IMPRESJA (RRSO 25,68%)

Loteria do 5.01.2023

POŻYCZKA GOTÓWKOWA (RRSO 12,83%)

Promocja do 20 stycznia 2023

ZWROTY ZA ZAKUPY

Przemyślany sposób na zakupy

Phishing a popularne usługi

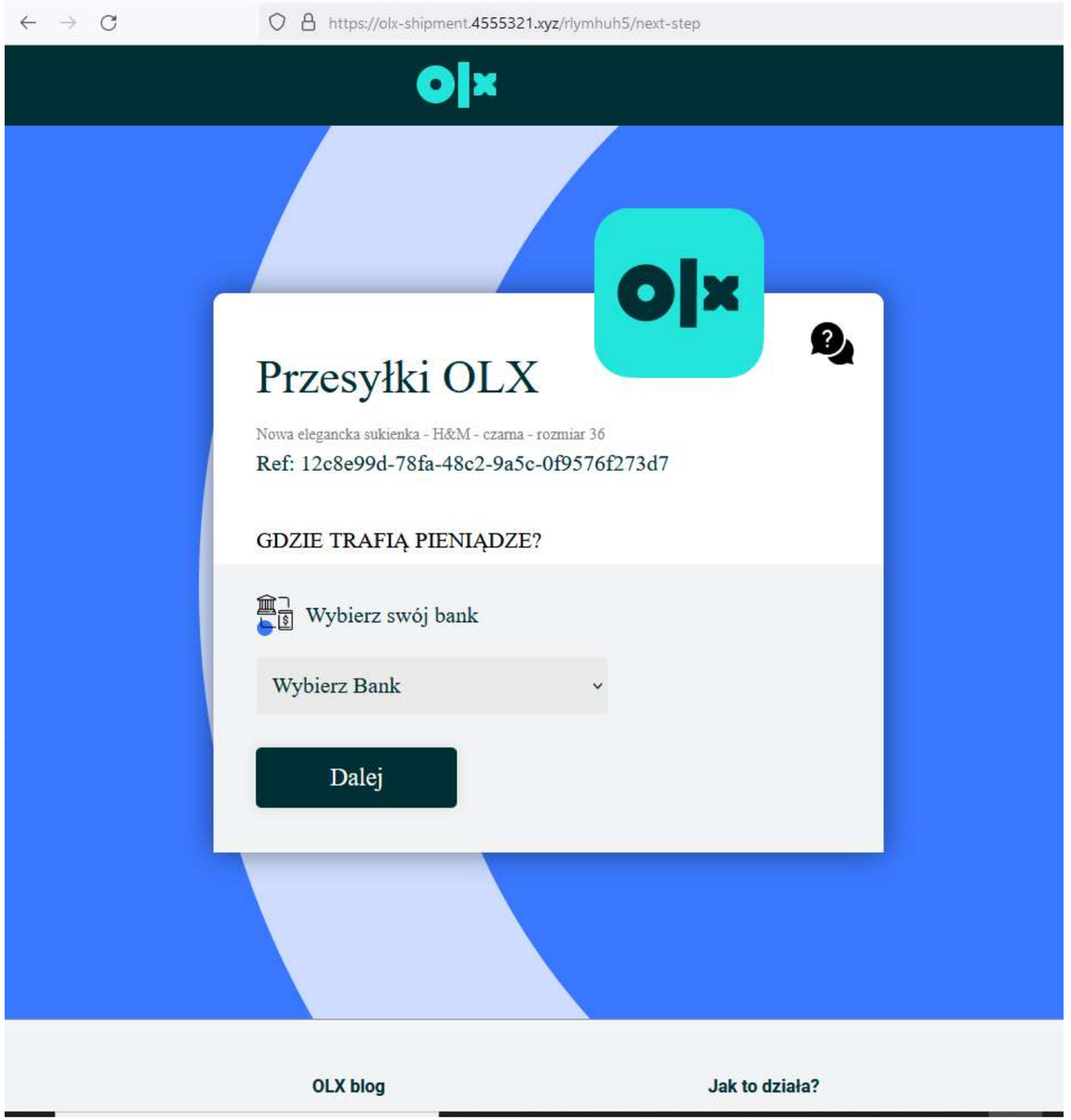
czyli częsty pretekst w phishingu masowym

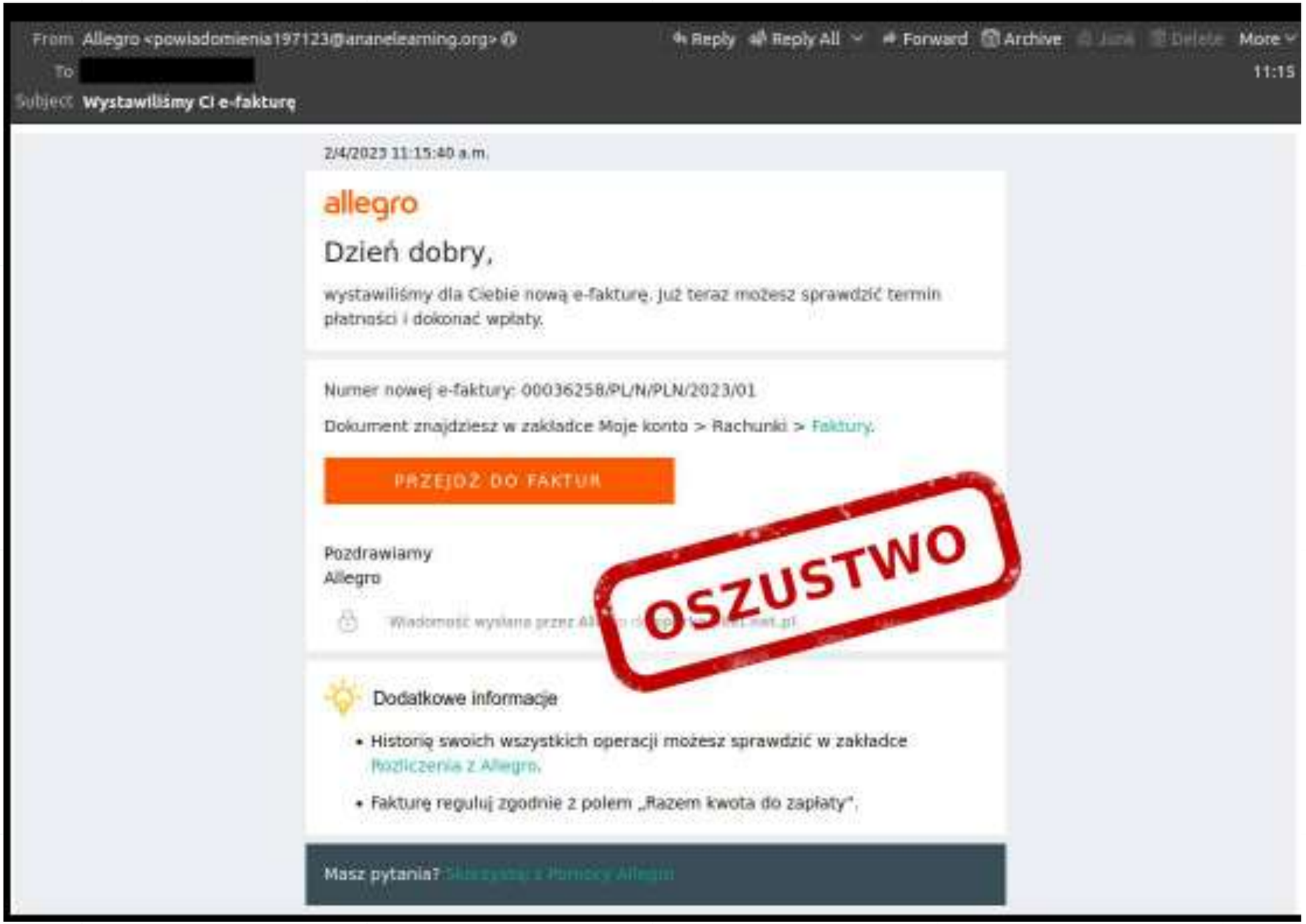
(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK


Olx
niedziela, 26 lutego 2023
Państwa przedmiot został zakupiony poprzez "Kup teraz" na OLX. Kupujący zapłacił za dostawę i towar. Kliknij na link, pod którym otrzymasz zapłatę za przedmiot i etykietę:
https://id-38965.icu/3aNseq0
12:16


https://olx-shipment.4555321.xyz/rlymhuh5/next-step
Przesyłki OLX
Nowa elegancka sukienka - H&M - czarna - rozmiar 36
Ref: 12c8e99d-78fa-48c2-9a5c-0f9576f273d7
GDZIE TRAFIĄ PIENIĄDZE?
Wybierz swój bank
Wybierz Bank
Dalej
OLX blog
Jak to działa?


From Allegro <powiadomienia197123@aranelearning.org>
Reply
Reply All
Forward
Archive
Junk
Delete
More
To
11:15
Subject Wystawiliśmy Ci e-fakturę
2/4/2023 11:15:40 a.m.
allegro
Dzień dobry,
wystawiliśmy dla Ciebie nową e-fakturę. Już teraz możesz sprawdzić termin płatności i dokonać wpłaty.
Numer nowej e-faktury: 00036258/PLN/PLN/2023/01
Dokument znajdziesz w zakładce Moje konto > Rachunki > Faktury.
PRZEJDŹ DO FAKTUR
Pozdrawiamy
Allegro
OSZUSTWO
Dodatkowe informacje
• Historię swoich wszystkich operacji możesz sprawdzić w zakładce Rozliczenia z Allegro.
• Fakturę reguluj zgodnie z polem „Razem kwota do zapłaty".
Masz pytania?

https://vintedl-polska29742dellfns.homedeliverypl007.icu/?idadvertise=3696&idproduct=2353182057&receivingfunds=5448993346

Vinted | Przedmioty | Szukaj przedmiotów | Sprzedaj teraz | PL

Kobiety | Mężczyźni | Dzieci | Dom | Rozrywka | Zwierzęta | O Vinted

Kupujący już zapłacił za Twój przedmiot.

Odbierz swoje pieniądze teraz

Suknia sprzedam

250.0 PLN

Twój przedmiot jest opłacony

Imię i nazwisko kupującego!

Anna Wuychik

Adres dostawy

Lodz Poland

Jak tylko otrzymasz pieniądze na kartę, kurier skontaktuje się z Tobą. Konieczne jest wskazanie dogodnego terminu przekazania towaru.

Przekazanie towaru musi nastąpić w ciągu tygodnia od daty otrzymania środków.

InPost | ORLEN | dpd

Numer ogłoszenia: **2353182057**

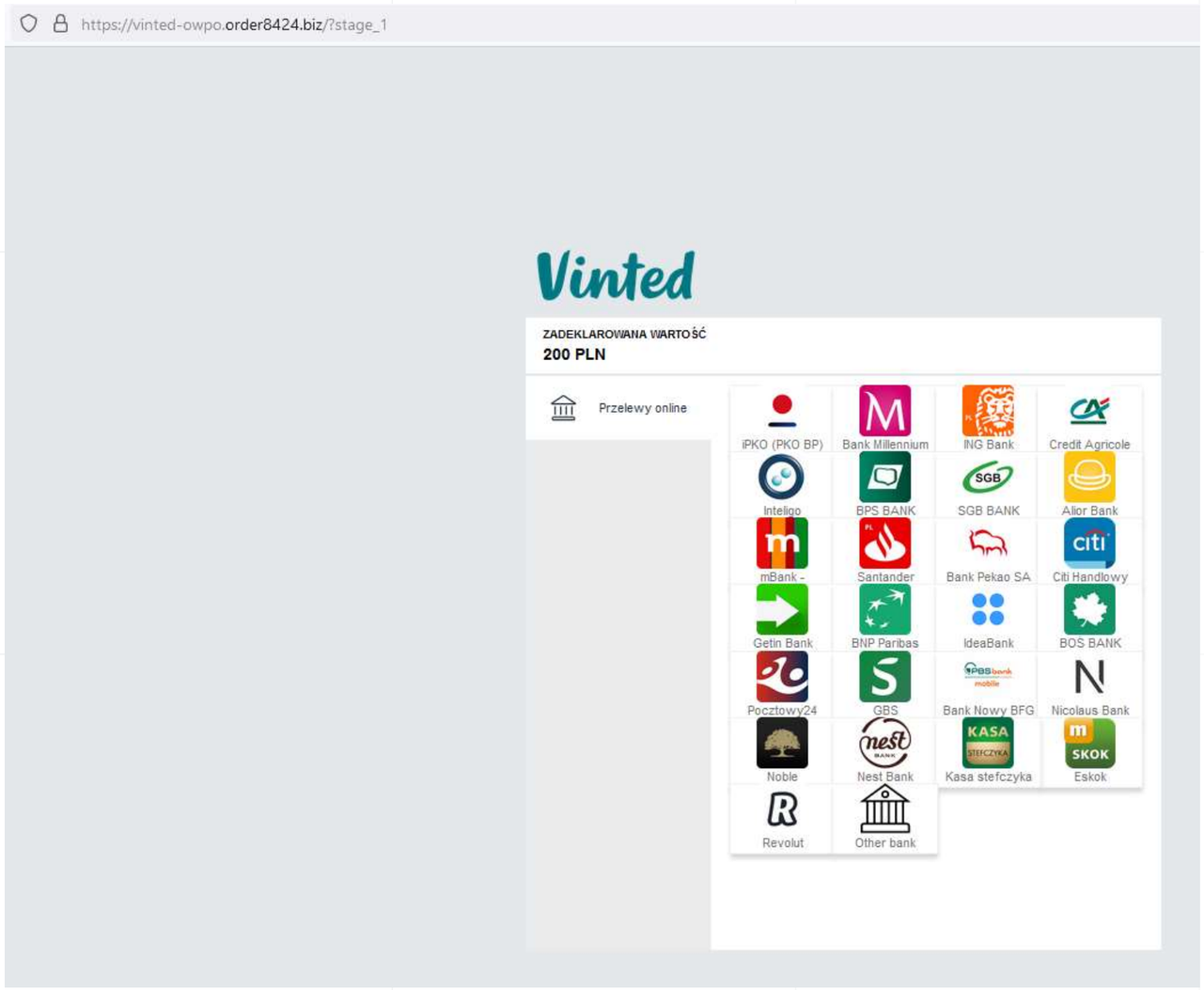
Otrzymanie środków

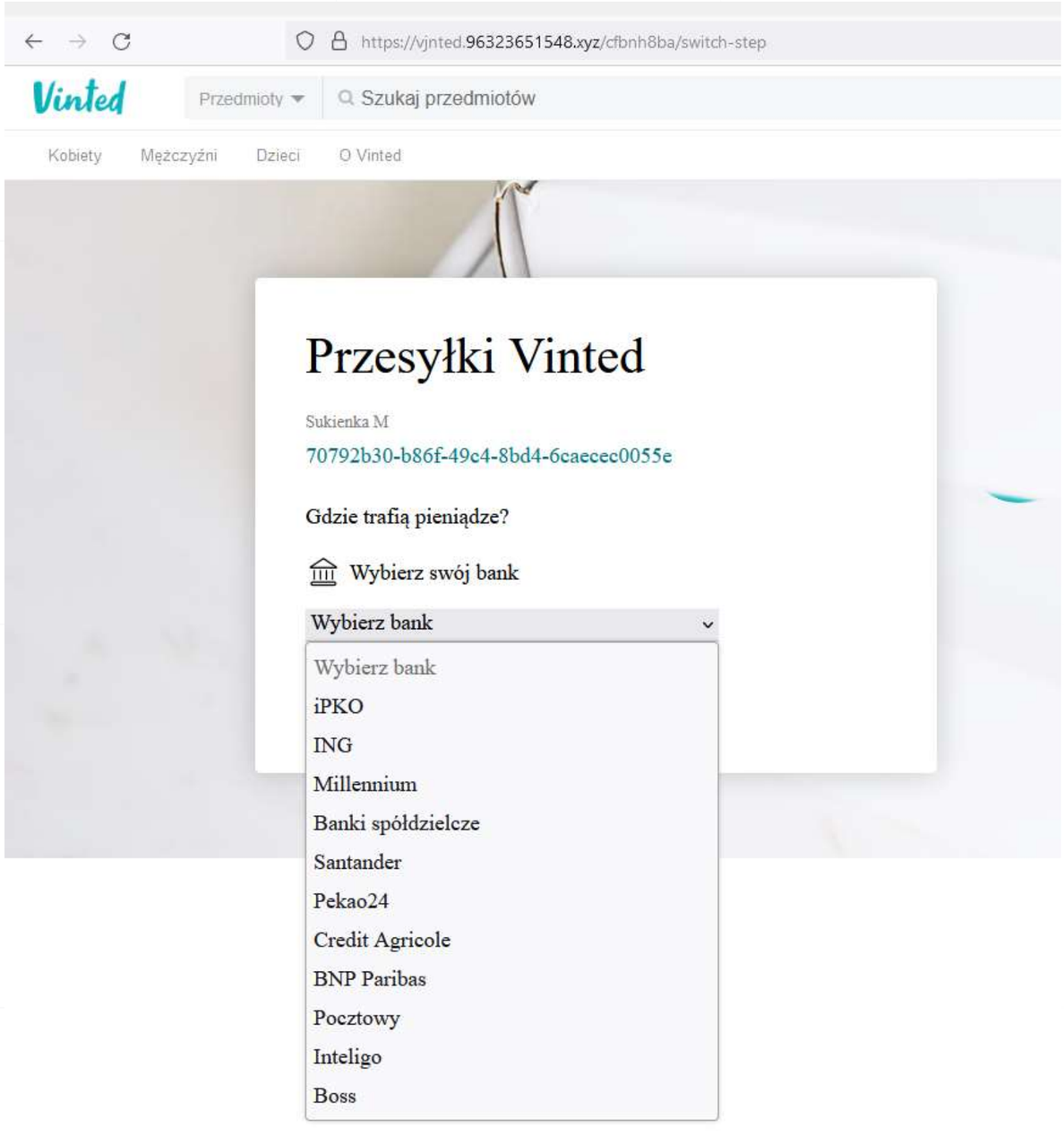
Kwota do otrzymania: 250.0 PLN

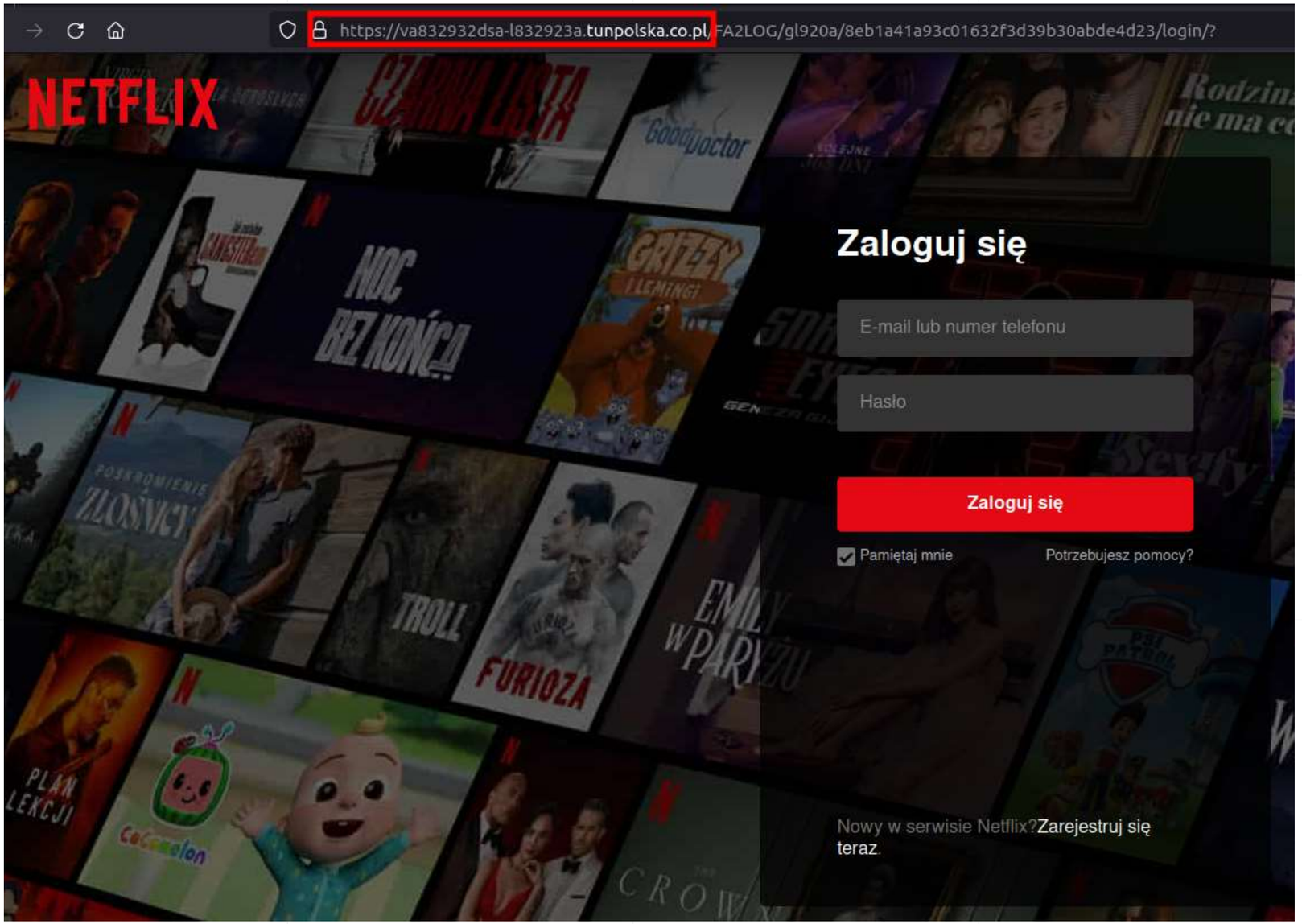
Suknia sprzedam

Zdobądź pieniądze

Dokonywanie płatności jest bezpieczne

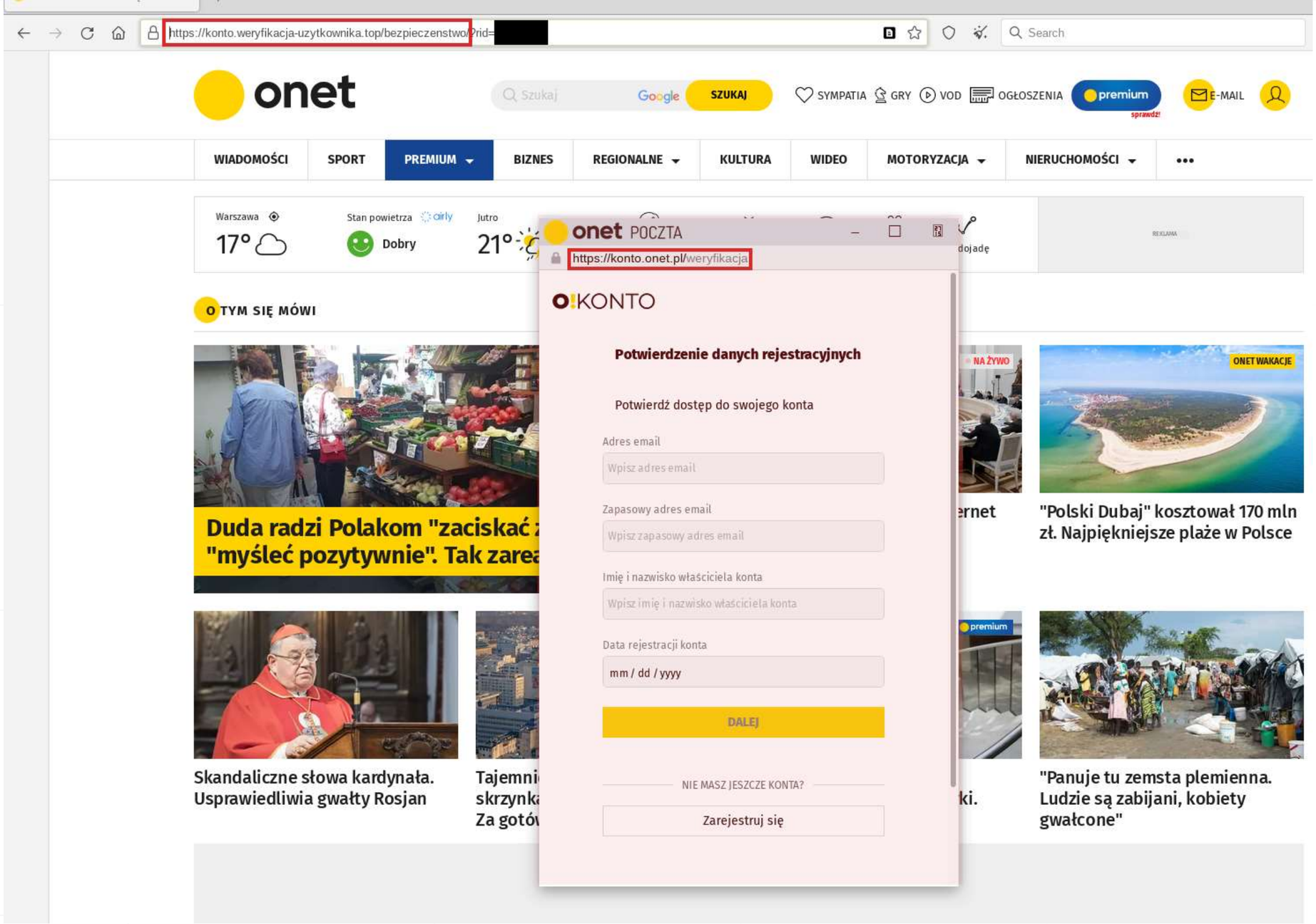

https://vinted-owpo.order8424.biz/?stage_1
Vinted
ZADEKLAROWANA WARTOŚĆ
200 PLN
Przelewy online
iPKO (PKO BP)
Bank Millennium
ING Bank
Credit Agricole
Inteligo
BPS BANK
SGB BANK
Alior Bank
mBank -
Santander
Bank Pekao SA
Citi Handlowy
Getin Bank
BNP Paribas
IdeaBank
BOS BANK
Pocztowy24
GBS
Bank Nowy BFG
Nicolaus Bank
Noble
Nest Bank
Kasa stefczyka
Eskok
Revolut
Other bank


https://vjnted.96323651548.xyz/cfbnh8ba/switch-step
Vinted
Przedmioty
Szukaj przedmiotów
Kobiety
Mężczyźni
Dzieci
O Vinted
Przesyłki Vinted
Sukienka M
70792b30-b86f-49c4-8bd4-6caecec0055e
Gdzie trafią pieniądze?
Wybierz swój bank
Wybierz bank
Wybierz bank
iPKO
ING
Millennium
Banki spółdzielcze
Santander
Pekao24
Credit Agricole
BNP Paribas
Pocztowy
Inteligo
Boss


https://va832932dsa-l832923a.tunpolska.co.pl/FA2LOG/gl920a/8eb1a41a93c01632f3d39b30abde4d23/login/?
NETFLIX
Zaloguj się
E-mail lub numer telefonu
Hasło
Zaloguj się
Pamiętaj mnie
Potrzebujesz pomocy?
Nowy w serwisie Netflix? Zarejestruj się teraz.


ka-985090.ingress-erytho.easywp.com
NETFLIX
Wyloguj się
KROK 1 Z 3
Skonfiguruj metodę płatności
VISA
Imię
Nazwisko
karta kredytowa lub debetowa
MM
YY
Kod zabezpieczający (CVV)

Metoda „Browser in the Browser”



(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

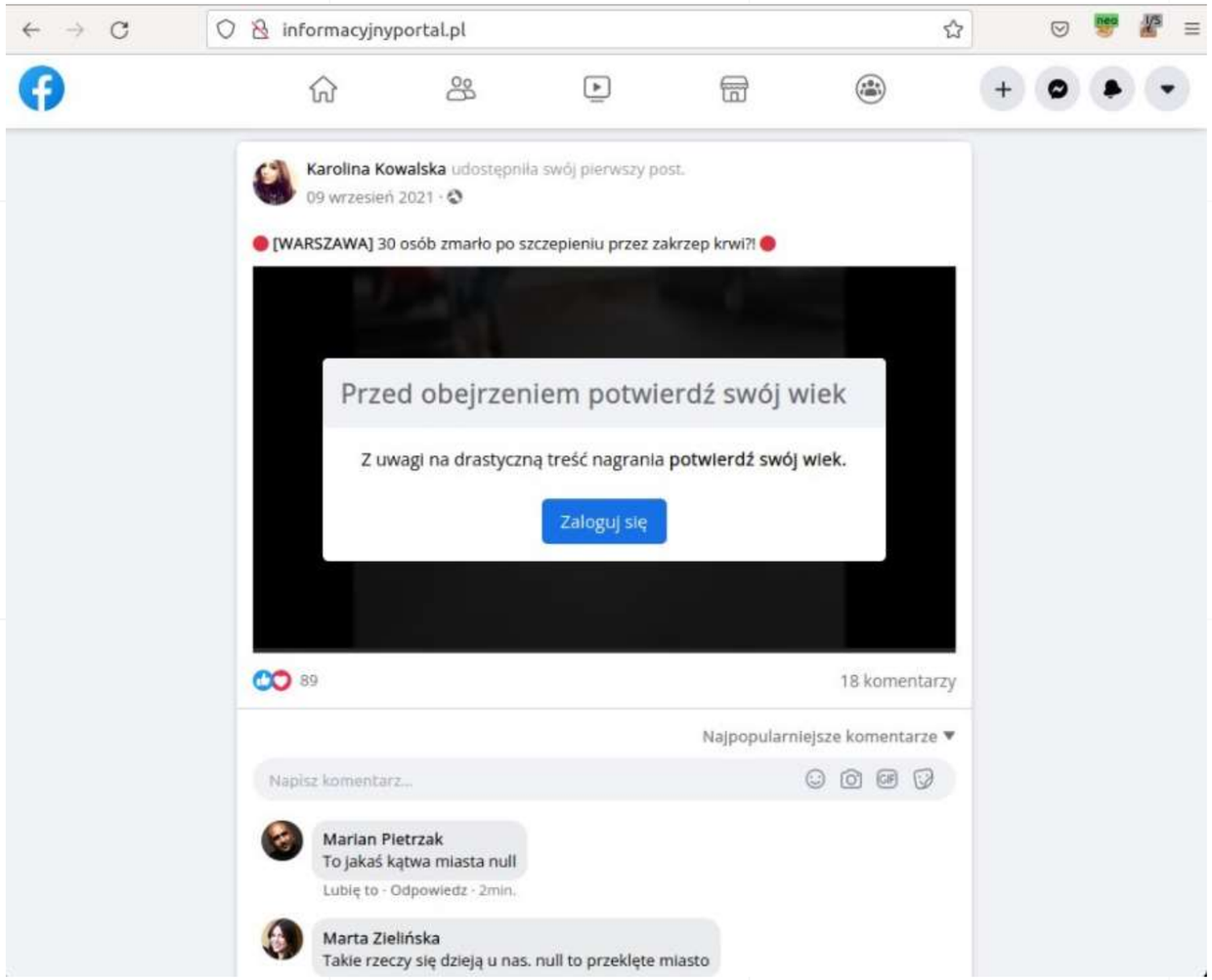
Ministerstwo Cyfryzacji

NASK

Ataki w mediach społecznościowych

Drastyczne i szokujące posty

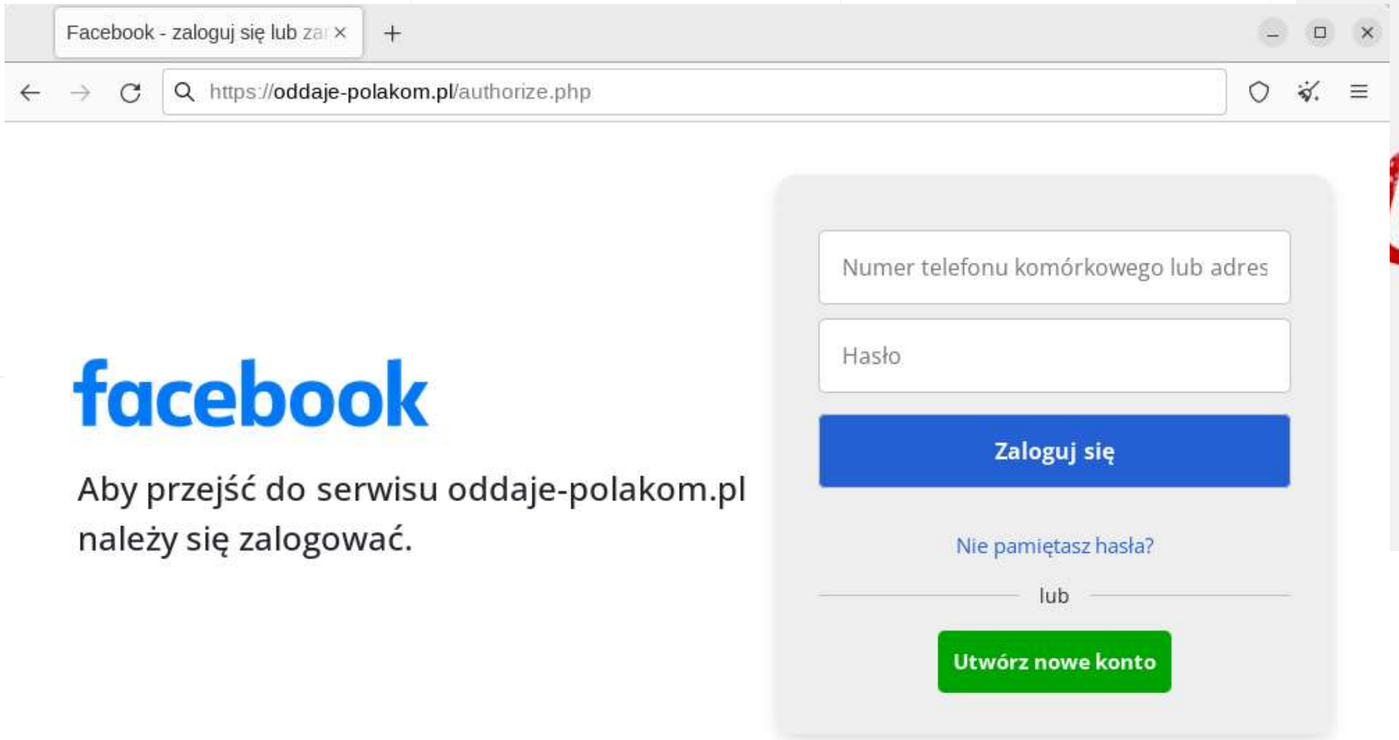
„Konieczność potwierdzenia wieku”

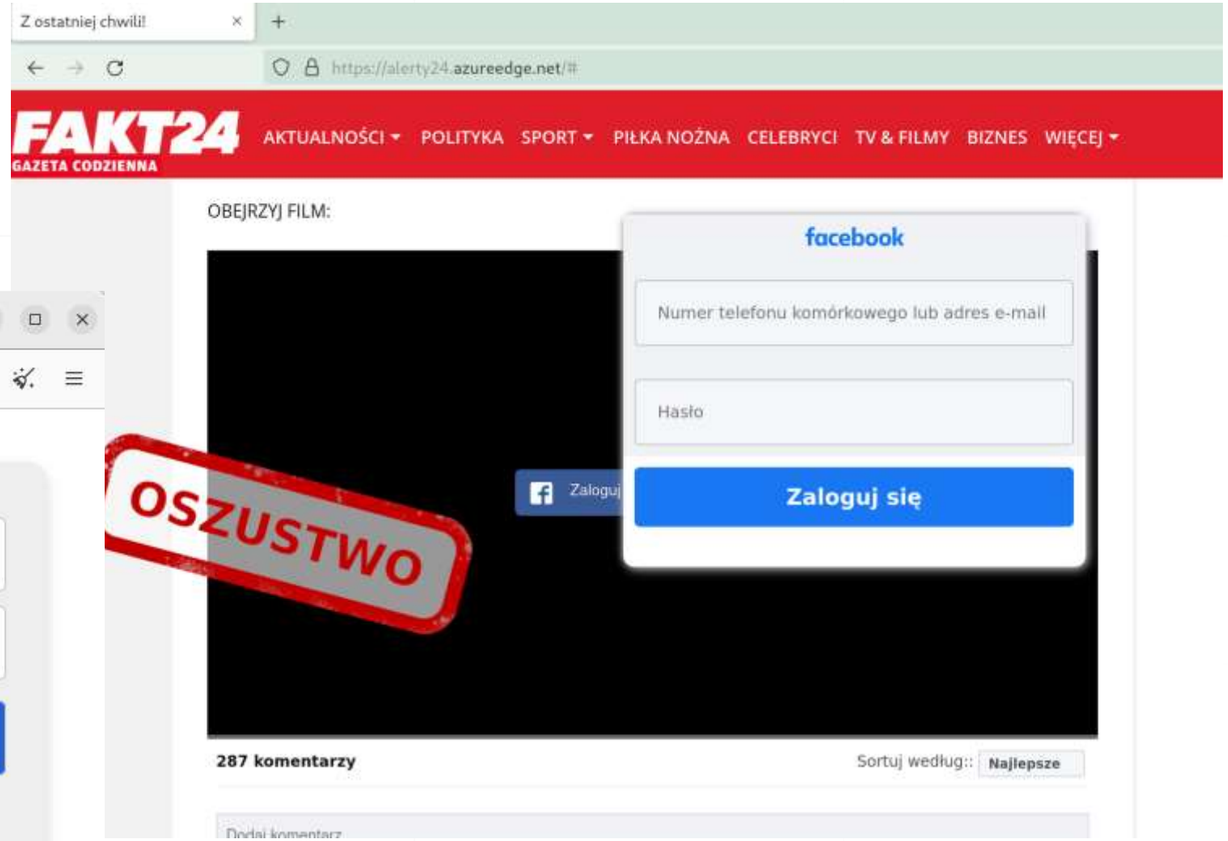


…lub inny dowolny pretekst:

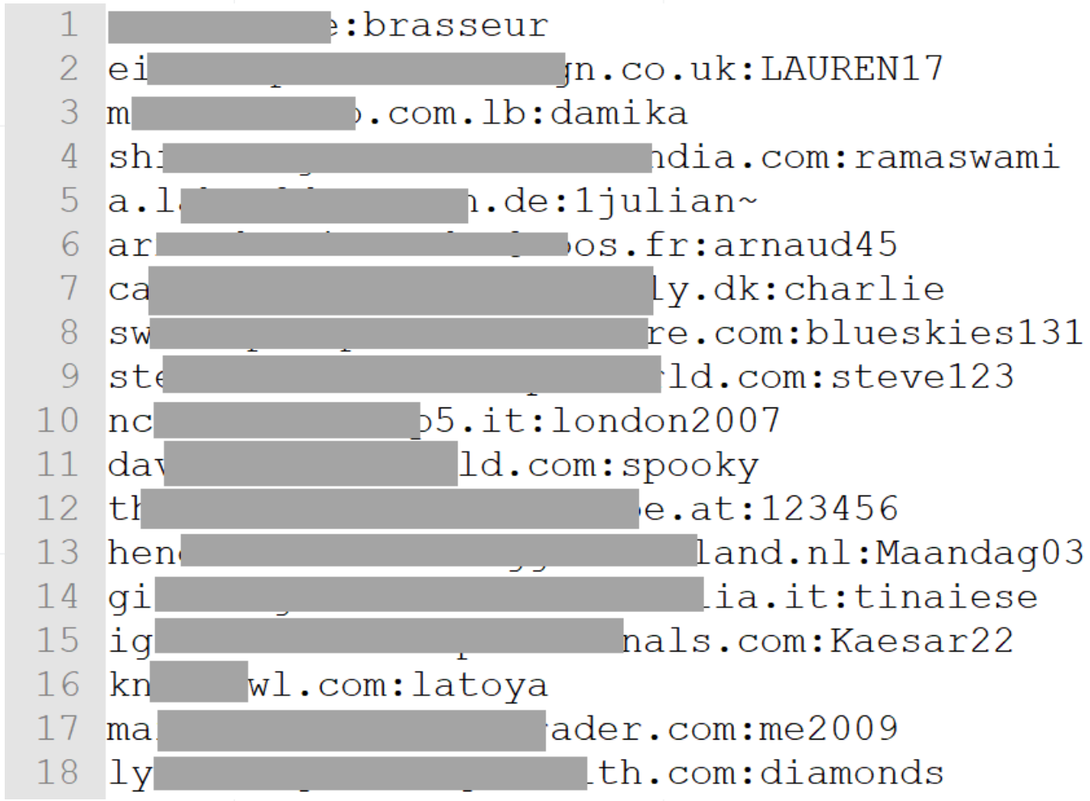
- Zakupy przez facebooka
- Prośba o udział w głosowaniu itp.

Fałszywy panel logowania



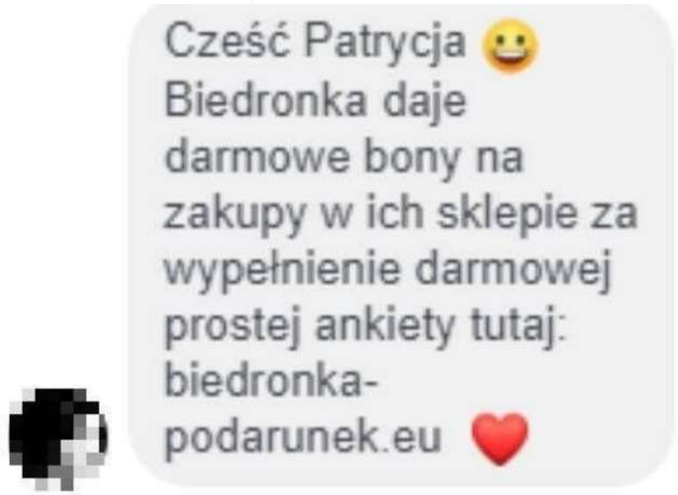


W efekcie – paczka danych: e-mail + hasło

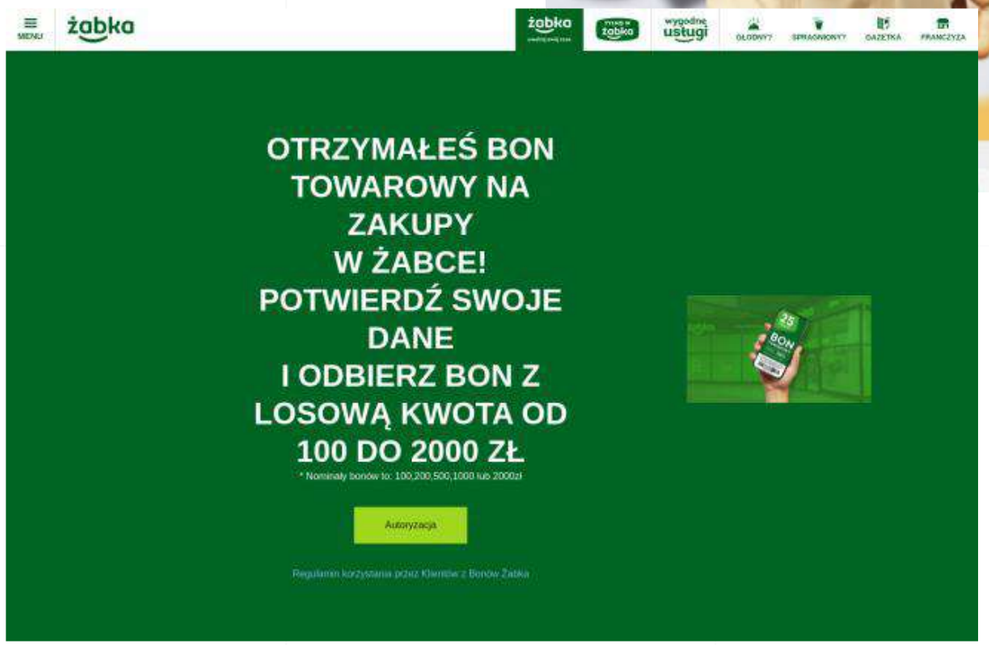


- troyhunt.com

Konkursy, loterie, bony w wiadomościach prywatnych



W tym przypadku nadawcą jest „ktoś ze znajomych”.



https://www.telepolis.pl/

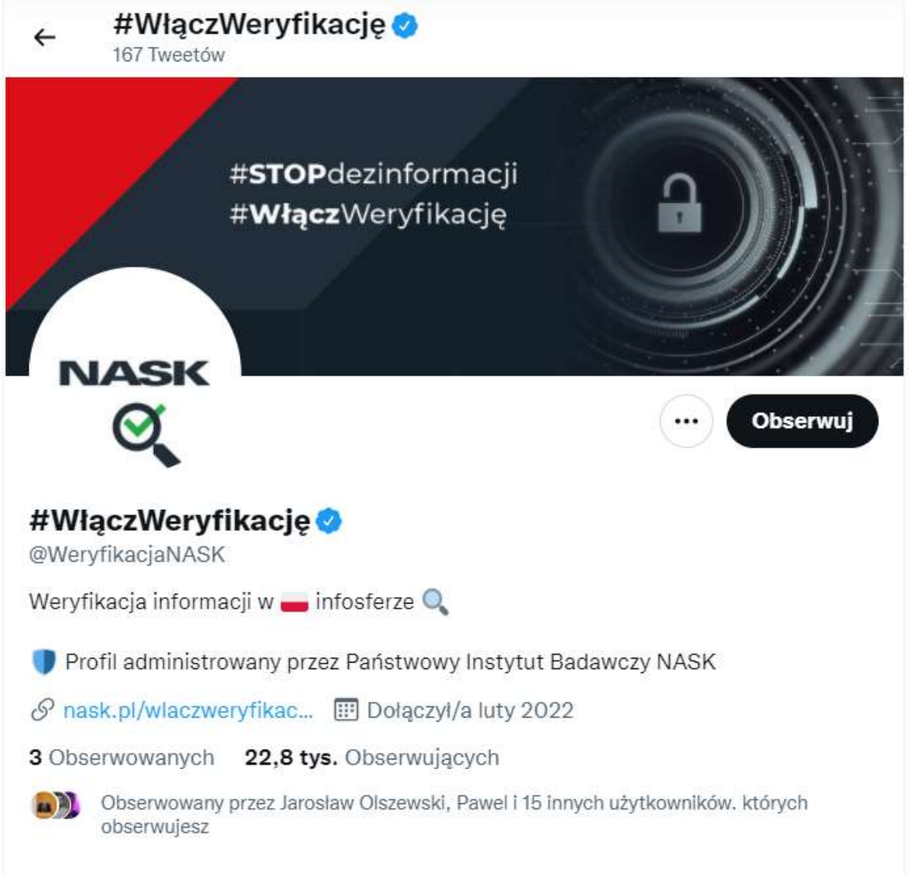
W jakim celu przestępcy atakują media społecznościowe?

- Przechwytywanie loginów i haseł do mediów społecznościowych.
- Uzyskiwanie dostępu do kontaktów i dalsze rozsyłanie wiadomości phishingowych, oszustw na kod BLIK i innych.
- Rozsyłanie/publikowanie dezinformacji, szkodliwych treści i/lub reklam.

Dlatego tak ważna jest **uważność** oraz **uwierzytelnienie dwuskładnikowe** przy logowaniu.

Dezinformacja w mediach społecznościowych

#WłączWeryfikację

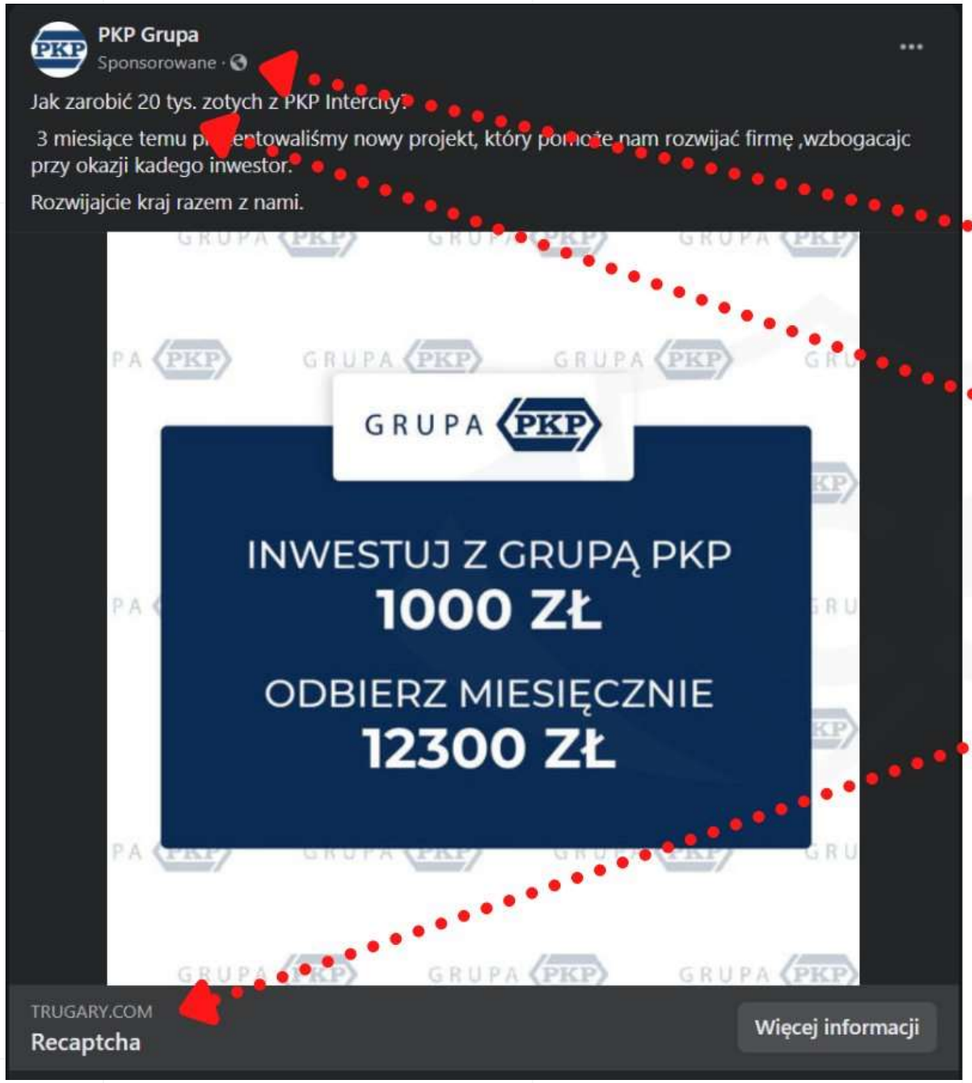


Zgłoś treści, które wzbudzają wątpliwości: informacje@nask.pl

Fałszywe reklamy

jak nie dać się złapać na świetną okazję

Reklamy „inwestycyjne”



Jak rozpoznać "Fałszywe Inwestycje"

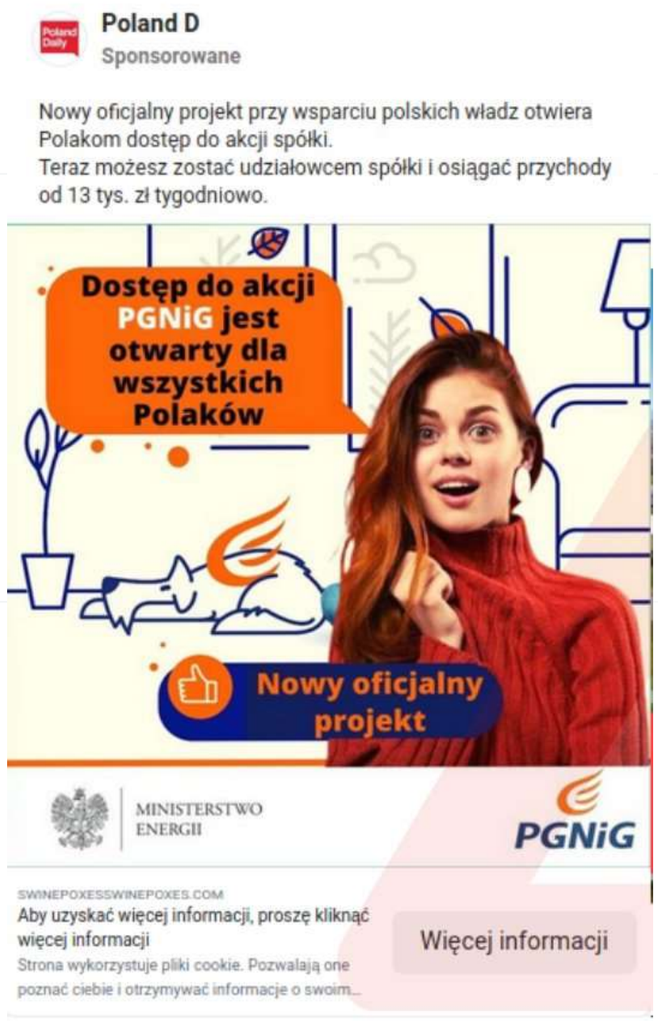
1. Reklama sponsorowana w Social Mediach.

2. W treści pojawiają się obietnice dużych zysków.

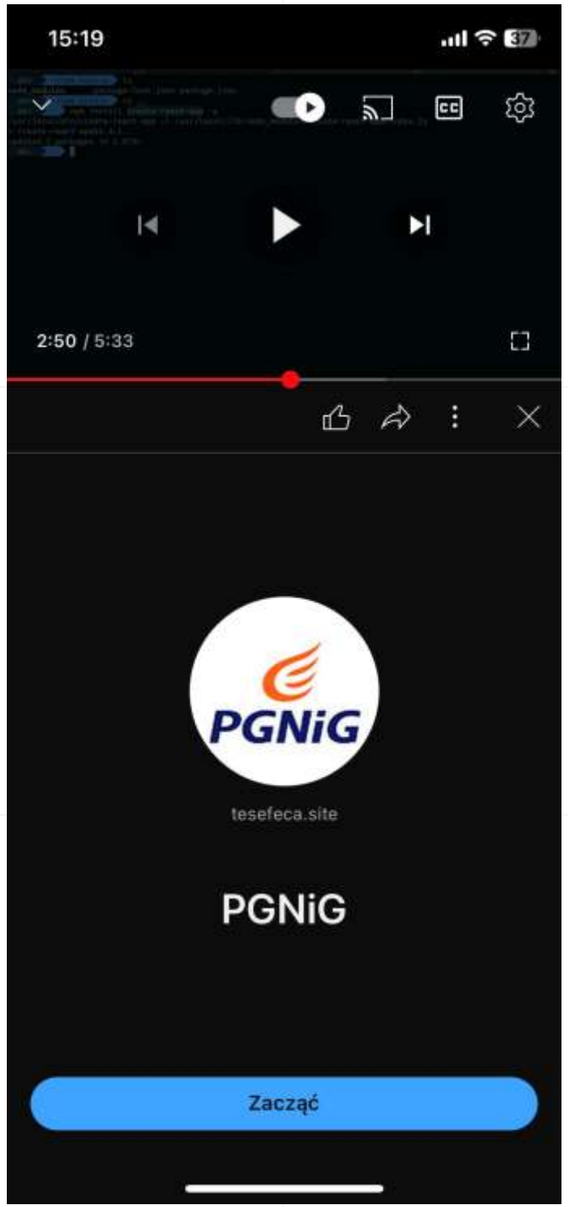
3. Domena niepowiązana z reklamującym się podmiotem.

4. Fałszywe komentarze, które nachalnie polecają inwestycje.

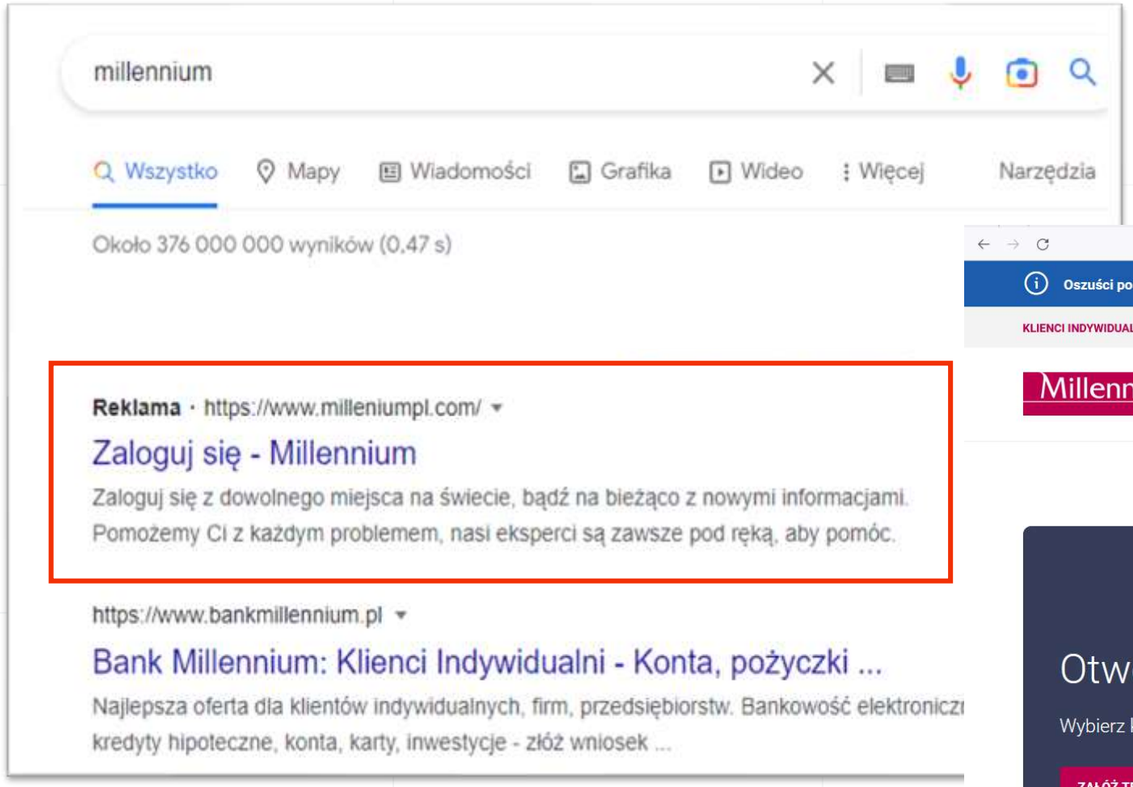
Znane marki, szybki zysk



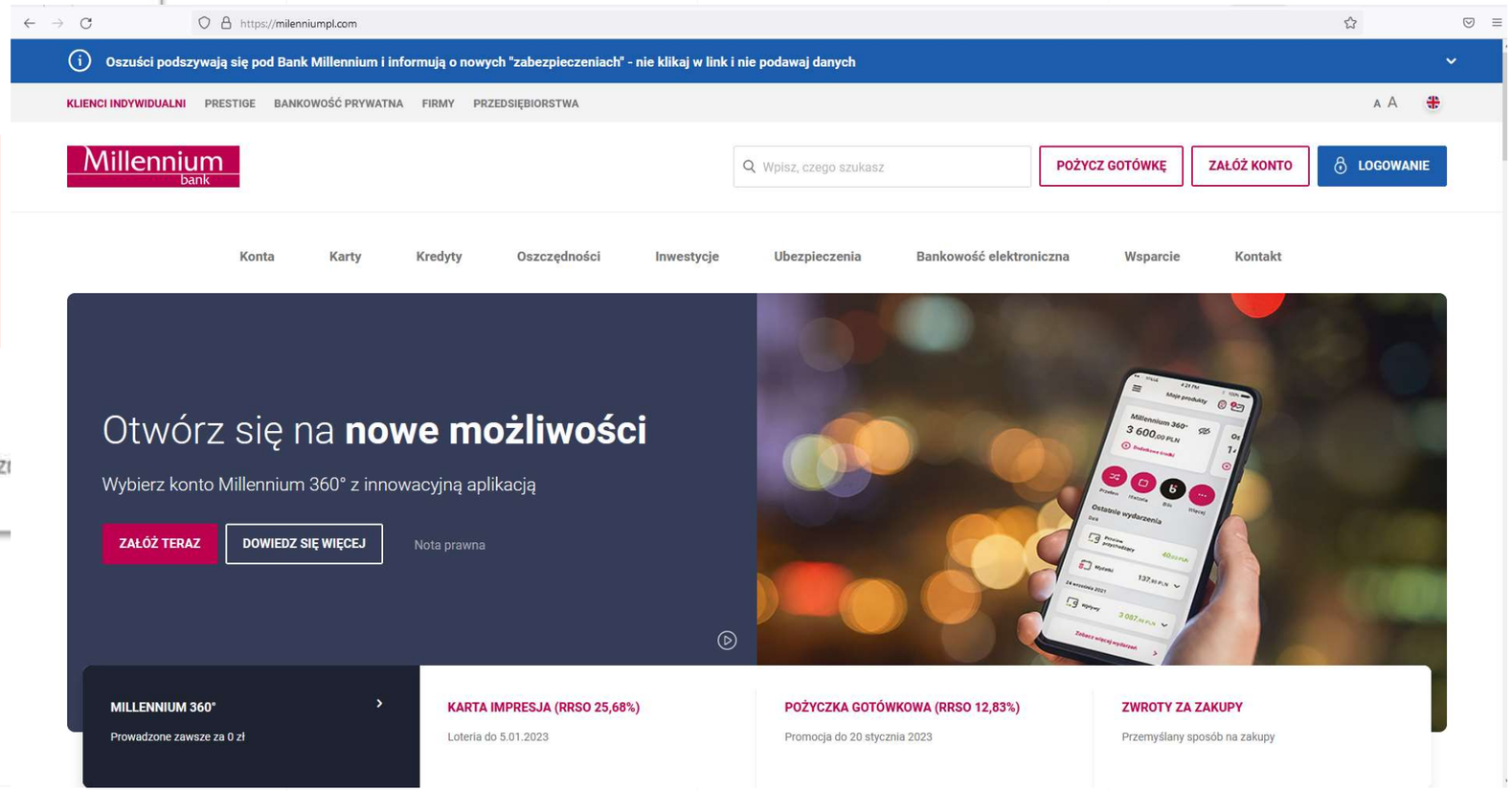
Reklamy na YouTube



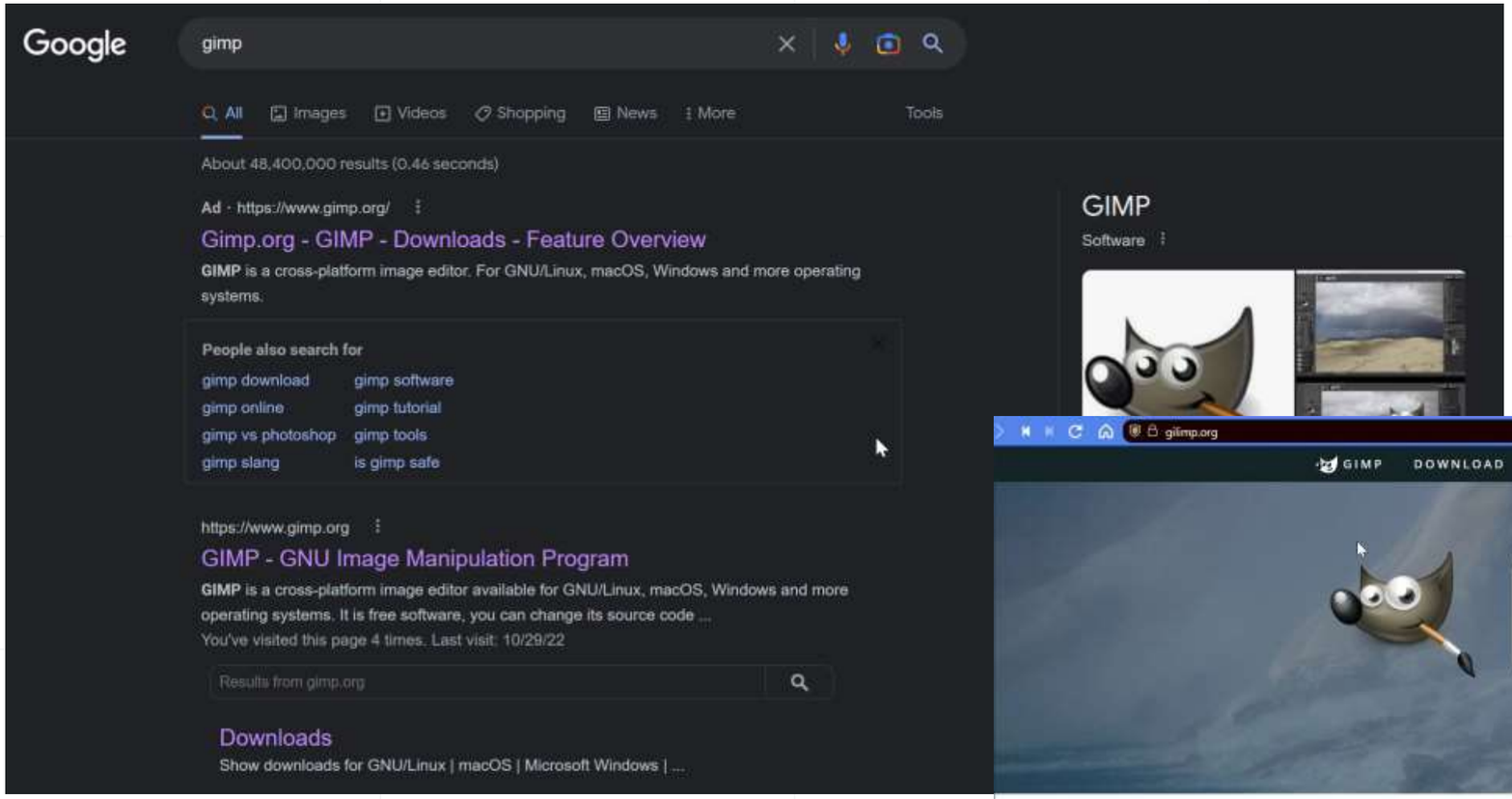
Google Ads...



...i strona phishingowa



… lub złośliwe oprogramowanie



Fałszywe sklepy internetowe

- Sprawdź opinie o sklepie, zanim cokolwiek w nim kupisz.
- Strzeż się reklam oferujących cudowne produkty i podejrzane przeceny!

Więcej informacji:

- Poradnik zespołu CERT POLSKA
- Baza wiedzy bezpiecznymiesiac.pl

Vishing

czyli oszustwo w rozmowie telefonicznej

Vishing – atak telefoniczny

ang. Voice + phishing

Uniwersalny **pretekst** rozmowy.

Techniki manipulacyjne w rozmowie.

Uwaga na **spoofing**!

Cele ataku

- Wyłudzenie informacji
- Instalacja oprogramowania
- Wykonanie przelewu/podanie kodów jednorazowych

Atak telefoniczny „odwrócony”, „na pomoc techniczną”

Twoja karta platnicza VISA zostala zablokowana ze wzgledow bepzieczenstwa. Prosimy o pilny kontakt mBankiem +48 42 6 300 800

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Microsoft account

Your account has been temporarily blocked

Someone may have used your account to send out a lot of junk messages or done something else that violates the Microsoft Services Agreement.

What do you need to do?

We'll send a verification code to your phone. After you enter the code, you can sign in.

Continue

Skip this for now *(some Microsoft sites and services might be disabled)*

(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location: United States

Your IP Address: 199.231.208.116

Date: Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free) for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

Possible network damages from potential threats: UNKNOWN

Data exposed to risk:

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Atak telefoniczny „na zdalny pulpit”

TeamViewer

AnyDesk

ALPEMIX

Vishing – jak reagować

Jeśli rozmówca wzbudzi Twoje podejrzenia – rozłącz się.

Jeśli chcesz się upewnić, skontaktuj się samodzielnie **wyszukując w zaufanym źródle** numer obsługi klienta danej instytucji/banku itp.

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Phishing, oszustwa – podsumowanie

- Zachowaj spokój i rozsądek – **patrz krytycznie** na wiadomości, strony internetowe, reklamy i inne treści w internecie.

- Zachowaj **czujność przy logowaniu** do usług, w rozmowach telefonicznych **nie podawaj poufnych informacji** (haseł, kodów jednorazowych i innych).

- W pracy – **trzymaj się wewnętrznych procedur dotyczących płatności.**

Złośliwe oprogramowanie

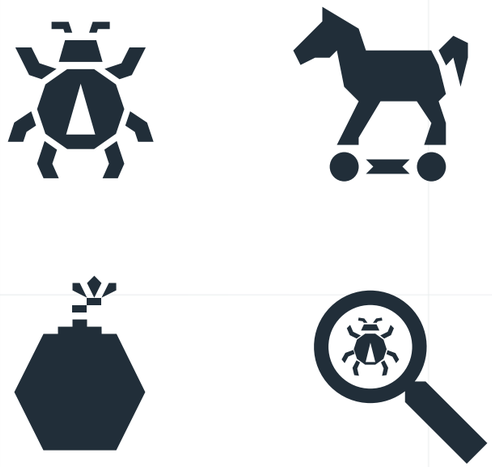
Złośliwe oprogramowanie

Szkodliwe oprogramowanie

ang. *malware* – zbitka słów *malicious* „złośliwy” i *software* „oprogramowanie”

Ogół programów o szkodliwym działaniu w stosunku do systemów komputerowych i/lub ich użytkowników.

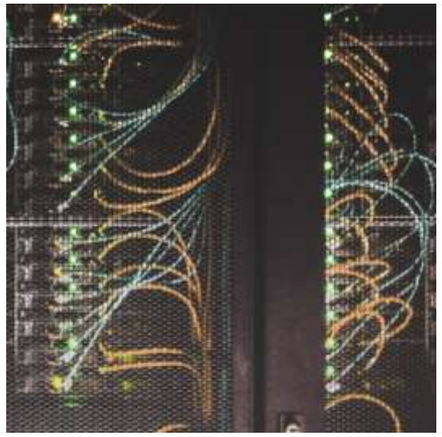
Rodzaje złośliwego oprogramowania



Podział ze względu na **sposób działania**:

- Ransomware
- Wiper
- Trojany bankowe (bankery)
- Spyware
- RAT (remote access trojan)
- ...

Źródła infekcji złośliwym oprogramowaniem

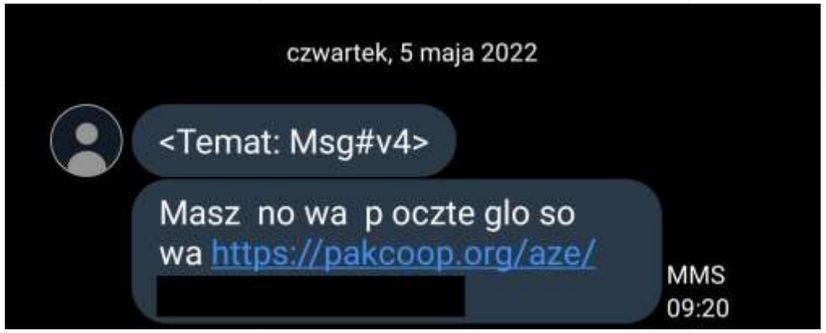


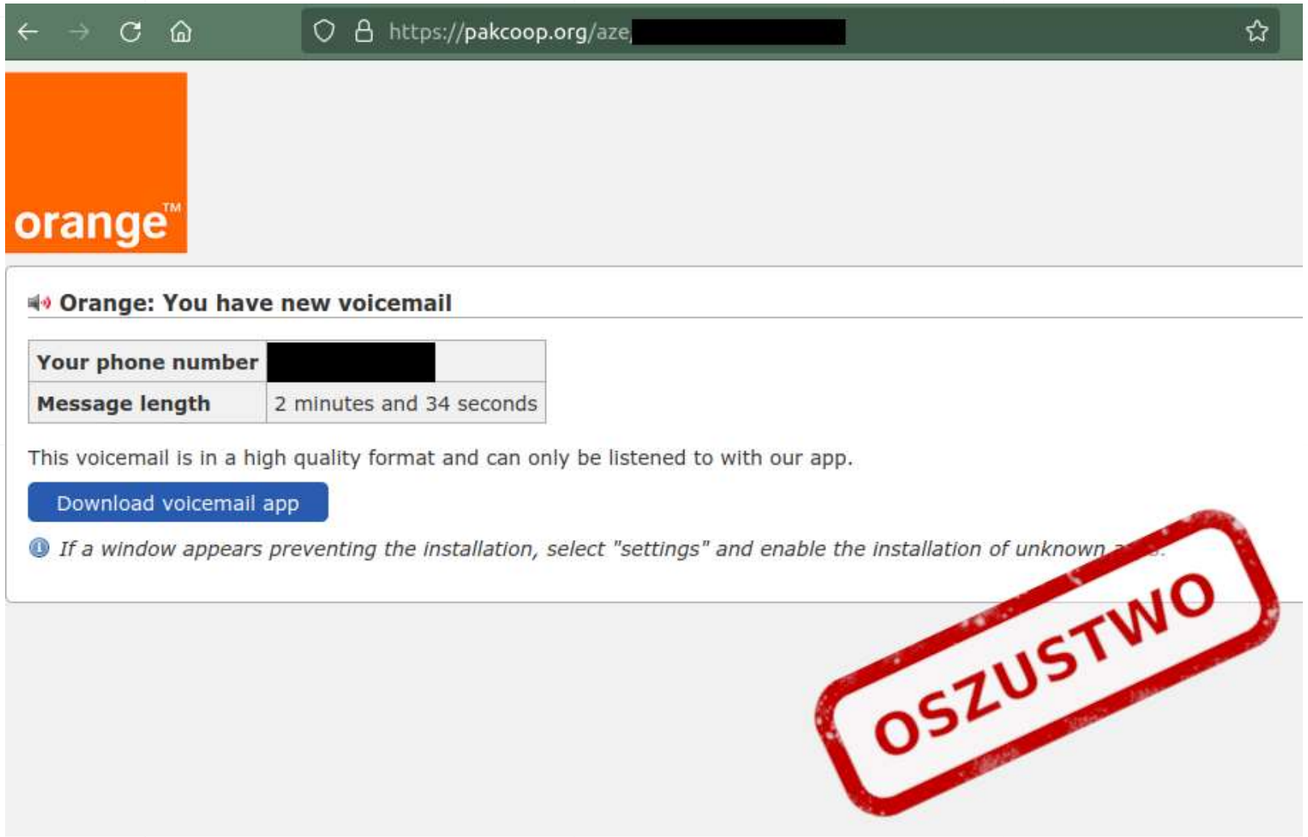
- **Podatności w publicznie dostępnych usługach,** takich jak VPN, zdalny dostęp, serwer pocztowy itp.

- **Niewystarczająco zabezpieczone kanały zdalnego dostępu** do infrastruktury sieciowej oraz publicznych usług.

- **Instalacja przez użytkowników – załączniki i linki z maili i SMSów** i/lub innych niezaufanych źródeł

Złośliwe oprogramowanie i SMShing





Została wyznaczona data kolejnego szczepienia. Więcej informacji w aplikacji https://cutt/ly/bQNgg0e

https://m-obywatel.pl/#

mObywatel - publiczna aplikacja mobilna

18,011

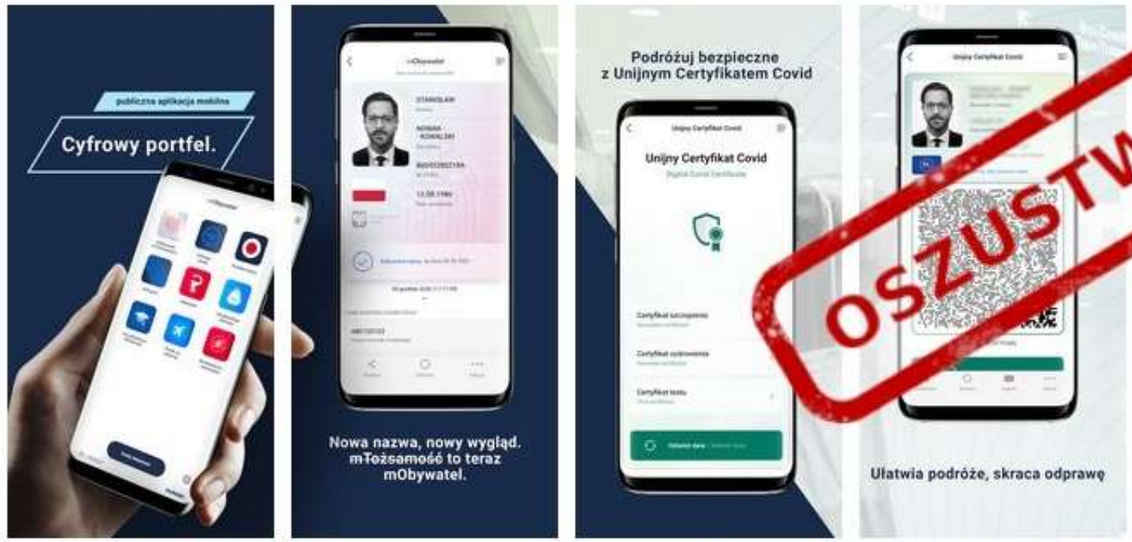
Kancelaria Prezesa Rady Ministrów Wydajność

3+

Dodaj do listy życzeń

Ta aplikacja jest dostępna na Twoje urządzenie

Zainstalować



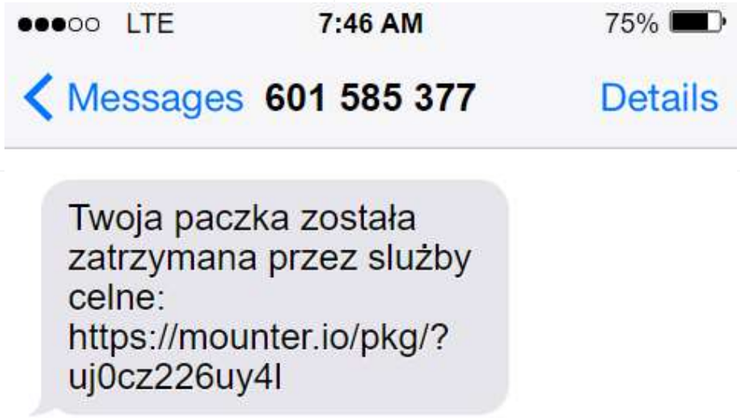
OSZUSTWO

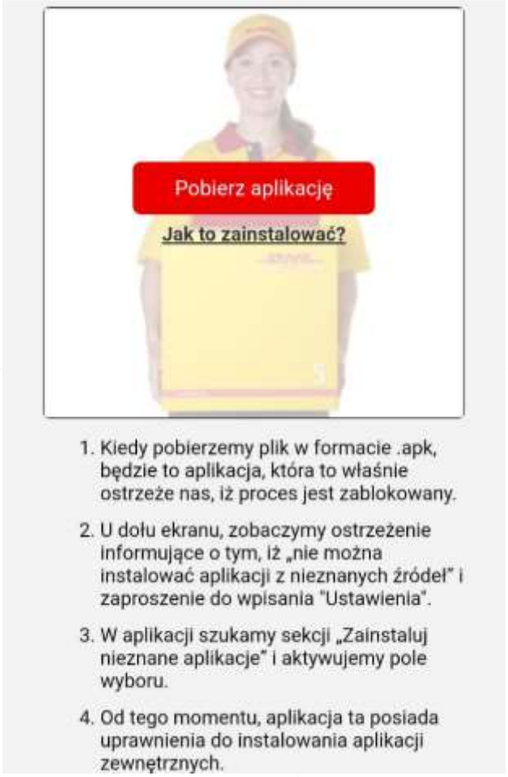
Wydawcą aplikacji jest Kancelaria Prezesa Rady Ministrów.

Z usługi mObywatel mogą korzystać wyłącznie osoby posiadające polskie obywatelstwo i ważny dowód osobisty.

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Złośliwe oprogramowanie z instrukcją instalacji





Skutek: Trojan bankowy

- wykradanie danych
- przechwytywanie komunikacji z bankiem

Złośliwe załączniki w mailach

Od BNP Paribas Bank Polska <recepcja=vhotel.pl@beep.pl>

Temat BNP Paribas - wyciąg bankowy

Data 2022-10-19 07:21:13

Dzień dobry,

W załączeniu przelew bankowy z dnia 19 października 2022

Jeżeli mieliby Państwo pytania, prosimy o kontakt pod numerem: 500 990 500.

Z pozdrowieniami
BNP Paribas Bank Polska S.A.

Nasz system wysłał tą wiadomość automatycznie - prosimy na nią nie odpowiadać.

Z pozdrowieniami,

Szymon Machniak

BNP PARIBAS

Bank zmieniającego się świata

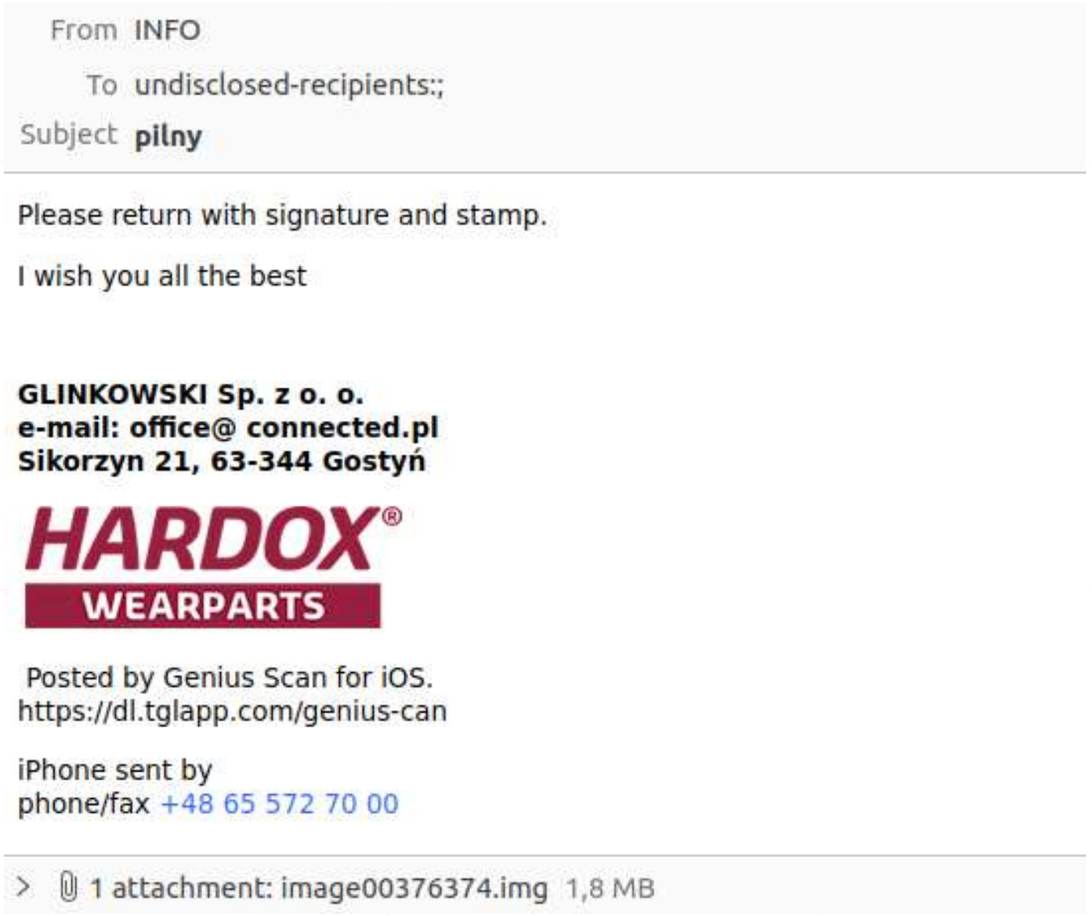
Szymon MACHNIAK
specjalista ds. obsługi klientów msp

BNP Paribas Bank Polska S.A.
Strefa Obsługi Biznesu
ul. Francuska 36
40-028 Katowice, Polska
SWIFT (BIC): PPABPLPKXXX
tel. +48 22 548 29 26
SOB@bnpparibas.pl
www.bnpparibas.pl

Pomyśl o środowisku, zanim wydrukujesz tę wiadomość

Kochaj naturę – uwolnij chmurę! Zawsze kasuj niepotrzebne e-maile

Załączniki WYCIAG BANKOWY 5791 4Z39PP 000 M 0214-2022 WZE 2022-10-01 pdf .img 78kB



From INFO

To undisclosed-recipients:;

Subject **pilny**

Please return with signature and stamp.

I wish you all the best

GLINKOWSKI Sp. z o. o.
e-mail: office@ connected.pl
Sikorzyn 21, 63-344 Gostyń

HARDOX® WEARPARTS

Posted by Genius Scan for iOS.
https://dl.tglapp.com/genius-can

iPhone sent by
phone/fax +48 65 572 70 00

> 1 attachment: image00376374.img 1,8 MB

Podejrzane załączniki

.zip

.rar

.iso

.img

.exe

.com

.scr

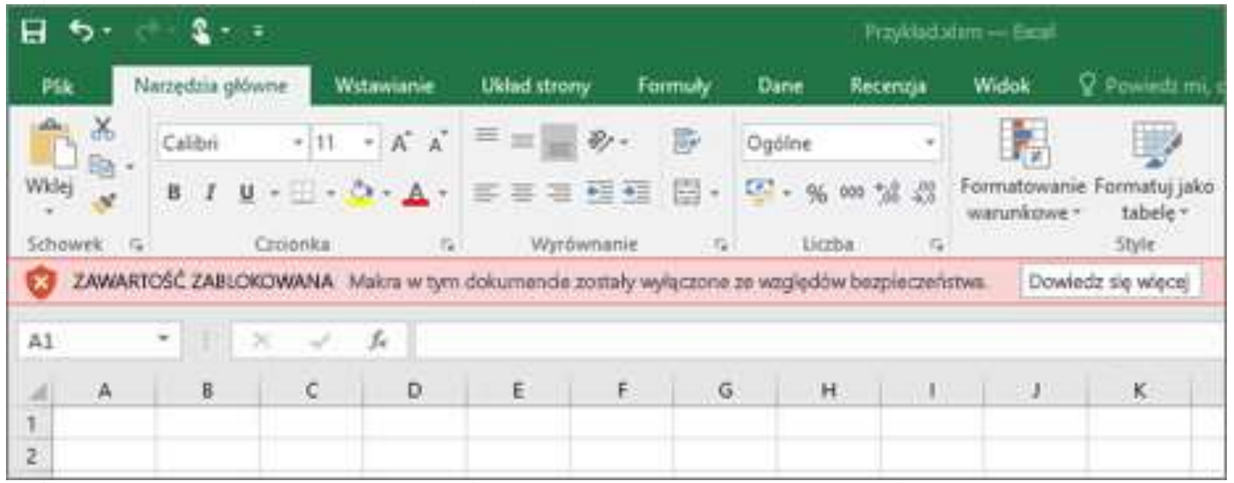
.vbs

.js

.htm / .html

.xlsx / .xlsm / .xls

Dawniej przestępcy często wykorzystywali funkcję makr w plikach programów MS Office.



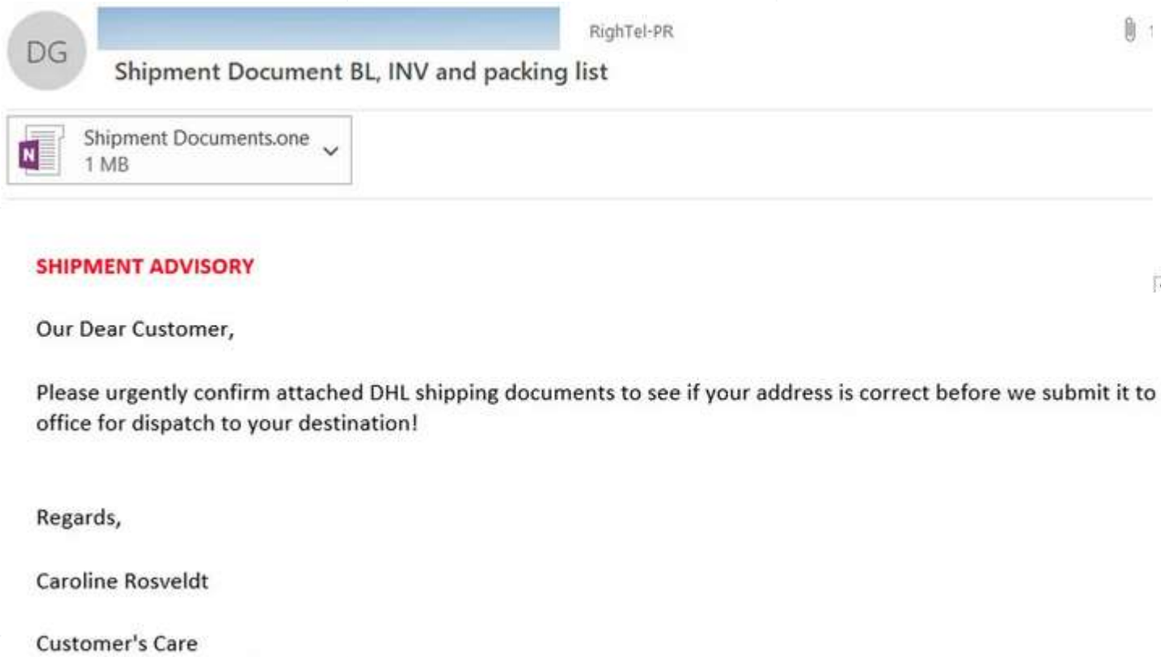
https://support.microsoft.com/

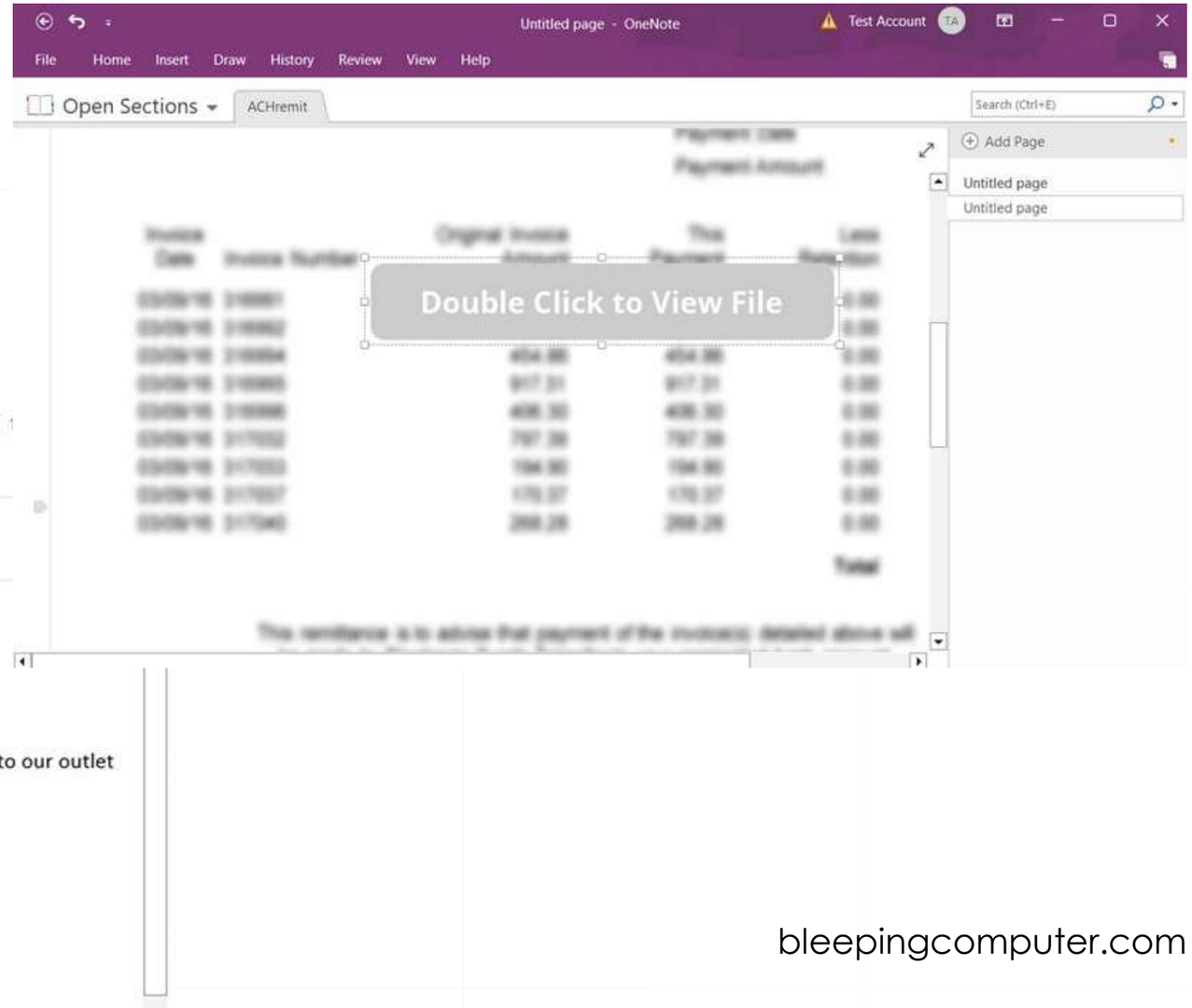
Podejrzane załączniki

MS One Note

.one

Trik: załączniki ze skryptem pod fałszywym klawiszem





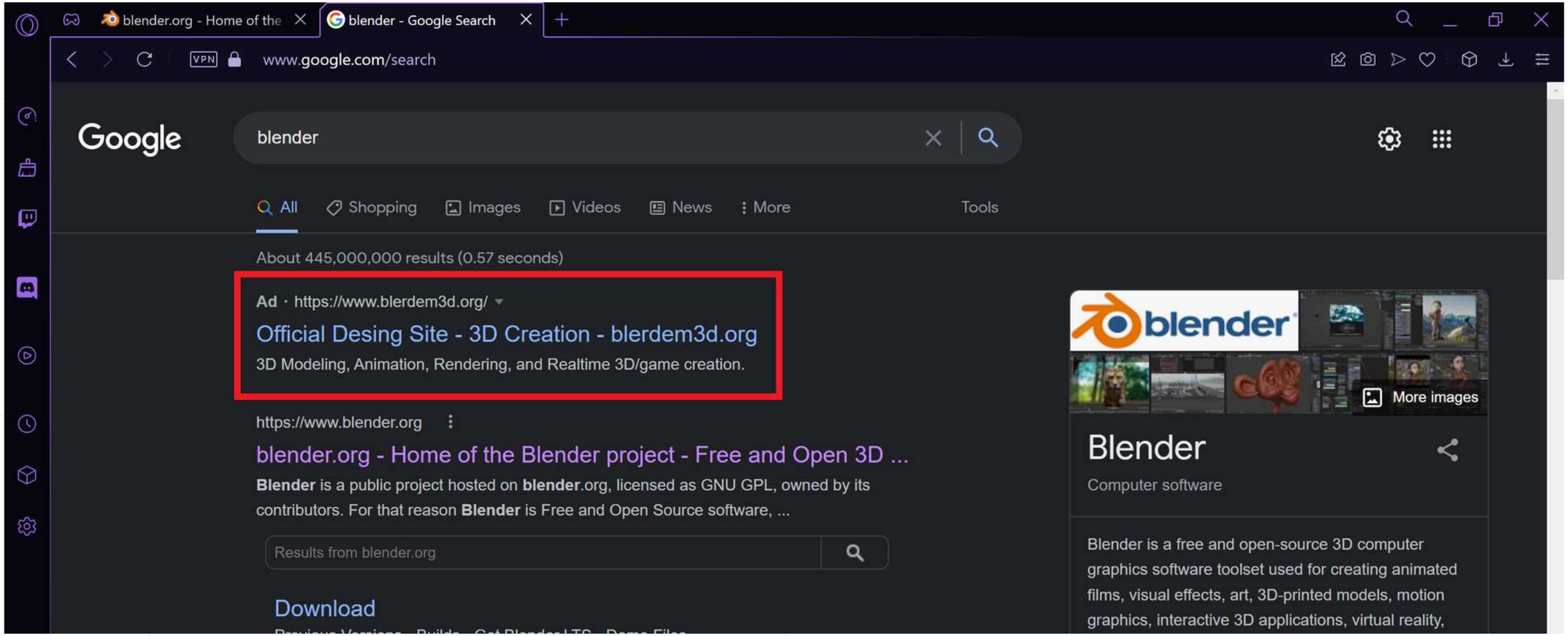
bleepingcomputer.com

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Złośliwe programy w Google Ads



Ransomware

Złośliwe oprogramowanie wykorzystywane do szyfrowania i blokowania dostępu do systemów i danych.

1

Celem ataku jest **wymuszenie okupu**

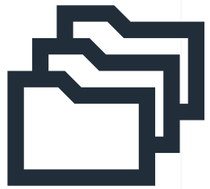
w zamian za odzyskanie danych.

Przebieg ataku ransomwarem

Włamanie do sieci

(przez podatność/ złośliwy załącznik)

Rozpoznanie sieci i systemów



Skopiowanie danych na serwer przestępców

Szyfrowanie kopii zapasowych i systemów

Szyfrowanie danych i systemu – **główny atak ransomware**


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Co po ataku?

W przypadku ataku ransomware, atakujący nie tylko szyfrują dane, ale także wykradają je, grożąc upublicznieniem w przypadku nie zapłacenia okupu.

Zapłacenie okupu **nie gwarantuje odzyskania danych!**

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Ransomware – prewencja

- **dobra strategia tworzenia i weryfikowania kopii zapasowych (3-2-1)**
- **regularna aktualizacja oprogramowania**
- **edukacja i aktualizowanie wiedzy**
- segmentacja sieci
- inwentaryzacja publicznie dostępnych usług
- zabezpieczenie potencjalnych źródeł infekcji
- aktywne monitorowanie zdarzeń w sieci

Zgłaszanie incydentów

czyli dbanie o wspólne bezpieczeństwo w sieci

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

prześlij na nr:
799 448 084

lub zgłoś przez formularz na stronie:
incydent.cert.pl

lub wyślij email na adres:
cert@cert.pl

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 wyłudzające dane osobowe lub środki finansowe
- Podejrzana wiadomość e-mail/SMS
  Podejrzane załączniki/SMSy, phishing, szantaż
- $ Oszustwo
  Fałszywe sklepy internetowe i inne próby podszywania się
- Złośliwe oprogramowanie
  Próbki wirusów lub pliki zaszyfrowane ransomware
- Podatności
  Błędy w oprogramowaniu lub aplikacjach internetowych
- Nielegalne treści
  Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl
- Inne
  Wszystkie inne incydenty niepasujące do poprzednich kategorii

NASK
CERT.PL

Zgłaszanie szkodliwych SMSów

- Wiadomości przekazuj dalej na numer **799 448 084.**
  Zapisz ten numer w telefonie, aby mieć go zawsze pod ręką.
- Z jednego numeru możesz zgłosić maksymalnie 3 wiadomości w ciągu 4 godzin.
- Numer służy do zgłaszania prób wyłudzeń internetowych (phishingu, fałszywych aplikacji) – nie przyjmujemy zgłoszeń dotyczących usług SMS premium.
- Przekaż nam całą wiadomość w oryginalnej formie tekstowej – nie wycinaj odnośnika, treści oraz nie przesyłaj jej w formie zdjęć czy zrzutów ekranu.
- Podany numer służy tylko do przyjmowania SMS-ów – numer do telefonicznego zgłaszania incydentów znajduje się na naszej stronie.

Opłata za wysłanie wiadomości SMS zgodna jest z taryfą operatora

NASK
CERT.PL

Zgłaszanie stron internetowych służących do wyłudzeń danych i środków finansowych

Zgłoszenie możesz wysłać przez incydent.cert.pl/domena

Wpisz wszystkie strony, które chcesz zgłosić – każdą w osobnej linii

W uzasadnieniu zgłoszenia opisz dlaczego powyższe domeny zostały przez Ciebie uznane za szkodliwe

Formularz ten służy zgłaszania prób wyłudzeń internetowych (phishingu, fałszywych aplikacji), nie przesyłaj nim np. podejrzanych sklepów internetowych

https://incydent.cert.pl/

NASK

CERT.PL

Zgłaszanie pozostałych oszustw komputerowych

Zgłoszenia możesz wysłać przez incydent.cert.pl

Wybierz odpowiedni rodzaj podmiotu – jeśli jesteś zwykłym użytkownikiem internetu będzie to "Osoba fizyczna"

Wybierz jaki rodzaj oszustwa chciałbyś zgłosić

Jeśli chcesz zgłosić szkodliwą wiadomość mail, pamiętaj o załączeniu wiadomości w formacie .eml lub .msg. Instrukcja jak pobrać wiadomość w takim formacie znajduje się na https://incydent.cert.pl/instrukcje-email

https://incydent.cert.pl/

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Dziękuję

Zespół Szkoleń i Ćwiczeń Cyberbezpieczeństwa

zbsc@nask.pl

Ministerstwo Cyfryzacji

NASK