



Szkolenie z cyberbezpieczeństwa dla firm



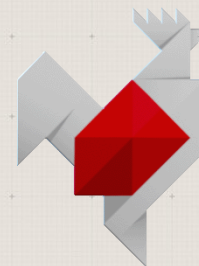
michal.sajdak@securitum.pl

Copyright (C) Securitum





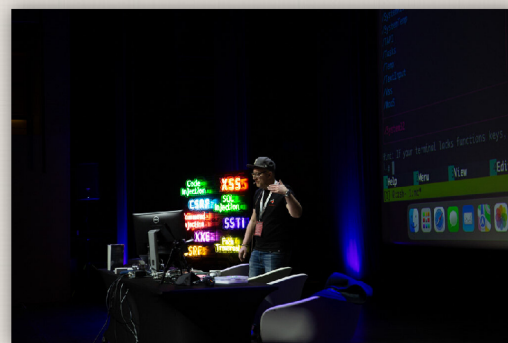
ksiazka.sekurak.pl



sekurak.pl



SEKURAK.ACADEMY



Mega Sekurak Hacking Party



securITUM



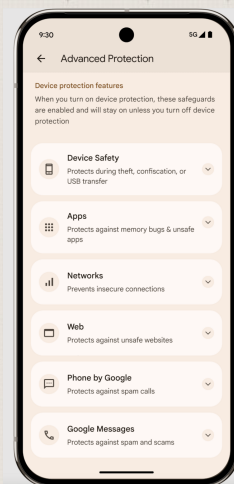
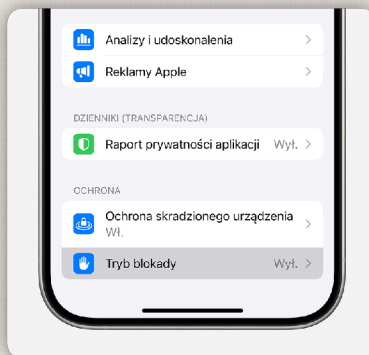
| securITUM

Informacje tylko w celach
edukacyjnych!

Nazwy firm / logotypy użyte są
w celach informacyjnych

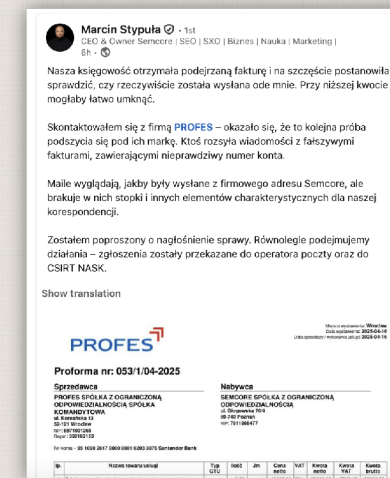
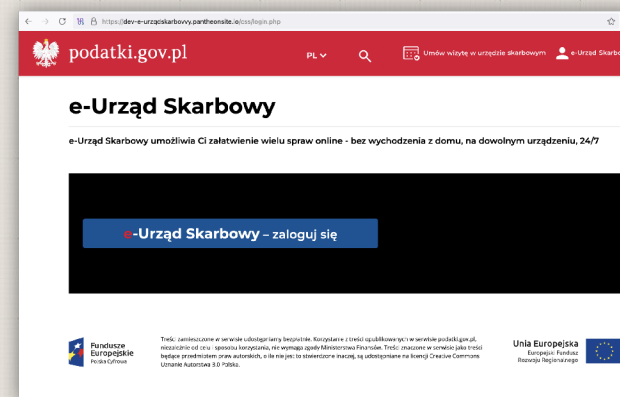
Cyberbezpieczeństwo smartfona

01



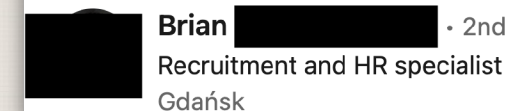
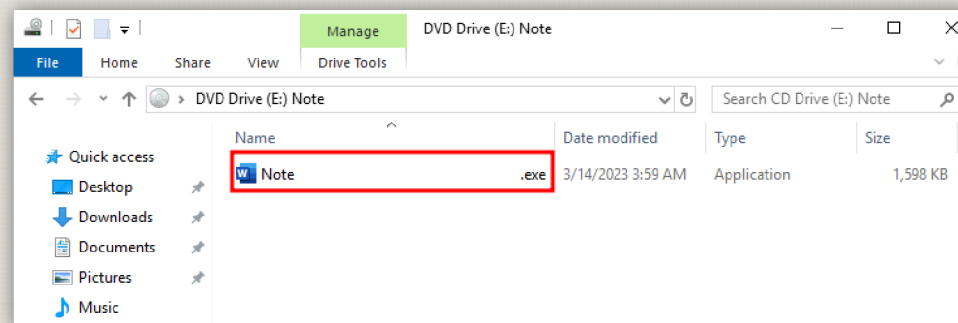
02

Przegląd najnowszych metod cyberoszustów skierowanych na pracowników firm



03

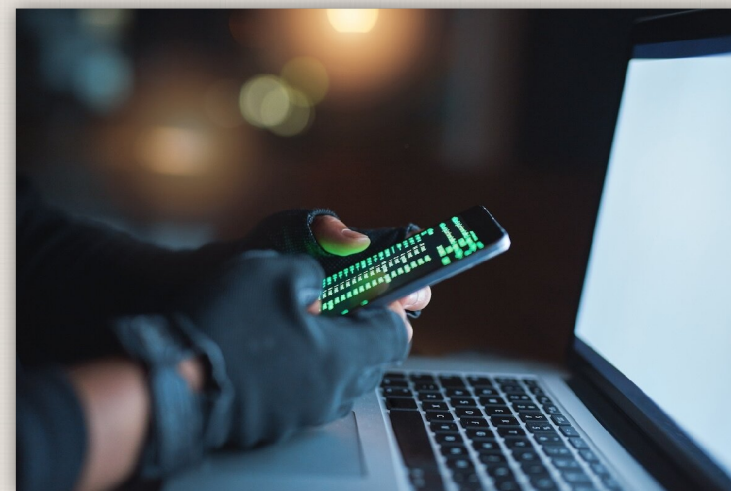
Jak rozpoznawać fałszywe / złośliwe załączniki?



Bezpieczeństwo smartfonów

Czy należy obawiać się Pegasus?

Zaawansowane narzędzie szpiegowskie,
umożliwiające uzyskanie zdalnego dostępu do telefonu

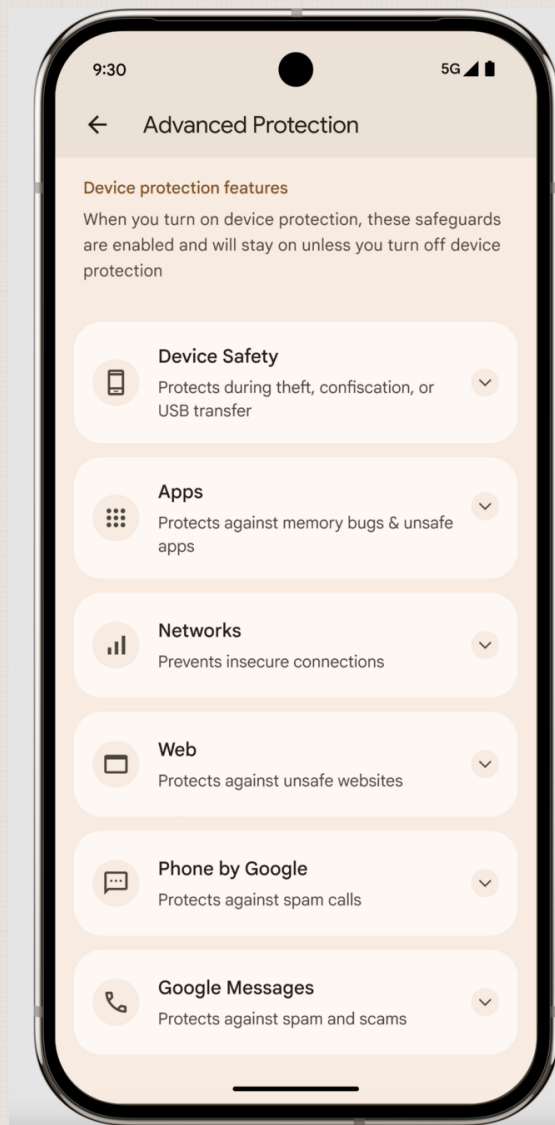


PARAGON'S ANDROID SPYWARE - WHATSAPP ZERO-CLICK FLOW



- 1 Attacker adds victim to WhatsApp group in a specific way
- 2 Attacker sends PDF to group
- 3 Victim's device automatically parses PDF, exploiting vulnerability
- 4 Graphite implant loaded into WhatsApp
- 5 Spyware escapes the Android sandbox and propagates to other apps on the device

<https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/>



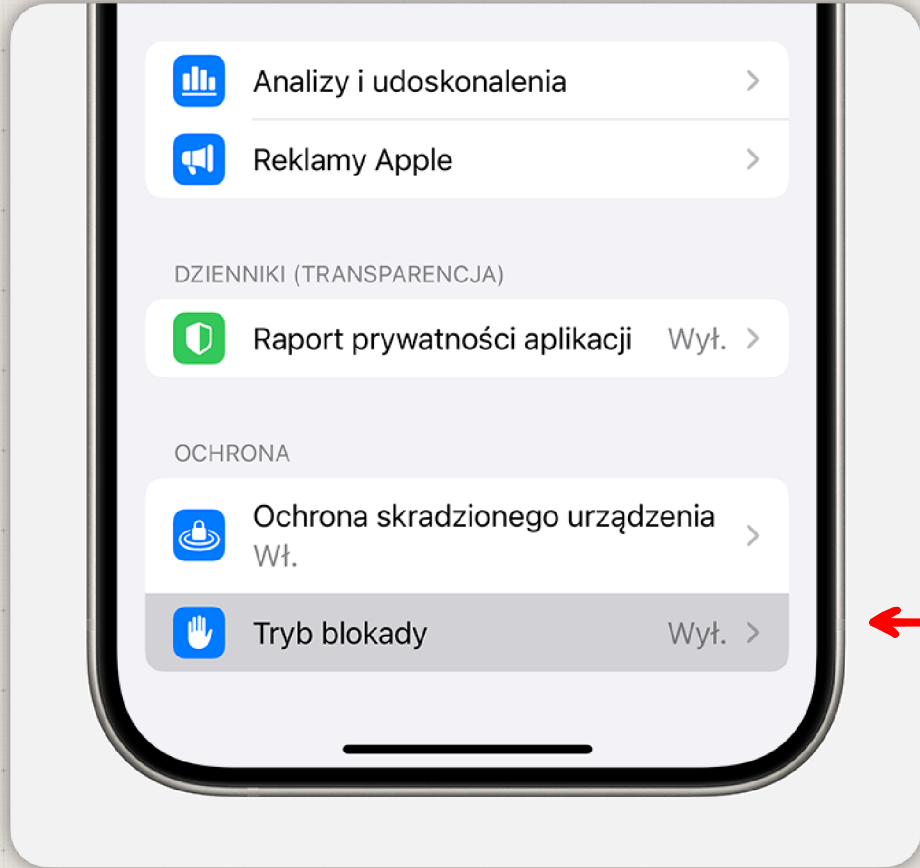
Device safety

- * Theft Detection Lock:** Your device will automatically lock itself if it detects suspicious activity indicative of theft.²
- * Offline Device Lock:** Your unlocked device will automatically lock itself if it goes offline for prolonged periods.²
- ‡ Inactivity Reboot:** Will automatically restart your device if locked for 72 hours. This process will make user data unreadable until a fresh unlock takes place, ensuring your information remains protected.
- * USB Protection:** Prevent physical attacks attempting to exploit the USB port by defaulting to charging only for any new USB connection while the device is locked.^{1,3}

Network

- * 2G Network Protection:** Your device will no longer connect to 2G networks.³
- ‡ Disable Auto-Reconnect to Insecure Networks:** Your device will no longer automatically reconnect to Wi-Fi networks known to be insecure (open, WEP, or OWE).¹

Android

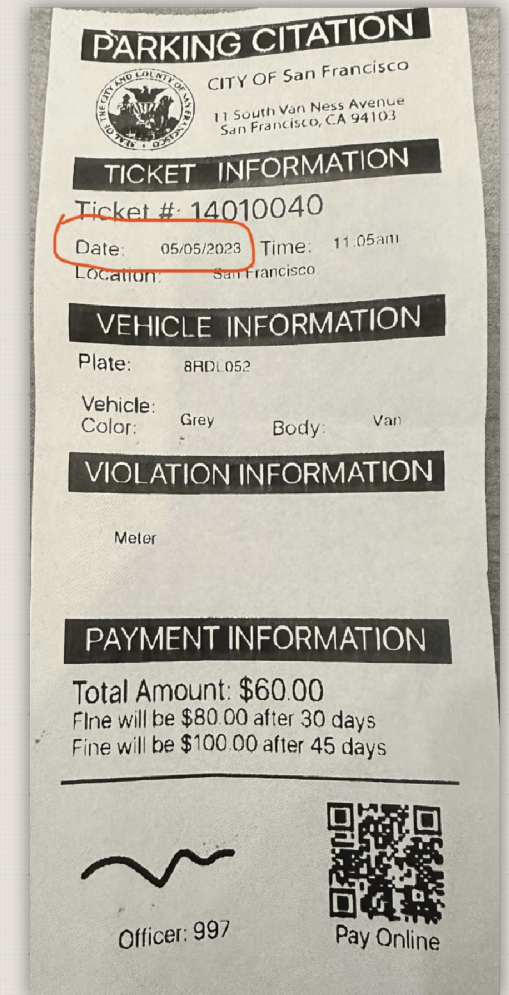
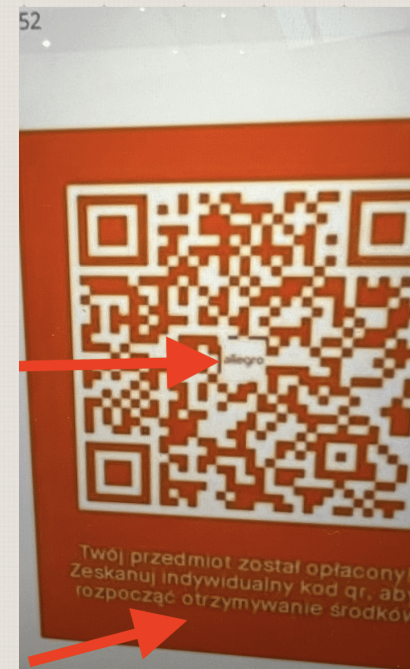
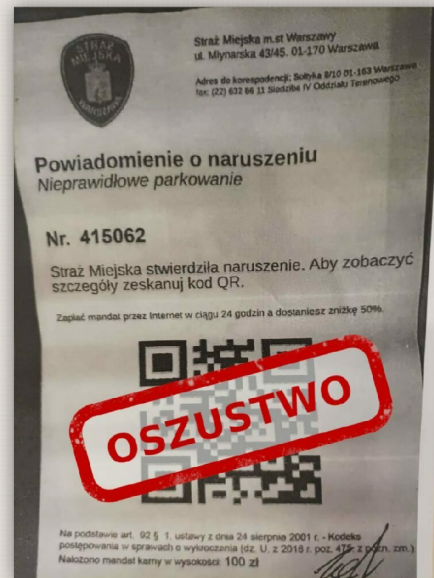
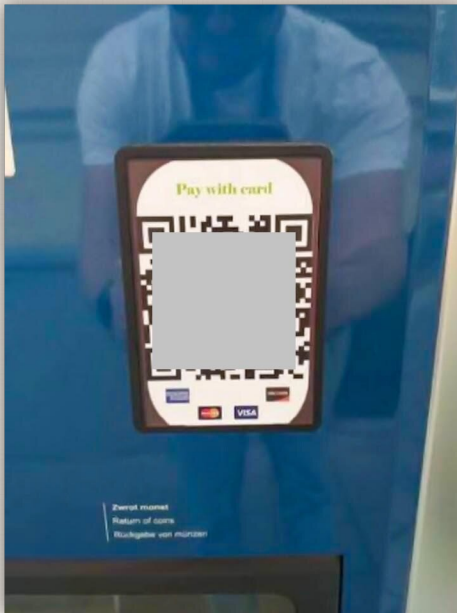


Tryb blokady to opcjonalny, nadzwyczajny tryb ochrony, przeznaczony dla bardzo nielicznych osób, które ze względu na to, kim są lub czym się zajmują, mogą być celem najbardziej wyrafinowanych zagrożeń cyfrowych. Większość ludzi nigdy nie będzie celem ataków tego rodzaju.

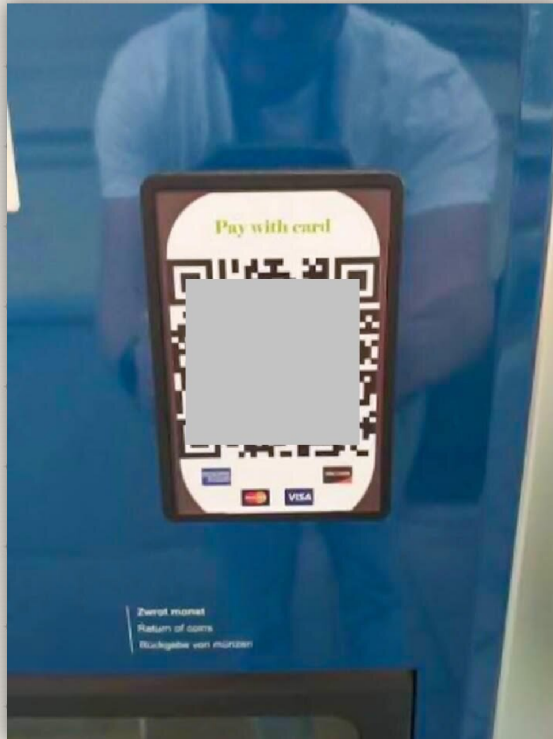
<https://support.apple.com/pl-pl/105120>

iOS

Czy kody QR są bezpieczne?



Czy kody QR są bezpieczne?



← → ↻ 🔍 kkrakowparking.website

 **Kraków**
   

Strefa A

Oплата за місце parkingowe/Parking fee

Numer rejestracyjny/Registration number

Ilość godzin parkowania samochodu/Number of hours of car parking

Akceptujemy karty/We accept cards:  

Numer karty*/Card number*

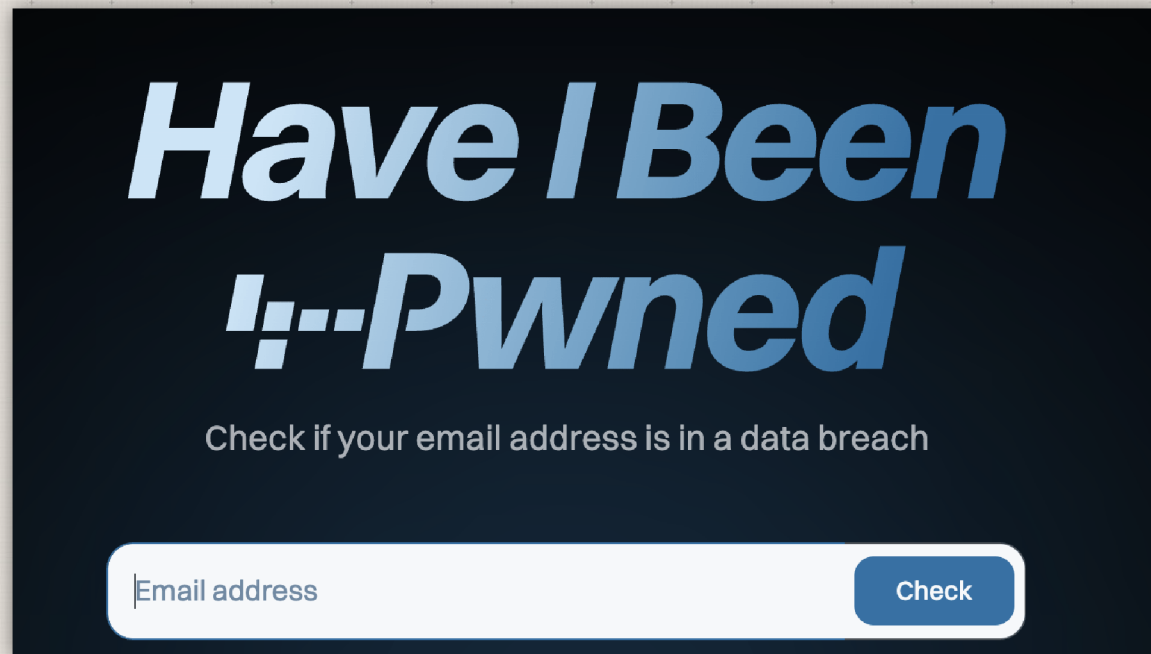
Data wygaśnięcia*/Expiration date*

CVV*:

ZAPŁAĆ



Jak oszukano jednego z najbardziej znanych specjalistów od cyberbezpieczeństwa - Troya Hunta?

The image shows the 'Have I Been Pwned' logo in a stylized blue font on a dark blue background. Below the logo, the text 'Check if your email address is in a data breach' is displayed. At the bottom, there is a white input field with the placeholder text 'Email address' and a blue 'Check' button to its right.

Have I Been
!Pwned

Check if your email address is in a data breach

Email address

Check



<https://www.troyhunt.com/a-sneaky-phish-just-grabbed-my-mailchimp-mailing-list/>



Sending Privileges Restricted

Hello,

We're reaching out to inform you that your Mailchimp account's sending privileges have been restricted due to a spam complaint received on March 24, 2025. We take these reports seriously to maintain a safe and trusted platform for all users.

What's Happening?

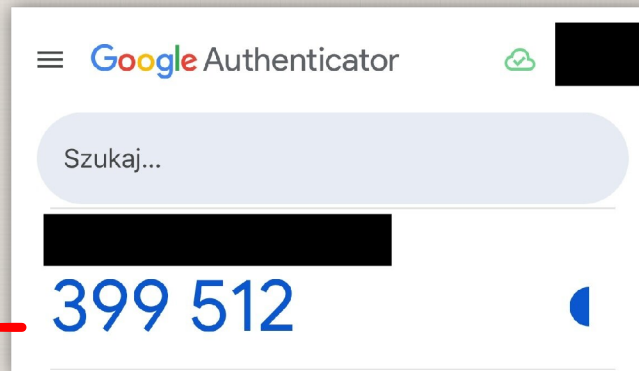
Your account has been flagged due to a spam complaint, and as a result, you are temporarily unable to send emails until this issue is resolved.

What You Need to Do

Please review your recent campaigns and audience lists to ensure compliance with our policies. **Click below to review your account and take the necessary steps to restore your sending privileges.**

[Review Account](#)

mailchimp-sso[.]com



Troy wpisał ręcznie:

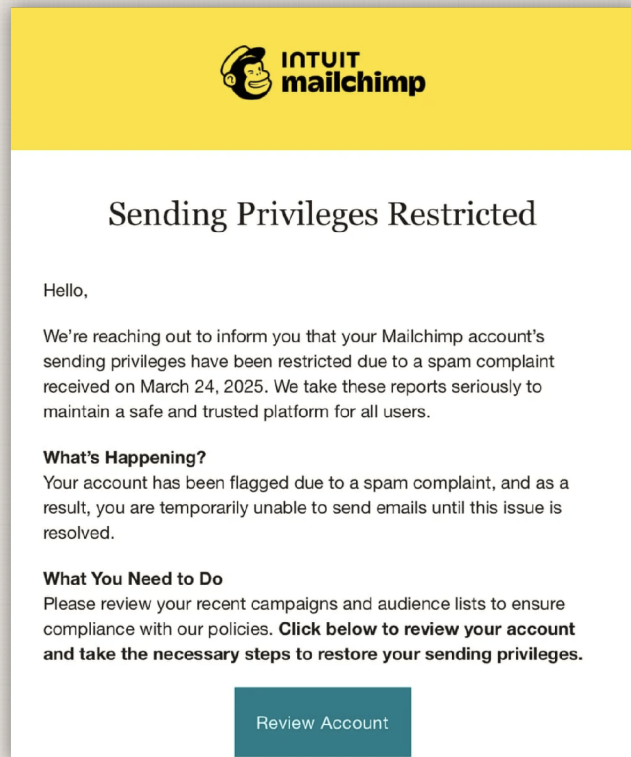
login / hasło / kod z apki Google Authenticator



Przeoczył fakt, że jego menedżer haseł: 1Password,
nie wypełnił automatycznie danych logowania

DEMO

Ale z jakiego adresu e-mail była wysłana wiadomość?



Istotny jest fakt, że Troy odebrał wiadomość **na telefonie**



01

***Zmęczenie** było głównym czynnikiem. Nie byłem wystarczająco czujny i nie przemyślałem porządnie tego, co robię.*

02

*To bardzo dobrze wykonany phishing. (...) Uwierzyłem, że nie będę w stanie wysłać mojego newslettera, więc wywołało to u mnie **strach**.*

03

*(...) **dane logowania nie były automatycznie uzupełniane przez 1Password**, więc dlaczego to zignorowałem? Bo to nic niezwykłego. Istnieje wiele usług, w których **rejestrujesz się w jednej domenie** (i ten adres jest przechowywany w 1Password), a następnie legalnie **logujesz się do innej domeny**.*



Aktualizuj telefon / apki



Minimalizuj liczbę apek na telefonie



Nie instaluj apek z podejrzanych źródeł



SMS



Polecenie od "konsultanta"



Nieznany adres
strony internetowej



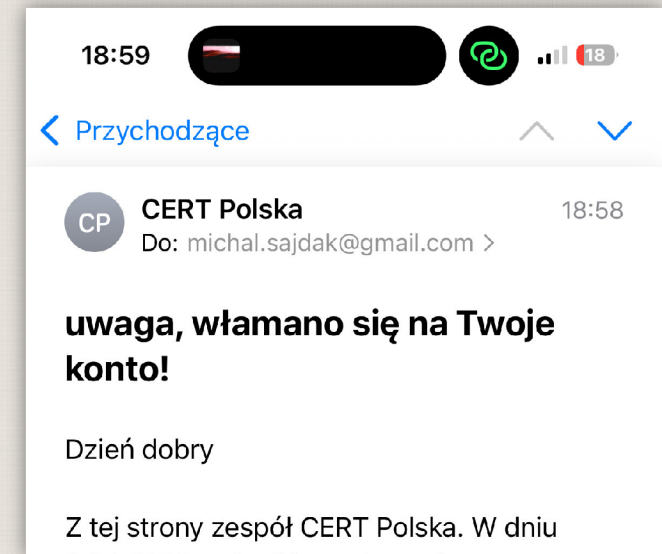
Aplikacje bankowe pobieraj z oficjalnych sklepów (App Store, Google Play) - z linków udostępnionych na stronie banku



Nie podawaj w apce PINu do karty płatniczej w celach "weryfikacji klienta"



Na smartfonie dokładnie weryfikuj nadawcę e-maila



"maile wysyłane z mBanku do klientów, którzy korzystają z poczty elektronicznej w serwisach Gmail, Interia, Onet oraz WP/O2, będą oznaczone jako pochodzące od sprawdzonego nadawcy."



| securiTUM



Weryfikuj, gdzie dokładnie prowadzi kod QR



Przegląd najnowszych metod cyberoszustów skierowanych na pracowników firm.



Marcin Stypuła ✓ • 1st
CEO & Owner Semcore | SEO | SXO | Biznes | Nauka | Marketing |
6h • 🔒

Nasza księgowość otrzymała podejrzaną fakturę i na szczęście postanowiła sprawdzić, czy rzeczywiście została wysłana ode mnie. Przy niższej kwocie mogłaby łatwo umknąć.

Skontaktowałem się z firmą **PROFES** – okazało się, że to kolejna próba podszycia się pod ich markę. Ktoś rozsyła wiadomości z fałszywymi fakturami, zawierającymi nieprawdziwy numer konta.

Maile wyglądają, jakby były wysłane z firmowego adresu Semcore, ale brakuje w nich stopki i innych elementów charakterystycznych dla naszej korespondencji.

Zostałem poproszony o nagłośnienie sprawy. Równolegle podejmujemy działania – zgłoszenia zostały przekazane do operatora poczty oraz do CSIRT NASK.

Show translation



Miejsce wystawienia: Wrocław
Data wystawienia: 2025-04-16
Data sprzedaży / wykonania usługi: 2025-04-16

Proforma nr: 053/1/04-2025

Sprzedawca

PROFES SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ SPÓŁKA
KOMANDYTOWA
ul. Koreńska 13
52-121 Wrocław
NIP: 8971001265
Regon: 930169153

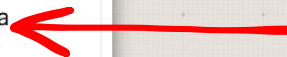
Nabywca

SEMOCRE SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ
ul. Głogowska 70/4
60-740 Poznań
NIP: 7611689477

Nr konta – 95 1090 2617 0000 0001 6203 3076 Santander Bank

Ip.	Nazwa towaru/usługi	Typ GTU	Ilość	Jm	Cena netto	VAT	Kwota netto	Kwota VAT	Kwota brutto
1.	Szkolenie w zakresie planowania strategicznego w zmiennym		2.00	szt	16000.00	23%	32000.00	7360.00	39360.00

Fałszywa faktura wysłana
do księgowości z adresu e-mail
prezesa



☆ MS Marcin Stypuła m.stypula@semcore.pl
PROF053-1/4-2025
Do: ksiegowosc@semcore.pl



W załączniku masz proformę do opłacenia, puść to jeszcze rano ekspresowym.



Miejsce wystawienia: Wrocław
Data wystawienia: 2025-04-16
Data sprzedaży / wykonania usługi: 2025-04-16

Proforma nr: 053/1/04-2025

Sprzedawca

PROFES SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ SPÓŁKA
KOMANDYTOWA
ul. Korańska 13
52-121 Wrocław
NIP: 6971001265
Regon: 930169153

Nr konta – 95 1090 2617 0000 0001 6203 3076 Santander Bank

Nabywca

SEM CORE SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ
ul. Głogowska 70/4
60-740 Poznań
NIP: 7811888477

Ip.	Nazwa towaru/usługi	Typ GTU	Ilość	Jm	Cena netto	VAT	Kwota netto	Kwota VAT	Kwota brutto
1.	Szkolenie w zakresie planowania strategicznego w zmiennym otoczeniu rynkowym (VUCA), z uwzględnieniem geopolityki, ESG i zmian regulacyjnych. (3dniowe)		2.00	szt	16000.00	23%	32000.00	7360.00	39360.00
SUMA: 39 360.00									

Sposób wpłaty: przelew
Termin zapłaty: nie dotyczy
2025-04-16

Stawka VAT	Netto	VAT	Brutto
23%	32 000.00	7 360.00	39 360.00
Razem	32 000.00	7 360.00	39 360.00

Razem do zapłaty: 39 360.00 PLN

Wpłacono: 0.00 PLN

Pozostało do zapłaty: 39 360.00 PLN

Kwota słownie: trzydzieści dziewięć tysięcy trzysta sześćdziesiąt PLN
00/100

Osoba upoważniona do odbioru

Osoba upoważniona do wystawienia

Jak do tego doszło?



Marcin Stypuła m.stypula@semcore.pl
PROF053-1/4-2025
Do: ksiegowosc@semcore.pl

Temat:eDoręczenie: przypomnienie o oczekujących przesyłkach.

Data:Mon, 07 Apr 2025 12:21:50 +0200

Nadawca:eSprawozdania <phtqgsdpvayl50msmlfdvofmmeikcz@ssl-mail.com>

Dzień dobry

Informujemy, że dla adresu do doręczeń elektronicznych **AE:PL-38996-59390-TFCUS-41**, założonego dla Państwa, oczekują na pobranie już od co najmniej 7 dni przesyłki numer: **PPSA-E-94eeaa6c-9416-4c0f-9465-85098dd19118**.

Zgodnie z Ustawą o doręczeniach elektronicznych z dnia 18.11.2020 r. (D. U. poz. 2320) za datę doręczenia korespondencji będzie uznany:

- dzień następujący po upływie 7 dni od dnia przygotowania przesyłki do pobrania przez adresata (jeżeli ostatni dzień terminu odbioru wypada w sobotę lub dzień ustawowo wolny od pracy to ten termin zostaje przedłużony do kolejnego dnia roboczego).

Przypominamy, że nieodebranie przesyłki skutkuje jej usunięciem z systemu po 7 dniach od dnia przygotowania przesyłki do pobrania. Z przesyłkami zapoznasz się po zalogowaniu do skrzynki doręczeń poprzez:

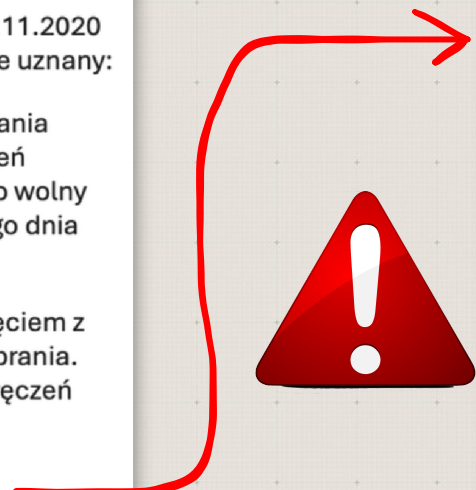
- [Panel Klienta e-Doreczenia](#)
- zintegrowany system kancelaryjny.

Operator Wyznaczony - Poczta Polska S.A.

#nowoczesna #bezpieczna #szybka

www.poczta-polska.pl

E-mail: kontakt@poczta-polska.pl



SCAM

← → ↺ 🔒 <https://govbiznes7pi3h5lz.blob.core.windows.net/vat/index.html>

gov.pl | Serwis Rzeczypospolitej Polskiej

Login Biznes.gov.pl

Zaloguj się przez adresu e-mail

Adres e-mail

[Nie pamiętam adres e-mail](#)

Hasło

[Nie pamiętam hasła](#)

ZALOGUJ SIĘ

e-Urząd Skarbowy – Ministerstwo Finansów

Ref: MOA3PCYZ7

Szanowni Państwo,

Informujemy, że na podstawie przeprowadzonej weryfikacji deklaracji podatkowej PIT-37 za rok podatkowy 2023, dokonanej zgodnie z art. 75 § 2 oraz art. 77 § 1 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz.U. 2023 poz. 1870 z późn. zm.), stwierdzono nadpłatę podatku dochodowego od osób fizycznych.

Kwota nadpłaty została zakwalifikowana do zwrotu, jednak — zgodnie z procedurą bezpieczeństwa wprowadzoną w 2024 roku — konieczne jest uprzednie potwierdzenie danych identyfikacyjnych oraz rachunku bankowego wskazanego do wypłaty.

[Przejdź do weryfikacji](#)

Uwaga:

Potwierdzenie danych umożliwia sprawne rozpoczęcie procedury zwrotu oraz przyspiesza termin wypłaty środków. Zalecamy dokonanie weryfikacji niezwłocznie po otrzymaniu niniejszego zawiadomienia.

Z wyrazami szacunku,
Departament Podatków Bezpośrednich
Ministerstwo Finansów

Wiadomość wygenerowana automatycznie. Prosimy nie odpowiadać.
© 2025 Ministerstwo Finansów – Wszystkie prawa zastrzeżone.

← → ↺ 🔒 https://dev-e-urzdskarbowvy.pantheonsite.io/css/login.php

 podatki.gov.pl

PL 🔍

 Umów wizytę w urzędzie skarbowym

 e-Urząd Skarbowy

e-Urząd Skarbowy

e-Urząd Skarbowy umożliwia Ci załatwienie sprawy





Treści zamieszczone w serwisie niezależnie od celu i sposobu będące przedmiotem praw autorskich

 Oczekujący Zwrot

Proszę wpisać dane bankowe, na które ma zostać dokonany zwrot środków

Akceptowane TYLKO banki: PKO Bank, Alior Kantor, Millennium, Credit Agricole, bnp paribas, SGB.

Numer karty:

Data ważności karty:

MM

RRRR

Kod CVC/CVV:

Jaki jest CVC/CVV kod zabezpieczający?

ZATWIERDŹ

SCAM

mBank | securITUM

Fałszywe rekrutacje – co powinno wzbudzić Twoje podejrzenia?



Brian • 2nd
Recruitment and HR specialist
Gdańsk

Rekruter na LinkedIn zaproponował udział w projekcie, oferując stawkę ~3500 zł / dzień



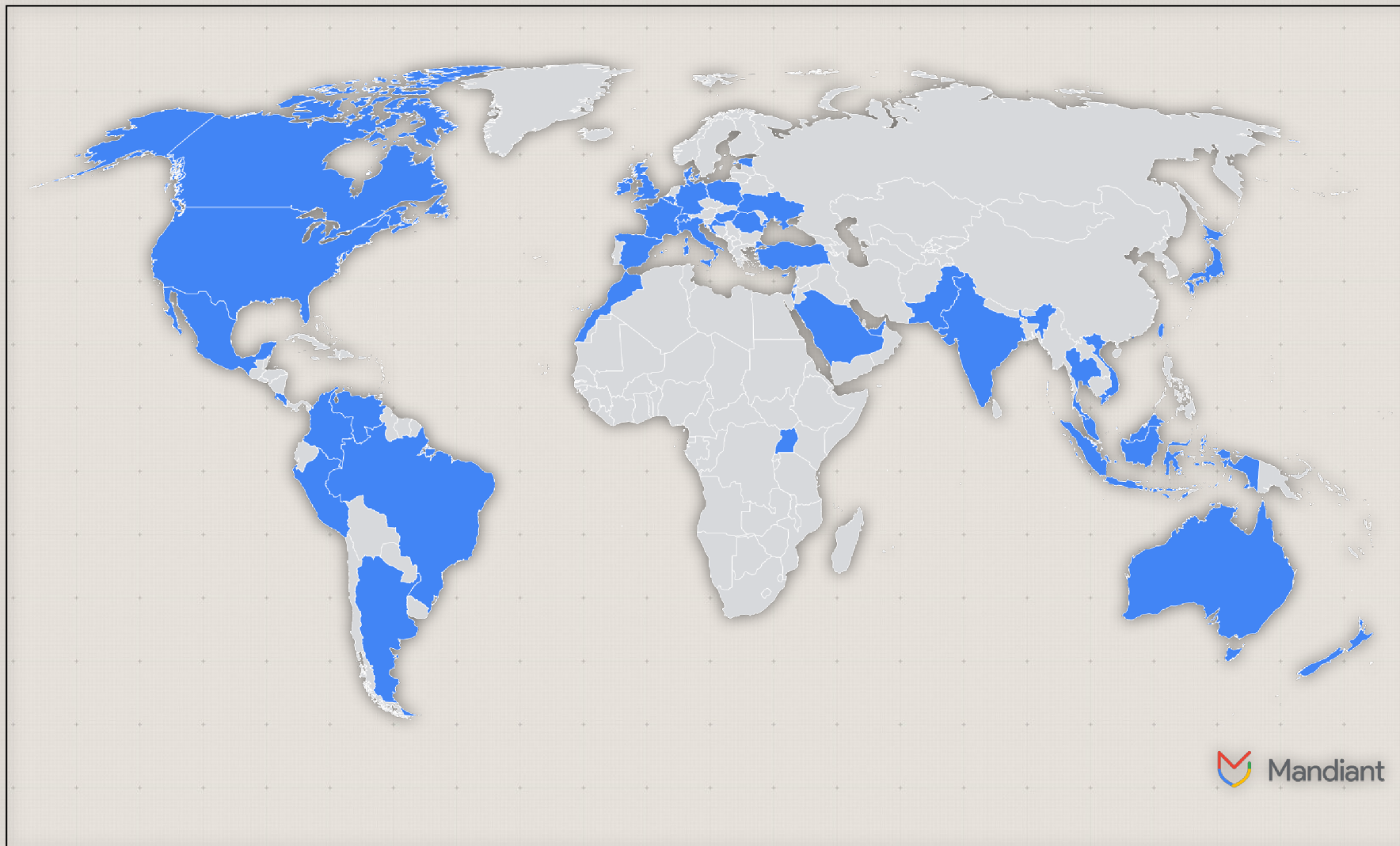
Mini rozmowa rekrutacyjna



"Każda jego odpowiedź była pozytywna, sugerując, że idealnie pasuję. Słyszałem: >Świetnie, dokładnie tego szukamy< "



"[rekruter] przesłał mi nawet dokument opisujący wymagania projektu i moje potencjalne obowiązki. Dokument zawierał listę zadań (ulepszenia UI, interakcje ze smart kontraktami, integracja z "platformą gier"). Wyglądał profesjonalnie i utwierdzał w przekonaniu o autentyczności oferty"



<https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale>



Weryfikuj **adres** e-mail nadawcy e-maila

Kancelaria Prawna SMM LEGAL Maciak Mataczyński <tranmantfescold1987@gmail.com>
to me ▾



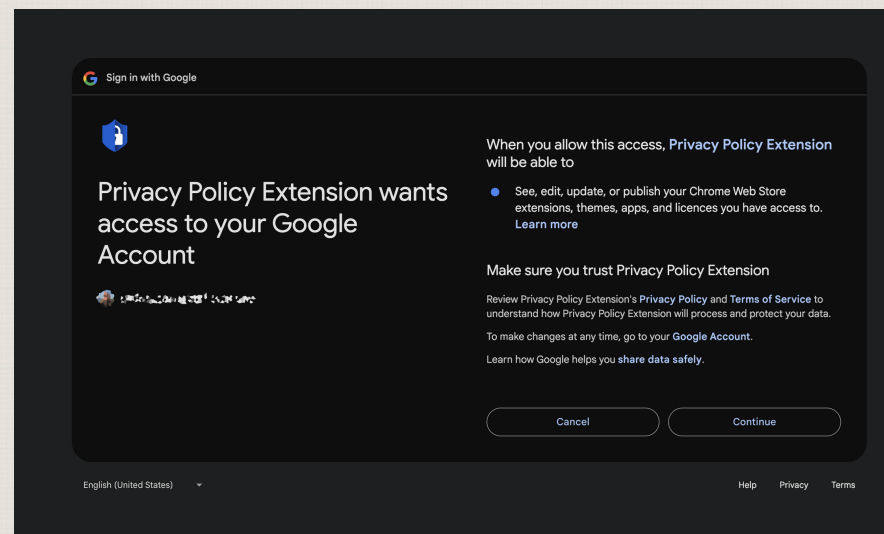
Uważaj, gdy ktoś informuje Cię o zmianie numeru konta



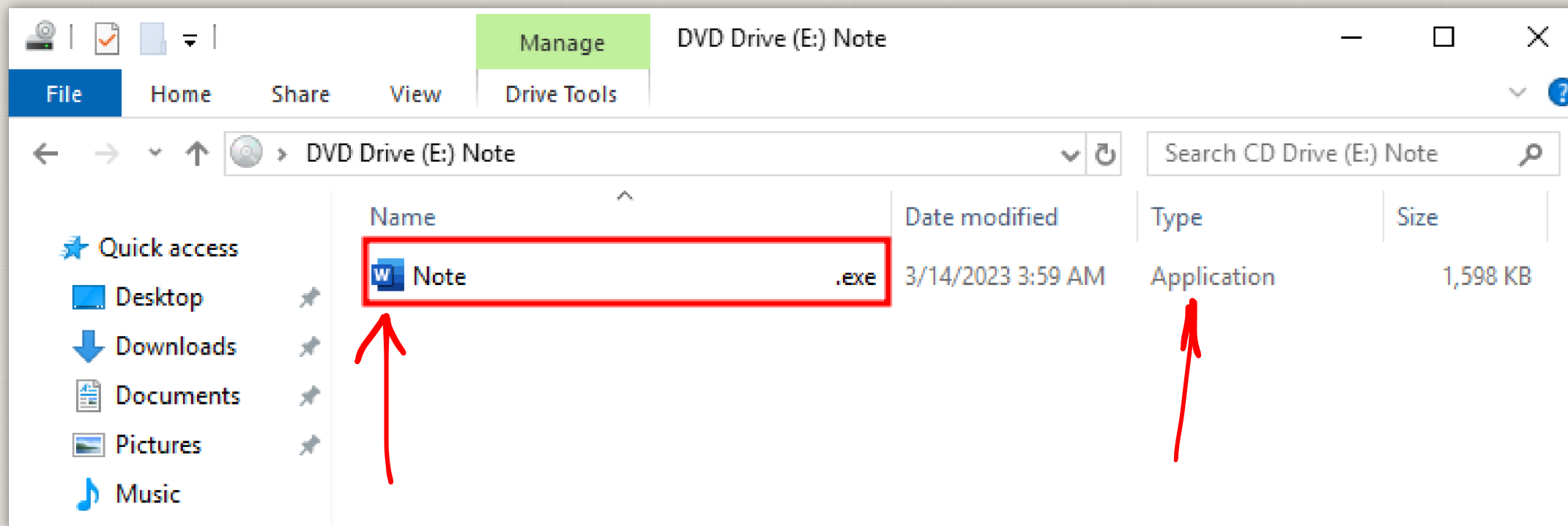
Nie instaluj żadnego oprogramowania polecanego przez rekruterów



Czytaj dokładnie komunikaty związane z bezpieczeństwem



Jak rozpoznawać fałszywe / złośliwe załączniki?



DEMO

Pytania?



michal.sajdak@securitum.pl

 sajdak.sekurak.pl