KPRM | KANCELARIA PREZESA RADY MINISTRÓW
Departament Cyberbezpieczeństwa

CYBER SAMORZĄD

#Cyberbezpieczny(Samo)rząd

Szkolenia dla kadry administracji publicznej

NASK

Przykłady najczęściej występujących zagrożeń w Polskiej cyberprzestrzeni

Przykłady zagrożeń

1. Spam
2. Phishing
3. Malware
4. Ransomware
5. Oszustwa komputerowe
6. 419, nigeryjski przekręt
7. BEC, oszustwo "na dyrektora”
8. Kradzież cyfrowej tożsamości

Spam

Jakie jest źródło spamu?

- Spam pojawia się w naszych skrzynkach pocztowych w wyniku nieuwagi.

Jak rozpoznać spam?

- Nasze skrzynki pocztowe otrzymują masę niechcianych wiadomości.

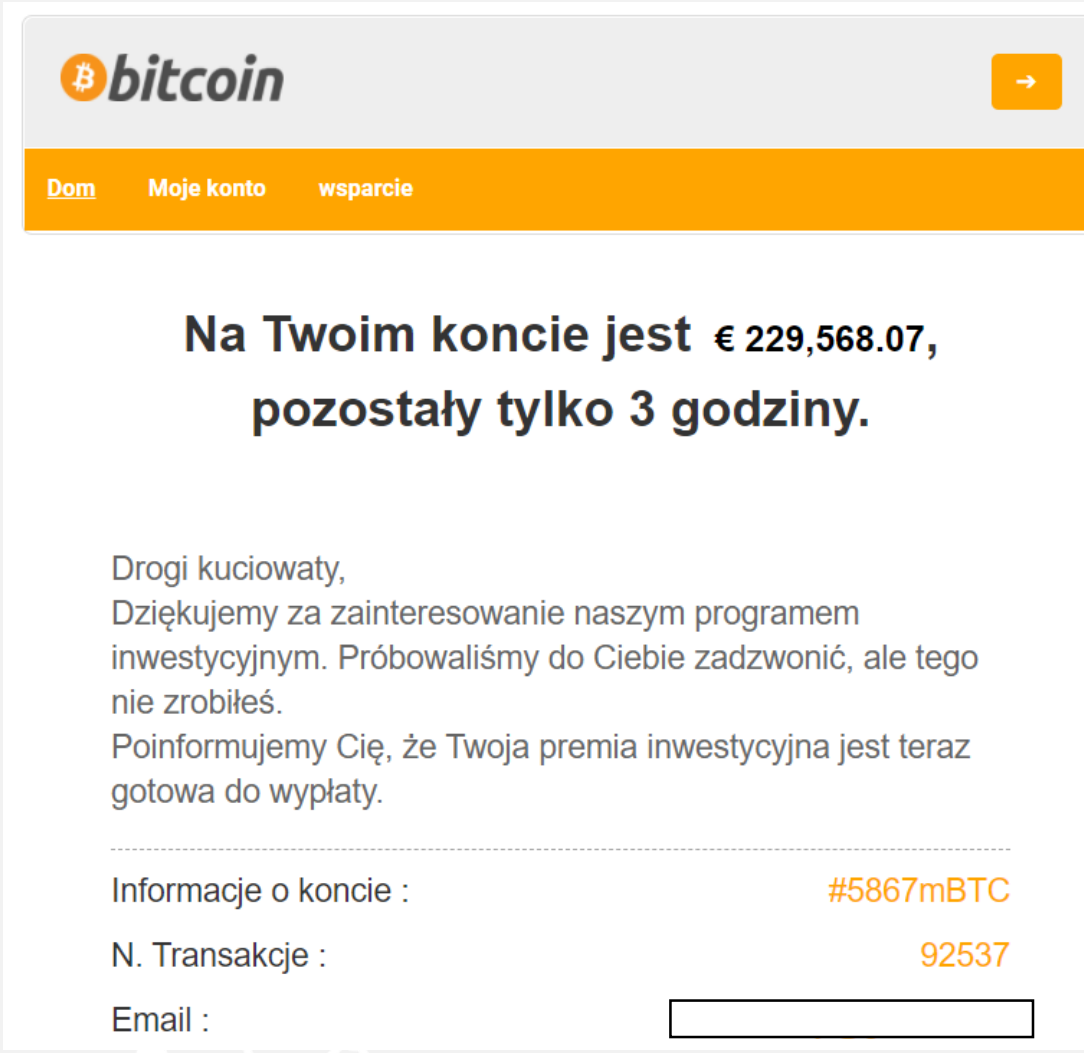
Jak pozbyć się spamu?

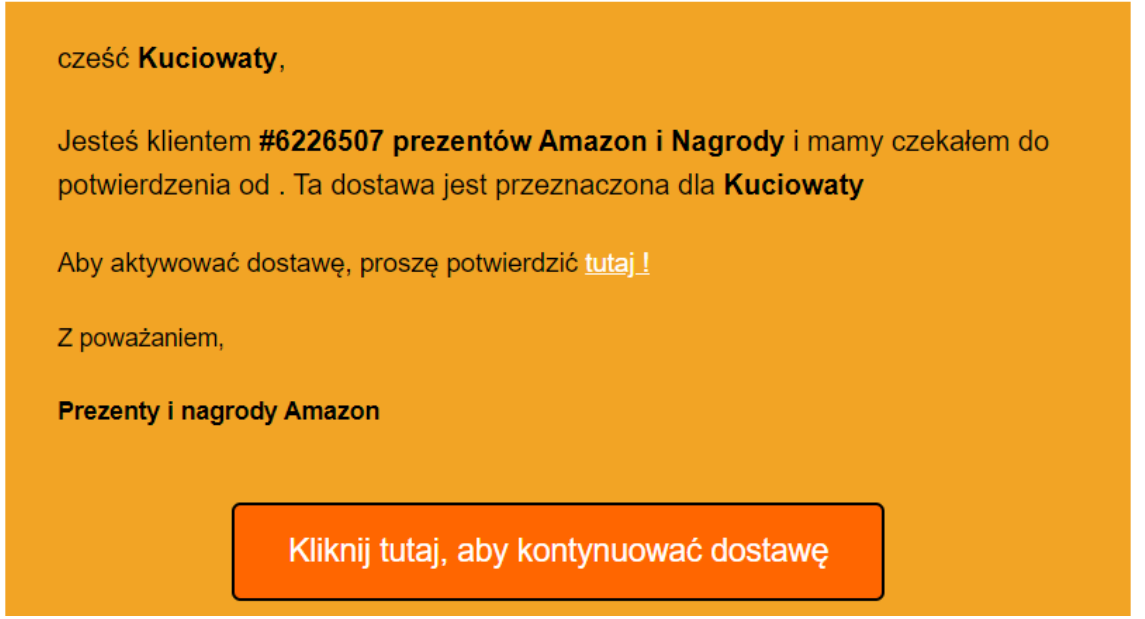
- Zwykle skrzynki odbiorcze mają ustawiony filtr antyspamowy.

Jak zapobiegać spamowi?

- Nie klikaj w linki, nie otwieraj załączników od nieznanych nadawców, nie odpowiadaj na wiadomości spamowe.

Spam


bitcoin
Dom
Moje konto
wsparcie
Na Twoim koncie jest € 229,568.07, pozostały tylko 3 godziny.
Drogi kuciowaty,
Dziękujemy za zainteresowanie naszym programem inwestycyjnym. Próbowaliśmy do Ciebie zadzwonić, ale tego nie zrobiłeś.
Poinformujemy Cię, że Twoja premia inwestycyjna jest teraz gotowa do wypłaty.
Informacje o koncie : #5867mBTC
N. Transakcje : 92537
Email :


cześć **Kuciowaty**,
Jesteś klientem **#6226507 prezentów Amazon i Nagrody** i mamy czekałem do potwierdzenia od . Ta dostawa jest przeznaczona dla **Kuciowaty**
Aby aktywować dostawę, proszę potwierdzić tutaj !
Z poważaniem,
Prezenty i nagrody Amazon
Kliknij tutaj, aby kontynuować dostawę


N.e.t.f.l.i.x riBrit.nooreply9tvu46vh...@wvz8wk5d9yxiop0.us przez i21tm.rev.cloudlinkd.net
niedz., 21 lut, 10:06
do cONTACT
Netflix
To Twoja szansa na uzyskanie dostępu do najpopularniejszych filmow i seriali przez cały rok!=>
- Informujemy jedynie zwycięzców konkursu! Jest nam bardzo miło, że dostałeś/aś się do finałowego etapu. Poświęć chwilę i wygraj rok Netflixa za darmo!

Phishing

Czym jest phishing?

- Metoda wyłudzenia danych

Jak rozpoznać phishing?

- Ataki phishingowe zwykle polegają na przesłaniu krótkich wiadomości tekstowych, które pobudzają silne emocje

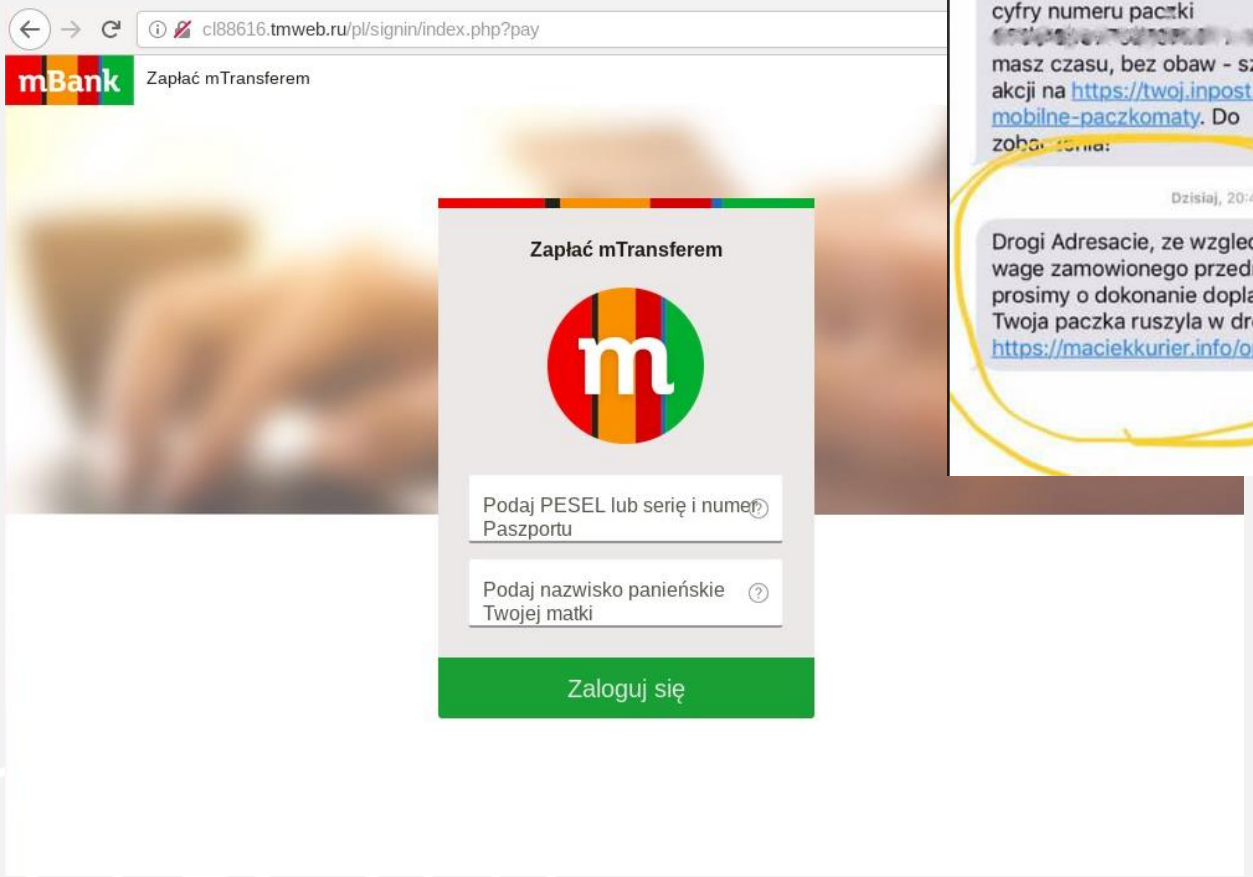
Phishing

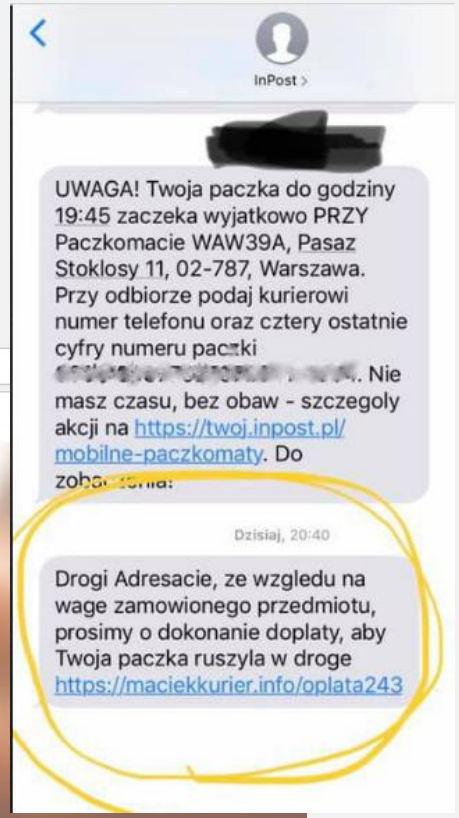
Metody manipulacji

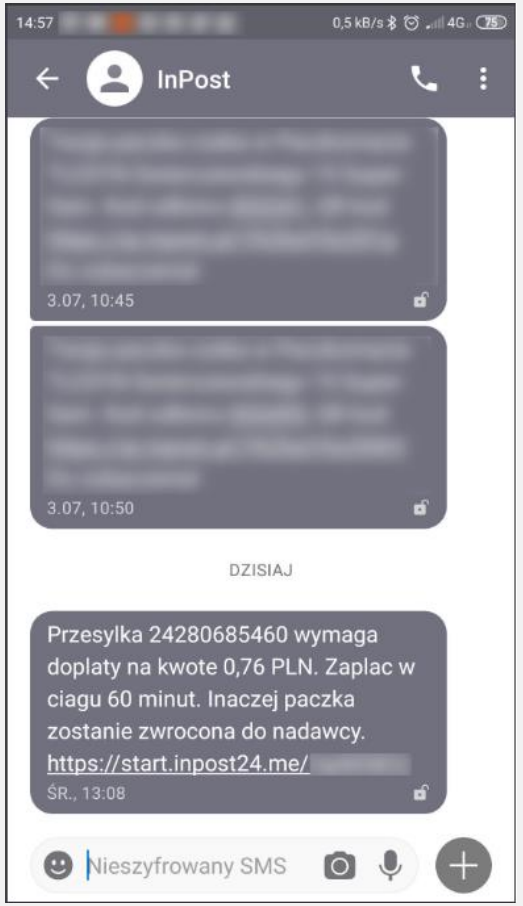
- ktoś nas okrada,
- dzieje się krzywda twoim bliskim,
- Ktoś nas szantażuje emocjonalnie,
- Oskarżają nas o popełnienie przestępstwa,
- Blokują nam środki na koncie.

Jak postępować po zidentyfikowaniu wiadomości typu phishing?

- Pierwsza reakcja
- Ocena sytuacji
- Reakcja końcowa


cl88616.tmweb.ru/pl/signin/index.php?pay
mBank
Zapłać mTransferem
Zapłać mTransferem
Podaj PESEL lub serię i numer Paszportu
Podaj nazwisko panieńskie Twojej matki
Zaloguj się


InPost
UWAGA! Twoja paczka do godziny 19:45 zaczeka wyjatkowo PRZY Paczkomacie WAW39A, Pasaz Stoklosy 11, 02-787, Warszawa. Przy odbiorze podaj kurierowi numer telefonu oraz cztery ostatnie cyfry numeru paczki
. Nie masz czasu, bez obaw - szczegoly akcji na https://twoj.inpost.pl/mobilne-paczkomaty. Do
Dzisiaj, 20:40
Drogi Adresacie, ze wzgledu na wage zamowionego przedmiotu, prosimy o dokonanie doplaty, aby Twoja paczka ruszyla w droge https://maciekkurier.info/oplata243


14:57
InPost
3.07, 10:45
3.07, 10:50
DZISIAJ
Przesylka 24280685460 wymaga doplaty na kwote 0,76 PLN. Zaplac w ciagu 60 minut. Inaczej paczka zostanie zwrocona do nadawcy. https://start.inpost24.me/
ŚR., 13:08
Nieszyfrowany SMS

Malware – definicje

Czym jest Malware?

- Malicious „złośliwy” + software „program”,
- Infekuje urządzenia,
- Działa na szkodę użytkownika (także straty finansowe).

Rodzaje

Kryterium sposobu infekcji:

- (Wirusy, robaki, trojany, inne)

Kryterium sposobu działania, efektu dla użytkownika:

- (Ransomware, spyware, adware, keyloggery, rootkity)

Malware – działanie

Źródła infekcji

- Załącznik lub odnośnik (link) w wiadomości e-mail,
- Przejęta przez przestępców lub podstawiona, fałszywa strona,
- Podstawione reklamy na zwykłych stronach,

Jak rozpoznać malware?

- Wykorzystywanie zasobów komputera, spowolnienie jego działania,
- Więcej spamu na poczcie, strony startowe, których użytkownik nie ustawiał w przeglądarce,
- Bardzo spektakularne działanie: blokada ekranu lub systemu przy ransomware,
- **Najczęściej jednak użytkownik nic nie zauważy –** celem jest skryte działanie.

Malware – zapobieganie

Jak zapobiegać?

- Aktualizuj system i oprogramowanie na nim zainstalowane,
- Posiadaj oprogramowanie antywirusowe,
- Regularnie skanuj urządzenie oprogramowaniem antywirusowym,
- Twórz kopie zapasowe danych,
- Włącz Firewall,
- System i aplikacje pobieraj z zaufanych źródeł,
- Czytaj okienka instalacyjne i uprawnienia przyznawanych aplikacjom,
- Nie otwieraj podejrzanych załączników,
- Wyłącz makra w dokumentach,
- Uważaj na podejrzane linki i strony internetowe.

Ransomware

Czym jest Ransomware?

- Jest obecnie jednym z najczęściej występujących zagrożeń w cyberprzestrzeni.

Metody ataku i źródła infekcji

- Złośliwe załączniki w wiadomościach e-mail zachęcających do kliknięcia,
- Złośliwe strony WWW,
- Złośliwe reklamy na legalnych stronach WWW,
- Złośliwe oprogramowanie, którym komputer był już zarażony wcześniej,
- Nieuprawniony zdalny dostęp do komputera przez osoby trzecie.
- Atak przeprowadzony w sposób pośredni bądź bezpośredni na stację roboczą użytkownika.

Ransomware

Rozpoznanie ataku

- Najczęściej po zainfekowaniu maszyny użytkownik otrzymuje komunikat o tym, że jego dane zostały zaszyfrowane i aby odzyskać dane trzeba opłacić okup.

Reagowanie podczas ataku

- W przypadku infekcji ransomware, pozostaw komputer włączony, ale odłącz go od sieci lokalnej (Internet), żeby nie doszło do infekcji innych komputerów.
- Zgłoś incydent do osoby odpowiedzialnej za obsługę incydentów w swoim urzędzie – helpdesku, osoby kontaktowej lub zespołu bezpieczeństwa teleinformatycznego.

Ransomware

Zapobieganie atakom

- **Nie ma jednego skutecznego środka na odzyskanie zaszyfrowanych plików.**
- Twórz na bieżąco kopie zapasowych swoich danych na zewnętrznych dyskach bądź przechowuj je w chmurach.
- Aktualizuj oprogramowanie zawierające wszelkie poprawki bezpieczeństwa.
- Korzystaj z aktualnej wersji oprogramowania antywirusowego, nie wyłączaj funkcji heurystycznych.
- Zwracaj uwagę na wiadomości, które otrzymujesz (email) ponieważ mogą być one częścią kampanii spamowej zawierającej zainfekowany plik. W ten sposób może dojść do infekcji poprzez otworzenie zainfekowanego pliku.
- Zachowaj ostrożność przeglądając strony internetowe tzn., zwróć uwagę na natrętne reklamy.

Ransomware

Nowy trend

- Przestępcy nie oczekują okupu za zwrot danych, lecz okupu za nieupublicznienie tych danych.

Działania przestępców

- Przeprowadzają włamanie do sieci.
- Wykorzystują podatności lub oprogramowanie do automatyzacji ataku.
- Przystępują do rozpoznania sieci i systemów, kopiują dane na swój serwer, szyfrują kopie zapasowe.
- Szyfrują system (główny atak).


```
ATTENTION!

Don't worry, you can return all your files!
All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-sTWdbjk1AY
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
gorentos@bitmessage.ch

Reserve e-mail address to contact us:
gerentoshelp@firemail.cc

Your personal ID:
0156mJddLsdH7gLV6tvVVoOOBw14Y3j2wMOTO2NnaiTCC9BpMbd6
```

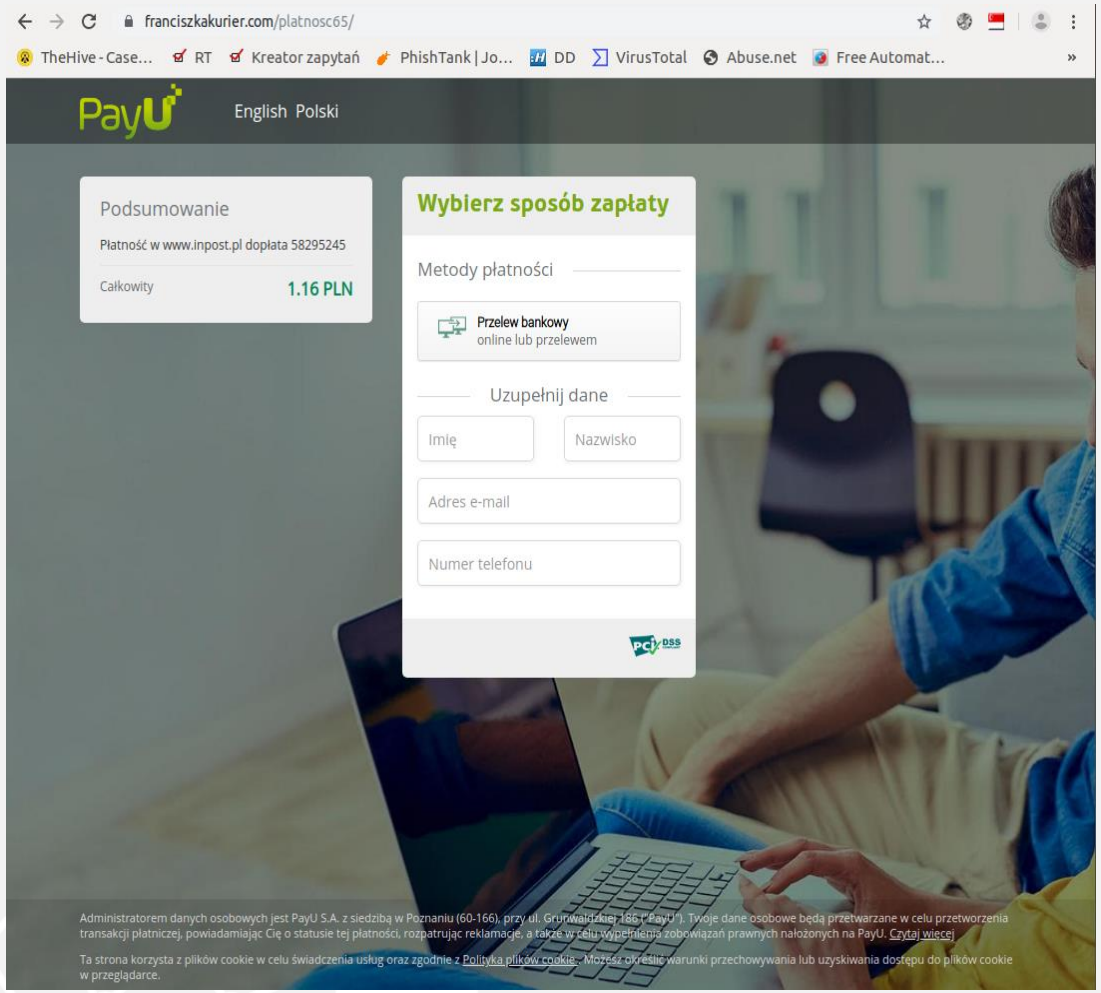
Oszustwo komputerowe

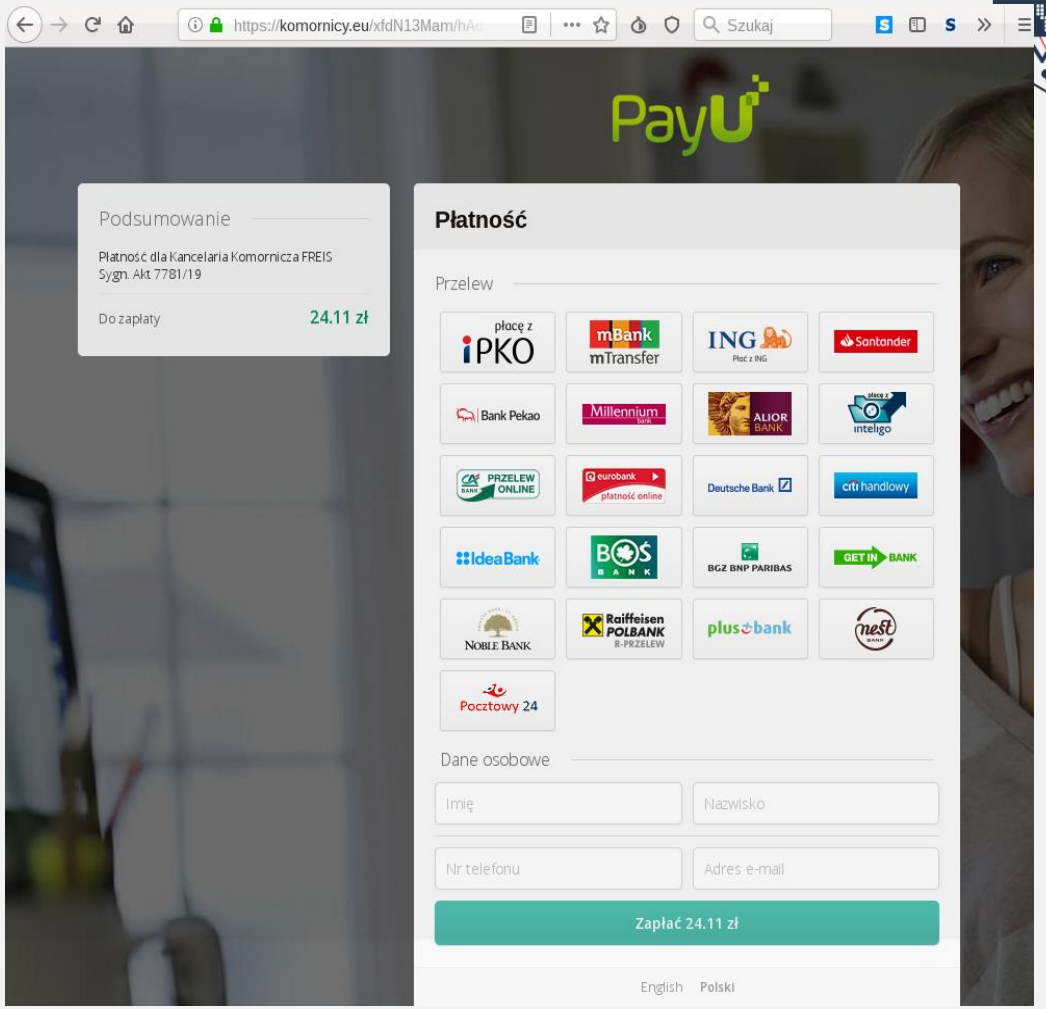
- Kodeks karny określa przestępstwa komputerowe oraz powiązane z nim artykuły dot. ochrony informacji (niejawnych, danych osobowy etc.).
- W kodeksie karnym przestępstwo komputerowe (art. 287 k.k.). Czyn zabroniony polega na wpływie na komputerowe zapisy informacji.
- Sprawcą oszustwa komputerowego może być każdy. Jest to powszechne przestępstwo. Przyjęto, że do popełnienia przestępstwa wymagany jest zamiar bezpośredni. Oznacza to, że sprawca popełniający czyn zabroniony w zamiarze bezpośrednim ma świadomość i wolę realizacji tego czynu.

Oszustwo komputerowe

Uwzględniając charakterystykę metod wykorzystywanych przez przestępców oraz zorganizowane grupy przestępcze, można wskazać następujące konsekwencje działań cyberprzestępców:

- Kradzież informacji
- Szyfrowanie informacji celem żądania okupu za odszyfrowanie danych
- Ujawnienie tajnych oraz prywatnych informacji (w tym danych osobowych)
- Niszczenie danych o strategicznym znaczeniu
- Straty finansowe
- Paraliż w sektorze prywatnym oraz w instytucjach państwowych
- Niedostępność usług internetowych


franciszkakurier.com/platnosc65/
TheHive - Case...
RT
Kreator zapytań
PhishTank | Jo...
DD
VirusTotal
Abuse.net
Free Automat...
PayU
English Polski
Podsumowanie
Płatność w www.inpost.pl dopłata 58295245
Całkowity
1.16 PLN
Wybierz sposób zapłaty
Metody płatności
Przelew bankowy
online lub przelewem
Uzupełnij dane
Imię
Nazwisko
Adres e-mail
Numer telefonu
Administratorem danych osobowych jest PayU S.A. z siedzibą w Poznaniu (60-166), przy ul. Grunwaldzkiej 186 ("PayU"). Twoje dane osobowe będą przetwarzane w celu przetworzenia transakcji płatniczej, powiadamiając Cię o statusie tej płatności, rozpatrując reklamację, a także w celu wypełnienia zobowiązań prawnych nałożonych na PayU. Czytaj więcej
Ta strona korzysta z plików cookie w celu świadczenia usług oraz zgodnie z Polityka plików cookies. Możesz określić warunki przechowywania lub uzyskiwania dostępu do plików cookie w przeglądarce.


https://komornicy.eu/xfdN13Mam/hA
Szukaj
PayU
Podsumowanie
Płatność dla Kancelaria Komornicza FREIS
Sygn. Akt 7781/19
Do zapłaty
24.11 zł
Płatność
Przelew
płacę z iPKO
mBank mTransfer
ING
Santander
Bank Pekao
Millennium
ALIOR BANK
inteligo
PRZELEW ONLINE
eurobank płatność online
Deutsche Bank
citi handlowy
IdeaBank
BOŚ BANK
BGZ BNP PARIBAS
GETIN BANK
NOBLE BANK
Raiffeisen POLBANK
plus bank
nest
Pocztowy 24
Dane osobowe
Imię
Nazwisko
Nr telefonu
Adres e-mail
Zapłać 24.11 zł
English
Polski

419, Nigeryjski przekręt

Czym jest 419?

- Oszustwo 419, oszustwo nigeryjskie po angielsku zwane 419 Fraud, West African Fraud - oszustwo z Zachodniej Afryki, czy też "na zaliczkę” (Advance Fee Fraud) - jest znane od XVI wieku. Wówczas nazywało się Listem Hiszpańskiego Więźnia
- Oszustwo 419 wzięło nazwę od numeru artykułu z nigeryjskiego kodeksu karnego.

419, Nigeryjski przekręt

Metoda ataku

- Oszustwo polega na wciągnięciu ofiary w grę psychologiczną poprzez wysyłanie e-maili. Przestępcy wykorzystują różne metody, żeby wyłudzić pieniądze. Najczęściej spotykane to podawanie się za:
  - uchodźcę politycznego,
  - dziedzica fortuny utraconej w trakcie przewrotu politycznego,
  - syna obalonego przywódcy jednego z państw afrykańskich.

Zapobieganie

- Nie odpisuj na podejrzane wiadomości i zaznaczaj je jako spam.
- Nie przesyłaj danych osobowych, numerów kont bankowych, informacji dotyczących polis ubezpieczeniowych.
- Podchodź z dystansem do historii opisywanych w mediach społecznościowych, portalach internetowych.
- Nie daj się skusić dużymi sumami pieniędzy. Propozycja ogromnej kwoty za pomoc uchodźcy politycznemu może być kłamstwem.

419, Nigeryjski przekręt

Susan Taylor <susantaylor.me@gmail.com>
do mnie

pt., 5 lut, 11:54

I hope all is well with you over there?

My name is Susan Taylor, a Senior Accountant at LLOYDS Bank and I hope my message meets you in good health.

After going through your profile on LinkedIn, I have an important proposal which will interest you and I strongly anticipate your cooperation to see if you can handle this in your country by maintaining confidentiality.

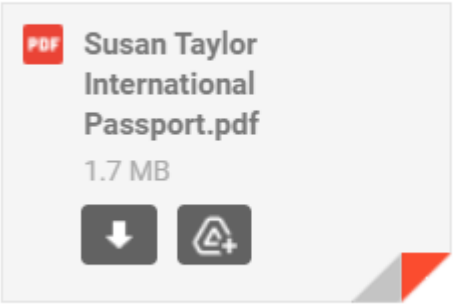
I await your response in adherence to strict confidentiality to the detailed information of the opportunity after I might have gotten your positive response.

Best Regards,
Susan Taylor

Kamil Kuć <kuciowaty@gmail.com>
do Susan

Susan,
Your email intrigues me. Please tell me more.
--
Best Regards
KK

2 załączniki



I am contacting you concerning an abandoned sum of 5,500,000.00 GBP. In June 2007 A customer called Edward Kuc a foreign investor in Bio - Technology London came to our bank for business discussions and investment, as the officer in charge of his transaction then, I encouraged him to consider various growth of funds with prime ratings. Then he invested Four Million Eight Hundred Thousand Pound's only. Based on my advice, we were able to spin the initial deposit with profit and interest to 5.5 million GBP. After few years; my bank (Lloyd's Bank) sent several notice to him without response and unfortunately, my client died in a car crash along with his nuclear family in France while on sabbatical in the summer of 2011, may their soul rest in peace. He died without leaving a Will and several efforts were made to find his extended family through your embassy without success. Because of the sensitive nature of private banking, most customers don't nominate next of kin in their investment, also usually in most cases leave their WILLS in our care, in this case our now deceased client died intestate.

It is quite clear now that our dear client died with no known or identifiable family member. According to practice, the Private banking sector will by the end of this year broadcast a request for statement of claim to Lloyd's Bank, failing to receive viable claims they will probably revert the deposit to the Management of Lloyd's Bank Ltd. This will result the money entering the Lloyd's Bank accounting system and the portfolio will be out of my hands and out of the private banking division. What bothers me most is that according to the laws of my country at the expiration of Ten {10} years the funds will revert to the ownership of the British Government if nobody applies to claim the funds.

Now, I am prepared to give the necessary details to you as the closest surviving relation of our deceased customer. I am also proposing that after a successful execution of this business deal, the funds will be shared in the ratio 40/60. You will get 40% and I will be entitled to 60% as the initiator of the deal. You know that I must have done my home work already before contacting you. Although the project is capital intensive, I know I will be able to pull it through following proper banking and legal channels with your assistance at your end. I will tidy up the legal aspect with the assistance of a lawyer who will prepare all the documents that will be needed to transfer the money from London to your country. Once more, I ask that if you find no interest in this project that you should discard this mail and forget I ever contacted you, I ask that you do not be vindictive and destructive; do not destroy my career. Opportunities like this only comes once in a lifetime. I am a family woman and this is an opportunity for me to give my family the best in life. I would want you to think about this and let me know your decision. If you give me a positive response, I will give you the relevant INFORMATION for the successful transfer of these funds and we both enjoy it in peace.

Kamil Kuć <kuciowaty@gmail.com> 6 lut 2021, 13:05

do Susan

Wow. I do not know what to say. I didn't know that my relative works in biotechnology, I mean he doesn't do it anymore .. but it's great news that he did it!

First of all, thank you for sharing this valuable information with me and I would like to say that I will keep this matter completely confidential. It's very good that you contact me by private email, I don't trust banks very much so it's good that we do it through informal communication channels.

I understand your situation. Late last year, I buried my parents who died of covid 19, I was a bit saddened by the news of another relative's death, but ... the news of the inheritance cheered me up. Don't get me wrong, there is no greater value to me than family and I can see you think so too, but in these times money is a very important thing.

I understand that you must have put a lot of work into this project, but your proposal is not satisfactory for me. Considering the enormity of your work, I propose 45% for me and 55% for you. Tell me what do you think? 5% more for me is not so much in terms of what you can actually get.

According to what you write, we have little time to finalize this transaction, so I am asking you to answer this matter very quickly.

BEC, oszustwo "na dyrektora"

Czym jest BEC?

- Atak BEC, czyli Business Email Compromise wykorzystuje phishing ukierunkowany na instytucje, przedsiębiorstwa i organizacje.

Metody manipulacji

- Metoda oparta jest na socjotechnice stosowanej wobec pracownika firmy.
- Atakujący wywiera wpływ poprzez nakłonienie do szybkiego wykonania określonego zadania nałożonego przez „kierownictwo wyższego szczebla”.

BEC, oszustwo "na dyrektora"

Sposób ataku

- Przestępcy prowadzą skanowanie sieci, aby odnaleźć słabe punkty w systemie.
- Prowadza podsłuch, celem uzyskania dostępu do informacji takich jak korespondencja wewnątrz organizacji, zawartość baz danych i treść innych ważnych dokumentów.
- Gdy mają dostęp do informacji przestępcy mogą zaczynają rozpoznanie struktury organizacyjnej.
- Przestępców interesują osoby, które obracają pieniędzmi w organizacji, czyli finansiści czy księgowi.
- Podszywają się pod kierownictwo wyższego szczebla i wykorzystują technikę spear phishing do ataku na księgowych.

BEC, oszustwo "na dyrektora"

Znaki ostrzegawcze, na które powinniśmy zwrócić uwagę w czasie takiego ataku:

- Bezpośredni kontakt kierownictwa z pracownikiem za pośrednictwem poczty mailowej lub połączenia telefonicznego, a nie w interakcji twarzą w twarz,
- Prośba o zachowanie pełnej poufności,
- Wywieranie nacisku i ponaglanie,
- Skrajności od poczucia zagrożenia po niecodzienne pochlebstwa,
- Wymagania sprzeczne z wewnętrznymi procedurami.

BEC, oszustwo "na dyrektora" - zapobieganie

Jako organizacja:

- Trzeba być świadomym ryzyka i informować pracowników o możliwości wystąpienia tego typu zagrożenia;
- Należy zwrócić uwagę pracowników do ostrożnego podejścia podczas dokonywanych płatności, szczególnie na wielkie sumy; Należy dbać o aktualizacje zabezpieczeń technicznych;
- W przypadku oszustwa należy kontaktować się z policją.

BEC, oszustwo "na dyrektora" - zapobieganie

Jako pracownik:

- O każdym podejrzanym mailu bądź telefonie informuj swój dział IT/bezpieczeństwa.
- Nie przekazuj informacji związanych z Twoją organizacją (procedury, hierarchia organizacji).
- W serwisach społecznościowych zastosuj zasadę ograniczonego zaufania i ogranicz informacje dotyczące Twojej organizacji.
- Nigdy nie otwieraj podejrzanych linków, załączników. Otwieraj te, których się spodziewasz lub potwierdź u nadawcy (jeśli to znajomy, współpracownik), że to on wysłał tego maila. Zachowaj szczególną ostrożność podczas korzystania z osobistej skrzynki pocztowej korzystając ze sprzętu firmowego.
- Ściśle stosuj się do wewnętrznych procedur dotyczących płatności i zamówień.

BEC, oszustwo "na dyrektora"

Od Jacek [redacted] <officemails018@gmail.com>

Temat **Pilne**

Do Skarbnik@[redacted]

Musimy dokonac pilnej platnosci w wysokosci 95 455,25 PLN. Czy mozemy
dokonac tej platnosci dzisiaj?

Pozdrowienia
Jacek [redacted]

Od Adam [redacted] <emailsoffice@naver.com>

Temat **Zapłata**

Do [redacted]@powiat.[redacted]

Czy możemy dziś zapłacić 36 tysięcy euro?

pozdrowienia
Adam [redacted]

Wysłane z mojego urządzenia mobilnego.

From: [redacted] [mailto:officemail045@gmail.com]
Sent: Friday, July 5, 2019 8:27 AM
To: [redacted]
Subject: Pilne

Musimy dokonac pilnej platnosci w wysokosci 75 455,25 PLN. Czy mozemy dokonac tej platnosci dzisiaj?

Pozdrowienia
[redacted]

BEC, oszustwo "na dyrektora"

Intermarche oszukane na 15 mln euro. Pieniądze trafiły na polskie konto

Sieć supermarketów Intermarche utraciła 15 mln euro na rzecz grupy oszustów, która przekonała jednego z pracowników firmy do przelania gigantycznej kwoty na konto, które miało rzekomo należeć do dyrektora generalnego Intermarche. Co ciekawe, pieniądze trafiły na konto w polskim banku - donosi "Retail Detail".

2,6 mln zł raty za nowe samoloty LOT-u trafiło na konto oszustów - dowiedziały się "Wydarzenia". Wszystko przez podrobioną fakturę, ze zmienionym numerem konta. Przelane pieniądze najpierw trafiły do banku na Cyprze, później błyskawicznie zostały przetransferowane przez oszustów do jednego z państw Azji.

Wchodząca w skład Polskiej Grupy Zbrojeniowej, handlująca bronią spółka Cenzin, ofiarą międzynarodowego oszustwa. Jak dowiedzieli się reporterzy śledczy RMF FM, straty wynoszą około 4 milionów złotych.

W kilku transzach przelano na fałszywe konto 4 miliony złotych (zdj. ilustracyjne) /Pixabay

Spółka Cenzin - jak ustalili dziennikarze RMF FM - padła ofiarą tzw. phishingu. Do firmy przyszło kilka e-maili od osoby lub osób podszywających się pod czeskiego dostawcę broni.

Kradzież cyfrowej tożsamości

Po co przestępcom twoje dane osobowe?

- Dokonają kradzieży pieniędzy z twojego konta bakowego
- Zaciągną pożyczkę na twoje dane
- Wykorzystają twoje dane, aby zrobić z ciebie „słupa”
- Będą szantażować ciebie wykradzionymi danymi

Kradzież cyfrowej tożsamości

1. Gdy zakładasz profil należy rozważyć czy konieczne jest, aby profil zawierał imię i nazwisko użytkownika.
2. Używaj silnego hasła (najlepiej składające się z losowych znaków – np. manager haseł) i inne niż wykorzystywane w pozostałych serwisach.
3. Skonfiguruj ustawienia prywatności konta.
4. Pamiętaj, że informacją jest:
   - tekst,
   - zdjęcie lub film,
   - charakterystyczne obiekty pozwalające na identyfikację Twojego miejsca przebywania lub Twoich bliskich,
   - polubione miejsca (jak również „meldowania”) lub grupy, do których należysz

Kradzież cyfrowej tożsamości

5. Pamiętaj, że korzystając z serwisów społecznościowych łatwo można (również nieintencjonalnie) zdradzić poufne i wrażliwe dane osób trzecich, pracodawcy, kontrahenta
6. Nie należy korzystać z prywatnych profili w celach zawodowych oraz przechowywać lub przesyłać dokumentacji służbowej za pomocą zewnętrznych nieautoryzowanych serwisów
7. Skasuj swój profil w serwisie, z którego nie będziesz więcej korzystać
8. Jeśli padłeś ofiarą przestępstwa internetowego nie kasuj żadnych danych, sporządź kopię całej korespondencji

Kradzież cyfrowej tożsamości

Pamiętaj, Twoje dane osobowe są cenne dla przestępców.

Ochrona przed oszustwami oznacza także ich bezpieczeństwo.

Kradzież cyfrowej tożsamości

policjaue.pl

RSS NEWSLETTER

FAKT24.PL

VOD.PL KUPONY GRY ONLINE PROGRAM TV HOROSKOP

WYDARZENIA FACET KOBIETA SPORT PIENIĄDZE HOBBY WIDEO NAJNOWSZE GALERIE ZDROWIE

POLSKA ŚWIAT POLITYKA WARSZAWA WROCŁAW POZNAŃ TRÓJMIASTO ŚLĄSK ŁÓDŹ KRAKÓW BIAŁYSTOK RZESZÓW

FAKT24.PL > Wydarzenia > Polska > Porwanie dziecka w centrum handlowym. [WIDEO] 1 Kwietnia ,12:00

r Browser

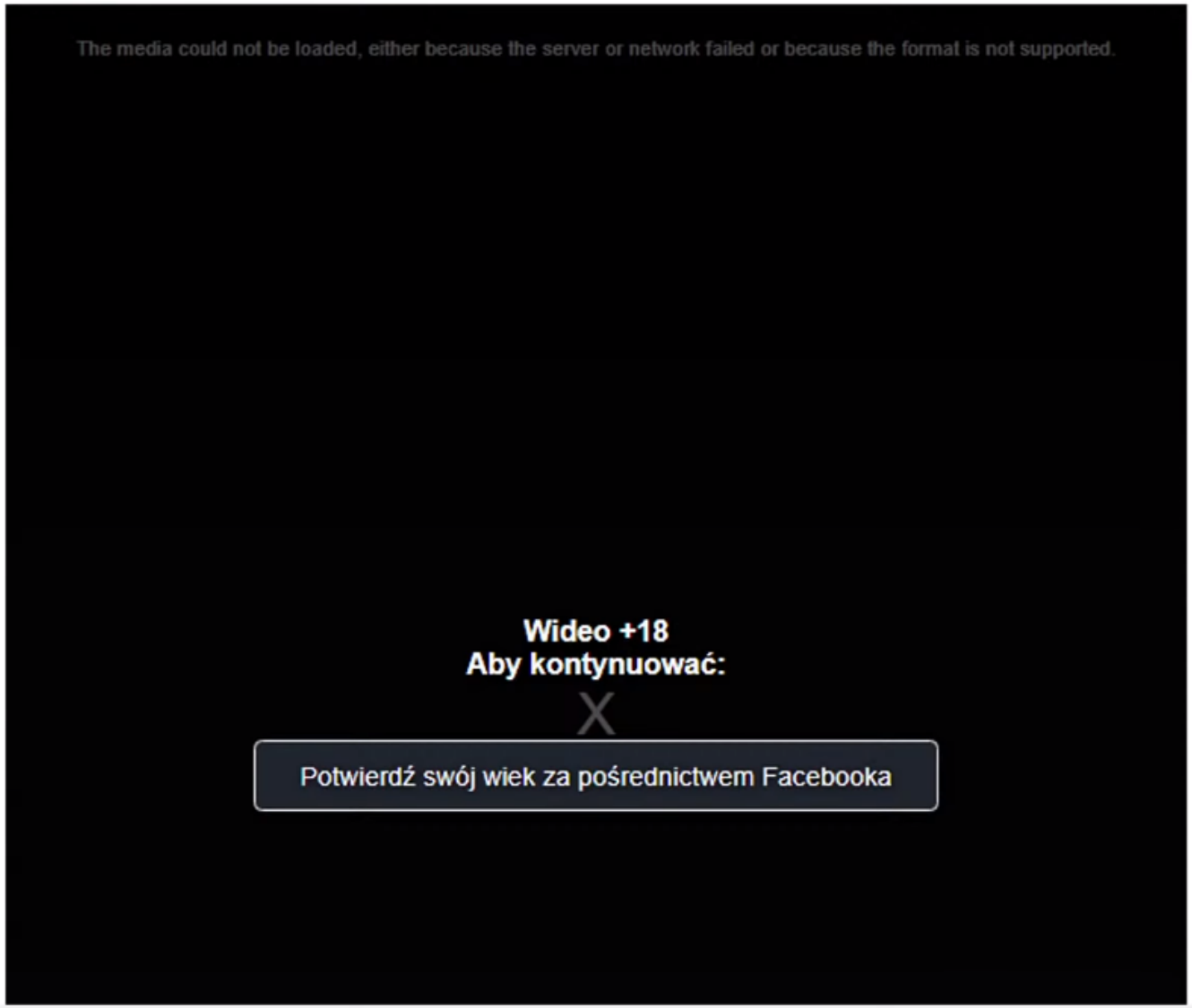
Porwanie dziecka w centrum handlowym. [WIDEO]

Porwanie dziecka w centrum handlowym. [WIDEO]

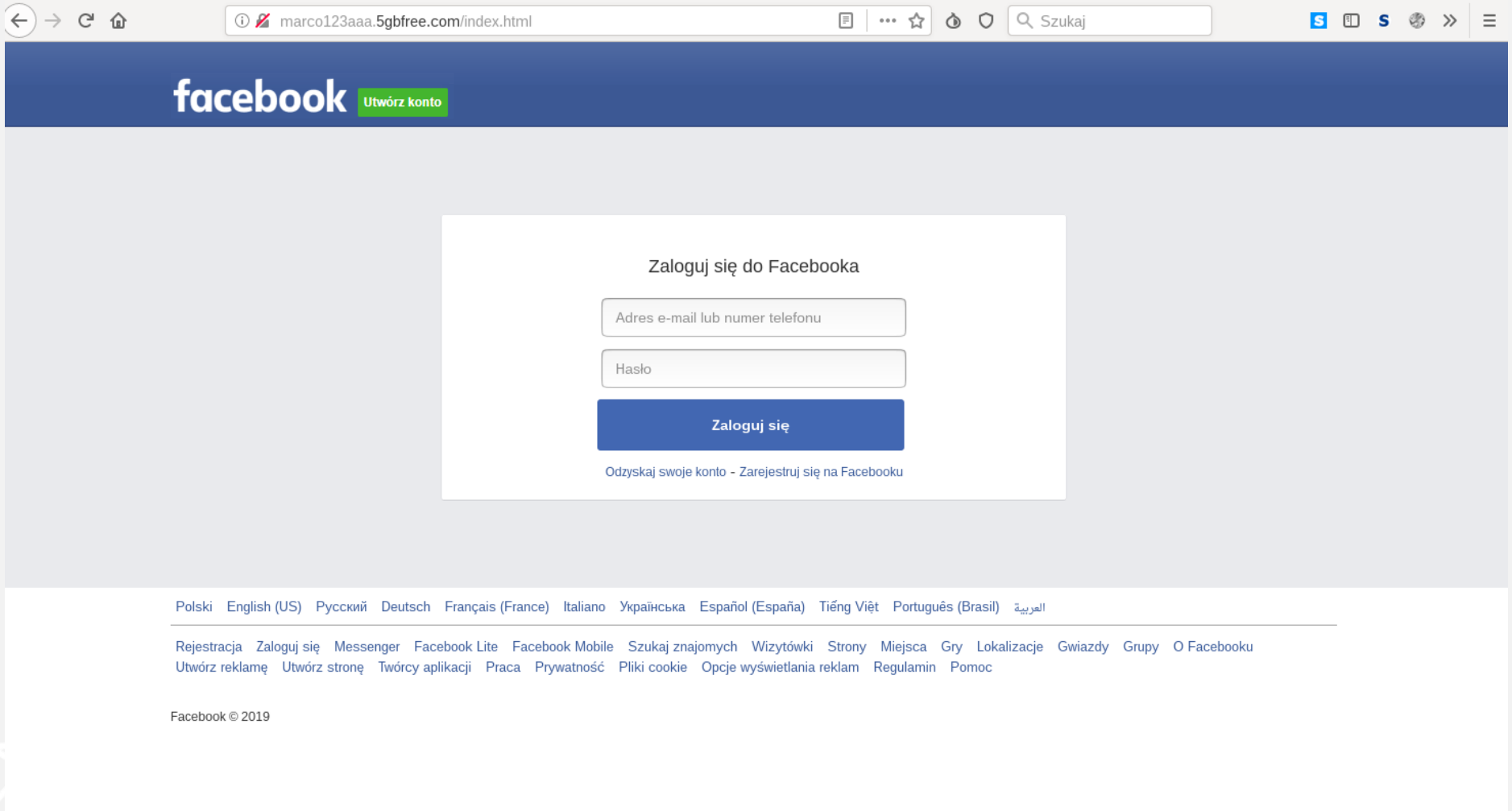
PODZIEL SIĘ

9-latka odwiedziła z rodzicami i bratem galerie handlową. Zaraz po tym zniknęła, wszystko nagrała kamera. Policjanci wciąż nie wiedzą kto ją porwał , 9-letnią Natalie S. Dziewczyna została uprowadzona dnia 2019-09-08 o godzinie 16 w Warszawskiej Galerii Handlowej: "Złote Tarasy". Siedziała z bratem w przejściu na pierwszym piętrze, zaraz po tym zniknęła bez śladu. Na prośbę policji i rodziców udostępniamy nagranie z

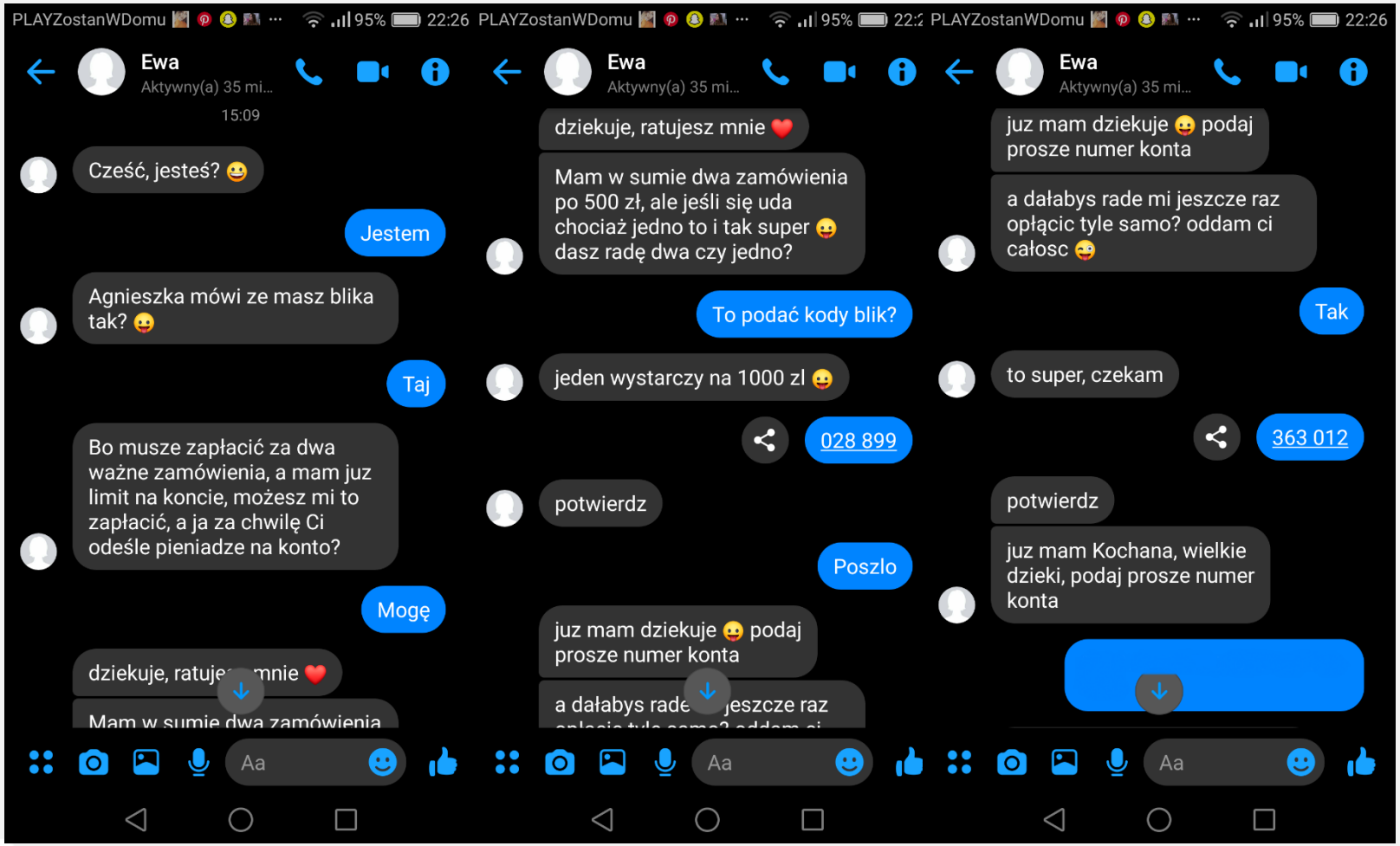
OBEJRZYJ WIDEO Z MONITORINGU (+18)



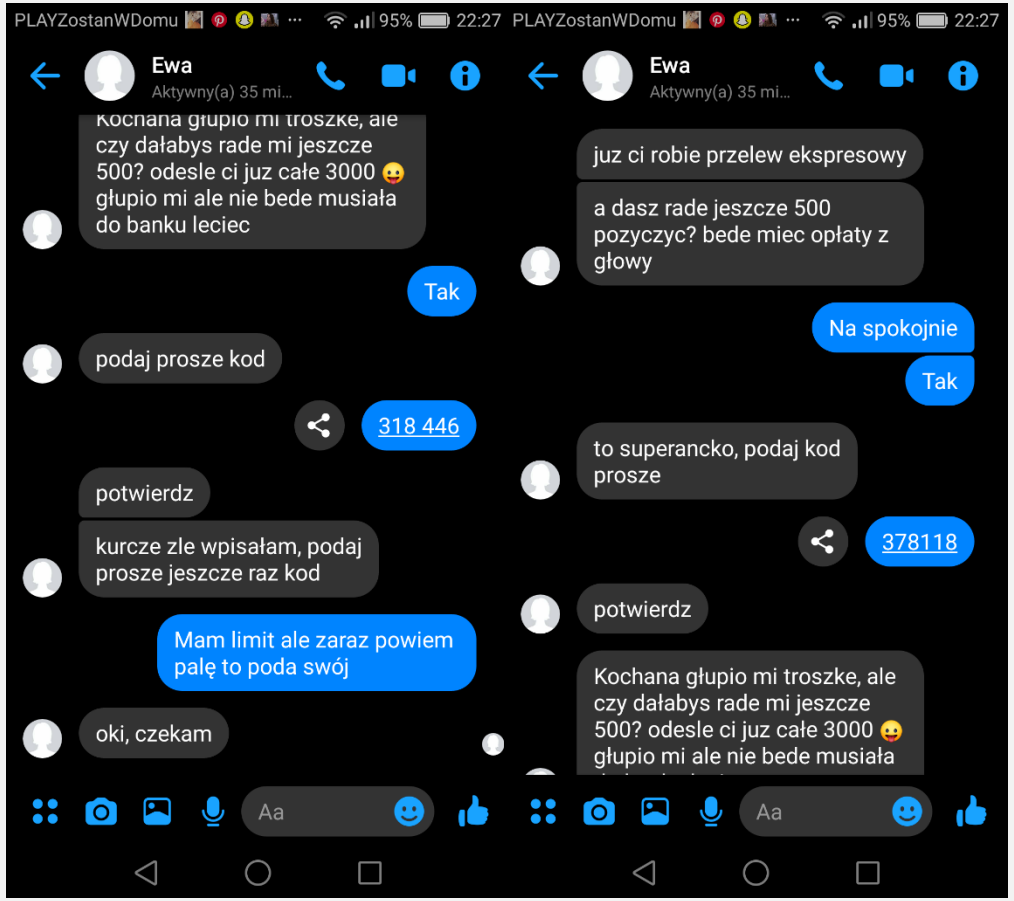
Kradzież cyfrowej tożsamości



Kradzież cyfrowej tożsamości



Kradzież cyfrowej tożsamości



Kradzież cyfrowej tożsamości

10 godz. ·

‼️ Drodzy znajomi ‼️

Gdybyście dostali wiadomość ode mnie lub Maćka z prośbą o pomoc w przelewie Blik- proszę od razu o informacje na tel i NIEREAGOWANIE na wiadomość. Grasuje ktoś, kto włamuje się na konta, podszywa pod ludzi i wyciąga od znajomych pieniądze na zasadzie „nie mam Blika, czy możesz mi pomóc, jutro oddam gotówkę”

Z góry dzięki

1

4 komentarze

NASK

Zespół Budowania Świadomości Cyberbezpieczeństwa

Zuzanna Polak
Katarzyna Koletyńska
Kamil Kuć
Marcin Napiórkowski

k.kuc@nask.pl
cwiczenia@nask.pl

KPRM | KANCELARIA PREZESA RADY MINISTRÓW
Departament Cyberbezpieczeństwa

CYBER SAMORZĄD

Zapraszamy na kolejne szkolenia