Miten toimit turvallisesti digimaailmassa?

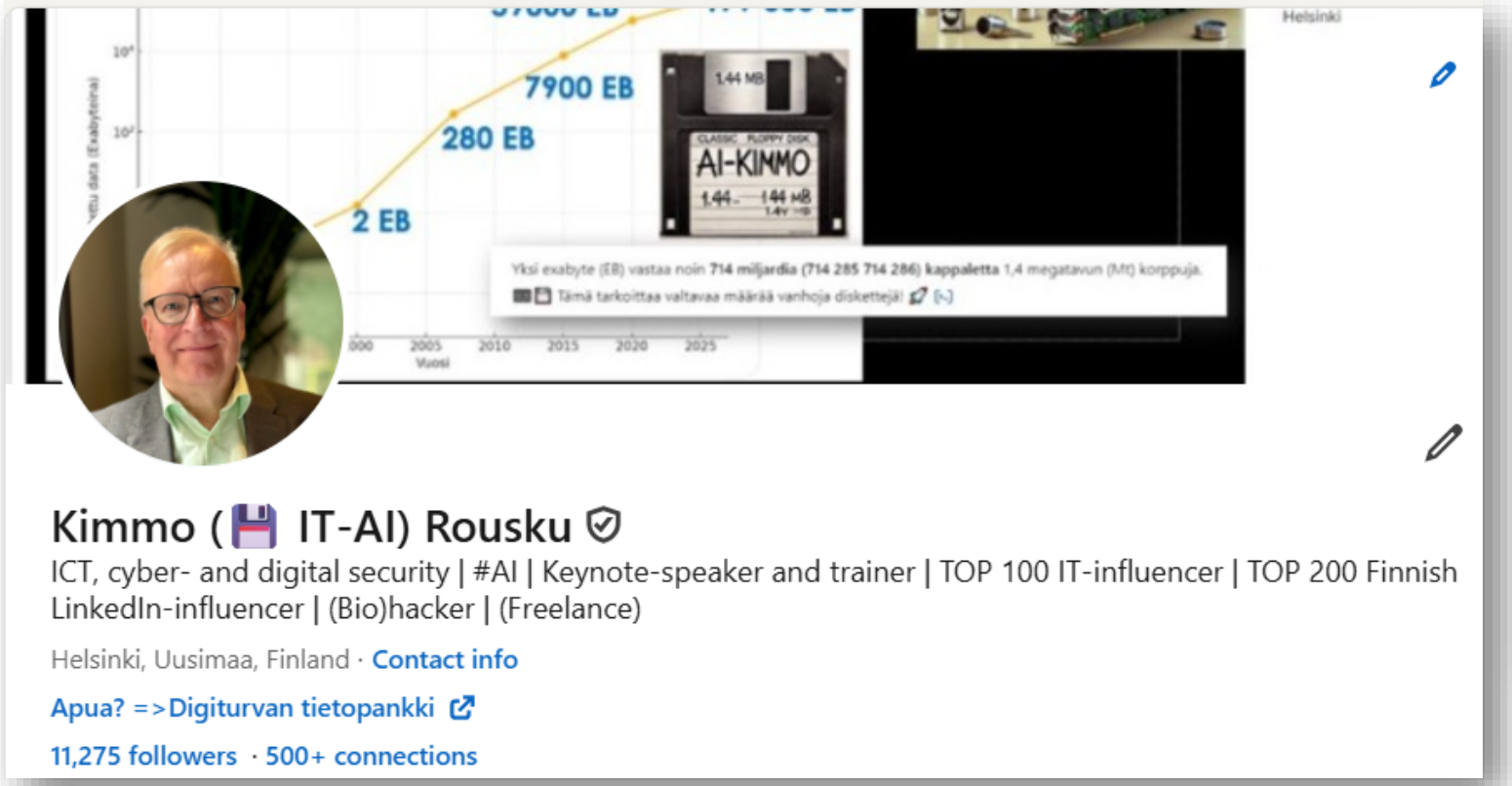
27.10.2025 SurfAreena
Kimmo Rousku – kimmo.rousku@dvv.fi
Vapaa-aika: kimmo.rousku@tietoturva.fi

DIGI- JA VÄESTÖTIETO-VIRASTO

Kimmo Rousku

- Ensimmäinen tietokone vuonna 1983 Commodore 64
- **Ensimmäinen pitämäni koulutus 15.2.1985**
- Freelancer 1986-1994, nyt sivutoiminen tietokirjailija ja kouluttaja
- Valtionhallinnossa 1994->
- Töissä Digi- ja väestötietovirasto (johtava erityisasiantuntija, VAHTI-verkoston pääsihteeri)
- ATK => ICT => Digitalisaation edistäminen
- Tietoturva => kyberturva => digiturvan edistäminen
- (Bio)hakkeri
- Harrastan digihärpättimiä, (virtuaali)matkailua, vanhoja äänentoistolaitteita
- Toimin Tietoturva ry hallituksen varapj ja olen Enter ry jäsen

Verkostoidu kanssani – saat paljon aiheeseen lisätietoa ja yhteyden minuun!



X/Twitter: @kimmorousku sekä @IT_kimmo

LinkedIn: https://www.linkedin.com/in/kimmorousku/

BluSkySocial: @kimmorousku
Meta Threads: @kimmorousku

Kimmo houkutteli Windows-huijarit ansaan – heittäytyi mukaan juoneen ja päästi käsiksi laitteilleen: Näin hulvaton operaatio eteni

Kimmo Rousku houkutteli Windows-huijarit ansaan ja dokumentoi operaation – kuuntele huijarin puhelinsoitto

Tietoturva-asiantuntija: Vastaamon johto vastuussa tietomurrosta – "Riskienhallinta petti, pahoin pelkään, että vastaavia tietomurtoja tulee jatkossakin"

Katso yllä oleva video: Kimmo Rousku kertoo, miten ulkomailla on toimittu tietomurtojen osalta.

TIETOTURVA

IT-Kimmon sähköpostiin pamahti samalla kertaa 10 huijausviestiä – antaa tärkeän ohjeen

Suomi.fi:n nimissä huijataan, ja kalasteluviestien kohteeksi joutui myös palvelusta vastaavassa virastossa työskentelevä asiantuntija.

JAA TALLENNA KOMMENTIT

Yksi pieni merkki kertoo paljon verkko-osoitteessa. KUVA: TOMASZ ZAJDA VIRRAGE IMAGES INC / COLOURBOX

Tuomas Linnake
15.3. 6:12

DIGI & TEKNIIKKA

DIGI & TEKNIIKKA | TIETOTURVA

Kaunis nainen pommitti Kimmoa mobiilipelissä – huijari ei tiennyt valinneensa huonoimman mahdollisen kohteen

Kalifornialaisnainen halusi suhteen, joka johtaisi avioliittoon.

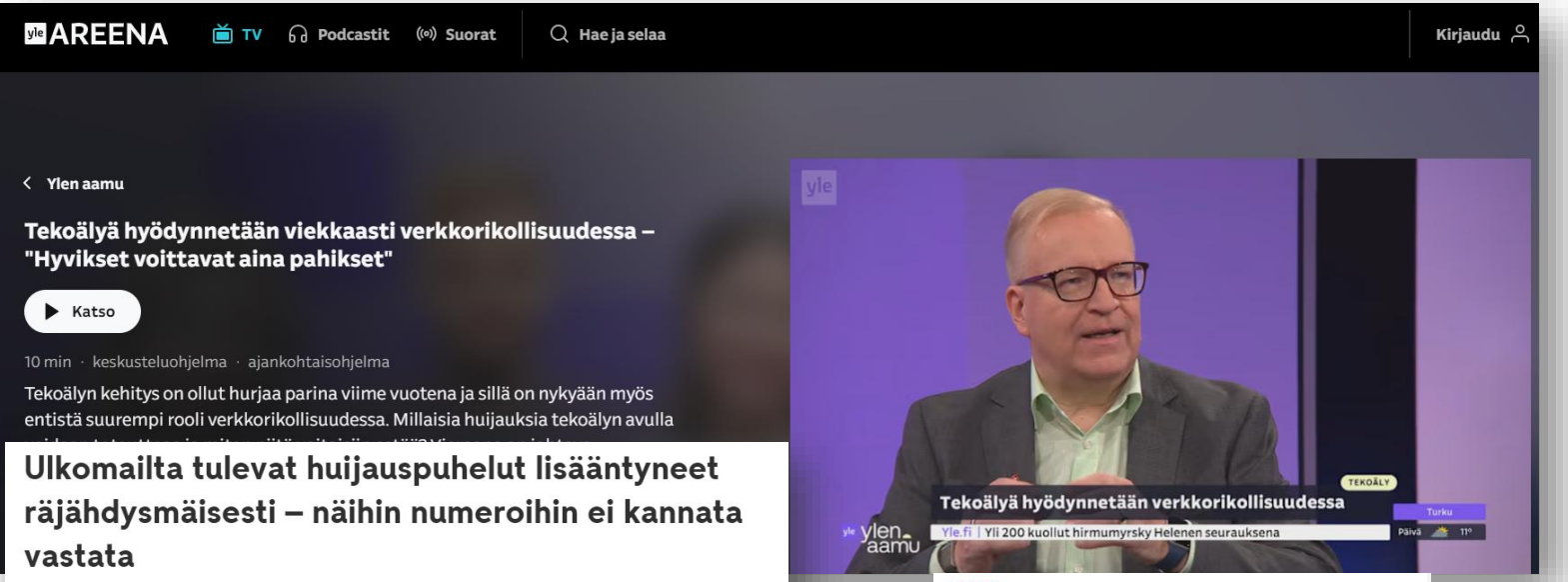
IT-asiantuntija Kimmo Rousku päätti huijata huijaria. DVV / KIMMO ROUSKU

Varo ovelia huijareita: Näin vuosia verkkorikollisia vastaan työskennellyttä ammattilaista on itseäänkin huijattu: "Se oli toistatuhatta euroa"

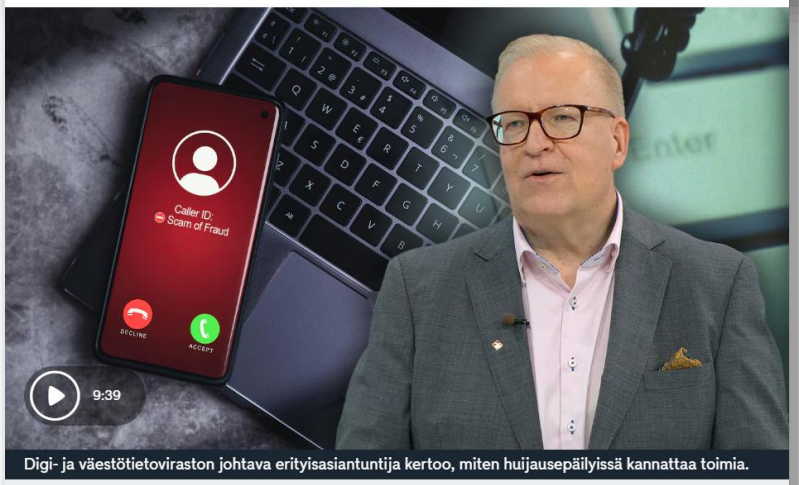
Katso videolta, kun ammattilainen kertoo kolme erilaista kokemaansa huijaustapausta.

Vapaa-ajalla paljastan verkkorikollisten petoksia

Vapaa-ajalla paljastan verkkorikollisten petoksia ja annan vinkkejä digiturvaan ja tekoälyyn



Ulkomailta tulevat huijauspuhelut lisääntyneet räjähdysmäisesti – näihin numeroihin ei kannata vastata



Digi- ja väestötietoviraston johtava erityisasiantuntija kertoo, miten huijausepäilyissä kannattaa toimia.

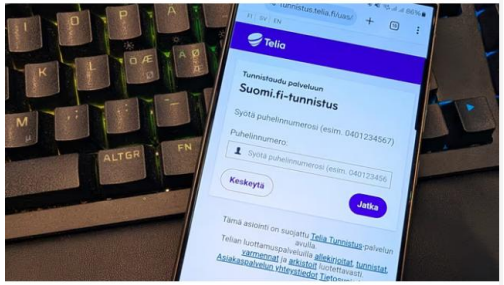
JULKAISTU 27.09.2024 19:00

TIETOTURVA

Käytätkö mobiilivarmennetta? Harkitse vakavasti tätä turva-keinoa – ei maksa mitään

Huijarit ovat jo alkaneet iskeä pelottavalla tavalla.

JAA TALLENNA KOMMENTIT



Mobiilivarmenne on pankkitunnuksia turvallisempi, mutta hyötyy silti lisäsuojasta. KUVA: HENRIK KÄRKKÄINEN / IS

TIETOTURVA

Hilton-hotellin tyynyä himoinneen Kimmon kävi köpelösti – näin vältät saman virheen

Hinta houkutti tekemään virheen.

JAA TALLENNA

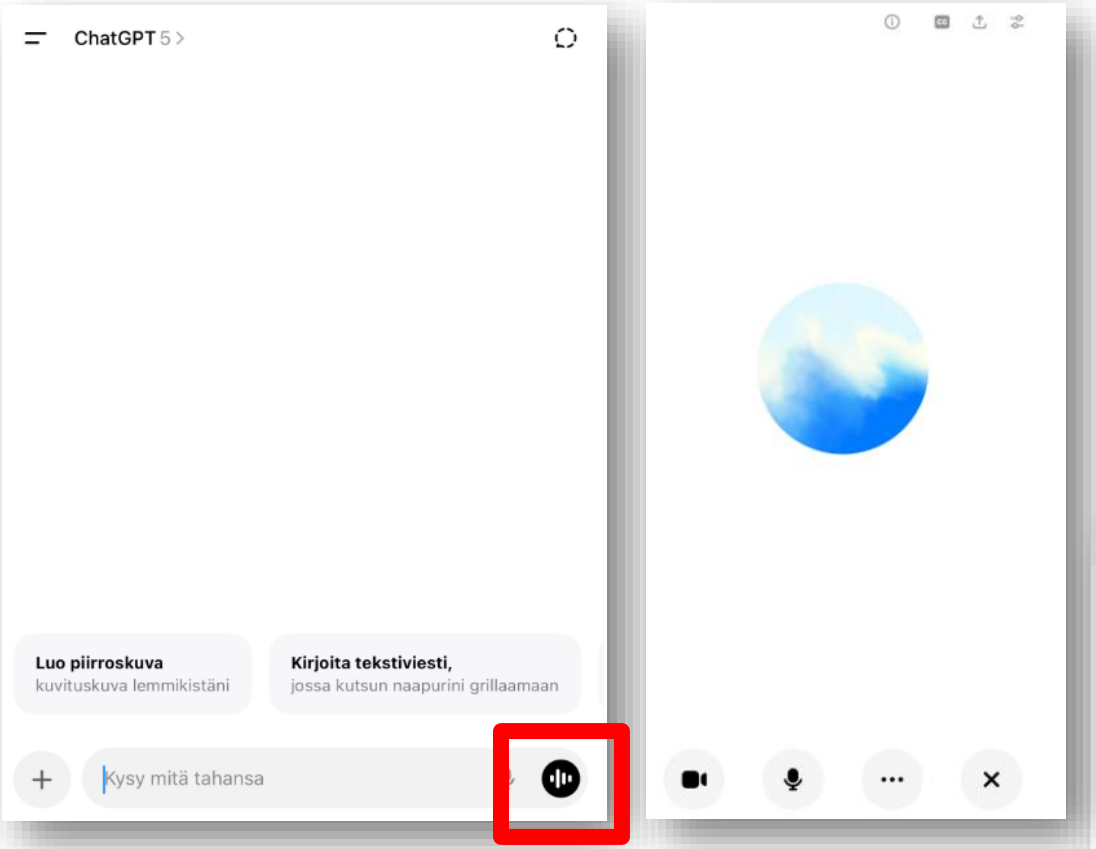
Vääriä verkkokauppoja ilmestyy ja katoaa jatkuvasti. KUVA: DIGI- JA VÄESTÖTIETOVIRASTO, JAQUE SILVA, /SOPA IMAGES / ZUMA / MVPHOTOS, DIGI- JA VÄESTÖTIETOVIRASTO, KUVAKAAPPAUKSIA

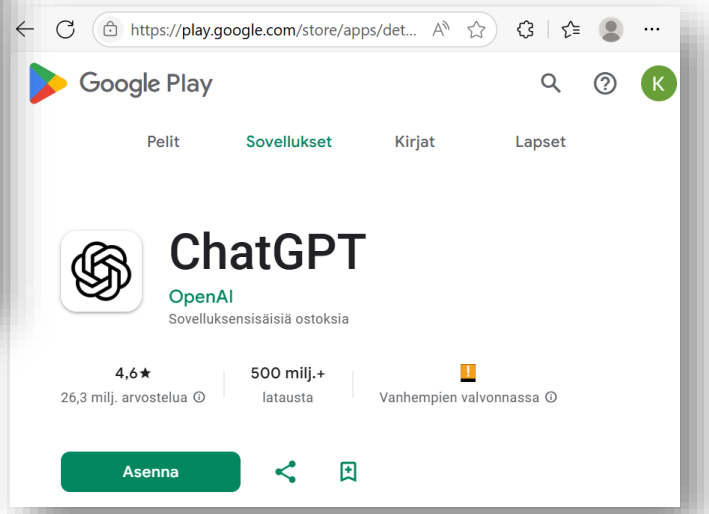
Kuuntele juttu

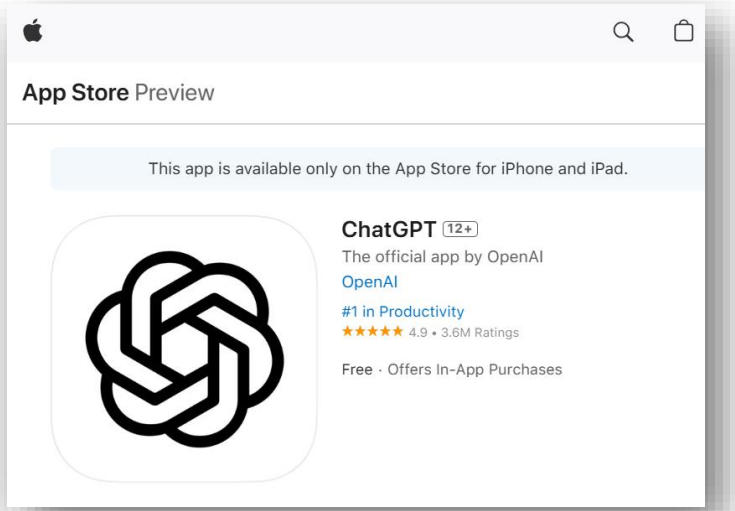
Tuomas Linnake

1.3. 8:33

#Ai-Kimmo (AiK) OpenAi ChatGPT-ohjelma - myös ilmaisversio





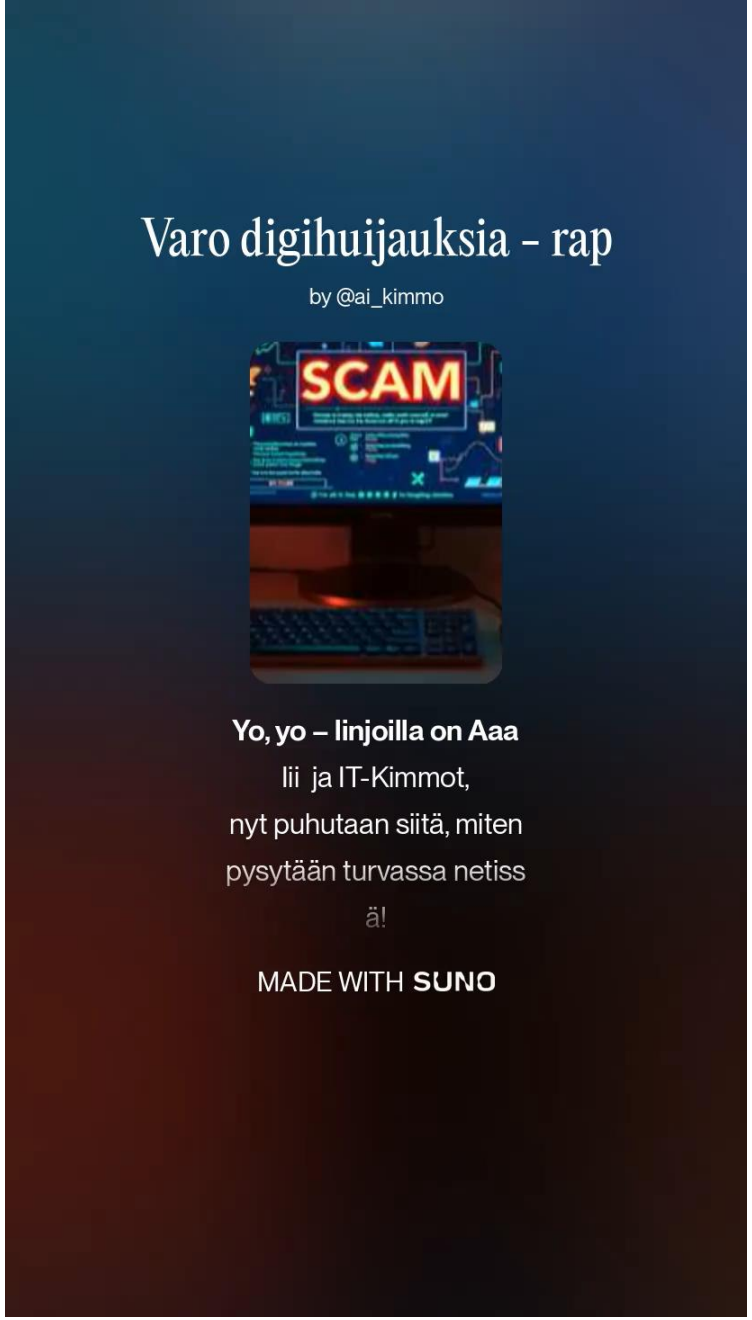


Esitykseni 60 minuuttia + aikaa keskusteluun

Miten pidän omat laitteeni ja tietoni turvassa? Miten huijaukset tunnistetaan, ja mitä uhkia ja mahdollisuuksia digiympäristö tuo mukanaan juuri nyt?

- Kyber-digimaailman uhkatilanne
- Miten meitä vastaan hyökätään – me ihmiset olemme haavoittuvaisia!
- Mitä kannattaa digiherätteessä katsoa ennen kuin klikkaat tai muuten ryhdyt toimenpiteisiin?

Aloitetaan laululla!



3 minuutin poplaulu

- Löytyy myös Facebook: https://www.facebook.com/662408328/videos/pcb.1016304686925329/758953713842043

Miten toimit turvallisesti digimaailmassa?

DIGI- JA VÄESTÖTIETOVIRASTO

Terminologia

- Digihuijaus?
- Nettihuijaus?
- Verkkohuijaus?
- Kalastelu tai kalasteluviesti?
- Huijaus tai huijausviesti?

⇒ PETOS tai

⇒ TÖRKEÄ PETOS

Kyber-digimaailman uhkatilanne

DIGI- JA VÄESTÖTIETOVIRASTO

Digimaailma on läsnä meillä kaikkialla

- **Kuinka toimit turvallisemmin digimaailmassa – samat periaatteet toimivat todella hyvin niin työpaikalla kuin vapaa-ajalla, arjessa ja kotona, sekä opiskeltaessa**

Poliisi epäilee kansainvälistä rikollisryhmää törkeistä petosrikoksista

2.10.2025 13.00

UUTINEN

Itä-Suomen poliisilaitos on johtanut keväästä 2024 alkaen laajaa rikostutkintakokonaisuutta. Esitutkinnassa on yhteensä yli kolmesataa epäiltyä rikosta, joita on tutkittu nimikkeillä petos, törkeää petos, rahanpesu sekä törkeä rahanpesu. Rikokset liittyvät huijauspuheluihin.

Poliisi epäilee rikoksista järjestäytynyttä, kansainvälistä rikollisryhmää. Poliisilla on tällä hetkellä 28 epäiltyä, joista suurin osa on Ruotsin ja Suomen kansalaisia. Pääepäiltynä on 19 henkilöä, jotka ovat iältään nuoria, noin 25–40-vuotiaita. Esitutkinnan perusteella he ovat toimineet merkittävissä rooleissa epäillyssä, järjestäytyneessä rikollisryhmässä.

Lisäksi poliisi on paljastanut 327 epäiltyä, suomalaista rahanpesijää, joiden esitutkintakokonaisuudet toimitetaan syyteharkintaan ympäri Suomea.

Poliisi on käyttänyt esitutkinnan aikana merkittävästi pakkokeinoja ja salaisia pakkokeinoja. 15 epäiltyä henkilöä on ollut vangittuna käräjäoikeuden päätöksin. Osa pääepäillyistä on edelleen pakkokeinojen kohteena.

Poliisi on takavarikoinut merkittävän määrän äänitallenteita esitutkinnan aikana. Äänitallenteiden avulla poliisi on estänyt huomattavan määrän rikoksia.
Kokonaisuus on ollut yhteiskunnallisesti merkittävä sen epäiltyjen ja uhrien määrän, rikoshyödyn sekä kansainvälisyyden takia.

🌍 Soittokeskuksia useissa maissa, uhreina pääosin iäkkäitä suomalaisia

- 28 epäiltyä, 19 pääepäiltyä
- 327 epäiltyä suomalaista rahanpesijää - uhrit pääosin eläkkeellä olevia ikäihmisiä,
- 220 henkilöä, joilta varastettu ainakin 2,2 miljoonaa euroa
- heille on voitu palauttaa 870 000 euroa yhteistyössä pankkien avulla

Epäillyt rikokset ovat noudattaneet selkeää kaavaa

Kaikissa rikoksissa näkyy yksinkertainen ja selkeä kaava. Pankin tai rahoituslaitoksen virkahenkilönä esiintyvä huijari on saanut uhrin uskomaan, että hänen nimissään on jätetty laina- tai rahoitushakemuksia. Kun uhri on ilmoittanut, ettei hän ole tehnyt tällaisia asioita, virkailijana esiintynyt henkilö on kertonut aloittavansa hakemusten peruuttamisen.

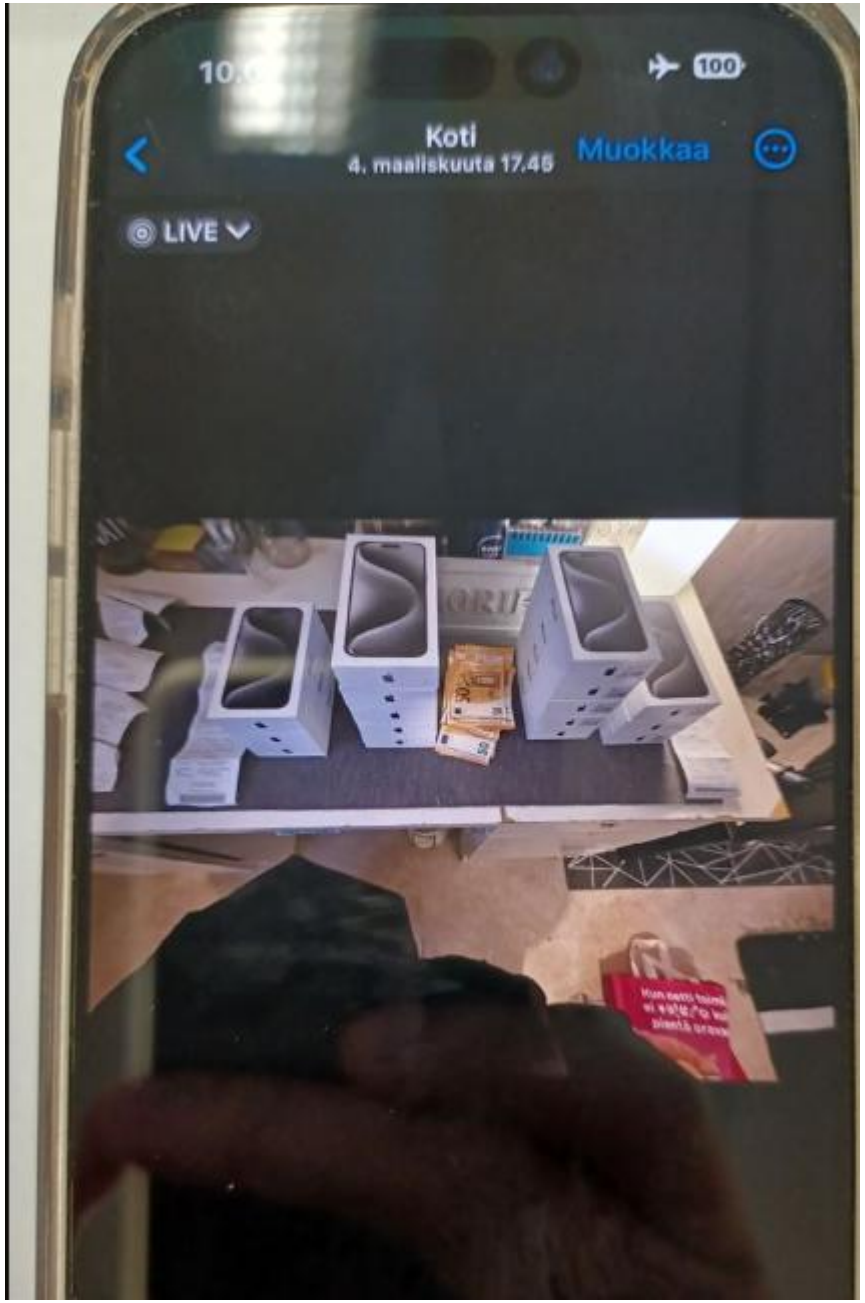
Todellisuudessa tilillä olleita varoja on alettu siirtää rikollisten hallinnoimille tileille. Tilisiirtoja varten uhri on saatu luovuttamaan huijarille pankkitunnuksensa ja kirjautumisvarmenteensa sekä hyväksymään tilisiirrot.

Tilisiirrot on tehty pääosin suomalaisille bulvaanitileille, joista rahat on nostettu käteiseksi tai niillä on ostettu matkapuhelimia, jotka on myyty eteen päin. Lopulta pesty rikoshyöty on saatu siirrettyä Suomen rajojen ulkopuolelle. Poliisin tiedossa on, että rikoshyötyä on muunnettu myös kryptovaluutoiksi.

Toiminta on ollut hyvin suunnitelmallista

Epäillyt ovat toimineet ammattimaisesti ja perustaneet organisaation rikosten tehtailua varten. Jokaisella on ollut toiminnassa oma selkeä roolinsa, joista on yhdessä muodostunut laaja rikoskokonaisuus ja organisaatio.

Rikollisryhmällä on ollut soittokeskukset Espanjassa, Marokossa, Irlannissa ja Ruotsissa, eli huijauspuheluja on soitettu sieltä keskitetysti. Myös Kuopioon on yritetty perustaa soittokeskusta.


Koti
4. maaliskuuta 17.45
Muokkaa
LIVE

Sit tota noin nii siin puhelussa vaan niinku sanot, että "moikka mun nimi on tää tää mä soitan Omalainalta. Varmistelisin tämmöstä lainahakemusta. Oot toivon mukaan hakenut meiltä lainaa viime viikon perjantaina."

Sit ne on sillee ei en oo hakenut mikä homma tää on...sit sä lähet selittää niille "joo meille on tullu lainahakemus viime viikon perjantaina, nimellä tää tää tää" eli sen nimellä. Sit sä sanot, et tässä hakemuksessa ollaan vielä vaadittu erillisesti, et rahat siirrettäis Osuuspankin tilille, jonka haltijan nimi ollu tällanen, kun [redacted] tai joku [redacted] joku tollanen, tiiätsä.

Sit jengi on sillee, voi... yleensä ne menee shokkiin. Sit sä käytät sitä, sä käytät sitä niiden shokkitilaa hyväkses. Sit sä oot sillee... sit sä jatkat lisää paskaa. Sit sä oot sillee, et "ja ollaan sähköpostiviestiin... sähköpostin sähköpostin välityksellä juteltu kans, tällasen sähköpostin, kun... sanot sen nimen ja kokonimen ja sit vaan keksit jonku niinku vaik lottaliisa2@gmail.com.

Sitten ne on sillee, et ei toi oo mun sähköposti ja sit sä sanot, että "joo nii mä arvelinki, mut tosiaan tämmösen sähköpostin välityksellä ollaan juteltu, että vaadit niinku, että olisit tätä lainaa halunnut siirrettäväks [redacted] tilille ku hän olisi ollu niinku perhetuttu ja olisit auttanut häntä ottamalla tämän lainan niinku ois saatu helpoiten sitten sillain, että ois menny suoraan sen [redacted] tilille". Sit ne on sillee, et ei... siinä vaiheessa ne yleensä menee shokkiin ja ne on sillee, et ei herranjumala blaa blaa blaa.

Sit sä vaan jauhat niiden kanssa vähän sillee, et tunnet sadness. Sit sä sanot, et nyt me lähetään poistelee hakemus kerran et oo tehnyt ja et tarvii ja sitten tehään rikosilmoitus niin poliisit on suhun yhteydessä.

Sitte perus, sun pitää myös painottaa siihen, et niinku henkilöllisyys ollaan vahvistettu, et löytyy kokonimi, syntymäaika, henkilötunnus ja sitten, että pankkitunnuksilla ollaan vahvistettu toi henkilöllisyys vielä pankkitunnistautumisen kautta et just Suomi.fin kautta.

Ja siinä vaiheessa ne on sillee, et ei vit... siinä vaiheessa ne menee oikeesti ihan sekasin. Ja sitten, et vähän siinä taas juttelet, et sitten oot vaan sillee, et joo hei tarvittais vielä virallinen vahvistus pankilta, ku tää on tosiaan vahvistettu sun tunnareilla, et pitää vielä varmistaa sieltä pankilta nii voisin antaa sulle lainan asianumeron ja yhdistää sinne nii... nii sitten saatais laina alta pois"

Okei mun ensimmäisen soittajan osuus olis tos. Sit toinen soittaja se on pankki Bum sä vastaat pankilt' [redacted] Osuuspankin asiakaspalvelusta kuinka voin auttaa" Bum se kertoo joo "Omalainalt soitettiin, lainaa oltiin haettu mun nimis blaa blaa blaa öö 8500 euroo mul ois tämmönen asiointinumero" Sit sen vaan pitäs esittää, et joo "annappa asiointinumero ja sano kokonimes" Buum se antaa sit siin sä juttelet sen kaa kyselet, et "ootko tehny mitään ulkomaanverkko-ostoja, ootko painellu näitä huijauslinkkejä tai onko tullu jotain huijaussoittoja" Et miten on sitte lähteny noi verkkopankkitunnukset leviimään ja on saatu vahvisteltua tällaisia tapahtumia ynnä muuta sellasta ja sitten vertaat siihen, että uskoisit... uskoisit, että tili on kopioitu, että jollakin on hallussa sitten tili, millä sitten pystyy vahvistamaan noita lainoja. Ehkä rahoja ei saatu siirrettyä, mutta kummiskin tollasia vahvisteluja pystyy tekee, että sitte.

Satojentuhansien eurojen huijaukset Itä-Suomessa – poliisi kehottaa tarkkaavaisuuteen

13.10.2025 8.29

UUTINEN

Itä-Suomen poliisi on saanut tutkittavakseen useita törkeitä huijauksia, joissa uhreilta on viety yhteensä satojatuhansia euroja. Huijaukset ovat tapahtuneet puhelimitse, sähköpostitse, sosiaalisessa mediassa ja verkkokaupoissa. Poliisi muistuttaa, että kuka tahansa voi joutua huijausten uhriksi, ja siksi huijausten tunnistaminen ja niistä puhuminen on tärkeää.

Tärkeimmät asiat, joiden avulla voit ehkäistä huijauksen uhriksi joutumista:

- Älä käytä pankkitunnuksiasi tai korttitietojasi teksti- tai sähköpostiviestissä olevan linkin kautta. Kirjaudu palveluihin aina niiden omilla verkkosivuilla tai sovelluksissa.
- Lue tarkasti mitä olet varmistamassa pankkitunnuksillasi.
- Pankki, poliisi tai kukaan muukaan laillinen toimija ei soita ja pyydä pankkitunnuksiasi tai pyydä siirtämään varojasi turvatilille.

👮‍♀️ Esimerkkejä verkkorikollisten onnistuneista digihuijauksista (esimerkiksi identiteettivarkaus, petos, törkeä petos)

💻 Facebook Marketplace -huijaus: Ostaja vaikutti aidolta ja halusi "vahvistaa myyjän tiedot". Rikollinen sai haltuunsa pankkikortin tiedot ja PIN-koodin → 💸 menetys noin 18 000 €

📧 Ulosottoviranomaiseksi tekeytynyt lähettäjä: Uhrille tuli sähköposti, jossa oli linkki pankkitunnistautumiseen. Rahaa siirtyi 50 000 €, josta poliisi sai palautettua 27 000 € 🙏

☎️ Pankkisoitot:
"Tilille pitää tehdä päivitys" → menetys lähes 170 000 € 😱
"Tilille pitää laittaa suojaus päälle" → menetys 12 000 €
"Viisi pankkitiliä on tyhjennetty" → pariskunta tunnistautui mobiilivarmenteella → menetys 40 000 € 💰

💌 Romanssihuijaus: "YK-lääkärinä Syyriassa" esiintynyt mies huijasi uhrilta 60 000 €

💔 Romanssi- ja lahjakorttihuijaukset kasvussa
🏪 ABC-liikenneasemalta ostettiin Apple-lahjakortteja 11 000 €:
Kyseessä oli romanssihuijaus, jonka kokonaisvahinko oli 109 000 € 😞

🎁 Mies osti lahjakortteja useana päivänä – jopa 8 000 € päivässä:
Lähetti ne "Sandra Bullockille", joka lupasi palkita hänet myöhemmin "ruhtinaallisesti"... 💌

🤦 Työntekijä sai "esimieheltään" sähköpostin:
Pyyntö ostaa kolme 100 € Apple-lahjakorttia ja lähettää kuvat koodeineen.
🕳️ Rikollinen oli murtautunut esimiehen sähköpostiin → menetys 600 €

🔒 Muista:
- Älä koskaan tunnistaudu sinulle lähetettyjen linkkien kautta 🔗
- Älä osta lahjakortteja kenenkään pyynnöstä ilman varmistusta ☑️
- Älä siirtele / maksa rahaa puhelinsoittojen tai viestien perusteella 💶
- Kysy tai tarkista aina, jos jokin tuntuu oudolta 🤔

💡 Kuka tahansa voi joutua huijatuksi, se ei ole häpeä, et ole tyhmä, myös minä olen menettänyt kolme kertaa rahaa!

FINANSSIALA

MUUTOS LOKAKUUSSA:

Verkkopankki alkaa syynätä maksutietosi.

Lue tästä, miksi

Mitä tämä tarkoittaa?

- Verkkopankki tarkistaa jatkossa maksutiedot: Pankkisi vertaa antamaasi maksun saajan nimeä ja tilinumeroa saajan pankissa oleviin tietoihin maksun saajan nimestä.
- **Jos nimi ei täsmää, verkkopankki ilmoittaa siitä. Maksun voi silti tehdä, mutta vastuu tilisiirrosta siirtyy maksajalle.**
- Verkkopankki kertoo, mikäli maksun vastaanottajan nimi *ei täsmää* tai jos se *melkein täsmää* tilinomistajan nimen kanssa. **Mikäli nimi *melkein täsmää,* ilmoittaa pankki tilinomistajaksi virallisesti merkityn nimen**.
- Käytännön toteutustapa riippuu pankista. Eri pankeissa voi olla erilaisia toteutustapoja.
- **Muutos tapahtuu viimeistään 9.10.** Joissakin pankeissa maksunsaajan tarkistus voidaan ottaa käyttöön jo aiemmin.

Tänään!

Verkkorikollisten reaktiot

- Odotan jo mielenkiinnolla, miten **verkkorikolliset alkavat selittämään sitä**, että nyt tehtävän maksun saaja on jokin kokonaan muu eli **NIMI EI TULE LAINKAAN TÄSMÄÄMÄÄN!**
  - Tästä kannattaa kertoa omassa lähipiirissä, sukulaisille ja kavereille – tällaisia tarinoita ei pidä uskoa!
  - Jos pankki varoittaa väärästä nimestä, kannattaa olla huolellinen, mutä tekee – itse ainakin mietin maksun keskeytystä ja selvitän, mistä on kyse!
- Toivotaan, että Suomessa pankit vihdoin heräävät tarjoamaan uusia turvaominaisuuksia samalla tavalla, mitä meidän tietoliikennepalveluiden tarjoajat – jolla puolella on tapahtunut merkittävät herääminen!

Poliisi varoittaa eSim-liittymistä

POLIISI HÄTÄNUMERO 112 SUOMI | SVENSKA | ENGLISH

Etusivu | Passit, henkilökortit, luvat | Rikokset | Tietoa poliisista

Poliisi › Uutishuone › Uutinen

Poliisi varoittaa puhelinliittymien kaappauksista

7.10.2025 9.28

UUTINEN

Itä-Suomen poliisissa on kiinnitetty huomiota viime vuosina yleistyneeseen SIM swapping -tekotapaan, jossa tietojenkalastelun uhrin, niin sanottu perinteistä SIM-korttia käyttävä, liittymä on muutettu eSIM-liittymäksi.

Huijaus alkaa pääsääntöisesti tietojenkalasteluviestillä, joka voi tulla minkä tahansa sovelluksen tai viestintäkanavan välityksellä. Kalastelun tarkoitus on saada haltuun uhrin henkilötietoja, joiden avulla rikollisen on mahdollisuus pyytää operaattorilta liittymän muuttamista eSIM-liittymäksi.

- **Sim-kortti** on **fyysinen puhelinliittymä**, **eSim** on **digitaalinen ohjelma**, joka toimii puhelimessasi

Näistä merkeistä voit tunnistaa SIM-korttihuijauksen

- Saat ilmoituksia liittymääsi koskevista palvelumuutoksista, joita et ole itse tehnyt.
- Saat ilmoituksia eSIM:n käyttöönotosta tai aktivointiin tarkoitetun QR-koodin, vaikka et ole tilannut sitä.
- Puhelinliittymä ei yhtäkkiä toimikaan omassa puhelimessa, eli et voi esimerkiksi soittaa ja vastaanottaa puheluita tai viestejä.
- Et pääse laitteeltasi sosiaalisen median tileillesi tai verkkopankkiin.
- Sosiaalisen median tileilläsi on tehty muutoksia tai tililtäsi on julkaistu sisältöä.

Jos olet joutunut huijauksen uhriksi, toimi seuraavasti:

- Ole yhteydessä teleoperaattoriisi.
- Ole yhteydessä pankkiisi.
- Tee asiasta rikosilmoitus poliisille.
- Pyri saamaan tilisi takaisin haltuusi ja vaihda salasanat.

Onko digimaailmasta tullut vaarallinen digitaalinen viidakko?

- Mutta viidakossakin selviää, kun osaa toimia siellä oikein!

- **Meitä uhkaavat:**
  - **Verkkorikolliset, digihuijarit, romanssihuijarit** – tietomurrot, kiristäminen
  - **Valtiolliset toimijat** – tiedonhaku, vaikuttaminen, hybridivaikuttaminen
  - **Informaatiovaikuttaminen ja häirintä**, kansalaisten kautta, organisaatio ja koko yhteiskuntatasolla
  - **Luonnonilmiöt** – sateet, myrskyt, tykkylumi – vaikuttavat meidän digitaaliseen yhteiskuntaan
  - **Inhimilliset virheet** – jonkin laitteen asetuksiin jää virheellinen asetus, joka mahdollistaa tietomurron
    - Tai me **klikkaamme linkkiä**, jota ei olisi saanut klikata tai **lähetämme vahingossa sähköpostissa** tietoja, joita siinä ei olisi pitänyt olla

Tärkeimmät turvaohjeet – muista ainakin nämä

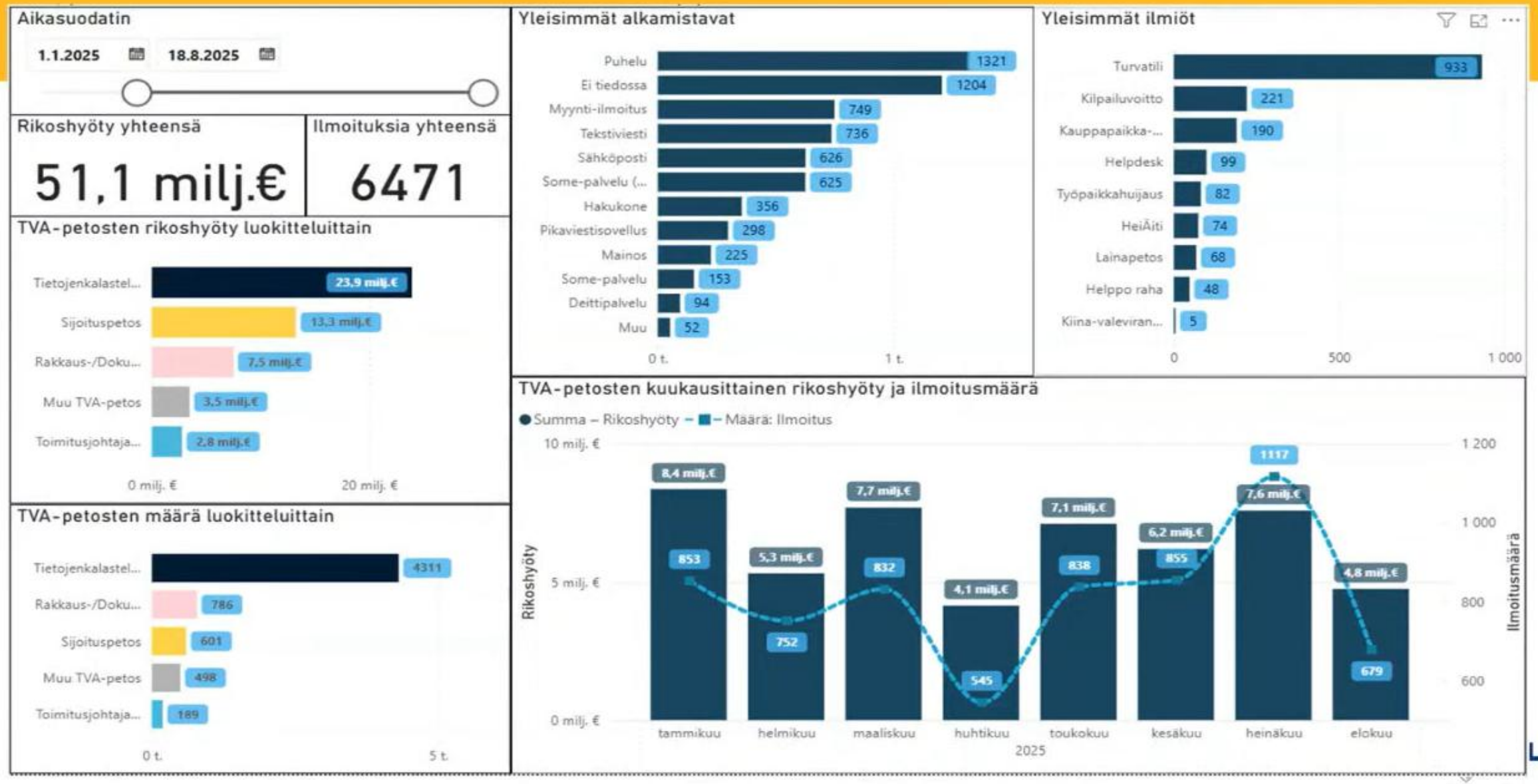
Jokaisen, joka on tutustunut uuteen ihmiseen netin välityksellä, kannattaa tutustua seitsemään tärkeimpään turvaohjeeseen. Niin kauan kuin ei ole tavannut toista kasvotusten, on syytä olla varovainen. Huijari voi olla suomalainen tai ulkomaalainen – siksi on tärkeää noudattaa näitä turvaohjeita kaikissa tilanteissa. Klikkaa ohjeen otsikkoa avataksesi lisätietoa turvaohjeesta.

- ▶ **1. Älä lähetä rahaa**
- ▶ **2. Suojaa oma postisi, älä vastaanota paketteja tai lähetyksiä**
- ▶ **3. Pidä pankkitilisi puhtaana, älä vastaanota rahansiirtoja tilillesi**
- ▶ **4. Ole tarkkana henkilötietojesi kanssa, älä luovuta tietojasi**
- ▶ **5. Sijoita vain pankkisi neuvoilla, älä ota vastaan sijoitusneuvoja**
- ▶ **6. Kerro avoimesti viestittelystä läheisillesi**
- ▼ **7. Tarkasta Toimintaohjebingo**

Nettideittiturvan Toimintaohjebingo listaa erilaisia varaan merkkejä viestittelyyn liittyen.

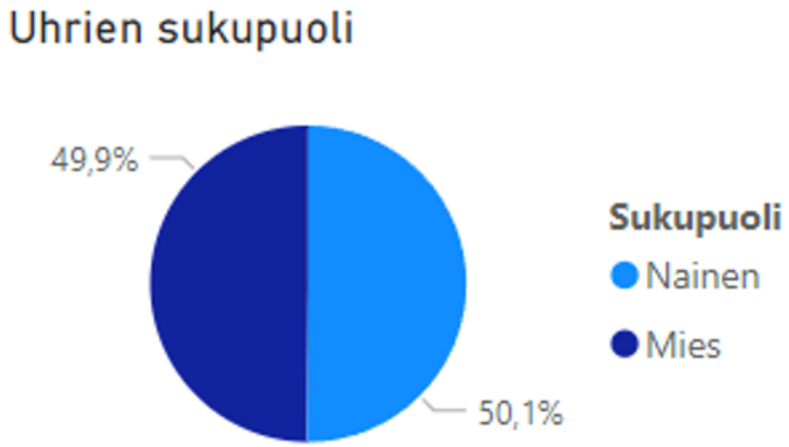
- https://nettideittiturva.fi

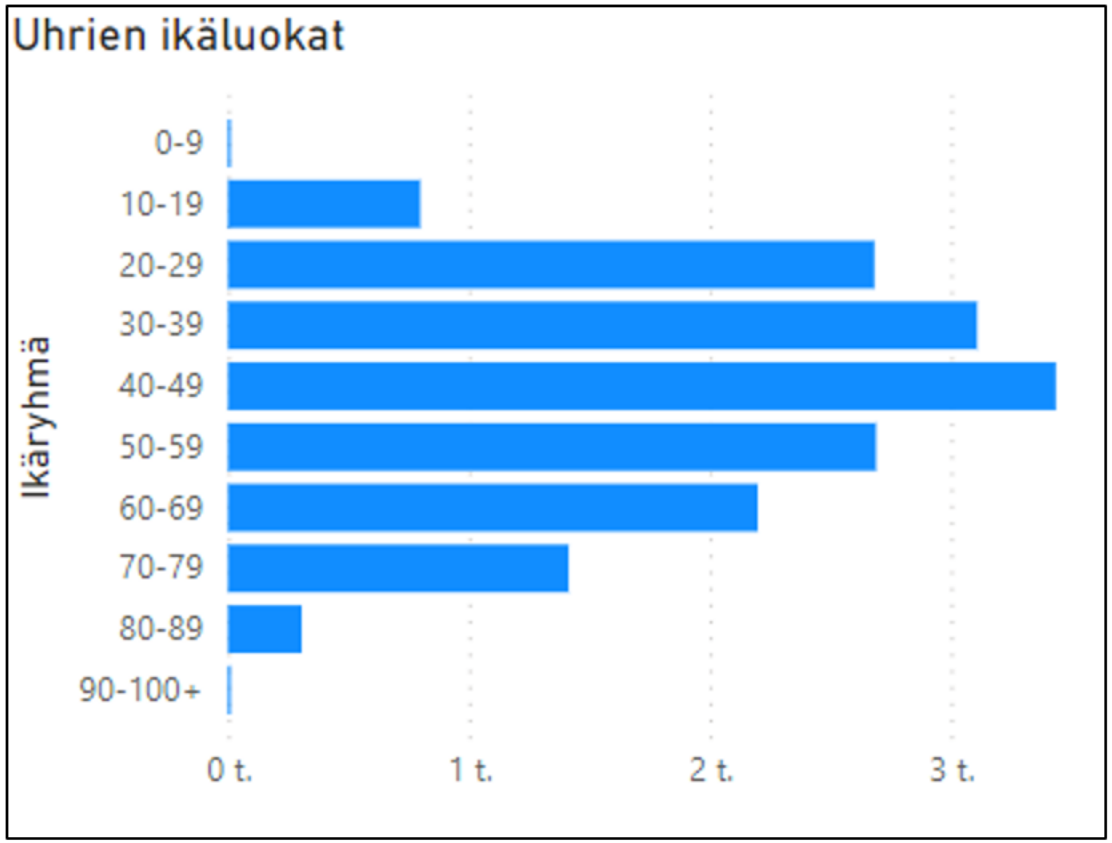
Poliisille ilmoitettuja rikoksia



Havaintoja rikosten uhreista

- Sukupuolella ei suurta merkitystä uhriutumisen kannalta.
- Uhrien ikäjakauma osoittaa, että kuka tahansa voi joutua petoksen uhriksi. Mikään ikäryhmä ei erityisesti korostu.





Sinä olet osa monikerroksellista tietoturvasipulia – et heikko, vaan vahva lenkki!

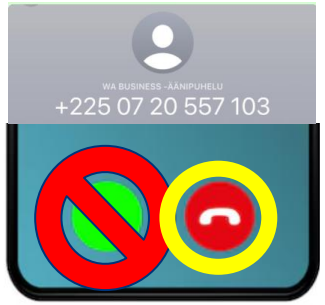
Me hyvikset vs noi pahikset

Meitä vastassa on paljon kansainvälisiä ammattilaisrikollisjärjestöjä!

Miten meitä vastaan hyökätään?

DIGI- JA VÄESTÖTIETOVIRASTO

Miten meitä vastaan hyökätään?

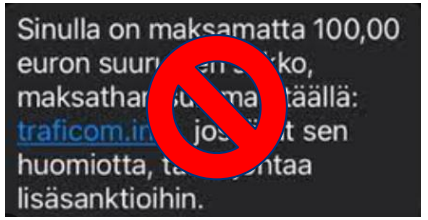


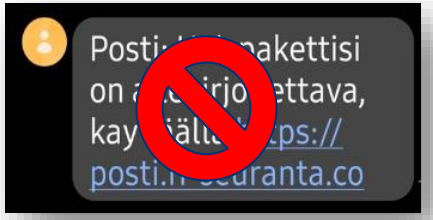
Puhelinsoitto

- Ulkomainen numero eli muu kuin +358 alkuinen eli nyt kevät 2025 +385…
- Puhutaan Suomea
- Soitetaan poliisista tai pankista?

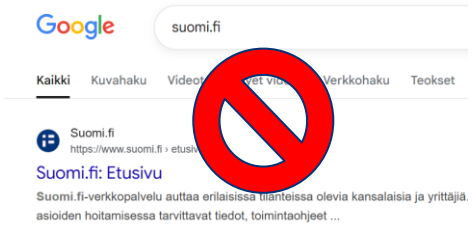
Tekstiviesti (sms) ja pikaviestit kuten WhatsApp, Messenger

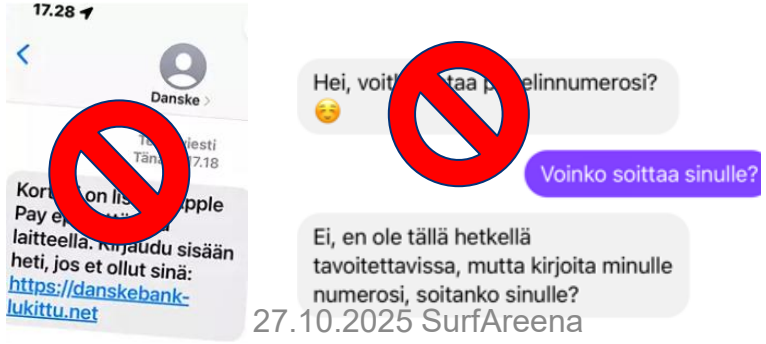
- Olet saamassa rahaa tai töitä
- Sinun pitää maksaa rahaa
- Sinulta urkitaan tietoja kuten puhelin-numeroa tai muita tietoja

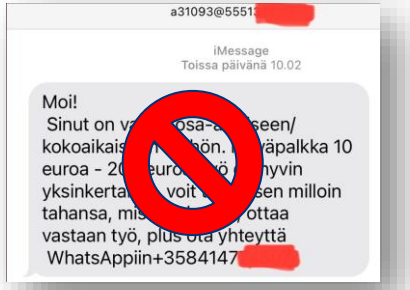




Hakukoneella sinulle esitettävä hakutulos

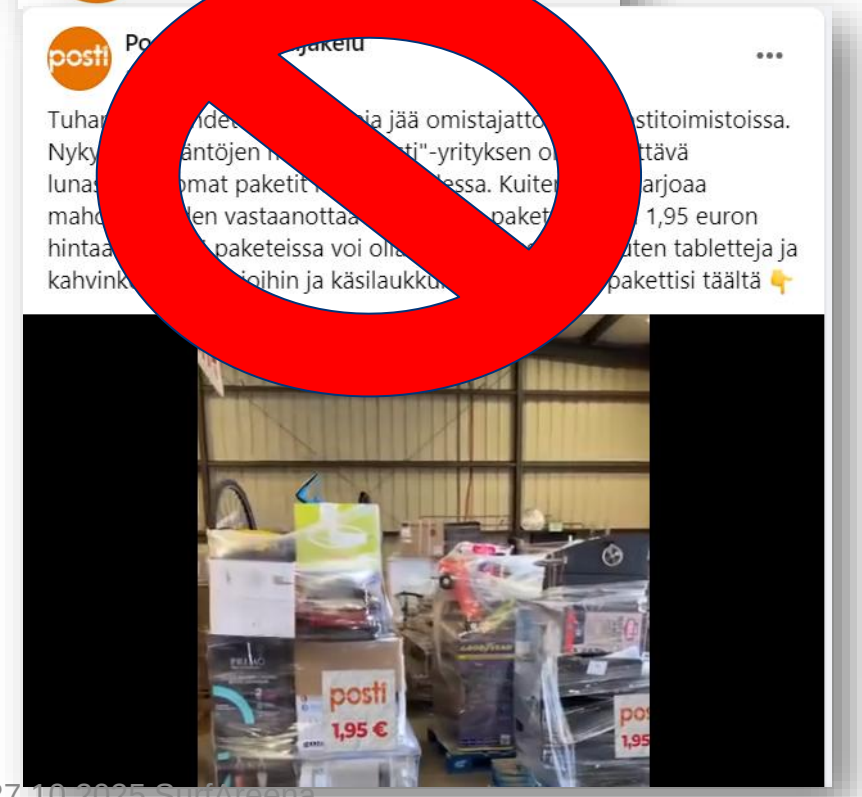


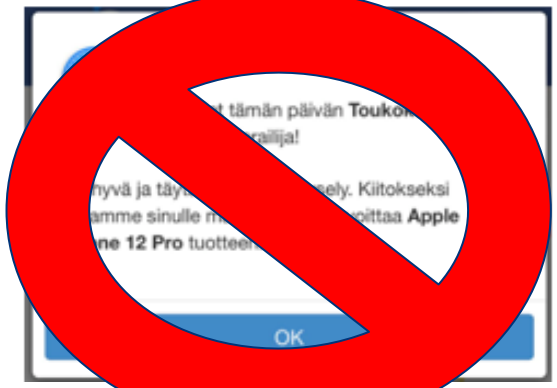


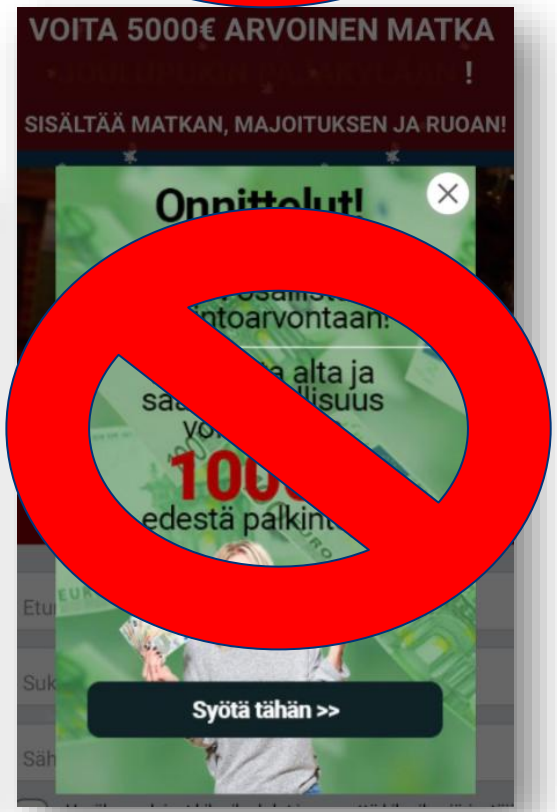


Miten meitä vastaan hyökätään?

Sosiaalisen median sivustot







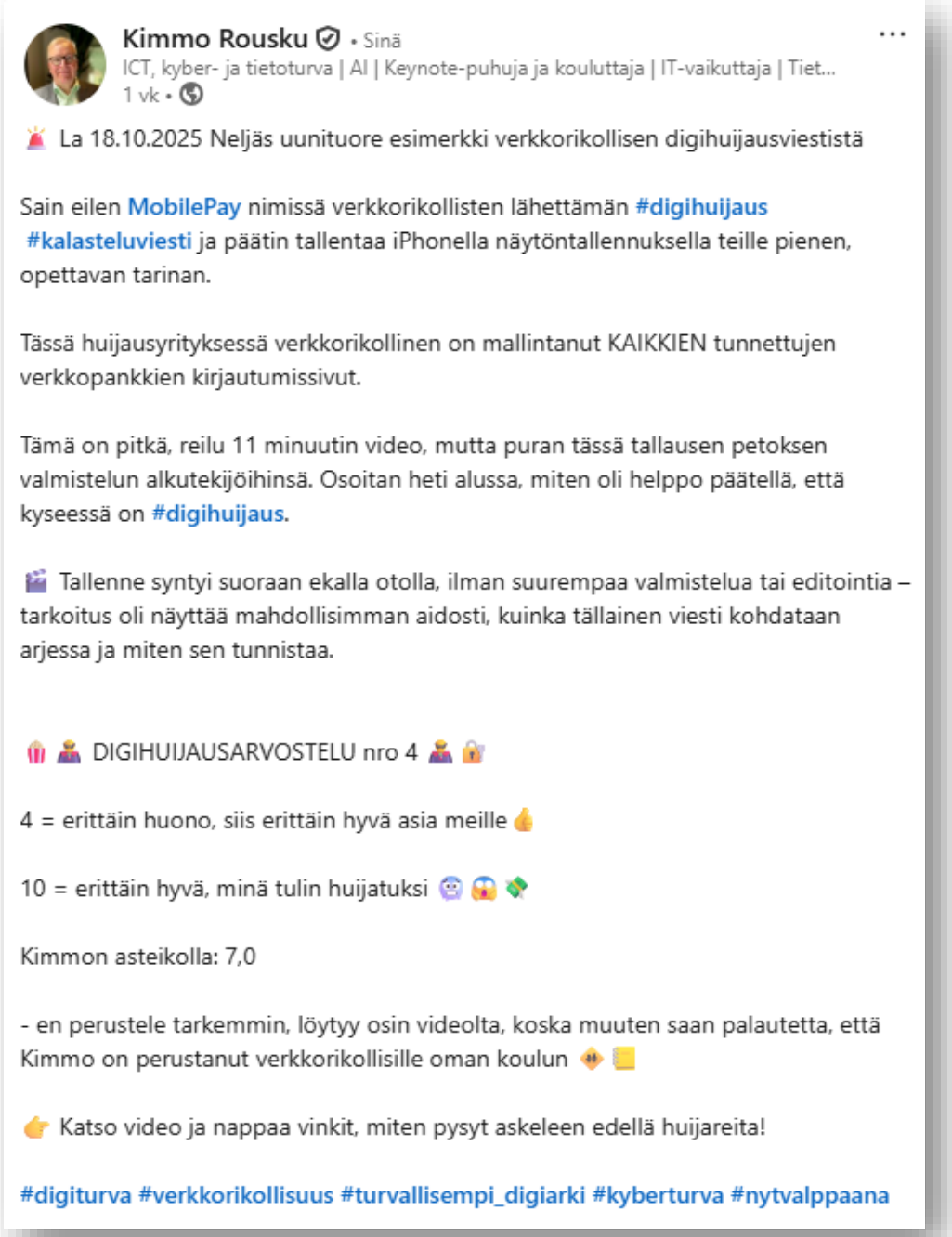
Mitä kannattaa digiherätteessä katsoa ennen kuin klikkaat tai muuten ryhdyt toimenpiteisiin?

Älä koskaan toimi kiireessä!

DIGI- JA VÄESTÖTIETOVIRASTO

Sinua lähestytään digipalvelussa tällaisella viestillä – mitkä asiat pitäisi herättää epäilyksen?

Tilisi jäädytetään pian	Saat laitteet pelkkien postikulujen hinnalla!	Postipakettisi edellyttää tullimaksujen maksua	Haluan ostaa xxx tuotteesi
Vastaa tähän 24 tunnin sisällä	Voitko lähettää tekstiviestinä tulleen koodin minulle?	Lähettäjä: admin@verkkopankki-fi.site	Olet saanut palautusta xxx euroa!
Sinun pitää maksaa 0,002 bitcoinia	Klikkaa tätä linkkiä vaihtaaksesi vaarantunut salasanasi	Napauta: kirjaudu.omapankki-fi.net	Sinulle on paketti, maksa xxx maksu saadaksesi
Olet voittanut arvonnassa!	Sinusta on kuvattu video ja voit estää sen julkaisun – napauta tätä	Hei isä – tarvitsen nopeasti 250 € vuokraan	Turvaposti-viesti



Kimmo Rousku • Sinä
ICT, kyber- ja tietoturva | AI | Keynote-puhuja ja kouluttaja | IT-vaikuttaja | Tiet...
1 vk •

🚨 La 18.10.2025 Neljäs uunituore esimerkki verkkorikollisen digihuijausviestistä

Sain eilen MobilePay nimissä verkkorikollisten lähettämän #digihuijaus #kalasteluviesti ja päätin tallentaa iPhonella näytöntallennuksella teille pienen, opettavan tarinan.

Tässä huijausyrityksessä verkkorikollinen on mallintanut KAIKKIEN tunnettujen verkkopankkien kirjautumissivut.

Tämä on pitkä, reilu 11 minuutin video, mutta puran tässä tallausen petoksen valmistelun alkutekijöihinsä. Osoitan heti alussa, miten oli helppo päätellä, että kyseessä on #digihuijaus.

🎬 Tallenne syntyi suoraan ekalla otolla, ilman suurempaa valmistelua tai editointia – tarkoitus oli näyttää mahdollisimman aidosti, kuinka tällainen viesti kohdataan arjessa ja miten sen tunnistaa.

🍿 🦹 DIGIHUIJAUSARVOSTELU nro 4 🦹 🔐

4 = erittäin huono, siis erittäin hyvä asia meille 👍

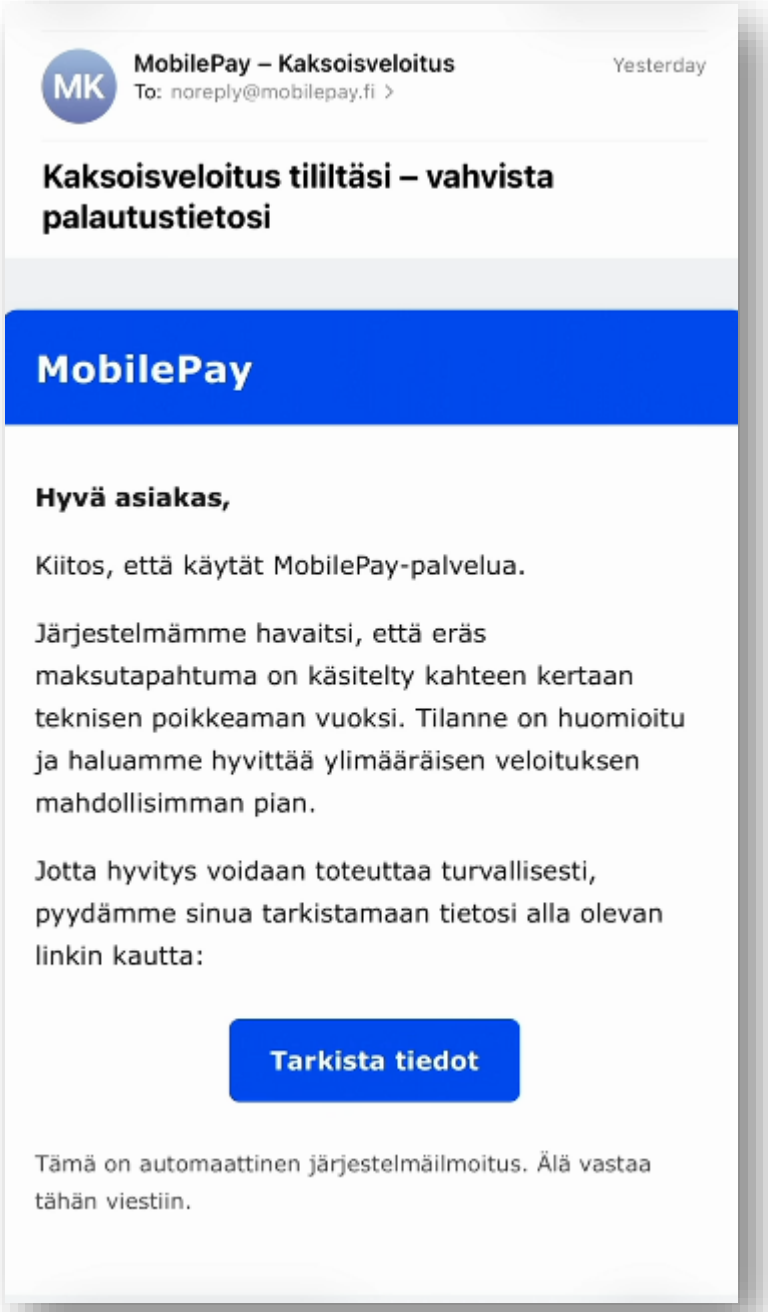
10 = erittäin hyvä, minä tulin huijatuksi 🤯 😱 💸

Kimmon asteikolla: 7,0

- en perustele tarkemmin, löytyy osin videolta, koska muuten saan palautetta, että Kimmo on perustanut verkkorikollisille oman koulun 🔶 🟨

👉 Katso video ja nappaa vinkit, miten pysyt askeleen edellä huijareita!

#digiturva #verkkorikollisuus #turvallisempi_digiarki #kyberturva #nytvalppaana



MK **MobilePay – Kaksoisveloitus** Yesterday
To: noreply@mobilepay.fi >

Kaksoisveloitus tililtäsi – vahvista palautustietosi

MobilePay

Hyvä asiakas,

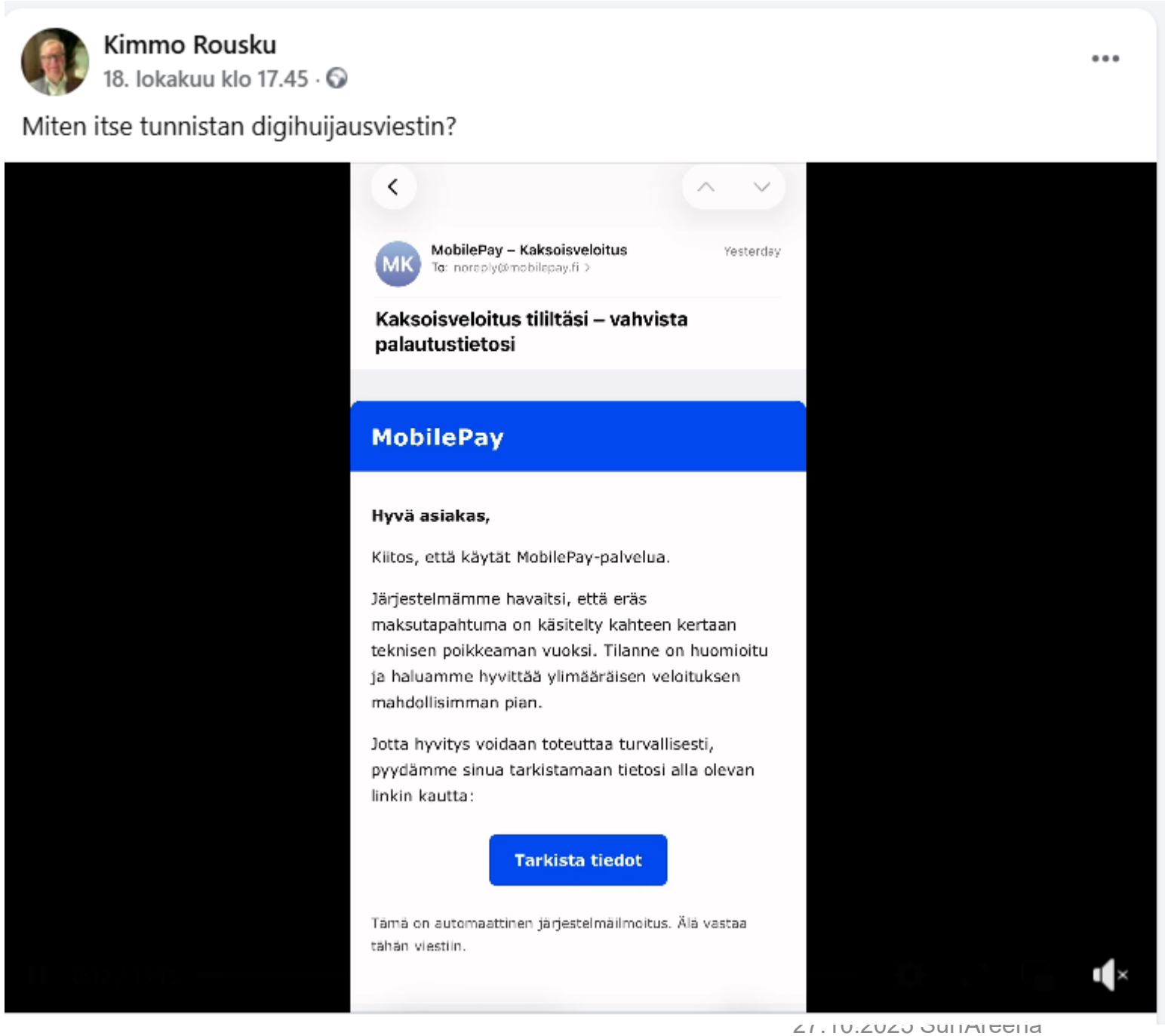
Kiitos, että käytät MobilePay-palvelua.

Järjestelmämme havaitsi, että eräs maksutapahtuma on käsitelty kahteen kertaan teknisen poikkeaman vuoksi. Tilanne on huomioitu ja haluamme hyvittää ylimääräisen veloituksen mahdollisimman pian.

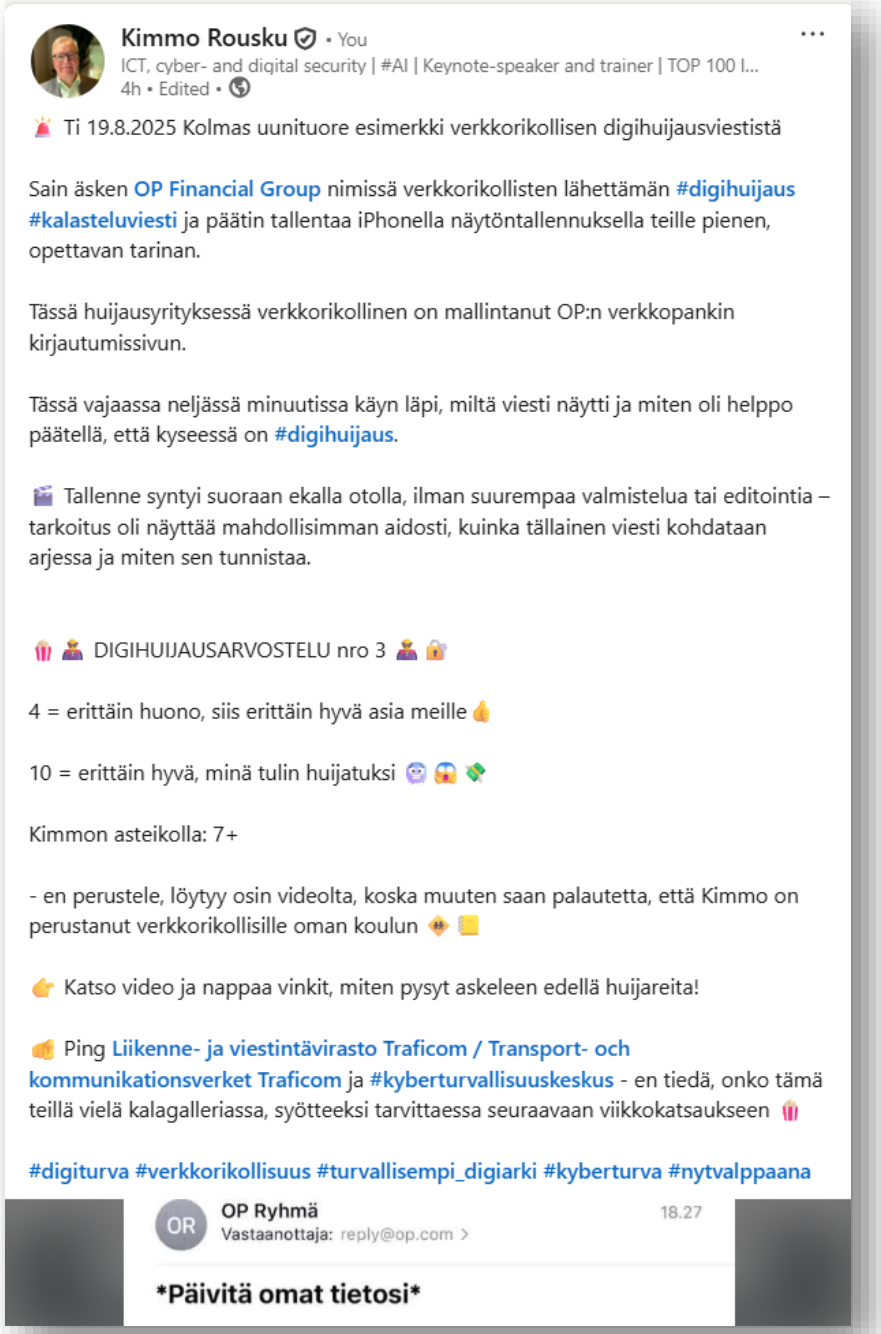
Jotta hyvitys voidaan toteuttaa turvallisesti, pyydämme sinua tarkistamaan tietosi alla olevan linkin kautta:

Tarkista tiedot

Tämä on automaattinen järjestelmäilmoitus. Älä vastaa tähän viestiin.



- Facebook
- https://www.facebook.com/share/v/1BCgZTz3QS/



Kimmo Rousku • You
ICT, cyber- and digital security | #AI | Keynote-speaker and trainer | TOP 100 I...
4h • Edited •

🚨 Ti 19.8.2025 Kolmas uunituore esimerkki verkkorikollisen digihuijausviestistä

Sain äsken OP Financial Group nimissä verkkorikollisten lähettämän #digihuijaus #kalasteluviesti ja päätin tallentaa iPhonella näytöntallennuksella teille pienen, opettavan tarinan.

Tässä huijausyrityksessä verkkorikollinen on mallintanut OP:n verkkopankin kirjautumissivun.

Tässä vajaassa neljässä minuutissa käyn läpi, miltä viesti näytti ja miten oli helppo päätellä, että kyseessä on #digihuijaus.

🎬 Tallenne syntyi suoraan ekalla otolla, ilman suurempaa valmistelua tai editointia – tarkoitus oli näyttää mahdollisimman aidosti, kuinka tällainen viesti kohdataan arjessa ja miten sen tunnistaa.

🍿 🕵️ DIGIHUIJAUSARVOSTELU nro 3 🕵️ 🔐

4 = erittäin huono, siis erittäin hyvä asia meille 👍

10 = erittäin hyvä, minä tulin huijatuksi 😇 😱 💸

Kimmon asteikolla: 7+

- en perustele, löytyy osin videolta, koska muuten saan palautetta, että Kimmo on perustanut verkkorikollisille oman koulun 🤦 📒

👉 Katso video ja nappaa vinkit, miten pysyt askeleen edellä huijareita!

👊 Ping Liikenne- ja viestintävirasto Traficom / Transport- och kommunikationsverket Traficom ja #kyberturvallisuuskeskus - en tiedä, onko tämä teillä vielä kalagalleriassa, syötteeksi tarvittaessa seuraavaan viikkokatsaukseen 🍿

#digiturva #verkkorikollisuus #turvallisempi_digiarki #kyberturva #nytvalppaana

OP Ryhmä 18.27
Vastaanottaja: reply@op.com
Päivitä omat tietosi

OP Ryhmä 16.27
Vastaanottaja: reply@op.com

Päivitä omat tietosi

OP Ryhmä.

Hyvä asiakaamme,

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.

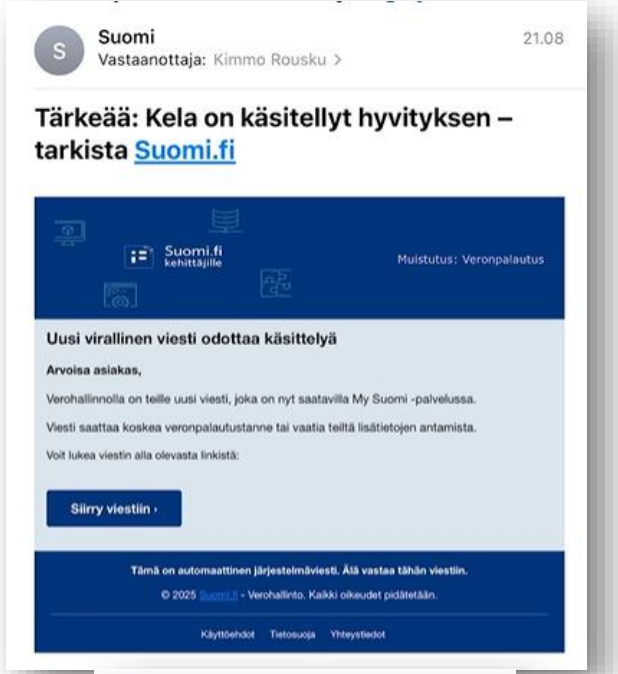
Päivitä Osuuspankin tunnuksilla

Prosessi järjestelmän ja tietojen päivittämiseksi on tehty mahdollisimman helpoksi ja sujuvaksi.
Näin päivität tietosi verkkopankissa Kirjaudu verkkopankkiin. Vastaa kirjautumisen jälkeen aukeavaan kyselyyn. Jos kyselyä ei aukea automaattisesti, klikkaa oikeasta yläkulmasta omaa nimeäsi ja valitse Henkilötiedot-otsikon alta Päivitä tiedot.

Tervesain
Osuuspankki
Asiakaspalvelu

OP Ryhmä BIC: OKOYFIHH

OP Gebhardinaukio 1, Helsinki P.O. Box 308, FI-00101 Helsinki



Suomi 21.08
Vastaanottaja: Kimmo Rousku

Tärkeää: Kela on käsitellyt hyvityksen – tarkista Suomi.fi

Suomi.fi kehittäjille
Muistutus: Veronpalautus

Uusi virallinen viesti odottaa käsittelyä

Arvoisa asiakas,

Verohallinnolla on teille uusi viesti, joka on nyt saatavilla My Suomi -palvelussa.

Viesti saattaa koskea veronpalautustanne tai vaatia teiltä lisätietojen antamista.

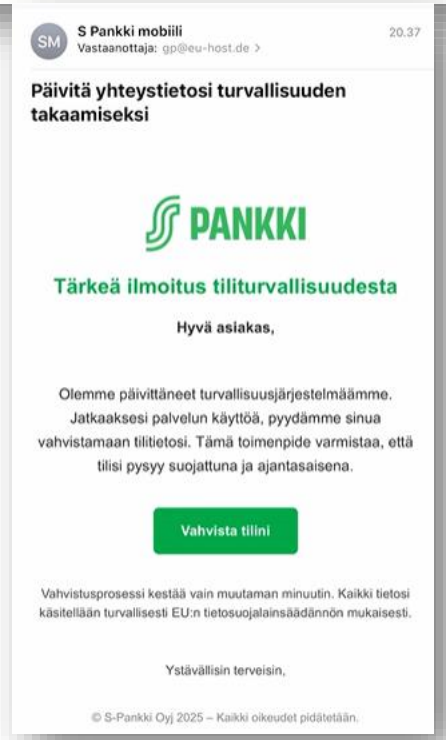
Voit lukea viestin alla olevasta linkistä:

Siirry viestiin ›

Tämä on automaattinen järjestelmäviesti. Älä vastaa tähän viestiin.

© 2025 Suomi.fi - Verohallinto. Kaikki oikeudet pidätetään.

Käyttöehdot Tietosuoja Yhteystiedot



S Pankki mobiili 20.37
Vastaanottaja: gp@eu-host.de

Päivitä yhteystietosi turvallisuuden takaamiseksi

PANKKI

Tärkeä ilmoitus tiliturvallisuudesta

Hyvä asiakas,

Olemme päivittäneet turvallisuusjärjestelmäämme. Jatkaaksesi palvelun käyttöä, pyydämme sinua vahvistamaan tilitietosi. Tämä toimenpide varmistaa, että tilisi pysyy suojattuna ja ajantasaisena.

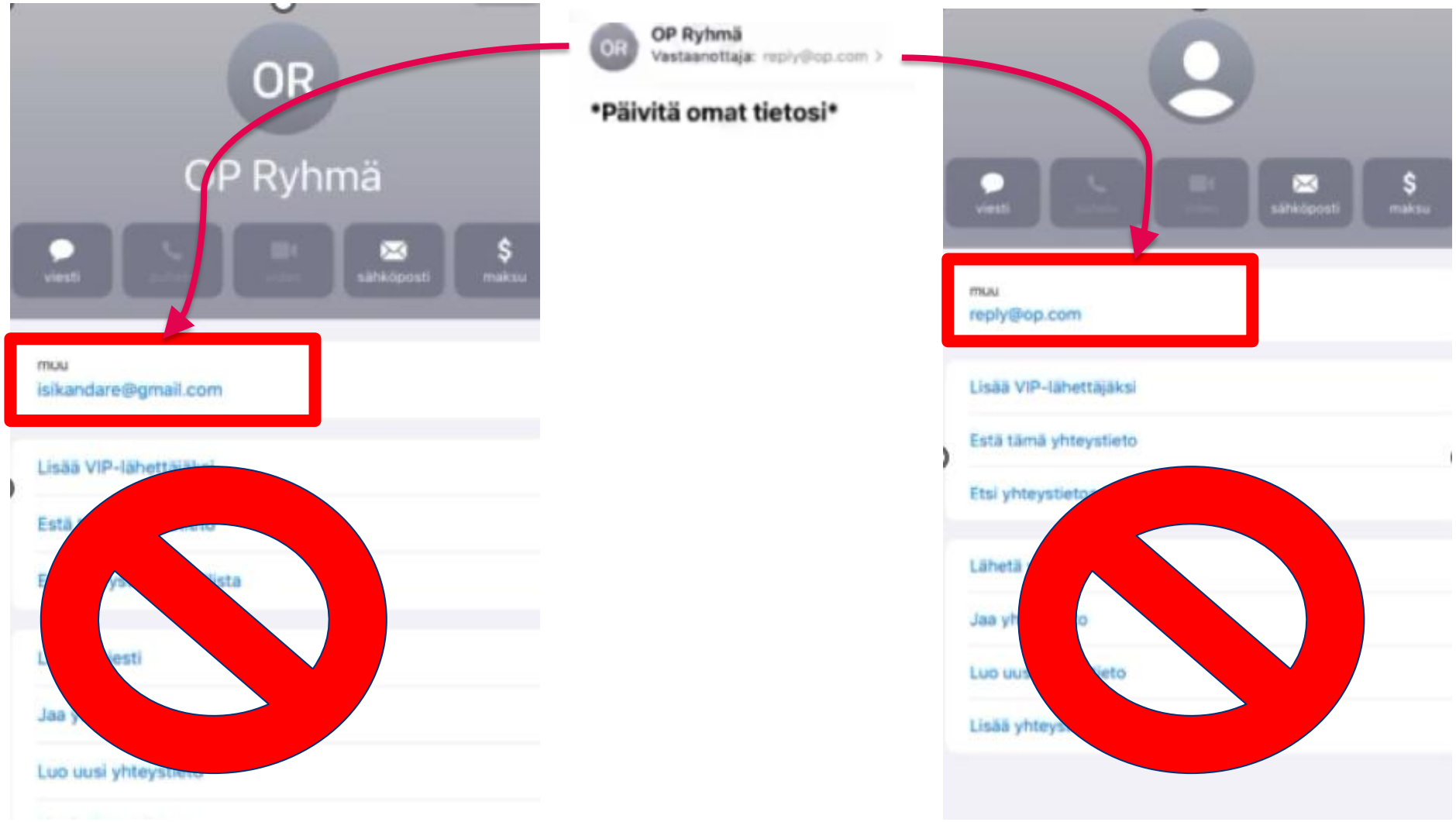
Vahvista tilini

Vahvistusprosessi kestää vain muutaman minuutin. Kaikki tietosi käsitellään turvallisesti EU:n tietosuojalainsäädännön mukaisesti.

Ystävällisin terveisin,

© S-Pankki Oyj 2025 – Kaikki oikeudet pidätetään.

Kuka on lähettäjä, kenelle viesti on lähetetty?

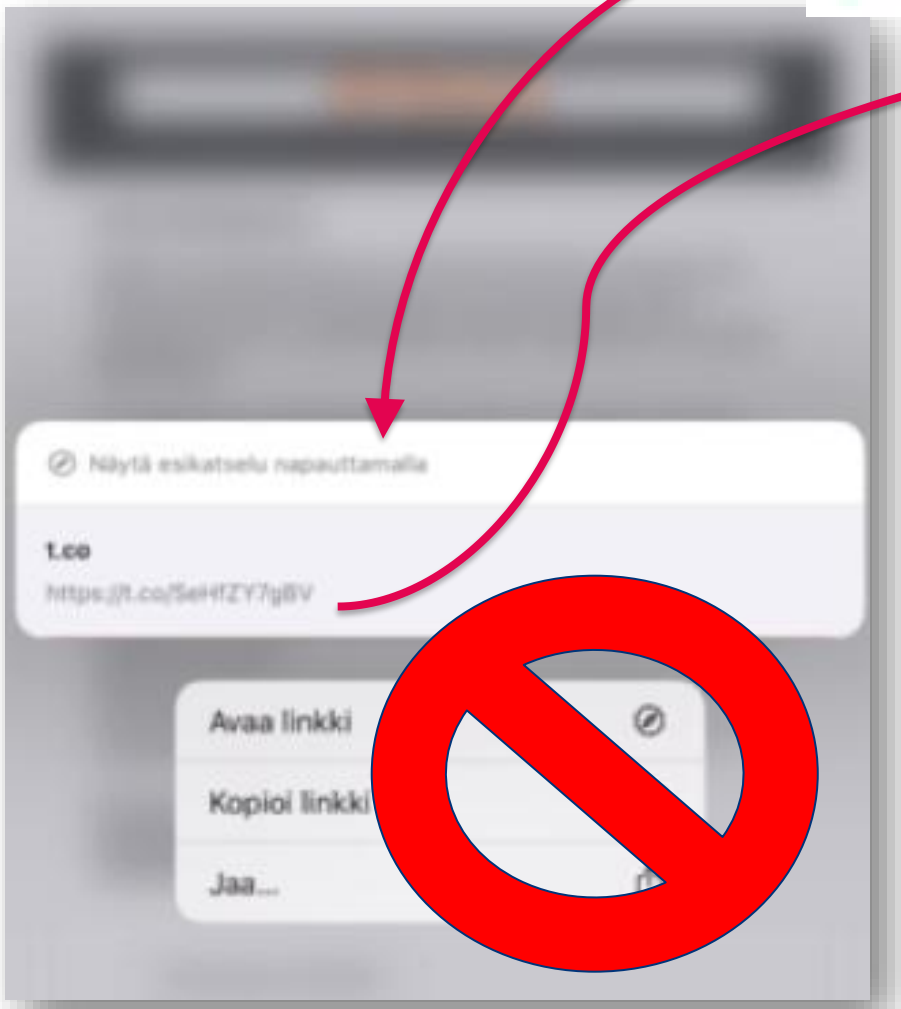


Minne linkki johtaa?

https://www.op.fi/henkiloasiakkaat/

Päivitä Osuuspankin tunnuksilla

https://op-ryhma-fi-paivita-omattietosi.i1li.org

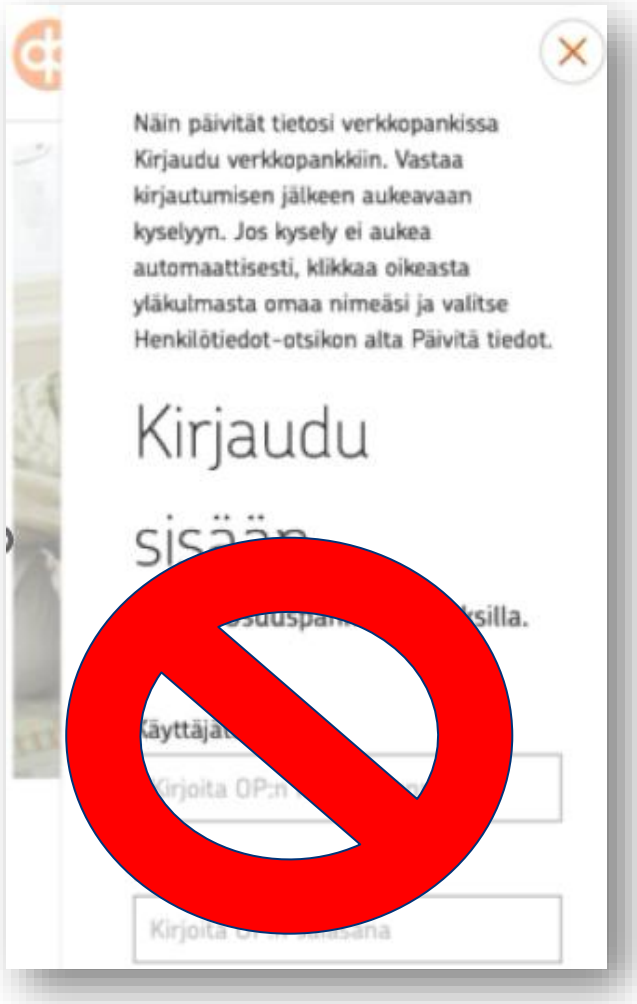


Jos osoite alkaa

https://t.co
https://bit.ly
https://tinyurl.com

<u>Älä avaa linkkiä</u> – tämä on lyhennetty osoite ja et voi tietää, minne tämä osoite johtaa!

Mikään viranomainen tai finanssialan toimija ei näitä käytä!



Tunnettuja finanssialan toimijoita

- OP Ryhmä https://www.op.fi
- Nordea https://www.nordea.fi
- Danske Bank https://danskebank.fi
- Handelsbanken https://www.handelsbanken.fi
- S-Pankki https://www.s-pankki.fi
- POP Pankki https://www.poppankki.fi
- Aktia https://www.aktia.fi
- Ålandsbanken https://www.alandsbanken.fi
- Hypo (Suomen Hypoteekkiyhdistys) https://www.hypo.fi

Tunnettuja viranomaisia

- Digi- ja väestötietovirasto (DVV) https://dvv.fi
- Verohallinto https://vero.fi
- Kela https://kela.fi
- Traficom https://traficom.fi
- Poliisi https://poliisi.fi
- Rajavartiolaitos https://raja.fi
- Puolustusvoimat https://puolustusvoimat.fi
- Onnettomuustutkintakeskus (OTKES) https://onnettomuustutkinta.fi
- Tietosuojavaltuutetun toimisto https://tietosuoja.fi
- Kilpailu- ja kuluttajavirasto (KKV) https://kkv.fi

IT-Kimmon kaksi vinkkiä

1. Aina kun olet syöttämässä tietojasi johonkin palveluun, **pysähdy miettimään**, miten olet siihen tilanteeseen päätynyt? Tietoisesti menemällä ostamaan verkkokaupasta tuotetta vai sms-tekstiviestinä tulleen **”mielenkiintoisen”** viestin klikkauksen kautta? **Mieti, mitä klikkaat!**

2. **Ennen kuin klikkaat, tarkista,** onko viranomaisen tai finanssialan toimijan osoitteessa https://organisaatio.fi/ eli **.fi/?**
   → **Ei ole, ÄLÄ KLIKKAA**

Esimerkiksi:
suomi.fi/sivut tai
posti.fi/ilmoitus

OK suomi**.fi/**sivut tai

OK posti**.fi/**ilmoitus


TIETOTURVA

IT-Kimmon sähköpostiin pamahti samalla kertaa 10 huijausviestiä – antaa tärkeän ohjeen

Suomi.fi:n nimissä huijataan, ja kalasteluviestien kohteeksi joutui myös palvelusta vastaavassa virastossa työskentelevä asiantuntija.

JAA TALLENNA KOMMENTIT

Yksi pieni merkki kertoo paljon verkko-osoitteessa. KUVA: TOMASZ ZAJDA VIRRAGE IMAGES INC / COLOURBOX

Tuomas Linnake
15.3. 6:12

Testi – ovatko seuraavat osoitteet turvallisia?

Pankki.tunnistus-nordea.com/pankkitilit/kirjaudu

Veronpalautus.verohallinto.fi/tunnistaudu

Suomi-fi-tunnistus.net/palvelut/turvallisuus

Rikosilmoitus.keskusrikospoliisi.biz/ilmoita

Osoitteesta puuttuu **.fi/**

Miten toimit turvallisemmin?

- 👉 Käynnistitkö itse tapahtuman (vaikka maksaaksesi laskun), vai ohjasiko joku **ULKOPUOLINEN** sinut tähän toimenpiteeseen (esimerkiksi **puhelinsoitolla**, **tekstiviestillä**, **pikaviestillä, sähköpostiviestillä, nettisivulta ponnahtaneella ilmoituksella**)?

  🚨 **VARO ULKOPUOLISTA VAIKUTTAMISTA** 🚨

  🛡️ Suurin uhka? Me suomalaiset olemme välillä liian hyväuskoisia.

  👉 Älä maksa mitään kiireessä. Kysy perheenjäseneltä tai kaverilta, ennen kuin toimit.

  👉 Jaa kokemuksia ja keskustelkaa kotona, sukulaisten kanssa näistä aiheista

- Osaathan tunnistaa nettisivujen oikeat osoitteet eli viranomaiset ja finanssialan toimijat – osoitteessa pitää olla tässävoilukeajotain.**fi** tai tässävoilukejotain.**fi/**osoitejatkuu

Oletko sijoittamassa rahaa?

Älä käytä nettiä, vaan ammattimaisia toimijoita apunasi!

DIGI- JA VÄESTÖTIETOVIRASTO

Varo ja VAROITA muita sijoitushuijareista – investointi tai muista epämääräisistä WhatsApp-ryhmistä ja sivuista!

Katleena Kortesuo · 1st
Owner at Katleena Kortesuo Oy | MBA, M.Sc.
1w ·

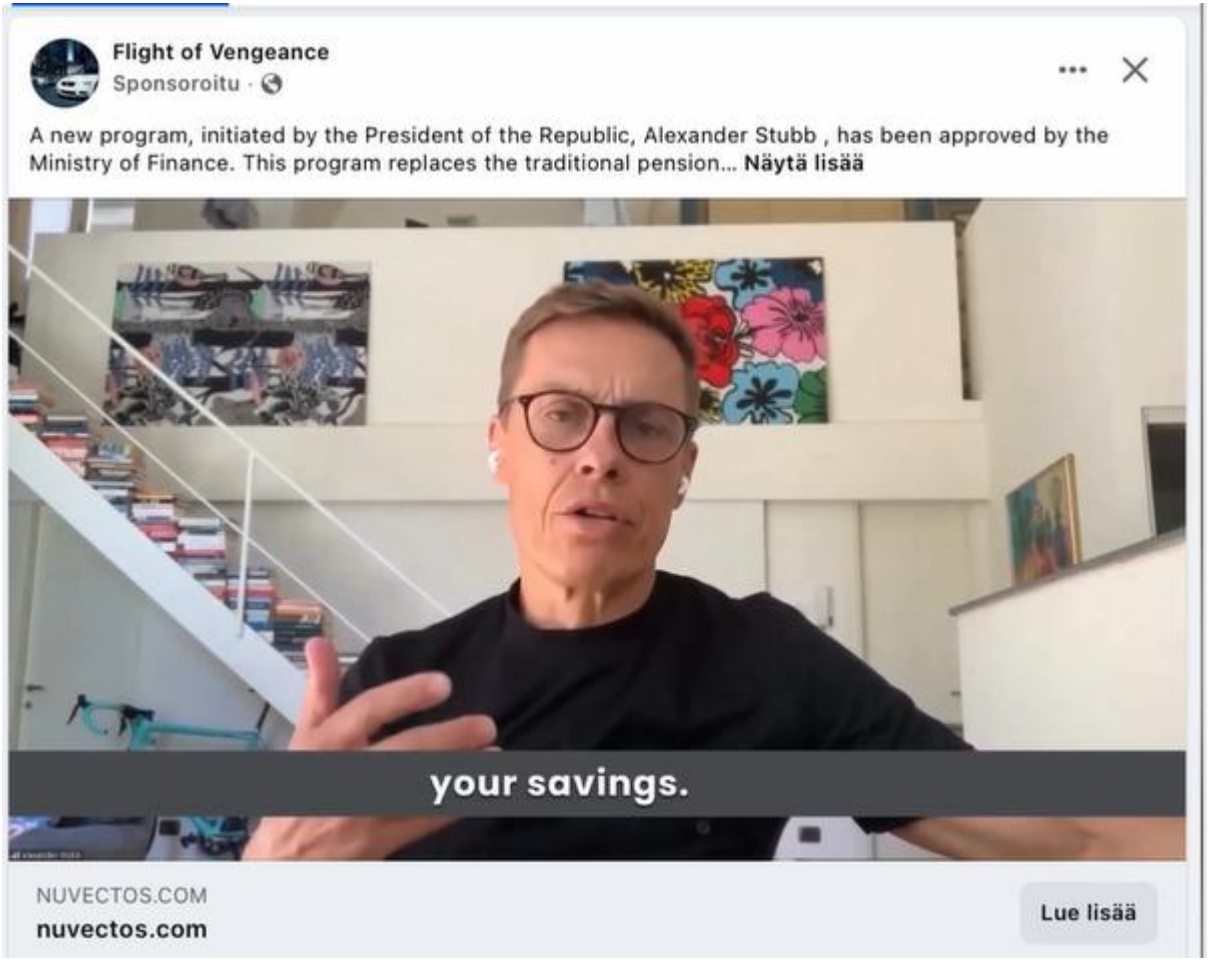
Facebookissa pyörii taas videohuijaus, jossa tällä kertaa "Alexander Stubb" kehuu jotain eläkesijoittamista. Video on tehty tekoälyllä, joten ulkonäkö on uskottava. Kuulemma vain 50 ensimmäistä pääsee mukaan.

Näitä pitää tietty aina ilmiantaa, mutta harva ilmianto toteutuu. Usein vastaukseksi tulee, että "mainos ei riko yhteisönormejamme". Mainoksia tarkastaa pelkkä automatiikka, joka ei tunnista julkisuuden henkilön identiteettivarkautta.

Mutta nyt tärkeä kysymys: oletko ilmiantanut Facebookissa onkin mainoksen ja ilmiantosi on hyväksytty? Yritän tässä selvittää suhdelukua. Meneekö ilmiannoista läpi 40 %, 10 % vai vain 0,01 %?

On selvää, että jokainen ilmianto ei voi mennä läpi. Muutenhan joku kiero yrittäjä klikkaisi kilpailijan mainokset pois markkinoilta. On siis oltava jokin kriteeri – esim ilmiantojen suuri määrä tai ilmiselvä identiteettivarkaus –, jolloin mainos hylätään. Mutta milloin se hylätään?

Videokaappauksessa feikkipresidentti mainostamassa tuotettaan. Varoittakaa perheen iäkkäitä, etteivät haksahda tällaiseen.



DIGIUUTISET

Professori Vesa Puttonen teki rikosilmoituksen: "En ole koskaan elämässäni kokenut mitään sellaista"

Professori Vesa Puttonen epäilee, että huijauksien takana on ammattimaista toimintaa.

Professori Vesa Puttonen tuntee itsensä avuttomaksi huijausvyöryn keskellä. KIMMO HAAPALA

~ Vesa Puttonen +358 46 8017528

📖📖Tämän illan kurssi päättyy tähän. Meidän kaikkien lopullinen tavoite sijoitusmarkkinoilla on tietenkin tehdä voittoa. Mutta miten voimme parantaa mahdollisuuksiamme tienata mahdollisimman paljon? Vastaus on selvä: oppimalla. Vain jatkuvalla opiskelulla ja sijoitustaitojen kehittämisellä pystyy liikkumaan osakemarkkinoilla sujuvasti ja vakaasti.

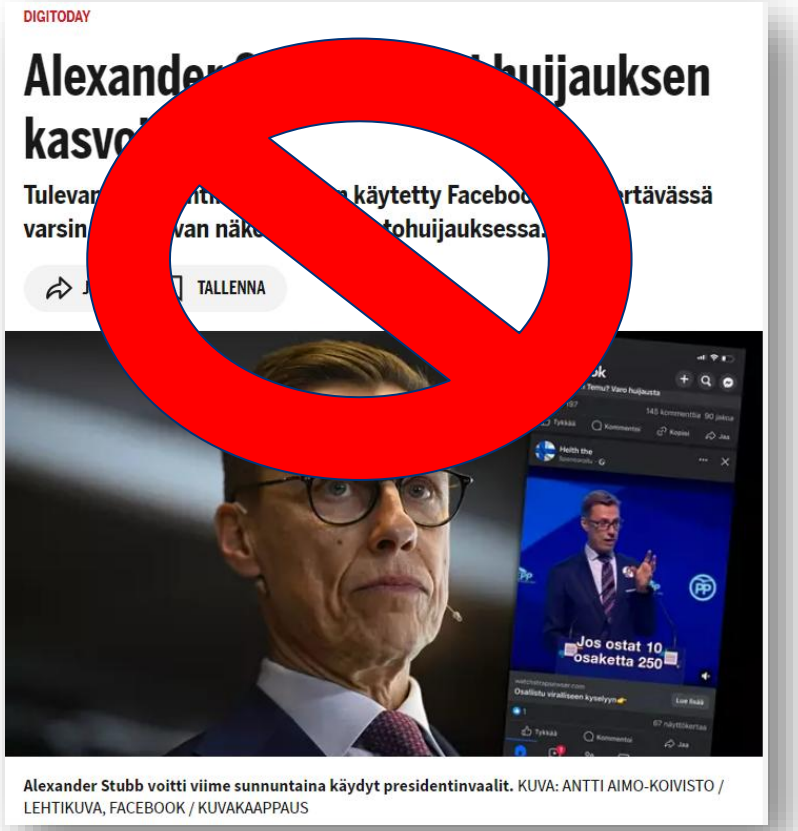
Jos taas kieltäydyt oppimasta ja sijoitat pelkän alkuperäisen ajattelutapasi varassa, markkinat saattavat muuttua sinulle kalliiksi "tiedon maksupalveluksi".

Ns. ”kryptovaluuttahuijaukset”

Muista edelleen, jos jokin on liian hyvää / halpaa ollakseen totta, kysy jonkun sinulle tutun ja luotettavan henkilön mielipidettä

KUVA: IS / ZUMAPRESS / MVPHOTOS

Henrik Kärkkäinen
22.12.2021 10:32



Alexander Stubb voitti viime sunnuntaina käydyt presidentinvaalit. KUVA: ANTTI AIMO-KOIVISTO / LEHTIKUVA, FACEBOOK / KUVAKAAPPAUS

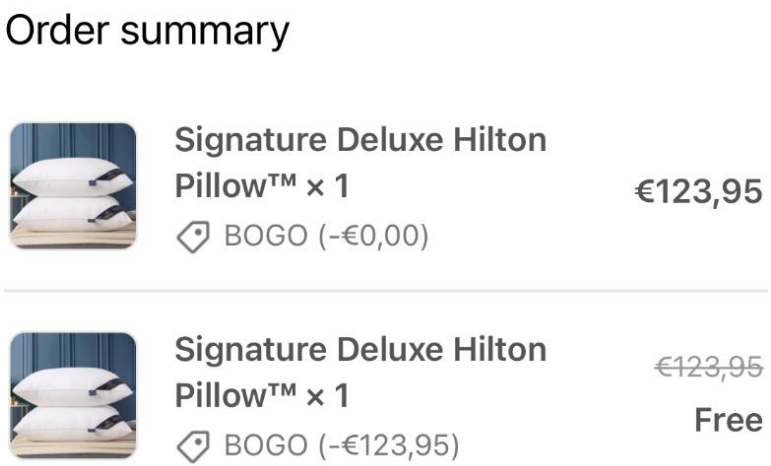
Yle
https://yle.fi › Yle Uutiset › Rikokset

Eteläsavolaismies haksahti julkkisten nimissä tehtyyn ...

28.3.2024 — Eteläsavolainen mies **menetti** 120 000 euroa sijoituspetoksen yhteydessä maaliskuussa, kertoo Itä-Suomen poliisi. Poliisin mukaan mies oli ...

Huijaukset eli petokset – myös MINÄ olen tullut huijatuksi

- **2008** ostin Mikko.fi palvelusta unelmieni Sonyn television – 1250 €
  - Melkein liian hyvää ollakseen totta
- **2024** myin digitaalisen hilavitkuttimen tori.fi – ostaja **VARASTI sen käsistäni** – 300 €
  - Älä luovuta esinettä käsistäsi, ellei tila ole hallussasi ja turvallinen
- **2025** ostin kaksi ”Hotelli Hilton tyynyä” erikoistarjouksessa – 123,95 €
  - Koska olin nähnyt mainokset jo aikaisemmin, en tehnyt tarkastuksia - sain rahat takaisin, koska maksoin luottokortilla – maksa kaikki nettiostokset **aina luottokortilla!**



Kimmo Rousku • You
ICT, cyber- and digital security | AI | Keynote-s...
3mo • Edited •

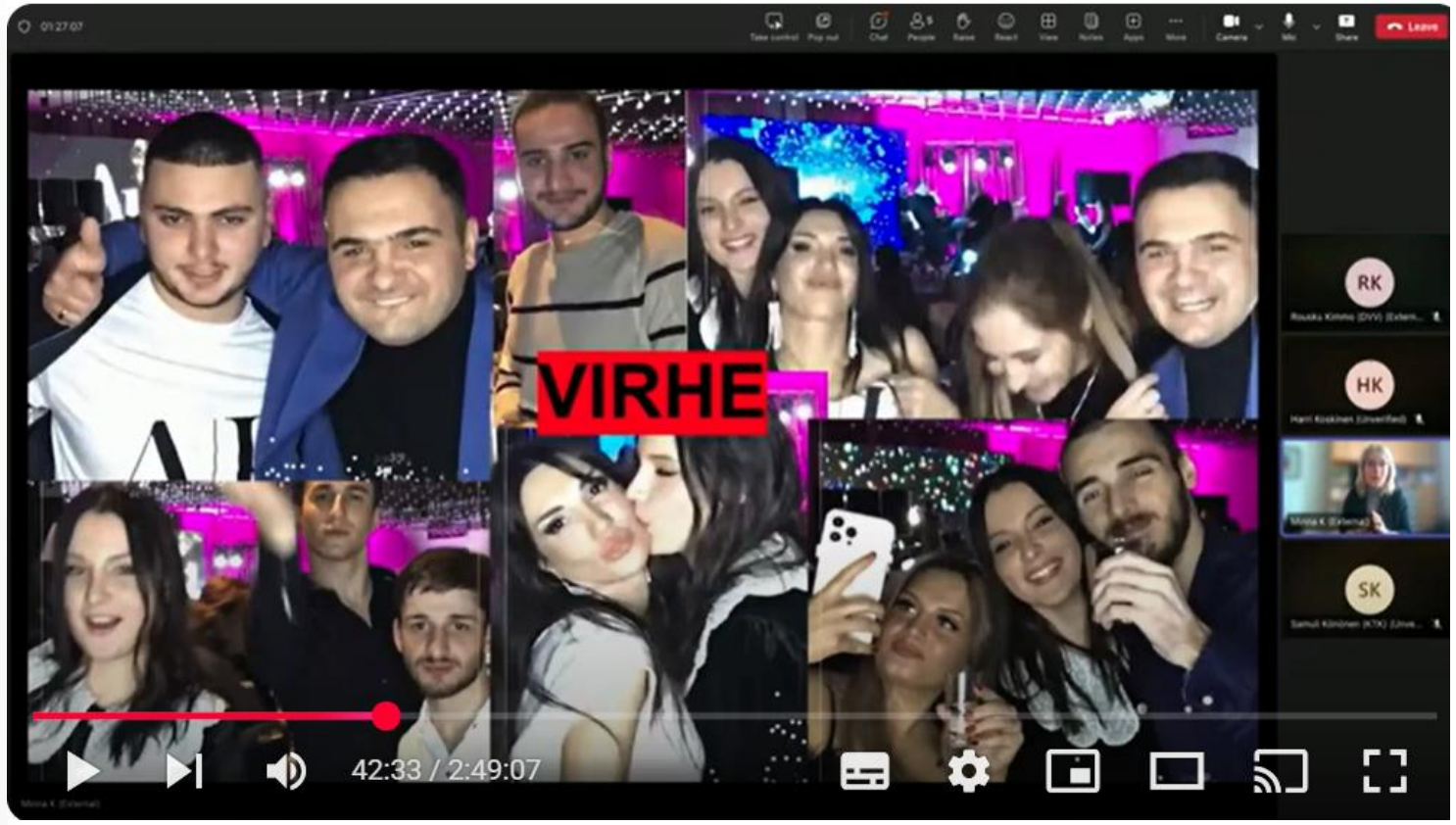
🚨 Miten kansainvälinen verkkorikollisuus toimii?
"Petostehdas Georgiassa"
- kiitos Minna Knus-Galán

👉 Tähän kannattaa tutustua niin ymmärrät, millaista tämä globaali verkkorikollisuus on, tässä tapauksessa rikoshyöty on kuitenkin "vain" 34 miljoonaa euroa ja taustalla 80 hengen petostehdas:
https://lnkd.in/d4YXb__R

"Valtava tietovuoto georgialaisesta petostehdasverkostosta on annettu Ruotsin yleisradioyhtiö SVT:lle, joka jakoi aineiston yli 30:lle medialle. Yle MOT-toimitus on ainoa suomalainen media, jolla on pääsy aineistoon.

Aineisto sisältää kolme miljoonaa tiedostoa, joista miljoona on huijauspuhelua."

💡 Kannatta huomata, että "Aineistosta löytyy reilut 1500 puhelua Suomeen, uhreja muutama kymmenen." sekä "Suomalaisilta varastetut summat vaihtelevat 250 euron ja 65 000 euron välillä." - siis jos uhreja ollut vaikka 30, niin joka 50 soitto käynnistää aina rikoksen?



- 21.3.2025 Digiturva - YouTube

Oletko ollut yhteydessä pankkiin ja tehnyt rajoituksia tilisiirtoihin ja pankki/luottokorttien rajoituksiin?

Älä säilytä nettikäytössä olevalla yhdellä tilillä enempää rahaa kuin minkä tarvitset kuukaudessa!

DIGI- JA VÄESTÖTIETOVIRASTO

Mitä uhkia tekoäly tuo mukanaan?

DIGI- JA VÄESTÖTIETOVIRASTO

Onko kuvassa näkyvä tarjous digihuijaus?

Kyllä, tämä vaikuttaa digihuijaukselta. Tässä on muutamia huijausviitteitä:

1. **Epäuskottava hinta:** 1,95 € hintainen Makita-työkalusarja kuulostaa liian hyvältä ollakseen totta. Laadukkaat työkalut eivät koskaan ole näin edullisia, vaikka pakkauksessa olisi pieniä vikoja.
2. **Bauhausin brändin käyttö:** Huijauksissa käytetään usein tunnettujen brändien nimiä, kuten Bauhaus ja Makita, luomaan luottamusta. Bauhaus ei ole ilmoittanut tällaisesta kampanjasta virallisilla kanavillaan.
3. **Linkin tai lomakkeen täyttäminen:** Huijaukset pyytävät usein täyttämään lomakkeen tai klikkaamaan linkkiä. Näiden kautta yritetään kerätä henkilökohtaisia tietoja tai maksukorttitietoja.
4. **Kuva ja teksti:** Kuvassa näkyvä henkilö oranssissa esiliinassa ei todennäköisesti ole Bauhausin työntekijä, ja tausta vaikuttaa varastolta, ei myymälältä. Tämä on tyypillistä huijauskuvissa.
5. **Facebook-sivu:** Sivun nimi *"Työkalupakki sinulle"* ei ole Bauhausin virallinen sivu. Huijarit luovat usein tällaisia sivuja jäljitelläkseen aitoja yrityksiä.

Turvallisuusvinkki:
Älä klikkaa linkkiä tai jaa henkilötietojasi. Jos olet epävarma, tarkista Bauhausin virallisilta verkkosivuilta tai sosiaalisen median tileiltä, onko tällainen tarjous oikeasti olemassa. Voit myös ilmoittaa tällaisesta julkaisusta Facebookille huijauksena.

Näitä kuvia ja videoita tehtäessä ei ole siis vahingoitettu yhtään oikeaa eläintä!

Kimmo Rousku • You
ICT, cyber- and digital security | #AI | Keynote-speaker and trainer | T...
1w •

😳 Onpas tämä ikävä päivä varoitella #tekoäly #AI väärinkäytön mahdollisuuksista.

Julkaisin hetki sitten varoituksen entistä automatisoidummista tekoälyn tuottamista lunnashaittaohjelmahyökkäyksistä ja muista väärinkäyttömahdollisuuksista:
🔗 https://lnkd.in/dYWyU79K

Nyt toinen varoitus koskee merkittävää loikkaa tekoälyn kyvyssä tuottaa entistä helpommin kehittyneitä syvävääreennettyjä valokuvia ja videoita.

🎥 Käytän esimerkkinä yksityistä valokuvaani, jossa noin 5-vuotiaana sain syntymäpäivälahjaksi Lulu-koiran, dalmatialaisen. Kuvassa on myös isäni.

Alkuperäinen kuva oli mustavalkoinen → tekoälyllä väritetty.
Nyt Google NanoBanana -palvelun avulla siitä luotiin lyhytvideo.

👉 Jos tällaisia 5–10 sekunnin videoita voidaan luoda näin helposti ja kohtalaisen laadukkaasti, niin milloin pystymme tuottamaan 10 minuutin 4K-tason dokumentteja?

🎬 Laillisena ja positiivisena käyttötapauksena voisi tehdä vaikka sukutarinan: yhdistää suvun valokuvia eri ikäkausilta, tarinoita ja tapahtumia ja luoda niistä videon – luonnollisesti lupien kera.

⛔ Mutta yhtä helposti tämä teknologia voi taipua laittomaan, loukkaavaan ja yksityisyyttä rikkovaan käyttöön.

⚠️ Kehitys on huimaa, ja siksi meidän on pakko tunnistaa tämänkin teknologialoikan sekä hyvät että pahat puolet. On selvää, että netti tulee pian täyttymään entistä enemmän erilaisista videotuotannoista.

Tekoälyn kehittyminen jatkuu eksponentiaalisesti – vuoden päästä 10x ja kahden vuoden päästä 100x ?

- Ole entistä varovaisempi kaikkien **valokuvien, videokuvien, äänien ja jopa videoneuvotteluiden kanssa.**

- Suosittelen perheen sisäiseen käyttöön **sopivan koodisanan käyttämistä**, jonka voi kysyä milloin tahansa ja jos vastapuoli (oletettu perheenjäsen) ei osaa sitä, kyseessä on syväväärennetty puhelu tai videoneuvottelu – tai jokin muu ulkopuolinen toimija.

YHTEENVETO – viisi tärkeintä vinkkiäni

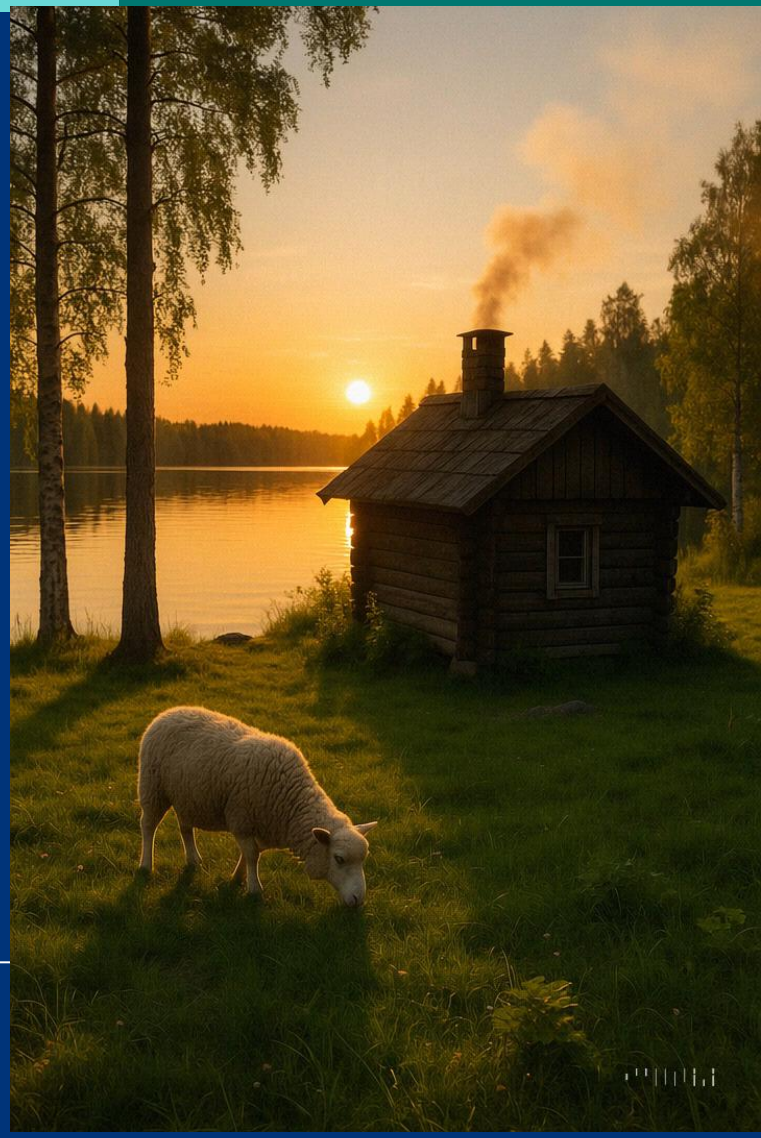
- **1. Verkkorikolliset hakevat ennen kaikkea rahaa!**
  - Aina kun **JOKU ULKOPUOLINEN** pyytää sinua maksamaan rahaa tai antamaan pääsyn pankkitille – **ÄLÄ ANNA**
  - antamaan tunnuksia tai salasanoja – **ÄLÄ ANNA**
    - Vain silloin, kun sinä olet itse käynnistänyt prosessin, toiminta on turvallista, esimerkiksi kun **menet oma-aloitteisesti maksamaan laskuja** tai **tilaat nettikaupasta jotakin**.
- **2. Käytä jokaisessa palvelussa ainutkertaista salasanaa!**
  - Jos salasanasi päätyy verkkorikollisten haltuun jonkin palvelun tietomurron seurauksena, se ei vaaranna tietojasi missään muussa palvelussa
- **3. Opettele tunnistamaan kotimaiset verkko-osoitteet** eli omapankkisi**.fi/**tunnistaudu tai nettikauppa**.fi/**tilaus
- 4. **Käytä vahvaa tunnistautumista**, aina kuin mahdollista – pankkitunnistus, mobiilivarmenne tai palvelun kaksivaiheinen tunnistautuminen
- 5. Pyri hankkimaan tai **käyttämään varalaitetta**, koska jos ainoa laitteesi hajoaa tai varastetaan, uuden laitteen käyttöönotto voi viedä aikaa kauan, etenkin jos käytettävissä ei ole mitään toimivaa vahvaa tunnistautumista – toinen laite voi olla tabletti tai useamman perheenjäsenen jakama varalaite

Kiitos!

Hyvää termisen loppukesän jatkoa vielä näin lokakuussa!

Kysymyksiä, kommentteja tai palautetta:
kimmo.rousku@dvv.fi

Vapaa-aika:
kimmo.rousku@tietoturva.fi



DIGI- JA VÄESTÖTIETOVIRASTO

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi