Cyberbezpieczeństwo

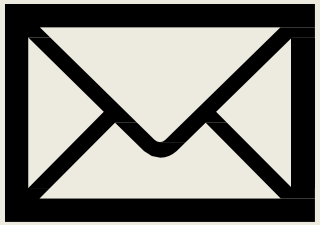
FRSI

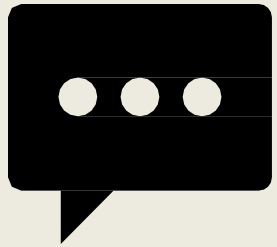
Zależy nam na **ludziach**
Doceniamy **technologie**

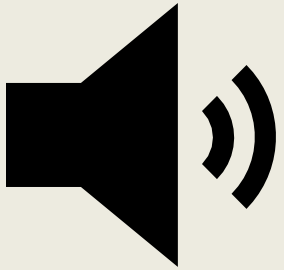
Czym jest socjotechnika?

Socjotechnika (social engineering) to czynność wywierania wpływu na ludzi poprzez praktyczne zastosowanie podstępu wykorzystującego uniwersalne mechanizmy reakcji psychologicznych. Celem takiego działania jest nieautoryzowane pozyskanie poufnych lub

niedostępnych w inny sposób informacji.







Rodzaje:

- Phishing
- SMShing
- Vishing/Spoofing

FRSI

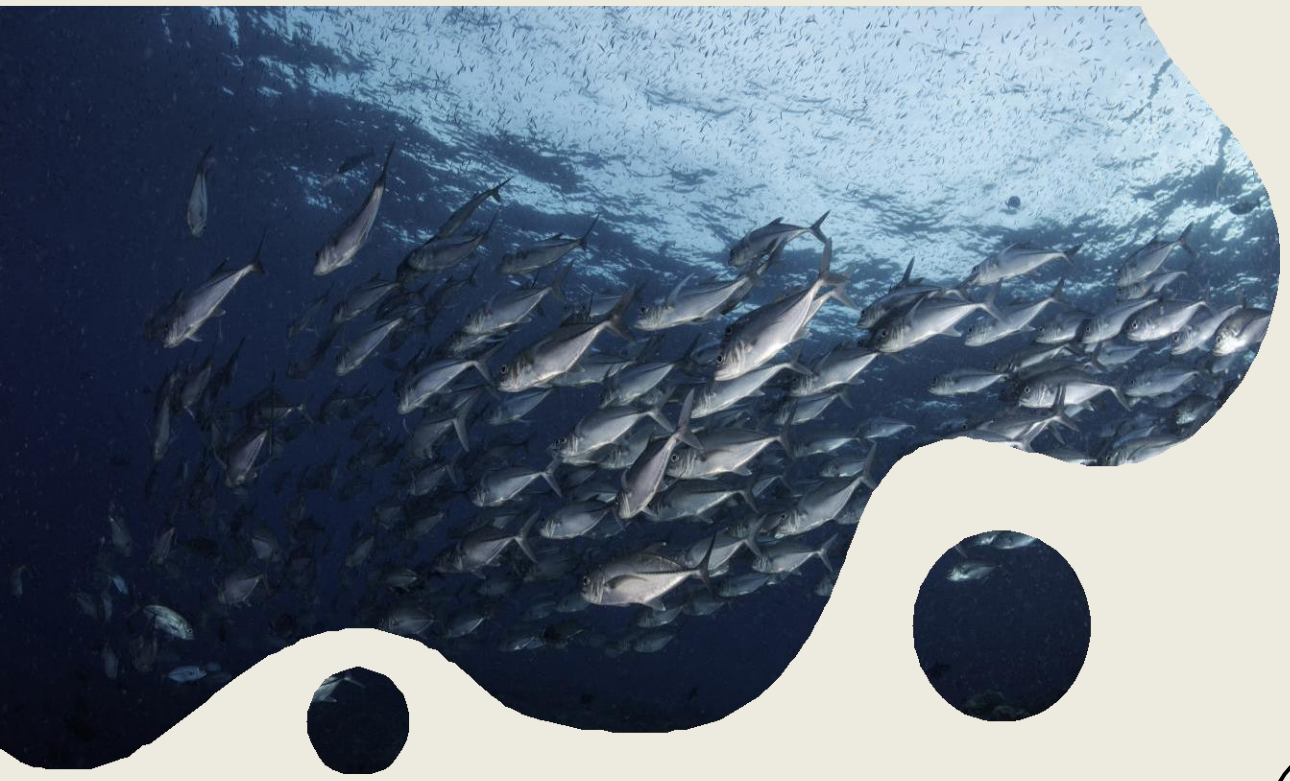
Phishing

Metoda oszustwa, w której przestępca podszywa się pod zaufaną osobę lub instytucję w celu:

- wyłudzenia poufnych informacji (np. dane do logowania);
- osiągnięcia korzyści majątkowej;
- nakłonienia do instalacji złośliwego oprogramowania.

Jest to rodzaj ataku wykorzystujący metody inżynierii społecznej.
Oparty jest na podstępie i manipulacji w połączeniu z prostymi rozwiązaniami technicznymi.

FRSI



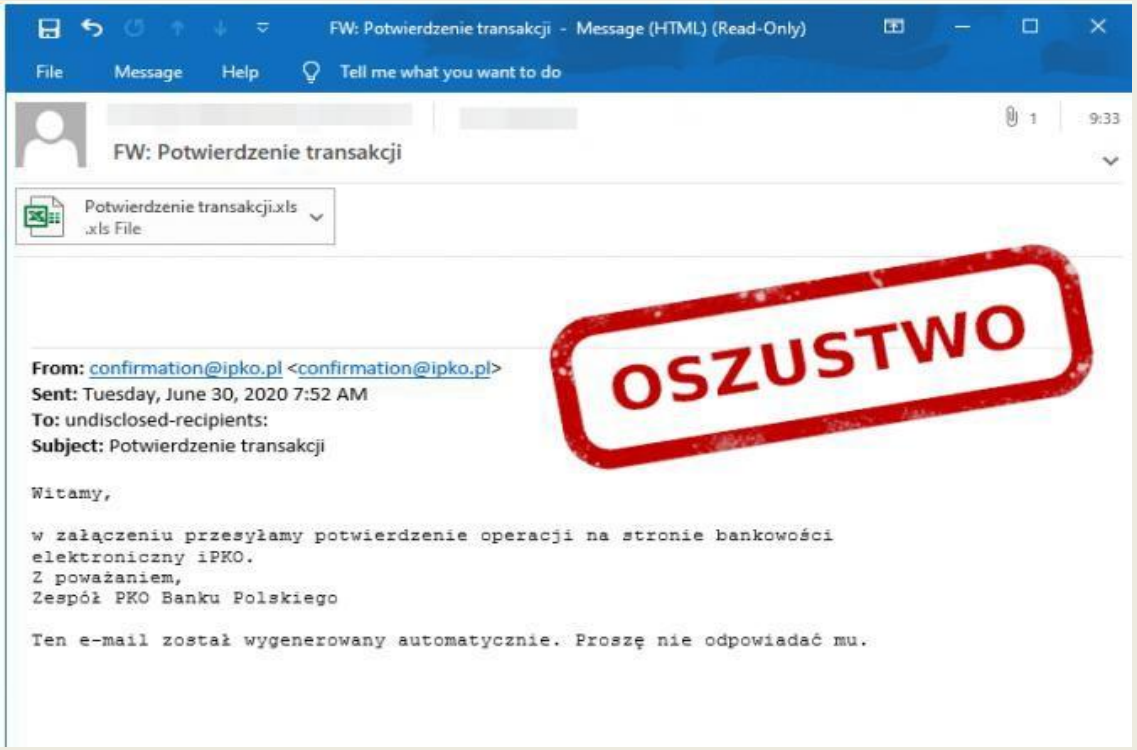
Atak masowy vs atak celowany

FRSI

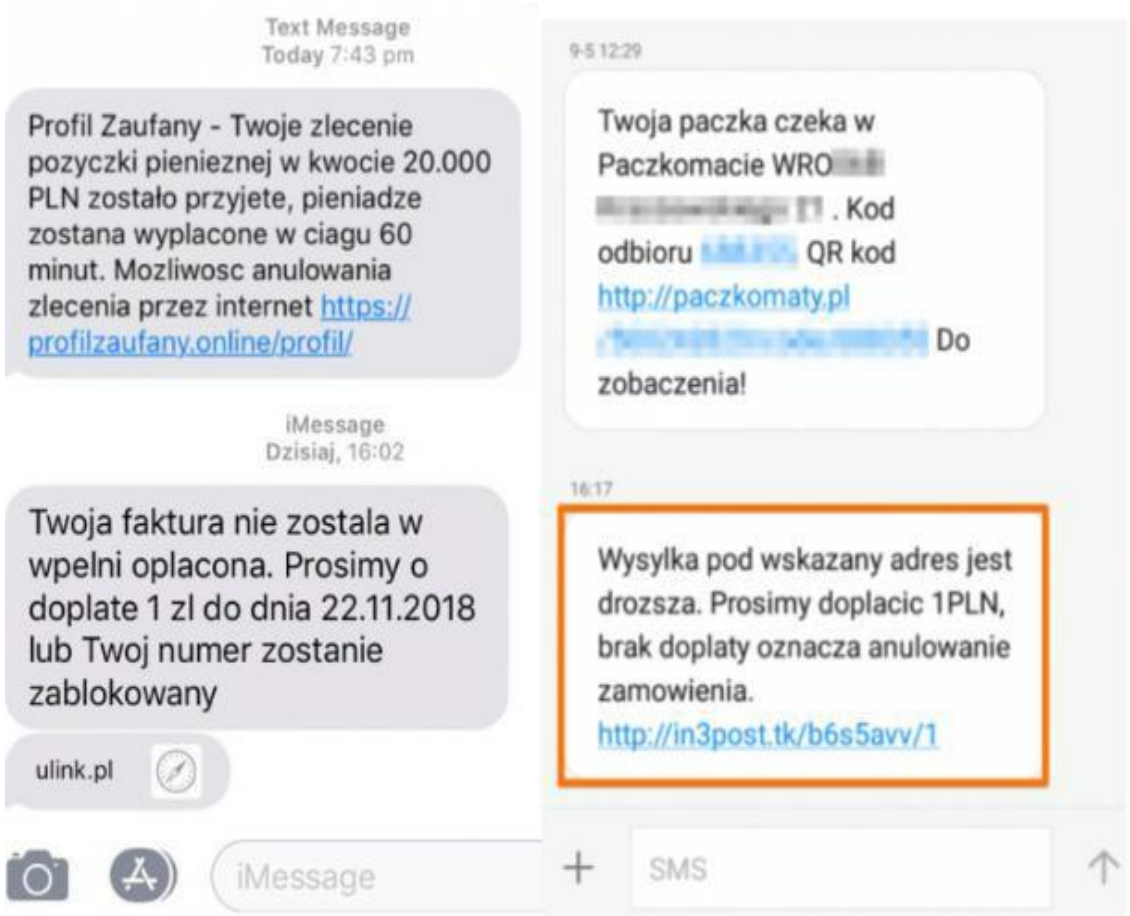
Manipulacja w phishingu

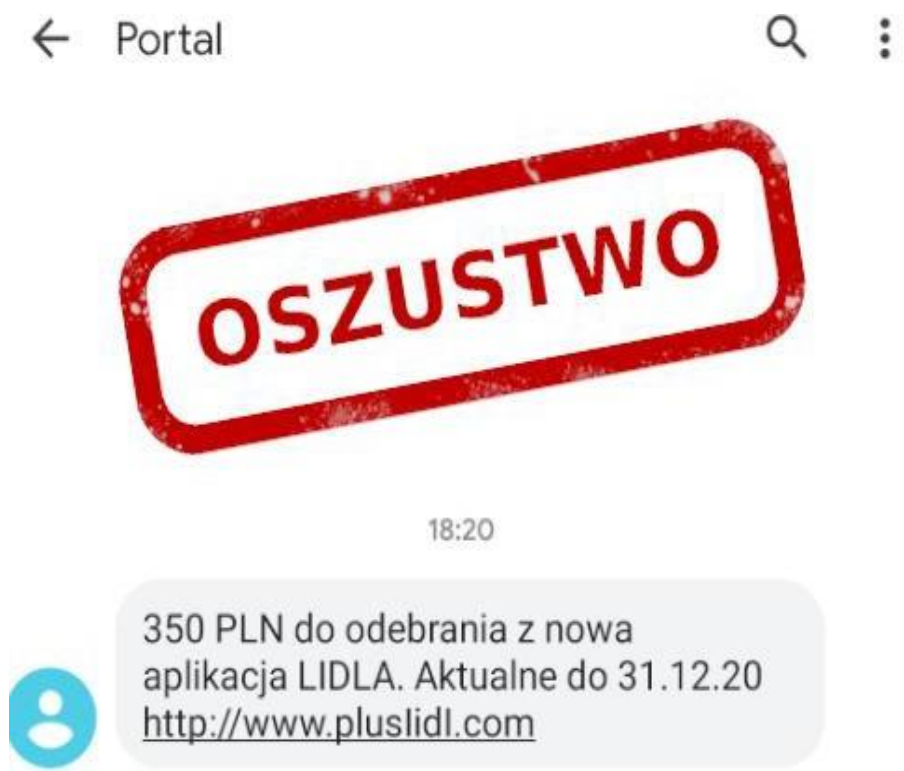
FRSI


Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane.
Odebrane x
mBank przez s7.jupe.pl
14:15 (7 minut temu)
do mnie
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


FW: Potwierdzenie transakcji - Message (HTML) (Read-Only)
File
Message
Help
Tell me what you want to do
FW: Potwierdzenie transakcji
Potwierdzenie transakcji.xls
.xls File
OSZUSTWO
From: confirmation@ipko.pl <confirmation@ipko.pl>
Sent: Tuesday, June 30, 2020 7:52 AM
To: undisclosed-recipients:
Subject: Potwierdzenie transakcji
Witamy,
w załączeniu przesyłamy potwierdzenie operacji na stronie bankowości elektroniczny iPKO.
Z poważaniem,
Zespół PKO Banku Polskiego
Ten e-mail został wygenerowany automatycznie. Proszę nie odpowiadać mu.

FRSI


Text Message
Today 7:43 pm
Profil Zaufany - Twoje zlecenie pozyczki pienieznej w kwocie 20.000 PLN zostało przyjete, pieniadze zostana wyplacone w ciagu 60 minut. Mozliwosc anulowania zlecenia przez internet https://profilzaufany.online/profil/
iMessage
Dzisiaj, 16:02
Twoja faktura nie zostala w wpelni oplacona. Prosimy o doplate 1 zl do dnia 22.11.2018 lub Twoj numer zostanie zablokowany
ulink.pl
9-5 12:29
Twoja paczka czeka w Paczkomacie WRO . Kod odbioru QR kod http://paczkomaty.pl Do zobaczenia!
16:17
Wysylka pod wskazany adres jest drozsza. Prosimy doplacic 1PLN, brak doplaty oznacza anulowanie zamowienia. http://in3post.tk/b6s5avv/1
iMessage
SMS


Portal
OSZUSTWO
18:20
350 PLN do odebrania z nowa aplikacja LIDLA. Aktualne do 31.12.20 http://www.pluslidl.com

FRSI

https://fdfghjklkjhgf.weebly.com

Szukaj

onet POCZTA

Zaloguj się do swojego konta

Adres email

Haslo

DALEJ

Czym charakteryzuje się darmowa poczta mailowa Onet?

INTELIGENTNE FOLDERY

Pozwól nam sortować Twoje wiadomości lub uporządkuj je po swojemu.

ALIASY

Wiele adresów w jednej skrzynce, dzięki aliasom.

PŁATNOŚCI

Proste płatności internetowe. Płać swoje rachunki bezpiecznie, bezpośrednio ze swojej poczty.

POWIADOMIENIA

Powiadomienia o nowych mailach, także w przeglądarce.

https://dantasensinar.com/?fbclid=IwAR3reLCxAyUVY-twMn9Ir5x7g6w-LhXm6uEpL3As6YBNf4xx6E3YxALSA-E

Santander

Kontakt Przejdź do santander Przejdź do innych serwisów

Bezpieczeństwo

1. Nie udostępniaj swoich danych.
2. Czytaj treść smsKodów.
3. Nie klikaj w linki i załączniki od nieznanych nadawców.

Więcej

Logowanie KROK 1

PL | EN | ES | UK | RU

Wpisz login

Dalej

Jak uzyskać dostęp?

Problem z logowaniem? Zresetuj swoje hasło

Sprzedajesz online? Uważaj na fałszywe wiadomości
Przestępcy wytudzają dane kart płatniczych oraz login i hasło do bankowości internetowej lub aplikacji mobilnej więcej >>

Informacje o zaplanowanych przerwach
Tutaj zawsze sprawdzisz informacje o zaplanowanych przerwach w bankowości internetowej i aplikacji mobilnej.

5% zwrotu za płatności w sklepach spożywczych

Z kartą kredytową Visa
RRSO: 23,30%

Sprawdź


Pekao24 - Logowanie
https://www.pękaobiznęs24.com
https://www.pękaobiznęs24.com
Bank Pekao
Nie masz konta? ZOSTAŃ KLIENTEM
Logowanie do Pekao24
WPISZ NUMER KLIENTA / NAZWĘ UŻYTKOWNIKA
Uzupełnij pole
Dalej
20.11.2021 Jeśli jesteś klientem korzystającym dotychczas z Idea Cloud, użyj swojego loginu z Idea Cloud, poprzedzając go małymi literami ib (bez znaków specjalnych). Więcej>>
Nie pamiętasz loginu z Idea Cloud? Kliknij tutaj>>
29.07.2021 Zachowaj czujność. Uważaj na telefony z fałszywych infolinii. Więcej>
Bezpieczeństwo
Pomoc w logowaniu
Kids

FRSI

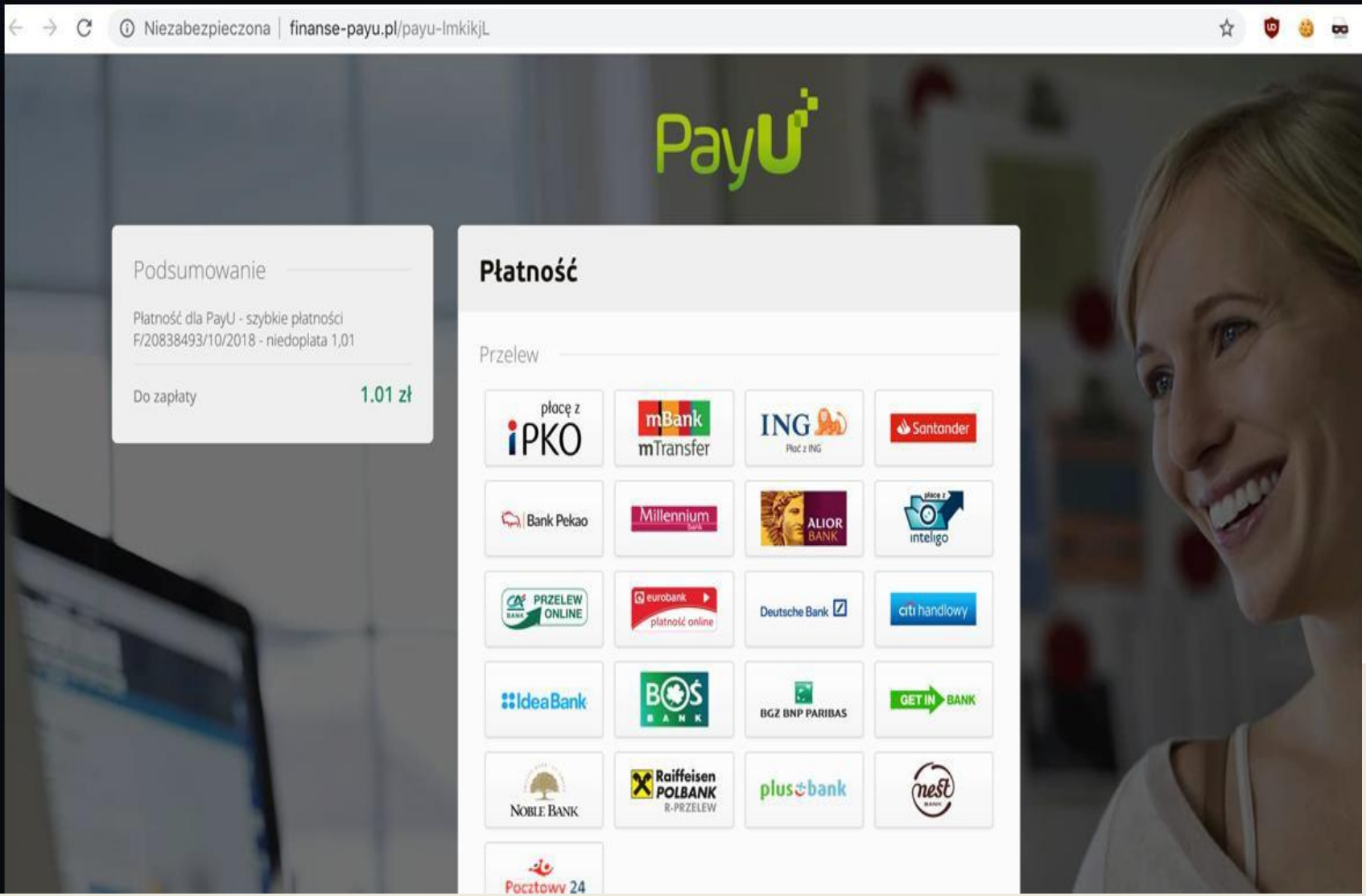
UWAGA NA FAŁSZYWE STRONY BANKOWOŚCI ELEKTRONICZNEJ!

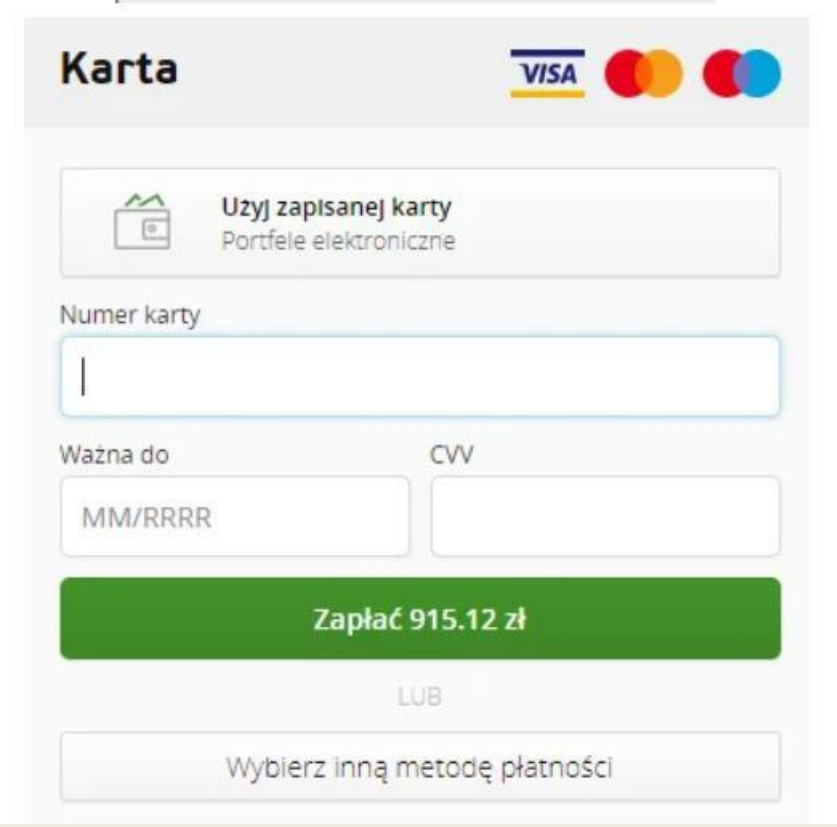
Prawdziwe domeny	Fałszywe domeny
bankmillennium.pl	bankmillenium-pl.com
online.mbank.pl	online-mbank.net
ca24.credit-agricole.pl	credit-agriolle.pl
bosbank24.pl	bosbank-24.com
login.ingbank.pl	loginingbank.online

Pamiętaj, aby zawsze dokładnie sprawdzać nazwę domeny!

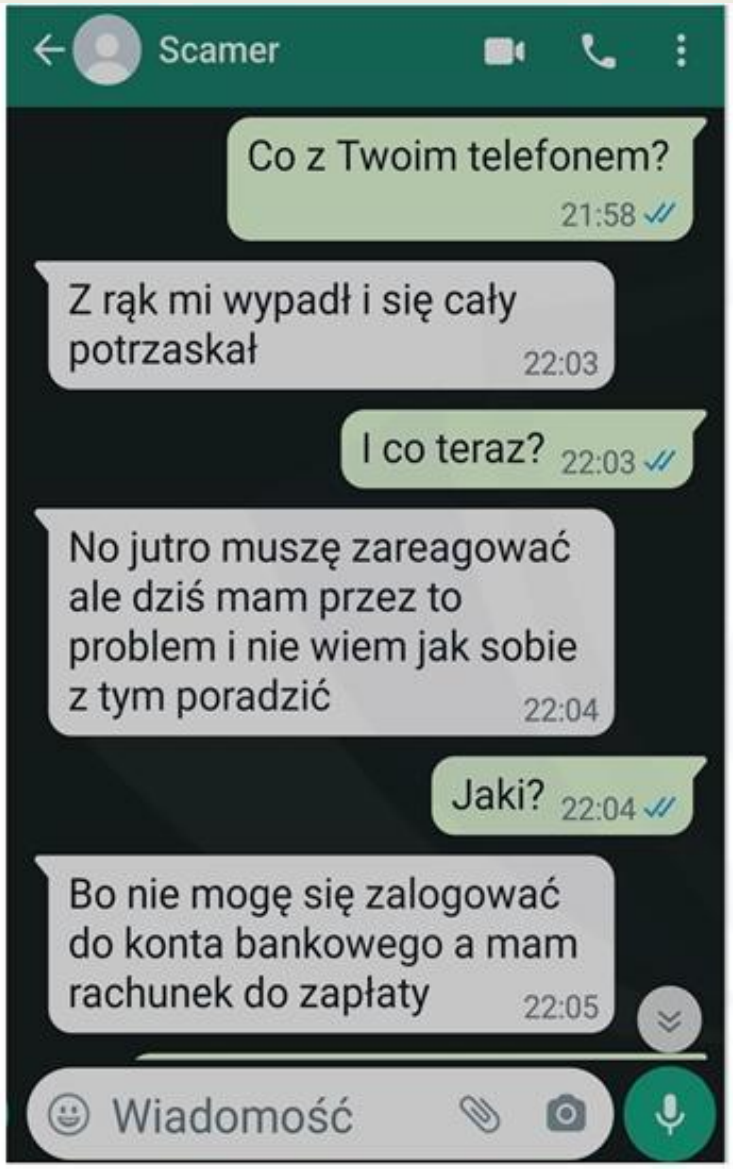
KNF CSIRT

FRSI

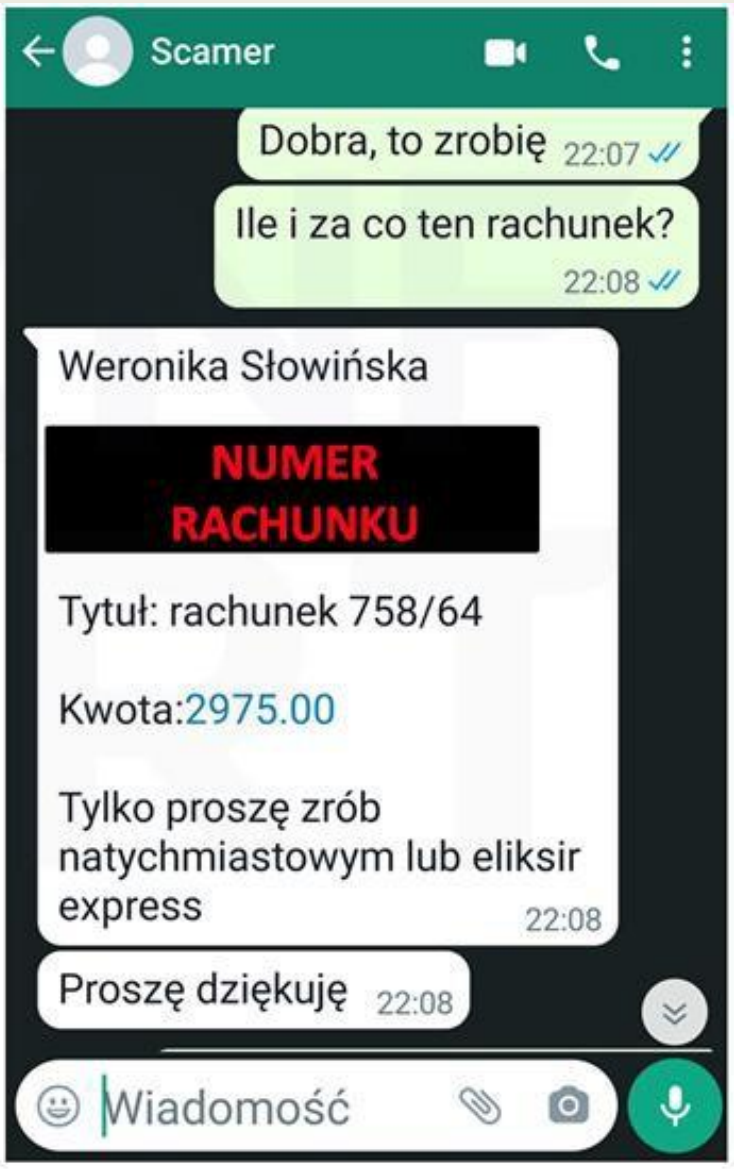

Niezabezpieczona | finanse-payu.pl/payu-lmkikjL
PayU
Podsumowanie
Płatność dla PayU - szybkie płatności
F/20838493/10/2018 - niedopłata 1,01
Do zapłaty 1.01 zł
Płatność
Przelew
płacę z iPKO
mBank mTransfer
ING Płać z ING
Santander
Bank Pekao
Millennium
ALIOR BANK
płacę z inteligo
PRZELEW ONLINE
eurobank płatność online
Deutsche Bank
citi handlowy
IdeaBank
BOŚ BANK
BGŻ BNP PARIBAS
GET IN BANK
NOBLE BANK
Raiffeisen POLBANK R-PRZELEW
plus bank
nest BANK
Pocztowy 24


Karta
VISA
Użyj zapisanej karty
Portfele elektroniczne
Numer karty
Ważna do
MM/RRRR
CVV
Zapłać 915.12 zł
LUB
Wybierz inną metodę płatności

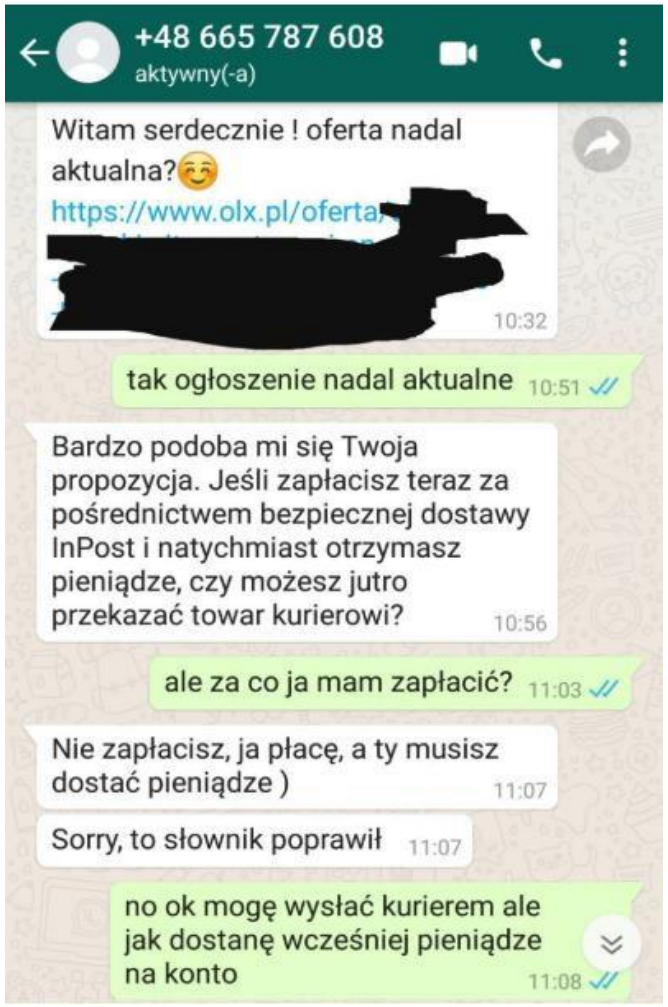
FRSI

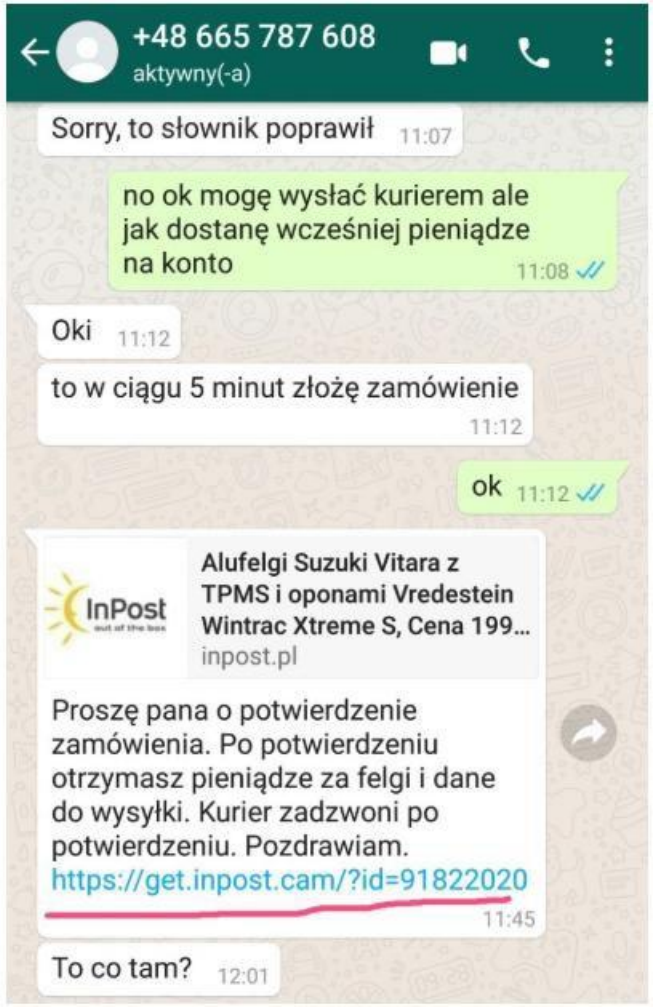

Scamer
Co z Twoim telefonem? 21:58
Z rąk mi wypadł i się cały potrzaskał 22:03
I co teraz? 22:03
No jutro muszę zareagować ale dziś mam przez to problem i nie wiem jak sobie z tym poradzić 22:04
Jaki? 22:04
Bo nie mogę się zalogować do konta bankowego a mam rachunek do zapłaty 22:05
Wiadomość


Scamer
A nie możesz na komputerze? 22:06
No nie bo nie mam karty SIM tamtej a mi SMS przychodzi 22:06
Zrobisz mi 22:06
Okej 22:07
?? 22:07
A o której będziesz w domu? 22:07
To sam sobie zrobisz z mojego konta 22:07
Wiadomość


Scamer
Dobra, to zrobię 22:07
Ile i za co ten rachunek? 22:08
Weronika Słowińska
NUMER RACHUNKU
Tytuł: rachunek 758/64
Kwota:2975.00
Tylko proszę zrób natychmiastowym lub eliksir express 22:08
Proszę dziękuję 22:08
Wiadomość


20:39
1%
Mateusz
19:20
Siemka. masz pożyczyć 800 zł do wieczora/jutro rana bo muszę opłacić rezerwację a mam jakąś przerwę w banku
Spokoo
Daj numer konta
możesz blika na nr do sprzedawcy od razu walnąć?
Właśnie ja nie mam blika
A ekspres możesz zrobić bo to pilna sprawa oddam ci
Ok
32102049550000760203154440
Oskar Jagoda
Daj znać jak p e
Aa


+48 665 787 608
aktywny(-a)
Witam serdecznie ! oferta nadal aktualna?
https://www.olx.pl/oferta/
10:32
tak ogłoszenie nadal aktualne 10:51
Bardzo podoba mi się Twoja propozycja. Jeśli zapłacisz teraz za pośrednictwem bezpiecznej dostawy InPost i natychmiast otrzymasz pieniądze, czy możesz jutro przekazać towar kurierowi? 10:56
ale za co ja mam zapłacić? 11:03
Nie zapłacisz, ja płacę, a ty musisz dostać pieniądze) 11:07
Sorry, to słownik poprawił 11:07
no ok mogę wysłać kurierem ale jak dostanę wcześniej pieniądze na konto 11:08


+48 665 787 608
aktywny(-a)
Sorry, to słownik poprawił 11:07
no ok mogę wysłać kurierem ale jak dostanę wcześniej pieniądze na konto 11:08
Oki 11:12
to w ciągu 5 minut złożę zamówienie 11:12
ok 11:12
InPost
Alufelgi Suzuki Vitara z TPMS i oponami Vredestein Wintrac Xtreme S, Cena 199...
inpost.pl
Proszę pana o potwierdzenie zamówienia. Po potwierdzeniu otrzymasz pieniądze za felgi i dane do wysyłki. Kurier zadzwoni po potwierdzeniu. Pozdrawiam.
https://get.inpost.cam/?id=91822020
11:45
To co tam? 12:01

Atak telefoniczny na zdalny pulpit (spoofing)

FRSI

Ocena sytuacji

1. Sprawdź czy **kontekst wiadomości** jest ukierunkowany na podjęcie przez ciebie szybkich działań.
2. Weryfikuj **adres domeny**, z której przyszedł e-mail (nazwa domenowa to część po znaku „@”)
3. Nie daj się zwieść **pozorom** (logo, stopki, format, kolorystyka, to wszystko można skopiować)
4. Zwracaj uwagę na błędy językowe (tutaj niestety z pomocą dla oszustów przychodzą modele językowe)

FRSI

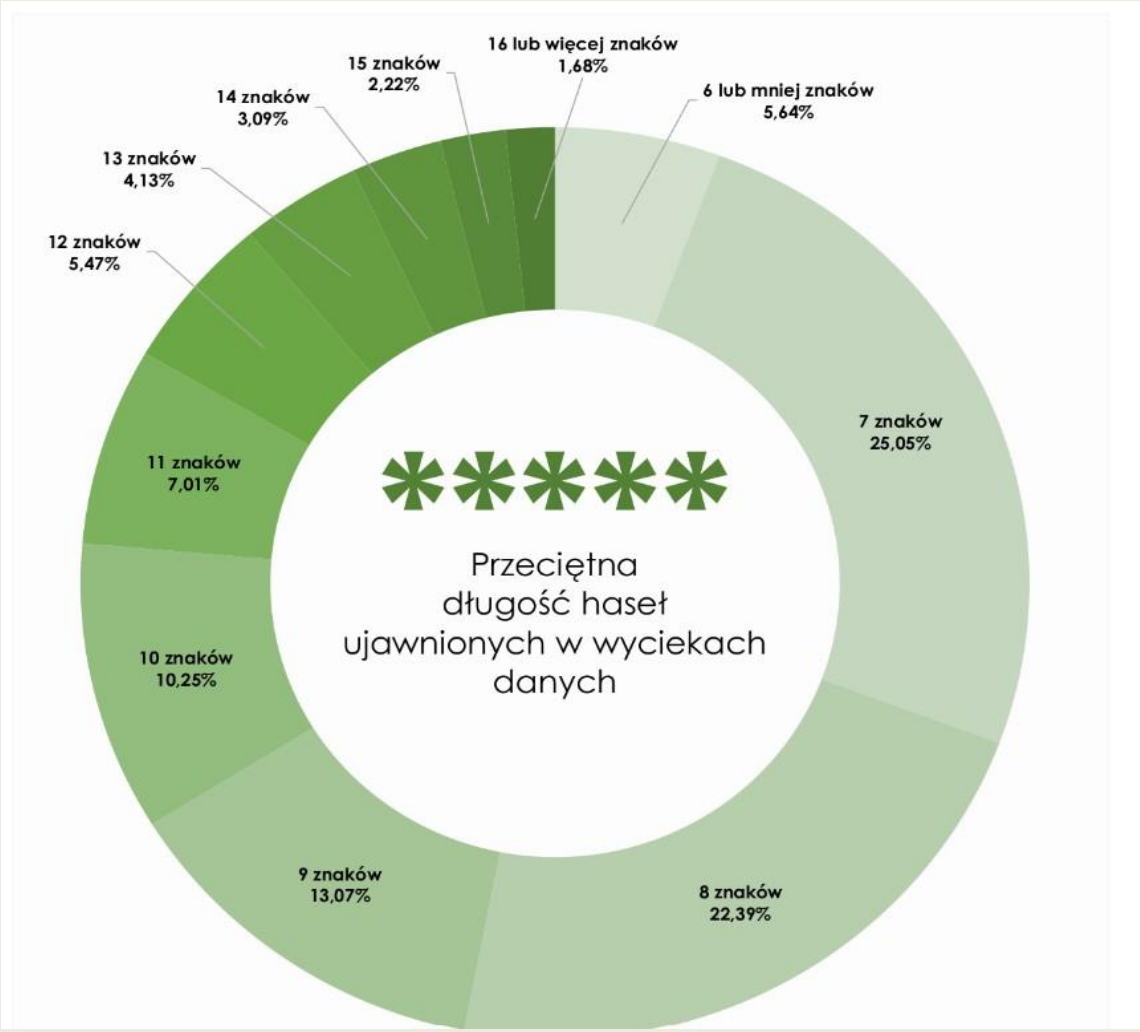
Czym jest cyfrowa tożsamość?

Cyfrowa tożsamość to zbiór informacji, które pozwalają na identyfikację osoby w świecie cyfrowym, czyli m.in.:

- Dane, którymi dzielimy się z własnej inicjatywy – np. media społecznościowe.
- Dane, które podajemy w celu skorzystania z wybranych usług np. sklepy internetowe.
- Dane wymagane prawem, rejestracja działalności gospodarczej.
- Dane, które na nasz temat posiadają/publikują organizacje.

Przykłady

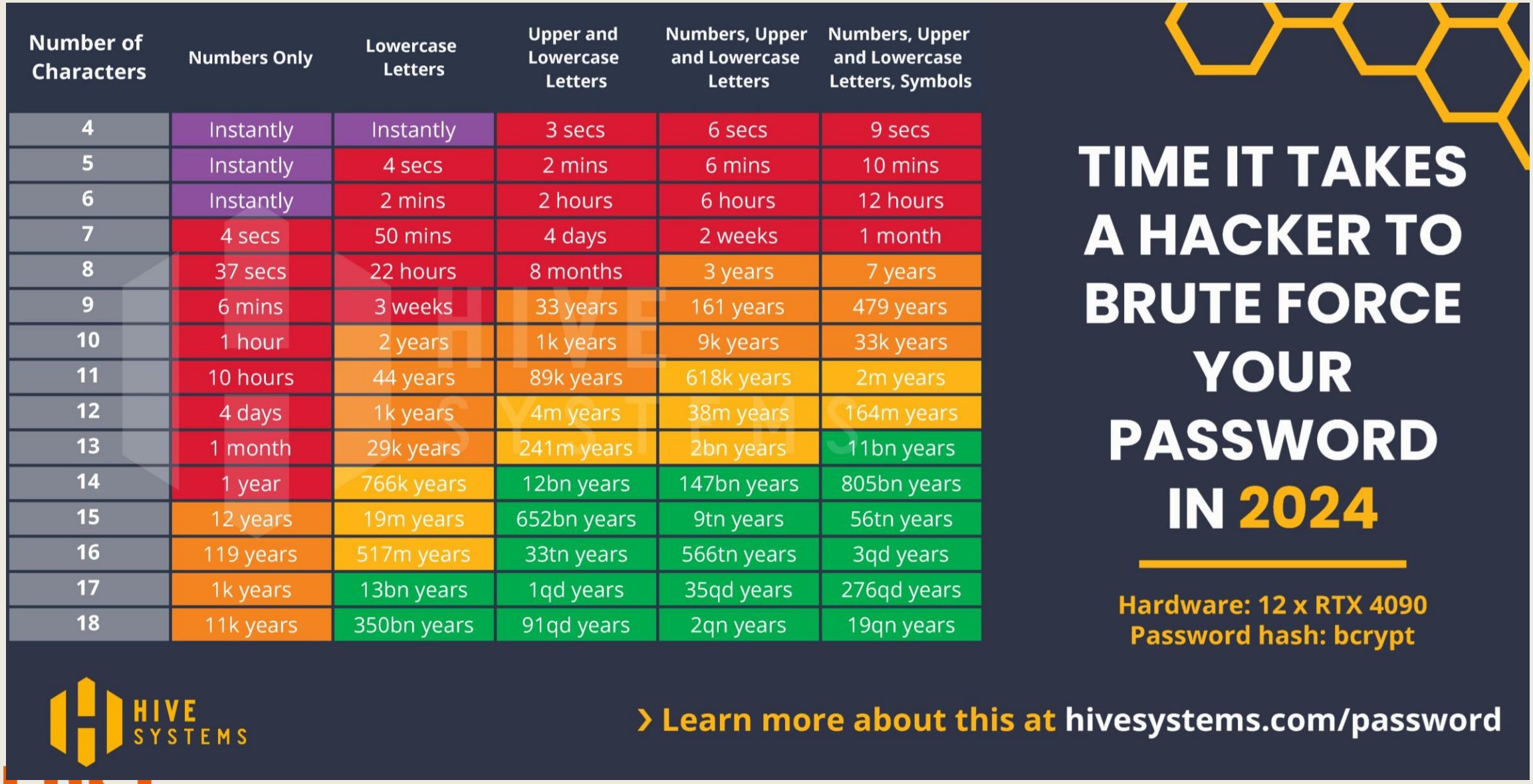
https://www.youtube.com/watch?v=Advj0Zlo5nQ
https://www.youtube.com/watch?v=F7pYHN9iC9I
https://www.youtube.com/watch?v=6xDA_7U95rs



Bezpieczeństwo haseł

- Jakie hasła są najlepsze?
- Czy powinno się cykliczne zmieniać hasło?
- Sejfy do przechowywania haseł,
- 2FA, drugi składnik logowania

FRSI


Number of Characters
Numbers Only
Lowercase Letters
Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters, Symbols
4 Instantly Instantly 3 secs 6 secs 9 secs
5 Instantly 4 secs 2 mins 6 mins 10 mins
6 Instantly 2 mins 2 hours 6 hours 12 hours
7 4 secs 50 mins 4 days 2 weeks 1 month
8 37 secs 22 hours 8 months 3 years 7 years
9 6 mins 3 weeks 33 years 161 years 479 years
10 1 hour 2 years 1k years 9k years 33k years
11 10 hours 44 years 89k years 618k years 2m years
12 4 days 1k years 4m years 38m years 164m years
13 1 month 29k years 241m years 2bn years 11bn years
14 1 year 766k years 12bn years 147bn years 805bn years
15 12 years 19m years 652bn years 9tn years 56tn years
16 119 years 517m years 33tn years 566tn years 3qd years
17 1k years 13bn years 1qd years 35qd years 276qd years
18 11k years 350bn years 91qd years 2qn years 19qn years
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024
Hardware: 12 x RTX 4090
Password hash: bcrypt
HIVE SYSTEMS
› Learn more about this at hivesystems.com/password

FRSI

„Czarny rynek” w internecie

Dark Web, możliwość zakupu danych pochodzących z kradzieży (wycieku) np. pary login i hasło, dane kart płatniczych.

Ogólnodostępne:
- listy najpopularniejszych haseł.

Te dane są wykorzystywane do dalszych działań np. fałszywe sklepy internetowe, ogłoszenia w olx itp, przejmowanie kont facebook…

FRSI

Dobre praktyki w tworzeniu silnych haseł

Hasła typu: xY7.10bK. . .. Są dobrymi oraz trudnymi do złamania hasłami lecz trudno aby pamiętać wiele takich haseł (hasła dla sejfu)

Dobrym sposobem na trudne do złamania hasło ale łatwe do zapamiętania będzie schemat typu: 4CzerwoneHulajnogiJedzaGofry# (długie, trudne do złamania, łatwe do zapamiętania)

W tworzeniu haseł warto pozwolić sobie na pewną abstrakcję, unikniemy dzięki temu haseł słownikowych.

FRSI

Wybrane metody łamania haseł

1. Atak słownikowy

- Wykorzystuje listy popularnych haseł lub słów występujących w słownikach.
- Skuteczny wobec słabych haseł (np. „password”, „123456”, „qwerty”).
- Nieskuteczny wobec długich i losowych haseł.

2. Atak brute-force (atak siłowy)

- Próbuje każdą możliwą kombinację znaków aż do znalezienia poprawnego hasła.

3. Atak na podstawie wycieku danych (Credential Stuffing)

- Wykorzystuje dane z wycieków (np. skradzione e-maile i hasła) do logowania się na inne konta.
- Skuteczny, ponieważ wielu użytkowników używa tych samych haseł na różnych platformach.

FRSI

4. Atak Man-in-the-Middle

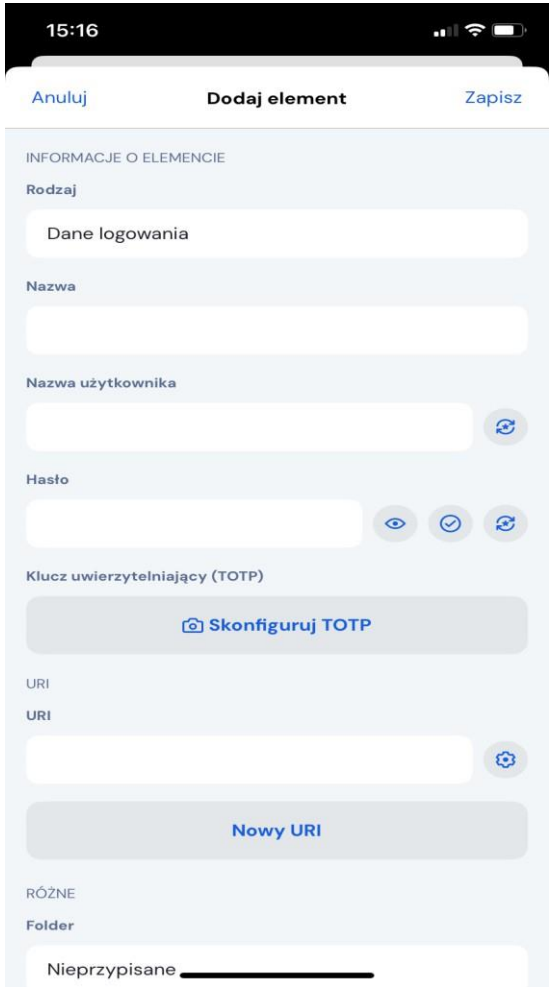
- Podsłuchiwanie komunikacji między użytkownikiem a serwerem w celu przechwycenia hasła.
- Wykorzystuje luki w niezabezpieczonych połączeniach (np. HTTP zamiast HTTPS).

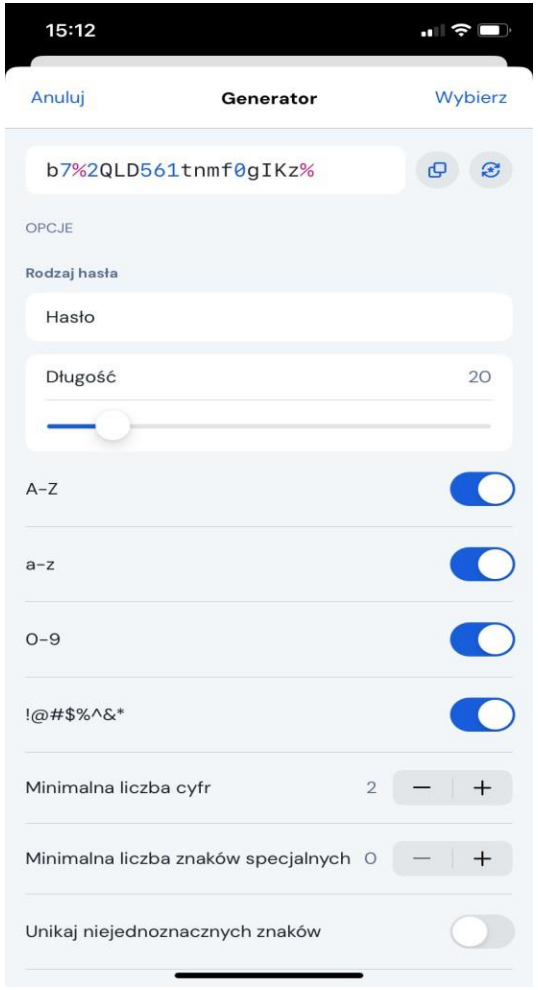
5. Keylogger

- Oprogramowanie (lub sprzęt), które zapisuje każdy naciśnięty klawisz na klawiaturze, w tym hasła.
- Może być stosowany przez malware lub wrogie oprogramowanie.

FRSI

Manager haseł

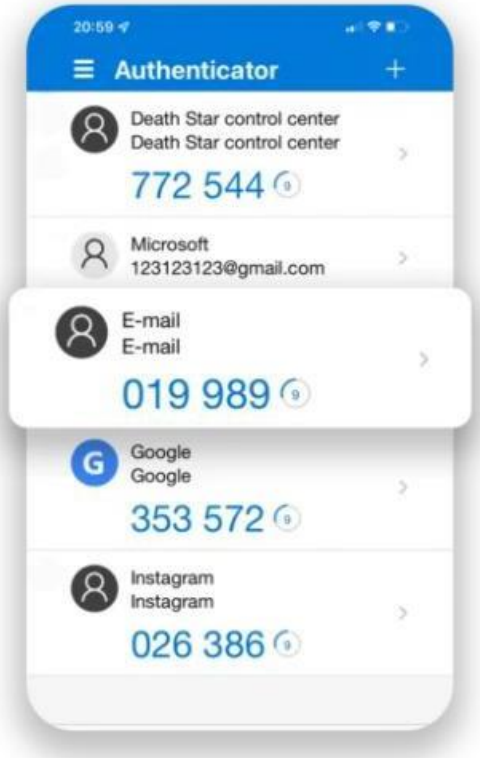


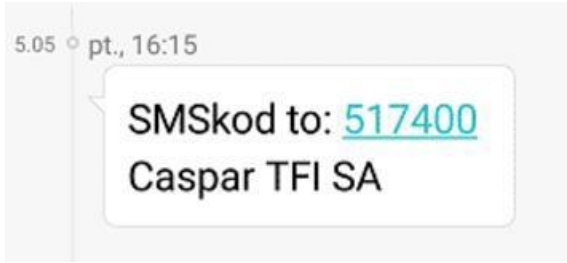


FRSI

Uwierzytelnianie dwuskładnikowe

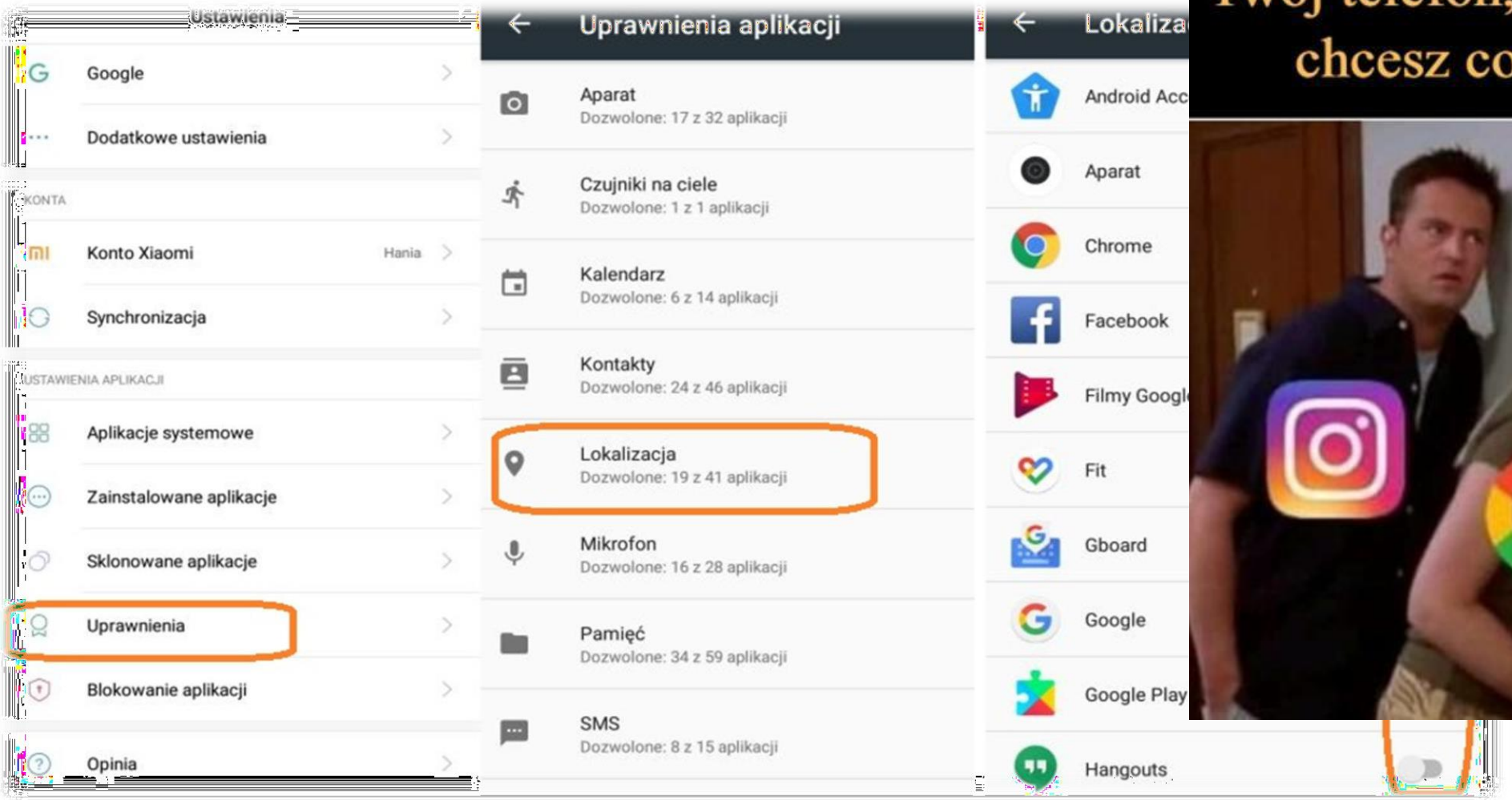
- Hasło + 2 element





FRSI

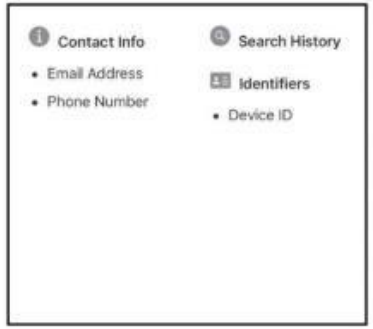
Bezpieczeństwo i uprawnienia aplikacji



FRSI

Signal
'Data Linked To You'

iMessage
'Data Linked To You'



WhatsApp
'Data Linked To You'

Facebook Messenger
'Data Linked To You'

Aktualizacja systemu

Aktualizacja systemu jest bardzo ważna z uwagi na to, iż pozwala nam wyeliminować znane luki pojawiające się w obecnej wersji oprogramowania.

- Włącz automatyczne aktualizacje oprogramowania, wszędzie gdzie jest to możliwe.
- Unikaj przestarzałego i niewspieranego oprogramowania.
- Oprogramowanie pobieraj bezpośrednio ze strony producenta (lub z dedykowanego sklepu, Google Play, App Store)

FRSI

Przykład trojana bankowego

Badania Zscaler ThreatLabz ujawniły, że groźny trojan bankowy Anatsa zainfekował aplikacje w Google Play, narażając miliony użytkowników na kradzież danych finansowych. Cyberprzestępcy ukrywają złośliwy kod w popularnych aplikacjach, takich jak czytniki PDF czy skanery QR.

Groźny wirus w Google Play

W ciągu ostatnich kilku miesięcy zespół Zscaler ThreatLabz odkrył i przeanalizował ponad 90 złośliwych aplikacji, które łącznie zostały pobrane ponad 5,5 miliona razy. Wśród nich szczególną uwagę przyciągnęły aplikacje dystrybuujące trojana Anatsa.

Anatsa jest wyjątkowo niebezpiecznym złośliwym oprogramowaniem, które wykorzystuje tzw. aplikacje droppery. Są to programy, które na pierwszy rzut oka wydają się nieszkodliwe – na przykład czytniki PDF czy aplikacje do skanowania kodów QR.

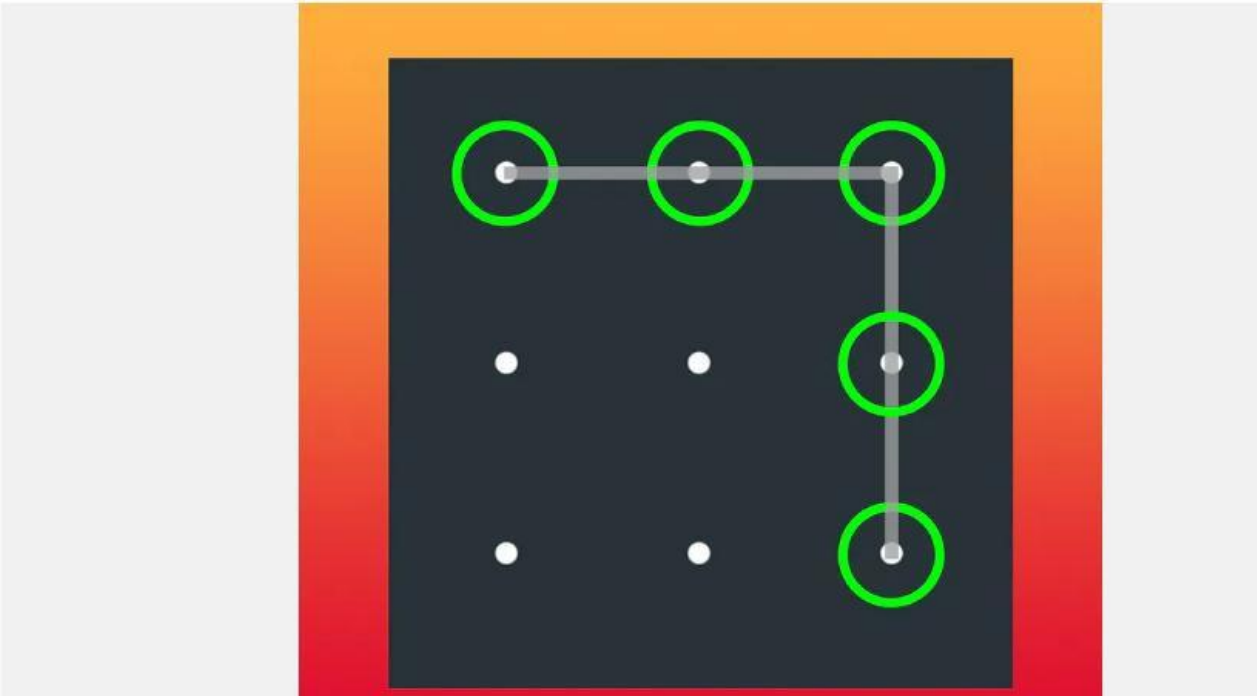
Jednak po ich pobraniu na urządzeniu użytkownika, aplikacje te ściągają i instalują złośliwy kod, który kradnie dane logowania do banków i inne poufne informacje finansowe.

FRSI

Zabezpieczenie telefonu

Jeżeli masz jedno z najpopularniejszych haseł na Android, to:

- **rozpoczynasz w punkcie w lewym górnym rogu ekranu** - dotyczy to prawie 50% przebadanych haseł



FRSI

Uwaga na urządzenia nieznanego pochodzenia

FRSI

Dodatkowe materiały + narzędzia z prezentacji

https://www.youtube.com/watch?v=SbCcmLqmQSs&t=1s

https://quiz.knf.gov.pl/quiz/rozpoznaj-phishing/2

https://pimeyes.com/en

https://yandex.com/

https://otwartezrodla.pl/

https://mysignins.microsoft.com/

https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

https://firmabezpiecznacyfrowo.pl/poradnik/podstawy-bezpieczenstwa-sieci/vpn/

https://cert.pl/ouch/

https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen

FRSI