Nie daj się cyberzbójom! v2.0

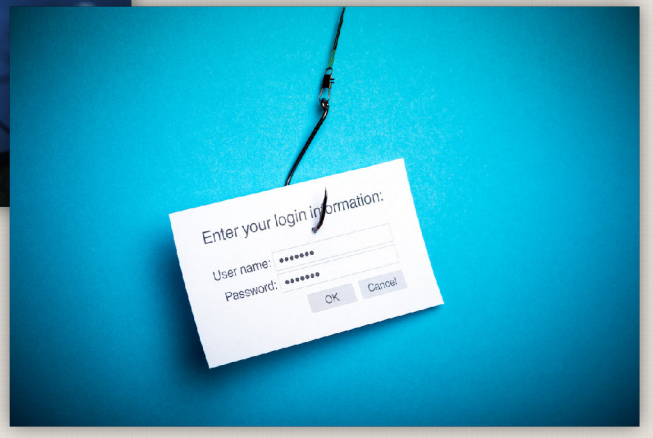
Podsumowanie prezentacji

michal.sajdak@securitum.pl
@sajdoor

Phishing

wykradanie danych

próba zainfekowania komputera



Sprawdź adres nadawcy e-maila, a nie jego nazwę

Od: "[redacted]" <amaia@dionisioormazabal.com>
Do: undisclosed-recipients:;
Data: 2022-09-11 23:17
Temat: Biznes.gov.pl - NOWE POWIADOMIENIE

DEMO

Nie klikaj w linki w e-mailach "bankowych"

Pamiętaj, że link może prowadzić do innego miejsca niż sugeruje jego nazwa

Aktywuj usługę:

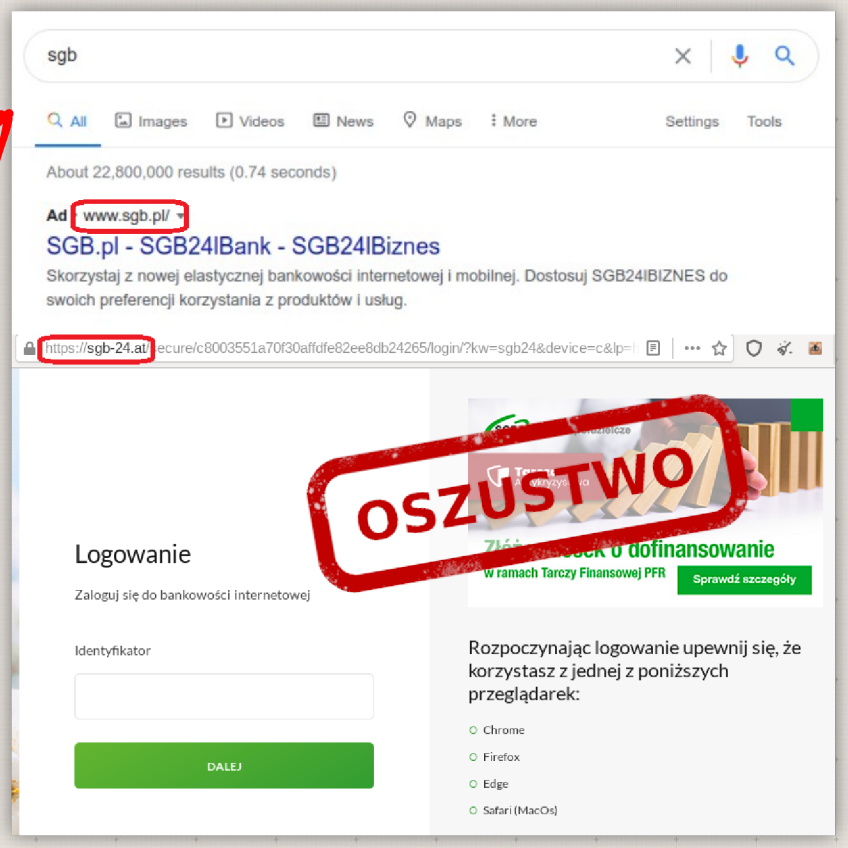
https://goonline.bnpparibas.pl/

1. Zidentyfikuj się za pomocą swoich danych bankowych.
2. Wpisz kod wysłany do Ciebie SMS-em na numer telefonu podany w Twoim banku.

https://anacetina.com/readme.php

Na strony bankowe wchodź
"ręcznie" lub z zakładek

stworzenie nowej zakładki:
ctrl+d w przeglądarce



nie używaj google
do wchodzenia na stronę swojego banku

Uważaj na załączniki przesyłane w e-mailu

wyciag-bankowy-pdf.vbs

wyciag-bankowy.pdf.exe

wyciag-bankowy.pdf

To najpewniej jest malware/wirus

DEMO


Witam,
Dobry dzień panu,

Mam nadzieję, że dzisiaj wszystko w porządku.
Mój kolega Pan Dawid Krawiec wysłał Państwu nasze zamówienie PO-Eu598303 w zeszłym tygodniu, ale jeszcze nie otrzymaliśmy od Państwa odpowiedzi.
Tutaj znów cię wysyłam. Prosimy o dostarczenie faktury proforma zgodnie z załączonym zamówieniem PO-Eu598303.

Mamy nadzieję, że niedługo się odezwiesz.

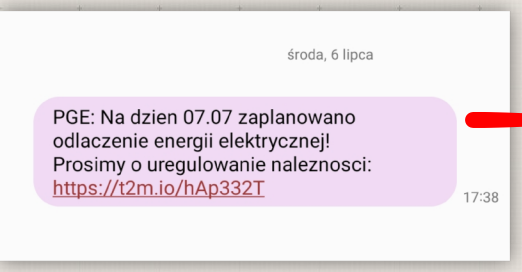
PDF

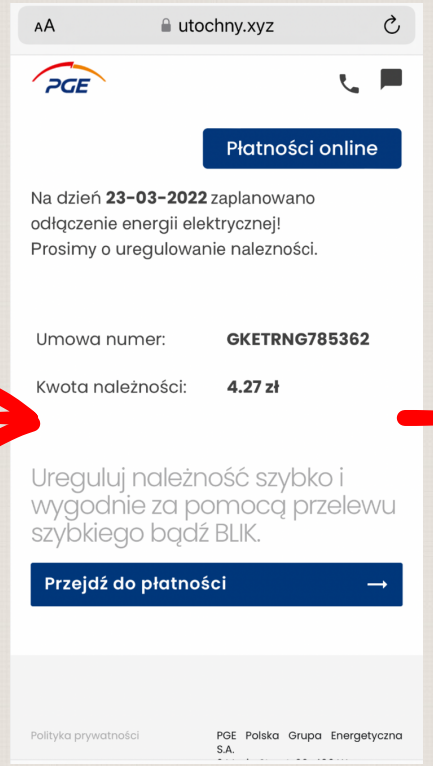
Zamowienie_zakupu_PO-Eu598303.pdf

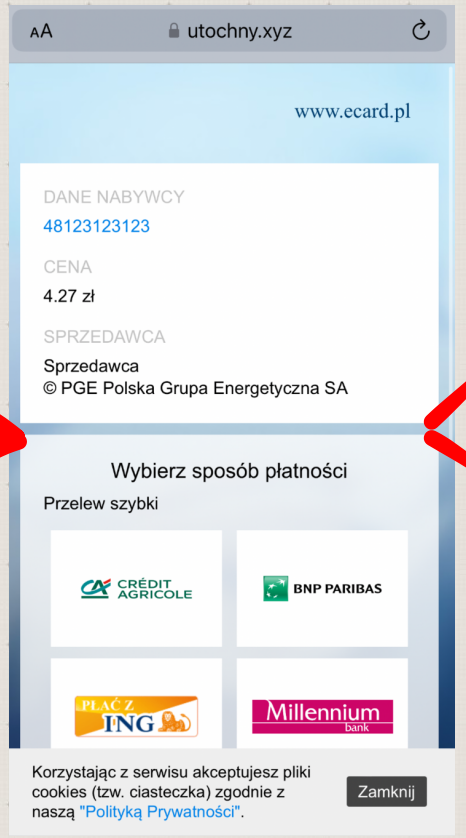
--

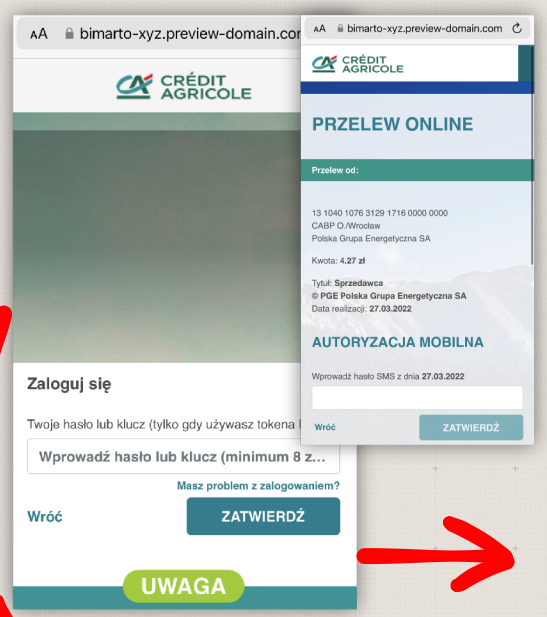
pozdrowienia
pani malgorzata berez
HBDTOYS SP.ZO.O
telefon: 48-71-7254955
faks: 48-71-7220091
e-mail : biuro@hbdtoys.com
adres: skierniewicka, nr 10a, lok. 6p

HBDTOYS SP.ZO.O
WIATOWY

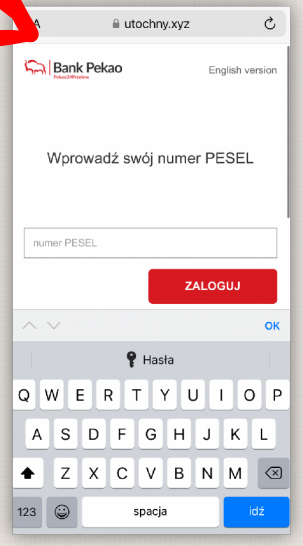

środa, 6 lipca
PGE: Na dzien 07.07 zaplanowano odlaczenie energii elektrycznej! Prosimy o uregulowanie naleznosci: https://t2m.io/hAp332T
17:38


AA
utochny.xyz
PGE
Płatności online
Na dzień 23-03-2022 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności.
Umowa numer: GKETRNG785362
Kwota należności: 4.27 zł
Ureguluj należność szybko i wygodnie za pomocą przelewu szybkiego bądź BLIK.
Przejdź do płatności
Polityka prywatności
PGE Polska Grupa Energetyczna S.A.


AA
utochny.xyz
www.ecard.pl
DANE NABYWCY
48123123123
CENA
4.27 zł
SPRZEDAWCA
Sprzedawca
© PGE Polska Grupa Energetyczna SA
Wybierz sposób płatności
Przelew szybki
CRÉDIT AGRICOLE
BNP PARIBAS
PŁAĆ Z ING
Millennium bank
Korzystając z serwisu akceptujesz pliki cookies (tzw. ciasteczka) zgodnie z naszą "Polityką Prywatności".
Zamknij


AA
bimarto-xyz.preview-domain.com
CRÉDIT AGRICOLE
Zaloguj się
Twoje hasło lub klucz (tylko gdy używasz tokena
Wprowadź hasło lub klucz (minimum 8 z...
Masz problem z zalogowaniem?
Wróć
ZATWIERDŹ
UWAGA

AA
bimarto-xyz.preview-domain.com
CRÉDIT AGRICOLE
PRZELEW ONLINE
Przelew od:
13 1040 1076 3129 1716 0000 0000
CABP O./Wrocław
Polska Grupa Energetyczna SA
Kwota: 4.27 zł
Tytuł: Sprzedawca
© PGE Polska Grupa Energetyczna SA
Data realizacji: 27.03.2022
AUTORYZACJA MOBILNA
Wprowadź hasło SMS z dnia 27.03.2022
Wróć
ZATWIERDŹ


AA
utochny.xyz
Bank Pekao
English version
Wprowadź swój numer PESEL
numer PESEL
ZALOGUJ
OK
Hasła
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
spacja
idź

Czy samo kliknięcie w podejrzanego linka czymś grozi?

Jeśli masz zaktualizowaną: przeglądarkę / rozszerzenia do przeglądarek / oprogramowanie na komputerze (telefonie)

To zazwyczaj NIE

Ale czasem tak!

pegasus

Forensic traces for PLPOI2 – Ryszard Brejza

Date (UTC)	Event
2019-07-11 12:15:35	SMS from **BramkaSMS**: Panie Prezydencie, widział Pan komentarze na portalu “ino” na temat skoszonej łąki? Proszę wejść i poczytać. Podsyłam link do artykułu: **http://tinyurl[.]com/y69p3pyk (https://newsportal24[.]online/mtM8dy6cz)**
2019-07-12 07:18:19	SMS from **PlatformaKO**: Już 12-13 lipca spotkajmy się na Forum Programowym Koalicji Obywatelskiej, by porozmawiać o Polsce! **http://tinyurl[.]com/y3cns-gzl (https://loginverify[.]net/EWSRfbj)**
2019-07-12 16:23:51	SMS from **HTC-Polska**: Zapisz sie do klubu HTC! Jako klubowicz będziesz otrzymywać niedostępne dla innych informacje o nowych produktach, akcesoriach i usługach. Korzystaj w pełni z możliwości swojego telefonu! **https://oneadjump[.]com/SQY8jBX**

Jeśli Cię jednak korci kliknięcie,
to... nie klikaj

Jeśli Cię jednak bardzo korci użyj np. przeglądarki
Edge oraz Nowe Okno Application Guard

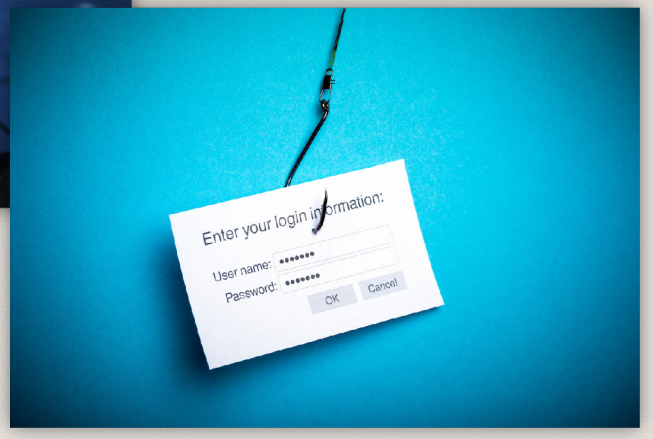
(wymaga Windowsa Pro :/ nie rób tego na komputerze firmowym!)

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview

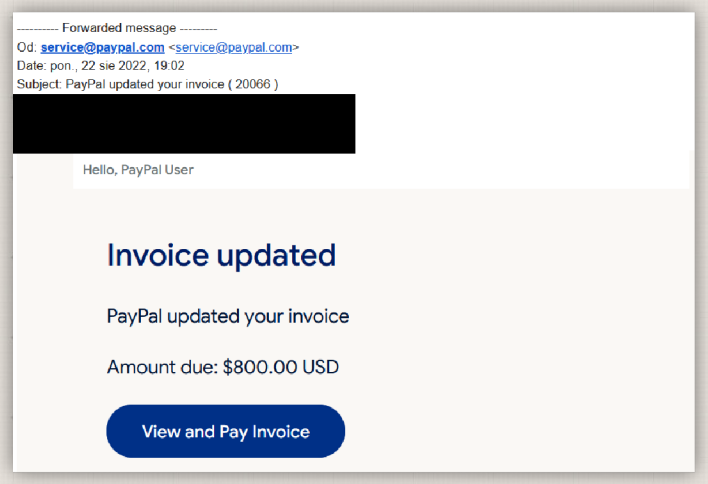
Nieco bardziej sprytny phishing

wykradanie danych

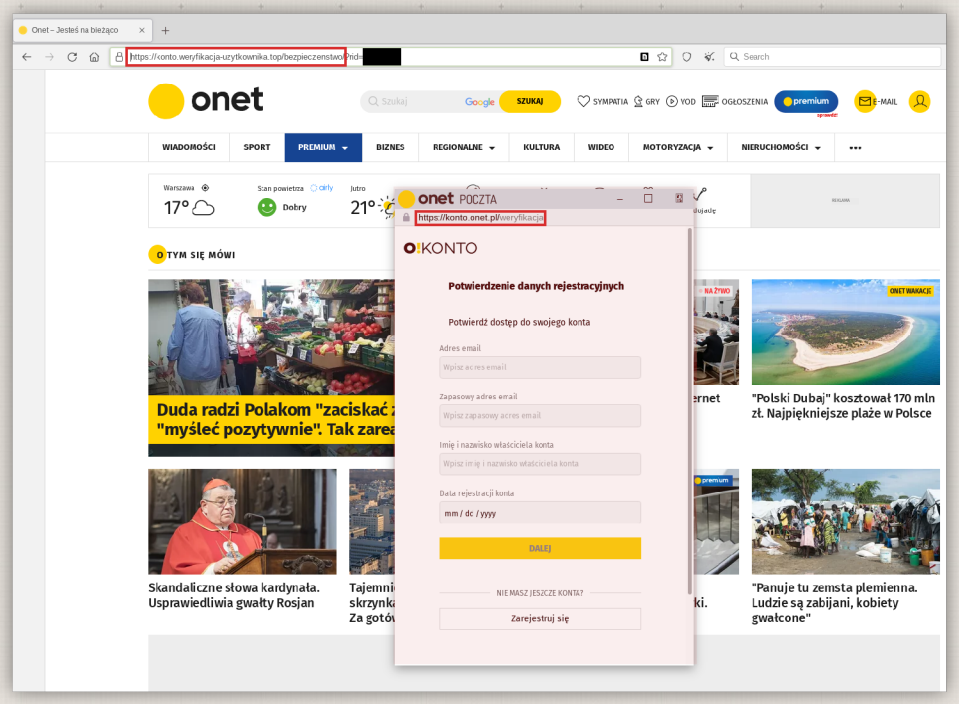
próba zainfekowania komputera



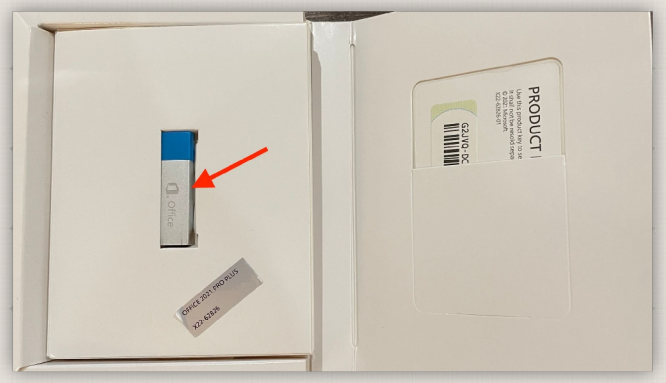
Pamiętaj, że phishing może być czasem wysłany z prawdziwych adresów e-mailowych!



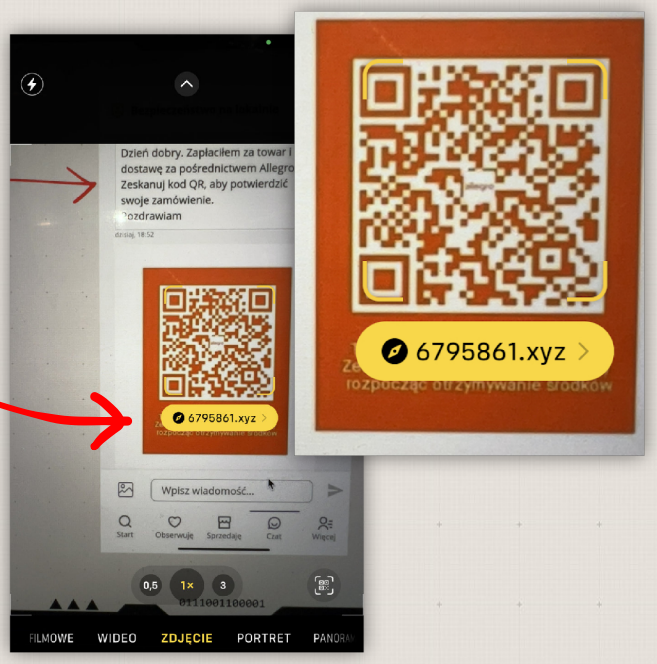
Nie daj się nabrać na technikę BITB (Browser In The Browser)



Uważaj na urządzenia USB otrzymane pocztą, rozdawane na konferencjach, ...

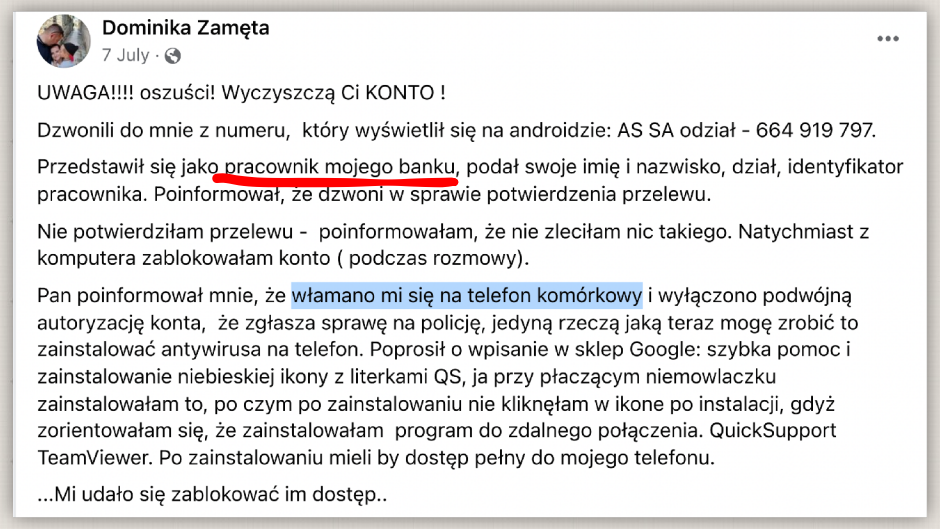


Również linki w kodach QR mogą prowadzić w niebezpieczne miejsca



Uważaj na telefony "z banku", telefony "z policji" ostrzegające "o ataku hackerskim"

Rozłącz się i sam zadzwoń w odpowiednie miejsce (np. bank) żeby potwierdzić czy sprawa nie jest oszustwem



Dominika Zamęta
7 July ·

UWAGA!!!! oszuści! Wyczyszczą Ci KONTO !

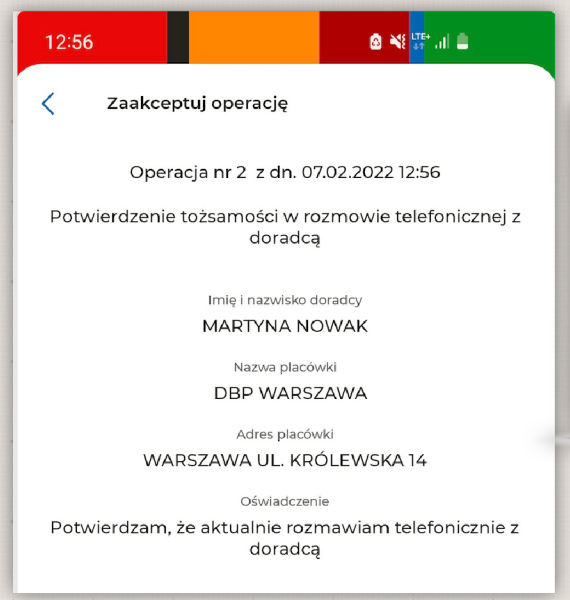
Dzwonili do mnie z numeru, który wyświetlił się na androidzie: AS SA odział - 664 919 797.

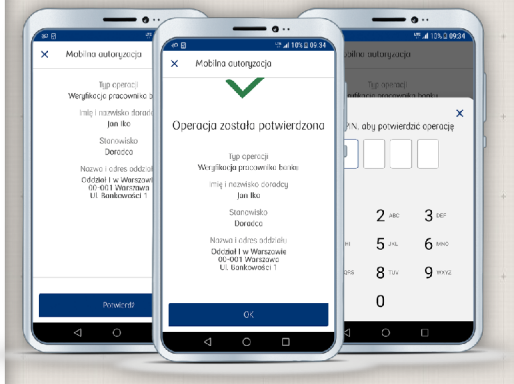
Przedstawił się jako pracownik mojego banku, podał swoje imię i nazwisko, dział, identyfikator pracownika. Poinformował, że dzwoni w sprawie potwierdzenia przelewu.

Nie potwierdziłam przelewu - poinformowałam, że nie zleciłam nic takiego. Natychmiast z komputera zablokowałam konto (podczas rozmowy).

Pan poinformował mnie, że włamano mi się na telefon komórkowy i wyłączono podwójną autoryzację konta, że zgłasza sprawę na policję, jedyną rzeczą jaką teraz mogę zrobić to zainstalować antywirusa na telefon. Poprosił o wpisanie w sklep Google: szybka pomoc i zainstalowanie niebieskiej ikony z literkami QS, ja przy płaczącym niemowlaczku zainstalowałam to, po czym po zainstalowaniu nie kliknęłam w ikone po instalacji, gdyż zorientowałam się, że zainstalowałam program do zdalnego połączenia. QuickSupport TeamViewer. Po zainstalowaniu mieli by dostęp pełny do mojego telefonu.

...Mi udało się zablokować im dostęp..





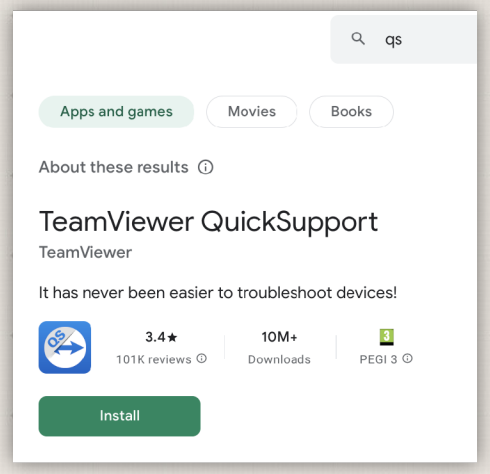
Cudowne okazje ;-(

Nazywam się Chang Dingxiang, jestem starszym personelem w publicznym banku w Wing Hang Bank w Hongkongu i mam 18 991 674 USD. że chcę wyjechać z kraju. Potrzebuję dobrego partnera, kogoś, komu mogę zaufać. To jest wolne od ryzyka i legalne. Odpowiedz na mój e-mail: changdingxiang708@gmail.com, aby uzyskać więcej informacji: pan Chang Dingxiang.

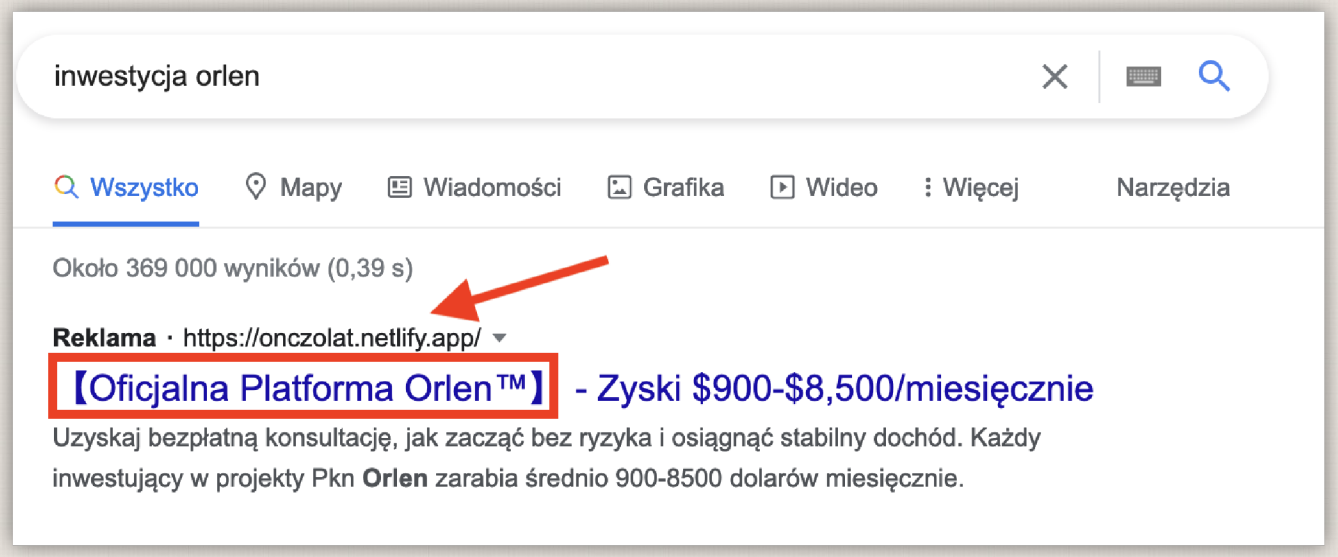
Uważaj na "cudowne okazje"

Nazywam się Chang Dingxiang, jestem starszym personelem w publicznym banku w Wing Hang Bank w Hongkongu i mam 18 991 674 USD. że chcę wyjechać z kraju. Potrzebuję dobrego partnera, kogoś, komu mogę zaufać. To jest wolne od ryzyka i legalne. Odpowiedz na mój e-mail: changdingxiang708@gmail.com, aby uzyskać więcej informacji: pan Chang Dingxiang.

Nie instaluj aplikacji, które "konsultant" poleca Ci przez telefon



Jeśli strona ma dużo polubień / komentarzy / reklamuje się - nie oznacza to automatycznie, że jest bezpieczna

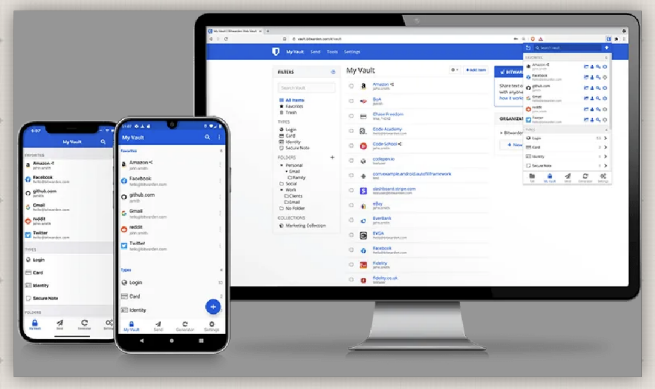


Używaj bezpiecznych haseł!

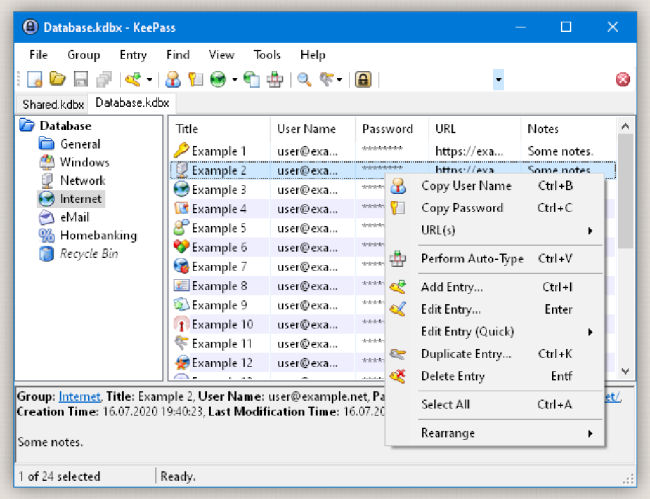
Idealnie: 4+ nieoczywiste sklejone słowa. Długość: > 15 znaków

weekendowepogodnekrakowaniehasel

Używaj managerów haseł!



Bitwarden



KeePass

Nie używaj tego samego hasła w wielu różnych miejscach!

włam do jednego miejsca może skutkować przejęciem wszystkich Twoich kont

Szczególnie chroń skrzynkę pocztową

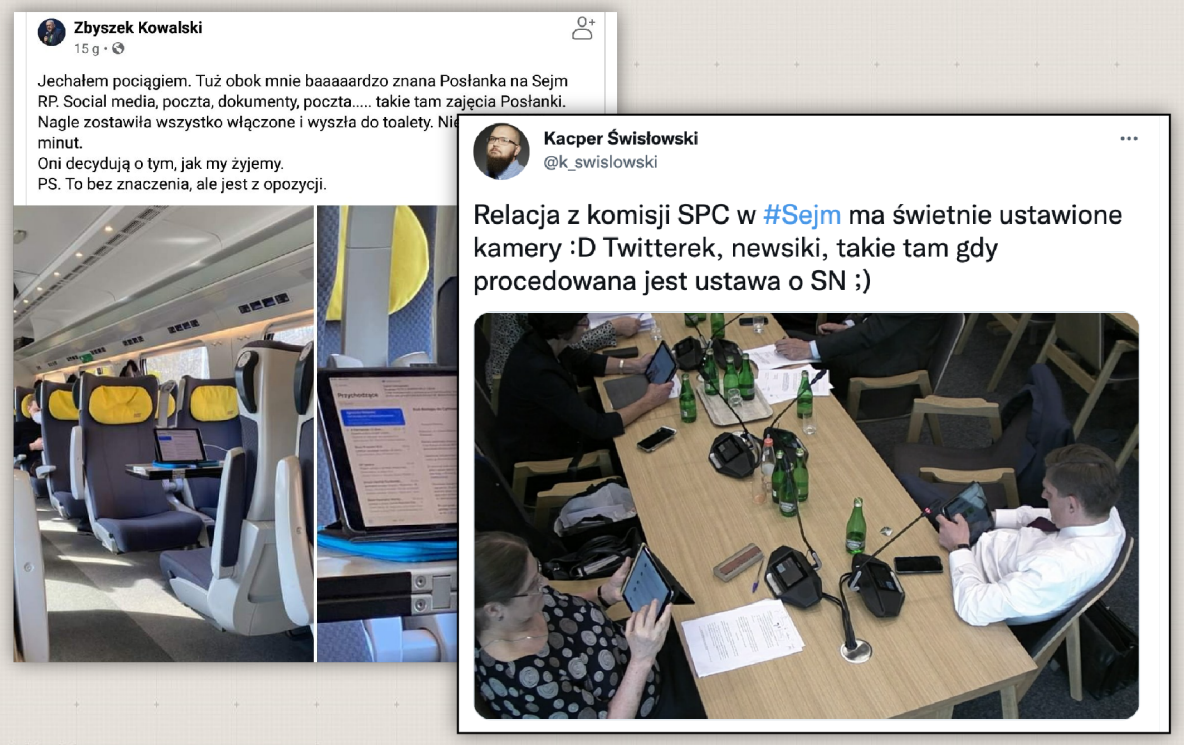
włam na skrzynkę umożliwia przejęcie kont, gdzie użyłeś tego maila do rejestracji

Pamiętaj o skonfigurowaniu 2FA (dwuczynnikowego uwierzytelnienia)

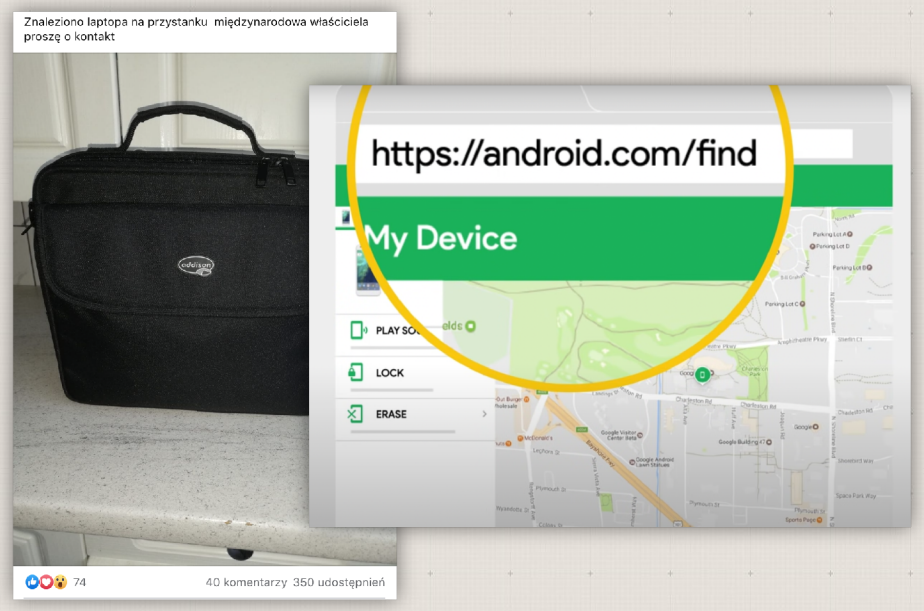
nawet jak ktoś ma login/hasło - nie dostanie się na Twoje konto

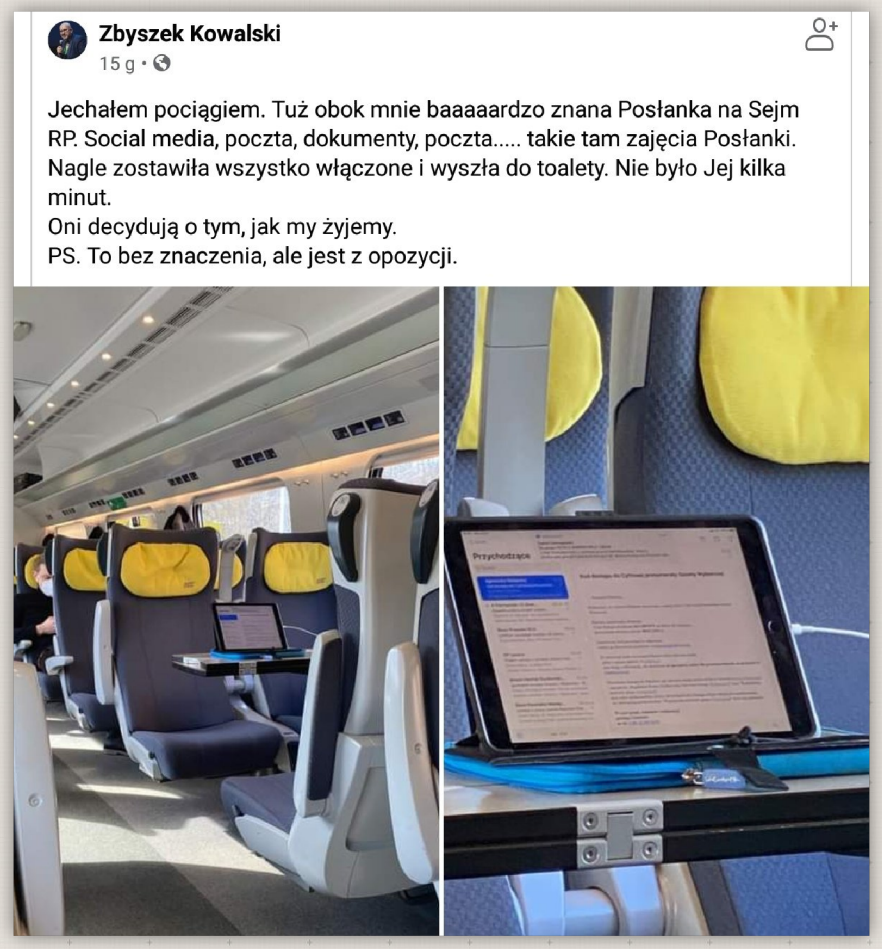
Bezpieczeństwo w podróży

Miejsce pracy (w tym dostęp do Internetu)

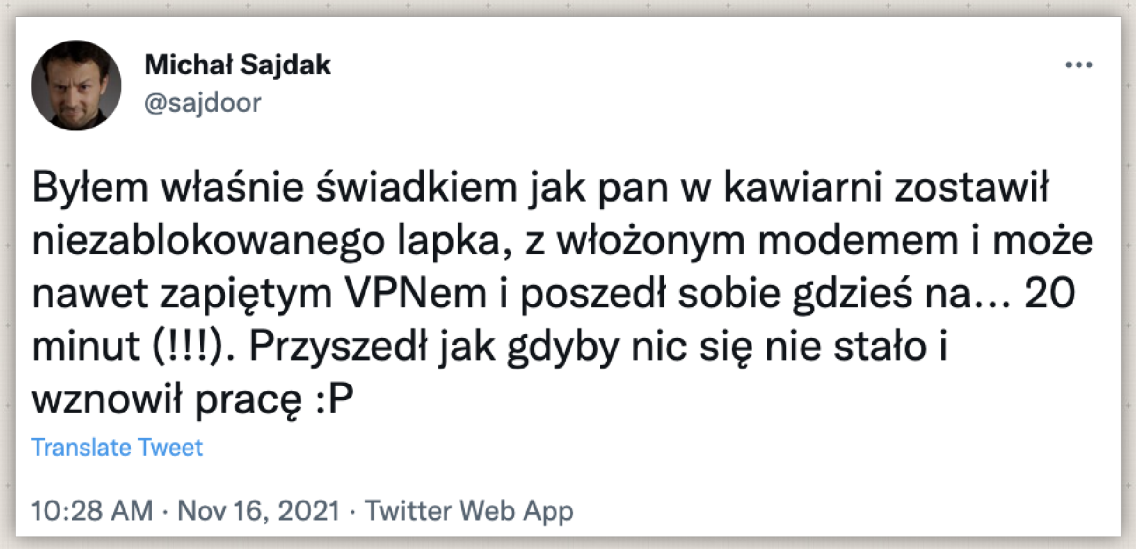


Przygotowanie się na ew. utratę telefonu / laptopa





- Nie zostawiaj komputera bez opieki
- Ustaw auto-blokadę komputera po np. minucie nieaktywności



Filtr prywatyzujący

https://www.kensington.com/c/products/data-protection/privacy-screens/?srt=relevance

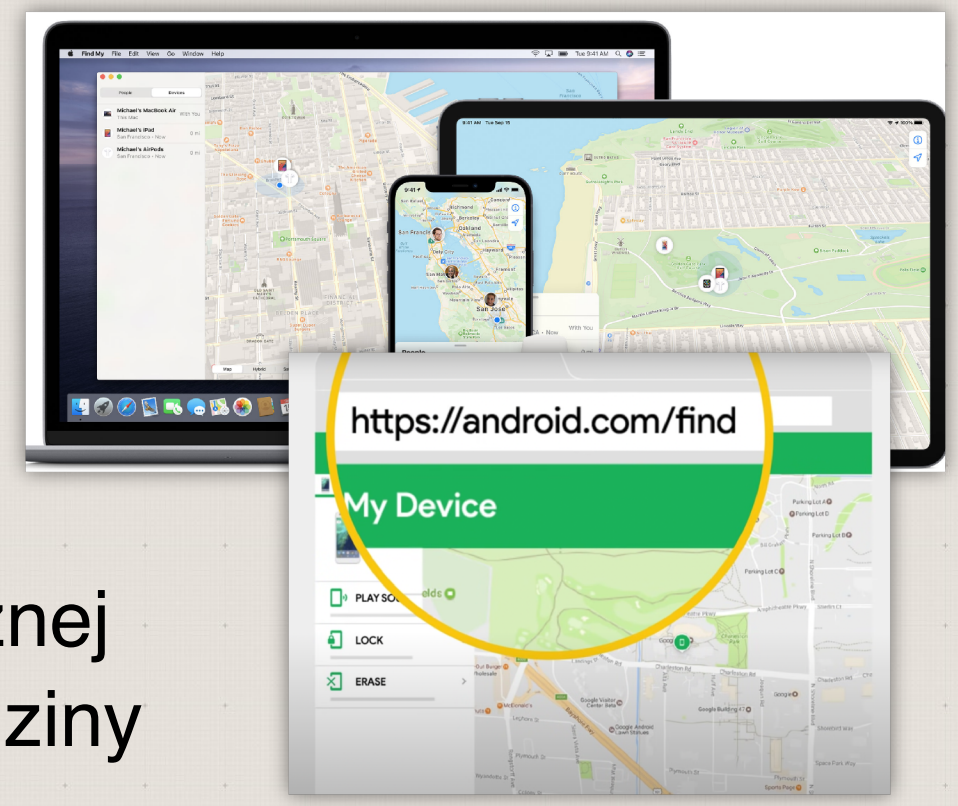
Wybierz bezpieczne miejsce pracy

Kamery!

Bezpieczeństwo WiFi

- Najlepiej nie korzystaj z publicznych sieci WiFi
- Korzystaj z hotspotu w telefonie
- Zadbaj o możliwość zwiększenia "limitu GB internetu" w telefonie

Włączenie zdalnego lokalizowania & kasowania zawartości telefonu / komputera



Do rozważenia wydzielenie fizycznej lokalizacji z telefonu w ramach rodziny

Umieść w walizce / portfelu lokalizator

Nie loguj się / nie podawaj żadnych Twoich danych na publicznie dostępnych komputerach!