



**KNF**

**CEDUR**  
Centrum Edukacji dla  
Uczestników Rynku

## **Na co uważać i jak nie dać się okraść w Internecie – bankowość elektroniczna dla seniorów. I edycja**

**Agata Ślusarek**

Departament Cyberbezpieczeństwa  
Urząd Komisji Nadzoru Finansowego  
24 kwietnia 2024 roku



# „Na co uważać i jak nie dać się okraść w Internecie – bankowość elektroniczna dla seniorów. I edycja”

## Agenda

- Przestępstwa w Internecie: co chcą ukraść cyberprzestępcy, gdzie oszukują i jakie metody stosują
- Cyberhigiena: jak rozpoznać fałszywą stronę, czy w Internecie można być anonimowym, dobre praktyki korzystania z urządzeń elektronicznych

Materiały szkoleniowe przygotowane zostały w ramach projektu Centrum Edukacji dla Uczestników Rynku – CEDUR. Autorskie prawa majątkowe do prezentowanych oraz przekazywanych materiałów są własnością Urzędu Komisji Nadzoru Finansowego (UKNF). Rozpowszechnianie, kopiowanie, utrwalanie, publiczne wykorzystywanie całości lub części dozwolone jest jedynie w celach niekomercyjnych, nieodpłatnie, za zgodą UKNF, pod warunkiem podania informacji o pochodzeniu materiałów. Stan prawny informacji zawartych w materiałach jest aktualny na dzień wygłoszenia prezentacji. Materiały przeznaczone są wyłącznie dla odbiorców określonych w programie seminarium, dostępnym na stronie [www.knf.gov.pl](http://www.knf.gov.pl). Prezentowane treści mają wyłącznie charakter ogólny i informacyjny, i nie stanowią ani porady prawnej, ani inwestycyjnej. UKNF nie ponosi odpowiedzialności za jakiegokolwiek decyzje podjęte przez odbiorców prezentacji w sprawach ich dotyczących lub za decyzje inwestycyjne podejmowane na rynku finansowym, w oparciu o informacje przekazane w prezentacji, ponieważ decyzje te powinny być każdorazowo przeanalizowane w ramach konkretnego stanu faktycznego, który w zależności od okoliczności, podmiotu, który decyzje podejmuje, potrzeb, założonych celów oraz posiadanych środków będzie uzasadniał zastosowanie adekwatnych działań, w tym przyjęcie konkretnego ryzyka, w celu osiągnięcia oczekiwanych skutków, które decyzja ma wywołać. W indywidualnych przypadkach należy skontaktować się z Urzędem Komisji Nadzoru Finansowego.

# URZĄD KOMISJI NADZORU FINANSOWEGO



# DEPARTAMENT CYBERBEZPIECZEŃSTWA





# Dlaczego robimy, to co robimy?

## Liczne zadania, m.in.:

- obsługa incydentów bezpieczeństwa,
- analizy grup przestępczych pod kątem zagrożenia dla ciągłości działania podmiotów sektora finansowego oraz klientów,
- prewencja działań przestępczych,
- współpraca z CSIRT MON, CSIRT GOV, CSIRT NASK,
- informowanie o bieżących zagrożeniach...

🏠 > Ministerstwo Cyfryzacji > Co robimy > Cyberbezpieczeństwo > Krajowy system cyberbezpieczeństwa

< Powrót

## Krajowy system cyberbezpieczeństwa

> Najczęściej zadawane pytania

> Akty prawne

> Operatorzy usług kluczowych

> Dostawcy usług cyfrowych

> Podmioty publiczne

> Organy właściwe

> Zespół Reagowania na Incydenty  
> Bezpieczeństwa Komputerowego (CSIRT)



# Przestępstwa w Internecie

1. Jakich metod używają przestępcy
2. Jak najczęściej oszukują
3. Które informacje chcą ukraść

# 1/3 Przestępstwa w Internecie: sztuczki przestępców

■ **Socjotechnika** - każde działania wpływające na inną osobę w celu **nakłonienia jej do podjęcia działań**, które może być niezgodne z osobistym interesem tej osoby

■ **Phishing** - rodzaj cyberataku, podczas którego cyberprzestępca próbuje **wyłudzić od ofiary poufne informacje**







# Dlaczego ataki socjotechniczne są skuteczne?

**„NAJSŁABSZYM OGNIWEM JEST CZŁOWIEK”**

- niedostateczna czujność
- braki szkoleniowe / brak świadomości
- poczucie bezpieczeństwa
- przyzwyczajenia, nawyki
- przeświadczenia, że mnie to nie dotyczy

## 2/3 Przestępstwa w Internecie: jak oszukują...

### Jak możemy zostać „zaatakowani”?

#### ■ wiadomości SMS

Millenium : od 12.03.2024 nie  
będziesz mógł korzystać ze swojego  
konta. Do czasu aktywacji nowej  
aktualizacji aktywuj ja teraz :  
Millenium-pl.com



Poczta Polska - Pamiętaj,  
że Twoja paczka nie mogła  
zostać wysłana z powodu  
nieprawidłowego adresu

wysyłki. Kliknij: [https://  
www.post-tel-me.top/](https://www.post-tel-me.top/),

aby zaktualizować swój  
adres. Przesyłka zostanie  
dostarczona 8 listopada!

08:18

Wiadomość RCS

10:50

54%



+48514059

1



Ta wiadomość pochodzi z niezapisanego numeru.  
Uważaj na smishing i phishing.

Blokuj numer

czwartek, 7 marca

ING: Zweryfikuj swoją  
tożsamość, w przeciwnym  
razie Twoje konto zostanie  
tymczasowo zablokowane:

<https://ing.se-code.org/a/>

10:48

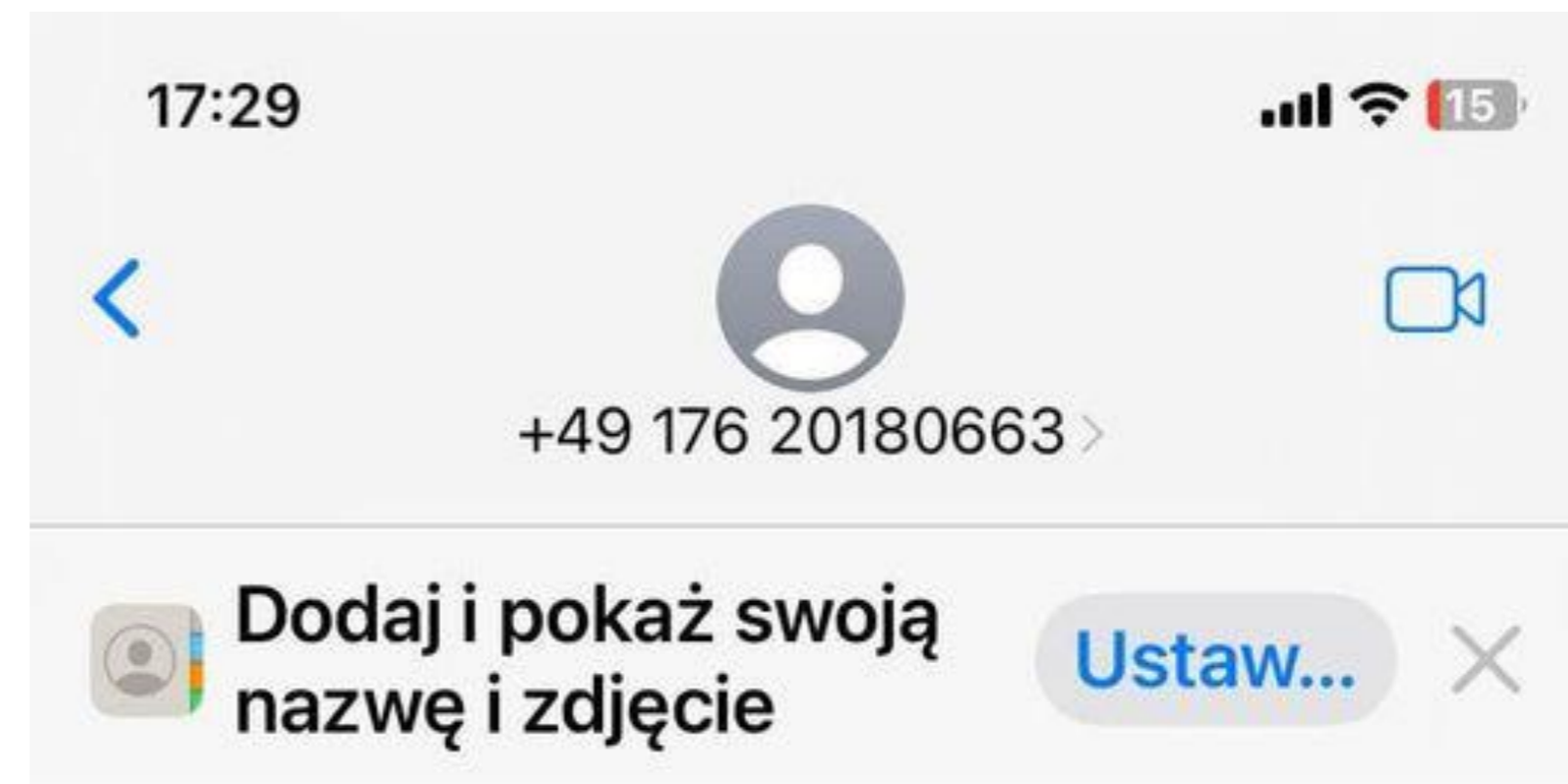


(InPost) Przesyłka dotarła do magazynu, ale nie może zostać dostarczona ze względu na niekompletne dane adresowe. Proszę potwierdzić swój adres za pomocą linku w ciągu 12 godzin.

<https://qrco.de/beuvdm?eCf=bvzgEyLRmm>

(Odpowiedz na 1, następnie wyjdź z SMS-a i otwórz ponownie link, aby aktywować SMS-a, lub skopiuj link i otwórz go w przeglądarce)

Miłego dnia życzy zespół InPost!



Wiadomość  
Dzisiaj, 17:18

Netflix: Ostatnie obciążenie nie powiodło się. Bez Twojej interwencji Twoje usługi zakończą się

28/03/2024 : <https://netflix-compte.info>



# 2/3 Przestępstwa w Internecie: jak oszukują...

## Jak możemy zostać „zaatakowani”?

- wiadomości SMS,
- wiadomość e-mail

### Zawieszenie Konta: Pilne Działanie Wymagane

Allegro powiadomienia@frydeed.pl

5 kwi 2024 06:18 (6 godzin temu)

do mnie [\(więcej\)](#)

Bezpieczeństwo:  Szyfrowanie TLS [Więcej informacji](#)

**allegro**

**Chcielibyśmy poinformować Cię o zawieszeniu Twojego konta na Allegro.**

Cześć!

Z powodu problemów z danymi rozliczeniowymi musieliśmy tymczasowo zawiesić Twoje konto.

Prosimy o dokonanie aktualizacji swoich danych płatnościowych w ciągu 12 godzin, abyśmy mogli szybko przywrócić dostęp do Twojego konta.

**AKTUALIZUJ SWOJE DANE**

**Allegro** powiadomienia@frydeed.pl

5 kwi 2024 06:18 (6 godzin temu)

do mnie [\(więcej\)](#)

Bezpieczeństwo:  Szyfrowanie TLS [Więcej informacji](#)

**allegro**

## Chcielibyśmy poinformować Cię o zawieszeniu Twojego konta na Allegro.

Cześć!

Z powodu problemów z danymi rozliczeniowymi musieliśmy tymczasowo zawiesić Twoje konto.

Prosimy o dokonanie aktualizacji swoich danych płatnościowych w ciągu 12 godzin, abyśmy mogli szybko przywrócić dostęp do Twojego konta.

**AKTUALIZUJ SWOJE DANE**





Allegro <info@bosowave.com>  
Do sara.drong@interia.pl

← Odpowiedz   ← Odpowiedz wszystkim   → Prześlij dalej   ...

czw. 01.02.2024 15:17

## Allegro.pl Marketplace

Szanowny,

Z przyjemnością informujemy, że została przeprowadzona korekta poprzednich zamówień na twoim koncie. Zgodnie z tym, przysługuje Ci zwrot środków w wysokości 130.12 zł.

Niestety, nie otrzymaliśmy odpowiedzi od Ciebie dotyczącej preferowanego sposobu zwrotu. Z uwagi na to, chcielibyśmy potwierdzić, czy życzylibyś sobie otrzymać te środki na swoją kartę debetową czy też w formie vouchera na naszej stronie Allegro.pl.

przez kliknięcie poniższego przycisku:

<https://aexperfumarias.com.br/news/103357914995>

Kliknij lub naciśnij, aby śledzić link.

**Odbierz Środki**

Jeśli nie otrzymamy odpowiedzi w ciągu najbliższych dni, zastrzegamy sobie prawo do zawieszenia twojego konta na Allegro.pl, a kwota środków zostanie skaowana.

Dziękujemy za zrozumienie i czekamy na twoją decyzję.

Z poważaniem,  
Zespół Allegro.pl

**Cześć,**

Otrzymałeś nową wiadomość na Santander Bank potwierdzającą Twój bezpieczny numer telefonu, dzięki czemu możesz bez wyjątku nadal korzystać z naszych usług online.

Musisz zakończyć aktualizację przed **30.03.2022**, w przeciwnym razie Twoje konto zostanie zablokowane i będziesz musiał odwiedzić jeden z naszych oddziałów Santander Bank.

Potwierdź swój numer telefonu, klikając poniższy link:

[Potwierdź mój numer telefonu](#)

**Santander Bank - POLSKA**

Copyright 2022, Santander Bank NV Polska, Warszawa.

**Cześć,**

Otrzymałeś nową wiadomość na MBank potwierdzającą Twój bezpieczny numer telefonu, dzięki czemu możesz bez wyjątku nadal korzystać z naszych usług online.

Musisz zakończyć aktualizację przed **15.03.2022**, w przeciwnym razie Twoje konto zostanie zablokowane i będziesz musiał odwiedzić jeden z naszych oddziałów MBank.

Potwierdź swój numer telefonu, klikając poniższy link:

[Potwierdź mój numer telefonu](#)

**MBank - POLSKA**

Copyright 2022, MBank NV Polska, Warszawa.

**Cześć,**

Otrzymałeś nową wiadomość na Bnpparibas Bank potwierdzającą Twój bezpieczny numer telefonu, dzięki czemu możesz bez wyjątku nadal korzystać z naszych usług online.

Musisz zakończyć aktualizację przed **30.03.2022**, w przeciwnym razie Twoje konto zostanie zablokowane i będziesz musiał odwiedzić jeden z naszych oddziałów Bnpparibas Bank.

Potwierdź swój numer telefonu, klikając poniższy link:

[Potwierdź mój numer telefonu](#)

**Bnpparibas Bank - POLSKA**

Copyright 2022, Bnpparibas Bank NV Polska, Warszawa.

## 2/3 Przestępstwa w Internecie: jak oszukują...

### Jak możemy zostać „zaatakowani”?

- wiadomości SMS
- wiadomość e-mail
- reklamy w mediach społecznościowych

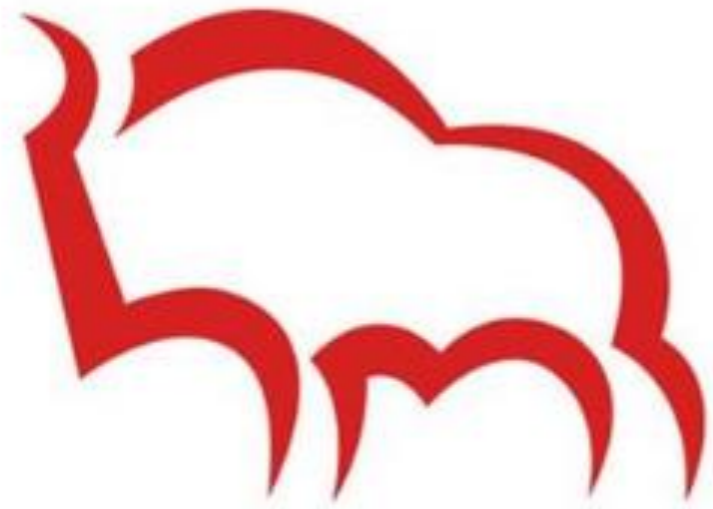




Bank PL  
Sponsorowane

Identyfikator biblioteki: 713883334291149

Jesteś aktywnym klientem PeoPay?  
Zaloguj się i odbierz 300 zł na konto osobiste!



# Bank Pekao

KLIENCI-INDYWIDUALNE-PEKAO-BANK.SETQAAN.COM  
Zaloguj się i odbierz 300 zł na konto osobiste!

Dowiedz się...



UrbanCard Wrocław  
Sponsorowane

Identyfikator biblioteki: 978581093665517

PL Wraz z nadejściem wiosny MPK oferuje:  
Ciesz się darmowymi przejazdami przez 90 dni z Wrocławską Kartą Miejską 🍷  
✅ Kup naszą kartę za jedyne 10 zł i zapomnij o prowizjach 🚇 🚊  
! Oferta jest ważna do 24.03.2024.  
Kliknij poniższy link, aby otrzymać nową spersonalizowaną kartę 📄  
<https://avivamientointernacional.com/9LkywbTk?>



UrbanCard Wrocław

Zamów teraz

# KNF

CEDUR  
Centrum Edukacji dla  
Uczestników Rynku



Potwierdź oskarżenia wobec Jerzego Owsiaaka! Sekret słynnego reportera w końcu zostaje ujawniony!



TODAYSFASHION.XYZ

**Tragiczny koniec Jerzego Owsiaaka! Dzisiejsza wiadomość zszokowała wszystkich!**

[Dowiedz się więcej](#)



# JAK ROZPOZNAĆ FAŁSZYWĄ REKLAMĘ INWESTYCYJNĄ?

**3. Używane jest logo zaufanych podmiotów.**

**5. Informacja o wysokich zyskach w krótkim czasie.**

**6. Informacja o ofercie ograniczonej czasowo.**

**1. Reklama wyświetlana z profilu o niskim poziomie zaufania.**

**2. Tekst mający na celu zachęcenie do potencjalnej inwestycji.**

**4. W reklamach wykorzystywane są wizerunki znanych osób.**

Hana Adams  
Sponsorowane

1. Zarejestruj się na stronie
2. Doładuj swoje konto na platformie
3. Uzyskaj miesięczny dochód pasywny

Dołącz do projektu i zyskuj co miesiąc na transporcie gazu do Europy.

BALTIC PIPE PROJECT **polsat news**

**!! DOSTĘPNE TYLKO DLA POLAKÓW! !!**

**KUPIĆ 1 AKCJĘ BALTIC PIPE ZA 1000 ZŁ  
GENEROWAĆ STAŁY DOCHÓD  
OD 29000 ZŁ MIESIĘCZNIE**

OFFICIALERTFD.COM  
Dostęp jest otwarty tylko do końca tego miesiąca!  
Nowe stawki, które obowiązują od stycznia 2022 roku zostały zatwierdzone przez Prezesa Urzędu Regulacji...

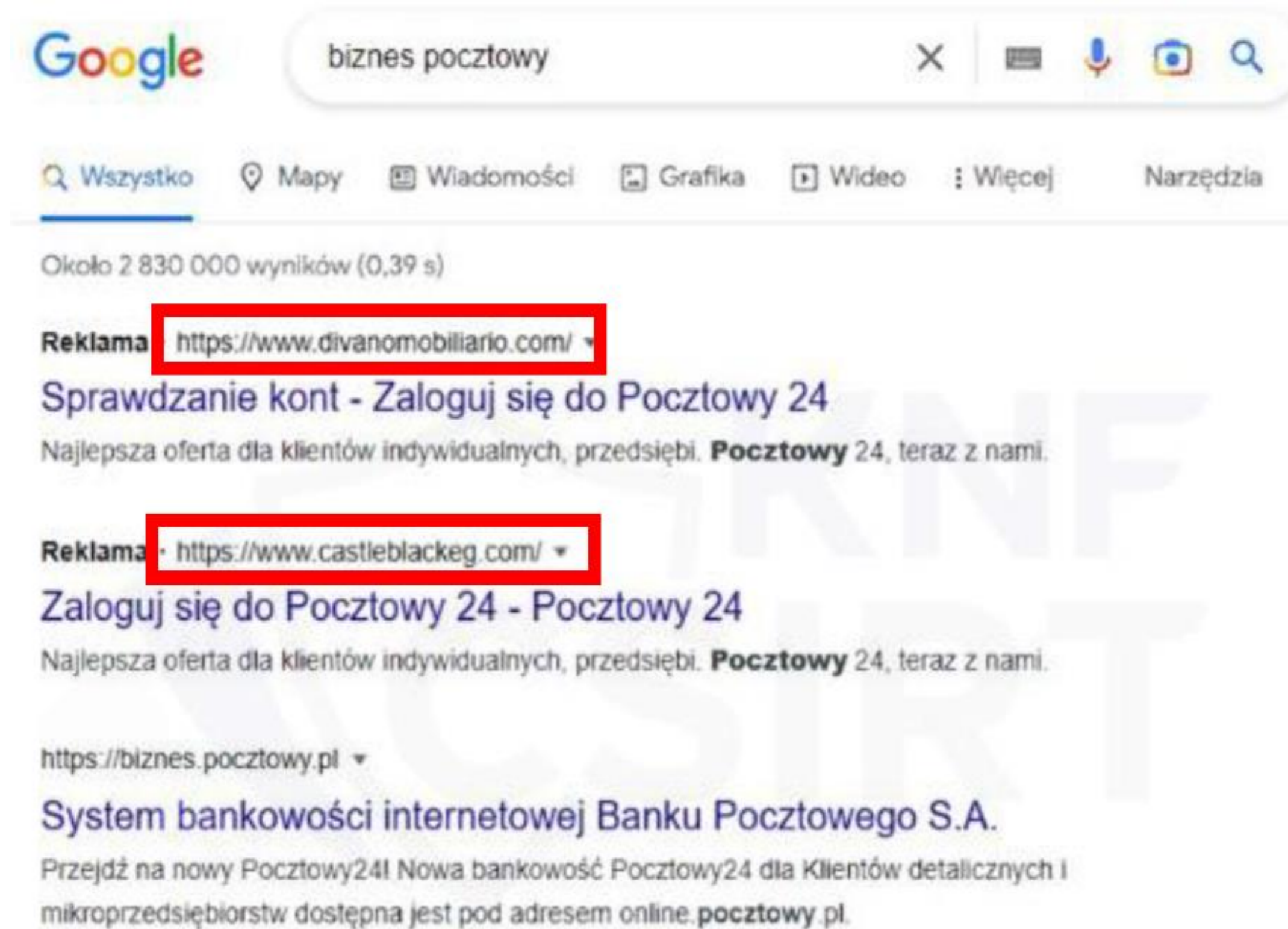
Dowiedz się...



## 2/3 Przestępstwa w Internecie: jak oszukują...

### Jak możemy zostać „zaatakowani”?

- wiadomości SMS
- wiadomość e-mail
- reklamy w mediach społecznościowych
- reklamy w wyszukiwarce Google



**FAŁSZYWE  
STRONY**

**PRAWDZIWA  
STRONA**



logowanie do mojego banku



Mail

Konto

Chrome

Settings

Wideo

Translate

Spaces

Grafika

Flights

**UWAGA**

**Te strony wyświetlą się jako pierwsze!**



# 2/3 Przestępstwa w Internecie: jak oszukują...

## Jak możemy zostać „zaatakowani”?

- wiadomości SMS
- wiadomość e-mail
- reklamy w mediach społecznościowych
- reklamy w wyszukiwarce Google
- przez telefon!

# VISHING...

## TO WIDZIMY



## TO JEST NAPRAWDĘ



# VISHING – za kogo podają się przestępcy?

- doradca Banku
- pośrednik Banku
- przedstawiciel jednostek technicznych
- pracownik działu bezpieczeństwa
- znajomy znajomego
- Biuro Bezpieczeństwa Narodowego
- Komisja Nadzoru Finansowego
- ...





# VISHING - scenariusze

- *„(...) czy to Pana transakcja? Nie?! Ojej!”*
- *„(...) Pani środki są w niebezpieczeństwie, ja je dla bezpieczeństwa schowam (...)”*
- *„(...) a może antywirus?”*
- *„(...) dzwonię z Banku, więc poproszę wszystkie Pana dane (...)”*
- *„(...) ten wniosek kredytowy z nocy – dokończymy?”*
- ...

# VISHING – częsta sztuczka przestępcza

**DZWONIĄCY (OSZUST):** Dzień dobry, dzwonię z Banku...

**ODBIERAJĄCY:** Ale jakiego?

**DZWONIĄCY (OSZUST):** No Pana/Pani...

**ODBIERAJĄCY:** Aaaa.... (podaje nazwę Banku)

# VISHING – częsta sztuczka przestępcza

# SPRAWNI

# MANIPULATORZY!



## 2/3 Przestępstwa w Internecie: co chcą ukraść...

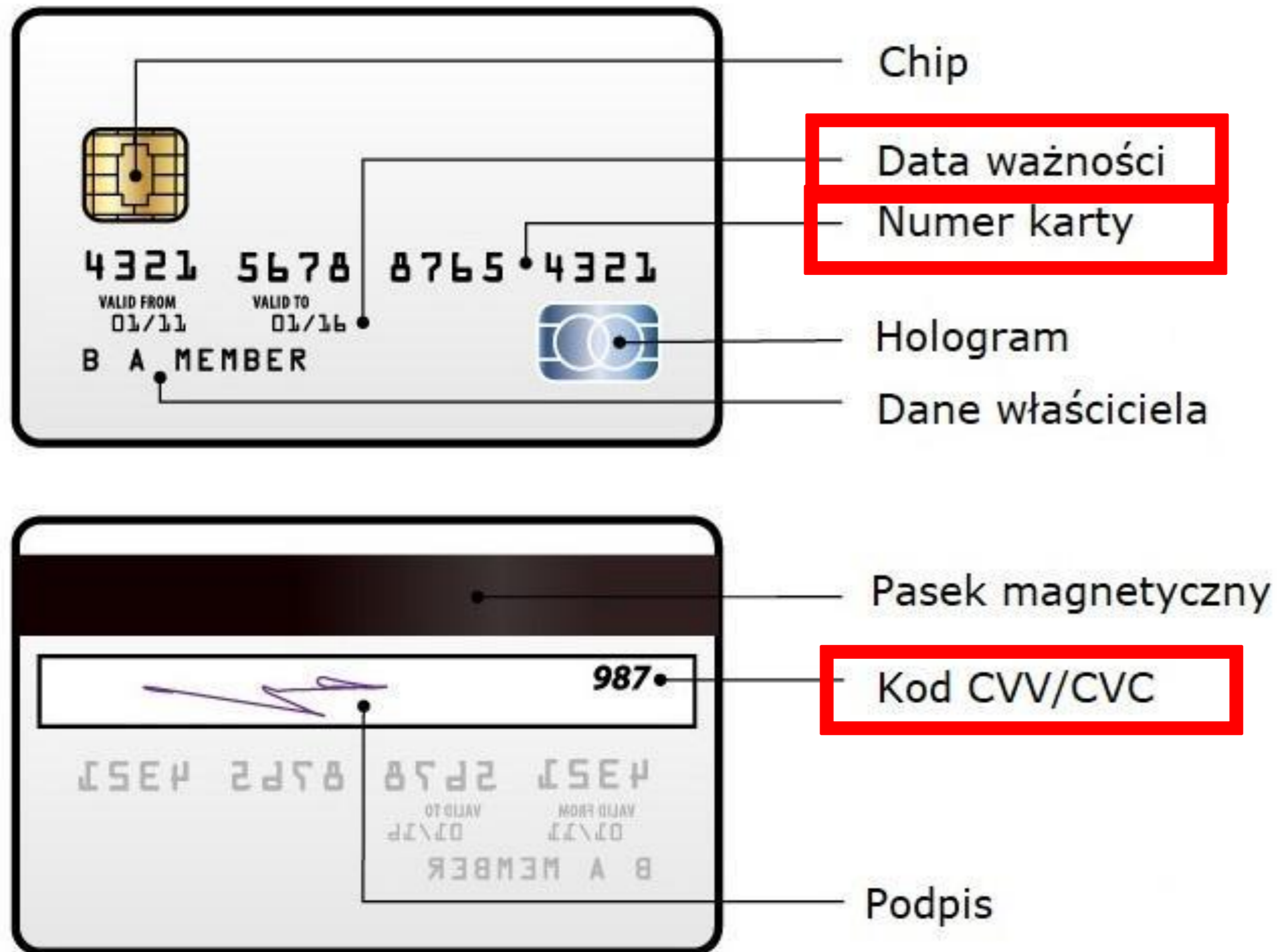
Co możemy stracić?

**WSZYSTKO, DZIĘKI  
CZEMU OSZUŚCI SIĘ  
WZBOGACĄ...**

# 2/3 Przestępstwa w Internecie: co chcą ukraść...

## Co możemy stracić?

- dane uwierzytelniające do bankowości elektronicznej
- dane kart płatniczych



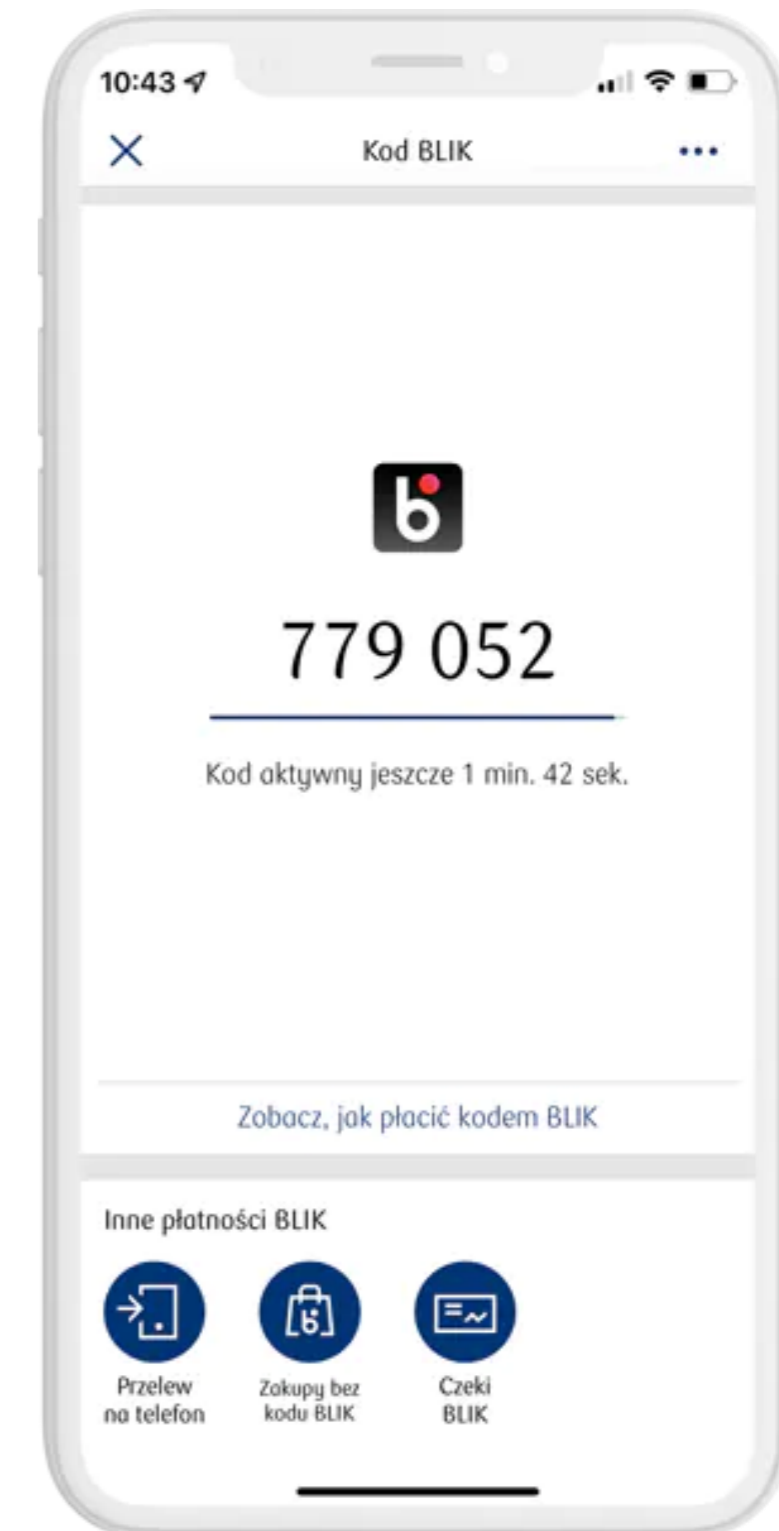
**+ KOD SMS  
(3D Secure)**



# 2/3 Przestępstwa w Internecie: co chcą ukraść...

## Co możemy stracić?

- dane uwierzytelniające do bankowości elektronicznej
- dane kart płatniczych
- kody BLIK



# 2/3 Przestępstwa w Internecie: co chcą ukraść...

## Co możemy stracić?

- dane uwierzytelniające do bankowości elektronicznej
- dane kart płatniczych
- kody BLIK
- bezpośrednio przelewy...

# „Na co uważać i jak nie dać się okraść w Internecie – bankowość elektroniczna dla seniorów. I edycja”

## Agenda – II część webinarium

- Cyberhigiena: jak rozpoznać fałszywą stronę, czy w Internecie można być anonimowym, dobre praktyki korzystania z urządzeń elektronicznych



# Cyberhigiena:

1. Jak rozpoznać fałszywą stronę
2. Wiedza to potęgi (obrony) klucz, czyli scenariusze oszustów
3. Dobre praktyki

# 1/3 Cyberhigiena: jak rozpoznać fałszywą stronę...

14:10

Twoje przesyłki nie mogą zostać dostarczone z powodu błędnie podanego adresu. Prosimy o aktualizację adresu w celu ponownej dostawy. <https://is.gd/ePWFoP>

Kliknij, aby wczytać podgląd

Śledzenie przesyłek - Tracking

Wybierając opcję śledzenia mogą Państwo sprawdzić aktualny status przesyłki, zarówno po stronie Poczty Polskiej jak i operatorów zagranicznych. Poczta Polska S.A. udostępni adresatowi dokument PZC nie wcześniej niż 7 dni kalendarzowych po doręczeniu lub wydaniu.

Wpisz numer przesyłki  SZUKAJ

**dostawa na zamówienie**

**Dane przesyłki**

Numer przesyłki	PX6786734221
Data nadania	2023-04-22
Rodzaj przesyłki	Pocztex
Kraj nadania	Polska
Kraj przeznaczenia	Polska
Urząd nadania	PP Warszawa W101 (ul. Łęczyny 8, 00-903 Warszawa)
Masa	1 kg

**Status przesyłki**

Nazwa zdarzenia	Data i czas	Jednostka pocztowa
Zarejestrowano	2023-04-22 08:00:40	WER
Odebrany	2023-04-22 08:00:41	WER
W transporcie	2023-04-22 10:49:55	
Przekazano do doręczenia	2023-04-23 09:37:40	WER
Nieudany doręczenie	2023-04-23 16:32:31	nastąpiła nieudana próba doręczenia z poczta komonki
Wysłano powiadomienie sms	2023-04-23 18:21:41	Centralna Baza Danych ZST

Aby wyszukać przesyłkę rejestrowaną należy w ramce wpisać numer (np.: 0015900773312345678, PX0000000013, RR123456789PL, GP123456789PL, VV123456789PL, EE123456789PL) podany na powiadzeniu nadania, bez spacji oraz nawiasów i nacisnąć [Szukaj]

Jeśli numer jest błędny lub w systemie nie zarejestrowano informacji o przesyłce z podanym numerem, pojawi się komunikat:

Podany numer przesyłki jest błędny

Jeśli w miejscu przeznaczonym do wpisania numeru przesyłki nie zostanie podany jej numer, pojawi się komunikat:

Podaj numer przesyłki

Jeśli wpisany identyfikator jest prawidłowy to pojawią się dane i historia zdarzeń dla określonej przesyłki. Jeżeli historia przesyłki lub informacje o niej są niezgodne z dowodem nadania należy sprawdzić poprawność wpisanego numeru.

System obecnie udostępni informacje o następujących rodzajach przesyłek:

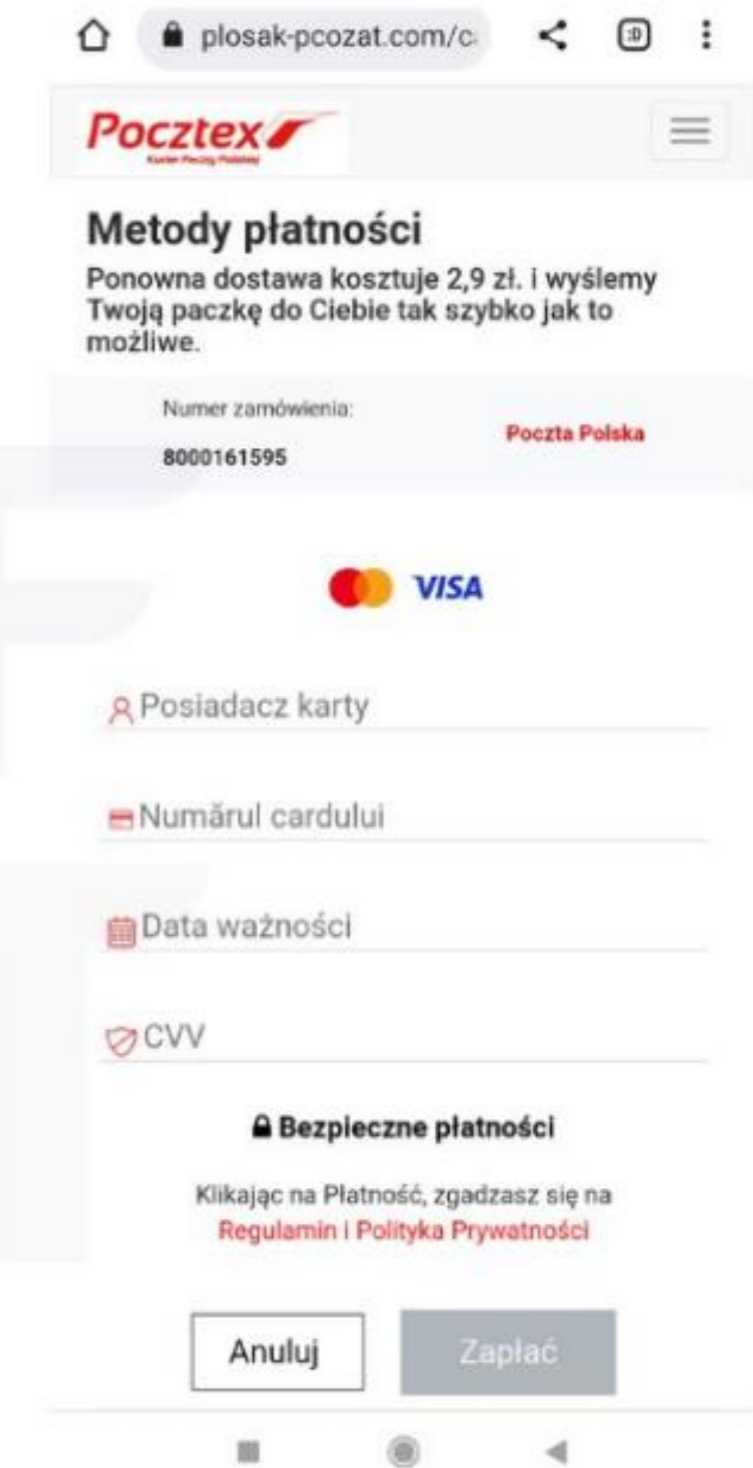
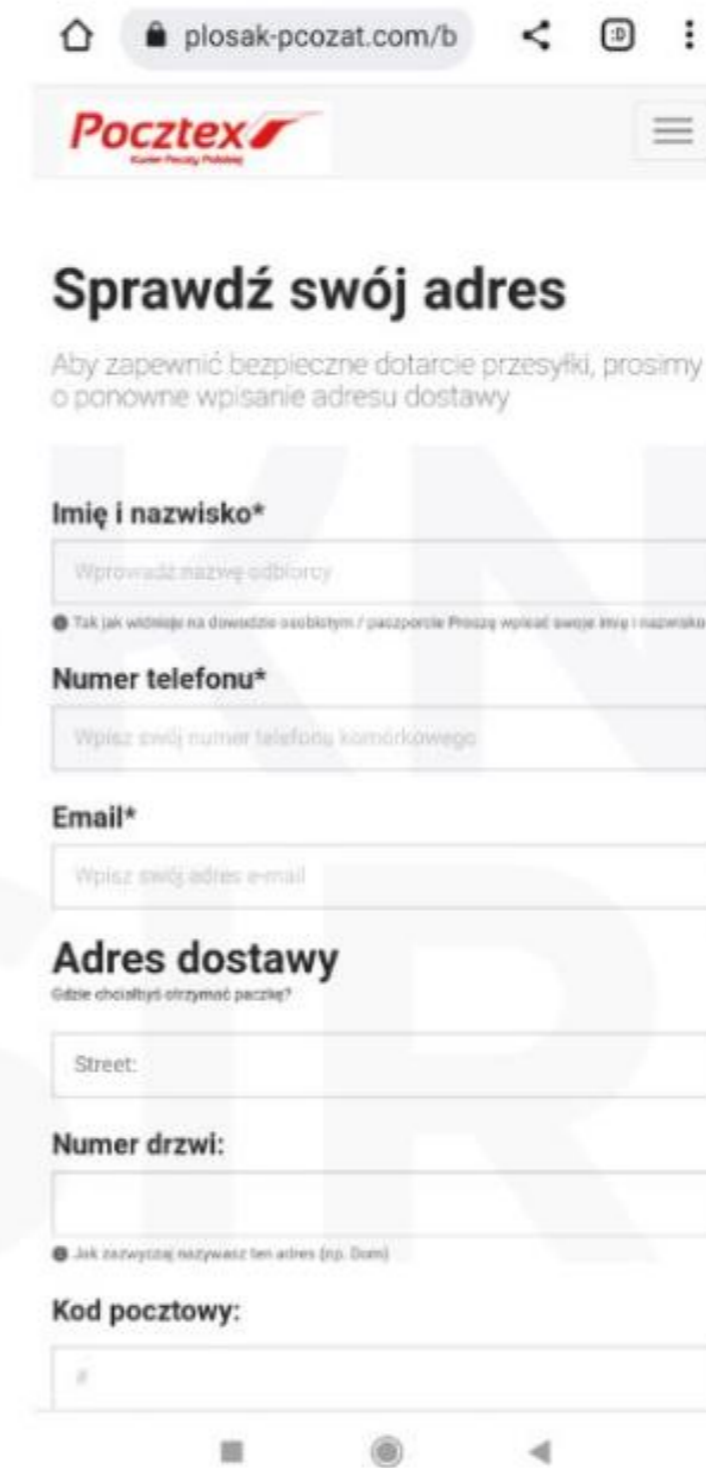
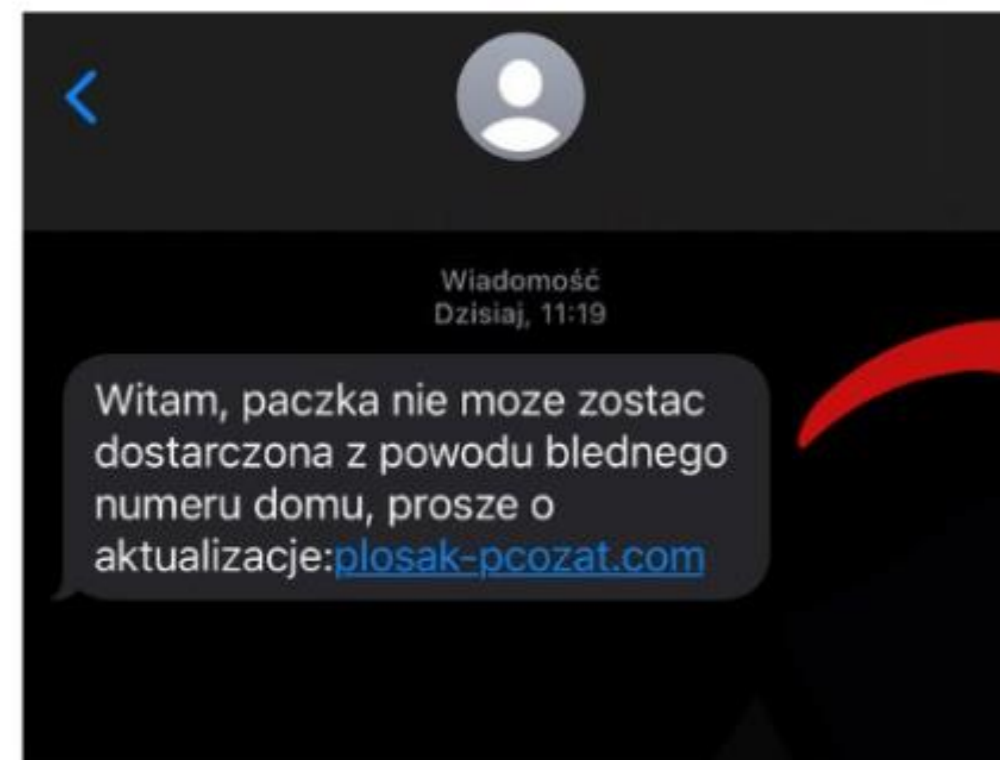
- w obszarze krajowym:
  - List polecony
  - Paczka pocztowa
  - PACZKA24.PACZKA48
  - Pocztex
  - Pocztex Procedura

Ta strona używa ciasteczek (cookies), dzięki którym nasz serwis może działać lepiej. Dowiedz się więcej.

Korzystając ze strony zgadzasz się na zapisywanie prywatnych danych zawartych w plikach cookies i in podobnych technologi w urządzeniu końcowym. Zapoznaj się z naszą polityką wykorzystywania danych. Zamknij

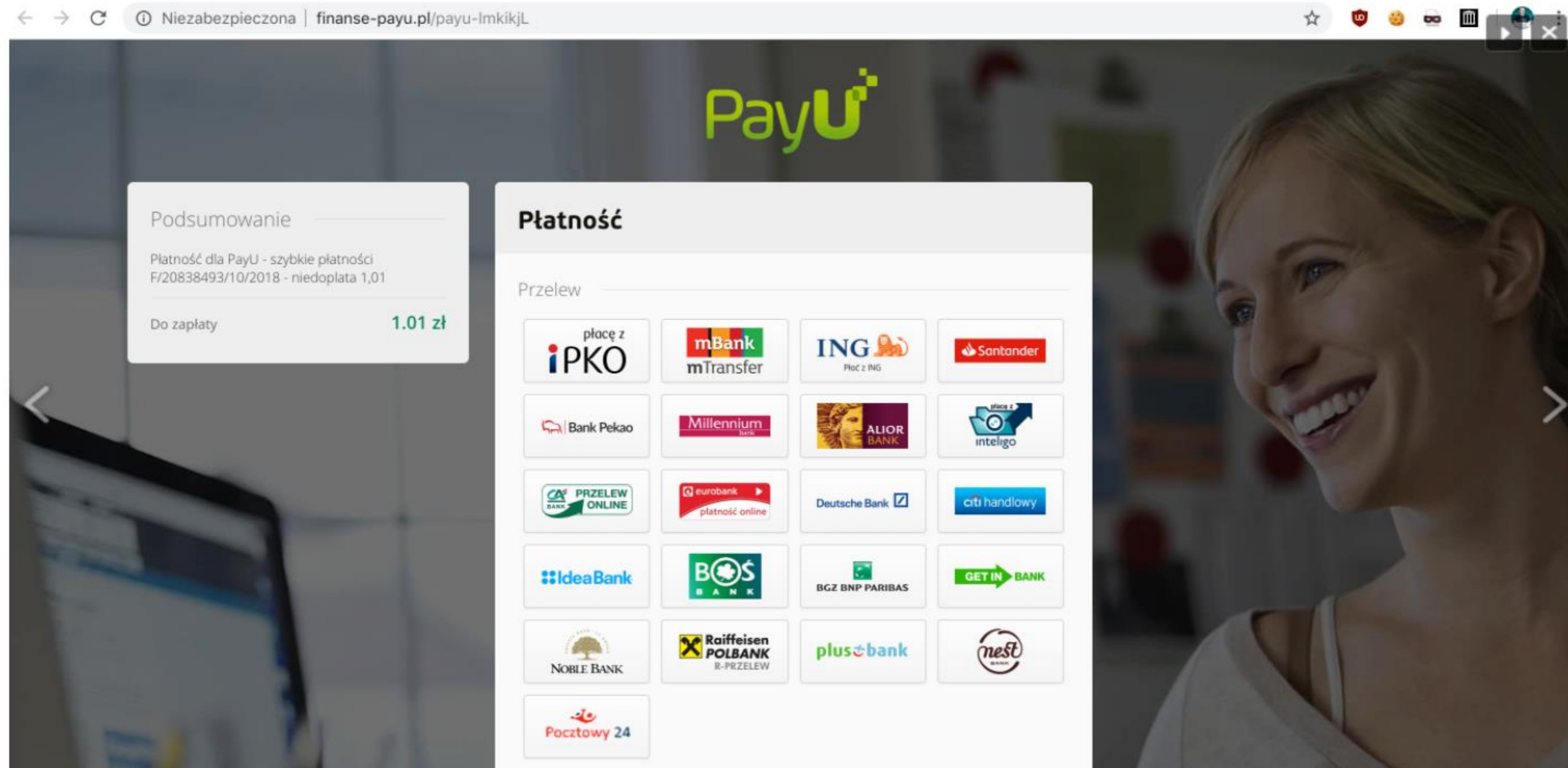


# 1/3 Cyberhigiena: jak rozpoznać fałszywą stronę...

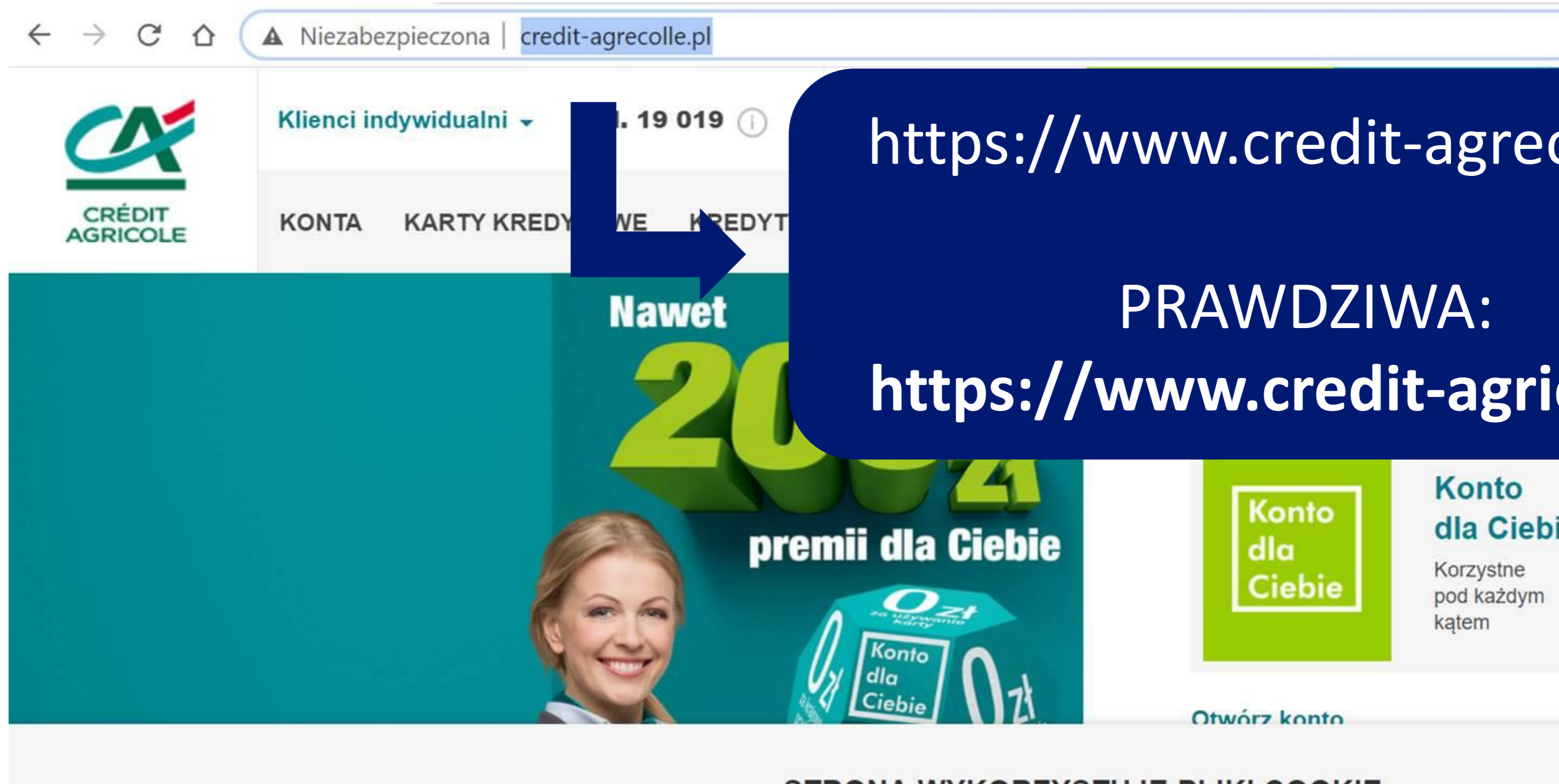




# Lub...



# Następnie...

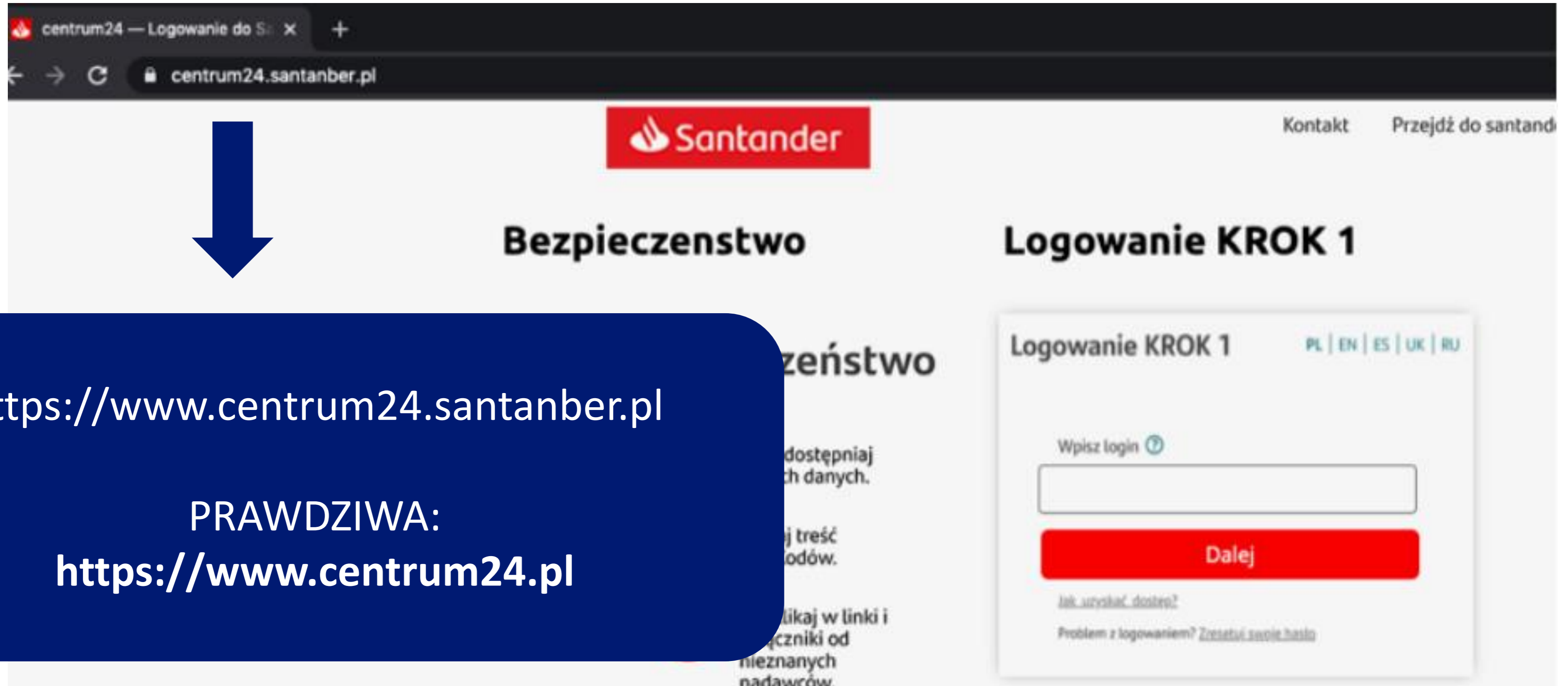


<https://www.credit-agrecolle.pl>

**PRAWDZIWA:**

<https://www.credit-agricole.pl>

# Następnie...



<https://www.centrum24.santanber.pl>

PRAWDZIWA:

<https://www.centrum24.pl>



# Przykładów nigdy dość...

## Prawdziwe domeny

**ipkobiznes.pl**

**goonline.bnpparibas.pl**

**pekao24.pl**

**secure.velobank.pl**

**login.ingbank.pl**

## Fałszywe domeny

**ipk0biznespl.online**

**bnpparibas.site**

**pekao-pl.net**

**velobannk.fun**

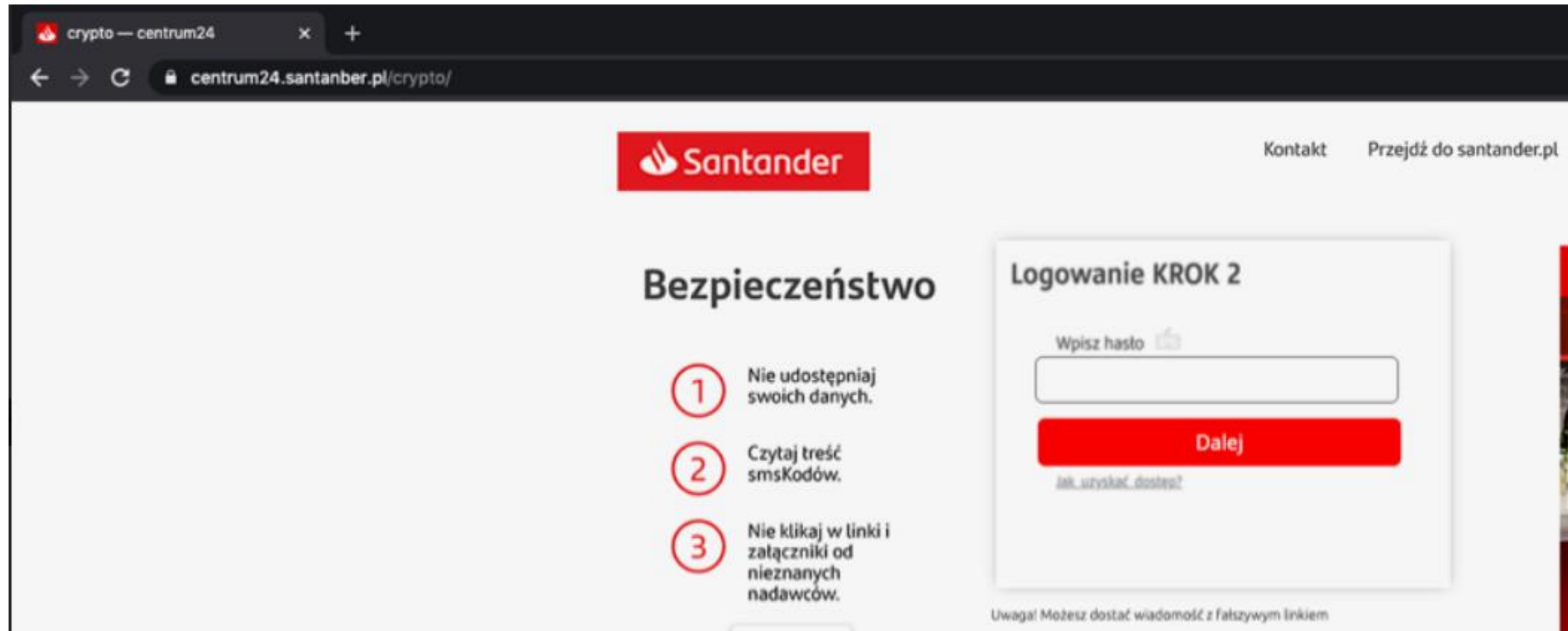
**ing-pl-app.org**

# Login

The screenshot shows a web browser window with the URL `centrum24.santander.pl`. The page features the Santander logo at the top center. On the right side, there are links for "Kontakt" and "Przejdź do santander". The main content is divided into two sections:

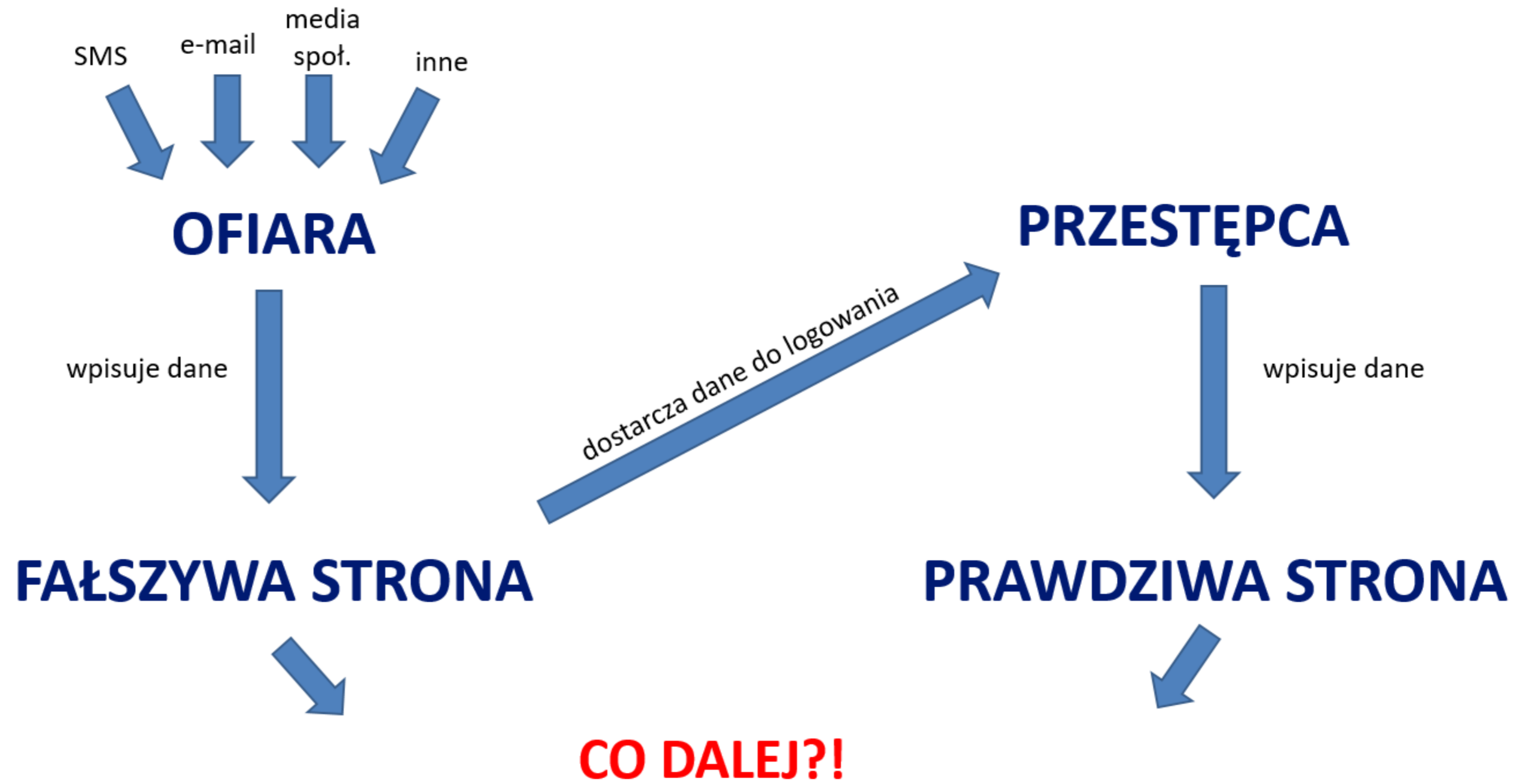
- Bezpieczeństwo** (Security): A section titled "Bezpieczeństwo" with three numbered instructions:
  - 1 Nie udostępniaj swoich danych.
  - 2 Czytaj treść smsKodów.
  - 3 Nie klikaj w linki i załączniki od nieznanymi nadawców.
- Logowanie KROK 1** (Login Step 1): A form titled "Logowanie KROK 1" with language options (PL | EN | ES | UK | RU). It includes a text input field labeled "Wpisz login" with a help icon, a red "Dalej" button, and links for "Jak uzyskać dostęp?" and "Problem z logowaniem? Zresetuj swoje hasło".

# Hasło





# Podsumujmy to...



## 2/3 Cyberhigiena: scenariusze przestępcze...

- oszustwa inwestycyjne
- metoda na wnuczka/policjanta
- wiele innych...

# Oszustwa inwestycyjne

## Zaczyna się od zachęty...

**Bezpieczeństwo Emerytalne**  
Sponsorowane  
Identyfikator biblioteki: 25115837538031503

⚠️Uwaga Polacy!  
⚠️Emerytura od 50 roku życia, czytajcie!



**PRAWO DOTYCZĄCE  
KAŻDEJ OSOBY, KTÓRA  
SKOŃCZYŁA 50 LAT**

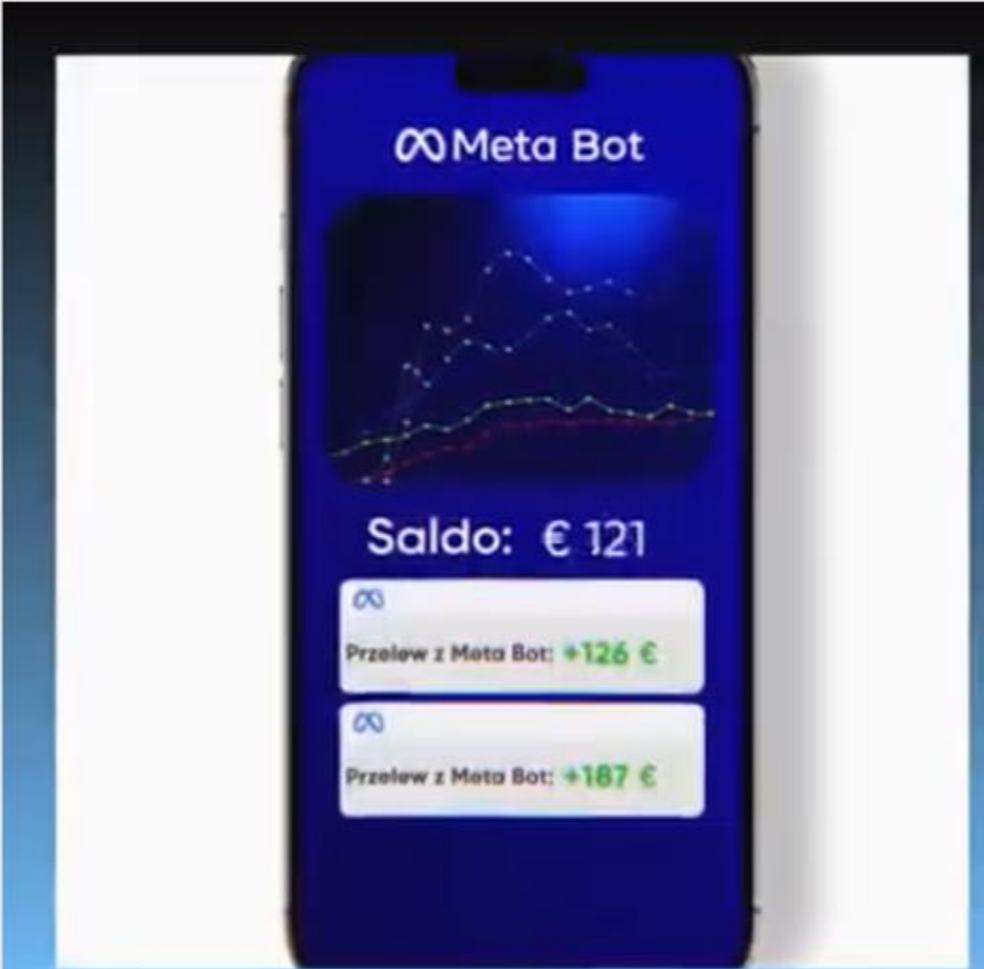
**CZYTAJ CIE ARTYKUŁ**

ANJANAUTOMOTIVES.COM  
Dowiedz się więcej na stronie. 📌  
Explore Stefan Raab's discography including top tracks, albums, and reviews. Learn all about Stefa...

Dowiedz się...

**Personal Manager**  
Sponsorowane

System ten jest innowacyjnym rozwiązaniem w świecie rynków finansowych, które pozwala inwestorom i traderom zautomatyzować i ulepszyć ich strategię handlową.  
Jest to kompleksowe narzędzie oparte na zaawansowanych technologiach i sztucznej inteligencji, które pozwala osiągać znakomite wyniki na rynkach finansowych.



**Meta Bot**

Saldo: € 121

Przelew z Meta Bot: +126 €

Przelew z Meta Bot: +187 €

CAKECRAFTACADEMY.COM  
Zrób krok w stronę lepszego jutra

Dowiedz się więcej

**Academia Genius**  
Sponsorowane



Stan konta  
**45 590 zł**

Zysk dzisiejszy  
**80 zł**

Zysk miesięczny  
**27 710 zł**

Metody płatności  
VISA Mastercard PayPal

REJESTRACJA

MCKARRIER.COM  
Dowiedz się więcej 📌

Dowiedz się więcej

Materiały szkoleniowe przygotowane zostają w ramach projektu Centrum Edukacji dla Uczestników Rynku – CEDUR. Autorskie prawa majątkowe do prezentowanych oraz przekazywanych materiałów są własnością Urzędu Komisji Nadzoru Finansowego (UKNF). Rozpowszechnianie, kopiowanie, utrwalanie, publiczne wykorzystywanie całości lub części dozwolone jest jedynie w celach niekomercyjnych, nieodpłatnie, za zgodą UKNF, pod warunkiem podania informacji o pochodzeniu materiałów. Stan prawny informacji zawartych w materiałach jest aktualny na dzień ogłoszenia prezentacji. Materiały przeznaczone są wyłącznie dla odbiorców określonych w programie seminarium, dostępnym na stronie [www.knf.gov.pl](http://www.knf.gov.pl). Prezentowane treści mają wyłącznie charakter ogólny i informacyjny, i nie stanowią porady prawnej oraz inwestycyjnej. UKNF nie ponosi odpowiedzialności za jakiegokolwiek decyzje podjęte przez odbiorców prezentacji w sprawach ich dotyczących lub za decyzje inwestycyjne podejmowane na rynku finansowym, w oparciu o informacje przekazane w prezentacji, ponieważ decyzje te powinny być każdorazowo przeanalizowane w ramach konkretnego stanu faktycznego, który w zależności od okoliczności, podmiotu, który decyzje podejmuje, potrzeb, założonych celów oraz posiadanych środków będzie uzasadniał zastosowanie adekwatnych działań, w tym przyjęcie konkretnego ryzyka, w celu osiągnięcia oczekiwanych skutków, które decyzja ma wywołać. W indywidualnych przypadkach należy skontaktować się z Urzędem Komisji Nadzoru Finansowego.



# Oszustwa inwestycyjne

## Zaczyna się od zachęty...





# Oszustwa inwestycyjne

## Zaczyna się od zachęty...

**Dolarplusvenezuela**  
Sponsorowane

✓ Twój sukces finansowy zaczyna się od Meta Bota!

Z Meta Botem inwestowanie staje się łatwe i opłacalne. Nasza innowacyjna platforma oferuje:

- 🔍 Analizę rynku: Meta Bot dostarcza Ci dokładne dane i analizy, abyś mógł podejmować przemyślane decyzje
- 👁️ ... Wyświetl więcej

**CEZARY PAZURA**

**CZAS NA ORZEZWNIENIE**

**DZISIEJSZY DOCHÓD: 951**

**PROGRAM PRZYNOŚI MI CO TYDZIEŃ 1500 DZ**

HEXACIU.COM

Dołącz do Meta Bota już dziś i odkryj nowe możliwości osiągnięcia finansowego sukcesu!

Dowiedz się więcej

**CEZARY PAZURA**

**CZAS NA ORZEZWNIENIE**

**DZISIEJSZY DOCHÓD: 763**

**PROGRAM PRZYNOŚI MI CO TYDZIEŃ 1500 DZ**

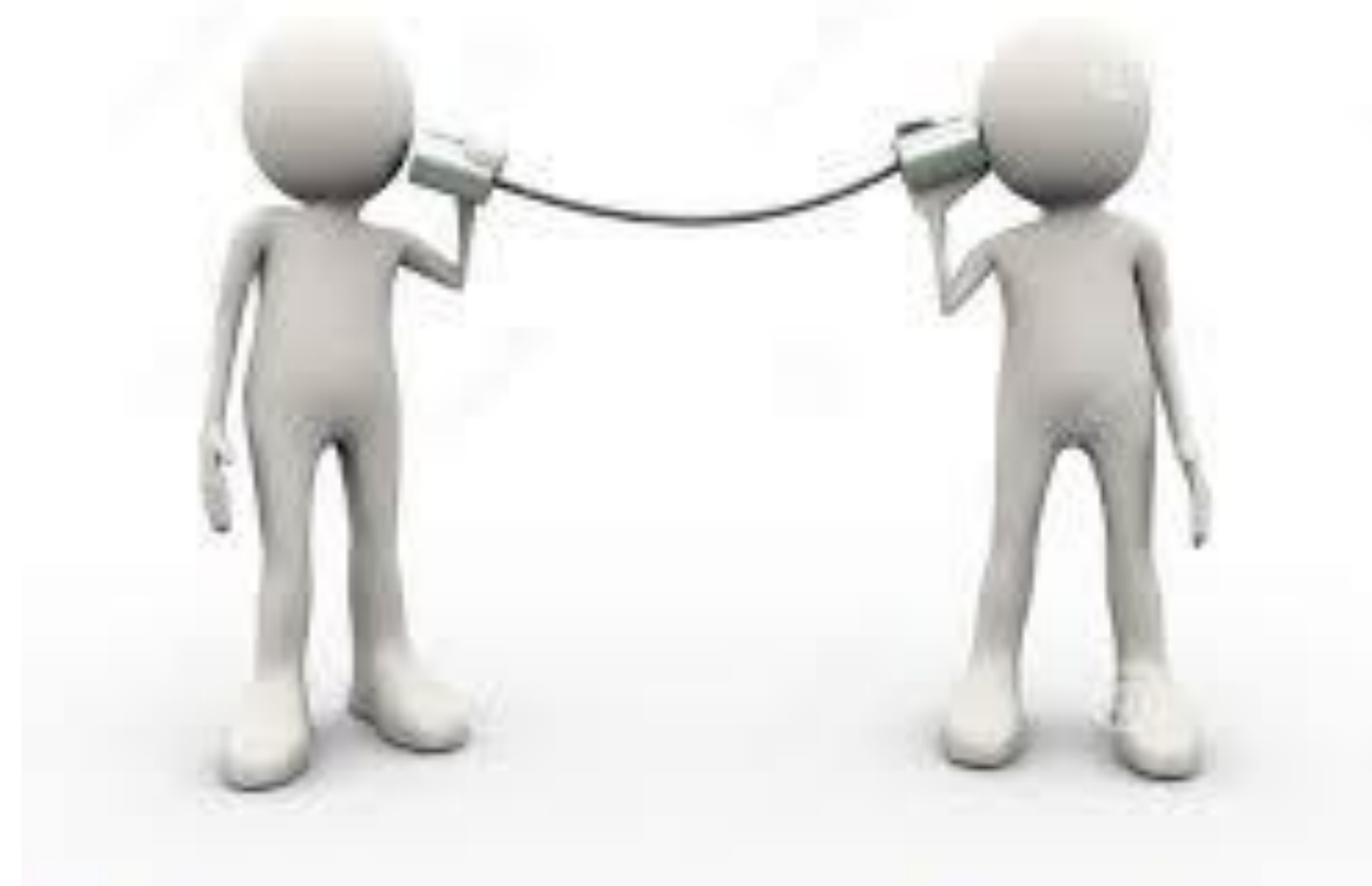
HEXACIU.COM

Dołącz do Meta Bota już dziś i odkryj nowe możliwości osiągnięcia finansowego sukcesu!

Dowiedz się więcej

# DEEPPFAKE

■ **Deepfake** - „(...) cyberprzestępcy korzystając z zaawansowanego oprogramowania zasilanego przez sztuczną inteligencję, klonują głosy i wizerunek (...) dowolnej osoby, a wystarczy do tego kilkusekundowe nagranie (...)”





# Oszustwa inwestycyjne

## Formularz kontaktowy...

**Dermat**  
Sponsorowane  
Identyfikator biblioteki: 2114815862218488

Gotów zainwestować w polski przemysł obronny? Dołącz do Polskiej Grupy Zbrojeniowej (PGZ)!

Wykorzystaj obecną sytuację dla perspektywicznej przyszłości! Polska Grupa Zbrojeniowa to jeden z największych koncernów obronnych w Europie.

**WYKORZYSTAJ OBECNĄ SYTUACJĘ DLA PERSPEKTYW STABILNEJ PRZYSZŁOŚCI**

**WYPEŁNIJ FORMULARZ I JUŻ DZIŚ ZAINWESTUJ W INNOWACYJNY PROJEKT**

DEFIGMI.COM  
Wykorzystaj tę okazję i zainwestuj w innowacyjny projekt już dziś!  
Inwestuj w technologie obronne:

[Dowiedz się...](#)

PGZ Invest

https://amazon-ca-return.com

PGZ PROJEKTOWANIE PROGNOZOWANY ZYSK JAK DZIAŁA PROJEKT DLACZEGO JEST TO OPŁACALNE?

## Tworzymy stabilność finansową i bezpieczną przyszłość Polski

**Inwestuj w technologie obronne:**

dochodowy potencjał przemysłu zbrojeniowego w innowacyjnych rozwiązaniach i bezpieczeństwie narodowym

**Zostań inwestorem**

**Formularz kontaktowy**

Nazwa

Nazwisko

E-mail

+48 512 345 678

**Inwestować w PGZ**

# Oszustwa inwestycyjne

## Rozmowa telefoniczna...

Ostatni krok! Otrzymujesz **bezpłatnego** analityka. Podaj swój numer kontaktowy i nie zapomnij odebrać telefonu!



# Oszustwa inwestycyjne

## Platforma „inwestycyjna” ...

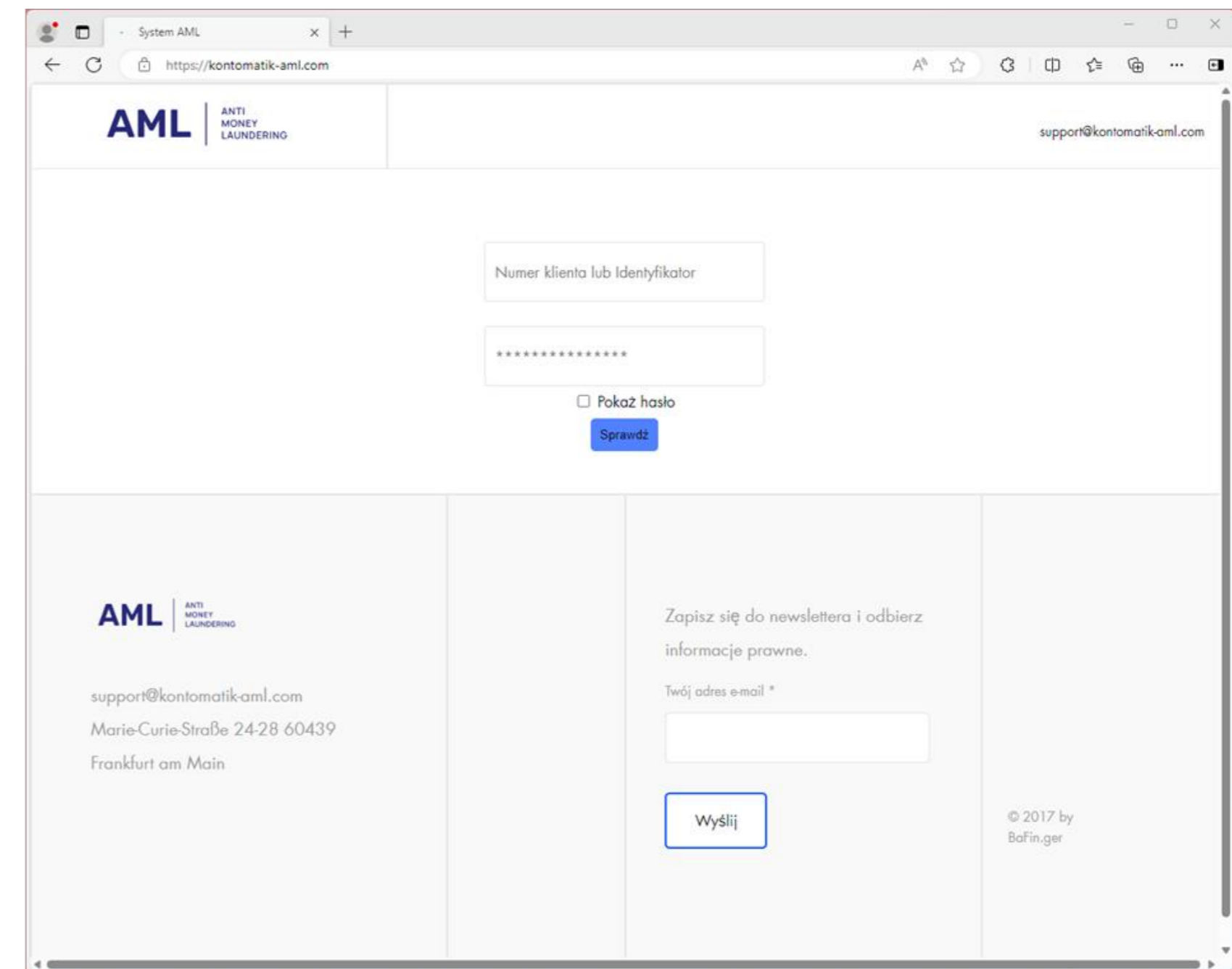
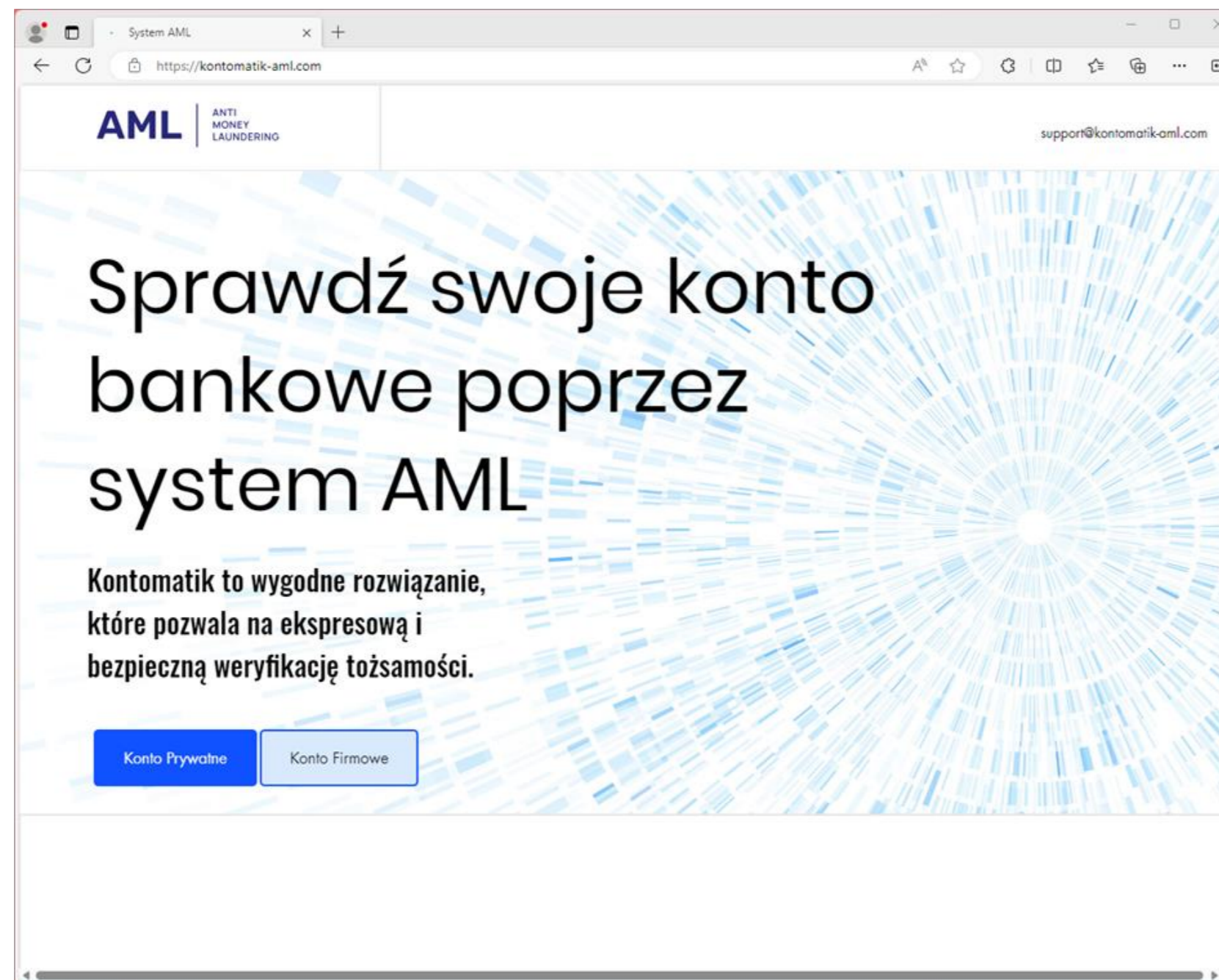


Materiały szkoleniowe przygotowane zostały w ramach projektu Centrum Edukacji dla Uczestników Rynku – CEDUR. Autorskie prawa majątkowe do prezentowanych oraz przekazywanych materiałów są własnością Urzędu Komisji Nadzoru Finansowego (UKNF). Rozpowszechnianie, kopiowanie, utrwalanie, publiczne wykorzystywanie całości lub części dozwolone jest jedynie w celach niekomercyjnych, nieodpłatnie, za zgodą UKNF, pod warunkiem podania informacji o pochodzeniu materiałów. Stan prawny informacji zawartych w materiałach jest aktualny na dzień ogłoszenia prezentacji. Materiały przeznaczone są wyłącznie dla odbiorców określonych w programie seminarium, dostępnym na stronie [www.knf.gov.pl](http://www.knf.gov.pl). Prezentowane treści mają wyłącznie charakter ogólny i informacyjny, i nie stanowią porady prawnej oraz inwestycyjnej. UKNF nie ponosi odpowiedzialności za jakiegokolwiek decyzje podjęte przez odbiorców prezentacji w sprawach ich dotyczących lub za decyzje inwestycyjne podejmowane na rynku finansowym, w oparciu o informacje przekazane w prezentacji, ponieważ decyzje te powinny być każdorazowo przeanalizowane w ramach konkretnego stanu faktycznego, który w zależności od okoliczności, podmiotu, który decyzje podejmuje, potrzeb, założonych celów oraz posiadanych środków będzie uzasadniał zastosowanie adekwatnych działań, w tym przyjęcie konkretnego ryzyka, w celu osiągnięcia oczekiwanych skutków, które decyzja ma wywołać. W indywidualnych przypadkach należy skontaktować się z Urzędem Komisji Nadzoru Finansowego.



# Oszustwa inwestycyjne

## Wyplata?



## Oszustwa inwestycyjne

# OGROMNE STRATY FINANSOWE

# Metoda np. na wnuczka / policjanta

 Polskie Radio Koszalin

## Seniorka ze Słupska straciła 21 tysięcy złotych. Została oszukana metodą "na wnuczka"

85-letnia słupszczanka przekazała pieniądze przekonana, że pomaga swojej wnuczce, która miała spowodować wypadek drogowy. O tym, że wnuczka...



 TVN24

## 83-latka oszukana metodą "na wnuczka". Oddała kosztowności warte milion euro

83-latka z Rzymu została oszukana przez dwóch mężczyzn. Jeden z nich podszywał się pod naczelnika poczty, rzekomo pomagającego jej wnuczce...



 Nowiny 24


## Metodą na wnuczka wyłudził 170 tys. zł od mieszkanki Lubziny. Ropczycka policja ujęła sprawcę. Grozi mu 12 lat ...

Brawa dla ropczyckich policjantów, którzy zatrzymali sprawcę oszustwa mieszkanki Lubziny. Wyłudził on kilka dni wcześniej od kobiety metodą...





# Metoda np. na wnuczka / policjanta

 Komenda Miejska Policji w Szczecinie

**UWAGA! Dzwonią późnym wieczorem! Oszuści metodą „na wnuczka” i „na policjanta” ponownie atakują w Szczecinie**

UWAGA! Dzwonią późnym wieczorem! Oszuści metodą „na wnuczka” i „na policjanta” ponownie atakują w Szczecinie - Aktualności - Nie po raz pierwszy ostrzegamy...



 tuLegnica.pl

**Seniorka oszukana metodą na wnuczka straciła 31 tysięcy złotych**

We wtorek Komenda Miejska Policji w Legnicy została zawiadomiona o popełnieniu kolejnego oszustwa metodą na wnuczka.



 TVN24

**Nowy Targ. Oszustwo "na wnuczka", seniorka straciła 55 tysięcy złotych. Oszuści zatrzymani z pieniędzmi w ...**

Trzy osoby podejrzane o wyłudzenie 55 tysięcy złotych metodą "na wnuczka" trafiły do aresztu. Kobieta zorientowała się, że została oszukana,...



# DEEPPFAKE

■ **Deepfake głosowy** - „(...) cyberprzestępcy korzystając z zaawansowanego oprogramowania zasilanego przez sztuczną inteligencję, klonują głosy (...) dowolnej osoby, a wystarczy do tego kilkusekundowe nagranie (...)”





# DEEPPFAKE

## LISTOPAD 2023 ROKU

## LUTY 2024 ROKU

### Wykorzystanie deepfake do "metody na wnuczka"

Wyjaśnienie pojęcia deepfake: *Deepfake to technologia wykorzystująca sztuczną inteligencję do generowania realistycznych filmów lub dźwięków, które są manipulacjami.* Deepfake wykorzystują techniki uczenia maszynowego i sztucznych sieci neuronowych do naśladowania wyglądu, głosu i manier osoby, tworząc fałszywe materiały wideo lub audio, które mogą wyglądać i brzmieć jak rzeczywiste. Technologia ta jest coraz częściej wykorzystywana w działaniach przestępczych.

Historia tego przestępstwa rozpoczęła się tak, jak wiele tego typu znanych historii. Do starszej Pani zadzwonił mężczyzna przedstawiający się jako policjant i poinformował, że jej córka miała wypadek i potrzebuje pomocy. Nowością w tego typu metodzie jest fakt, że (zgodnie z relacją poszkodowanej) w kolejnym etapie, od rzekomego policjanta słuchawkę przejęła „jej córka”. Następnie głosem podszywający się pod córkę została przekazana informacja, że potrzebne jest 70 000zł w gotówce, aby uniknąć pójścia do więzienia za spowodowanie wypadku drogowego. Rozmowy odbyły się dwie, pierwsza trwała ponad 1 min, kolejna była już krótsza, bardziej mająca na celu ponaglenie (trwała ok. 30s). Zgodnie z pozyskanym opisem w tle nie było słyhać żadnych głosów ani podczas rozmowy z „policjantem”, ani „córką”. Rozmowa odbywała się płynnie (co może oznaczać, że przestępcy korzystali z narzędzia do deepfake live) jednak przez stres przy pierwszym połączeniu, ofiara nie zadała zbyt wielu pytań. Przy drugiej rozmowie była świadoma oszustwa, po serii pytań, przestępcy początkowo odpowiadali, potem rozłączyli się.

Osoba, pod której głos się podszywano, w krótki czasie przez tym zdarzenie otrzymała kilka połączeń telefonicznych a’la ankieterzy. Istnieje podejrzenie mówiące, że mogła w ten sposób zostać nagrana próbka jej głosu, jednak nie posiadamy dowodów wskazujących, że na pewno miało to miejsce. Podczas oszustwa numer telefonu córki nie był spoofowany, wyświetlił się jako zastrzeżony.

W opisanym wyżej przypadku, ofiara została w porę ostrzeżona dzięki czemu nie podjęła działań dyktowanych przez przestępców, należy mieć jednak na uwadze fakt, że wykorzystanie technologii deepfake, mającej ogromne możliwości wynosi działania przestępcze na nowy poziom, dający atakującym pakiet, nieznanych do tej pory, możliwości. Z jednej strony mogą oni tworzyć nowe scenariusze działania, z drugiej udoskonalają te z których korzystają od lat, sprawiając, że manipulacja i stosowana socjotechnika będzie jeszcze trudniejsza do odkrycia, dla standardowego „użytkownika Internetu”. W Polsce obecnie najwięcej przypadków wykorzystania technologii deepfake do przestępstwa obserwujemy w przygotowanych nagraniach video w scenariuszach znanych pod nazwą "fraud inwestycyjny" (opisany w cyklu schematów, dostępny [tutaj](#)), czy kampaniach podszywających się pod Elona Muska i oferujące rzekomą możliwość odebrania ETC. Za granicą krajobraz ten jest jednak znacznie szerszy i prognozuje się, że również na rynku polskim ataki tego typu będą pojawiać się coraz częściej.

„ Opowiem Wam historię o kolejnym „numerze” przez telefon. Niedawno moja znajoma otrzymała pewien telefon, a głos w słuchawce oznajmił, że jest prokuratorem. Po przedstawieniu się rozmówcy, pan prokurator przeszedł do rzeczy. Otóż ów Pan miał wstrząsającą wiadomość, poinformował znajomą o tym, że jej syn Adam jest rzekomo sprawcą tragicznego wypadku drogowego, do którego doszło w konkretnym miejscu (wskazany został nawet numer drogi), a w wyniku śmierć poniosła jedna niewinna osoba. Cała sytuacja nabrała jeszcze bardziej przerażającego obrotu oraz wiarygodności, gdy pan prokurator przekazał do telefonu syna. I w tym momencie matka usłyszała głos swojego syna Adama w słuchawce telefonu, który powiedział jej, że zabił człowieka i potrzebuje pieniędzy, aby jakoś rozwiązać tę dramatyczną sytuację...

Matka była w szoku, jednak rzekomy prokurator swojego celu nie osiągnął. Siostra Pana Adama, towarzysząca akurat mamie, zareagowała prawidłowo. Zadzwoniła do swojego brata, a ten odebrał – był bardzo zaskoczony, ale nie znajdował się na wskazanej drodze, a w pracy, jak zazwyczaj. Do przekazania pieniędzy więc nie doszło, dzięki szybkiej reakcji rodziny. Tym razem przestępcom się nie udało, jednak coraz więcej słyszy się o podobnych sytuacjach, a wykorzystanie głosu członka rodziny daje atakującym ogromną przewagę.

Źródło: <https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf>

Źródło: [https://sekurak.pl/oszustwo-przez-telefon-objasniamy-jak-dzialaja-przestepcy-na-podstawie-prawdziwego-incydentu?trk=public\\_post\\_comment-text](https://sekurak.pl/oszustwo-przez-telefon-objasniamy-jak-dzialaja-przestepcy-na-podstawie-prawdziwego-incydentu?trk=public_post_comment-text)

Materiały szkoleniowe przygotowane zostały w ramach projektu Centrum Edukacji dla Uczestników Rynku – CEDUR. Autorskie prawa majątkowe do prezentowanych oraz przekazywanych materiałów są własnością Urzędu Komisji Nadzoru Finansowego (UKNF). Rozpowszechnianie, kopiowanie, utrwalanie, publiczne wykorzystywanie całości lub części dozwolone jest jedynie w celach niekomercyjnych, nieodpłatnie, za zgodą UKNF, pod warunkiem podania informacji o pochodzeniu materiałów. Stan prawny informacji zawartych w materiałach jest aktualny na dzień ogłoszenia prezentacji. Materiały przeznaczone są wyłącznie dla odbiorców określonych w programie seminarium, dostępnym na stronie [www.knf.gov.pl](http://www.knf.gov.pl). Prezentowane treści mają wyłącznie charakter ogólny i informacyjny, i nie stanowią porady prawnej oraz inwestycyjnej. UKNF nie ponosi odpowiedzialności za jakiegokolwiek decyzje podjęte przez odbiorców prezentacji w sprawach ich dotyczących lub za decyzje inwestycyjne podejmowane na rynku finansowym, w oparciu o informacje przekazane w prezentacji, ponieważ decyzje te powinny być każdorazowo przeanalizowane w ramach konkretnego stanu faktycznego, który w zależności od okoliczności, podmiotu, który decyzje podejmuje, potrzeb, założonych celów oraz posiadanych środków będzie uzasadniał zastosowanie adekwatnych działań, w tym przyjęcie konkretnego ryzyka, w celu osiągnięcia oczekiwanych skutków, które decyzja ma wywołać. W indywidualnych przypadkach należy skontaktować się z Urzędem Komisji Nadzoru Finansowego.



## 2/3 Cyberhigiena: scenariusze przestępcze...

- oszustwa inwestycyjne
- metoda np. na wnuczka / policjanta

# WIELE INNYCH, BO...

## 2/3 Cyberhigiena: scenariusze przestępcze...

# PRZESTĘPCÓW OGRANICZA TYLKO KREATYWNOŚĆ

# 3/3 Cyberhigiena: jak nie dać się oszukać

- weryfikacja adresu strony internetowej



# Weryfikacja domeny...



Domena!

<https://strona.abc/dalsza/czesc/adresu>

Adres URL

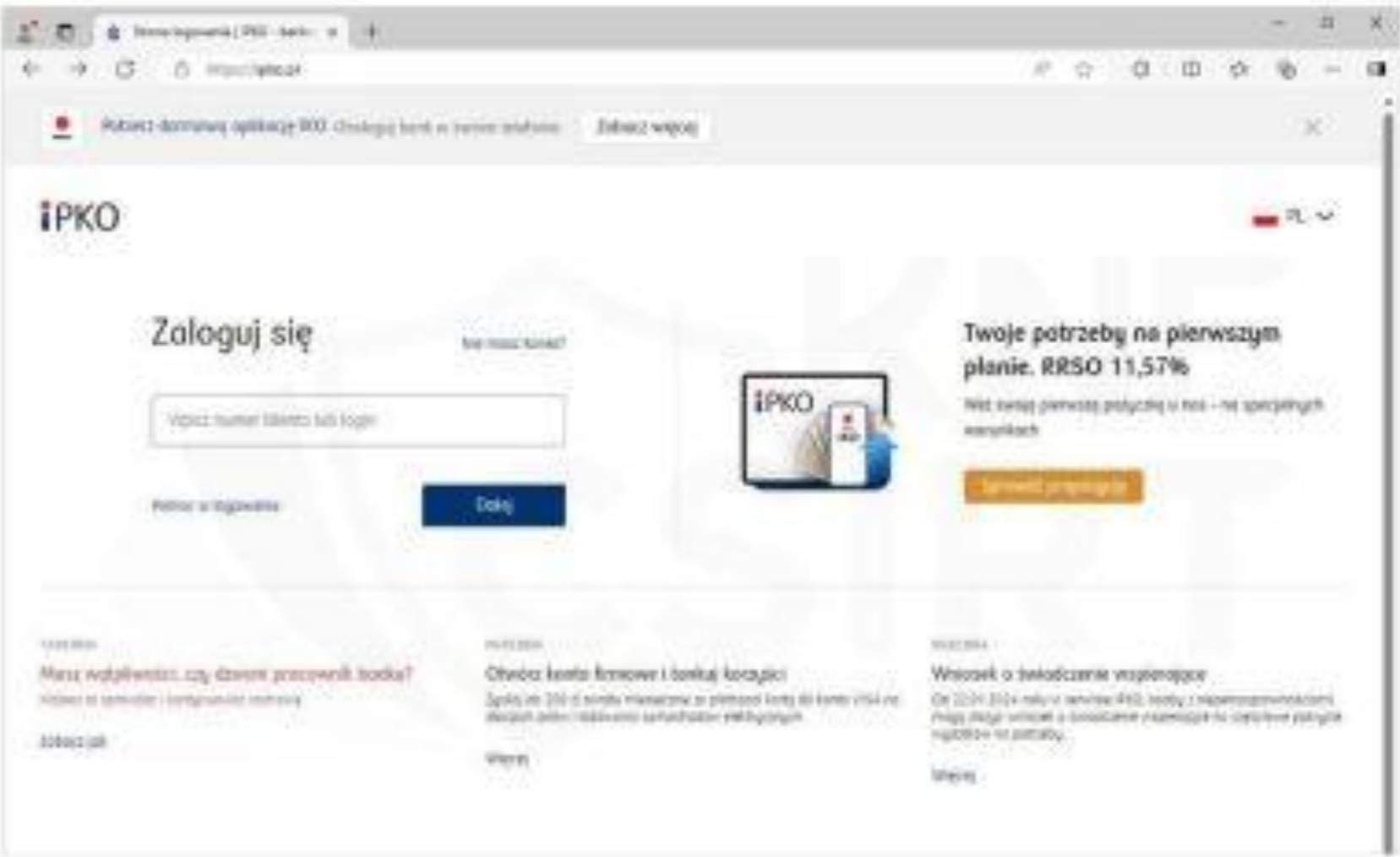
**Fałszywa domena**

<https://pkobp.info/VerificationUid=39495023/verify324.php>



**Prawdziwa domena**

<https://ipko.pl/>



## 3/3 Cyberhigiena: złote zasady jak nie dać się oszukać

- weryfikacja adresu strony internetowej
- dodanie adresu strony swojego banku do zakładek
- szczególna uwaga na pojawiające się przy wynikach wyszukiwania pogrubiony napis „reklama”
- dokładne czytanie treści wiadomości SMS z kodem autoryzacyjnym, zawierających opis dokonywanej transakcji...

# ZASADY OGRANICZONEGO ZAUFANIA

## 3/3 Cyberhigiena: a jak już się zdarzy...

- szybki telefon do Banku – TO NIE WSTYD
- blokada możliwości wykorzystania danych, które poznał oszust
- reklamacja w Banku
- zgłoszenie się na policję

## Co robić zawsze?

**Śledzić informacje o przestępstwach  
i ostrzegać innych!**



# Media społecznościowe - @CSIRT KNF

- Facebook
- Twitter
- LinkedIn
- Strona internetowa – CEBRF [<https://cebrf.knf.gov.pl/>]

**KNF CSIRT** **CSIRT KNF @CSIRT\_KNF** · 10 sie

Oszuści, aby uśpić czujność użytkowników, tworzą fałszywe witryny jak najbardziej zbliżone do oryginalnych. Zachęcamy do zapoznania się z naszą grafiką, prezentującą przykładowe domeny wykorzystywane w atakach. Pamiętajcie, aby dokładnie weryfikować adres strony Waszego banku! 🇵🇱

**UWAGA NA FAŁSZYWE STRONY BANKOWOŚCI ELEKTRONICZNEJ!**

Prawdziwe domeny	Fałszywe domeny
centrum24.pl	centrum24.cc
secure.getinbank.pl	secured-getin.com
pekao24.pl	logowanie-pekao24.pl
bnpparibas.pl	bnpparilas.in
aliorbank.pl	aliorbank-pl.com
ipko.pl	iko-pkobpi.com

OVERVIEW OF SELECTED SCAMS  
March 2024

OVERVIEW OF SELECTED SCAMS - MARCH 2024

15 kwiecień 2024

czytaj więcej

PRZEGLĄD WYBRANYCH OSZUSTW  
Marzec 2024

PRZEGLĄD WYBRANYCH OSZUSTW INTERNETOWYCH - MARZEC 2024

09 kwiecień 2024

czytaj więcej

PRZEGLĄD WYBRANYCH OSZUSTW  
Styczeń 2024

PRZEGLĄD WYBRANYCH OSZUSTW INTERNETOWYCH - STYCZEŃ 2024

09 luty 2024

czytaj więcej

JAK SZTUCZNA INTELIGENCJA PRZETWARZA DANE

JAK SZTUCZNA INTELIGENCJA PRZETWARZA DANE

24 styczeń 2024

czytaj więcej

OVERVIEW OF SELECTED SCAMS  
December 2023

OVERVIEW OF SELECTED SCAMS - DECEMBER 2023

18 styczeń 2024

czytaj więcej

PRZEGLĄD WYBRANYCH OSZUSTW  
Grudzień 2023

PRZEGLĄD WYBRANYCH OSZUSTW INTERNETOWYCH - GRUDZIEŃ 2023

16 styczeń 2024

czytaj więcej

SZTUCZNA INTELIGENCJA

WPROWADZENIE DO SZTUCZNEJ INTELIGENCJI

08 styczeń 2024

czytaj więcej

OVERVIEW OF SELECTED SCAMS  
November 2023

OVERVIEW OF SELECTED SCAMS - NOVEMBER 2023

18 grudzień 2023

czytaj więcej



# Media społecznościowe - @CSIRT KNF



OVERVIEW OF  
SELECTED SCAMS -  
MARCH 2024

2024

[czytaj więcej](#)



PRZEGLĄD  
WYBRANYCH  
OSZUSTW  
INTERNETOWYCH -  
MARZEC 2024

09 kwiecień 2024

[czytaj więcej](#)



PRZEGLĄD  
WYBRANYCH  
OSZUSTW  
INTERNETOWYCH -  
STYCZEŃ 2024

09 luty 2024

[czytaj więcej](#)



JAK SZTUCZNA  
INTELIGENCJA  
PRZETWARZA DANE

24 styczeń 2024

[czytaj więcej](#)



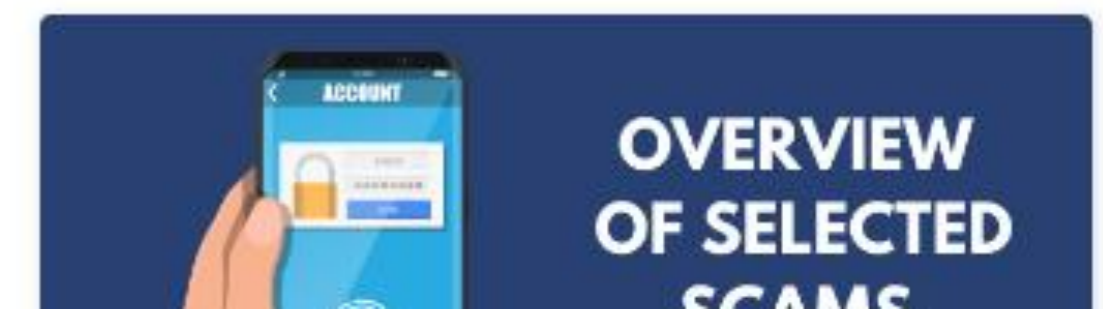
OVERVIEW OF  
SELECTED  
SCAMS



PRZEGLĄD  
WYBRANYCH  
OSZUSTW



KNF  
CSIRT



OVERVIEW OF  
SELECTED  
SCAMS



# PYTANIA I ODPOWIEDZI



# Dziękujemy za uwagę

Zapraszamy na profile UKNF  
[X \(Twitter\)](#) [Facebook](#) [Instagram](#) [LinkedIn®](#) [YouTube](#)

**Departament Cyberbezpieczeństwa**  
tel. +48 22 262 55 90, dcb@knf.gov.pl  
Urząd Komisji Nadzoru Finansowego  
ul. Piękna 20, 00-549 Warszawa  
[\*\*www.knf.gov.pl\*\*](http://www.knf.gov.pl)