



(CYBER)SZKOLENIA

KRAJOWY SYSTEM
CYBERBEZPIECZEŃSTWA

Phishing, oszustwa w sieci i ransomware.

Najpowszechniejsze
cyberzagrożenia – jak rozpoznać,
jak zapobiegać



Plan części pierwszej



– Rodzaje i charakterystyka cyberzagrożeń



– Rozpoznawanie



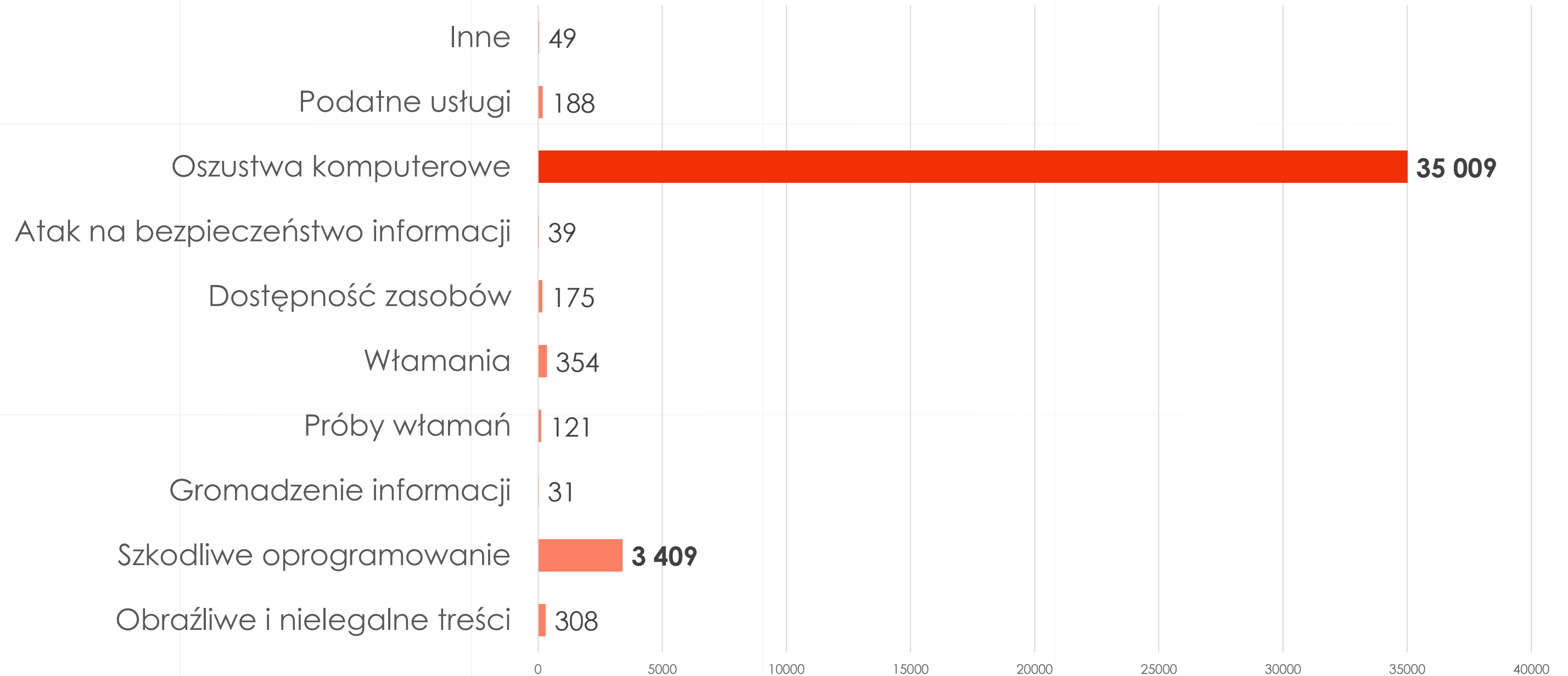
– Reagowanie i zapobieganie



– Zgłaszanie incydentów



Incydenty zarejestrowane przez CERT Polska w 2022 roku



Oszustwa komputerowe



– Ataki wykorzystujące **socjotechnikę**.



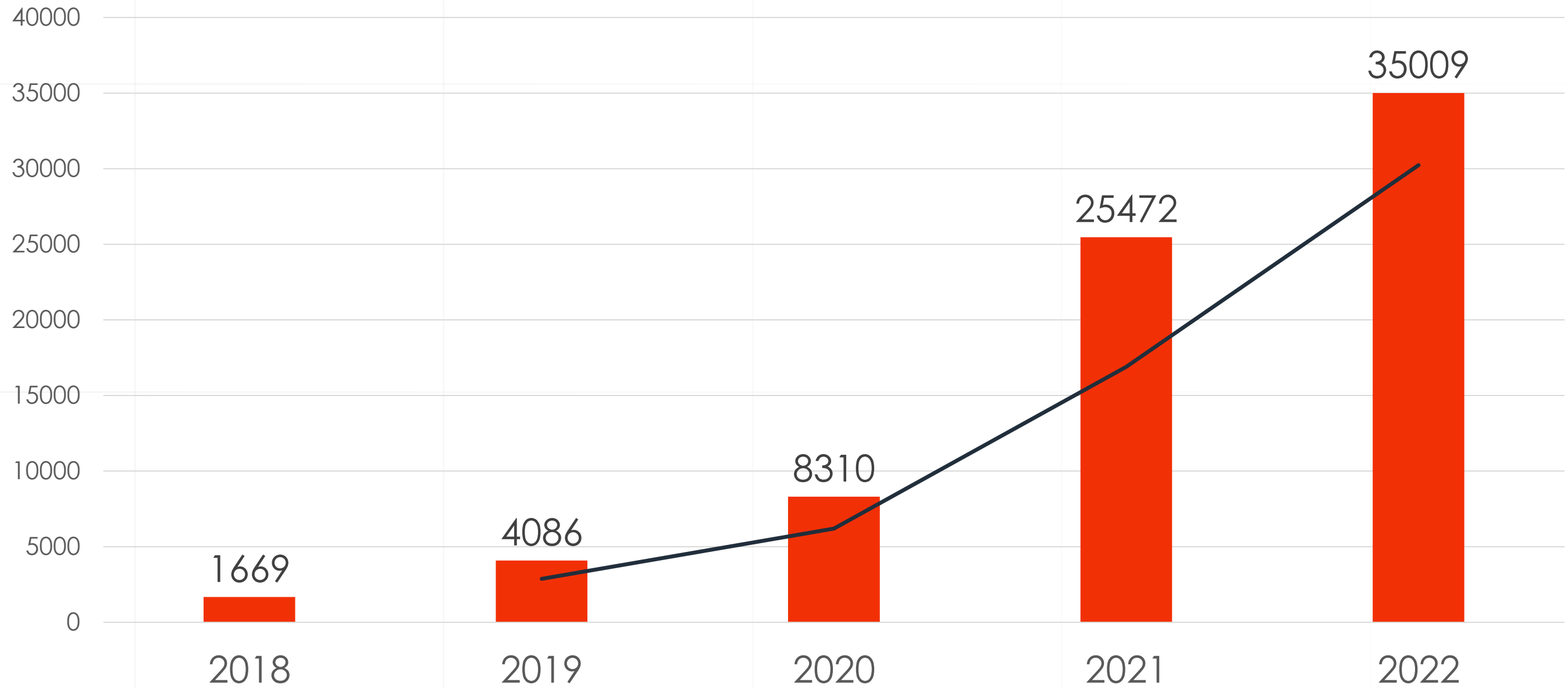
– Przeważnie podszywanie się pod inne osoby bądź instytucje.



– Cel: osiągnięcie korzyści majątkowej lub wyrządzenie innej osobie szkody.



Oszustwa zarejestrowane przez CERT Polska w latach 2018-2022



Phishing

— czyli o metodach ataku i socjotechnice

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



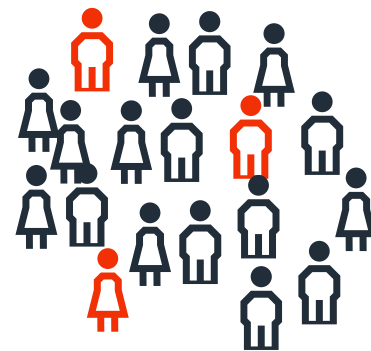
SMShing



Vishing



w reklamach,
ogłoszeniach,
w mediach itp.



masowy



spersonalizowany

Phishing masowy



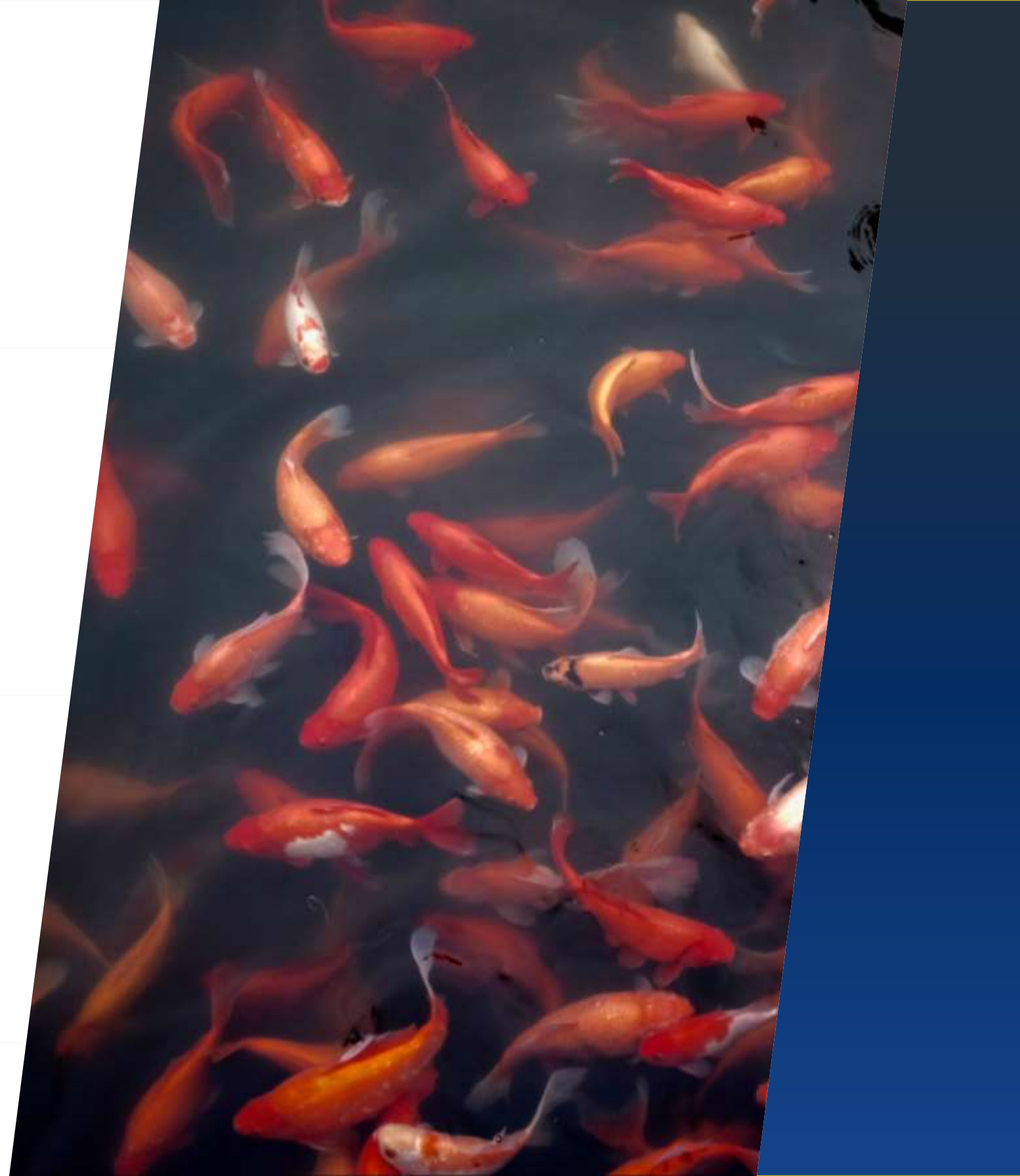
Wysyłka masowa, malspam.



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*)



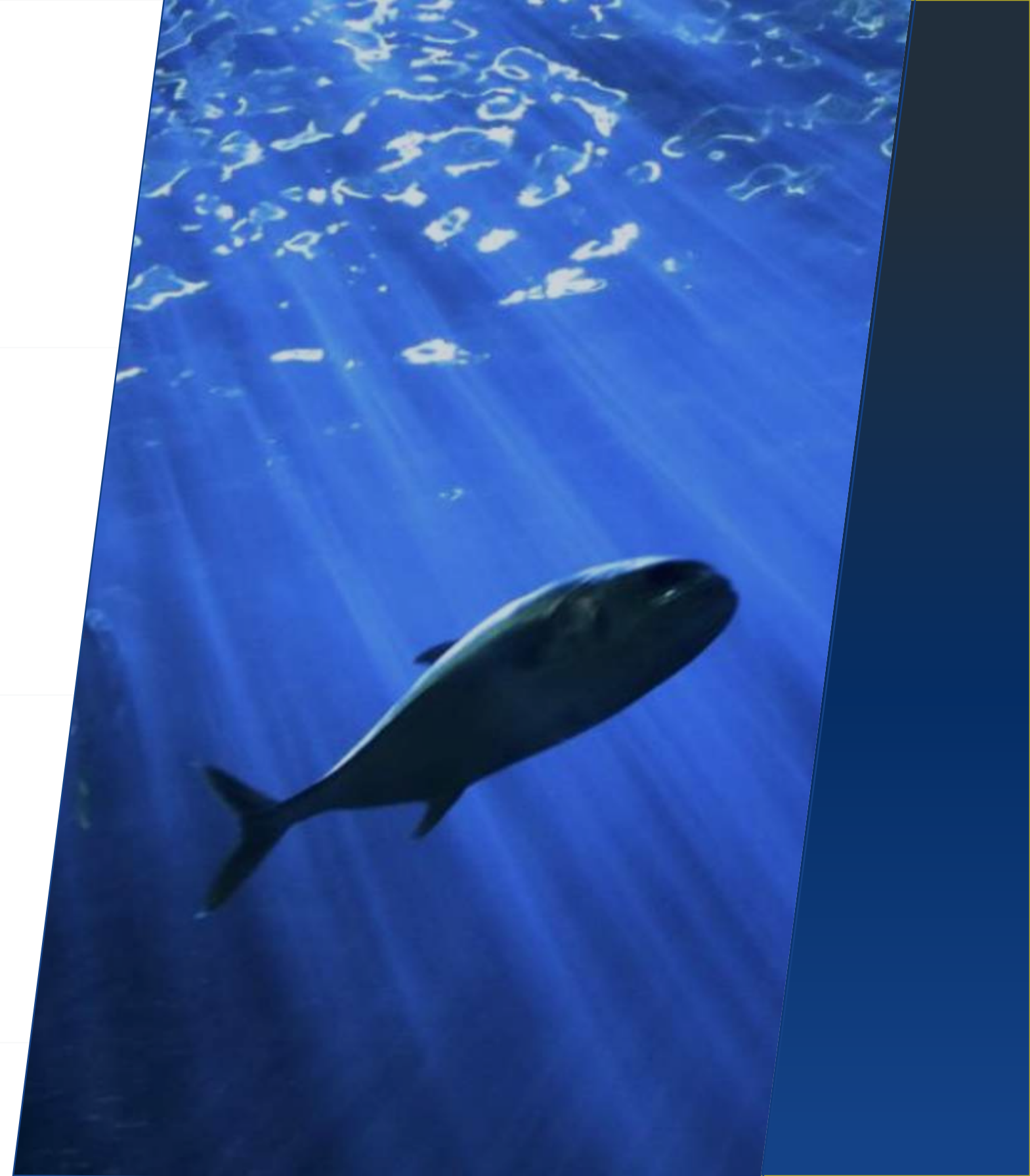
Precyzyjnie wybrany cel – osoba lub grupa;
duży jednorazowy zysk.



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!

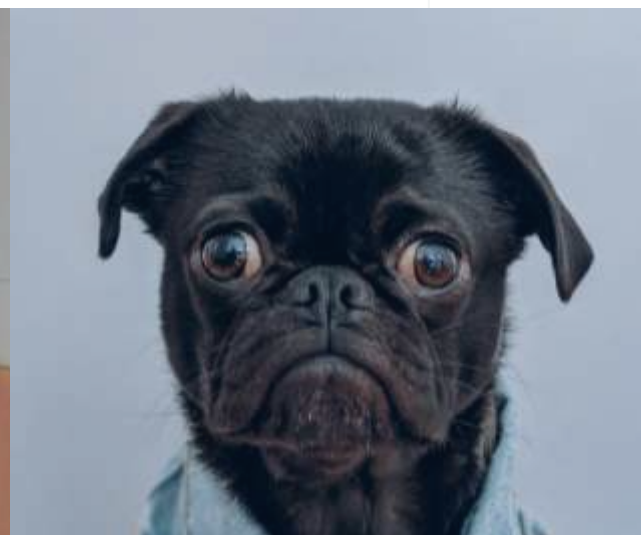
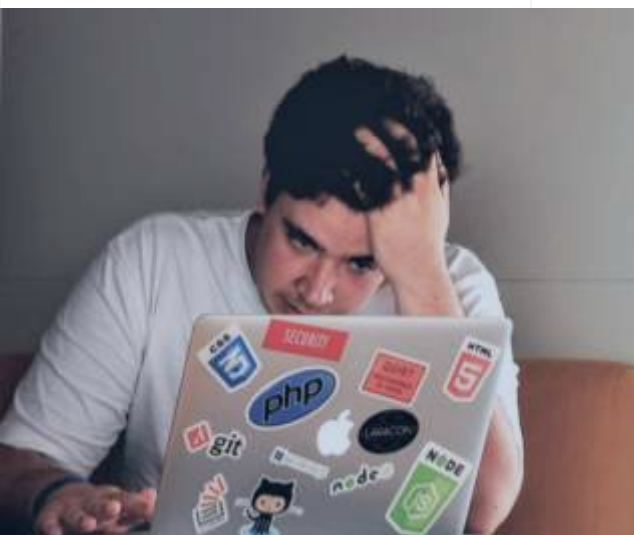
– Potrzebna jest twoja pomoc!

– 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 !**

Podjmij 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



Nowe powiadomienie o paczce Message 1 of 33

From: No-Reply <support@vertexplus.net>
To:
Date: Thu 14:40



Szanowny Kliencie

Dziękujemy za skorzystanie z Poczty Polskiej, Twoja przesyłka czeka na Ciebie. Należy dokończyć wpłatę (9,06 zł).

co muszę zrobić ?

Kliknij poniższy bezpieczny link, aby dokończyć uiszczenie opłat za wysyłkę

Przewidywany termin dostawy: 25 października przed końcem dnia roboczego.

Z poważaniem.
Obsługa klienta Poczty Polskiej.



- Uniwersalny pretekst
- „Zaufany nadawca”
- Czynniki wzbudzające emocje
- Link do strony

Co tu nie gra?



Dzień dobry,

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

Aby rozwiązać problem z odsetkami zaloguj się 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 odpowiadać 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.

Jeśli nie jesteś adresatem tej wiadomości:

- powiadom nas o tym w mailu zwrotnym (dziękujemy!);
- usuń trwale tę wiadomość (i wszystkie kopie, które wydrukowałeś lub zapisałeś na dysku).

Wiadomość ta może zawierać chronione prawem informacje, które może wykorzystać tylko adresat. Przypominamy, że każdy, kto rozpowszechnia (kopiuje, rozprowadza) tę wiadomość lub podejmuje podobne działania, narusza prawo i może podlegać karze.
mBank S.A. z siedzibą w Warszawie, ul. Prosta 18, 00-850 Warszawa, Sąd Rejonowy dla m. st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, KRS 0000025237, NIP: 526-021-50-88. Kapitał zakładowy (opłacony w całości) według stanu na 01.01.2022 r. wynosi 169.539.536 złotych.

If you are not the addressee of this message:

- let us know by replying to this e-mail (thank you!);
- delete this message permanently (including all the copies which you have printed out or saved).

This message may contain legally protected information, which may be used exclusively by the addressee. Please be reminded that anyone who disseminates (copies, distributes) this message or takes any similar action, violates the law and may be penalised.





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:

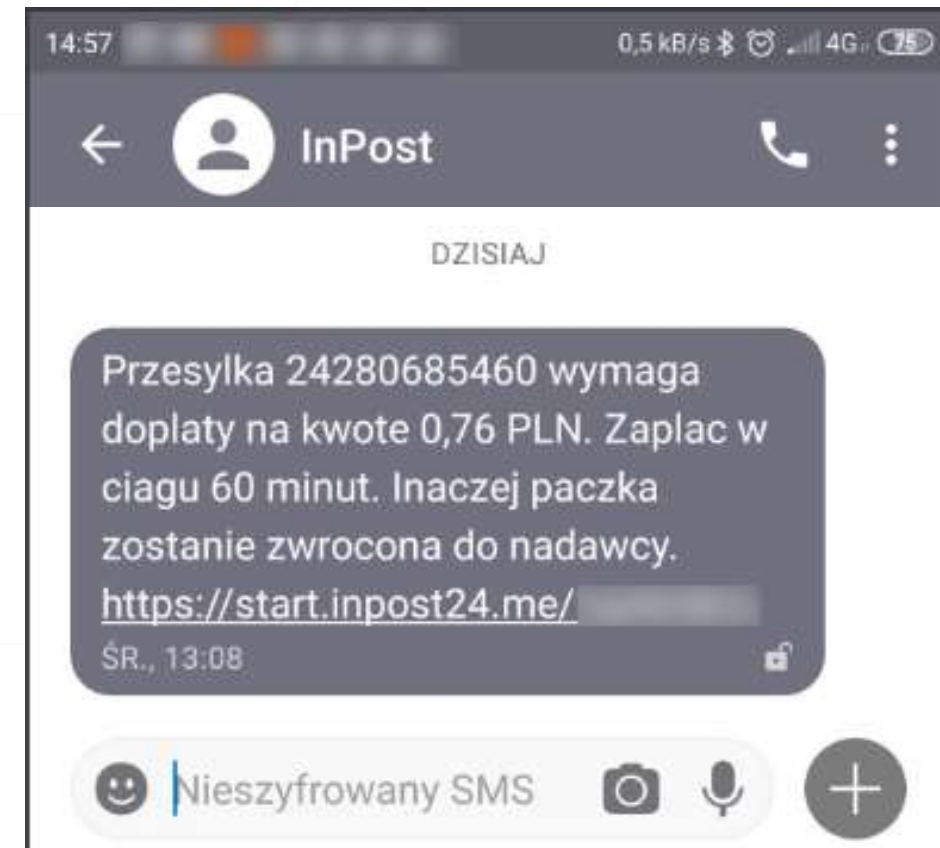
Zmiana adresu dostawy

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 zadłużenie w Urzędzie Skarbowym. Kwota 4,91 zł. Prosimy o wpłatę do dnia 29.03.2022 lub sprawa trafi do sądu.
<https://rachunek4212.net/412>

Przed chwilą

OSZUSTWO

+

+

SMS

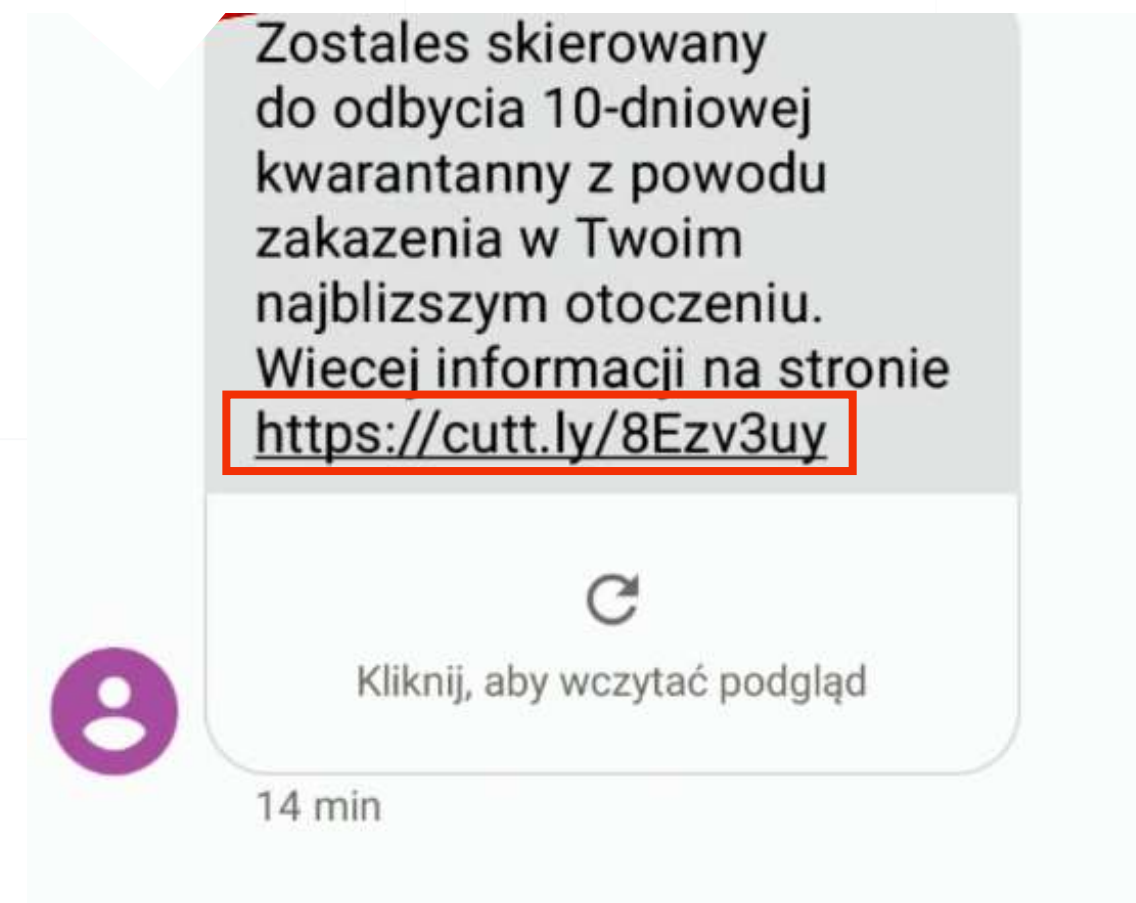
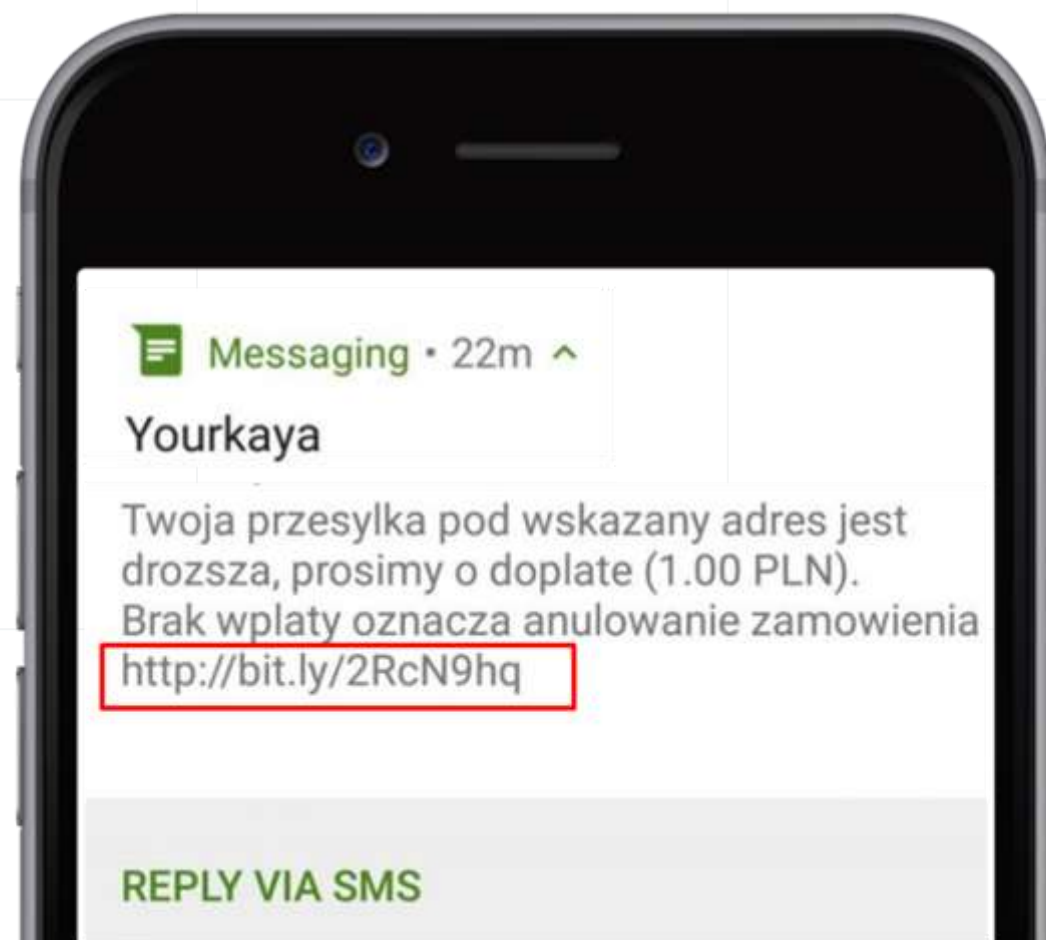
😊

🎤

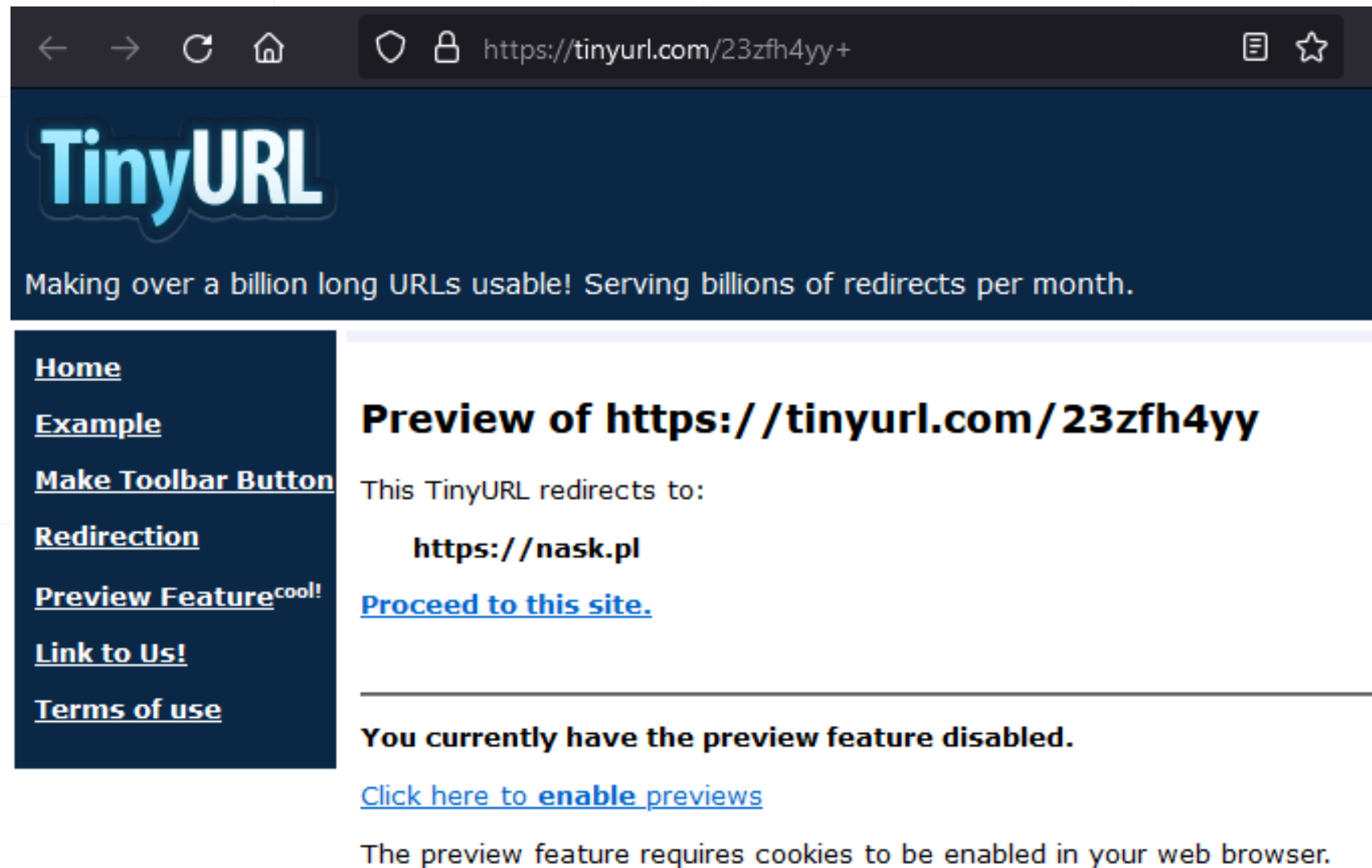
Witaj Mirosław. Otrzymujesz nagrodę w wysokości 150zł na kartę Moja Biedronka. Odbierz: <https://www.gang-bystrzakow.art/g/ang?w=0bEeb>

14:18

Skracarki linków



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



← → ↻ 🏠 🔒 https://tinyurl.com/23zfh4yy+ 📄 ☆

TinyURL

Making over a billion long URLs usable! Serving billions of redirects per month.

- [Home](#)
- [Example](#)
- [Make Toolbar Button](#)
- [Redirection](#)
- [Preview Feature^{cool!}](#)
- [Link to Us!](#)
- [Terms of use](#)

Preview of <https://tinyurl.com/23zfh4yy>

This TinyURL redirects to:

<https://nask.pl>

[Proceed to this site.](#)

You currently have the preview feature disabled.

[Click here to enable previews](#)

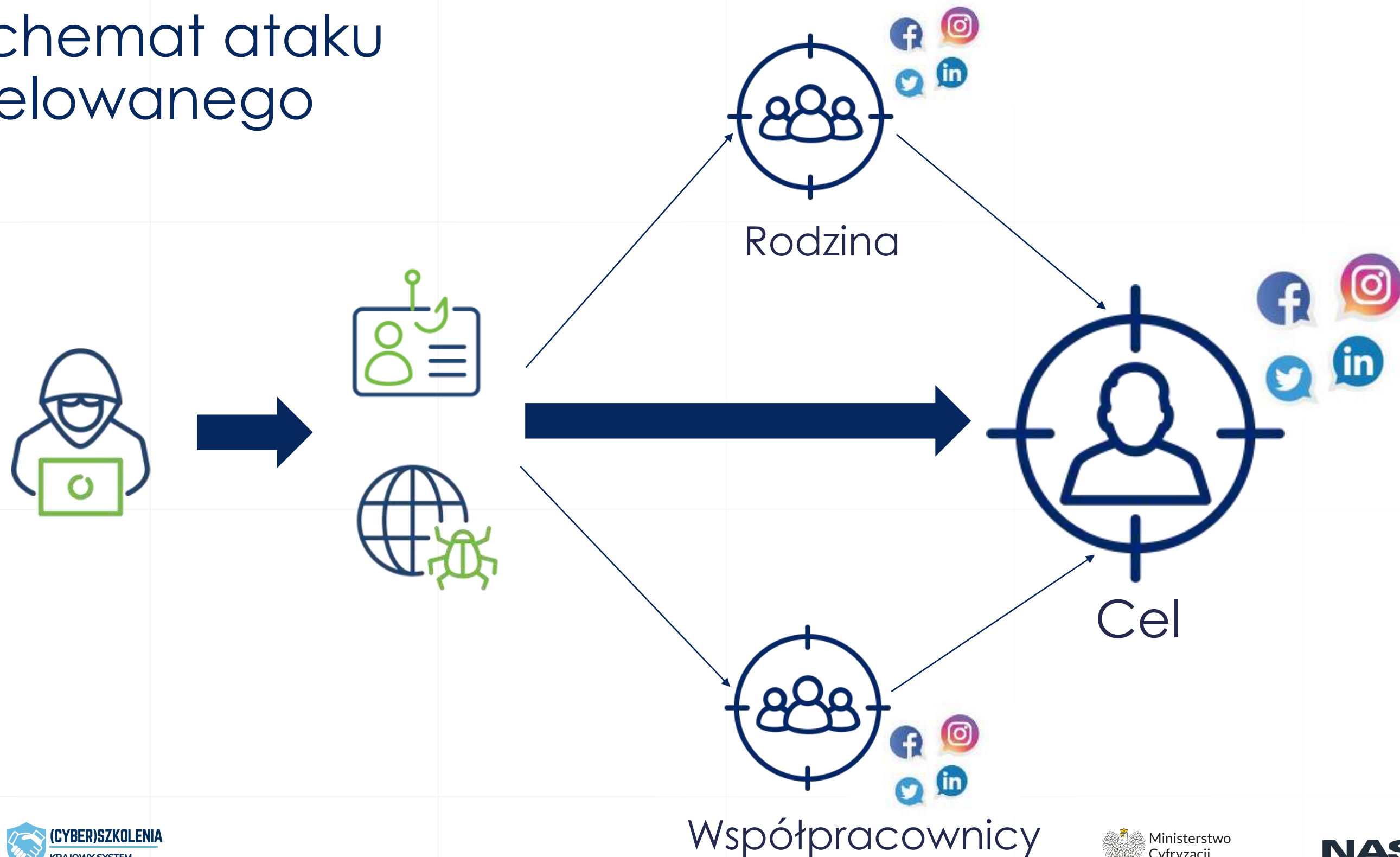
The preview feature requires cookies to be enabled in your web browser.



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 Rzęśnia padła ofiarą oszustwa. Z gminnej kasy wyparowało 5 milionów złotych.

Prokuratura Rejonowa w Wieluniu prowadzi śledztwo w sprawie zuchwałego oszustwa, do którego doszło w Urzędzie Gminy w Rzęśni. Z nieoficjalnych ustaleń wynika, że ze skarbnik Urzędu Gminy w Rzęśni 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*

Od Jacek ██████████ <officemails018@gmail.com> ☆

Temat **Pilne**

Do Skarbnik@██████████ ☆

Musimy dokonac pilnej platnosci w wysokosci 95 455,25 PLN. Czy mozemy dokonac tej platnosci dzisiaj?

Pozdrowienia
Jacek ██████████

From: ██████████ [mailto:officemail045@gmail.com]

Sent: Friday, July 5, 2019 8:27 AM

To: ██████████

Subject: Pilne

Musimy dokonac pilnej platnosci w wysokosci 75 455,25 PLN. Czy mozemy dokonac tej platnosci dzisiaj?

Pozdrowienia
██████████, ██████████

Spoofing

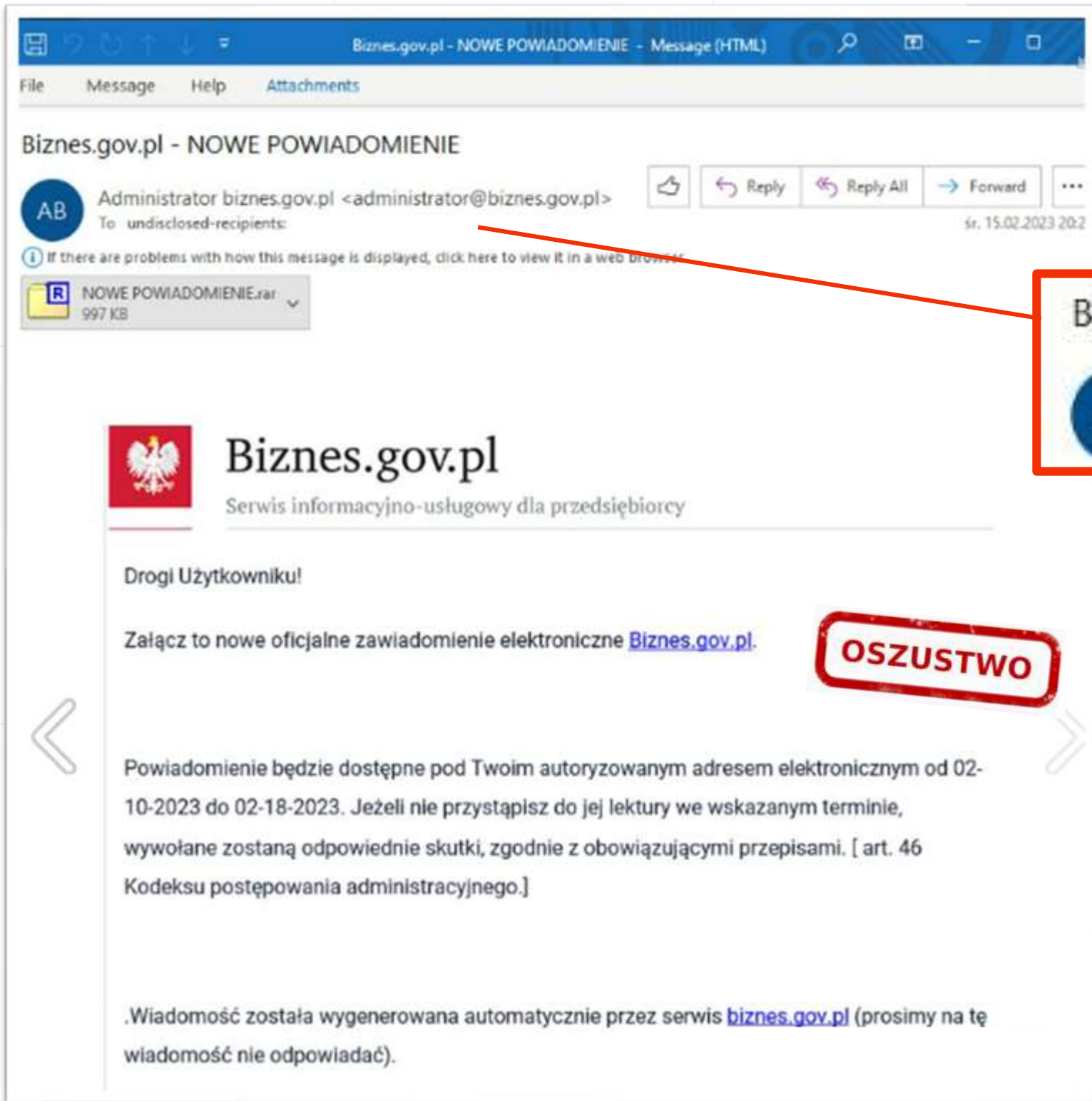
– podstawiony numer
lub nazwa nadawcy



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



Spooftng mailowy

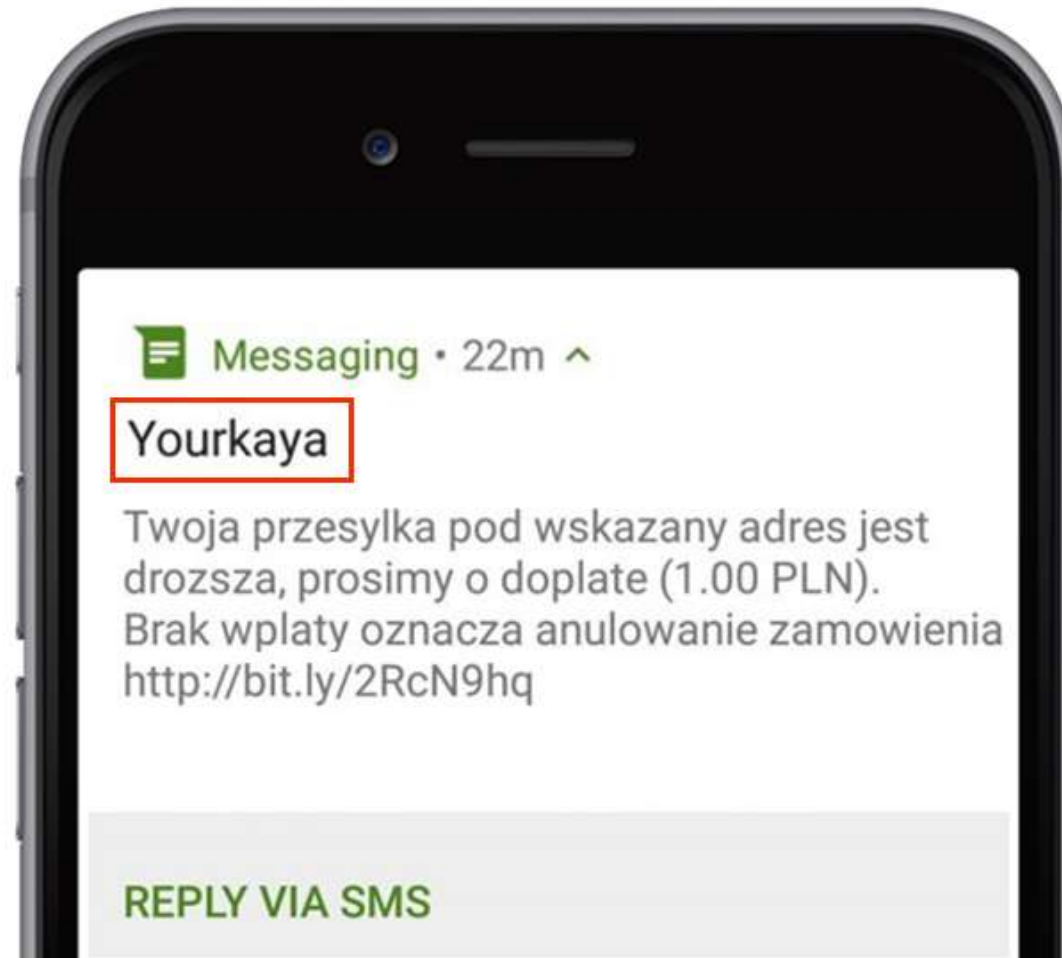


The screenshot shows an email interface with a blue header bar containing the text "Biznes.gov.pl - NOWE POWIADOMIENIE - Message (HTML)". Below the header, the email header information is displayed: "Biznes.gov.pl - NOWE POWIADOMIENIE", "Administrator biznes.gov.pl <administrator@biznes.gov.pl>", and "To: undisclosed-recipients:". A red box highlights this header information. The main body of the email features the Biznes.gov.pl logo and name, followed by the text "Drogi Użytkowniku!", "Załącz to nowe oficjalne zawiadomienie elektroniczne [Biznes.gov.pl](#)", and a red stamp that says "OSZUSTWO". The email concludes with a footer: ".Wiadomość została wygenerowana automatycznie przez serwis [biznes.gov.pl](#) (prosimy na tę wiadomość nie odpowiadać)."

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

Spooftng telefoniczny

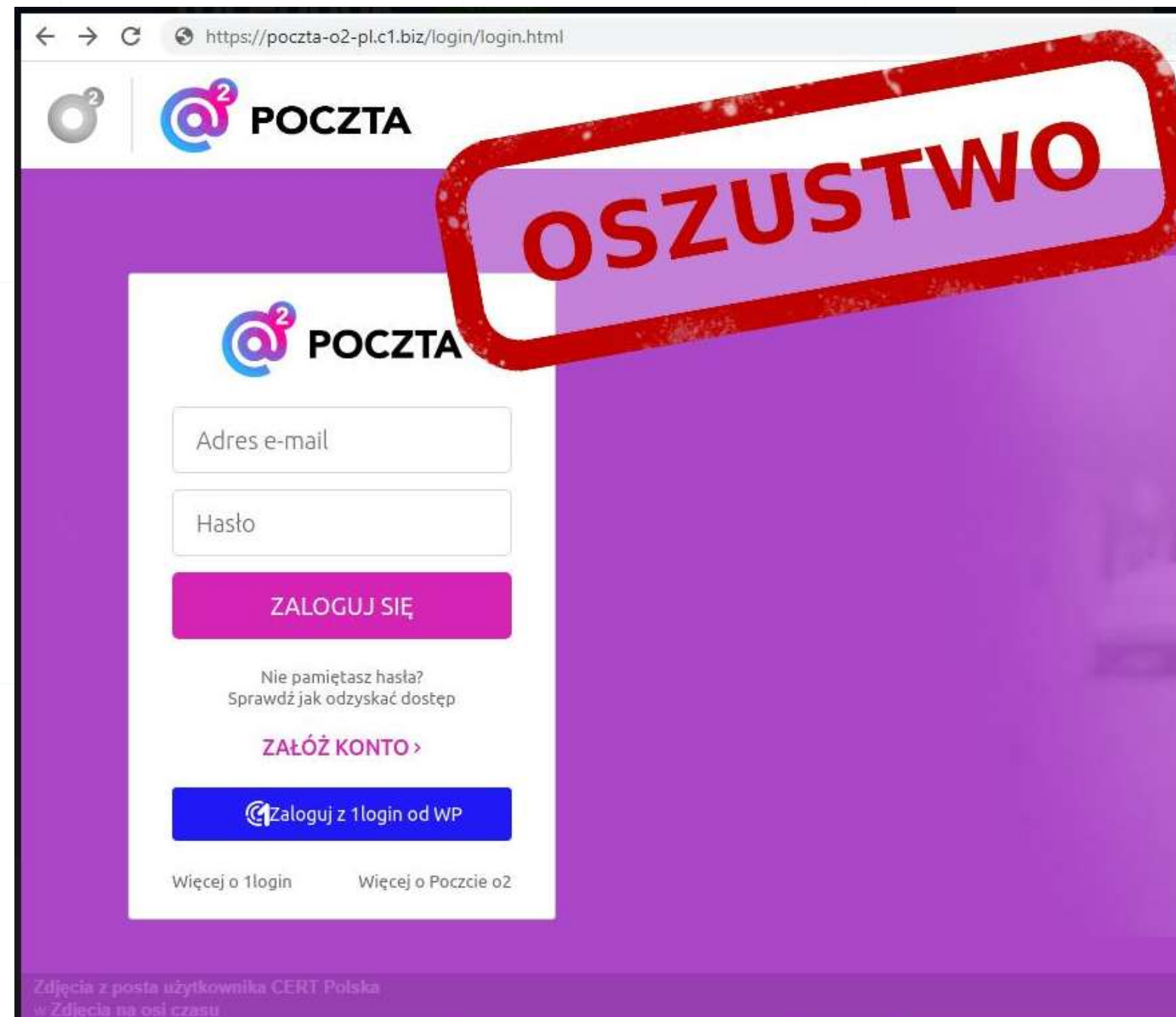
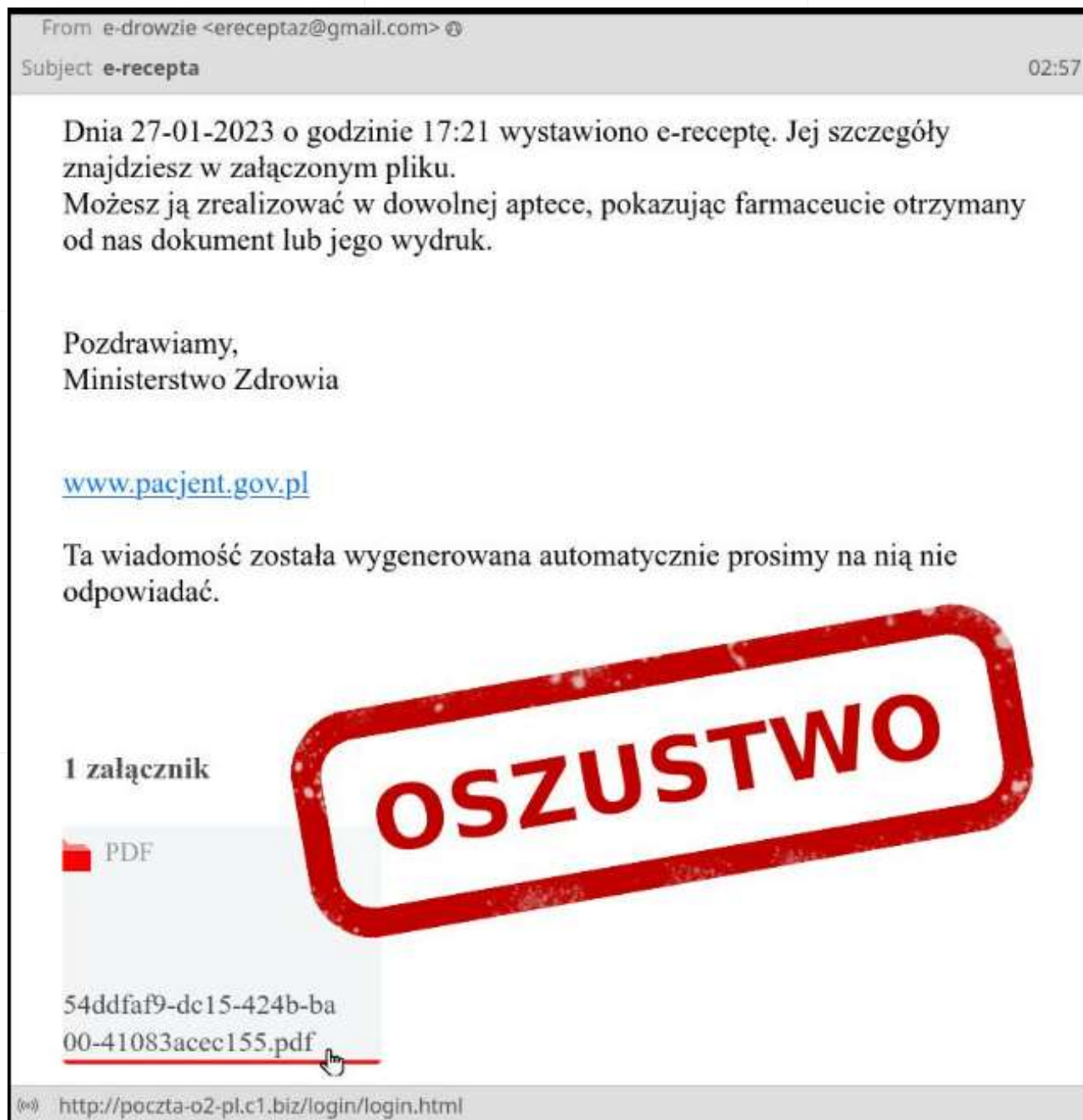
Występuje często!

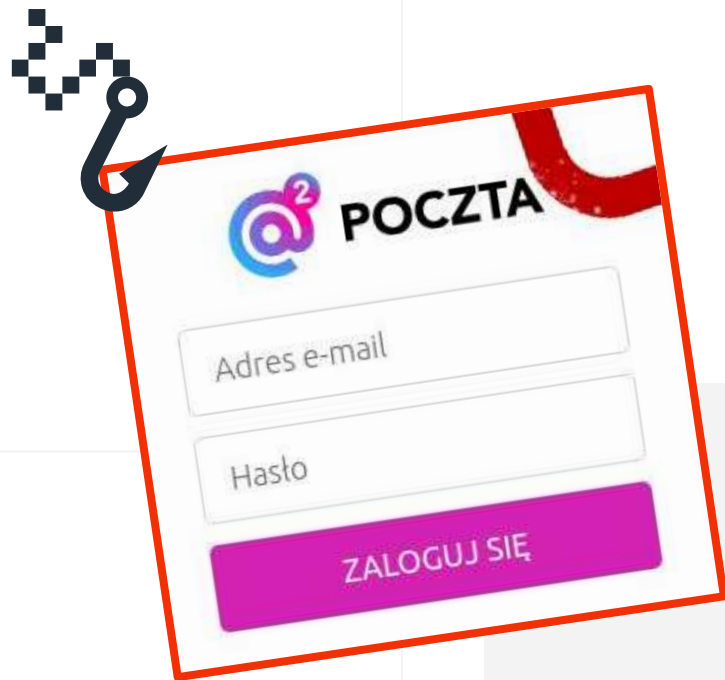




Co jeśli dasz się złapać?

Phishing masowy – o co tak naprawdę chodzi...





adamek*****@o2.pl

adam*****@o2.pl

adame*****@o2.pl

adame*****@o2.pl

adamekwitk*****@o2.pl

adame*****@o2.pl

adamia*****@o2.pl

adamia*****@o2.pl

no*****

12*****

me*****

ad*****

fb*****

la*****

ku*****

ly*****

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



Płatności online

Zamierzasz uregulować należność za paczkę oczekującą w Paczkomacie. Poniżej znajdziesz szczegóły płatności.

Paczka numer:

604086896000449218079098

Wartość pobrania:

0,50 zł

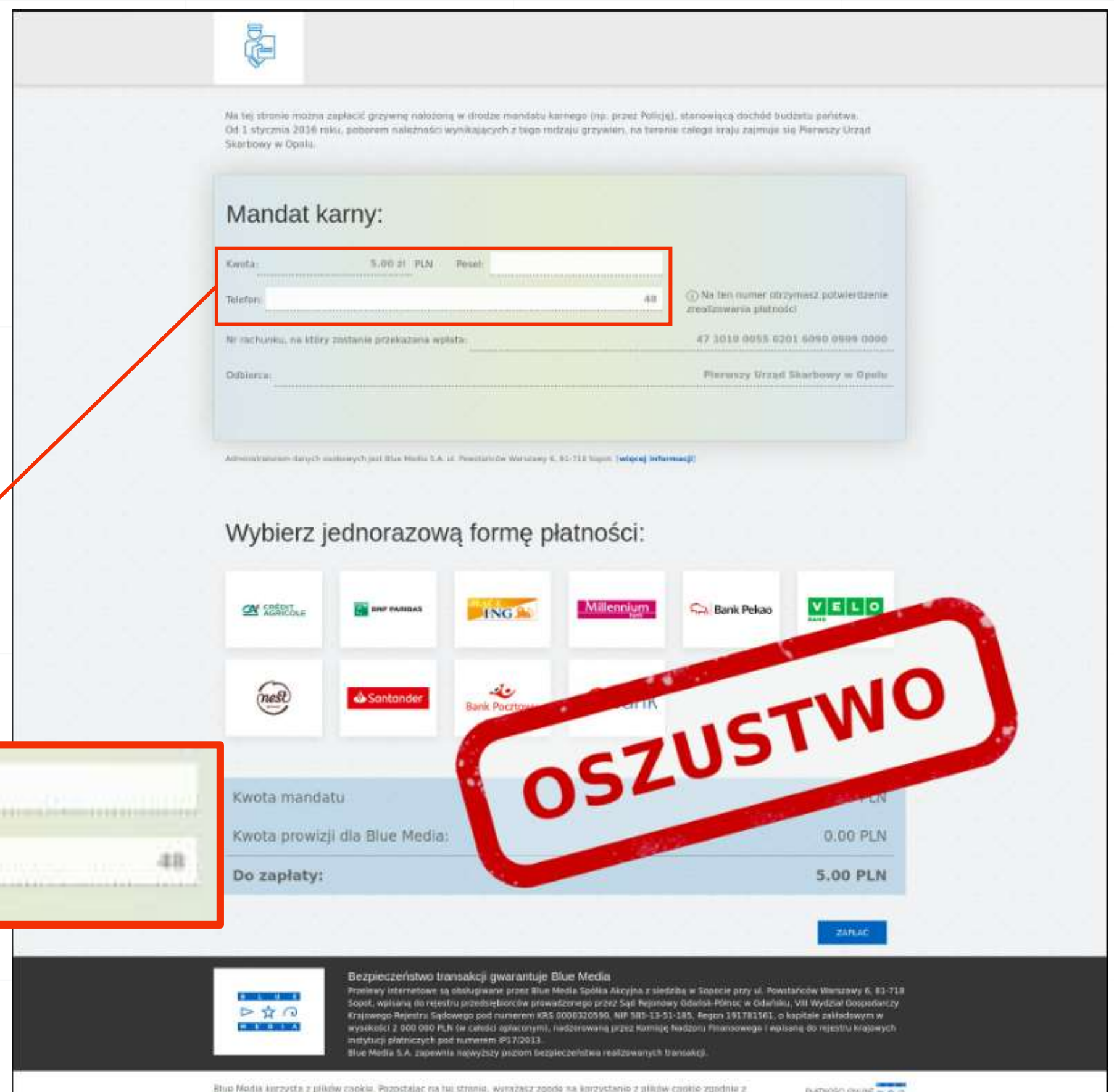
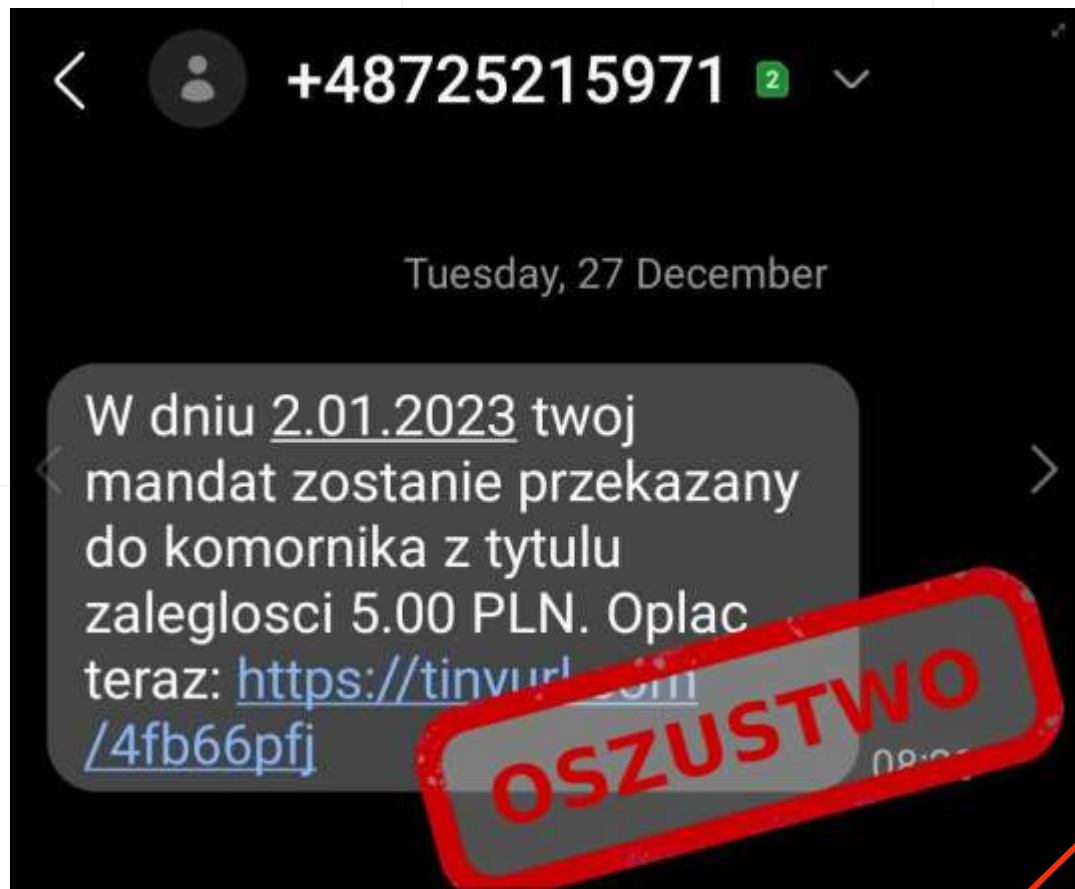
Imię

Nazwisko

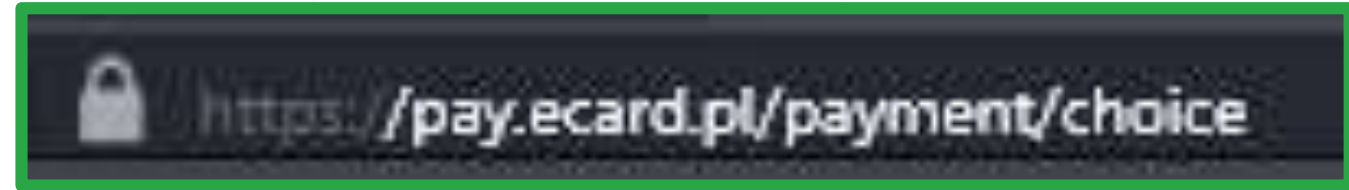
Akceptuję regulamin

Dalej

REZYGNUJĘ



Fałszywe bramki e-płatności



https://kiporta.online/pge/pay.php

e
CARD www.ecard.pl

DANE NABYWCY
48779457345

CENA
3.46 zł

SPRZEDAWCA
Sprzedawca
© PGE Polska Grupa
Energetyczna SA

Przelew szybki **Wybierz sposób płatności**

BANK SPÓŁDZIELCZY W BRZOZOWICY

Akceptuję postanowienia [Regulaminu rozpatrywania reklamacji Klientów eCard S.A.](#)

Dalej →

Transakcje autoryzuje eCard S.A. Gwarancja bezpieczeństwa

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, że administratorem Pani/Pana danych osobowych jest eCard S.A. z siedzibą w Warszawie, ul. Czackiego 7/9/11.

10:25 AA Niezabezpieczona — paczkomat24.xyz

e
CARD www.ecard.pl

DANE NABYWCY
Test Test

CENA
0.50 PLN



SPRZEDAWCA
InPost Sp. z o.o.

Wybierz sposób płatności
Przelew szybki


Fałszywe panele płatności kartą

https://esigner.siamapp.net/inpostsrv/gateway.php?data=payment

InPost Pokaż szczegóły









Transakcje są autoryzowane przez eCard S.A.  

PEŁNE IMIE I NAZWISKO
Adam

NUMER KARTY
XXXX XXXX XXXX XXXX 

TERMIN WAŻNOŚCI CVC2/CVV2
MM / YY CVC

Potwierdź płatność



Zwrot środków - dane bankowe beneficjenta

OGÓLNE INFORMACJE

Odbiorca zwrotu
Jak otrzymać
Liczba plików
Kwota Refundacji
Data
Warunki płatności

Karta kredytowa
XXXX - XXXX - XXXX - XXXX

Termin ważności
-- / ----

CVV (3 Dane na odwrocie)
XXX

Naprzód

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	FI	Poland	10.00 \$
[03.07.2022] dispute MIX Refundable CVR 41%	557511	01/2024		UNKNOWN	NA	Zwoler...Błh	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	WaU0142Brzych	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	Bielskobaaa	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

Bank Pekao Nie masz konta?

Logowanie do Pekao24  

WPISZ NUMER KLIENTA / NAZWĘ UŻYTKOWNIKA 

Dalej

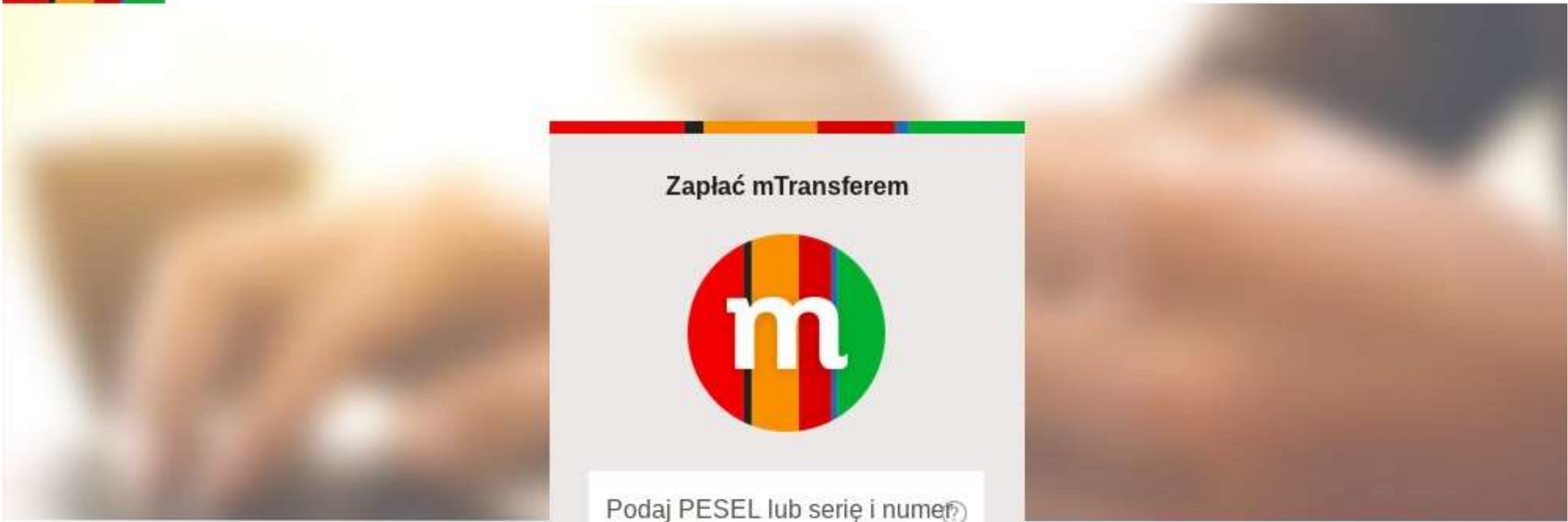
02.04.2022 Ostrzegamy przed wiadomościami SMS od nadawców podszywających się pod Bank Pekao S.A. [Więcej>](#)

25.02.2022 W niektórych agencjach Western Union w Ukrainie odbiór przekazu pieniężnego może być niedostępny ze względu na nieczynne placówki. [Więcej>](#)

Aplicacja PeoPay

[Bezpieczeństwo](#) [Pomoc w logowaniu](#)

801 365 365 +48 22 59 12 232 [Bezpieczeństwo](#) [RODO](#) [Polityka prywatności](#) [Kontakt](#)



Zapłać mTransferem



Podaj PESEL lub serię i numer
Paszportu

Podaj nazwisko panięńskie
Twojej matki

Zaloguj się



Wpisz, czego szukasz

POŻYCZ GOTÓWKĘ

ZAŁÓŻ KONTO

LOGOWANIE

- Konta
- Karty
- Kredyty
- Oszczędności
- Inwestycje
- Ubezpieczenia
- Bankowość elektroniczna
- Wsparcie
- Kontakt

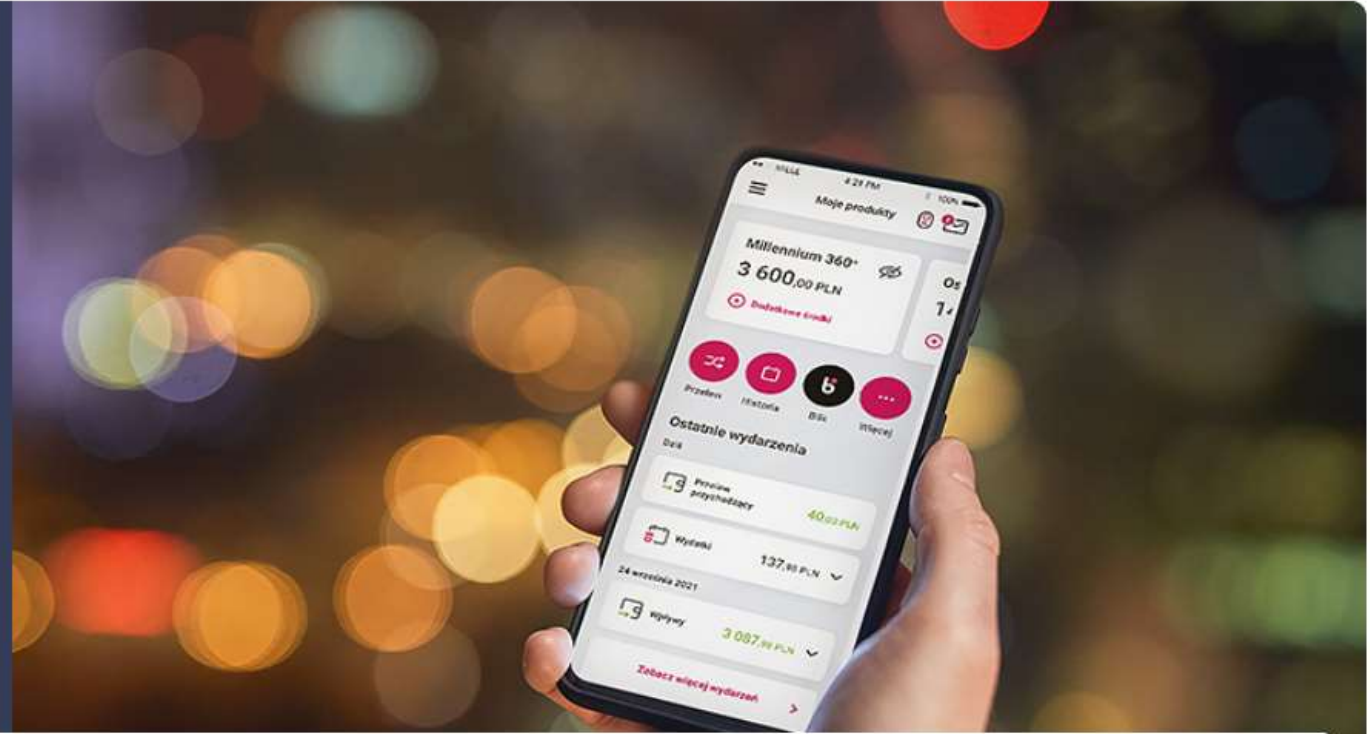
Otwórz się na **nowe możliwości**

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

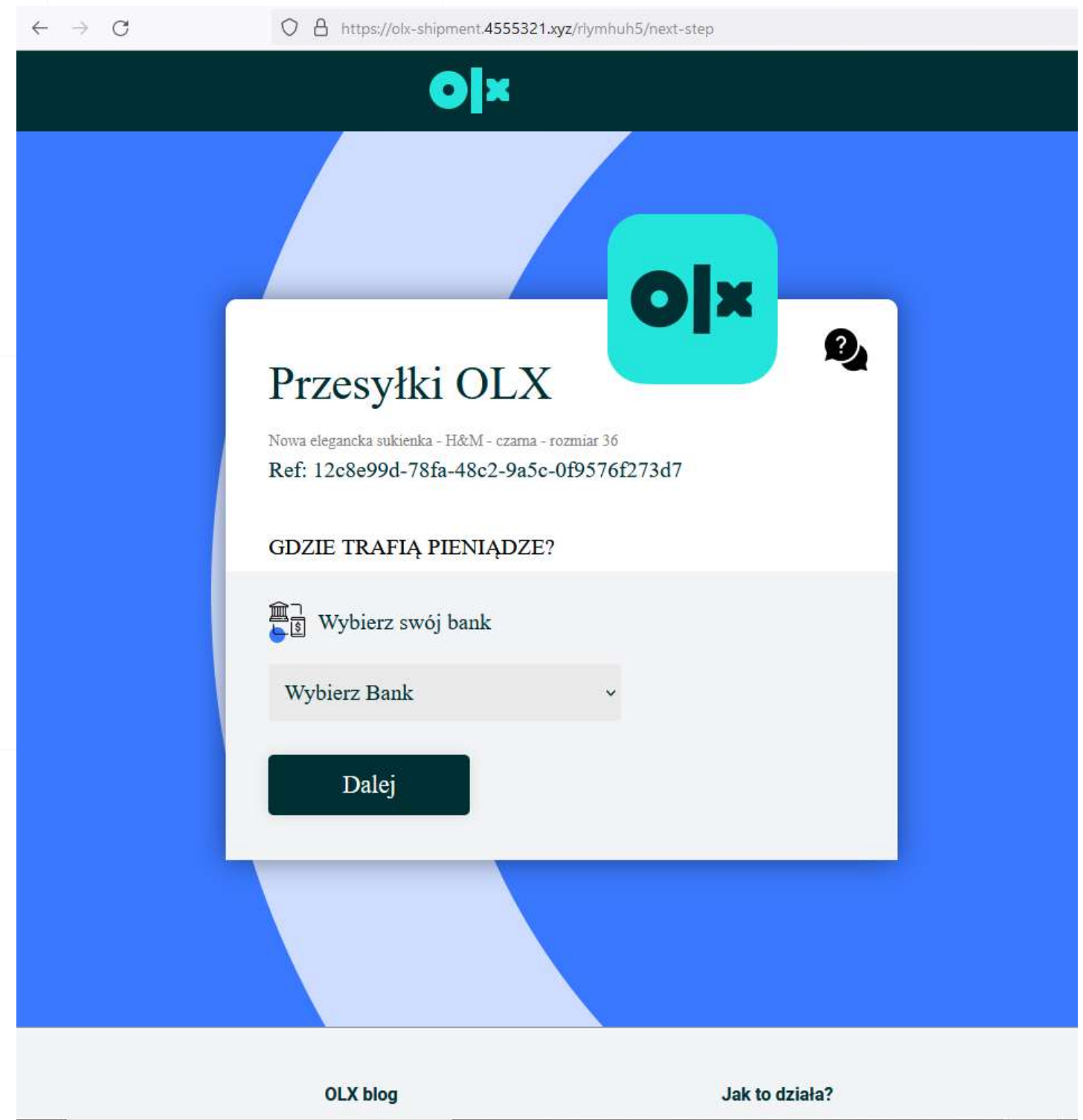
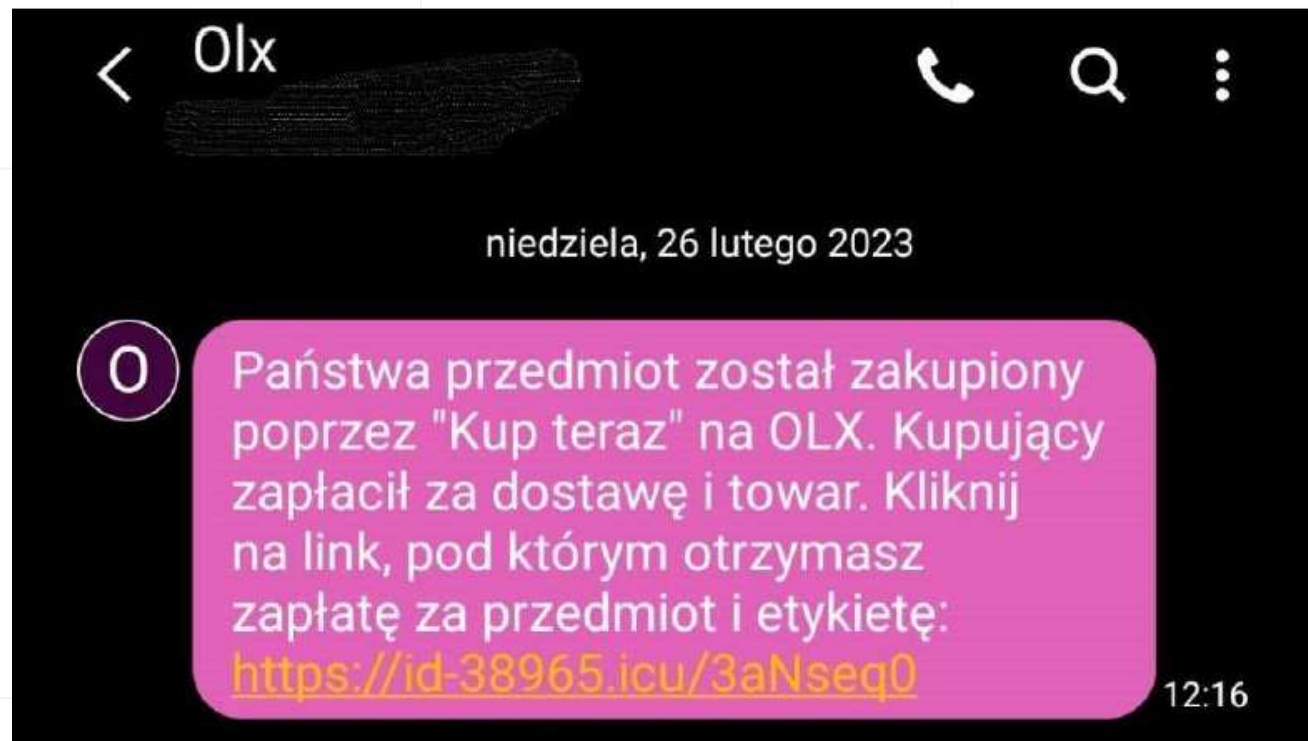
POŻYCZKA GOTÓWKOWA (RRSO 12,83%)
Promocja do 20 stycznia 2023

ZWROTY ZA ZAKUPY
Przemysłany sposób na zakupy

Phishing a popularne usługi

czyli częsty pretekst w phishingu masowym





From Allegro <powiadomienia197123@allegro.pl>

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/PL/N/PLN/2023/01

Dokument znajdziesz w zakładce Moje konto > Rachunki > [Faktury](#).

[PRZEJDZ DO FAKTUR](#)

Pozdrawiamy
Allegro



Wiadomość wysłana przez Allegro <powiadomienia197123@allegro.pl>



Dodatkowe informacje

- Historię swoich wszystkich operacji możesz sprawdzić w zakładce [Rozliczenia z Allegro](#).
- Fakturę reguluj zgodnie z polem „Razem kwota do zapłaty”.

Masz pytania? [Skorzystaj z Pomocy Allegro](#)





Kupujący już zapłacił za Twój przedmiot.

Odbierz swoje pieniądze teraz



Suknia sprzedam

250.0 PLN

Twój przedmiot jest opłacony

Imię i nazwisko kupującego!

Anna Wychik

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.



Otrzymanie środków

Kwota do otrzymania: 250.0 PLN

Suknia sprzedam

Zdobądź pieniądze



Dokonywanie płatności jest bezpieczne

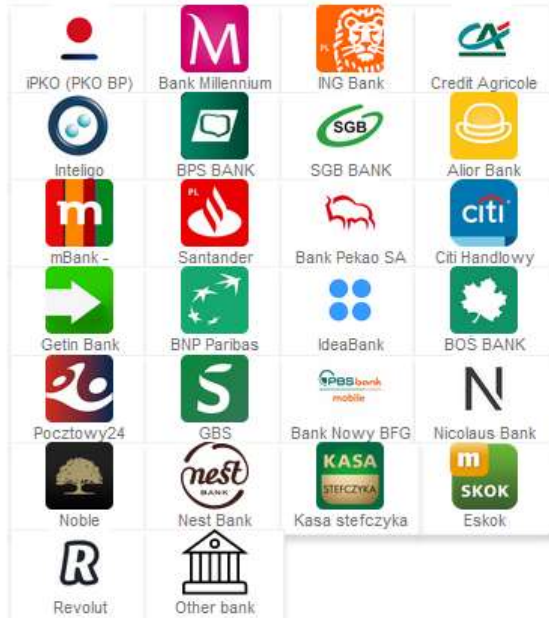


Numer ogłoszenia: 2353182057



ZADEKLAROWANA WARTOŚĆ
200 PLN

Przelewy online



Przedmioty ▾

🔍 Szukaj przedmiotów

Kobiety Mężczyźni Dzieci Vinted

Przesyłki Vinted

Sukienka M

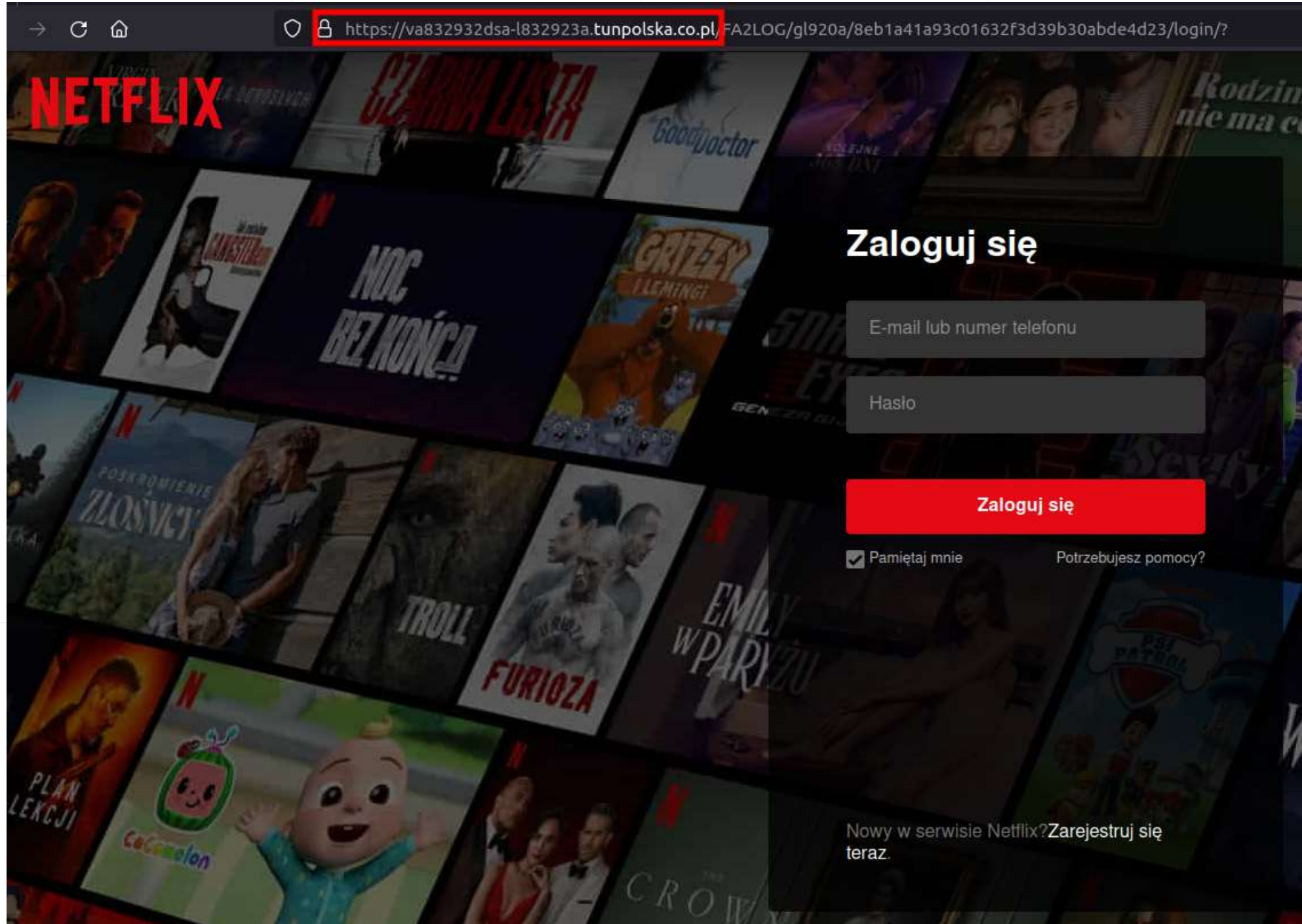
70792b30-b86f-49c4-8bd4-6caeecec0055e

Gdzie trafią pieniądze?

Wybierz swój bank

Wybierz bank ▾

- Wybierz bank
- iPKO
- ING
- Millennium
- Banki spółdzielcze
- Santander
- Pekao24
- Credit Agricole
- BNP Paribas
- Pocztowy
- Inteligo
- Boss



Metoda „Browser in the Browser”

The screenshot illustrates a "Browser in the Browser" attack on the onet.pl website. A secondary browser window is overlaid on the main page, displaying a registration confirmation form for an onet account. The URL of the secondary window is <https://konto.onet.pl/weryfikacja>, which is highlighted with a red box. The main page shows news articles and navigation menus.

onet POCZTA

<https://konto.onet.pl/weryfikacja>

KONTO

Potwierdzenie danych rejestracyjnych

Potwierdź dostęp do swojego konta

Adres email

Zapasowy adres email

Imię i nazwisko właściciela konta

Data rejestracji konta

DALEJ

NIE MASZ JESZCZE KONTA?

o TYM SIĘ MÓWI

Duda radzi Polakom "zaciskać" i "myśleć pozytywnie". Tak zareagują

Skandaliczne słowa kardynała. Usprawiedliwia gwałty Rosjan

Tajemnica skrytka. Za gotówkę

"Polski Dubaj" kosztował 170 mln zł. Najpiękniejsze plaże w Polsce

"Panuje tu zemsta plemienna. Ludzie są zabijani, kobiety gwałcone"

Ataki w mediach społecznościowych

Drastyczne i szokujące posty

MEBLE UŻYWANE I GRATY WARSZAWA

17h

Hania została zgwałcona... Musicie nam pomóc, szukamy sprawcy, w artykule jest nagranie z tego zdarzenia :(Jeśli możesz, udostępnij ten post gdzie się da, w innych grupach, u siebie na profilu... Razem uda się na pewno



WIADOMOSCI.WP.PL

Szukają podejrzanego o gwałt na nieletniej. Policja prosi o pomoc

Policjanci z Łodzi prowadzą poszukiwania mężczyzny podejrzanego o gwałt na nieletniej dziewczynce...

10 Comments 216 Shares

Like Comment Share

Grupa Stary dawny Szczecin

7m

w 14 sekundzie widać, że panu komornikowi się chyba podoba, tak jęczy i się wypina hahah, albo to ból. W sumie gościu z marszu ściągnął spodnie, i mu włożył hahahah



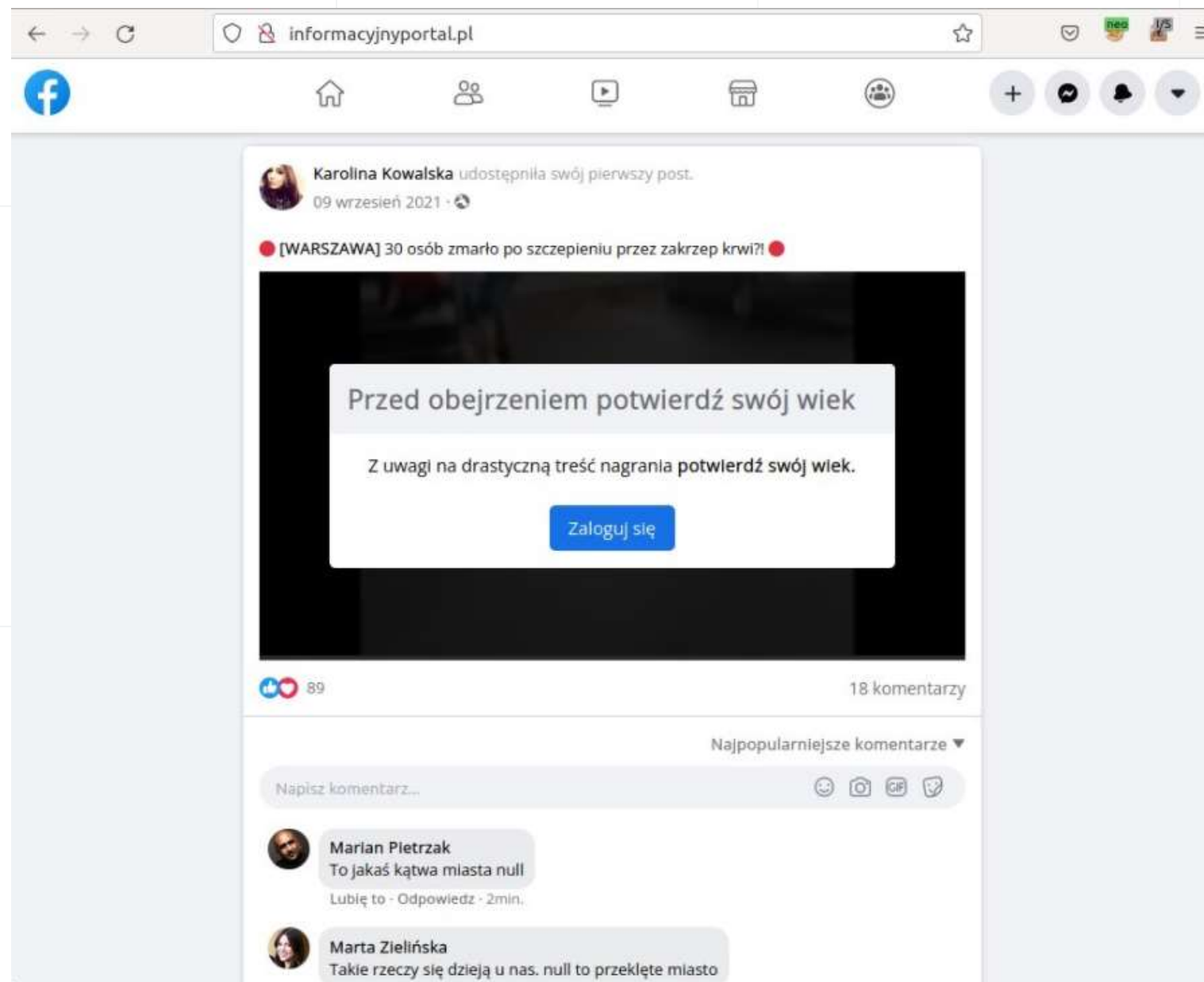
PUDELEK-ONET-43856872713.AZUREEDGE.NET

Szczecin: 42 latek zgwałcił Komornika , całą sytuację nagrał i udostępnił w sieci. [WIDEO]

1

Like Comment Share

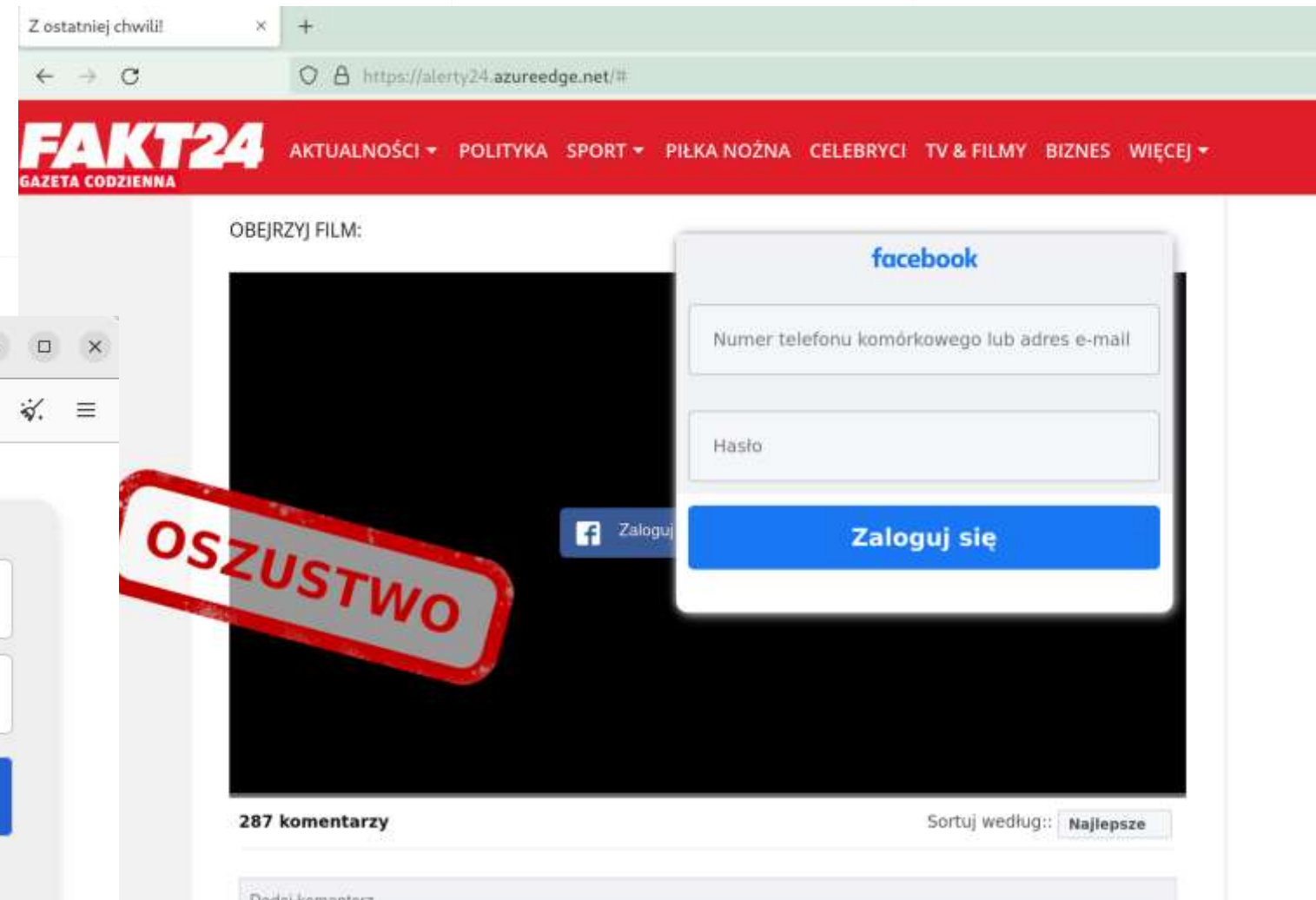
„Konieczność potwierdzenia wieku”



...lub inny dowolny pretekst:

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

Fałszywy panel logowania



facebook

Aby przejść do serwisu oddaje-polakom.pl należy się zalogować.

A screenshot of a fake Facebook login form. It features a light gray background with a white input field for 'Numer telefonu komórkowego lub adres' and another for 'Hasło'. Below these fields is a blue button labeled 'Zaloguj się'. Underneath the button, there is a link 'Nie pamiętasz hasła?' and the word 'lub' followed by a green button labeled 'Utwórz nowe konto'.

W efekcie – paczka danych: e-mail + hasło

```
1 [redacted]:brasseur
2 ei[redacted]jn.co.uk:LAUREN17
3 m[redacted].com.lb:damika
4 sh[redacted]ndia.com:ramaswami
5 a.l[redacted]n.de:ljulian~
6 ar[redacted]os.fr:arnaud45
7 ca[redacted]ly.dk:charlie
8 sw[redacted]re.com:blueskies131
9 ste[redacted]ld.com:steve123
10 nc[redacted]p5.it:london2007
11 dav[redacted]ld.com:spooky
12 th[redacted]e.at:123456
13 hen[redacted]land.nl:Maandag03
14 gi[redacted]ia.it:tinaiese
15 ig[redacted]nals.com:Kaesar22
16 kn[redacted]wl.com:latoya
17 ma[redacted]ader.com:me2009
18 ly[redacted]th.com:diamonds
```

– troyhunt.com

Konkursy, loterie, bony w wiadomościach prywatnych

Cześć Patrycja 😊
Biedronka daje darmowe bony na zakupy w ich sklepie za wypełnienie darmowej prostej ankiety tutaj: biedronka-podarunek.eu ❤️

W tym przypadku nadawcą jest „ktos ze znajomych”.



Biedronka
Człowiek widać serce

Wygraj bon o wartości 2000zł

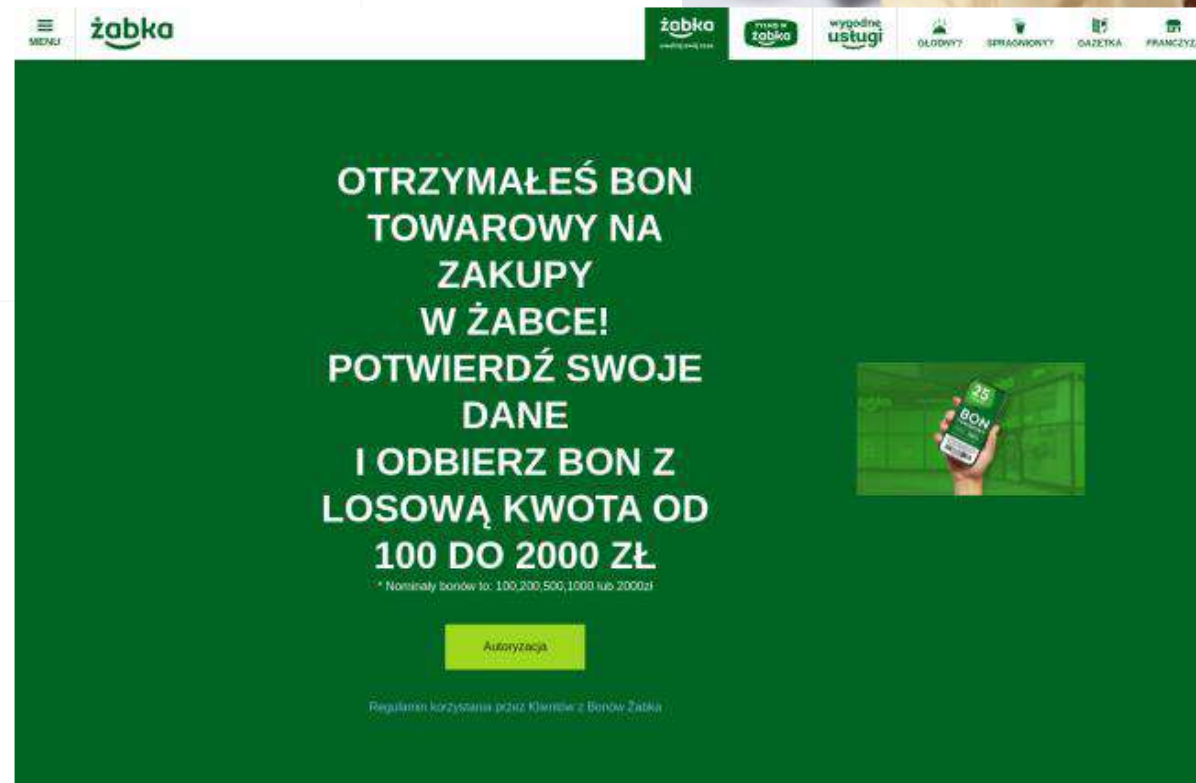
Zaloguj się do twojej szansy na wygranie!

E-mail: _____

Wyrażam zgodę na otrzymywanie za pośrednictwem poczty elektronicznej oraz drogą telefoniczną, włącznie z wiadomościami sms, i pocztową ofert wybranych Sponsorów, którym udostępniły Pana/Pani dane. Klikając tutaj można zapoznać się z należącymi do nich firmami.
Tym samym zezwalam na wykorzystanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego.

Aby uzyskać dostęp do strony bez otrzymywania wiadomości o charakterze marketingowym, należy kliknąć tutaj.

DARMOWA REJESTRACJA



żabka

OTRZYMAŁEŚ BON TOWAROWY NA ZAKUPY W ŻABCE! POTWIERDŹ SWOJE DANE I ODBIERZ BON Z LOSOWĄ KWOTA OD 100 DO 2000 ZŁ

* Nominały bonów to: 100,200,500,1000 lub 2000zł

Autoryzacja

Regulamin korzystania przez Klientów z Bonów Żabka

<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 **uwaga** oraz **uwierzytelnienie dwuskładnikowe** przy logowaniu.

Dezinformacja w mediach społecznościowych

#WłączWeryfikację

← #WłączWeryfikację 167 Tweetów

#STOPdezinformacji
#WłączWeryfikację

NASK

Obserwuj

#WłączWeryfikację
@WeryfikacjaNASK

Weryfikacja informacji w infosferze

Profil administrowany przez Państwowy Instytut Badawczy NASK

nask.pl/wlaczweryfikac... Dołączył/a luty 2022

3 Obserwowanych 22,8 tys. Obserwujących

Obserwowany przez Jarosław Olszewski, Paweł i 15 innych użytkowników, których obserwujesz

#WłączWeryfikację @WeryfikacjaNASK · 19 g.

⚠️ Budowanie antagonizmów między Polakami a Ukraińcami może być częścią akcji dezinformacyjnej.

➡️ Apelujemy o zwiększenie uwagi na pojawiające się treści i zgłaszanie podejrzanych profili.

#STOPfakenews

ALERT DEZINFORMACYJNY

NASK

#STOPfakenews

Foliarz Warszawski @FoliarzWawa

W Polsce panem jest Ukraińiec. Polak jest śmieciem, psem, popychadłem, ma nosić kaganiec. Czy takiej Polski chcemy, wroziej i nieprzyjaznej dla własnych obywateli i służącej obcym? @PKPIntercityPDP, to też pytanie do was.

Treść wpisu może być częścią akcji dezinformacyjnej

8 46 85

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

Fałszywe reklamy

— jak nie dać się złapać na świetną okazję

Reklamy „inwestycyjne”

PKP Grupa
Sponsorowane

Jak zarobić 20 tys. złotych z PKP Intercity?

3 miesiące temu przedstowaliśmy nowy projekt, który pomoże nam rozwijać firmę, wzbogacając przy okazji każdego inwestor.

Rozwijajcie kraj razem z nami.

GRUPA **PKP**

INWESTUJ Z GRUPĄ PKP
1000 ZŁ

ODBIERZ MIESIĘCZNIE
12300 ZŁ

TRUGARY.COM
Recaptcha

Więcej informacji

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

 **Poland D**
Sponsorowane

Nowy oficjalny projekt przy wsparciu polskich władz otwiera Polakom dostęp do akcji spółki. Teraz możesz zostać udziałowcem spółki i osiągać przychody od 13 tys. zł tygodniowo.



Dostęp do akcji PGNiG jest otwarty dla wszystkich Polaków

Nowy oficjalny projekt

 MINISTERSTWO ENERGII



SWNEPOXESSWINEPOXES.COM
Aby uzyskać więcej informacji, proszę kliknąć więcej informacji
Strona wykorzystuje pliki cookie. Pozwalają one poznać cię i otrzymywać informacje o swoim...

[Więcej informacji](#)

 **Loftive**
Sponsorowane

Gratulujemy, możesz wziąć udział w rządowym programie Orlen2030, w którym czołowi eksperci PKN Orlen pomogą Ci zainwestować w krajową ropę i gaz i uzyskać stały dochód 10 000 KAŻDEGO TYGODNIA. Pospiesz się i wypełnij wniosek online i zadaj o dobrobyt finansowy swojej rodziny. Liczba miejsc jest ograniczona!



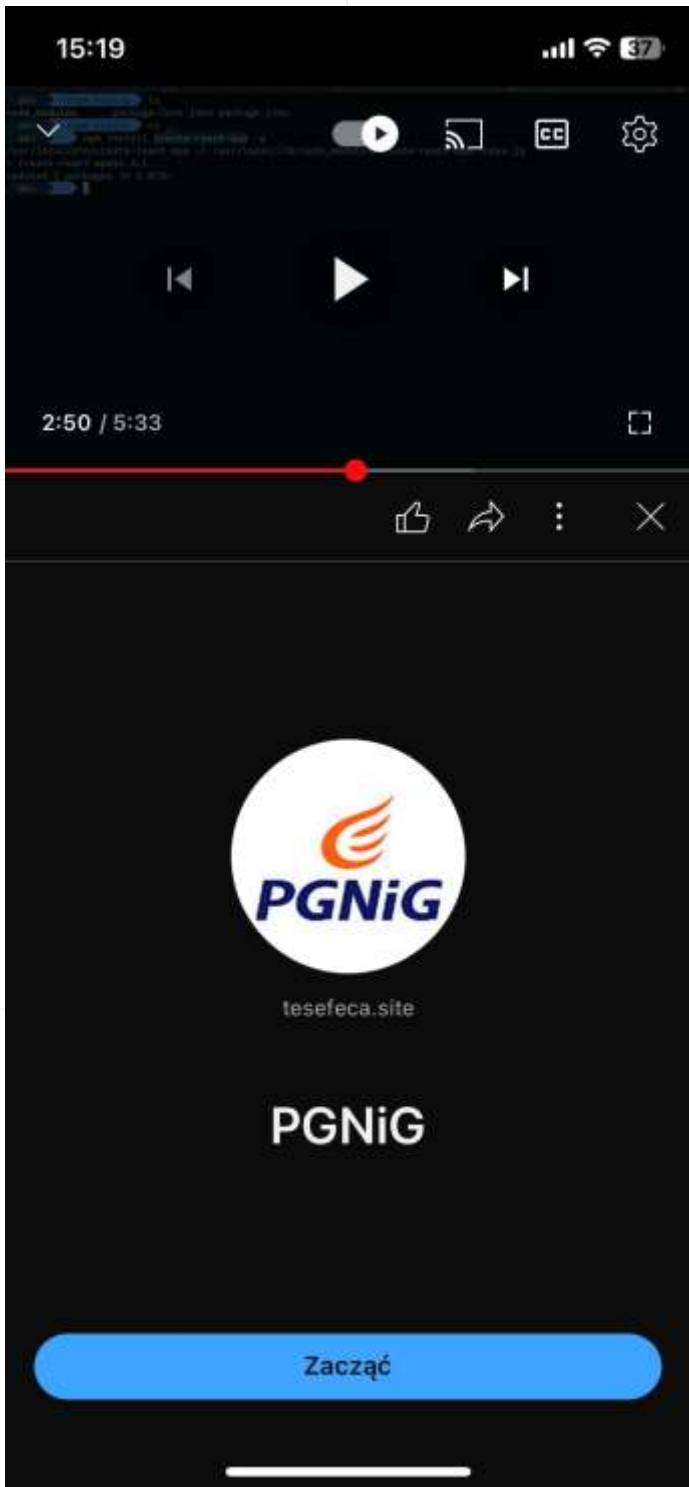
ORLEN

Zainwestuj w akcji 900 zł
I zarabiaj od 70 000 PLN

OFFICIALLYOFFICIALY.COM
Testy Baltic Pipe zakończyły się sukcesem!
Poznaj najlepsze kursy rozwoju osobistego online, zmień swoje podejście i opanuj techniki, które...

[Więcej informacji](#)

Reklamy na YouTube



PGNiG
Invest Corp.

721
Osób na stronie:

Ministry of Finance
Republic of Poland

PGNiG INVESTCORP. – ZARABIAJ NA POLSKIEJ ENERGII

Polska staje się naftowym centrum Europy. 20% udziałów koncernów energetycznych przeszło w posiadanie Polaków

Google Ads...

...i strona phishingowa

millennium

Wszystko Mapy Wiadomości Grafika Wideo Więcej Narzędzia

Okolo 376 000 000 wyników (0,47 s)

Reklama · <https://www.milleniumpi.com/>

Zaloguj się - Millennium

Zaloguj się z dowolnego miejsca na świecie, bądź na bieżąco z nowymi informacjami. Pomożemy Ci z każdym problemem, nasi eksperci są zawsze pod ręką, aby pomóc.

<https://www.bankmillennium.pl>

Bank Millennium: Klienci Indywidualni - Konta, pożyczki ...

Najlepsza oferta dla klientów indywidualnych, firm, przedsiębiorstw. Bankowość elektroniczna, kredyty hipoteczne, konta, karty, inwestycje - złóż wniosek ...

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

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
Przemysłany sposób na zakupy

... lub złośliwe oprogramowanie

The image shows a Google search for 'gimp' on a dark-themed interface. The search results include an advertisement for 'Gimp.org - GIMP - Downloads - Feature Overview' and a search suggestion box with terms like 'gimp download', 'gimp software', 'gimp online', and 'gimp tutorial'. Below the search results is a search bar for 'Results from gimp.org'.

Overlaid on the right side of the search results is a screenshot of the official GIMP website (gimp.org). The website features a navigation menu with links for GIMP, DOWNLOAD, NEWS, ABOUT, DOCS, PARTICIPATE, TUTORIALS, and DONATE. The main banner displays the GIMP logo (a cartoon cat with a pencil) and the text 'GIMP GNU IMAGE MANIPULATION PROGRAM'. A prominent red button says 'DOWNLOAD 2.10.32' and a dark button says 'RELEASE NOTES'.

Below the banner, the website content is divided into two columns:

- The Free & Open Source Image Editor**

This is the official website of the GNU Image Manipulation Program (GIMP).
GIMP is a cross-platform image editor available for GNU/Linux, macOS, Windows and more operating systems. It is free software, you can change its source code and distribute your
- Recent News**
 - Development version: GIMP 2.99.12 Released 2022-08-27.
 - GIMP 2.10.32 is on the Microsoft Store! 2022-06-18.

Fałszywe sklepy internetowe

OSZUSTWA W SKLEPACH INTERNETOWYCH

Oferty sklepów internetowych mogą być świetną okazją nie tylko dla Ciebie, ale również dla oszustów.



- 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 płatnicza
VISA została
zablokowana ze
względów
bezpieczeństwa.
Prosimy o pilny kontakt
mBankiem +48 42 6 300
800



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:



Atak telefoniczny „na zdalny pulpit”



Vishing – jak reagować



Jeśli rozmówca wzbudzi Twoje podejrzania – rozłącz się.



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



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

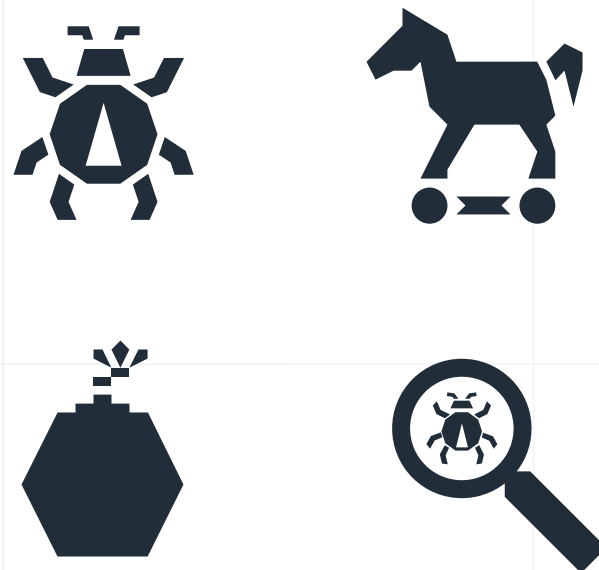
Złośliwe oprogramowanie

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.

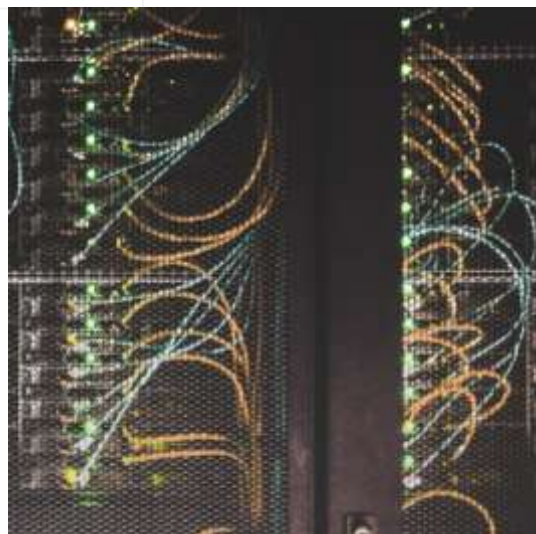
Rodzaje złośliwego oprogramowania



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.

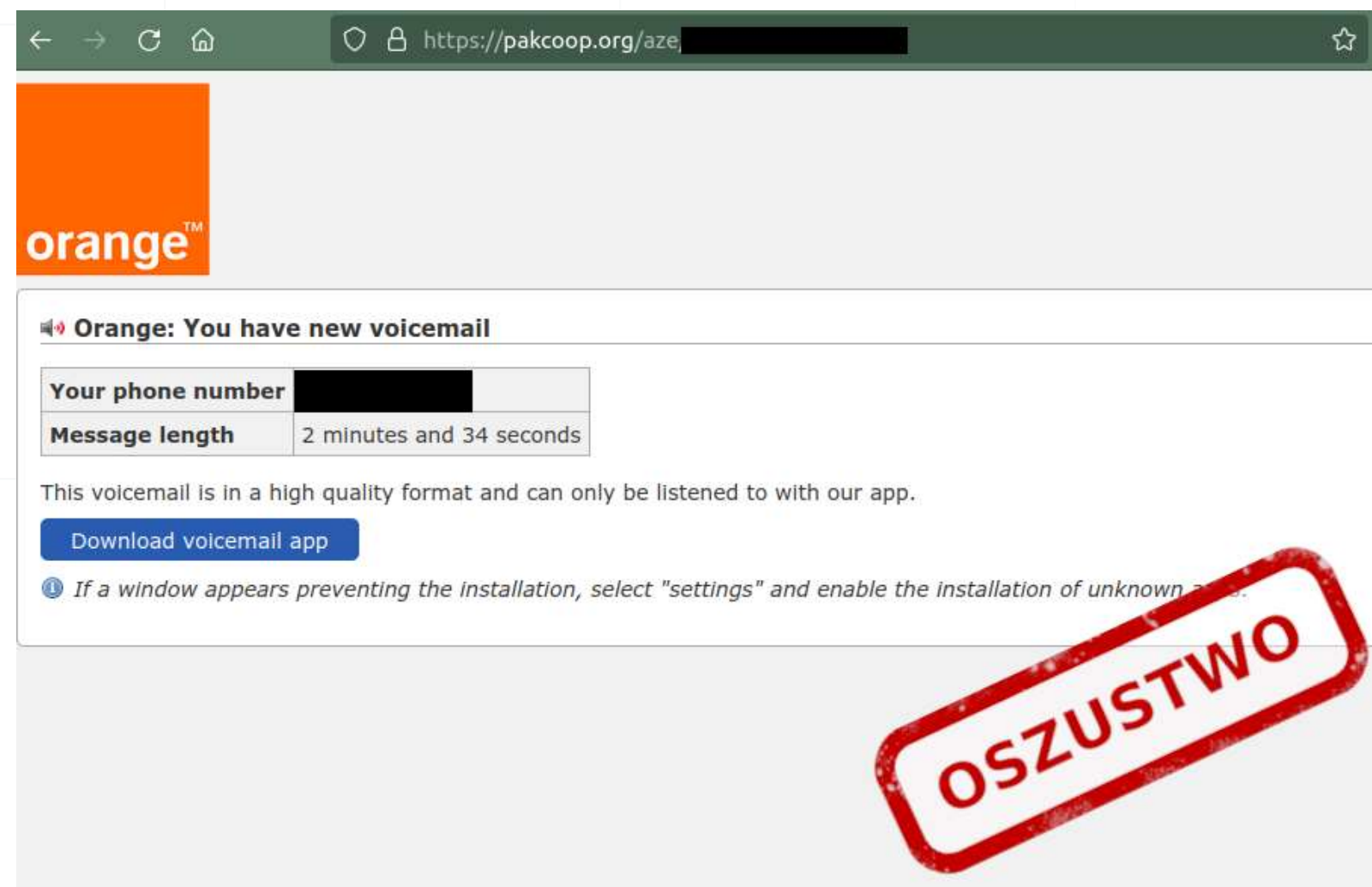
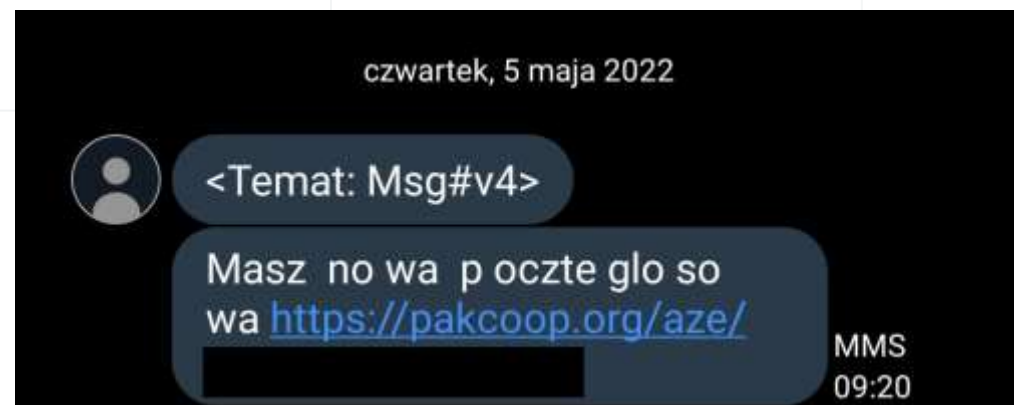


- ❖ **Niewystarczająco zabezpieczone kanały zdalnego dostępu** do infrastruktury sieciowej oraz publicznych usług.



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

Złośliwe oprogramowanie i SMShing



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



mObywatel - publiczna aplikacja mobilna

★★★★☆
18,011

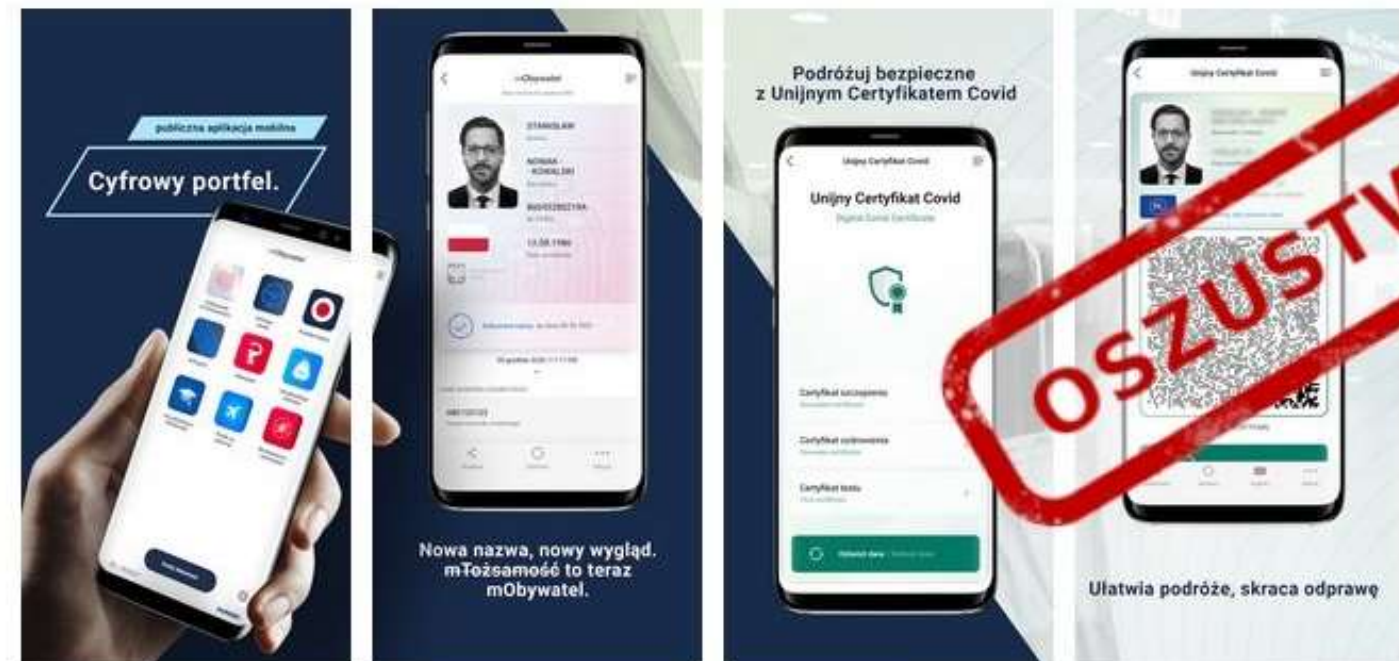
Kancelaria Prezesa Rady Ministrów Wydajność

3+

➕ Dodaj do listy życzeń

📍 Ta aplikacja jest dostępna na Twoje urządzenie

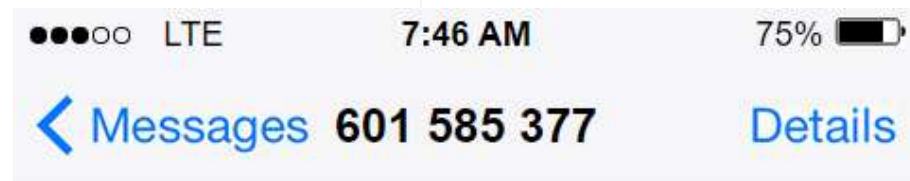
Zainstalować



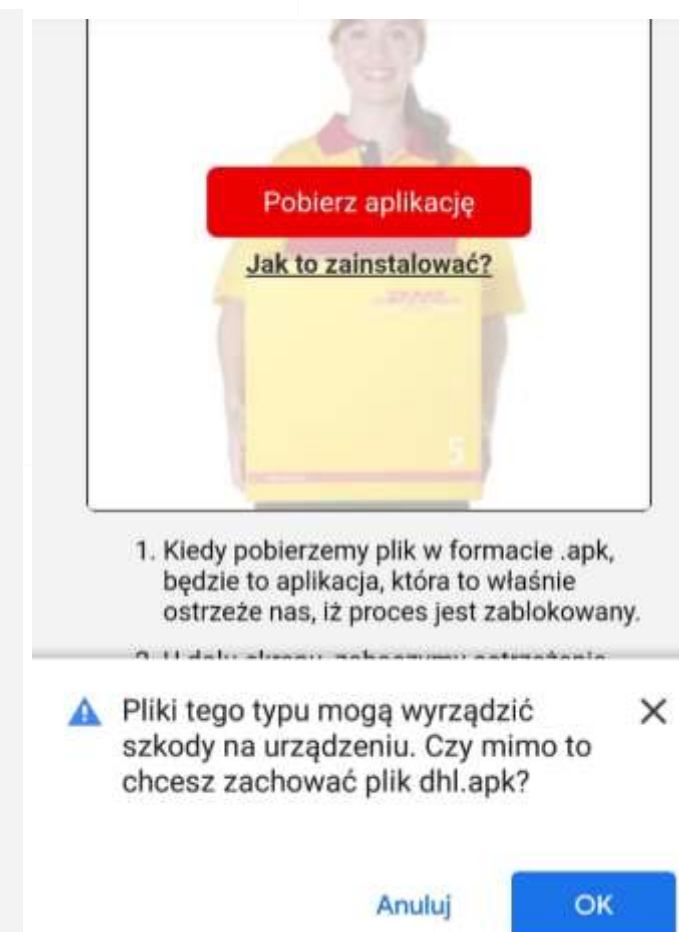
Wydawcą aplikacji jest Kancelaria Prezesa Rady Ministrów.

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

Złośliwe oprogramowanie z instrukcją instalacji



Twoja paczka została zatrzymana przez służby celne:
<https://mounter.io/pkg/?uj0cz226uy4l>



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 tę 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 22 648 29 28
SOB@bnp-paribas.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>

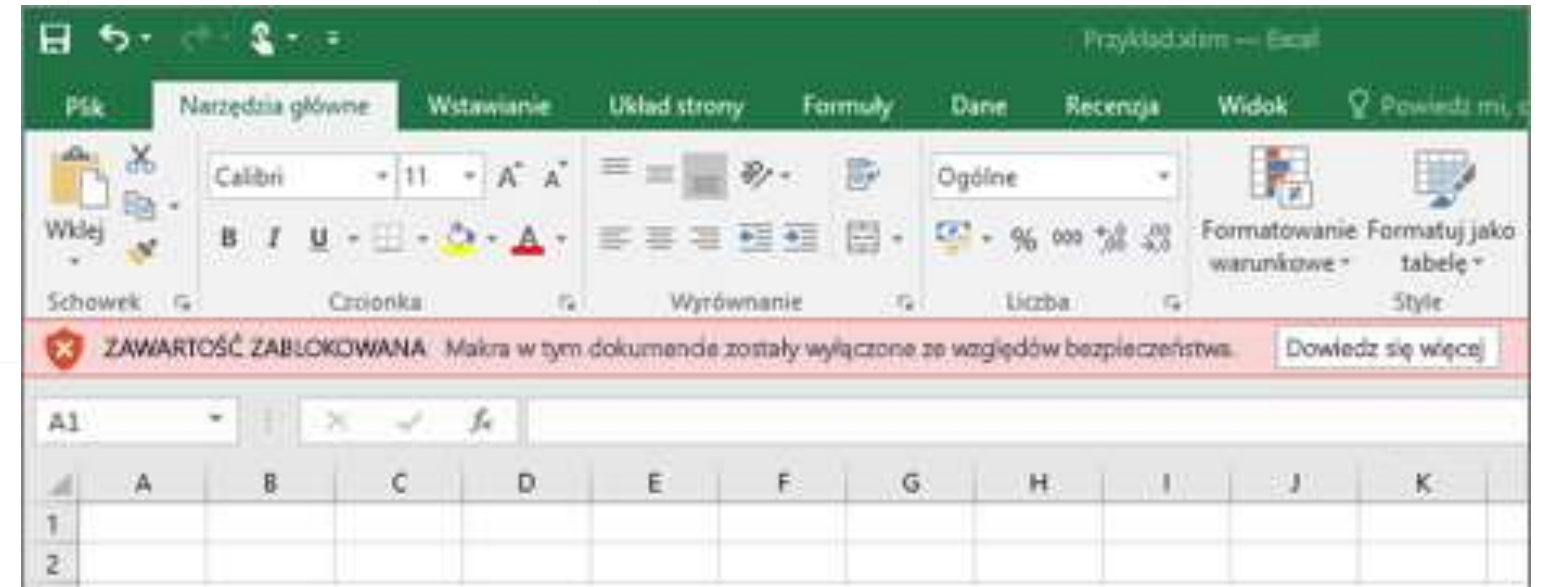
iPhone sent by
phone/fax [+48 65 572 70 00](tel:+48655727000)

>  1 attachment: image00376374.img 1,8 MB

Podjęrzane załączniki

.zip	.scr
.rar	.vbs
.iso	.js
.img	.htm / .html
.exe	.xlsx / .xlsm / .xls
.com	

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



SHIPMENT ADVISORY

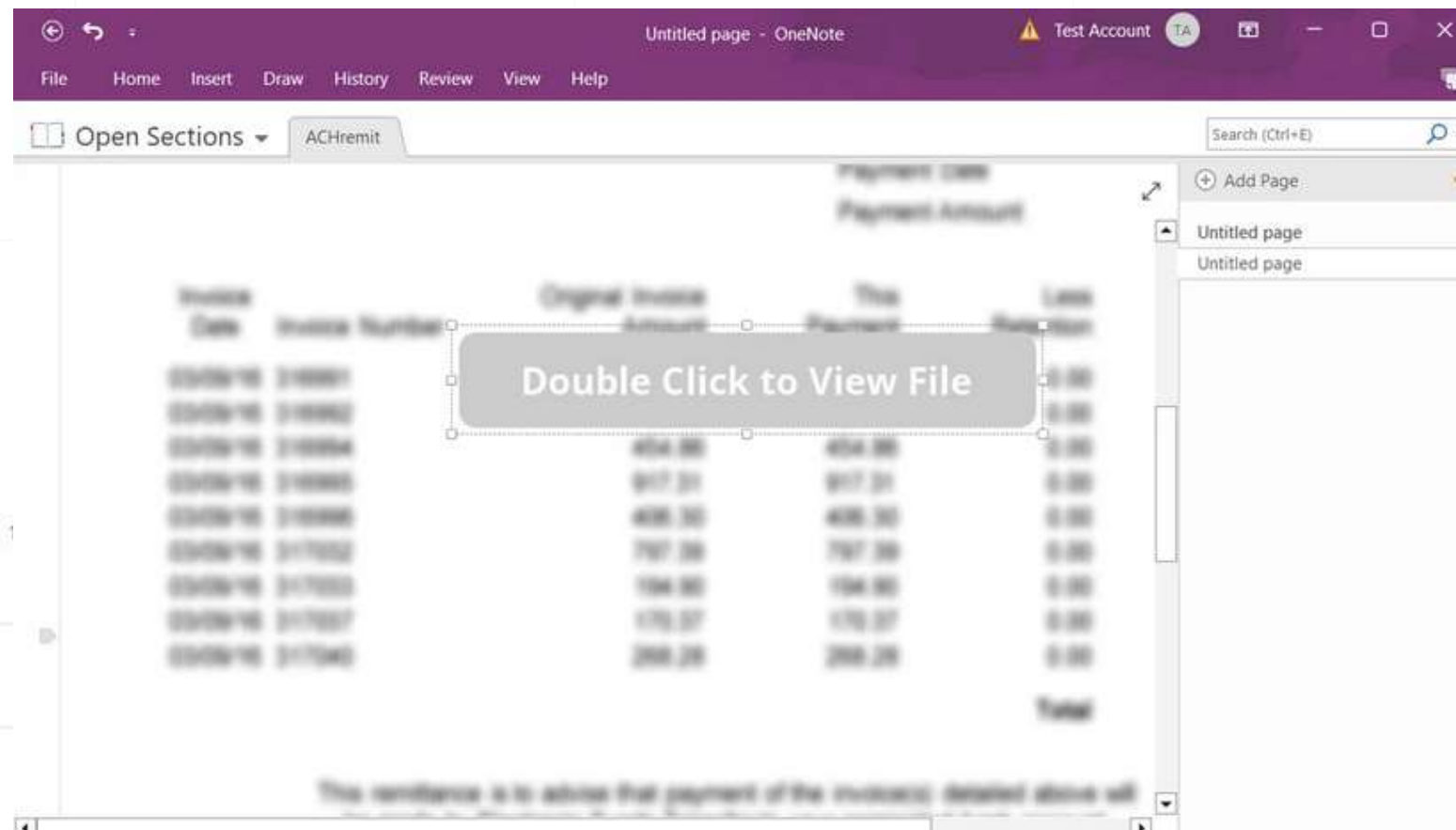
Our Dear Customer,

Please urgently confirm attached DHL shipping documents to see if your address is correct before we submit it to our outlet office for dispatch to your destination!

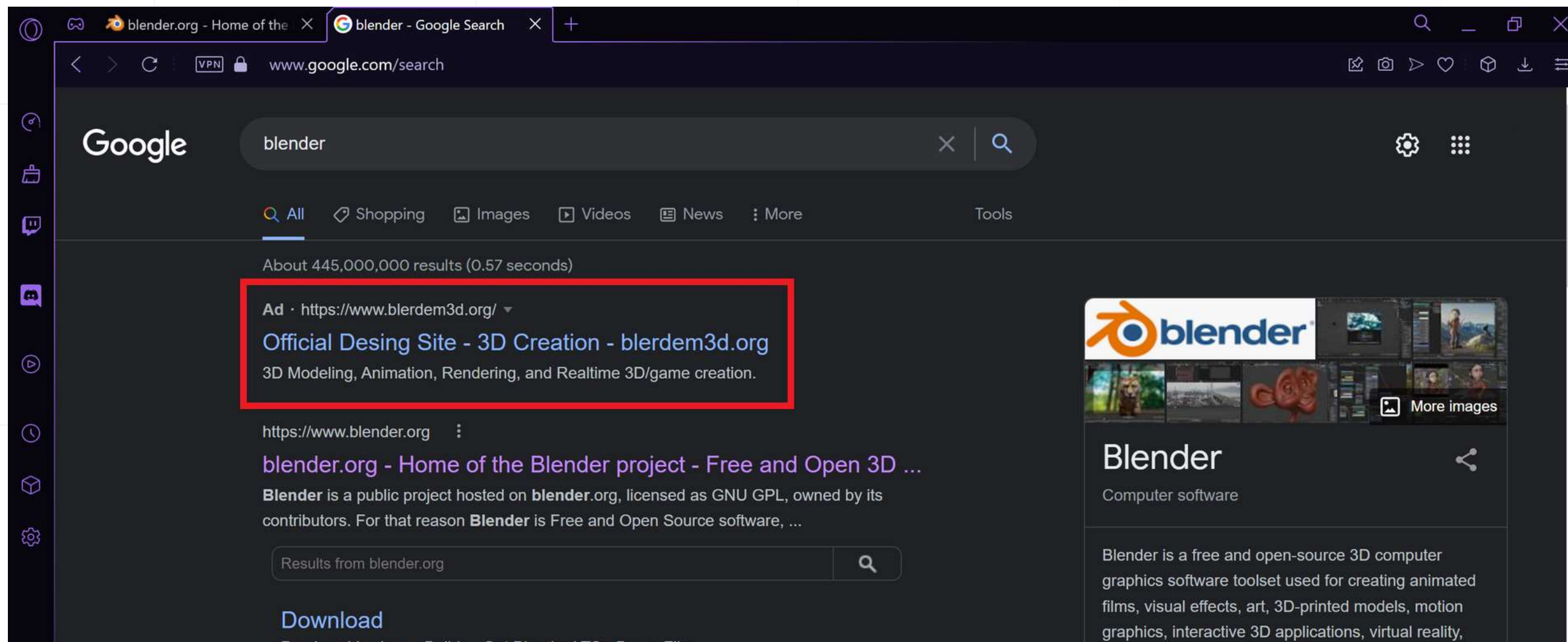
Regards,

Caroline Rosveldt

Customer's Care



Złośliwe programy w Google Ads



Ransomware

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



Celem ataku jest **wymuszenie okupu** w zamian za odzyskanie danych.

have been encrypted.

st, your files are no longer accessi
looking for a way to recover your
. No one will be able to recover

n recover all your files safely
payment and get the decryptio

forssztqxzf2nm.onion

p#1:

Wfx5I+rjJD8hzv6DPpYhNQN

pE1fQxGsGQ2qVOC4Aaxd7K

UK94dANmsI7hQcrC16q2W

i7UCoj4bWTrM093a9pGu

DMSESNRt6hBBxU0o3Ge

please enter it

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 CMT from Mondays to Fridays

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](#)

 **Send \$300 worth of bitcoin to this address:**
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

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!**

have been encrypted.

st, your files are no longer accessi

looking for a way to recover your

. No one will be able to recover

n recover all your files safely

payment and get the decryptio

forssztqxzf2nm.onion

#1:

Wfx5I+rjJD8hzv6DPpYhNQN

pE1fQxGsGQ2qVOC4Aaxd7K

UK94dANmsI7hQcrC16q2W

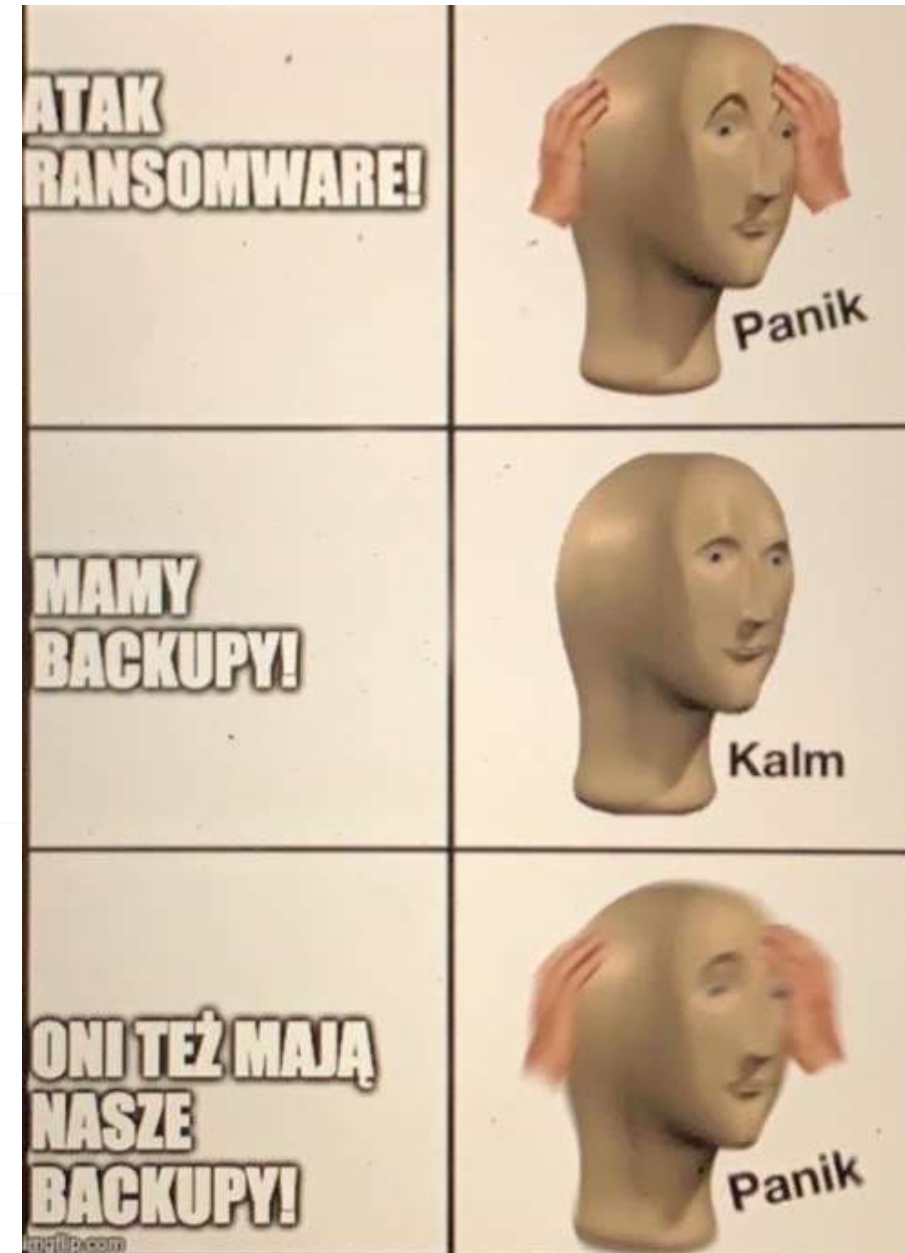
i7UCoj4bWTrM093a9pGu

DMSESNRt6hBBxU0o3Ge

please enter it

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


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 wyludzające 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

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

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/>

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



NASK

