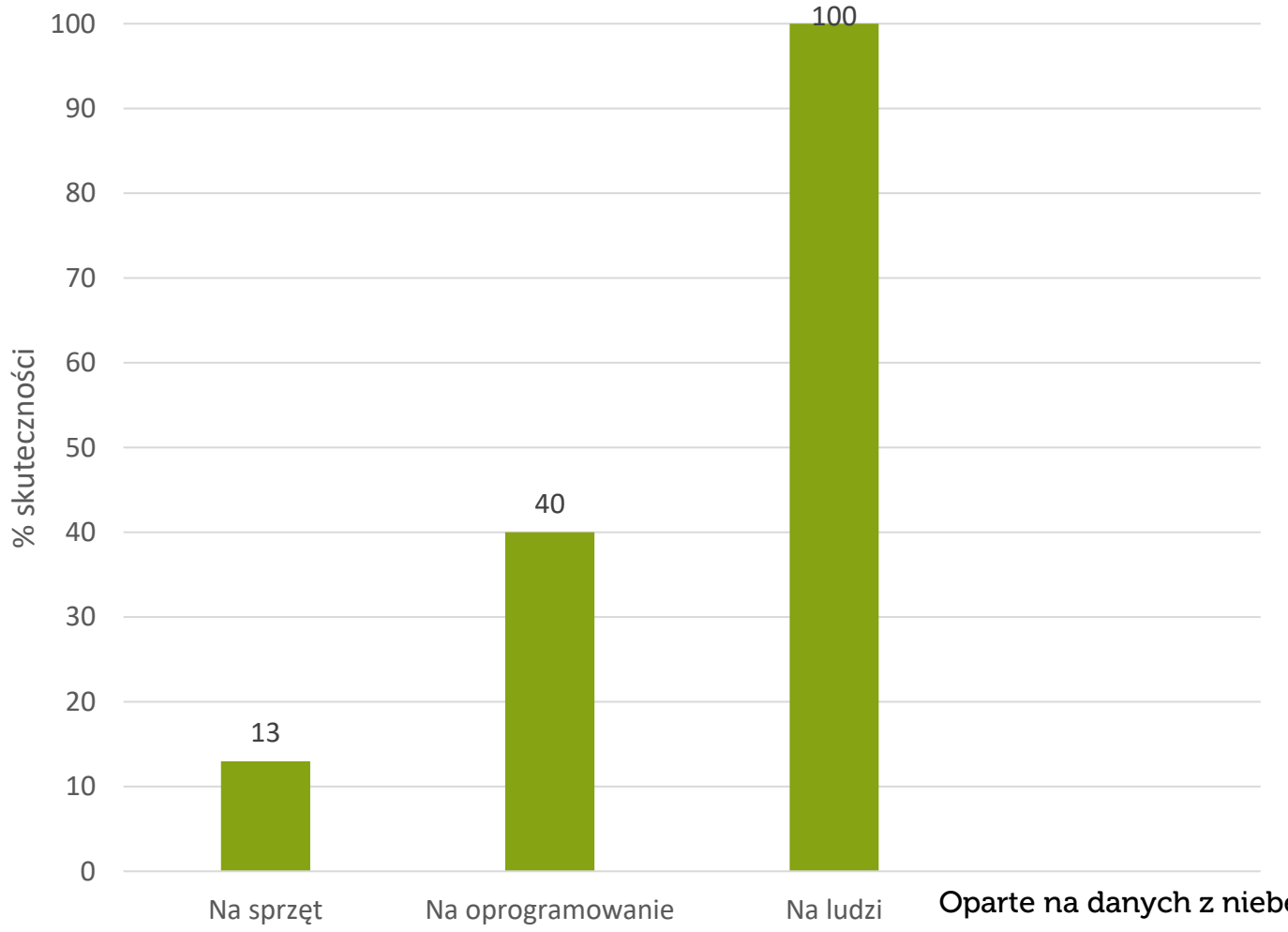
Związek Harcerstwa Polskiego

Cybersecurity
Najsłabszym ogniwem są ludzie

phm. Grzegorz Wąs

Skuteczność ataków



Oparte na danych z niebezpiecznik.pl

„Łamałem ludzi, nie hasła"

~Kevin Mitnick – najsławniejszy haker na świecie

Tak naprawdę hakerzy nigdy nie próbowali łamać trudnych haseł i zabezpieczeń.

Większość ataków na firmy odbywa się na ich pracowników i te ataki zawsze mają 100% skuteczność!

Rodzaje ataków - Socjotechnika

1. Wyłudzanie informacji przez phishing – rozmowy telefoniczne, SMSy, maile itd. (najskuteczniejsza metoda)
2. Nakłonienie kogoś do otwarcia pliku lub kliknięcia w link – kończy się zainfekowaniem urządzenia i podsłuchiwaniem co się dzieje.

W każdym przypadku gubi nas pośpiech lub użycie sztucznego autorytetu przez atakującego:

Mail o 16:00, kiedy mamy już iść do domu - „Pani Basiu proszę wykonać ten przelew eskpresem na poniższy numer konta, Pozdrawiam Prezes"

SMS przed świętami - „Przesyłka została wstrzymana, dopłać brakujące 0,27zł aby otrzymać ją przed świętami. Kliknij w poniższy link"

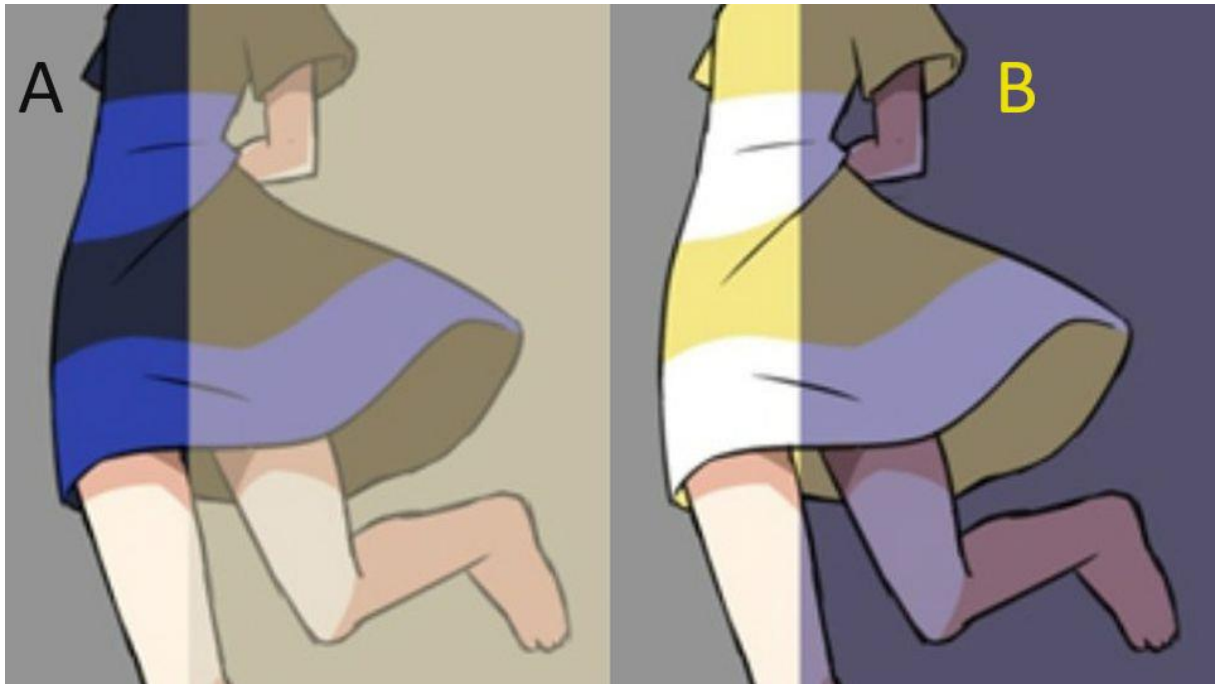
Dzwoni członek działu bezpieczeństwa banku - „Wykryliśmy nieautoryzowaną operację na twoim koncie bankowym, na szczęście zatrzymaliśmy hakerów. Musisz tylko zainstalować naszą aplikację żeby sprawdzić czy nie masz wirusów na swoim telefonie!"

Dlaczego człowiek jest najsłabszym ogniwem?

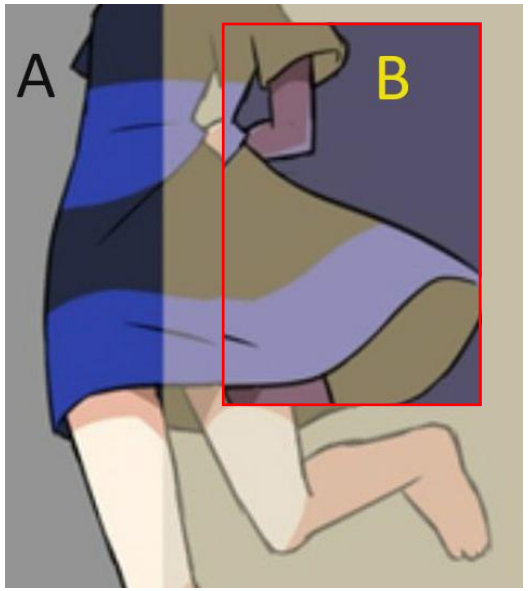
Związek Harcerstwa Polskiego

Sprawdźmy zatem jak działa ludzki mózg i dlaczego potrafimy się nabrać

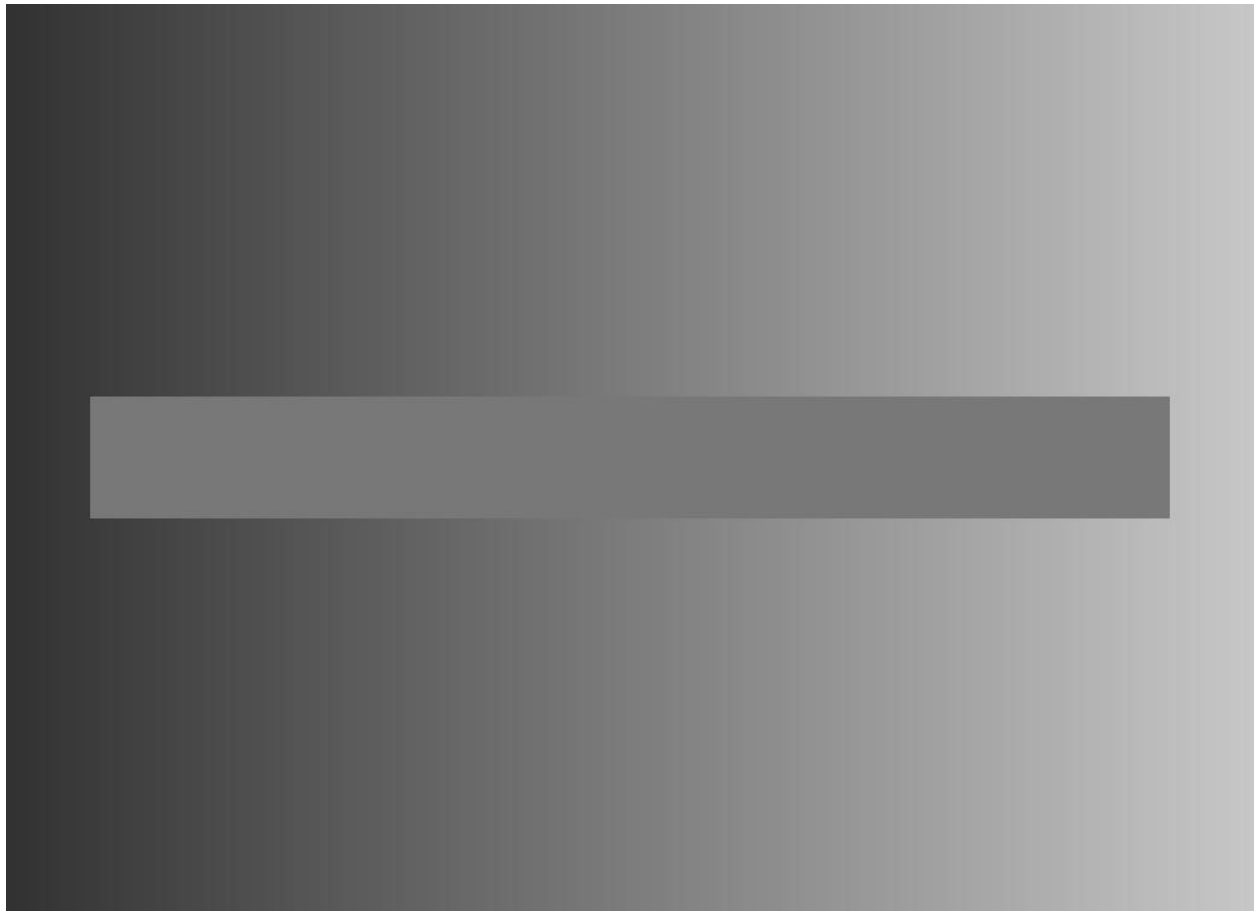
Czy sukienka na tych dwóch obrazkach jest tego samego koloru?



Tak!



Czy prostokąt w środku ma ten sam kolor na całej długości?



Tak!

Spróbuj znaleźć dwa błędy w dwóch dolnych linkach

mbank.pl

rnbank.pl

mbank.pl

Dałeś radę? To spróbuj teraz spojrzeć w prawy dolny róg ;)

mbank.pl

rnbank.pl

mbank.pl

Dla porównania to są te same linki napisane czcionką o rozmiarze 11, czyli taką jaką znajdziecie w mailach.
Spróbuj teraz dostrzec różnice :)

mbank.pl

rnbank.pl

mbank.pl

Który z tych dwóch linków jest fałszywy?

Inpost.pl

Inpost.pl

Dolny ponieważ zamiast wielkiej litery „i” jest tam małe „l”

INPOST.PL

LNPOST.PL

Dla porównania to są te same linki napisane czcionką o rozmiarze 11, czyli taką jaką znajdziecie w mailach.
Spróbuj teraz dostrzec różnice :)

Inpost.pl

lnpost.pl

Który z tych dwóch linków jest fałszywy?

pkobp.pl

pkobp.pl

Dałeś radę? To spróbuj teraz spojrzeć w prawy dolny róg ;)

pkobp.pl

pkobp.pl

Dla porównania to są te same linki napisane czcionką o rozmiarze 11, czyli taką jaką znajdziecie w mailach.
Spróbuj teraz dostrzec różnice :)

pkobp.pl

pkobp.pl

Dlaczego człowiek jest najsłabszym ogniwem?

Czy podacie komuś swój PESEL i nazwisko panieńskie matki?

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

To zależy jak zadamy pytanie, na tym właśnie polega socjotechnika

Czy jest jakaś uniwersalna technika samoobrony?

Scammerzy (oszuści) liczą na prosty zarobek, jeśli dopadną tych, którzy nie potrafili się odpowiednio zabezpieczyć, to nie będą ścigać nikogo więcej.

Waszym zadaniem jest być szybszym od tego najwolniejszego. Im więcej kłód rzucicie oszustom pod nogi tym bardziej ich zniechęcicie ;)

Zróbmy prostą kalkulację, scammer wysyła 250 tys. maili, nawet jeśli nabierze się tylko 10 osób i średnio na swoim koncie posiadają oni 10-15 tys. zł (średnie oszczędności Polaków) to ukradną ok. 150 000 zł na czysto.

Hasła słownikowe – masz takie? To je zmień ;)

Hasła słownikowe to hasła, które znajdują się w słownikach haseł dostępnych online np.: zuzia, kalina, jamesbond007, Grzegorz, wiedzmin itd..

Największy taki słownik waży 15GB i ma w sobie 1 493 677 782 hasła. Dużo? -> https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm

Karta graficzna z przeciętnej półki potrafi sprawdzić 52 miliardy takich haseł w ciągu sekundy, a przy trudniejszych kombinacjach zaledwie 19 miliardów. Oczywiście żeby wzmocnić nasze hasła słownikowe dodajemy na końcu cyfry lub znaki specjalne. Więc crackerzy są sprytniejsi i sprawdzają czy właśnie Twoje tajne słownikowe hasło nie dodało sobie kilku losowych znaków ;)

Zapisz teraz na kartce jak myślisz w jakim czasie uda się złamać hasło „Grzegorz123!”?

Albo 11 cyfrowy numer PESEL? Którym banki kochają zabezpieczać przesyłane nam dokumenty.

Hasła słownikowe – Grzegorz123!

```
e7d97a30d5c8e932a10f702e770dc878:Grzegorz123!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: e7d97a30d5c8e932a10f702e770dc878
Time.Started.....: Fri Nov 03 22:17:46 2023 (1 min, 6 secs)
Time.Estimated...: Fri Nov 03 22:18:52 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (.\dictionaries\crackstation-human-only.txt.gz)
Guess.Mod........: Rules (.\rules\oneruletorulethemall.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 20567.1 MH/s (7.31ms) @ Accel:128 Loops:128 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1289266334725/3324615882655 (38.78%)
Rejected.........: 16496921605/1289266334725 (1.28%)
Restore.Point....: 23893027/63941069 (37.37%)
Restore.Sub.#1...: Salt:0 Amplifier:38912-39040 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: Gdynia-s3099 -> Gevisser's2766
Hardware.Mon.#1..: Temp: 69c Fan: 82% Util: 31% Core:2459MHz Mem:1990MHz Bus:16

Started: Fri Nov 03 22:17:43 2023
Stopped: Fri Nov 03 22:18:53 2023
PS E:\Dokumenty\Programy\hashcat-6.2.6>
```

Złamanie hasła „Grzegorz123!" zajęło nam 1 minutę i 6 sekund, a karta graficzna potrafiła przejrzeć 20567,1 MH/s (Mega Hashy na sekundę).

Czyli 20 567 100 000 haseł na sekundę.

Dla ciekawskich:

Hash to ciąg znaków stworzony przez nieodwracalny algorytm i w takiej formie zapisywane są hasła w bazach danych. To właśnie hashe łamią crackerzy. Dla naszego hasła widać go w lewym górnym rogu (użyty został najprostszy algorytm md5). Tutaj można sobie potworzyć takie hashe -> https://www.md5hashgenerator.com/

Karty graficzne potrafią je tworzyć szybciej niż procesory, ponieważ mają one więcej niż procesor jednostek potrafiących wykonywać takie obliczenia równolegle.

Hasła słownikowe – PESEL

```
6e3087661ce42e489403b7ad9507768e 92011185376

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 6e3087661ce42e489403b7ad9507768e
Time.Started.....: Fri Nov 03 22:27:18 2023 (2 secs)
Time.Estimated...: Fri Nov 03 22:27:20 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: ?d?d?d?d?d?d?d?d?d?d?d [11]
Guess.Queue......: 1/5 (20.00%)
Speed.#1.........: 53740.3 MH/s (10.22ms) @ Accel:128 Loops:500 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 78446592000/100000000000 (78.45%)
Rejected.........: 0/78446592000 (0.00%)
Restore.Point....: 77856768/100000000 (77.86%)
Restore.Sub.#1...: Salt:0 Amplifier:0-500 Iteration:0-500
Candidate.Engine.: Device Generator
Candidates.#1....: 12387636818 -> 68598542382
Hardware.Mon.#1..: Temp: 56c Fan: 34% Util: 46% Core:2446MHz Mem:1990MHz Bus:16

Started: Fri Nov 03 22:27:15 2023
Stopped: Fri Nov 03 22:27:20 2023
PS E:\Dokumenty\Programy\hashcat-6.2.6>
```

A jak wypadł PESEL?

Złamanie losowego numeru PESEL „92011185376” zajęło nam 2 sekundy, a karta graficzna potrafiła przejrzeć 53740,3 MH/s

Czyli 53 740 300 000 haseł na sekundę.

Wszystkie numery od 00000000000 do 99999999999, jesteśmy w stanie przejrzeć w niecałe **2 sekundy**, bez używania słowników.

Ponieważ możliwych jest zaledwie 100 miliardów takich kombinacji z 11 cyframi.

Ile zajmuje łamanie haseł, ale niesłownikowych?

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	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tn years	100tn years	7qd years

Tabelkę po lewej i jej opis możecie znaleźć na stronie:

https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=header

Zobacz, że nasz PESEL da się złamać w 2 sekundy. Dokładnie w tyle ile widziałeś na poprzedniej stronie ;)

Hasła niesłownikowe

```
ahkame!Qui7noo1F aegh]ai6Zie8ieFo quei~ghah?G,ei8o cahF<eehebi6nieh
aik%aip7Iemei8oe da,u9Ahw,iej6guw ooh6cien[eiwooBa gaeyiegaipe[C6ah
eiz0owaeni}Fai6f Az7eigho*es5iepi yiej6fee9ool{aNg Mieziequ0TaeHah|
Ahqua3zahch3ba^u hoZ4mee>vei{fush ath&eeSev3jai@sh sha1Tei0aich>ueJ
AiDei?v7eengugai eireikeiTh0phoh" Ve6roch7Iighew]e kauSi^ar0Jahthoh
Ade>tae2TeiVohwe eijahHeiw3gaLu?k shah(x0baejie8Su eeyei1oop_a6ZeC^
EiR@eu3Oe7eenieW ooSh1Mahch8quoo] cuo%ngu8ak'ai4Ai chahC=ang)uegh5i
aik0Ahz`eiguukoh phod9eehia8kei;W Esai-K1ohz9Chooj ahPh@is_ie4foh7A
Ohph!eica2teB9on eb4loh@feeM4Aecu iewo7Vah>gh1te\e EeGh7caeNg#ai2ai
ahXoo5phai_ngahy beshooGh!ishi0ah lahBi2Vaiboo~que ahM2Di2ahC=ie|S7
Hee\neiphae0ood^ Thagiagh"eiph3im ohM_o\he2sheg<oh ohque0boo@B,ieRe
Oov>e4aip0aochae eigu6Rei3eaj=eus ae3sooW"aip4osiW az8yu6ia8ii-Weex
eij!ooquaPh4Ieli boo>Ng9Ahqueishe foolo<Z1oongei1e boh1Ail.etho4que
uriTh]oo@c>oh8Fa phoh,Rah8rooh1oh EeR3ooShaih&alei oMa^x4lah6ahraw0
aiw{aJ8voo3wo#to Coiha0six|ei3onu zei6Aip3wai|gah3 ohB1Aev~iez>ea9e
taew,aifae@k8Yai Eey6ta[k}aG4Eon7 OoYoo;tah_yi0Pai Choh4ohja{j`oop4
amu6chazoo!v?eaB ol$ahtohze5Zae\k Vaeraix2eiF~iH5x AiFei2ahv)a7Mao9
Xohngie'dujue,b9 Uv\o1fee4eey,ahy oo0Hoo+rea7Wada( mais8ooK@ieQuahy
Roh3Yai[ghu2fahk Quux.ahthaich1pi Foo=Thu4Uyiegh4p ooj_ooph0teeXe4r
iet`a2ooLuol5uj0 ta*fa2udu0bae>Ch ahGh7lee5ait/ohk sha'pahkie3ohS6i
```

Po lewej możesz znaleźć 16-znakowe hasła niesłownikowe wygenerowane przez jeden z programów dostępnych pod linuxem (pwgen).

W przeciwieństwie do haseł słownikowych, człowiek nie jest w stanie ich zapamiętać robiąc tylko rzut okiem.

P.S. Nie używajcie żadnego z nich ;) są już dostępne publicznie więc można powiedzieć, że są spalone :)

Jeśli z całej prezentacji masz zapamiętać jedną rzecz, to zapamiętaj to:

DO KAŻDEGO SERWISU UŻYJ INNEGO HASŁA

Ale jak? Przecież sklepów, social mediów i innych portali mam około 400-tu…

Zmień je następnym razem jak będziesz się tam logował :)

Ale gdzie je zapisać?

Użyj menedżera haseł

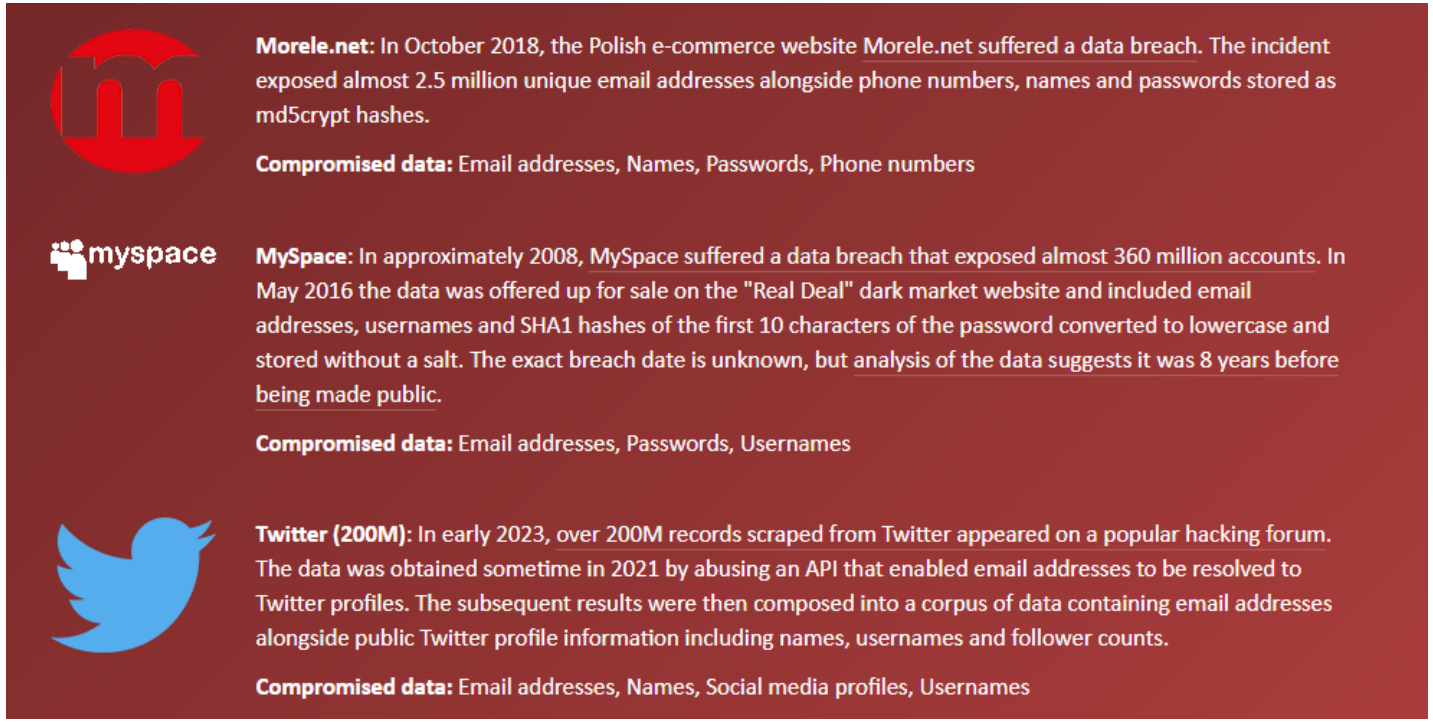
Nie ważne jakiego menedżera użyjecie, ważne żeby dostęp do niego był jak najbardziej utrudniony (trudne hasło, które zapamiętacie, zapiszecie na kartce i włożycie do sejfu ;) i najlepiej jak będzie jeszcze zabezpieczony 2FA). To może być na przykład:

- Bitwarden (online) – https://bitwarden.com/
  - Jest banalnie prosty w obsłudze
  - Jest darmowy
  - Ciągle rozwijany
  - Ma wtyczki do każdej przeglądarki
  - Ma aplikację na każdego smartfona
  - Instrukcja w języku polskim - https://sekurak.pl/jak-uzywac-bitwarden-a-kompleksowy-poradnik-uzywania-tego-bezplatnego-menadzera-hasel/
  - Filmik w języku angielskim - https://www.youtube.com/watch?v=30QqIeb1Pu4
- Google Chrome (online) – pamiętaj, że jak ktoś przejmie twojego smartfona to ma dostęp do haseł
- Mozilla Firefox (online)
- Apple'owy keychain (pęk kluczy) – całkiem dobra opcja dla posiadaczy iOS i Maców
- KeePass (offline) – dla entuzjastów IT i lekkich masochistów ;)

Czy można gdzieś sprawdzić czy mój e-mail, adresy, hasła mogły wyciec?

Można to zrobić w serwisie
https://haveibeenpwned.com/

Niestety nie dowiecie się jakie to były hasła i czy zostały złamane, ale uzyskacie informacje co się wydostało w takim wycieku.



P.S.

Zauważcie, że w wycieku z morele.net wyciekły hasła, które zostały zabezpieczone w bazie danych właśnie najprostszym algorytmem hashującym md5 ;)

Dla ciekawskich:

Dlaczego nie powinno się używać algorytmu md5, możesz przeczytać tutaj (wymagany angielski):

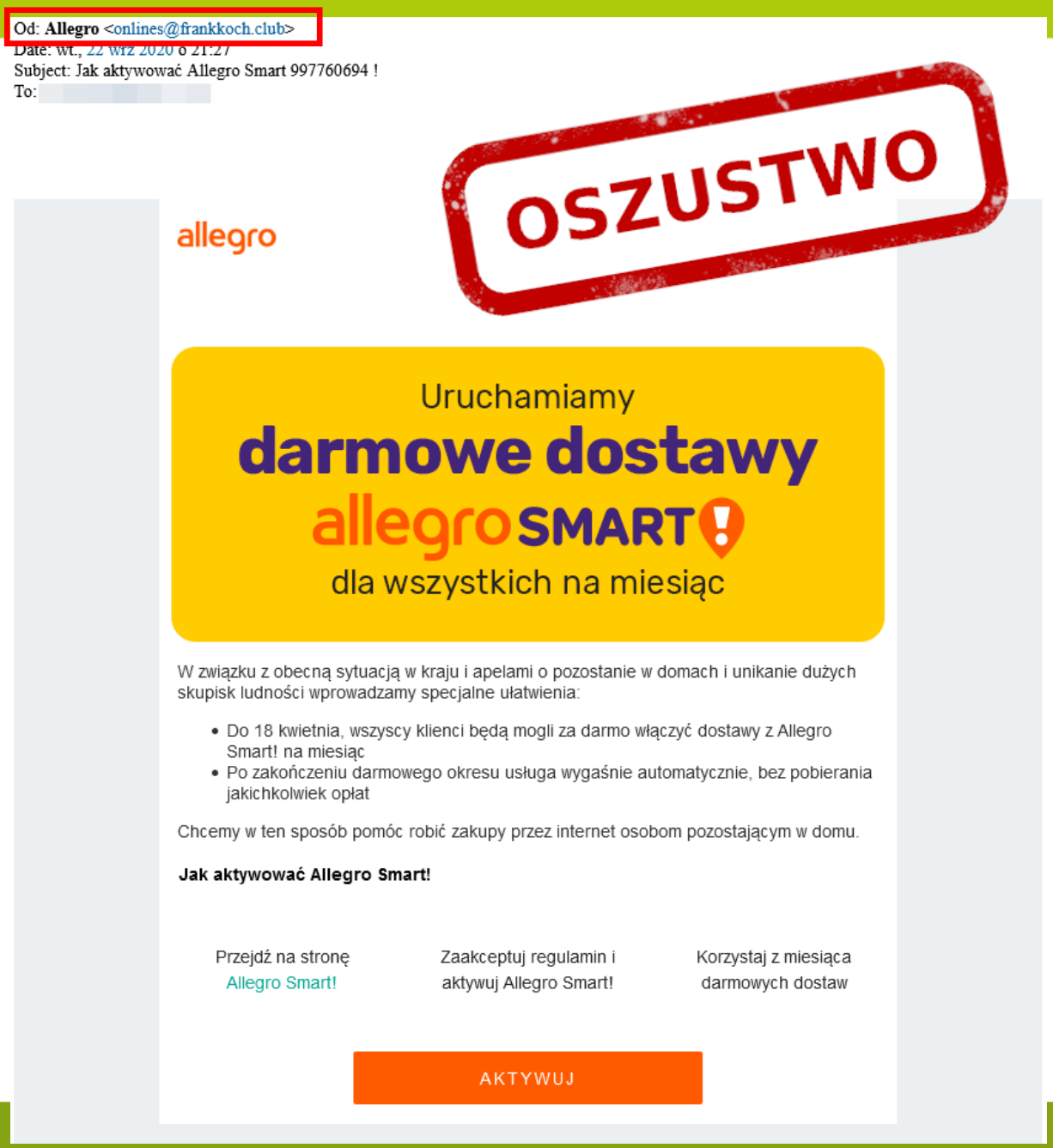
https://www.okta.com/identity-101/md5/

W skrócie: ponieważ jest za prosty.

Związek Harcerstwa Polskiego

Phishing – czyli idziemy łowić najwolniejszych w stadzie

Materiały znalezione na: https://kwestiabezpieczenstwa.pl/phishing/



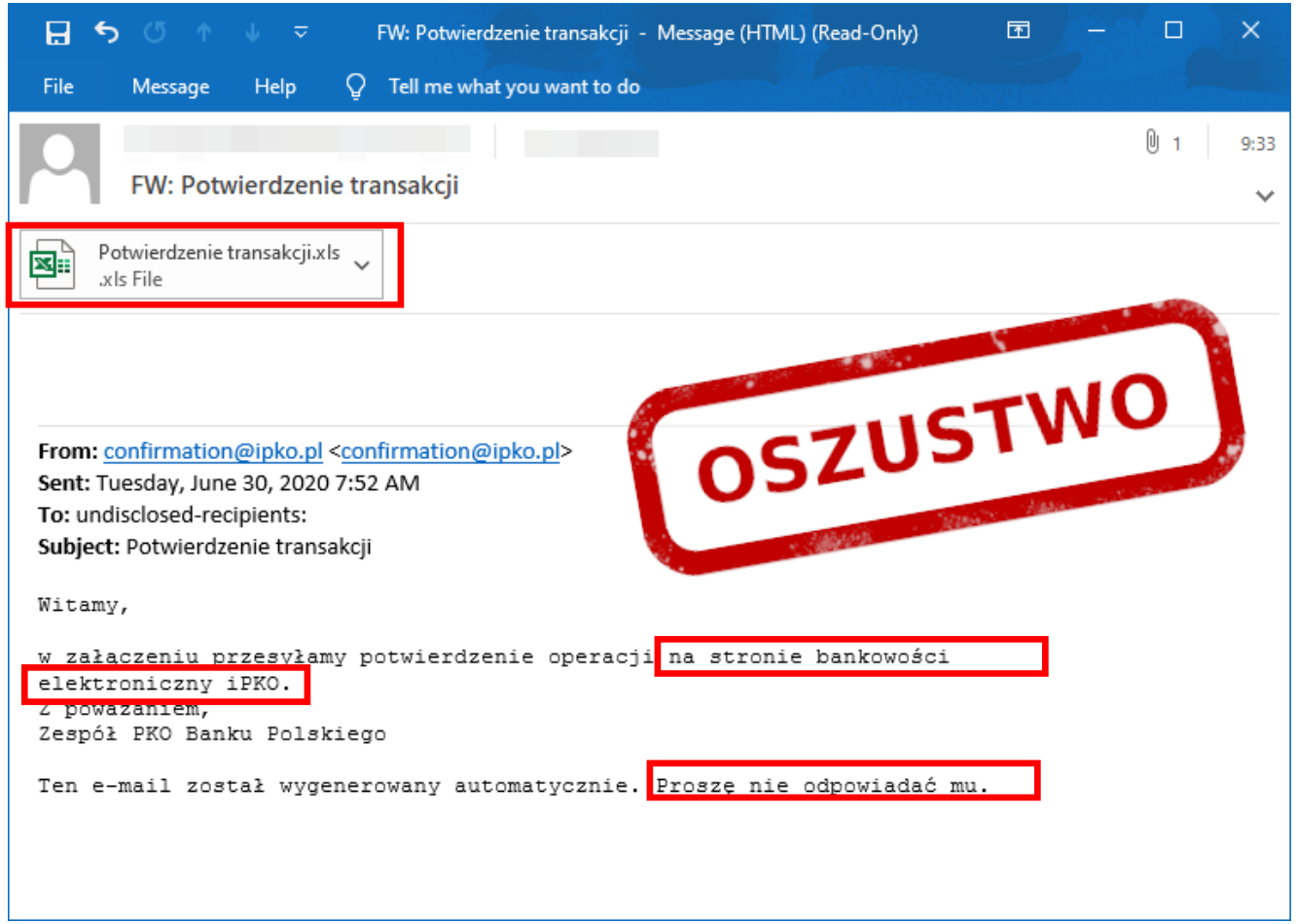
Phishing polega na:

- Wysłaniu do was fałszywego (zespoofowanego) maila lub SMSa
- Fałszywym telefonie z takich instytucji jak na przykład:
  - Działu bezpieczeństwa banku
  - Policji
  - Cyber Prokuratury (moje ulubione ;))
  - BIKu

W przykładzie po lewej macie fałszywego maila, którego możecie rozpoznać po tym, że przyszedł z adresu: onlines@frankkoch.club co widać w lewym górnym rogu.

Sama treść jest idealnie skomponowana i obrandowana dokładnie w takim sam sposób jak robi to Allegro.

Zauważcie też, że nazwa nadawcy to **Allegro**. Jeśli nie sprawdzicie jaki był adres nadawcy, który znajdziecie między znakami „< >”, to możecie się łatwo nabrać.



W tym mailu już nie jest tak prosto. Mail przyszedł niby z adresu: confirmation@ipko.pl.

Domena **ipko.pl** to oficjalna domena PKO BP. Więc wygląda na to, że jest to prawdziwy mail, pytanie jak rozpoznać, że może być fałszywy?

1. Potwierdzenia transakcji raczej nie przychodzą w plikach *.xls
2. Sam mail zawiera błędy gramatyczne:
    1. Na stronie bankowości elektroniczny PKO – powinno być „Na stronie bankowości **elektronicznej** PKO”
    2. Proszę nie odpowiadać mu – powinno być „Prosimy na niego nie odpowiadać”

No dobra, ale przecież w przykładzie z Allegro mail był idealnie podrobiony i co wtedy? Mamy dwa wyjścia:

1. Możemy zadzwonić do banku, albo zalogować się na nasze konto i sprawdzić czy jakaś nieautoryzowana transakcja miała miejsce.
2. Możemy sprawdzić nagłówki wiadomości e-mail. Tutaj polecam artykuł niebezpiecznika: https://niebezpiecznik.pl/post/jak-namierzyc-nadawce-falszywego-e-maila/

Czy trudno jest wysłać takiego maila z oficjalnej domeny na przykład Prezydenta Polski?

Jeśli myślisz, że wysłanie fałszywego maila z oficjalnej domeny jest trudne, to niestety muszę cię zmartwić. Jest sporo darmowych stron, które pozwalają to zrobić.

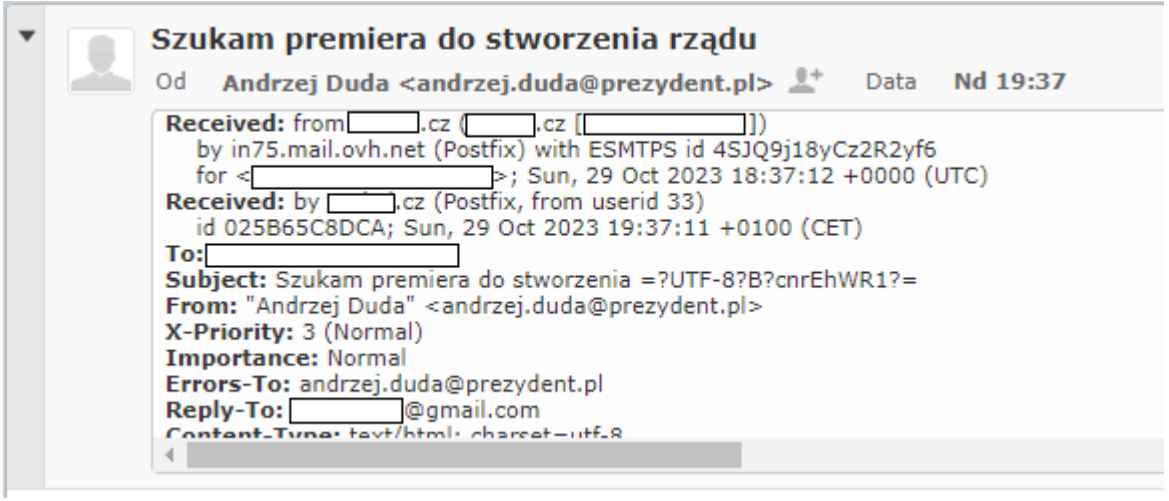
Na szczęście skrzynki dużych dostawców takich jak Microsoft czy Google, potrafią wyłapać maile z tych stron i je po prostu wyciąć, tak aby nawet do Ciebie nie dotarły.

Po prawej nagłówki takiego fałszywego maila z domeny **prezydent.pl**, który został wysłany z właśnie takiej darmowej strony.

Dane serwera, zostały zakryte ;) natomiast widać, że serwer pocztowy był z domeny **.cz**, a nie **prezydent.pl.**

Ponownie odsyłam do artykułu na temat nagłówków:

https://niebezpiecznik.pl/post/jak-namierzyc-nadawce-falszywego-e-maila/

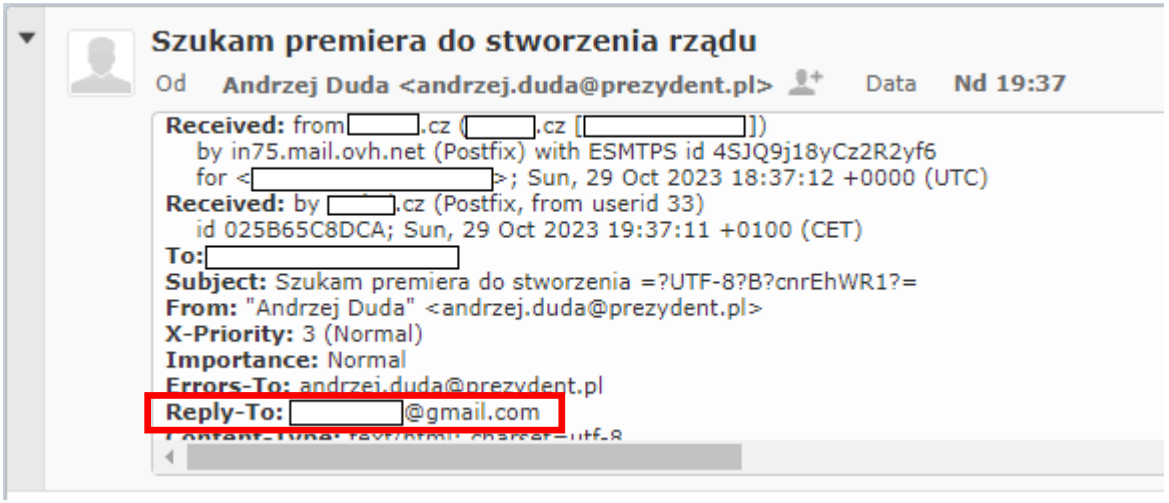


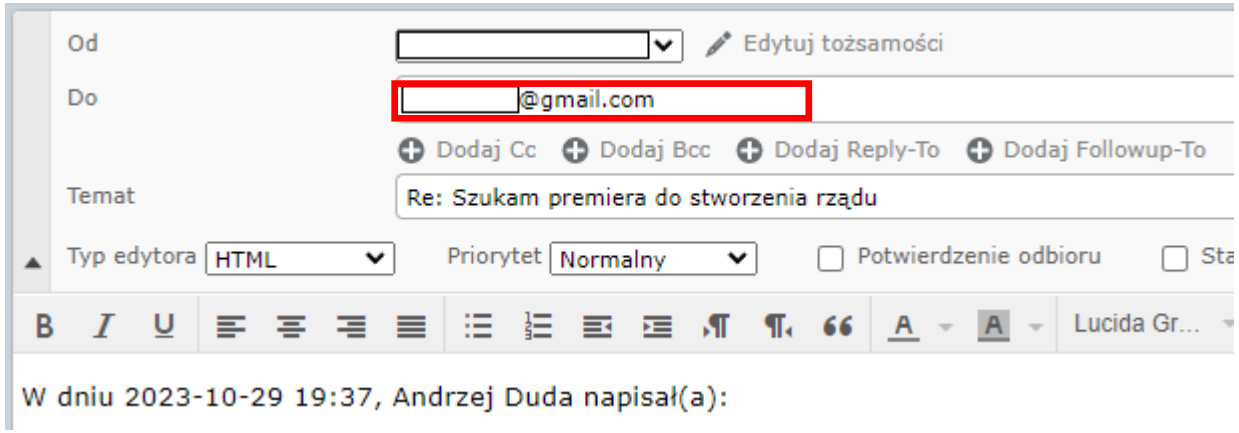
Czy da się to jakoś jeszcze zweryfikować oprócz sprawdzania nagłówków?

Tak! Chociaż nie zawsze.

Oszustom najczęściej nie zależy żebyście odpisywali do na przykład Prezydenta Polski, ponieważ to mogłoby spalić cały atak, dlatego ustawia się pole **odpowiedz do** (**Reply-To** – patrz po prawej).

Jeśli klikniecie „Odpowiedz na maila" to zobaczcie poniżej, że będziemy odpowiadać nie do Prezydenta tylko na jakiegoś maila w domenie **gmail.com**. To powinno zapalić wam lampkę ostrzegawczą, że coś jest nie tak.





Niestety nie zawsze, jest to oznaka że mail jest fałszywy bo:

1. Może to być mail z firmy marketingowej i po kliknięciu odpowiedz, pojawi się mail firmy docelowej (tak robi np. RTV Euro AGD)
2. Oszust mógł zostawić tam prawdziwy mail Prezydenta licząc, że na niego nie odpiszecie.

Inne pułapki w mailu

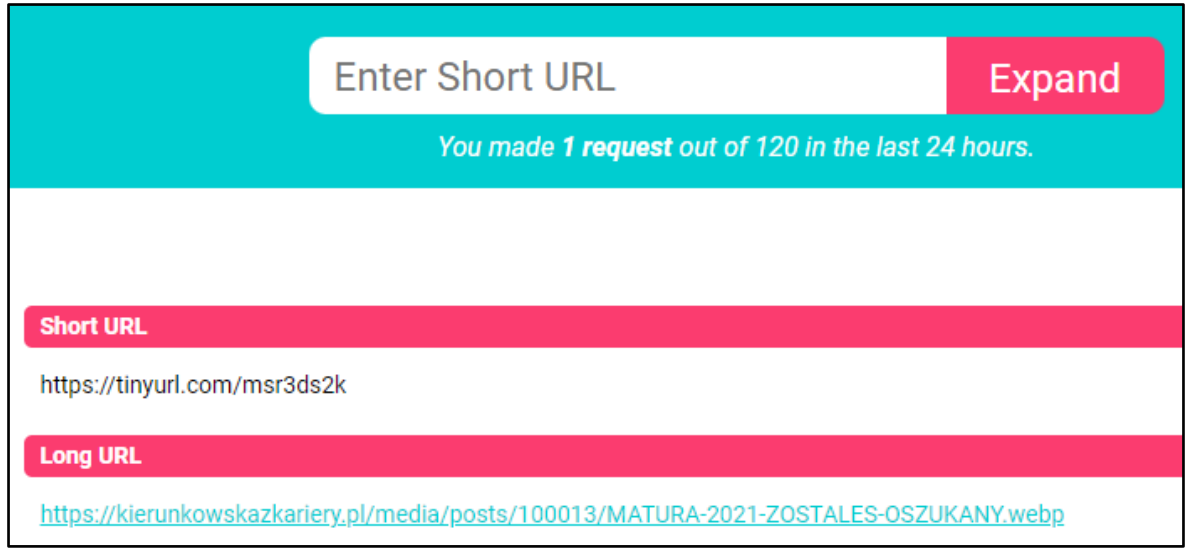
W mailach czyha na nas jeszcze jedna pułapka, czyli fałszywe linki. W każdej przeglądarce jesteście w stanie sprawdzić dokąd prowadzi link.

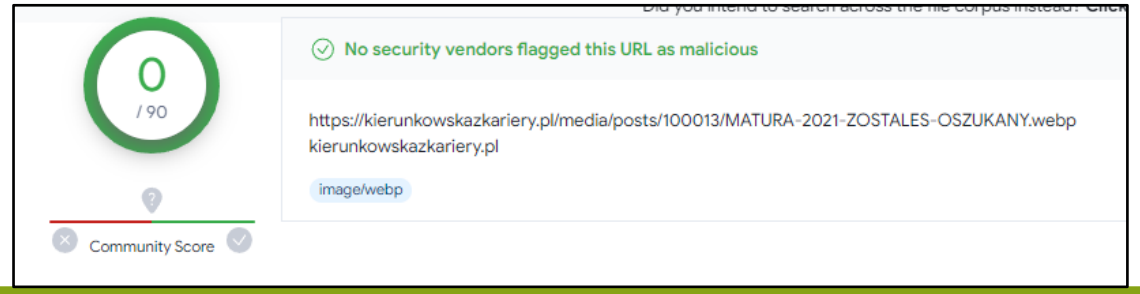
Wystarczy najechać na niego myszką, a w prawym lub lewym dolnym rogu pojawi się link docelowy. Niestety często ukrywa się docelowe strony w linkach skróconych zaczynających się od np.: **tinyurl.com**, **bit.ly** itd..

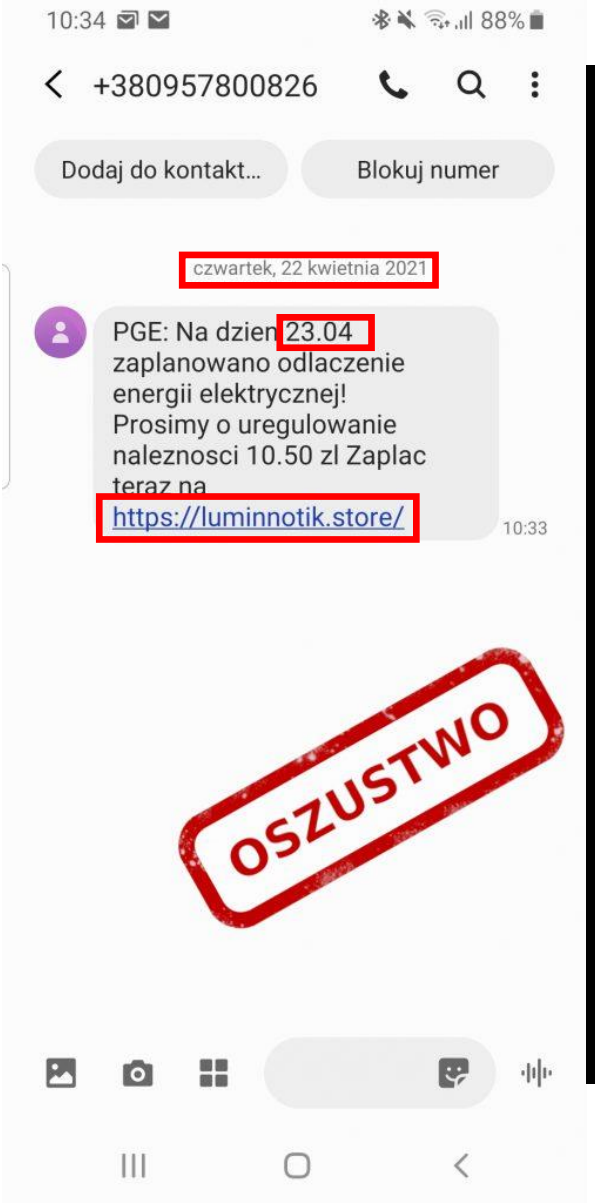
Na szczęście jest strona, która potrafi je rozszyfrować bez narażania nas na klikanie w te teoretycznie złośliwe linki. Wystarczy wejść na https://checkshorturl.com/, wkleić link i zobaczyć dokąd on prowadzi.

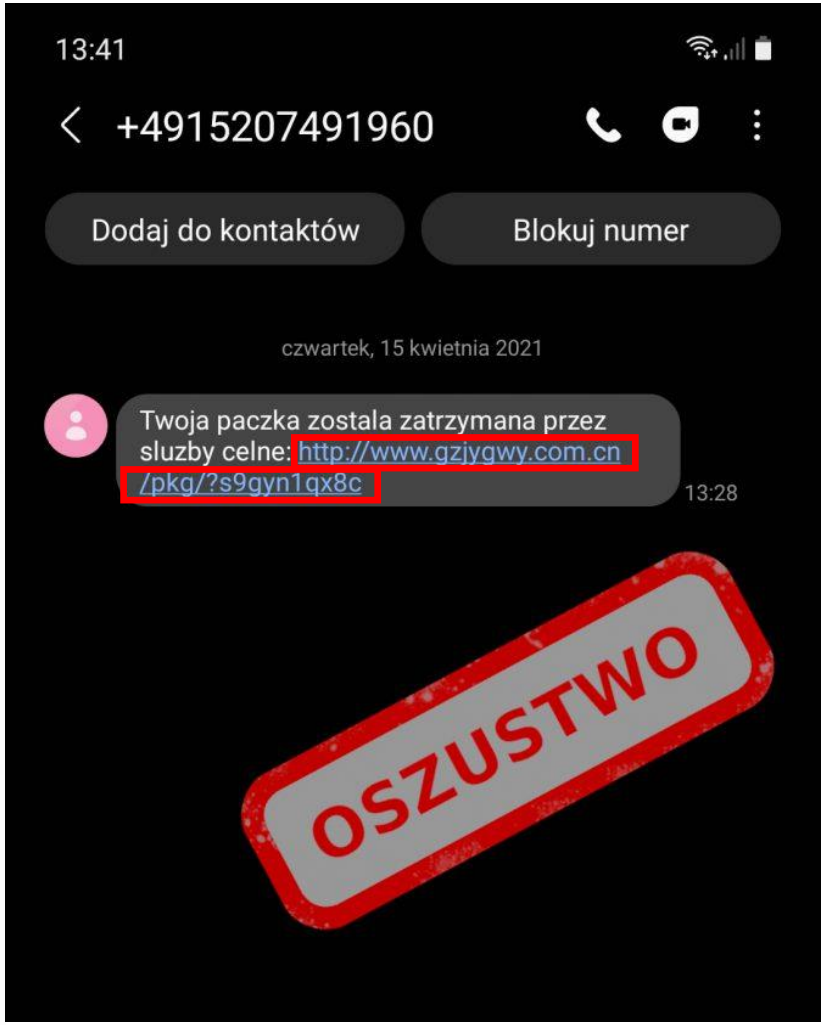
Żeby skopiować adres linku, kliknij na nim prawym przyciskiem myszy i wybierz **Kopiuj adres linku**.

Jeśli masz już docelowy adres i nadal nie jesteś pewny to wklej go na stronie https://virustotal.com/ wybierając opcję **URL,** ona sprawdzi czy nie ma tam złośliwych reklam lub kodu, albo czy strona nie została już gdzieś zgłoszona jako fałszywa.









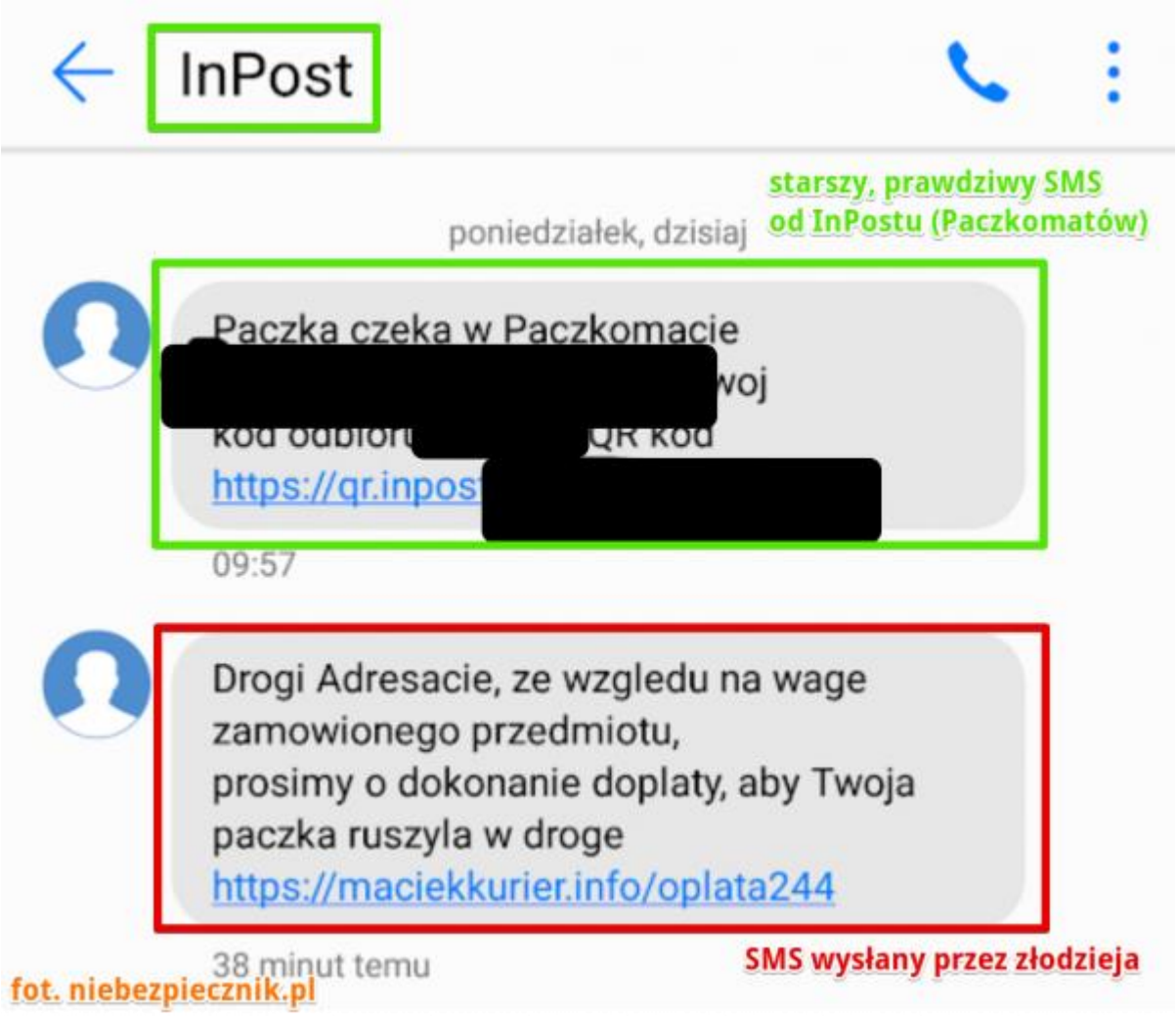
Po lewej mamy dwa przykłady fałszywych SMSów.

Zwróćcie uwagę, że pierwsze co robi się w takich SMSach to budowanie zagrożenia. Nie bez powodu „PGE" wysyła nam informację, że już jutro odłączą nam prąd (spójrzcie na daty), a w drugim SMSie jak nie zapłacimy to nie dostaniemy naszej wymarzonej paczki.

Zobaczcie też na numery kierunkowe. Polski numer kierunkowy to +48 i dziwnym trafem oba fałszywe zaczynają się od bardzo zbliżonych do niego +49 i +38 co w stresie można łatwo przeoczyć.

Druga sprawa to linki, których w SMSach na szczęście nie da się podrobić tak jak w mailach. Ciekawe czemu PGE używa strony **luminnotik.store** do płatności za faktury ;)

Pamiętaj, jeśli nie jesteś pewien czy informacja jest prawdziwa to zadzwoń do tej instytucji lub wejdź na swoje konto online. Tylko znajdź oficjalny numer na stronie internetowej, a nie oddzwaniaj na ten z SMSa :)



fot. niebezpiecznik.pl

Tutaj jest jeszcze gorzej, bo fałszywy SMS jest w tym samym wątku co SMS InPostu!

Tak, da się to zrobić i nie, nie jest to wcale takie trudne. Wystarczy znaleźć bramkę SMS, która pozwala nam podstawić nadawcę.

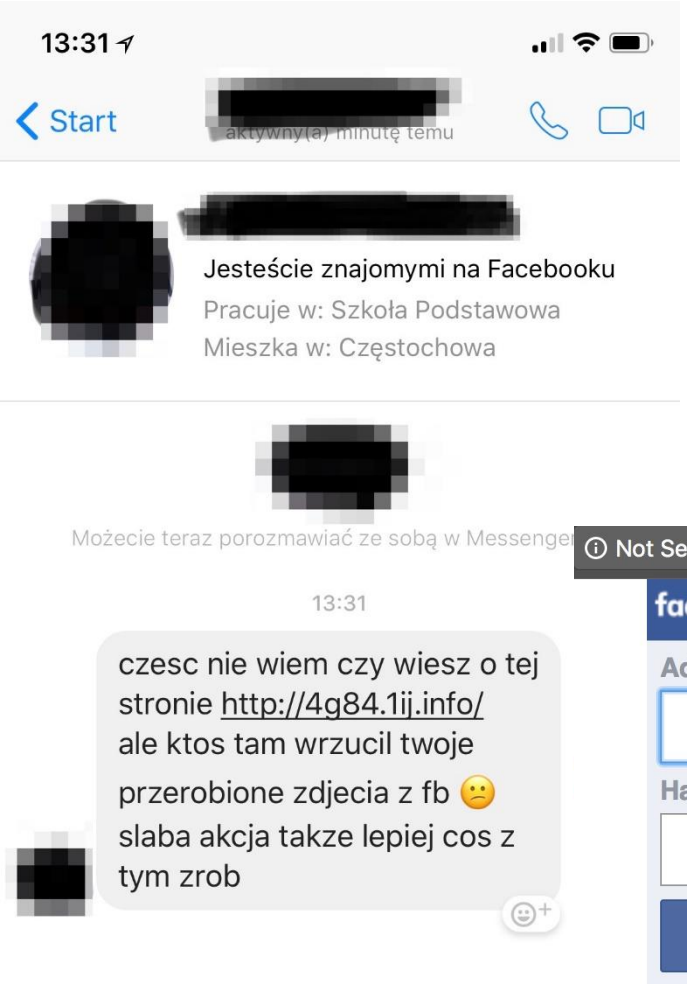
Tutaj znów zwróćcie uwagę na link, prowadzi on na stronę **maciekkurier.info**, a nie na oficjalną stronę InPostu.

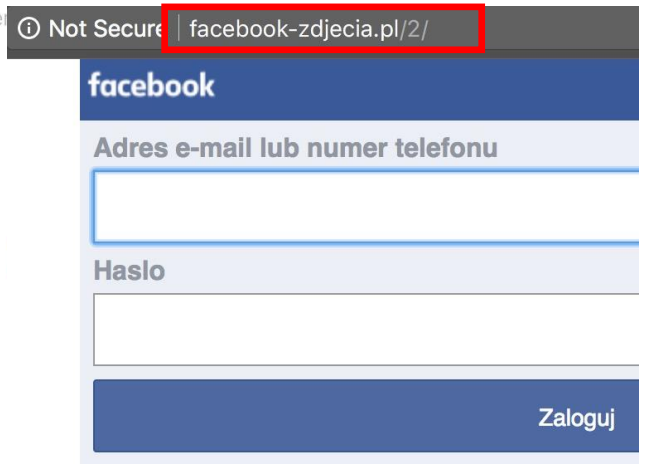
Dla ciekawskich:

Opis krok po kroku co się dzieje po kliknięciu w link ze złośliwego SMSa

https://niebezpiecznik.pl/post/uwaga-na-smsy-od-w-sprawie-przesylek/

Phishing na fejsie – typowe naciąganie na SMSy premium





Na pewno każdy z nas dostał kiedyś taką wiadomość od swojego znajomego. Jego konto zostało przejęte i automat rozsyła do jego znajomych łańcuszek, że niby znalazł jego przerobione foty na jakimś fanpejdżu.

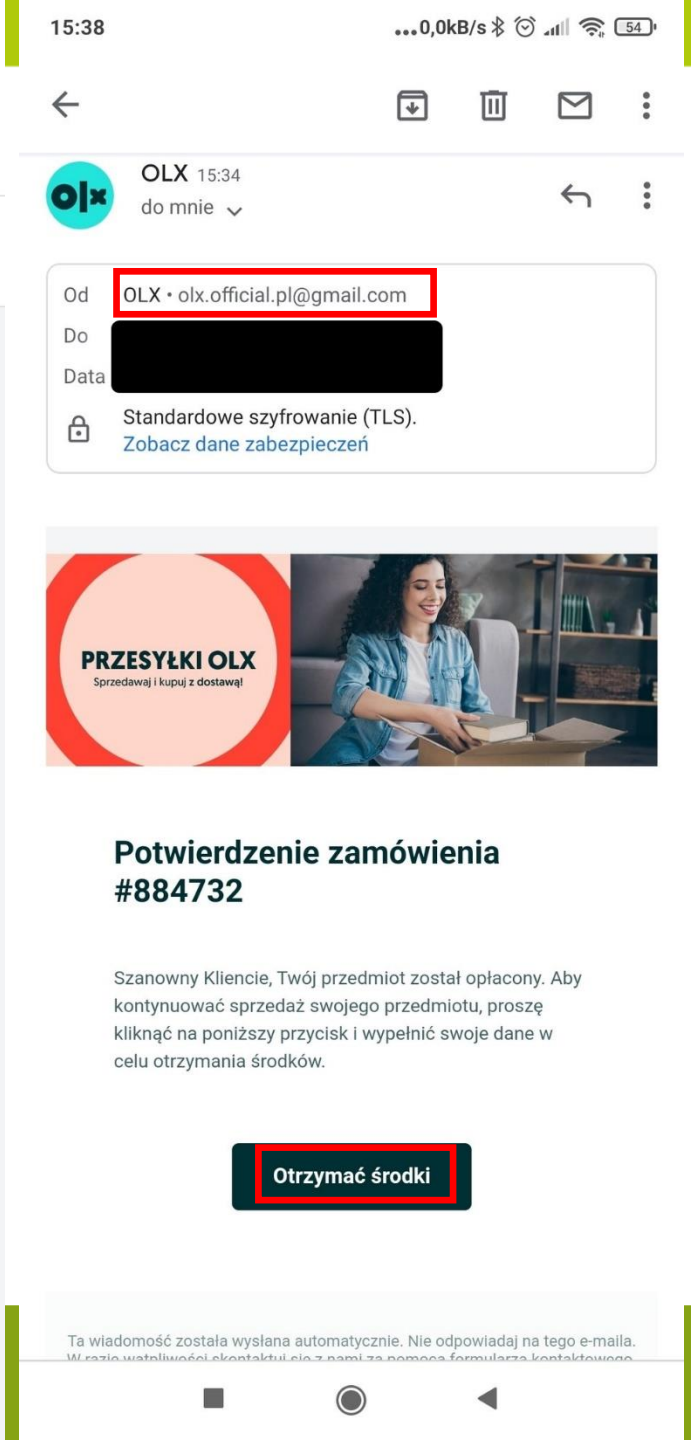
Tutaj mamy kolejne zastosowanie socjotechniki opierające się na budowaniu zagrożenia i ludzkiej ciekawości. Kto z nas nie chciałby usunąć swoich lub zobaczyć czyichś przerobionych fotek ;)

Po kliknięciu ukazywała nam się strona logowania do fałszywego facebooka i w taki sposób oszuści uzyskiwali dostęp do waszego konta. Zwróćcie uwagę, że strona to **facebook-zdjecia.pl**.

Dla ciekawskich:

Opis krok po kroku co się dzieje po kliknięciu w link

https://niebezpiecznik.pl/post/ktos-wrzucil-tu-twoje-przerobione-zdjecia-z-facebooka-uwaga-na-nowy-atak/



Istnieje też phishing na OLX lub Allegro.

Tutaj spójrzcie, że kupujący prosi was o wasz adres e-mail, bo OLX tego od niego wymaga.

Po pierwsze OLX nie wymaga od kupującego waszego adresu, bo już go ma. Po drugie ten adres e-mail, który OLX ukrywa przed kupującym jest im potrzebny do wysłania wam fałszywego maila.

Zwróćcie też uwagę na to jak te zdania są budowane, nikt normalny tak nie pisze. Na sam koniec koniecznie musimy się upewnić, że mail nie wylądował w SPAMie ;)

Mail oczywiście przychodzi z innego adresu niż z domeny olx.pl. Tutaj nawet nie było za dużego wysiłku bo jest to po prostu Gmail: **olx.official.pl@gmail.com**.

Dla ciekawskich:

Opis krok po kroku co się dzieje po kliknięciu w link

https://niebezpiecznik.pl/post/olx-scam-karta-platnicza/

Związek Harcerstwa Polskiego

Phishing na telefon

Przykład takiego scamu

https://www.youtube.com/watch?v=SbCcmLqmQSs

Podcast ogólnie o scamach i dlaczego się nabieramy

https://www.youtube.com/watch?v=IQL3YoZxNso

Phishing na telefon

Zadzwoń na mLinię

z aplikacji mobilnej
mLinia na klik, bez dodatkowych haseł

+48 42 6 300 800

To jest kadr z innego filmu pokazującego phishing na telefon. Spójrzcie, że wyświetlany numer to oficjalny numer mLinii z mBanku!

Tak da się podszyć pod nawet wasz numer. Są strony, które to umożliwiają za kilka euro/złotych.

Na szczęście jak oddzwonicie to połączycie się z bankiem

Dla osób technicznych:

Gdyby ktoś był zainteresowany dlaczego można się podszyć pod czyiś numer, to więcej informacji można znaleźć tutaj:

https://niebezpiecznik.pl/post/spoofing-rozmow-telefonicznych/

lub posłuchać podcastu:

https://www.youtube.com/watch?v=ucALPEjBAKo

Phishing

Phishing zazwyczaj będzie się opierał na:

1. Dopłacie do paczki
2. Nieopłaconej fakturze od dostawcy usług – jeszcze zaraz na konto wejdzie komornik
3. Nowej umowie od dostawcy prądu/wody itd..
4. Przelewie z dziwnego miejsca, który został dobrodusznie zablokowany przez bank
5. Nieautoryzowanej wypłacie z konta w innym kraju
6. Telefonie z BIKu, że ktoś wziął pożyczkę na nasz dowód
7. Nigeryjskim księciu/prawniku itd.. – https://cert.pl/posts/2023/02/nigerian-scam/ i https://pl.wikipedia.org/wiki/Nigeryjski_szwindel
8. Albo Michaelu Jacksonie, który jednak żyje i brakuje mu 600 dolców, żeby wrócić do USA aby mógł nagrać nowe piosenki

Swoją drogą, było kilka scamów opartych na postaci Brada Pitta:

https://www.antyradio.pl/news/Brad-Pitt-zostal-oskarzony-o-wyludzenie-150-tysiecy-zlotych-Sad-wydal-wyrok-w-sprawie-aktora-44774

https://english.elpais.com/spain/2023-06-30/fake-brad-pitt-scams-180000-from-middle-aged-woman-in-spain.html

A Michael Jackson niestety już nie wróci, nawet jeśli napisał do was z konta o nazwie „**therealmichaeljackson1111**"

Phishing na bliczka

Jeśli napisze do was znajomy o blika, to zadzwońcie do niego i się upewnijcie, że to on. Jak już wiecie przejęcie konta na facebooku nie jest takie trudne, wystarczy wpisać swój login i hasło w złym miejscu.

Czy poza SMSami premium i tysiakiem na blika, możemy stracić coś więcej?

Na przykład jeśli ktoś pozbiera sobie informacje takie jak:

1. PESEL
2. Nr telefonu
3. Nazwisko panieńskie matki
4. Nr dowodu osobistego

To może:

1. Zadzwonić do operatora i poprosić o przekierowanie rozmów na inny numer lub wyrobi sobie dowód kolekcjonerski i pójdzie do salonu, gdzie wyrobi duplikat twojej karty SIM.
2. Zainstaluje aplikację bankową i żeby się uwierzytelnić to bank będzie potrzebował do niego zadzwonić/napisać SMSa z kodem. A jak wiemy wszystkie rozmowy zostały przekierowane na inny numer
3. Tym samym od tego momentu ma pełną kontrolę nad twoim kontem bankowym

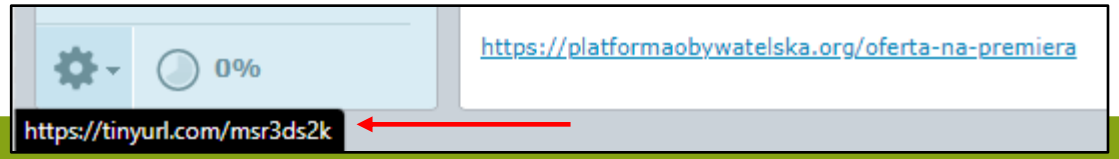
https://niebezpiecznik.pl/post/duplikat-karty-sim-kradziez-bank-mbank-bzwbk/

Co nas gubi?

1. Pośpiech – chcesz wyjść z pracy bo jest 15:58 w piątek, a prezes kazał ci wykonać na cito ekspresowy przelew do jakiegoś kontrahenta na pół miliona złotych
2. Zmęczenie – jak myślisz dlaczego najwięcej maili i SMSów przychodzi w godzinach wieczornych, albo gdy kończysz pracę?
3. Stworzenie iluzorycznego zagrożenia – komornik, policja, prokuratura, kredyt na ogromne pieniądze itd..
4. Chaos – robisz obiad, dziecko płacze i jeszcze dzwoni ktoś z banku, że poszedł z twojego konta przelew do innego kraju typu Chiny, Pakistan czy Indie.

Jak nie wpaść?

1. Telefon – jeśli dzwoni do was ktoś z banku/policji/innej instytucji i zaczyna prosić o jakieś dane to rozłączcie się i oddzwońcie tam sami, ale na oficjalny numer znaleziony na stronie internetowej
2. SMS – jeśli widzicie, że link nie należy do domeny firmy, która do was pisze to nie klikajcie w niego. Żaden kurier nie będzie chciał od was dopłaty bo paczka była za ciężka. Zawsze możecie też zadzwonić na infolinię i zweryfikować te informacje.
3. Fejs – jeśli pisze do was znajomy i prosi o hajs, to zadzwońcie do niego i upewnijcie się, że to faktycznie on.
4. Chroń swoje dane osobowe, nie podawaj ich tam gdzie nie musisz.
5. Uspokój się i zacznij sprawdzać:
    1. Czy nie ma błędów ortograficznych/gramatycznych w wiadomości
    2. Czy link posiada domenę dostawcy usług
    3. Czy link faktycznie prowadzi tam gdzie powinien - można to sprawdzić najeżdżając na niego myszką



Jak sprawdzić linki? - przypominajka

- https://checkshorturl.com/- możesz zobaczyć co kryje się pod takim skróconym linkiem
- https://www.virustotal.com/ - możesz sprawdzić tutaj nie tylko linki, ale też pliki

Związek Harcerstwa Polskiego

Czy sieci WiFi mogą być niebezpieczne?

Czy sieci WiFi mogą być niezbezpieczne?

20 lat temu, tak.

Dzisiaj wszystkie strony używają HTTPSa (zielonej kłódki) i cały ruch jest szyfrowany.

Nawet jeśli ktoś ten ruch przechwyci to nic z niego nie odczyta.

W zasadzie są tylko dwa odstępstwa od powyższej reguły:

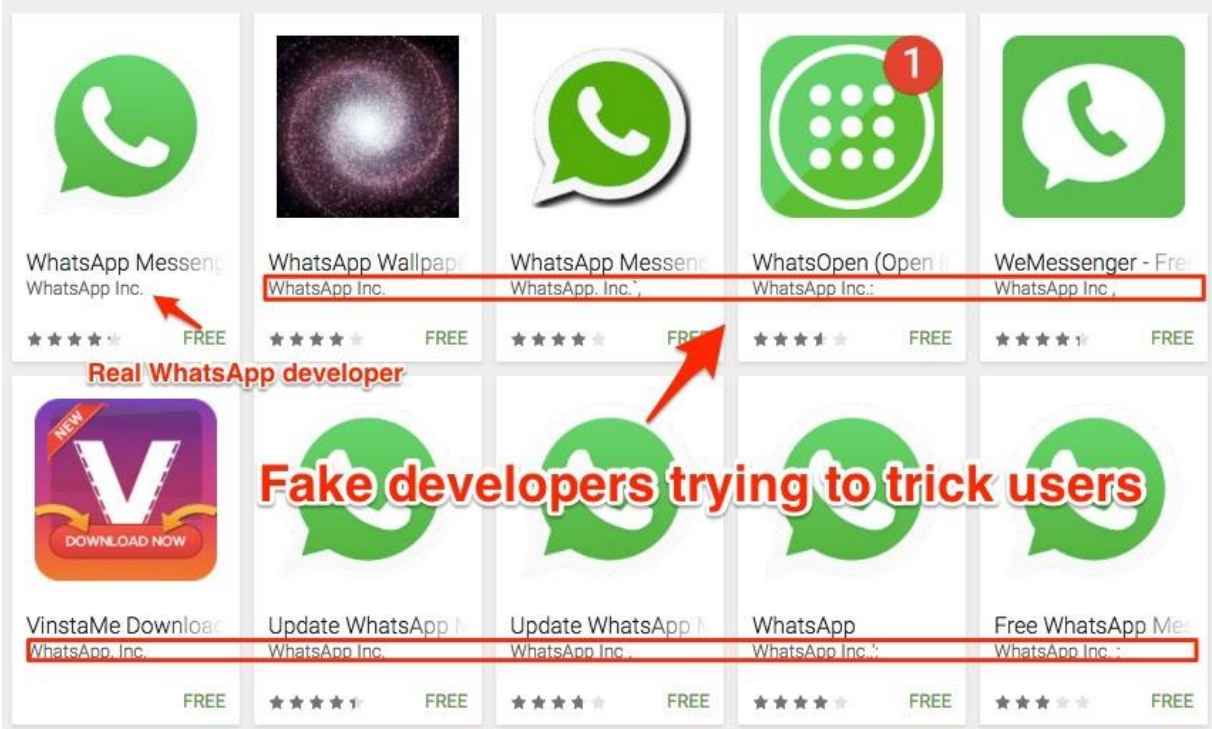
1. Kiedy sieć jest całkowicie otwarta bez żadnego hasła – wtedy w promieniu 200 metrów każdy wie co robimy i na jakie wchodzimy strony. Nadal nie zobaczy co tam wpisujemy ale prawdopodobieństwo ataku rośnie
2. Kiedy przy użytkowaniu sieci musimy przeklikać formularz i proszą nas o dane osobowe, albo dane naszej karty płatniczej – te formularze często są nieszyfrowane i tutaj już ktoś może przechwycić taką komunikację

P.S. polecam używać sieci komórkowej, jest o wiele bardziej bezpieczna.

Związek Harcerstwa Polskiego

Pozostałe zagrożenia

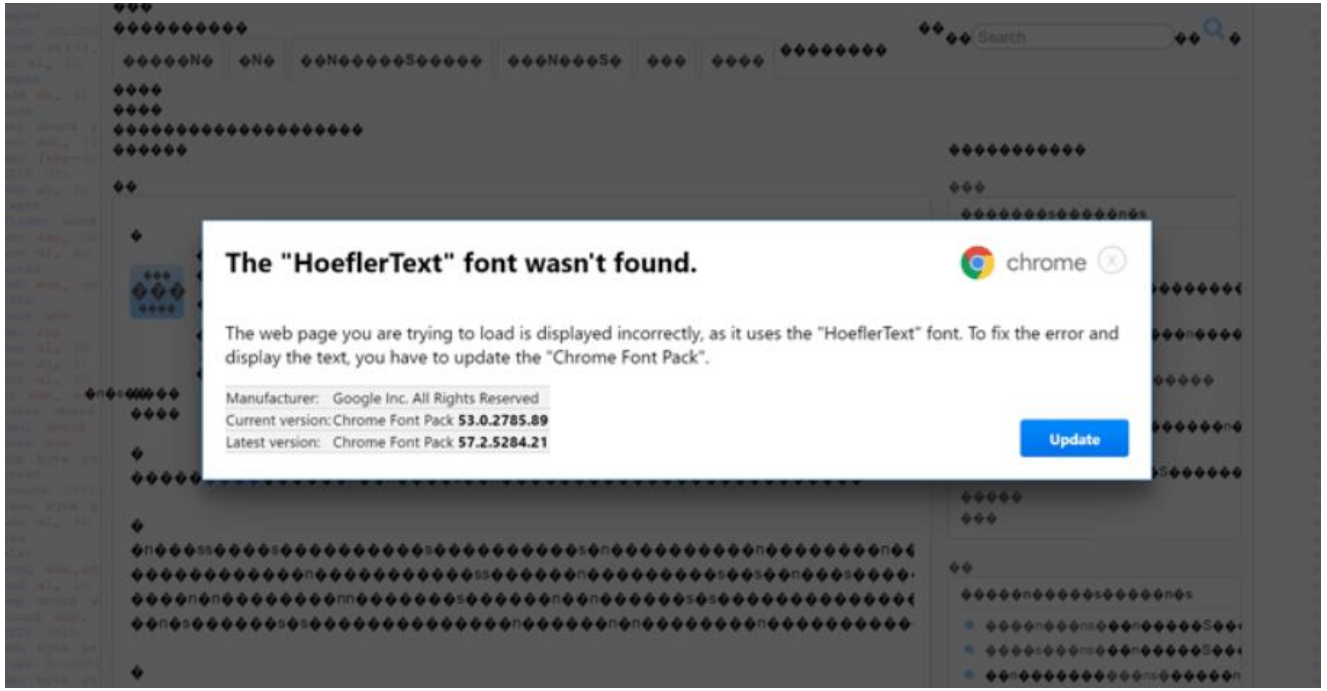
Złośliwe aplikacje



Najwięcej tego typu aplikacji jest w sklepie Google Play. Dlatego, że Google nie wymaga za dużej weryfikacji treści i udostępnianie tam aplikacji jest darmowe.

W sklepie Apple problem jest minimalny, ponieważ trzeba tam zapłacić za udostepnienie swojej aplikacji i do tego musi ona spełniać pewne normy.

Brakujące czcionki



Znacie ten moment kiedy szukacie od dwóch godzin instrukcji do waszej pralki, która jest produkcji chińskiej i w końcu znajdujecie ją na dziesiątej stronie Google, po czym okazuje się że nie macie czcionki?

Instalacja takiej „czcionki” może zakończyć się zainstalowaniem złośliwego dodatku do waszej przeglądarki, który będzie przesyłał do oszustów wszystko co wpiszecie na klawiaturze. Albo co gorsza przejmie wasze konto Google razem z mailem i hasłami jeśli je tam trzymacie.

Taniej wyjdzie kupić nową pralkę ;)

Fałszywe transmisje z wydarzeń sportowych – za darmo!

Podobnie jak z czcionką, jeśli szukacie darmowego streamu z olimpiady albo mistrzostw świata i w końcu znajdujecie taką stronę, ale nagle chce ona zainstalować jeden mały dodatek do waszej przeglądarki bo inaczej nic nie wyświetli. To wyłączcie ją i zapłaćcie za dostęp do oficjalnych transmisji.

Strona może i jest darmowa, ale płacicie waszym bezpieczeństwem i dostępem do waszych kont.

Złośliwe QR Kody

Jak myślisz, czy ciężko jest wydrukować taką samą kartkę jak na zdjęciu i umieścić ją gdzieś w autobusie/tramwaju, ale ze złośliwym QR kodem? Albo umieścić taki QR kod w wiadomości e-mail czy w załączniku z „fakturą” za prąd?

Zamiast skanować nieznane kody QR po prostu przepisz ten kod do aplikacji lub wejdź na stronę dostawcy usług i zapłać faktury przez stronę.

https://niebezpiecznik.pl/post/atak-na-parkomaty-w-krakowie/

https://niebezpiecznik.pl/post/qrishing-trudniej-go-wykryc-i-rzadziej-sie-przed-nim-ostrzega/

Aplikacje, które chcą za dużo uprawnień

Latarka, która nagle chce mieć dostęp do: kontaktów, zdjęć, plików, lokalizacji itd..
To nie jest normalna latarka ;)

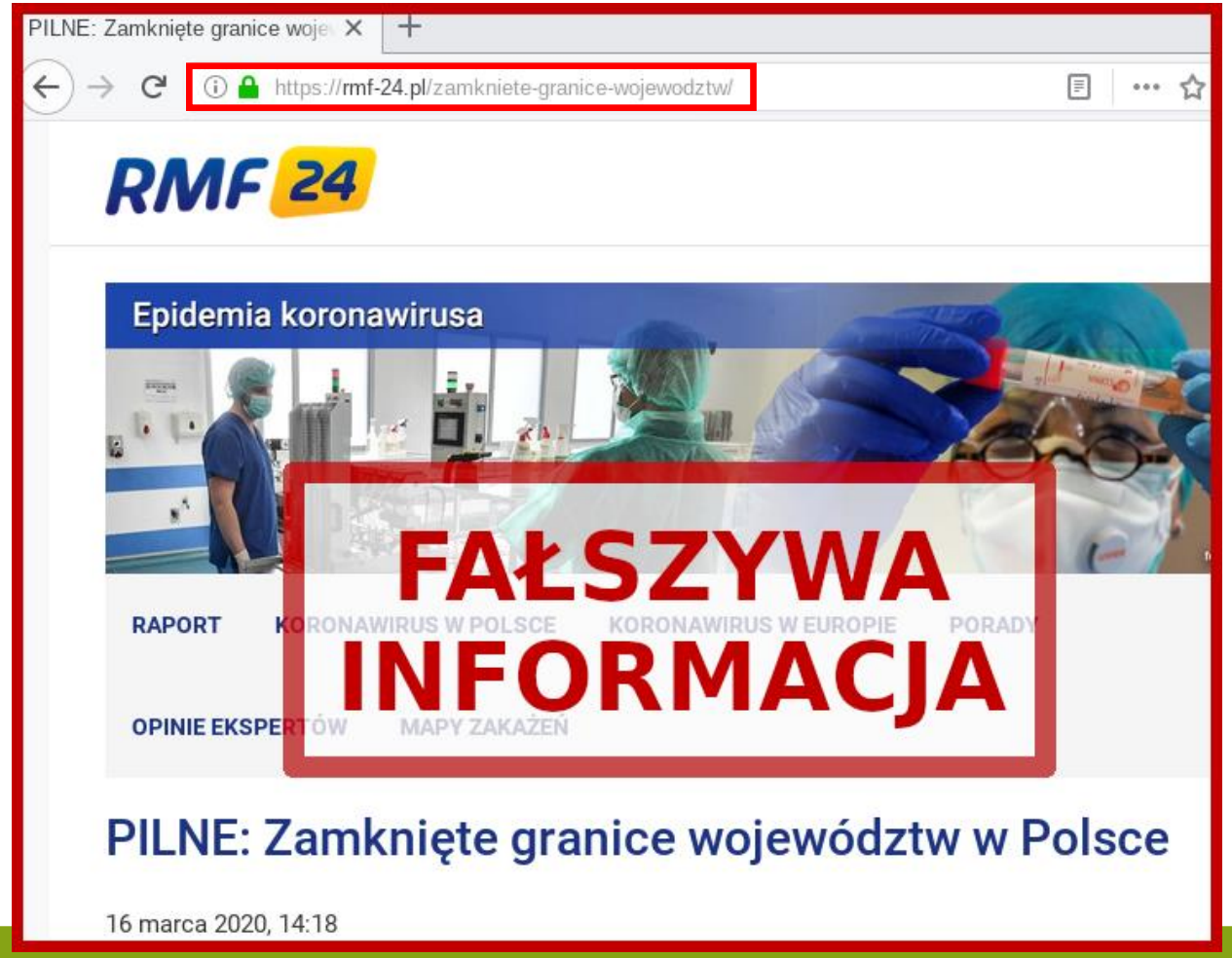
Znalezione pendrive'y

Nigdy nie wkładaj znalezionego pendrive'a do swojego komputera. Jeśli nikt się do niego nie przyznaje to po prostu go wyrzuć.

Dlaczego?

1. Pendrive będzie zawierał zawirusowane pliki, które po uruchomieniu będą wykradać wszystko co wpiszecie na klawiaturze.
2. Będzie to tak zwana gumowa kaczuszka, która po podpięciu zamienia się w klawiaturę i w mgnieniu oka bez waszej wiedzy przejmuje kontrolę nad waszym komputerem - https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/falszywy-hakerski-pendrive-stal-sie-jeszcze-grozniejszy-jest-jeden-sposob-zeby-sie/7l4v3re
3. Ktoś dla zabawy podrzucił Ci USB killera - https://www.youtube.com/watch?v=BhGit8mz7LQ Mało prawdopodobne, ale ciekawostka ;)

Zielona kłódka, która nie gwarantuje bezpieczeństwa i prawdziwych informacji



Po lewej fałszywa strona RMF24, zwróćcie uwagę, że jest zielona kłódka, połączenie jest szyfrowane, a sama strona wyglądem nie wzbudza podejrzeń.

Problem w tym, że oficjalna strona RMF24 to **rmf24.pl**, a nie **rmf-24.pl**

Związek Harcerstwa Polskiego

Podsumowując

DO KAŻDEGO SERWISU UŻYJ INNEGO HASŁA

P.S. pamiętaj o menedżerze haseł ;)

I zmień hasło do domowego WiFi!

Zablokuj SMSy premium

P.S. więcej informacji pod tym linkiem:

https://niebezpiecznik.pl/post/nie-daj-sie-naciagaczom-zablokuj-uslugi-premium-rate-radzimy-jak-to-zrobic/

Czytaj uważnie linki i patrz dokąd prowadzą

P.S. pamiętaj, że po najechaniu na link myszką, pojawi ci się w dolnym prawym lub lewym rogu prawdziwy link

Zanim otworzysz załącznik zastanów się dwa razy czy jest prawdziwy

P.S. jak zobaczysz, że excel potrzebuje uruchomić makra to od razu go zamknij

Jeśli nie jesteś pewien rozmówcy, to się rozłącz i oddzwoń na oficjalny numer

P.S. pamiętaj, że można się podszyć pod każdy numer telefonu

Zielona kłódka nie gwarantuje, że strona nie jest złośliwa i zawiera prawdziwe informacje

Usuń ze swojego maila wiadomości w których są skany dowodów, umowy, umowy kredytowe itd. Wszystko w czym mogą znajdować się twoje dane osobowe.

Jeśli kiedyś stracisz nad nim kontrolę to przynajmniej nie stracisz swoich danych i utrudnisz oszustowi życie.

Związek Harcerstwa Polskiego

Bądźcie bezpieczni! :)

phm. Grzegorz Wąs