NIC

EMPOWER

November 13-15, Oslo Spektrum

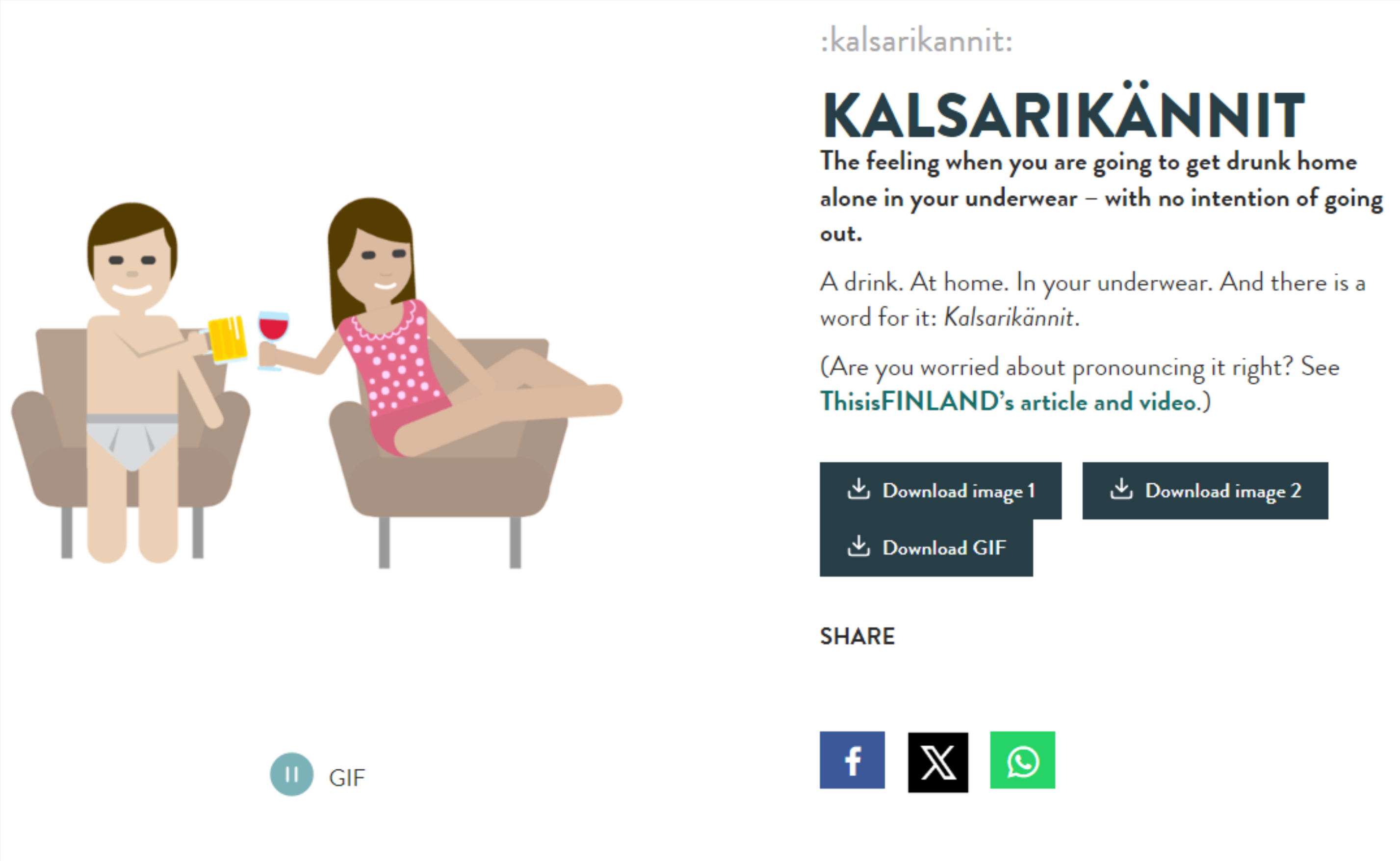
Sami Laiho

Forward to the Past and Back to the Future - Cybercrime in 2023/2024

NIC
EMPOWER

Sami Laiho
Chief Research Officer / MVP

- IT Admin since 1995 / MCT since 2001
- MVP in Windows OS since 2011
- ”100 Most Influencial people in IT in Finland” – TiVi’2019→
- Specializes in and trains:
    - Troubleshooting
    - Windows Internals
    - Security, Social Engineering, Auditing
- Trophies:
    - Best Session at Advanced Threat Summit 2020
    - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020, 2022 and 2023
    - Ignite 2018 – Session #1 and #2 (out of 1708) !
    - TechEd Europe and North America 2014 - Best session, Best speaker
    - TechEd Australia 2013 - Best session, Best speaker



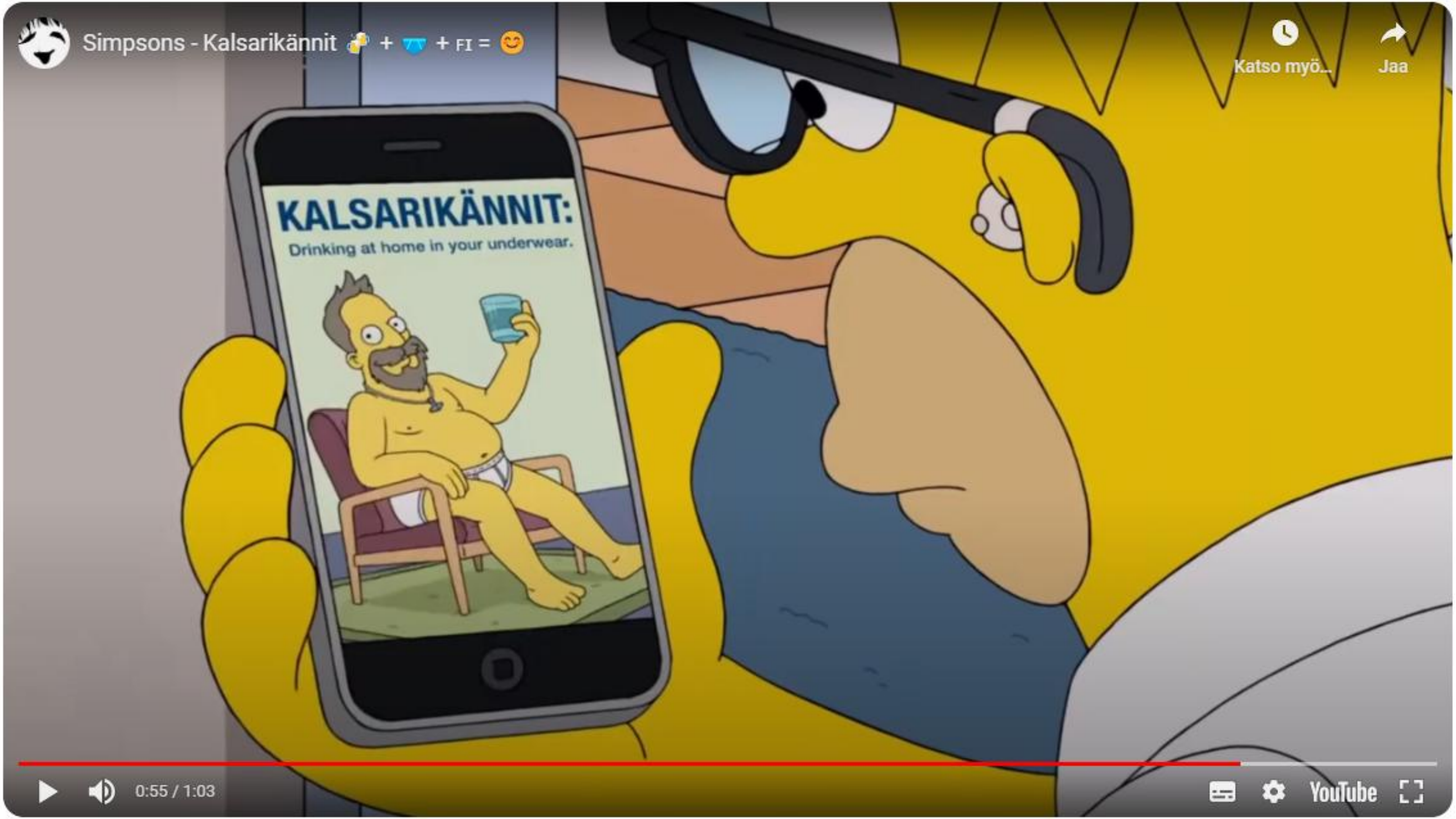
:kalsarikannit:

KALSARIKÄNNIT

The feeling when you are going to get drunk home alone in your underwear – with no intention of going out.

A drink. At home. In your underwear. And there is a word for it: *Kalsarikännit*.

(Are you worried about pronouncing it right? See **ThisisFINLAND's article and video**.)



Simpsons - Kalsarikännit 🍻 + 🩲 + FI = 😊

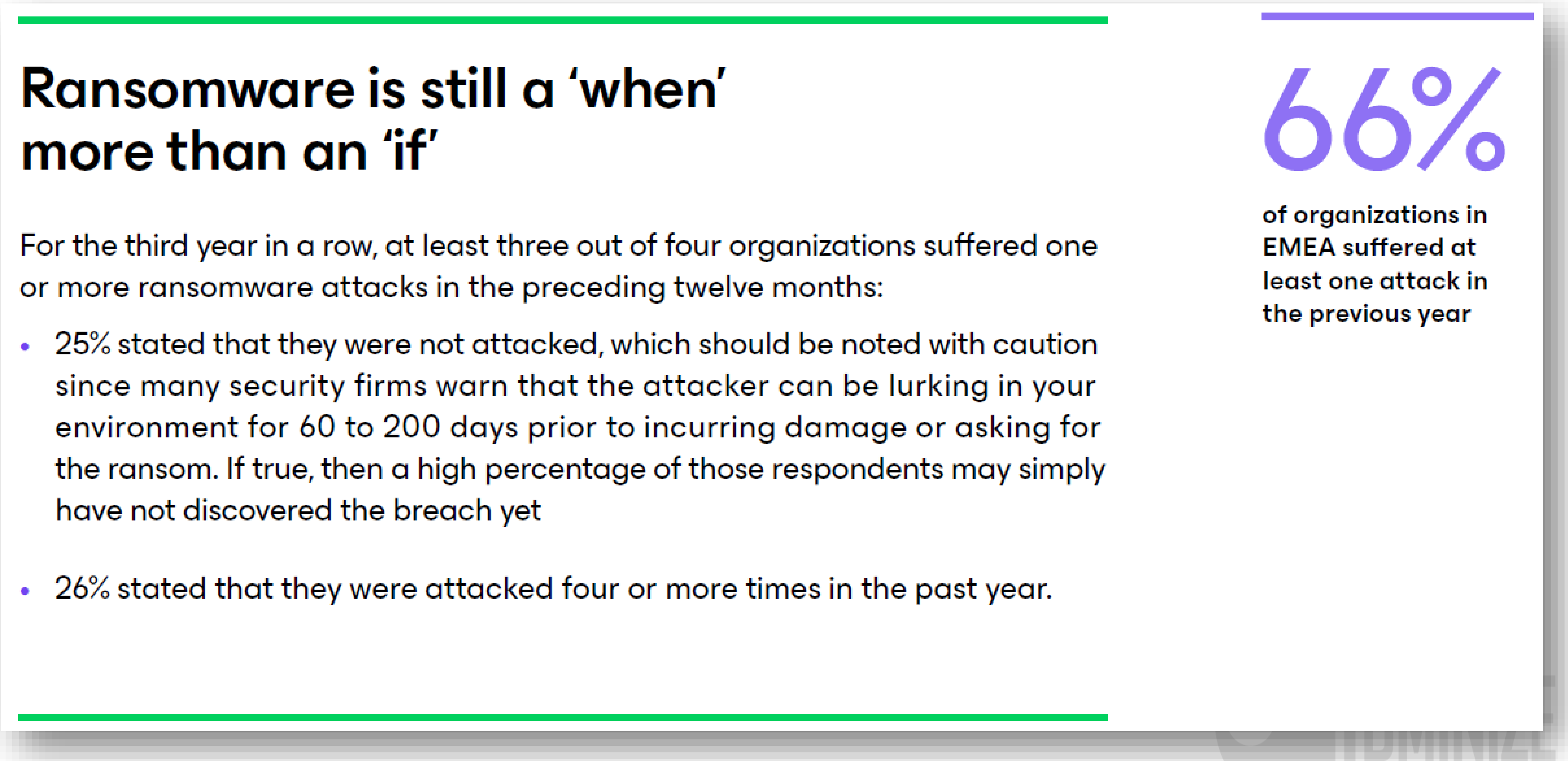
KALSARIKÄNNIT:

Drinking at home in your underwear.

X (ex-Twitter): @samilaiho
Bluesky: @samilaiho.com
LinkedIn

Case Helsinki

21.5.2024 – At least 150000 impacted



Ransomware is still a 'when' more than an 'if'

For the third year in a row, at least three out of four organizations suffered one or more ransomware attacks in the preceding twelve months:

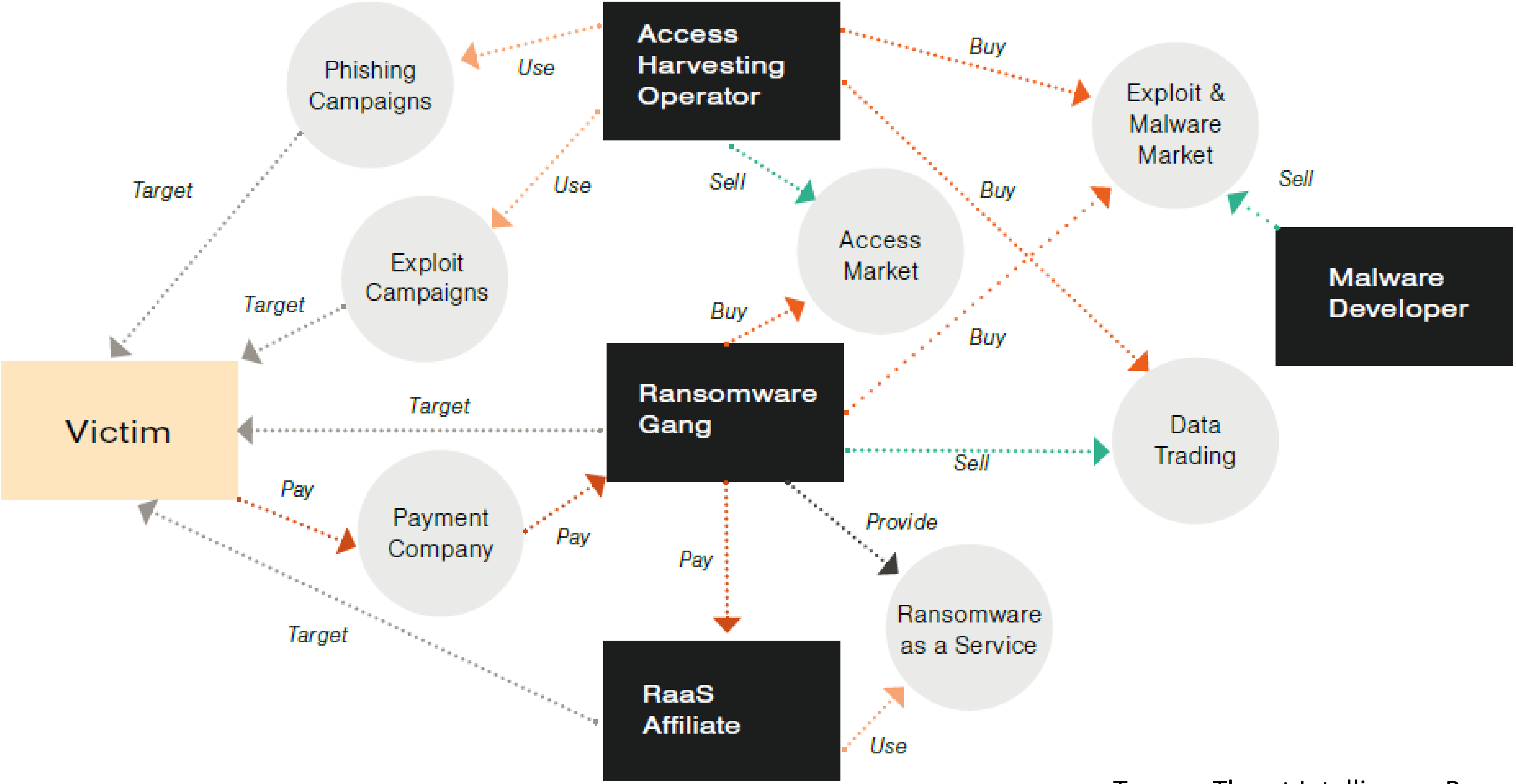
- 25% stated that they were not attacked, which should be noted with caution since many security firms warn that the attacker can be lurking in your environment for 60 to 200 days prior to incurring damage or asking for the ransom. If true, then a high percentage of those respondents may simply have not discovered the breach yet

- 26% stated that they were attacked four or more times in the past year.

66%

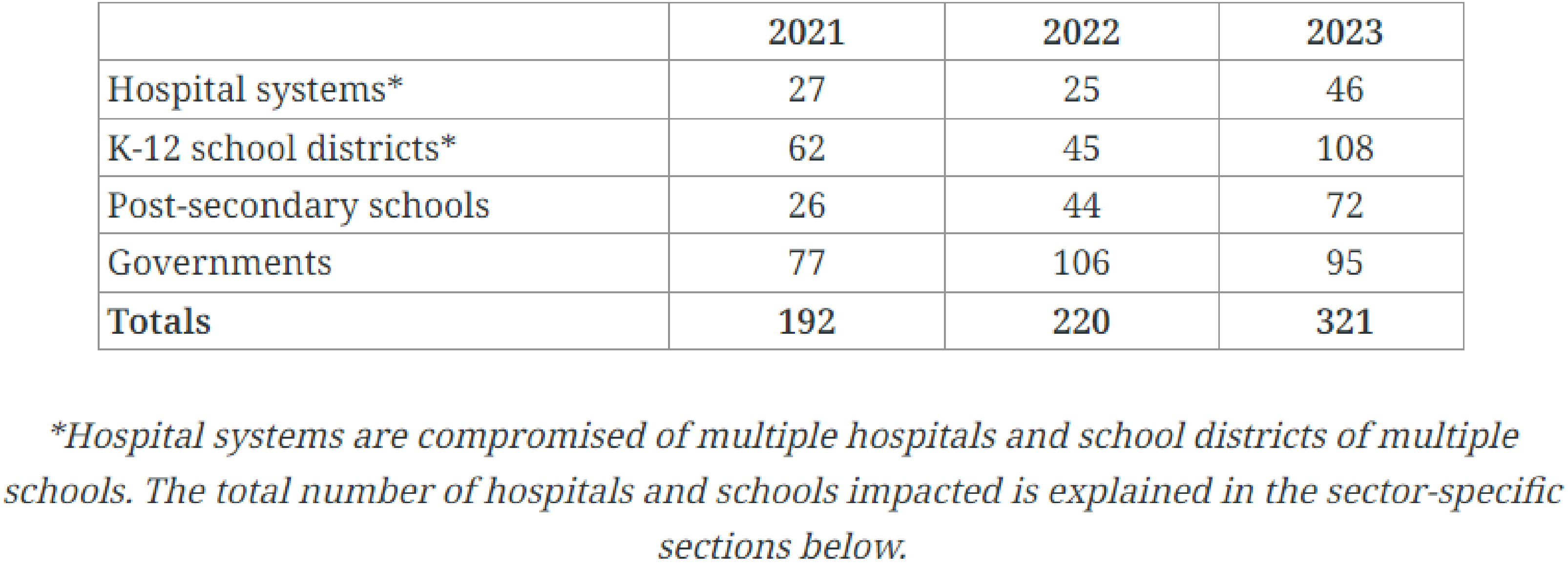
of organizations in EMEA suffered at least one attack in the previous year

* Veeam EMEA



Truesec Threat Intelligence Report

USA – Ransomware Cases



	2021	2022	2023
Hospital systems*	27	25	46
K-12 school districts*	62	45	108
Post-secondary schools	26	44	72
Governments	77	106	95
Totals	**192**	**220**	**321**

**Hospital systems are compromised of multiple hospitals and school districts of multiple schools. The total number of hospitals and schools impacted is explained in the sector-specific sections below.*

Average Ransoms Paid in US

- 2018 = 5000$
- 2023 = 1.500.000$

Last week VmWare 0-day vulnerability

- Price: 1,7M$
- When Criminals get more money their budget for the next attacks increase → 0-Day attacks become more common
- Sadly, the enemy is also becoming more bold and cruel…

NOT Happy #1

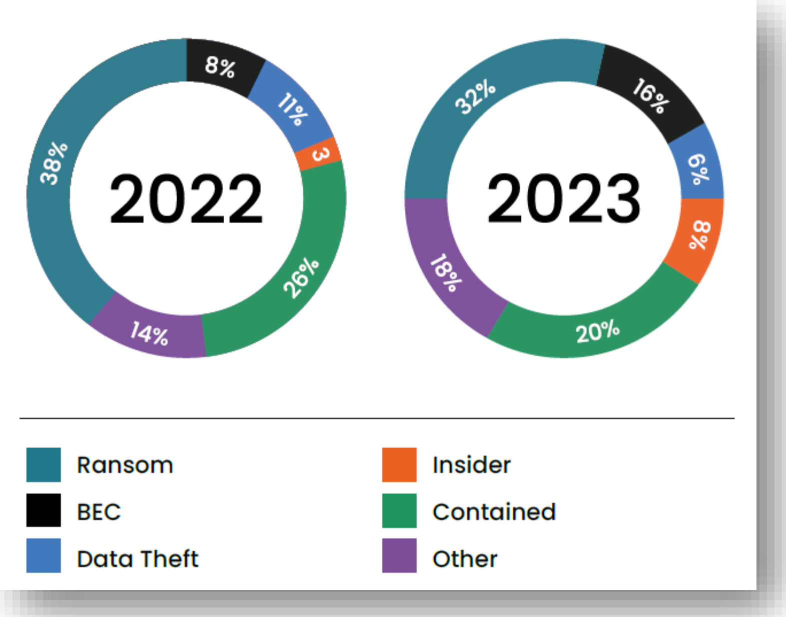
- "Nearly 83% of all traffic to Finland was network-layer attack traffic. China followed closely with 68% and Singapore again with 49%".

NIC
EMPOWER

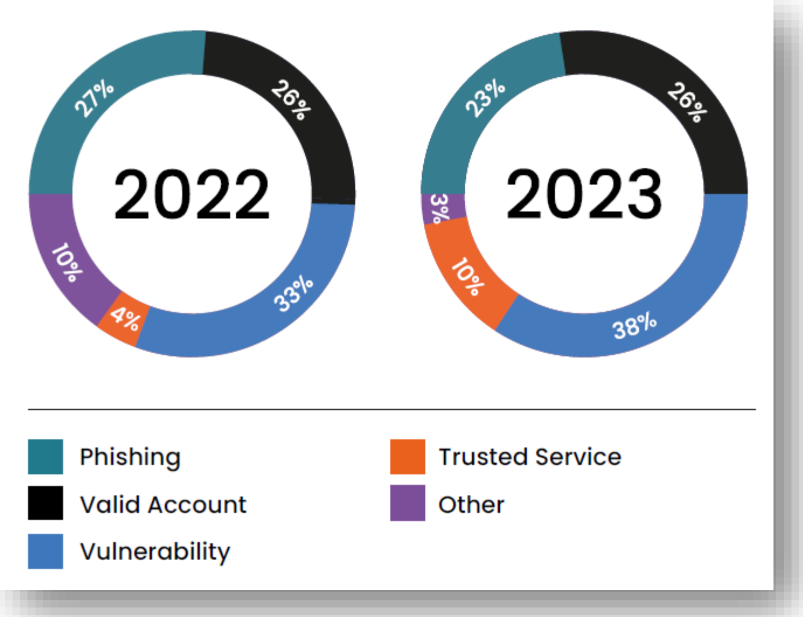
Nordea DDoS

Attack coming from Nordic homes

Attack types

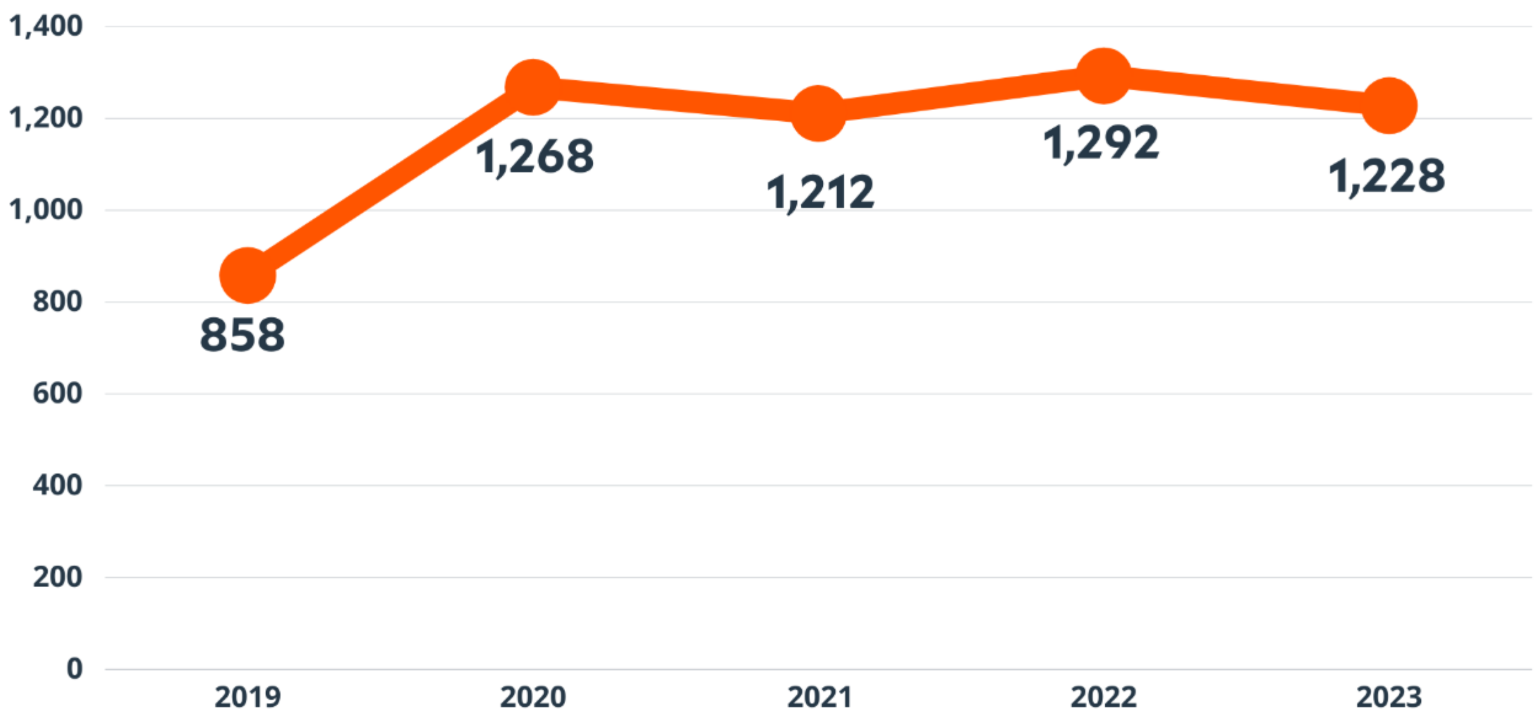


Attack vectors



*Truesec Threat Intelligence Report 2024

Total Number of Microsoft Vulnerabilities (2019-2023)



Finland in 2023

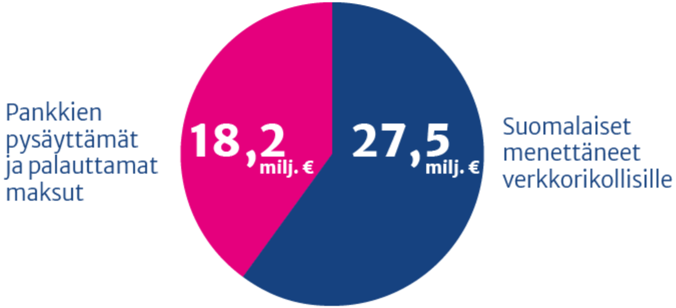
HUIJAUKSET JA PETOKSET

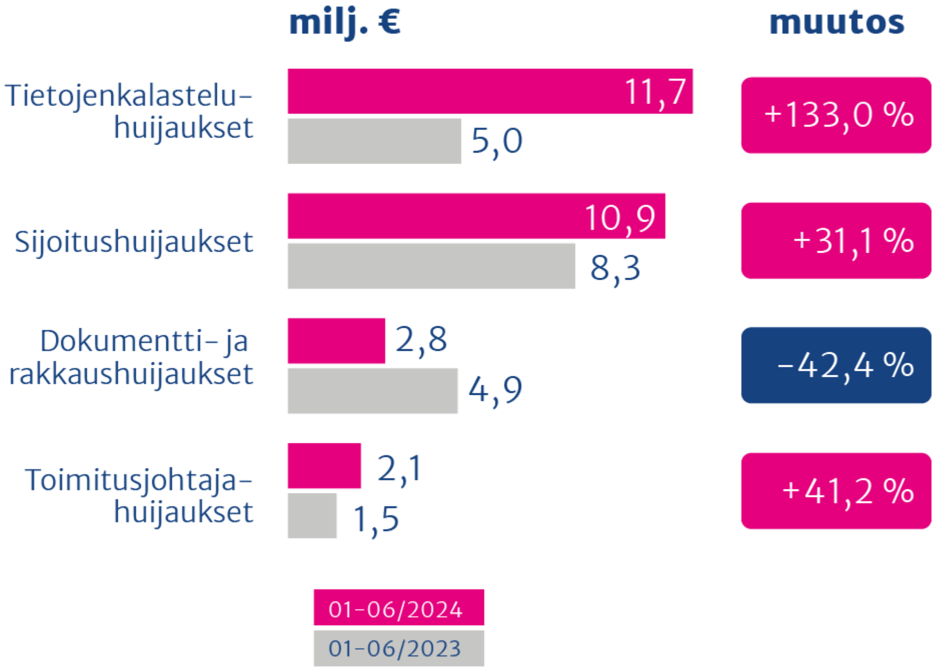
PANKKIEN TIETOON TULLEET HUIJAUKSET

Huijauksia yhteensä 01–06/2024

45,7 milj. €

+28,2 % vrt. 01–06/2023

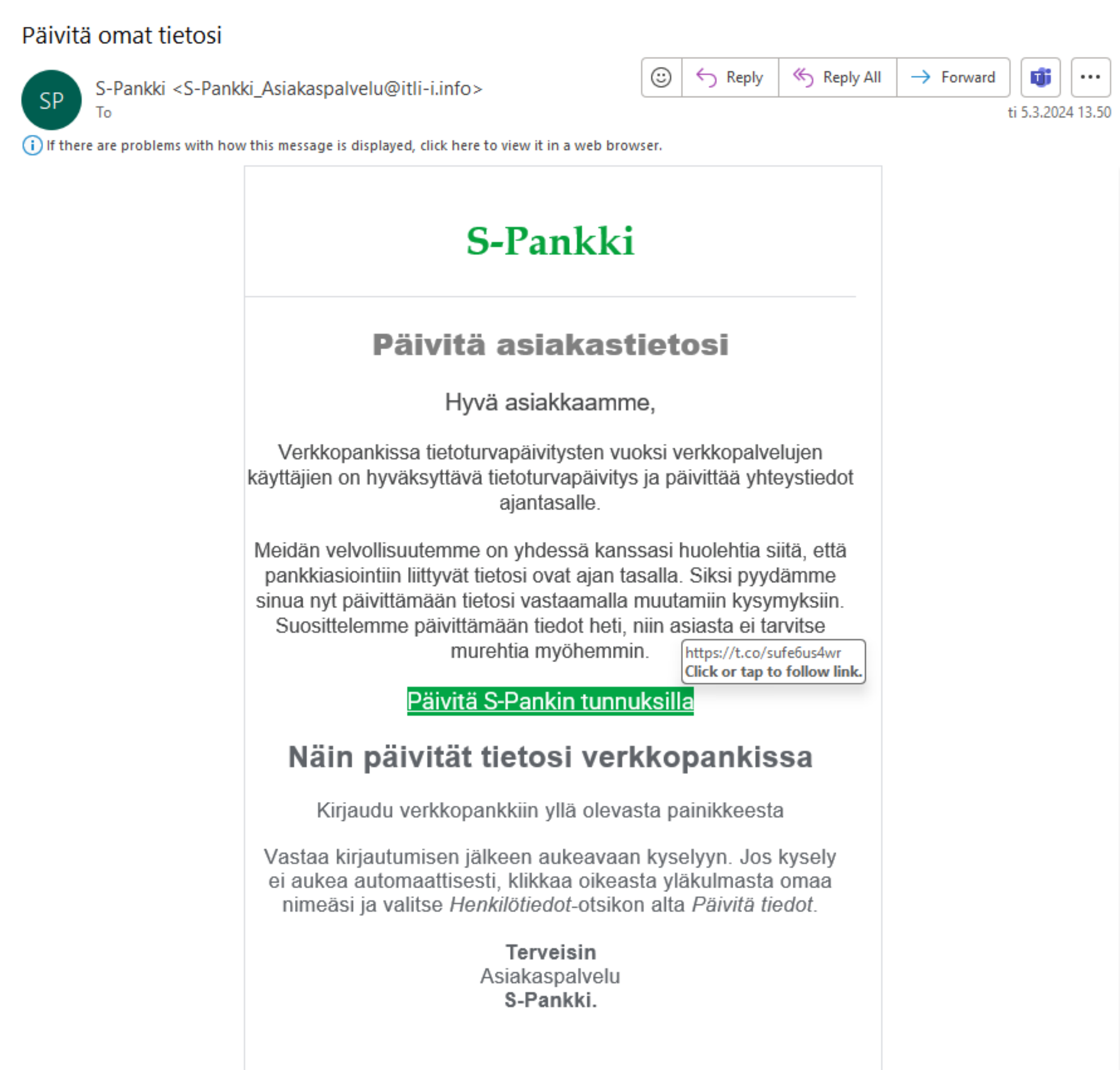




Lähde: FA

How to avoid being scammed

- Call Back!
  - “Because of recent security incidents, I need to call you back”
- Remember that banks (and other officials) do not send links in messages or email
  - When you open an SMS on the phone and reply to it, the links get activated – Hence, if someone instructs you to do so, they are not up to any good
- When ever you visit a website that handles money (or equal assets) or your private information, always use their address (or a shortcut you built) directly, and NEVER through a Google search!
  - Make shortcuts/favorites for the ones you use constantly, and use them
- If someone says that they know your password or other personal information, don’t care – they have been found on some other breach and used to make you convinced that they have hacked you – They have not.
  - New twist is the “I know where you live” scam using Google Street View images



Päivitä omat tietosi

S-Pankki <S-Pankki_Asiakaspalvelu@itli-i.info>
To

ti 5.3.2024 13.50

If there are problems with how this message is displayed, click here to view it in a web browser.

S-Pankki

Päivitä asiakastietosi

Hyvä asiakkaamme,

Verkkopankissa tietoturvapäivitysten vuoksi verkkopalvelujen käyttäjien on hyväksyttävä tietoturvapäivitys ja päivittää yhteystiedot ajantasalle.

Meidän velvollisuutemme on yhdessä kanssasi huolehtia siitä, että pankkiasiointiin liittyvät tietosi ovat ajan tasalla. Siksi pyydämme sinua nyt päivittämään tietosi vastaamalla muutamiin kysymyksiin. Suosittelemme päivittämään tiedot heti, niin asiasta ei tarvitse murehtia myöhemmin.

https://t.co/sufe6us4wr
Click or tap to follow link.

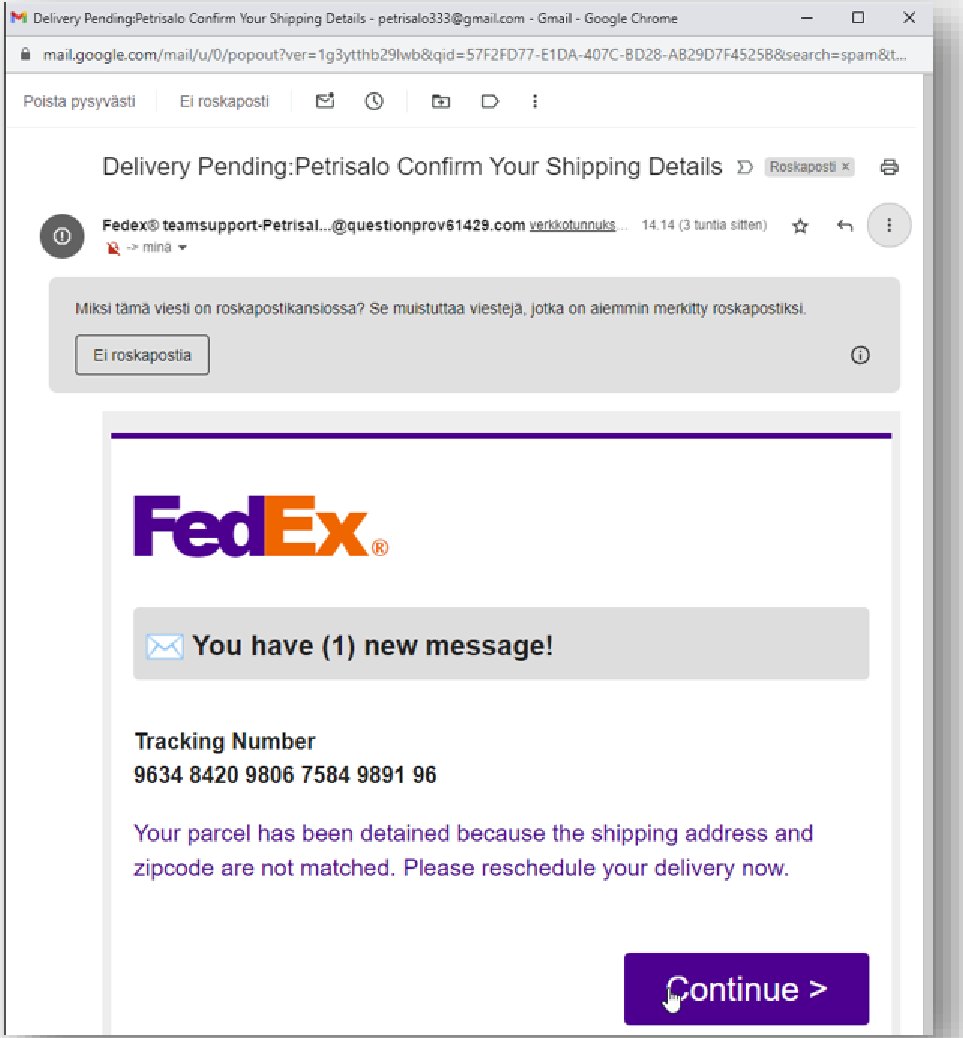
Päivitä S-Pankin tunnuksilla

Näin päivität tietosi verkkopankissa

Kirjaudu verkkopankkiin yllä olevasta painikkeesta

Vastaa kirjautumisen jälkeen aukeavaan kyselyyn. Jos kysely ei aukea automaattisesti, klikkaa oikeasta yläkulmasta omaa nimeäsi ja valitse *Henkilötiedot*-otsikon alta *Päivitä tiedot*.

Terveisin
Asiakaspalvelu
S-Pankki.


Delivery Pending:Petrisalo Confirm Your Shipping Details - petrisalo333@gmail.com - Gmail - Google Chrome
mail.google.com/mail/u/0/popout?ver=1g3ytthb29lwb&qid=57F2FD77-E1DA-407C-BD28-AB29D7F4525B&search=spam&t...
Poista pysyvästi
Ei roskaposti
Roskaposti ×

Delivery Pending:Petrisalo Confirm Your Shipping Details

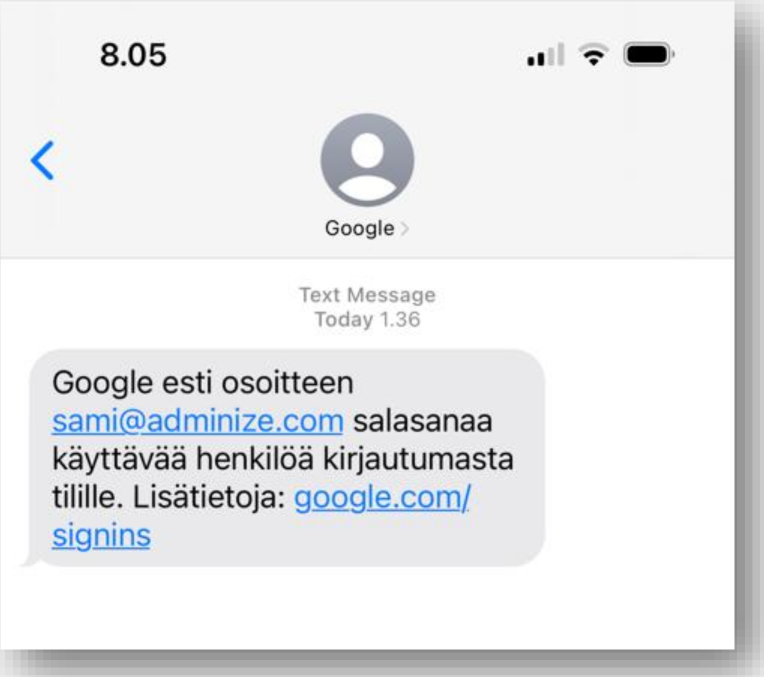
Fedex© teamsupport-Petrisal...@questionprov61429.com verkkotunnuks... 14.14 (3 tuntia sitten)
-> minä

Miksi tämä viesti on roskapostikansiossa? Se muistuttaa viestejä, jotka on aiemmin merkitty roskapostiksi.

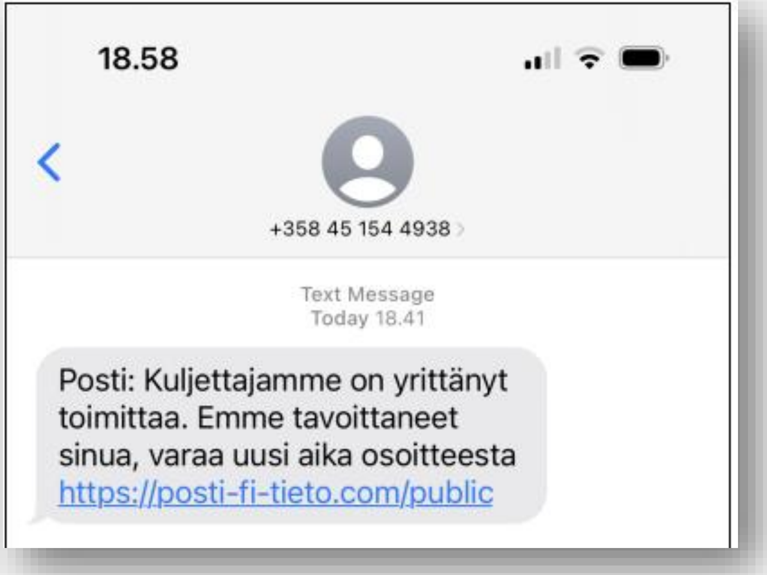
✉️ You have (1) new message!

Tracking Number
9634 8420 9806 7584 9891 96

Your parcel has been detained because the shipping address and zipcode are not matched. Please reschedule your delivery now.

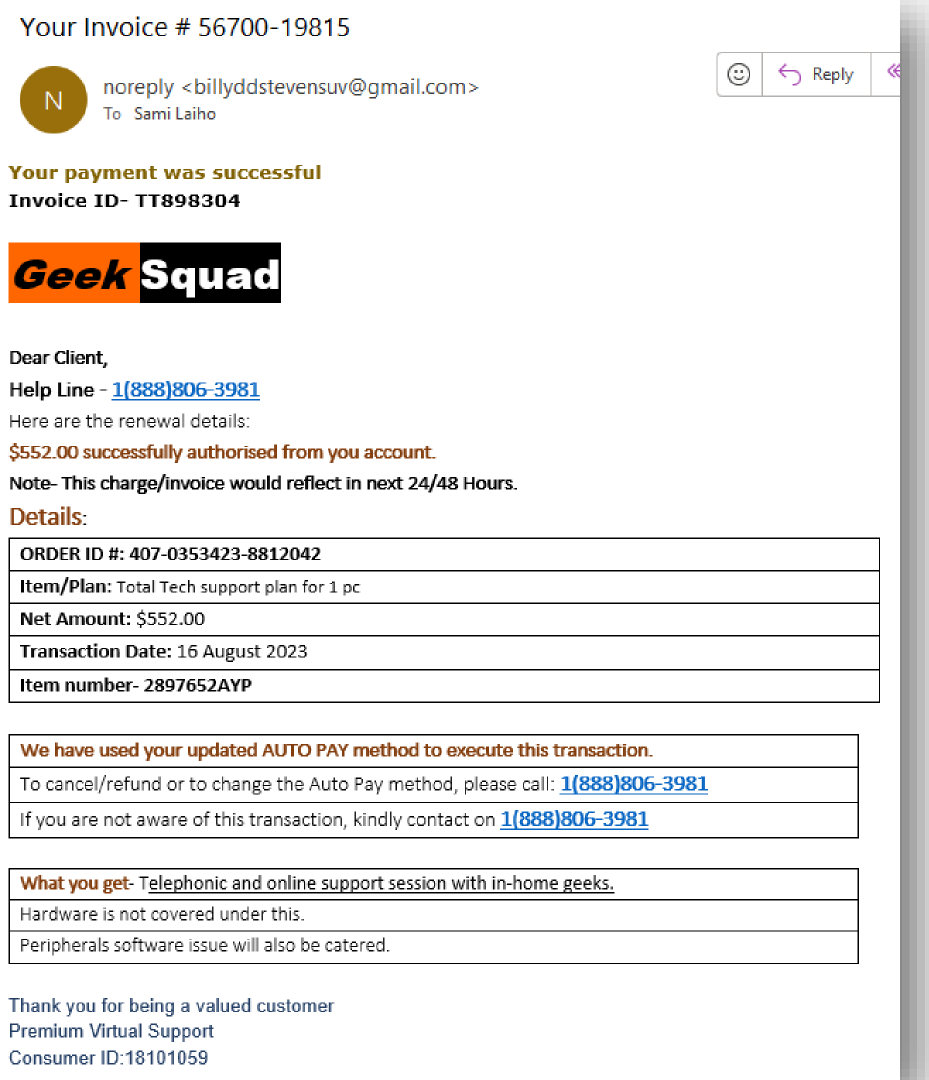


Google esti osoitteen sami@adminize.com salasanaa käyttävää henkilöä kirjautumasta tilille. Lisätietoja: google.com/signins



Posti: Kuljettajamme on yrittänyt toimittaa. Emme tavoittaneet sinua, varaa uusi aika osoitteesta https://posti-fi-tieto.com/public

NIC
EMPOWER



Your Invoice # 56700-19815

noreply <billyddstevensuv@gmail.com>
To Sami Laiho

Your payment was successful
Invoice ID- TT898304

Dear Client,
Help Line - 1(888)806-3981

Here are the renewal details:

$552.00 successfully authorised from you account.

Note- This charge/invoice would reflect in next 24/48 Hours.

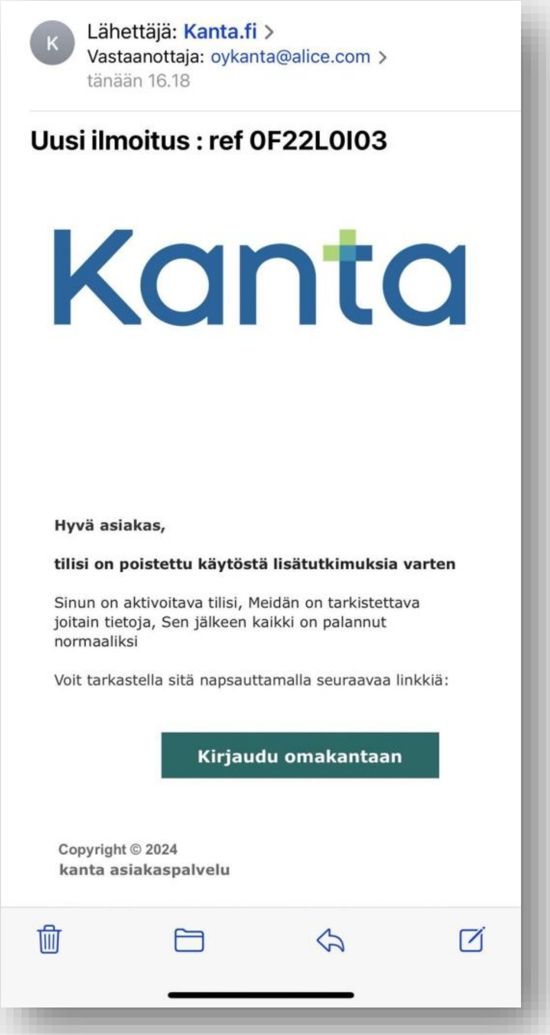
Details:

ORDER ID #: 407-0353423-8812042
Item/Plan: Total Tech support plan for 1 pc
Net Amount: $552.00
Transaction Date: 16 August 2023
Item number- 2897652AYP

We have used your updated AUTO PAY method to execute this transaction.
To cancel/refund or to change the Auto Pay method, please call: **1(888)806-3981**
If you are not aware of this transaction, kindly contact on **1(888)806-3981**

What you get- Telephonic and online support session with in-home geeks.
Hardware is not covered under this.
Peripherals software issue will also be catered.

Thank you for being a valued customer
Premium Virtual Support
Consumer ID:18101059



Lähettäjä: Kanta.fi
Vastaanottaja: oykanta@alice.com
tänään 16.18

Uusi ilmoitus : ref 0F22L0I03

Hyvä asiakas,

tilisi on poistettu käytöstä lisätutkimuksia varten

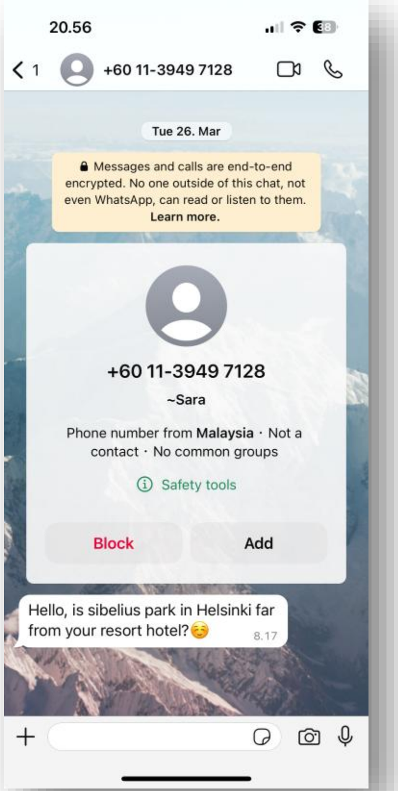
Sinun on aktivoitava tilisi, Meidän on tarkistettava joitain tietoja, Sen jälkeen kaikki on palannut normaaliksi

Voit tarkastella sitä napsauttamalla seuraavaa linkkiä:

Copyright © 2024
kanta asiakaspalvelu

WhatsApp / Signal Scams

"Carly"



20.56

+60 11-3949 7128

Tue 26. Mar

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. **Learn more.**

+60 11-3949 7128

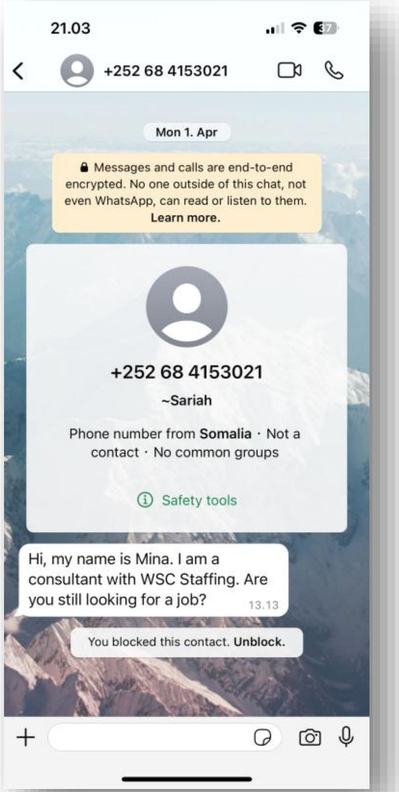
~Sara

Phone number from **Malaysia** · Not a contact · No common groups

ⓘ Safety tools

Block | Add

Hello, is sibelius park in Helsinki far from your resort hotel?☺️ 8.17



21.03

+252 68 4153021

Mon 1. Apr

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. **Learn more.**

+252 68 4153021

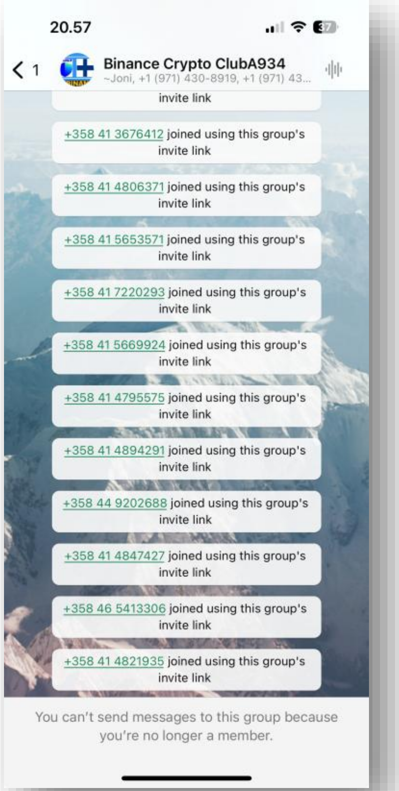
~Sariah

Phone number from **Somalia** · Not a contact · No common groups

ⓘ Safety tools

Hi, my name is Mina. I am a consultant with WSC Staffing. Are you still looking for a job? 13.13

You blocked this contact. **Unblock.**



20.57

Binance Crypto ClubA934

~Joni, +1 (971) 430-8919, +1 (971) 43...

invite link

+358 41 3676412 joined using this group's invite link

+358 41 4806371 joined using this group's invite link

+358 41 5653571 joined using this group's invite link

+358 41 7220293 joined using this group's invite link

+358 41 5669924 joined using this group's invite link

+358 41 4795575 joined using this group's invite link

+358 41 4894291 joined using this group's invite link

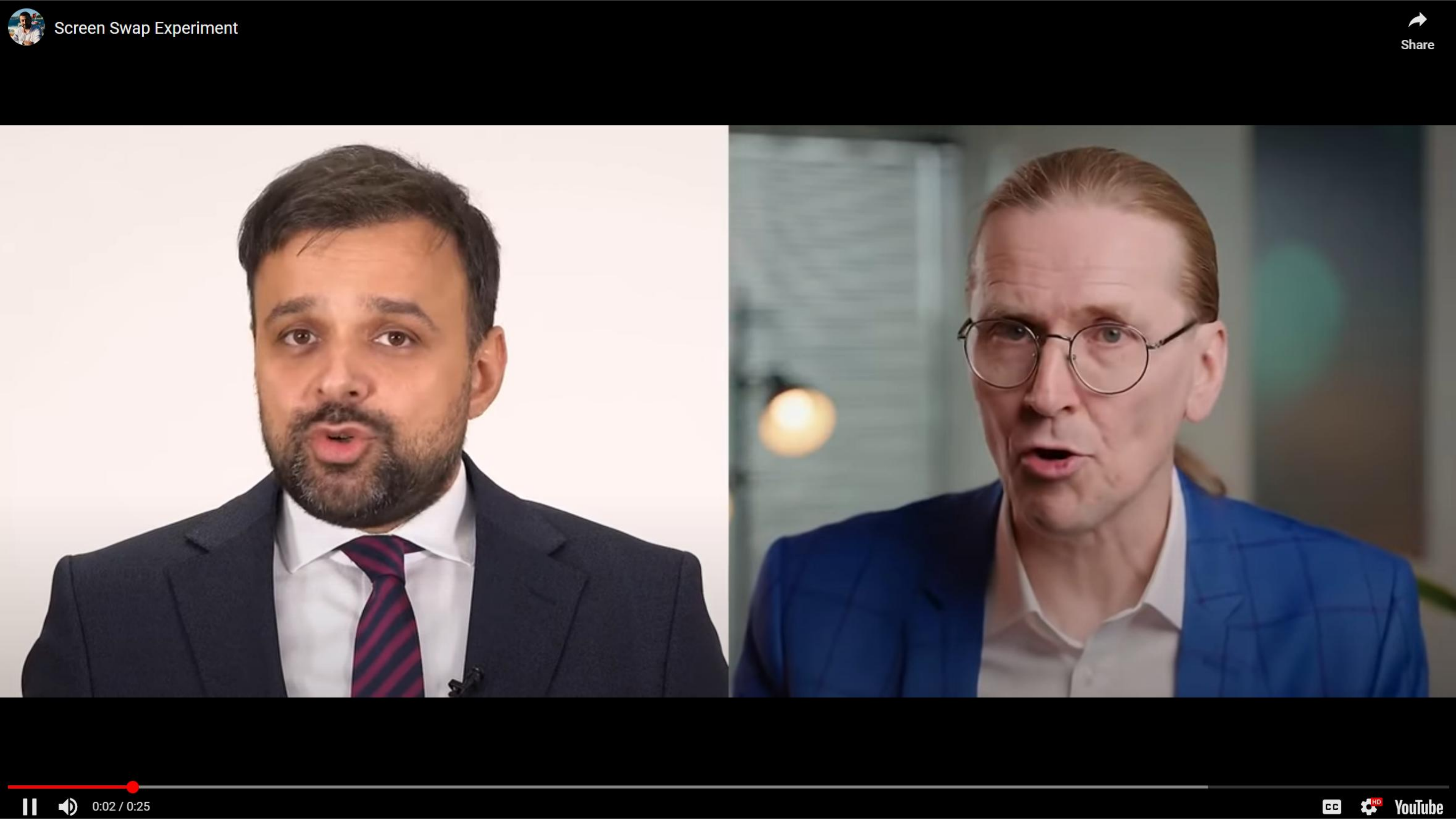
+358 44 9202688 joined using this group's invite link

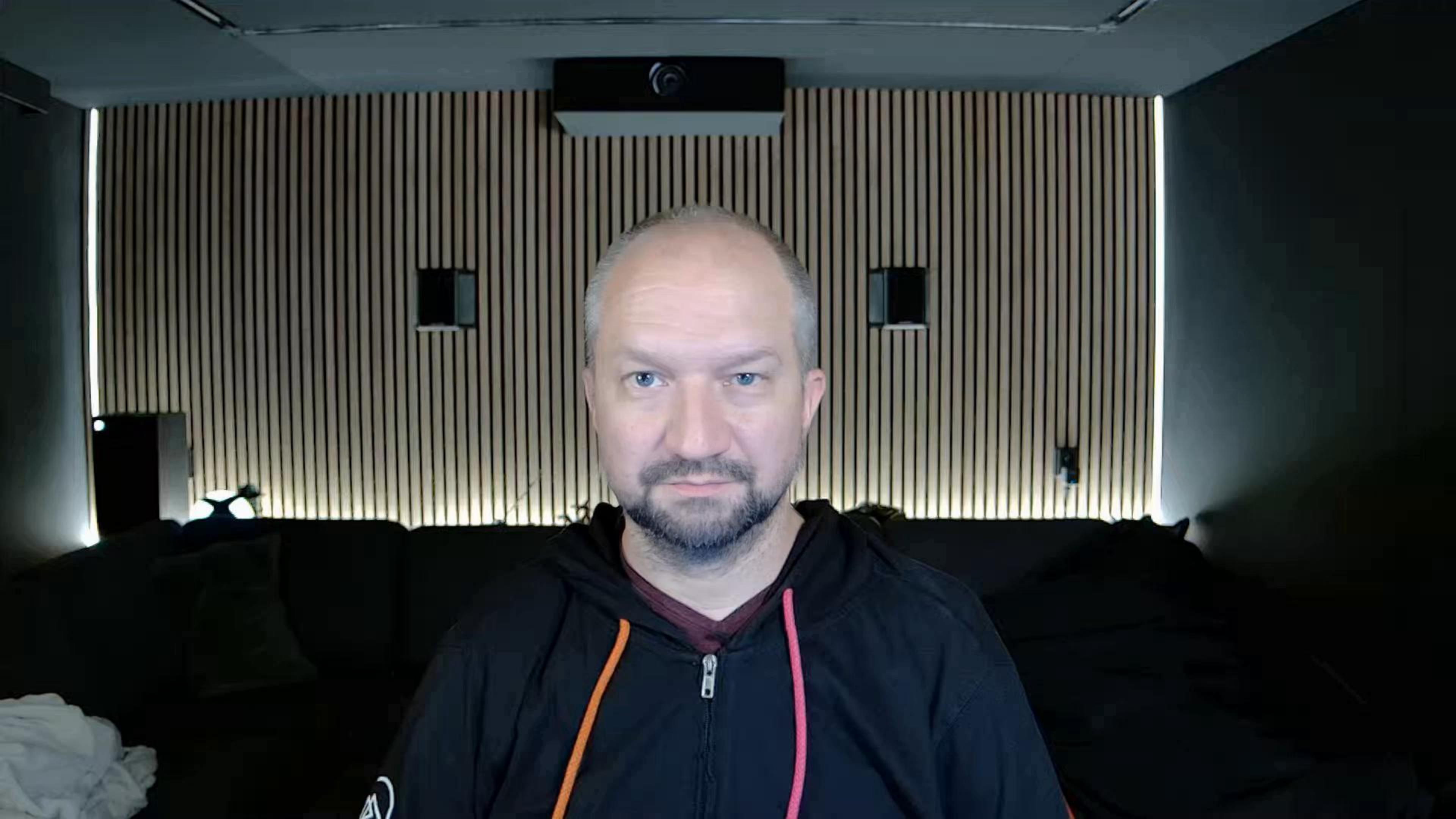
+358 41 4847427 joined using this group's invite link

+358 46 5413306 joined using this group's invite link

+358 41 4821935 joined using this group's invite link

You can't send messages to this group because you're no longer a member.


Screen Swap Experiment
Share
0:02 / 0:25
YouTube



TED

16.1.2024

First Recorded Case of CEO Scam^2 in Finland

Meet SamiBot

What can I do to avoid AI-scams?

Call back

Ask to turn their head

Secret word or secret gesture

Password Quality

NIST SP 800-63 standard

- Passwords shorter than eight characters are prohibited, with a minimum of 15 characters recommended.
- Scheduled, mandatory password rotation is considered an outdated practice and therefore prohibited.
- It’s also prohibited to impose requirements on password composition (such as “your password must contain a letter, a number, and a symbol”).
- It’s recommended to allow using any visible ASCII characters, spaces, and most Unicode symbols (such as emojis).
- Maximum password length, if enforced, must be at least 64 characters.
- Using and storing password hints or security questions (such as “your mother’s maiden name”) is prohibited.
- Commonly used passwords must be eliminated through the use of a stop-list of popular or leaked passwords.
- Compromised passwords (for example, appearing in data breaches) must be reset immediately.
- Login attempts must be limited in both rate and number of unsuccessful attempts.

How to protect your home computer/network

- Make your daily account a limited user, and create a separate admin-account
  - Or use MakeMeAdmin https://github.com/pseymour/MakeMeAdmin
- Update system updates instantly when you get them
  - "Short and controlled downtime" vs "Long and expensive downtime controlled by someone else"
- Set routers and IoT devices to automatically update themselves
- If you use a 4G/5G connection on your laptop, block Remote Desktop in your Windows firewall – It's open buy default
- If you are Tec savvy
  - separate IoT-devices to separate network
  - and you need to access your devices from the outside, use Tailscale or equal Wireguard VPN

How to protect your home computer/network

- Use a different password for every system
  - You should have a password manager
  - It’s more important to have a strong password than it is to periodically change them
- Never leave the default password on anything!
- Use Biometrics or PIN-codes if they are available
  - In Windows a 6 digit PIN-code is safer than a 15 character password, as it is tied to the security chip (TPM) of your computer and will not work anywhere else
- Always use MFA if available

How to protect against scams at home

- Always use a phone/tablet rather than a computer
  - Reboot your handheld devices occasionally
- Use a mobile certificate (in Finland we have this thing called the "Mobiilivarmenne") for everything else except online banking

- You should do a favor for your parents as well by teaching them to do the same

Contact

- sami@adminize.com
- Twitter: @samilaiho
- BlueSky: @samilaiho.com
- Free newsletter: http://eepurl.com/F-Goj
- Find me on LinkedIn – **Please!**
- My trainings:
- Corellia (FIN)
- ETC.at (ENG)
- https://win-fu.com/dojo/
    - Free for one month!!
        - Promo Code: TRIAL2023

Thank you!
Remember the Evals

NIC
EMPOWER