POWIAT MYŚLENICKI
ZIEMIA W DOBRYM KLIMACIE

Bezpieczeństwo informatyczne

Agenda

- Bezpieczeństwo informatyczne w zakresie RODO
- Bezpieczeństwo systemów informatycznych

1.
Bezpieczeństwo informatyczne w zakresie RODO

Polityka haseł

Polityka haseł

- **Hasła co najmniej 12 znaków**
- Hasła zawierają duże litery+małe litery+cyfry+znaki specjalne
- Hasła nie mogą być łatwe do odgadnięcia, bez dat, własnych imion, nazwisk itd.
- Hasła muszą być zmieniane co 30 dni
- Zabrania się używania tych samych haseł w wielu miejscach
- Nie należy zapisywać haseł na kartkach i w notesach, nie nie naklejać na monitorze, nie trzymać pod klawiaturą itd..
- Zabrania się używania haseł, których jeden człon pozostaje niezmienny (np. Anna001, Anna002 itd.)

Polityka haseł

Jak powinno wyglądać silne hasło?

Silne hasła możliwe do zapamiętania

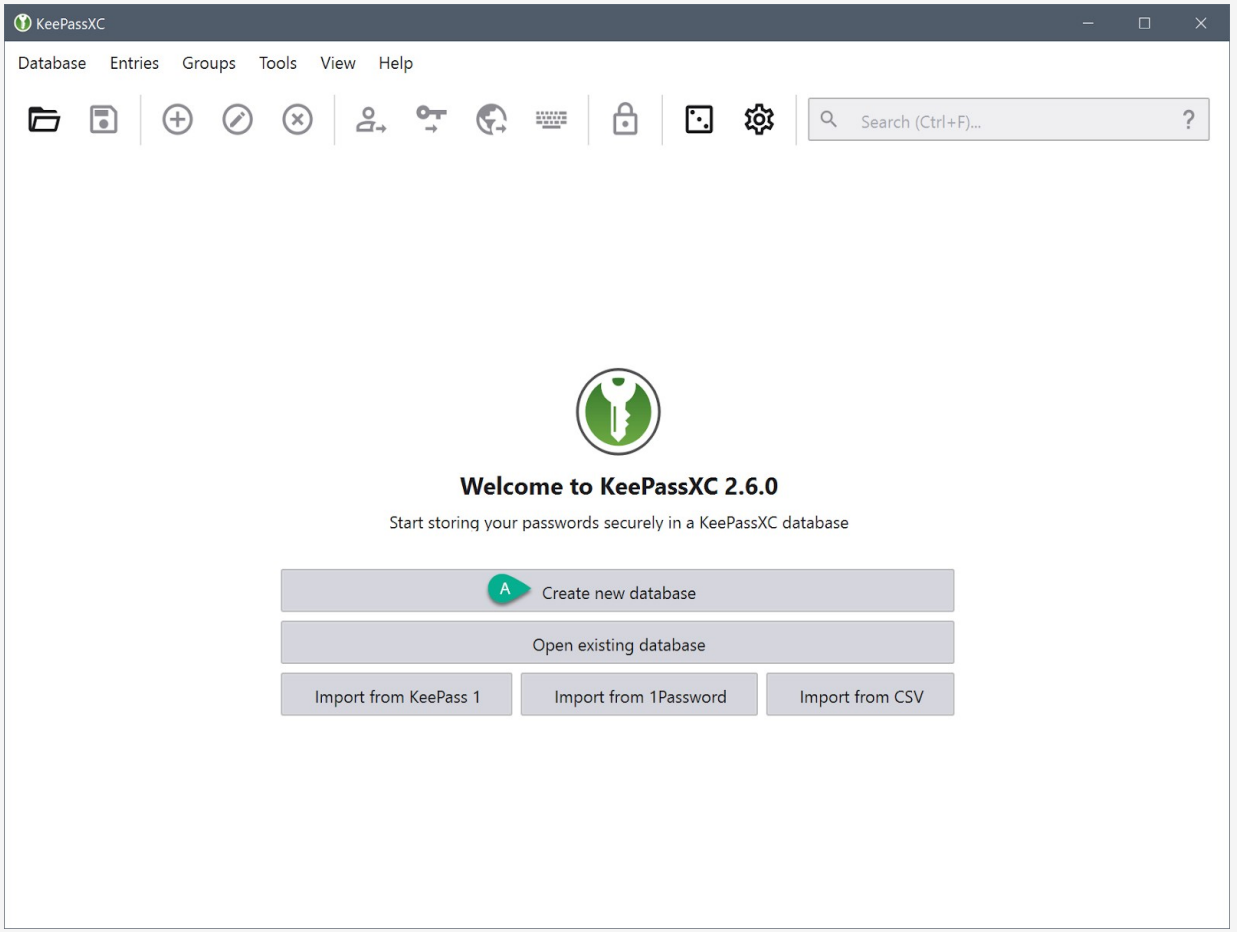
kL43wIAt@r56#

Zi3lony&Samochod#

W!ozacy3#cytrynY

potulnY@Pi3sGrajacyWpilke%

Łatwy sposób na tworzenie i przechowywanie silnych haseł



Menadżer haseł np. KeePassXC

Nośniki danych

Poniższe wymagania RODO w zakresie urządzeń mobilnych dotyczą komputerów

przenośnych (laptopów), pendrive’ów, telefonów lub innych zewnętrznych pamięci.

Nośniki danych

- Każdy mobilny IND (informatyczny nośnik danych) powinien być szyfrowany, kiedy opuszcza miejsce przetwarzania – miejsce firmy / urzędu.
- Dostęp do IND powinien być zapewniony tylko dla właściciela, poprzez wprowadzenie np. loginu i hasła, przykładowo funkcja BitLocker.
- Administrator systemu powinien prowadzić rejestr wydanych urządzeń mobilnych.
- Każdy komputer powinien blokować możliwość podłączenia nieautoryzowanego IND np. pendrive.
- Każdy IND powinien być obowiązkowo skanowany programem antywirusowym,

Nośniki danych

- Użytkownicy nie mogą wynosić na zewnątrz jednostki wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody bezpośredniego przełożonego
- W sytuacji przekazywania nośników z danymi osobowymi poza obszar jednostki można stosować następujące zasady:

✔ dane przed wysłaniem / przekazaniem powinny zostać zaszyfrowane a hasło podane adresatowi innym kanałem komunikacyjnym (np. wysyłka zaszyfrowanego pliku drogą mailową a hasło poprzez **bramkę sms**)

Nośniki danych

Wydziały wykorzystujące nośniki danych często różnią się specyfiką pracy.

Pełne wdrożenie zasad RODO związanych z urządzeniami mobilnymi wymaga indywidualnej analizy.

Zasady konta użytkowników

- Każdy użytkownik systemu informatycznego (systemu operacyjnego, programu, CRM, itp.) powinien mieć indywidualny login i hasło, znane tylko danemu użytkownikowi
- Użytkownicy powinni wykonywać swoją pracę bez uprawnień administracyjnych danego systemu
- Nie zezwala się na instalację plugin-ów w przeglądarkach internetowych

Ochrona fizyczna

- Każde urządzenie, które przetwarza dane osobowe powinno być zabezpieczone przed nieautoryzowanym dostępem np. pomieszczenie zamykane na klucz.
- Powinna być wdrożona procedura, uniemożliwiająca wyniesienie komputerów i urządzeń sieciowych ze strefy bezpieczeństwa.
- Dostęp do pomieszczeń w których przetwarzane są dane osobowe, powinien być rejestrowany, np. system kontroli dostępu lub książka wydawania kluczy.

Pozostałe zalecenia

- Należy zgłaszać Informatykowi przypadki podejrzanych maili oraz nietypową pracę programu antywirusowego
- Nie otwierać załączników od nieznanych / podejrzanych adresów mailowych (*.zip, *.xlsm, *.exe, *.bat itp.)
- Nie klikać na linki (hiperłącza) w mailach
- Zachować ostrożność podczas uruchamiania makr w plikach excel oraz word (skonsultować próbę uruchomienia makr z ZI)
- Wysyłanie / odpowiadanie na pisma tylko na adresy mailowe służbowe, jeśli to możliwe należy wykorzystać do tego platformą e-puap

Pozostałe zalecenia

- Odchodząc od komputera, należy blokować ekran np. skrótem klawiszowym **WIN + L**

2. Bezpieczeństwo systemów informatycznych

Socjotechnika

Technika manipulacji człowiekiem. Poprzez działania oparte na słabościach ludzkiej osobowości (ciekawość, lenistwo, złość, współczucie, itp.),próbuje się nakłonić osobę poddaną socjotechnice do określonego działania.

Przykłady socjotechnik

- **korzystanie z przynęty**, aby nakłonić do pobrania/zainstalowania malware
- **wyłudzanie danych**, poprzez fałszywe strony lub złośliwe oprogramowanie
- **podszywanie się**, w celu wyłudzenia danych
- **scareware**, przekonywanie użytkownika, że jego urządzenie jest zainfekowane, aby namówić go do pobrania/zainstalowania malware (wirus komp.)

Łamanie ludzi, a nie hasła

Łatwiej jest **namówić człowieka** do określonego działania, niż złamać systemowe zabezpieczenia danych.

Cyberzagrożenia w Polsce

Najpopularniejszym typem incydentów w 2021 r. był **phishing** – stanowiący aż **76,57%** wszystkich obsłużonych incydentów.

Liczba incydentów zaklasyfikowanych jako phishing w porównaniu do roku poprzedniego **wzrosła o 196%**.

CERT Polska, Statystyki obsługi incydentów w 2021 (28.04.2022 r.)

Definicja

Phishing to jedna z metod oszustw w Internecie. Za jej pośrednictwem oszuści, podszywając się najczęściej pod jakąś firmę, instytucję lub osobę, wyłudzają dane osobiste jak np. numery kont bankowych i kart kredytowych czy dane do logowania w różnych serwisach internetowych.

Phishing

wykradanie danych

próba zainfekowania komputera

Phishing cz.1.

Proste przykłady wykonane niestarannie, **łatwe do wykrycia**.

Phishing nr1 – klasyczny przykład, który ciagle występuje w różnych odmianach

Cześć!

Niestety, mam dla Ciebie złe wiadomości.
Parę miesięcy temu zdobyłem dostęp do urządzenia, którego używasz do przeglądania internet.
Od tego czasu monitorowałem Twoją aktywność internetową.

Jako regularny odwiedzający stron dla dorosłych, mogę potwierdzić, że ty jesteś za to odpowiedzialny.
Mówiąc wprost, strony, które odwiedzasz, dały mi dostęp do Twoich danych.

Załadowałem Trojana w bazę Twoich driverów, który uaktualnia swoją sygnaturę parę razy dziennie, co sprawia, że antywirus nie jest w stanie go wykryć.
Na dodatek daje mi on dostęp do Twojej kamery i mikrofonu.
Co więcej, zapisałem wszystkie dane, w tym zdjęcia, media społecznościowe, czaty i kontakty.

Ostatnio wpadłem na zajebisty pomysł stworzenia filmu, gdzie dochodzisz w jednej części ekranu, gdy w drugiej jednocześnie odtwarza się film, który oglądałeś.
To było śmieszne!

Bądź spokojny, że z łatwością mogę wysłać ten film do wszystkich Twoich kontaktów paroma klikami, zakładam, że wolałbyś uniknąć takiego scenariusza.

Mając to na uwadze, taka jest moja propozycja:
Prześlij równowartość 1230 EUR na mój portfel Bitcoin, a zapomnę o całej sprawie. Usunę również wszystkie dane i filmy na zawsze.

Według mnie to dość umiarkowana cena za moją pracę.
Możesz zorientować się, jak kupić Bitcoiny za pomocą wyszukiwarek Google, czy Bing, sam zobaczysz, że nie jest to aż tak trudne.

Mój portfel Bitcoin (BTC): 15f7b4FfPS8fWwkDmh4QMdvsfhja1yN8As

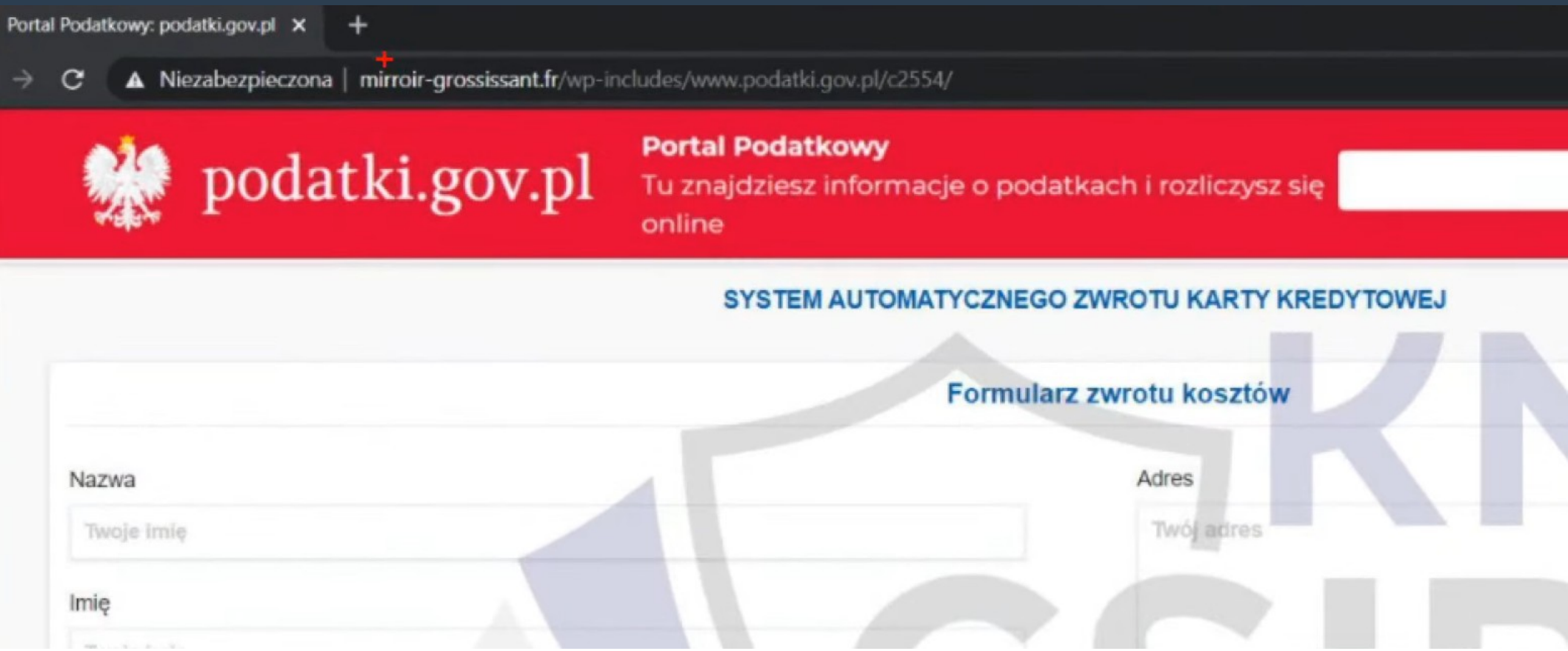
Masz 48 godzin na odpowiedź, powinieneś pamiętać o tym, że:
Nie ma sensu mi odpowiadać — adres został wygenerowany automatycznie.
Nie ma sensu narzekać, ponieważ wiadomość wraz z portfelem Bitcoin nie mogą być namierzone.
Wszystko zostało precyzyjnie zaplanowane.

Jeśli wykryję, że powiedziałeś komuś o tym liście – film natychmiast zostanie udostępniony, a Twoje kontakty otrzymają go jako pierwsze.
Następnie film zostanie opublikowany w sieci!

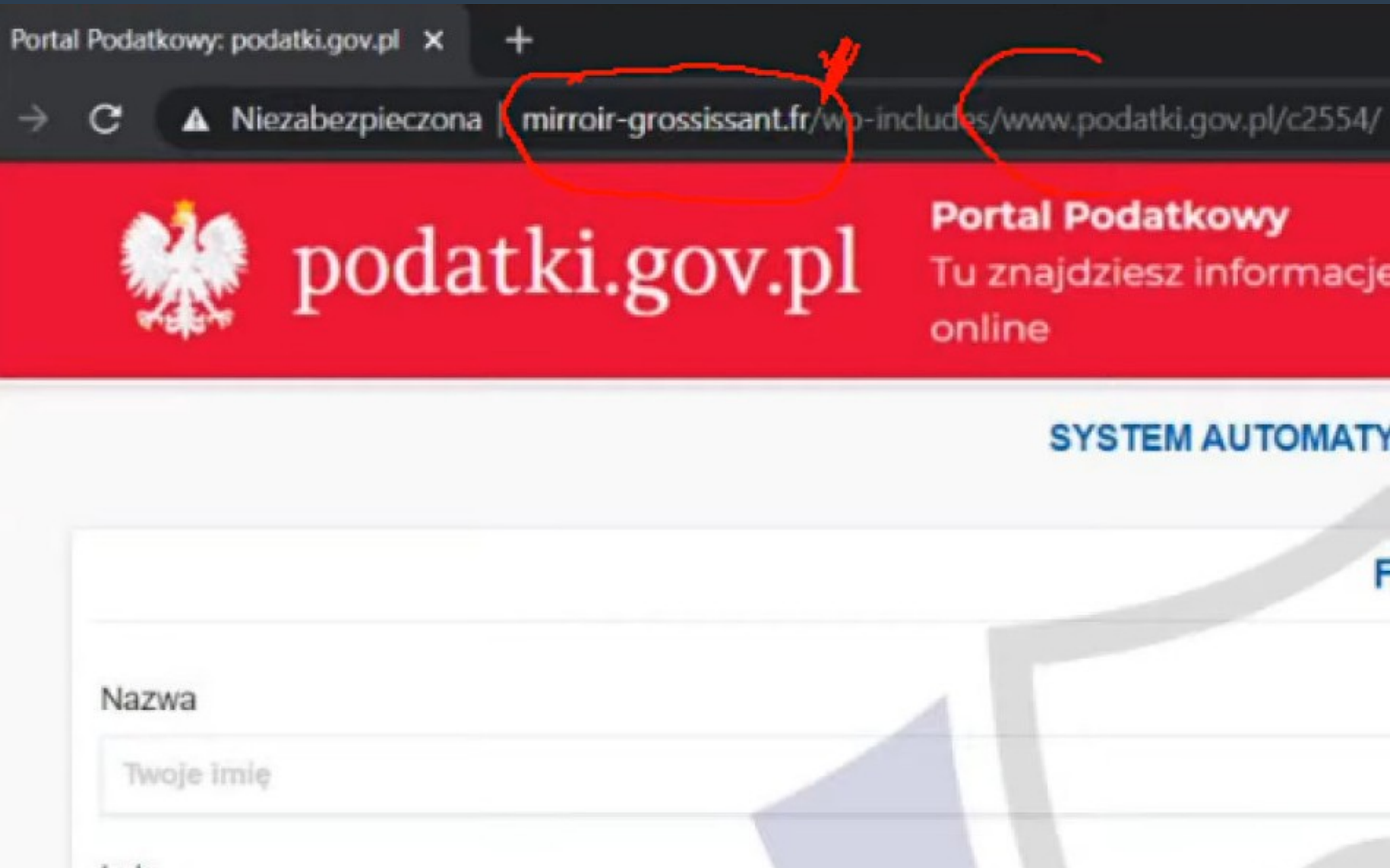
P.S. Czas odliczania się rozpocznie, gdy otworzysz ten list. (Program ma wbudowany zegar).

Powodzenia i uważaj na siebie! Miałeś pecha, następnym razem bądź ostrożniejszy.

Przykład nr2



Przykład nr2

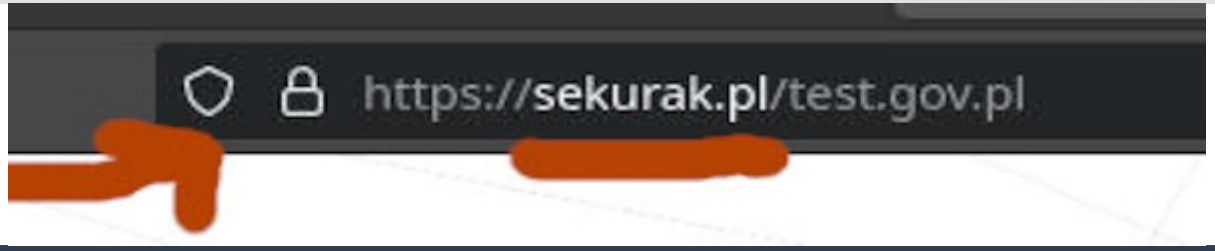


Phishing – jak wykryć?

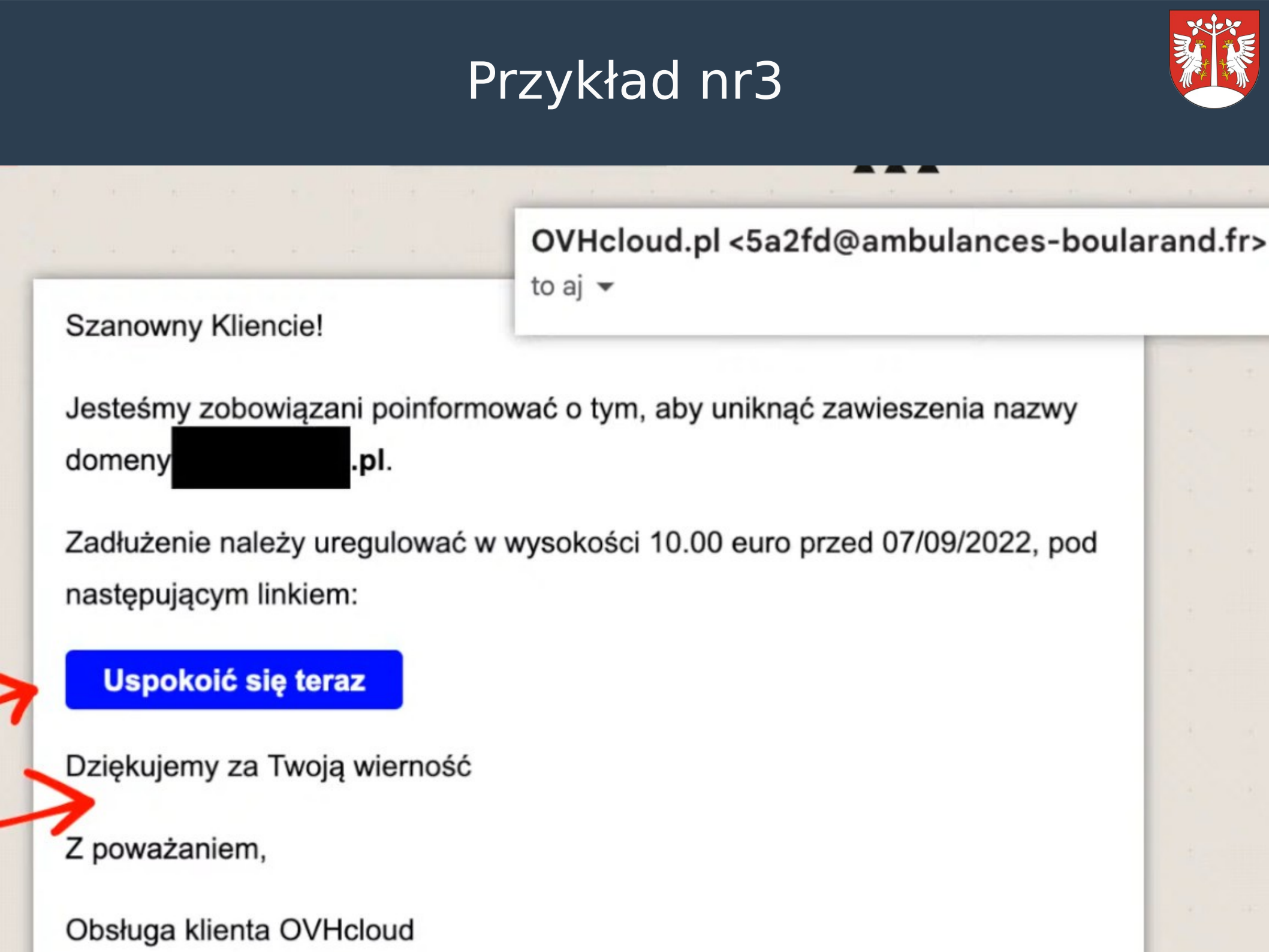
https://sekurak.pl/test.gov.pl

Szyfrowanie połączenie

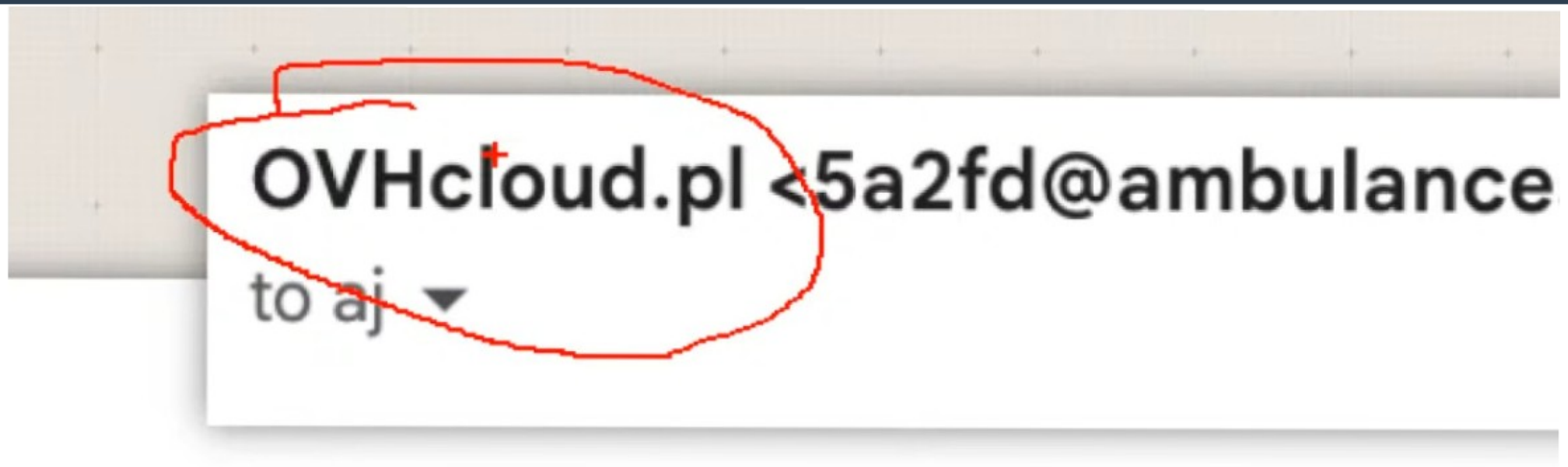
Prawdziwy adres serwera



Przykład nr3



Przykład nr3



ormować o tym, aby uniknąć zawieszenia na

ać w wysokości 10.00 euro przed 07/09/2022

Przykład nr4

Witam,
Dobry dzień panu,

Mam nadzieję, że dzisiaj wszystko w porządku.
Mój kolega Pan Dawid Krawiec wysłał Państwu nasze zamówienie PO-Eu598303 w zeszłym tygodniu, ale jeszcze nie otrzymali
Tutaj znów cię wysyłam. Prosimy o dostarczenie faktury proforma zgodnie z załączonym zamówieniem PO-Eu598303.

Mamy nadzieję, że niedługo się odezwiesz.

Zamowienie_zakupu_PO-Eu598303.pdf

--

pozdrowienia
pani malgorzata berez
HBDTOYS SP.ZO.O
telefon: 48-71-7254955
faks: 48-71-7220091
e-mail : biuro@hbdtoys.com
adres: skierniewicka, nr 10a, lok. 6p

Przykład nr4

Zamowienie_zakupu_PO-Eu598303.7z

Witam,
Dobry dzień panu,

Mam nadzieję, że dzisiaj wszystko w porządku.
Mój kolega Pan Dawid Krawiec wysłał Państwu nasze zamówienie PO-Eu598303 w zeszłym tygodniu, ale jeszcze nie otrzymaliśmy od Państwa odpowiedzi.
Tutaj znów cię wysyłam. Prosimy o dostarczenie faktury proforma zgodnie z załączonym zamówieniem PO-Eu598303.

Mamy nadzieję, że niedługo się odezwiesz.

PDF

Zamowienie_zakupu_PO-Eu598303.pdf

--

pozdrowienia
pani malgorzata berez
HBDTOYS SP.ZO.O
telefon: 48-71-7254955
faks: 48-71-7220091
e-mail : biuro@hbdtoys.com
adres: skierniewicka, nr 10a, lok. 6p

HBDTOYS SP.ZO.O
WIATOWY

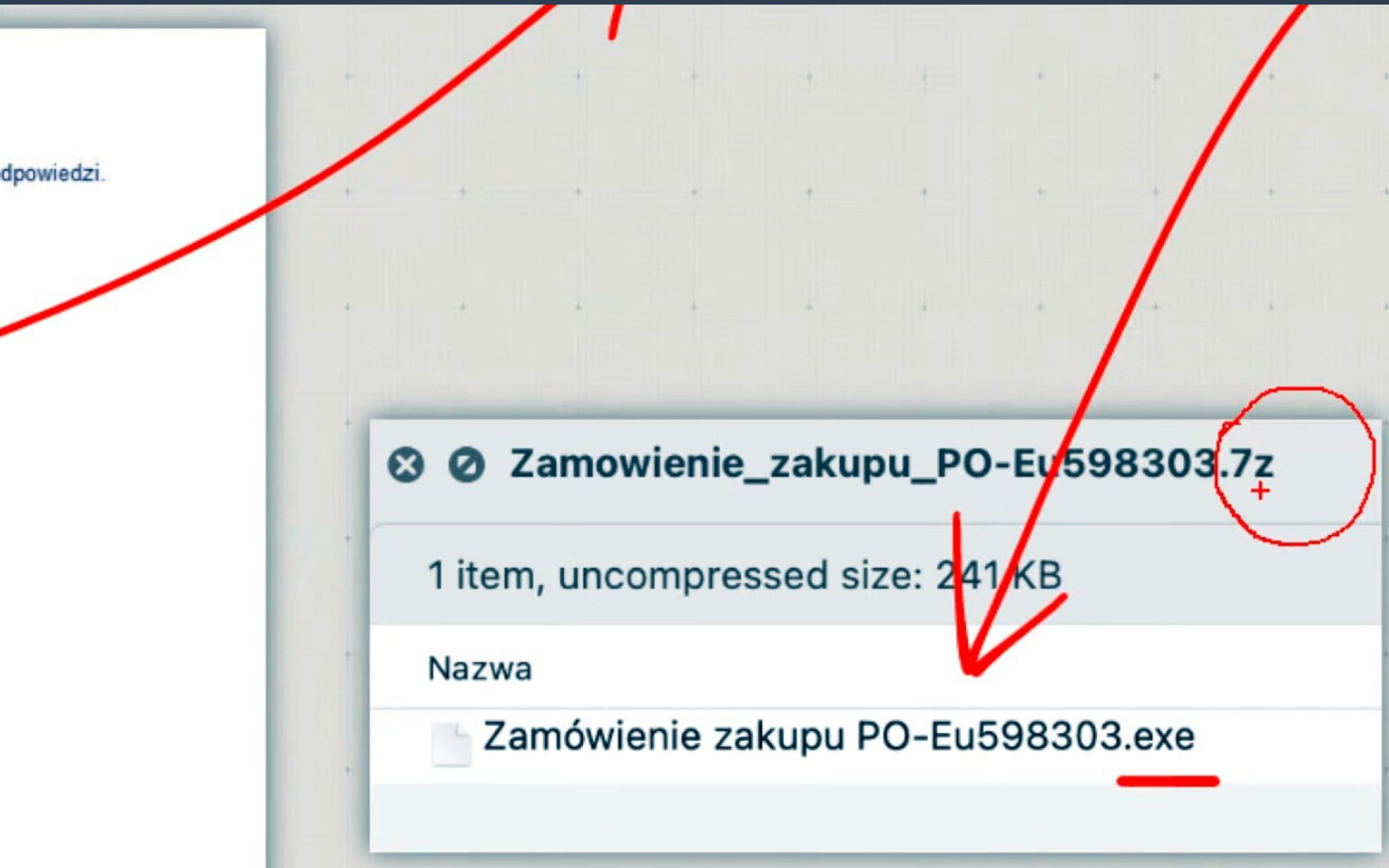
Zamowienie_zakupu_PO-Eu598303.7z

1 item, uncompressed size: 241 KB

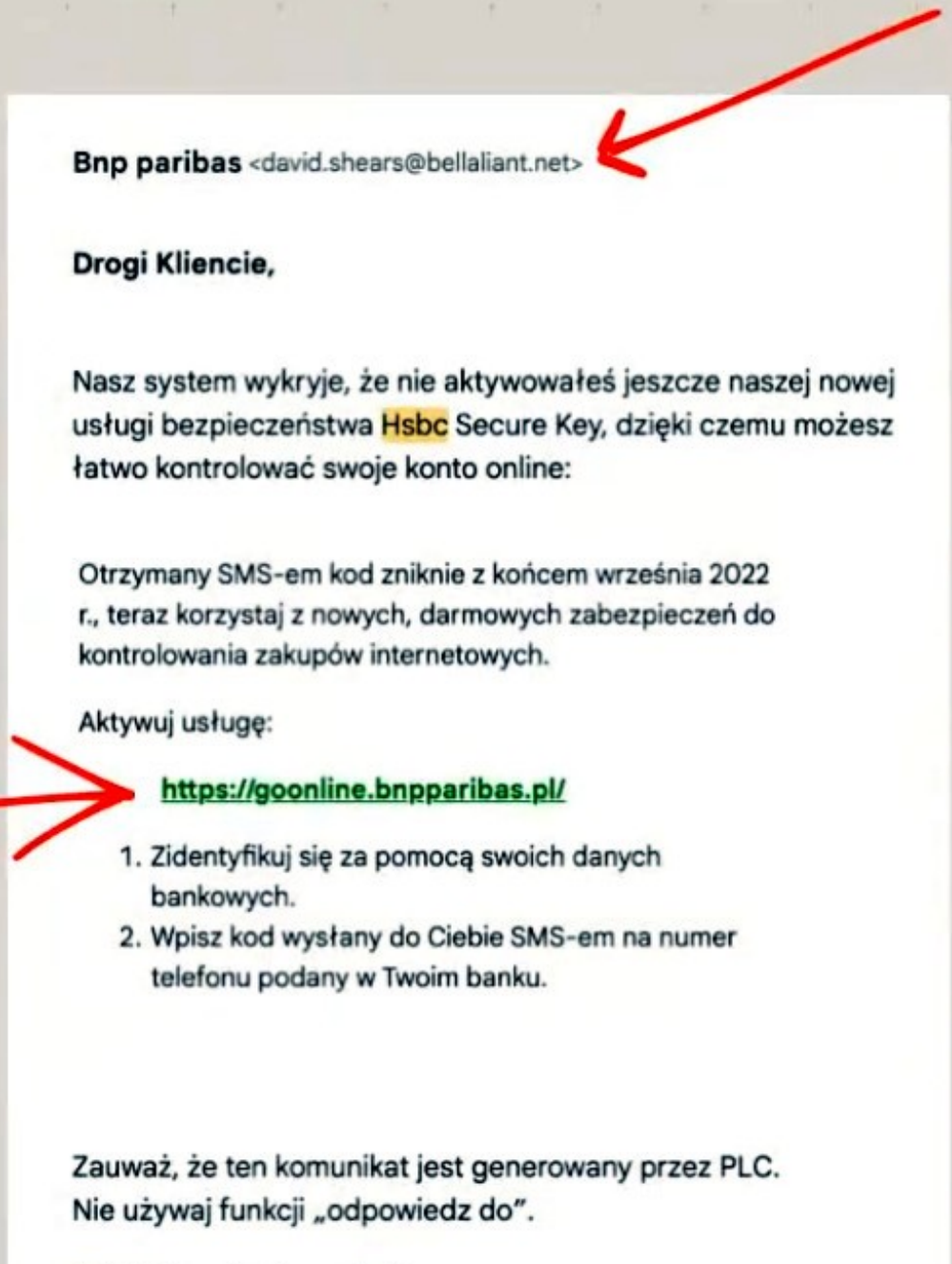
Nazwa

Zamówienie zakupu PO-Eu598303.exe

Przykład nr4



Przykład nr5



Bnp paribas <david.shears@bellaliant.net>

Drogi Kliencie,

Nasz system wykryje, że nie aktywowałeś jeszcze naszej nowej usługi bezpieczeństwa Hsbc Secure Key, dzięki czemu możesz łatwo kontrolować swoje konto online:

Otrzymany SMS-em kod zniknie z końcem września 2022 r., teraz korzystaj z nowych, darmowych zabezpieczeń do kontrolowania zakupów internetowych.

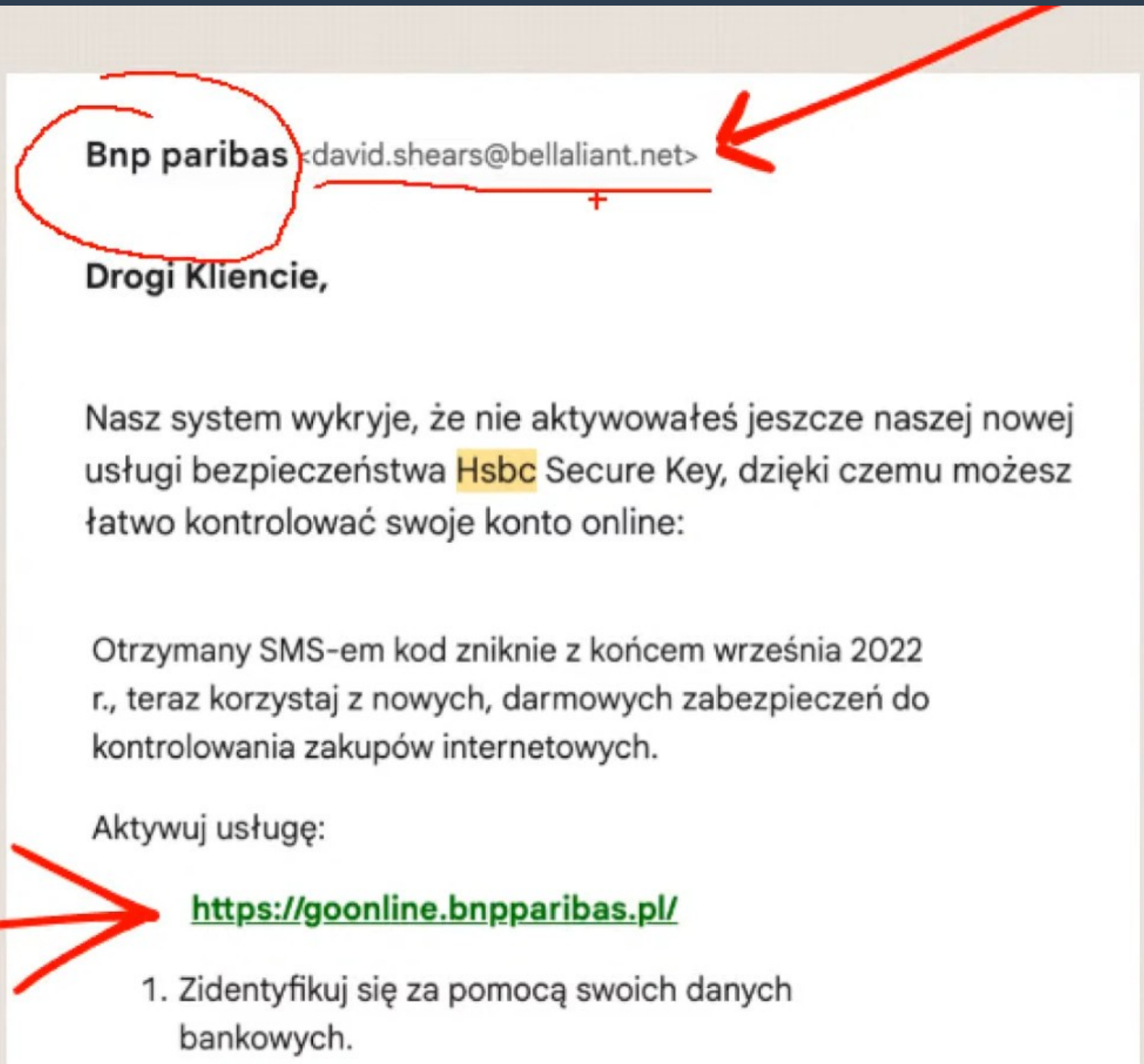
Aktywuj usługę:

https://goonline.bnpparibas.pl/

1. Zidentyfikuj się za pomocą swoich danych bankowych.
2. Wpisz kod wysłany do Ciebie SMS-em na numer telefonu podany w Twoim banku.

Zauważ, że ten komunikat jest generowany przez PLC.
Nie używaj funkcji „odpowiedz do".

Przykład nr5



Bnp paribas <david.shears@bellaliant.net>

Drogi Kliencie,

Nasz system wykryje, że nie aktywowałeś jeszcze naszej nowej usługi bezpieczeństwa Hsbc Secure Key, dzięki czemu możesz łatwo kontrolować swoje konto online:

Otrzymany SMS-em kod zniknie z końcem września 2022 r., teraz korzystaj z nowych, darmowych zabezpieczeń do kontrolowania zakupów internetowych.

Aktywuj usługę:

https://goonline.bnpparibas.pl/

1. Zidentyfikuj się za pomocą swoich danych bankowych.

Przykład nr5

Bnp paribas <david.shears@bellaliant.net>

Drogi Kliencie,

Nasz system wykryje, że nie aktywowałeś jeszcze naszej nowej usługi bezpieczeństwa Hsbc Secure Key, dzięki czemu możesz łatwo kontrolować swoje konto online:

Otrzymany SMS-em kod zniknie z końcem września 2022 r., teraz korzystaj z nowych, darmowych zabezpieczeń do kontrolowania zakupów internetowych.

Aktywuj usługę:

https://goonline.bnpparibas.pl/

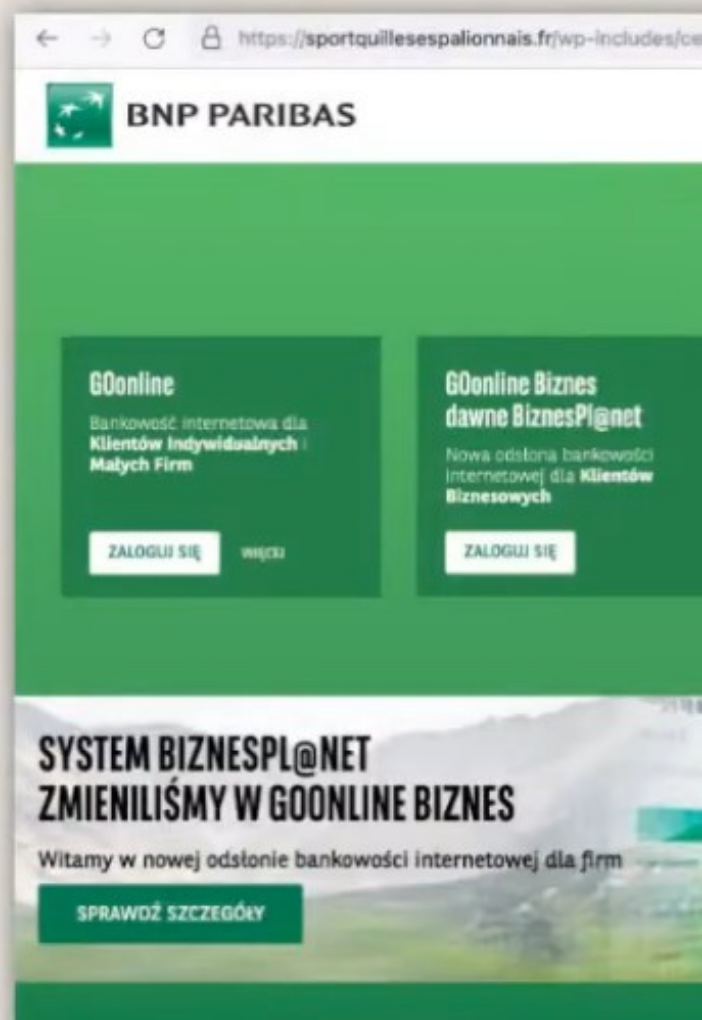
1. Zidentyfikuj się za pomocą swoich danych bankowych.
2. Wpisz kod wysłany do Ciebie SMS-em na numer telefonu podany w Twoim banku.

Zauważ, że ten komunikat jest generowany przez PLC. Nie używaj funkcji „odpowiedz do".

Dziękuję za twoje zaufanie.

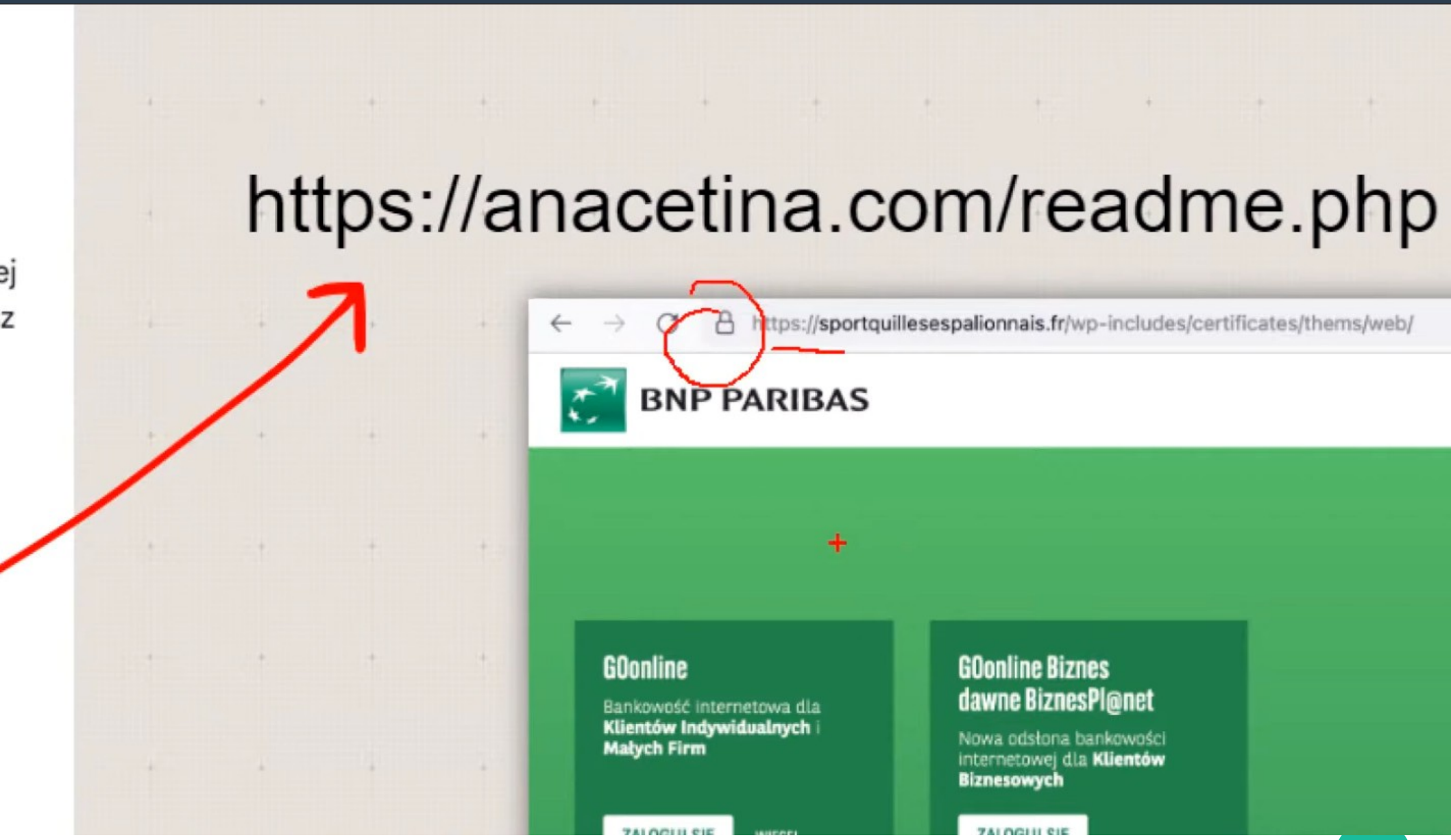
Grupa BNP Paribas.

https://anacetina.com/readm



Przykład nr5

https://anacetina.com/readme.php



Przykład nr6

Bank Pekao

Szanowny Kliencie

Aby chronić klientów Bank Pekao klientów bankowości cyfrowej musimy zweryfikować ich tożsa
na pewne problemy z bezpieczeństwem, które ostatnio napotkaliśmy. Aby go zobaczyć, kliknij

https://www.pekao.log/klientindywidualny/banko-wosc-elektroniczna

Wszystkie nasze zespoły doceniają Twoje zaufanie.

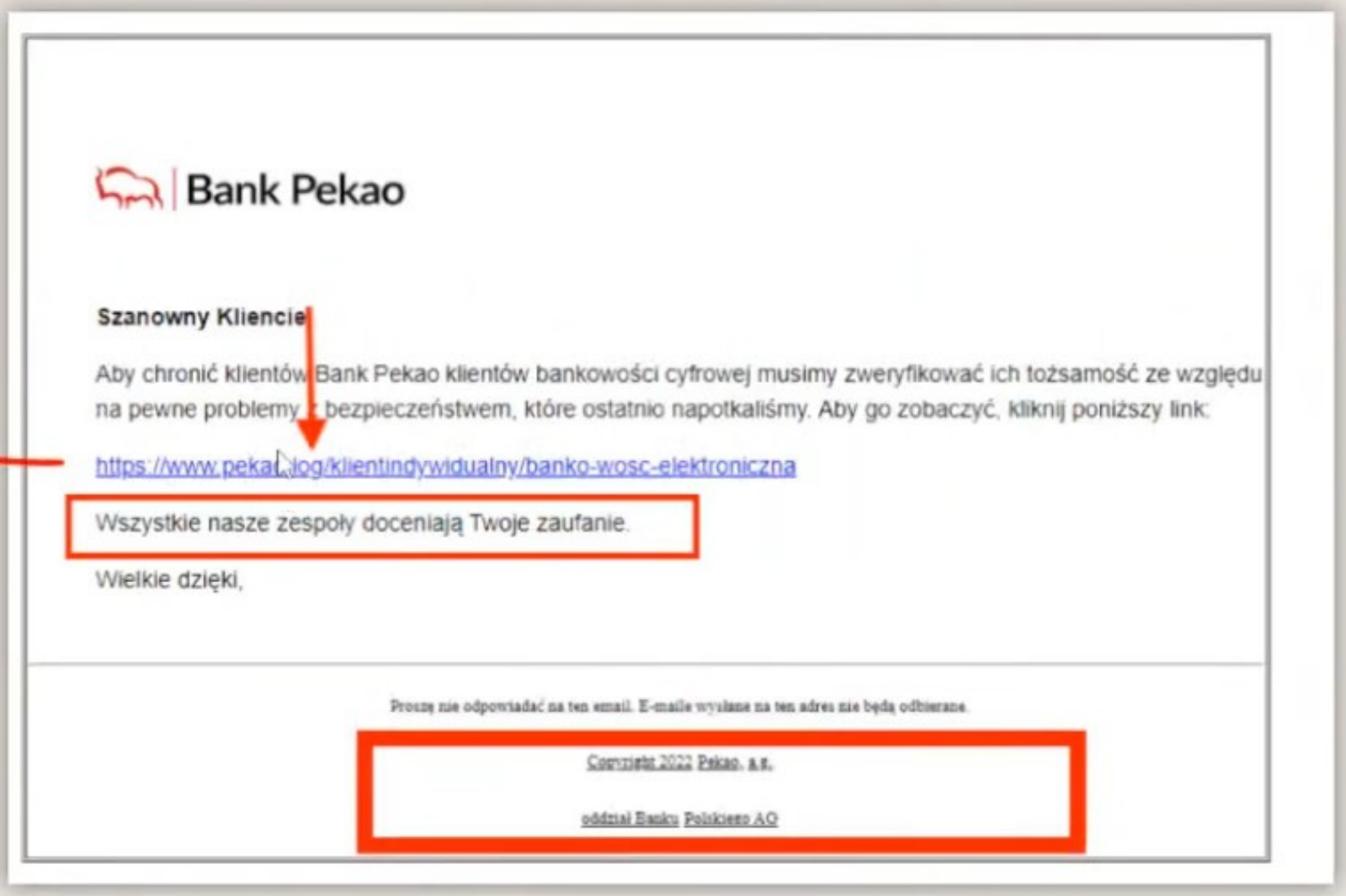
Wielkie dzięki,

Proszę nie odpowiadać na ten email. E-maile wysłane na ten adres nie będą odbierane.

Copyright 2022 Pekao, a.g.

oddział Banku Polskiego AG

Przykład nr6



Bank Pekao

Szanowny Kliencie

Aby chronić klientów Bank Pekao klientów bankowości cyfrowej musimy zweryfikować ich tożsamość ze względu na pewne problemy z bezpieczeństwem, które ostatnio napotkaliśmy. Aby go zobaczyć, kliknij poniższy link:

https://www.pekao.log/klientindywidualny/banko-wosc-elektroniczna

Wszystkie nasze zespoły doceniają Twoje zaufanie.

Wielkie dzięki,

Proszę nie odpowiadać na ten email. E-maile wysłane na ten adres nie będą odbierane.

Copyright 2022 Pekao, a.g.

oddział Banku Polskiego AO

http://google.mellrichstadt-stadtkapelle.de/pl

Przykład nr7

Od: "Administrator biznes.gov.pl" <amaia@dionisioormazabal.com>
Do: undisclosed-recipients:;
Data: 2022-09-11 23:17
Temat: Biznes.gov.pl - NOWE POWIADOMIENIE

Biznes.gov.pl

Serwis informacyjno-usługowy dla przedsiębiorcy

Drogi Użytkowniku!

Załącznik to oficjalne powiadomienie elektroniczne od Biznes.gov.pl

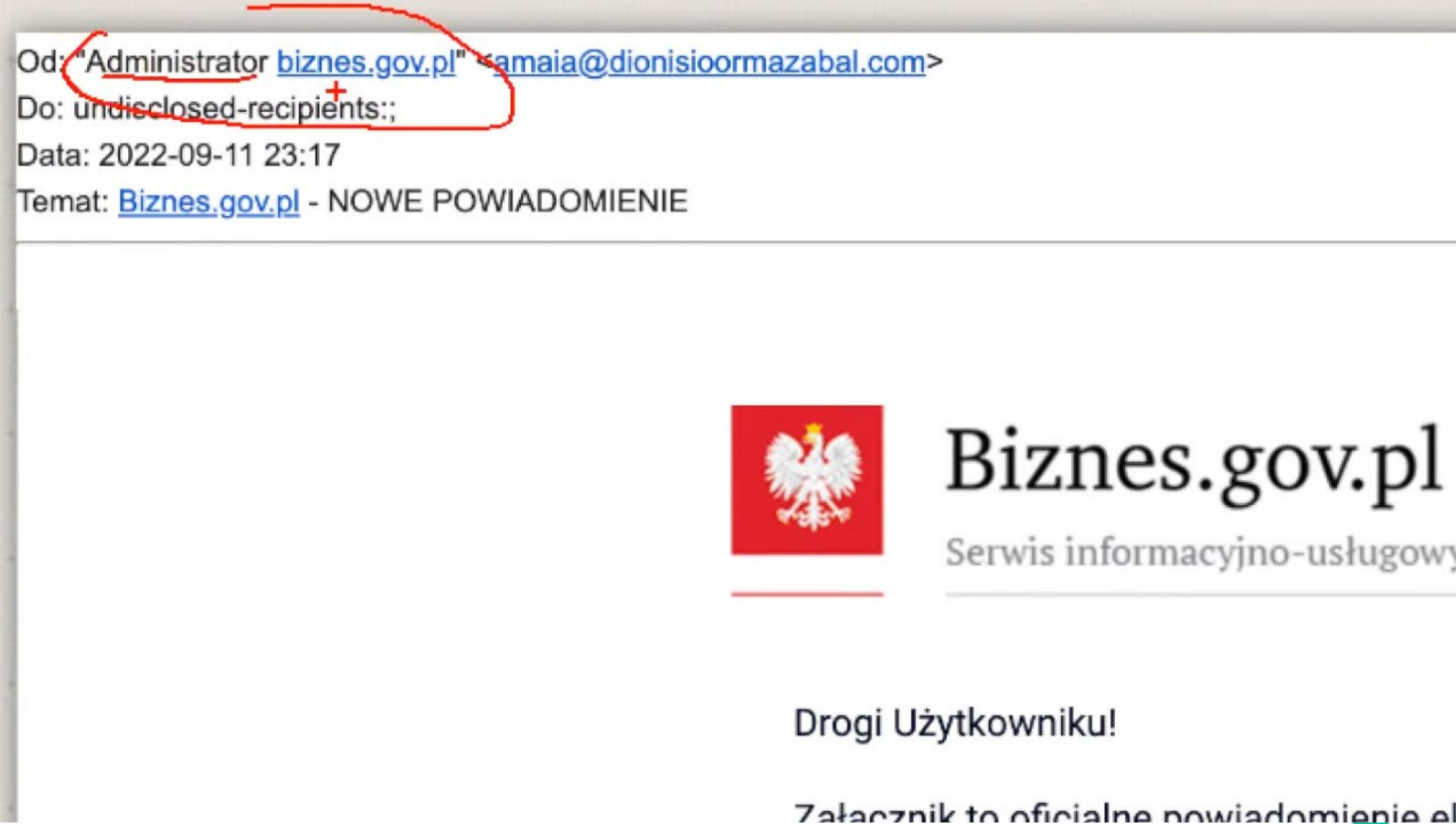
Powiadomienie będzie dostępne na Twoim Autoryzowanym Koncie od 09-08-2022 do 09-17-2022. Jeżeli nie przystąpisz do jej lektury we wskazanym terminie, wywołane zostaną odpowiednie skutki, zgodnie z obowiązującymi przepisami.[Art. 46 Kodeksu postępowania administracyjnego.]

Wiadomość została wygenerowana automatycznie przez serwis biznes.gov.pl (prosimy na tę wiadomość nie odpowiadać).

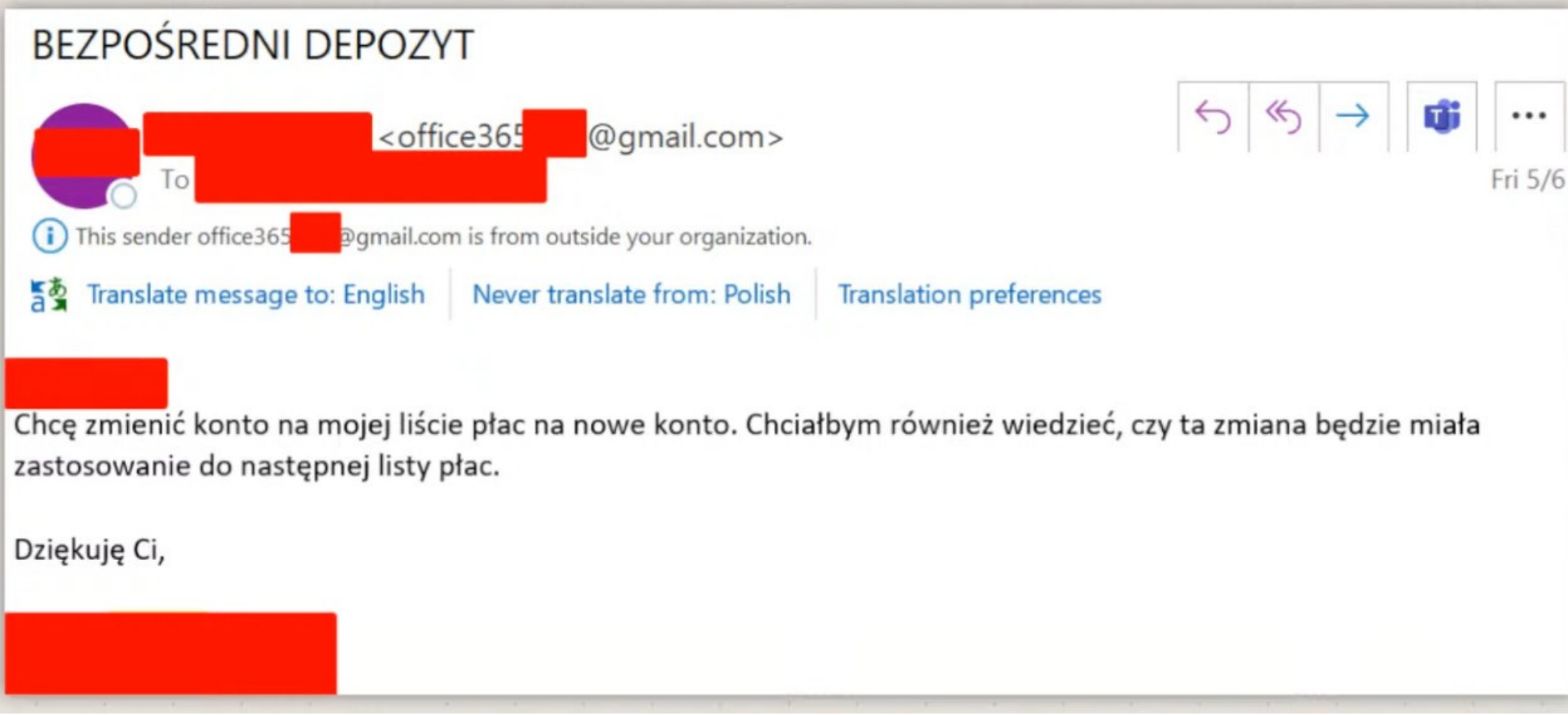
Pozdrawiamy,
Zespół Biznes.gov.pl

gov.pl / Biznes.gov.pl

Przykład nr7



Przykład nr8



Wskazówki

Sprawdź adres nadawcy e-maila,
a nie jego nazwę

Wskazówki

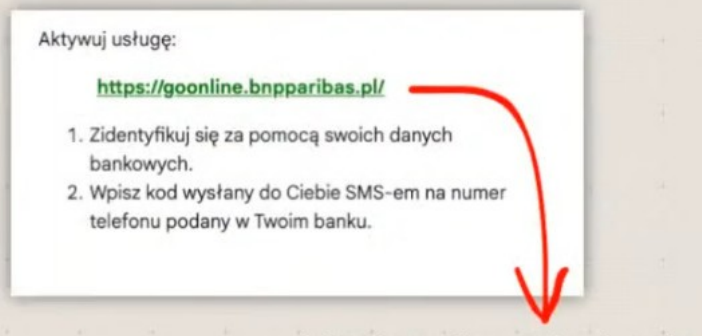
Sprawdź adres nadawcy e-maila, a nie jego nazwę

Nie klikaj w linki w e-mailach "bankowych"

Wskazówki

- Sprawdź adres nadawcy e-maila, a nie jego nazwę

- Nie klikaj w linki w e-mailach "bankowych"
- Pamiętaj, że link może prowadzić do innego miejsca niż sugeruje jego nazwa



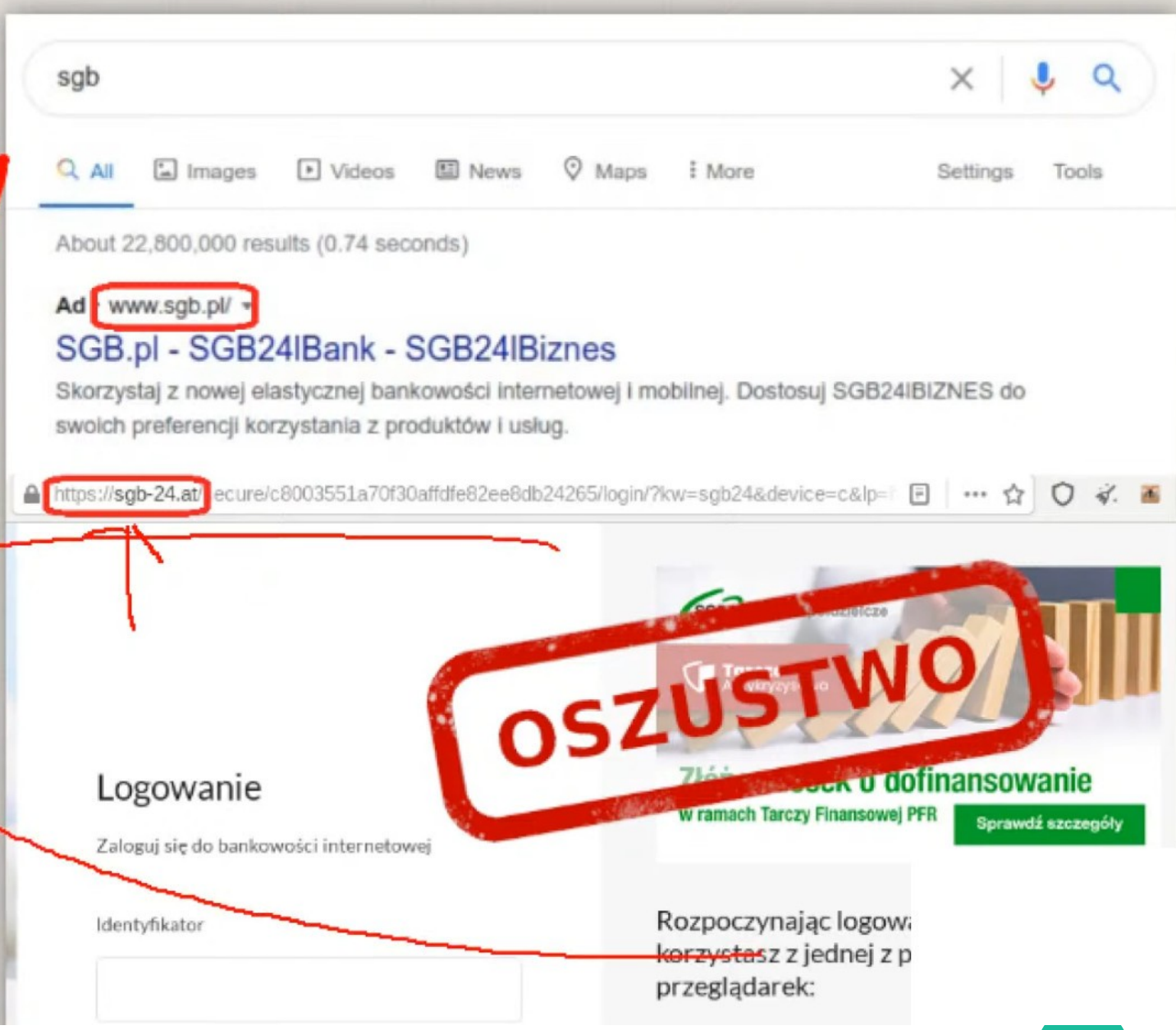
Wskazówki

Na strony bankowe wchodź
"ręcznie" lub z zakładek

stworzenie nowej zakładki:
ctrl+d w przeglądarce

Wskazówki

chodź
dek



Wskazówki

Uważaj na załączniki przesyłane w e-mailu

wyciag-bankowy-pdf.vbs

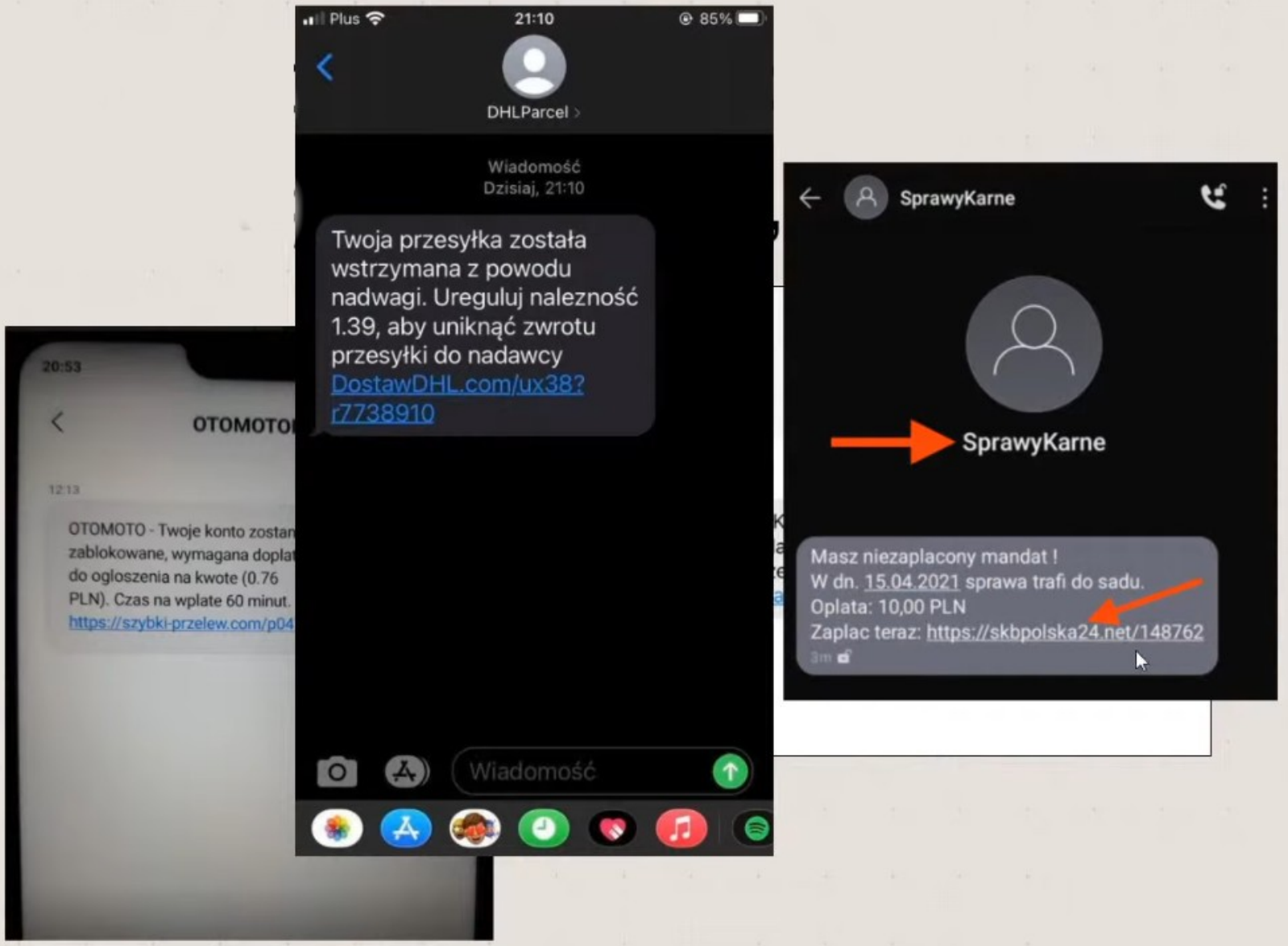
wyciag-bankowy.pdf.exe

To najpewniej jest malware/wirus

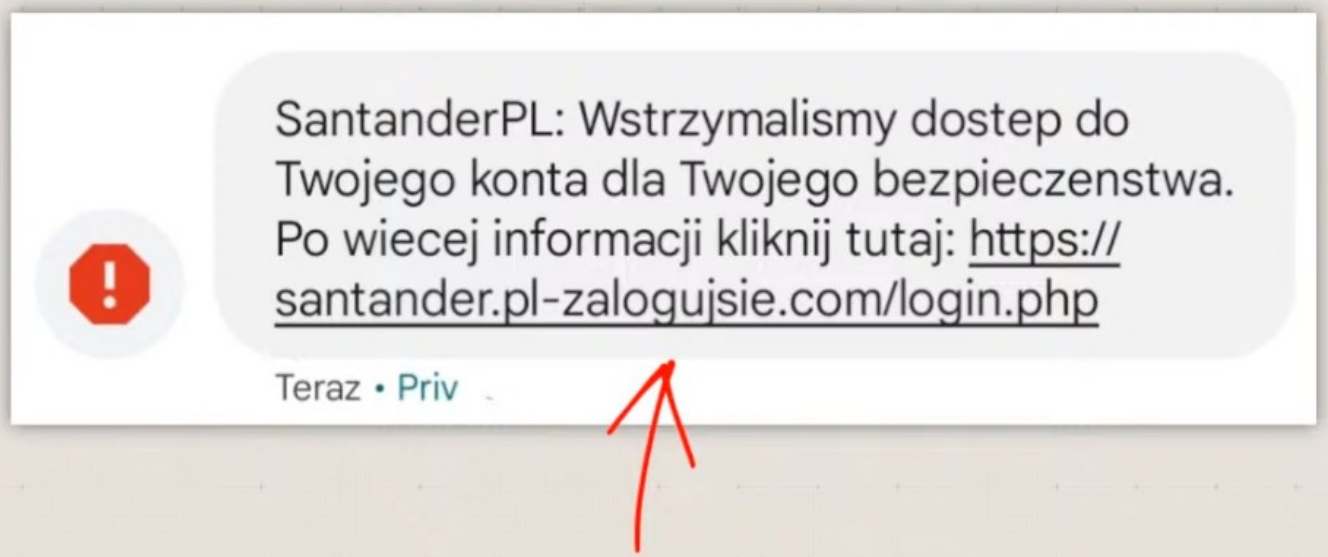
Phishing cz.2. - oszustwa SMS-owe

Przykłady oszustw trochę trudniejsze w identyfikacji.

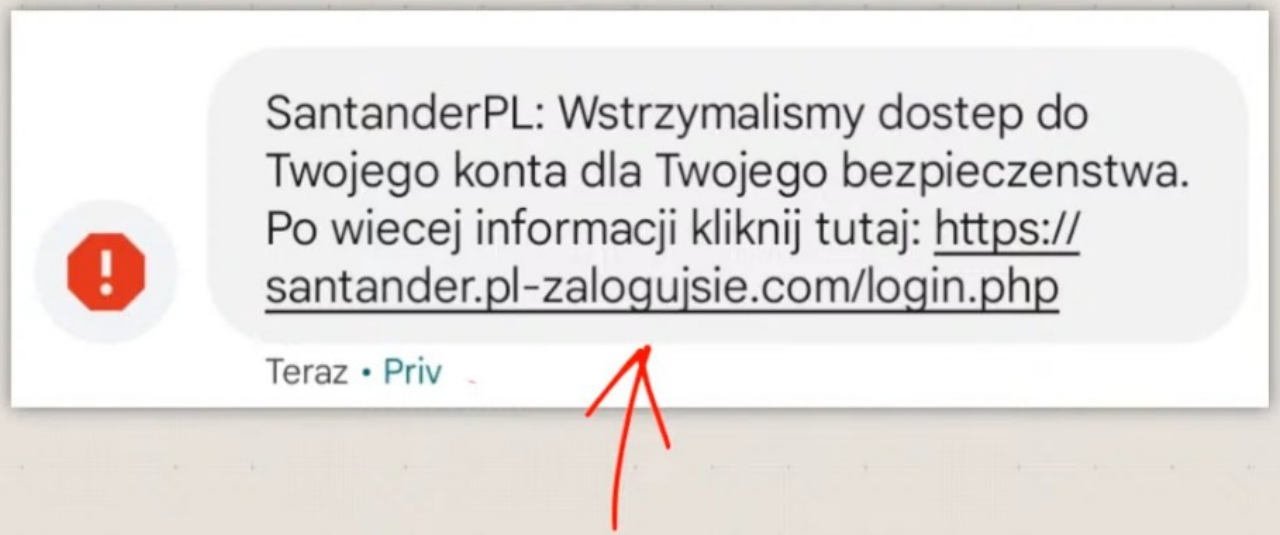
Phishing cz.2. - oszustwa SMS-owe

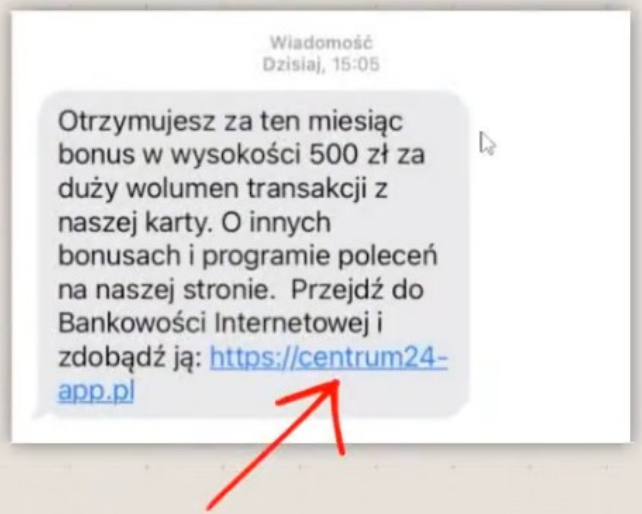


Phishing cz.2. - oszustwa SMS-owe

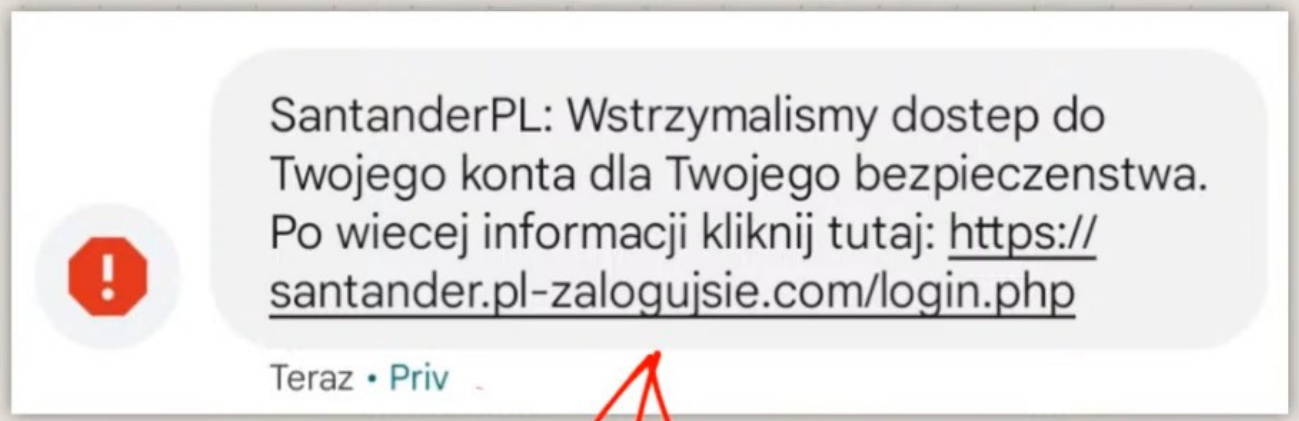


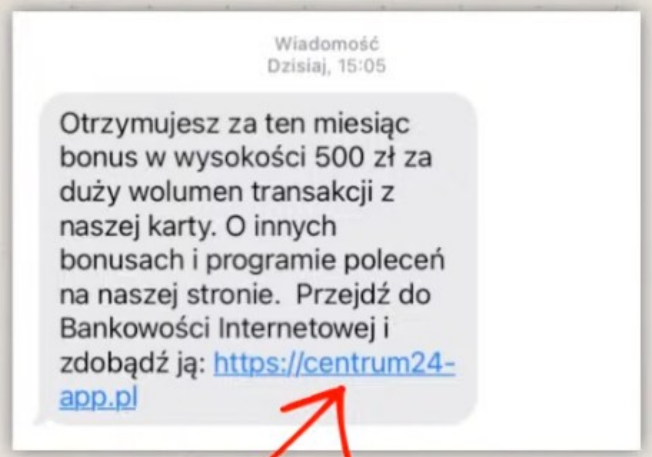
Phishing cz.2. - oszustwa SMS-owe

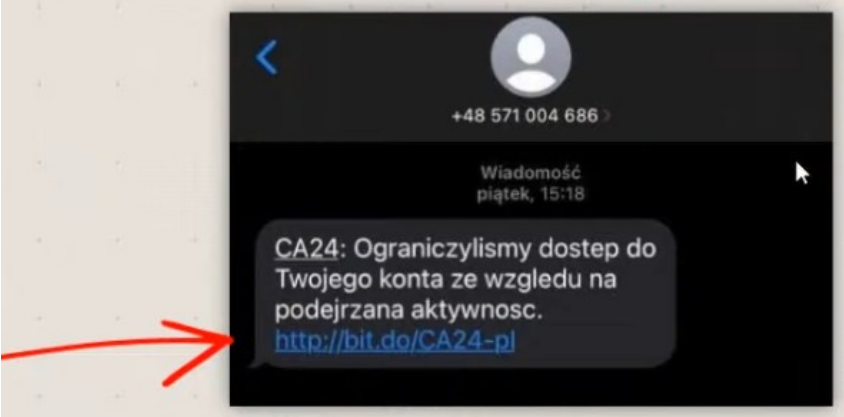




Phishing cz.2. - oszustwa SMS-owe

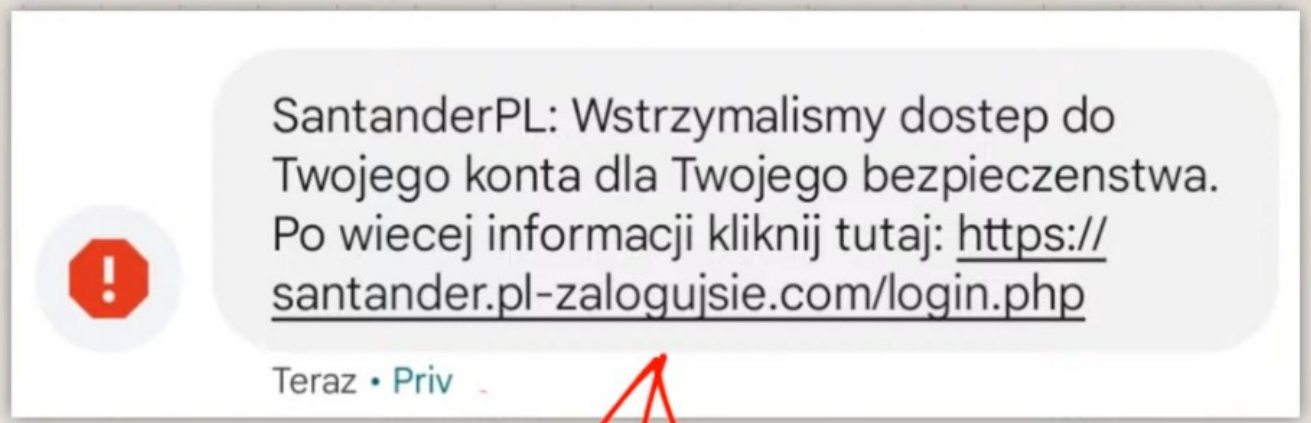


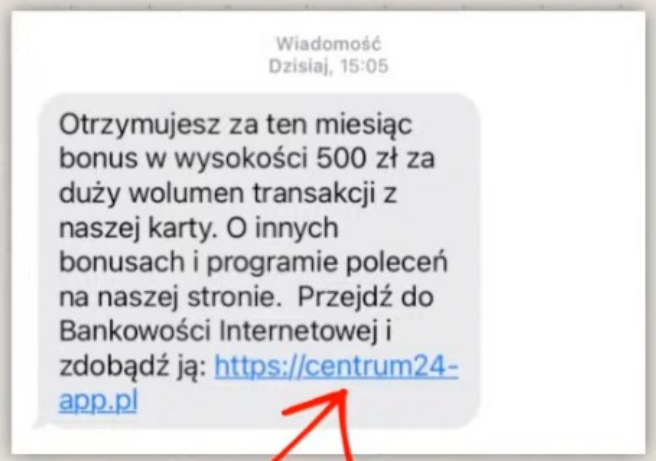


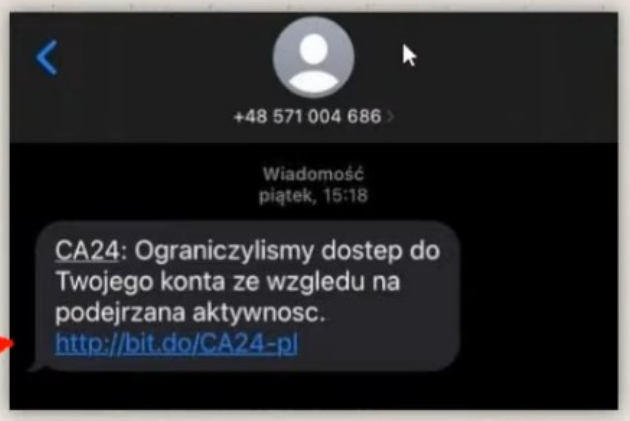


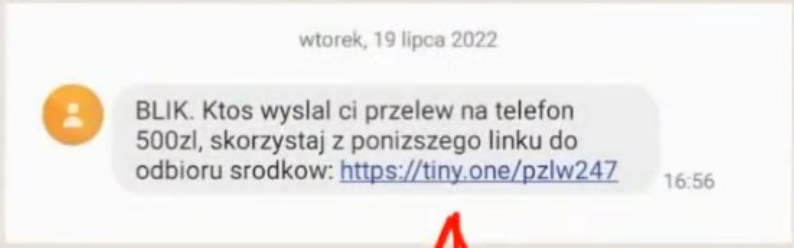
Phishing cz.2. - oszustwa SMS-owe

Oszutwa SMSowe cały czas są bardzo popularne

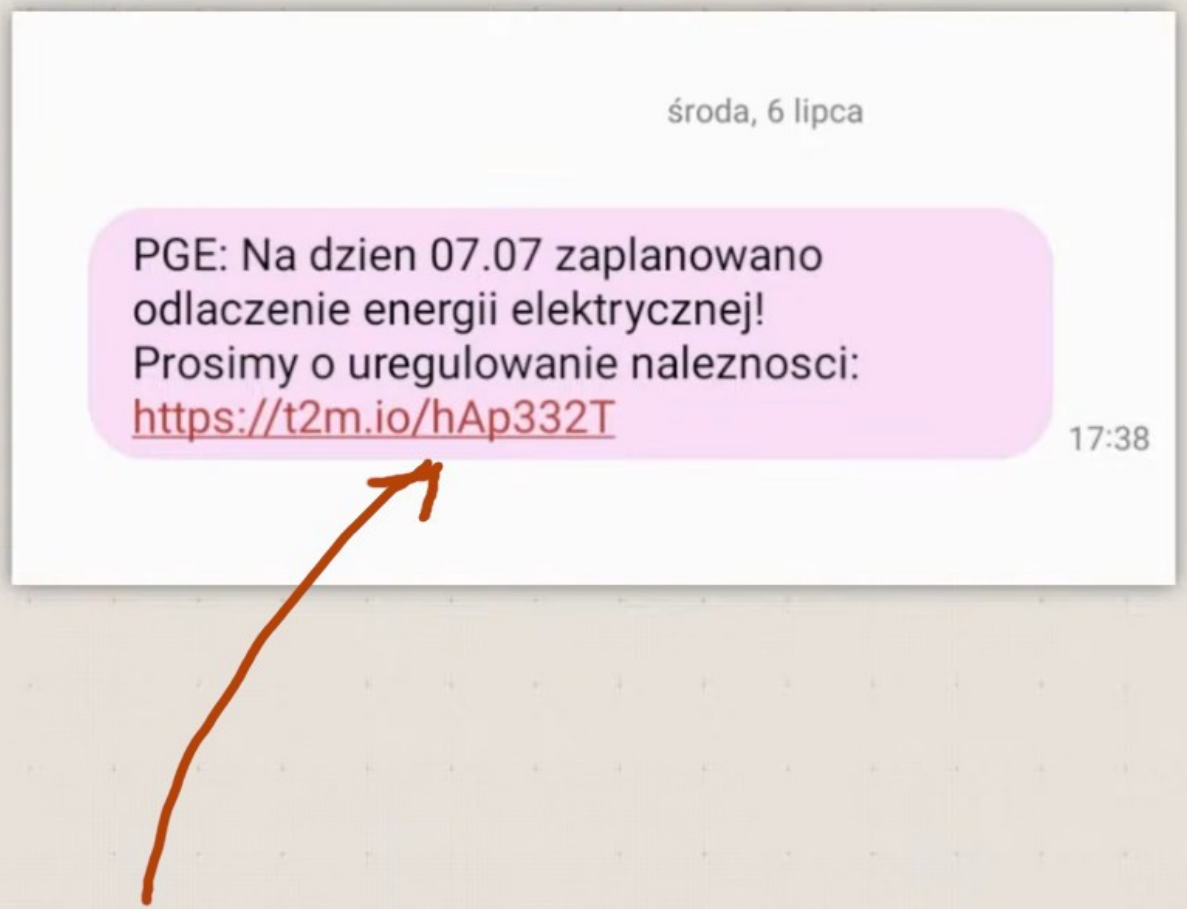




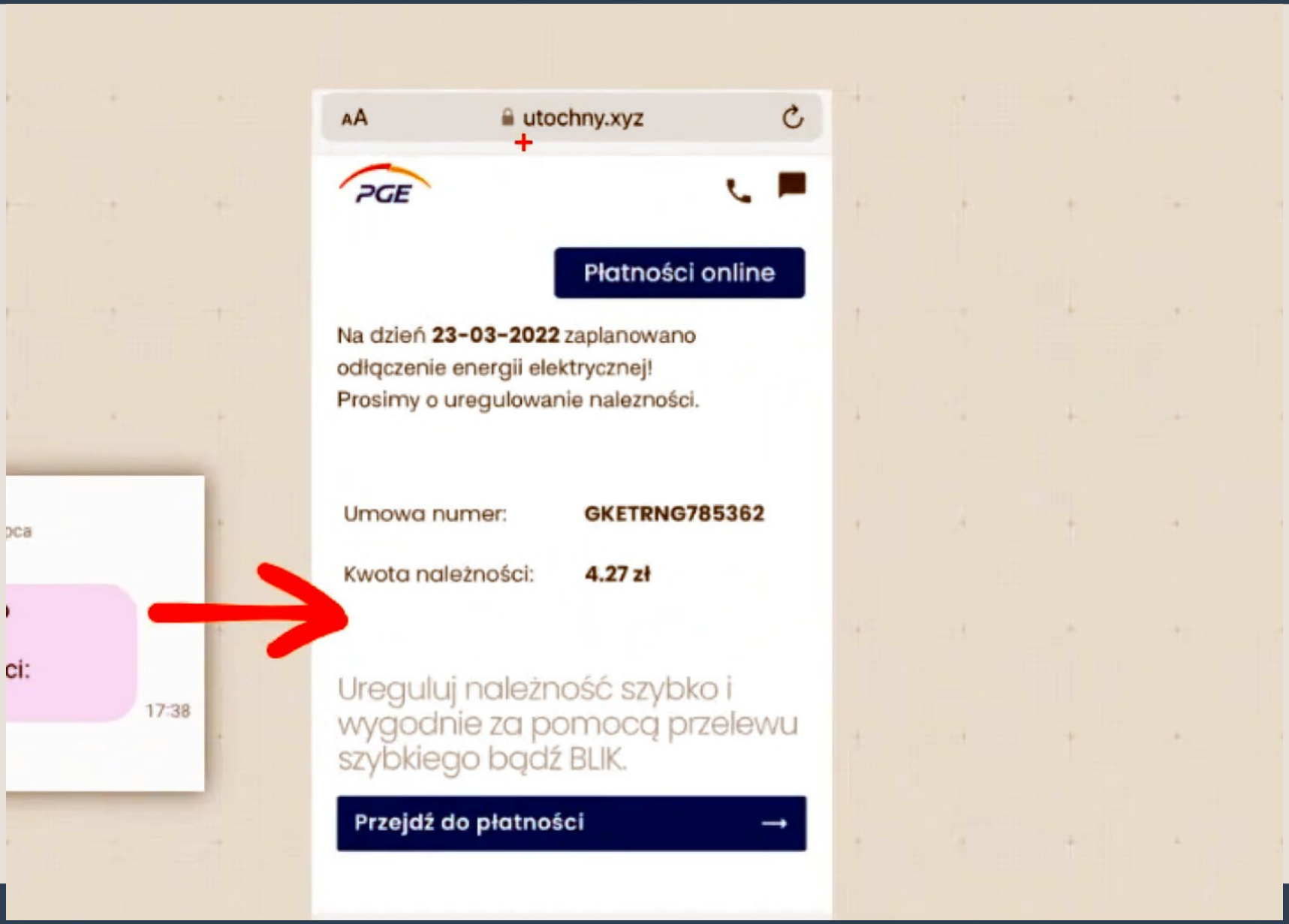




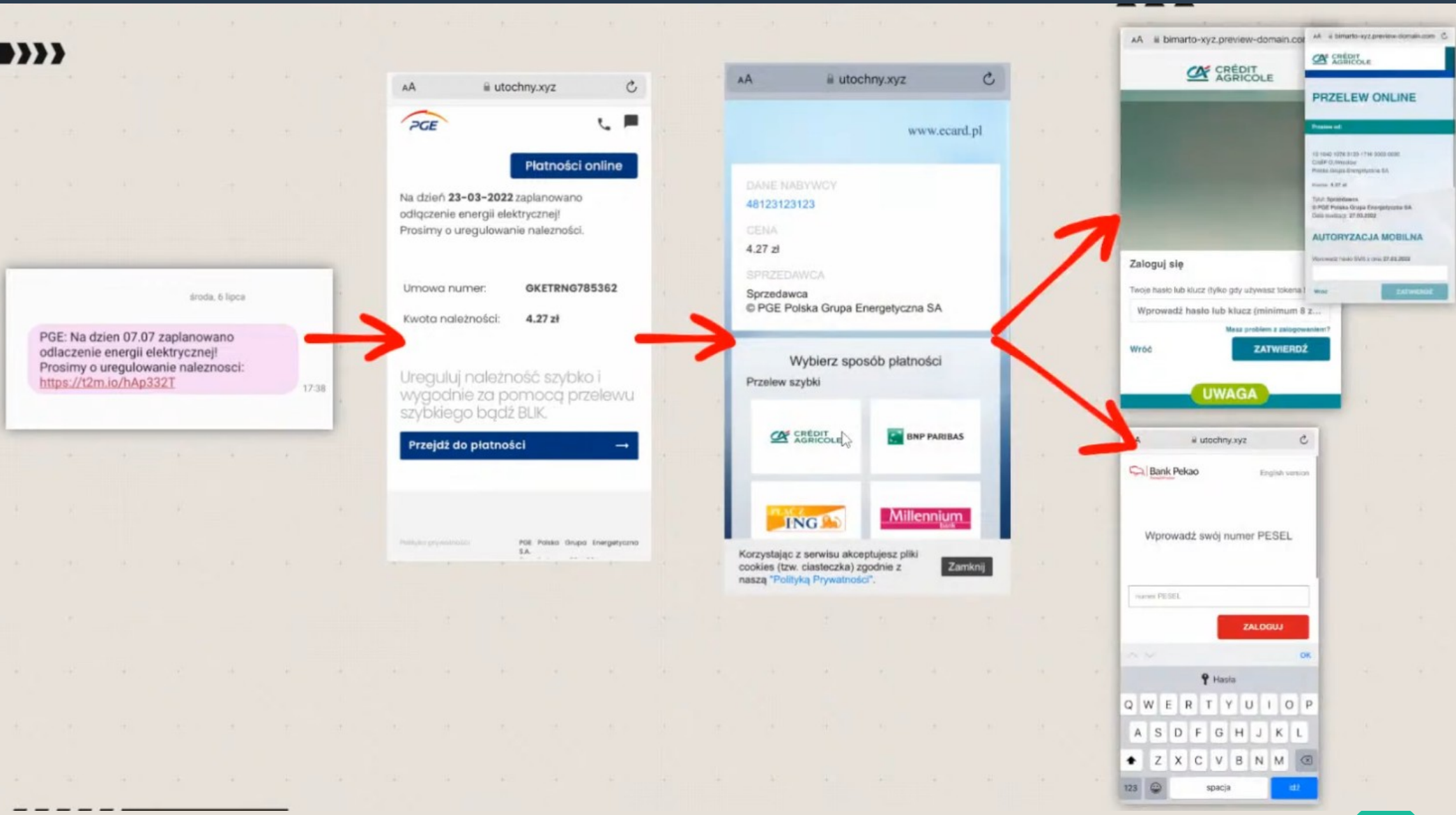
Fałszywy SMS udający PGE – jak to działa?



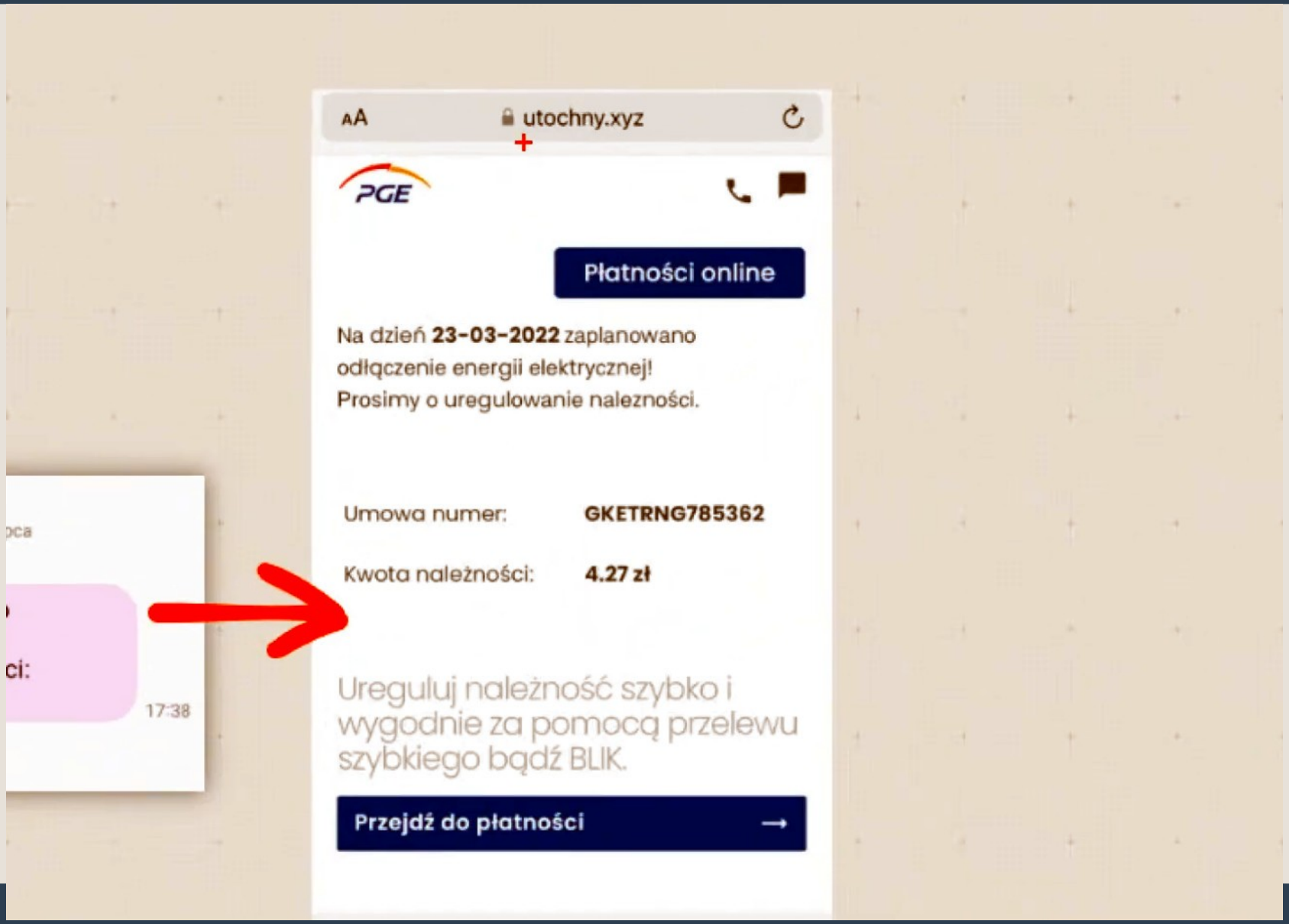
Fałszywy SMS udający PGE – jak to działa?



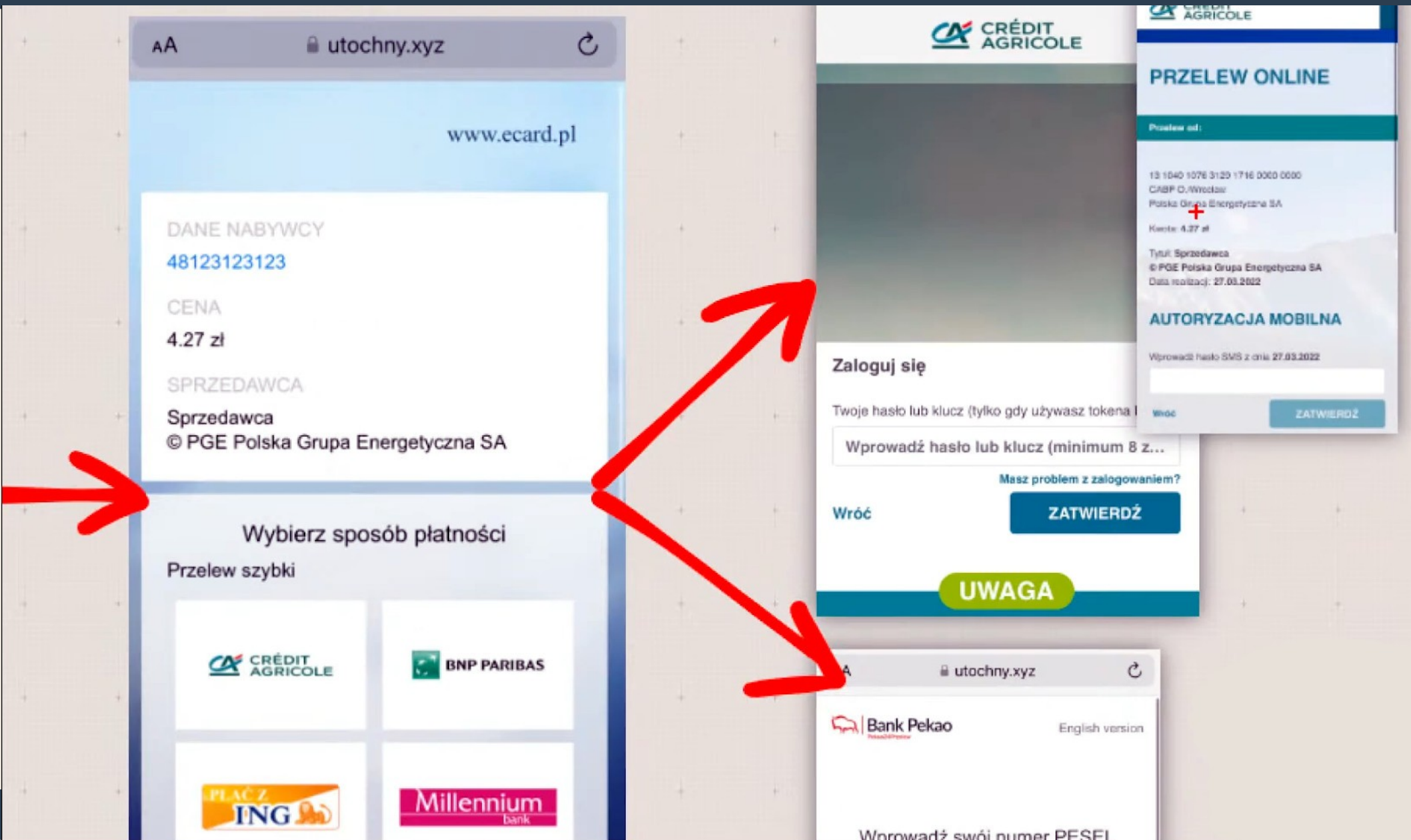
Fałszywy SMS udający PGE – jak to działa?



Fałszywy SMS udający PGE – jak to działa?



Fałszywy SMS udający PGE – jak to działa?



Fałszywy SMS

Czy samo kliknięcie w podejrzanego linka czymś grozi?

Wskazówka

Czy samo kliknięcie w podejrzanego linka czymś grozi?

Jeśli masz zaktualizowaną: przeglądarkę / rozszerzenia do przeglądarek / oprogramowanie na komputerze (telefonie)

To zazwyczaj NIE

Wskazówka

- Jeśli Cię jednak korci kliknięcie, to... nie klikaj :-)
- Jeśli Cię jednak bardzo korci użyj np. przeglądarki Edge oraz Nowe Okno Application Guard

Wskazówka

Czy samo otwarcie PDFa / pliku Microsoft Office czymś grozi?

Trochę zależy czy otworzyłem PDFa, a nie np. plik exe (wykonywalny)


Witam,
Dobry dzień panu.

Mam nadzieję, że dzisiaj wszystko w porządku.
Mój kolega Pan Dawid Krawiec wysłał Państwu nasze zamówienie PO-Eu598303 w zeszłym tygodniu, ale jeszcze nie otrzymaliśmy od Państwa odpowiedzi.
Tutaj znów cię wysyłam. Prosimy o dostarczenie faktury proforma zgodnie z załączonym zamówieniem PO-Eu598303.

Mamy nadzieję, że niedługo się odezwiesz.

PDF

Zamowienie_zakupu_PO-Eu598303.pdf

--

pozdrowienia
pani malgorzata berez
HBDTOYS SP.ZO.O
telefon: 48-71-7254955
faks: 48-71-7220091
e-mail : biuro@hbdtoys.com
adres: skierniewicka, nr 10a, lok. 6p

HBDTOYS SP.ZO.O

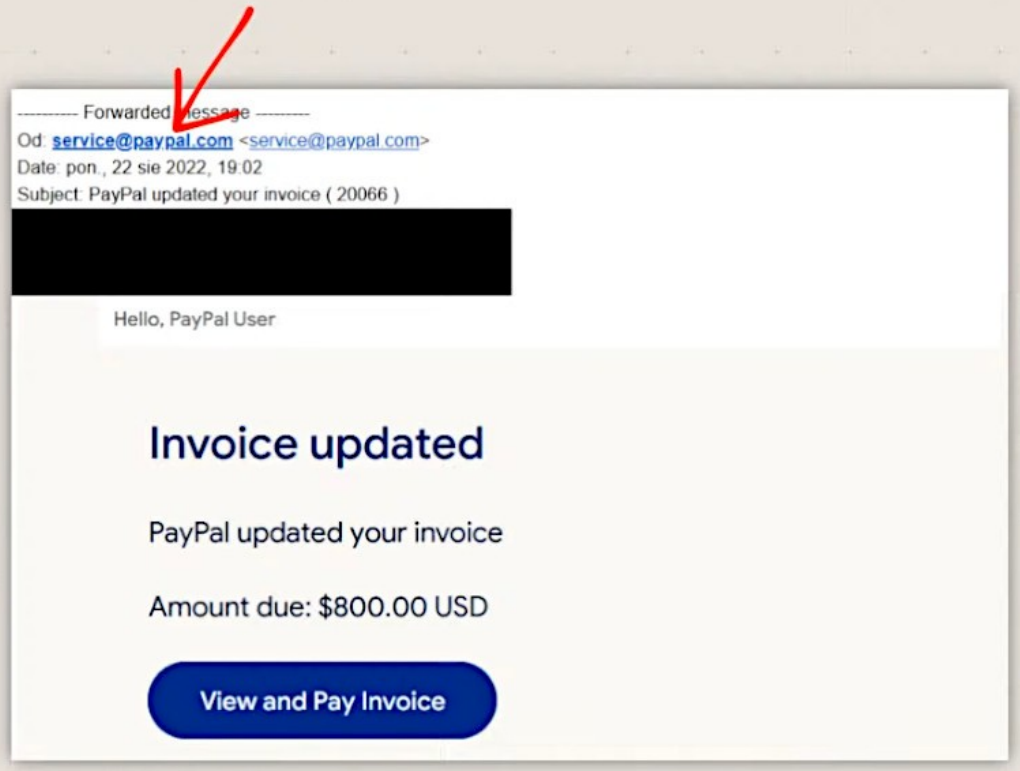
Inna przykładowa zmyłka:

wyciag-bankowy.pdf.exe

Phishing cz.3

Przykłady zaawansowanych oszustw.

Phishing cz.3 – przykład nr1



---------- Forwarded message ---------
Od: service@paypal.com <service@paypal.com>
Date: pon., 22 sie 2022, 19:02
Subject: PayPal updated your invoice (20066)

[redacted]

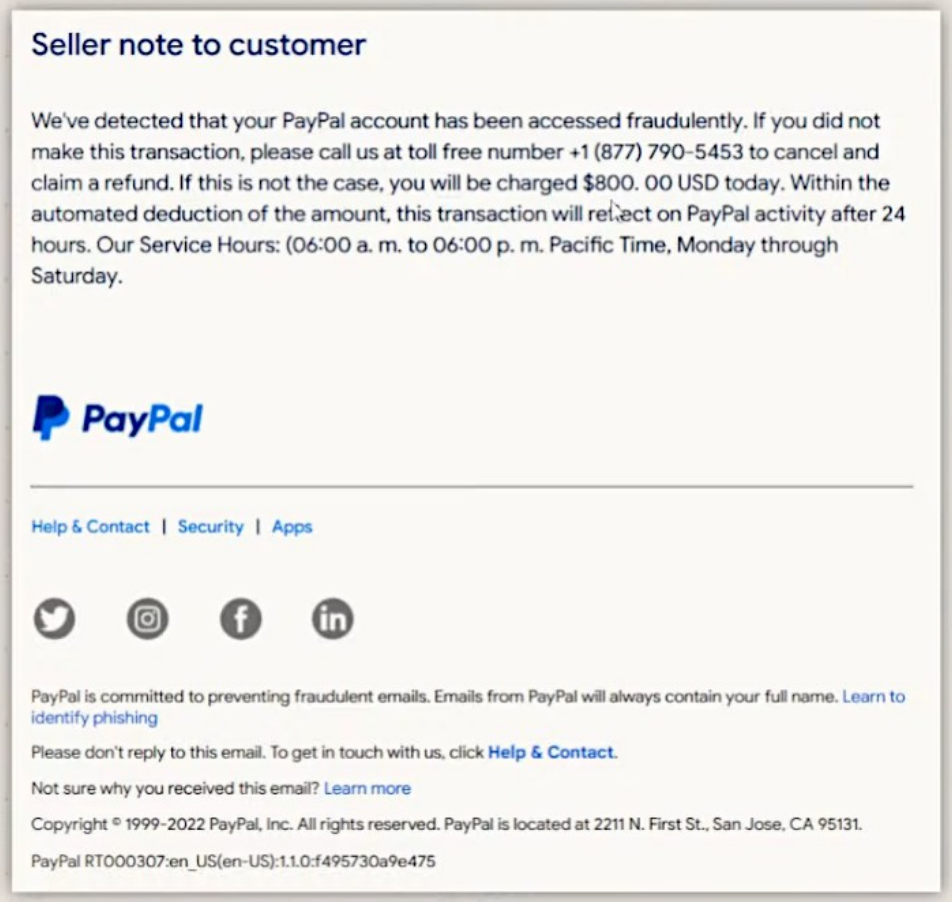
Hello, PayPal User

Invoice updated

PayPal updated your invoice

Amount due: $800.00 USD

View and Pay Invoice



Seller note to customer

We've detected that your PayPal account has been accessed fraudulently. If you did not make this transaction, please call us at toll free number +1 (877) 790-5453 to cancel and claim a refund. If this is not the case, you will be charged $800. 00 USD today. Within the automated deduction of the amount, this transaction will reflect on PayPal activity after 24 hours. Our Service Hours: (06:00 a. m. to 06:00 p. m. Pacific Time, Monday through Saturday.

PayPal

Help & Contact | Security | Apps

PayPal is committed to preventing fraudulent emails. Emails from PayPal will always contain your full name. Learn to identify phishing

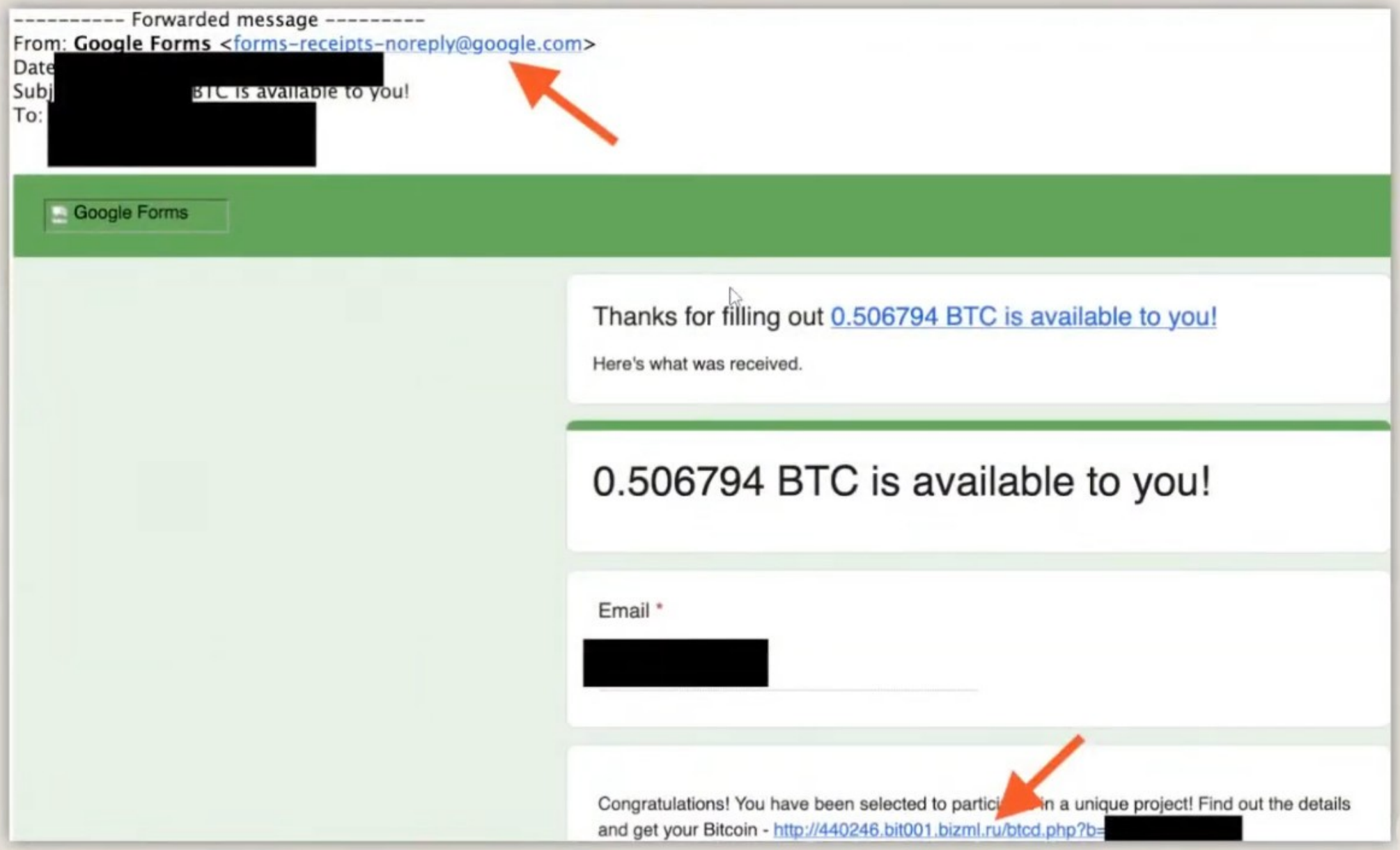
Please don't reply to this email. To get in touch with us, click Help & Contact.

Not sure why you received this email? Learn more

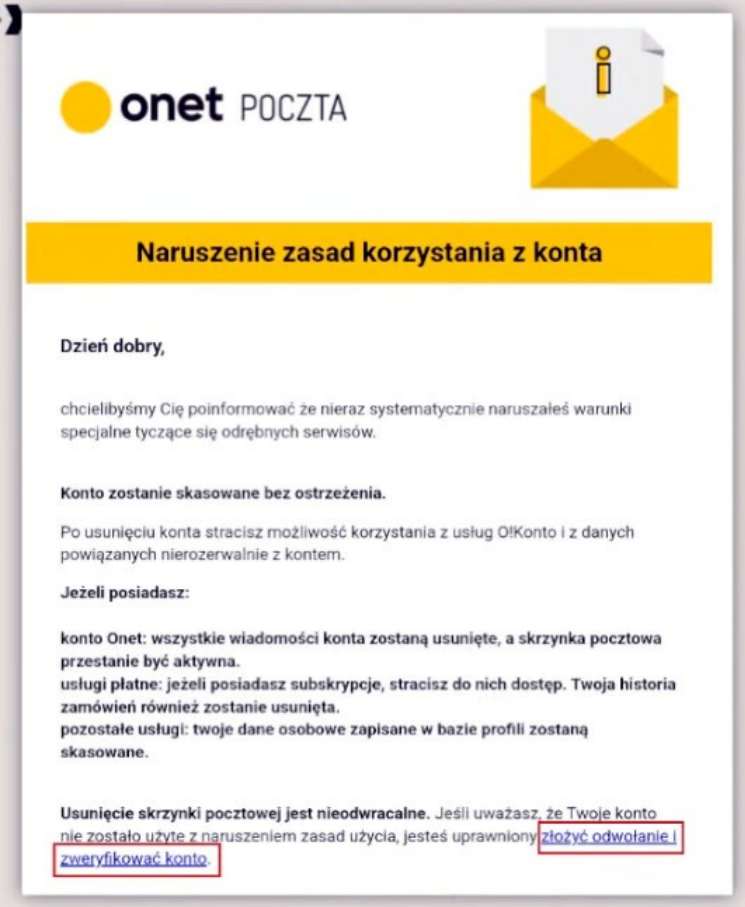
Copyright © 1999-2022 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

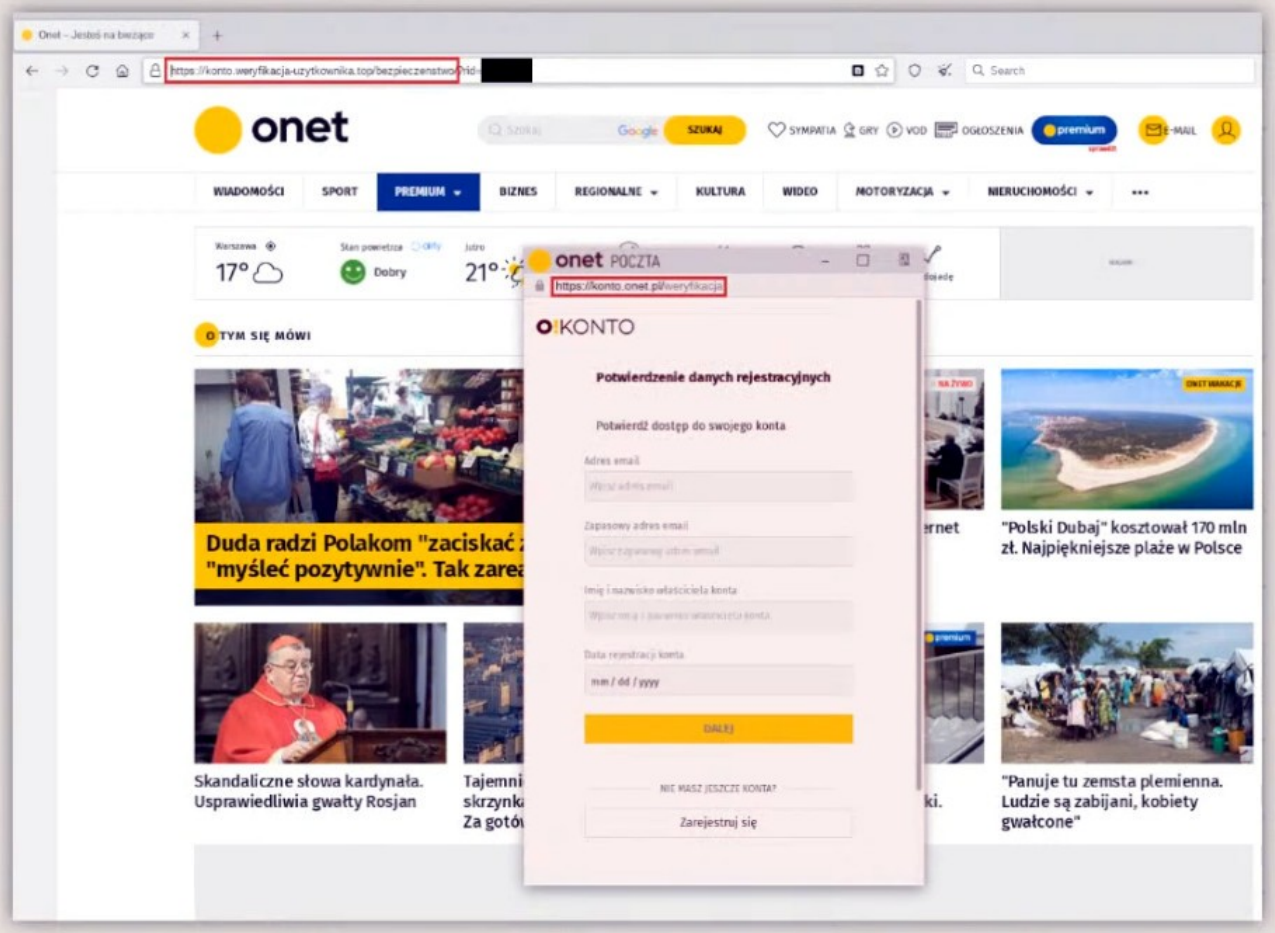
PayPal RT000307:en_US(en-US):1.1.0:f495730a9e475

Phishing cz.3 – przykład nr2



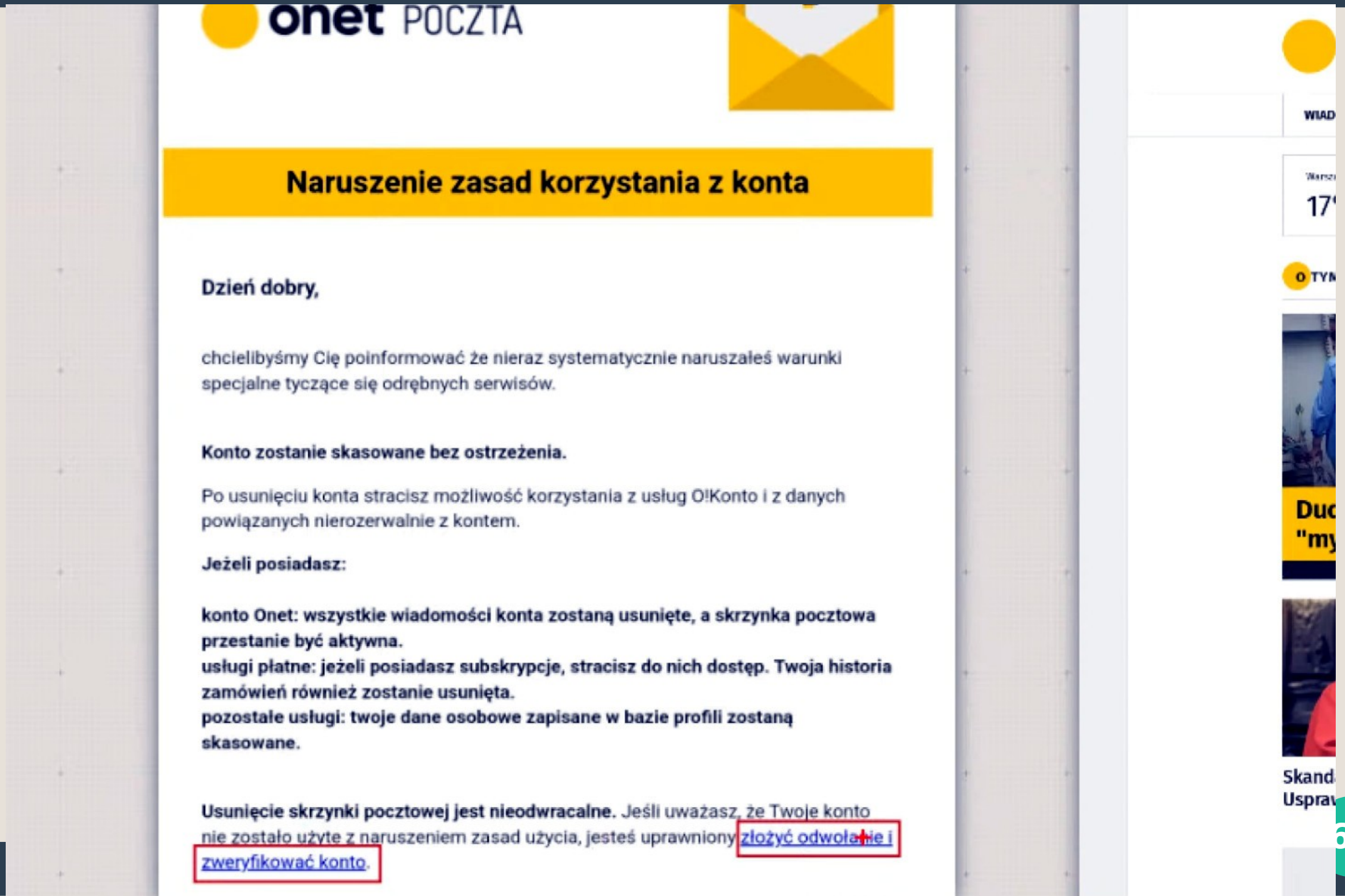
Phishing cz.3 – przykład nr3





https://cert.pl/posts/2022/07/techniki-unc115

Phishing cz.3 – przykład nr3



onet POCZTA

Naruszenie zasad korzystania z konta

Dzień dobry,

chcielibyśmy Cię poinformować że nieraz systematycznie naruszałeś warunki specjalne tyczące się odrębnych serwisów.

Konto zostanie skasowane bez ostrzeżenia.

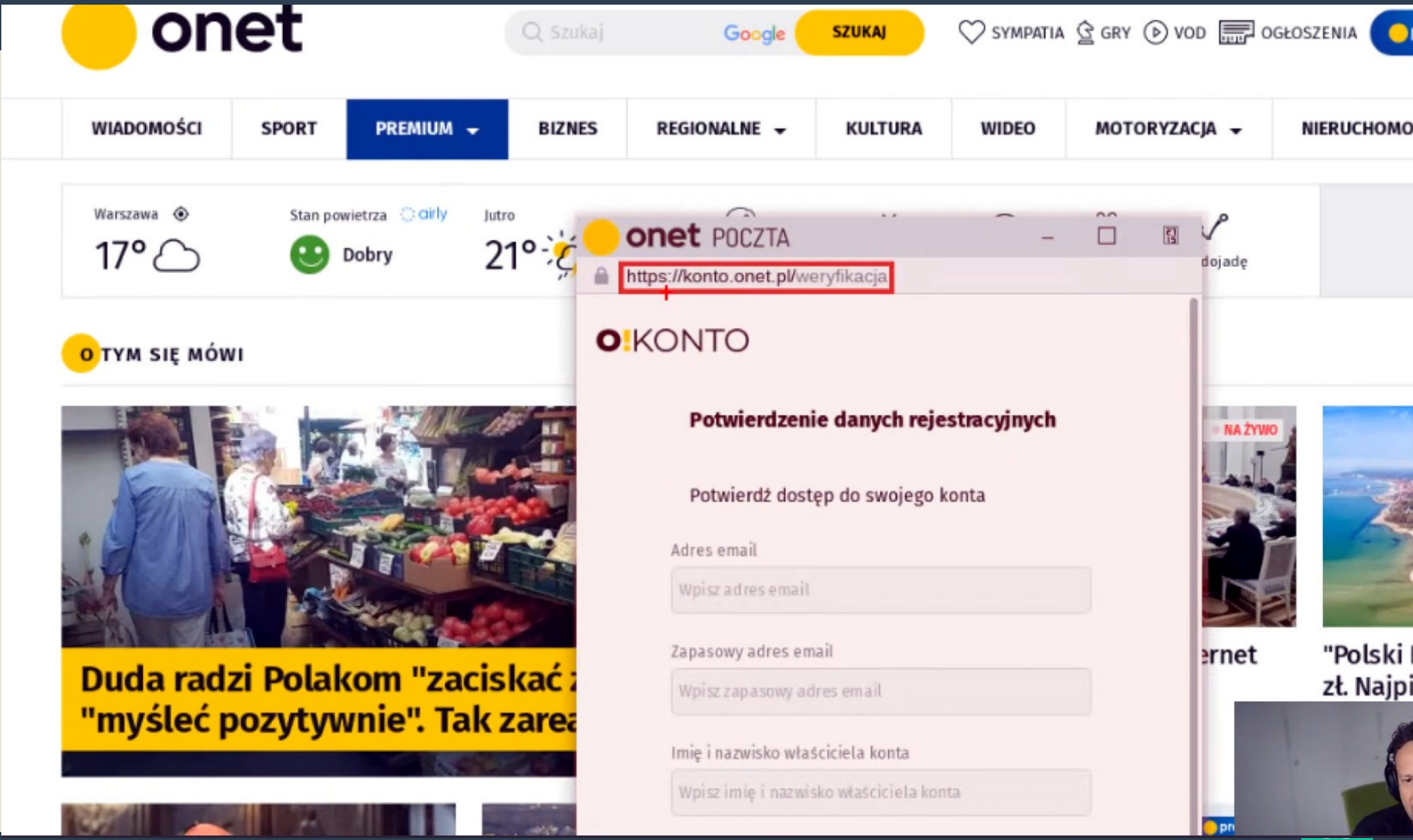
Po usunięciu konta stracisz możliwość korzystania z usług O!Konto i z danych powiązanych nierozerwalnie z kontem.

Jeżeli posiadasz:

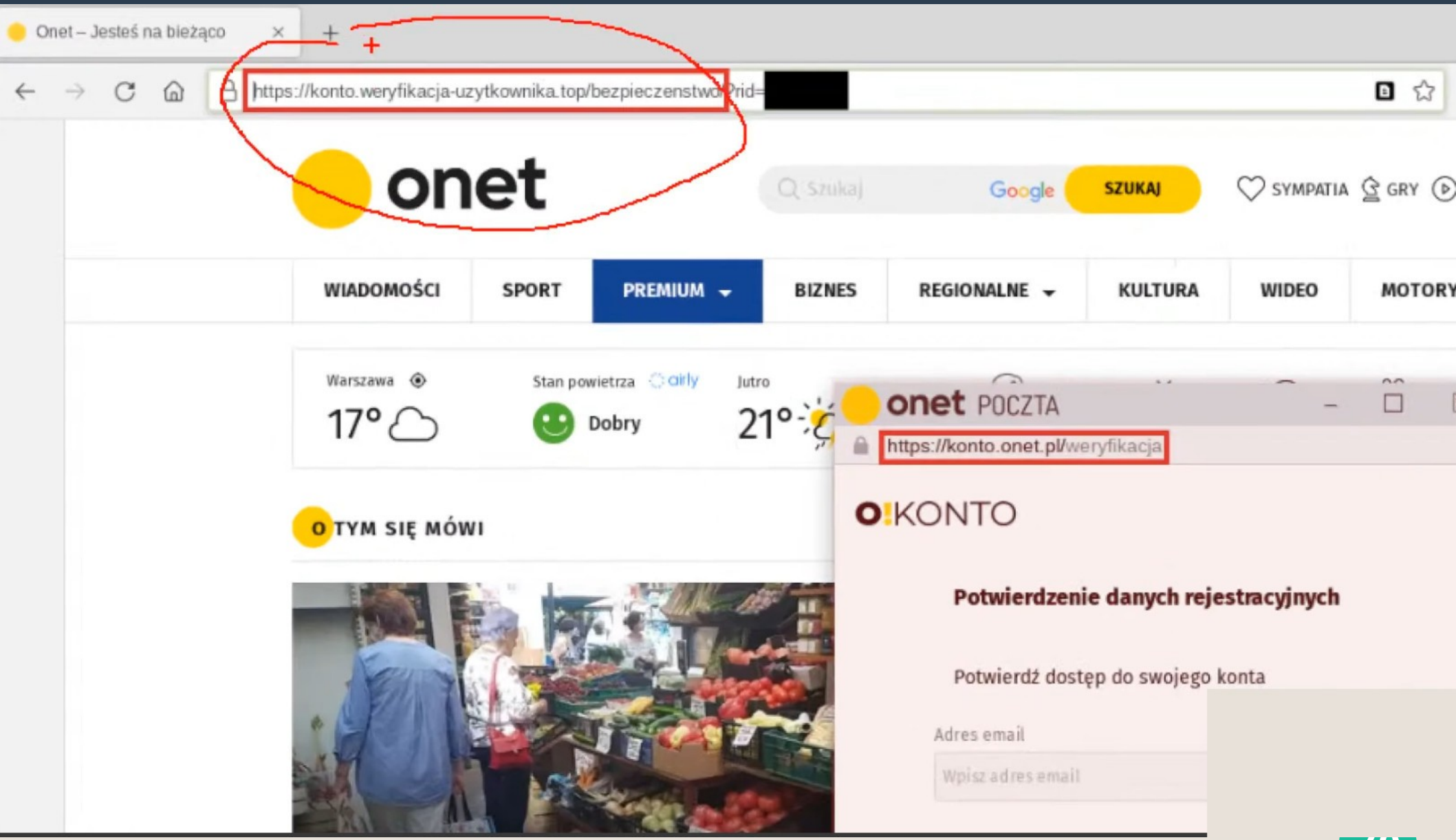
konto Onet: wszystkie wiadomości konta zostaną usunięte, a skrzynka pocztowa przestanie być aktywna.
usługi płatne: jeżeli posiadasz subskrypcje, stracisz do nich dostęp. Twoja historia zamówień również zostanie usunięta.
pozostałe usługi: twoje dane osobowe zapisane w bazie profili zostaną skasowane.

Usunięcie skrzynki pocztowej jest nieodwracalne. Jeśli uważasz, że Twoje konto nie zostało użyte z naruszeniem zasad użycia, jesteś uprawniony złożyć odwołanie i zweryfikować konto.

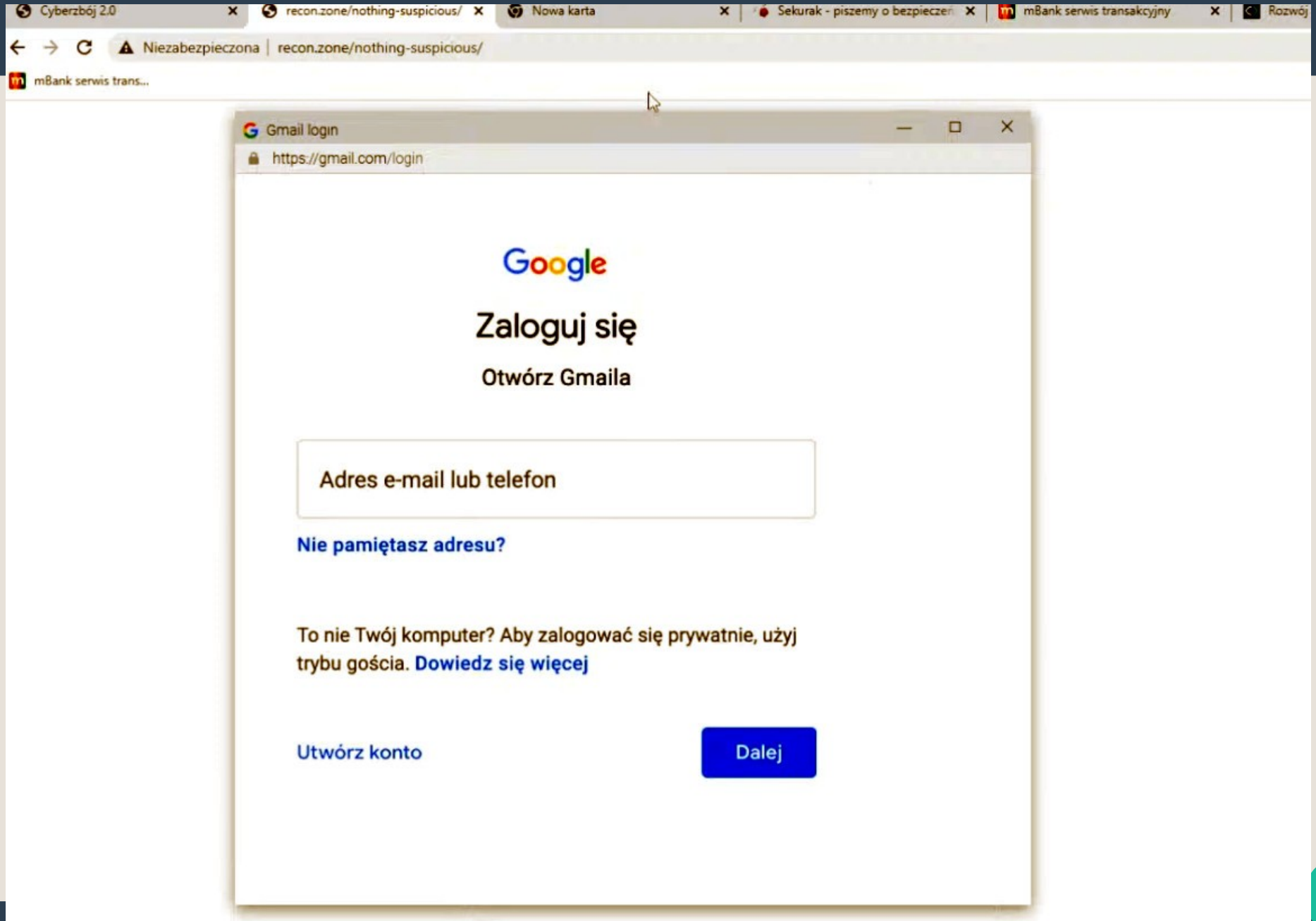
Phishing cz.3 – przykład nr3



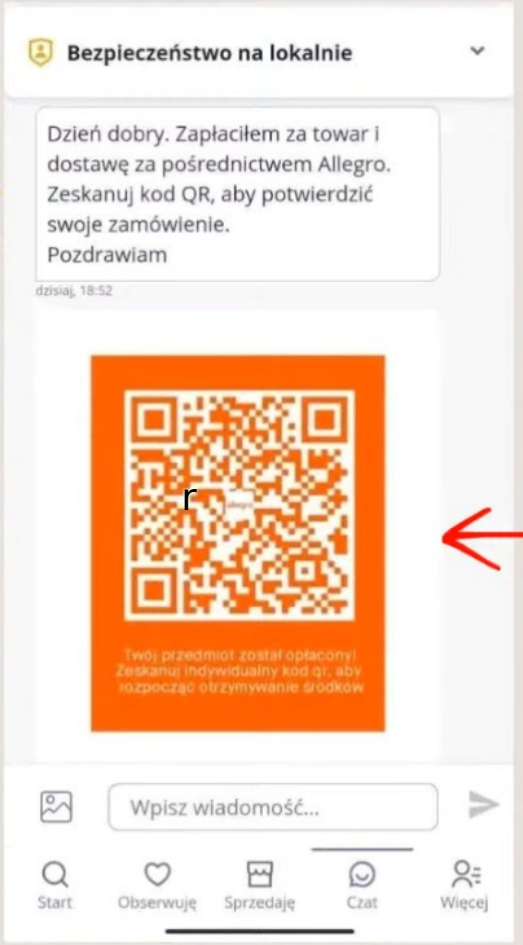
Phishing cz.3 – przykład nr3



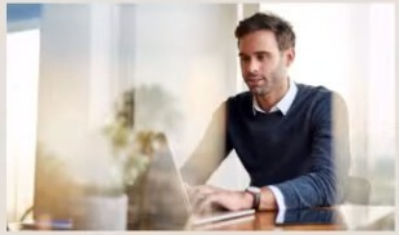
Phishing cz.3 – przykład nr4



Phishing cz.3 – kod QR – przykład nr4



kliknąć? nie kliknąć?



Phishing cz.3 – kod QR – przykład nr4

DHL EXPRESS

Zamówienie: PI#6517898987
Termin przyjazdu: 14,czerwca,2022

Szanowny Kliencie,
Twoja przesyłka dotarła na pocztę. Nasz kurier nie mógł dostarczyć Ci paczki.

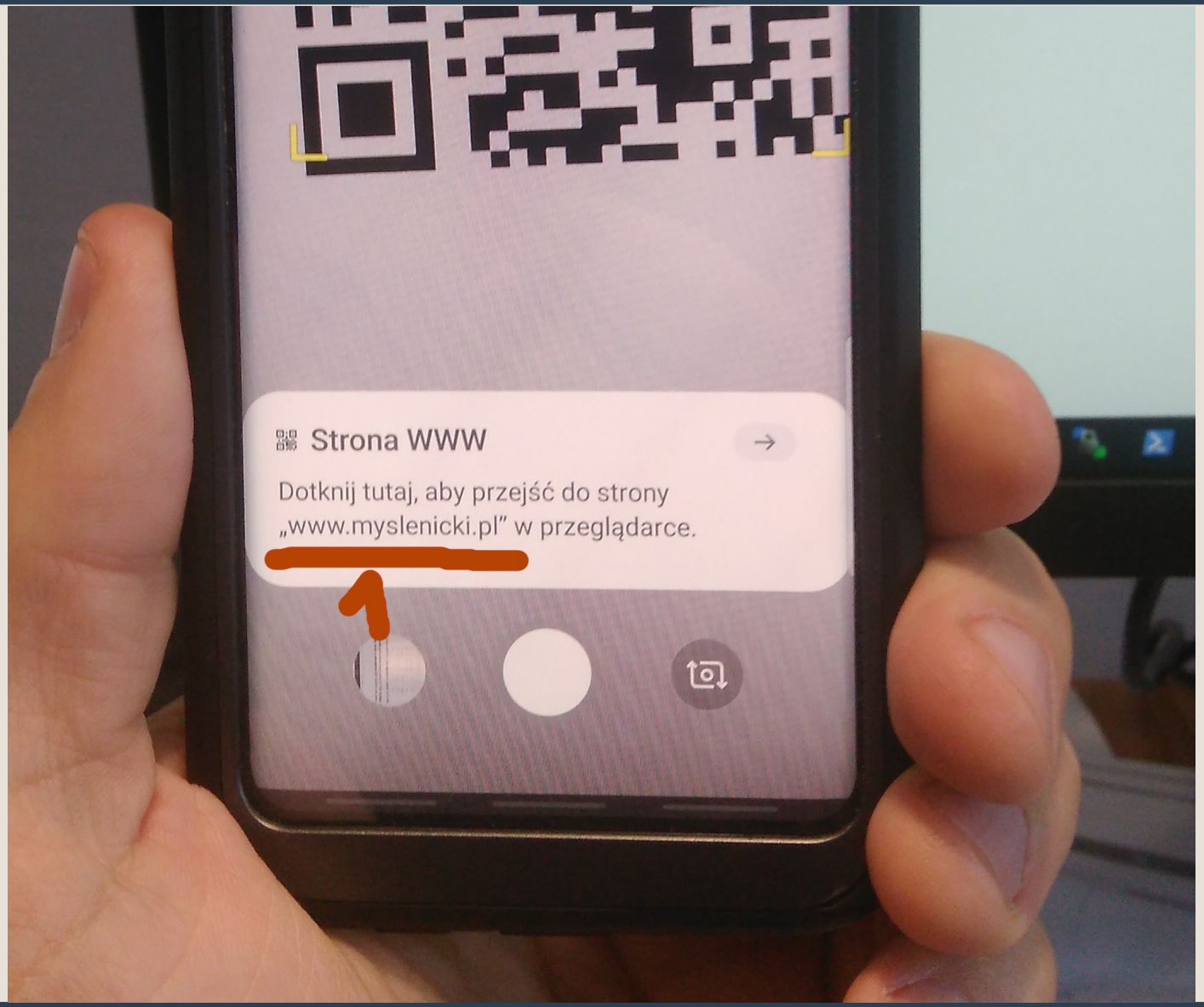
Aby zakończyć cały proces, zeskanuj poniższy kod QR przed odebraniem przesyłki.

Phishing cz.3 – kod QR – przykład nr4

Wskazówka


Bixby Vision
Ik. emoji AR
Strona WWW
Dotknij tutaj, aby przejść do strony „www.myslenicki.pl" w przeglądarce.
03/10/2022 10:25:41

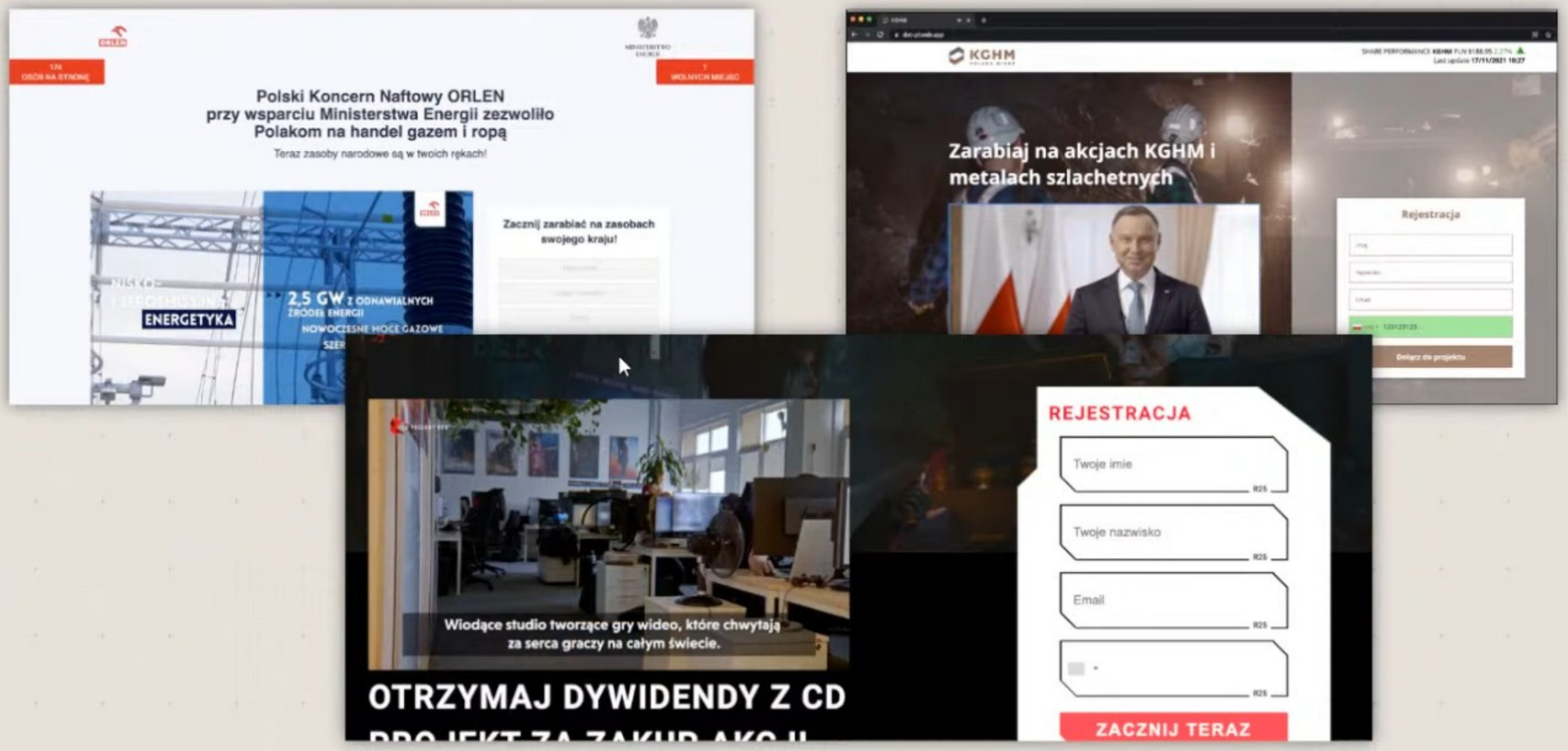
Wskazówka


Strona WWW
Dotknij tutaj, aby przejść do strony „www.myslenicki.pl” w przeglądarce.

Wskazówka


2
0
Strona WWW
Dotknij tutaj, aby przejść do strony „www.myslenicki.pl” w przeglądarce.

UWAGA! Na super okazje

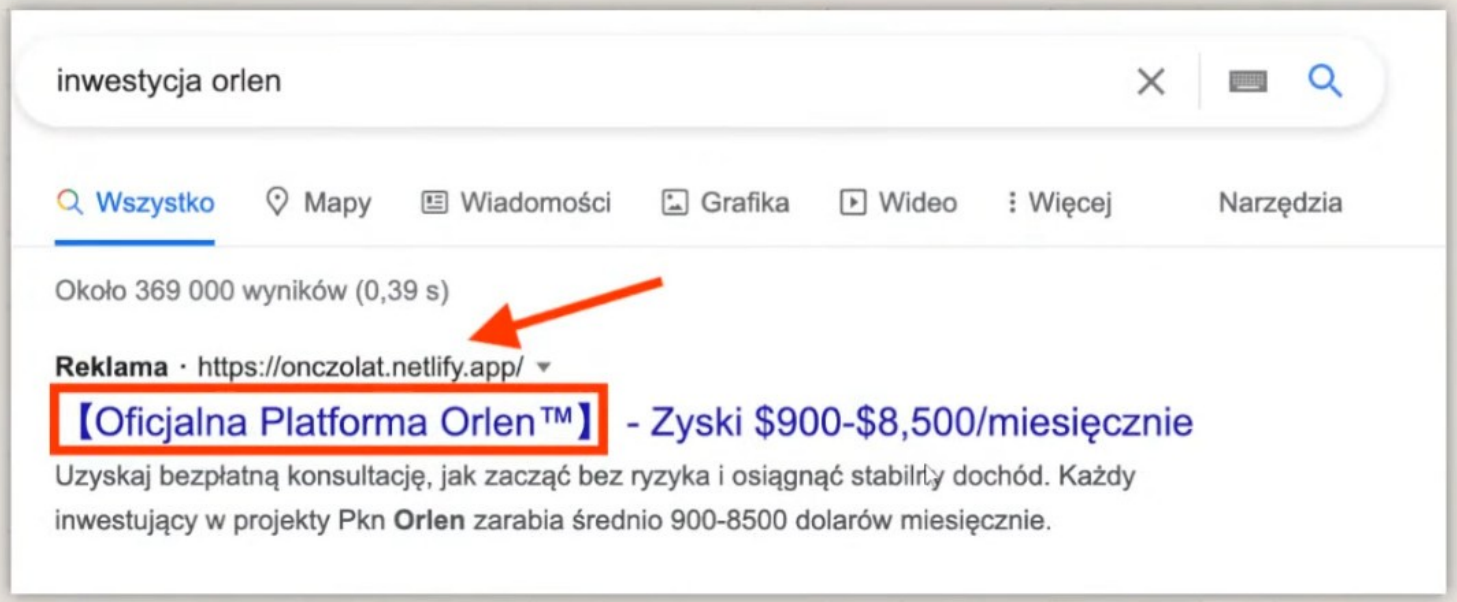


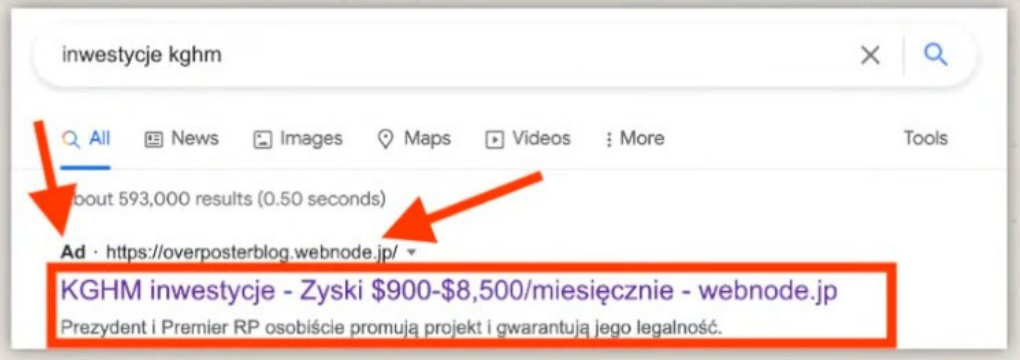
UWAGA! Na super okazje

Pan Maciek(*) kliknął w reklamę super inwestycji.
Całość wspierał wizerunek „znanego polityka”.
Gdańszczanin stracił ~750 000 zł

https://gdansk.policja.gov.pl/pm1/informacje/wiadomosci/113553,Chcial-pomnozyc-swoje-oszczednosci-a-wszystko-stracil.html

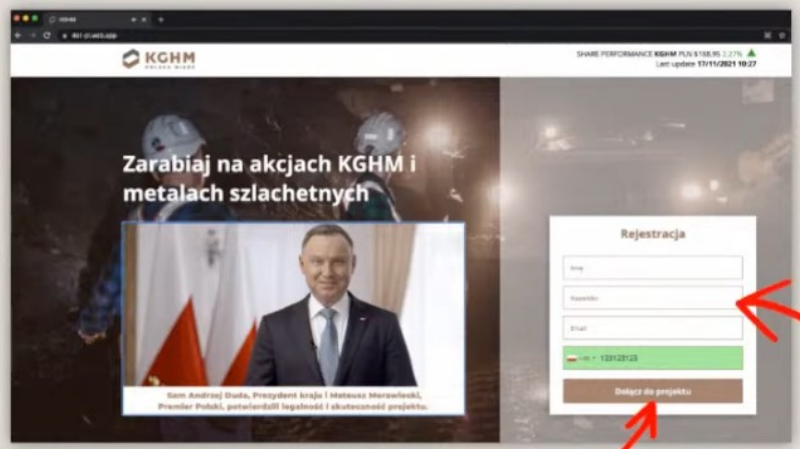
UWAGA! Na super okazje

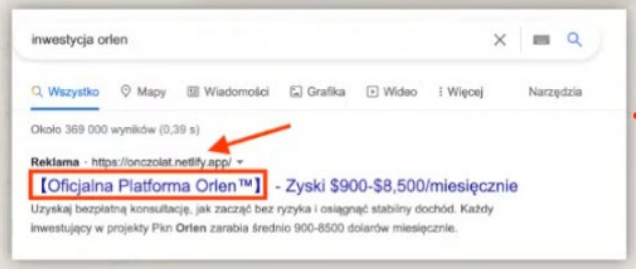




UWAGA! Na super okazje

UWAGA! Na super okazje

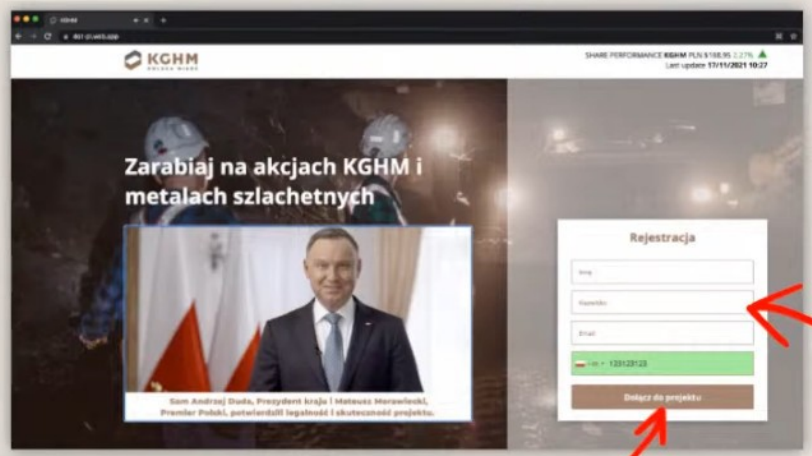




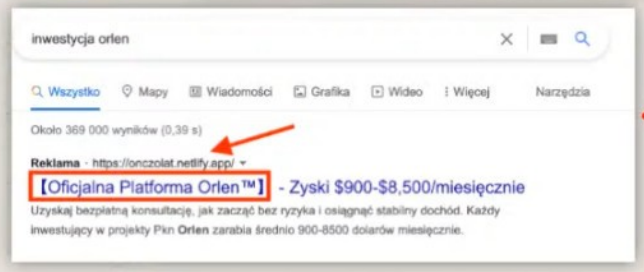
halo, czy to pan się rejestrował na naszej platformie?

UWAGA! Na super okazje

Google



halo, czy to pan się rejestrował na naszej platformie?



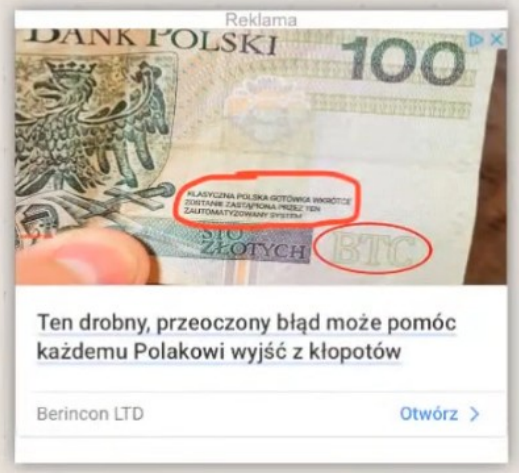
YouTube

Nie inwestował pan jeszcze w akcje? Nie ma problemu, już pomogę. Proszę zainstalować narzędzie anydesk na komputerze / telefonie

Wskazówka

- Uważaj na "cudowne okazje"

Nazywam się Chang Dingxiang, jestem starszym personelem w publicznym banku w Wing Hang Bank w Hongkongu i mam 18 991 674 USD. że chcę wyjechać z kraju. Potrzebuję dobrego partnera, kogoś, komu mogę zaufać. To jest wolne od ryzyka i legalne. Odpowiedz na mój e-mail: changdingxiang708@gmail.com, aby uzyskać więcej informacji: pan Chang Dingxiang.

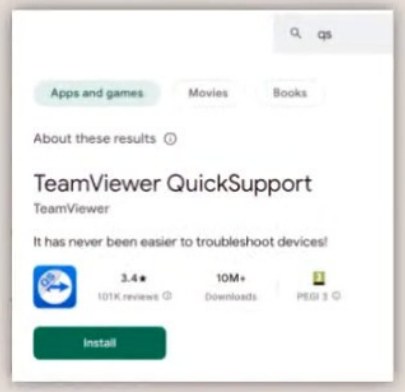


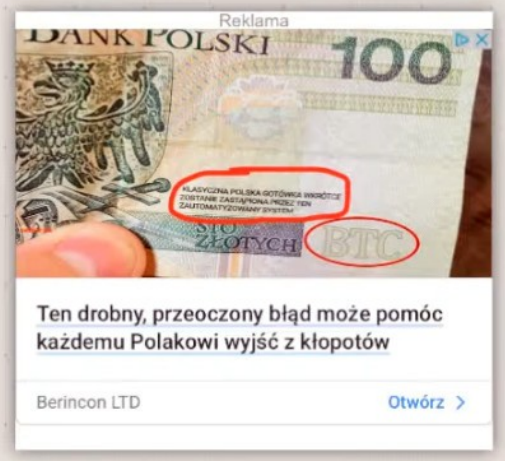
Wskazówka

Uważaj na "cudowne okazje"

Nazywam się Chang Dingxiang, jestem starszym personelem w publicznym banku w Wing Hang Bank w Hongkongu i mam 18 991 674 USD. że chcę wyjechać z kraju. Potrzebuję dobrego partnera, kogoś, komu mogę zaufać. To jest wolne od ryzyka i legalne. Odpowiedz na mój e-mail: changdingxiang708@gmail.com, aby uzyskać więcej informacji: pan Chang Dingxiang.

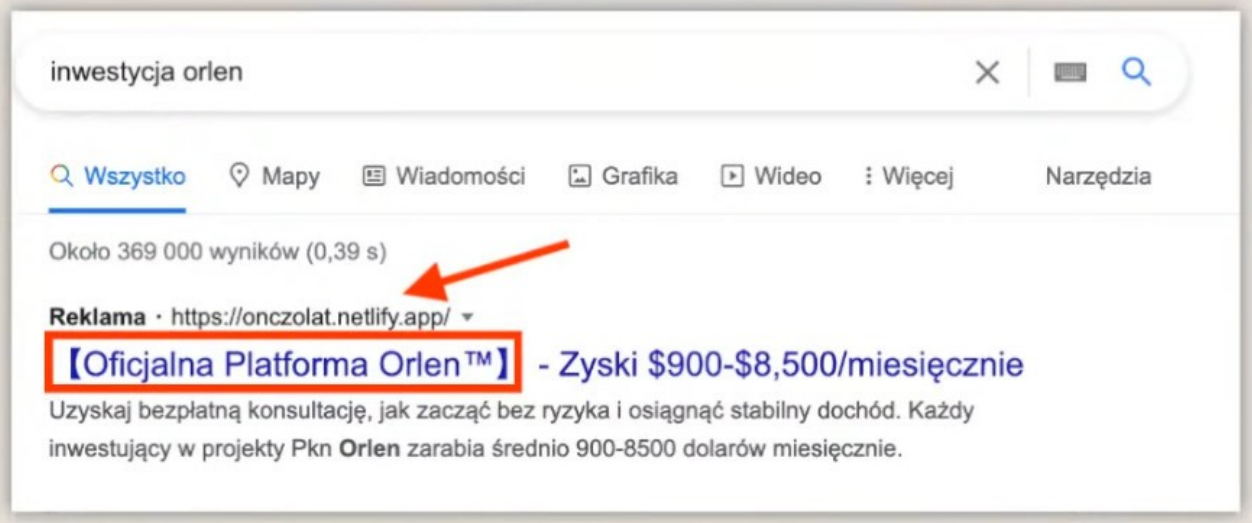
Nie instaluj aplikacji, które "konsultant" poleca Ci przez telefon





Wskazówka

Jeśli strona ma dużo polubień / komentarzy / reklamuje się
- nie oznacza to automatycznie, że jest bezpieczna



UWAGA! Na super okazje

Używaj bezpiecznych haseł!

np. takich!?
(poczta.onet.pl)

Wskazówka

Używaj bezpiecznych haseł!

Idealnie: 4+ nieoczywiste sklejone słowa. Długość: > 15 znaków

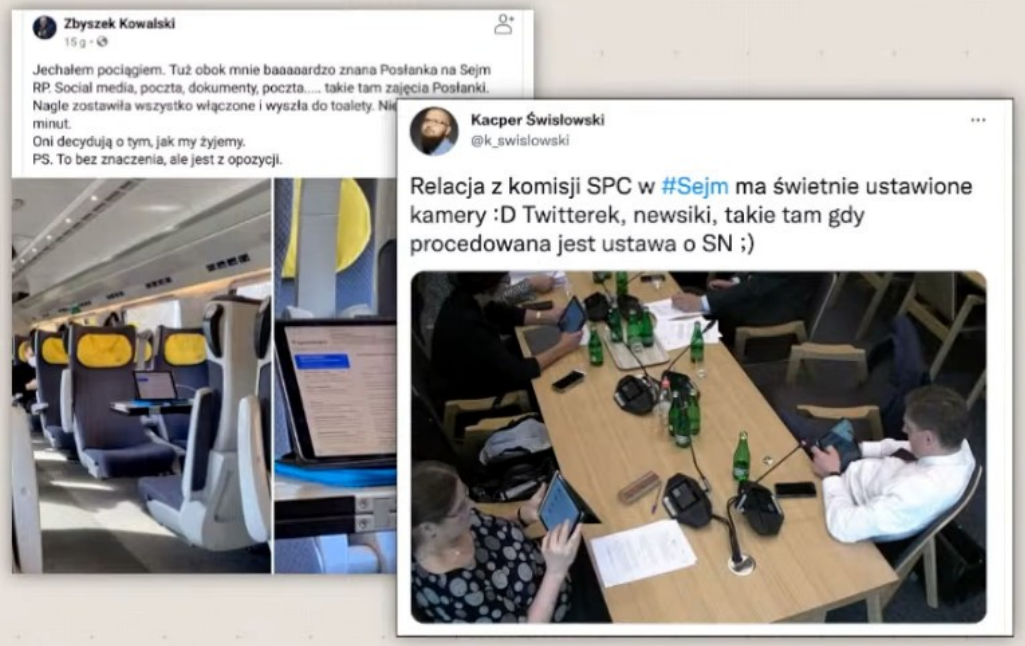
weekendowepogodnekrakowaniehasel

Wskazówka

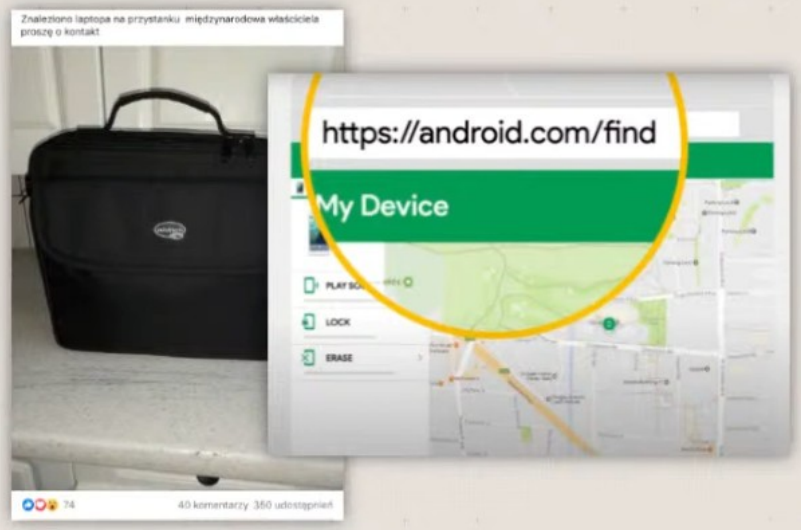
- Nie używaj tego samego hasła w wielu różnych miejscach!
  - włam do jednego miejsca może skutkować przejęciem wszystkich Twoich kont
- Szczególnie chroń skrzynkę pocztową
  - włam na skrzynkę umożliwia przejęcie kont, gdzie użyłeś tego maila do rejestracji
- Pamiętaj o skonfigurowaniu 2FA (dwuczynnikowego uwierzytelnienia)
  - nawet jak ktoś ma login/hasło - nie dostanie się na Twoje konto

Wskazówka

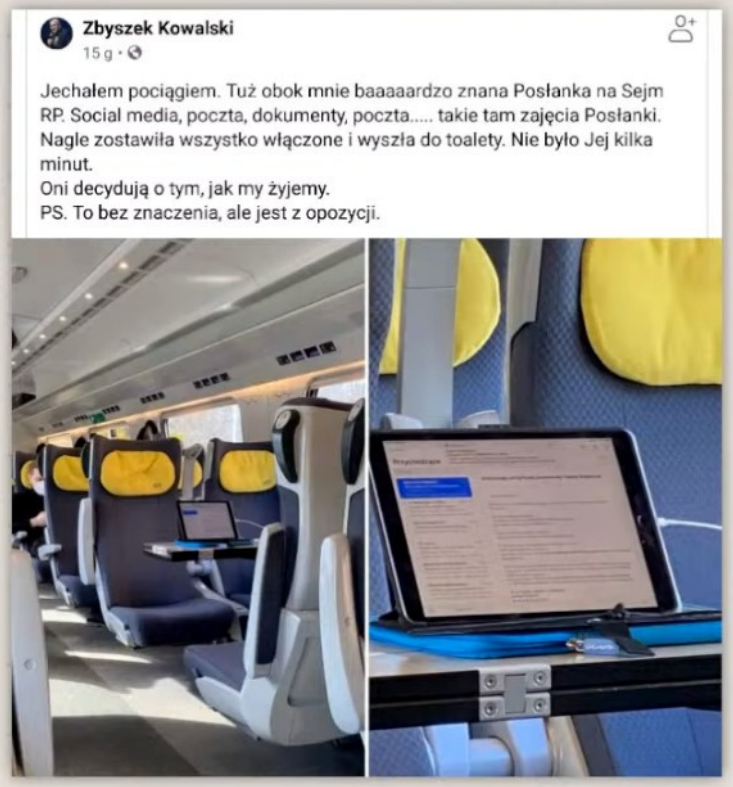
Miejsce pracy (w tym dostęp do Internetu)



Przygotowanie się na ew. utratę telefonu / laptopa



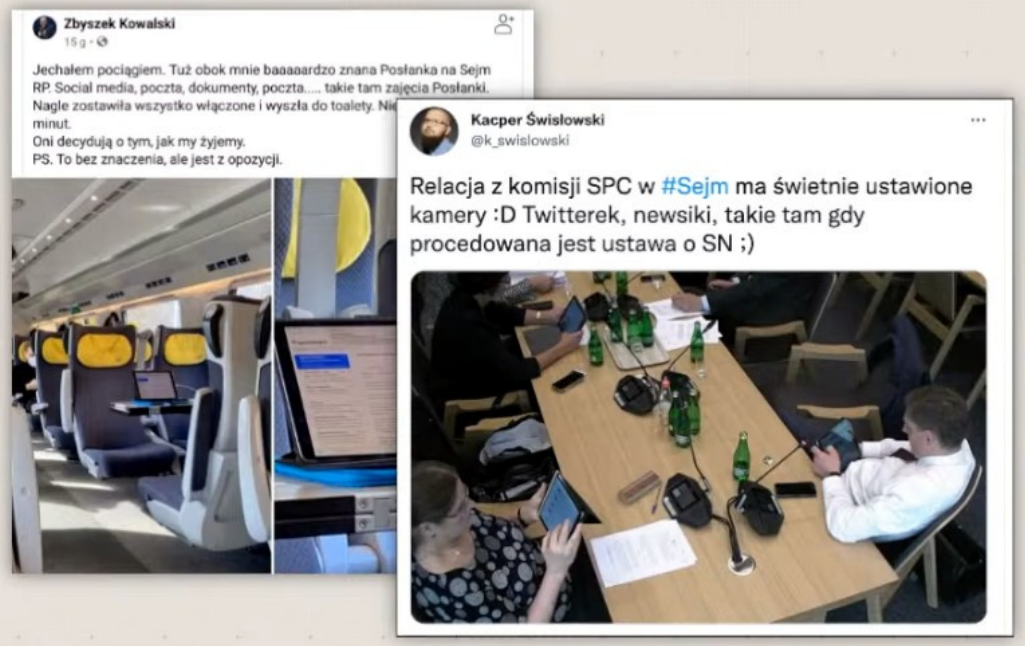
Wskazówka



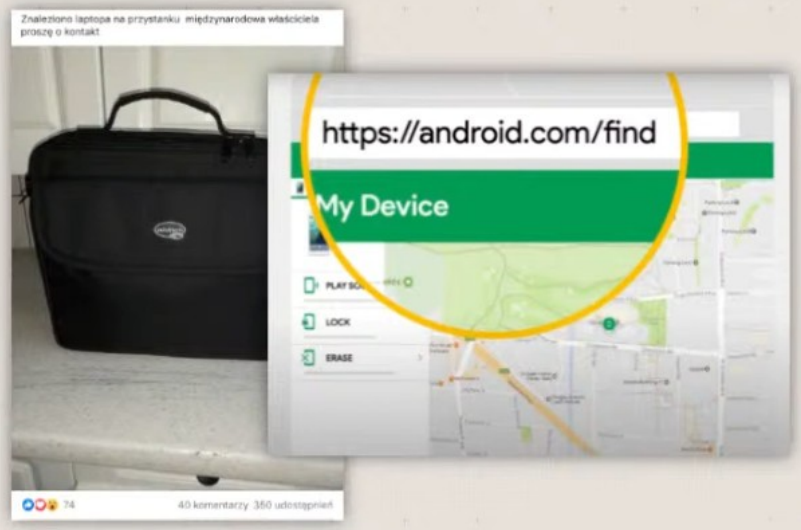
- Nie zostawiaj komputera bez opieki
- Ustaw auto-blokadę komputera po np. minucie nieaktywności

Wskazówka

Miejsce pracy (w tym dostęp do Internetu)



Przygotowanie się na ew. utratę telefonu / laptopa



Wskazówka

Filtr prywatyzujący

https://www.kensington.com/c/products/data-protection/privacy-screens/?srt

Wskazówka

Wybierz bezpieczne miejsce pracy

Kamery!

Kamery :)


Kacper Świsłowski
@k_swislowski
Relacja z komisji SPC w #Sejm ma świetnie ustawione kamery :D Twitterek, newsiki, takie tam gdy procedowana jest ustawa o SN ;)

KONIEC :)