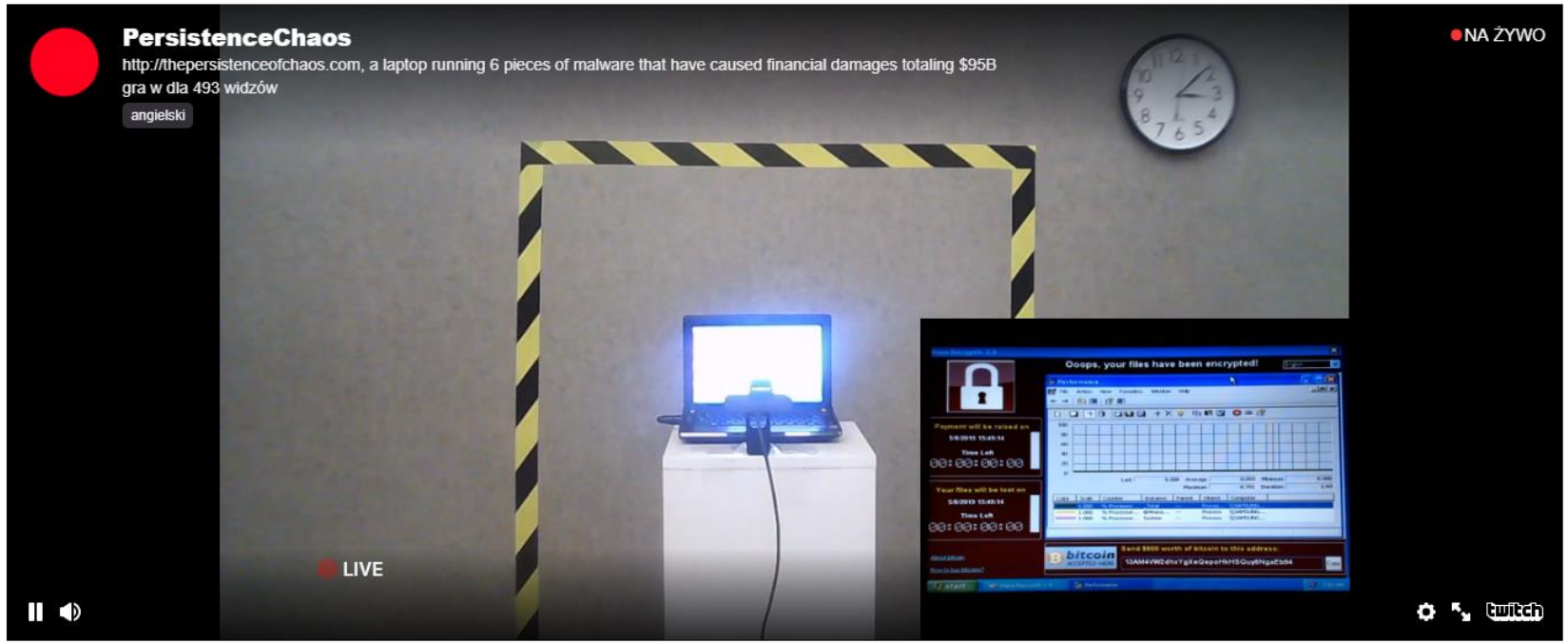
ANATOMIA CYBERBEZPIECZEŃSTWA

JAKUB JAGIELAK CERTIFIED ETHICAL HACKER

You Know
Nothing
Jon Snow

The Persistence of Chaos, 2019

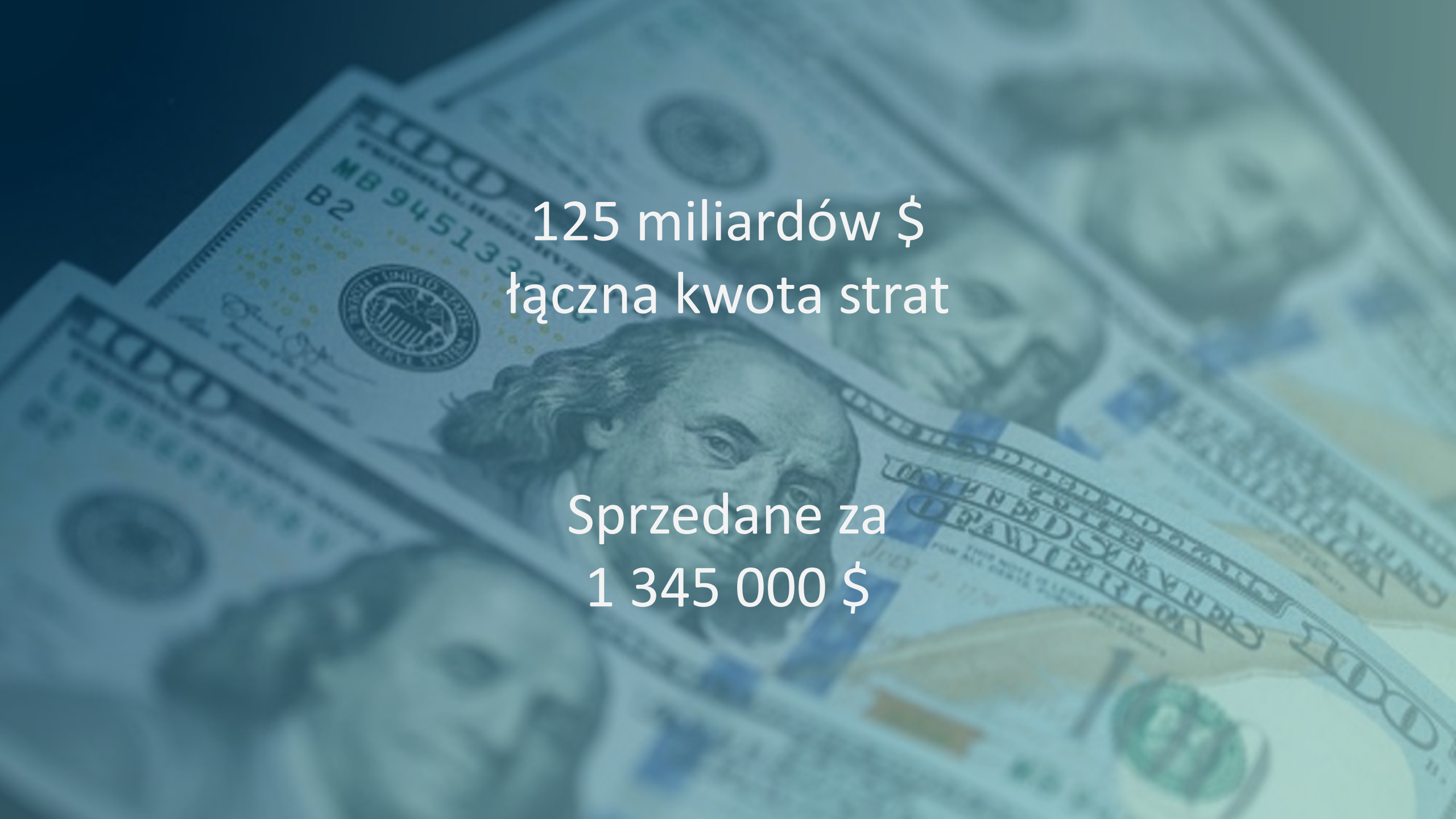
GUO O DONG



This page is livestreaming The Persistence of Chaos, a laptop running 6 pieces of malware that have caused financial damages totaling $95B. The piece is isolated and airgapped to prevent against spread of the malware.

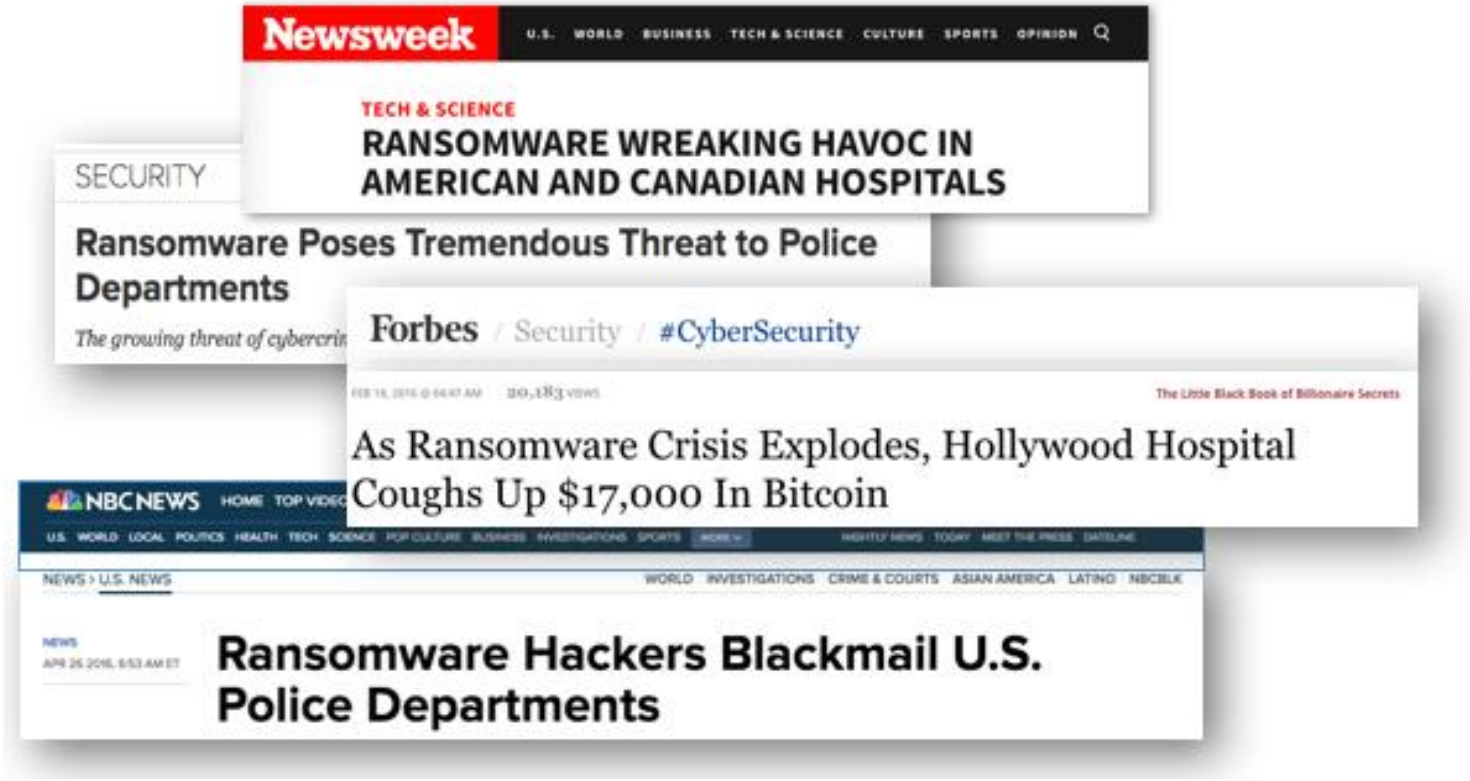
HTTPS://THEPERSISTENCEOFCHAOS.COM/

- **ILOVEYOU**
  - The ILOVEYOU virus, distributed via email and file sharing, affected 500,000+ systems and caused $15B in damages total, with $5.5B in damages being caused in the first week.
- **MyDoom**
  - MyDoom, potentially commissioned by Russian e-mail spammers, was one of the fastest spreading worms. It's projected that this virus caused $38B in damages.
- **SoBig**
  - SoBig was a worm and trojan that circulated through emails as viral spam. This piece of malware could copy files, email itself to others, and could damage computer software/hardware. This piece of malware caused $37B in damages and affected hundreds of thousands of PCs.
- **WannaCry**
  - WannaCry was an extremely virulent ransomware cryptoworm that also set up backdoors on systems. The attack affected 200,000+ computers across 150 countries, and caused the NHS $100M in damages with further totals accumulating close to $4B.
- **DarkTequila**
  - A sophisticated and evasive piece of malware that targeted users mainly in Latin America, DarkTequila stole bank credentials and corporate data even while offline. DarkTequila costed millions in damages across many users.
- **BlackEnergy**
  - BlackEnergy 2 uses sophisticated rootkit/process-injection techniques, robust encryption, and a modular architecture known as a "dropper". BlackEnergy was used in a cyberattack that prompted a large-scale blackout in Ukraine in December 2015.



125 miliardów $
łączna kwota strat

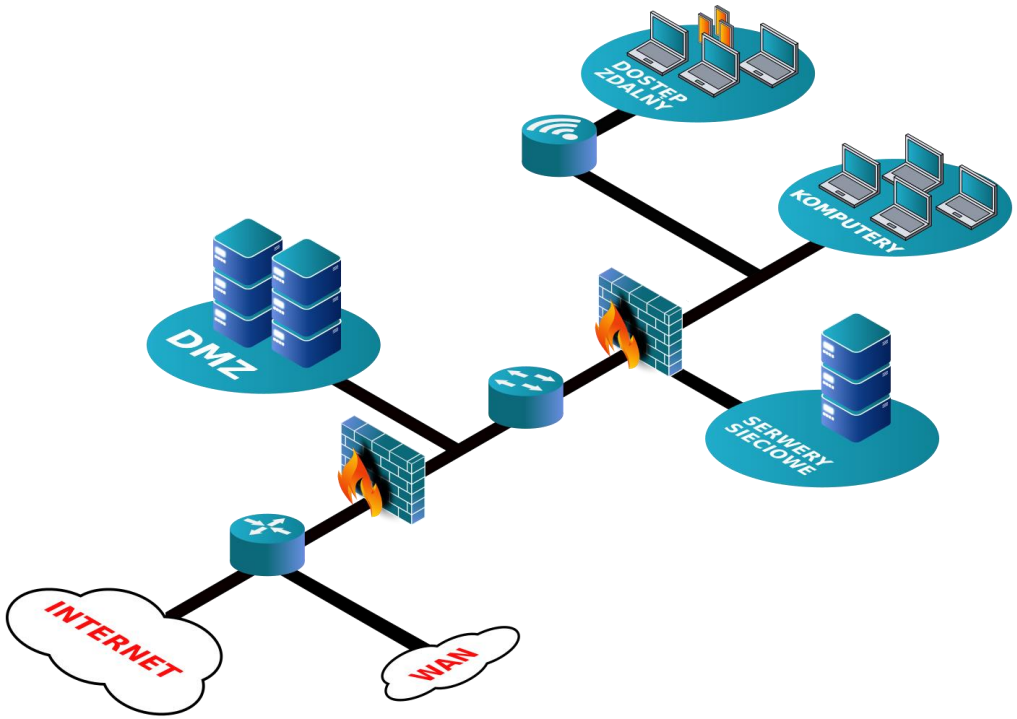
Sprzedane za
1 345 000 $

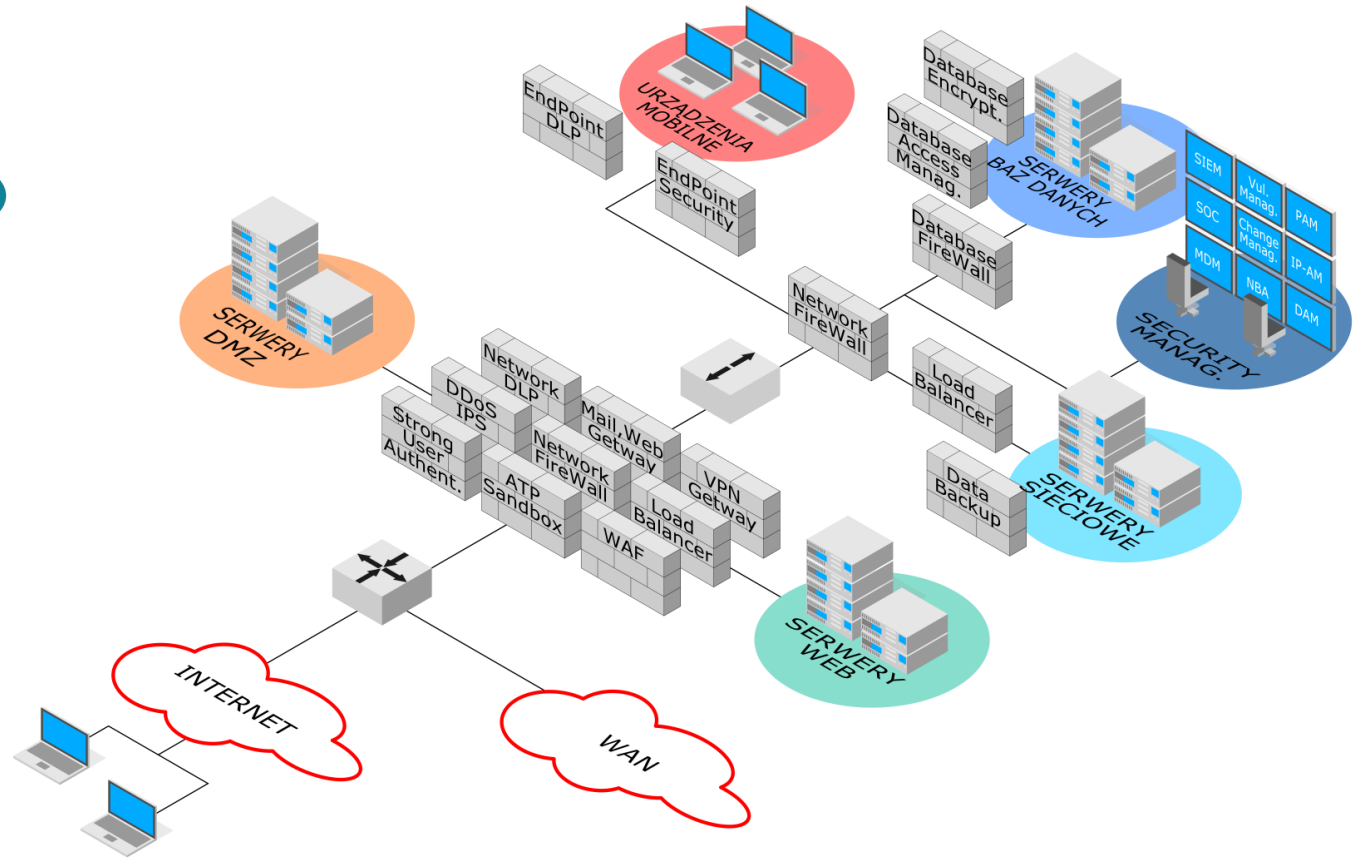

Newsweek
U.S. WORLD BUSINESS TECH & SCIENCE CULTURE SPORTS OPINION
TECH & SCIENCE
RANSOMWARE WREAKING HAVOC IN AMERICAN AND CANADIAN HOSPITALS
SECURITY
Ransomware Poses Tremendous Threat to Police Departments
Forbes / Security / #CyberSecurity
As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin
NBC NEWS
NEWS > U.S. NEWS
Ransomware Hackers Blackmail U.S. Police Departments


Hackers hit
"What's been taken is bits of data that the

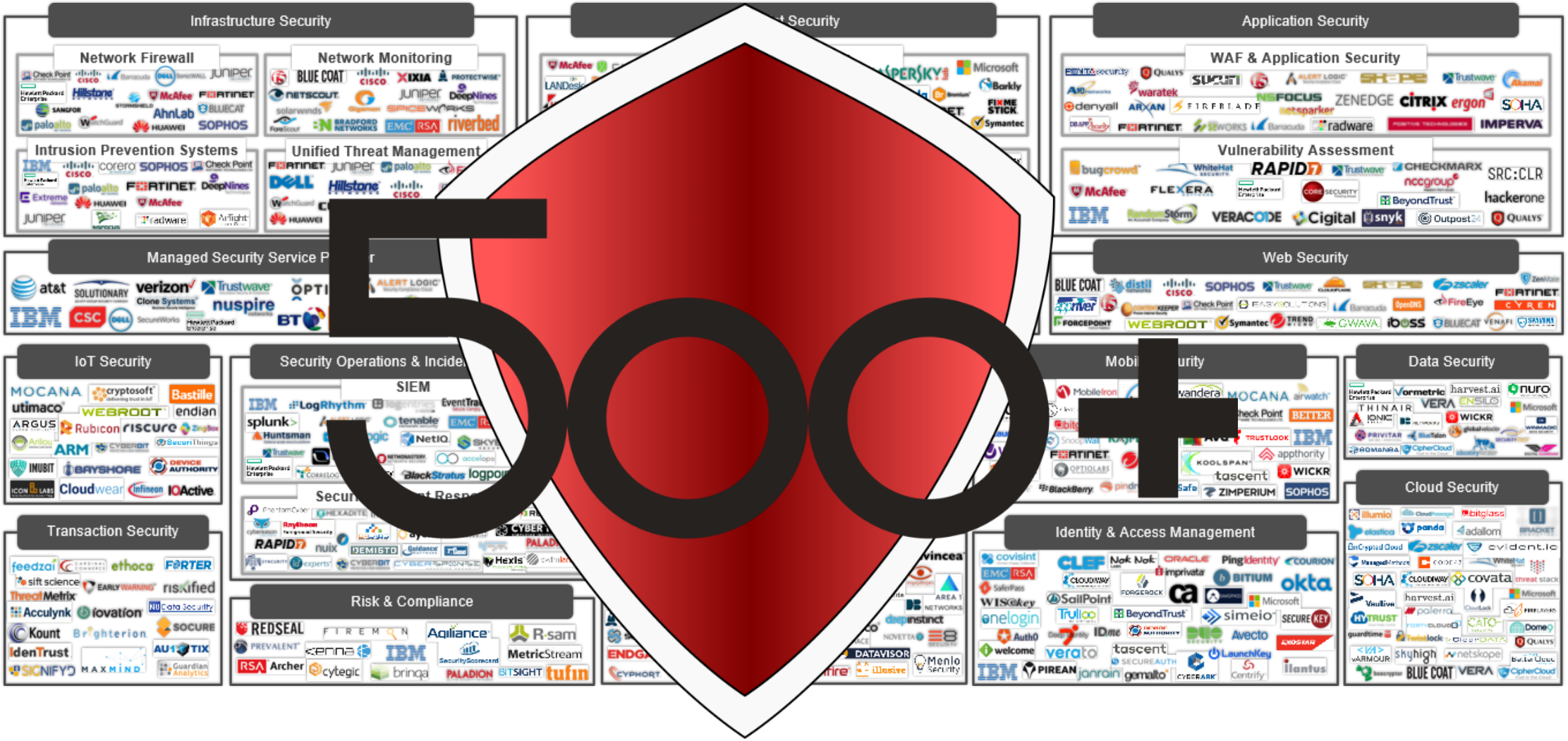

moves to internet
High-tech gadgets bring new opportunities for hackers!
FBI announces arrests in $70 million cyber-theft
Phising
Malware
2011 will see increased security threats on mobile devices.
Apple can't
Tunes charge scam
Online holiday
Six people have been arrested over a scam wich police
Online scam 'breached security


The New York Times
U.S. Banks Again Hit by Wave of Cyberattacks
abc NEWS
Cyber Attack
Latest Cyber Attack News
CNN Politics
Watch where you click: International cyber attacks on the rise
THE WALL STREET JOURNAL.
Cyber Attackers Target Building Management Systems
Article
Comments
Increasingly, companies are connecting building energy management systems to networks and to the Internet in an effort to automate lighting, heating and air conditioning. The danger is that criminals could use those connections to unlock doors, turn off lights or sabotage data centers by turning up the heat.

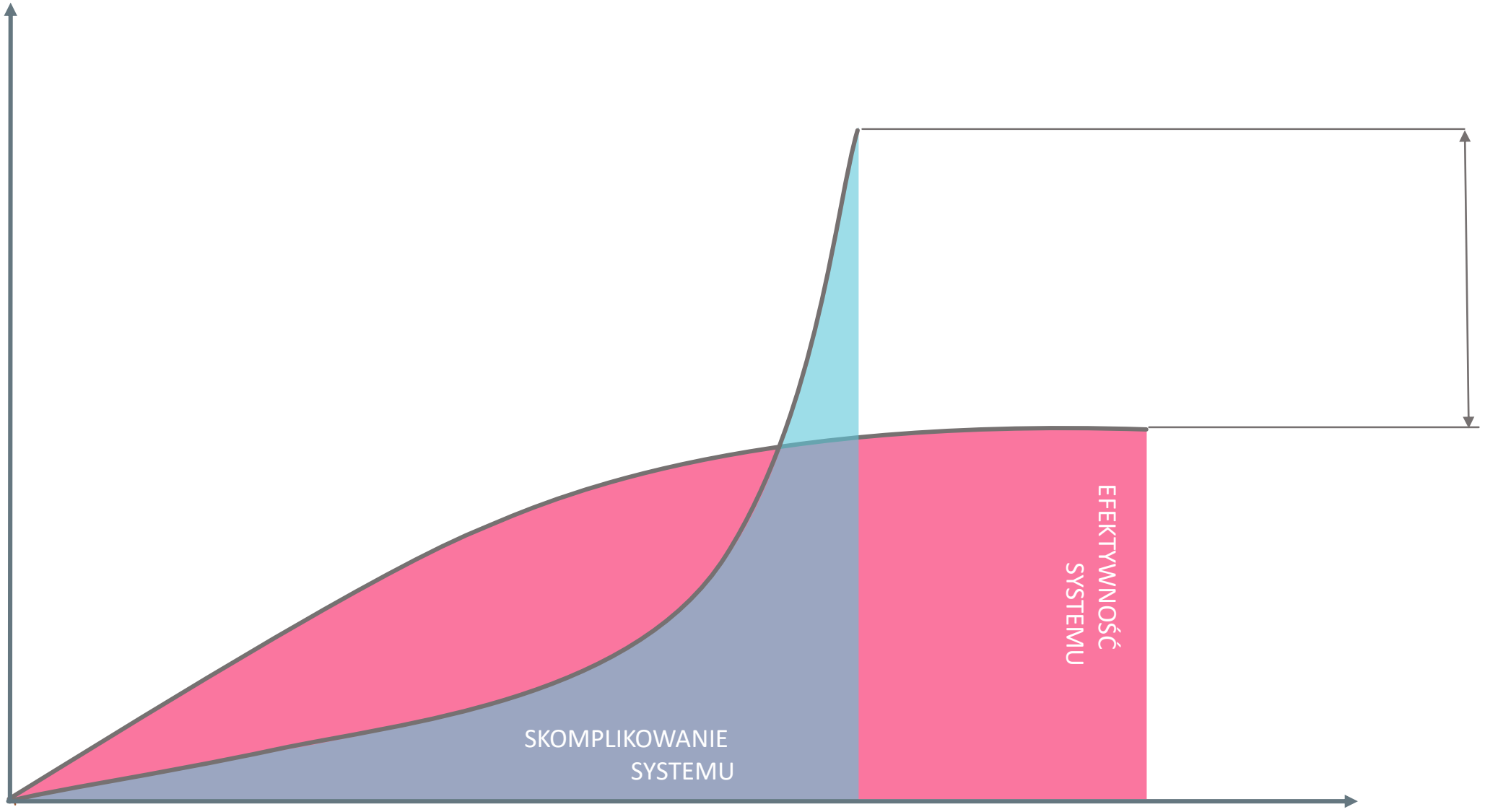

DOSTĘP ZDALNY
KOMPUTERY
DMZ
SERWERY SIECIOWE
INTERNET
WAN


URZĄDZENIA MOBILNE
EndPoint DLP
EndPoint Security
Database Encrypt.
Database Access Manag.
SERWERY BAZ DANYCH
Database FireWall
SIEM
Vul. Manag.
PAM
SOC
Change Manag.
IP-AM
MDM
NBA
DAM
SECURITY MANAG.
SERWERY DMZ
Network DLP
DDoS IPS
Strong User Authent.
Network FireWall
Mail,Web Getway
ATP Sandbox
VPN Getway
Load Balancer
WAF
Network FireWall
Load Balancer
Data Backup
SERWERY SIECIOWE
SERWERY WEB
INTERNET
WAN

I BĄDŹ TU MĄDRY



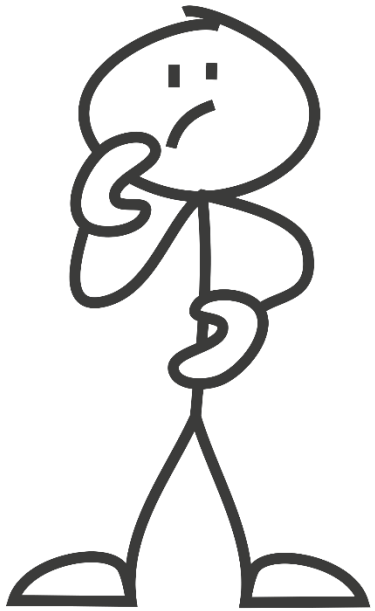
SECURITY GAP



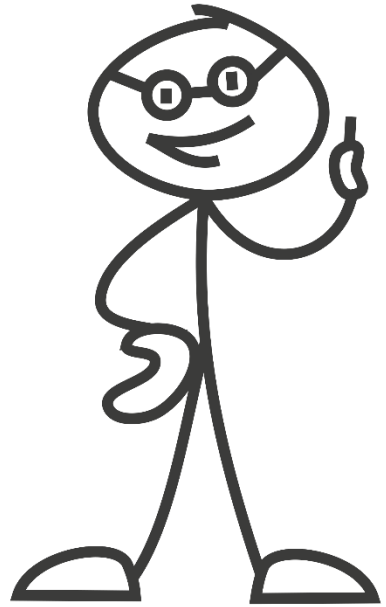
Jak to się zaczęło

```
print("Hello, World!")
```

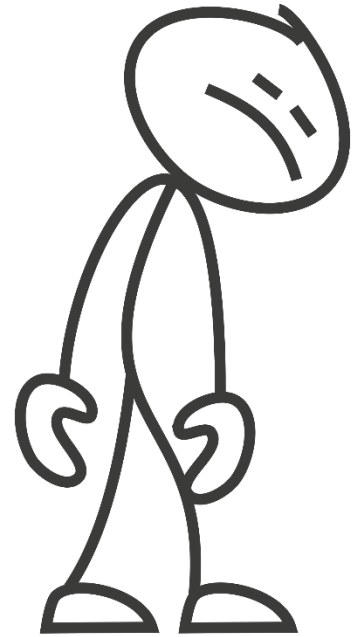
HAKERZY



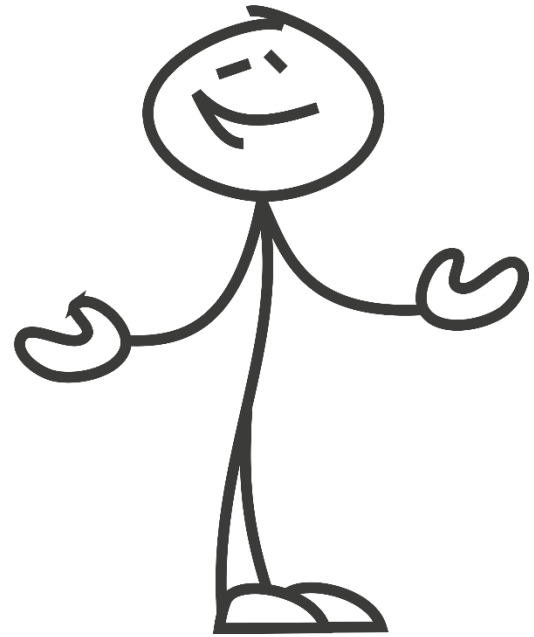
Nie wie ale robi



Wie i robi



Nie wie i nie robi



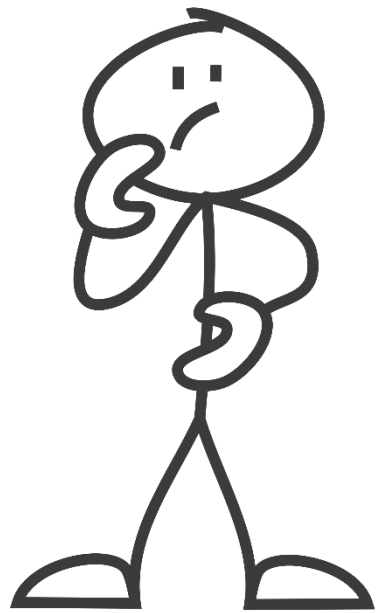
Wie ale nie robi

Angielskie słowo hacker pochodzi od hack.

Termin **hack** wśród studentów Massachusetts Institute of Technology w latach 60. odnosił się do płatanych żartów, takich jak np. owinięcie górującej nad kampusem uniwersyteckim kopuły folią odbijającą promienie świetlne. Aby zasłużyć na to określenie żarty musiały się wyróżniać szczególną pomysłowością i stylem oraz nie przynosić szkody

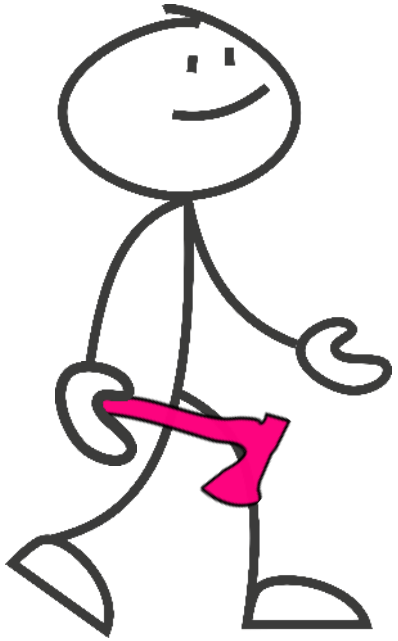
www.mit.edu.com

HAKERZY



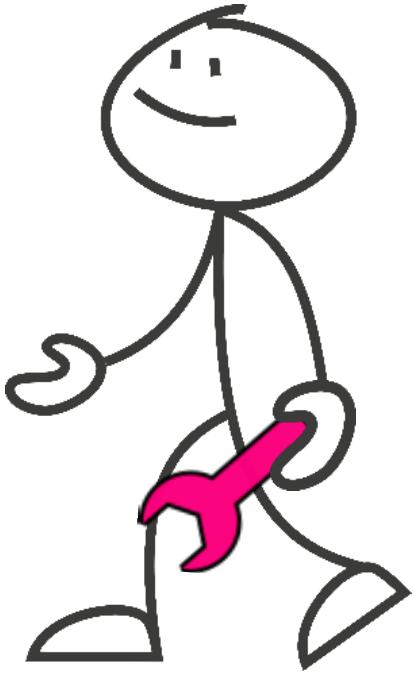
Nie wie ale robi

Wie i robi



HAKER – OSOBA KTÓRA ANGAŻUJE SIĘ W AKTYWNOŚĆ BEZ WIEDZY I UMIEJĘTNOŚCI

HAKER – OSOBA O BARDZO DUŻYCH, PRAKTYCZNYCH UMIEJĘTNOŚCIACH INFORMATYCZNYCH



HACKOWANIE - UŻYWANIE, WYKORZYSTYWANIE RZECZY DO CELÓW DO KTÓRYCH NIE SĄ PRZEZNACZONE, ZAPROJEKTOWANE.

Słownik języka polskiego

Google Maps Hacks

HAKER != PRZESTĘPCA

HAKER TO OSOBA CZYNU

HAKERZY / CYBERPRZESTĘPCY

White HAT

1

Gray HAT

2

Black HAT

3


MOTYWACJA GRUP PRZESTĘPCZYCH
ZYSK
ZEMSTA
TERRORYZM
SZPIEGOSTWO
HAKTYWIZM
DLA ROZRYWKI

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ M721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex:.....MALE
Race:.....WHITE
Place of Birth:.....VAN NUYS, CALIFORNIA
Date(s) of Birth:.....08/06/63; 10/18/70
Height:.....5'11"
Weight:.....190

Łamałem ludzi, nie hasła

— Kevin D. Mitnick —

„Sztuka Podstępu 1994r.”


Dlaczego ?

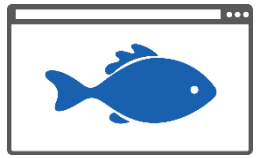
Cytat Dnia

Pracownicy mają bezpieczeństwo w…*

Borys Łącki

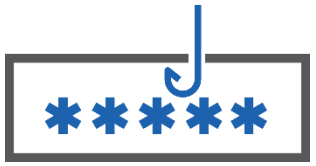
*) Dokumencie polityki bezpieczeństwa

Co 20 adres www jest podejrzany



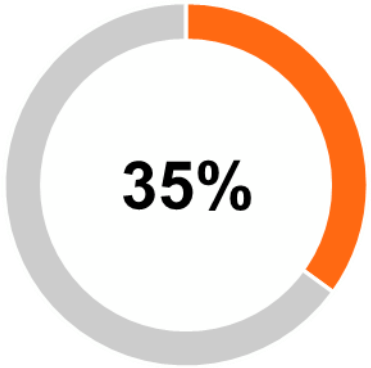
Praktycznie każda strona wykorzystywana do phishingu wykorzystuje protokół HTTPS

90% złośliwego oprogramowania dostarczone pocztą elektroniczną

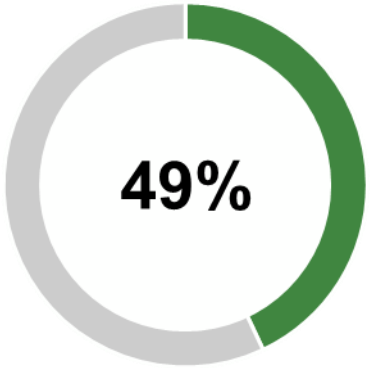


Większość naruszeń realizowana jest za pomocą skradzionych danych uwierzytelniających

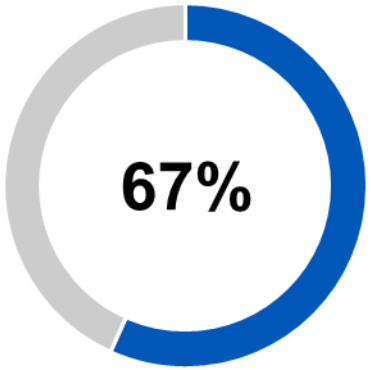
LUDZIE WIEDZĄ LEPIEJ ?



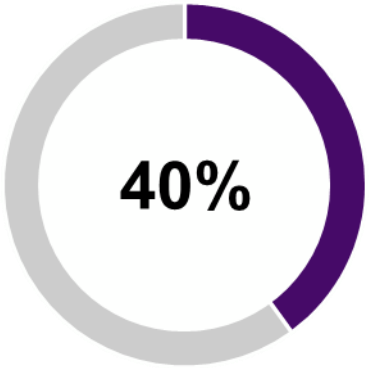
pracowników, którzy wiedzą, że zostali zhakowani, nie przejmuje się później zmianą haseł



pracowników przyznaje, że podczas pracy klika linki w wiadomościach od nieznanych nadawców

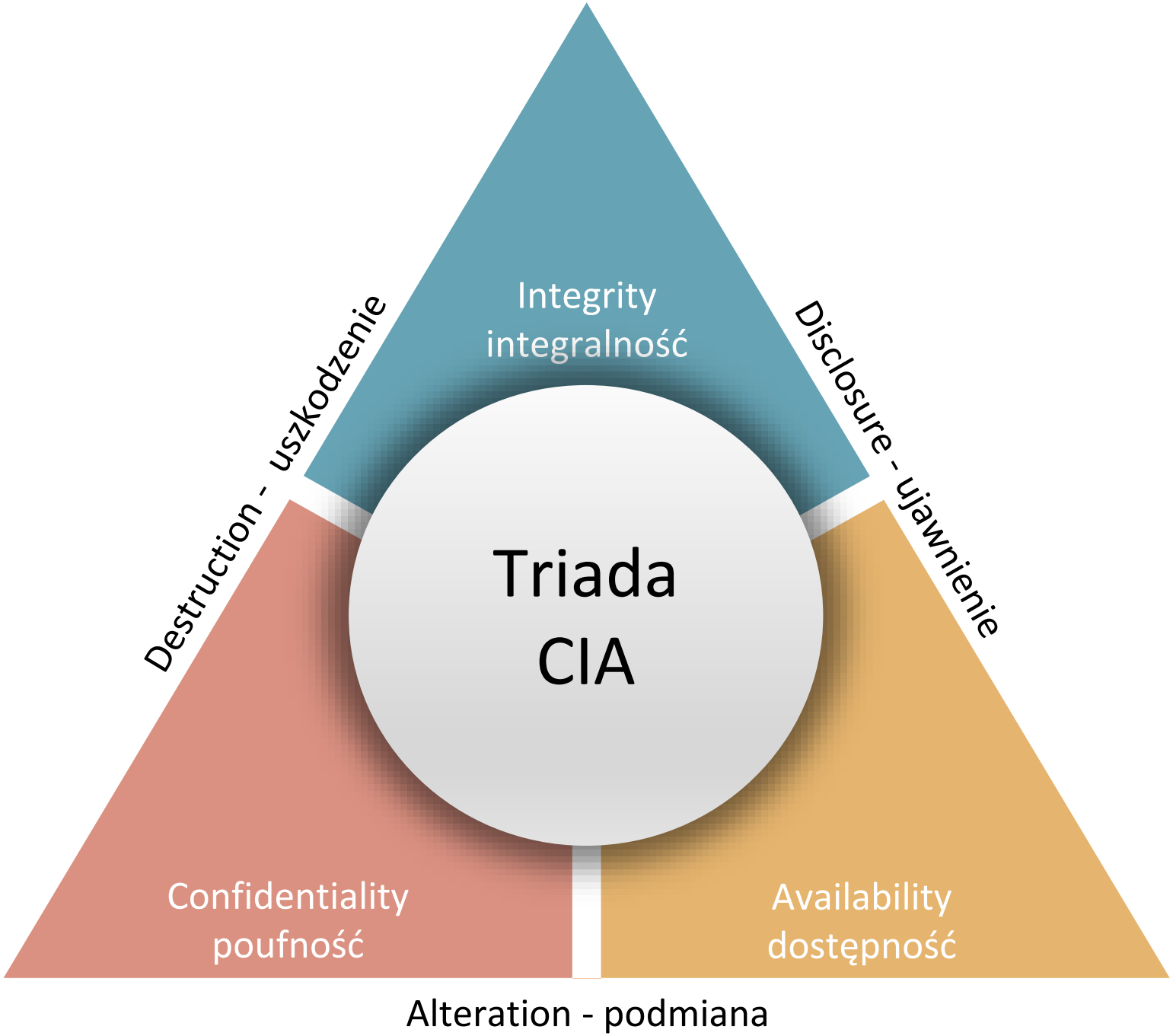


pracowników ma pewność, że otrzymali co najmniej jedną wiadomość phishingową w pracy



Spośród osób, które otrzymały wiadomość e-mail z phishingiem, około 40% go nie zgłosiło

Badania zrealizowana przez firmę CISCO w Europie w roku 2019


Integrity
integralność
Destruction - uszkodzenie
Disclosure - ujawnienie
Triada
CIA
Confidentiality
poufność
Availability
dostępność
Alteration - podmiana

malicious software

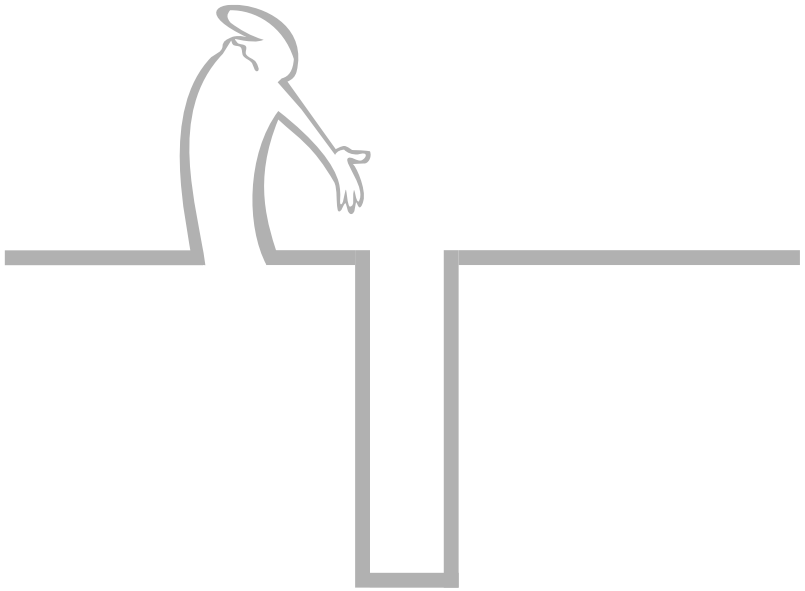
malicious
software

mal

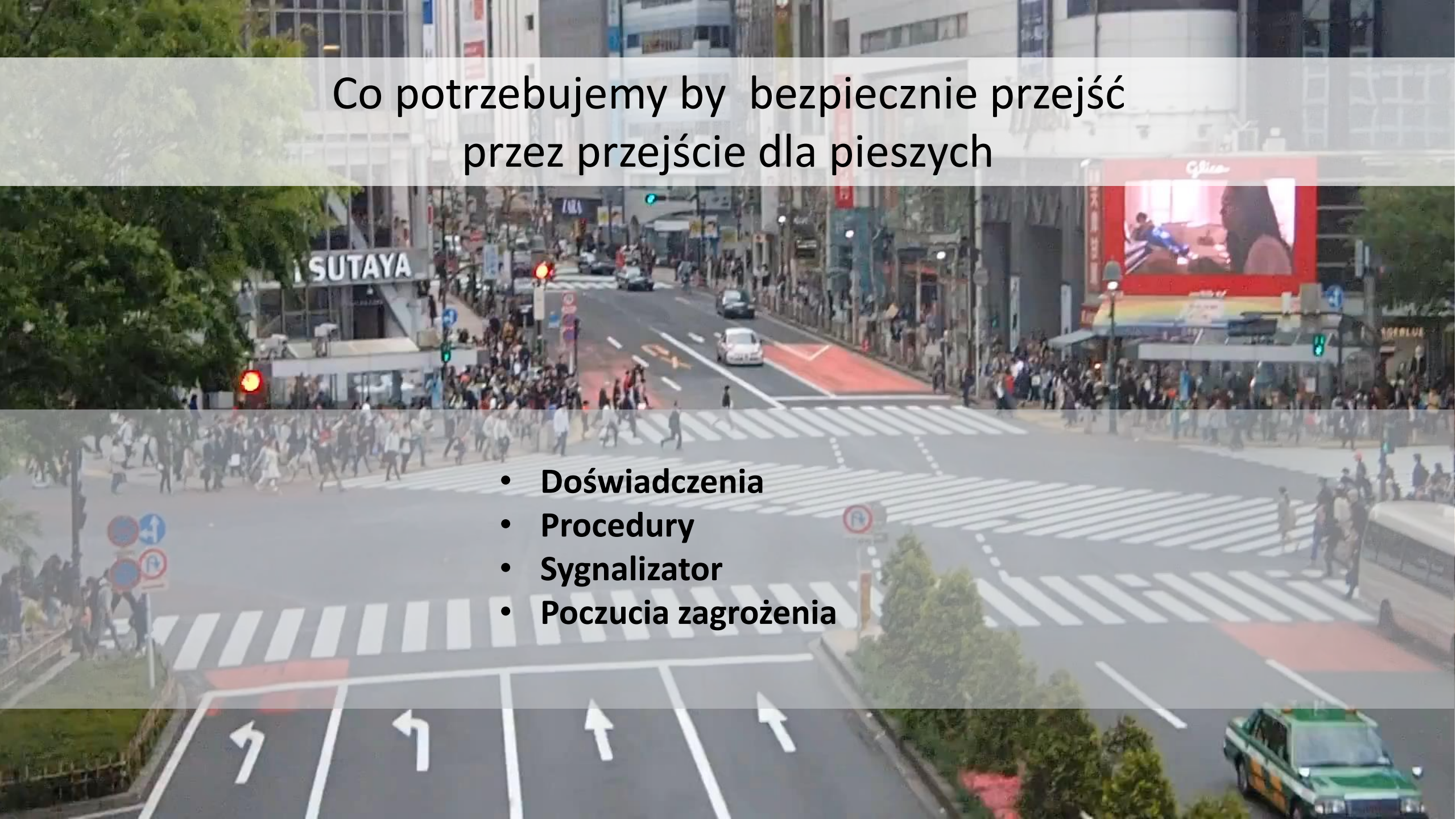
ware

1. Kradzież danych
2. Ransomware
3. Złośliwe oprogramowanie (malware)
4. Botnety
5. SPAM
6. Ataki DDoS
7. Kradzież tożsamości
8. Oszustwa (socjotechniki)
9. Dezinformacja *fake news*
10. Kopanie kryptowalut

NO RISK NO FUN



Co potrzebujemy by bezpiecznie przejść przez przejście dla pieszych

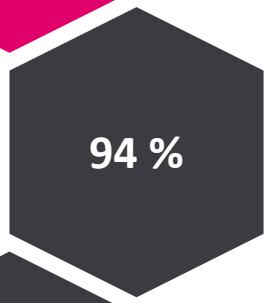


- **Doświadczenia**
- **Procedury**
- **Sygnalizator**
- **Poczucia zagrożenia**

PHISHING

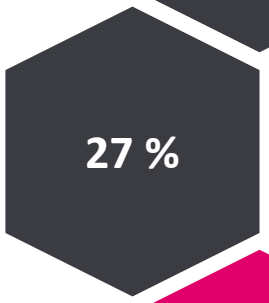
Raport CERT Polska 2019

incydentów bezpieczeństwa w sieci stanowi phishing



Data Breach Investigations Report 2019

cyberzagrożeń ma swoje źródło w emailach

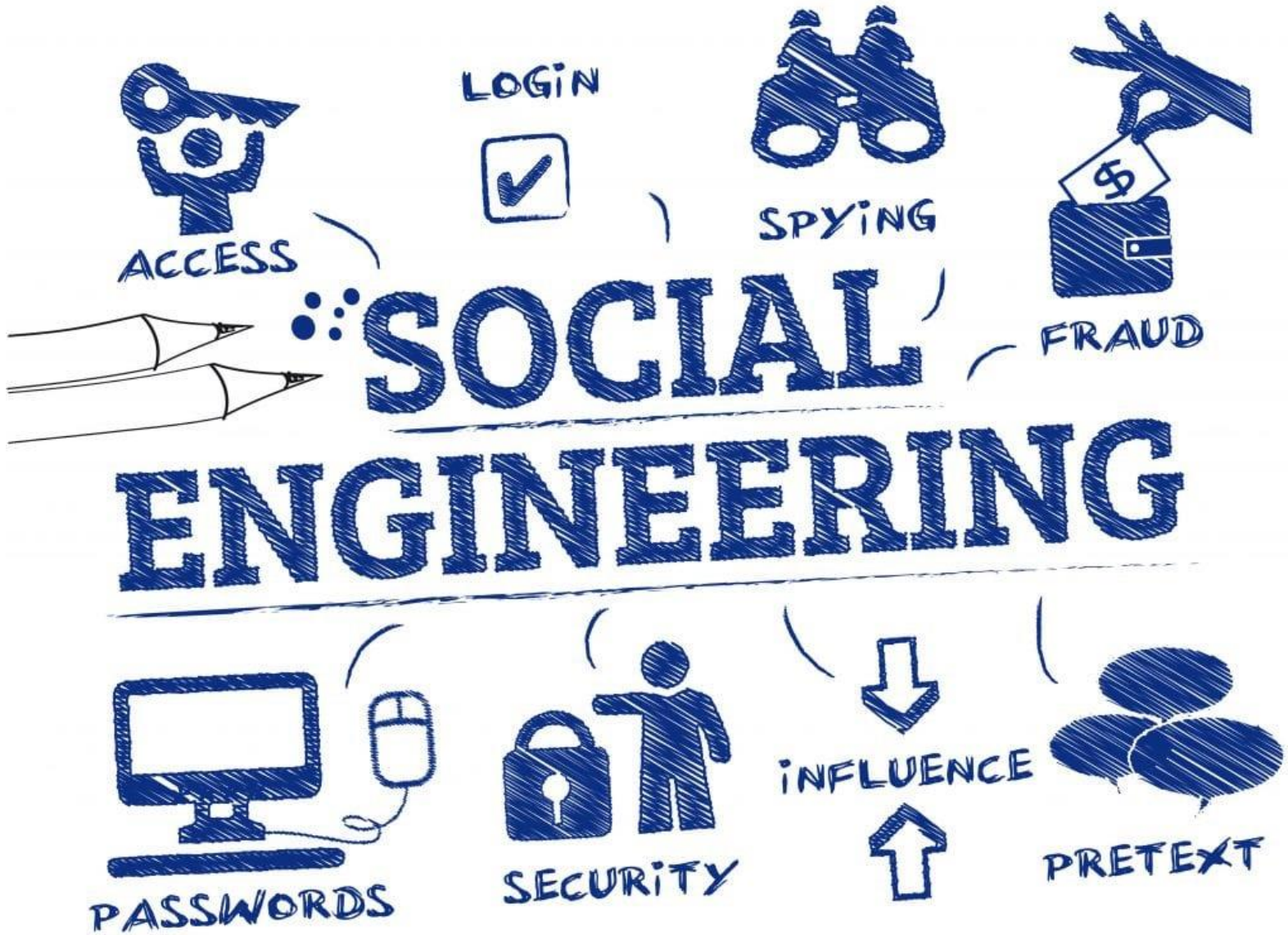


Badanie Forrester. „The Forrester Wave Enterprise Email Security, Q2 2019.” Maj 2019

ataków na firmy zostało wykonanych za pomocą skradzionych danych uwierzytelniających

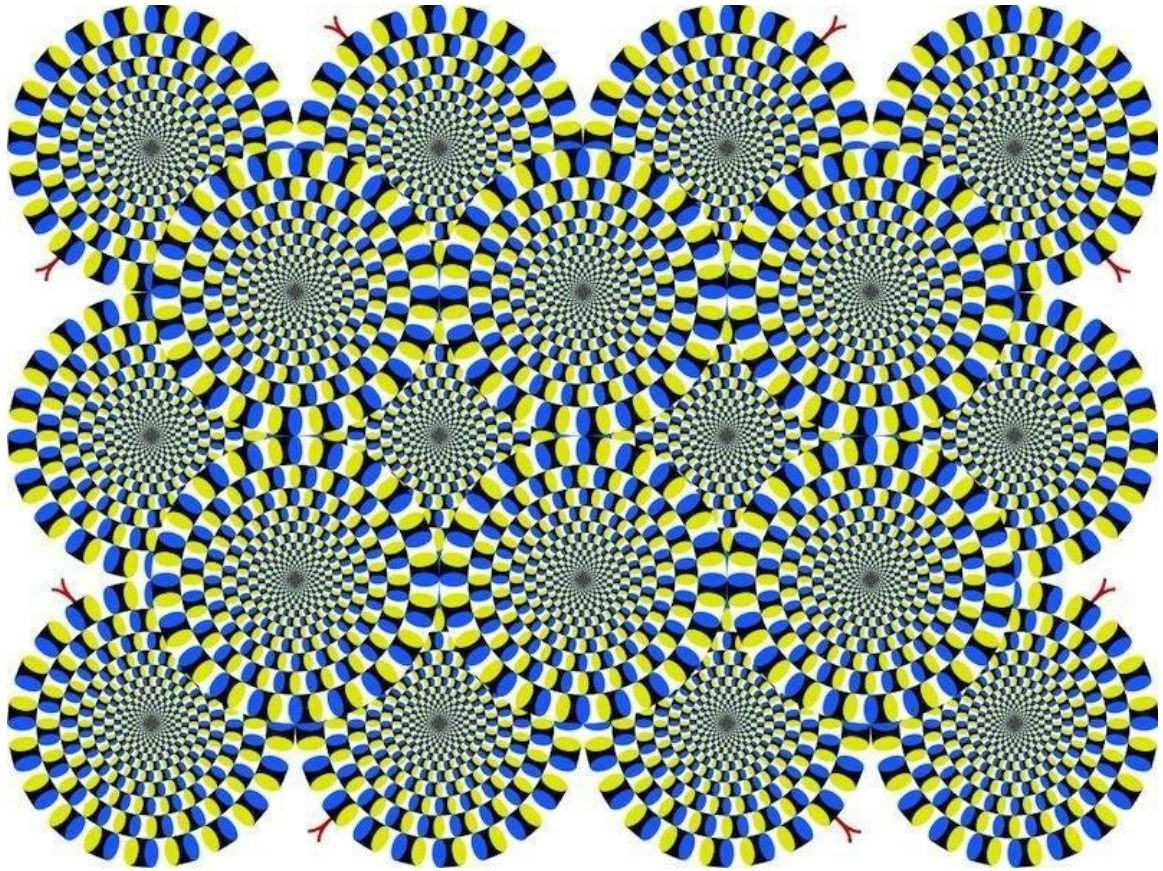
Krajobraz bezpieczeństwa polskiego internetu 2019, Cert 2020

zgłoszeń dotyczących phishingu hostowanego w polskich sieciach


LOGIN
ACCESS
SPYING
FRAUD
SOCIAL
ENGINEERING
PASSWORDS
SECURITY
INFLUENCE
PRETEXT

Phishing - Inżyniera społeczna

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań



Zdognie z nanjwoymszi baniadmai perzporawdzomyni na bytyrijskch uweniretasytch nie ma zenacznia kojnoleść ltier przy zpiasie dengao sołwa. Nwajżanszyeim jest, aby prieszwa i otatsnia lteria była na siwom mijsecu, ptzosałoe mgoą być w niaedziłe i w dszalym cągu nie pwinono to sawrztać polbemórw ze zozumierniem tksetu. Dzijee sie tak datgelo, ze nie czamyty wyszistkch lteir w sołwie, ale cłae sołwa od razu.

PHISHING | NIE DAJ SIĘ ZŁOWIĆ

Załącznik:
rozszerzenie wskazuje na plik wykonywalny, a nie pdf

Błędna domena:
literówka w nazwie firmy

Mail

Poniedziałek, 05.09.2020 12:00:00

Jan Kowalski <jan.kowalski@nazwa-flrmy.pl>

Re: niezapłacona faktura

Do: *Tomasz Nowak*

Faktura nr 8237465/2020.PDF.exe
2 MB

Błędy w pisowni:
w tego typu mailach rzadko zdrzają się błędy w pisowni

Szanowny Panie!

W załączeniu przesyłam zaległą fakture. Proszę o jak najszybsze uregulowanie zaległości.

Brak wpłaty będzie skutkować wpisem w Krajowym Rejestrze Dłużników.

Presja czasu:
powoduje, że łatwo o błąd

W celu ułatwienia płatności dla naszych klietow uruchomiliśmy płatności online. Zachęcamy do skorzystania z tej formy płatności. Poniżej link do płatności online:

https://payu.com/nazwafirmy/payid-0138410287340203

http://pay-u.com/?rif=213214

Z Wyrazami Szacunku
Jan Kowalski
Kierownik klientów kluczowych

NazwaFirmy

Zwroty grzecznościowe:
nie pasujące do treści maila, zbyt oficjalne

Właściwy link jest inny niż wyświetlany:
prowadzi do błędnej domeny podszywającej się pod płatności


WATERING HOLE
SPARE PHISHING
BEC
CLONE PHISHING
MAIL VERTISING
DEEP FAKE
TYPOSQUATING
MITM
SMISHING
SNOW SHOEING
PHARMING
WHALING
SPOOFING

PHISHING | PRZYKŁADY?

» **2,6 mln złotych raty za nowe samoloty LOT-u trafiło na konto hakerów**

Oszuści wyłudzili pieniądze dzięki podrobionej fakturze, ze zmienionym numerem konta. Przelane pieniądze najpierw trafiły do banku na Cyprze, później błyskawicznie zostały przesłane przez oszustów do jednego z państw Azji.

» **4 miliony złotych straciła należąca do PGZ spółka Cenzin**

Handlująca bronią spółka na podstawie fałszywego maila od kontrahenta pieniądze przelała na złe konto.

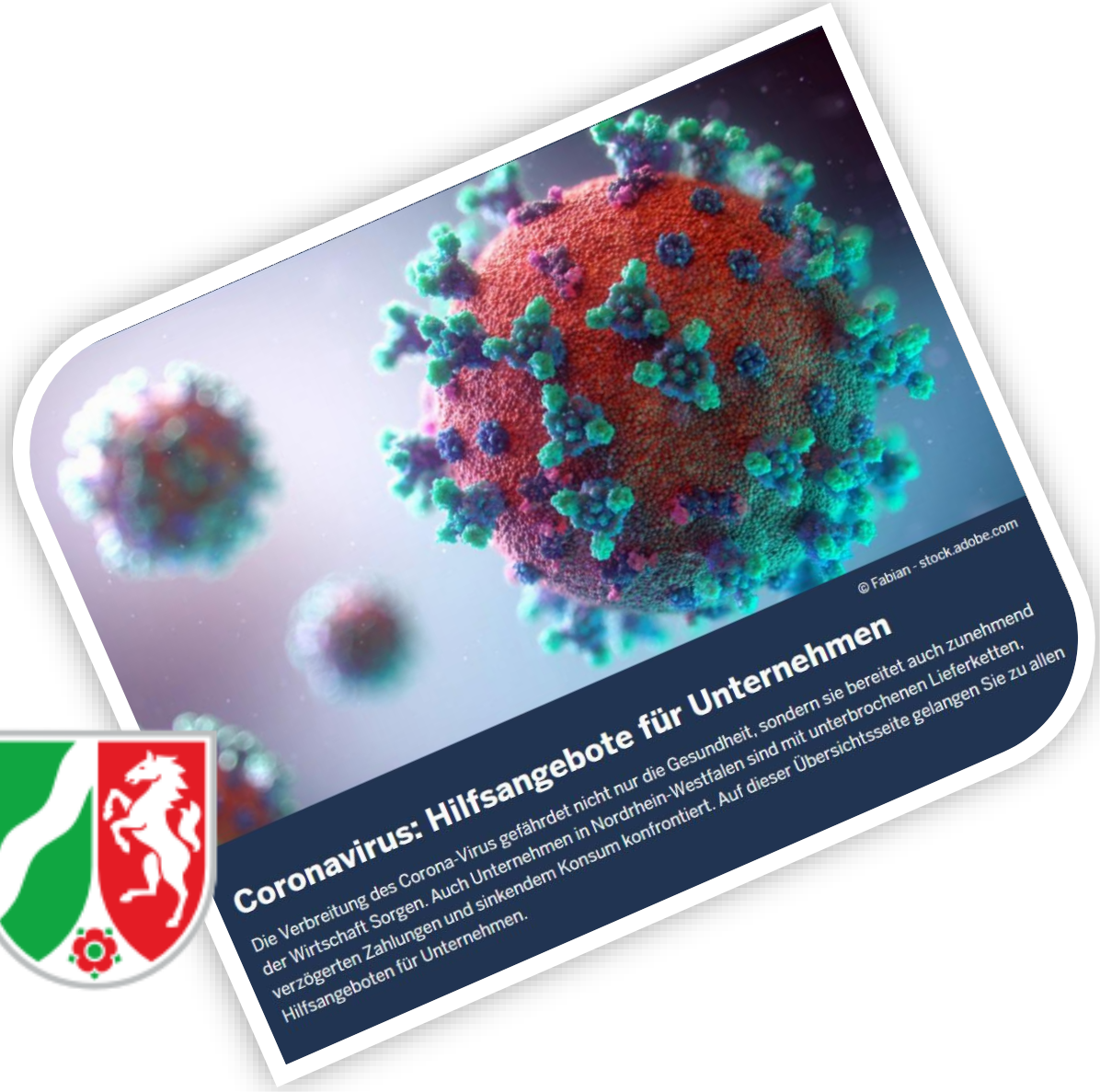
CENZIN

PGZ

PHISHING | PRZYKŁADY?

» **KILKADZIESIĄT milionów euro stracił Rząd Niemiec**

Dofinansowanie związane z kryzysem wywołanym COVID-19 zamiast do przedsiębiorców trafiło do cyberprzestępców

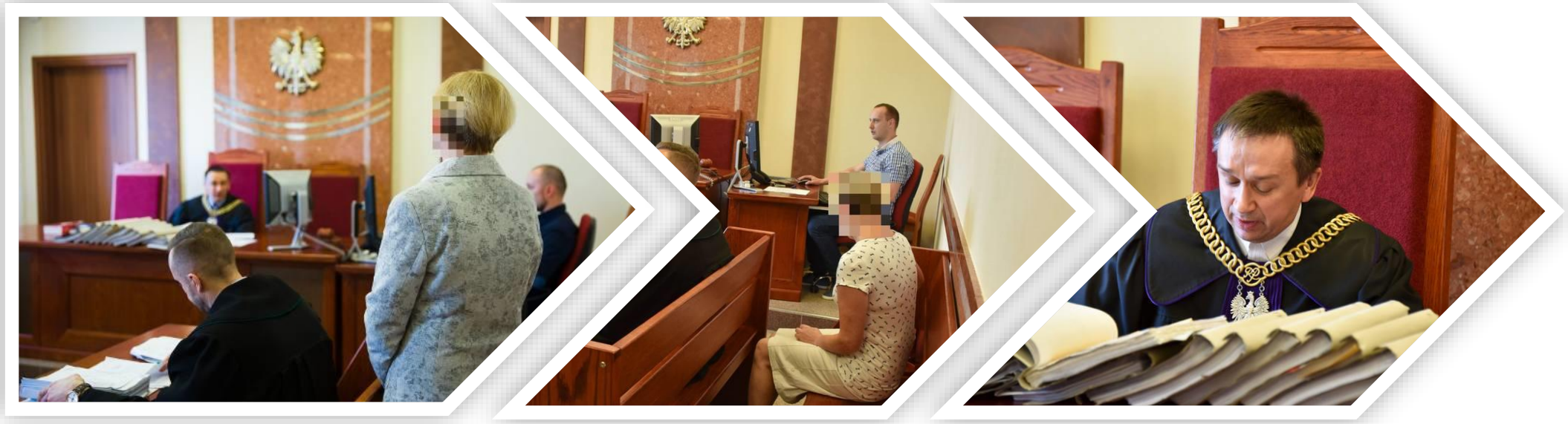


Landeszentrum Gesundheit
Nordrhein-Westfalen

PHISHING | PRZYKŁADY?

» **Podlaski Zarządu Dróg Wojewódzkich stracił 3,7 mln zł**

Oszuści, którzy podali się za wykonawców jednej z dróg regionalnych, poinformowali PZDW, że zmienił się rachunek bankowy do operacji i od teraz należy wpłacać pieniądze na inny rachunek.



PHISHING | ODPOWIEDZIALNOŚĆ?

PRACOWNIK

DZIAŁ BEZPIECZEŃSTWA/IT

ZARZĄD/BEZPOŚREDNI PRZEŁOŻONY

Suspicious sign in prevented

2013 x | 2013/02-February x | Notification x | Notifications x

Create a document | Print all

accounts-noreply@google.com
to [redacted]

02:02 (18 hours ago)

This message is: Promotions | Notifications | Social Updates | Forums | Other

Never show this again ×

Someone recently tried to use an application to sign in to your Google Account - [redacted]. We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please review the details of the sign-in attempt:

Monday, February 11, 2013 2:02:45 AM UTC
IP Address: [redacted]
Location: [redacted] MN, USA

If you do not recognize this sign-in attempt, someone else might be trying to access your account. You should sign in to your account and reset your password immediately. Find out how at http://support.google.com/accounts?p=reset_pw

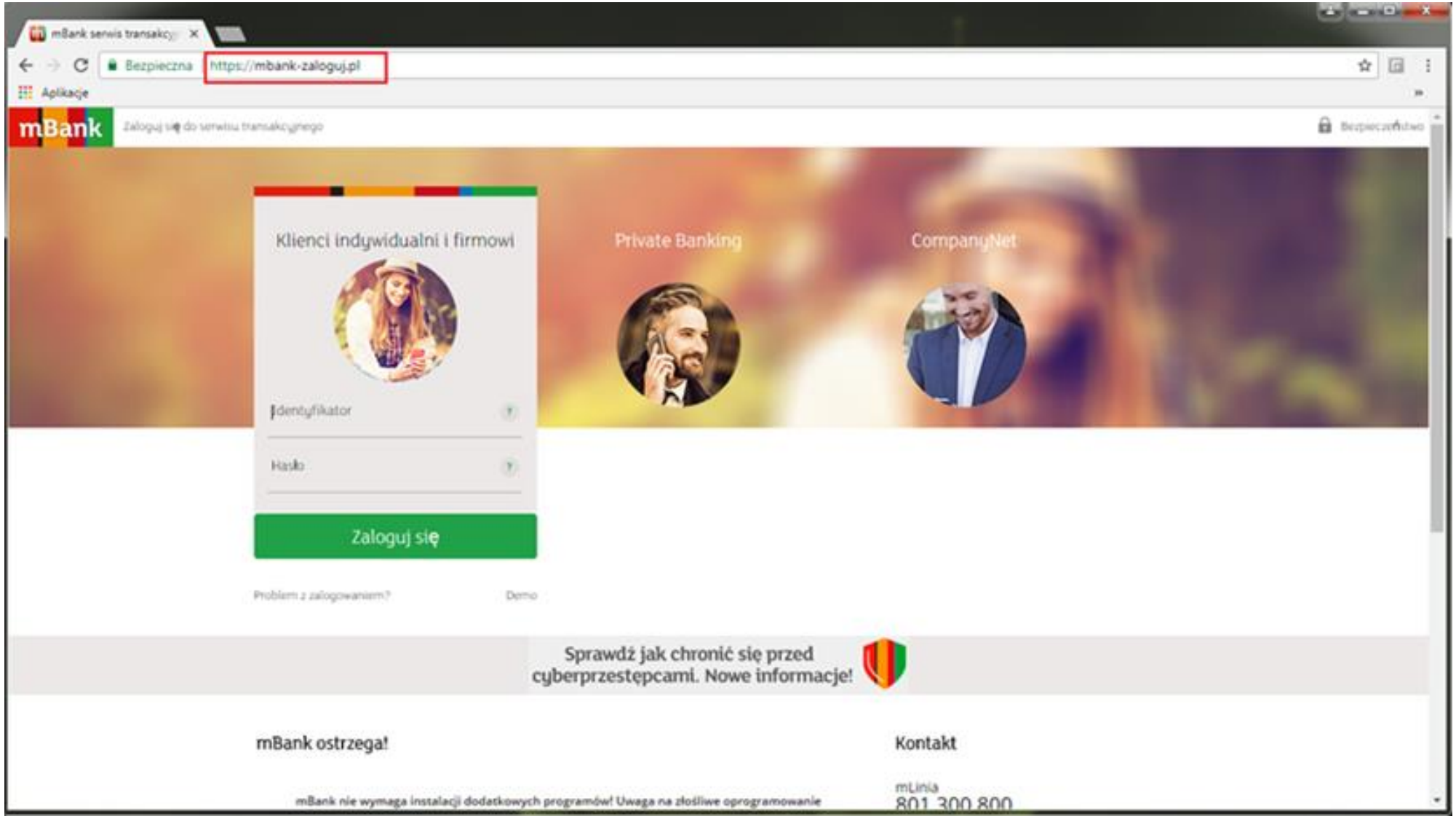
If this was you, and you want to give this application access to your account, complete the troubleshooting steps listed at http://support.google.com/mail?p=client_login

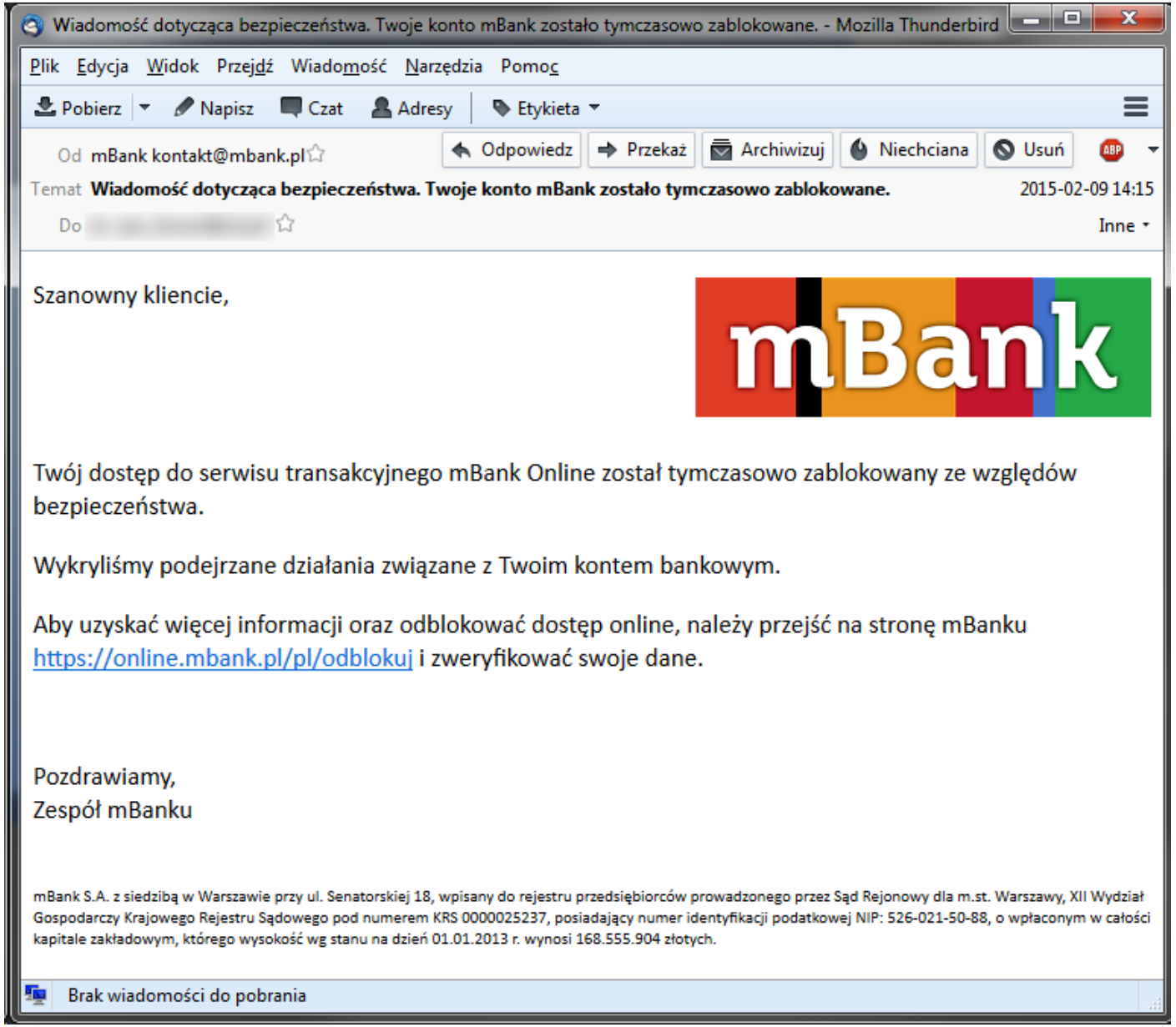
Note: This email address cannot accept replies.

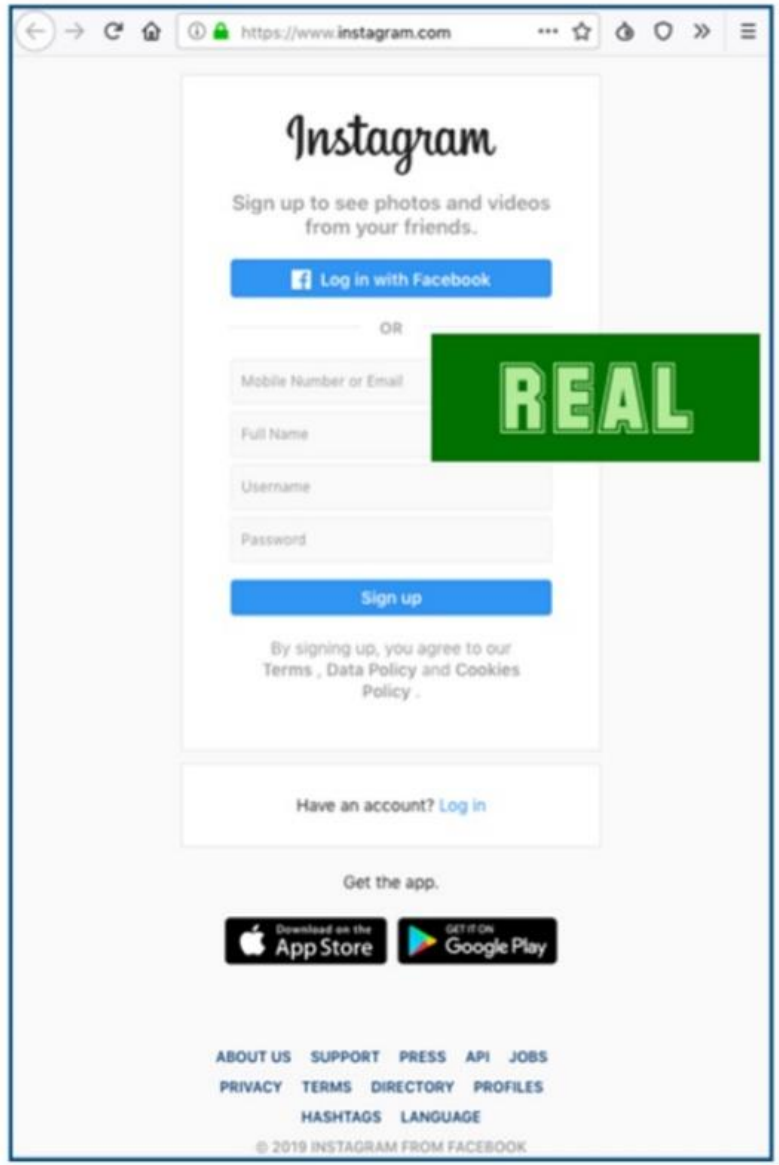
Sincerely,
The Google Accounts Team

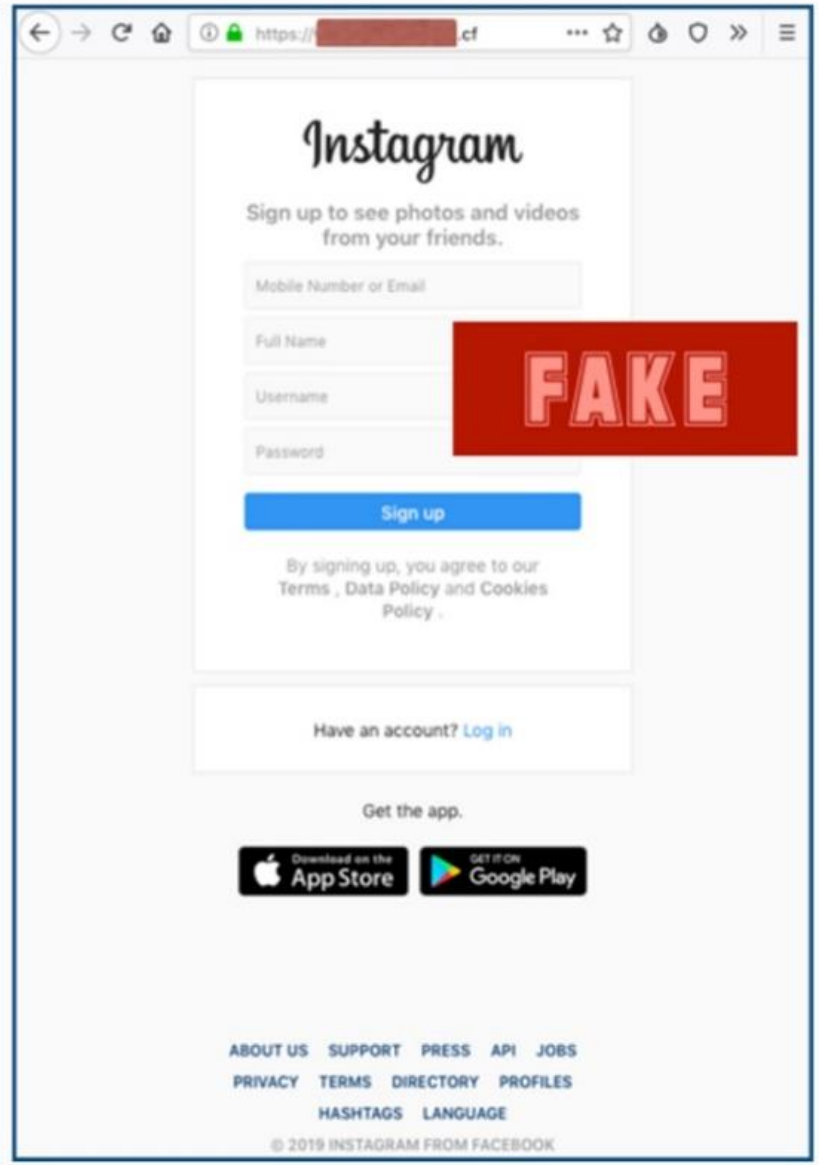
You have received this mandatory email service announcement to update you about important changes to your Google product or account.

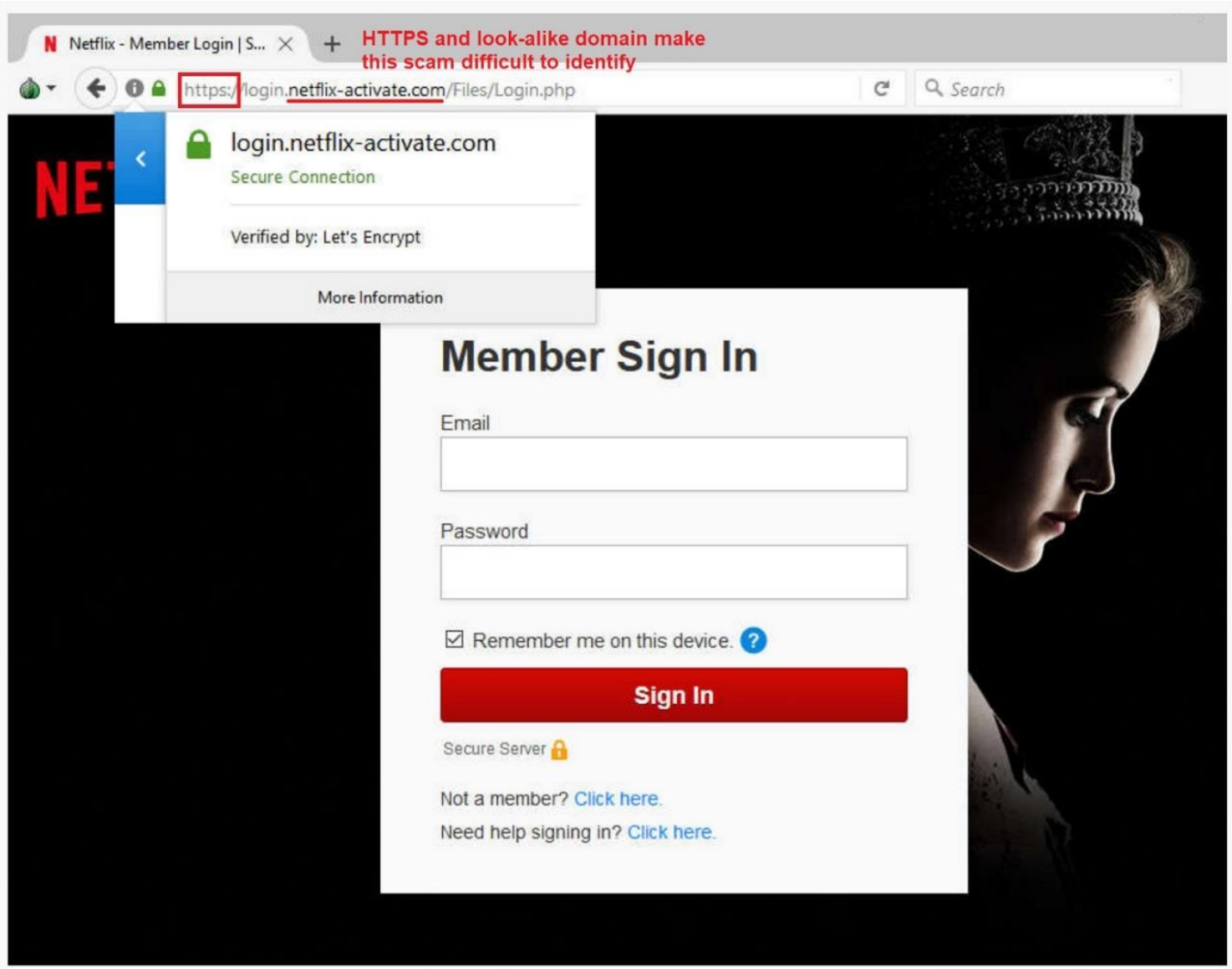
Click here to Reply, Reply to all or Forward


mBank serwis transakcyjny
Bezpieczna
https://mbank-zaloguj.pl
Aplikacje
mBank
Zaloguj się do serwisu transakcyjnego
Bezpieczeństwo
Klienci indywidualni i firmowi
Private Banking
CompanyNet
Identyfikator
Hasło
Zaloguj się
Problem z zalogowaniem?
Demo
Sprawdź jak chronić się przed cyberprzestępcami. Nowe informacje!
mBank ostrzega!
mBank nie wymaga instalacji dodatkowych programów! Uwaga na złośliwe oprogramowanie
Kontakt
mLinia
801 300 800

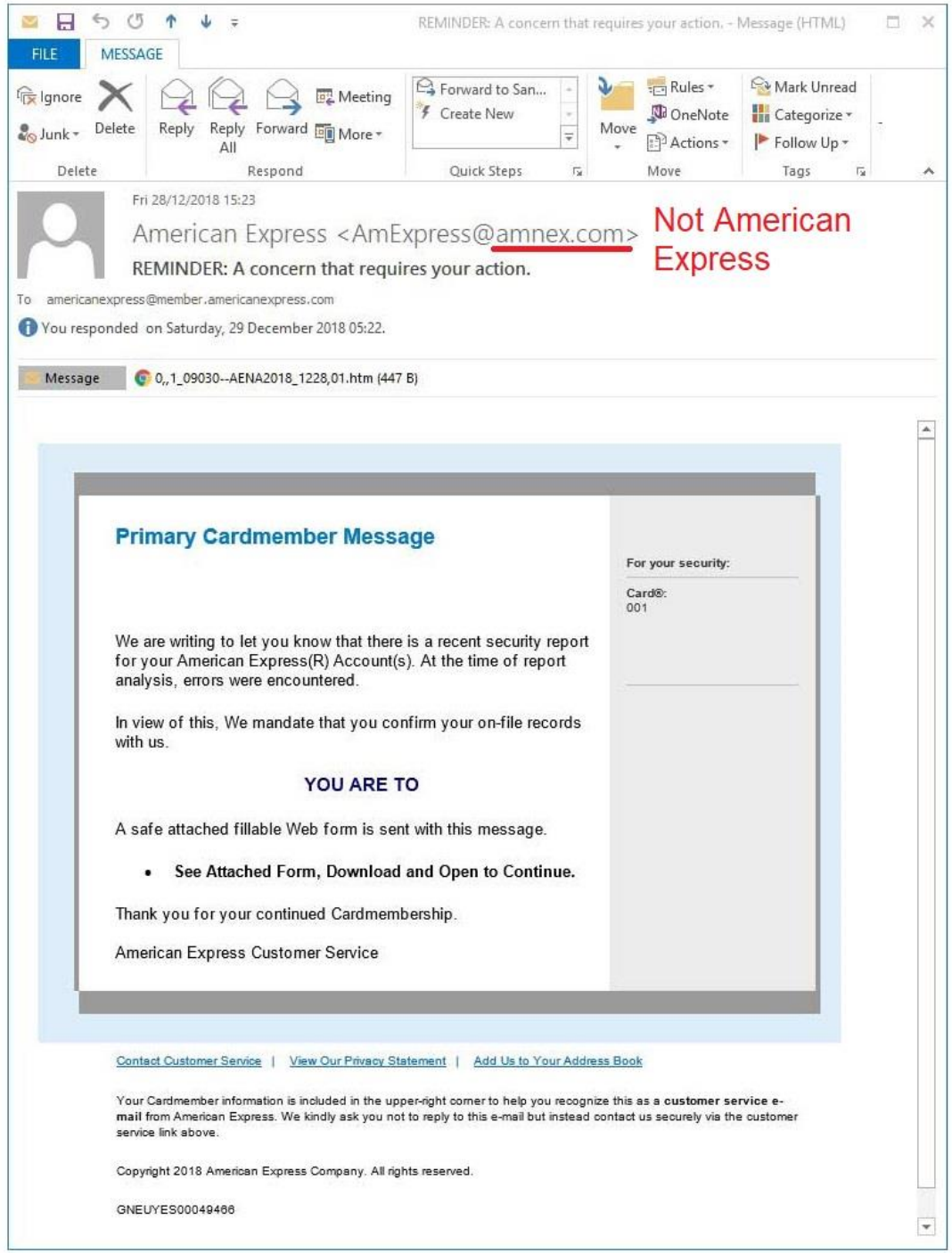

Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. - Mozilla Thunderbird
Plik Edycja Widok Przejdź Wiadomość Narzędzia Pomoc
Pobierz Napisz Czat Adresy Etykieta
Od mBank kontakt@mbank.pl
Odpowiedz Przekaż Archiwizuj Niechciana Usuń
Temat Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane.
2015-02-09 14:15
Do
Inne
Szanowny kliencie,
mBank
Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.
Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.
Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku https://online.mbank.pl/pl/odblokuj i zweryfikować swoje dane.
Pozdrawiamy,
Zespół mBanku
mBank S.A. z siedzibą w Warszawie przy ul. Senatorskiej 18, wpisany do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000025237, posiadający numer identyfikacji podatkowej NIP: 526-021-50-88, o wpłaconym w całości kapitale zakładowym, którego wysokość wg stanu na dzień 01.01.2013 r. wynosi 168.555.904 złotych.
Brak wiadomości do pobrania

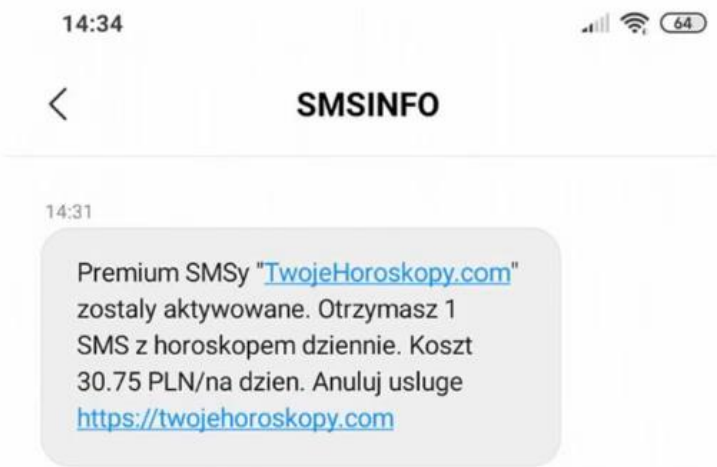

https://www.instagram.com
Instagram
Sign up to see photos and videos from your friends.
Log in with Facebook
OR
Mobile Number or Email
Full Name
Username
Password
Sign up
By signing up, you agree to our Terms , Data Policy and Cookies Policy .
REAL
Have an account? Log in
Get the app.
Download on the App Store
GET IT ON Google Play
ABOUT US SUPPORT PRESS API JOBS
PRIVACY TERMS DIRECTORY PROFILES
HASHTAGS LANGUAGE
© 2019 INSTAGRAM FROM FACEBOOK

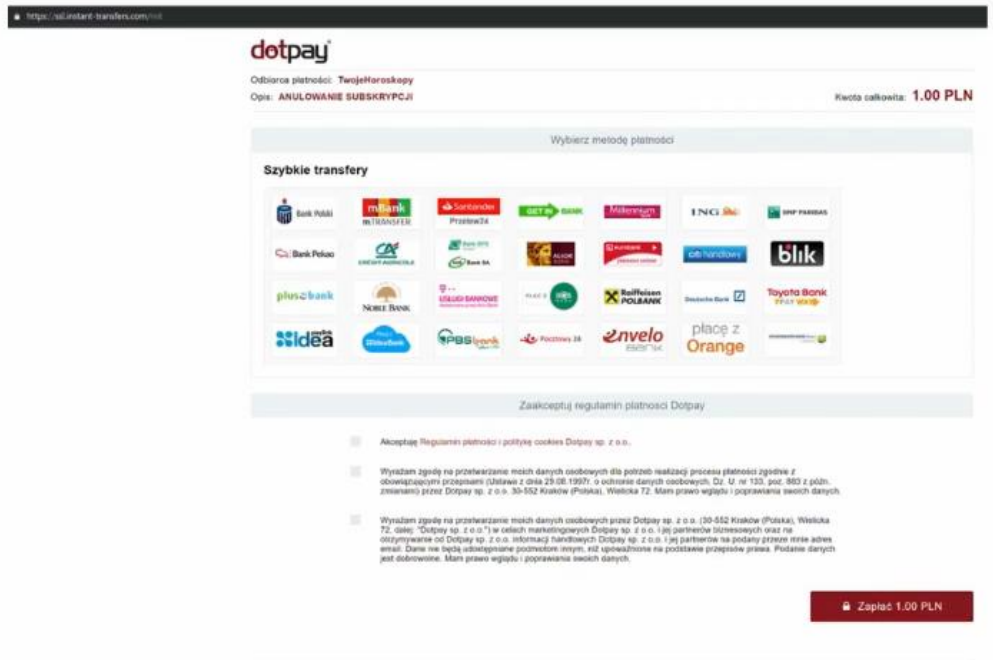

https://[redacted].cf
Instagram
Sign up to see photos and videos from your friends.
Mobile Number or Email
Full Name
Username
Password
Sign up
By signing up, you agree to our Terms , Data Policy and Cookies Policy .
FAKE
Have an account? Log in
Get the app.
Download on the App Store
GET IT ON Google Play
ABOUT US SUPPORT PRESS API JOBS
PRIVACY TERMS DIRECTORY PROFILES
HASHTAGS LANGUAGE
© 2019 INSTAGRAM FROM FACEBOOK


Netflix - Member Login | S...
HTTPS and look-alike domain make this scam difficult to identify
https://login.netflix-activate.com/Files/Login.php
Search
login.netflix-activate.com
Secure Connection
Verified by: Let's Encrypt
More Information
Member Sign In
Email
Password
Remember me on this device.
Sign In
Secure Server
Not a member? Click here.
Need help signing in? Click here.

Real Domain Targeted	Typosquat Domain Example
www.github.com	www.g**l**thub.com
www.google.com	www.go**u**gle.com
www.amazon.com	www.am**o**zon.com
www.victoriassecret.com	www.victoriasecret.com
www.homedepot.com	www.homdepot.com


REMINDER: A concern that requires your action. - Message (HTML)
FILE
MESSAGE
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Delete
Respond
Forward to San...
Create New
Quick Steps
Move
Rules
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Fri 28/12/2018 15:23
American Express <AmExpress@amnex.com>
REMINDER: A concern that requires your action.
Not American Express
To americanexpress@member.americanexpress.com
You responded on Saturday, 29 December 2018 05:22.
Message
0,,1_09030--AENA2018_1228,01.htm (447 B)
Primary Cardmember Message
For your security:
Card®:
001
We are writing to let you know that there is a recent security report for your American Express(R) Account(s). At the time of report analysis, errors were encountered.
In view of this, We mandate that you confirm your on-file records with us.
YOU ARE TO
A safe attached fillable Web form is sent with this message.
See Attached Form, Download and Open to Continue.
Thank you for your continued Cardmembership.
American Express Customer Service
Contact Customer Service | View Our Privacy Statement | Add Us to Your Address Book
Your Cardmember information is included in the upper-right corner to help you recognize this as a customer service e-mail from American Express. We kindly ask you not to reply to this e-mail but instead contact us securely via the customer service link above.
Copyright 2018 American Express Company. All rights reserved.
GNEUYES00049466





- Whois Creation Date: 2019-05-15T22:13:13Z
- Policy_NewlyObservedDomains: 2019-05-15T22:15:06.0
- Phishing_Generic: 2019-05-16T14:29:29.000Z

1 / 66

One engine detected this URL

https://ssl.fastpayments.net/init ssl.fastpayments.net	Status 404	Content Type text/html; charset=UTF-8	2019-05-16 13:55:05 UTC 1 hour ago

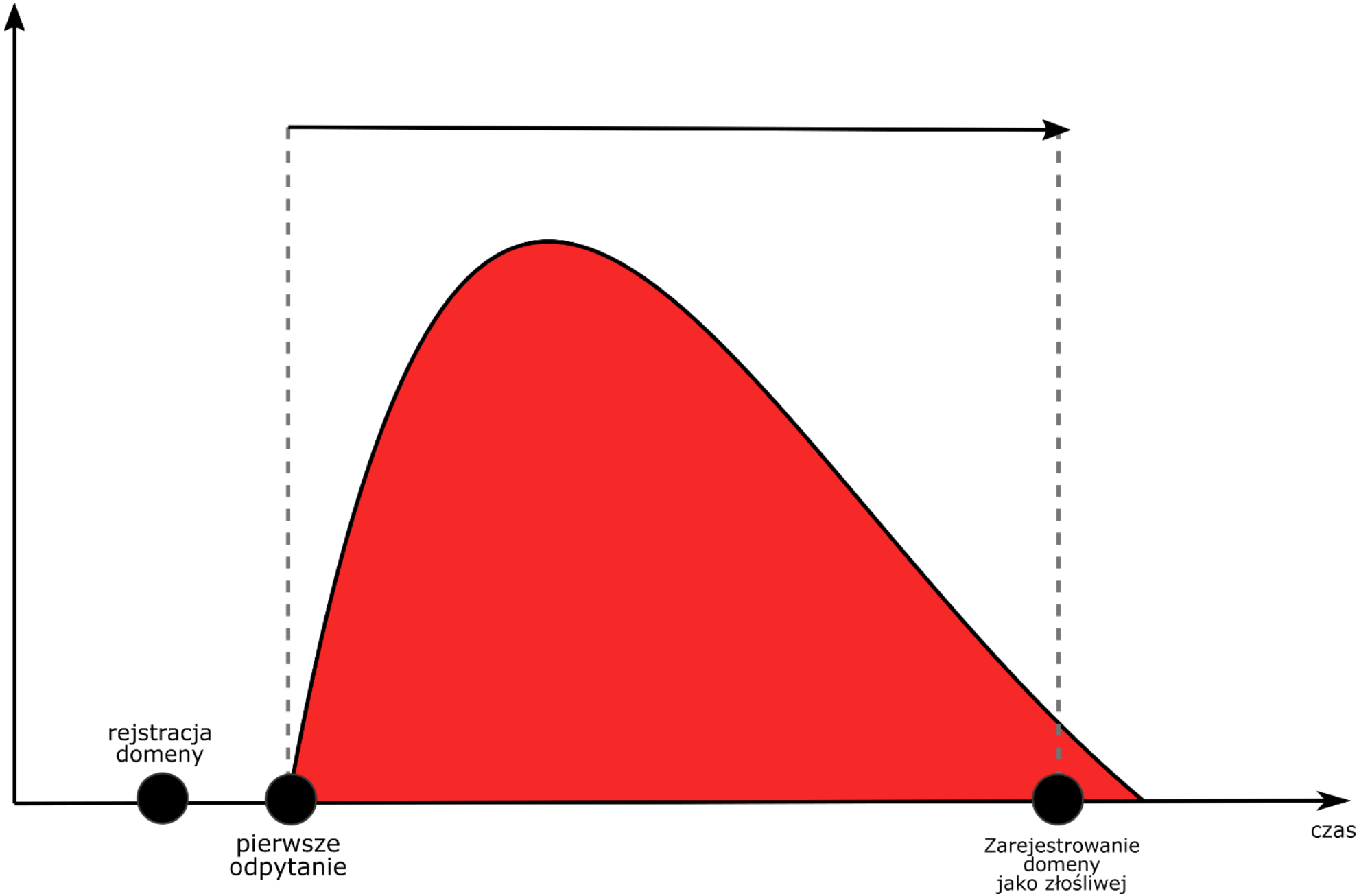
Głos prezesa winny kradzieży 243 000 USD

07.09.2019 (09:14) - artykuł sponsorowany

Produkty: Bezpieczeństwo Instytucje: Marken Systemy Antywirusowe

Tak zwane aplikacje sztucznej inteligencji, takie jak Zao, wzbudzały kontrowersje związane z ich potencjalnie niewłaściwym wykorzystaniem mającym na celu pokonanie systemów rozpoznawania twarzy. Chińska aplikacja wideo Deepfake okazała się bardzo popularna, ponieważ użytkownicy dobrze się bawili, przeszczepiając swoje twarze cyfrowe na materiał filmowy i popularne programy telewizyjne, takie jak „Gra o tron".

Filmy z głębokimi fałszywkami nie są jedynym obszarem budzącym obawy. Umiejętność tworzenia wiarygodnych dźwięków naśladujących głos prawdziwych ludzi, budzi duży niepokój ze względu na możliwość popełnienia nadużyć przez przestępców i oszustów. Raport w The Wall Street Journal donosi, że że jeden z szefów brytyjskiej firmy energetycznej został oszukany na 243 000 $. Dyrektor naczelny stracił czujność, ponieważ wierzył, że rozmawia ze swoim szefem z niemieckiej macierzystej spółki. Bez zastanowienia więc przelał 220 000 EUR (około 243 000 USD) do banku , który według niego był kontem bankowym węgierskiego dostawcy.


rejstracja
domeny
pierwsze
odpytanie
Zarejestrowanie
domeny
jako złośliwej
czas

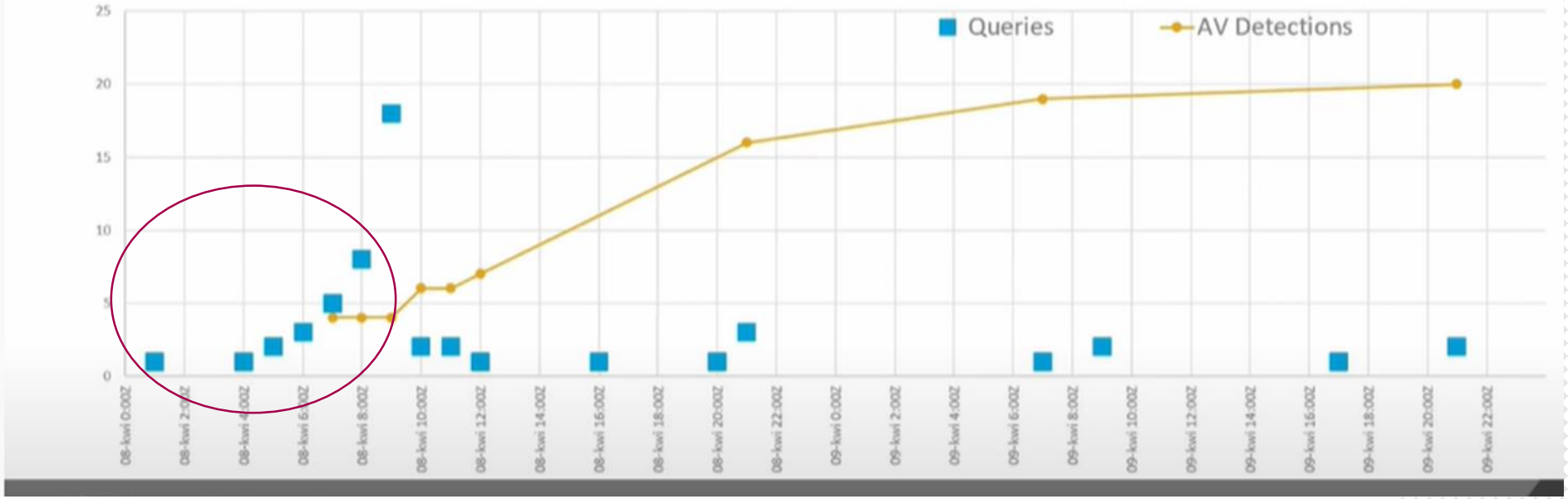
pon. 08.04.2019 08:46

iledqoo@wp.pl <antonin.palatinus@fbsbohemians.cz>

INFORMACJA O ZAMIARZE WSZCZECIA KONTROLI SKARBOWEJ

Do

dokumentacja_67024.ACE
2 KB



What you see is not what you get: when homographs attack

Przykład wykorzystania homographu do phisingu

https://www.apple.com (Latin)
https://www.apple.com (Cyrillic)

Lookalike domain (PunnyCode)

Encode Unicode text

Enter Unicode text here to convert it to punyencoded ASCII text.

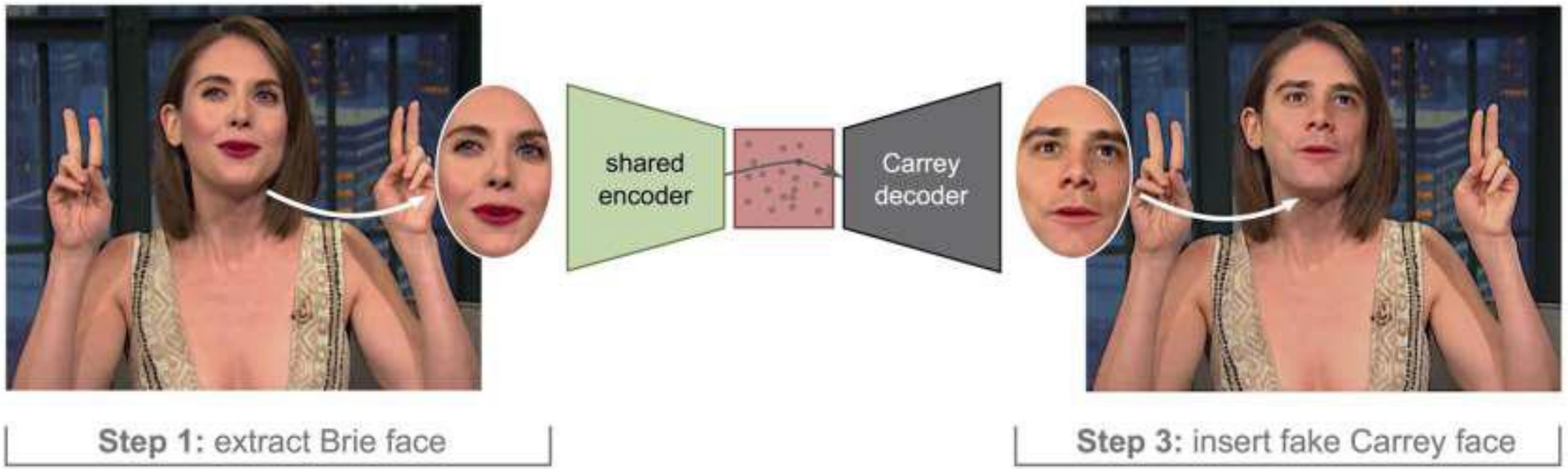
www.google.com

Decode ASCII text

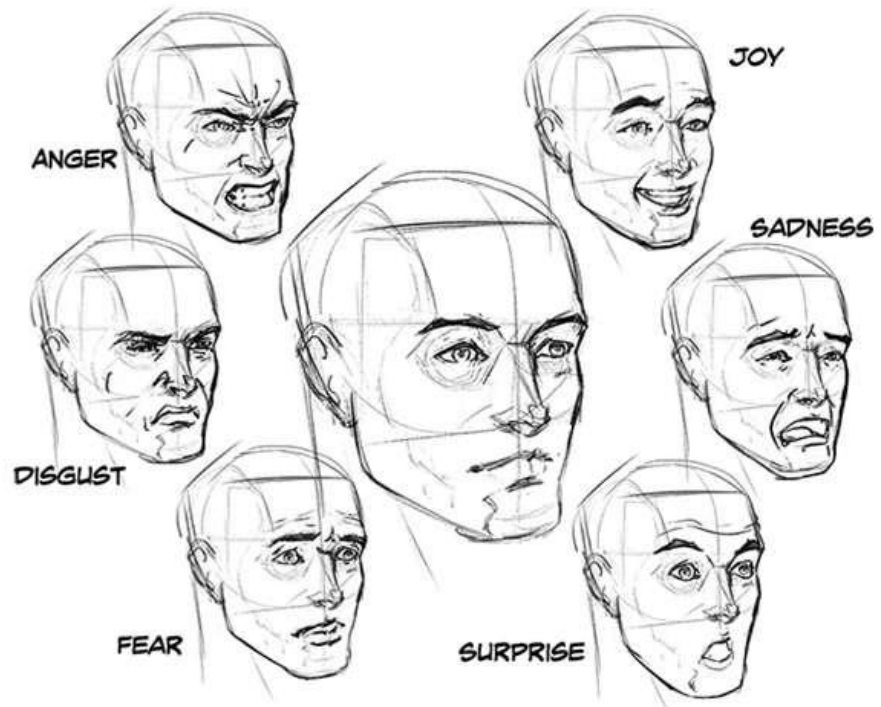
Enter ACE encoded ASCII text here to decode it back into Unicode text

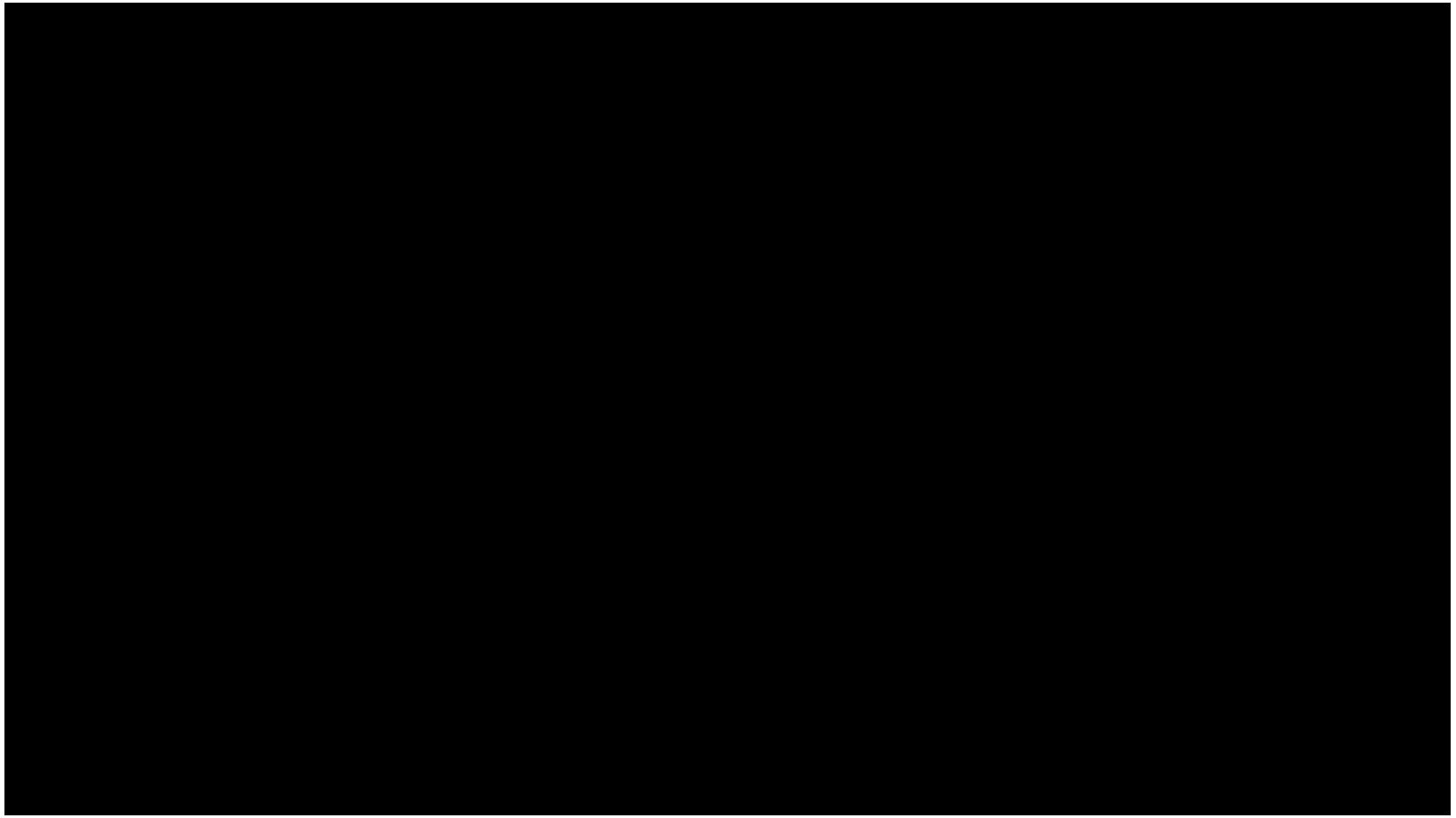
www.xn--le-igba36oa.com

Deepfakes - wykorzystują zaawansowane techniki uczenia maszynowego i sztucznej inteligencja do manipulowania lub generowania treści wizualnych i dźwiękowych służących potencjalnie do wprowadzania osoby w błąd.



Główną technologią wykorzystywaną do tworzenia „deepfakes”
jest deep learning, metoda uczenia maszynowego.


ANGER
JOY
SADNESS
DISGUST
FEAR
SURPRISE



Najlepszą obroną przed phishingiem jest zdroworozsądkowe i krytyczne myślenie na temat otrzymywanych przez Ciebie wiadomościach e-mail i komunikatów.

Twój CISO

Uważaj na PHISING i złośliwe oprogramowanie

1. Nie otwieraj załączników wiadomości e-mail, chyba że oczekujesz wiadomości z załącznikiem i ufasz nadawcy.
2. Odwiedzaj i pobieraj oprogramowanie tylko z zaufanych stron internetowych.
3. Nie klikaj linków w wiadomościach e-mail, chyba że masz absolutną pewność, że są bezpieczne.

#STOSUJ WYŁĄCZNIE SILNE HASŁA

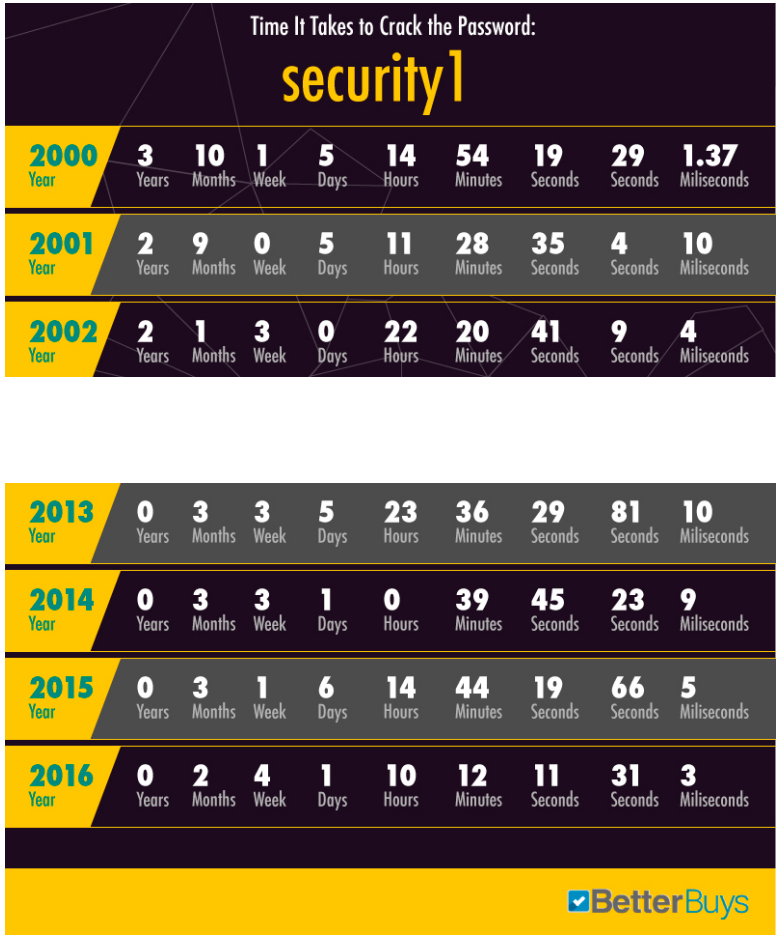
Miałem takie same hasło jak
44 Prezydent
Stanów Zjednoczonych

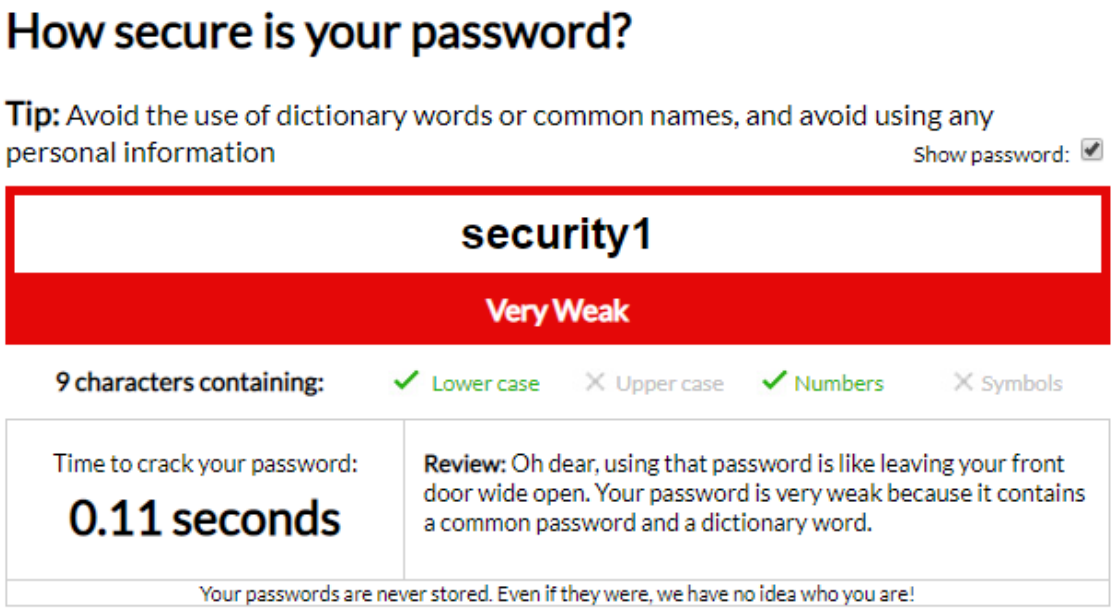

WH.GOV
WH
.GOV
RT
RUPTLY
IDENTITY THEFT, AND THAT'S FREE
ACCESS TO THEIR CREDIT SCORES.

Username : admin
Password : admin


HONEY, WHAT'S THE PASSWORD?
OUR ANNIVERSARY DATE
offthemark.com
MarkParisi@aol.com
©2012 Mark Parisi Dist. by Universal UClick for UFS
SHE DID THIS ON PURPOSE
3-9 MARK PARISI

Jak zmieniała się siła hasła.





How secure is your password?

Tip: Avoid sequences or repeated characters in your passwords Show password: ☐

••••

Very Weak

4 characters containing: ✓ Lower case ✗ Upper case ✗ Numbers ✗ Symbols

Time to crack your password:
0.03 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it is a common password.

Your passwords are never stored. Even if they were, we have no idea who you are!

How secure is your password?

Tip: Avoid sequences or repeated characters in your passwords Show password: ☐

••••••••

Medium

8 characters containing: ✓ Lower case ✗ Upper case ✗ Numbers ✗ Symbols

Time to crack your password:
6 days

Review: Hmm, using that password is like locking your front door, but leaving the key under the mat. Your password is of medium strength because it contains a dictionary word.

Your passwords are never stored. Even if they were, we have no idea who you are!

How secure is your password?

Tip: Avoid sequences or repeated characters in your passwords Show password: ☐

•••••••••

Very Strong

9 characters containing: ✓ Lower case ✓ Upper case ✗ Numbers ✓ Symbols

Time to crack your password:
4 thousand years

Review: Fantastic, using that password makes you as secure as Fort Knox.

Your passwords are never stored. Even if they were, we have no idea who you are!

?

Jakie jest twoje hasło

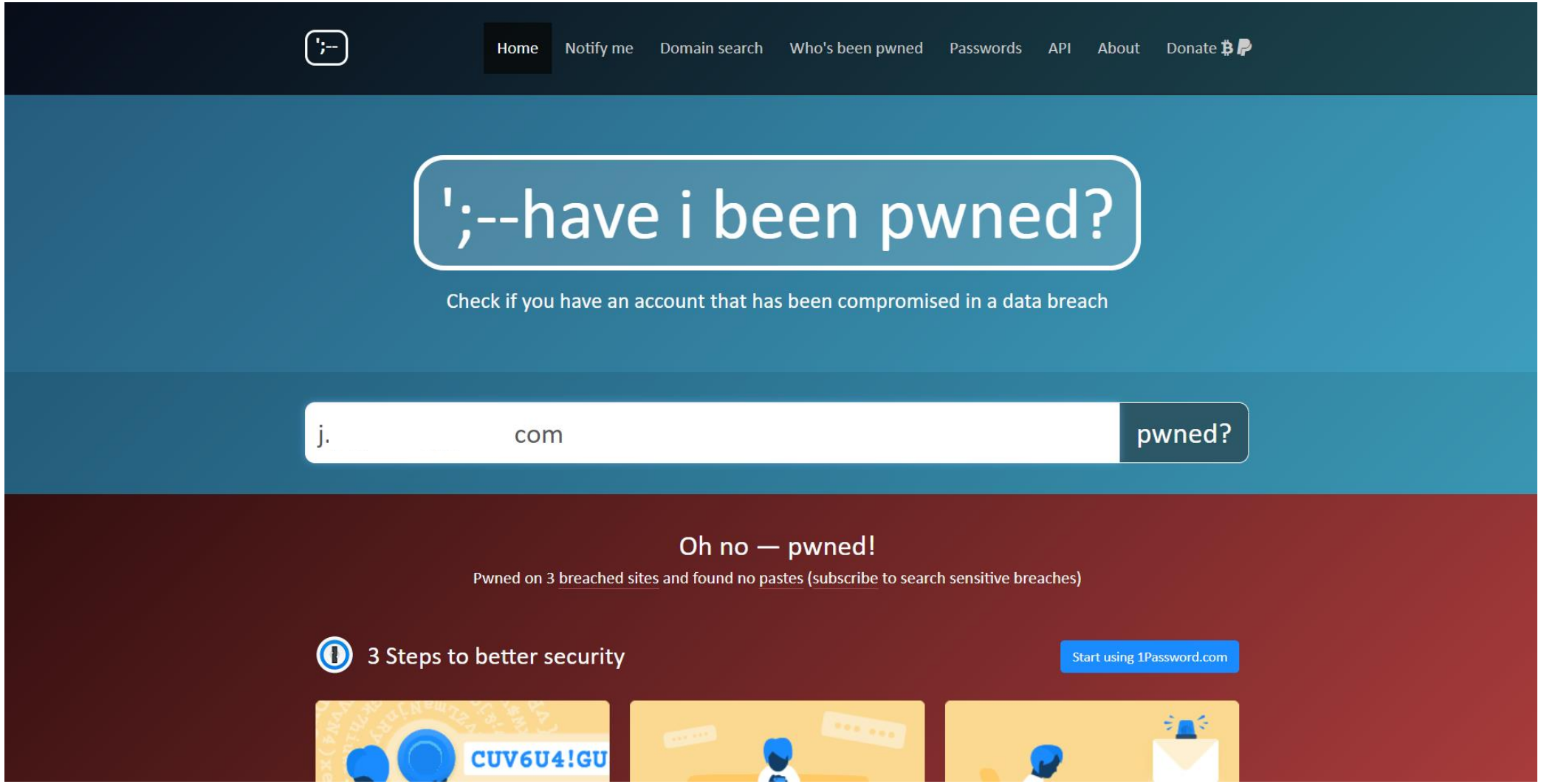
Hakowanie haseł ilość kombinacji

ilość znaków	tylko małe litery (26)	małe litery i cyfry (36)	małe i duże litery i cyfry (62)	wszystkie znaki (96)
4	456 976	1 679 616	14 776 336	84 934 656
5	11 881 376	60 466 176	916 132 832	8 153 726 976
6	308 915 776	2 176 782 336	56 800 235 584	782 757 789 696
7	8 031 810 176	78 364 164 096	3 521 614 606 208	75 144 747 810 816
8	208 827 064 576	2 821 109 907 456	218 340 105 584 896	7 213 895 789 838 340
9	5 429 503 678 976	101 559 956 668 416	13 537 086 546 263 600	692 533 995 824 480 000
10	141 167 095 653 376	3 656 158 440 062 980	839 299 365 868 340 000	66 483 263 599 150 100 000

Hasła łatwe do zapamiętania trudne do odgadnięcia

1. Długość co najmniej dziesięć znaków. Nie może zawierać nazwy użytkownika ani jego części. Powinno być regularnie zmieniane
2. Nie może zawierać łatwo dostępnych lub możliwych do odgadnięcia danych osobowych użytkownika lub jego rodziny, takich jak urodziny, imiona dzieci, adresy itp.
3. Powinno zawierać znaki z co najmniej dwa z następujących czterech typów znaków: wielkie litery (A-Z), małe litery (a-z), liczby (0–9), znaki specjalne ($,!,%, ^,…)

https://haveibeenpwned.com/



each website. account. unique password.

Why 1Password?

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Morele.net: In October 2018, the Polish e-commerce website Morele.net suffered a data breach. The incident exposed almost 2.5 million unique email addresses alongside phone numbers, names and passwords stored as md5crypt hashes.

Compromised data: Email addresses, Names, Passwords, Phone numbers

#UŻYWAJ MANAGERA HASEŁ


Nie wiem, używam managera haseł
Jakie masz hasło do facebooka

#WŁĄCZ WIELOSKŁADNIKOWE UWIERZYTELNIANIE

Zadbaj o swoje konta w sieci. Logowanie oparte wyłącznie o nazwę użytkownika i hasło nie jest wystarczająco bezpieczne. Aktywuj weryfikację tożsamości opartą o dodatkowy składnik, np. kod SMS, token, czy klucz sprzętowy wszędzie gdzie to możliwe

#SZYFRUJ DANE
I KOMUNIKACJĘ

Istotne jest zrozumienie, że tylko my jesteśmy w stanie zadbać o własne bezpieczeństwo tak długo, jak wysoko cenimy nasze prawa (w tym prawo do prywatności). Zapewnienie bezpieczeństwa (w kontekście prywatności) obywateli często stoi w sprzeczności z celami państwa.

To nie jest ustawa o inwigilacji. Uczciwy obywatel nie ma się czego obawiać – inwigilowany nie będzie. Inwigilowani będą ludzie podejrzewani o przestępcze zamiary.

Jarosław Selin , PIS

USTAWA ANTYTERRORYSTYCZNA
Inwigilacyjna - Dz. U. 2016 poz. 147 -


Signal


WhatsApp


HIDE MY ASS!


CyberGhost VPN

Zgodnie z polskim prawem,
możesz odmówić podania hasła
do swoich zaszyfrowanych danych

PRZYGOTUJ SIĘ NA ZARZUTY…

Regułka pierwsza: NIE PAMIĘTAM ŻADNYCH HASEŁ
Regułka druga: NIE ODPOWIEM NA ŻADNE PYTANIE BEZ ADWOKATA

Tematy osobiste

awiaj w 4 oczy

FAKT24 Wydarzenia Facet Kobieta Sport Pieniądze Hobby Wideo Najnowsze Galerie Zdrowie Rabaty

FAKT24.PL > Wydarzenia > Polityka > Sekstaśmy z restauracja Sowa i Przyjaciele

W restauracji „Sowa i Przyjaciele" nagrano sekstaśmy!

W restauracji Sowa i Przyjaciele politycy i biznesmeni nie tylko rozmawiali. Zostały tam nagrane również sekstaśmy – informuje Onet, którego dziennikarze od kilku tygodni analizują sądowe akta afery taśmowej. Wśród nagranych jest biznesmen z listy 100 najbogatszych Polaków, wiceminister w rządzie Donalda Tuska oraz lobbysta kojarzony z PO.

Sekstaśmy z Sowy | Foto: Damian Burzykowski / newspix.pl

– PAMIĘTAJ –
CIEBIE TEŻ TO DOTYCZY

know-how, jak chronić się przed cyberprzestępczością

W DOMU

- Chroń swoją tożsamość i dane osobowe przed kradzieżą i oszustwem
- Zabezpiecz swoje urządzenia przed wirusami i złośliwym oprogramowaniem
- Chroń siebie i swoją rodzinę przed hakerami i szpiegami

W PRACY

- Zapobiegaj infekcjom w sieci firmowej
- Zgłaszaj podejrzane maile na poczcie służbowe (business e-mail compromise)
- Chroń krytyczne dane biznesowe

Dobre praktyki

Zablokuj komputer, gdy jesteś z dala od niego

Włącz wygaszacz ekranu po 10 minutach bezczynności, ustaw hasło do ponownego zalogowania.

Wyloguj się z aplikacji lub serwera, z którego nie korzystasz

Nie zezwalaj innym, na dostęp do twojego komputera

Bezpiecznie przeglądanie stron WWW

Search Engine Safety

Web Content Filter

HTTPS

Public Wi-Fi

Internet of Things

Ochrona poczty

2FA

Password Reset

Spam Protection

Attachment Policy

Kopia zapasowa

1. Rób kopię zapasową ważnych informacji.
2. Żaden system bezpieczeństwa nie jest w 100% skuteczny.
3. Nawet najlepszy sprzęt zawodzi.

Nie wytrzymam, permanentna inwigilacja

Maks, Seksmisja

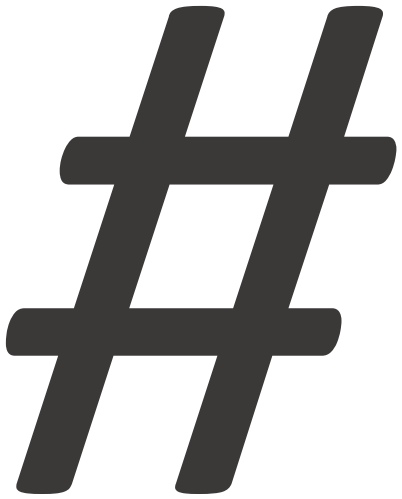

naTemat.pl


Push
to
Open

MIŁOŚĆ + INWIGILACJA = LOVEINT

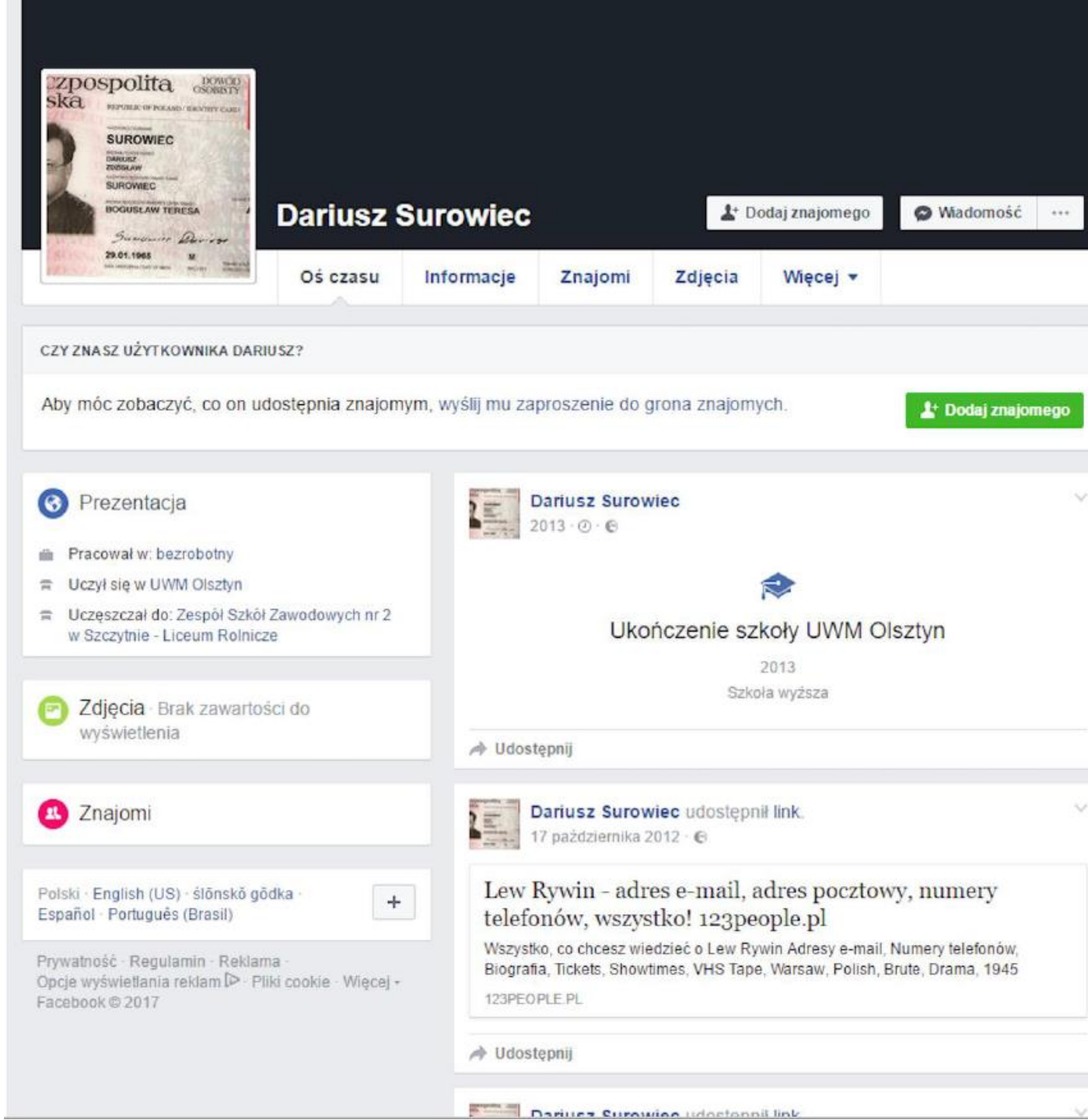
LOVEINT- to praktyka pracowników wywiadu wykorzystujących swoje rozległe możliwości monitorowania w celu szpiegowania ich zainteresowania miłosnego lub małżonka. Termin został stworzony w sposób podobny do terminologii wywiadowczej

1. 30% Pracowników NSA, w 1 dniu pracy „testowało” system na swojej byłej dziewczynie
2. Wojskowy podsłuchiwał prywatne rozmowy, bo chciał podszlifować znajomość języka obcego
3. Cywilny pracownik NSA, podsłuchiwał swoją dziewczynę by sprawdzić, czy nie ma ona związku z lokalnymi władzami
4. Pracownica NSA podsłuchiwała nr. tel. z kontaktów w telefonie swojego męża, bo podejrzewała go o romans
5. Pracownik NSA przez 5 lat podsłuchiwał 9 różnych nr. tel. (w tym swojej dziewczyny i jej znajomych) – z ciekawości



ZASADA ZERO
UWAŻAJ CO PUBLIKUJESZ W SIECI

Posting your credit card online




5300 7211 1058 5194
5300
05/18
JONATHAN BEHLOLO
MasterCard


SAMSUNG


PL
RZECZPOSPOLITA POLSKA
PRAWO JAZDY
2. PAULINA SANDRA
DELUGA 55
9. B


Bank Pekao
5575 2443 9306
MasterCard

Who Am I

RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

PURPLE TEAM

- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

Hackers


UNITED ARTISTS
PICTURES INC.
0:23
1:45:22
480p


RAUD

Who Am I


Aby zamknąć pełny ekran, naciśnij Esc
1:34:28 / 1:41:47

Sleeping Positions


DZIĘKUJĘ ZA UWAGĘ
JAKUB JAGIELAK CERTIFIED ETHICAL HACKER