

TRAFICOM

Liikenne- ja viestintävirasto

Nyt valppaana!

Mediatilaisuus 2.12.2025

Aalto yliopisto, Digi- ja väestötietovirasto,
Poliisi ja Traficom Kyberturvallisuuskeskus

A circular inset image showing a woman with grey hair wearing a bright yellow button-down shirt, sitting in the driver's seat of a car. She is looking down at a white smartphone in her hands. The background is blurred, showing the interior of the car and some outdoor elements. Overlaid on the image is white text in Finnish.

a kaikki
ole sitä
yttää.

ana.fi

Ohjelma 2.12.2025

- Tietoverkkoavusteiset petokset poliisin näkökulmasta - Rikosylikonstaapeli Juha Springare, Keskusrikospoliisi
- Miten suojaudut verkkohuijauksilta - Erityisasiantuntija Juha Tretjakov, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
- Digiturvabarometrin tuloksia - Johtava erityisasiantuntija Kimmo Rousku, Digi- ja väestötietovirasto
- Ihmisen rooli kyberturvallisuudessa - Projektipäällikkö, tutkija Marianne Lindroth, Aalto-yliopisto
- Kysymyksiä kaikille puhujille



Tietoverkkoavusteiset petokset poliisin näkökulmasta

2.12.2025

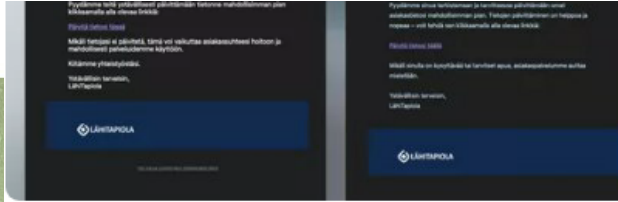
Keskusrikospoliisi
Rikosylikonstaapeli Juha Springare

Kirja: Jarmo Koski menetti säästönsä nettihuijauksessa

Salattujen elämien Seppo Taalasmaana tunnettu näyttelijä Jarmo Koski menetti melkein kaikki rahansa. Hän kertoo asiasta ensimmäistä kertaa elämäkerrassaan.

JAA

TALLENNA



Poikkeuksellinen varoitus kajahti suomalaisille – Varo tällaisia viestejä

Varo: Ilmoitus virheellisestä pysäköinnistä voi tyhjentää tilin

Vakava varoitus: Tällainen puhelu tarkoittaa, että rikolliset ovat kohtuullasi



Poliisi varoittaa "Osuus-
turvahenkilöistä" – Huij-
veivät jättisumman

Rakkaushuijausten ja verkkorikosten jäljet johtavat usein "scam centeriin"

USA:n kongressi tutkii Muskin Starlink-satelliittien yhteyttä Myanmarin huijauskeskuksiin



Huijauskeskusten katoille on alkan

STT-AFP

14.10. 5:13

Myanmar on ryhtynyt alk-
nettihuijauksiin, joita my-

Myanmarissa tuhotaan huijauskeskuksia

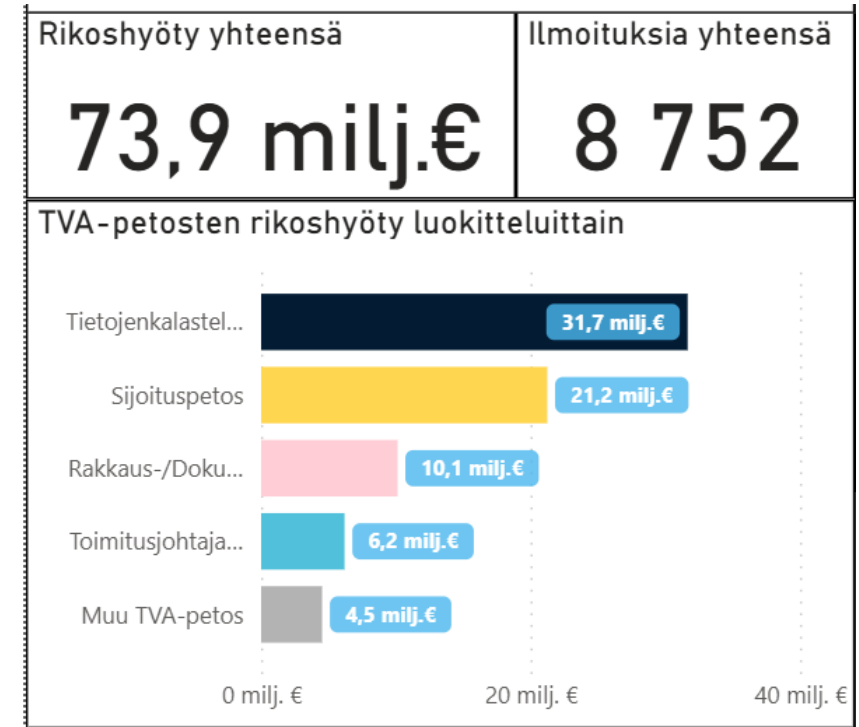


JULKAISTU 26.11.2025 12:26

2.12.2025

Tietoverkkoavusteiset petokset (TVA-petokset)

- Globaali "megatrendi", eniten kasvava rikosala Euroopassa (Europol SOCTA 2025)
- Suomalaisilta yritettiin huijata vuonna 2024 yli 107 miljoonaa euroa. Pankit pysäyttivät tästä n. 44 miljoonaa euroa (Finanssiala ry)
- Suomessa on kykyä estää TVA-petoksia



Kuva 1. Poliisille kirjatut rikosilmoitukset keskeisistä TVA-petoksista 1.1.-31.10.2025 (Lähde: Valtakunnallinen TVA-yksikkö). Rikosvahinko kirjaushetken perusteella.

TOP 4 vahingollisinta petosten tekotapaa

- ▶ Tietojenkalastelu
 - Nopeita, paljon uhreja, tarina turvatilistä pahin → hätä ja kiire
- ▶ Sijoituspetokset
 - Pitkäaikaisia – kryptot
- ▶ Rakkaus- ja dokumenttipetokset
 - Pitkäaikaisia – voimakkaita tunteita
- ▶ Toimitusjohtajapetokset
 - Nopeita – suuret kertavahingot

Miksi petokset onnistuvat?

- ▶ **Voimakas sosiaalinen manipulointi:** hätä, empatia, luottamus, vaurastumisen halu
- ▶ "Huono hetki"
 - Tämä on meillä kaikilla yhä useammin
- ▶ Teknologinen kehitys

Tilimuulit petoksissa – rahanpesurikokset haasteena

- ▶ Uhrin varoja siirretään portaittain alkuperän häivyttämiseksi
- ▶ Tilimuuli jää usein kiinni ja rikosvastuu kohdentuu häneen
- ▶ **Rekrytoinnin kohteena yhä enemmän lapsia ja nuoria**
- ▶ **Väylä rikollisverkostoihin ja rikoskierteeseen → Kansallinen ongelma**

Kiitos

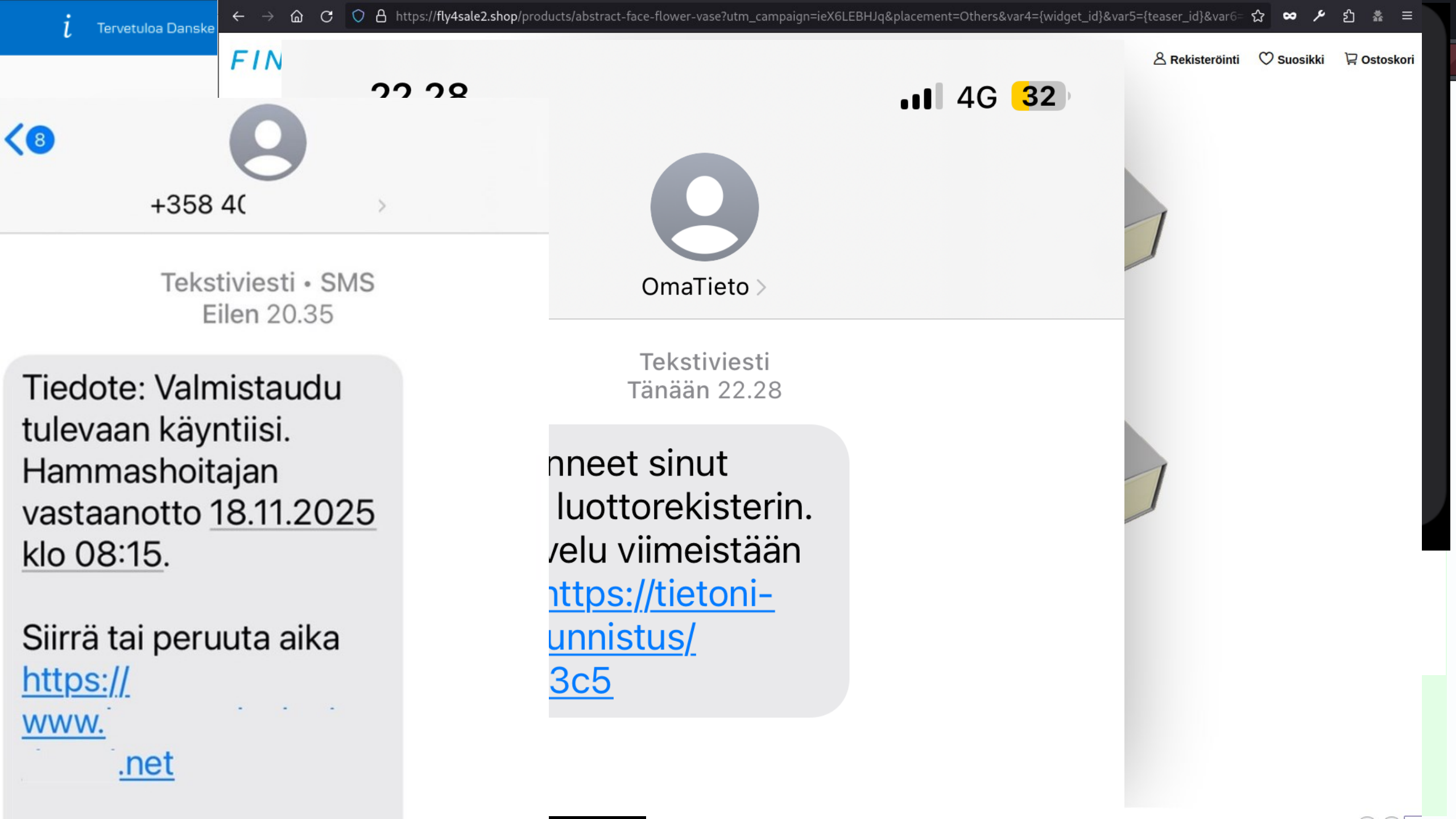


TRAFICOM

Liikenne- ja viestintävirasto

Miten suojaudut verkkohuijauksilta

Erityisasiantuntija Juha Tretjakov,
Liikenne- ja viestintävirasto
Traficomin Kyberturvallisuuskeskus



Tervetuloa Danske

FIN

22 28

4G 32

Rekisteröinti Suosikki Ostoskori



+358 40

Tekstiviesti • SMS
Eilen 20.35

Tiedote: Valmistaudu tulevaan käyntiisi.
Hammashoitajan vastaanotto 18.11.2025
klo 08:15.

Siirrä tai peruuta aika
<https://www...net>



OmaTieto >

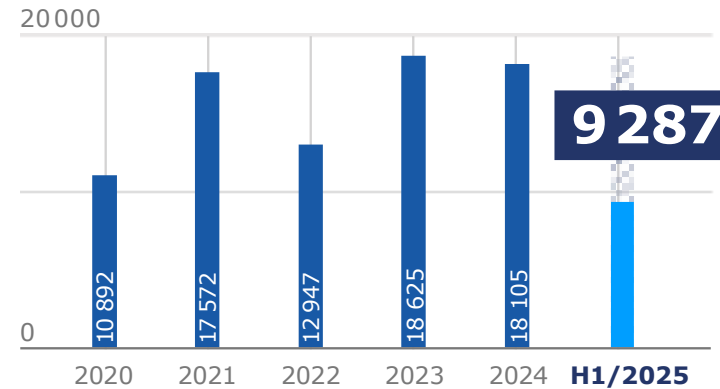
Tekstiviesti
Tänään 22.28

...nneet sinut
...luottorekisterin.
...velu viimeistään
<https://tietoni-unnistus/3c5>

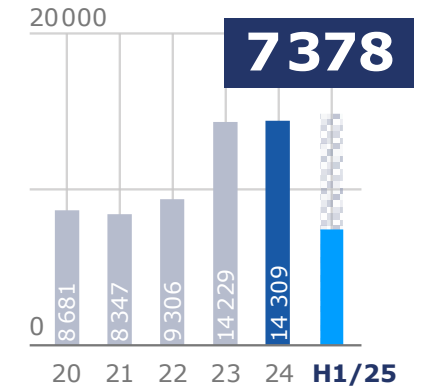
2025 numeroina

Kyberpoikkeamailmoitukset 2020–2024

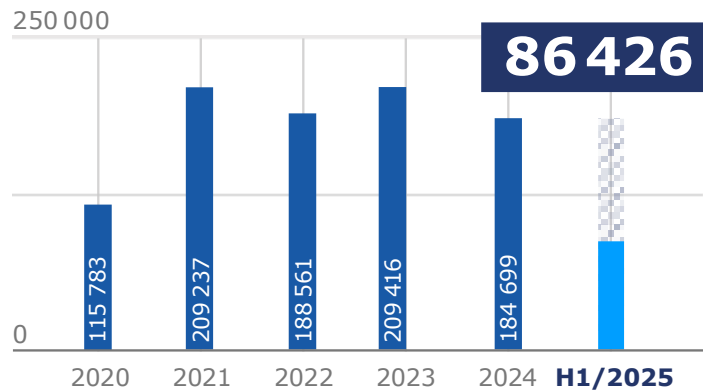
Kaikki kyberpoikkeamailmoitukset



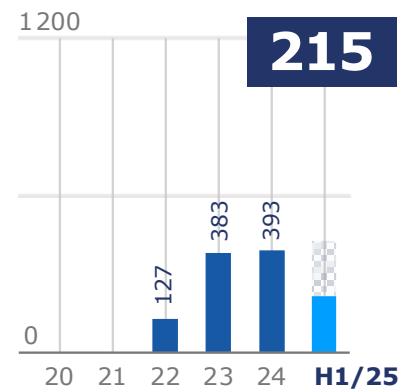
Huijaukset ja kalastelut¹



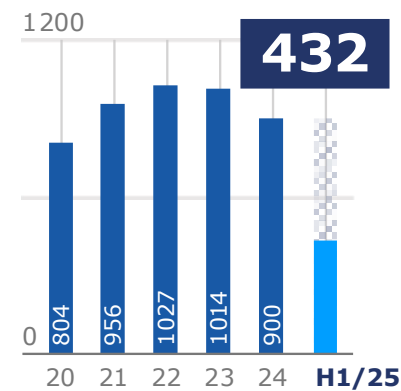
Automaattisesti käsitellyt ilmoitukset



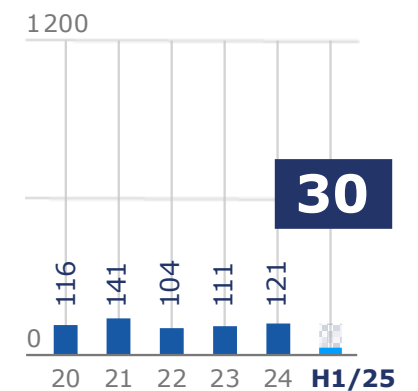
Tietomurron yritykset²



Tietomurrot



Tietovuodot



■ ilmoitukset vuosina 2021–2024 ■ ilmoitukset 01–06/2025 ■ ennuste, perustuen 01–06/2025 lukuihin

LÄHDE: Kyberturvallisuuskeskus | ¹ Huijauksen ja kalastelujen tilastointi on muuttunut vuonna 2024, joten luvut eivät ole täysin verronnollisia. | ² Tietomurtoyritysilmoituksia on raportoitu alkaen vuodesta 2022.

Rikollinen käyttää kaikkia keinoja

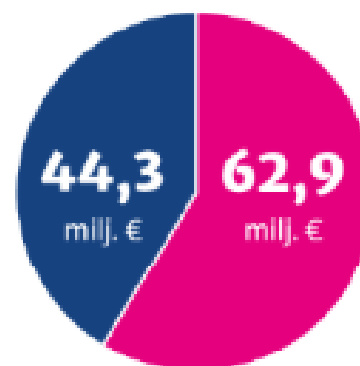


VAHINGOT 2024

107,2
milj. €

+39 %
vrt. 2023

Pankkien
pysäyttämät ja
palauttamatt
maksut

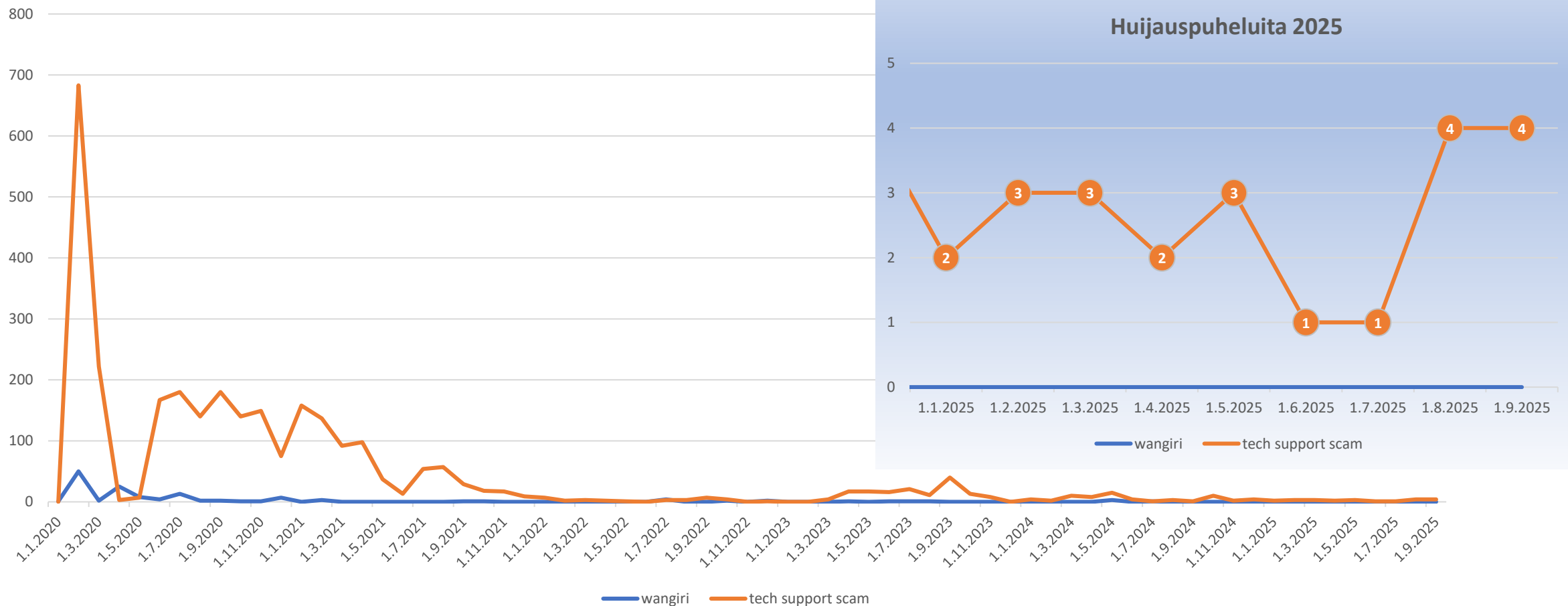


Suomalaiset
menettäneet
verkkorikollisille

Lähde: FA

Puhelinväärennosten tekninen estäminen tepsii

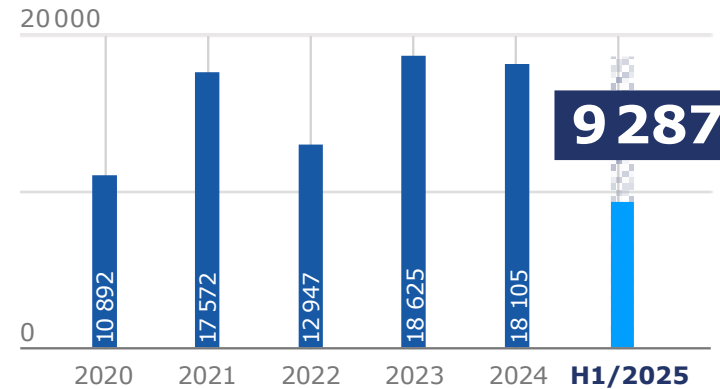
KTK:lle tehdyt ilmoitukset puhelinhuijauksista



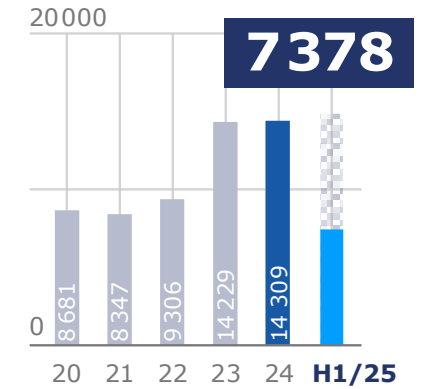
2025 numeroina

Kyberpoikkeamailmoitukset 2020–2024

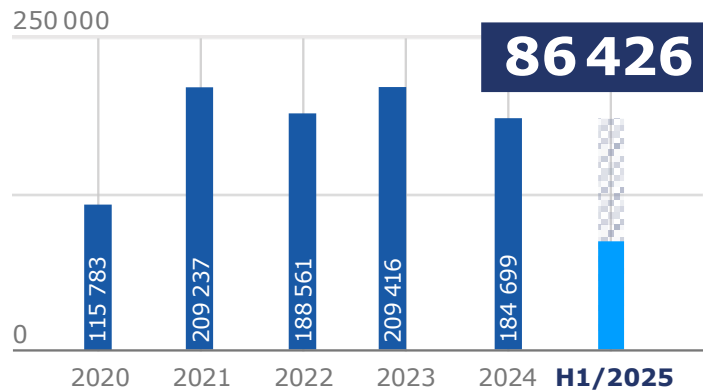
Kaikki kyberpoikkeamailmoitukset



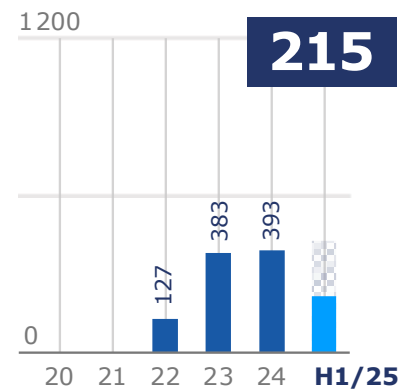
Huijaukset ja kalastelut¹



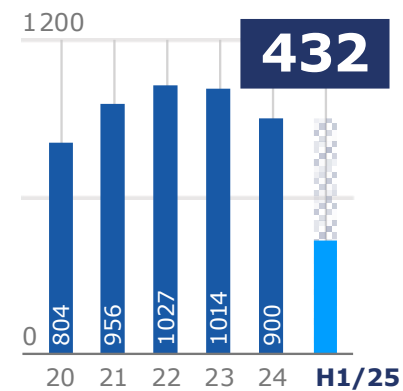
Automaattisesti käsitellyt ilmoitukset



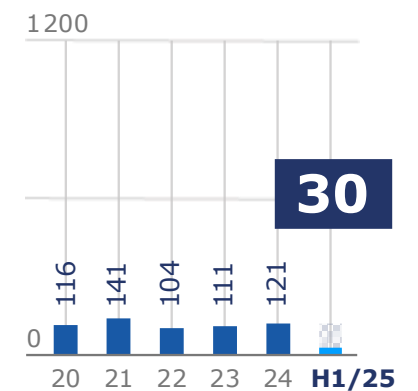
Tietomurron yritykset²



Tietomurrot



Tietovuodot



■ ilmoitukset vuosina 2021–2024 ■ ilmoitukset 01–06/2025 ▤ ennuste, perustuen 01–06/2025 lukuihin

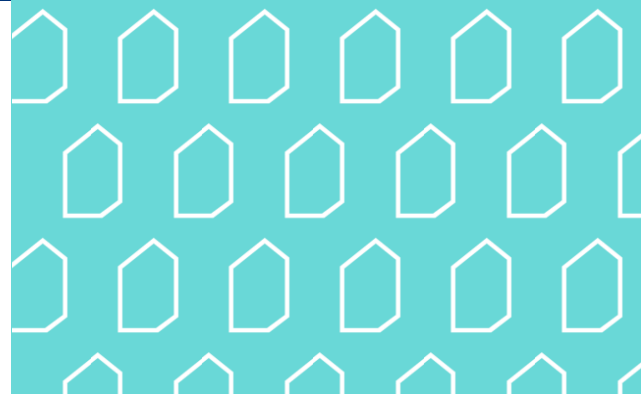
LÄHDE: Kyberturvallisuuskeskus | ¹ Huijauksen ja kalastelujen tilastointi on muuttunut vuonna 2024, joten luvut eivät ole täysin verronnollisia. | ² Tietomurtoyritysilmoituksia on raportoitu alkaen vuodesta 2022.

Nyt valppaana- mediatilaisuus 2.12.2025

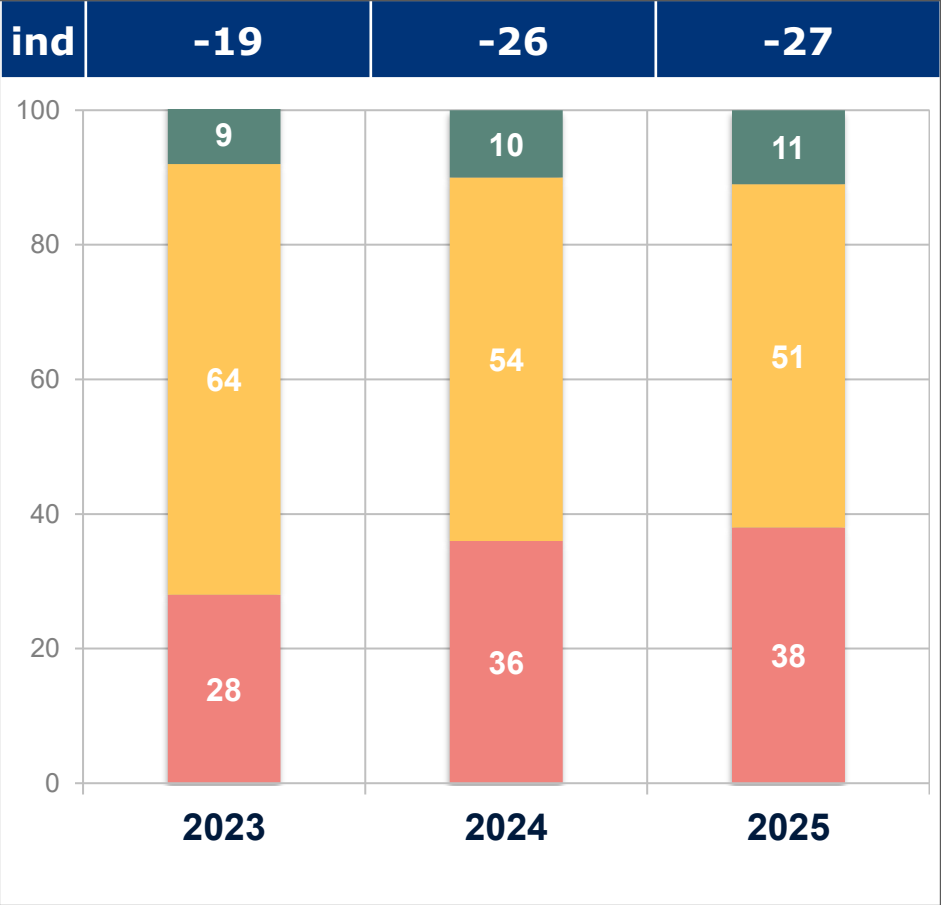
Kimmo Rousku



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



Onko luottamus digitaaliseen turvallisuuteen muuttunut viimeisen vuoden aikana?



Palkeissa %-osuus	Heikentynyt	Pysynyt samana	Vahvistunut
-------------------	-------------	----------------	-------------

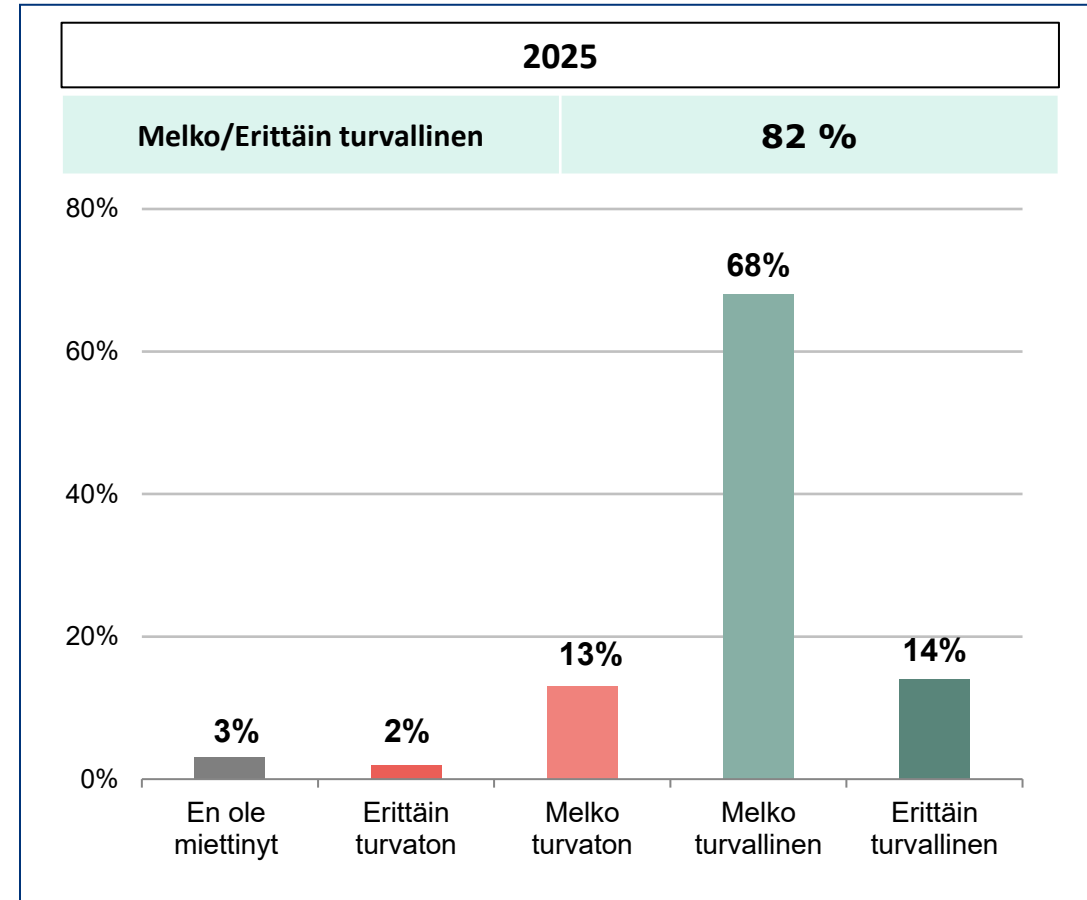
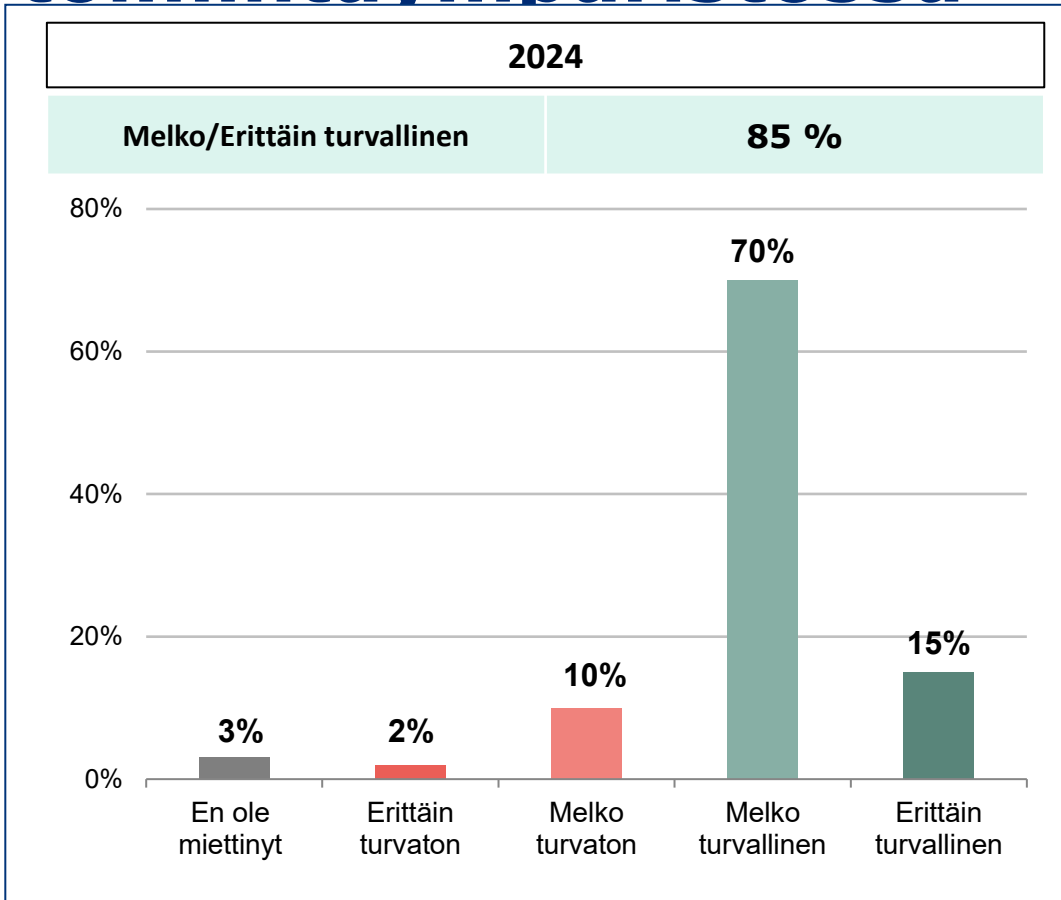
Indeksi = vahvistunut-heikentynyt

Perustelut
Vahvistunut - Yleisesti koetaan, että nykyään käydään enemmän keskustelua digiturvallisuudesta ja siihen liittyvistä riskeistä ja uhkista. Mediassa nostetaan esille ajankohtaisia huijauksia ja kerrotaan neuvoja, miten tilanteissa tulisi toimia. - Moni kokee, että osaa tunnistaa mahdollisia riskejä ja että oma osaaminen on kehittynyt. - Nähdään myös, että digiturvallisuuden parantamiseksi tehdään paljon toimenpiteitä.
Pysynyt samana - Omassa arjessa ei ole tapahtunut muutoksia, jotka vaikuttaisivat turvallisuuden tunteeseen. Uhkakuvat eivät ole (vielä) realisoituneet itselle tai lähipiirissä. - Monelle luottamus perustuu omaan harkintaan ja varovaisuuteen digitaalisessa ympäristössä. Uskotaan, että osataan toimia oikein. - Tietoisuus erilaisista uhkista, huijauksista ja petoksista on kasvanut, mutta se ei ole heikentänyt omaa turvallisuudentunnetta. Tieto on myös auttanut varautumaan uhkiin.
Heikentynyt - Moni kokee, että erilaisia uhkia on jatkuvasti enemmän ja niiden perässä pysyminen on työlästä ja heikentää omaa luottamusta digitaaliseen turvallisuuteen. - Erityistä huolta aiheuttaa tekoälyn käyttö huijauksissa. Sen avulla huijauksista on tullut entistä uskottavampia ja vaikeammin tunnistettavia. Omaa osaamista kyseenalaistetaan. - Moni myös kertoo konkreettisista huijaukokemuksista tai omasta pelostaan joutua huijauksen uhriksi.

Onko luottamuksesi digipalveluiden ja -laitteiden turvallisuuteen muuttunut viimeisen vuoden aikana?

Perustelisitko vielä vastaustasi, miksi?

Turvallisuuden tunne digitaalisessa toimintaympäristössä



Miten turvalliseksi tunnet päivittäisen toiminnan digitaalisessa toimintaympäristössä?

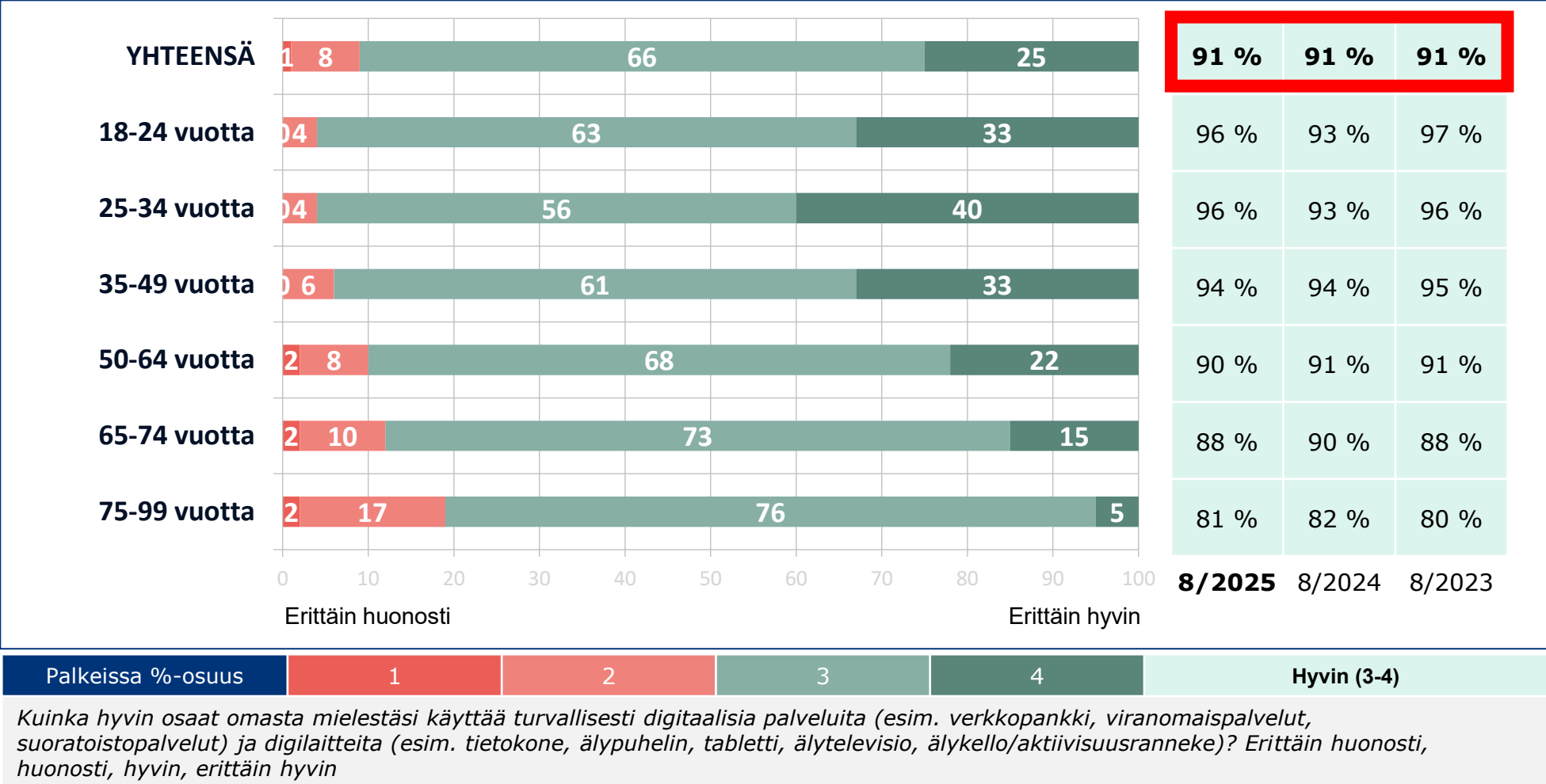
Kansalaiset uskovat osaavansa toimia turvallisesti – mikä on totuus?

- ▶ Digiturvabarometrin mukaan luottamus on säilynyt useassa kysymyksessä edelleen korkealla, mutta yleinen suuntaus vuosien 2022-2025 ajalta on luottamuksen tasainen heikentyminen.

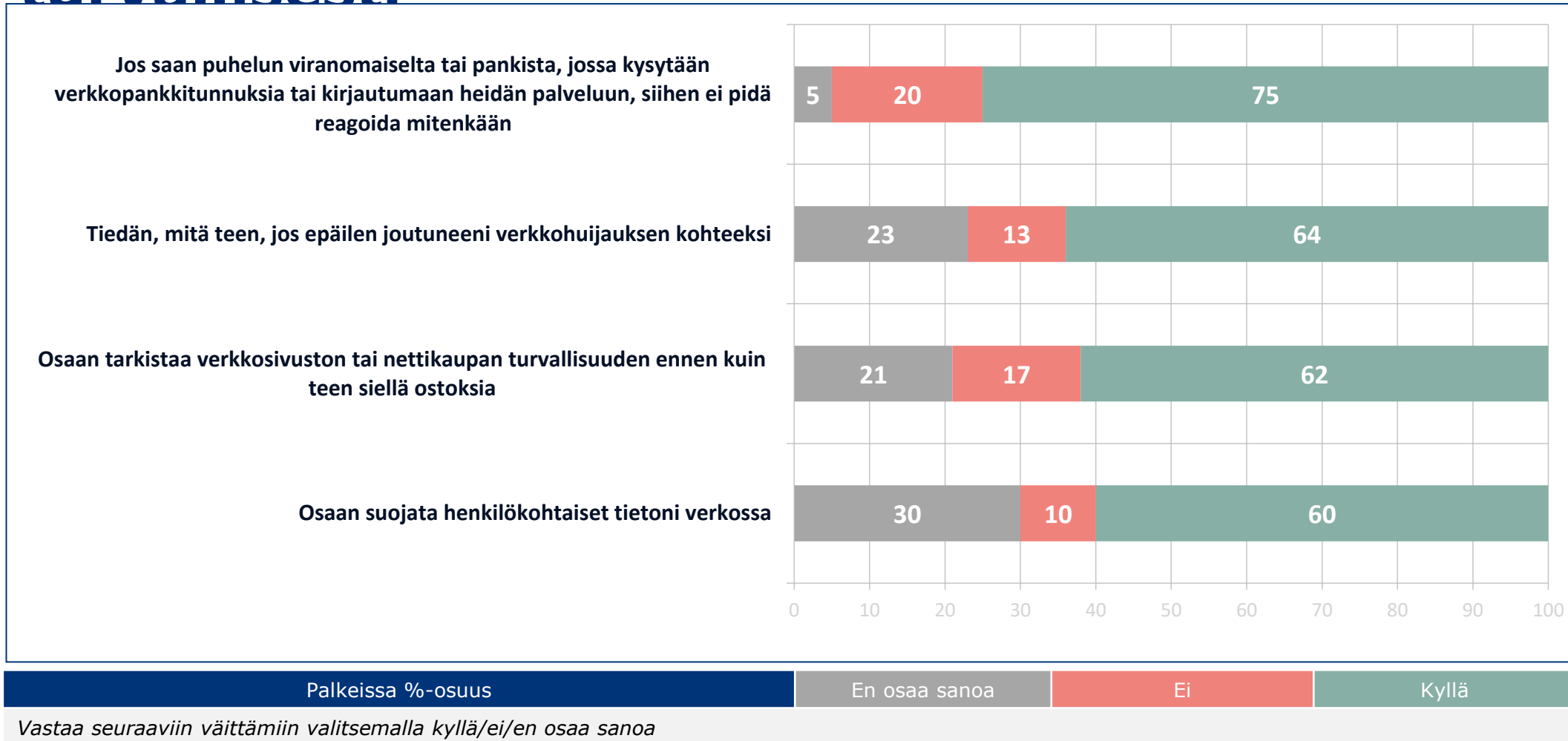
Nyt lisättyjen uusien kysymysten avulla erityisesti kansalaisten omaa uskoa kykyyn toimia turvallisesti (91 % vastaajista arvioinut vuosina 2023-2025) voidaan haastaa, koska

- ▶ 48 % ei käytä tai osaa sanoa, käyttääkö joka palvelussa eri salasanaa
- ▶ 40 % ei tiedä tai osaa sanoa, miten suojataan henkilökohtaiset tiedot verkossa
- ▶ 38 % ei osaa tarkistaa verkkosivun tai nettikaupan turvallisuutta ennen kuin tekee siellä ostoksia
- ▶ 36 % ei tiedä, miten pitää toimia, jos epäilee joutuneensa verkkohuijauksen kohteeksi
- ▶ 25 % reagoi tai ei tiedä, miten toimia, jos viranomaisesta tai pankista soitetaan, ja kysytään pankkitunnuksia tai kirjautumaan heidän palveluun

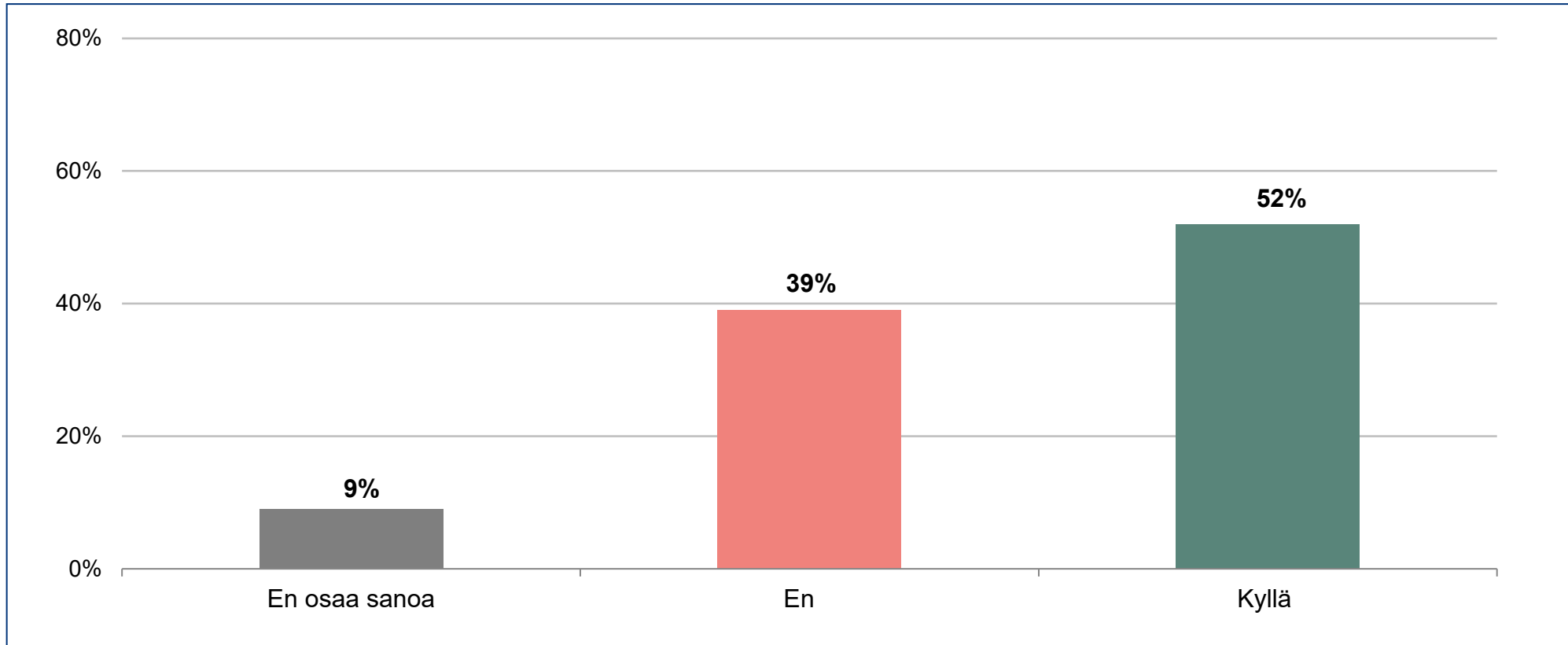
Kuinka hyvin osataan käyttää digitaalisia palveluita ja digilaitteita turvallisesti? ikävertailu



Tietämys digiturvasta ja osaaminen toimia turvallisesti



Käytän jokaisessa eri verkkopalveluissa eri salasanaa



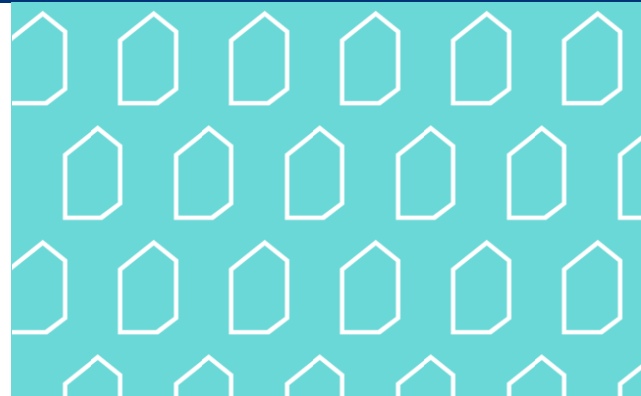
Vastaa seuraaviin väittämiin valitsemalla kyllä/ei/en osaa sanoa

**Huom! Tämän kysymyksen vastaukset kerättiin osana Omnibus-kyselyä (n=1000 vastaajaa, valtakunnallisesti edustava otos sukupuolen, iän ja asuinalueen mukaan. Virhemarginaali on 95 % todennäköisyydellä +/- 3,2.*

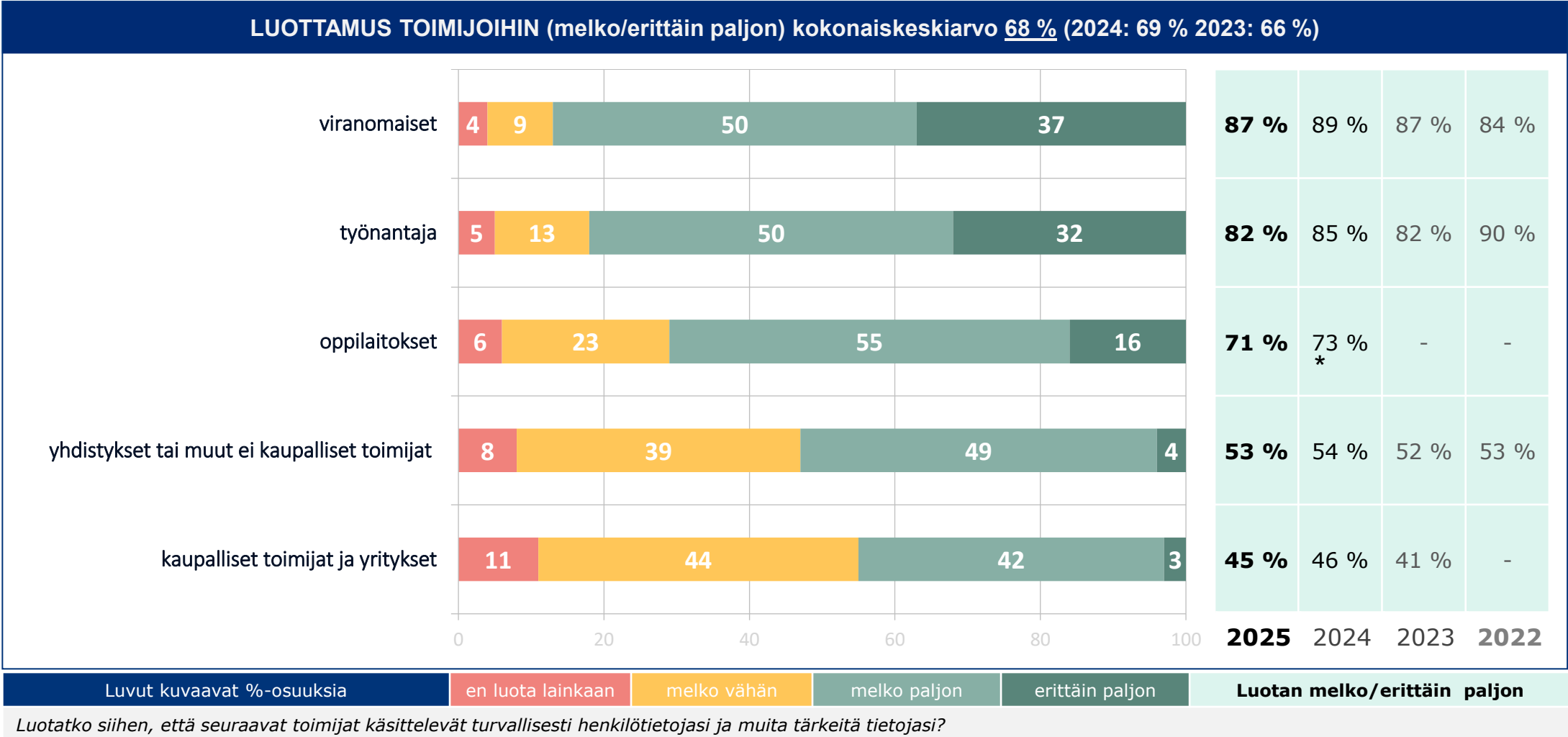
Pari positiivista havaintoa



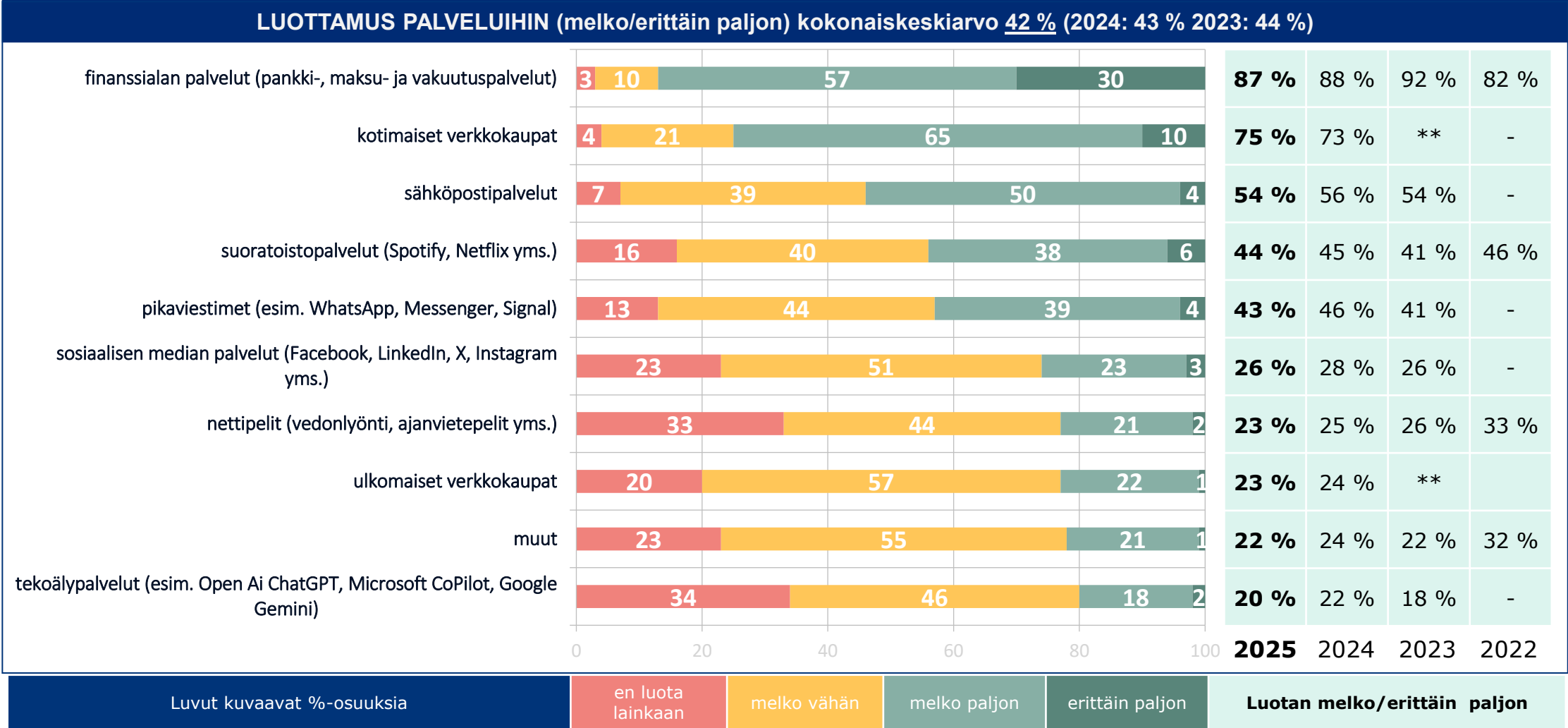
**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



Luottamus siihen, että omia tietoja käsitellään turvallisesti

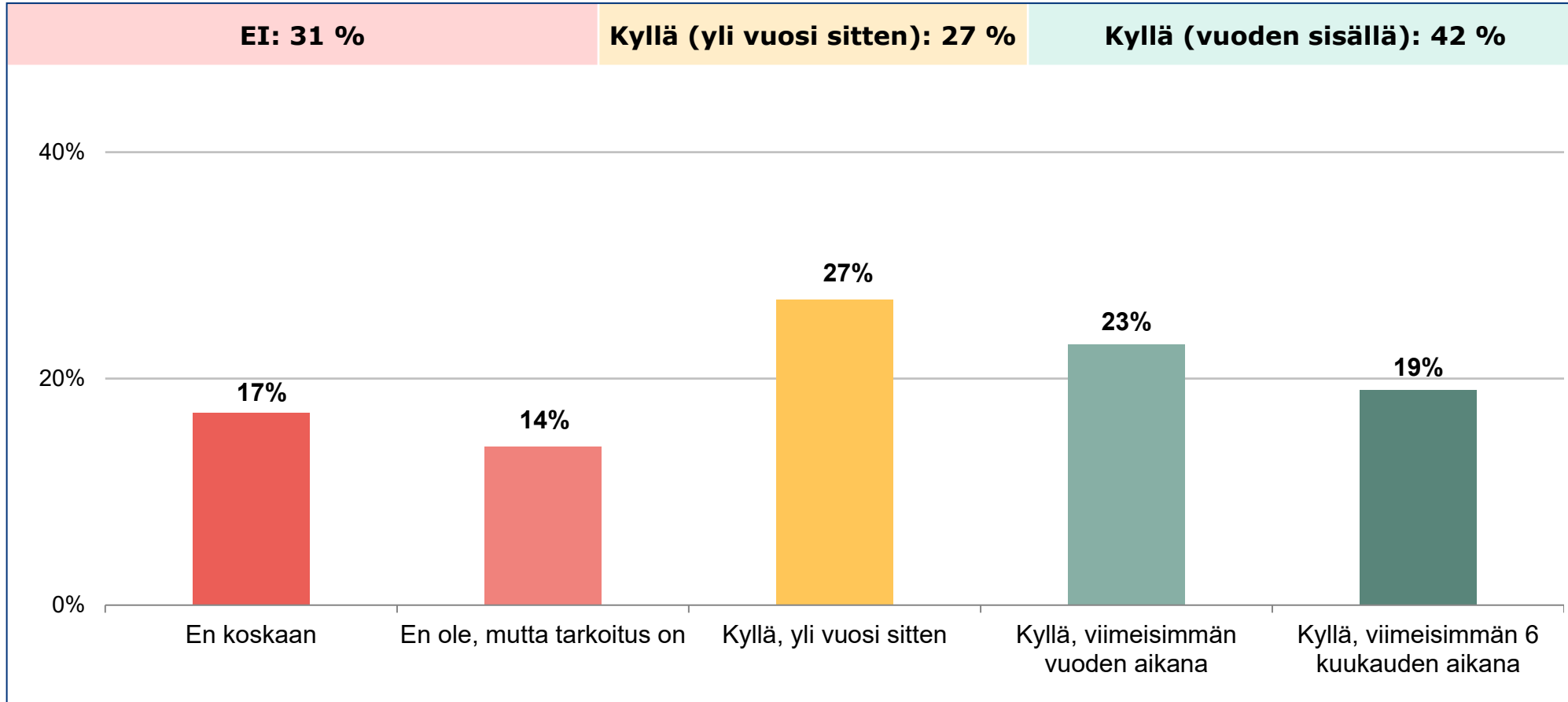


Luottamus siihen, että omia tietoja käsitellään turvallisesti



Luotatko siihen, että seuraavat palvelut käsittelevät turvallisesti henkilötietojasi ja muita tärkeitä tietojasi?

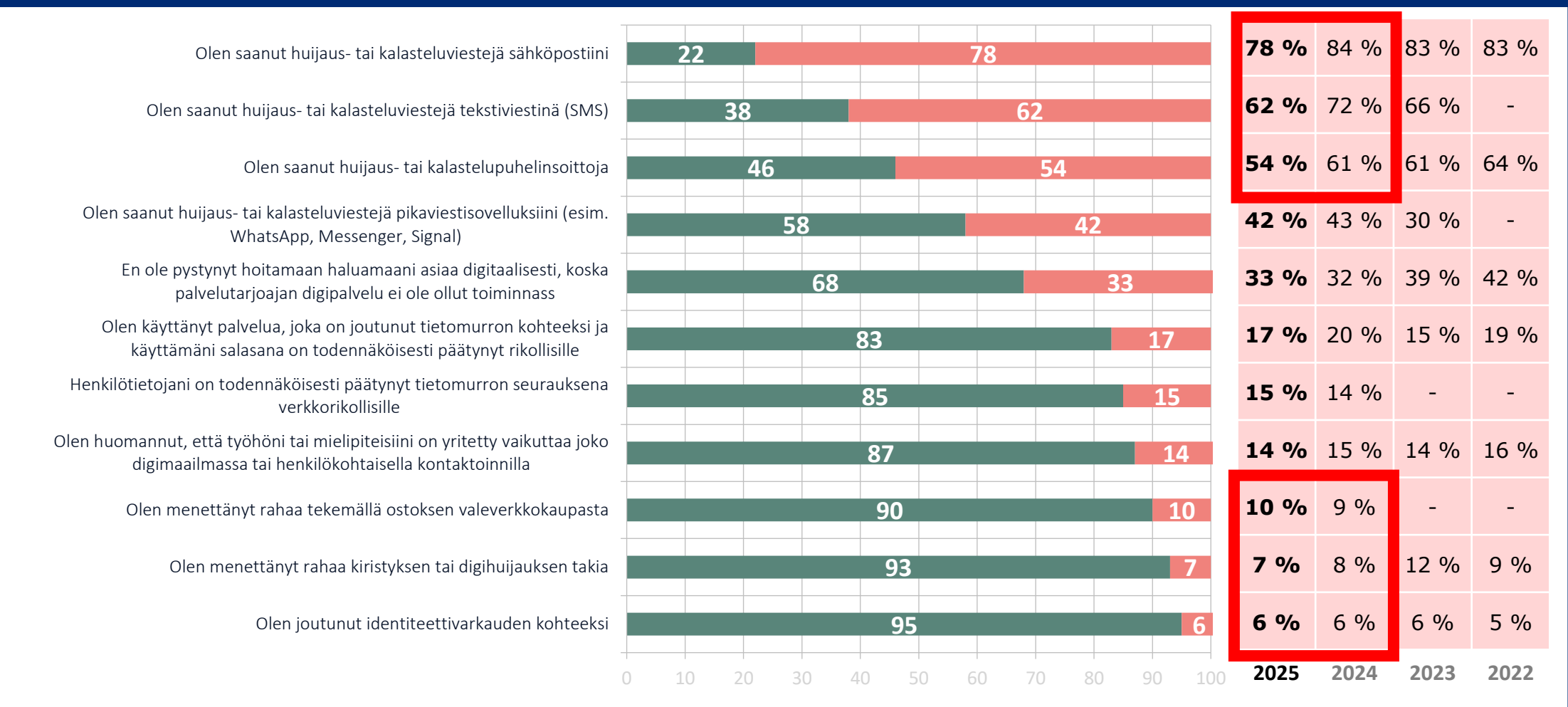
Maksukorttien ja tilien turvallisuuden parantaminen



Oletko itse parantanut maksukorttiesi ja tiliesi käyttöön liittyvää turvallisuutta tai varmistanut näitä asioita pankiltasi?

Digiturvallisuuteen liittyvien uhkien toteutuminen itselle

Uhkien toteutuminen itselle kokonaiskeskiarvo 31 % (2024: 33 %)

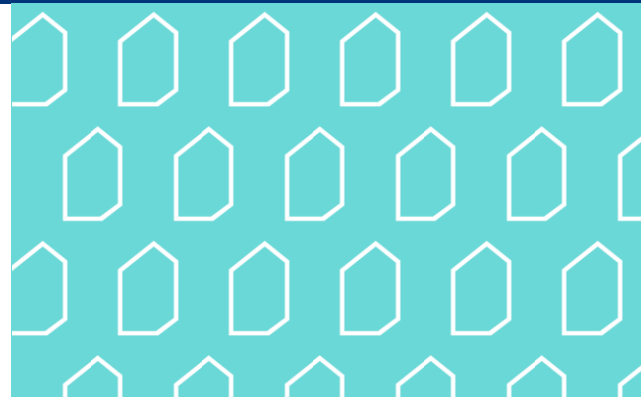


Palkkien luvut kuvaavat %-osuutta
Ei ole tapahtunut minulle
Kyllä, on tapahtunut minulle

Miten nämä heijastuvat arkeen tai yhteiskunnallisen tason luottamukseen?



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



Kuinka paljon kansalaisiin kohdistuvilla digihuijauksilla on vaikutusta – marraskuu 2025?

▶ Huolestuttaa

- ▶ 59 % paljon (24 % erittäin paljon)
- ▶ 41 % vähän

▶ Omaan arkeen

- ▶ 77 % vähän
- ▶ 23 % paljon

▶ Luottamukseen digitaalista yhteiskuntaan kohtaan

- ▶ 53 % paljon (15 % erittäin paljon)
- ▶ 47 % vähän

▶ Miten suomalainen yhteiskunta on varautunut digihuijausten estämiseen ja torjumiseen?

- ▶ 59 % huonosti
- ▶ 41 % hyvin

Entä yhteiskuntaan kohdistuvilla kyberhyökkäyksillä?

• Huolestuttaa

- 59 % paljon (14 % erittäin paljon)
- 41 % vähän

• Omaan arkeen

- 83 % vähän
- 17 % paljon

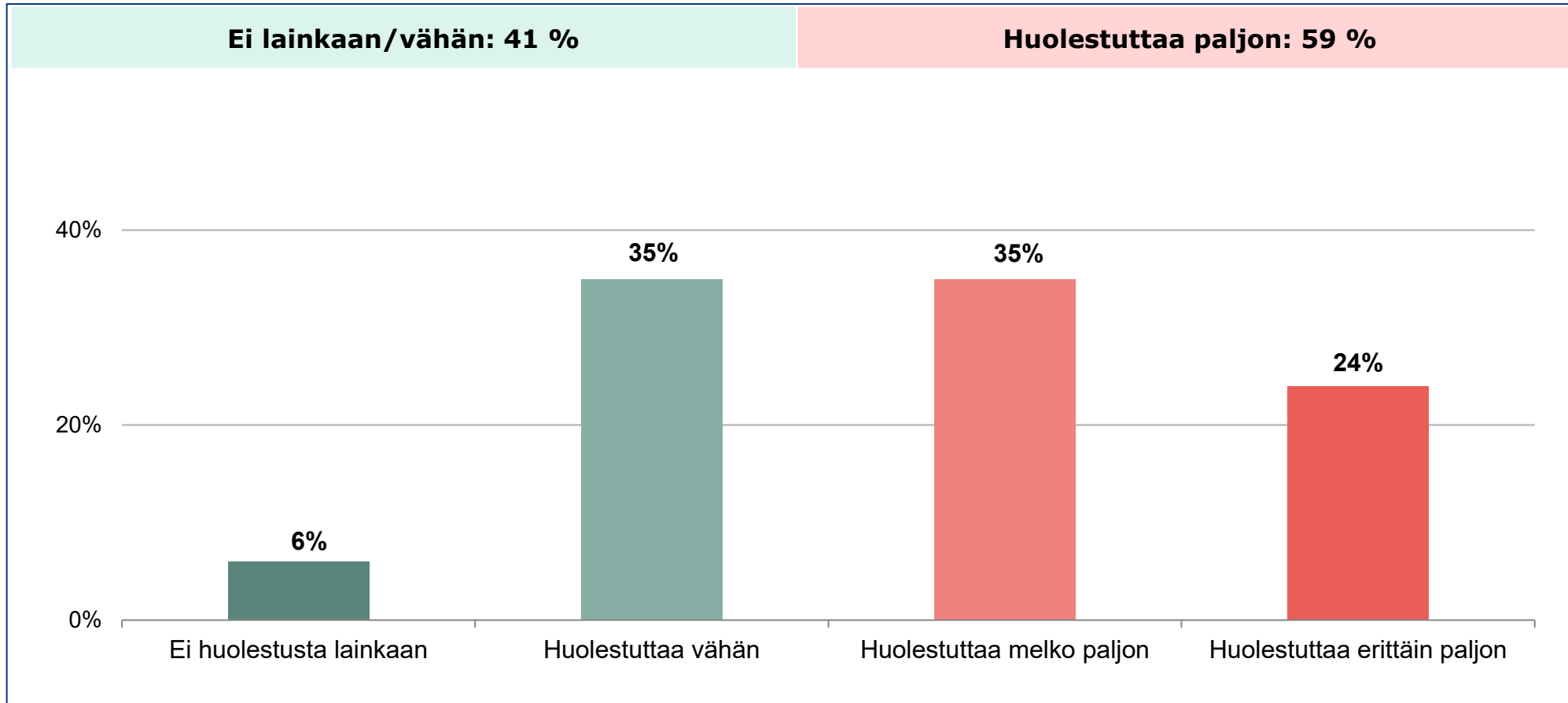
• Luottamukseen digitaalista yhteiskuntaan kohtaan

- 51 % paljon (14 % erittäin paljon)
- 49 % vähän

• Miten suomalainen yhteiskunta on varautunut kyberhyökkäysten estämiseen ja torjumiseen?

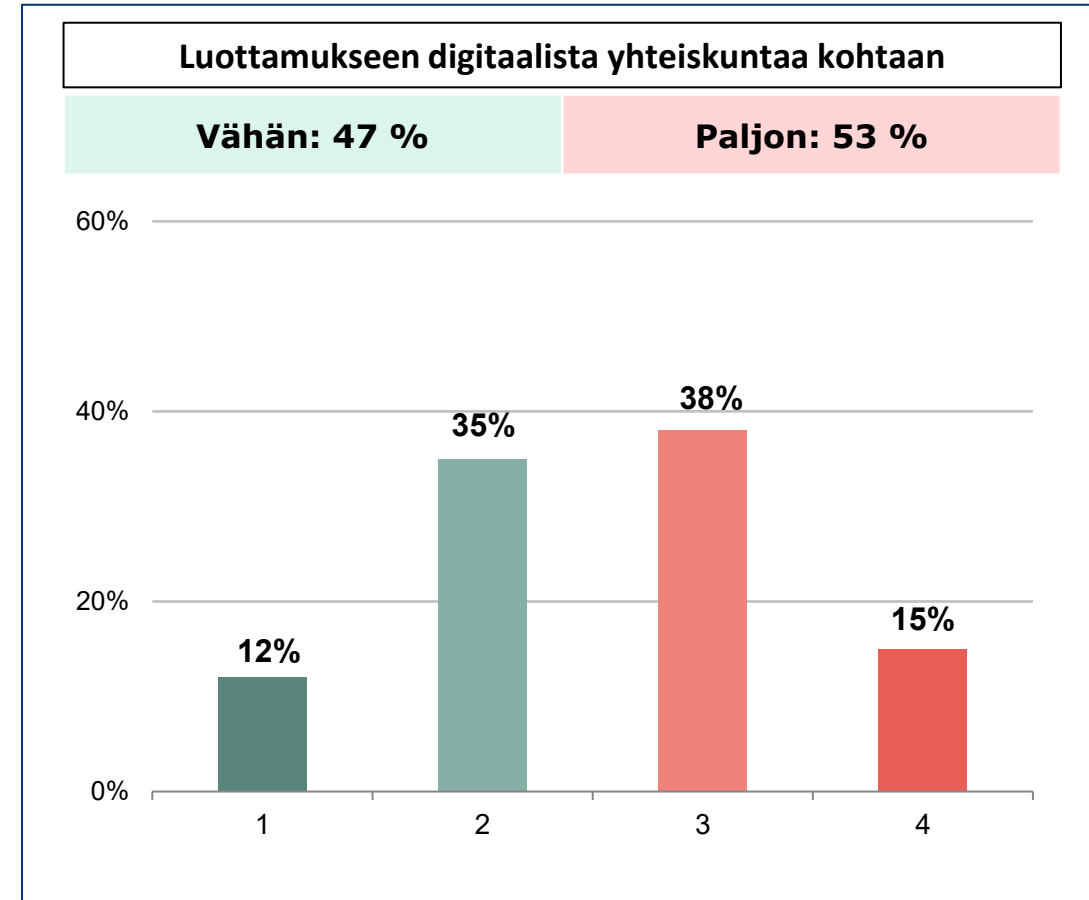
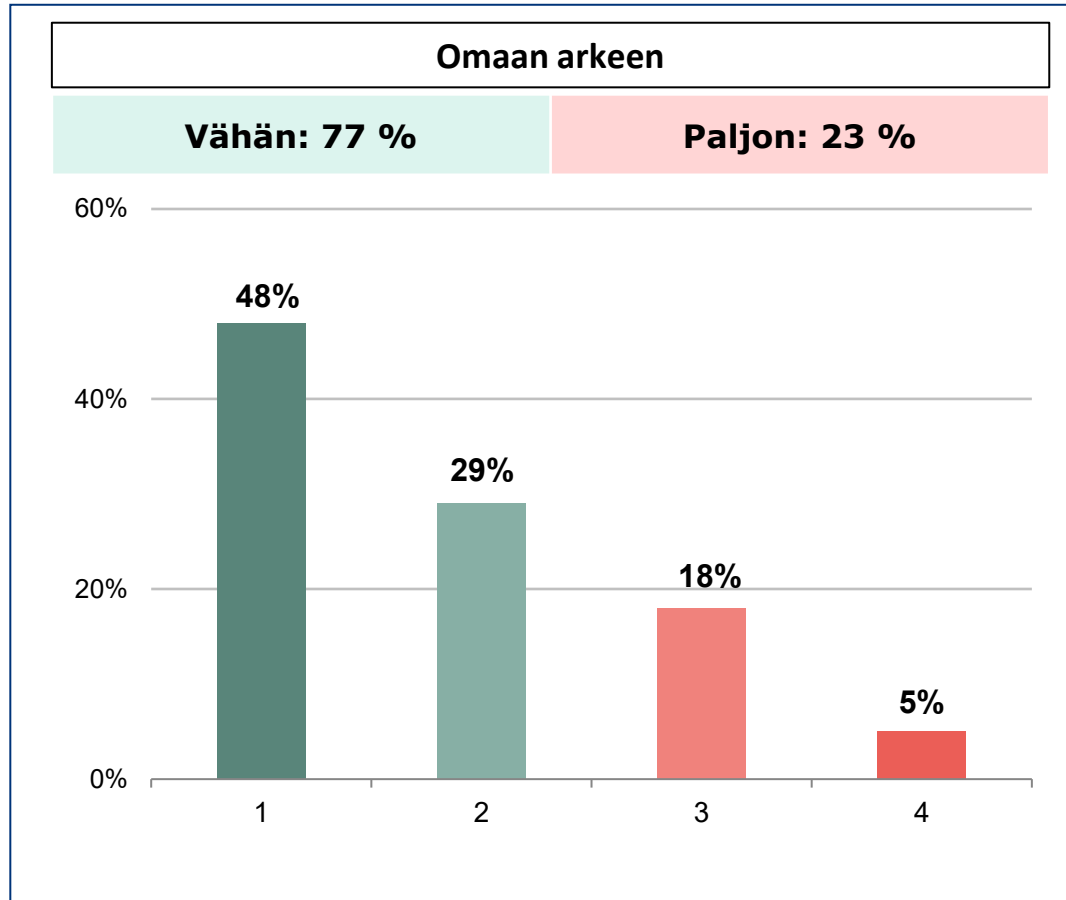
- 55 % huonosti
- 45 % hyvin

Huoli kansalaisiin kohdistuvista digihuijauksista



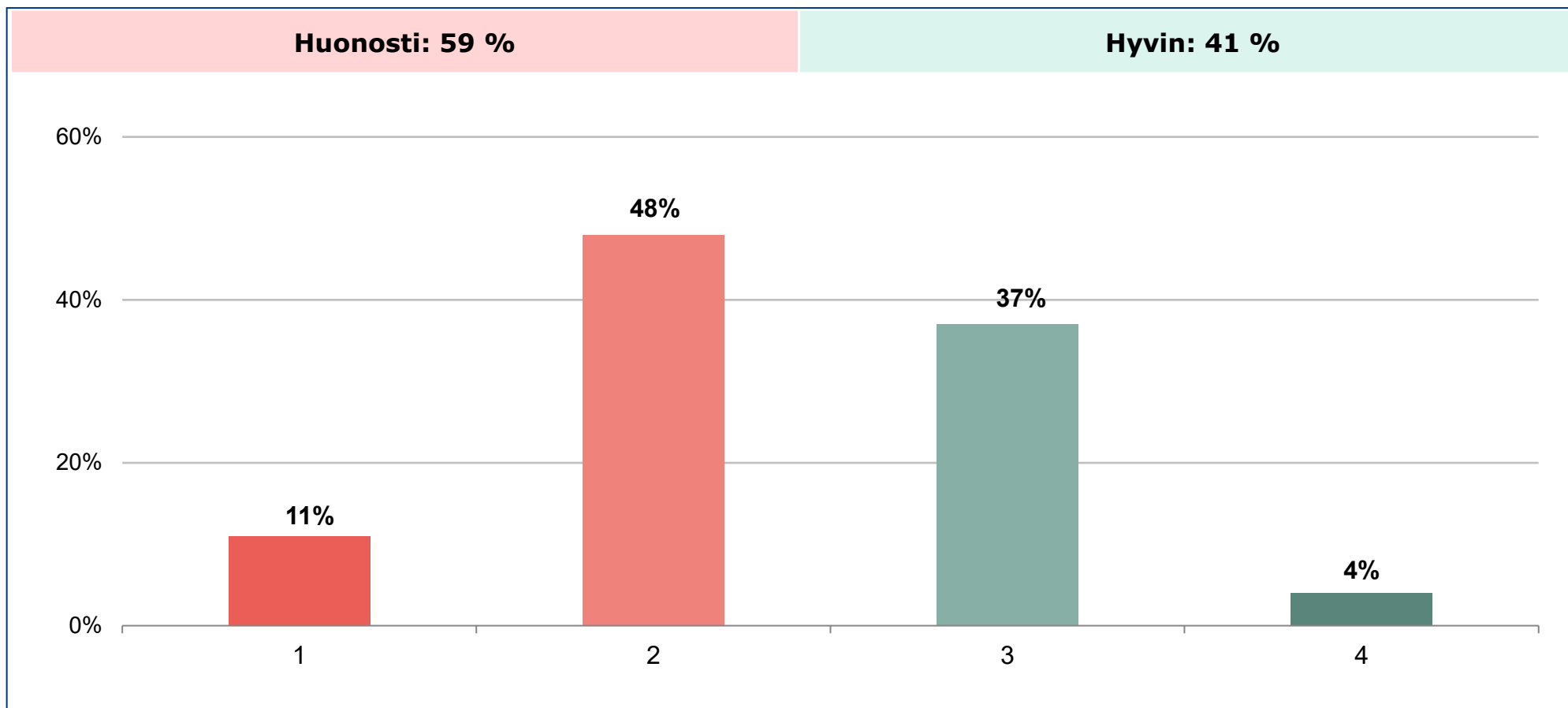
Mitä mieltä olet kansalaisiin kohdistuvista digihuijauksista?

Kansalaisiin kohdistuvien digihuijauksien vaikutus



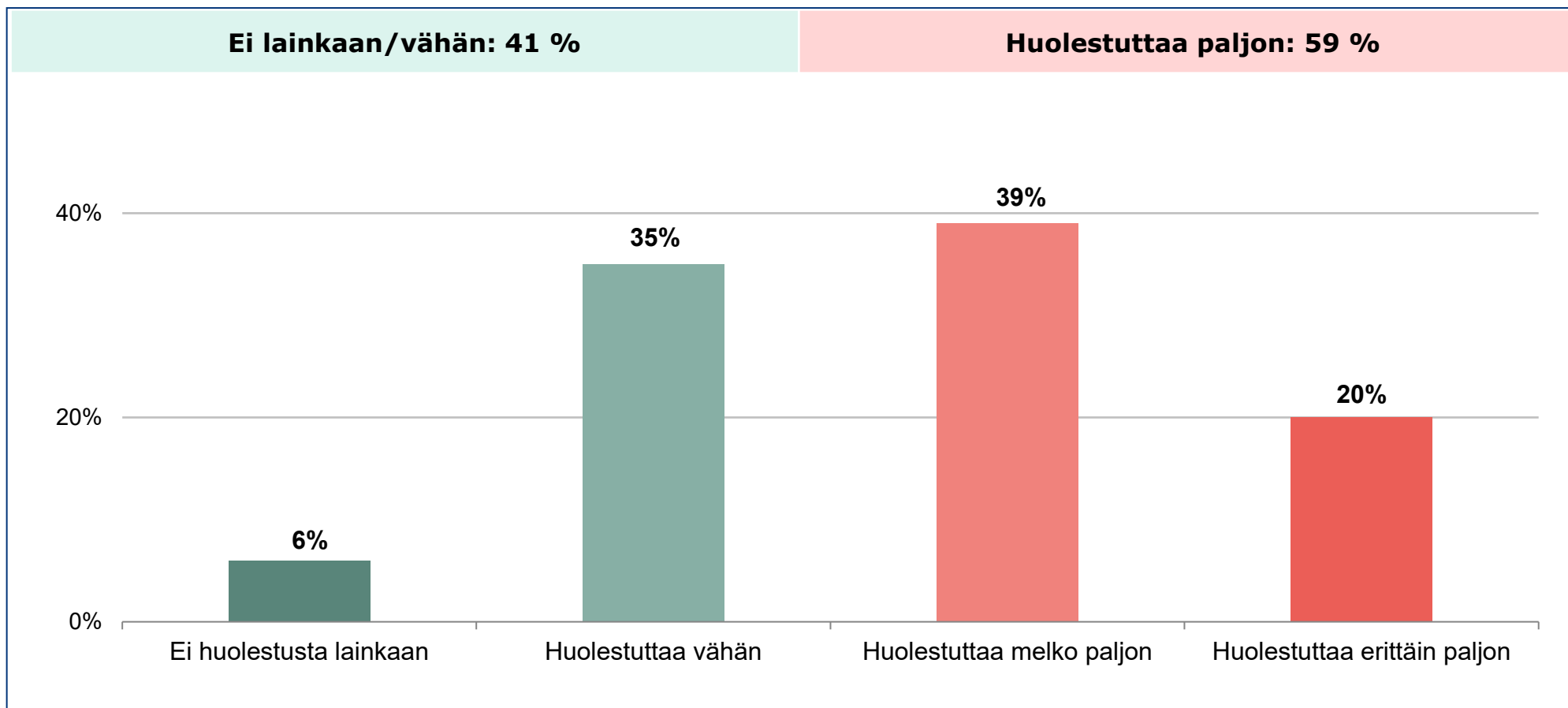
Kuinka paljon kansalaisiin kohdistuvilla digihuijauksilla on ollut vaikutusta? Asteikolla 1-4, jossa 1=erittäin vähän ja 4=erittäin paljon

Suomalaisen yhteiskunnan varautuminen digihuijausten estämiseen ja torjumiseen



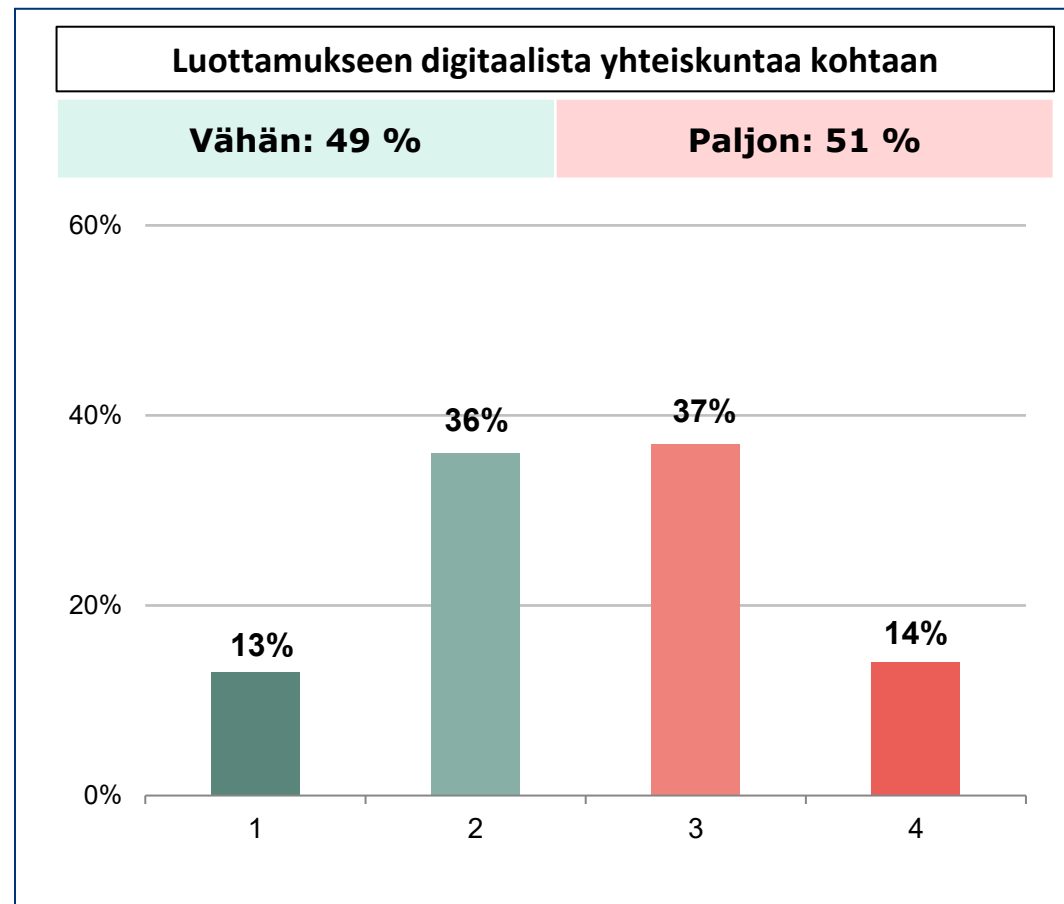
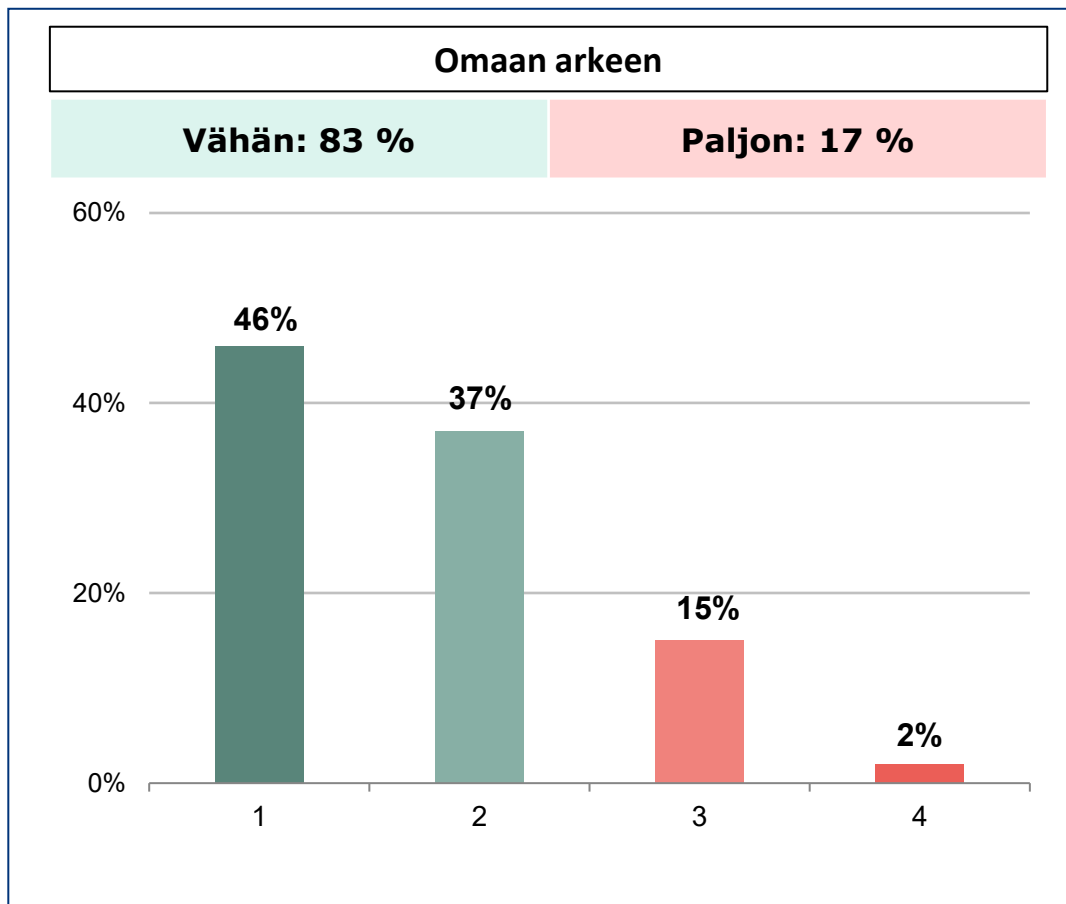
Miten suomalainen yhteiskunta on mielestäsi varautunut digihuijausten estämiseen ja torjumiseen? Asteikolla 1-4, jossa 1=erittäin huonosti ja 4=erittäin hyvin

Huoli yhteiskuntaan kohdistuvista kyberhyökkäyksistä



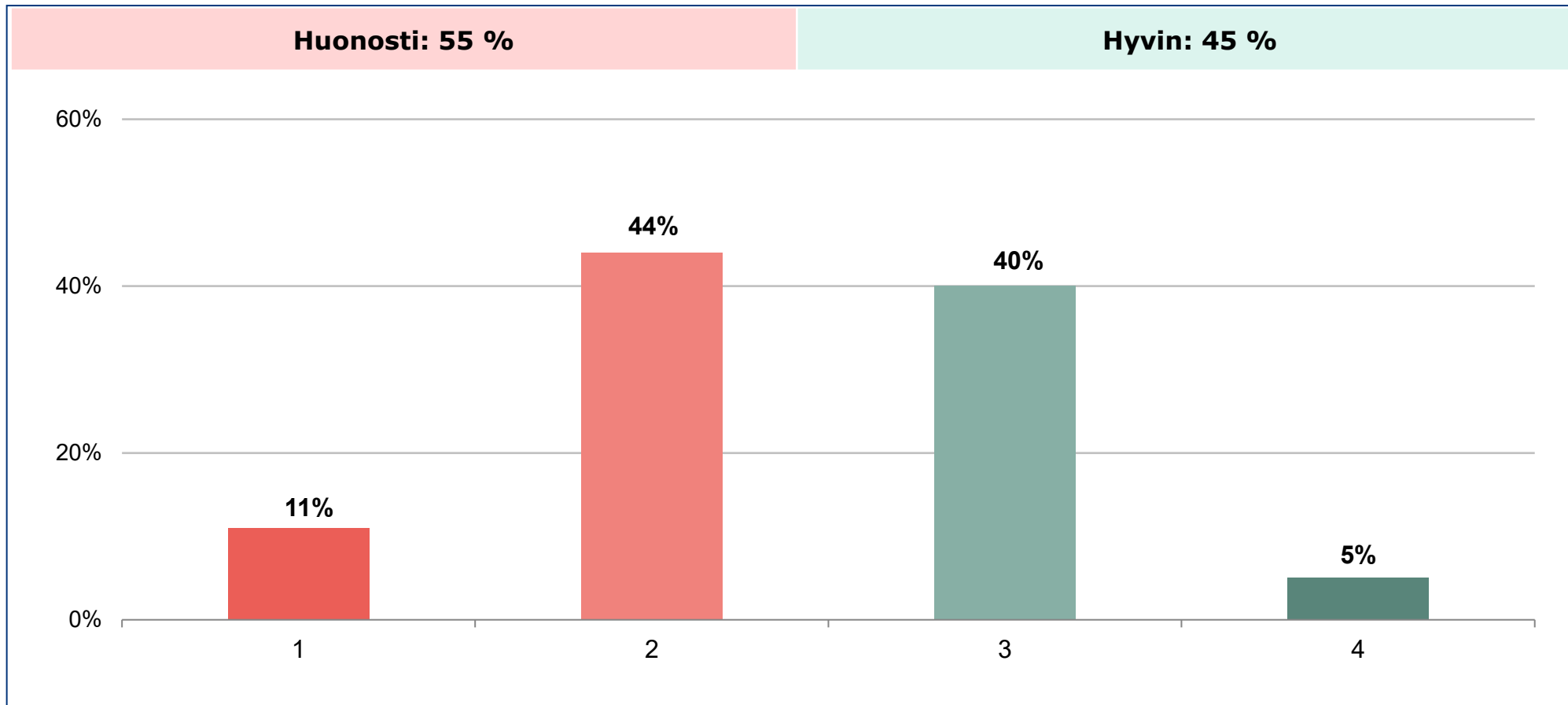
Mitä mieltä olet suomalaisen yhteiskuntaan kohdistuvista kyberhyökkäyksistä?

Yhteiskuntaan kohdistuvien kyberhyökkäyksien vaikutus



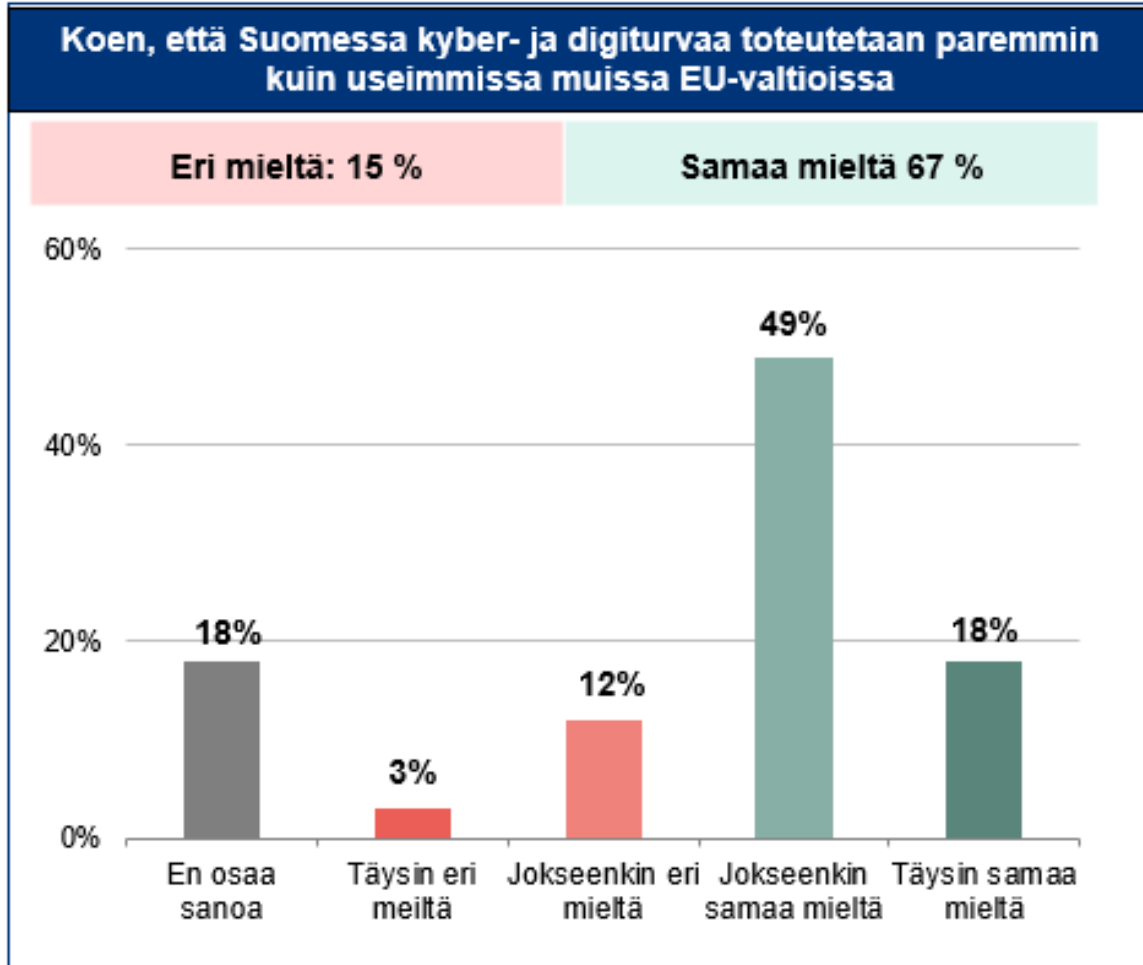
Kuinka paljon yhteiskuntaan kohdistuvilla kyberhyökkäyksillä on ollut vaikutusta? Asteikolla 1-4, jossa 1=erittäin vähän ja 4=erittäin paljon

Suomalaisen yhteiskunnan varautuminen kyberhyökkäyksien estämiseen ja torjumiseen



Miten suomalainen yhteiskunta on mielestäsi varautunut digihuijausten estämiseen ja torjumiseen? Asteikolla 1-4, jossa 1=erittäin huonosti ja 4=erittäin hyvin

Miten Suomi koetaan osana EU-aluetta?



- ▶ Suomea pidetään varautumisen mallimaana, verkkorikollisuus on ollut Suomessa kasvussa, mutta mielestäni vähemmän kuin muissa EU-valtioissa saati Euroopan ulkopuolella.

▶ Meidän täytyy jatkaa

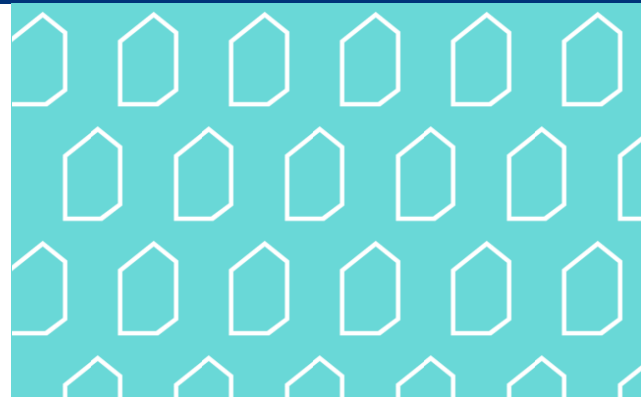
- ▶ Aktiivista kansalaisten ja henkilöstön tiedottamista uhkista
- ▶ Teknisten suojaratkaisujen kehittämistä, esimerkiksi tekoälypalveluiden käytön laajentamista tietoturvallisuuden kehittämisessä

Yhteenveto

Digihuijaukset ja kyberhyökkäykset eivät vaikuta niin paljon arkeen, mutta ne vaikuttavat luottamukseen digitaaliseen yhteiskuntaan



**DIGI- JA
VÄESTÖTIETO-
VIRASTO**



Tutkimuksen tausta ja toteutus

- ▶ Digiturvabarometritutkimuksen tavoitteena on selvittää digitaalisen turvallisuuden nykytilaa Suomessa kartoittamalla suomalaisten digiturvaosaamista ja -asenteita.
- ▶ Digi- ja väestötietoviraston aiemmin toteuttama Digiturvabarometri uudistettiin vuonna 2022. Vuonna 2023 toteutettiin kaksi seurantatutkimusta, ensimmäinen keväällä ja toinen syksyllä.
- ▶ Sen jälkeen tutkimus on toteutettu kerran vuodessa, elokuussa 2024 ja nyt elokuussa 2025.
- ▶ Tutkimuksen toteutti Digi- ja väestötietoviraston toimeksiannosta strateginen tutkimustoimisto Vastakaiku Oy. Vastakaiku on viestintätoimisto Kaiun sisaryritys.
- ▶ Tutkimuksen tiedonkeruu toteutettiin Bilendi Oy:n ylläpitämässä M3 Panelissa heinä-elokuussa. Kohderyhmänä olivat täysi-ikäiset suomalaiset. Tutkimukseen vastasi 1250 vastaajaa ja painotettuna se on valtakunnallisesti edustava otos sukupuolen, iän ja asuinalueen mukaan. Tuloksista voidaan yleistää se, miten täysi-ikäiset suomalaiset kokevat digiturvallisuuden tällä hetkellä Suomessa. Tutkimuksen virhemarginaali on 95 % luotettavuudella +/- 3,0 %.

Ihmisen rooli kyberturvallisuudessa

2.12.2025, Marianne Lindroth, Aalto-yliopisto, Cyber Citizen -hanke

Cyber Citizen hankkeen lähestymistapa

Pohjautuu tutkimukselle

Hanke pohjaa vahvasti tutkimukseen siitä, miten kyberturvataitoja parhaiten kehitetään.

Erilaisia oppimistapoja tukien

Pelit ja muut vaihtoehtoiset oppimistavat auttavat saavuttamaan laajan joukon yksilöitä

Yhteistyössä eurooppalaisten kybertoimijoiden kanssa

Työssä on hyödynnetty laajasti eurooppalaisten kybertoimijoiden osaamista.

Hankkeen kesto: 2022–

Rahoitus: Viiden miljoonan euron rahoitus EU:n elpymisvälineestä kolmen vuoden jaksolle, 2025 alkaen kansallinen rahoitus

Tilaaaja: Liikenne- ja viestintäministeriö

Toteuttaja: Aalto-yliopisto

Projektipäällikkö: Marianne Lindroth

Vastuullinen tutkija: Yki Kortensniemi

Vastaava professori: Petri Mähönen



Ihmisen rooli kyberturvallisuudessa

- Ihminen on keskeinen tekijä lähes kaikissa vakavissa kyberhyökkäyksissä.
- Kyberturvallisuus on uusi kansalaistaito: arjen valinnat vaikuttavat koko yhteiskunnan resilienssiin.
- Oppimista motivoi oma arki, työelämä ja perheen suojeleminen, ei tekninen terminologia.
- Työpaikat ja oppilaitokset ovat Euroopan tärkein kyberkoulutusverkosto.
- Yleiset ongelmat liittyvät kalasteluun, kuormitukseen, eriarvoisuuteen ja epäselviin ohjeisiin.
- Käyttäytymisen muuttaminen on vaikeaa, mutta pienillä toimilla voidaan saada suuri vaikutus.

Miksi ja miten ihmiset oppivat?

► Motivaatio

- Suojataan oma talous, identiteetti ja perhe.
- Työelämä edellyttää perustaitoja.
- Hyökkäykset kohdistuvat yksilöihin, eivät vain organisaatioihin.
- Arjen sujuvuus ja hallinnan tunne kasvaa.

► Miten ihmiset oppivat?

- Ei yhtä tapaa → visuaalisesti, kokemuksellisesti, toistamalla, tunteiden kautta.
- Harjoittelu voittaa teorian (pelit, simulaatiot, skenaariot).
- Käyttäytyminen muuttuu toiston ja arkeen sidottujen esimerkkien avulla.
- Tunteet (epävarmuus, huoli, onnistuminen) ankkuroivat opit.

Työpaikat ja oppilaitokset Euroopan tärkeimpiä kyberkouluttajia

- Valtaosa ihmisten kyberturvataidoista opitaan työpaikoilla ja oppilaitoksissa.
- Tavoittavuus paras siellä, missä ihmiset jo ovat (esim. koulu, työpaikka, kunta, kirjasto, järjestö).
- Koulutus leviää perheisiin ja lähipiiriin.



Keskeiset haasteet

- Tietojenkalastelu ja sosiaalinen manipulointi yleisimpiä ihmisiin kohdistuvia uhkia.
- Salasanojen heikkous ja sekavat ohjeet.
- Digitaalinen eriarvoisuus.
- Koulutuksen pirstaleisuus: materiaalia on, mutta se ei ole kohdennettua.
- Kognitiivinen kuorma ja ihmisen rajallinen muisti.



Miksi käyttäytymisen muuttaminen on vaikeaa?

- Aivot suosivat nopeita ratkaisuja → klikataan kiireessä.
- Päätösväsymys ja kuormitus heikentävät tarkkaavaisuutta.
- Tunteet ohjaavat päätöksiä enemmän kuin logiikka.
- Ohjeet vanhenevat nopeasti muuttuvan uhkakuvan vuoksi.
- Turvallisuuden ja helppokäyttöisyyden ristiriita koetaan päivittäin.
- Muutos vaatii kokemusta, toistoa ja tukea, ei pelkkää informaatiota.



Mihin keskittyä vaikuttavuuden näkökulmasta?

- Tietojenkalastelun tunnistaminen
- Salasanakäytännöt
- Päivitysten automatisointi ja turvalliset oletusasetukset → vähentävät virheitä
- Tunnetriggereiden tunnistaminen (kiire, pelko, auktoriteetti, uteliaisuus)
- Erityisryhmien tukeminen → resilienssi nousee koko yhteiskunnassa
- **Kriittinen ajattelu**



Lähteet

- Aalto-yliopisto (Limnell et al., 2023; Lindroth et al., 2024): Kyberkansalaistaidot, EU-laajuiset oppimismallit ja tutkimus 27 maasta.
- EuRepoC (European Repository of Cyber Incidents): Analyysi eurooppalaisista kyberhyökkäyksistä ja niiden trendeistä.
- MITRE CVE: Teknisten haavoittuvuuksien globaali luokittelu (taustakonteksti käyttäytymisen ja teknisten riskien suhteelle).
- Hadlington, L. (2017): Inhimilliset tekijät, impulsiivisuus ja riskikäyttäytyminen kyberturvallisuudessa.
- Kävrestad, Nohlberg & Varga (2023): Katsaus tehokkaihin koulutusmenetelmiin (pelillisuus, simulaatiot, skenaariot).
- Elmali et al. (2020); Martzoukou et al. (2020, 2021): Oppiminen, opettajien rooli ja digitaaliset taidot.
- Gratian et al. (2018): Persoonallisuus, stressi ja digitaalinen käyttäytyminen.
- Sheng et al. (2010): Kalastelu-alttius ja käyttäjäryhmien erot.
- Shropshire et al. (2015): Henkilökohtaiset tekijät ja tietoturvakäyttäytyminen.
- Dhillon & Moores (2001): Ihmisen ja järjestelmän välinen jännite tietoturvassa.
- Furnell et al. (2006): Haasteet kyberturvallisuustietoisuuden rakentamisessa.

A!

—

Kiitos
aalto.f
i

marianne.lindroth@aal
to.fi

Kiitos!