(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Phishing, oszustwa w sieci i ransomware.

Najpowszechniejsze cyberzagrożenia
– jak rozpoznać, jak zapobiegać

Zespół Szkoleń i Ćwiczeń Cyberbezpieczeństwa
NASK – PIB

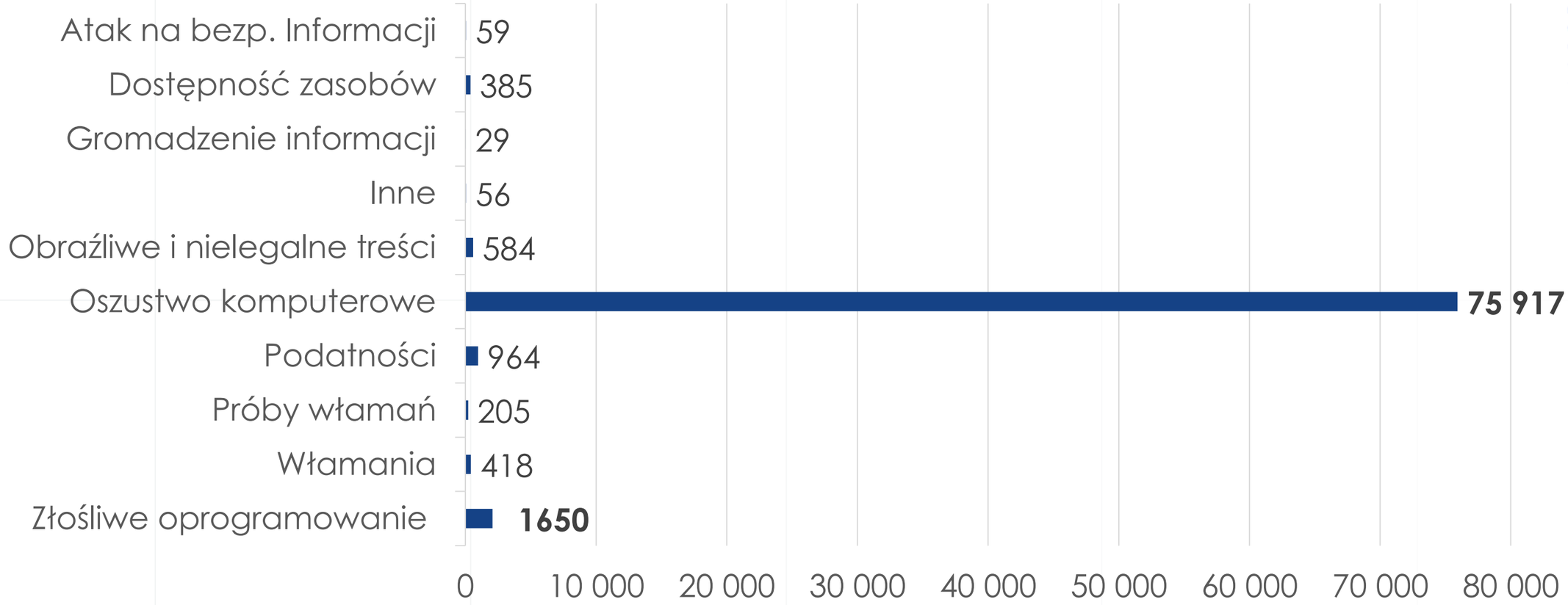
Ministerstwo Cyfryzacji

NASK

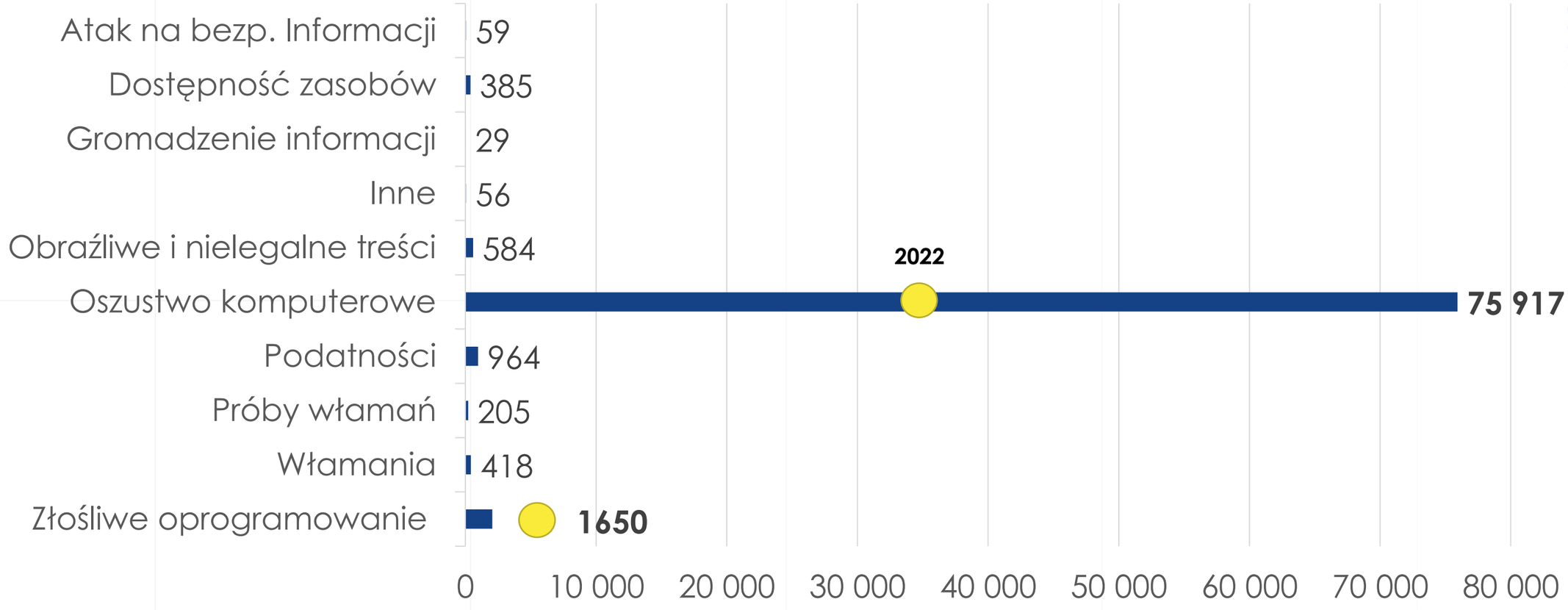
Cyberzagrożenia w liczbach

- statystyki incydentów zgłaszanych do CERT POLSKA

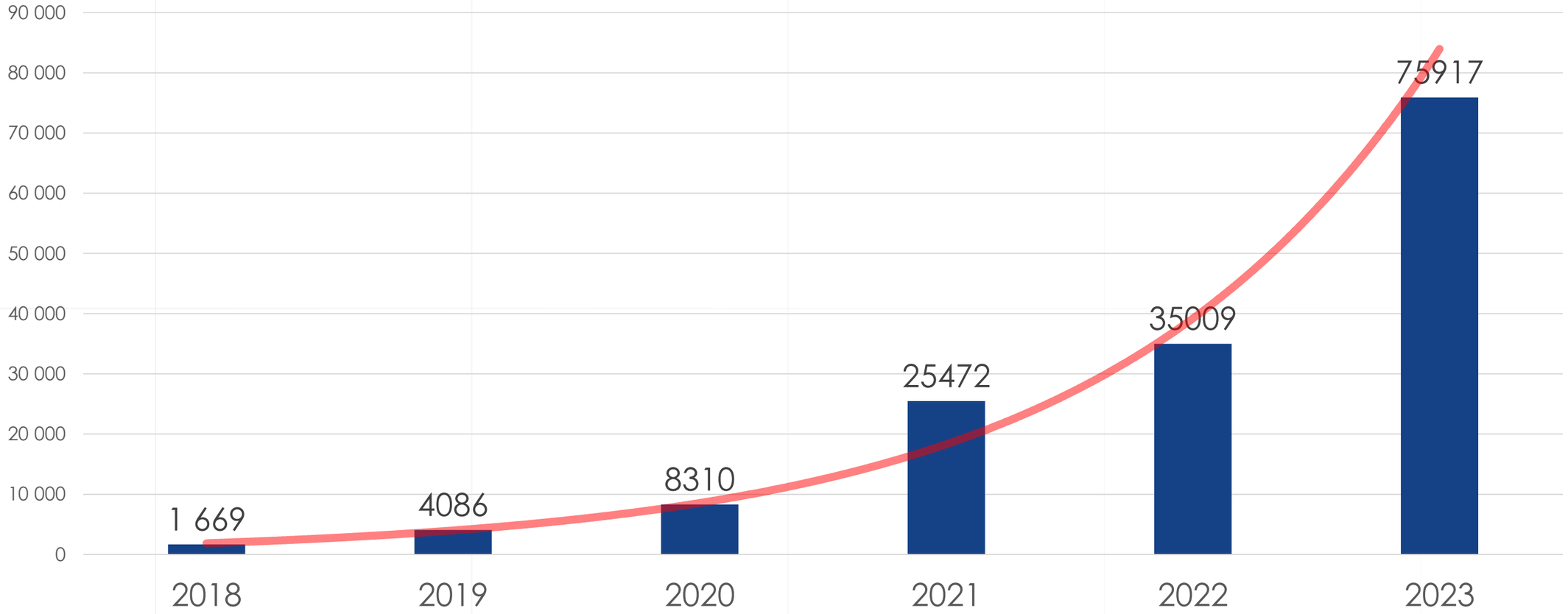
Incydenty zarejestrowane przez CERT Polska w 2023 roku



Incydenty zarejestrowane przez CERT Polska w 2023 roku



Oszustwa zarejestrowane przez CERT Polska w latach 2018-2023



Phishing

- Metody ataku i socjotechnika

Phishing

Popularny atak socjotechniczny.

Wprowadzenie ofiary w błąd poprzez **podszywanie się pod zaufany podmiot lub osobę.**

Wykorzystanie **fałszywych** wiadomości, **podrobionych** stron internetowych, nieprawdziwych informacji itp.

Cele ataku:

Przejęcie poufnych danych

Kradzież pieniędzy

Instalacja złośliwego oprogramowania

W jaki sposób jesteśmy atakowani?

W mailach

SMSami

Przez telefon

W reklamach, mediach społecznościowych, przez kod QR itp.

Granie na **emocjach** odbiorców

– **Należy dokonać pilnej płatności!**

– **Potrzebna jest twoja pomoc!**

– **Stało się coś strasznego!**

– **Ktoś Cię okrada!**

– **Wygrywasz na loterii!**

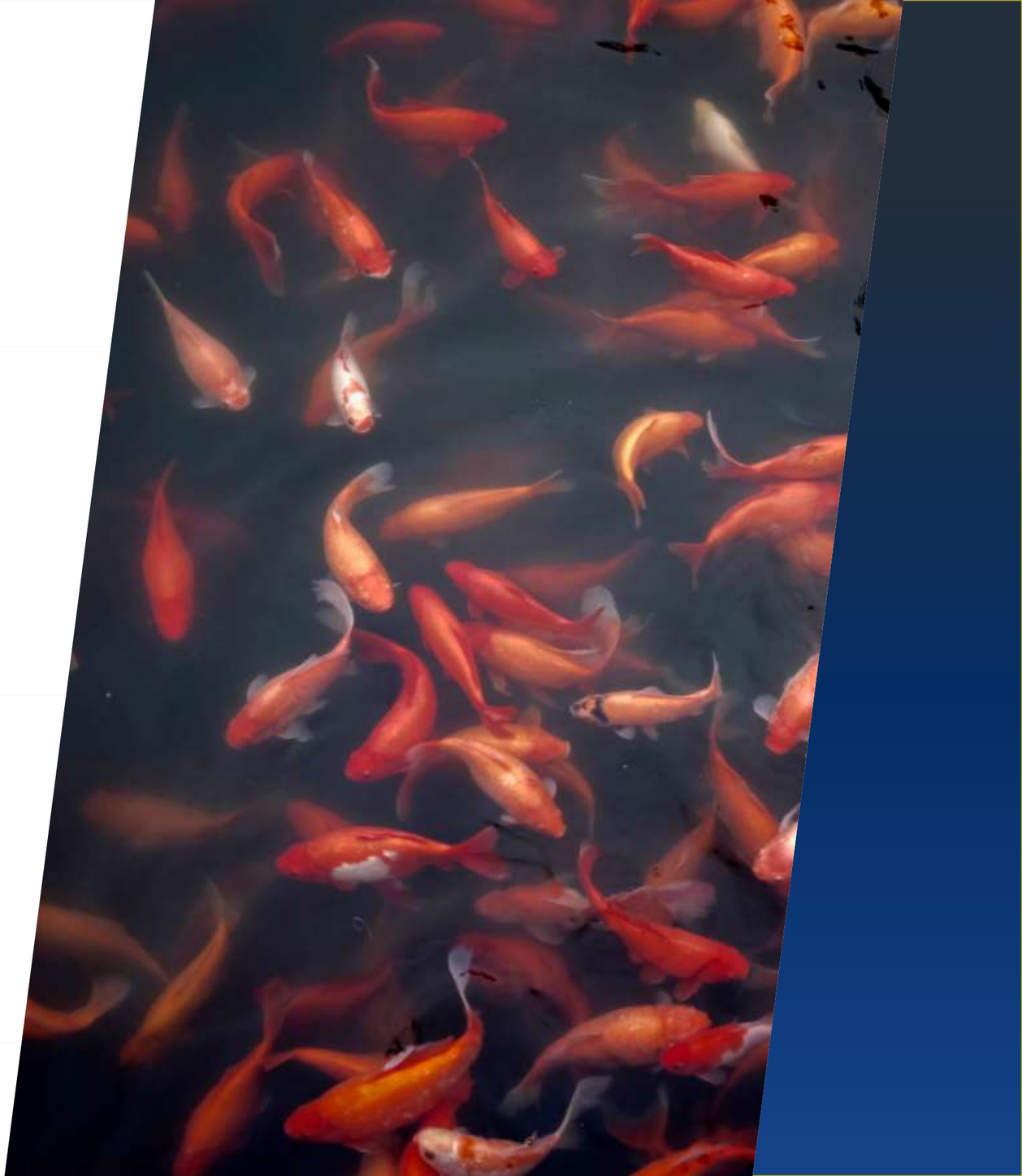
Jak to wygląda w praktyce?





Phishing masowy

- Wysyłka fałszywych wiadomości do **setek/tysięcy odbiorców;**
- Pretekst kontaktu i historia wykorzystana do ataku jest **uniwersalna**;
- Liczy się **skala ataku**, bo tylko odsetek odbiorców uda się w ten sposób oszukać.



Podszywanie się pod instytucje publiczne

Powiadomienie o zwrocie środków

From Ministerstwo Finansów - Portal Gov.pl <support@widok.justsport.it>
To
Date Today 11:19

gov.pl | Serwis Rzeczypospolitej Polskiej

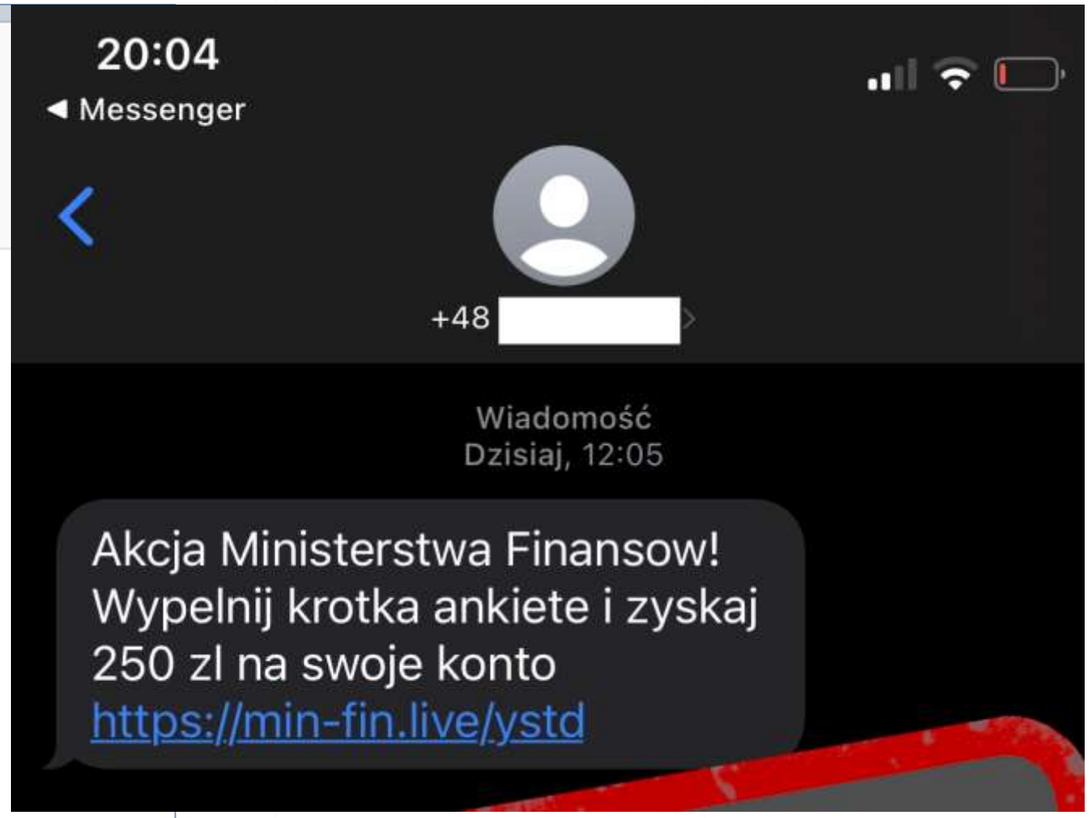
Portal podatkowy

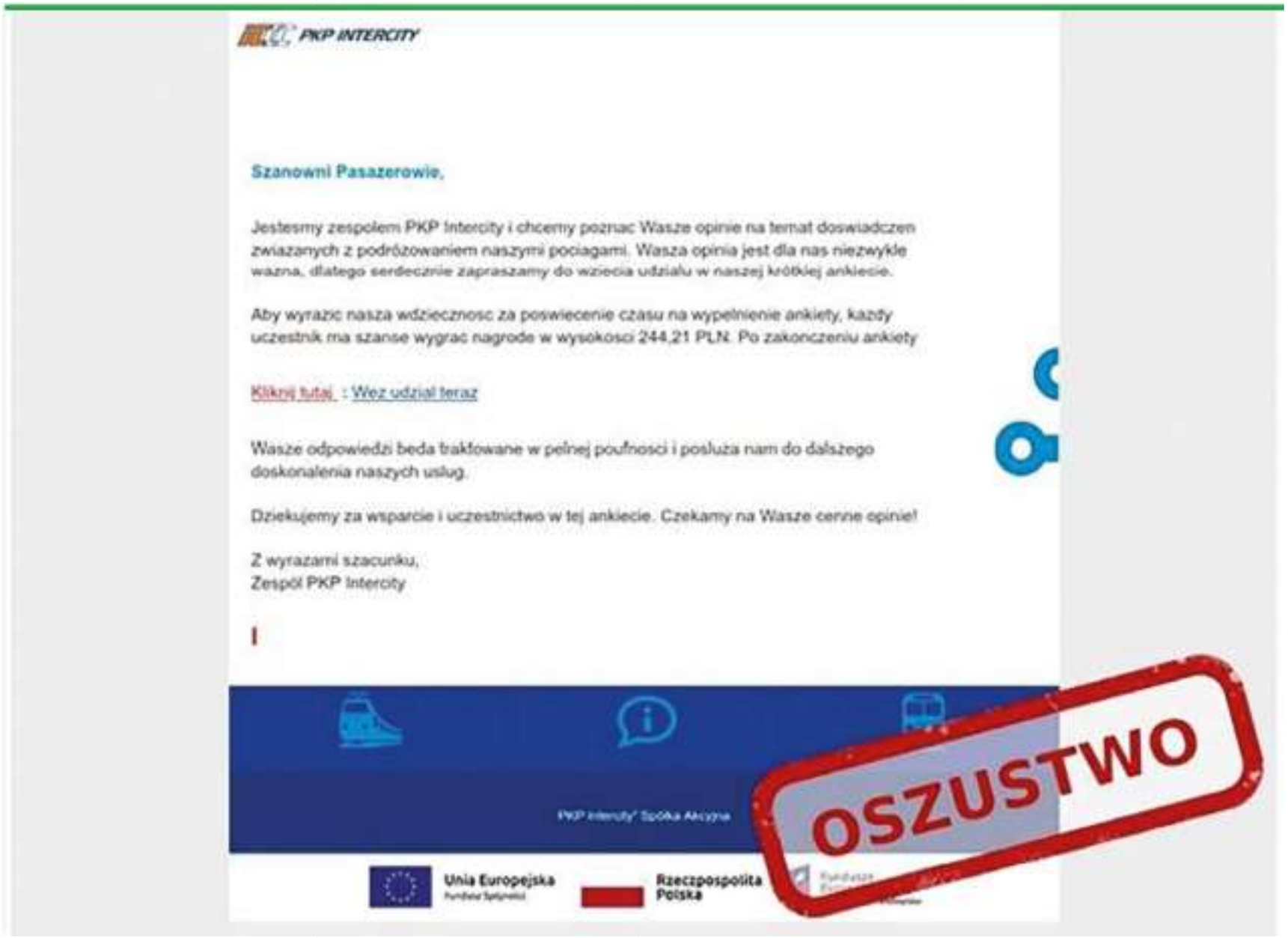
Drodzy Klienci,

Masz prawo do zwrotu podatku w wysokości **634.79 PLN**
Prześlij poniższy formularz, abyśmy mogli go przetworzyć
Prosimy o jak najszybszy zwrot pieniędzy.

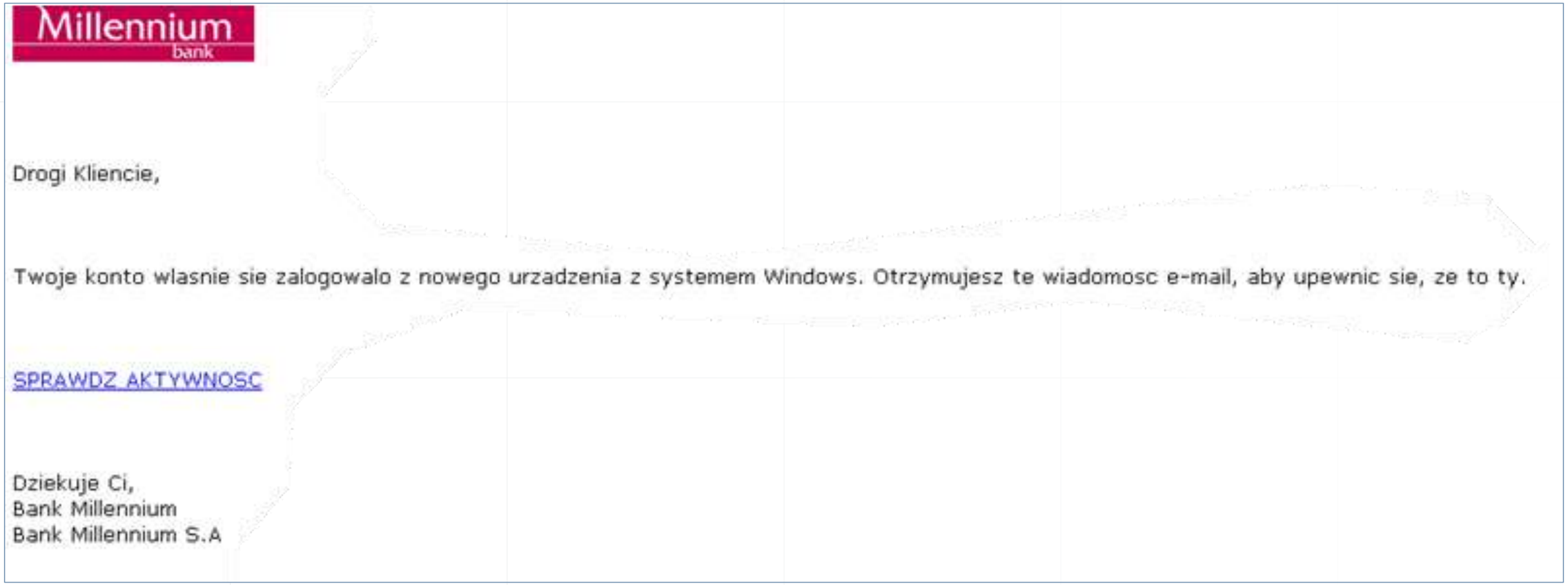
Uzyskaj dostęp do formularza

Kontynuacja procesu zwrotu kosztów może zająć do 24 godzin.
Ten proces może zostać opóźniony, jeśli formularz zwrotu nie zostanie prawidłowo przesłany

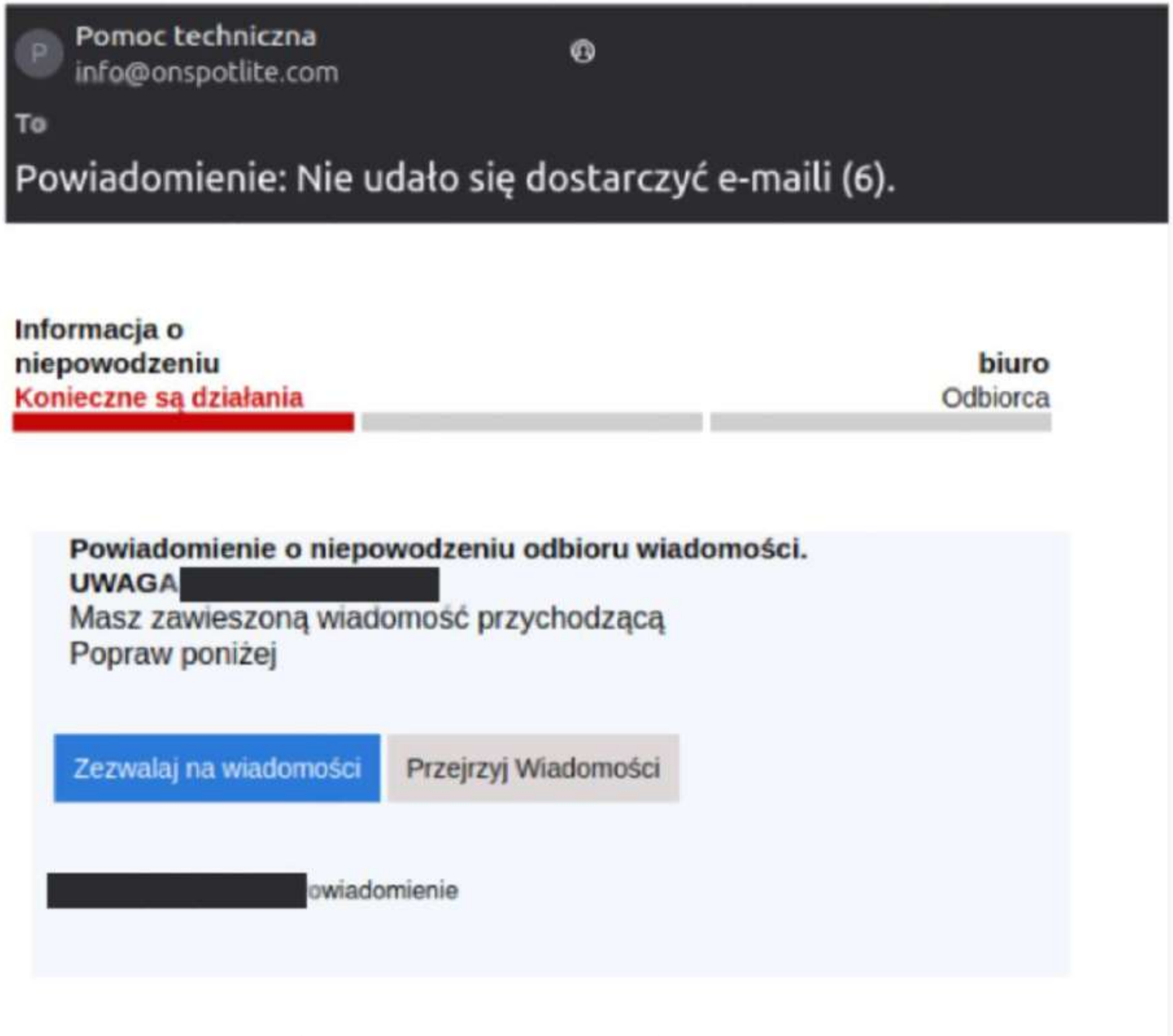



PKP INTERCITY
Szanowni Pasazerowie,
Jestesmy zespołem PKP Intercity i chcemy poznac Wasze opinie na temat doswiadczen zwiazanych z podróżowaniem naszymi pociagami. Wasza opinia jest dla nas niezwykle wazna, dlatego serdecznie zapraszamy do wziecia udziału w naszej krótkiej ankiecie.
Aby wyrazic nasza wdziecznosc za poswiecenie czasu na wypełnienie ankiety, kazdy uczestnik ma szanse wygrac nagrode w wysokosci 244,21 PLN. Po zakonczeniu ankiety
Kliknij tutaj : Wez udział teraz
Wasze odpowiedzi beda traktowane w pełnej poufnosci i posłuza nam do dalszego doskonalenia naszych usług.
Dziekujemy za wsparcie i uczestnictwo w tej ankiecie. Czekamy na Wasze cenne opinie!
Z wyrazami szacunku,
Zespół PKP Intercity
Unia Europejska
Rzeczpospolita Polska
OSZUSTWO

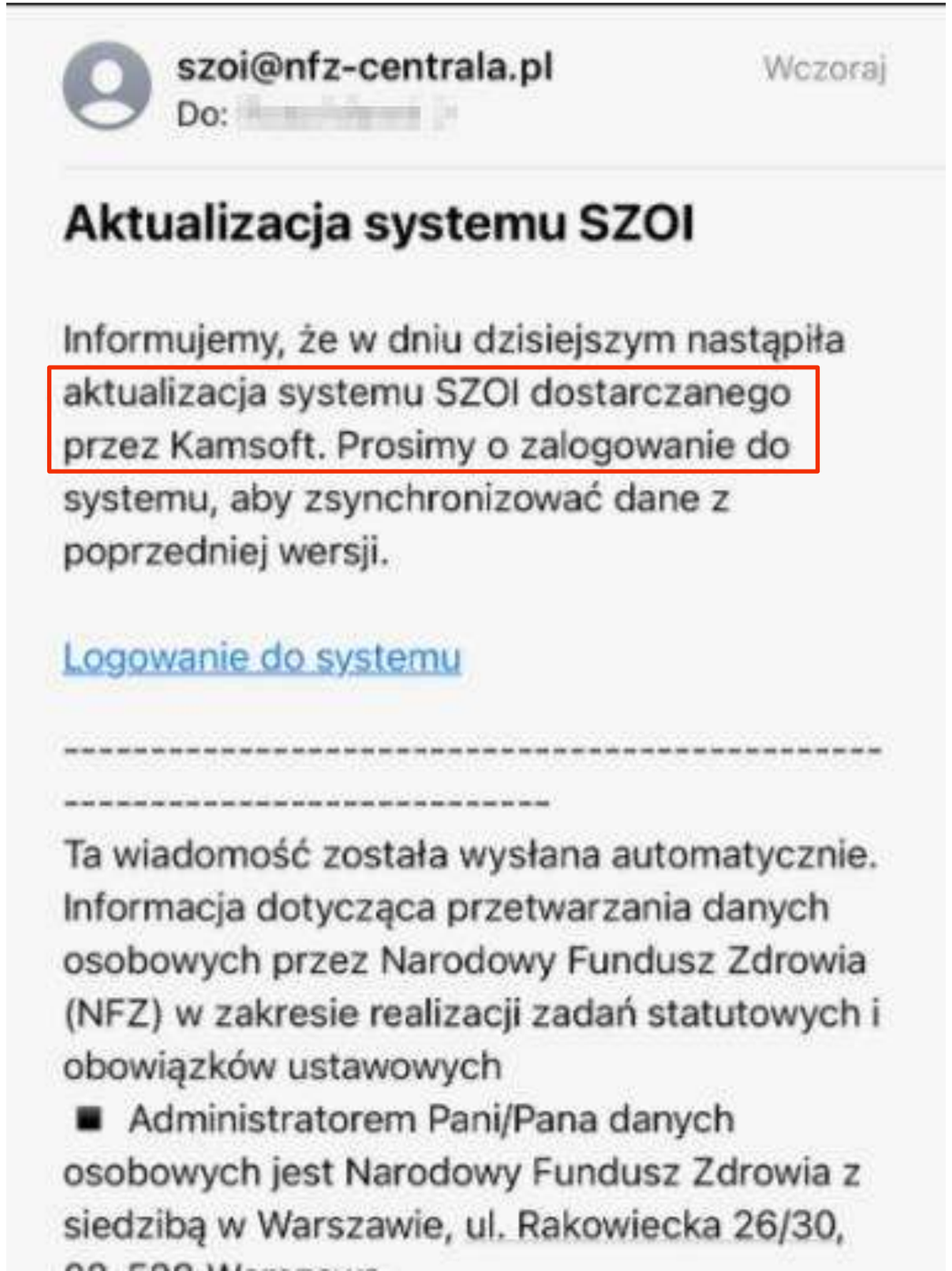
Podszywanie się pod banki



Podszywanie się pod pomoc techniczną



Wiadomości techniczne



szoi@nfz-centrala.pl Wczoraj
Do:

Aktualizacja systemu SZOI

Informujemy, że w dniu dzisiejszym nastąpiła aktualizacja systemu SZOI dostarczanego przez Kamsoft. Prosimy o zalogowanie do systemu, aby zsynchronizować dane z poprzedniej wersji.

Logowanie do systemu

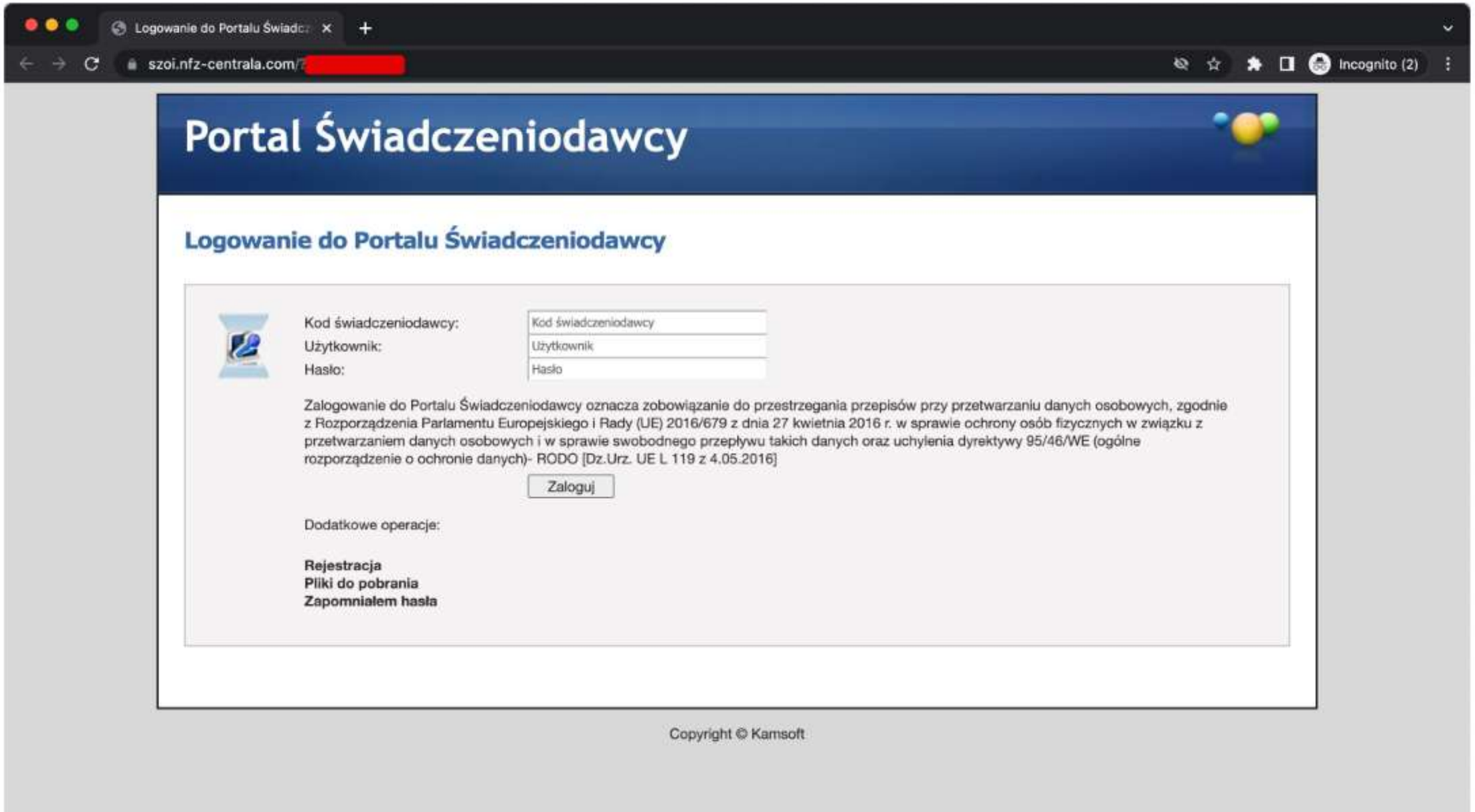
Ta wiadomość została wysłana automatycznie. Informacja dotycząca przetwarzania danych osobowych przez Narodowy Fundusz Zdrowia (NFZ) w zakresie realizacji zadań statutowych i obowiązków ustawowych

- Administratorem Pani/Pana danych osobowych jest Narodowy Fundusz Zdrowia z siedzibą w Warszawie, ul. Rakowiecka 26/30,

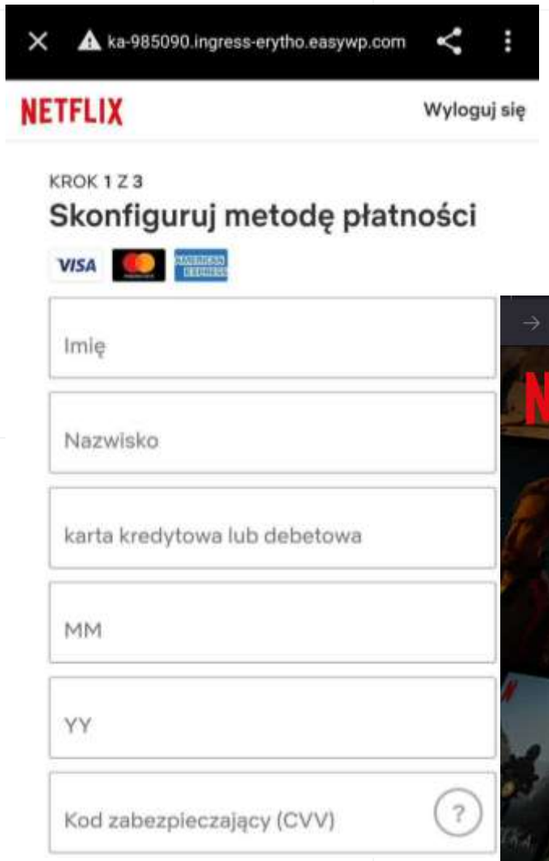
Źródło: www.nfz.gov.pl

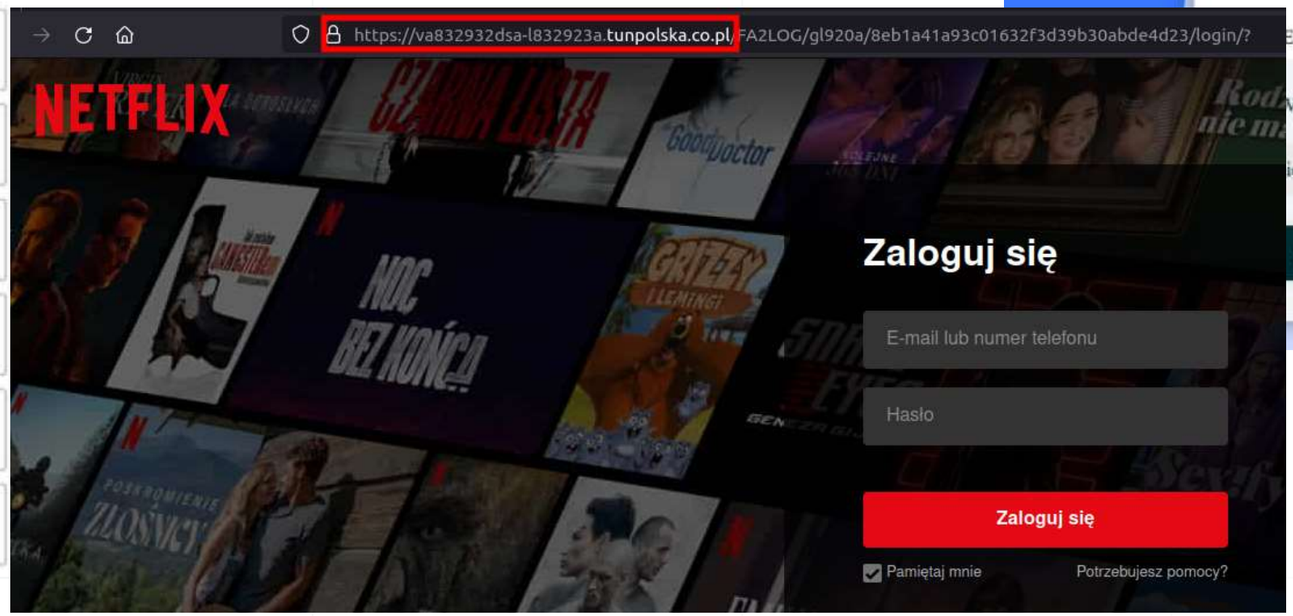
Źródło: www.nfz.gov.pl

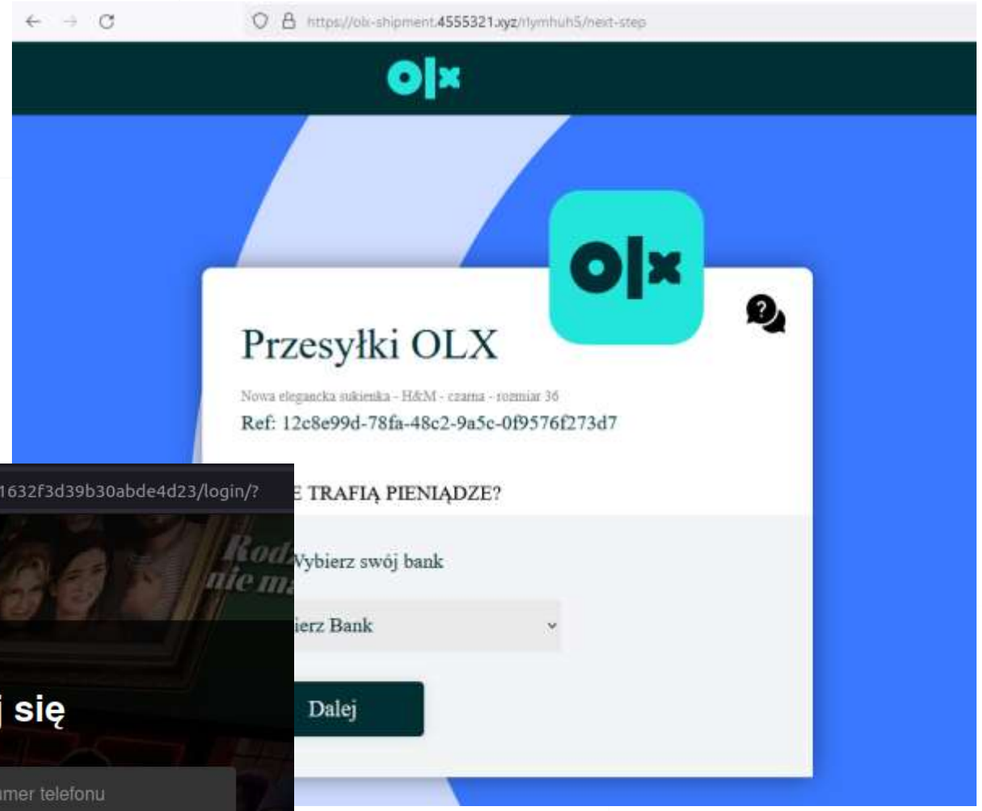
Fałszywy panel do logowania do systemu

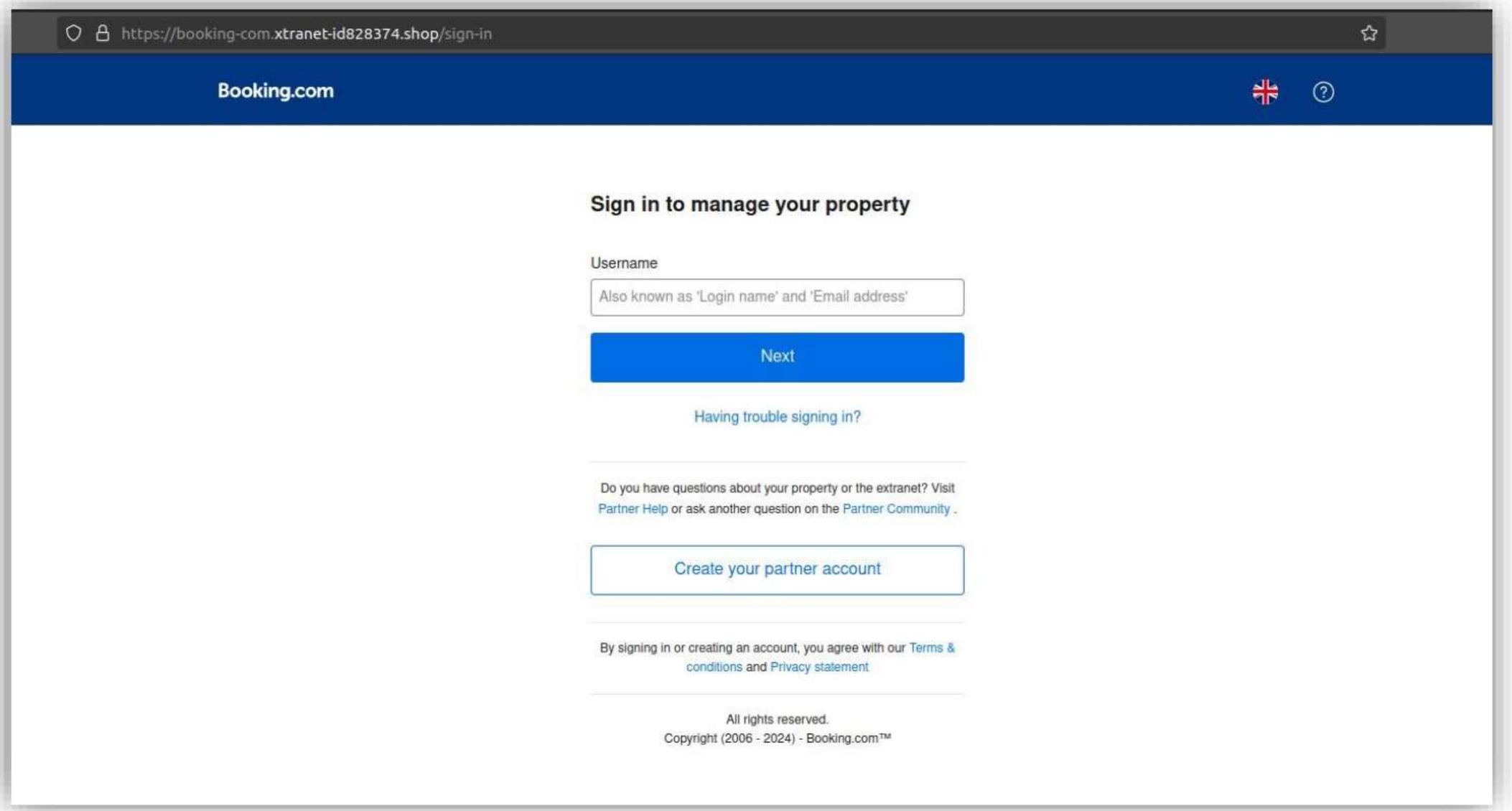


Inne przykłady – podszywanie się pod popularne serwisy

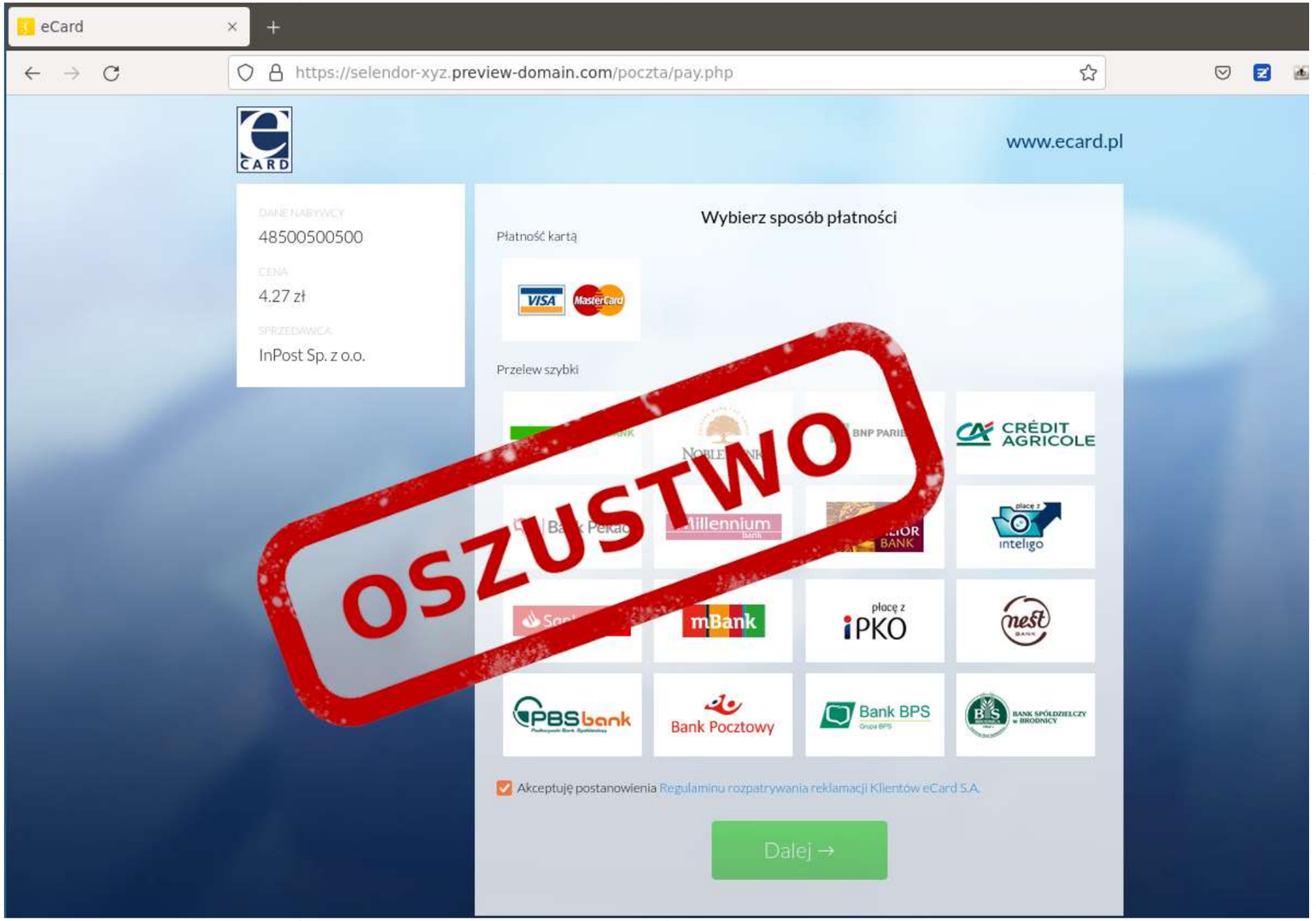




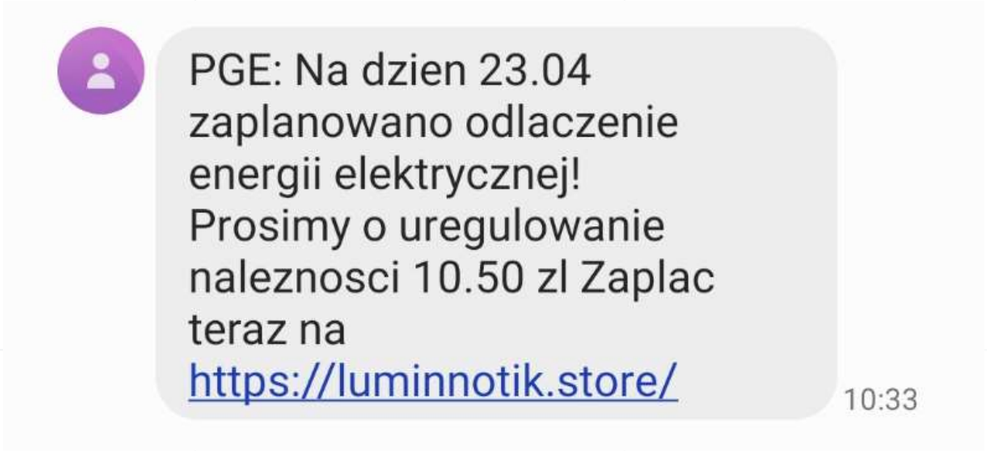



https://booking-com.xtranet-id828374.shop/sign-in
Booking.com
Sign in to manage your property
Username
Also known as 'Login name' and 'Email address'
Next
Having trouble signing in?
Do you have questions about your property or the extranet? Visit Partner Help or ask another question on the Partner Community .
Create your partner account
By signing in or creating an account, you agree with our Terms & conditions and Privacy statement
All rights reserved.
Copyright (2006 - 2024) - Booking.com™

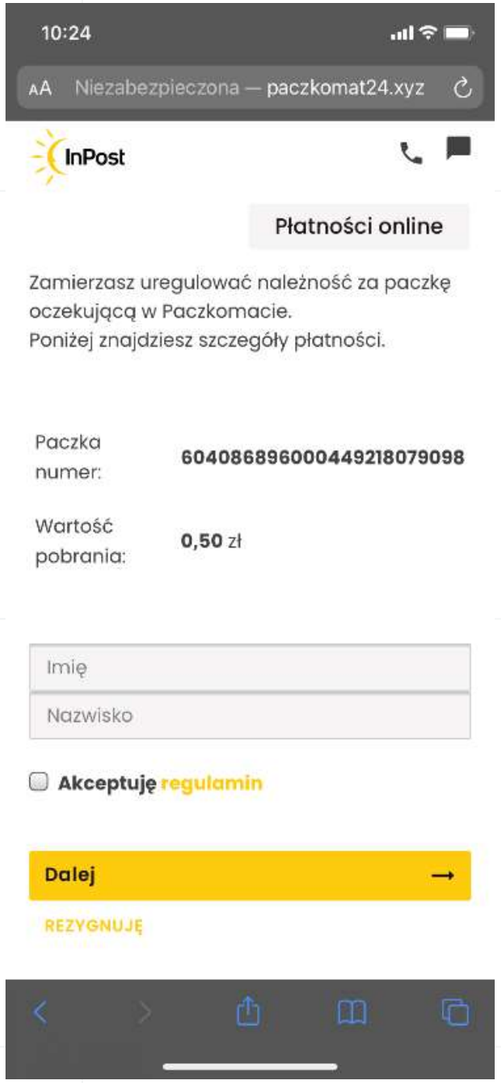
Fałszywe bramki płatności

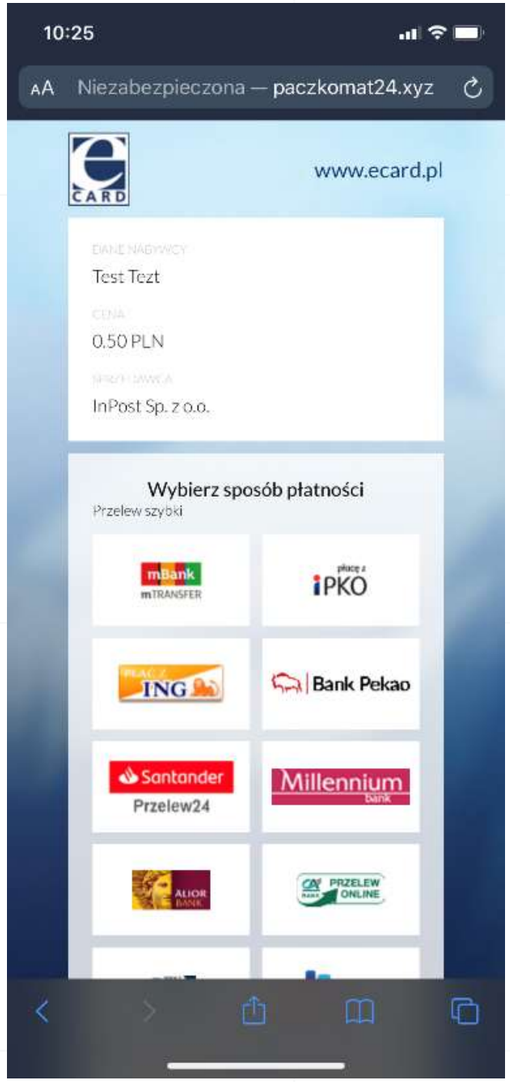


Opłaty, nadpłaty, ankiety w SMSach

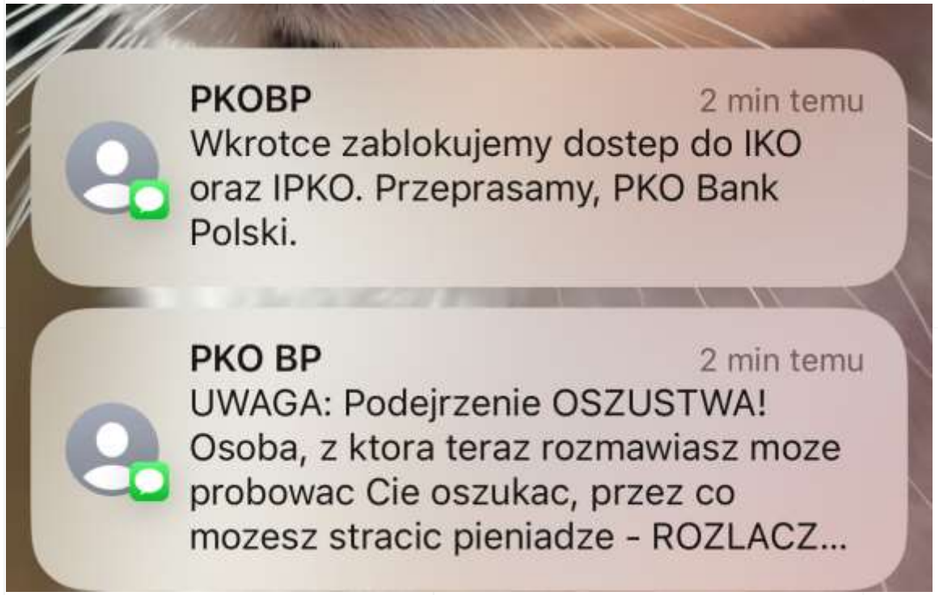


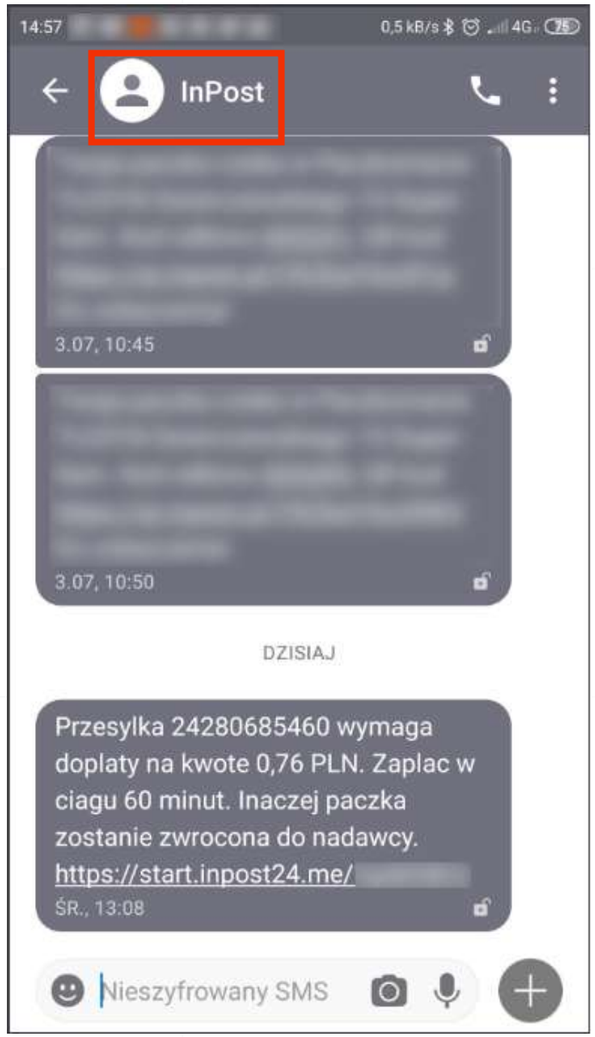
Wyłudzanie danych i środków pieniężnych





Uwaga na **spoofing,**
czyli **podszywanie się pod zaufany numer telefonu!**

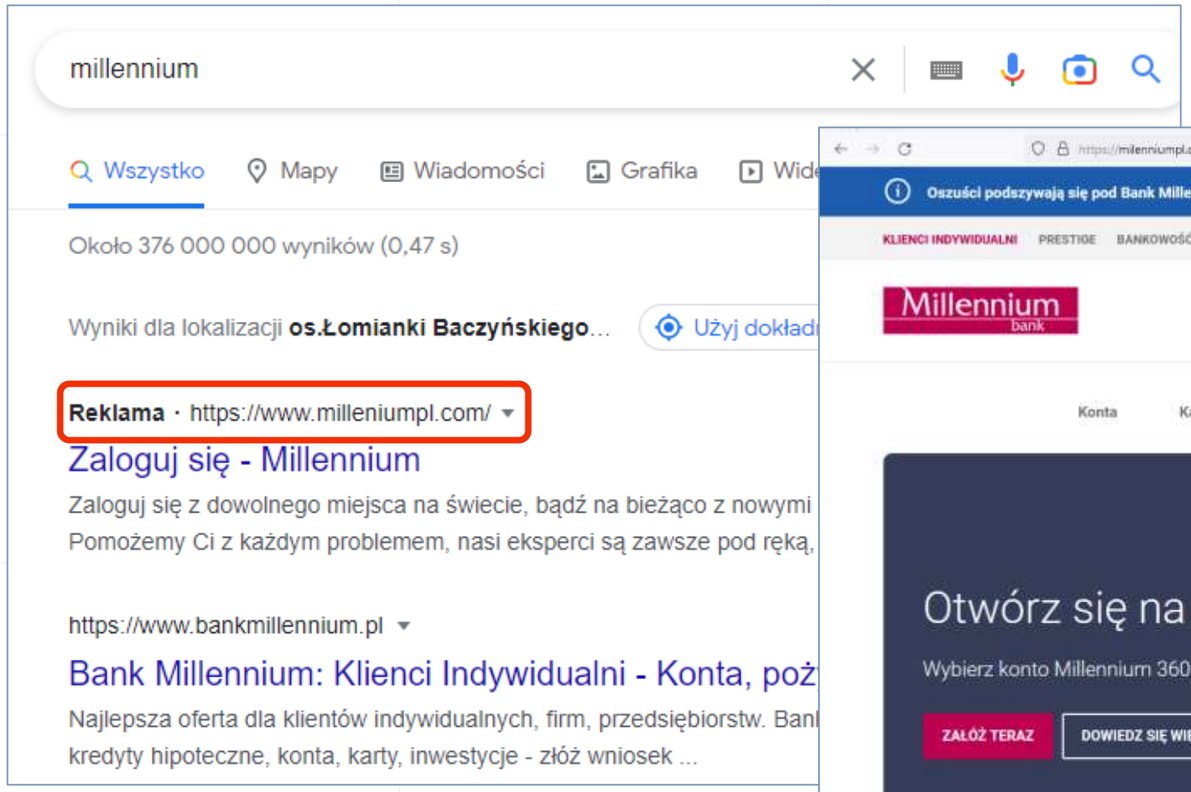


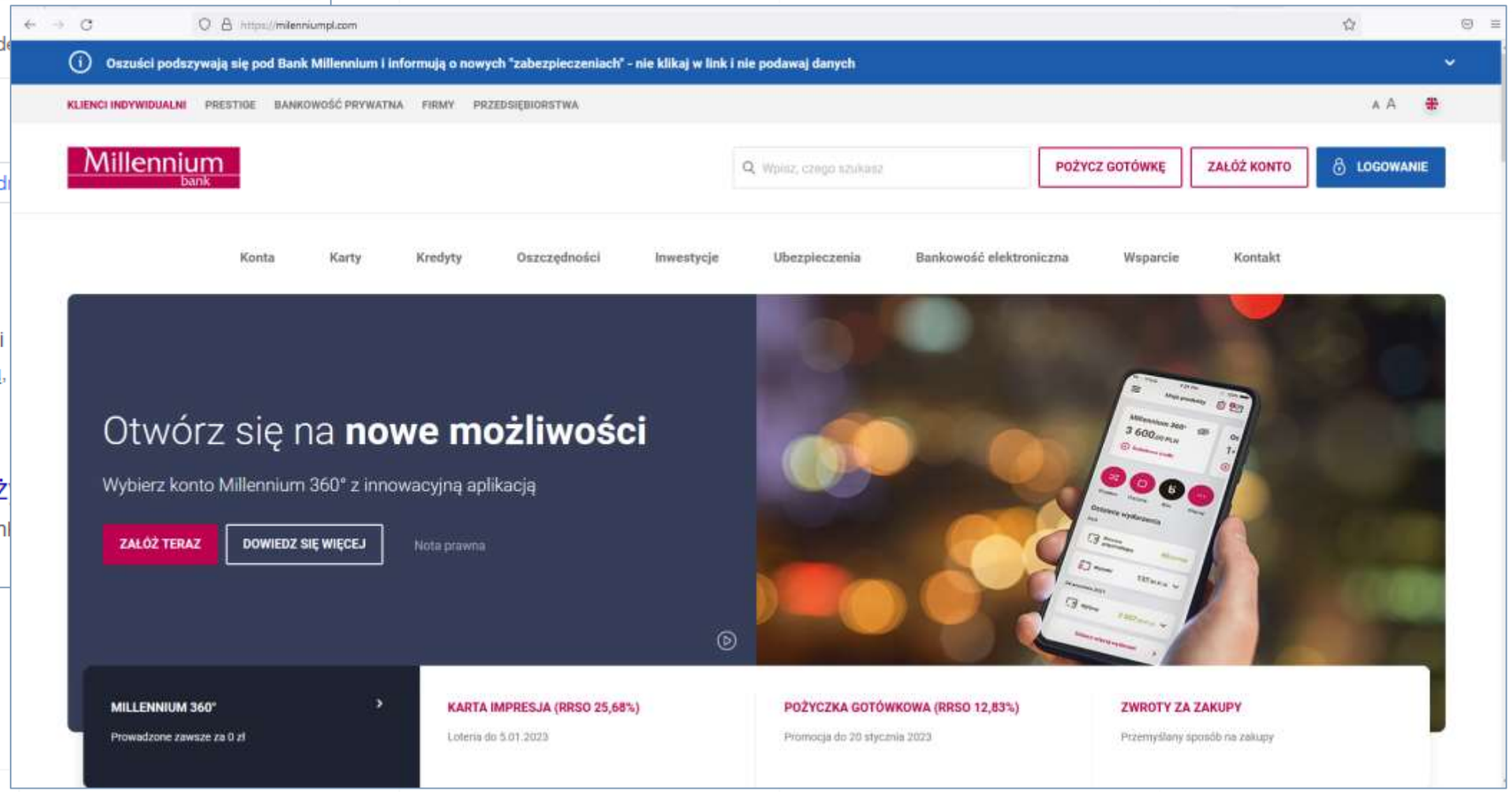


Inne oszustwa

- Metody ataku i socjotechnika

Fałszywe reklamy, fałszywe strony

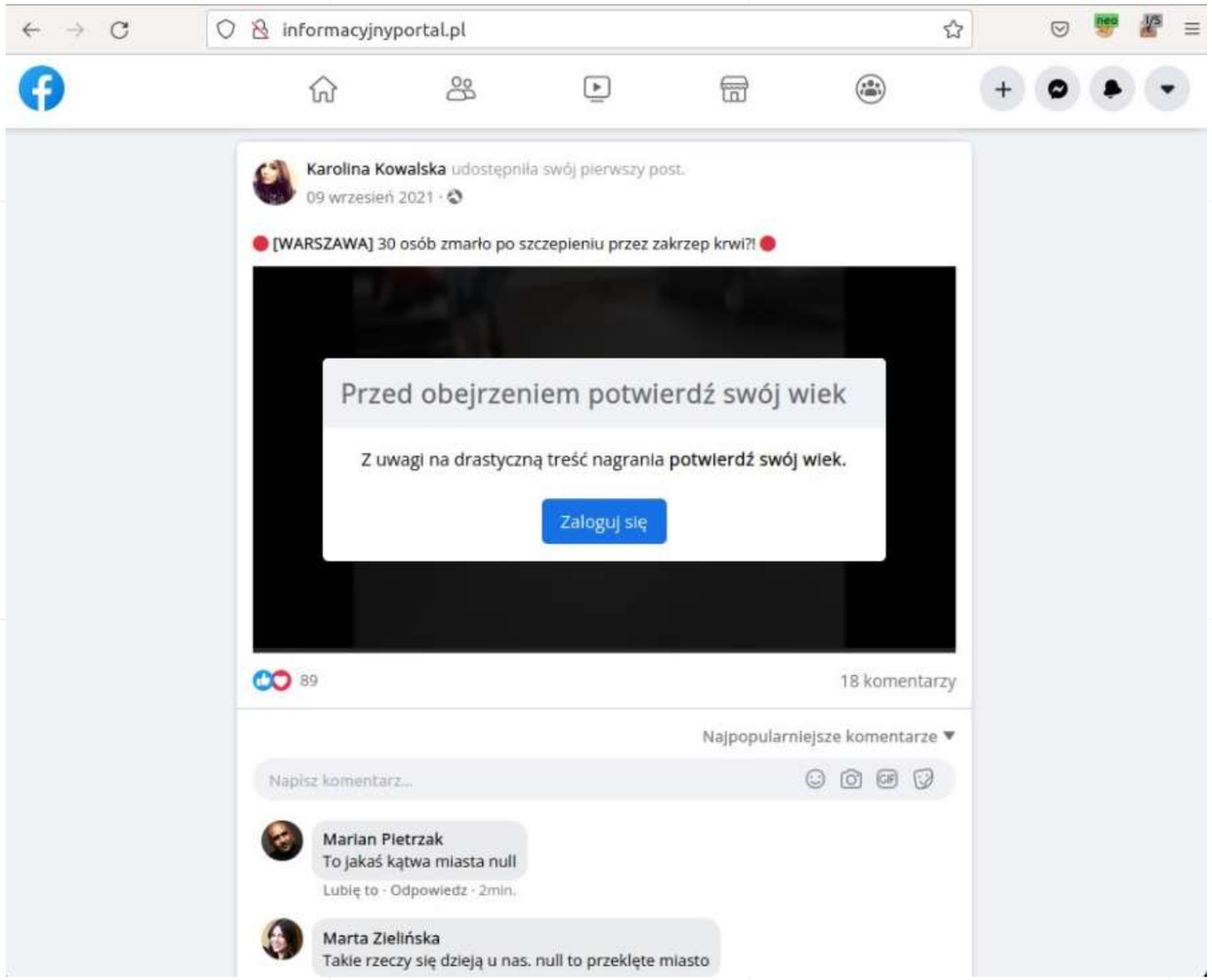




Oszustwa w mediach społecznościowych

Ataki na użytkowników mediów społecznościowych

Konieczność „potwierdzenia wieku”

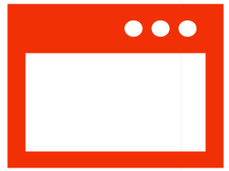


…lub inny dowolny pretekst:

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

Podsumowując…

Dostajemy:



Tracimy:

Login i hasło, czasem kod jednorazowy

Dane **karty płatniczej**/ numer blik → pieniądze

Dane osobowe

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********

Ochrona przed phishingiem

Jak postępować po otrzymaniu **KAŻDEJ** wiadomości?

Zatrzymaj się.

Daj sobie czas na ocenę sytuacji…

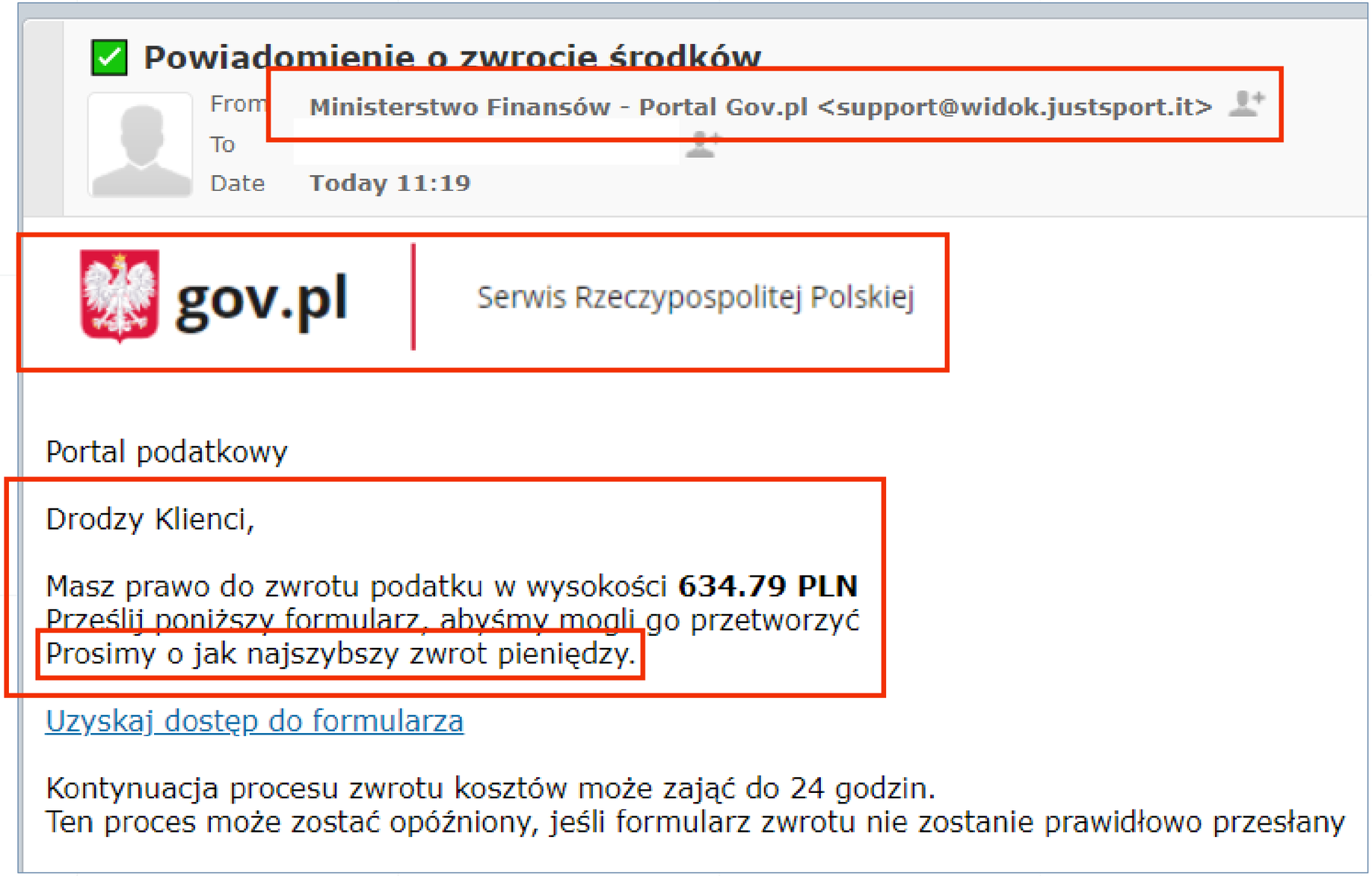
Ocena sytuacji
– **Jak patrzeć na wiadomość?**

1. Sprawdź czy **kontekst wiadomości** jest ukierunkowany na podjęcie przez ciebie szybkich działań.

2. Weryfikuj **adres domeny**, z której przyszedł e-mail (nazwa domenowa to część adresu po znaku „@”).

3. Nie daj się zwieść **pozorom** (logo, stopki, formatu i kolorystyki maili).

4. Zwracaj uwagę na **błędy językowe** (ale: wykorzystanie modeli językowych, coraz lepsza treść).



Powiadomienie o zwrocie środków

From: **Ministerstwo Finansów - Portal Gov.pl <support@widok.justsport.it>**

To:

Date: **Today 11:19**

gov.pl | Serwis Rzeczypospolitej Polskiej

Portal podatkowy

Drodzy Klienci,

Masz prawo do zwrotu podatku w wysokości **634.79 PLN**
Prześlij poniższy formularz, abyśmy mogli go przetworzyć
Prosimy o jak najszybszy zwrot pieniędzy.

Uzyskaj dostęp do formularza

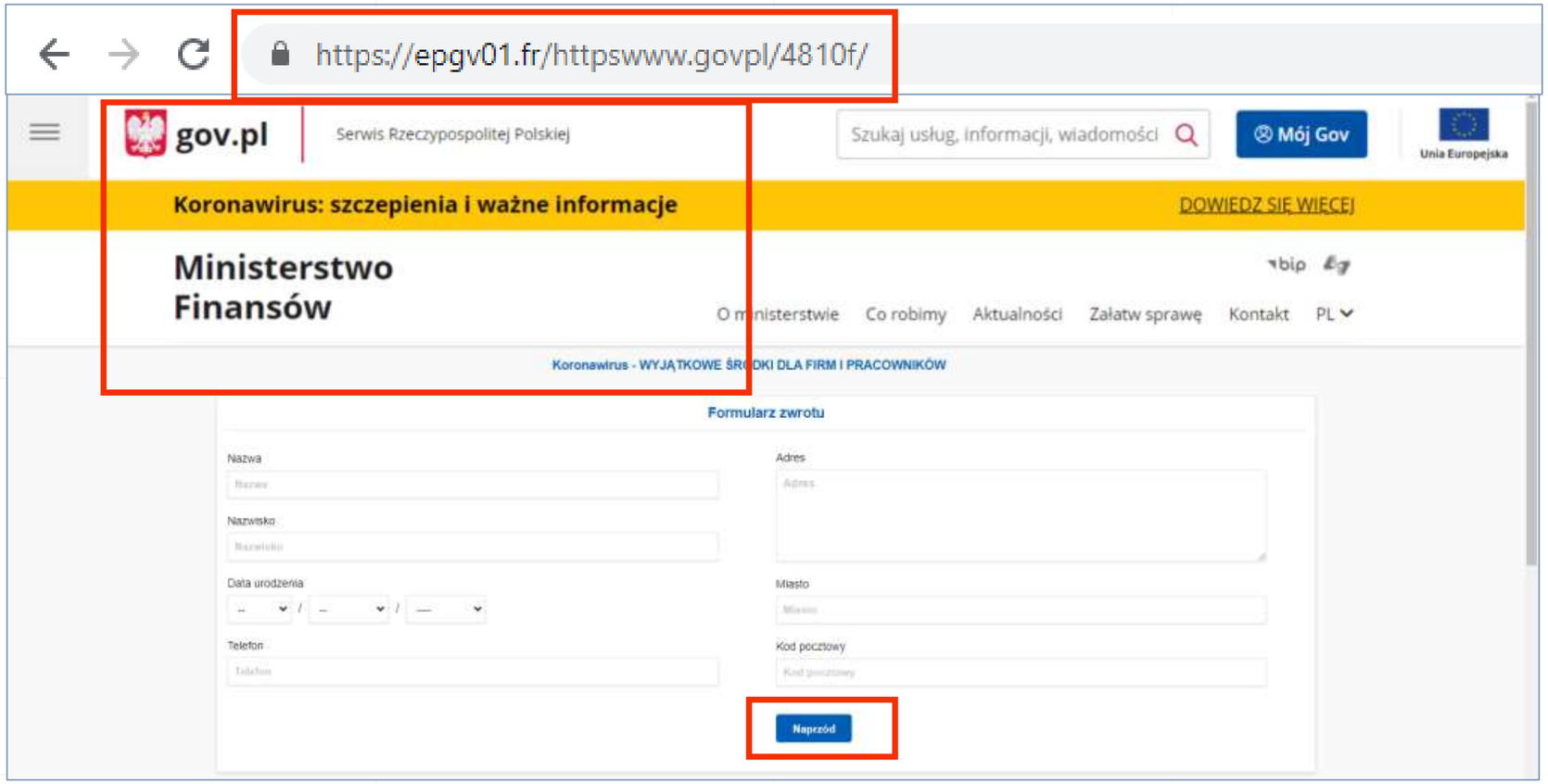
Kontynuacja procesu zwrotu kosztów może zająć do 24 godzin.
Ten proces może zostać opóźniony, jeśli formularz zwrotu nie zostanie prawidłowo przesłany

Jeżeli masz wątpliwości, nie ryzykuj.

Jeżeli zauważysz któryś z wcześniej wymienionych symptomów:

- nie klikaj w linki.
- nie pobieraj (i nie otwieraj!) załączników.
- nie odpowiadaj na wiadomość.

Zgłoś otrzymaną wiadomość do CERT Polska, a następnie usuń ją.


https://epgv01.fr/httpswww.govpl/4810f/
gov.pl
Serwis Rzeczypospolitej Polskiej
Szukaj usług, informacji, wiadomości
Mój Gov
Unia Europejska
Koronawirus: szczepienia i ważne informacje
DOWIEDZ SIĘ WIĘCEJ
Ministerstwo Finansów
O ministerstwie
Co robimy
Aktualności
Załatw sprawę
Kontakt
PL
Koronawirus - WYJĄTKOWE ŚRODKI DLA FIRM I PRACOWNIKÓW
Formularz zwrotu
Nazwa
Adres
Nazwisko
Data urodzenia
Miasto
Telefon
Kod pocztowy
Naprzód


Zwrot środków - dane bankowe beneficjenta
Karta kredytowa
Termin ważności
CVV (3 Dane na odwrocie)
Naprzód
OGÓLNE INFORMACJE DOTYCZĄCE ZWROTU PIENIĘDZY
Odbiorca zwrotu
Smiki Nowak
Jak otrzymać
Karta kredytowa
Liczba plików
21926AXD197
Kwota Refundacji
634.86 PLN
Data
26/03/2021
Warunki płatności
24 godziny

Oszustwo w rozmowie telefonicznej

- czyli **vishing** (voice phishing)

Vishing – atak telefoniczny

ang. Voice + phishing

Uniwersalny pretekst kontaktu.

Stosowanie technik manipulacji w rozmowie.

Uwaga na **spoofing**,
czyli **podszywanie się pod zaufany numer telefonu!**

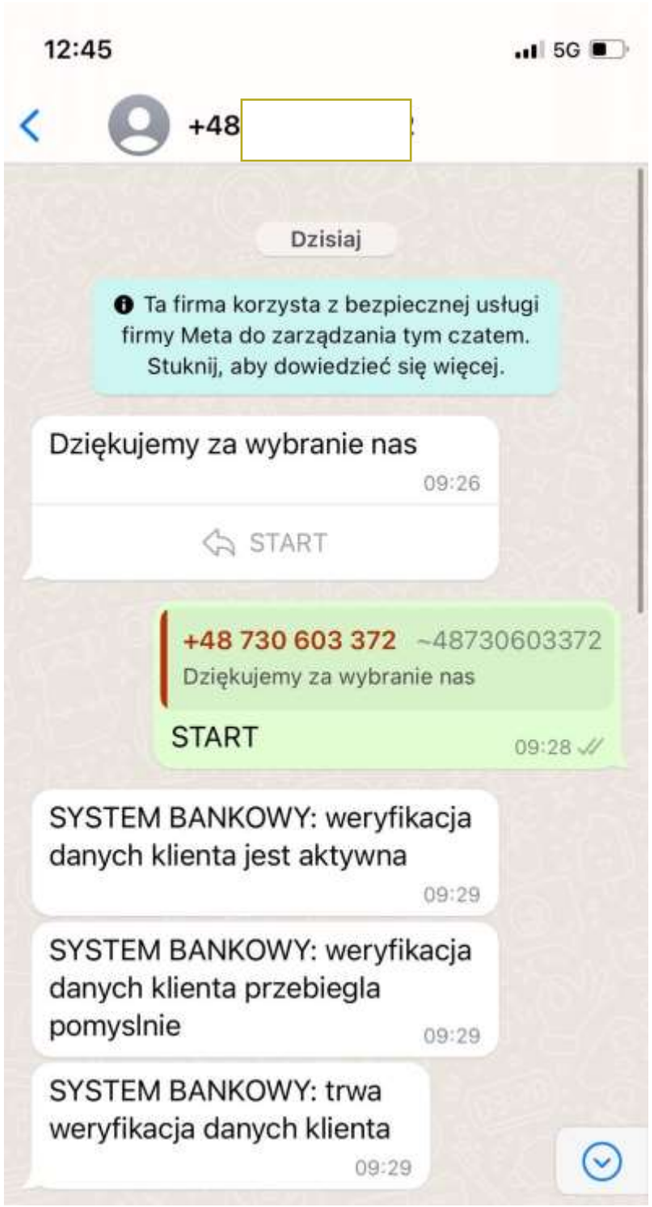
(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

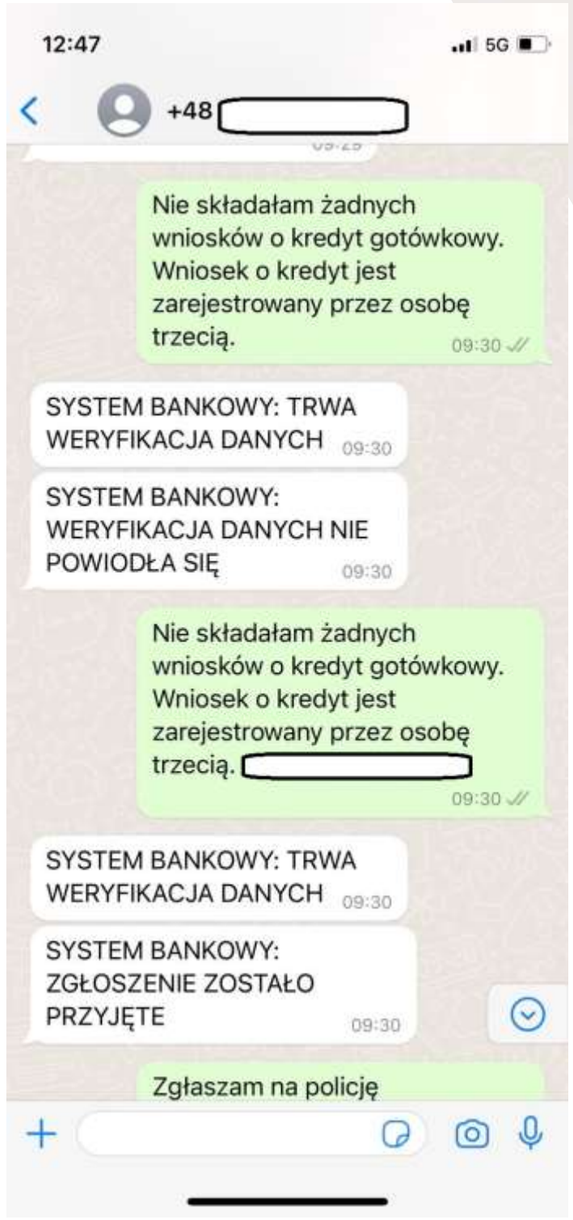
Ministerstwo Cyfryzacji

NASK

Cele ataku

- Wyłudzenie informacji
- Instalacja oprogramowania
- Wykonanie przelewu





(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Atak telefoniczny „na zdalny pulpit”

TeamViewer

AnyDesk

ALPEMIX

Atak 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

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

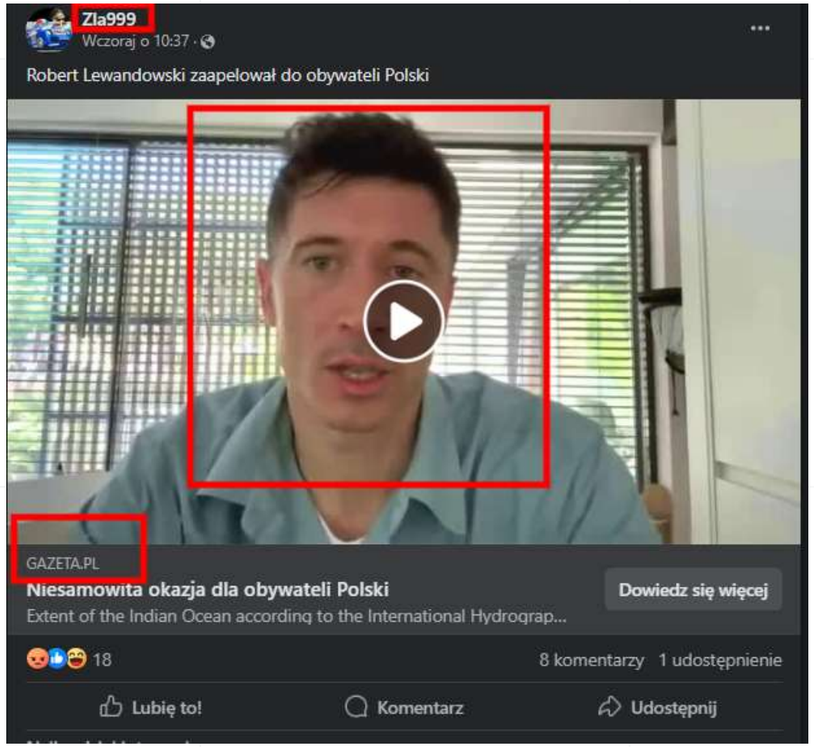
Ministerstwo Cyfryzacji

NASK

Deep fake

- czyli jak oszuści wykorzystują AI

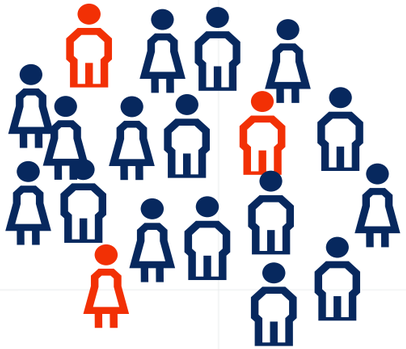
Wykorzystanie wizerunku znanych postaci



Materiał o Deep fake'ach, Adrian Kilar:
https://www.youtube.com/watch?v=-nys7TAzSBg

Źródło:
https://sportowefakty.wp.pl/pilka-nozna/1118746/oszusci-wykorzystuja-nagranie-z-lewandowskim-jest-ostrzezenie

Rodzaje ataków w zależności od grupy docelowej



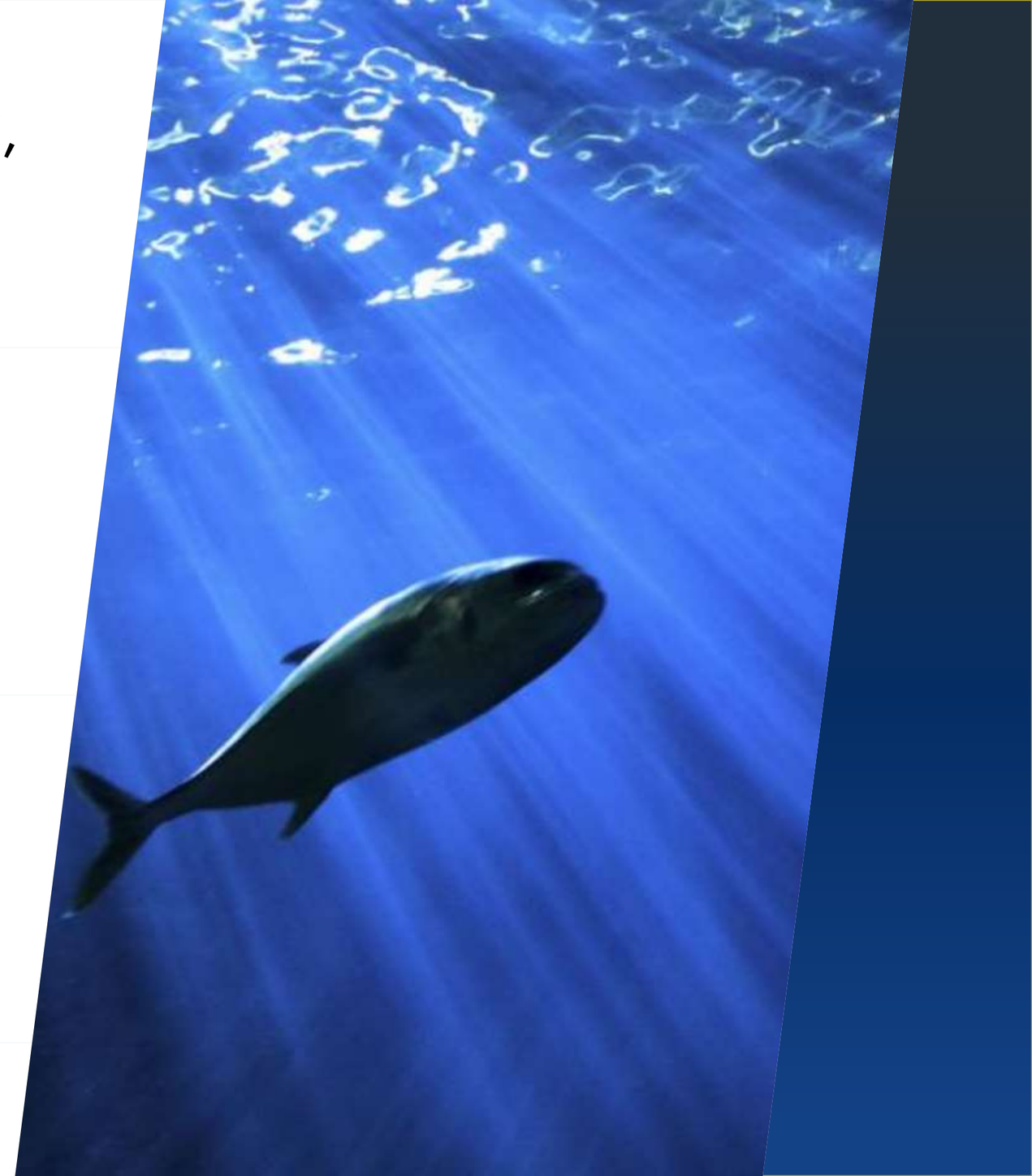
masowy

spersonalizowany

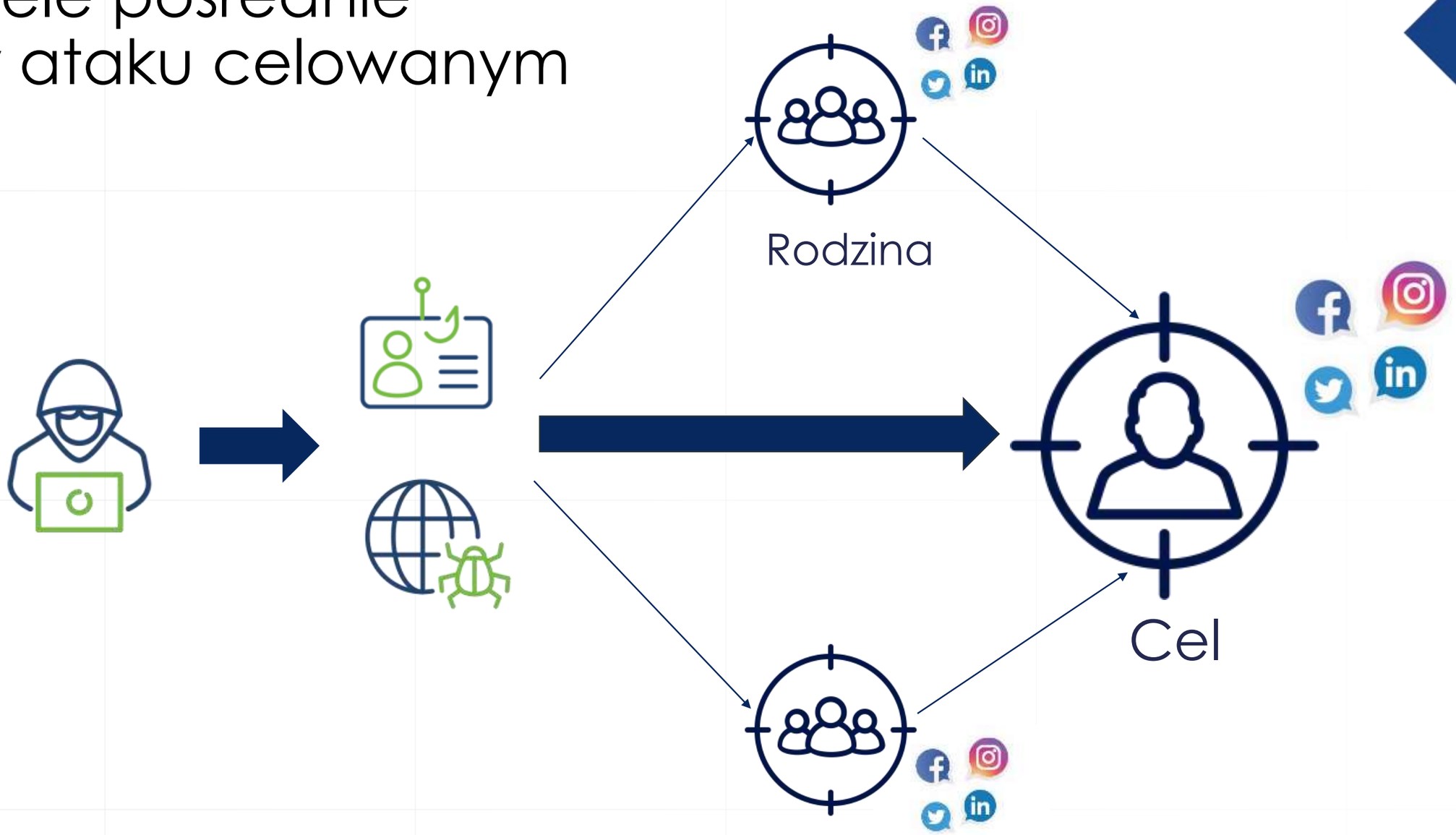
Phishing spersonalizowany, celowany

ang. Spear phishing, whaling

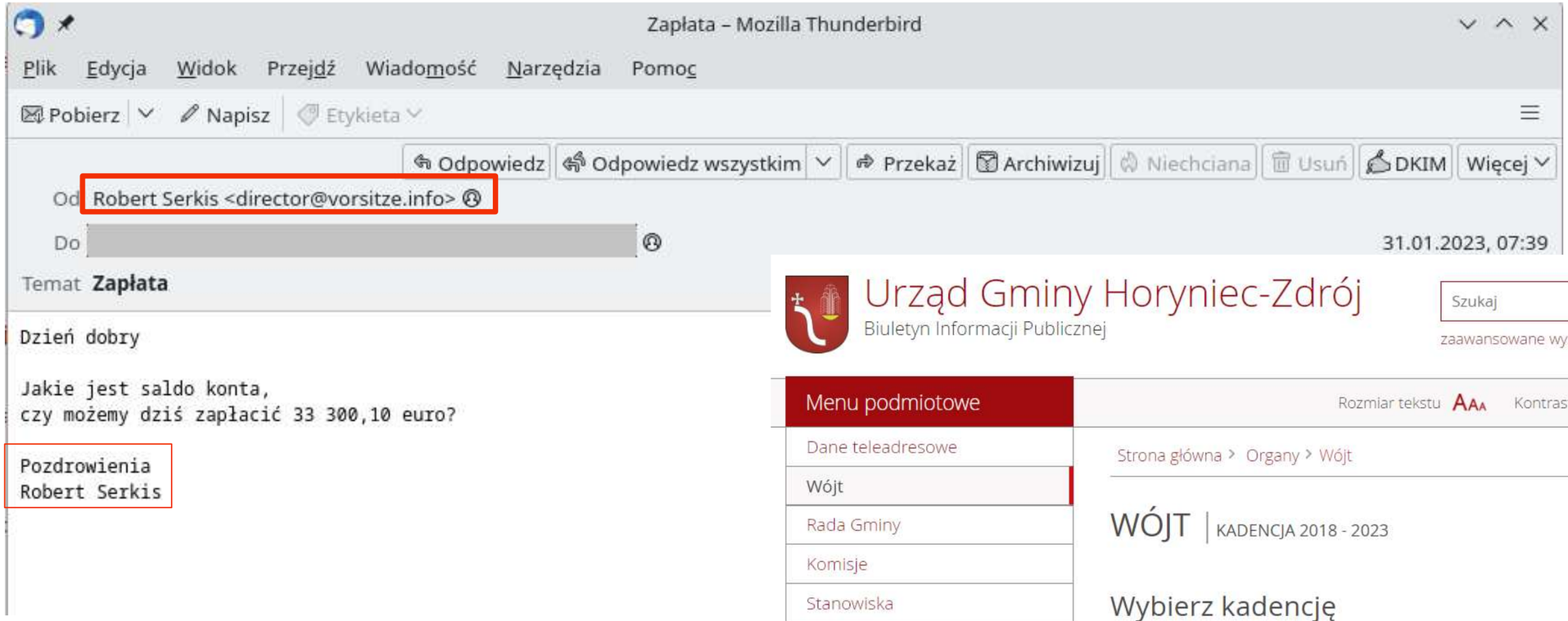
- **Precyzyjnie wybrany cel** – osoba lub grupa;
- **Rozpoznanie** celu i jego otoczenia;
- Pretekst i historia ataku **precyzyjnie dopasowane**.

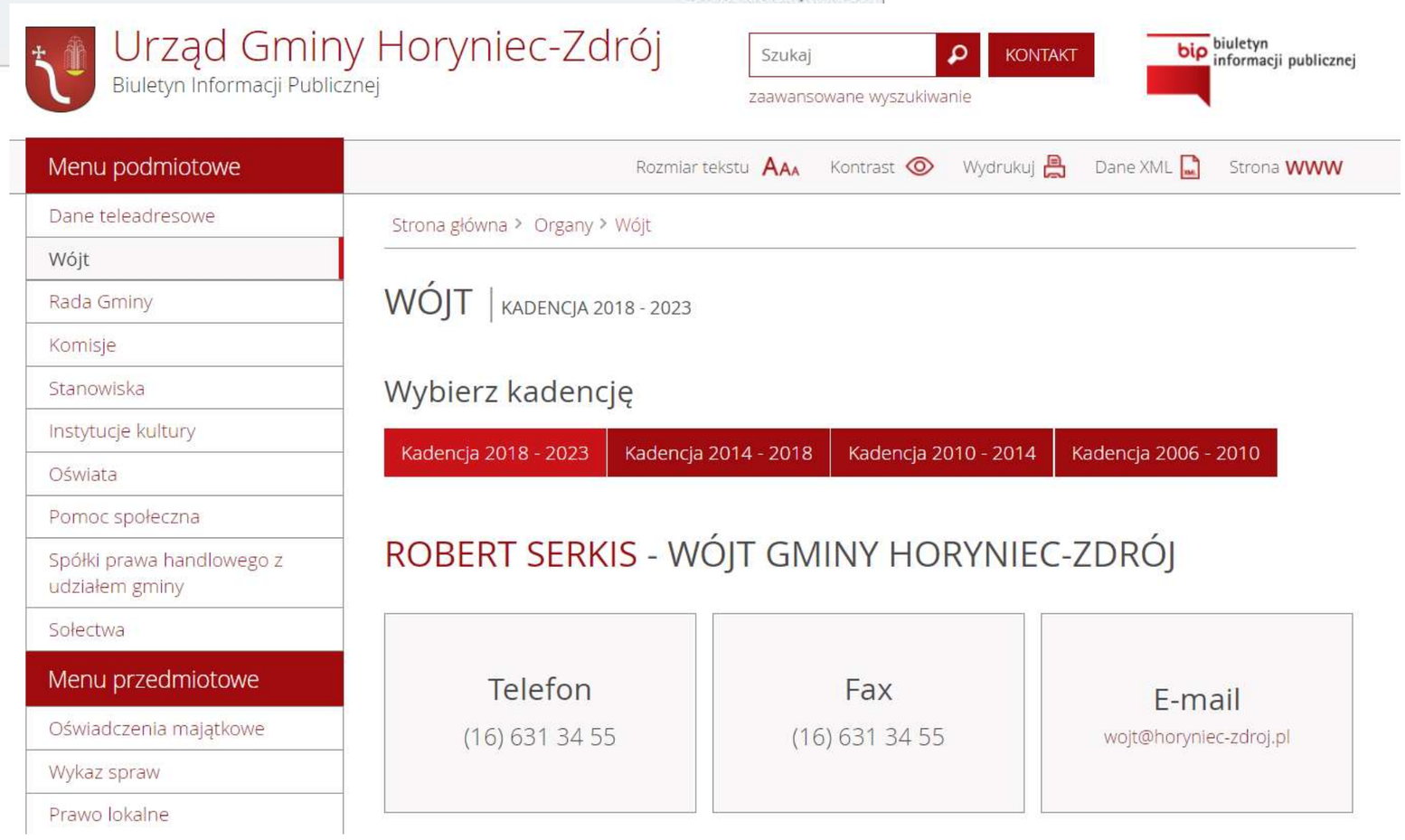


Cele pośrednie w ataku celowanym



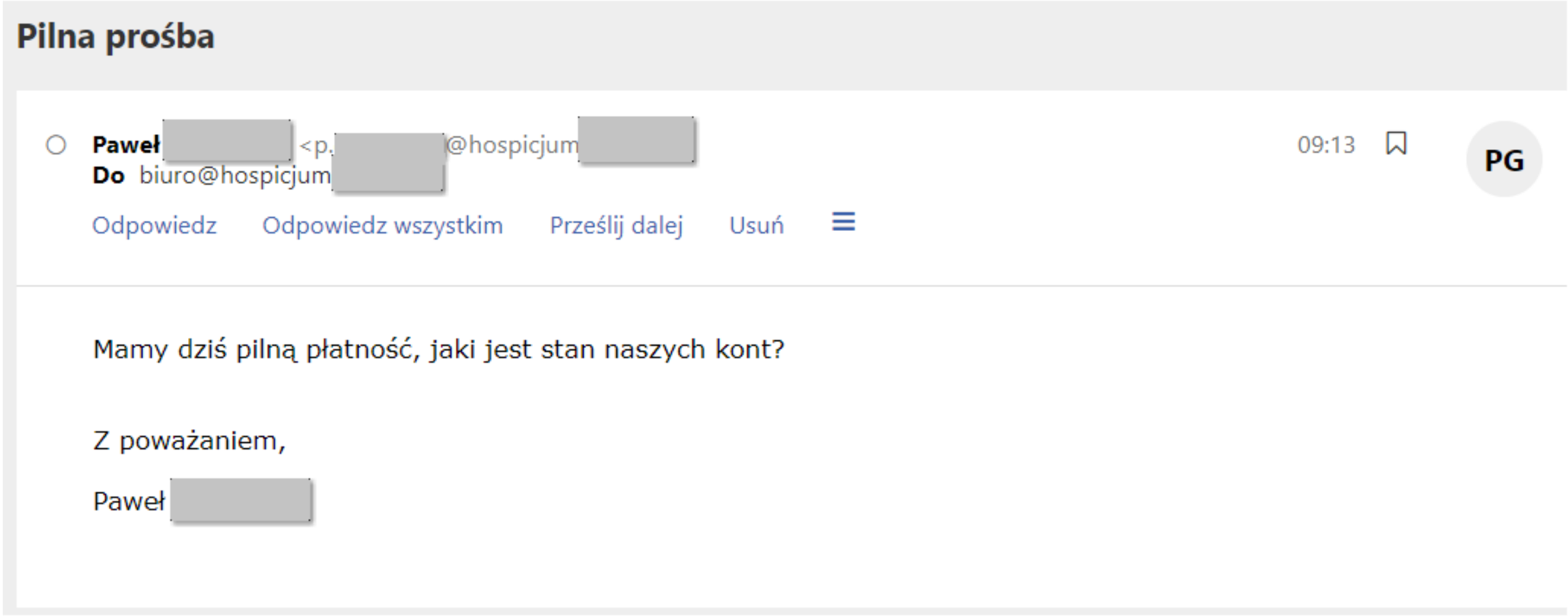
„Oszustwo na dyrektora” – atak na JST





(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

„Oszustwo na dyrektora” ze spoofingiem



Pilna prośba

Paweł <p.@hospicjum
Do biuro@hospicjum

09:13

PG

Odpowiedz Odpowiedz wszystkim Prześlij dalej Usuń

Mamy dziś pilną płatność, jaki jest stan naszych kont?

Z poważaniem,

Paweł

Przykład oszustwa skierowanego do gminy

Pobierz | Napisz | Etykieta

Odpowiedz | Odpowiedz wszystkim | Przekaż | Archiwizuj | Niechciana | Usuń | DKIM | Więcej

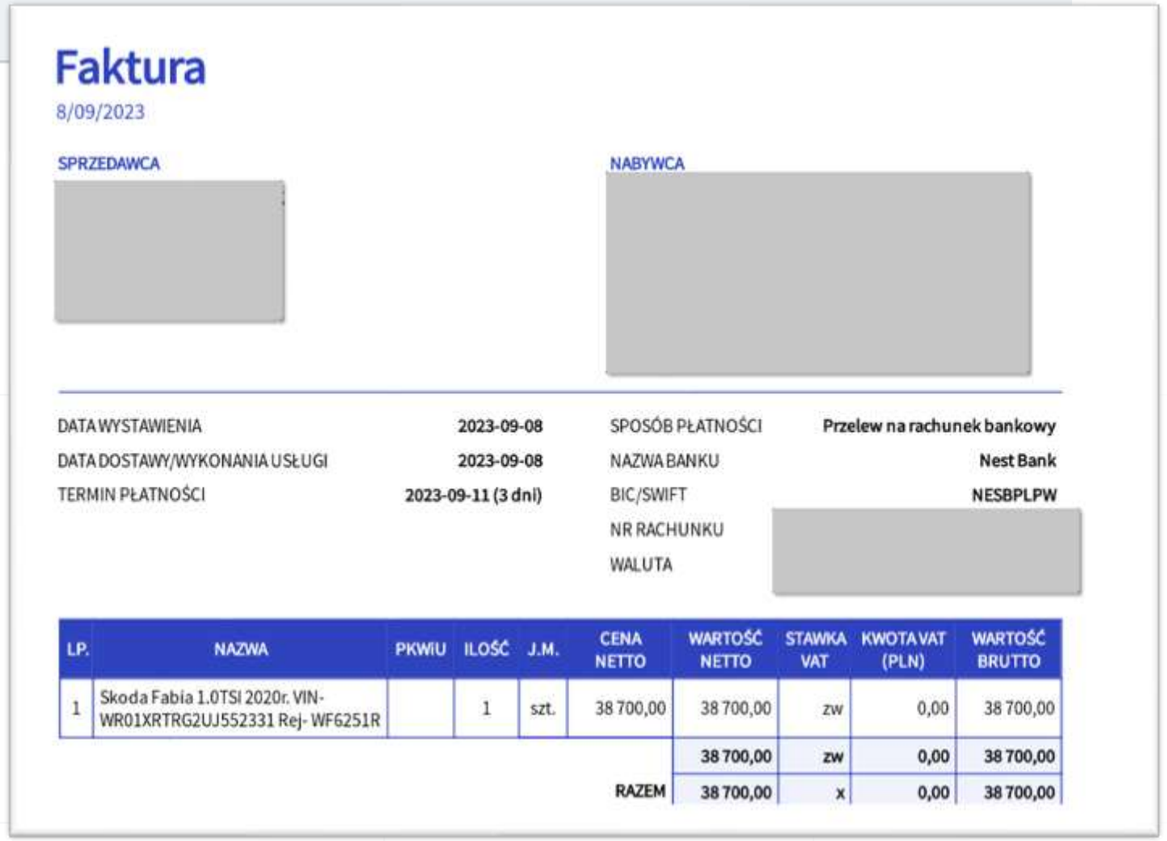
Od j.r[redacted]pl <j.[redacted]com>

Do [redacted]<skarbnik@[redacted]pl>

14.09.2023, 11:26

Temat **Re: RE: Faktura**

W załączniku faktura do opłaty.



Faktura

8/09/2023

SPRZEDAWCA [redacted]

NABYWCA [redacted]

DATA WYSTAWIENIA	2023-09-08	SPOSÓB PŁATNOŚCI	Przelew na rachunek bankowy
DATA DOSTAWY/WYKONANIA USŁUGI	2023-09-08	NAZWA BANKU	Nest Bank
TERMIN PŁATNOŚCI	2023-09-11 (3 dni)	BIC/SWIFT	NESBPLPW
		NR RACHUNKU	[redacted]
		WALUTA	

LP.	NAZWA	PKWiU	ILOŚĆ	J.M.	CENA NETTO	WARTOŚĆ NETTO	STAWKA VAT	KWOTA VAT (PLN)	WARTOŚĆ BRUTTO
1	Skoda Fabia 1.0TSI 2020r. VIN-WR01XRTRG2UJ552331 Rej- WF6251R		1	szt.	38 700,00	38 700,00	zw	0,00	38 700,00
						38 700,00	**zw**	**0,00**	**38 700,00**
					RAZEM	**38 700,00**	**x**	**0,00**	**38 700,00**

Złośliwe oprogramowanie

- czyli o szkodliwych programach i socjotechnice raz jeszcze

Złośliwe oprogramowanie

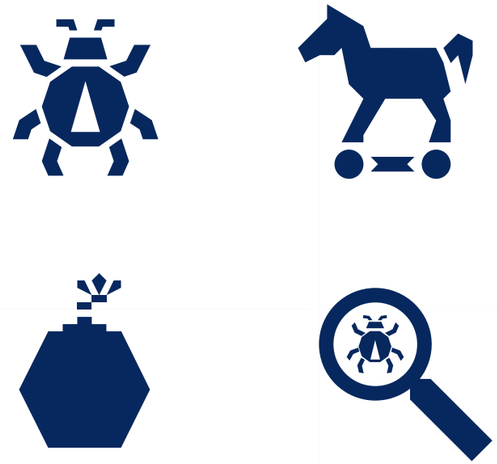
ang. **malware** (*malicious* - złośliwy i *software* - oprogramowanie)

– ogół programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkowników.

Złośliwe oprogramowanie

Aktualnie stosuje się podział ze względu na **sposób działania**:

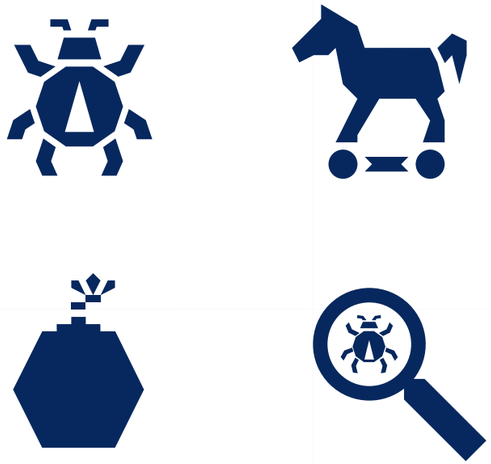
- ransomware
- trojany bankowe (bankery)
- spyware
- RAT (remote access trojan)
- kryptokoparki
- ...



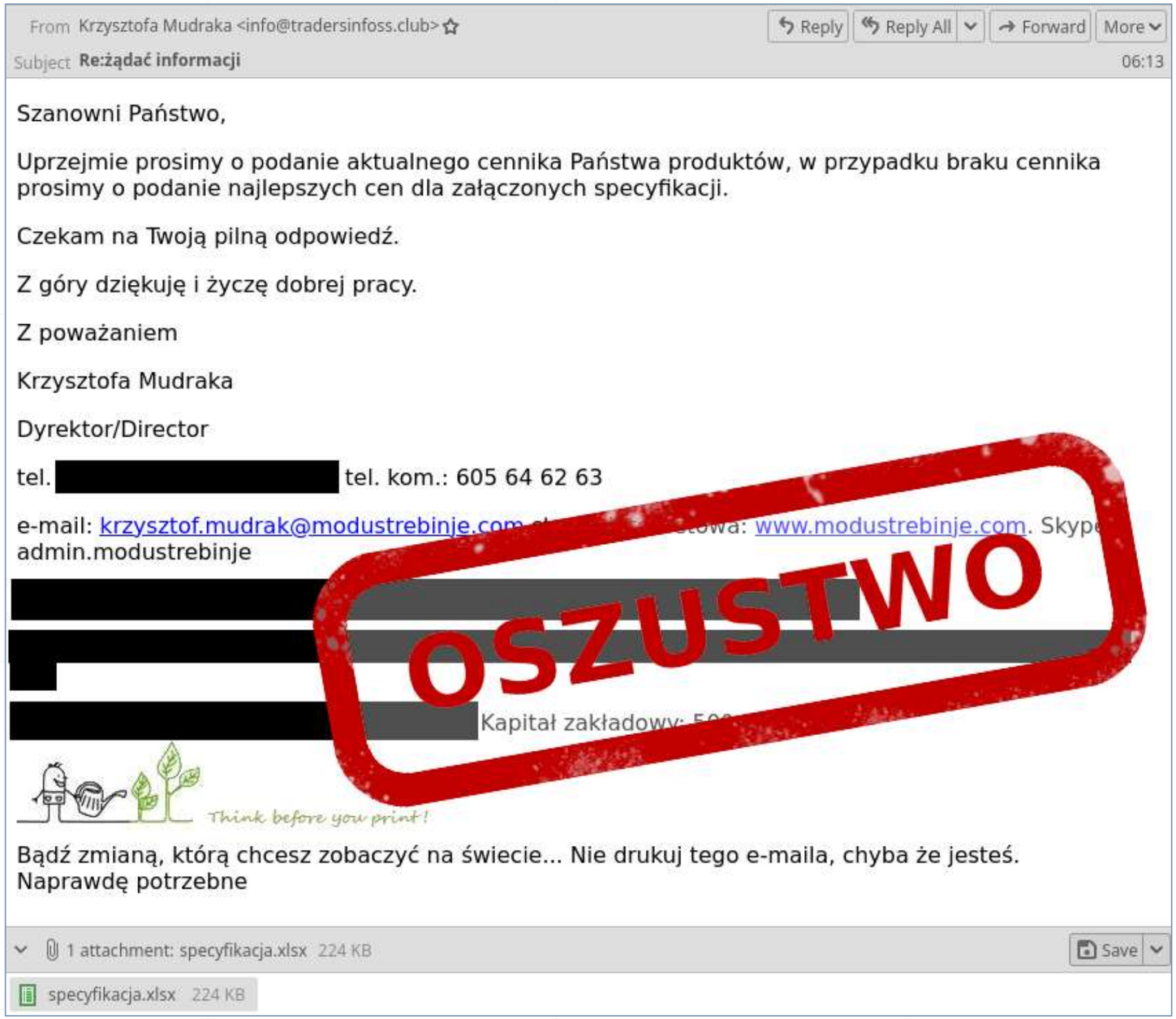
W jaki sposób przestępcy infekują urządzenia?

Źródła infekcji

- Luki bezpieczeństwa w publicznie dostępnych usługach;
- Niewystarczające zabezpieczenia dostępu do infrastruktury oraz publicznych usług (często zbyt słabe hasło);
- **Maile nakłaniające do pobrania i uruchomienia pliku załączonego lub umieszczonego w linku.**



Załączniki w spreparowanych mailach



(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Najczęściej stosowane załączniki

Obecnie najbardziej podejrzane:

- **archiwa i obrazy dysków:**

.zip .rar .iso .img

- pliki wykonywalne
  (najczęściej wewnątrz poprzednich)

.exe .com .scr .vbs .js

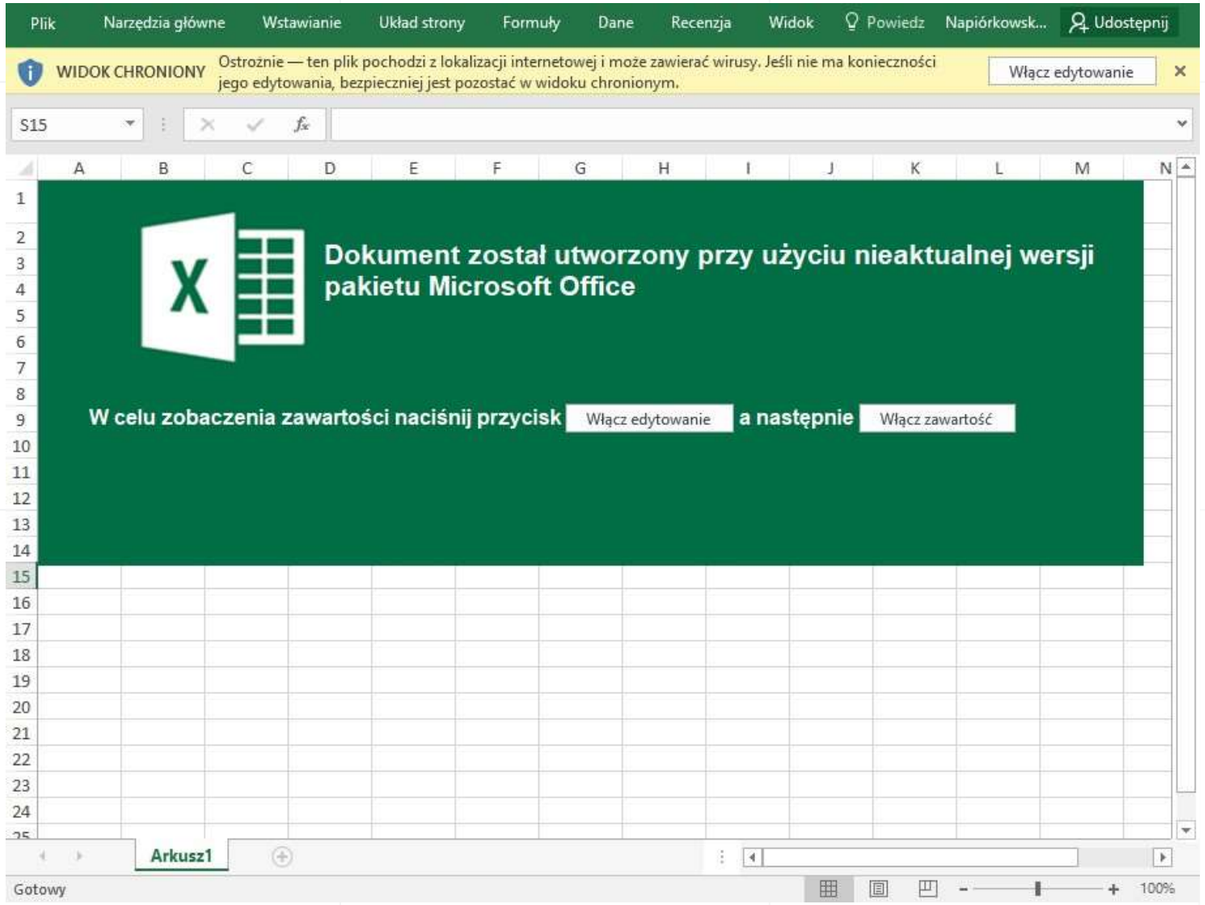
- linki i kopie stron (z dodatkową zawartością)

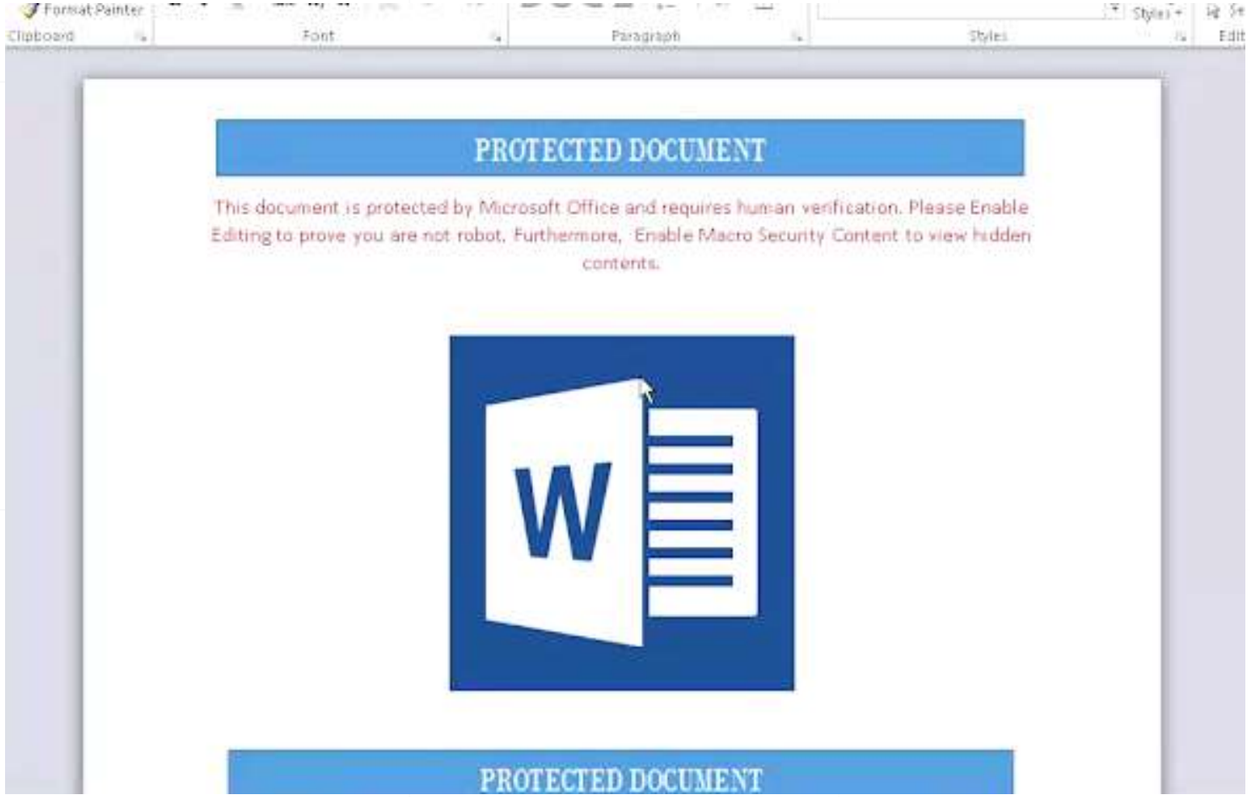
.lnk .htm .html

- pliki oprogramowania biurowego

. one .xlsx .xlsm .xls .doc

Złośliwy kod w plikach MS Office



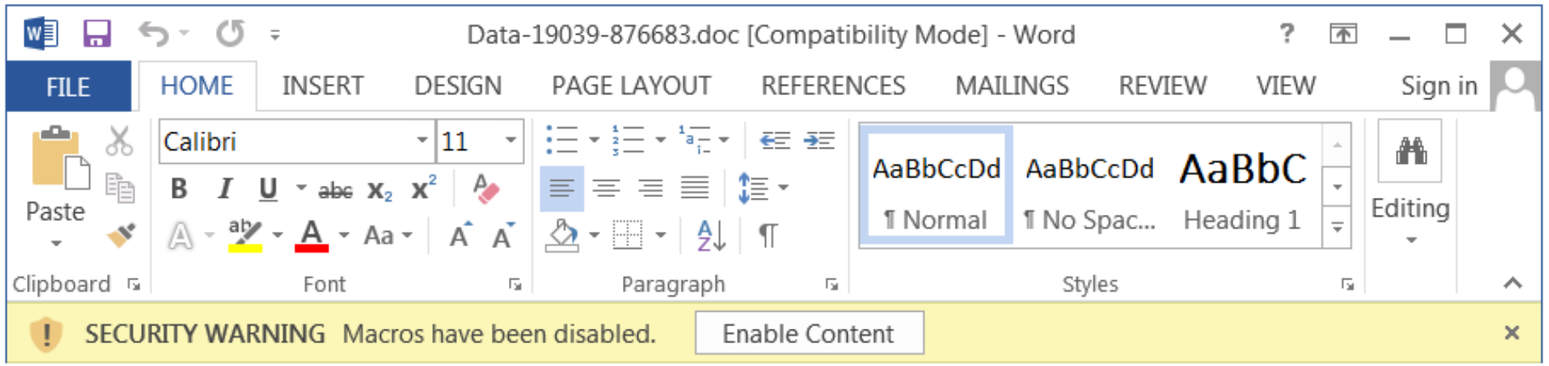


(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

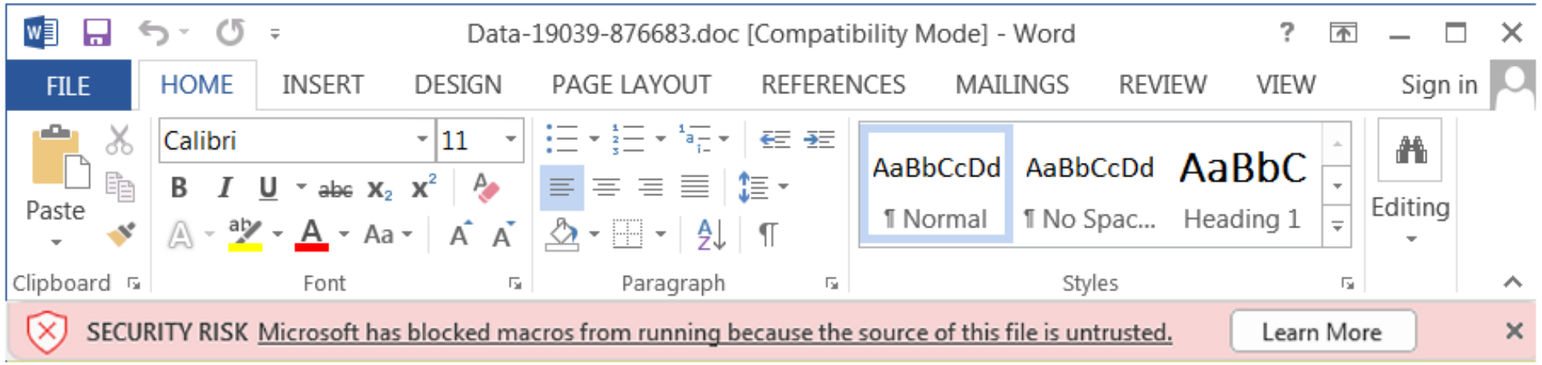
Ministerstwo Cyfryzacji

NASK

Zabezpieczenie plików MS Office



OLD SECURITY ALERT



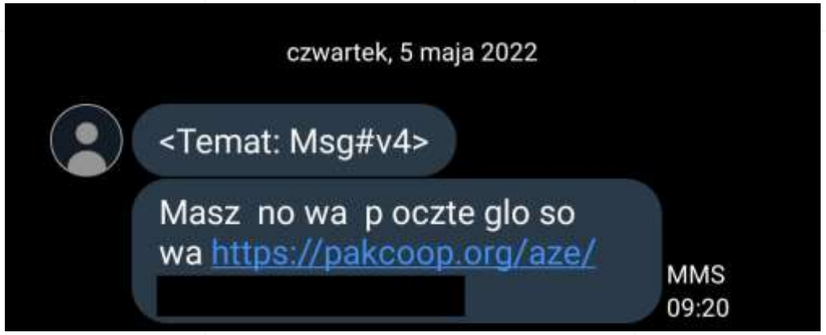
NEW SECURITY ALERT

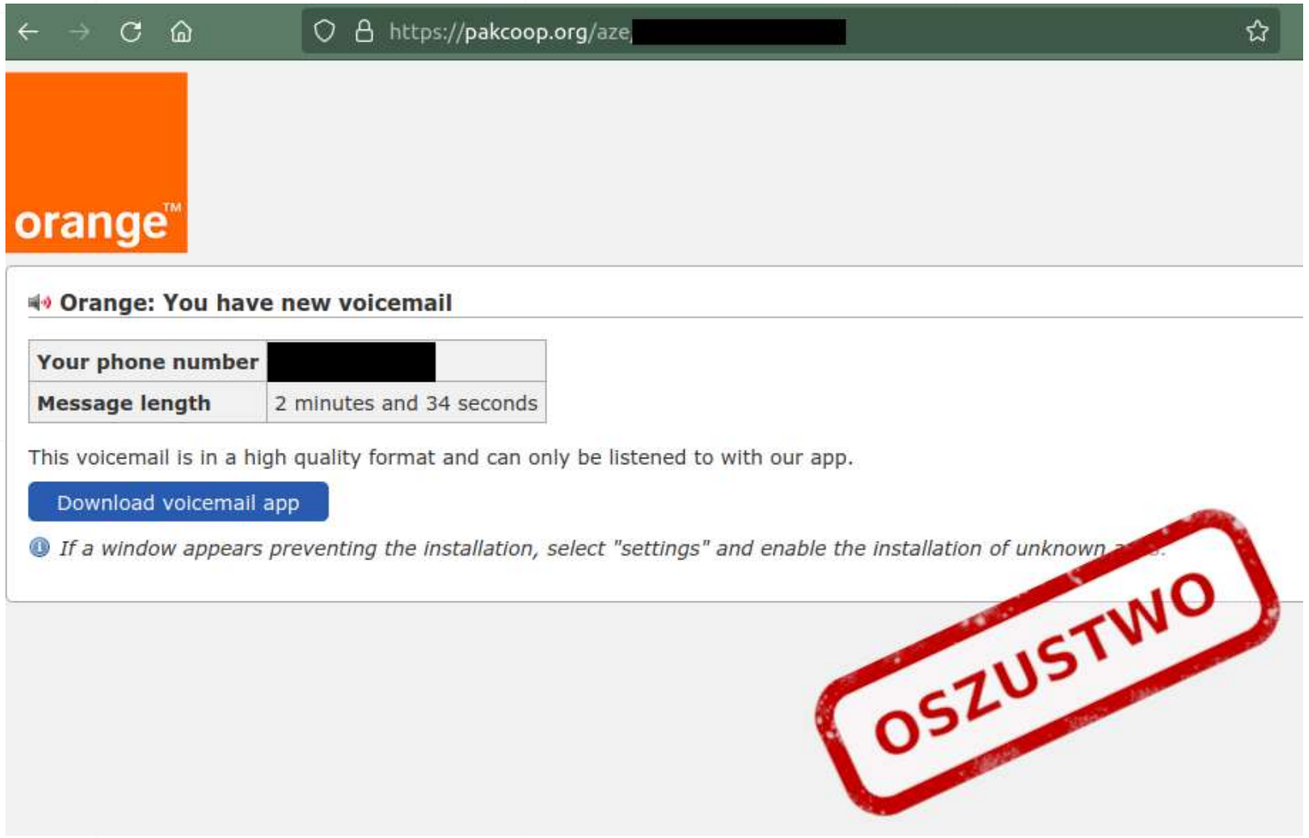
- bleepingcomputer.com

Złośliwe oprogramowanie na telefon

Sygnały alarmowe:

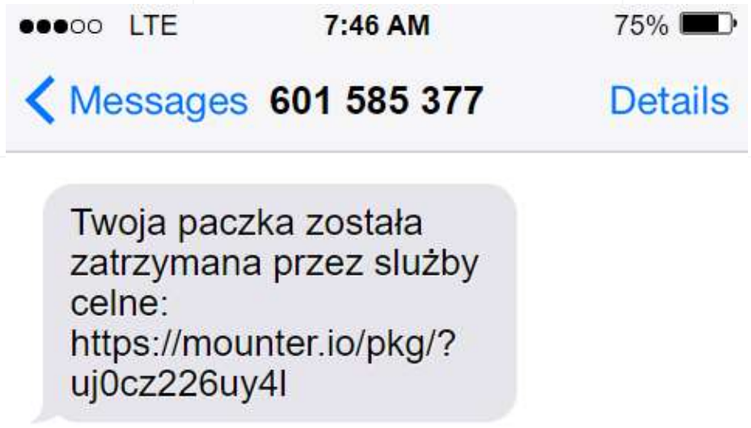
- **instalowanie „z nieznanych źródeł”**
- aplikacja żąda uprawnień **ułatwienia dostępu**

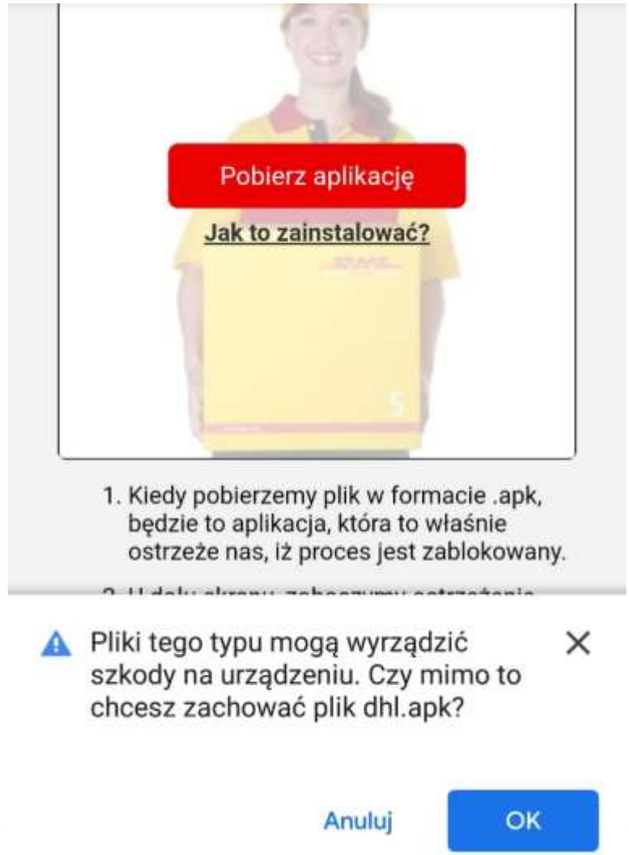




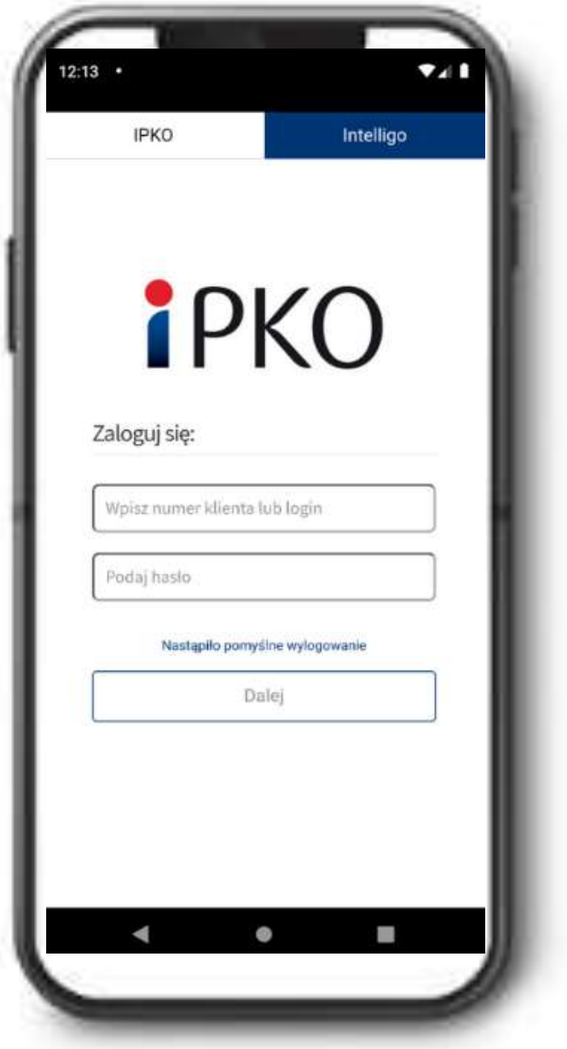
Złośliwe oprogramowanie na telefon

- instalacja z nieznanych źródeł **jest domyślnie wyłączona**, stąd instrukcja instalacji dla odbiorców ataku.

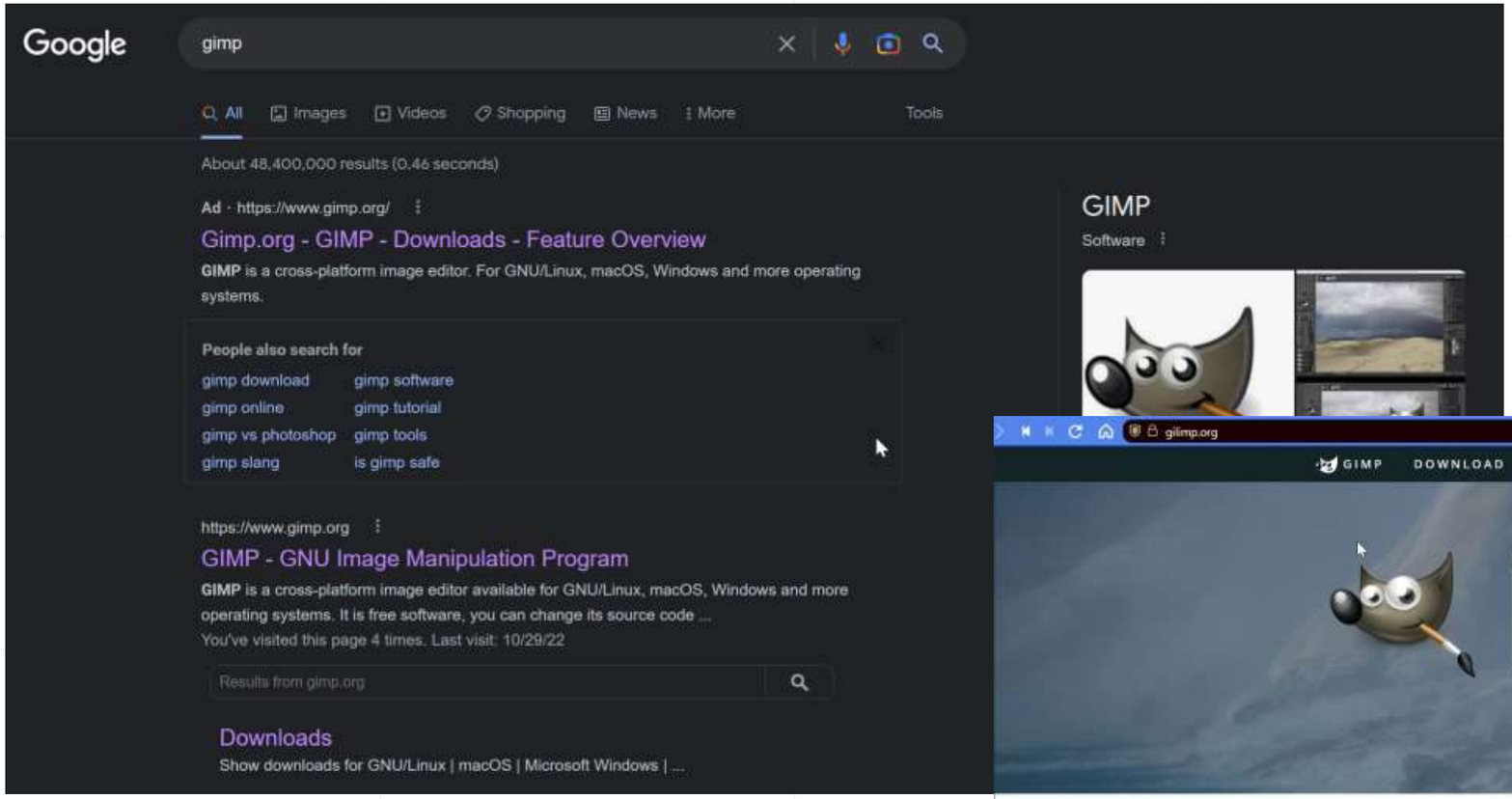




Trojan bankowy, wykradanie danych



Złośliwe oprogramowanie w reklamach

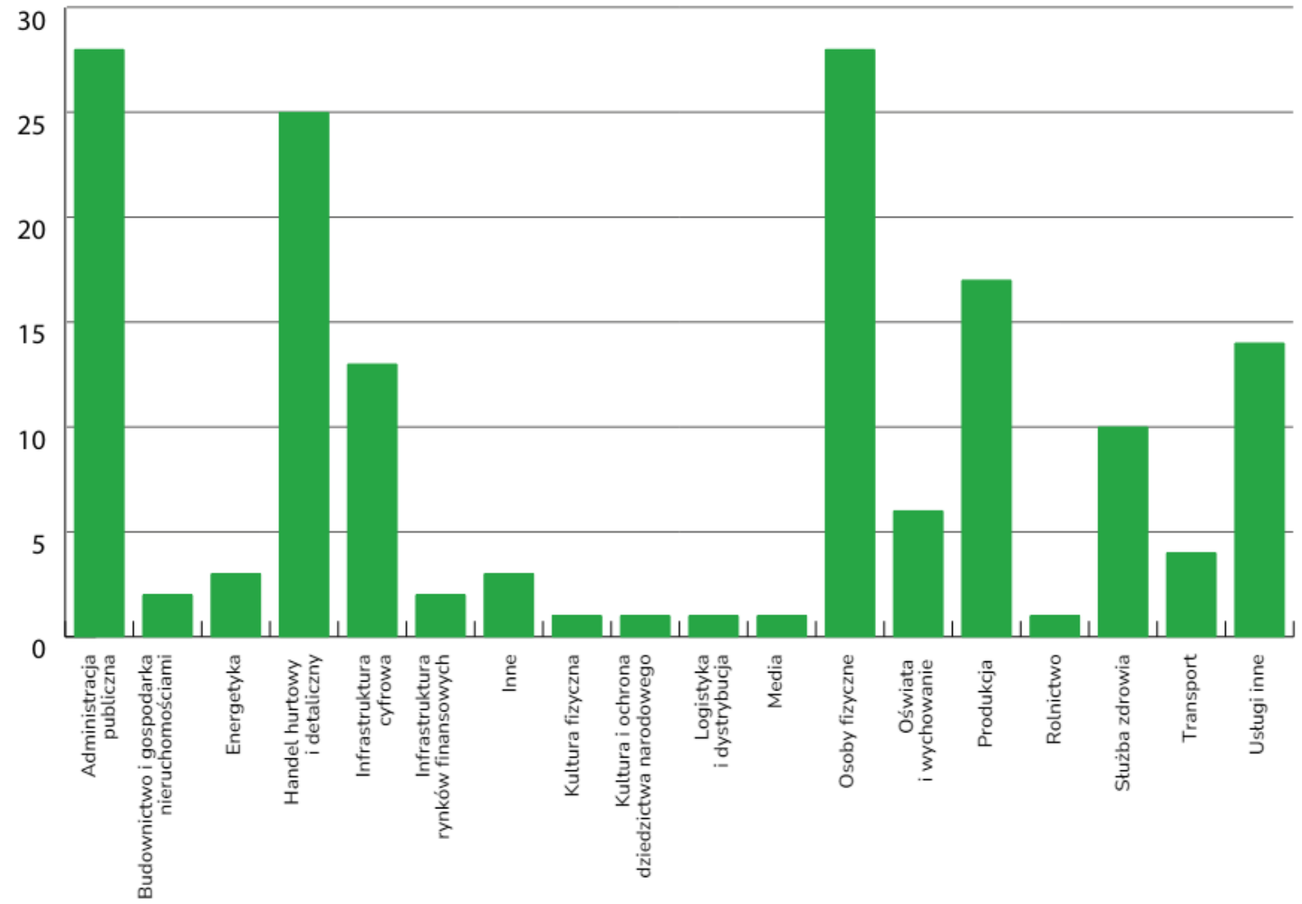


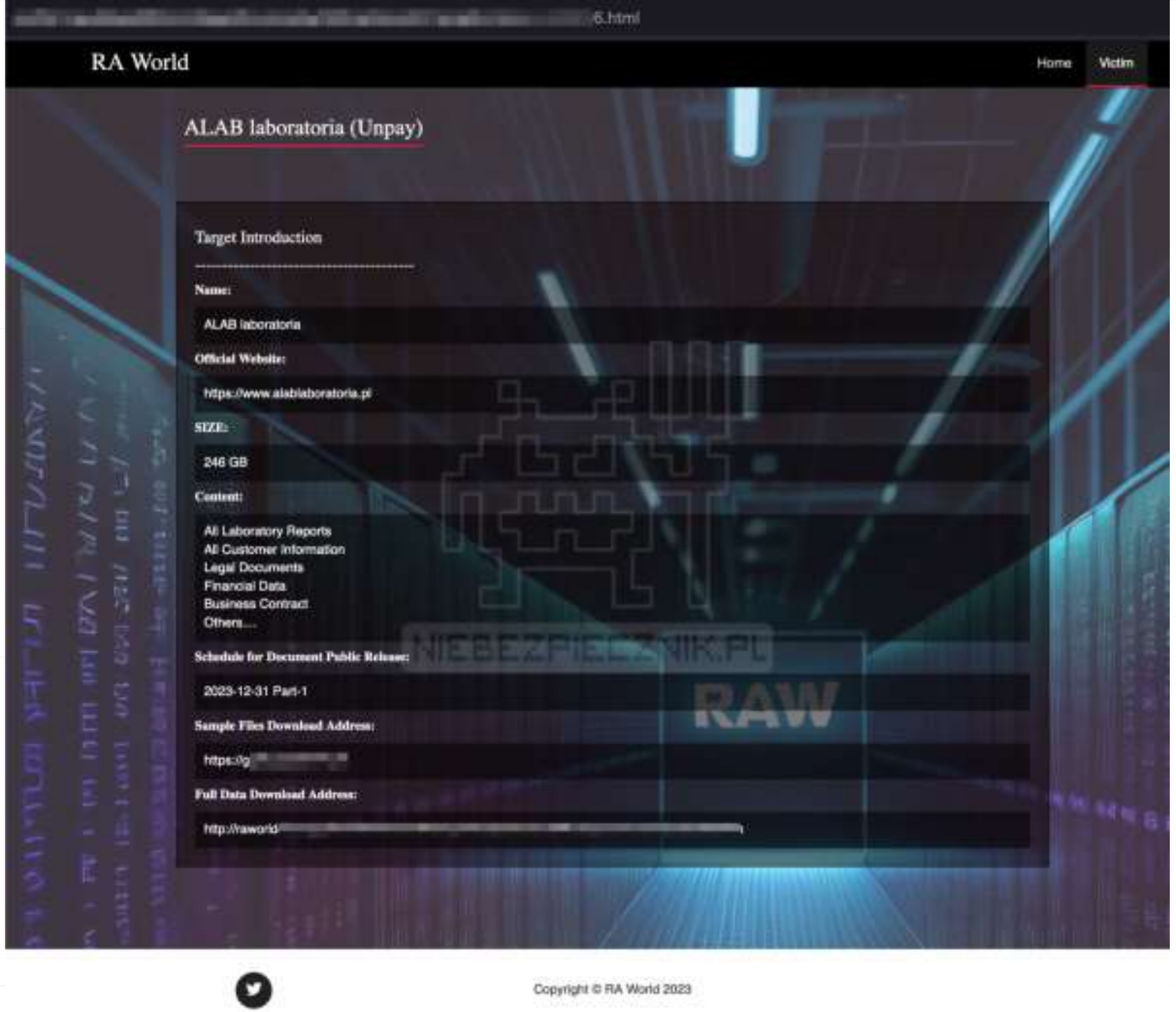
Ransomware

- Oprogramowanie blokujące system komputerowy

Nota z żądaniem okupu

Raport CERT Polska 2023 – ataki ransomware





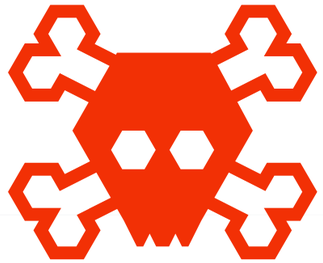
Źródło: https://niebezpiecznik.pl/tag/alab-laboratoria/

Ransomware – konsekwencje ataku

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

Często dochodzi również do **zaszyfrowania kopii zapasowych**.

Zapłacenie okupu nie gwarantuje odzyskania danych i nie jest wskazane.



Ransomware – prewencja

Podstawowe środki ochrony:

- **dobra strategia tworzenia i weryfikowania kopii zapasowych** **zasada 3-2-1** (prywatnie warto mieć dysk zewnętrzny na który kopiujemy dane albo trzymamy kopię plików w chmurze);
- **regularna aktualizacja oprogramowania,**
- **edukacja własna i użytkowników.**

(CYBER)SZKOLENIA

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

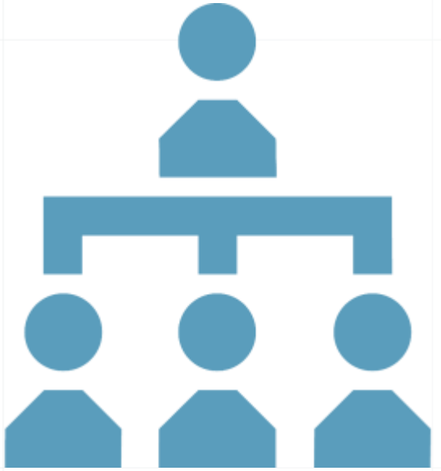
Zgłaszanie incydentu

Ministerstwo Cyfryzacji

NASK

Kto zgłasza incydent w organizacji?

Incydent w środowisku służbowym może i powinna zgłaszać **każda osoba** w organizacji, ale:



Pracownicy zgłaszają do **zespołu bezpieczeństwa/ helpdesku.**

Do CSIRT incydent zgłasza **wyznaczona osoba** (lub komórka organizacyjna).

Zgłoszenie incydentu do CSIRT NASK

- Wyznaczona osoba/ zespół bezpieczeństwa
- Incydent należy **zgłosić niezwłocznie, nie później niż w ciągu 24 godzin** od momentu wykrycia do właściwego CSIRT.
- Zgłoszenie przekazywane jest **w postaci elektronicznej**, poprzez uzupełnienie **formularza internetowego** znajdującego się na stronie: **https://incydent.cert.pl**.

24 godz.

https://incydent.cert.pl

lub

w systemie S46

Informacje prawnie chronione

- Poszczególne **zespoły CSIRT mają prawo przetwarzać dane osobowe**, w tym także **tajemnice prawnie chronione**, które są niezbędne do obsługi incydentów i zagrożeń cyberbezpieczeństwa.
- Zgłoszenie incydentu **powinno zawierać dane osobowe**, a także **tajemnice prawnie chronione**, jeżeli jest to konieczne do realizacji zadań CSIRT.

RODO (art. 23), inne tajemnice prawnie chronione.

bez informacji niejawnych!

Pamiętaj, aby wysyłając zgłoszenie **oznaczyć informacje prawnie chronione**, w tym stanowiące tajemnicę przedsiębiorstwa. Aby to zrobić, użyj nawiasów kwadratowych, na przykład: `[Incydent w systemie bankowym miał wpływ na 10 tysięcy użytkowników końcowych.]`

Uwaga: Nieuzasadnione użycie oznaczeń może wydłużyć czas odpowiedniej reakcji.

Obowiązek informacyjny

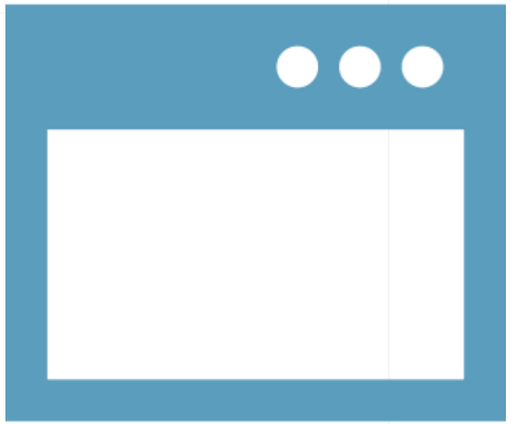
- Obsługa incydentu wiąże się również z **obowiązkiem przekazania informacji** osobom, na rzecz których realizuje się zadanie publiczne.
- **Osoby mają prawo dostępu do wiedzy pozwalającej na:**

zrozumienie zagrożeń cyberbezpieczeństwa.

stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Obowiązek informacyjny może zostać spełniony poprzez publikacje stosownego komunikatu na stronie internetowej.

Zgłoszenie incydentu **prywatnie**



przez formularz:
https://incydent.cert.pl

lub przez SMS
(SMShing)

Zgłoszenie przez SMS

Wiadomości z podejrzanymi linkami najwygodniej zgłaszać za pomocą SMSa.

Wystarczy przekazać treść otrzymanej wiadomości na numer **CERT Polska.**

Trafi ona do analityków CERT Polska, którzy zdecydują o dopisaniu podejrzanej domeny do listy ostrzeżeń.

8080

Lista ostrzeżeń

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie (aktualizowana co 5 minut):

https://cert.pl/lista-ostrzezen/

https://hole.cert.pl/domains/

Budowana na podstawnie m.in. zgłoszonych podejrzanych domen
– **obrona przed phishingiem**

Wdrażają operatorzy telekomunikacyjni
– **automatyzacja**

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Źródła obrazków/zdjęć

Jeżeli nie zaznaczono inaczej zrzuty ekranu pochodzą z materiałów CSIRT KNF i CERT Polska

https://pixabay.com

https://www.pexels.com

https://unsplash.com/

Dziękuję!

NASK – PIB,
Zespół Szkoleń i Ćwiczeń Cyberbezpieczeństwa,
zbsc@nask.pl

Ministerstwo Cyfryzacji

NASK