

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 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#

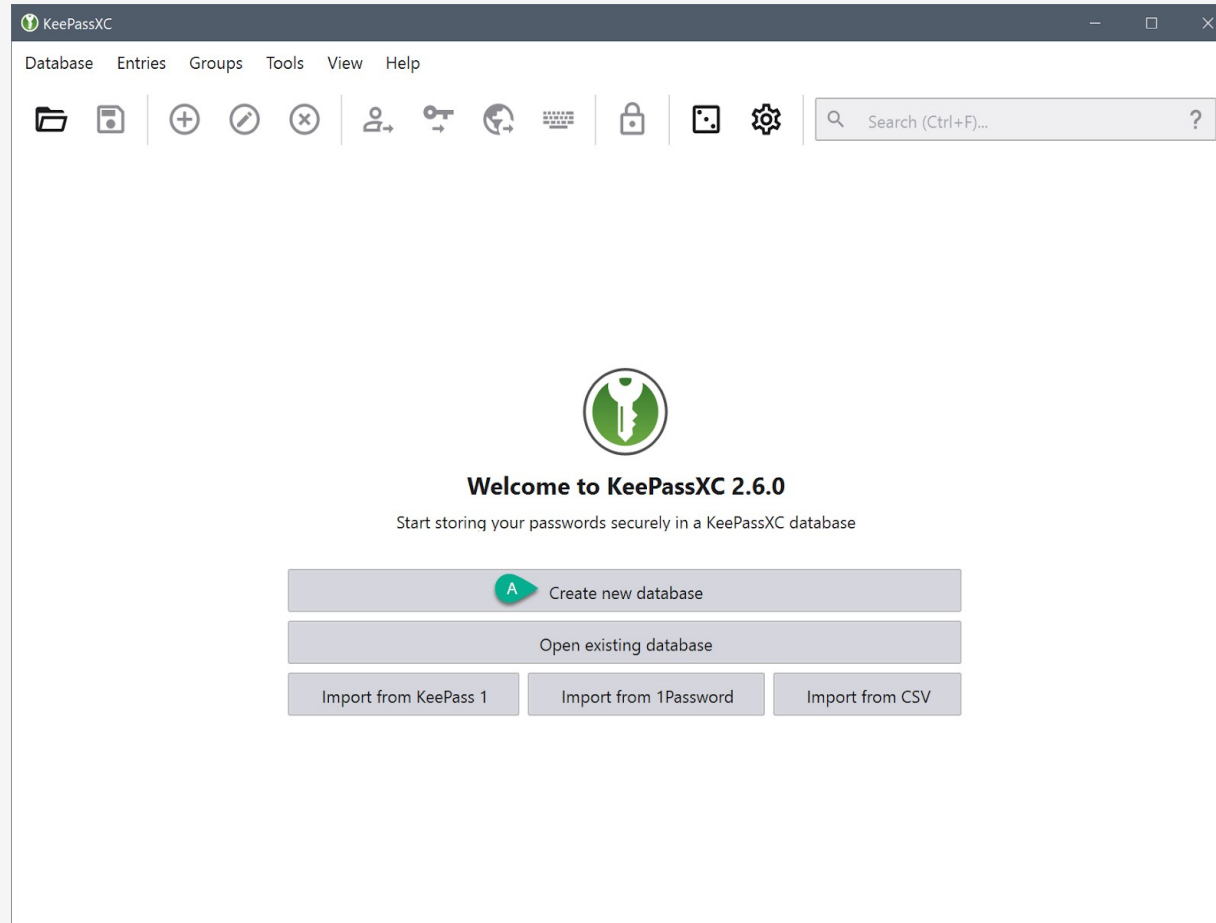
Zi3lony&Samochood#

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
- **podszycwanie 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 obsługiwanych 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.)



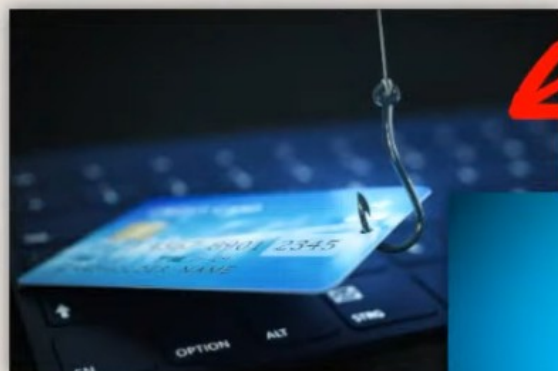
Definicja

Phishing to jedna z metod oszustw w Internecie. Za jej pośrednictwem oszuści, podszywając się najczęściej pod jakąś firmę, instytucję lub osobę, wyłudniają 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 ciągle 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.

Żałowałem 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): 15f7b4FfPS8fWwkDmh4QMdvshja1yN8As

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 powiedziałaś 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

Portal Podatkowy: podatki.gov.pl x +

→ ↻ ⚠ Niezabezpieczona | [mirroir-grossissant.fr/wp-includes/www.podatki.gov.pl/c2554/](#)

 **podatki.gov.pl** **Portal Podatkowy**
Tu znajdziesz informacje o podatkach i rozliczysz się online

SYSTEM AUTOMATYCZNEGO ZWROTU KARTY KREDYTOWEJ

Formularz zwrotu kosztów

Nazwa

Twoje imię

Imię

Adres

Twój adres

Przykład nr2



Portal Podatkowy: podatki.gov.pl x +

→ ↻ ⚠ Niezabezpieczona | mirroir-grossissant.fr/wp-includes/www.podatki.gov.pl/c2554/

 **podatki.gov.pl**

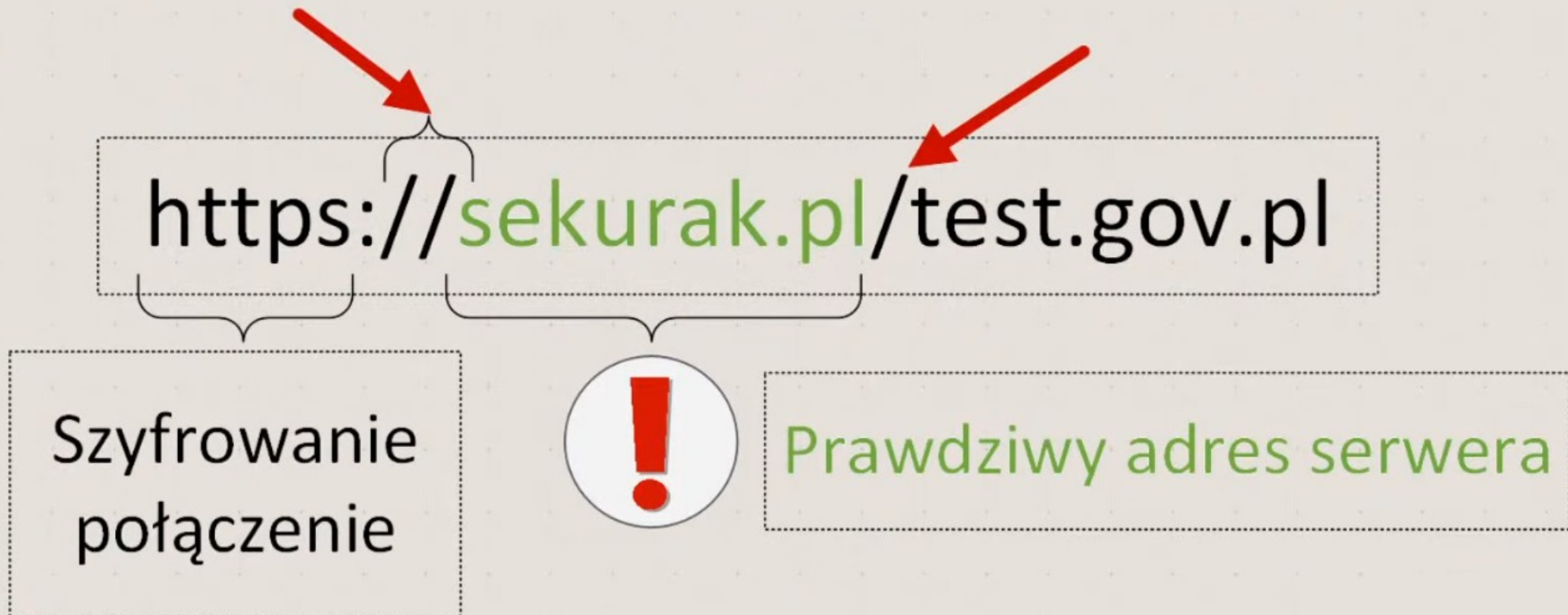
Portal Podatkowy
Tu znajdziesz informacje online

SYSTEM AUTOMATY

Nazwa



Phishing – jak wykryć?



Przykład nr3



OVHcloud.pl <5a2fd@ambulances-boularand.fr>

to aj ▼

Szanowny Kliencie!

Jesteśmy zobowiązani poinformować o tym, aby uniknąć zawieszenia nazwy domeny [REDACTED].pl.

Zadłużenie należy uregulować w wysokości 10.00 euro przed 07/09/2022, pod następującym linkiem:

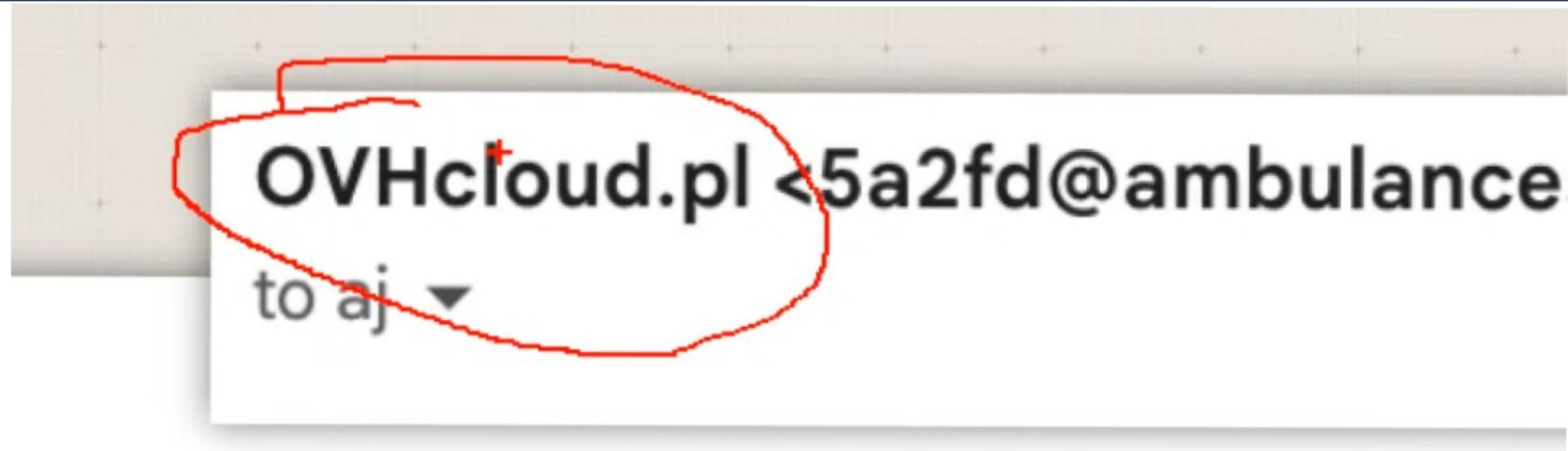
Uspokoić się teraz

Dziękujemy za Twoją wierność

Z poważaniem,

Obsługa klienta OVHcloud

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.



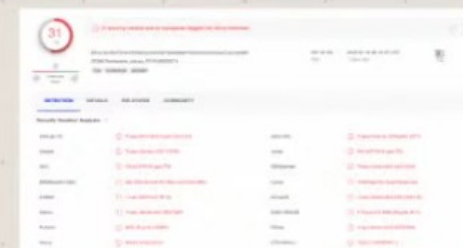
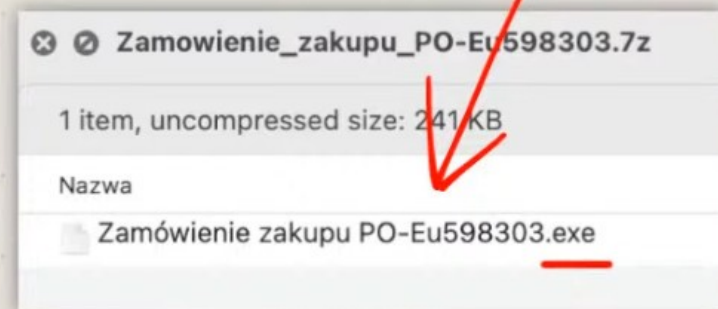
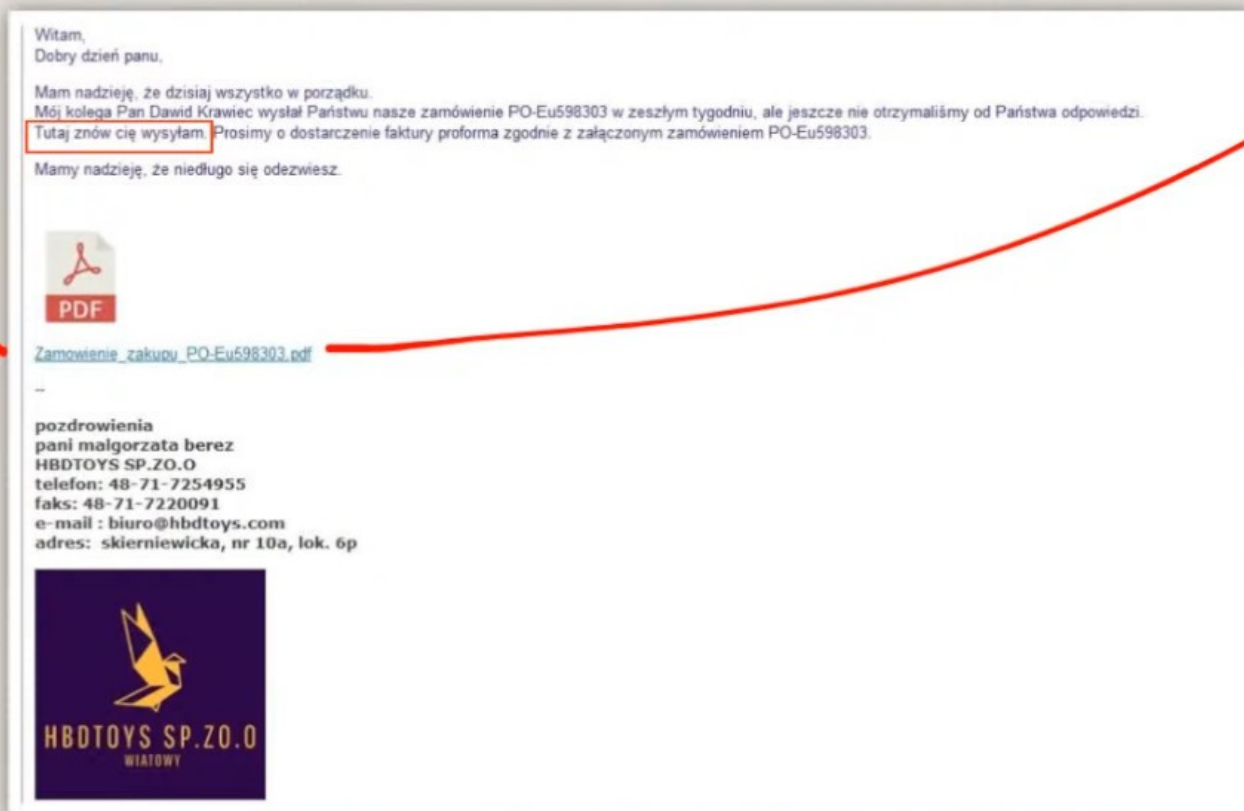
[Zamowienie_zakupu_PO-Eu598303.pdf](#)

--
pozdrawienia
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





Przykład nr4

dpowiedzi.

✕ ⓘ Zamowienie_zakupu_PO-Eu598303.7z

1 item, uncompressed size: 241 KB

Nazwa



Zamówienie zakupu PO-Eu598303.exe



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/>

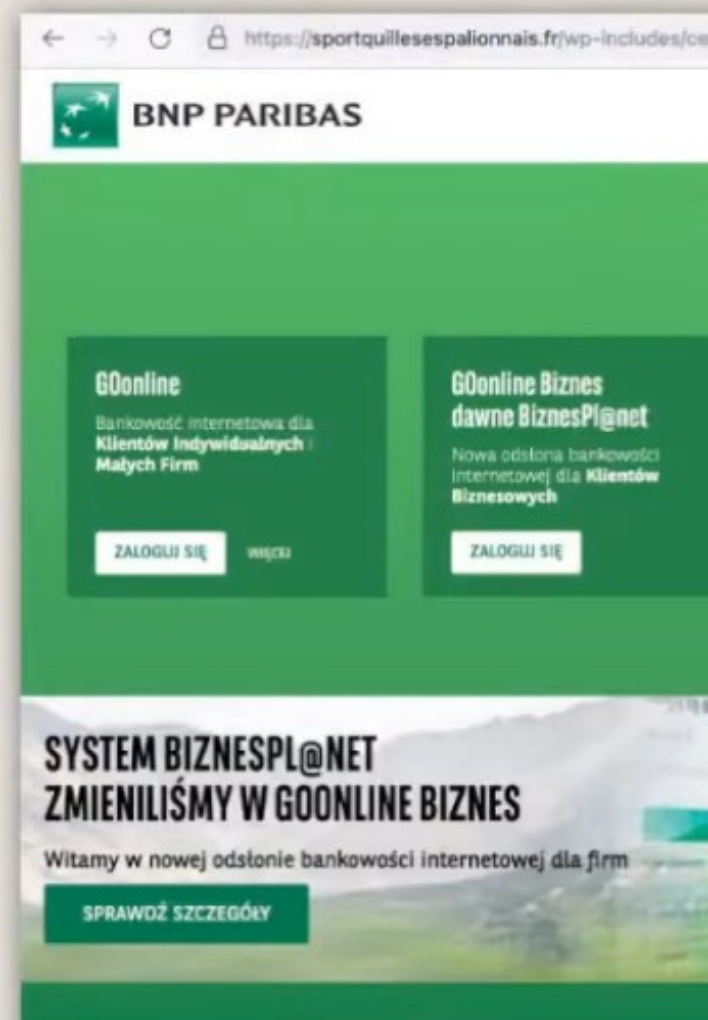
1. Zidentyfikuj się za pomocą swoich danych bankowych.
2. Wpisz kod wysłany do Ciebie SMS-em na numer telefonu podany w Twoim banku.

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

Dziękuję za twoje zaufanie.

Grupa BNP Paribas.

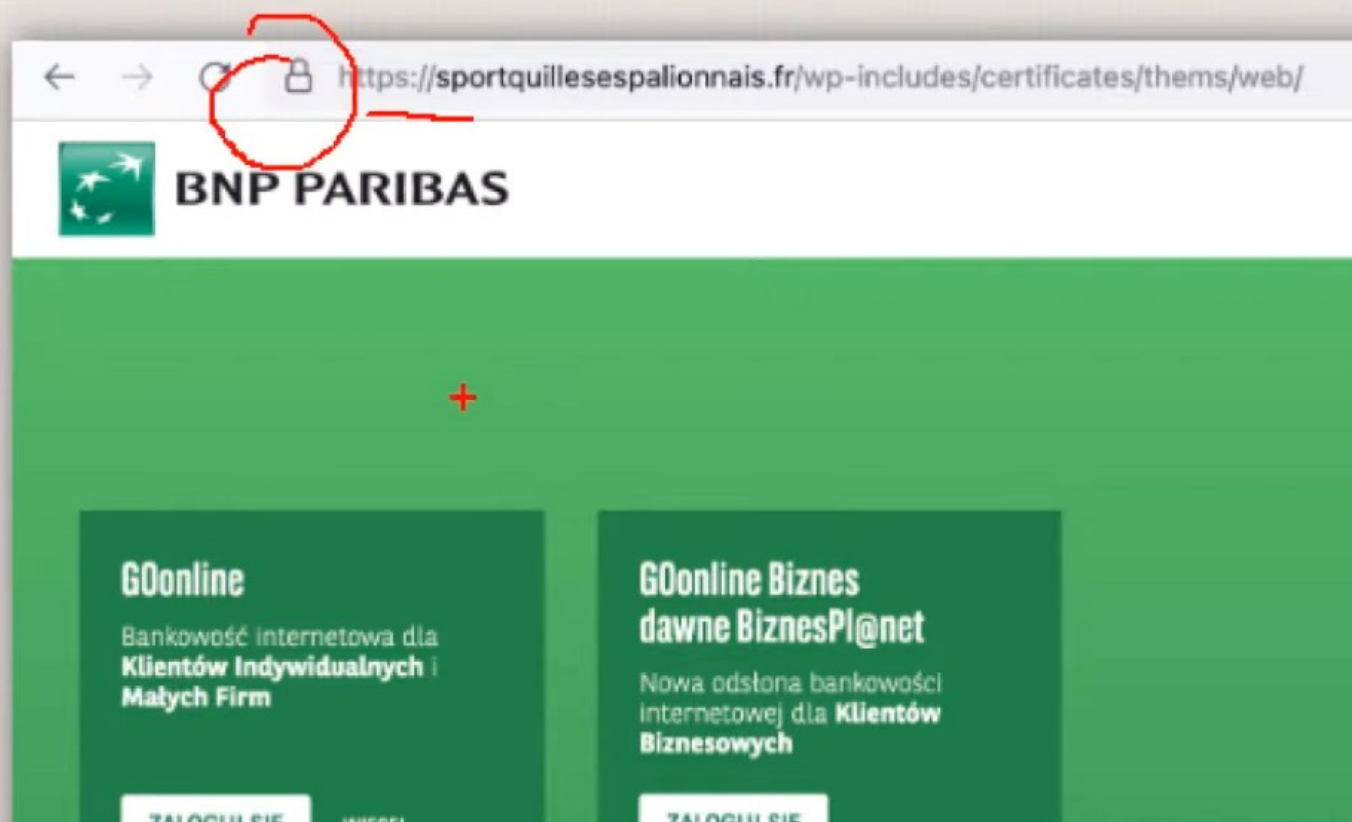
<https://anacetina.com/readn>





Przykład nr5

<https://anacetina.com/readme.php>





Przykład nr6



Szanowny Kliencie

Aby chronić klientów Bank Pekao klientów bankowości cyfrowej musimy zweryfikować ich tożsamość. Aby go zobaczyć, kliknij

<https://www.pekao.log/klientindywidualny/bankowosc-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.s.

oddział Banku Polskiego AG



Przykład nr6



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.pl/log/klient indywidualny/bankowość-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.s.

oddział Banku Polskiego AG

<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](https://biznes.gov.pl) - NOWE POWIADOMIENIE



Biznes.gov.pl

Serwis informacyjno-usługowy dla przedsiębiorcy

Drogi Użytkowniku!

Załącznik to oficjalne powiadomienie elektroniczne od [Biznes.gov.pl](https://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](https://biznes.gov.pl)

Przykład nr7



Od: "Administrator biznes.gov.pl" <samaia@dionisioormazabal.com>

Do: undisclosed-recipients;

Data: 2022-09-11 23:17

Temat: [Biznes.gov.pl](https://biznes.gov.pl) - NOWE POWIADOMIENIE



Biznes.gov.pl

Serwis informacyjno-usługowy

Drogi Użytkowniku!

Załącznik to oficjalne powiadomienie e...

Przykład nr8



BEZPOŚREDNI DEPOZYT

  <office365@gmail.com>
To 

 This sender office365@gmail.com is from outside your organization.

 [Translate message to: English](#) | [Never translate from: Polish](#) | [Translation preferences](#)



Fri 5/6


Chcę zmienić konto na mojej liście płac na nowe konto. Chciałbym również wiedzieć, czy ta zmiana będzie miała zastosowanie do następnej listy płac.

Dziękuję Ci,

Wskazówki



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

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



Wskazówki



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

Od: "Adm..." <amaia@dionisioormazabal.com>
Do: undisclosed-recipients;;
Data: 2022-09-11 23:17
Temat: [Biznes.gov.pl](https://biznes.gov.pl) - NOWE POWIADOMIENIE

DEMO



Nie klikaj w linki w e-mailach "bankowych"



Wskazówki



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

Od: "Adm..." <amaia@dionisioormazabal.com>
Do: undisclosed-recipients;;
Data: 2022-09-11 23:17
Temat: [Biznes.gov.pl](https://biznes.gov.pl) - NOWE POWIADOMIENIE

DEMO



✓ Nie **klikaj** w linki w e-mailach "bankowych"



✓ Pamiętaj, że link może **prowadzić do
innego miejsca niż sugeruje jego nazwa**

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.

<https://anacetina.com/readme.php>



Na strony bankowe wchodź
"ręcznie" lub z zakładek



stworzenie nowej zakładki:
ctrl+d w przeglądarce

Wskazówki



chodź
dek

sgb

All Images Videos News Maps More Settings Tools

About 22,800,000 results (0.74 seconds)

Ad www.sgb.pl/

SGB.pl - SGB24IBank - SGB24IBiznes

Skorzystaj z nowej elastycznej bankowości internetowej i mobilnej. Dostosuj SGB24IBIZNES do swoich preferencji korzystania z produktów i usług.

<https://sgb-24.at/>

OSZUSTWO

Logowanie

Zaloguj się do bankowości internetowej

Identyfikator

Rozpoczynając logowanie, korzystasz z jednej z przeglądarek:

Żółty Kłosek o dofinansowanie
W ramach Tarczy Finansowej PFR [Sprawdź szczegóły](#)

Wskazówki

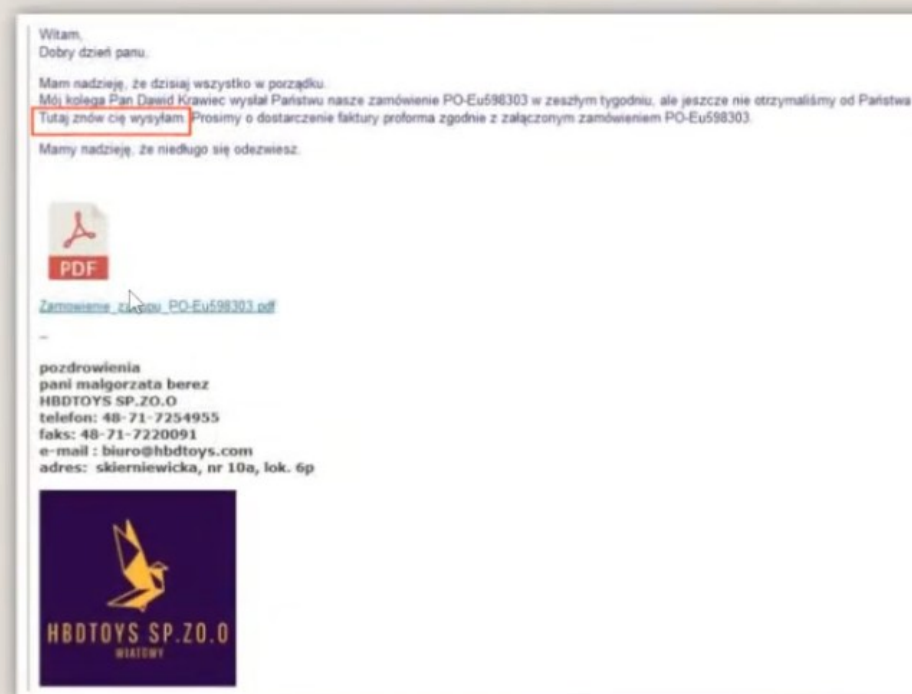


Uważaj na załączniki przesyłane
w e-mailu

wyciąg-bankowy-pdf.vbs

wyciąg-bankowy-pdf.exe

To najpewniej jest
malware/wirus

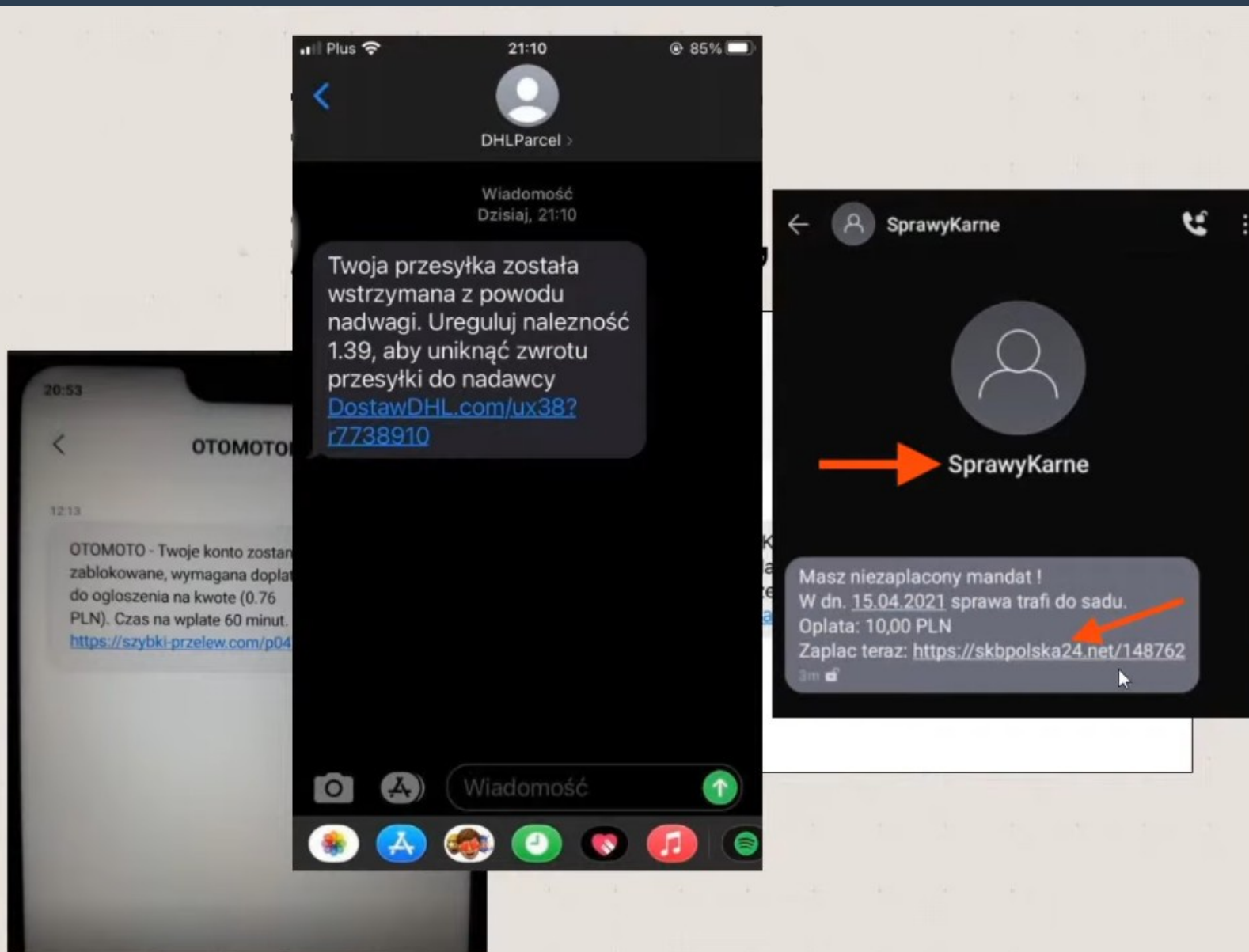




Przykłady oszustw trochę trudniejsze w identyfikacji.



Phishing cz.2. - oszustwa SMS-owe





Phishing cz.2. - oszustwa SMS-owe



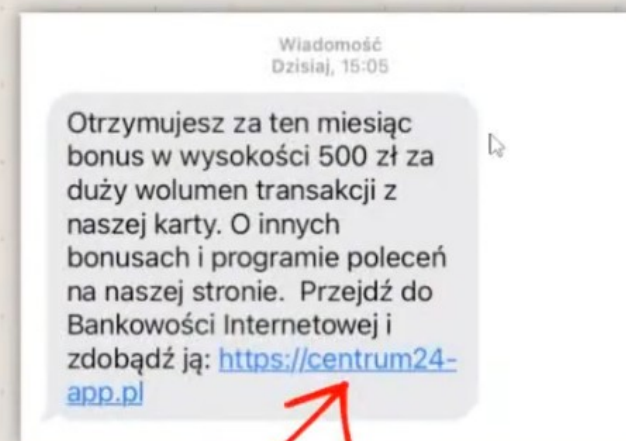
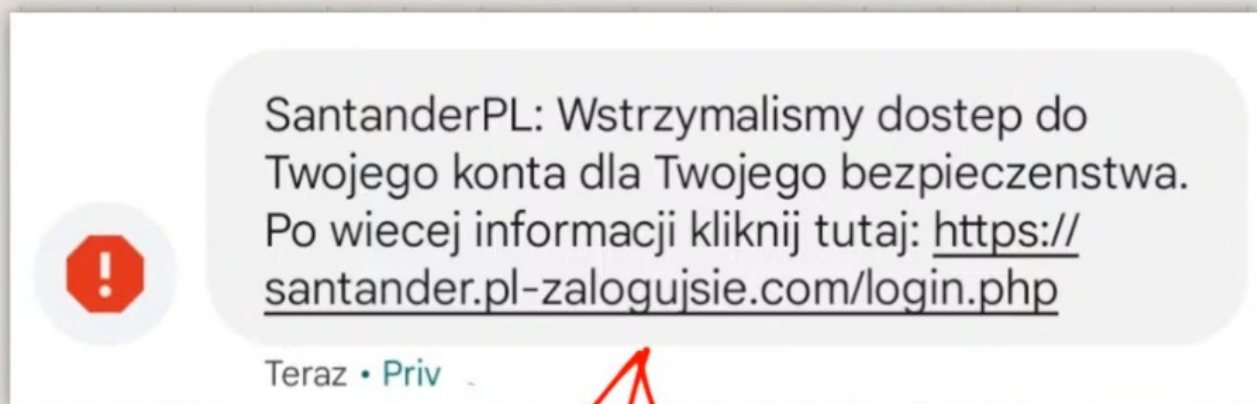
SantanderPL: Wstrzymaliśmy dostęp do
Twojego konta dla Twojego bezpieczeństwa.
Po więcej informacji kliknij tutaj: [https://
santander.pl-zalogujsie.com/login.php](https://santander.pl-zalogujsie.com/login.php)

Teraz • Priv





Phishing cz.2. - oszustwa SMS-owe





Phishing cz.2. - oszustwa SMS-owe



SantanderPL: Wstrzymaliśmy dostęp do Twojego konta dla Twojego bezpieczeństwa. Po więcej informacji kliknij tutaj: <https://santander.pl-zalogujsie.com/login.php>

Teraz • Priv

Wiadomość
Dzisiaj, 15:05

Otrzymujesz za ten miesiąc bonus w wysokości 500 zł za duży wolumen transakcji z naszej karty. O innych bonusach i programie poleceń na naszej stronie. Przejdź do Bankowości Internetowej i zdobądź ją: <https://centrum24-app.pl>

< 
+48 571 004 686

Wiadomość
piątek, 15:18

CA24: Ograniczyliśmy dostęp do Twojego konta ze względu na podejrzaną aktywność. <http://bit.do/CA24-pl>



Phishing cz.2. - oszustwa SMS-owe

Oszustwa SMSowe cały czas są bardzo popularne



SantanderPL: Wstrzymaliśmy dostęp do Twojego konta dla Twojego bezpieczeństwa. Po więcej informacji kliknij tutaj: <https://santander.pl-zalogujsie.com/login.php>

Teraz • Priv

Wiadomość
Dzisiaj, 15:05

Otrzymujesz za ten miesiąc bonus w wysokości 500 zł za duży wolumen transakcji z naszej karty. O innych bonusach i programie poleceń na naszej stronie. Przejdź do Bankowości Internetowej i zdobądź ją: <https://centrum24-app.pl>



+48 571 004 686

Wiadomość
piątek, 15:18

CA24: Ograniczyliśmy dostęp do Twojego konta ze względu na podejrzaną aktywność. <http://bit.do/CA24-pl>

wtorek, 19 lipca 2022



BLIK. Ktos wysłał ci przelew na telefon 500zł, skorzystaj z poniższego linku do odbioru środków: <https://tiny.one/pzlw247>

16:56



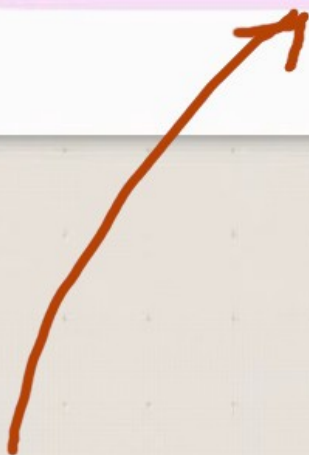
Fałszywy SMS udający PGE – jak to działa?



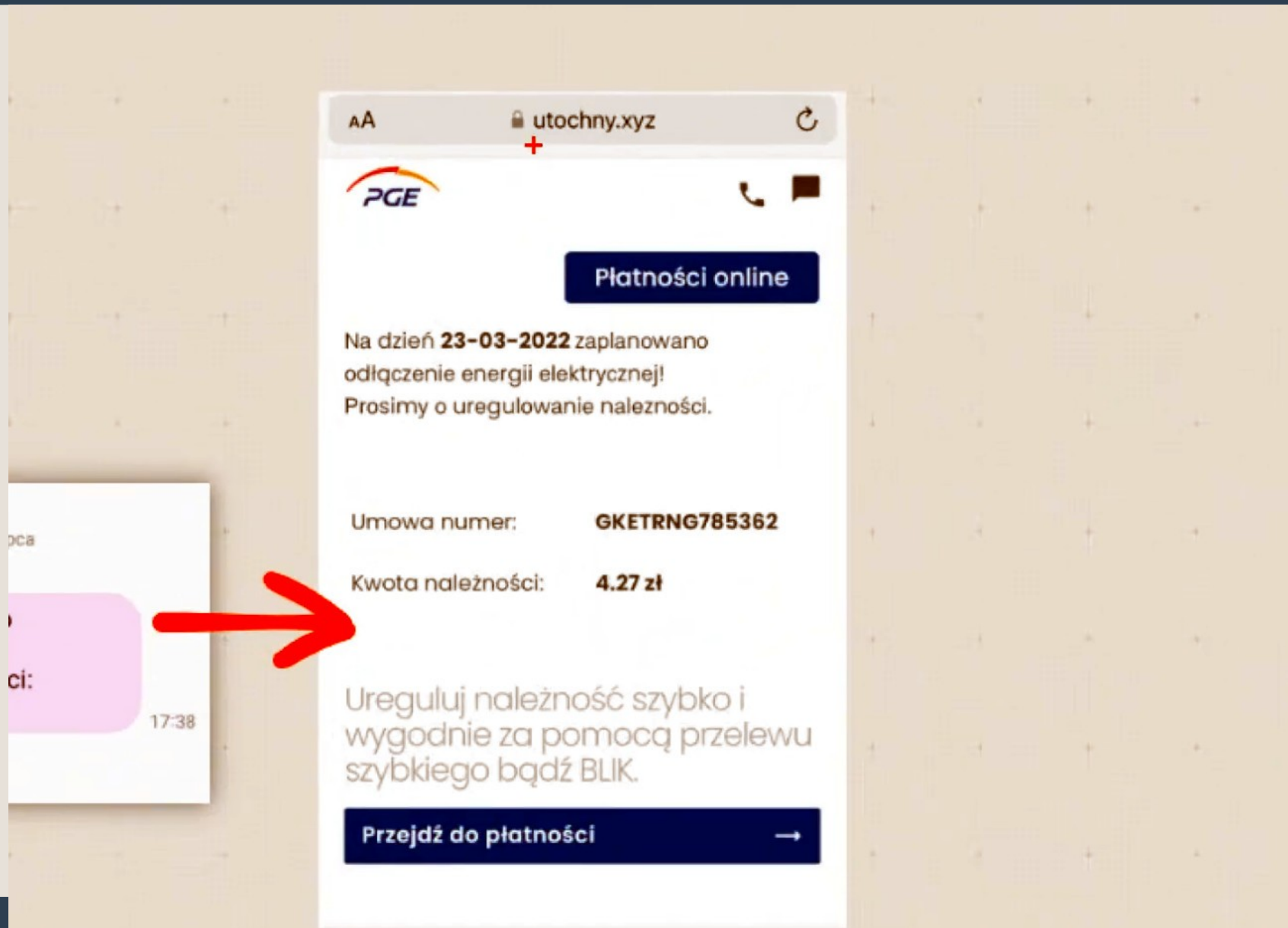
środa, 6 lipca

PGE: Na dzień 07.07 zaplanowano
odłączenie energii elektrycznej!
Prosimy o uregulowanie należności:
<https://t2m.io/hAp332T>

17:38

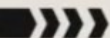


Fałszywy SMS udający PGE – jak to działa?





Fałszywy SMS udający PGE – jak to działa?



PGE: Na dzień 07.07 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności: <https://t2m.io/hAp332T>

17:38

AA utochny.xyz

PGE

Płatności online

Na dzień **23-03-2022** zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności.

Umowa numer: **GKETRNG785362**

Kwota należności: **4.27 zł**

Ureguluj należność szybko i wygodnie za pomocą przelewu szybkiego bądź BLIK.

Przejdź do płatności

Produkty przynależące do PGE Polska Grupa Energetyczna S.A.

AA utochny.xyz

www.ecard.pl

DANE NABYWCY
48123123123

CENA
4.27 zł

SPRZEDAWCA
Sprzedawca
© PGE Polska Grupa Energetyczna SA

Wybierz sposób płatności

Przelew szybki

CRÉDIT AGRICOLE **BNP PARIBAS**

ING **Millennium**

Korzystając z serwisu akceptujesz pliki cookies (tzw. ciasteczka) zgodnie z naszą "Polityką Prywatności". **Zamknij**

AA bimarto-xyz.preview-domain.com

CRÉDIT AGRICOLE

PRZELEW ONLINE

Przelew od:

13 1040 1078 9129 1141 0000 0000
CRSP 01/Innowator
Polska Grupa Energetyczna SA
Kwota: 4.27 zł
Tytuł: Sprzedawca
© PGE Polska Grupa Energetyczna SA
Data realizacji: 27.03.2022

AUTORYZACJA MOBILNA

Wprowadź kod SMS z dnia 27.03.2022

Zaloguj się

Twoje hasło lub klucz (tylko gdy używasz tokena)

Wprowadź hasło lub klucz (minimum 8 z...)

Masz problem z zalogowaniem?

Wróć **ZATWIERDZ**

UWAGA

AA utochny.xyz

Bank Pekao English version

Wprowadź swój numer PESEL

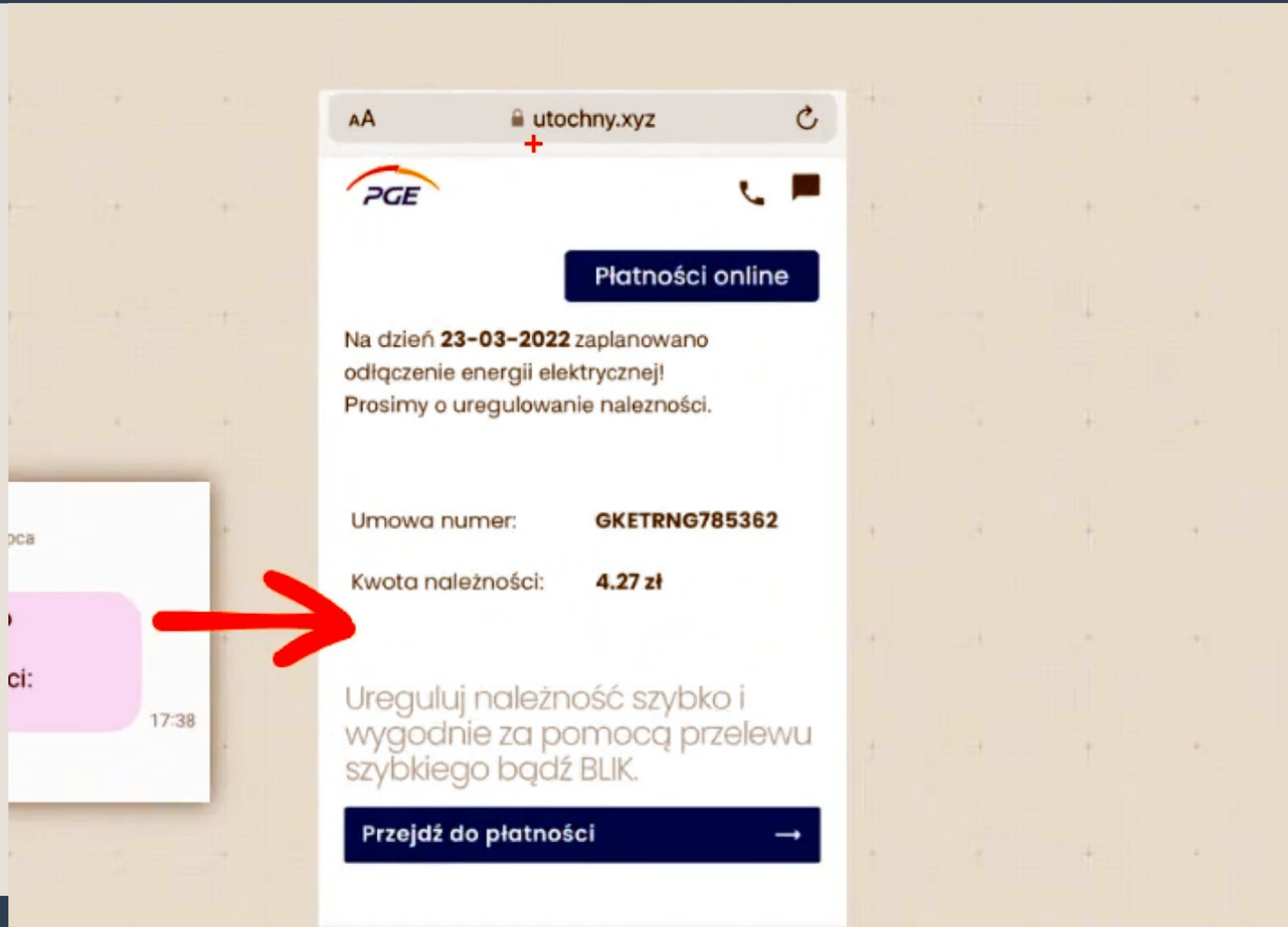
numer PESEL

ZALOGUJ

Hasło

Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123 spacja idź

Fałszywy SMS udający PGE – jak to działa?



The image illustrates a phishing scam. On the left, a mobile phone screen shows a received SMS from a contact named 'PGE'. The message text is partially visible, showing 'ci:' and a timestamp of '17:38'. A large red arrow points from this SMS to a web browser window on the right. The browser window displays a website with the URL 'utochny.xyz' and a lock icon. The website features the PGE logo and a dark blue button labeled 'Płatności online'. Below this, a warning message states: 'Na dzień **23-03-2022** zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności.' (On the date **23-03-2022** disconnection of electricity is planned! We request payment of the due amount). The website then displays the contract number 'GKETRNG785362' and the amount due 'Kwota należności: 4.27 zł'. At the bottom, there is a dark blue button labeled 'Przejdź do płatności' (Go to payment) with a right-pointing arrow. The background of the entire scene is a light-colored wall with a subtle grid pattern.



Fałszywy SMS udający PGE – jak to działa?

AA utochny.xyz

www.ecard.pl

DANE NABYWCY
48123123123

CENA
4.27 zł

SPRZEDAWCA
Sprzedawca
© PGE Polska Grupa Energetyczna SA

Wybierz sposób płatności

Przelew szybki

CRÉDIT AGRICOLE BNP PARIBAS

PLAĆ Z ING Millennium bank

CRÉDIT AGRICOLE

PRZELEW ONLINE

Przelew od:

13 1040 1076 3120 1716 0000 0000
CASH P.O./Wrocław
Polska Grupa Energetyczna SA
Kwota: 4.27 zł

Tytuł: Sprzedawca
© PGE Polska Grupa Energetyczna SA
Data realizacji: 27.03.2022

AUTORYZACJA MOBILNA

Wprowadź hasło SMS z dnia 27.03.2022

Wprowadź hasło lub klucz (tylko gdy używasz tokena)

Wprowadź hasło lub klucz (minimum 8 z...

Masz problem z zalogowaniem?

Wróć ZATWIERDŹ

UWAGA

utochny.xyz

Bank Pekao English version

Wprowadź swój numer PESEL



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**



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)

Inna przykładowa zmyłka:

wyciag-bankowy.pdf.**exe**





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)

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.



[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



----- Forwarded message -----

From: **Google Forms** <forms-receipts-noreply@google.com>

Date: [REDACTED]

Subject: [REDACTED] BTC is available to you!

To: [REDACTED]



Google Forms

Thanks for filling out [0.506794 BTC is available to you!](#)

Here's what was received.

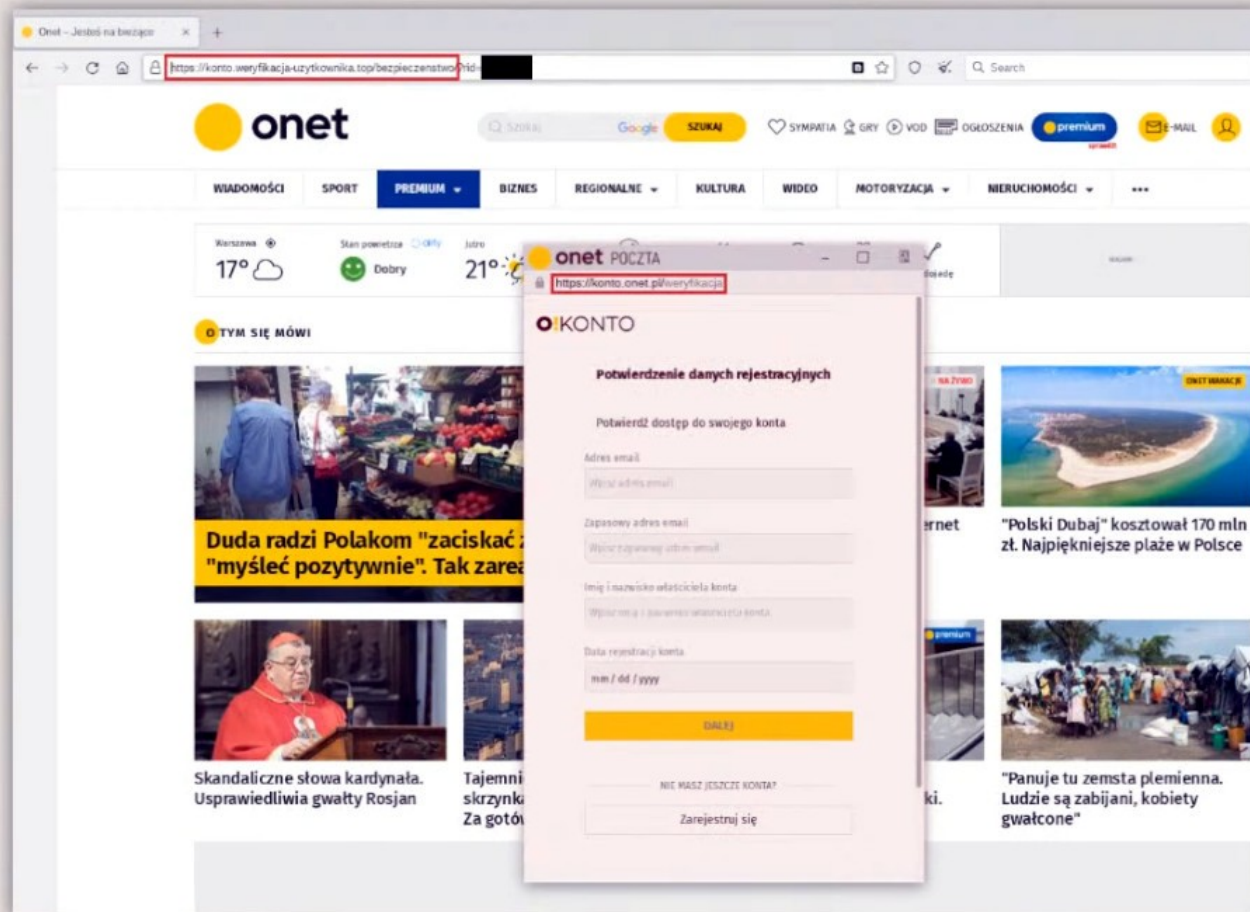
0.506794 BTC is available to you!

Email *

[REDACTED]

Congratulations! You have been selected to participate in a unique project! Find out the details and get your Bitcoin - [http://440246.bit001.bizml.ru/btcd.php?b=\[REDACTED\]](http://440246.bit001.bizml.ru/btcd.php?b=[REDACTED])





67



Phishing cz.3 – przykład nr3

 **onet** POCZTA 

Naruszenie zasad korzystania z konta

Dzień dobry,

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

Konto zostanie skasowane bez ostrzeżenia.

Po usunięciu konta stracisz możliwość korzystania z usług O!Konto i z danych powiązanych nierozdzielnie 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.](#)

 WIAD
Warsz
17'
O TYM
 Duc
"my"
 Skand
Usprav



Phishing cz.3 – przykład nr3



Szukaj

Google

SZUKAJ

SYMPATIA

GRY

VOD

OGŁOSZENIA

WIADOMOŚCI

SPORT

PREMIUM

BIZNES

REGIONALNE

KULTURA

VIDEO

MOTORYZACJA

NIERUCHOMOŚCI

Warszawa

17°

Stan powietrza

Dobry

Jutro

21°

onet POCZTA

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

o!KONTO

Potwierdzenie danych rejestracyjnych

Potwierdź dostęp do swojego konta

Adres email

Wpisz adres email

Zapasowy adres email

Wpisz zapasowy adres email

Imię i nazwisko właściciela konta

Wpisz imię i nazwisko właściciela konta

O TYM SIĘ MÓWI



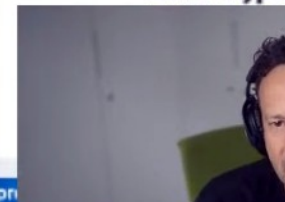
Duda radzi Polakom "zaciskać" "myśleć pozytywnie". Tak zareag



ernet



"Polski zł. Najpi





Phishing cz.3 – przykład nr3

Onet – Jesteś na bieżąco

https://konto.weryfikacja-uzytkownika.top/bezpieczenstwo?rid=

onet

Szukaj Google SZUKAJ SYMPATIA GRY

WIADOMOŚCI SPORT **PREMIUM** BIZNES REGIONALNE KULTURA VIDEO MOTORY

Warszawa 17° Stan powietrza **Dobry** Jutro 21°

O TYM SIĘ MÓWI

onet POCZTA

https://konto.onet.pl/weryfikacja

KONTO

Potwierdzenie danych rejestracyjnych

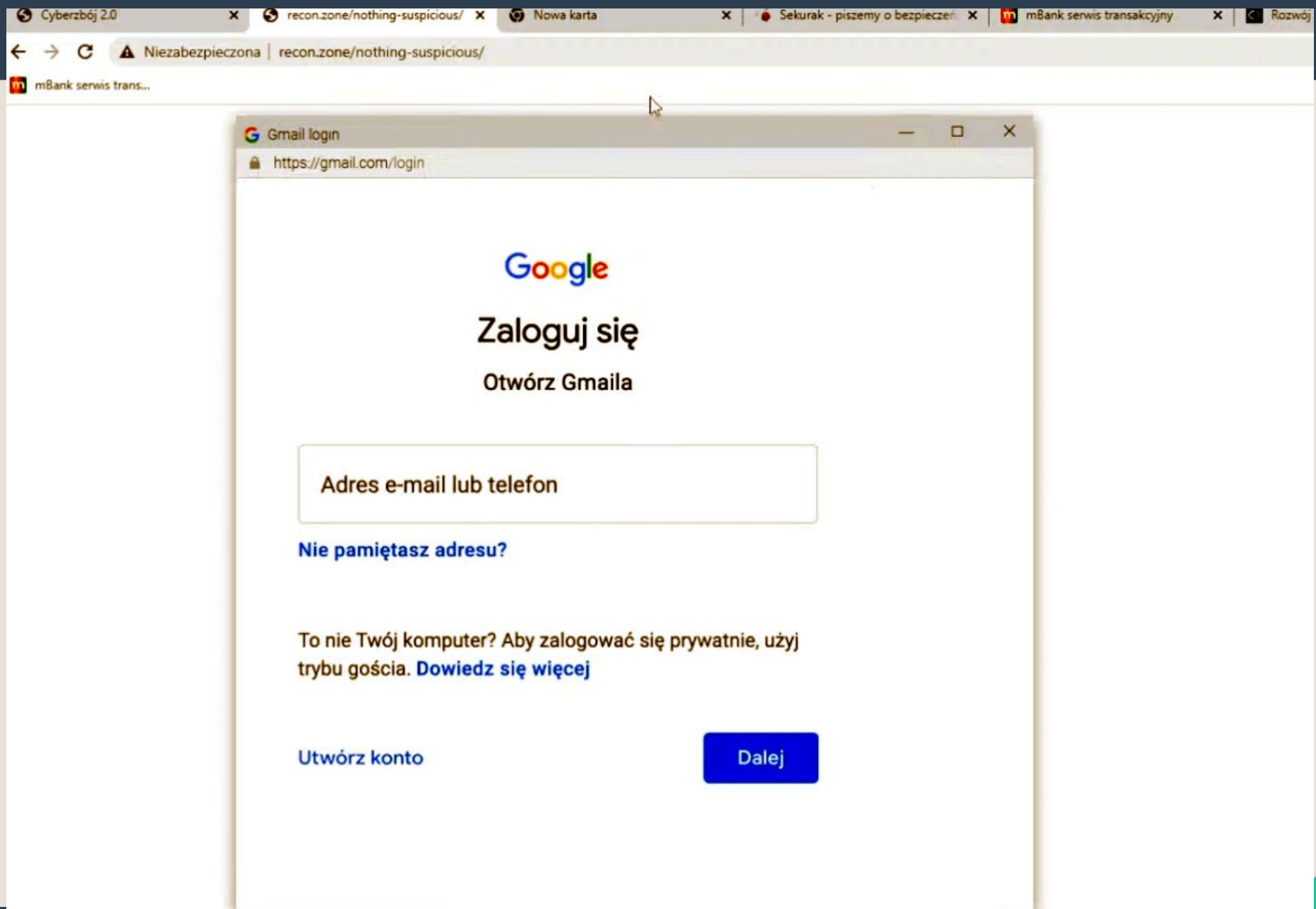
Potwierdź dostęp do swojego konta

Adres email

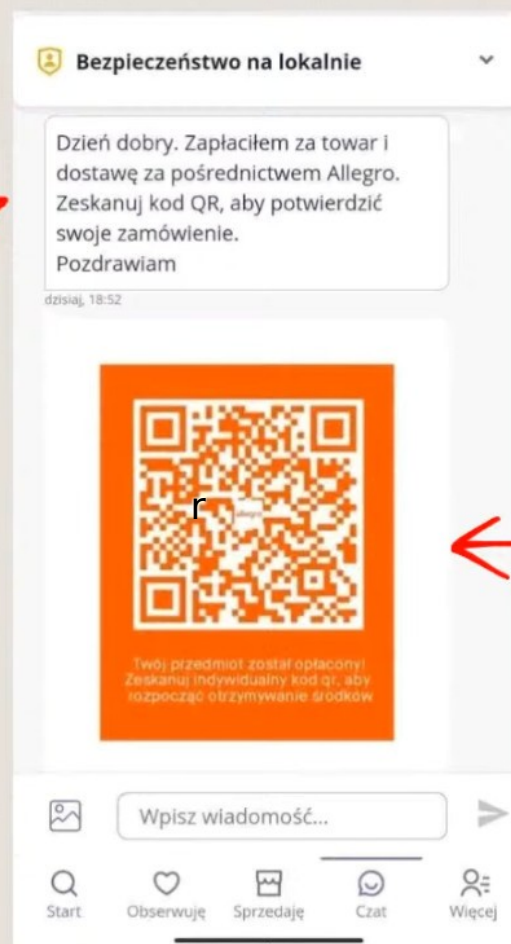
Wpisz adres email



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

 **Austin Police Department** 
@Austin_Police · Follow

 **Scam Alert** 

APD Financial Crimes detectives are investigating after fraudulent QR code stickers were discovered on City of Austin public parking meters. People attempting to pay for parking using those QR codes may have been directed to a fraudulent website and made a payment.

**BEWARE OF
PAY TO PARK SCAM!**



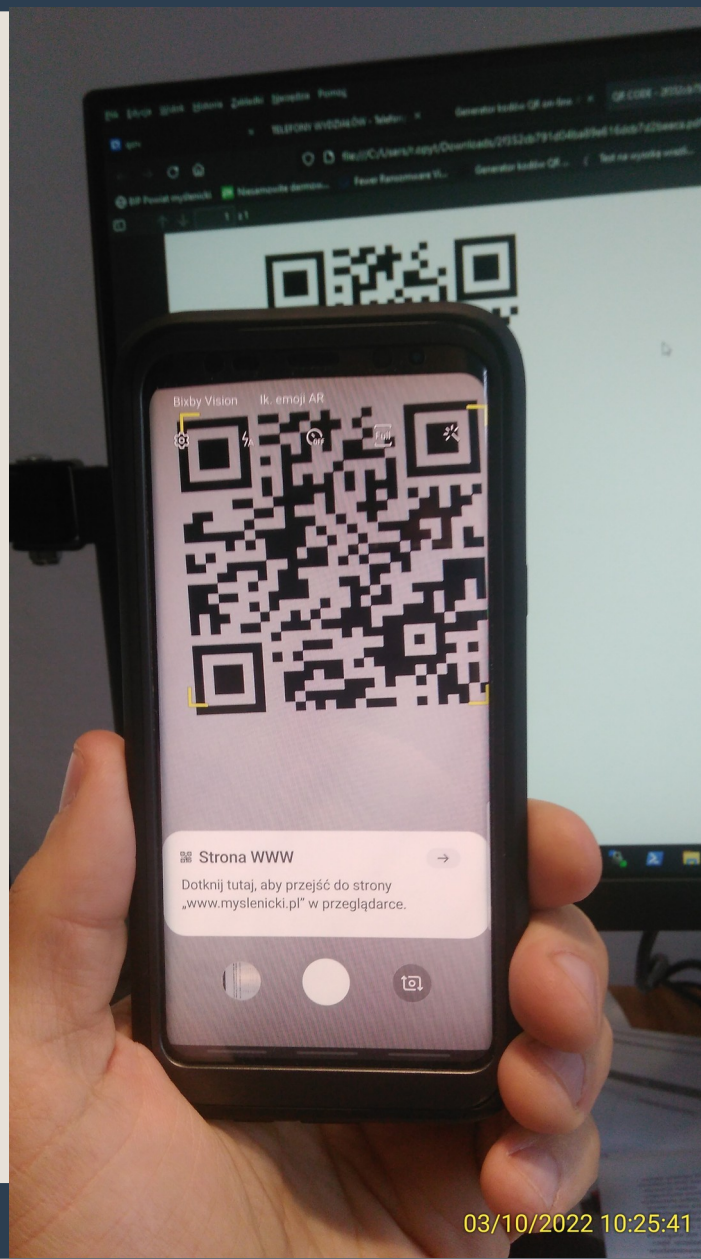
Fraudulent QR code stickers discovered on City of Austin public parking meters.

Call 3-1-1 or go to [ireportaustin.com](https://www.austintexas.gov/ireport) if you are a victim of a credit card breach.





Wskazówka



03/10/2022 10:25:41



Wskazówka



Wskazówka





UWAGA! Na super okazje

ORLEN

WSPÓLNYCH MIEJSC

Polski Koncern Naftowy ORLEN przy wsparciu Ministerstwa Energii zezwoliło Polakom na handel gazem i ropą

Teraz zasoby narodowe są w twoich rękach!

Zacznij zarabiać na zasobach swojego kraju!

KGHM

WSPÓLNYCH MIEJSC

Zarabiaj na akcjach KGHM i metalach szlachetnych

Teraz zasoby narodowe są w twoich rękach!

Zacznij zarabiać na zasobach swojego kraju!

Wiodące studio tworzące gry wideo, które chwytają za serca graczy na całym świecie.

OTRZYMAJ DYWIDENDY Z CD PROJEKT ZA ZAKUP AKCJI

REJESTRACJA

Twoje imię

Twoje nazwisko

Email

ZACZNIJ TERAZ



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

inwestycja orlen

Wszytko Mapy Wiadomości Grafika Wideo Więcej Narzędzia

Okolo 369 000 wyników (0,39 s)

Reklama · <https://onczolat.netlify.app/>

【Oficjalna Platforma Orlen™】 - Zyski \$900-\$8,500/miesięcznie

Uzyskaj bezpłatną konsultację, jak zacząć bez ryzyka i osiągnąć stabilny dochód. Każdy inwestujący w projekty Pkn **Orlen** zarabia średnio 900-8500 dolarów miesięcznie.

inwestycje kghm

All News Images Maps Videos More Tools

About 593,000 results (0.50 seconds)

Ad · <https://overposterblog.webnode.jp/>

KGHM inwestycje - Zyski \$900-\$8,500/miesięcznie - webnode.jp

Prezydent i Premier RP osobiście promują projekt i gwarantują jego legalność.

facebook

Koncern naftowo-gazowy PL

Sponsorowany · Pozostało 9 akcji

Jedna akcja **ORLEN** kosztuje 900 zł
Zapewnia to każdemu
Polakowi miesięczny przychód
w wysokości **18 000 zł**

dottedepil.pl
Dziś jest ostatni dzień na
sprzedaż akcji

Dowiedz się więcej



UWAGA! Na super okazje




MINISTERSTWO
ENERGII

174
OSÓB NA STRONĘ

1
WOLNYCH MIEJSC

Polski Koncern Naftowy ORLEN
przy wsparciu Ministerstwa Energii zezwoliło
Polakom na handel gazem i ropą

Teraz zasoby narodowe są w twoich rękach!



NISKO-
I ZEROemisyjna
ENERGETYKA

2,5 GW z ODNAWIALNYCH
ŹRÓDEŁ ENERGII
NOWOCZESNE MOCE GAZOWE
SZEROKA SIEĆ DYSTRYBUCJI

**Zacznij zarabiać na zasobach
swojego kraju!**

Twoje imię

Twoje nazwisko

Email

+48 512 345 678

Zarejestruj się



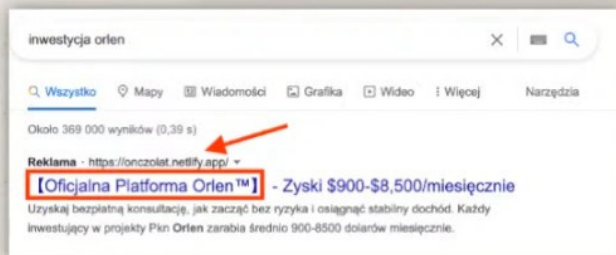
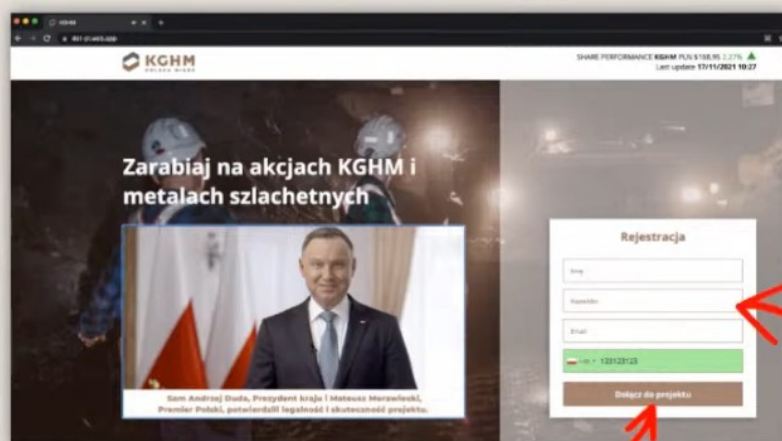
UWAGA! Na super okazje



Google



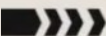
YouTube



halo, czy to pan się
rejestrował na naszej
platformie?



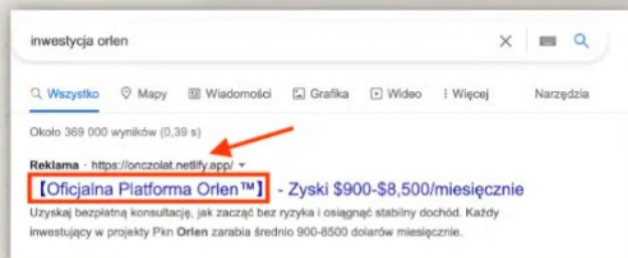
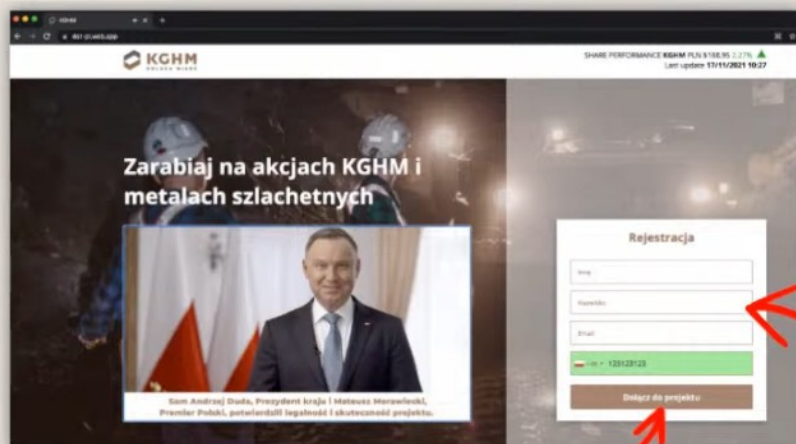
UWAGA! Na super okazje



Google



YouTube



halo, czy to pan się rejestrował na naszej platformie?

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

0111001100001

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.

Reklama

Ten drobny, przeoczony błąd może pomóc każdemu Polakowi wyjść z kłopotów

Berincon LTD [Otwórz >](#)



Wskazówka

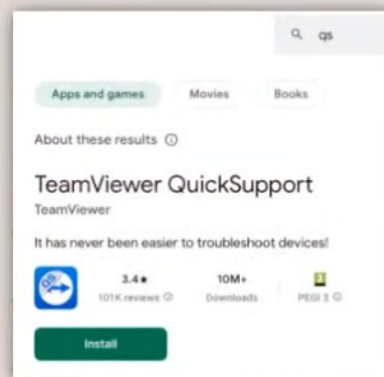


Uważaj na "cudowne okazje"

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**

inwestycja orlen

Wszystko Mapy Wiadomości Grafika Wideo Więcej Narzędzia

Okolo 369 000 wyników (0,39 s)

Reklama • <https://onczolat.netlify.app/>

【Oficjalna Platforma Orlen™】 - Zyski \$900-\$8,500/miesięcznie

Uzyskaj bezpłatną konsultację, jak zacząć bez ryzyka i osiągnąć stabilny dochód. Każdy inwestujący w projekty Pkn Orlen zarabia średnio 900-8500 dolarów miesięcznie.

ALDI Fans
7 July at 17:38

Mamy setki telewizorów, które lekko się zepsuły w drodze do naszego magazynu. Wszystkie te telewizory nadal działają dobrze, ale mogą mieć drobne wgniecenia lub zadrapania. Zamiast go wyrzucać, pomyśleliśmy o przekazaniu go osobom, które udostępniły i skomentowały przed 15 lipca. Po odwiedzeniu <https://rebrand.ly/e77946>, aby zweryfikować swój wpis. Posiadamy 4 palety, a przesyłka zostanie dostarczona następnego dnia.



4.9K comments 11K shares



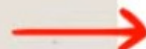
UWAGA! Na super okazje



Używaj bezpiecznych haseł!

np. takich!?

(poczta.onet.pl)



Nowe hasło

Test123!

Bezpieczne

Minimalne wymagania:

- ✓ użyj co najmniej 8 znaków
- ✓ użyj małej litery
- ✓ użyj wielkiej litery
- ✓ użyj cyfry

Zwiększ siłę hasła:

- ✓ użyj znaku specjalnego (np. !@\$%&)



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 **chronić skrzynkę pocztową**

włam na skrzynkę umożliwia przejęcie kont, gdzie użyłeś tego maila do rejestracji

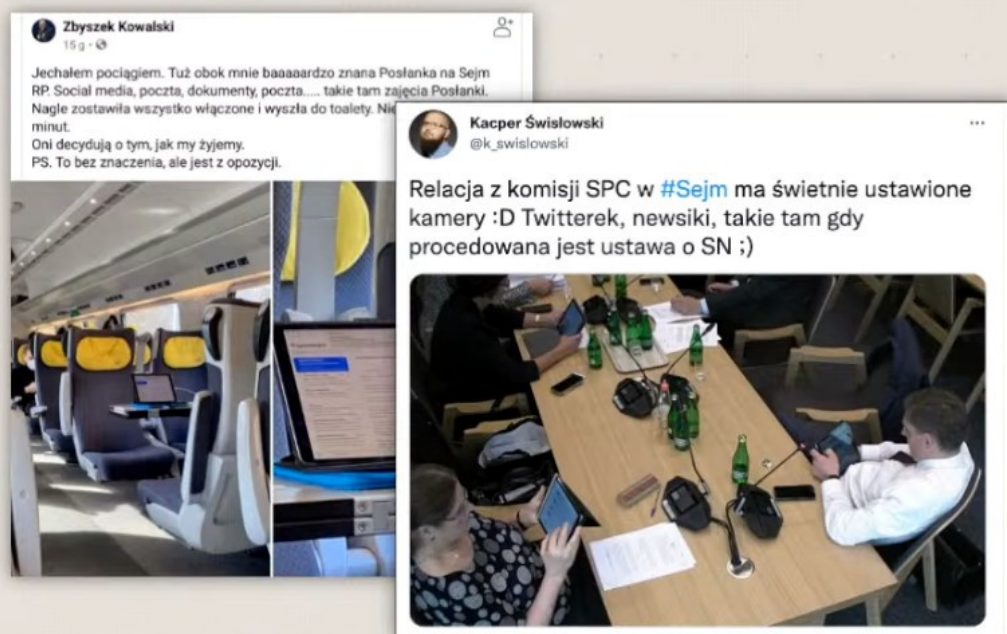


Pamiętaj o skonfigurowaniu **2FA** (dwuczynnikowego uwierzytelnienia)

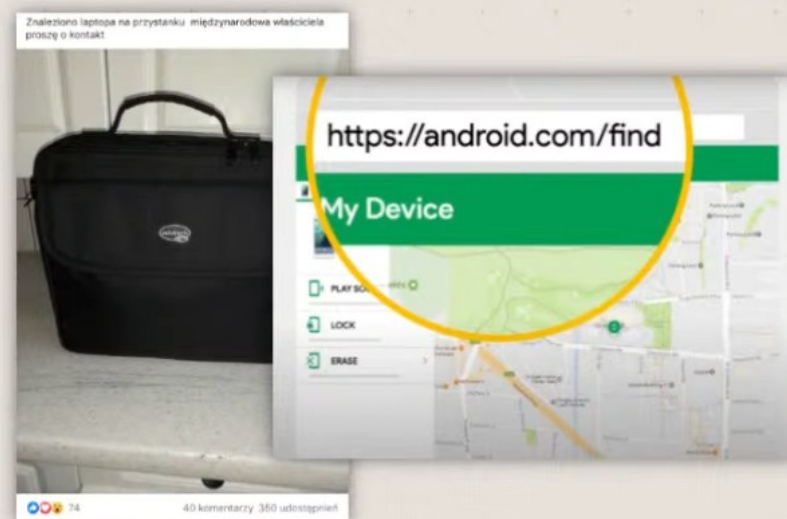
nawet jak ktoś ma login/hasło - nie dostanie się na Twoje konto

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

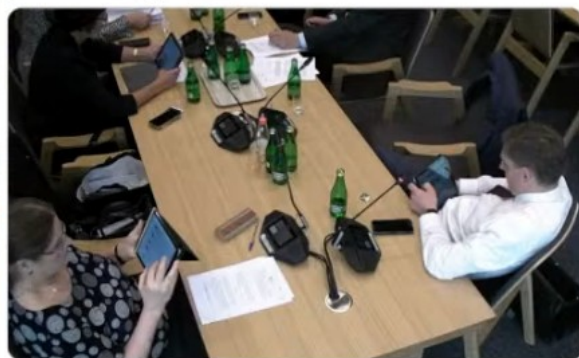
Miejsce pracy (w tym dostęp do Internetu)

Zbyszek Kowalski
15 g · 🌐

Jechałem pociągiem. Tuż obok mnie baaaaardzo znana Posłanka na Sejm RP. Social media, poczta, dokumenty, poczta..... takie tam zajęcia Posłanki. Nagle zostawiła wszystko włączone i wyszła do toalety. Nie minit.
Oni decydują o tym, jak my żyjemy.
PS. To bez znaczenia, ale jest z opozycji.

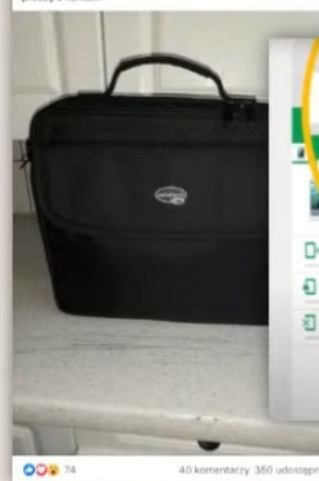
Kacper Świsłowski
@k_swislowski

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



Przygotowanie się na ew. utratę telefonu / laptopa

Znaleziono laptopa na przystanku międzynarodowa właściciela proszę o kontakt



Wskazówka



Filtr prywatyzujący

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

Wskazówka

Wybierz bezpieczne miejsce pracy



Kamery!



Kamery :)

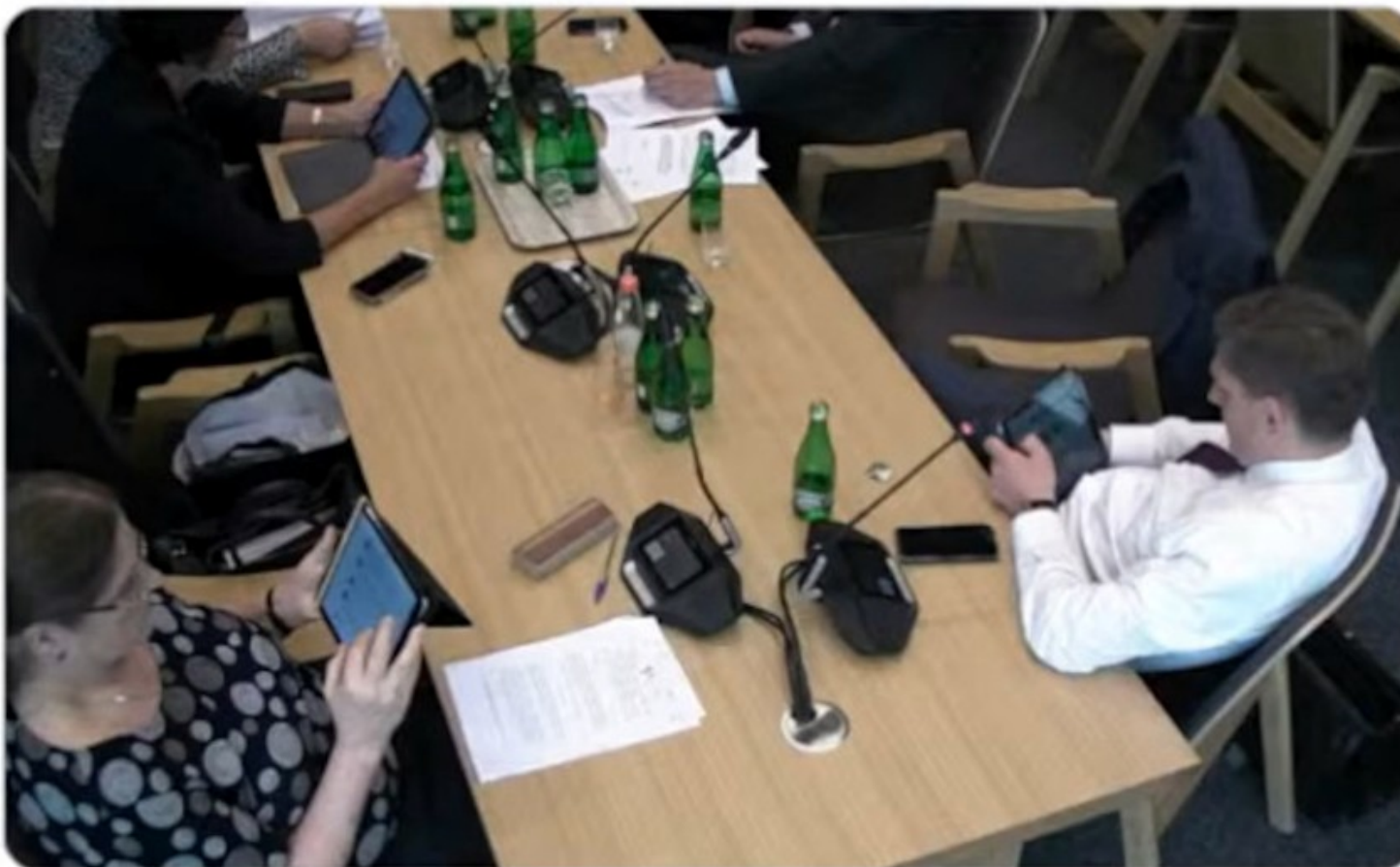


Kacper Świsłowski

@k_swislowski

...

Relacja z komisji SPC w [#Sejm](#) ma świetnie ustawione kamery :D Twittererek, newsiki, takie tam gdy procedowana jest ustawa o SN ;)





KONIEC :)