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

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

„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 fałszywa stronę, czy w Internecie można być anonimowym, dobre praktyki korzystania z urządzeń elektronicznych

Agata Ślusarek
Departament Cyberbezpieczeństwa
Urząd Komisji Nadzoru Finansowego
24 kwietnia 2024 roku

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. Prezentowane treści mają wyłącznie charakter ogólny i informacyjny, i nie stanowią ani porady prawnej, ani inwestycyjnej. UKNF nie ponosi odpowiedzialności za jakiekolwiek 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

źródło: Materiały CSIRT KNF

Dlaczego robimy, to co robimy?

Liczne zadania, m.in.:

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

źródło: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-

Przestępstwa w Internecie

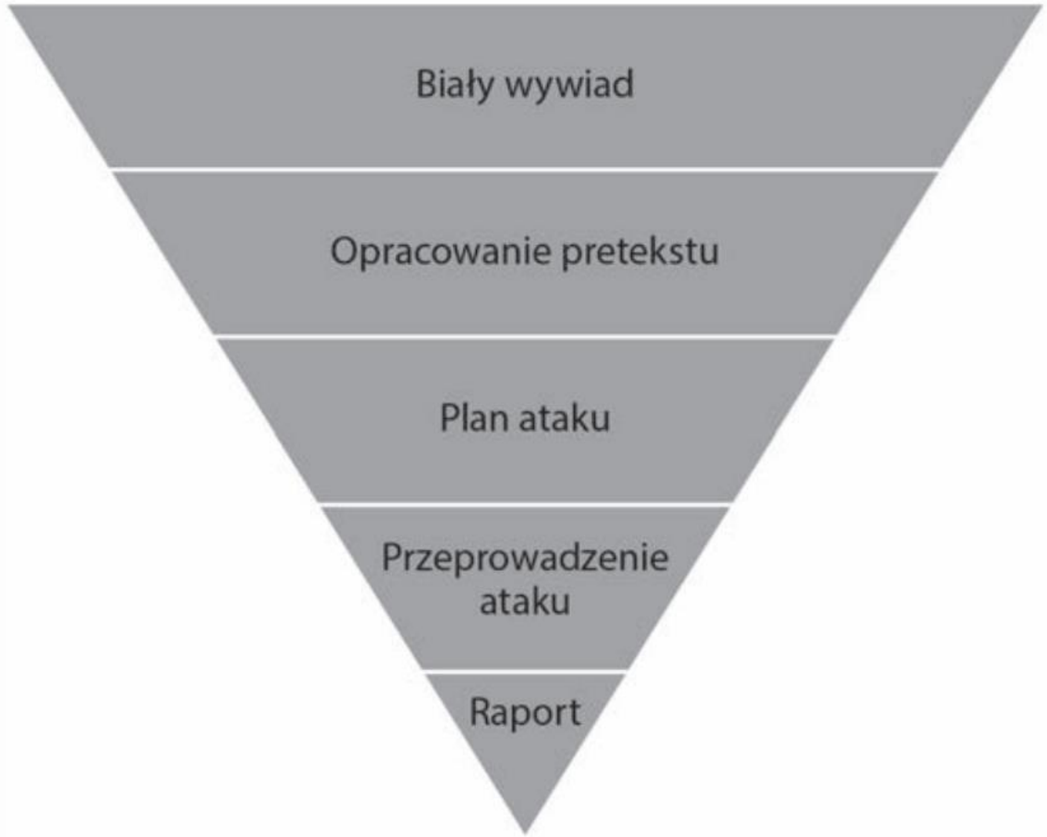
1. Jakich metod używają przestępcy
2. Jak najczęściej oszukują
3. Które informacje chcą ukraść

źródło: Materiały CSIRT KNF

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**



Źródło: Socjotechnika. Sztuka zdobywania władzy nad umysłami., Christopher Hadnagy

Źródło: Socjotechnika, sztuka zdobywania…, Wiley

Dlaczego ataki socjotechniczne są skuteczne?

„NAJSŁABSZYM OGNIWEM JEST CZŁOWIEK”

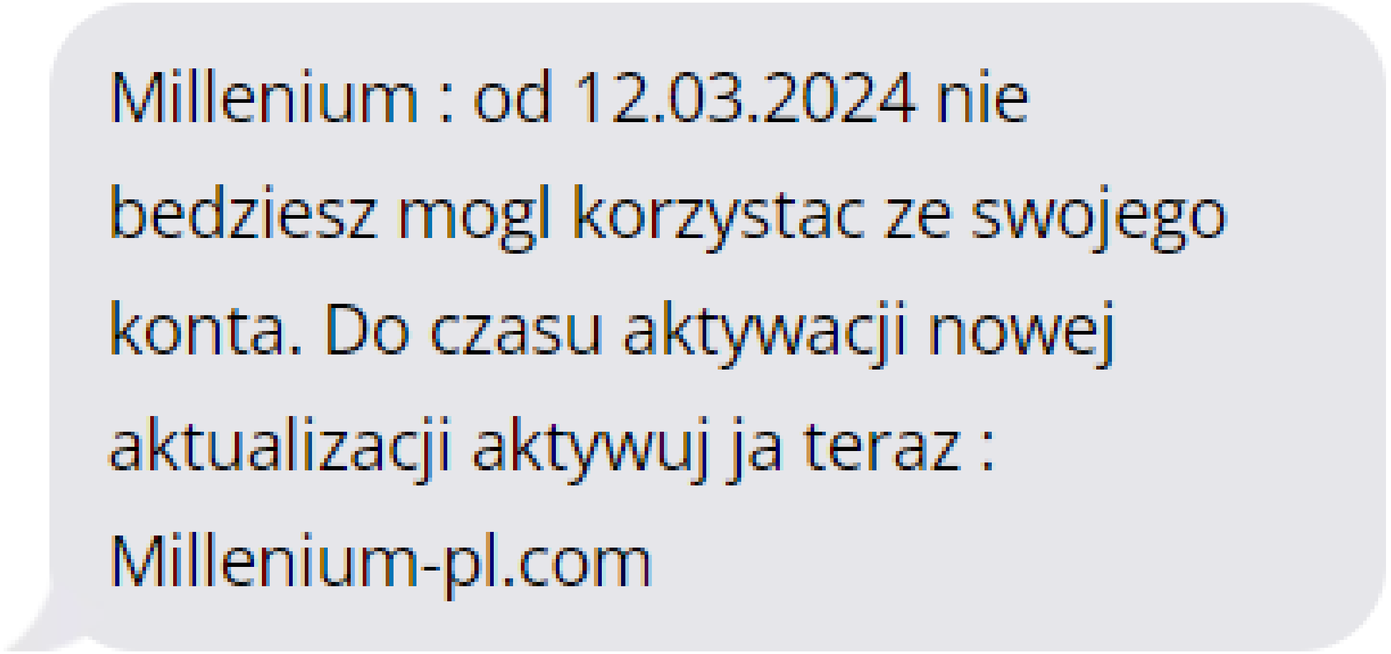
- niedostateczna czujność
- braki szkoleniowe / brak świadomości
- poczucie bezpieczeństwa
- przyzwyczajenia, nawyki
- przeświadczenia, że mnie to nie dotyczy

źródło: Materiały CSIRT KNF

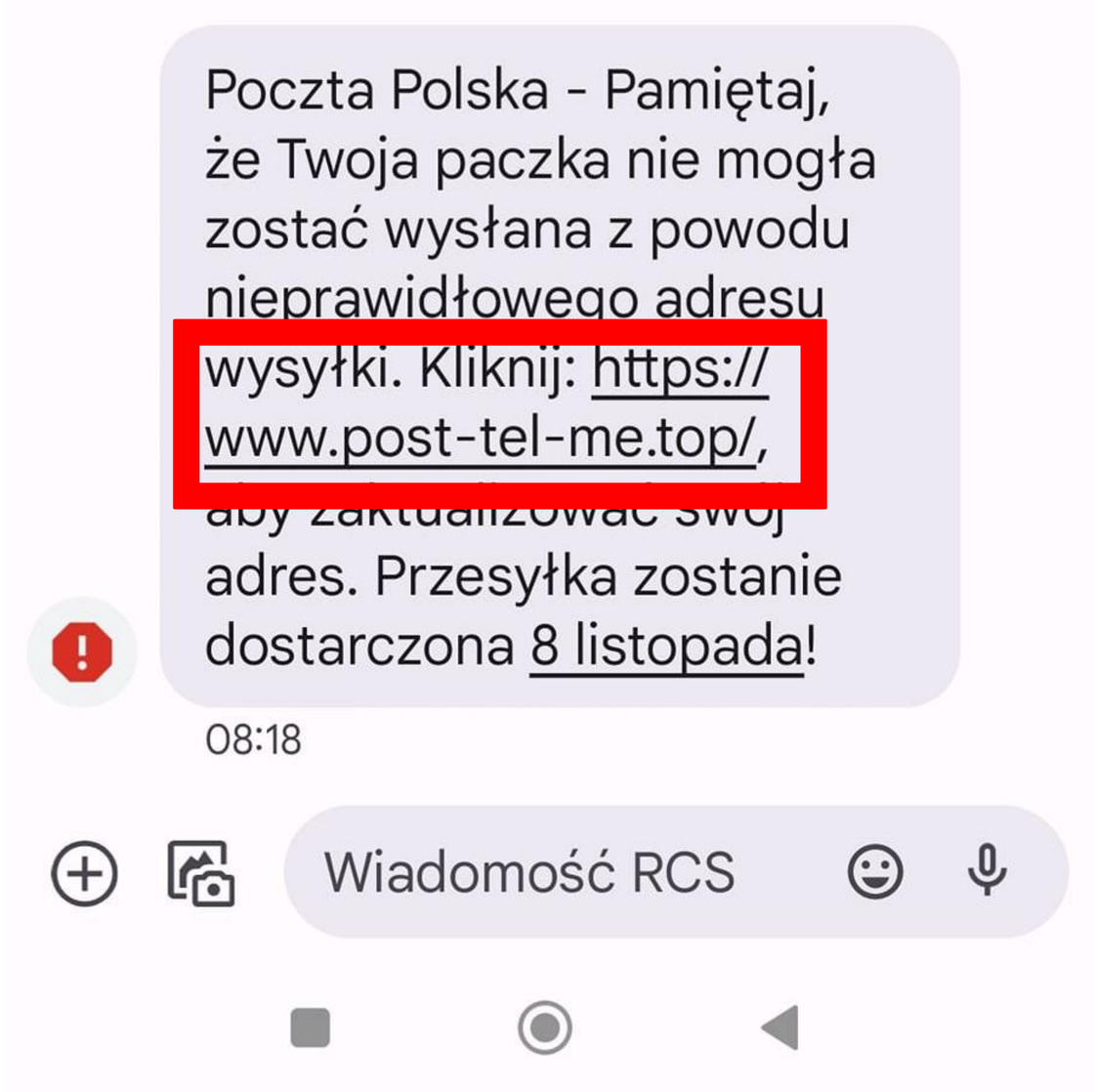
2/3 Przestępstwa w Internecie: jak oszukują…

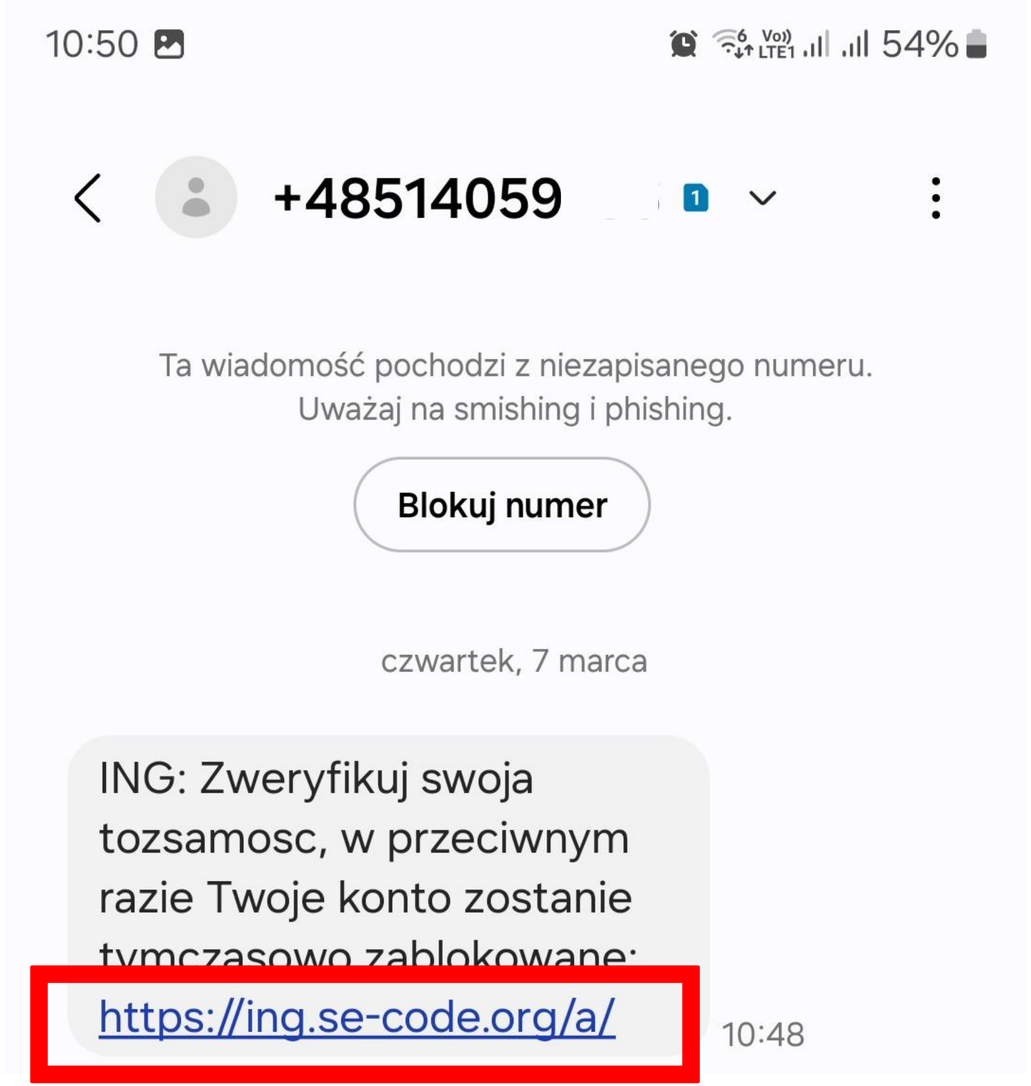
Jak możemy zostać „zaatakowani”?

- wiadomości SMS

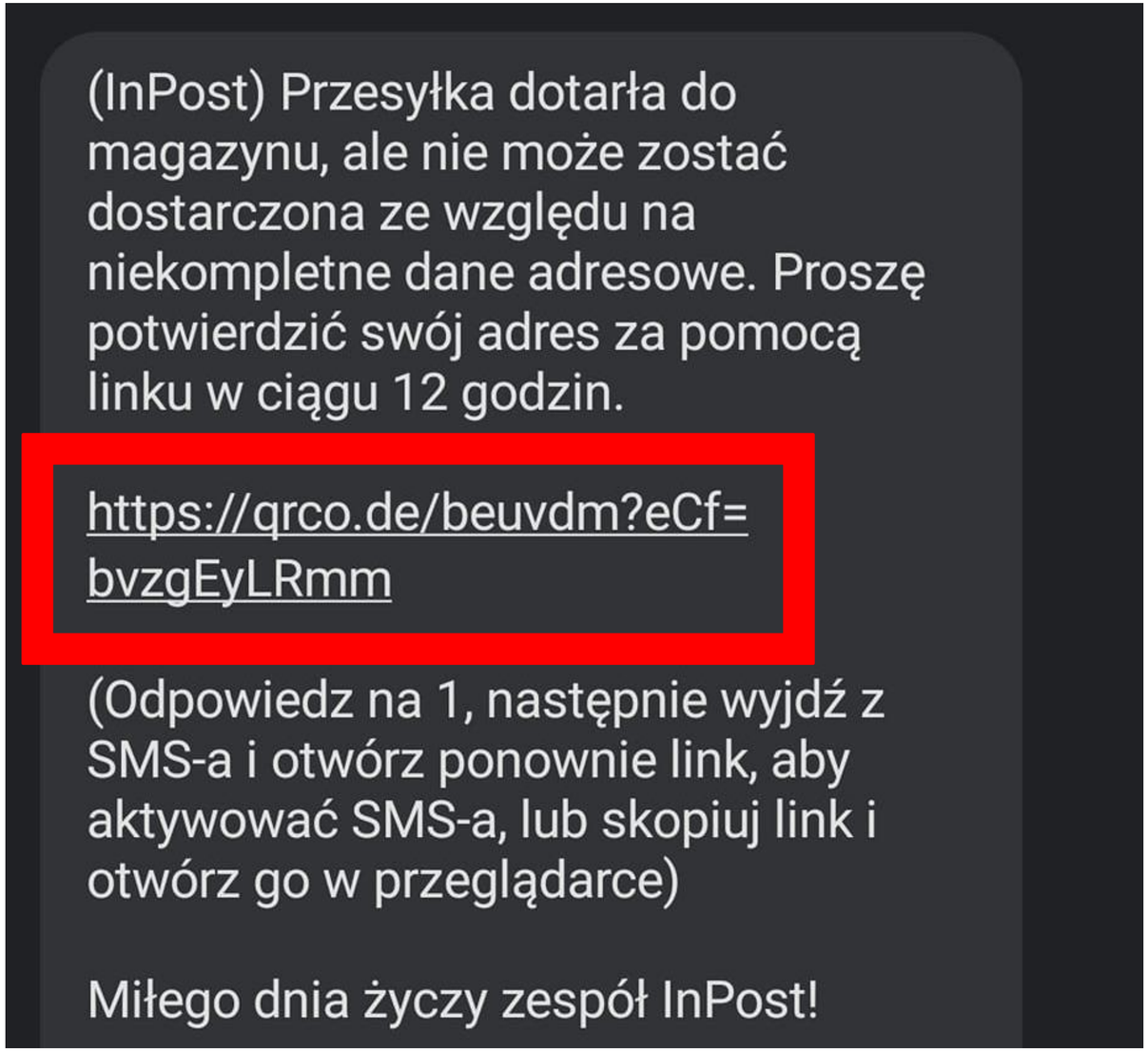


źródło: Materiały CSIRT KNF





źródło: Materiały CSIRT KNF

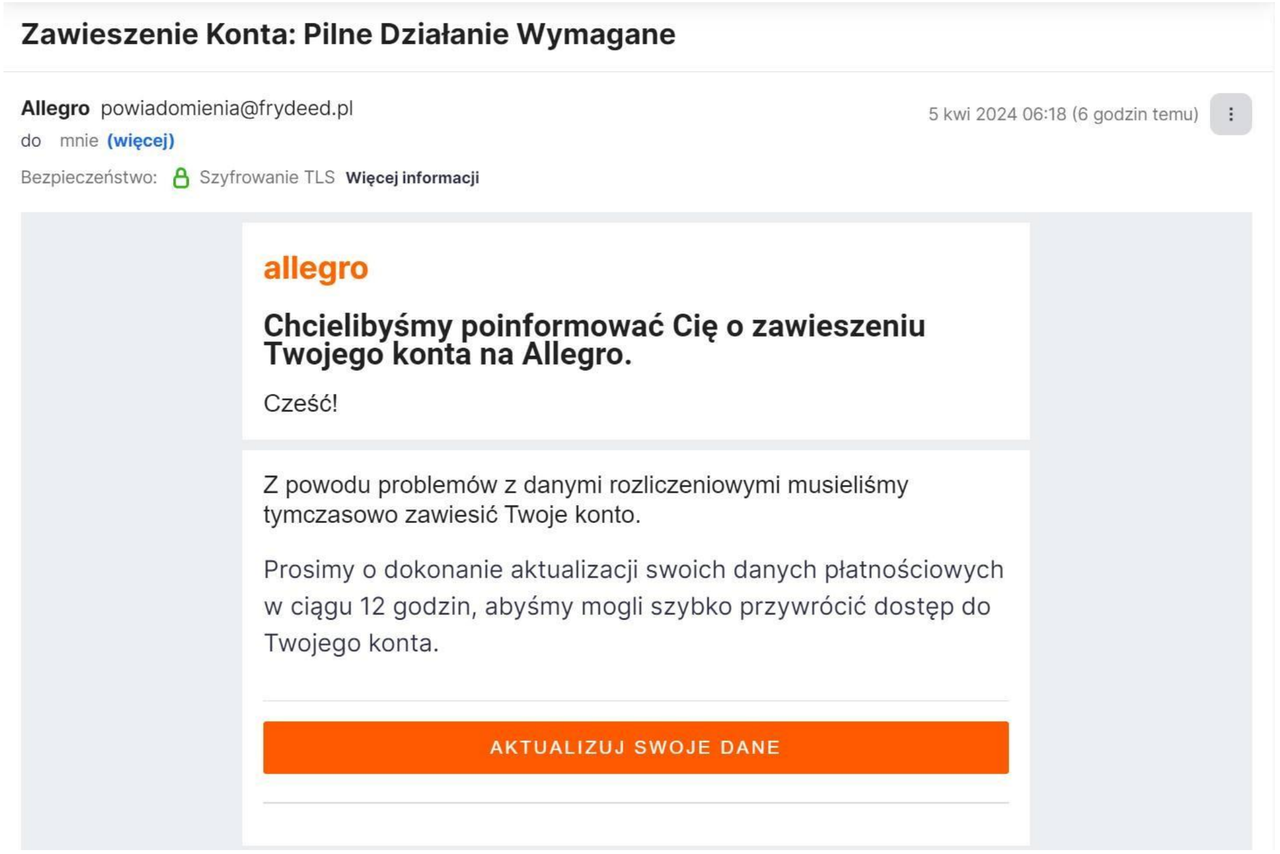


źródło: Materiały CSIRT KNF

2/3 Przestępstwa w Internecie: jak oszukują…

Jak możemy zostać „zaatakowani”?

- wiadomości SMS,
- wiadomość e-mail



źródło: Materiały CSIRT KNF

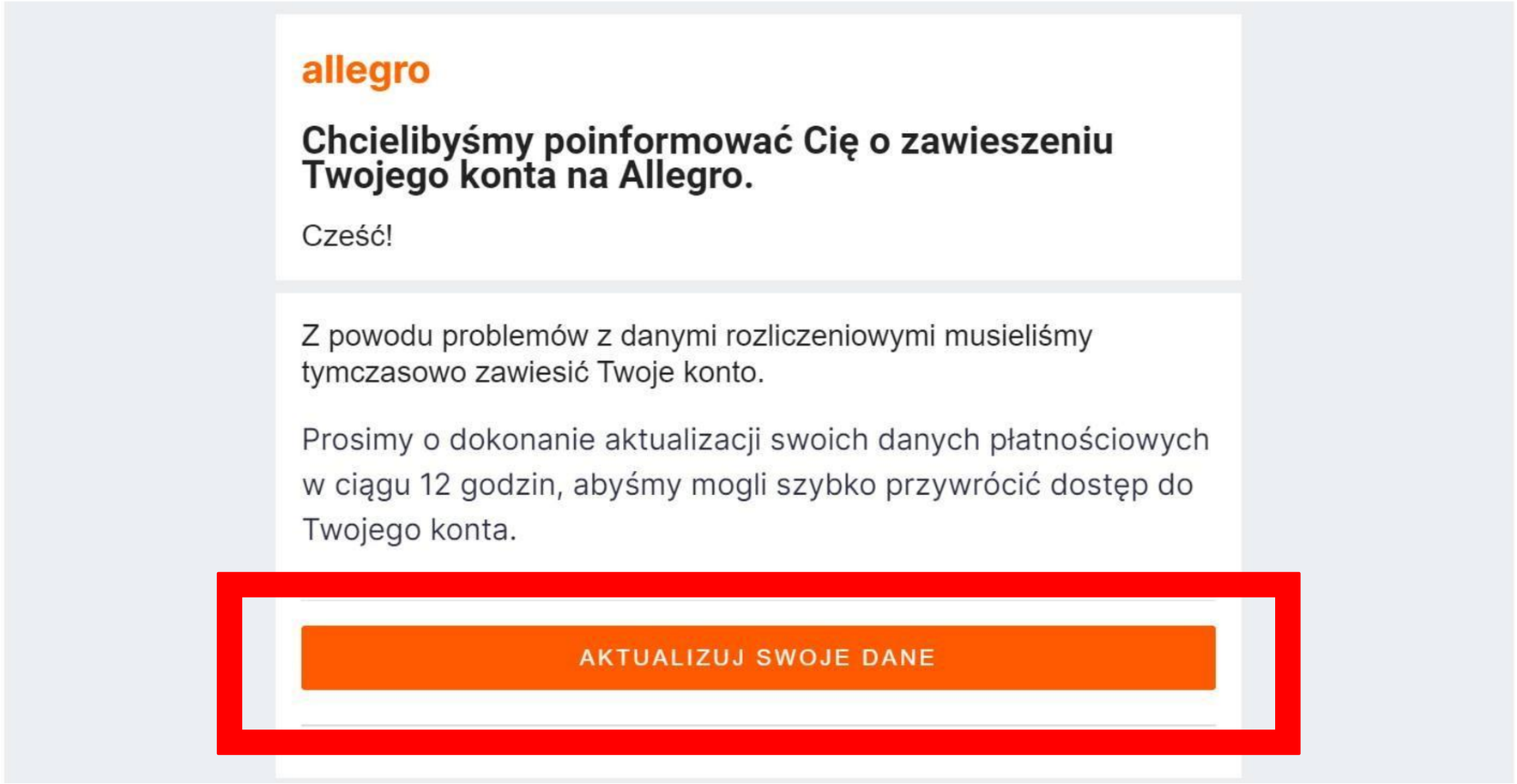
Zawieszenie Konta: Pilne Działanie Wymagane

Allegro powiadomienia@frydeed.pl

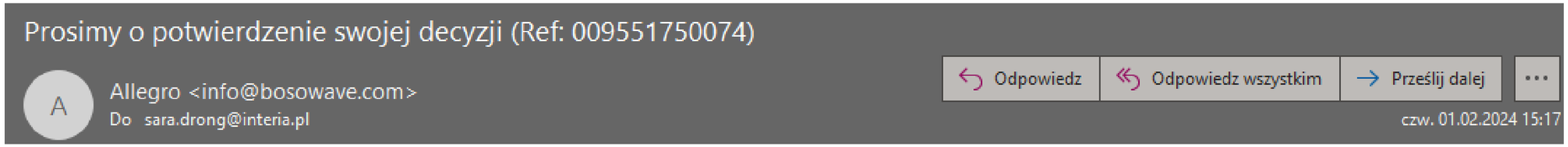
do mnie **(więcej)**

5 kwi 2024 06:18 (6 godzin temu)

Bezpieczeństwo: Szyfrowanie TLS **Więcej informacji**



źródło: Materiały CSIRT KNF



Allegro.pl Marketplace

Szanowny,

Z przyjemnocią informujmy, że została przeprowadona korekta poprzednich zamówień na twoim koncie. Zgodnie z tym, przysługuje Ci zwrot środków w wysokości 130.12 zł.

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

rzez kliknięcie poniższego przcisku:

https://aexperfumarias.com.br/news/103357914995
Kliknij lub naciśnij, aby śledzić link.

Odbierz Środki

ajbliższych dni, zastrzegamy sobie prawo do zawieszenia twojego konta na Alegro.pl, a kwota środków zostanie skaowana.

Dziękujemy za zrozumienie i czekamy natwoją decyzję.

Z poważaniem,
Zespół Allegro.pl

źródło: Materiały CSIRT KNF

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.

źródło: Materiały CSIRT KNF

2/3 Przestępstwa w Internecie: jak oszukują…

Jak możemy zostać „zaatakowani”?

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

źródło: Materiały CSIRT KNF

Bank PL
Sponsorowane
Identyfikator biblioteki: 713883334291149

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

Bank Pekao

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

Dowiedz się...

UrbanCard Wrocław
Sponsorowane
Identyfikator biblioteki: 978581093665517

PLWraz z nadejściem wiosny MPK oferuje:
Ciesz się darmowymi przejazdami przez 90 dni z Wrocławska Karta Miejska 🔥
✅ 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

źródło: Materiały CSIRT KNF

Farghly Blax
Sponsorowane ·

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

TODAYSFASHION.XYZ

Tragiczny koniec Jerzego Owsiaka! Dzisiejsza wiadomość zszokowała wszystkich!

Dowiedz się więcej

źródło: Materiały CSIRT KNF

JAK ROZPOZNAĆ FAŁSZYWĄ REKLAMĘ INWESTYCYJNĄ?

1. Reklama wyświetlana z profilu o niskim poziomie zaufania.

2. Tekst mający na celu zachęcenie do potencjalnej inwestycji.

3. Używane jest logo zaufanych podmiotów.

4. W reklamach wykorzystywane są wizerunki znanych osób.

5. Informacja o wysokich zyskach w krótkim czasie.

6. Informacja o ofercie ograniczonej czasowo.

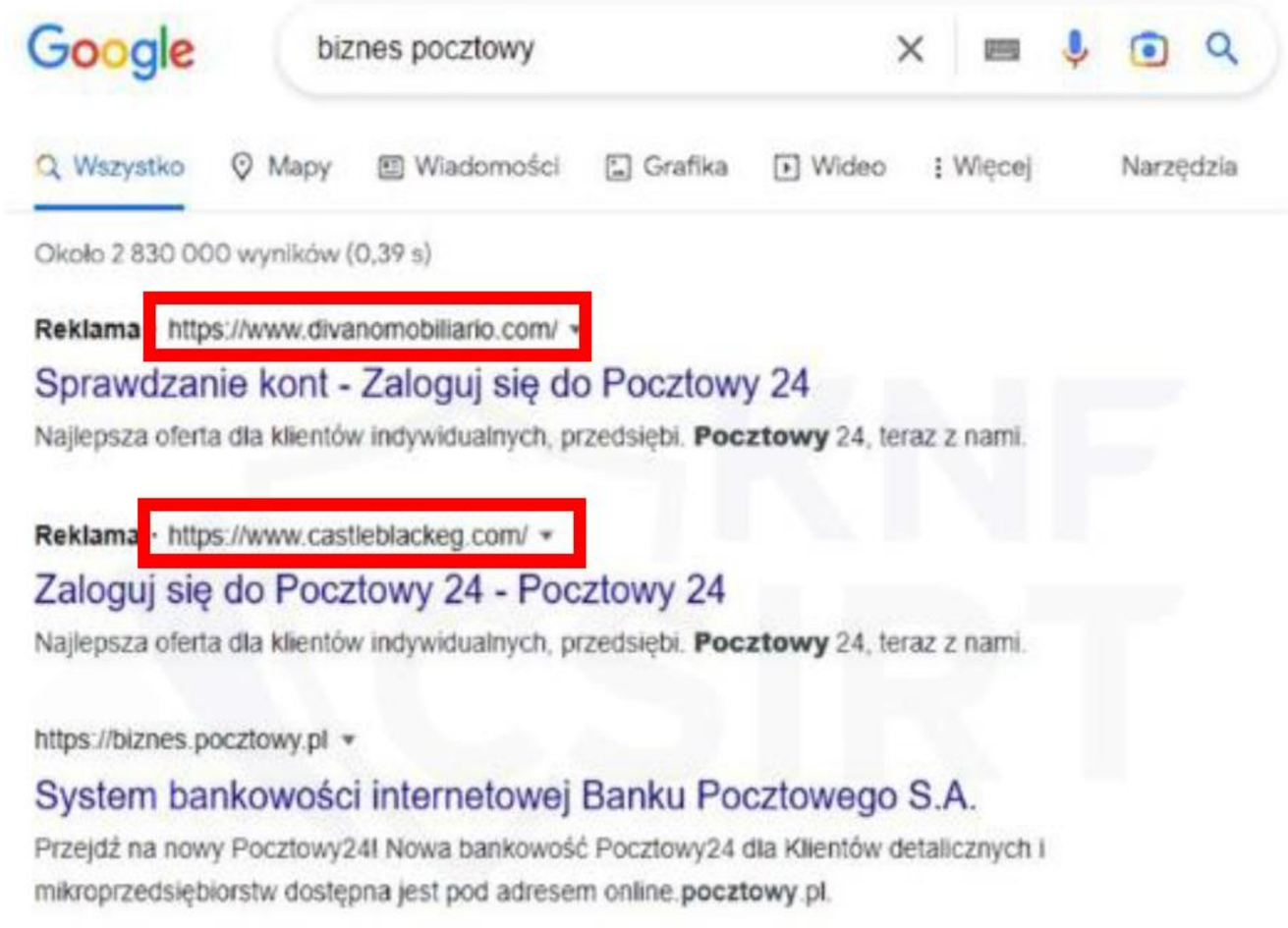
źródło: Materiały CSIRT KNF

2/3 Przestępstwa w Internecie: jak oszukują…

Jak możemy zostać „zaatakowani”?

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

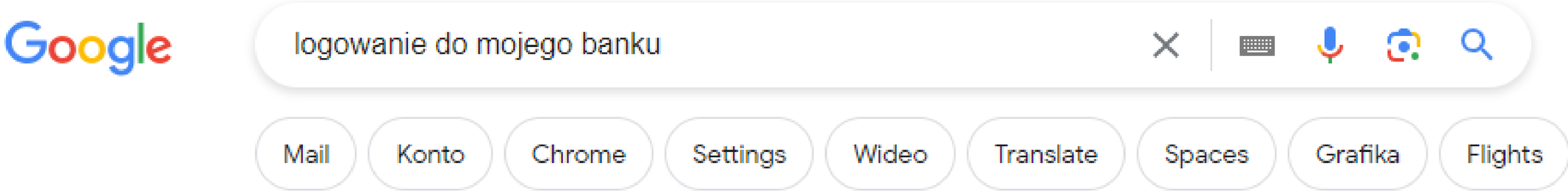
źródło: Materiały CSIRT KNF



FAŁSZYWE STRONY

PRAWDZIWA STRONA

źródło: Materiały CSIRT KNF



Te strony wyświetlą się jako pierwsze!

źródło: Materiały CSIRT KNF

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!

źródło: Materiały CSIRT KNF

VISHING…

TO WIDZIMY

TO JEST NAPRAWDĘ

Źródło: silentbreach.com; incibe.es/

VISHING – za kogo podają się przestępcy?

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

Źródło: https://silentbreach.com/

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?”*
- …

Źródło: opracowanie własne

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?

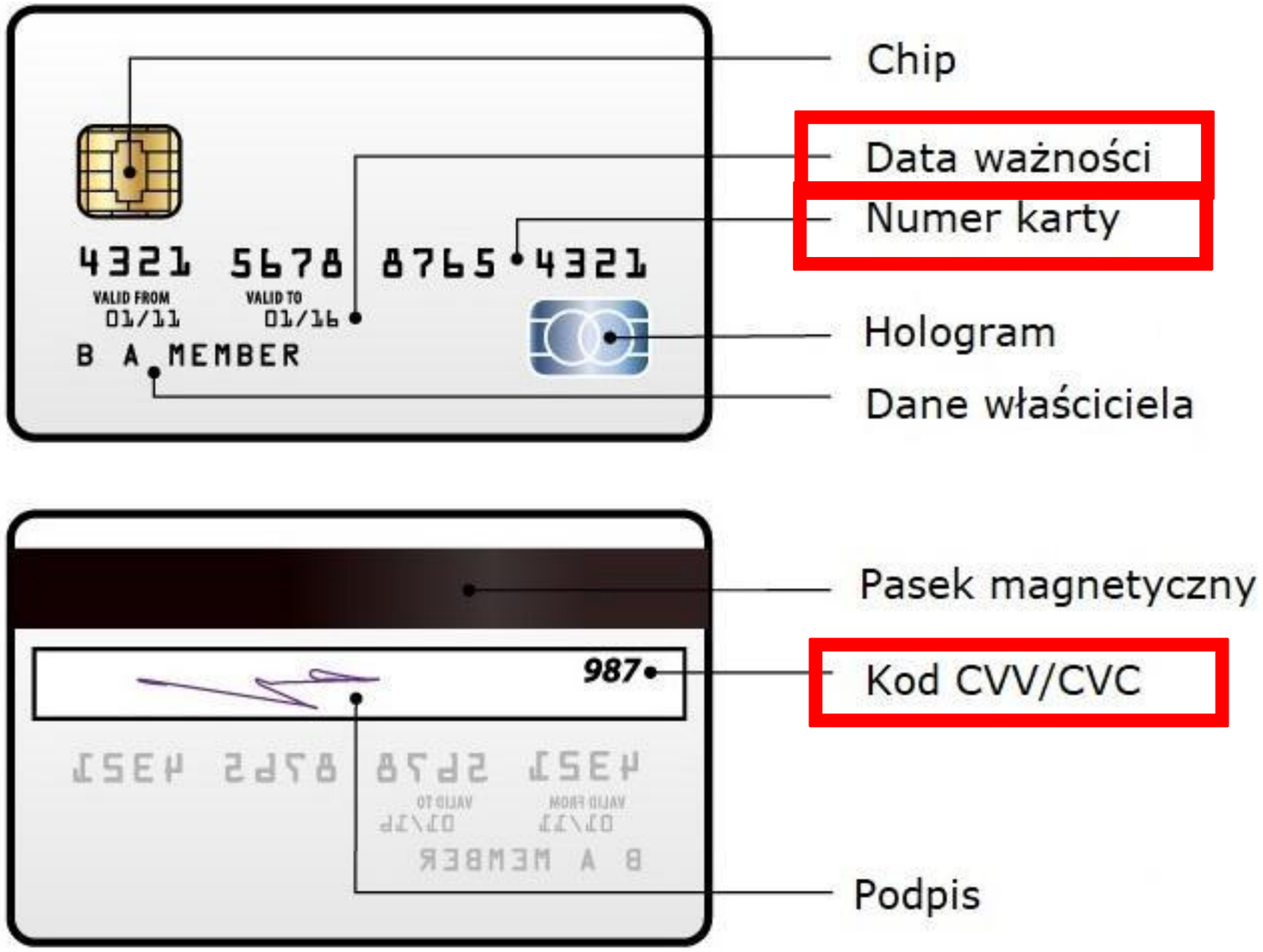
WSZYSTKO, DZIĘKI CZEMU OSZUŚCI SIĘ WZBOGACĄ…

2/3 Przestępstwa w Internecie: co chcą ukraść…

Co możemy stracić?

- dane uwierzytelniające do bankowości elektronicznej
- dane kart płatniczych

źródło: Materiały CSIRT KNF



+ KOD SMS (3D Secure)

źródło: bankier.pl

2/3 Przestępstwa w Internecie: co chcą ukraść…

Co możemy stracić?

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

źródło: przelewy24.pl

2/3 Przestępstwa w Internecie: co chcą ukraść…

Co możemy stracić?

- dane uwierzytelniające do bankowości elektronicznej
- dane kart płatniczych
- kody BLIK
- bezpośrednie przelewy…

źródło: przelewy24.pl

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

„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

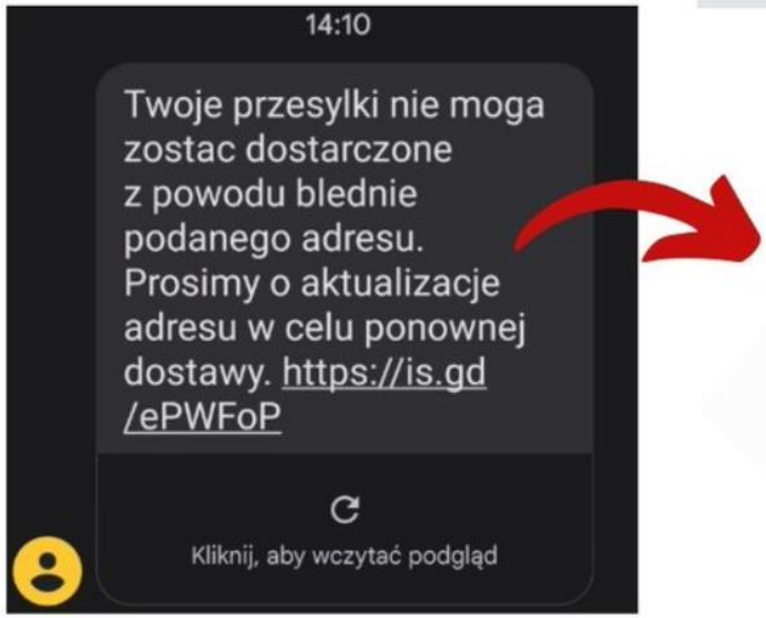
Agata Ślusarek
Departament Cyberbezpieczeństwa
24 kwietnia 2024 roku

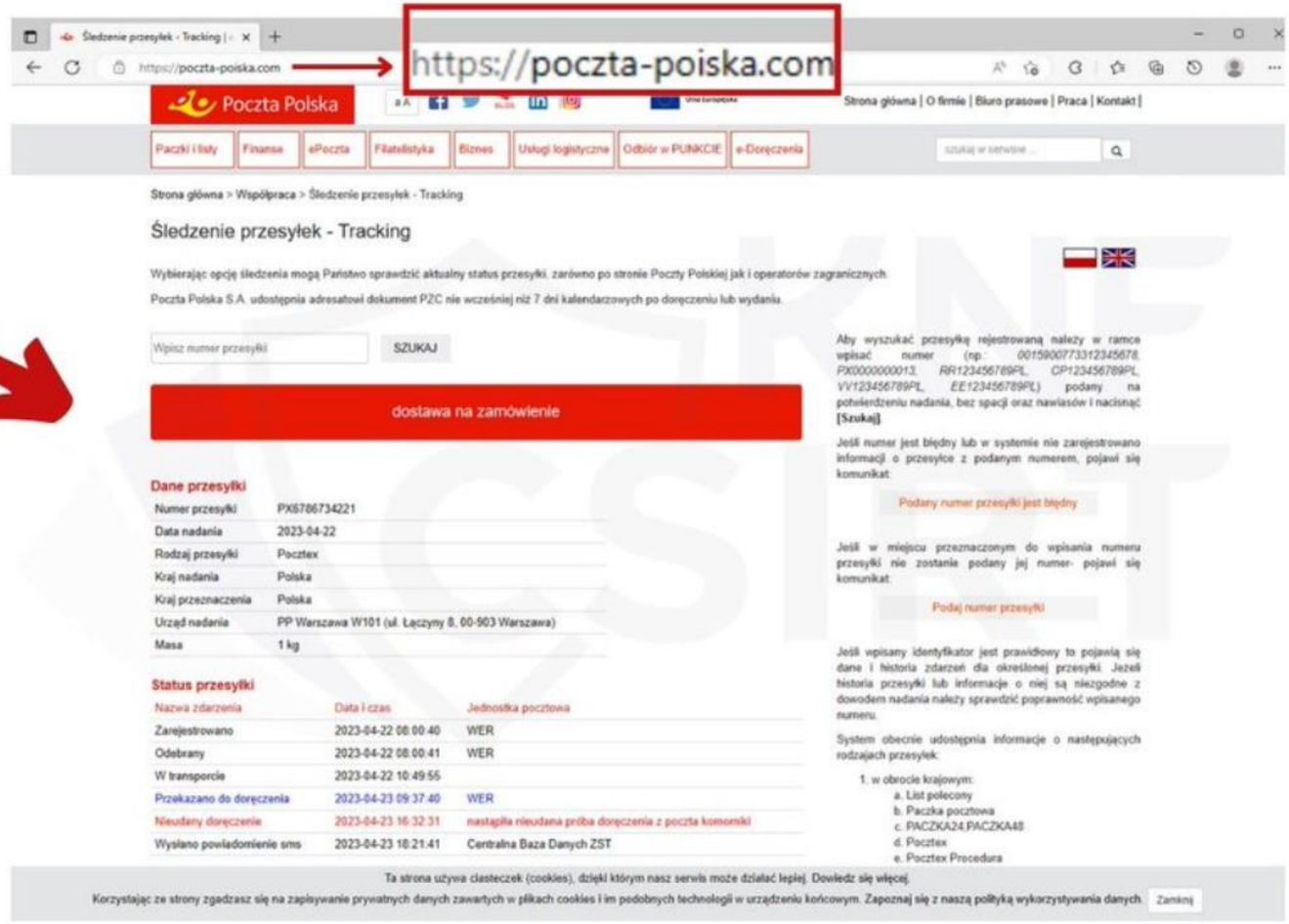
Cyberhigiena:

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

źródło: Materiały CSIRT KNF

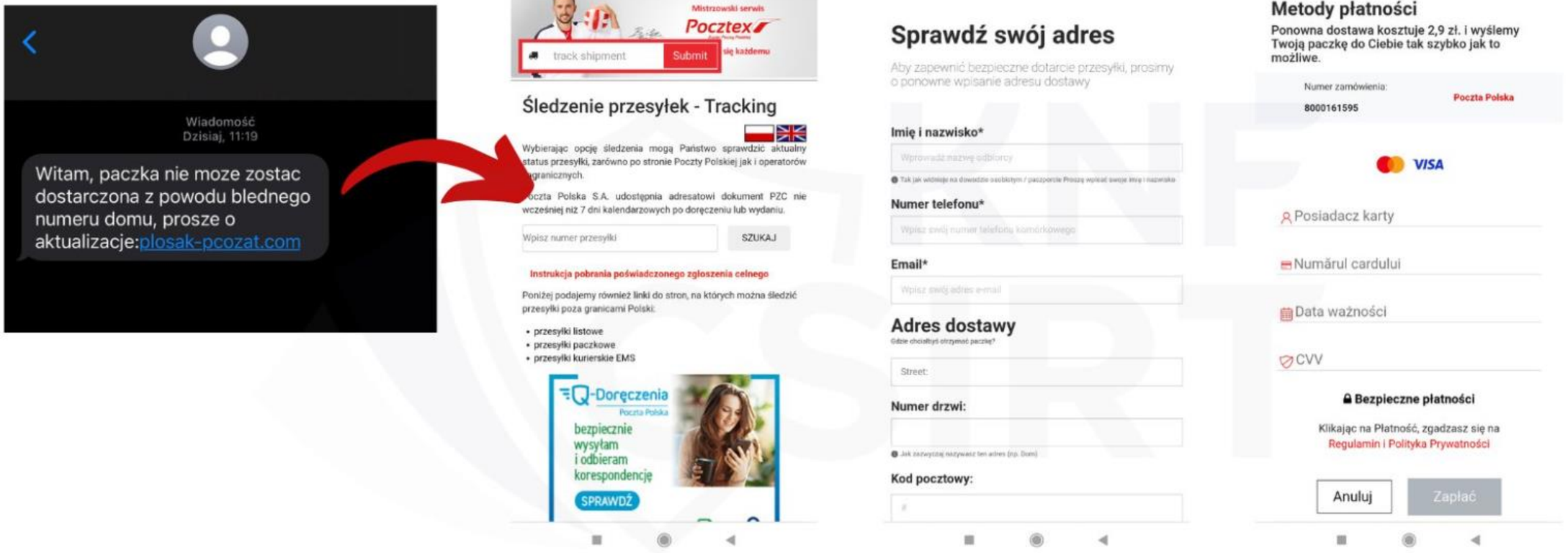
1/3 Cyberhigiena: jak rozpoznać fałszywą stronę…





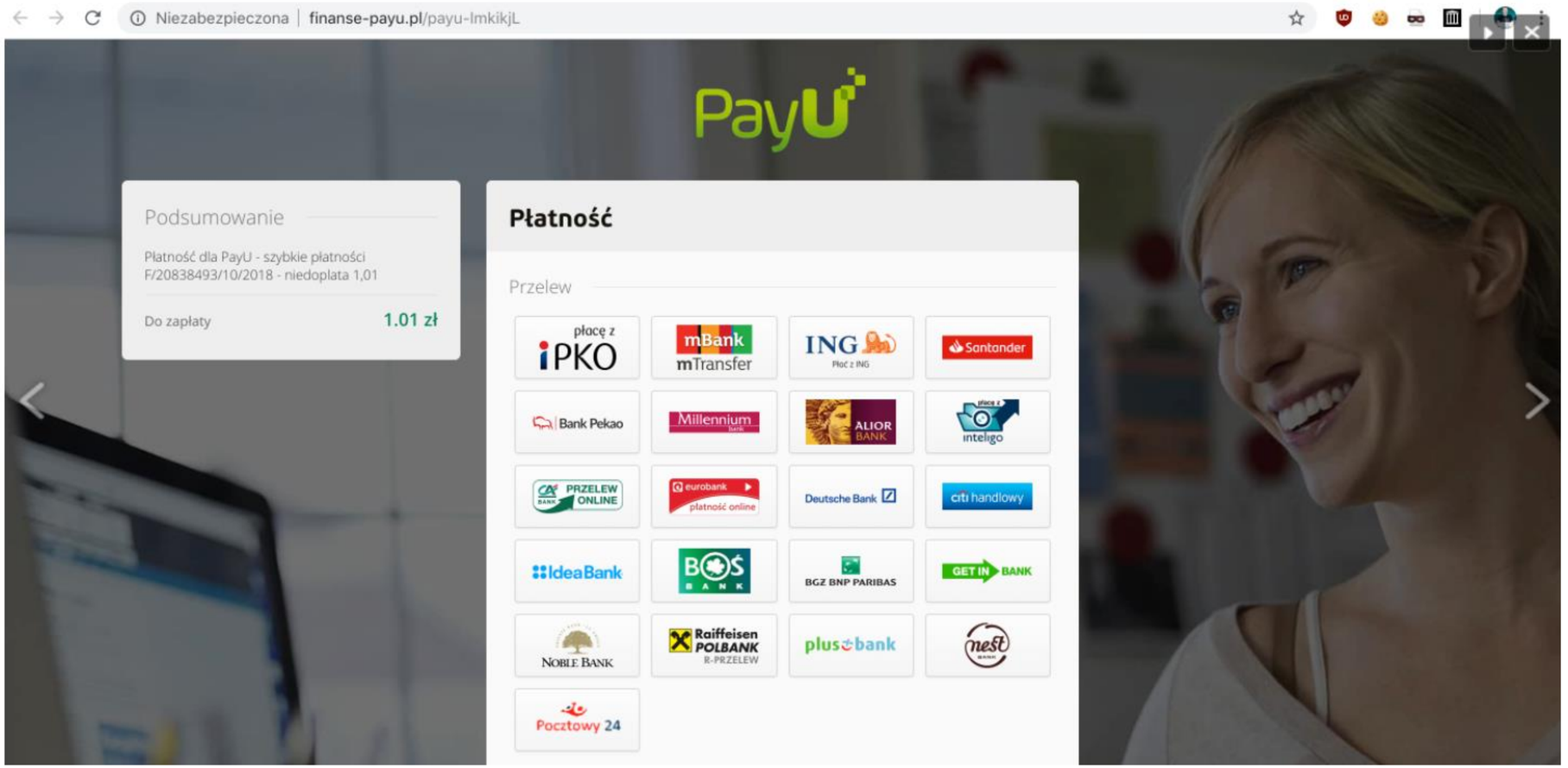
źródło: Materiały CSIRT KNF

1/3 Cyberhigiena: jak rozpoznać fałszywą stronę…



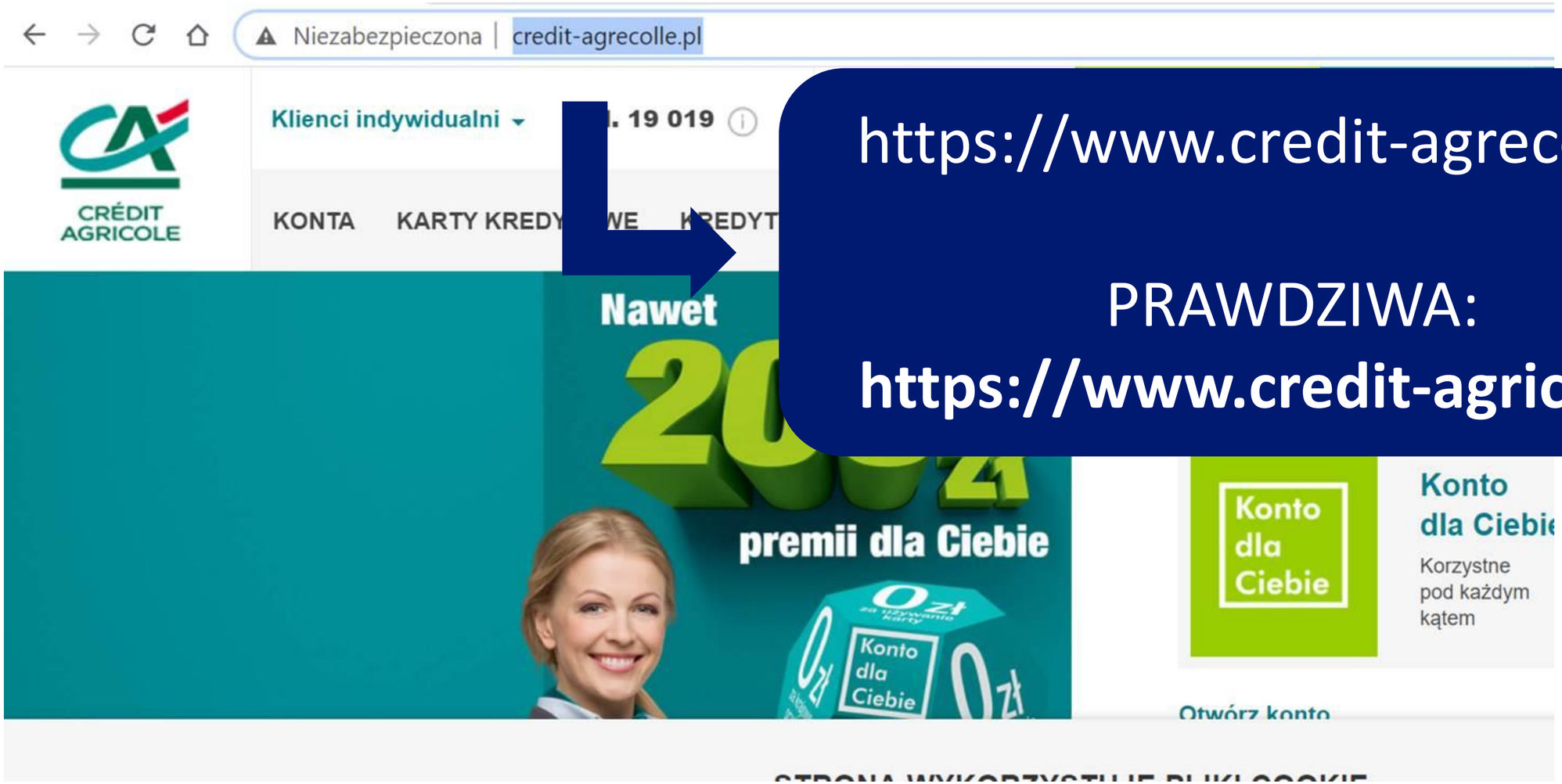
źródło: Materiały CSIRT KNF

Lub...



źródło: Materiały CSIRT KNF

Następnie…



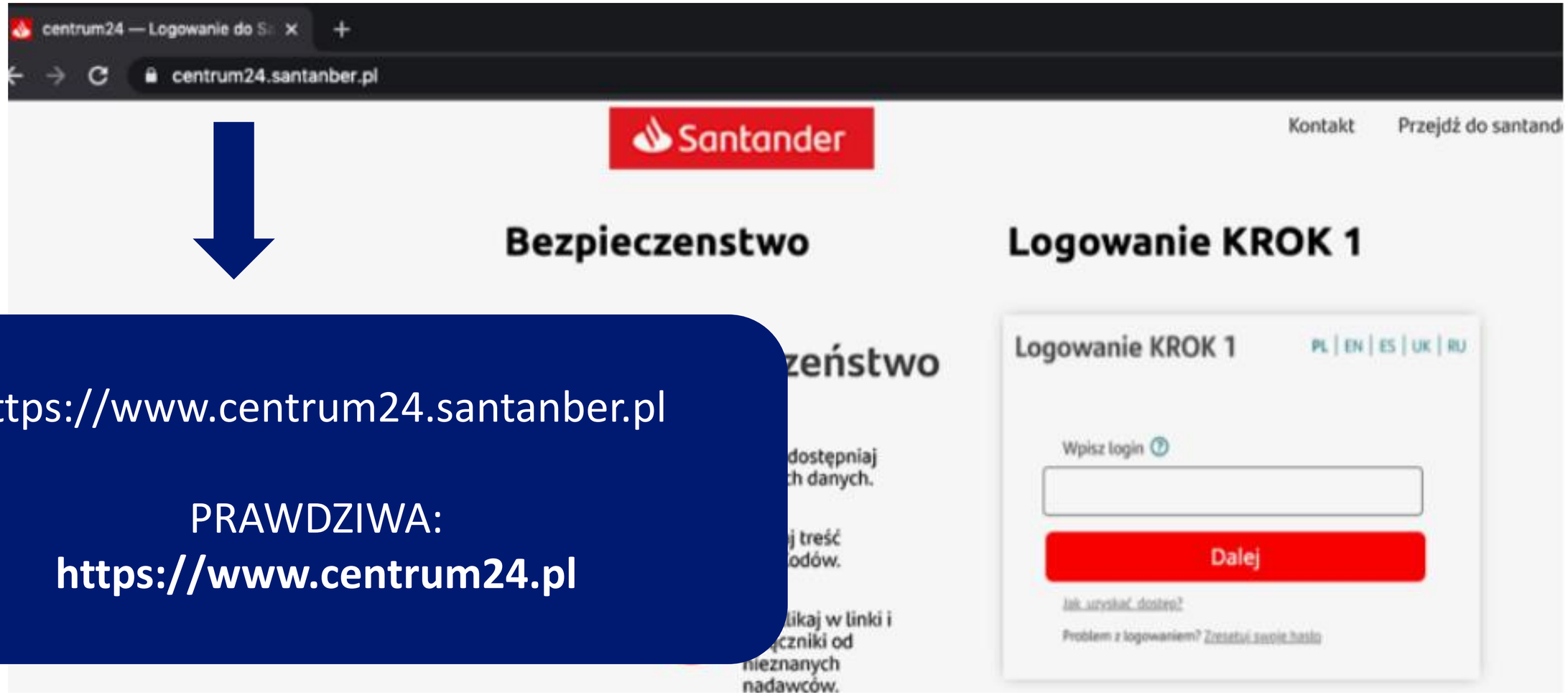
https://www.credit-agrecolle.pl

PRAWDZIWA:

https://www.credit-agricole.pl

źródło: Materiały CSIRT KNF

Następnie…



https://www.centrum24.santanber.pl

PRAWDZIWA:
https://www.centrum24.pl

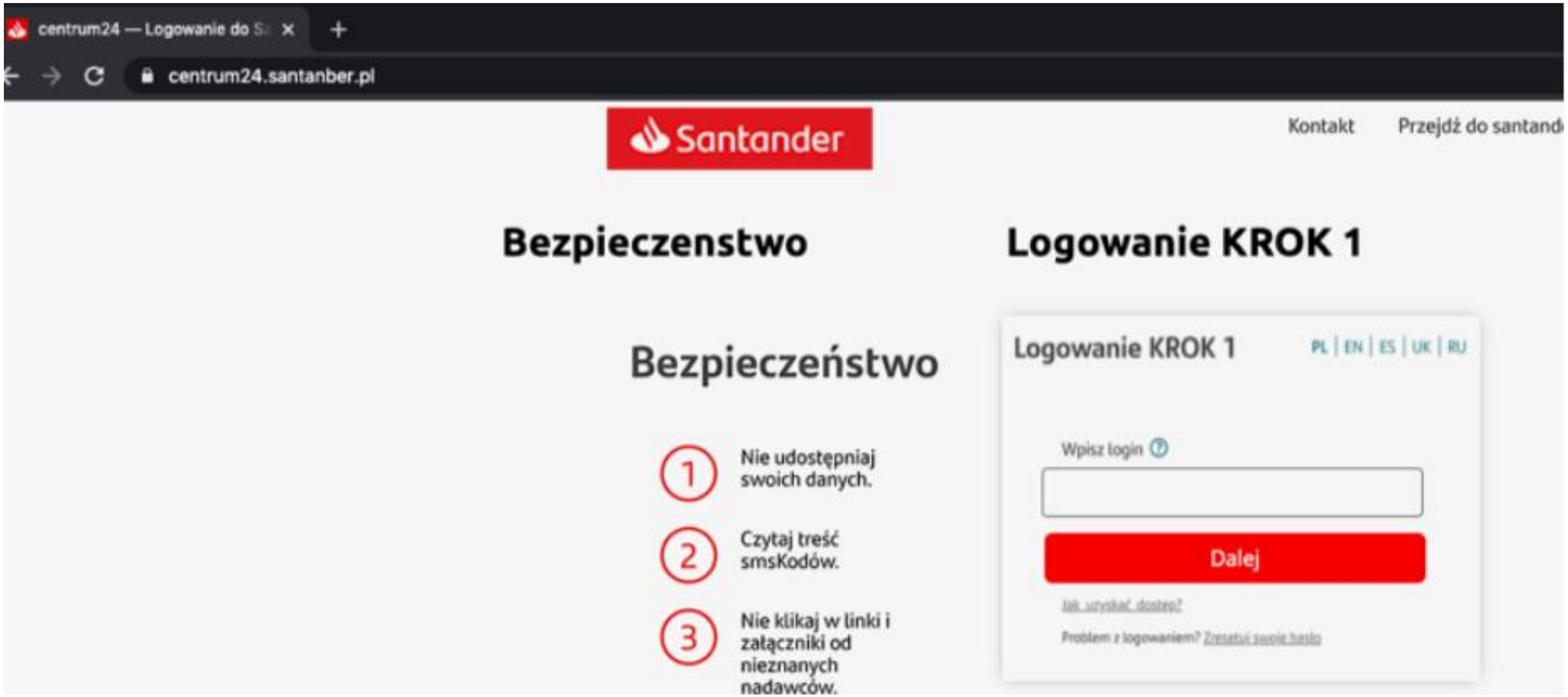
źródło: Materiały CSIRT KNF

Przykładów nigdy dość…

Prawdziwe domeny	Fałszywe domeny
ipkobiznes.pl	ipk0biznespl.online
goonline.bnpparibas.pl	bnpparlbas.site
pekao24.pl	pekao-pl.net
secure.velobank.pl	velobannk.fun
login.ingbank.pl	ing-pl-app.org

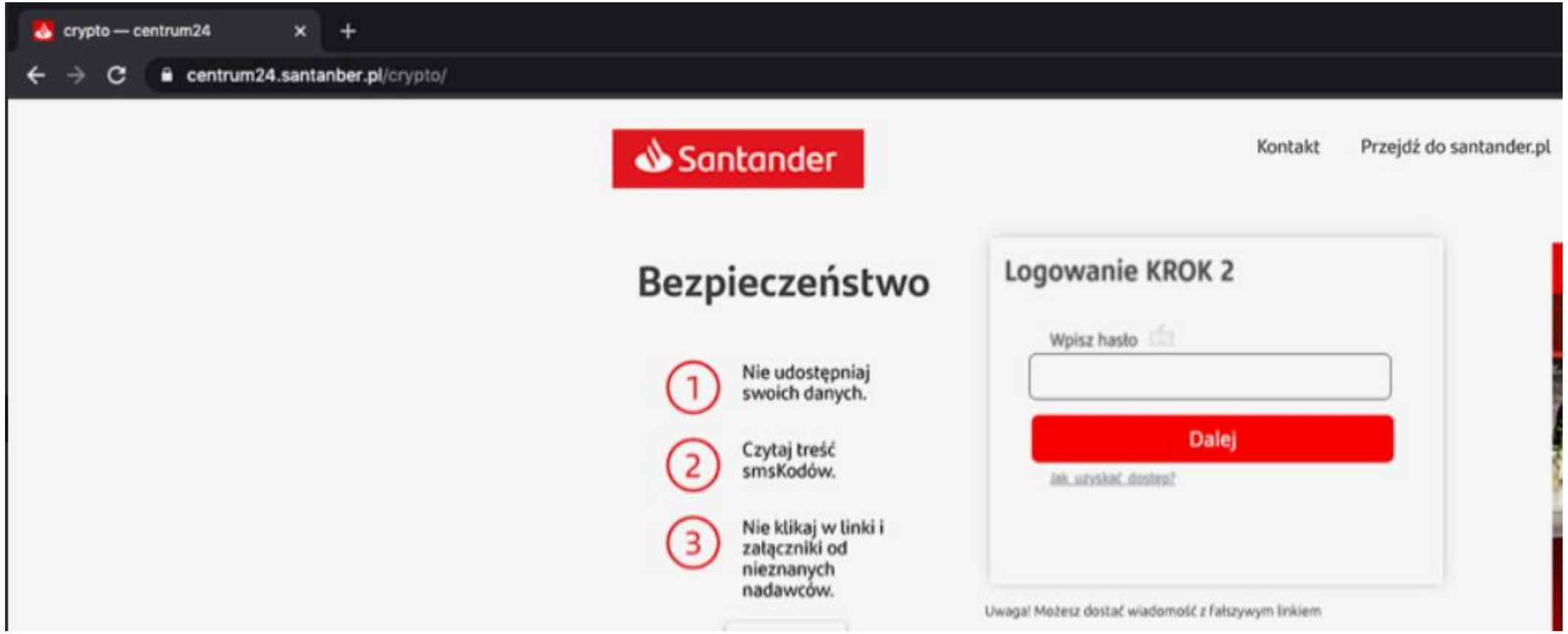
Źródło: twitter.com/csirt_knf

Login



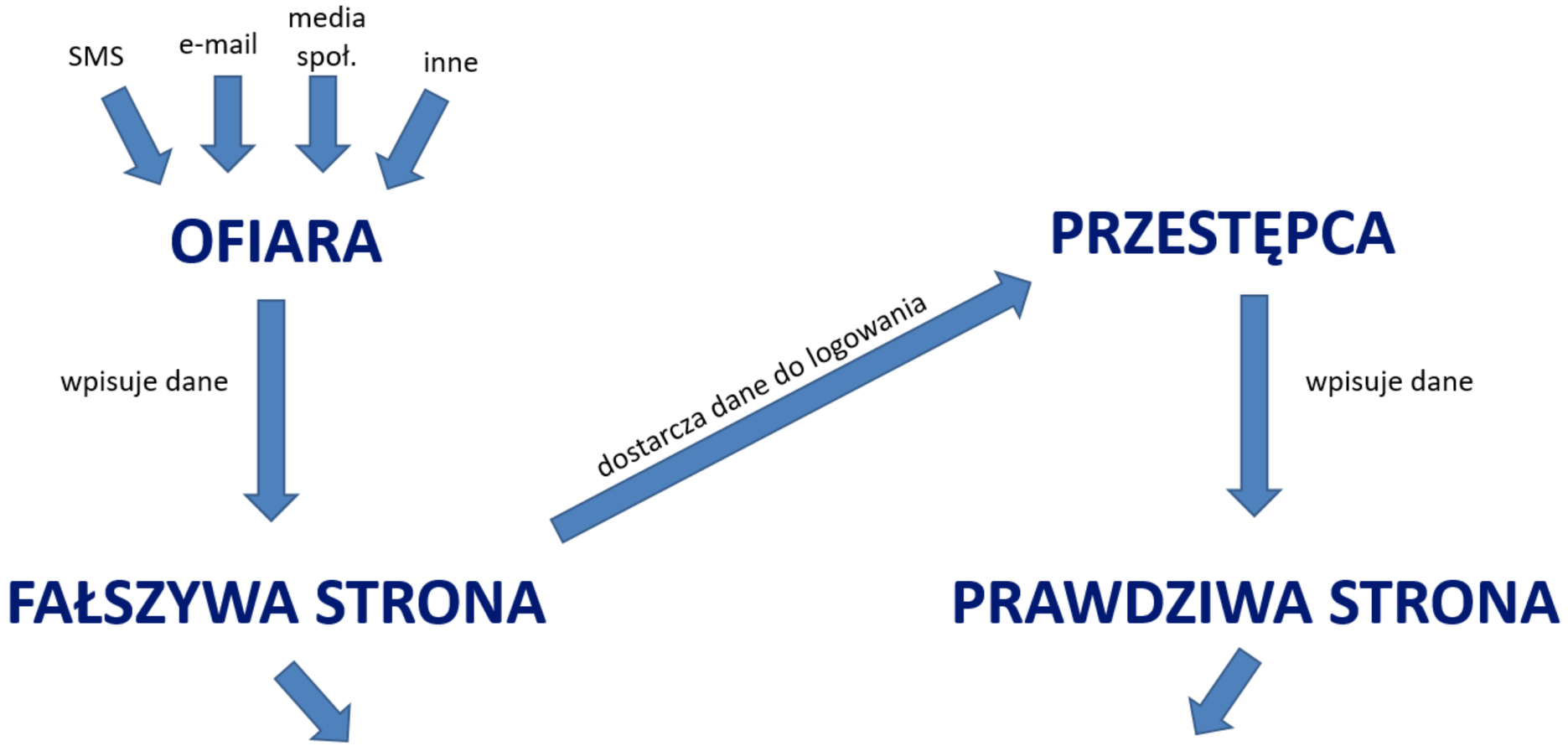
źródło: Materiały CSIRT KNF

Hasło



źródło: Materiały CSIRT KNF

Podsumujmy to…



źródło: Materiały CSIRT KNF

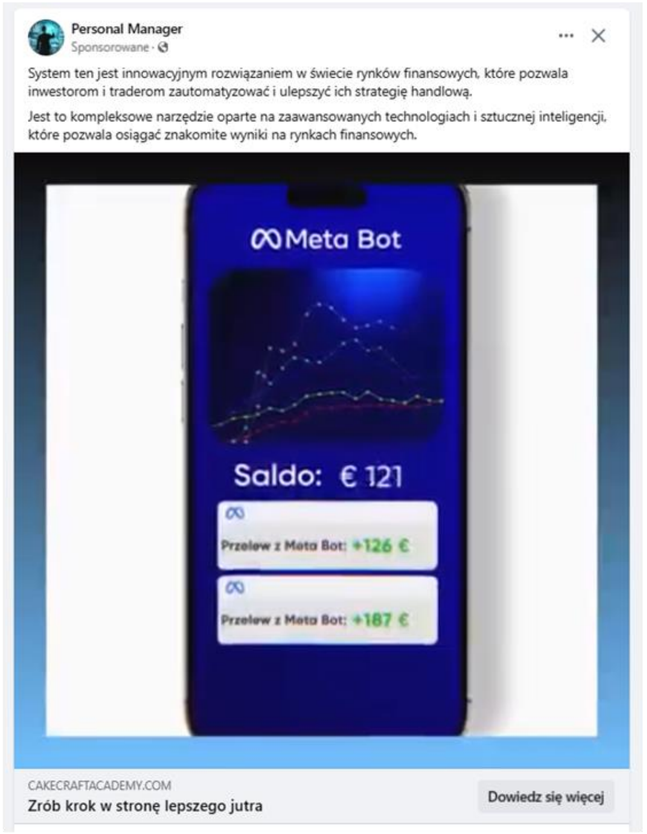
2/3 Cyberhigiena: scenariusze przestępcze…

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

źródło: Materiały CSIRT KNF

Oszustwa inwestycyjne

Zaczyna się od zachęty…



źródło: Materiały CSIRT KNF

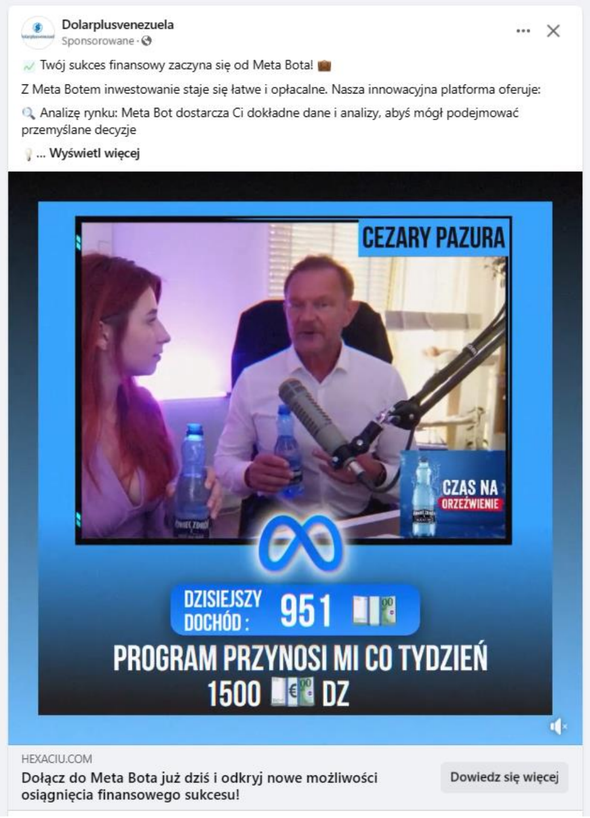
Oszustwa inwestycyjne

Zaczyna się od zachęty…

źródło: Materiały CSIRT KNF

Oszustwa inwestycyjne

Zaczyna się od zachęty…



źródło: Materiały CSIRT KNF

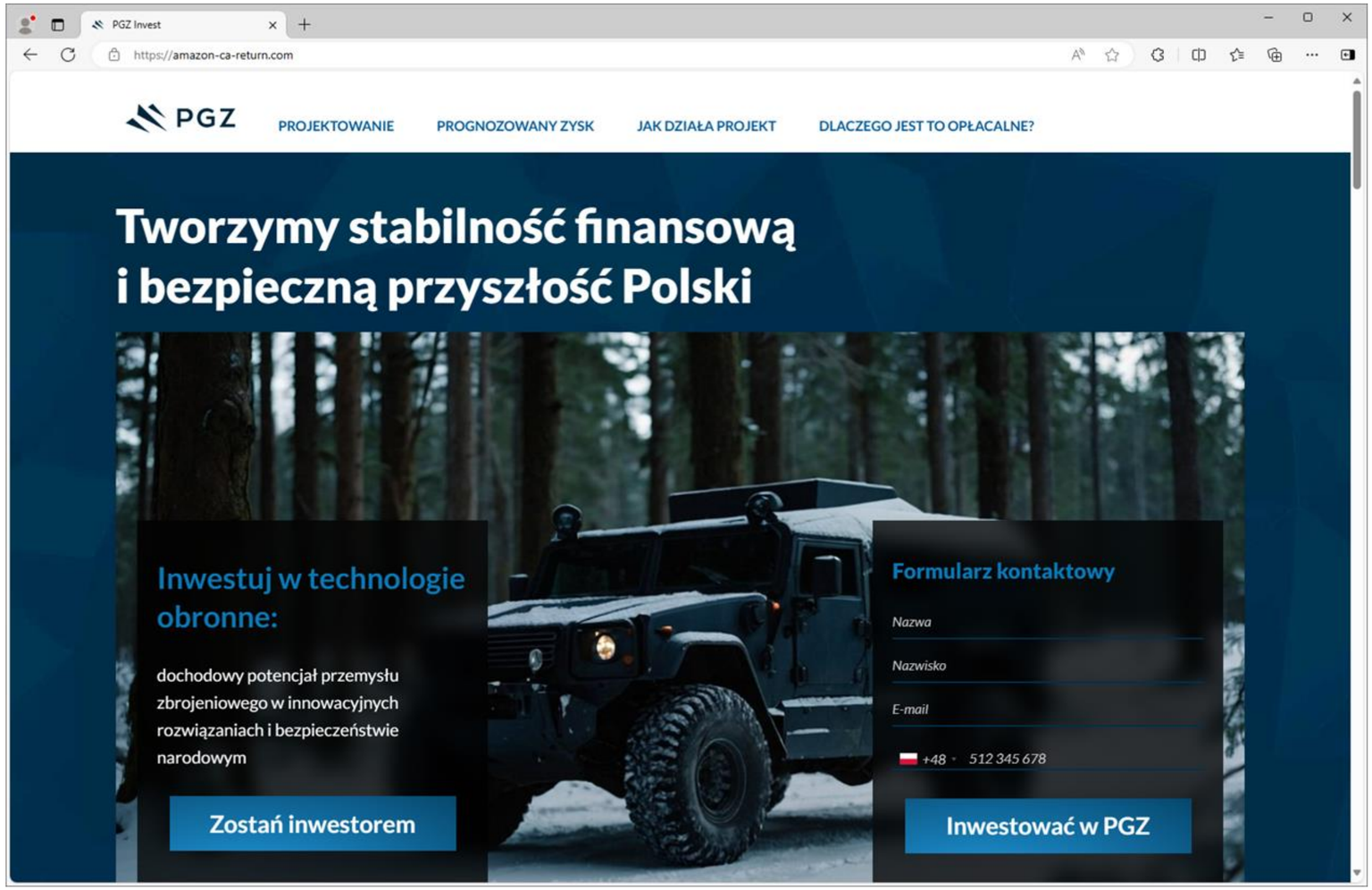
DEEPFAKE

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

Źródło: Chadha A., Kumar V., Kashyap S., Gupta M. 2021, Deepfake: An Overview. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Ganzha, M., Rodrigues, J.J.P.C. (eds) Proceedings of Second International Conference on Computing, Communications, and Cyber-Security, 2021 Lecture Notes in Networks and Systems, vol 203. Springer, Singapore

Oszustwa inwestycyjne

Formularz kontaktowy…



źródło: Materiały CSIRT KNF

Oszustwa inwestycyjne

Rozmowa telefoniczna…

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

źródło: Materiały CSIRT KNF

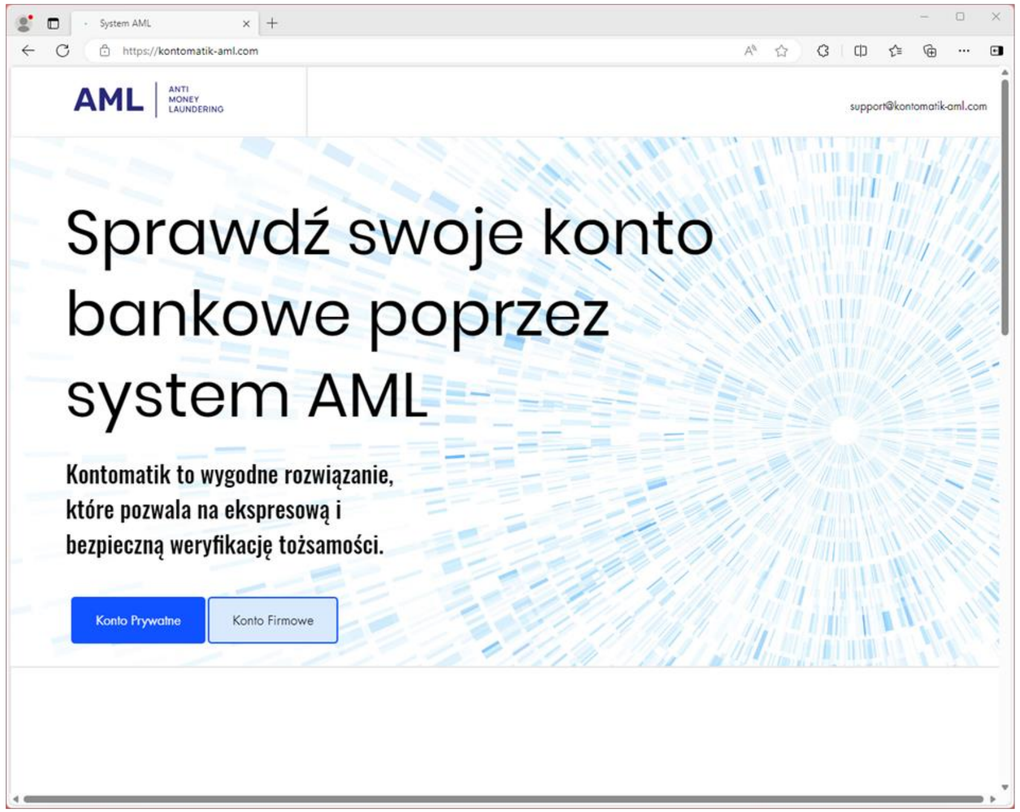
Oszustwa inwestycyjne

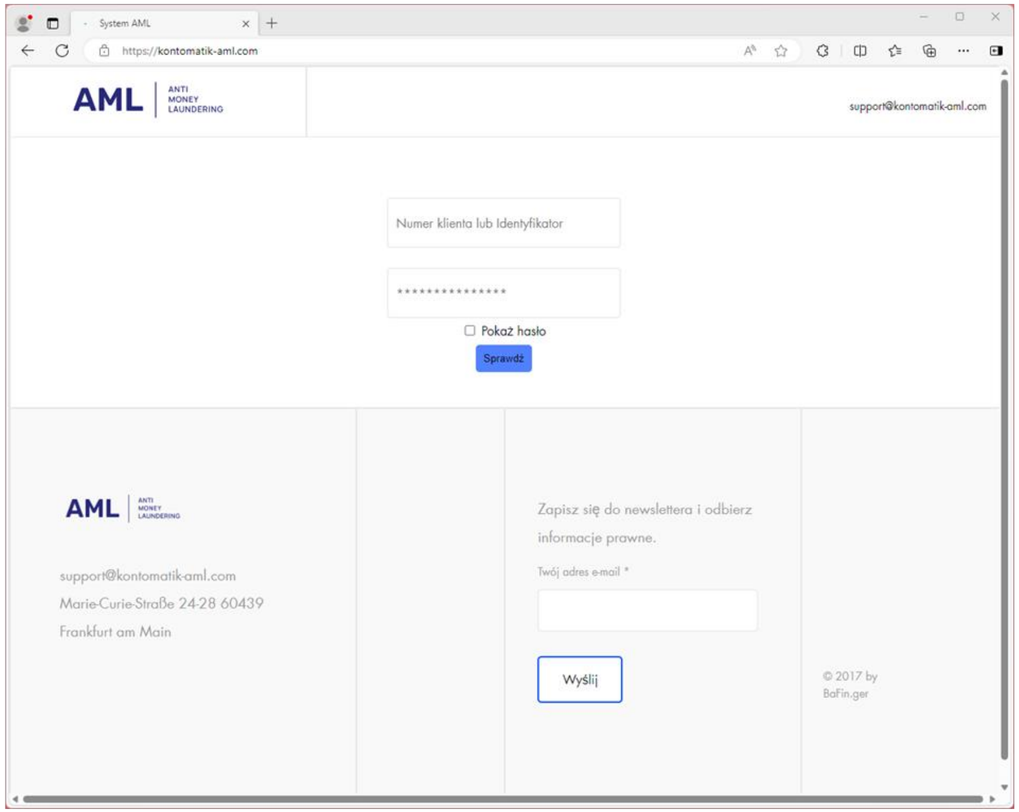
Platforma „inwestycyjna”…

źródło: Materiały CSIRT KNF

Oszustwa inwestycyjne

Wypłata?





źródło: Materiały CSIRT KNF

Oszustwa inwestycyjne

OGROMNE STRATY FINANSOWE

źródło: Materiały CSIRT KNF

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 wnuczkowi...

Nowiny 24

Metodą na wnuczka wyłudzili 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...

Źródło: opracowanie własne

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,...

Źródło: opracowanie własne

DEEPFAKE

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

Źródło: Chadha A., Kumar V., Kashyap S., Gupta M. 2021, Deepfake: An Overview. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Ganzha, M., Rodrigues, J.J.P.C. (eds) Proceedings of Second International Conference on Computing, Communications, and Cyber-Security, 2021 Lecture Notes in Networks and Systems, vol 203. Springer, Singaporel

DEEPFAKE

LISTOPAD 2023 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 wykorzystywania w działaniach przestępczych.*

Historia tego przestępstwa rozpoczęła się tak, jak wiele tego typu znanych historii. Do starszej Pani zadzwonił mężczyzn 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 słychać 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 głosy, 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.

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

LUTY 2024 ROKU

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: SEKURAK

Źródło: https://sekurak.pl/oszustwo-przez-telefon-objasniamy-jak-dzialaja-przestepcy-na-podstawie-prawdziwego-incydentu/?trk=public_post_comment-text

2/3 Cyberhigiena: scenariusze przestępcze…

- oszustwa inwestycyjne
- metoda np. na wnuczka / policjanta

WIELE INNYCH, BO…

źródło: Materiały CSIRT KNF

2/3 Cyberhigiena: scenariusze przestępcze…

PRZESTĘPCÓW OGRANICZA TYLKO KREATYWNOŚĆ

źródło: Materiały CSIRT KNF

3/3 Cyberhigiena: jak nie dać się oszukać

- weryfikacja adresu strony internetowej

Źródło: opracowanie własne

Weryfikacja domeny…

źródło: Materiały CSIRT KNF

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

Źródło: opracowanie własne

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!

Źródło: opracowanie własne

Media społecznościowe - @CSIRT KNF

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

OVERVIEW OF SELECTED SCAMS - MARCH 2024

15 kwiecień 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 - DECEMBER 2023

18 styczeń 2024

czytaj więcej

PRZEGLĄD WYBRANYCH OSZUSTW INTERNETOWYCH - GRUDZIEŃ 2023

16 styczeń 2024

czytaj więcej

WPROWADZENIE DO SZTUCZNEJ INTELIGENCJI

08 styczeń 2024

czytaj więcej

OVERVIEW OF SELECTED SCAMS - NOVEMBER 2023

18 grudzień 2023

czytaj więcej

Źródło: https://cebrf.knf.gov.pl

Media społecznościowe - @CSIRT KNF

RVIEW OF
CTED SCAMS -
CH 2024

2024

czytaj więcej

PRZEGLĄD WYBRANYCH OSZUSTW INTERNETOWYCH - MARZEC 2024

09 kwiecień 2024

czytaj więcej

PRZEGLĄD WYBRANYCH OSZUSTW INTERNETOWYCH - STYCZEŃ 2024

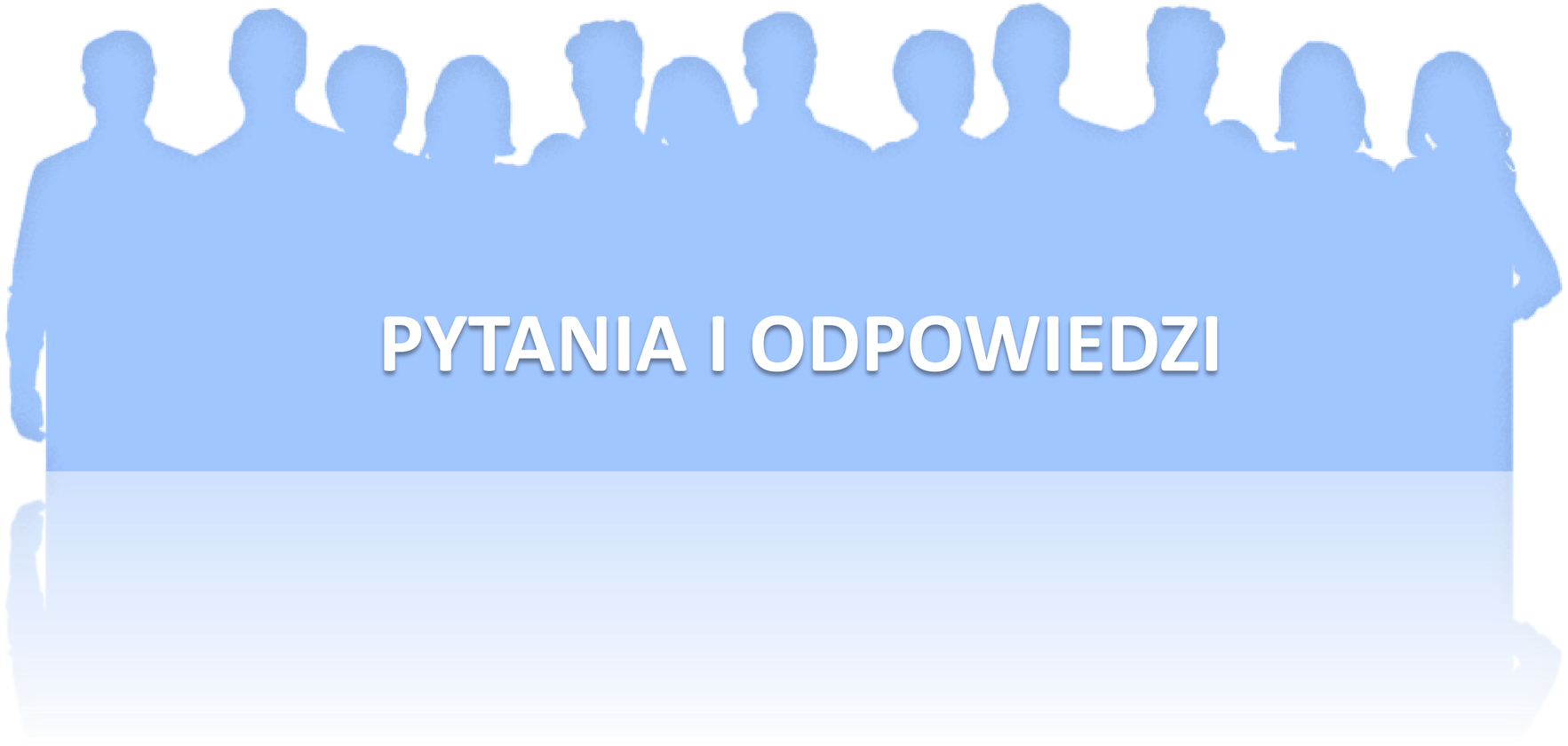
09 luty 2024

czytaj więcej

JAK SZTUCZNA INTELIGENCJA PRZETWARZA DANE

24 styczeń 2024

czytaj więcej



PYTANIA I ODPOWIEDZI

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

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