



Nie daj się cyberzbójom! v2.0

Podsumowanie prezentacji

michal.sajdak@securITum.pl

 @sajdoor

Copyright (C) SecurITum

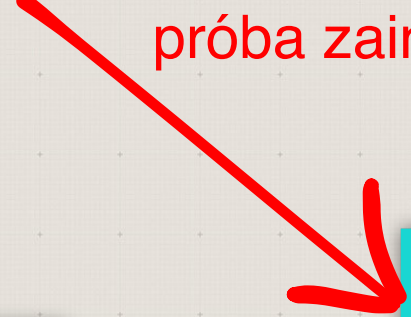
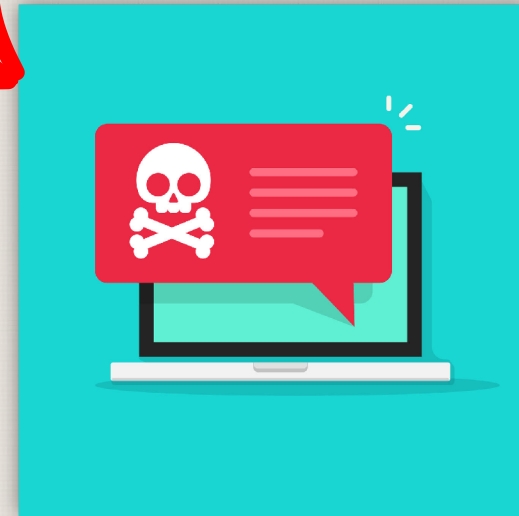




Phishing

wykradanie danych

próba zainfekowania komputera





✓ Sprawdź **adres** nadawcy e-maila,
a nie jego nazwę

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



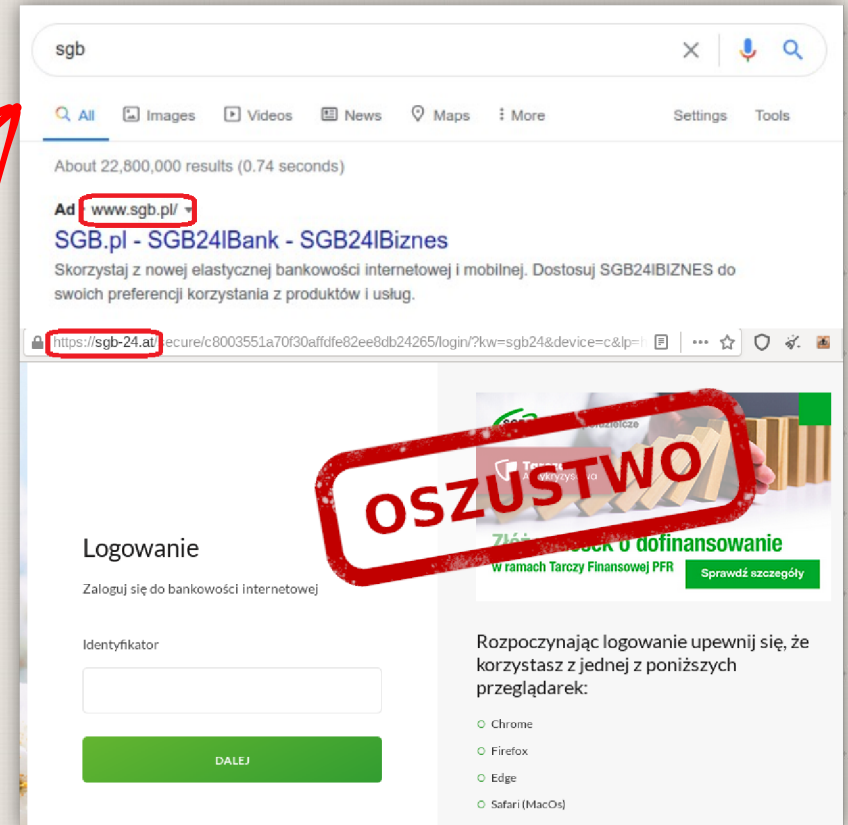
Na strony bankowe wchodzić "ręcznie" lub z zakładek



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.



Zamowienie_zakupu_PO-Eu598303.pdf

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




środa, 6 lipca

PGE: Na dzień 07.07 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności: <https://t2m.io/hAp332T>

17:38

AA utochny.xyz



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
- PLAĆ Z ING
- Millennium bank

Korzystając z serwisu akceptujesz pliki cookies (tzw. ciasteczka) zgodnie z naszą "Polityką Prywatności". **Zamknij**

AA bimarto-xyz.preview-domain.com



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**

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 utochny.xyz



English version

Wprowadź swój numer PESEL

numer PESEL

ZALOGUJ

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

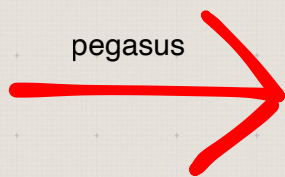


Czy samo kliknięcie w podejrzanego linka czymś grozi?

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


To zazwyczaj **NIE**

Ale czasem tak!




Forensic traces for PLP0I2 – 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 się 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**

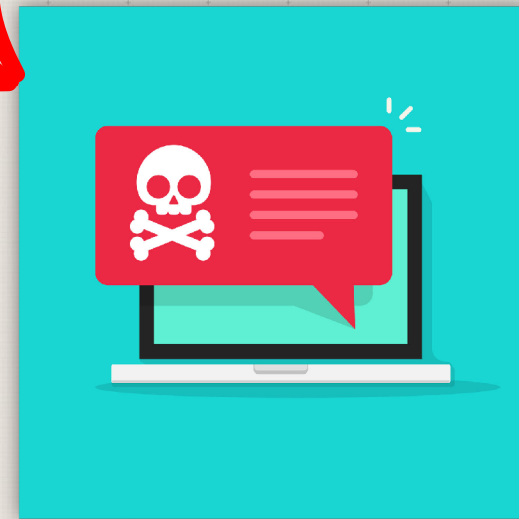
(wymaga Windowsa Pro :/ nie rób tego na komputerze firmowym!)

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

Nieco bardziej sprytny phishing

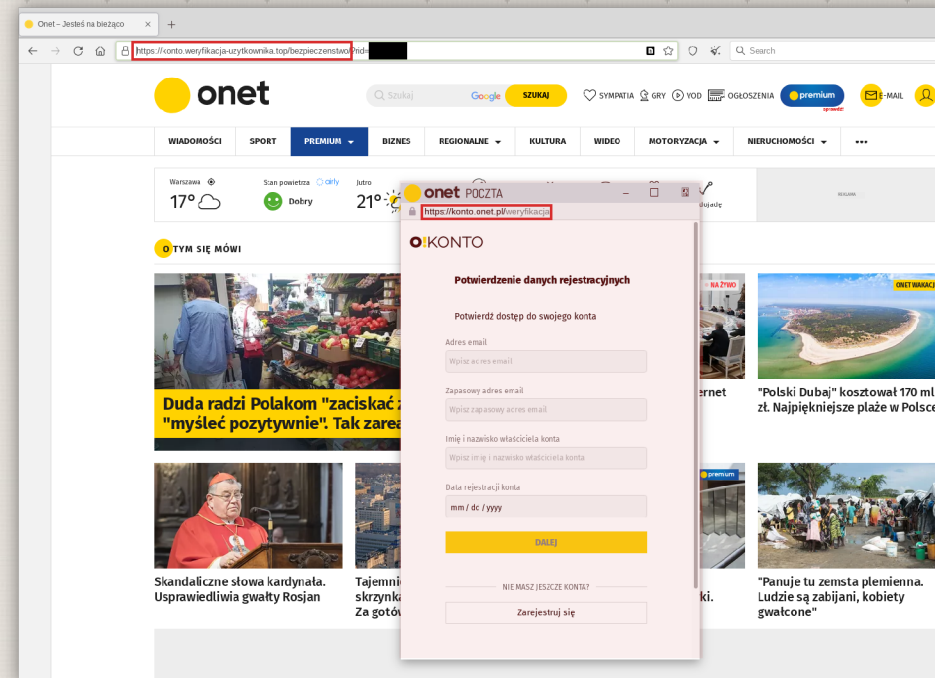
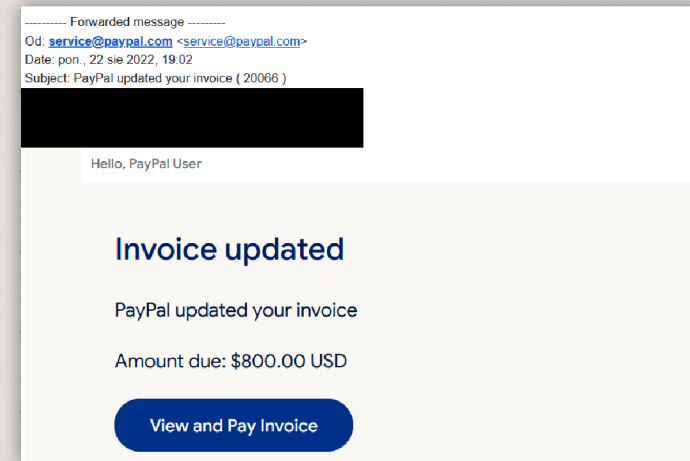
wykradanie danych

próba zainfekowania komputera



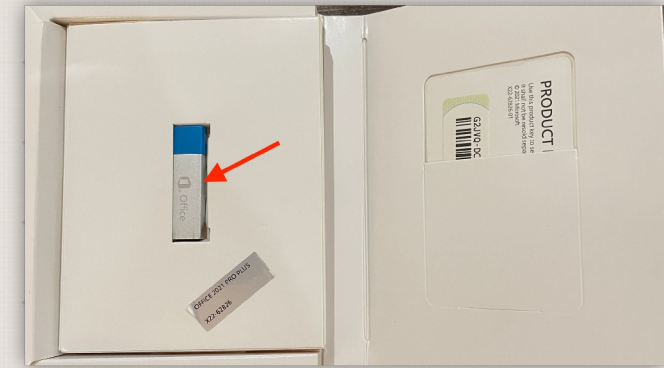
Pamiętaj, że phishing może być czasem wysłany z prawdziwych adresów e-mailowych!

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

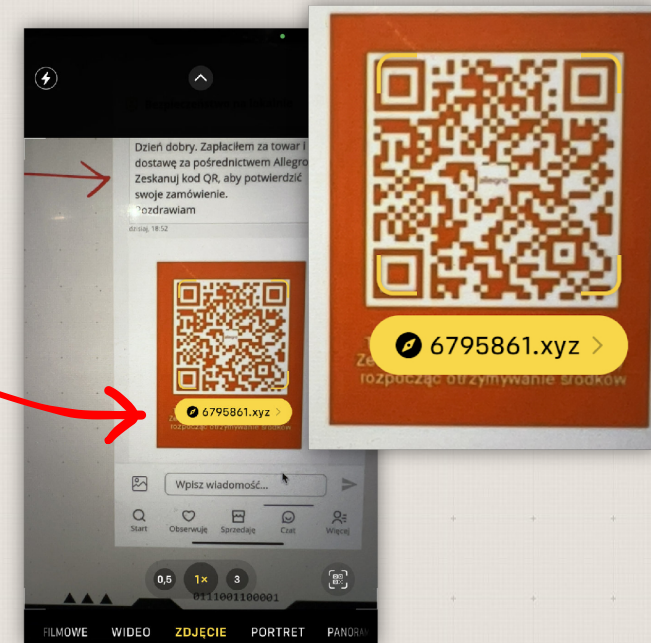




Uważaj na urządzenia USB
otrzymane pocztą, rozdawane na
konferencjach, ...

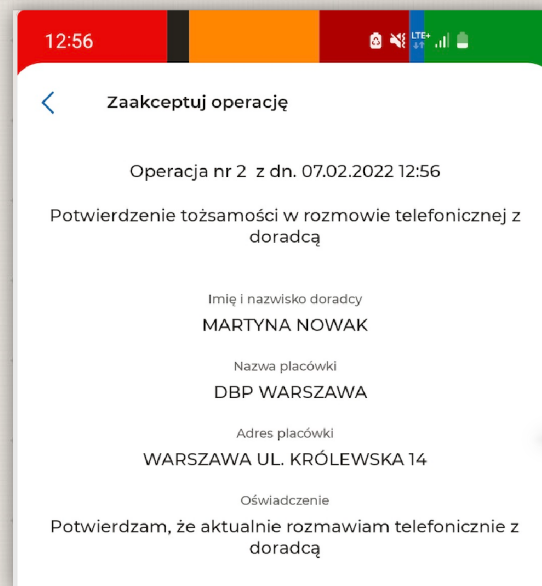
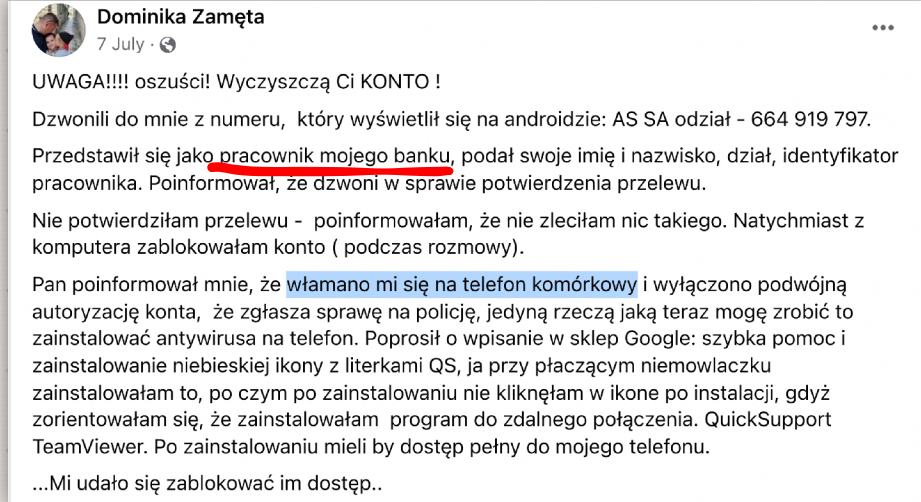


Również linki w kodach QR mogą
prowadzić w niebezpieczne miejsca



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





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.

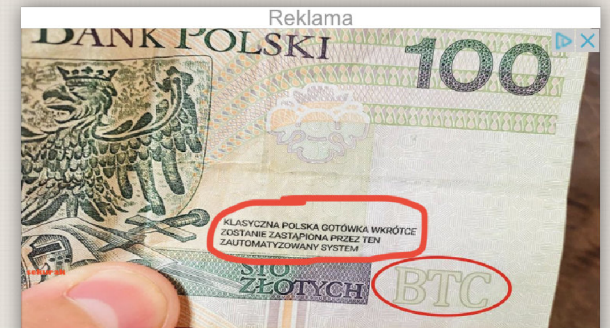


Uważaj na "cudowne okazje"

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



Ten drobny, przeoczony błąd może pomóc każdemu Polakowi wyjść z kłopotów

Berincon LTD

Otwórz >

AnyDesk Why AnyDesk Solutions Pricing Services Company my.AnyDesk Downloads

Access.Now.

Access any device at any time. From anywhere. Always secure and fast.

Download Now Order Now

macOS (10.5 MB)

Apps and games Movies Books

About these results

TeamViewer QuickSupport
TeamViewer

It has never been easier to troubleshoot devices!

3.4★ 101K reviews 10M+ Downloads PEGI 3

Install





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

inwestycja orlen

Wszystko Mapy Wiadomości Grafika Wideo Więcej Narzędzia

Około 369 000 wyników (0,39 s)

Reklama · <https://onczolat.netlify.app/>

[Oficjalna Platforma Orlen™] - Zyski \$900-\$8,500/miesięcznie

Uzyskaj bezpłatną konsultację, jak zacząć bez ryzyka i osiągnąć stabilny dochód. Każdy inwestujący w projekty Pkn Orlen zarabia średnio 900-8500 dolarów miesięcznie.

ALDI Fans
 7 July at 17:38

Mamy setki telewizorów, które lekko się zepsuły w drodze do naszego magazynu. Wszystkie te telewizory nadal działają dobrze, ale mogą mieć drobne wgniecenia lub zadrapania. Zamiast go wyrzucać, pomyśleliśmy o przekazaniu go osobom, które udostępniły i skomentowały przed 15 lipca. Po odwiedzeniu <https://rebrand.ly/e77946>, aby zweryfikować swój wpis. Posiadamy 4 palety, a przesyłka zostanie dostarczona następnego dnia.

1.9K 4.9K comments 11K shares



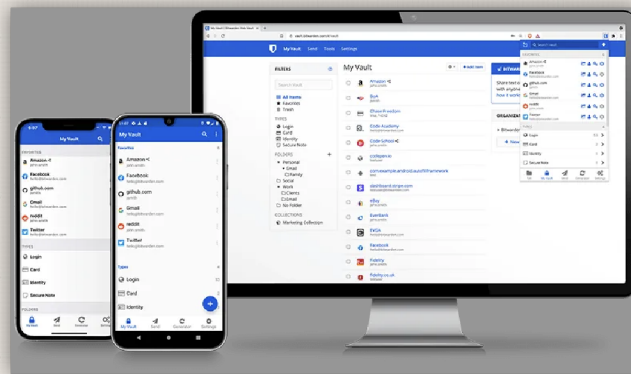
Używaj bezpiecznych haseł!

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

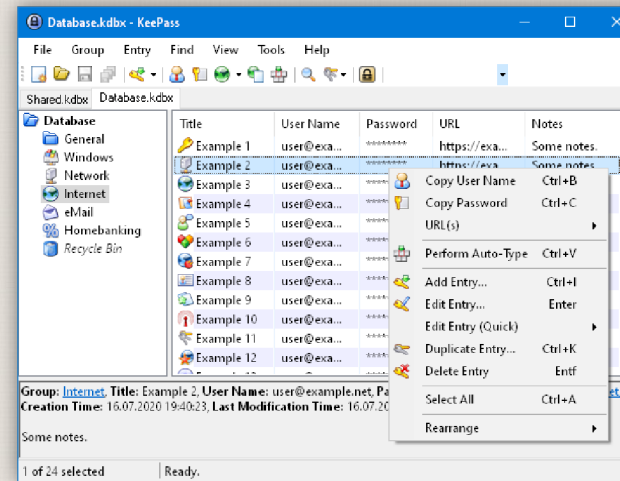
weekendowepogodnekrakowanieihaseł



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)

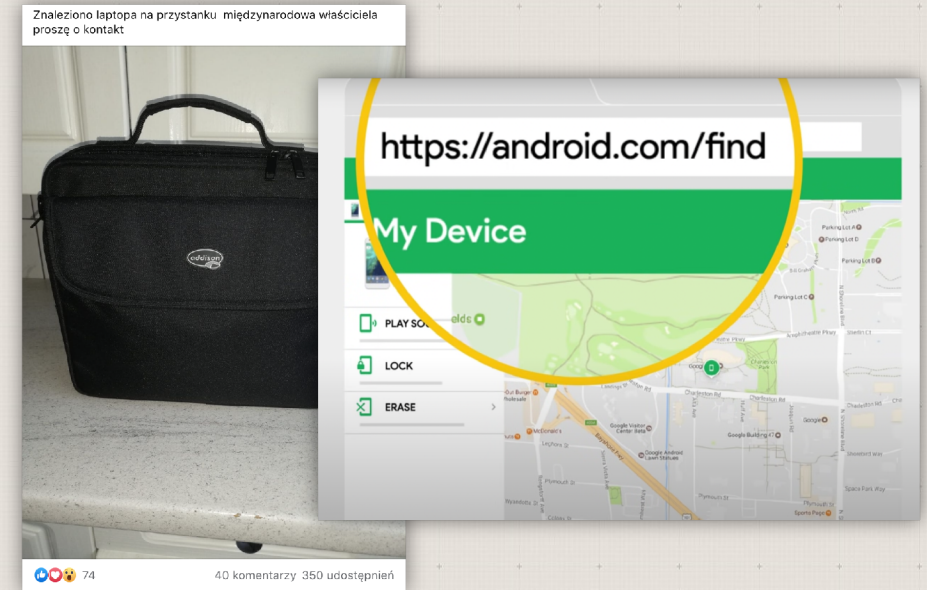
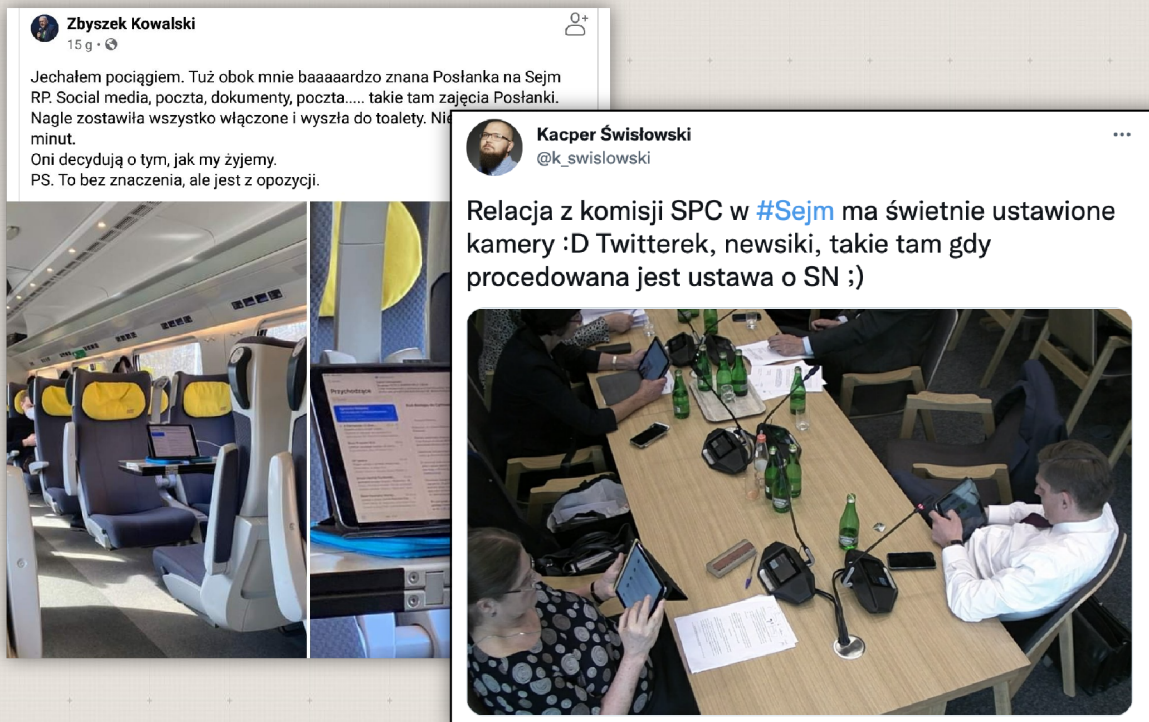
nawet jak ktoś ma login/hasło - nie dostanie się na Twoje konto



Bezpieczeństwo w podróży

Miejsce pracy (w tym dostęp do Internetu)

Przygotowanie się na ew. utratę telefonu / laptopa





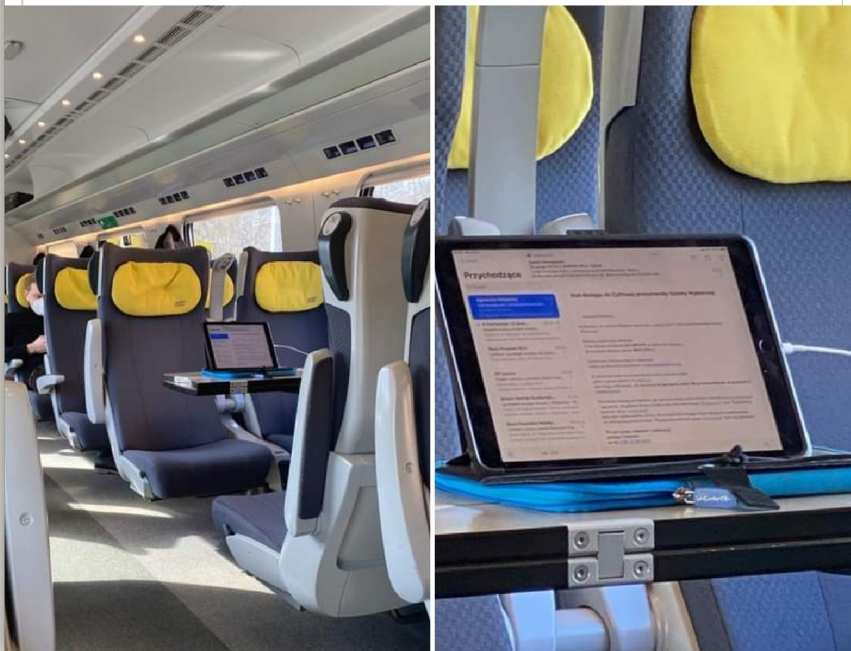
Nie zostawiaj komputera bez opieki



Ustaw auto-blokadę komputera po np. minucie nieaktywności

Zbyszek Kowalski
15 g • 🌐

Jechałem pociągiem. Tuż obok mnie baaaaardzo znana Posłanka na Sejm RP. Social media, poczta, dokumenty, poczta..... takie tam zajęcia Posłanki. Nagle zostawiła wszystko włączone i wyszła do toalety. Nie było Jej kilka minut.
Oni decydują o tym, jak my żyjemy.
PS. To bez znaczenia, ale jest z opozycji.



Michał Sajdak
@sajdoor



Byłem właśnie świadkiem jak pan w kawiarni zostawił niezablokowanego laptopa, z włożonym modemem i może nawet zapiętym VPNem i poszedł sobie gdzieś na... 20 minut (!!!). Przyszedł jak gdyby nic się nie stało i wznowił pracę :P

[Translate Tweet](#)

10:28 AM · Nov 16, 2021 · Twitter Web App





Filtr prywatyzujący

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



Wybierz bezpieczne miejsce pracy



Kamery!



Kacper Świsłowski
@k_swislowski

Relacja z komisji SPC w [#Sejm](#) ma świetnie ustawione kamery :D Twitterek, newsiki, takie tam gdy procedowana jest ustawa o SN ;)



Bezpieczeństwo WiFi



Najlepiej nie korzystaj z publicznych sieci WiFi



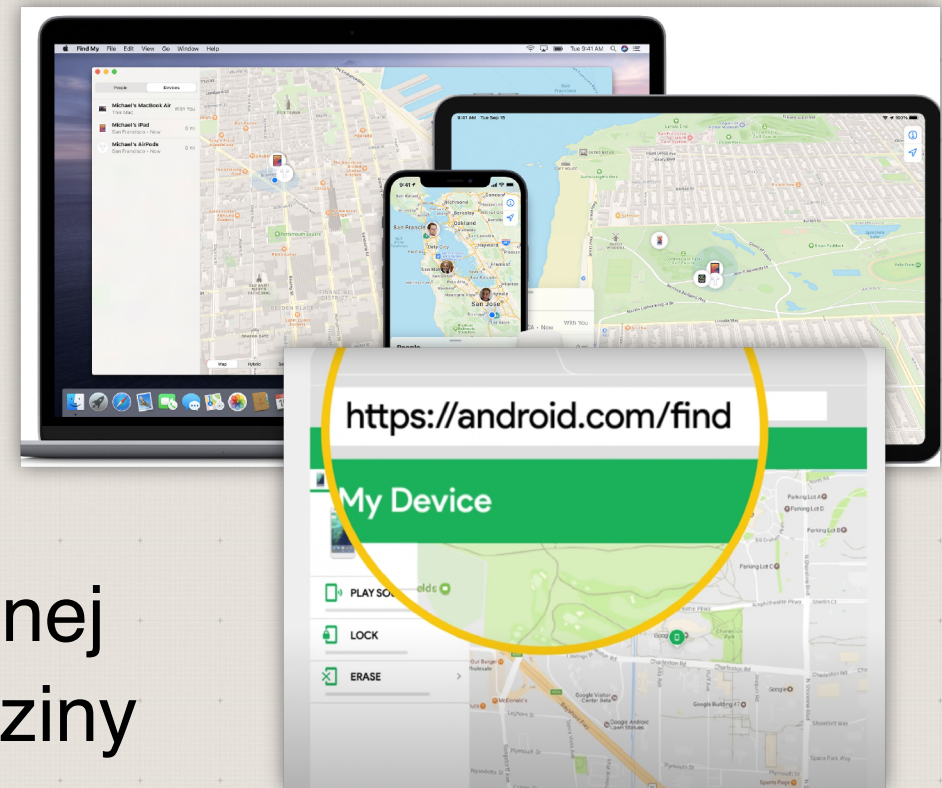
Korzystaj z hotspotu w telefonie



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!

Hansen @Hansen49030246 · Jul 21, 2019

Google chrome stores all your **password** if you allow it. Also, the plaintext is always available. This means that if you forget to logout your google account in a **public computer**, all of your **password** will be leaked...
[#SecurityEverywhere](#)

Auto Sign-in
 Automatically sign in to websites using stored credentials. If disabled, you will be asked for confirmation every time before signing in to a website. 🔴

View and manage saved **passwords** in your Google Account

Saved **Passwords**

Website	Username	Password	👁	⋮
🔗 uac.10010.com	18	👁	⋮
🔗 uac.10010.com	18	👁	⋮
🔗 127.0.0.1:8080	ha	...	👁	⋮
🔗 email.163.com	13	👁	⋮
🔗 reg.email.163.com	18	👁	⋮
🔗 mail.163.com	ha	👁	⋮
🔗 dl.reg.163.com	ha	👁	⋮

Roblox @Roblox · Sep 18, 2018

Protect your account 🛡️! Use a strong **password**, make sure to always log out of Roblox if you're on a **public computer**, like at school or a library, and enable 2-Step Verification. Learn more on our latest safety blog: goo.gl/25NiQn

PROTECT YOUR ACCOUNT

Your Roblox account is one-of-a-kind. You might've gotten really far in a game, saved up a lot of Robux, or obtained a super cool Limited item. No matter how valuable your account is, it's always important to do the smart thing and protect it against hackers and scammers. Don't share your password with anyone—even if they say they're from Roblox—and enable 2-Step Verification in your settings.



ROBLOX SAFETY TIP #5

98 57 562

