Przykłady zagrożeń

Przykłady zagrożeń

- Spam
- Phishing
- Malware
- Ransomware
- Oszustwa komputerowe
- 419, nigeryjski przekręt
- BEC, oszustwo "na dyrektora”
- 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

Receiving and placing orders for IT development Phishing ×

Ana <sveta.12@adcash.com>
do mnie

pon., 13 sty, 11:43

Good afternoon
We are launching the telegram channel, which, among other things, allows developers to earn money by reselling their modules, designs, and programs. And it also save your time on the purchase of ready-made solutions. For customers, this is an opportunity to get better trends vision and significantly save on development.

How it works:
Customer sent to us his task and its estimated price.
For a small commission, we publish this task in the channel.
Proggramers replies sent to us.
We send responses to the customer.

You will find more information in the channel info.
Telegram channel: https://t.me/itgreat
...

Jessie <vip.nkov@dreamhost.com>
do mnie

rosyjski › polski Wyświetl oryginalną wiadomość

S niski koszt, br przykład urządzenia oksy pod wszystkimi zadania y e.
₽ od Aketi $ 25 / miesiąc. aż do $ 5000 / *m* ec! W **meta-ty** na keto w:
MIX ~ ₴ 0-25k SOCKS4 / 5 - Przepływ i portów bez strat, a in- wszystko o t O - 25 $ miesięcznie
MIESZAĆ ~ 20-2 **7k** SOCKS4 / 5; Przepływy 2-3k ma $ 150 A miesiąc
MIX ~ 10-15k więc cks4 / 5; 10k płynie od 600 **$** miesięcznie
ARR aschaytes *i* widzimy ~~się~~ nam *pokazać* AM pokaż wszystko Linijki ~~taryf~~ i n ed ~~umieścić~~ TES T.
Proxy **a** także na podstawie § odpadów parsowanie, **mailing,** praca z siemienia lnianego Social S *M* i sieci! Hooked rzhivaetsya dowolny rotokol ~~twierdzenic!~~

Budżet, inteligentne proxy dla wszelkich zadań.
Paczka *wiek* s od **lutego 5** $ / miesiąc. up t o 5000 $ / Miesiąc ₽ ackage F T y p:
MIX ~ 20-25k *s* ocks4 / 5 ~~**– Stre AMS por ts bez**~~ e strictions R, A L L protokoły - $ am 25 H ont
MIX ~ 20-27k SOCKS4 / 5; 2-3k strumieni $ 150 A miesiąc
MIX ~ **1** 0-1 *5* k SOCKS4 / 5; 10k $ strumieni 60 miesiąc *0*
Contac t nas i będziemy w stanie pokazać **ty cała li ne taryf z** d zapewnić t est.
`Prox tj s są dobrze przystosowane do pars` l ng, Mailin g, pracując wi th sieci społecznych. Każdy wspornik protokołem e d.

https://hellototracks.com/polenpost/pl/?cep Szukaj

Poczta Polska

Strona główna | O firmie | Biuro prasowe | Praca | Kontakt |

Paczka zatrzymana w terminalu

- Wciąż brakuje płatności za fracht: 9zł

Nadawca: Media Markt
Opis: „Telefon wygrany w konkursie"

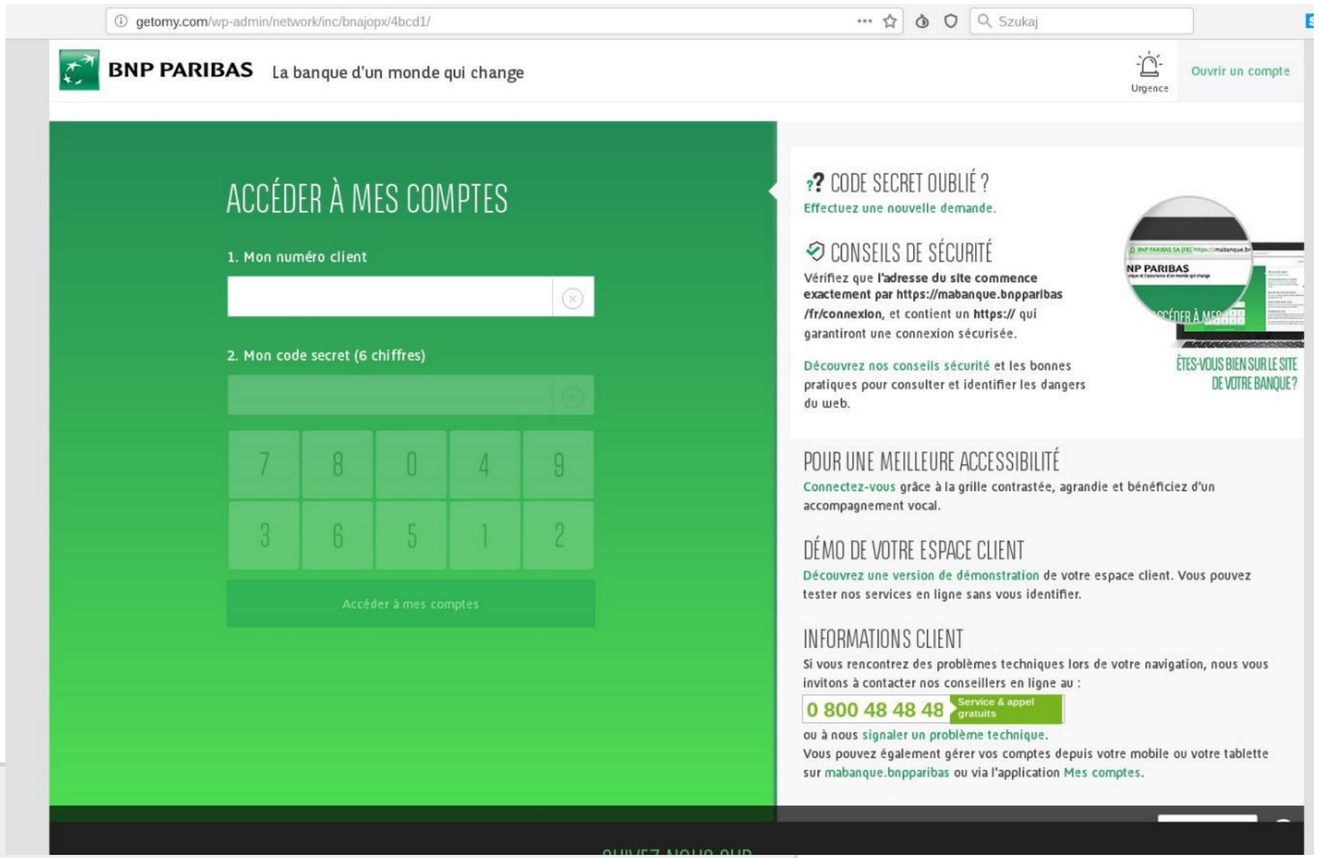
Paczka zostanie wysłana natychmiast po opłaceniu frachtu

Zapłać fracht

Dostawa : 1-2 dni

Phishing

- Czym jest phishing?
  - Metoda wyłudzenia danych
- Jak rozpoznać phishing?
  - Ataki phishingowe zwykle polegają na przesłaniu krótkich wiadomości tekstowych, które pobudzają silne emocje.
- Metody manipulacji
  - ktoś nas okrada,
  - dzieje się krzywda twoim bliskim,
  - szantaż,
  - oskarżenie o popełnienie przestępstwa,
  - blokada środków na koncie.
- Jak postępować po zidentyfikowaniu wiadomości typu phishing?
  - Pierwsza reakcja
  - Ocena sytuacji
  - Reakcja końcowa



Anna <Anna@0589230952602282.947114.love.com>
do 637348210

Hi,
Whenever you enter the building I blush.. I'm hoping you didn't notice it, I'd be very shy if you did. I'm usually quite cool with men, I don't know what happens to me when I see u :) Text me if u like..

Check out her Profile, or browse her Photo Album

REPLY | Unsubscribe Me! | Report Spam

Malware – definicje

- Czym jest Malware?
  - 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)
- Źródła infekcji
  - Załącznik lub odnośnik (link) w wiadomości e-mail
  - Przejęta przez przestępców lub podstawiona, fałszywa strona
  - Podstawione reklamy na zwykłych stronach

Malware – działanie

- 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
- Jak zapobiegać?
  - Aktualizacje
  - Oprogramowanie antywirusowe
  - Regularne skanowanie oprogramowaniem antywirusowym
  - Kopie zapasowe danych
  - Firewall

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

Ransomware

- 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.
- Zapobieganie atakom
  - <u>Nie ma jednego skutecznego środka na odzyskanie zaszyfrowanych plików.</u>
  - 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.

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).


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

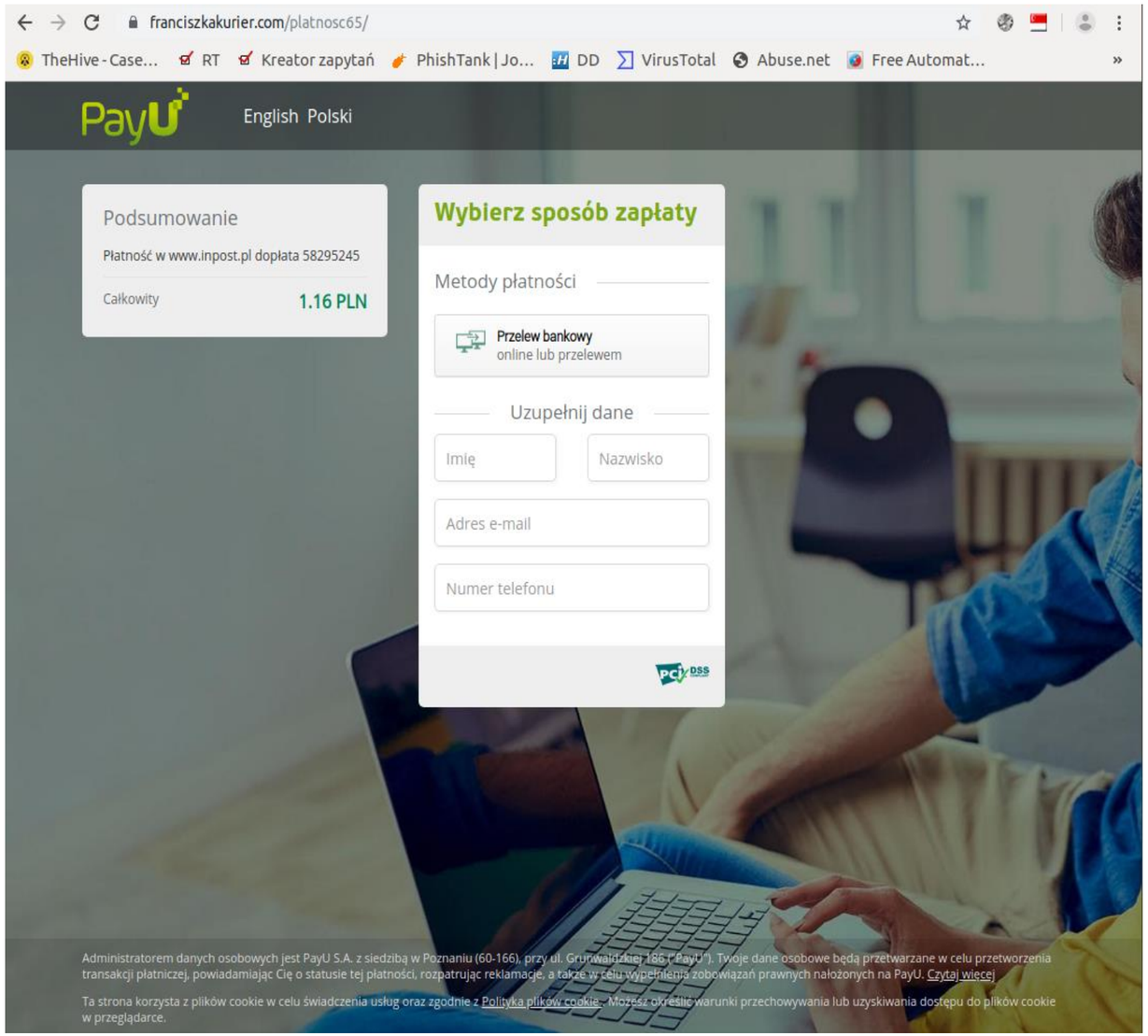
Oszustwo komputerowe

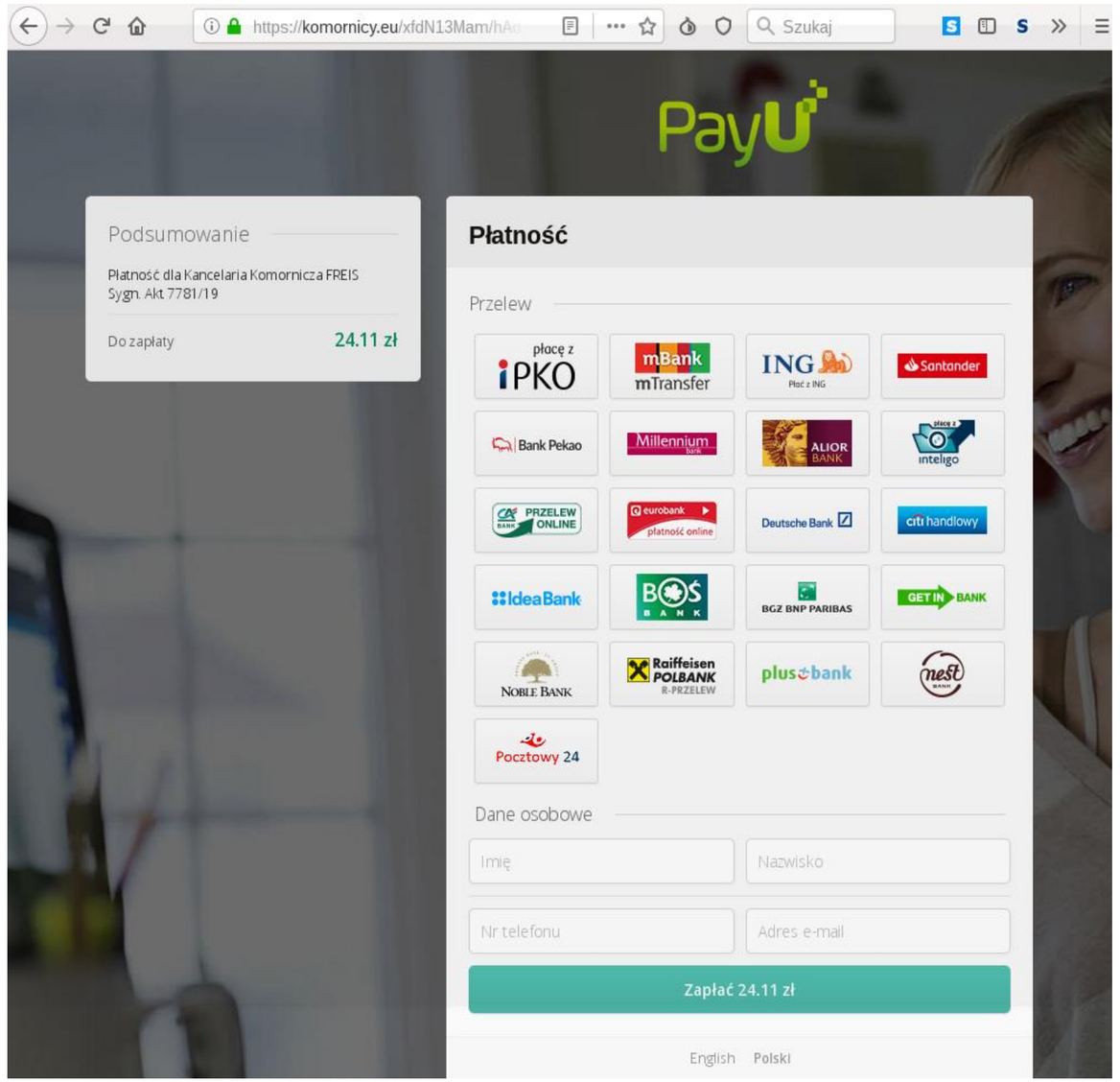
- Kodeks karny określa przestępstwa komputerowe oraz powiązane z nim artykuły dot. ochrony informacji (niejawnych, danych osobowy etc.).
- W kodeksie karnym przestępstwo komputerowe (art. 287 k.k.). Czyn zabroniony polega na wpływie na komputerowe zapisy informacji.
- Sprawcą oszustwa komputerowego może 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 reklamacje, 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 cookie. 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
GET IN BANK
NOBLE BANK
Raiffeisen POLBANK
plus bank
nest BANK
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 wzięło nazwę od numeru artykułu z nigeryjskiego kodeksu karnego.
  - Jest znane od XVI wieku. Wówczas nazywało się Listem Hiszpańskiego Więźnia.
- 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

FDJ <info@cox.net>
do

pon., 20 kwi, 12:20

Ta wiadomość może być niebezpieczna

Podobne wiadomości posłużyły już w przeszłości do kradzieży danych osobowych. Nie klikaj żadnych linków, nie pobieraj załączników ani nie odpowiadaj z użyciem swoich danych osobowych.

Wygląda bezpiecznie

Attn: You have a charity donation of $ 1,500,000.00 from Mrs. Julie Leach, a power-ball jackpot lottery winner of $ 310 Million. For claim, Reply to: julieleach014@yahoo.com

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”.
- 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.
- 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,

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.

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]

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]

Wysłane z mojego urządzenia mobilnego.

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

- Gdy zakładasz profil należy rozważyć czy konieczne jest, aby profil zawierał imię i nazwisko użytkownika.
- Używaj silnego hasła (najlepiej składające się z losowych znaków – np. manager haseł) i inne niż wykorzystywane w pozostałych serwisach.
- Skonfiguruj ustawienia prywatności konta.
- 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
- Pamiętaj, że korzystając z serwisów społecznościowych łatwo można (również nieintencjonalnie) zdradzić poufne i wrażliwe dane osób trzecich, pracodawcy, kontrahenta
- Nie należy korzystać z prywatnych profili w celach zawodowych oraz przechowywać lub przesyłać dokumentacji służbowej za pomocą zewnętrznych nieautoryzowanych serwisów
- Skasuj swój profil w serwisie, z którego nie będziesz więcej korzystać
- 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