



DIGI- JA
VÄESTÖTIETO-
VIRASTO

Digiturvabarometri 2025

Raportti tuloksista

6.10.2025



6.10.2025

Sisällysluettelo

1	Johdanto	3
2	Digiturvabarometrin johtopäätökset ja yhteenveto	4
2.1	Yhteenveto tuloksista	4
2.2	Kolme avainnostoa Digiturvabarometrasta 2025.....	8
3	Yksityiskohtaiset tulokset	10
3.1	Digitaalisten palveluiden käyttö ja sovellusten merkitys itselle	10
3.1.1	Digipalveluiden ja -sovellusten merkitys arjessa - kuinka tärkeäksi koet erilaiset digipalvelut ja -sovellukset omassa arjessasi?	10
3.1.2	Digipalveluiden ja -sovellusten käytön laajuus - minkä verran käytät erilaisia digipalveluita ja -sovelluksia tyypillisesti päivän aikana?	11
3.1.3	Tekoälypalveluiden käytön laajuus - kuinka paljon käytät itse tekoälypalveluita (esim. OpenAI ChatGPT, Microsoft CoPilot, Google Gemini)?.....	12
3.1.4	Tekoälypalveluiden käytön laajuus: ikävertailu Kuinka paljon käytät itse tekoälypalveluita (esim. OpenAI ChatGPT, Microsoft CoPilot, Google Gemini)?	13
3.1.5	Älylaitteiden parissa käytetty aika - uusi Kuinka monta tuntia arvioit keskimäärin käyttäväsi aikaa älylaitteiden parissa viikossa (ns. "ruutuaika")?	14
3.1.6	Onko viikoittainen ruutuaikasi mielestäsi liikaa? Uusi.....	16
3.1.7	Onko viikoittainen ruutuaikasi mielestäsi liikaa – ikäryhmittäin? Uusi	17
3.2	Oma osaaminen ja siihen tarvittava tuki	18
3.2.1	<i>Kuinka hyvin osaat omasta mielestäsi käyttää turvallisesti digitaalisia palveluita (esim. verkkopankki, viranomaispalvelut, suoratoistopalvelut) ja digilaitteita (esim. tietokone, älypuhelin, tabletti, älytelevisio, älykello/aktiivisuusranneke)?</i>	<i>18</i>
3.2.2	Tiedon ja koulutuksen saatavuus Minkä verran olet saanut tietoa ja/tai koulutusta (esim. työpaikalla, oppilaitoksessa, mediasta) seuraavista tilanteista ja niissä toimimisesta?	20
3.2.3	Tietämys digiturvasta ja osaaminen toimia turvallisesti - Uusi	21
3.3	Yleinen luottamus digitaaliseen toimintaympäristöön	23
3.3.1	Onko luottamus digitaaliseen turvallisuuteen muuttunut viimeisen vuoden aikana? ...	23
3.3.2	Turvallisuuden tunne digitaalisessa toimintaympäristössä – ikävertailu Miten turvalliseksi tunnet päivittäisen toiminnan digitaalisessa toimintaympäristössä?	25
3.3.3	Turvallisuuden tunne digitaalisessa toimintaympäristössä töissä	26
3.3.4	Digiturvallisuuteen liittyvät huolestuttavat asiat Miten paljon seuraavat asiat huolestuttavat sinua?	27
3.4	Luottamus tietojen käsittelyyn ja sisältöihin.....	29
3.4.1	Luottamus siihen, että omia tietoja käsitellään turvallisesti Luotatko siihen, että seuraavat toimijat käsittelevät turvallisesti henkilötietojasi ja muita tärkeitä tietojasi?	29
3.4.2	Luottamus tahojen/palvelujen tuottamaan sisältöön Kuinka hyvin luotat seuraavien tahojen/palveluiden tuottamaan sisältöön?	31



6.10.2025

3.5	Digiturvallisuus arjessa.....	32
3.5.1	Digiturvallisuuteen liittyvien uhkien toteutuminen itselle Mitä seuraavista on tapahtunut sinulle viimeisimmän vuoden aikana?	32
3.5.2	Rikoksen uhriksi joutuminen digimaailmassa/internetissä ja rikosilmoituksen tekeminen Oletko joutunut digimaailmassa/internetissä digihuijauksen, petoksen tai rikoksen uhriksi? ...	34
3.5.3	Rikoksen uhriksi joutuminen digimaailmassa/internetissä ja rikosilmoituksen tekeminen Teitkö rikosilmoituksen tästä digihuijauksesta, petoksesta tai rikoksesta?	35
3.5.4	Maksukorttien ja tilien turvallisuuden parantaminen Oletko itse parantanut maksukorttiesi ja tiliesi käyttöön liittyvää turvallisuutta tai varmistanut näitä asioita pankiltasi? Uusi	36
3.5.5	Käytän jokaisessa eri verkkopalveluissa eri salasanaa - uusi	37
3.5.6	Olen klikannut linkkiä, joka osoittautui huijausyritykseksi - uusi Olen viimeisen vuoden aikana klikannut vähintään kerran linkin tai avannut liitteen, joka on osoittautunut huijausyritykseksi - uusi	38
3.6	Kyberhyökkäykset, digihuijaukset ja suhtautuminen digiturvaan.....	39
3.6.1	Huoli suomalaiseen yhteiskuntaan kohdistuvista kyberhyökkäyksistä ja digihuijauksista - uusi	39
3.6.2	Kyberhyökkäyksien ja digihuijauksien vaikutus Kuinka paljon kyberhyökkäyksillä ja digihuijauksilla on ollut vaikutusta? Uusi	40
3.6.3	Yhteiskunnan varautuminen digiturvaan Miten suomalainen yhteiskunta on mielestäsi varautunut kyberhyökkäysten ja digihuijausten estämiseen ja torjumiseen? Uusi Koen, että Suomessa kyber- ja digiturvaa toteutetaan paremmin kuin useimmissa muissa EU-valtioissa - uusi	41
3.6.4	Olen huolissani henkilötietojeni väärinkäytöstä verkossa - uusi	42
3.6.5	Suhtautuminen digiturvaan - uusi.....	43
3.6.6	Suhtautuminen tekoälyyn - uusi.....	44
3.6.7	Yhteenvedo tekoälystä: vertailu tekoälyn käytön mukaan - uusi.....	45



6.10.2025

Digiturvabarometri 2025

1 Johdanto

Digi- ja väestötietoviraston Digiturvabarometri-tutkimuksella selvitetään kansalaisten kyber- ja digiturvaosaamista sekä asenteita Suomessa. Tavoitteena on kartoittaa, miten täysi-ikäiset suomalaiset kokevat digiturvallisuuden nykytilan osana omaa arkeaan.

Digiturvabarometriä on toteutettu vuodesta 2020 alkaen, ja sen konsepti uudistettiin syksyllä 2022. Tuolloin tutkimuksen toteutus annettiin toimeksiantona tutkimustoimisto Vastakaiku Oy:lle, joka kerää tarvittavat tiedot Bilendi Oy:n ylläpitämän M3-paneelin avulla.

Tämä raportti käsittelee Digiturvabarometrin tuloksia vuosilta 2022–2025. Tutkimuksen kohderyhmänä ovat täysi-ikäiset suomalaiset. Kyselyyn vastasi 1250 henkilöä heinä–elokuussa 2025. Tulokset on painotettu siten, että ne muodostavat valtakunnallisesti edustavan otoksen sukupuolen, iän ja asuinalueen mukaan. Vertailutulokset vuosilta 2024, 2023 ja 2022 viittaavat edellisten Digiturvabarometriä aineistoihin. Vuoden 2025 tutkimuksen virhemarginaali on +/- 3,0 % (95 % luotettavuudella).

Tulosten perusteella voidaan tehdä yleistyksiä muun muassa siitä, miten täysi-ikäiset suomalaiset kokevat digitaalisen maailman merkityksen ja kuinka aktiivisesti he sitä hyödyntävät. Niistä selvisi myös, millaisia näkemyksiä heillä on tekoälyn käytöstä ja siihen liittyvästä luottamuksesta, sekä millaisena he näkevät digiturvallisuuden tilanteen Suomessa. Tutkimuksessa pureuduttiin myös siihen, millaista osaamista suomalaisilla on, millainen heidän turvallisuuden tunteensa on arjessa ja työpaikalla, sekä millaisia uhkia he ovat tunnistaneet. Lisäksi selvitettiin, millainen luottamus suomalaisilla on eri toimijoihin ja digipalveluihin henkilötietojen sekä muiden tärkeiden tietojen käsittelyssä. Raportin loppupuolella on mukana myös uusia kysymyksiä, jotka koskevat muun muassa suhtautumista kyberhyökkäyksiin, digihuijauksiin ja digiturvaan yleisemmin. Vuonna 2025 mukaan otettujen uusien kysymysten otsikon perässä lukee sana **uusi**. Tämän raportin tuottamisessa on hyödynnetty myös tekoälypalveluita.

Digi- ja väestötietovirasto hyödyntää Digiturvabarometrin havaintoja Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) toiminnassa sekä omissa hankkeissaan. Lisätietoa VAHTI-toiminnasta löytyy osoitteesta dvv.fi/vahti.

Lisätietoja

Kimmo Rousku

VAHTI-pääsihteeri, johtava erityisasiantuntija
etunimi.sukunimi@dvv.fi tai digiturva@dvv.fi



6.10.2025

2 Digiturvabarometrin johtopäätökset ja yhteenveto

Digitaaliset palvelut ovat vakiintuneet osaksi kaikkien ikäryhmien arkea. Käyttö on runsasta, ja omaa osaamista pidetään hyvänä, mutta osaamisen painopiste on edelleen perustaidoissa.

Tekoälyn turvallinen hyödyntäminen sekä kyvykkyys reagoida huijausyrityksiin kaipaavat vahvistamista. Luottamus digitaaliseen turvallisuuteen ja eri toimijoihin on pienessä laskussa. Viranomaiset ja finanssiala säilyttävät korkeimman luottamuksen. Sen sijaan kaupallisten palveluiden, sosiaalisen median ja tekoälypalveluiden turvallisuuteen suhtaudutaan varauksellisesti. Tämä heijastuu myös turvallisuuden tunteeseen, joka on lievästi heikentynyt vastaajien arjessa.

Kansalaisia huolettaa eniten tekoälypalveluiden nopea kehitys. Tekoälyn käyttö lisääntyy erityisesti nuorissa ikäryhmissä, mutta luottamus siihen ei kasva samaa tahtia. Identiteettivarkauksien ja huijausviestien pelko on hieman laantunut, mikä viittaa viranomaisten ja teleoperaattoreiden torjuntatoimien tehoon.

Uudet kysymykset paljastavat, että kansalaiset kokevat kyberhyökkäykset ja digihuijaukset merkittäväksi uhaksi paitsi omassa arjessaan, myös laajemmin yhteiskunnallisen luottamuksen näkökulmasta. Enemmistö arvioi Suomen pärjäävän muihin EU-maihin verrattuna hyvin, mutta kansalaisten arviot varautumisesta jakautuivat lähes tasan myönteisten ja kielteisten välillä.

Suurin osa suomalaisista on valmis näkemään vaivaa oman turvallisuutensa eteen ja pitää digitaalista turvallisuutta olennaisena osana arkea. Salasanojen kierrättäminen ja epärointi huijaustilanteissa osoittavat kuitenkin, että yksilön vastuun rinnalla tarvitaan yhä vahvempia yhteiskunnallisia ja palveluntarjoajien toimia turvallisuuden varmistamiseksi.

2.1 Yhteenveto tuloksista

Kansalaiset kokevat digitaaliset palvelut tärkeiksi ja käyttävät niitä aktiivisesti myös vanhemmissa ikäryhmissä. 54 % 75–99-vuotiaista pitää digipalveluja tärkeinä ja 45 % käyttää niitä päivittäin paljon. Nuorimmassa, 18–24-vuotiaiden ikäryhmässä vastaavat luvut ovat 86 % ja 91 %.

Luottamus tekoälyn kykyyn käsitellä henkilötietoja ei ole kasvanut, ja tekoälyn nopea kehitys koetaan merkittäväksi huolenaiheeksi. Tekoälypalveluiden käyttö on lisääntynyt huomattavasti vuoden aikana. Kuukausittain tai useammin palveluita käyttää nyt 31 % vastaajista, kun vuosi sitten ensimmäistä kertaa kysyttäessä osuus oli 20 %. Nuorimmista 35 % ja vanhimmasta ikäryhmästä 11 % käyttää tekoälyä vähintään viikoittain. Lähes päivittäin tekoälyä käyttävien osuus on noussut neljästä kymmeneen prosenttiin.

Uutena kysymyksenä selvitettiin ruutuaikaa. Kaikkien vastaajien keskiarvona oli 22 tuntia ruutuaikaa viikossa, eli runsaat kolme tuntia päivässä. Kysymyksessä ei eroteltu työn, opiskelun ja vapaa-ajan osuutta. Jopa 46 % vastaajista piti ruutuaikaansa liian korkeana ja 7 % aivan liian korkeana, jopa huolestuttavana.



6.10.2025

Nuorimmassa ikäryhmässä (18–24-vuotiaat) 71 % oli huolissaan omasta ruutuajastaan.

91 % vastaajista katsoi osaavansa käyttää digipalveluita ja -laitteita turvallisesti. Tulos on pysynyt samana jo kolme vuotta.

Tiedon ja koulutuksen osalta on tapahtunut nousua. Tutkimuksessa kysyttiin 14 eri osa-alueesta. 60 % vastaajista kertoi saavansa niistä tietoa melko paljon tai paljon. Eniten tietoa oli saatavilla vahvasta tunnistautumisesta (74 %), vähiten tekoälyn turvallisesta hyödyntämisestä (36 %).

Toisena uutena kysymyksenä selvitettiin reagointia neljään erilaiseen digimaailman tilanteeseen. Esimerkiksi jos vastaaja saa puhelun viranomaiselta tai pankista, jossa pyydetään verkkopankkitunnuksia tai kirjautumista palveluun, 75 % ei reagoi tähän oikeaoppisesti lainkaan, kun taas 20 % reagoi ja 5 % ei osaa sanoa. Tämä osoittaa, että viestintä ja koulutus eivät ole vielä tavoittaneet kaikkia kansalaisia. Lisäksi 36 % ei tiedä, mitä tehdä, jos epäilee joutuneensa verkkohuijauksen kohteeksi. 38 % ei osaa tarkistaa verkkosivuston tai verkkokaupan turvallisuutta ennen ostoksia. Tulosten mukaan vain 60 % osaa suojata henkilökohtaiset tietonsa verkossa. Nämä luvut osoittavat, että vaikka vastaajat mielestään osaavat käyttää palveluita turvallisesti, tämä ei toteudu käytännössä.

Luottamus digitaaliseen turvallisuuteen on laskenut viime vuodesta kaksi prosenttiyksikköä. 38 % kokee luottamuksensa heikentyneen. 11 % kertoo luottamuksen vahvistuneen, mikä on vain yhden prosenttiyksikön parannus viime vuoteen. Suurimmat syyt luottamuksen heikentymiseen ovat lisääntynyt verkkorikollisuus ja tekoälyyn liittyvät huolet. Luottamuksen vahvistumista on kasvattanut keskustelu aiheesta, oman osaamisen kehittyminen sekä luottamusta parantavat toimenpiteet.

Tämä heijastuu myös turvallisuuden tunteeseen digimaailmassa. 82 % kokee olonsa melko (68 %) tai erittäin (14 %) turvalliseksi, mikä on kolme prosenttiyksikköä vähemmän kuin vuosi sitten. Työpaikalla turvallisuuden tunne on 88 %, jossa on nousua kaksi prosenttiyksikköä. Lisäksi työssä turvallisuuden tunteen jakautuminen on tasaisempaa: 44 % kokee olonsa erittäin ja 44 % melko turvalliseksi.

Vuonna 2025 eniten kansalaisia huolestutti tekoälypalveluiden nopea kehittyminen. Huolestuneiden osuus on noussut 59 prosentista 63 prosenttiin. Kaikkien huolestuttavien aiheiden keskiarvo on kuitenkin laskenut 46 prosentista 44 prosenttiin. Suurin lasku koskee identiteettivarkauksia. Niiden uhriksi joutumista pelkää 51 %, mikä on viisi prosenttiyksikköä vähemmän kuin viime vuonna.

Eräs barometrin tärkeimmistä kysymyksistä liittyi luottamukseen siitä, että eri toimijat ja palvelut käsittelevät vastaajan tietoja turvallisesti.

Toimijat	2025	2024	2023
Viranomaiset	87 %	89 %	87 %
Finanssialan palvelut	87%	88 %	92 %



6.10.2025

Työntaja	82 %	85 %	82 %
Oppilaitokset	71 %	73 %	-
Yhdistykset ja muut ei kaupalliset toimijat	53 %	54 %	52 %
Kaupalliset toimijat ja yritykset	45 %	46 %	41 %

Palvelut

Kotimaiset verkkokaupat	75 %	73 %	-
Sähköpostipalvelut	54 %	56 %	54 %
Suoratoistopalvelut	44 %	45 %	41 %
Pikaviestimet	43 %	46 %	41 %
Sosiaalisen median palvelut	26 %	28 %	26 %
Nettipelit	23 %	25 %	26 %
Ulkomaiset verkkokaupat	23 %	24 %	-
Muut	22 %	24 %	22 %
Tekoälypalvelut	20 %	22 %	18 %

Kotimaisia verkkokauppoja lukuun ottamatta kaikkien muiden osalta on tapahtunut yhden-kolmen prosenttiyksikön lasku. Tietomurtojen määrä, muut mahdolliset väärinkäytökset sekä näiden toimijoiden nimissä lähetetyt (kymmenet) miljoonat digihuijausviestit voivat vaikuttaa tähän pieneen laskuun. Luottamus viranomaisiin, finanssialan palveluntarjoajiin ja omaan työnantajaan on edelleen korkea.

Luottamus kysyttyjen toimijoiden tai palveluiden tuottamaan sisältöön on noussut joiltain osin, mutta myös laskenut. Keskiarvo on pysynyt samana (54 %).

Toimija tai palvelut	2025	2024	2023
Viranomaiset	88 %	89 %	88 %
Tunnetut kotimaiset uutismediat	69 %	69 %	67 %
Yritykset	65 %	64 %	61 %
Tunnetut ulkomaiset uutismediat	55 %	57 %	54 %
Yhdistykset tai muut ei kaupalliset toimijat	54 %	55 %	52 %
Sosiaalisen median palvelut	25 %	24 %	20 %
Tekoälypalvelut	21 %	19 %	15 %

Luottamus tekoälypalveluihin on noussut kahdessa vuodessa 15 prosentista 21 prosenttiin, eli kaikkiaan kuusi prosenttiyksikköä. Toivomme tämän kehityksen jatkuvan myös tulevaisuudessa.

Erilaisista digimaailman uhkista kysyttäessä keskiarvo (31 %) on laskenut kahdella prosenttiyksiköllä viime vuoden arvosta (33 %). Kehityksen suunta on positiivinen.



6.10.2025

	2025	2024
Olen saanut huijaus- tai kalasteluviestejä sähköpostiini	78 %	84 %
Olen saanut huijaus- tai kalasteluviestejä tekstiviestinä (SMS)	62 %	72 %
Olen saanut huijaus- tai kalastelupuhelinsoittoja	54 %	61 %

Yllä olevien, vastaajien eniten havainnoimien ilmiöiden osalta on tapahtunut merkittävää laskua. Tähän on vaikuttanut viranomaisten ja esimerkiksi teleoperaattoreiden yhteistyö verkkorikollisuuden vähentämiseksi.

	2025	2024
Olen menettänyt rahaa tekemällä ostoksen valeverkkokaupasta	10 %	9 %
Olen menettänyt rahaa kiristyksen tai digihuijauksen takia	7 %	8 %
Olen joutunut identiteettivarkauden kohteeksi	6 %	6 %

Vähiten havainnoitujen ilmiöiden määrässä ei ole tapahtunut suurta muutosta.

Vuosien 2023–2025 aikana rikoksen uhriksi digimaailmassa tai internetissä joutuneiden määrä on pysynyt lähes samana. Se oli 28 % kahtena edellisellä vuotena ja 26 % vuonna 2023. Rikosilmoituksen tehneiden määrä on laskenut kolme prosenttiyksikköä viime vuodesta, 51 prosentista 48 prosenttiin.

28 % täysi-ikäisistä suomalaisista on joutunut digihuijauksen, petoksen tai muun rikoksen uhriksi verkossa. Heistä 52 % on tehnyt rikosilmoituksen, joista 40 % viimeisen vuoden aikana. Käytännössä 6 % täysi-ikäisistä suomalaisista on tehnyt vuoden sisällä rikosilmoituksen digirikoksesta tai -petoksesta.

Uutena kysymyksenä selvitettiin maksukorttien ja tilien turvallisuuden parantamista: oletko itse parantanut korttiesi ja tiliesi turvallisuutta tai varmistanut asiaa pankiltasi? On ilahduttavaa, että 42 % on tehnyt parannuksia viimeisen vuoden aikana ja 27 % yli vuosi sitten. 41 % ei ole tehnyt parannuksia lainkaan. Finanssialan toimijoiden olisi tärkeää aktivoida asiakkaitaan hyödyntämään nykyisiä ja uusia tietoturvaominaisuuksia. Esimerkiksi EU:n lokakuussa 2025 voimaan astuva pikamaksuasetus varmistaa, että maksajan ilmoittama vastaanottajan nimi vastaa tilin omistajaa.

Vastaukset kysymykseen ”Käytän jokaisessa verkkopalvelussa eri salasanaa” ovat huolestuttavia. Vain 52 % vastasi kyllä, 39 % ei käytä ja 9 % ei osaa sanoa. Käytännössä lähes puolella suomalaisista on parantamisen varaa salasanakäytännöissä.

Hieman parempi tulos saatiin kysymyksestä ”Olen klikannut linkkiä, joka osoittautui huijausyritykseksi viimeisen vuoden aikana.” 21 % kertoo tunnistaneensa huijausviestin liian myöhään, 10 % ei osaa sanoa ja 69 % ei ole kohdannut tällaista tilannetta.

Kysymys ”Huoli suomalaiseen yhteiskuntaan kohdistuvista kyberhyökkäyksistä ja digihuijauksista” paljasti, että 60 % vastaajista on asiasta huolissaan (45 % melko paljon, 15 % erittäin paljon). 37 % on huolissaan vähän ja 3 % ei lainkaan. Näitä

6.10.2025

lukuja on mielenkiintoista seurata tulevina vuosina. Huolta todennäköisesti lisäävät kyberturvallisuuden kohonnut uhkataso, verkkorikollisuuden yleistyminen ja median näkyvä uutisointi.

Kolmantena uutena kysymyksenä kysyttiin kyberhyökkäysten ja digihuijausten vaikutuksesta omaan arkeen ja luottamukseen digitaaliseen yhteiskuntaan, joka koettiin pienenä. Omaan arkeen vaikutusta koki paljon (13 %) tai erittäin paljon (3 %), yhteensä 16 % vastaajista. Loput 84 % kokivat vaikutuksen vähäiseksi. Luottamukseen digitaalista yhteiskuntaa kohtaan vaikutukset olivat suuremmat. 34 % koki vaikutusta paljon ja 8 % erittäin paljon (yhteensä 42 %). Vähemmän vaikutusta koki 58 % (41 % vähän, 17 % erittäin vähän). Tämä on hyvä mittari seuraamaan uhkatason ja konkreettisten hyökkäysten vaikutuksia.

Neljäs uusi kysymys oli "Miten suomalainen yhteiskunta on varautunut kyberhyökkäysten ja digihuijausten torjumiseen?" Kysymyksen vastaukset jakautuivat tasaisesti. 51 % mielestä hyvin (5 % erittäin hyvin, 46 % hyvin) ja 49 % mielestä huonosti (42 % huonosti, 7 % erittäin huonosti). Tämä oli poikkeuksellisen paljon mielipiteitä jakava kysymys.

Viidenteen uuteen kysymykseen "Koen, että Suomessa kyber- ja digiturvaa toteutetaan paremmin kuin useimmissa muissa EU-valtioissa" vastasi myönteisesti 67 % (18 % täysin samaa mieltä, 49 % jokseenkin samaa mieltä). Eri mieltä oli 15 % (12 % jokseenkin, 3 % täysin eri mieltä). Tavallista suurempi osuus (18 %) vastaajista ei osaa sanoa.

Kuudes uusi kysymys henkilötietojen väärinkäytön pelosta verkossa osoitti, että 75 % vastaajista on tilanteesta huolissaan. 26 % oli täysin samaa mieltä ja 49 % jokseenkin samaa mieltä. 19 % oli jokseenkin eri mieltä ja 2 % täysin eri mieltä.

Viimeinen uusi kysymys koski suhtautumista digiturvaan. 89 % vastaajista oli valmiita näkemään vaivaa oman turvallisuutensa varmistamiseksi verkossa (8 % ei ole, ja 3 % ei osaa sanoa). 89 % koki digitaalisen turvallisuuden olevan olennainen osa arkea (7 % ei ole, 4 % ei osaa sanoa). Kysymyksestä "Digitaalinen turvallisuus on ensisijaisesti yksilön vastuulla" oli samaa mieltä 75 % vastaajista. Eri mieltä oli 20 % ja 5 % ei osaa sanoa.

2.2 Kolme avainnostoa Digiturvabarometrissa 2025

1. Luottamus digiin on koetuksella

Yleinen luottamus digitaaliseen turvallisuuteen on heikentynyt, ja suunta on ollut laskeva jo useamman vuoden ajan. Erityisesti tekoälyn nopea kehitys sekä lisääntyneet huijaukset ja kyberhyökkäykset huolettavat suomalaisia. Ne saavat monet epäilemään, pysykö oma osaaminen mukana uhkien tahdissa.

2. Tekoäly muuttaa arkea ja siihen suhtaudutaan varauksella



6.10.2025

Tekoälyn käyttö yleistyy vauhdilla, mutta luottamus sen turvallisuuteen on erittäin matalaa. Tämä kahtiajako osoittaa, että vaikka teknologia tarjoaa uusia mahdollisuuksia, riskit ja tietosuojaan liittyvät kysymykset painavat vaakakupissa paljon.

3. Haluamme toimia turvallisesti, mutta teoissa on parannettavaa

Motivaatio oman digiturvan parantamiseen on poikkeuksellisen korkea. Käytännön toiminna, kuten salasanojen hallinnassa, digihuijausten tunnistamisessa ja rikosilmoitusten tekemisessä, on kuitenkin yhä selviä puutteita. Kuilun umpeen kuominen vaatii paitsi yksilön ponnistuksia, myös helppokäyttöisempiä ja turvallisempia palveluita.



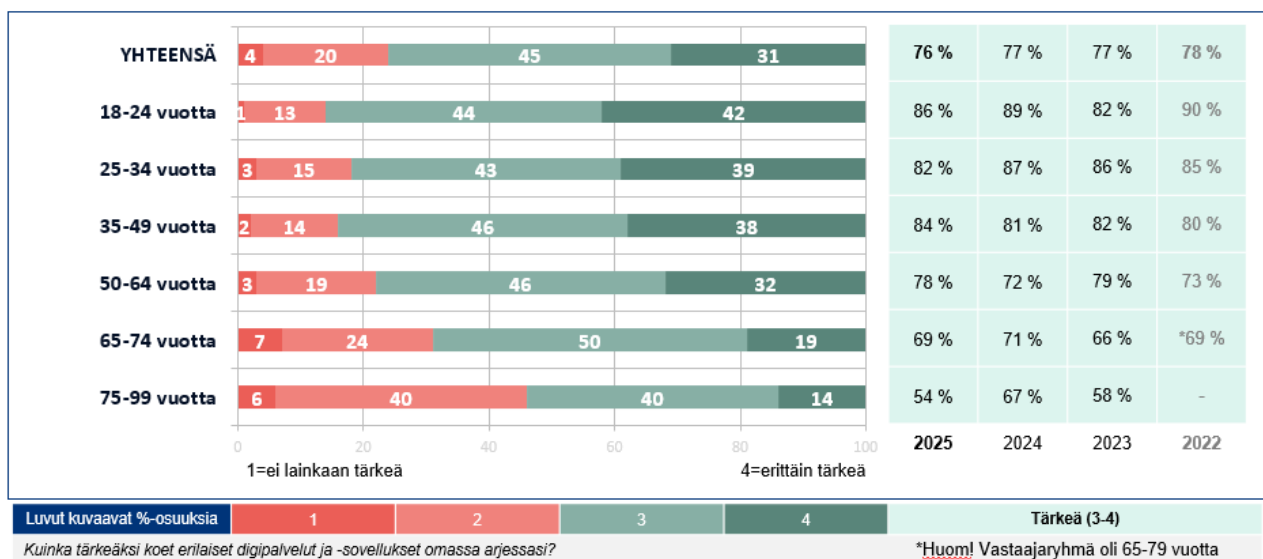
6.10.2025

3 Yksityiskohtaiset tulokset

Tässä luvussa käydään läpi Digiturvabarometrin vuoden 2025 tuloksia.

3.1 Digitaalisten palveluiden käyttö ja sovellusten merkitys itselle

3.1.1 Digipalveluiden ja -sovellusten merkitys arjessa - kuinka tärkeäksi koet erilaiset digipalvelut ja -sovellukset omassa arjessasi?



Analyysi

Kokonaiskuva on vakaa. Neljä viidestä (76 %) pitää digipalveluja vähintään melko tärkeinä, ja jakauma on pysynyt vuosittain lähes muuttumattomana. Tärkeyden kokemukseen vaikuttaa vastaajan ikä. Nuorissa ryhmissä korostui ”erittäin tärkeä” (4), erityisesti 18–24-vuotiailla (42 %). Keski-ikäisillä 3–4-arviot olivat korkeita (35–49-vuotiaat: 84 %), mutta ”erittäin tärkeä” laski asteittain vanhemmissa ikäryhmissä. Yli 65-vuotiailla paino siirtyi arvoon 2 (65–74-vuotiaat: 24 %; 75–99-vuotiaat: 40 %), ja 4-arvioita on selvästi vähemmän (19 % ja 14 %).

Vuositason vaihtelut ovat pieniä ja ryhmäkohtaisia. 18–34-vuotiailla 3–4-osuus notkahti vuodesta 2024, kun taas 50–64-vuotiailla nähtiin nousua (72 % → 78 %). Vanhimmassa ryhmässä vuoden 2025 tulos (54 %) on matala verrattuna vuoteen 2024 (67 %). Tämä voi kertoa otosvaihtelusta tai segmentin heterogeenisyydestä – tulkinnassa on syytä olla varovainen.

Havainnot

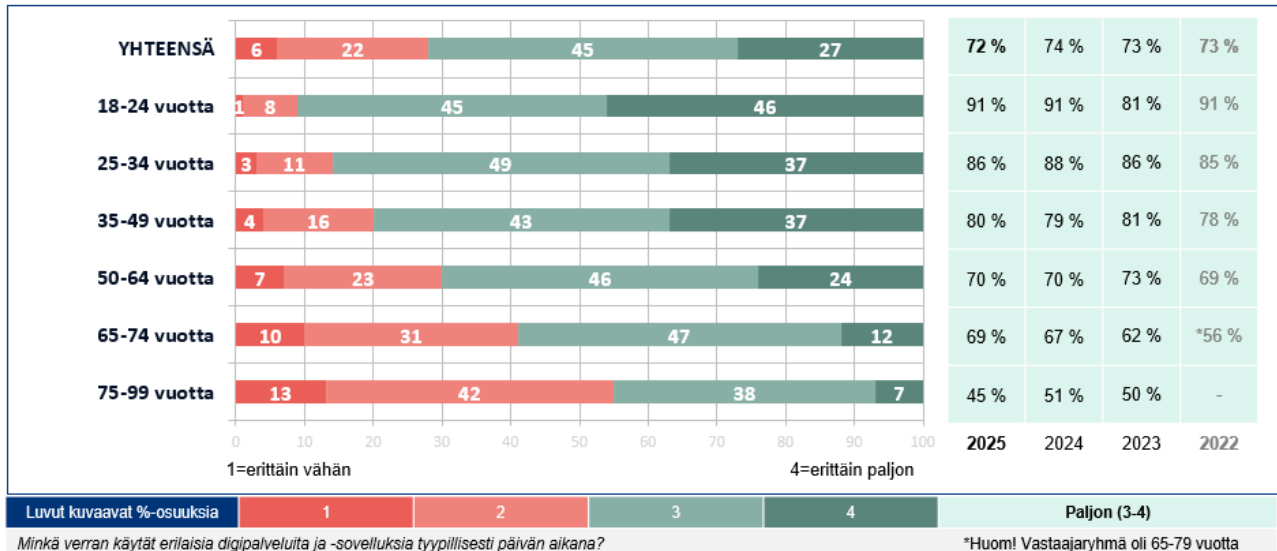
Me suomalaiset olemme todellista digikansaa ja pidämme digipalveluiden merkitystä



6.10.2025

tärkeänä. Huomionarvoista on, että 24 % eli jopa yli miljoona kansalaista ei pidä näitä tärkeinä tai ei lainkaan tärkeinä.

3.1.2 Digipalveluiden ja -sovellusten käytön laajuus - minkä verran käytät erilaisia digipalveluita ja -sovelluksia tyypillisesti päivän aikana?



Analyysi

Digipalveluiden ja -sovellusten käyttö on kautta linjan runsasta. 72 % suomalaisista käyttää digipalveluita päivittäin vähintään melko paljon (3–4). Nuorimmat käyttävät palveluita selvästi enemmän (18–24-vuotiaat: 91 %, 4-arvio 46 %). Myös 25–49-vuotiaat ylsivät 80–86 % tasolle. Vastaaajien iän kasvaessa paino siirtyy selvästi kohtuulliseen käyttöön (65–74-vuotiaat: 47 % antoi arvon 3, mutta vain 12 % arvon 4). Vanhimmissa ryhmässä korostuu vähäinen tai kohtalainen käyttö (75–99-vuotiaat: 1–2, yhteensä 55 %).

Tulos on pysynyt vuodesta toiseen kokonaisuudessaan vakaana (73–74 % → 72 %), mutta ikäryhmittäin on eroja. 25–34-vuotiaat ja 18–24-vuotiaat olivat lievästi alempana kuin vuonna 2024. 65–74-vuotiaat jatkoivat nousua (56 % → 62 % → 67 % → 69 %), mikä kertoo tottumisen ja tarpeiden kasvusta. 75–99-vuotiaiden notkahdus (51 % → 45 %) voi johtua sekä otosvaihtelusta, että käytön polarisoitumisesta.

Havainnot

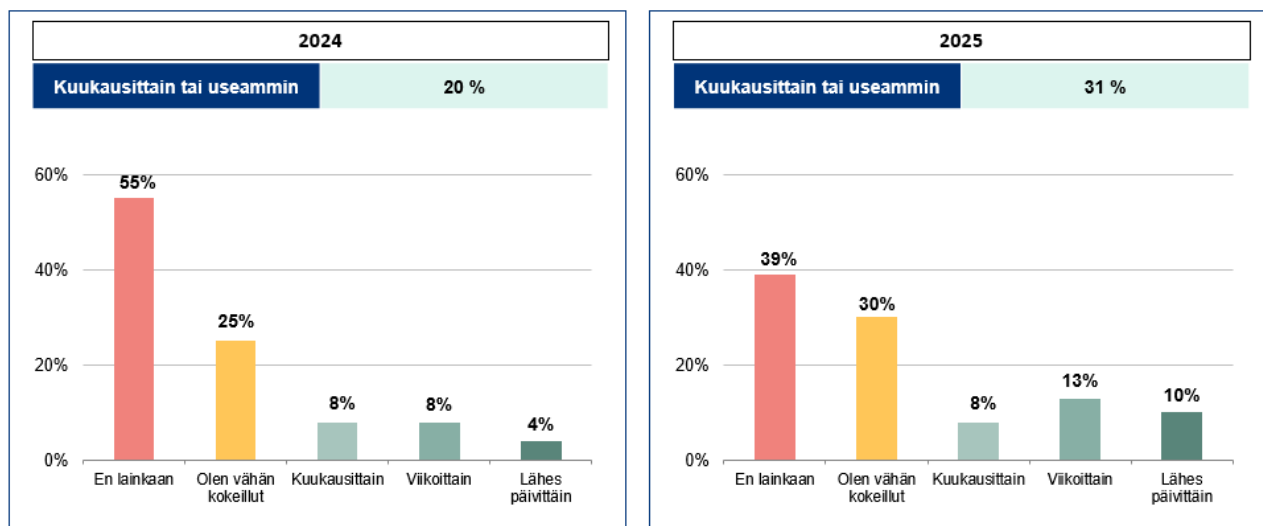
Yhdistettynä edelliseen ”Kuinka tärkeäksi koet erilaiset digipalvelut ja -sovellukset omassa arjessasi” -kaavioon tulkinta on selkeä. Nuorilla digipalvelut ovat sekä tärkeitä, että intensiivisessä käytössä. Keski-ikäisillä käyttö on tasaista ja työarkea palvelevaa. Vanhin ikäryhmä kokee palvelut hyödyllisiksi, mutta käyttö jää useammin maltillisiksi. Kasvun vipuja vanhimille ovat käytettävyyden parantaminen (selkeys, valmiit, turvalliset oletusasetukset), luottamusta lisäävät ratkaisut (opastus, vahvistukset) ja aidot arjen hyödyt (asiointi, terveys, yhteydenpito). Palveluita eniten

6.10.2025

käyttävillä kannattaa tarjota digitaalisen hyvinvoinnin kontrollit (ilmoitushallinta, ajanhallinta), ettei arjen kuormitus kasva.

Keskimäärin 72 % käyttää digipalveluita ja -sovelluksia paljon tai erittäin paljon, ja jopa 65–75-vuotiailla tämä luku on 69 %. Kun digimaailma koetetaan tärkeäksi, sitä myös käytetään paljon arjessa. Tässäkin tulee huomata 28 % ryhmä, joka käyttää vähän tai erittäin vähän digipalveluita ja -sovelluksia. Tätä kysymystä voidaan välillisesti käyttää arvioimaan jatkossa, miten esimerkiksi vuonna 2026 lisääntyvä viranomaisten sähköinen asiointi näkyy tuloksissa.

3.1.3 Tekoälypalveluiden käytön laajuus - kuinka paljon käytät itse tekoälypalveluita (esim. OpenAI ChatGPT, Microsoft CoPilot, Google Gemini)?



Kuinka paljon käytät itse tekoälypalveluita (esim. OpenAI ChatGPT, Microsoft CoPilot, Google Gemini)?

Analyysi

Tekoälyn käyttö yleistyy nopeasti. Vähintään kuukausittain käyttävien osuus kasvoi 20 prosentista 31 prosenttiin (+11 prosenttiyksikköä, ~+55 %). Erityisen vahvaa kasvu oli usein käyttävissä: viikoittain ja lähes päivittäin käyttävien määrä lähes kaksinkertaistui (12 % → 23 %).

Samalla tekoälyä lainkaan käyttämättömien osuus pieneni selvästi (55 % → 39 %, -16 prosenttiyksikköä). Ensikokeilijoiden osuus nousi (25 % → 30 %) ja aktiivisten käyttäjien osuus laajeni (viikoittain +5 %, lähes päivittäin +6 %). Kuukausittainen käyttö pysyi ennallaan (8 %). Tämä viittaa siihen, että uudet käyttäjät jakautuvat joko kevyiksi kokeilijoiksi tai suoraan intensiivisiksi käyttäjiksi.

Tulokset kertovat kypsymisestä. Integraatiot (esim. toimisto-ohjelmistoissa), parempi tekoälypalveluiden saatavuus ja selkeytyvät käyttötapaukset ovat siirtäneet massaa "ei lainkaan" -kategoriasta sekä kokeiluun, että säännölliseen käyttöön. Silti 39 % ei käytä tekoälyä lainkaan. Tekoälyn hyödyntämisen kuilu syntyy osaamisen, luottamuksen ja hyödyllisen käytön tunnistamisen ympärille.

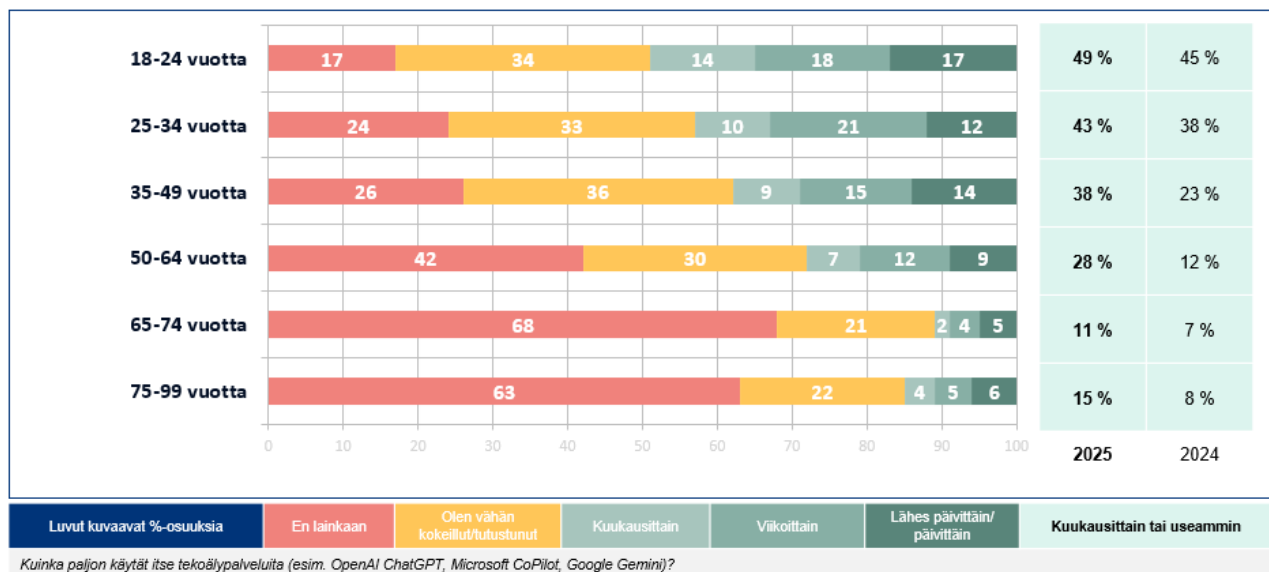
6.10.2025

Havainnot

Tekoälyn mahdollisuuksia kannattaisi nostaa esille niille henkilöille, jotka jo käyttävät sitä aktiivisesti esimerkiksi työroolissa tai vapaa-ajalla. Kynnystä kannattaisi madaltaa ei-käyttäjille. Tässä voisivat auttaa lyhyet demot, esimerkkiprompteilla toteutetut ”15 minuutin hyödyt” ja ”kuinka käytät tekoälypalveluita turvallisesti ja henkilötiedot turvaten” - ohjeistukset.

Tekoälypalveluiden käyttö siirtyy kokeiluista kohti arkea. Erityisesti viikoittaisessa ja päivittäisessä käytössä kasvu on jyrkkää, mutta merkittävä osa kansalaisista on yhä tekoälyn käytöstä sivussa. Tekoälypalveluiden mainetta ja luotettavuutta tulisi parantaa niiden parissa, jotka eivät sitä vielä halua, uskalla tai osaa hyödyntää.

3.1.4 Tekoälypalveluiden käytön laajuus: ikävertailu Kuinka paljon käytät itse tekoälypalveluita (esim. OpenAI ChatGPT, Microsoft CoPilot, Google Gemini)?



Analyysi

Tekoälyn käyttö on selvästi yleistynyt kaikissa ikäryhmissä. Vähintään kuukausittaisten käyttäjien osuus kasvoi vuosina 2024–2025 kautta linjan. Eniten kasvua tapahtui 35–49-vuotiailla (+15 prosenttiyksikköä) ja 50–64-vuotiailla (+16 prosenttiyksikköä). Nuorimmat käyttäjät ovat edelleen aktiivisimpia: 18–24-vuotiaista lähes joka toinen (49 %) käyttää vähintään kuukausittain, ja viikoittain tai päivittäin 35 % (18 % + 17 %).

Tekoälyä käytetään vähemmän vanhemmissa ikäryhmissä (44–67 % 50+-vuotiaiden ryhmissä). Joukossa on mielenkiintoinen aktiivinen vähemmistö: myös 75–99-vuotiaista 15 % käytti tekoälyä jo kuukausittain tai useammin (5 % kuukausittain, 4 % viikoittain, 6 % lähes päivittäin). Tämä sekä 65–74-vuotiaiden ryhmän kasvu (7 % →

6.10.2025

11 %) viittaavat osaamisen lisääntymiseen ja onnistuneisiin käyttötapausesimerkkeihin.

Kategorioista näkyy kaksi polkua:

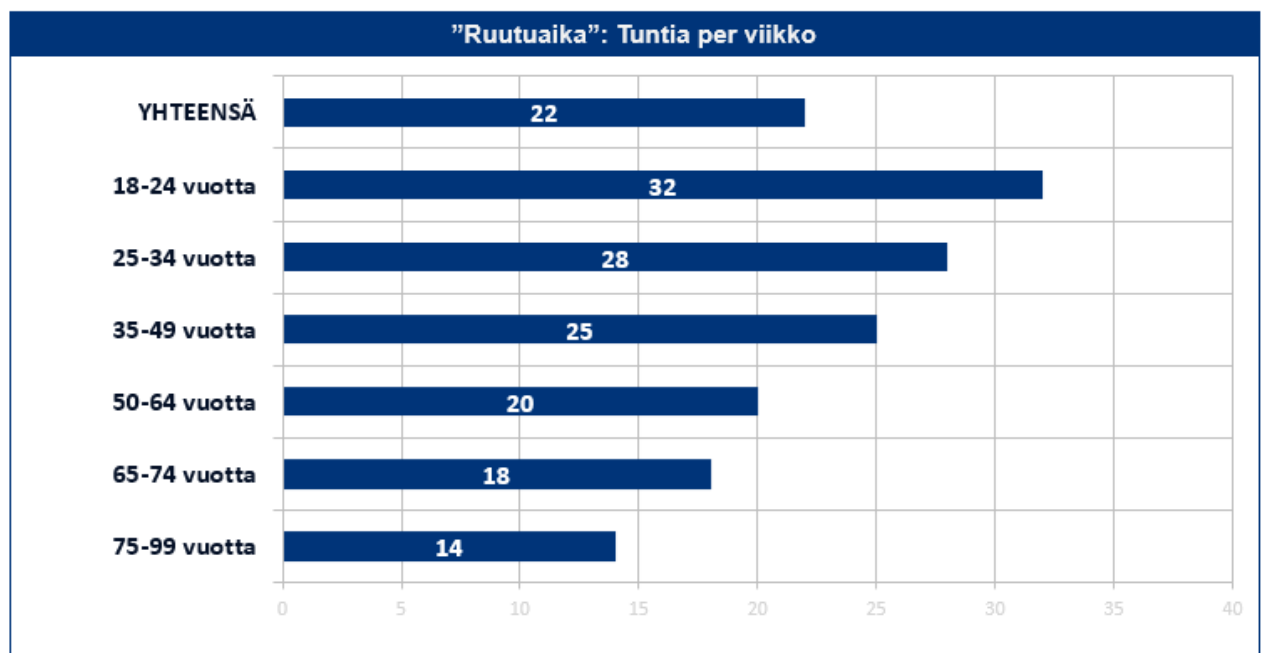
- Kynnyskäyttäjät ("Olen vähän kokeillut") ovat iso massa 18–49-vuotiaissa (33–36 %). Heidän muuttamisensa säännöllisiksi käyttäjiksi ratkaisee seuraavan kasvuaallon.
- Usein käyttävien määrä (viikoittain tai päivittäin) kasvoi nopeasti etenkin 25–49-vuotiailla (29–33 %). Tämä kertoo tekoälyn käytöstä arjen työssä (tuottavuus- ja kirjoitusassistentit, koodiavustajat).

Havainnot

Tekoälyn kokeilijat pitäisi saada säännöllisiksi käyttäjiksi tarjoamalla esimerkiksi 10 minuutin mikro-koulutuksia ja valmiita malliprompteja.

Vanhemmille ikäryhmille kannattaisi tarjota matalan kynnyksen hyötyjä (asiointi, tiivistys ja muistilistat). Lisäksi kannattaisi panostaa läpinäkyvään, palveluiden tietoturvalliseen ja tietosuojan huomioivaan hyödyntämiseen. Tällä voitaisiin laskea "En lainkaan" -vastausten osuutta.

3.1.5 Älylaitteiden parissa käytetty aika - uusi Kuinka monta tuntia arvioit keskimäärin käyttäväsi aikaa älylaitteiden parissa viikossa (ns. "ruutuaika")?



Kuinka monta tuntia arvioit keskimäärin käyttäväsi aikaa älylaitteiden parissa viikossa (ns. "ruutuaika")?

6.10.2025

Analyysi

Nuoret käyttävät älylaitteita merkittävästi enemmän kuin vanhemmat ikäryhmät. Erot ovat merkittäviä. 18–24-vuotiaat ovat keskimäärin noin 1,5 kertaa enemmän ruudun ääressä kuin koko otos ja yli 2 kertaa enemmän kuin vanhin ryhmä (75–99-vuotiaat).

Tätä voi selittää esimerkiksi:

- Sosiaalisuus ja viihde: nuoret käyttävät enemmän somea, videoita ja pelipalveluja.
- Työ ja opiskelu: 25–49-vuotiaiden korkea luku voi sisältää etätyötä ja opiskeluun liittyvää ruutuaikaa.
- Teknologian omaksuminen: vanhemmilla ikäryhmillä laitteiden käyttö ja tarve ovat usein vähäisempiä.
- Elämäntilanne: lapsiperheissä voi olla enemmän ruutuaikaa lasten tai perheen hallinnoinnin takia (tämä näkyy 35–49-vuotiaiden ryhmässä).

Havainnot

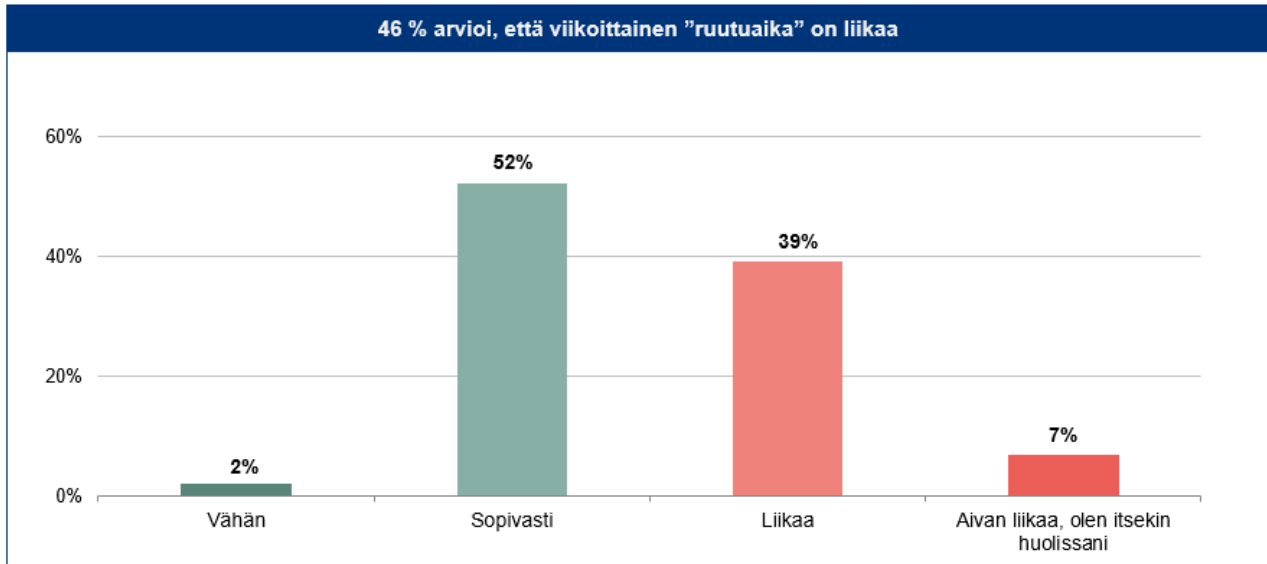
Nuorten korkeampi ruutuaika tukee aiempaa havaintoa siitä, että digitaalisen hyvinvoinnin toimenpiteet kannattaa kohdistaa nuoriin aikuisiin ja teini-ikäisiin.

25–49-vuotiaat tarvitsevat toisaalta työelämän ja vapaa-ajan erottelua koskevia ohjeita. Osa ruutuaikasta voi olla työaikaa, mikä muuttaa tarvittavia toimenpiteitä (esimerkiksi ergonomia, tauotus).

Vanhemmille ikäryhmille voidaan tarjota koulutusta ja parempaa saavutettavuutta, kun tavoitteena on palveluiden käyttö (eikä hyvinvointihälytys).

6.10.2025

3.1.6 Onko viikoittainen ruutuaikasi mielestäsi liikaa? Uusi



Analyysi

Yhteensä 46 % vastaajista koki, että viikoittainen ruutuaika on liikaa (39 % + 7 %).

Enemmistö (52 %) koki oman ruutuaikansa sopivana, mutta lähes joka toinen oli huolissaan tai koki ruutuajan liian suureksi. Tämä kertoo voimakkaasta jakautumisesta asenteissa: osa ihmisistä on rauhallisia oman digikäyttätymisensä suhteen, mutta osa kokee joko haittaa tai epävarmuutta.

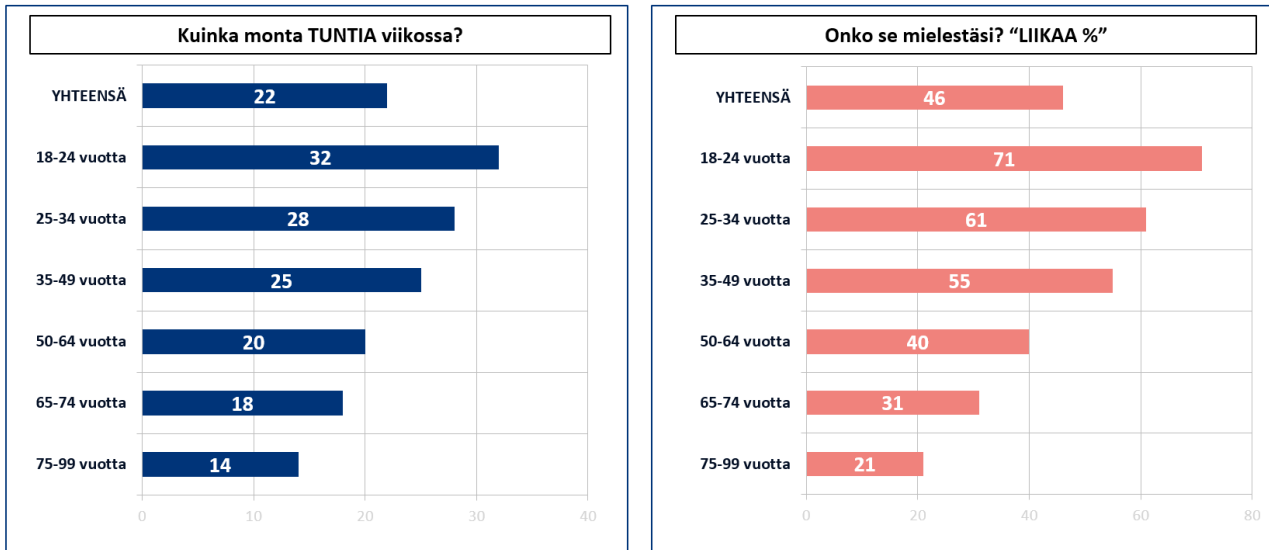
Eroja asenteissa voi selittää mm. ikä, työrooli (etätyö vs. konttorityö), perhetilanne (lapsiperheissä enemmän huolta lasten ruutuajasta), sekä subjektiivinen määritelmä siitä, mitä ruutuaika sisältää (työ, viihde, oppiminen). Myös omat odotukset ja vertailu muihin vaikuttavat vastauksiin.

Havainnot

Lähes puolet vastaajista kokee ruutuajan liian suurena, joten viestintä- ja hyvinvointitoimet ovat perusteltuja. Organisaatioissa ja julkisissa toimenpiteissä kannattaa huomioida sekä oman hallinnan tukeminen, että rakenteelliset keinot (esim. työn tauottaminen, digihygieniaohjeet, opetuksen suositukset).

6.10.2025

3.1.7 Onko viikoittainen ruutuaikasi mielestäsi liikaa – ikäryhmittäin? Uusi



Analyysi

Kaavio näyttää ikäjakauman sekä käytetyissä tunneissa, että kokemuksessa "liiallisesta" ruutuajasta. Keskimäärin ruutuaikaa kertyy 22 tuntia/viikko, eli noin 3,1 tuntia/päivä.

Nuorimmat käyttävät eniten ja kokevat käytön useimmin liialliseksi. 18–24-vuotiailla ruutuaikaa on 32 tuntia/viikko (noin 4 tuntia 34 min/päivä) ja heistä 71 % pitää määrää liian suurena. 25–34-vuotiailla tunnit laskivat 28 tuntiin/viikko (noin 4 tuntia/päivä) ja "liikaa"-vastausten osuus oli 61 %. Luvut kertovat sekä laitteiden korkeasta käytöstä, että melko hyvästä itsereflektion tasosta. Nuoret huomaavat itsekin, että määrä tuntuu suurelta.

Keski-ikäisistä yli puolet kokee käyttävänsä laitteita liikaa. 35–49-vuotiailla käyttö on 25 tuntia/viikko (noin 3 tuntia 34 min/päivä), ja 55 % kokee määrän liialliseksi. Työn, perheen ja vapaa-ajan useamman ruudun käyttö näkyy. Tuntimäärä ei ole nuorten tasoa, mutta kuormittavuuden kokemus on edelleen korkea.

Vanhemmissa ikäryhmissä sekä käyttö että liiallisuuden kokemus laskivat:

- 50–64-vuotiaat: 20 tuntia/viikko (noin 2 tuntia 51 min/päivä), 40 % kokee sen olevan liikaa.
- 65–74-vuotiaat: 18 tuntia/viikko (noin 2 tuntia 34 min/päivä), 31 % kokee sen olevan liikaa.
- 75–99-vuotiaat: 14 tuntia/viikko (noin 2 tuntia/päivä), 21 % kokee sen olevan liikaa.

6.10.2025

Tämä voi kertoa eri elämäntavoista, vähemmästä työn kautta kertyvästä ruutuajasta ja toisaalta maltillisemmasta some- ja viihdekäytöstä.

Molemmissa kaavioissa ikäryhmien järjestys on lähes sama. Enemmän ruutuaikaa johtaa useammin kokemukseen liiallisesta käytöstä. Subjekttiivinen ”liikaa”-tunne skaalautuu karkeasti tuntien mukana.

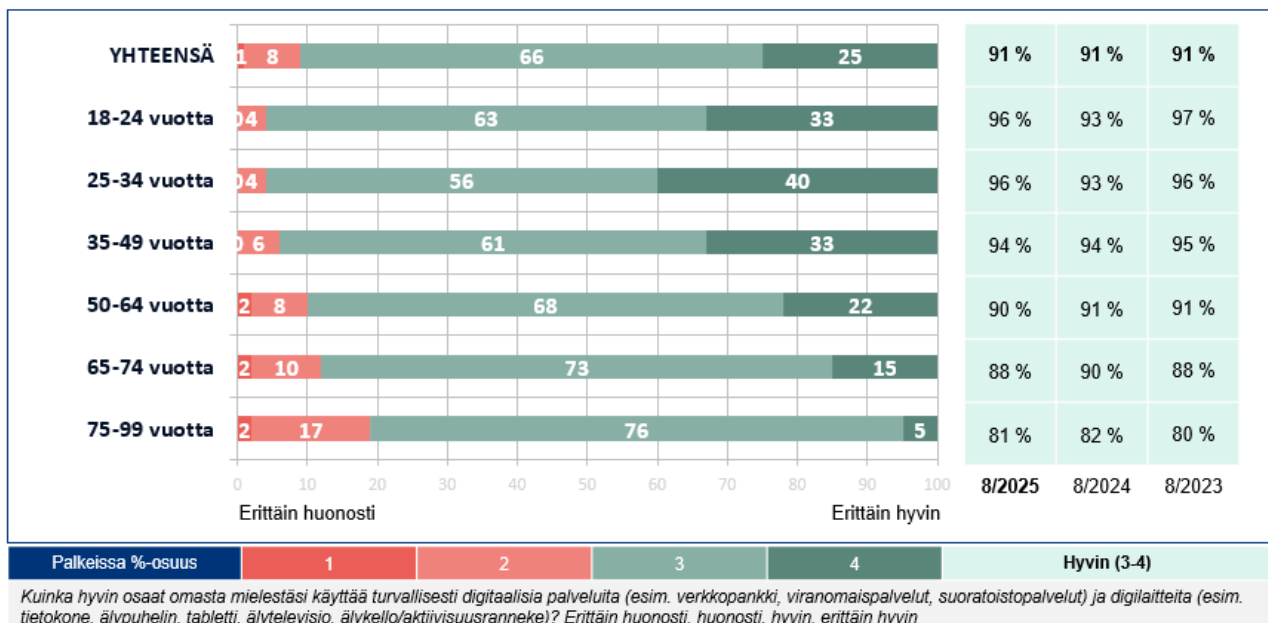
Havainnot

18–34-vuotiaille kannattaa kohdistaa konkreettisia digihyvinvoinnin keinoja (hiljaiset jaksot, ilmoituskatkot ja nukkumaanmenorajat). 35–49-vuotiaille painopiste on työn ja vapaa-ajan rajojen selkeyttämisessä (esim. ilmoitusten ajoitus ja työviestinnän pelisäännöt). Vanhempien ikäryhmien fokus kannattaa suunnata vähempään, mutta laadukkaampaan käyttöön (yhteydenpito, asiointi ja turvallisuus).

Seuraavaan kyselyyn kysymystä kannattaa täsmentää niin, että siinä erotellaan työ ja vapaa-aika, sekä määritellään aktiivinen vs. passiivinen ruutuaika.

3.2 Oma osaaminen ja siihen tarvittava tuki

3.2.1 Kuinka hyvin osaat omasta mielestäsi käyttää turvallisesti digitaalisia palveluita (esim. verkkopankki, viranomaispalvelut, suoratoistopalvelut) ja digilaitteita (esim. tietokone, älypuhelin, tabletti, älytelevisio, älykello/aktiivisuusranneke)?



Analyysi

Kokonaiskuva on poikkeuksellisen myönteinen ja vakaa. 91 % kokee osaavansa käyttää digipalveluja ja -laitteita turvallisesti (arviot 3–4). Taso on pysynyt samana jo

6.10.2025

kolme vuotta peräkkäin. Nuoret aikuiset erottuivat erittäin itsevarmoina (18–34-vuotiaat: 96 %), mutta myös 50–64-vuotiaat ylivät 91 prosenttiin. Vastaajien iän kasvaessa “erittäin hyvin” (4) -arvioiden osuus laski (25–34-vuotiaat: 40 %, 75–99-vuotiaat: 5 %). “Hyvin” (3) -vastausten taso oli korkea myös vanhemmissa ikäryhmissä (65–74-vuotiaat: 73 %, 75–99-vuotiaat: 76 %).

Vuosien 2024 ja 2025 väliset vaihtelut ovat pieniä. 65–74-vuotiaiden ryhmä notkahti hieman (90 % → 88 %), kun taas muissa ikäluokissa pysyttiin käytännössä ennallaan. Tämä viittaa siihen, että turvallisen käytön perusosaaminen on laajasti sisäistetty, vaikka subjektiivisen erinomaisuuden tunnetta on vähemmän vanhemmissa ikäryhmissä.

Havainnot

Painopiste tulisi saada siirtymään 3 → 4. Monella (erityisesti 50+-vuotiaiden ryhmissä) on vahva “hyvin” osaamisen taso, mutta “erittäin hyvin” osaavien määrä jää matalaksi. Kohdennettu koulutus (digiuhijauskuvioden tunnistaminen, vahvatunnistautuminen, salasanojen hallinta, varmuuskopiointi) voi nostaa varmuutta ilman suurta lisäkuormaa.

Vanhemmat ikäryhmät kaipaavat tukea. Vaikka 65+-vuotiaat kokevat osaavansa hyvin, käytännön esteet (pienet näytöt, monivaiheiset vahvistukset) laskevat 4-tason arvioita. Selkeä käyttöliittymä, vaihtoehtoiset varmennustavat ja ihmistuki nostavat laatua ilman, että turvallisuudesta tingitään.

Nuoret altistuvat digilaitteille jatkuvasti, ja heidän korkea varmuutensa yhdistyy intensiiviseen käyttöön. Nuorten kannattaa panostaa digitaalisen hygienian rutiineihin (salasanojen hallinta, laitepäivitykset, datajakamisen minimointi) ja sosiaalisen manipuloinnin sekä informaatiovaikuttamisen vastaisiin taitoihin, jotta riskit eivät kasva käytön mukana.

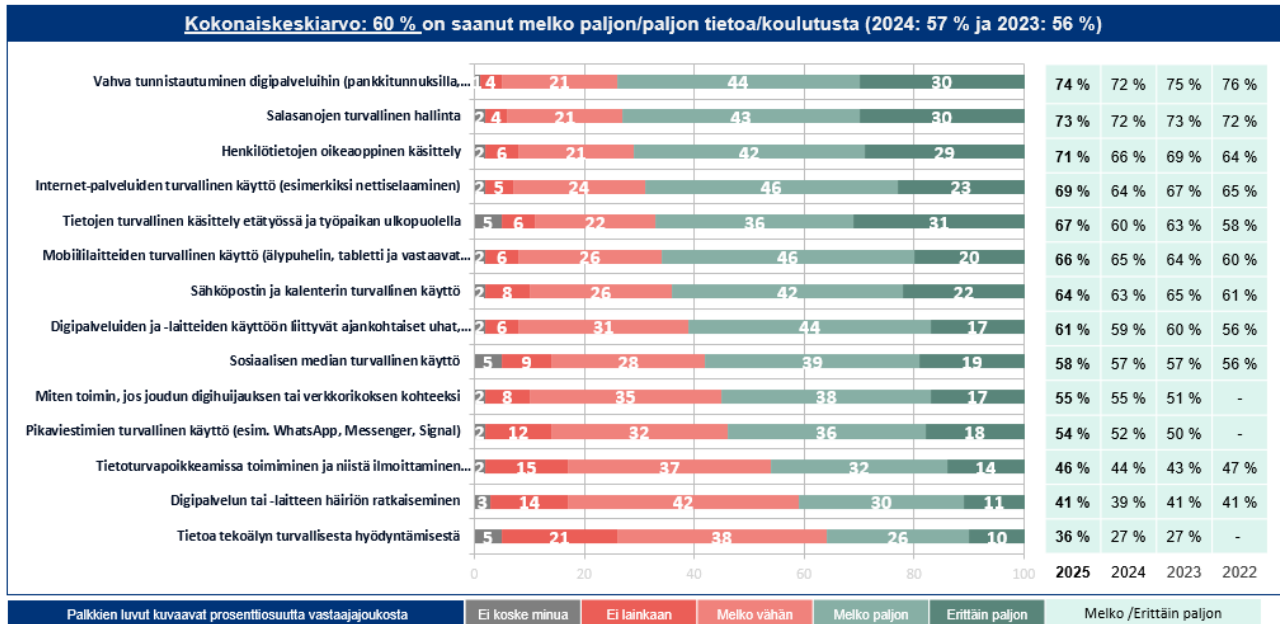
Turvallisen käytön subjektiivinen osaaminen on Suomessa erittäin vahvaa ja tasainen yli ikäluokkien. Kehityksen seuraava taso syntyisi siitä, että “hyvin” osaamisen taso muuttuisi toistettavaksi rutiiniksi kriittisissä tilanteissa. Se vaatii pieniä, säännöllisiä, todennettavia harjoitteita.



6.10.2025

3.2.2 Tiedon ja koulutuksen saatavuus

Minkä verran olet saanut tietoa ja/tai koulutusta (esim. työpaikalla, oppilaitoksessa, mediasta) seuraavista tilanteista ja niissä toimimisesta?



Minkä verran olet saanut tietoa ja/tai koulutusta (esim. työpaikalla, oppilaitoksessa, mediasta) seuraavista tilanteista ja niissä toimimisesta?

Analyysi

Turvallisen kyberhygienian teemat ovat vahvoja. Vahva tunnistautuminen (74 %), salasanojen hallinta (73 %) ja henkilötietojen käsittely (71 %) ovat kärjessä. Nämä ovat olleet pitkään myös eniten ohjeistettuja ja koulutettuja teemoja. Tulos osoittaa, että nämä opit ovat menneet perille osana vakiintunutta koulutusta ja viestintää.

Arjen käyttötilanteet ovat hyvällä tasolla, mutta eivät huippuja. Internetin turvallinen käyttö (69 %), etätö ja työpaikan ulkopuolella toimiminen (67 %), mobiililaitteet (66 %) sekä sähköposti/kalenteri (65 %) muodostavat toisen tärkeän ryhmän. Näissä taso on korkea, mutta ei vielä kata aivan kaikkea.

Reaktiokyvyn ja operatiivisten prosessien aukot näkyvät. Tietoturvapoikkeamissa toimiminen (46 %) ja häiriön ratkominen (41 %) ovat selvästi jäljessä. Kun jotain oikeasti tapahtuu, monelta puuttuu varmuus siitä, *mitä tehdä heti* ja *mistä apu löytyy*.

Uudempi teema laahaa jäljessä. Tekoälyn turvallinen hyödyntäminen (36 %) on matalalla tasolla, vaikka käyttö yleistyy nopeasti (katso aiemmin tulokset koskien tekoälyn käyttöä). Tämä epäsuhta kasvattaa operatiivista riskiä.

Sosiaalinen media ja pikaviestimet (58–54 %) ovat keskitasolla. Näiden palveluiden avulla käynnistetään usein digihuijauksia ja muita väärinkäytöksiä, joten palveluiden osaamisen tasoa pitäisi saada nostettua korkeammaksi.



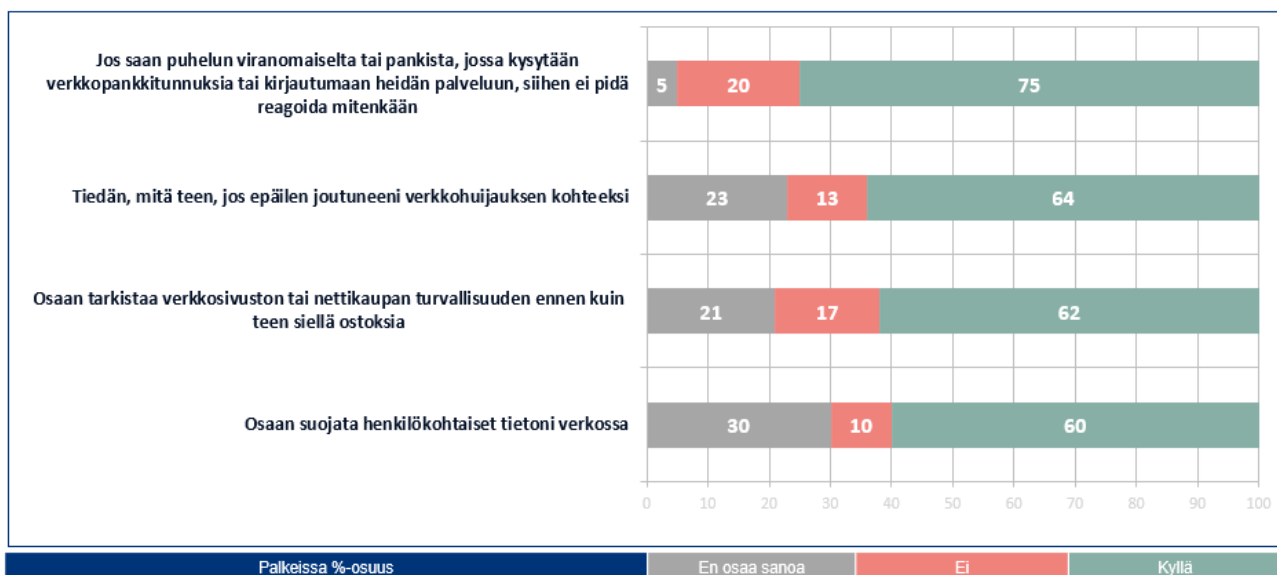
6.10.2025

Mediassa ja koulutuksissa on nostettu paljon esille ohjeistusta siitä, miten pitää toimia, jos joutuu digihuijauksen tai verkkorikoksen uhriksi. Siitä huolimatta osaamisen taso on pysynyt samalla tasolla (55 %) jo kaksi vuotta.

Havainnot

Kokonaisuuden keskiarvo on noussut 60 prosenttiin. Tällöin vastaaja on saanut melko paljon tai paljon tietoa tai koulutusta kysytyistä aiheista. On ilahduttavaa havaita, että keskiarvo on noussut kolme prosenttiyksikköä viime vuodesta ja neljä prosenttiyksikköä vuoteen 2023 verrattuna. Digihuijauksen tai verkkorikoksen kohteeksi joutuneiden koulutusta ja ohjeistusta tulee entisestään tehostaa. Vaikka keskiarvo on noussut, seuraavat kysymykset osoittavat, että kaikki oppi ei ole kuitenkaan jalkautunut arjen käytännöiksi.

3.2.3 Tietämys digiturvasta ja osaaminen toimia turvallisesti - Uusi



Analyysi

Kaavio tarkastelee vastaajien itsearvioimaa osaamista eri digiturvan arjen tilanteissa.

Vahvin osaaminen: huijauspuheluihin reagoiminen

75 % tiesi, ettei verkkopankkitunnuksia pidä antaa puhelimesta. Vain 5 % ei osannut sanoa ja 20 % vastasi väärin ("ei"), mikä kertoo siitä, että joka viides voisi yhä olla vaarassa langeta huijauspuheluun. Tämä on merkittävä riskiryhmä.

Huijauksen tunnistaminen

64 % uskoi osaavansa toimia oikein, jos epäilee joutuneensa verkkohuijauksen kohteeksi. 13 % vastasi suoraan "ei" ja 23 % "en osaa sanoa". Tämä paljastaa epävarmuutta: neljäsosa ei tiedä, miten reagoida huijausyritykseen.

6.10.2025

Verkkokaupan ja sivuston turvallisuuden arviointi

62 % koki osaavansa tarkistaa sivuston luotettavuuden, mutta 21 % ei osannut sanoa ja 17 % vastasi, ettei osaa. Tämä on heikko kohta. Käytännössä lähes 40 % on epävarmoja, tai ei osaa arvioida verkkokaupan luotettavuutta, mikä altistaa huijauksille etenkin nettiosastoissa tai sivustoissa, joissa luovutetaan henkilötietoja.

Henkilötietojen suojaaminen verkossa

60 % koki osaavansa suojata tietonsa, 10 % ei osaa ja 30 % ei osaa sanoa. Tämä on huolestuttavaa, koska "en osaa sanoa" -vastausten osuus on suurin kaikista väittämistä. Tietosuojakäytännöt ovat monille epäselviä, mikä lisää riskiä joutua identiteettivarkauden tai tietovuodon uhriksi.

Eniten varmuutta koetaan selkeissä, konkreettisissa huijaustilanteissa (puhelin, suorat huijausyritykset). Eniten epävarmuutta liittyy arjen verkkokäytäntöihin (nettiosastot, tietojen suojaaminen). "En osaa sanoa" -vastauksia on paljon (10–30 %), mikä kertoo, että osalla kansalaisista ei mielestään ole edes perustietoa aiheesta. Tämä epävarmuus on yhtä suuri riski kuin suora osaamattomuus.

Havainnot

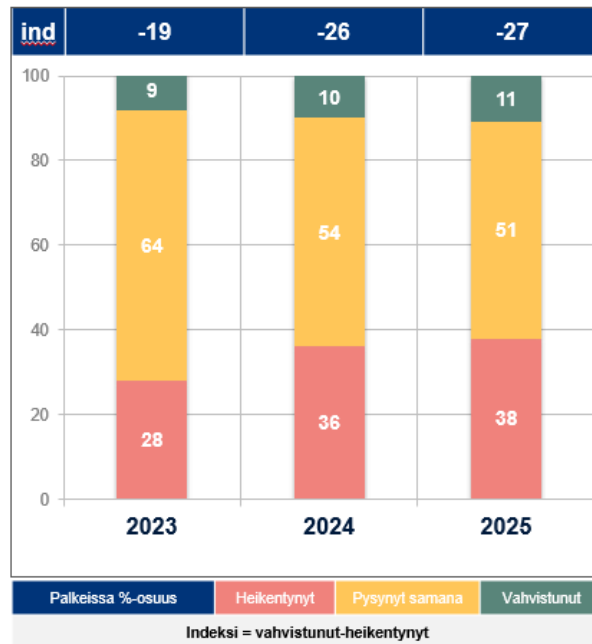
Suomessa on hyvä pohjataso digiturvatietytyydessä, mutta käytännön taitojen (verkkokauppojen turvallisuus, tietojen suojaus) osalta osaaminen on repaleista. Koulutuksissa ja kampanjoissa kannattaa painottaa nimenomaan arjen käytäntöjä, jotka eivät ole yhtä yksiselitteisiä kuin "älä anna tunnuksia puhelimesiä".

Hyödyllistä olisi myös kehittää yksinkertaisia tarkistuslistoja ja käytännön esimerkkejä, joilla epävarmat käyttäjät voisivat varmistaa omaa toimintaansa. Tämä kaventaishi "en osaa sanoa" -vastaajien ryhmää, joka on tällä hetkellä liian suuri.

6.10.2025

3.3 Yleinen luottamus digitaaliseen toimintaympäristöön

3.3.1 Onko luottamus digitaaliseen turvallisuuteen muuttunut viimeisen vuoden aikana?



Tämä on digiturvabarometrin yksi merkittävimpiä kysymyksiä, jota on nyt kysytty vuodesta 2023 saakka.

Analyysi

Prosenttijakaumat vuosittain:

- 2023: heikentynyt 28 %, pysynyt samana 64 %, vahvistunut 9 % → indeksi -19.
- 2024: heikentynyt 36 %, pysynyt samana 54 %, vahvistunut 10 % → indeksi -26.
- 2025: heikentynyt 38 %, pysynyt samana 51 %, vahvistunut 11 % → indeksi -27.

Päähavaintona negatiivinen suunta on vahvistunut.

Vuodesta 2023 lähtien luottamuksen heikentyneiksi arvioivien osuus on kasvanut merkittävästi (28 % → 38 %), kun taas pysynyt samana -ryhmä on supistunut (64 % → 51 %).

Vahvistunutta luottamusta kokevien osuus on kasvanut vain vähän (9 → 11 %). Indeksi syvenee -19 → -27, eli nettotilanne on yhä enemmän heikentynyt.

6.10.2025

Yleistynyt huoli tai konkreettiset negatiiviset kokemukset selittävät heikentymisarvioiden kasvun.

Luottamus on pysynyt samana -ryhmän pienentyminen viittaa siihen, että aiemmin tilannetta neutraalina pitäneiden osuus on kallistunut negatiiviseen arvioon.

Vahvistunutta luottamusta kokevien määrän pieni kasvu voi kertoa siitä, että parannuksia nähdään vain harvoissa tapauksissa, tai että luottamusta parantaneita kokemuksia ei ole paljoa.

Havainnot

Tilanne vaatii reagointia. Kasvava huoli (heikentynyt luottamus) vaatii toimia, ei pelkästään tiedottamista.

Strategian tulee sisältää sekä tilanteen korjaamista (mistä heikentyminen johtuu), että luottamuksen rakentamista (mitä on tehty ja millä aikataululla näkyviä parannuksia tulee).

Mitkä tekijät ovat vaikuttaneet vastauksiin – mikä on avovastausten yhteenveto?

1. Luottamus vahvistunut – luottamusta ja osaamisen kasvua

Tässä ryhmässä näkyy myönteinen kehityskaari. Digiturvasta puhutaan enemmän, mediassa on ohjeita ja neuvoja, ja ihmiset kokevat oppineensa tunnistamaan riskejä. Osa kokee myös, että viranomaiset ja yritykset tekevät konkreettisia toimenpiteitä turvallisuuden parantamiseksi. Tämä luo tunnetta, että varustautumisen taso on aiempaa parempi. Kyse on osittain kollektiivisesta “turvaverkko”-kokemuksesta: jos ympärillä näkyy aktiivisuutta, se vahvistaa omaa luottamusta.

2. Luottamus on pysynyt samana – arjen realismi ja varovaisuus

Tämän ryhmän ihmiset eivät ole kokeneet merkittäviä muutoksia omassa elämässään. He eivät ole joutuneet huijauksen kohteeksi, ja siksi turvallisuudentunne ei ole järkkynyt. Heidän luottamuksensa perustuu ennen kaikkea omaan harkintaan ja varovaisuuteen. He tiedostavat uhat, mutta uskovat osaavansa toimia oikein. Tietoisuus riskeistä ei automaattisesti vähennä luottamusta – päinvastoin, se voi jopa vahvistaa varautumisen tunnetta. Tämä ryhmä toimii rationaalisesti: “Tiedän riskit, mutta hallitsen ne.”

3. Luottamus on heikentynyt – uhat kasvavat ja osaamista epäillään

Heikentyneen luottamuksen ryhmässä korostuu kokemus uhkien jatkuvasta lisääntymisestä. Uhkien nopea kehittyminen – erityisesti tekoälyn tuomat uudet (digi)huijaukskeinot – luovat tunnetta, ettei oma osaaminen pysy perässä. Konkreettiset huijaukokemukset ja pelko joutua seuraavaksi uhriksi murentavat turvallisuudentunnetta. Tämä on psykologisesti raskain ryhmä, sillä tunne “en voi hallita kaikkea” syö luottamusta koko digitaaliseen ympäristöön.

Yhteenveto

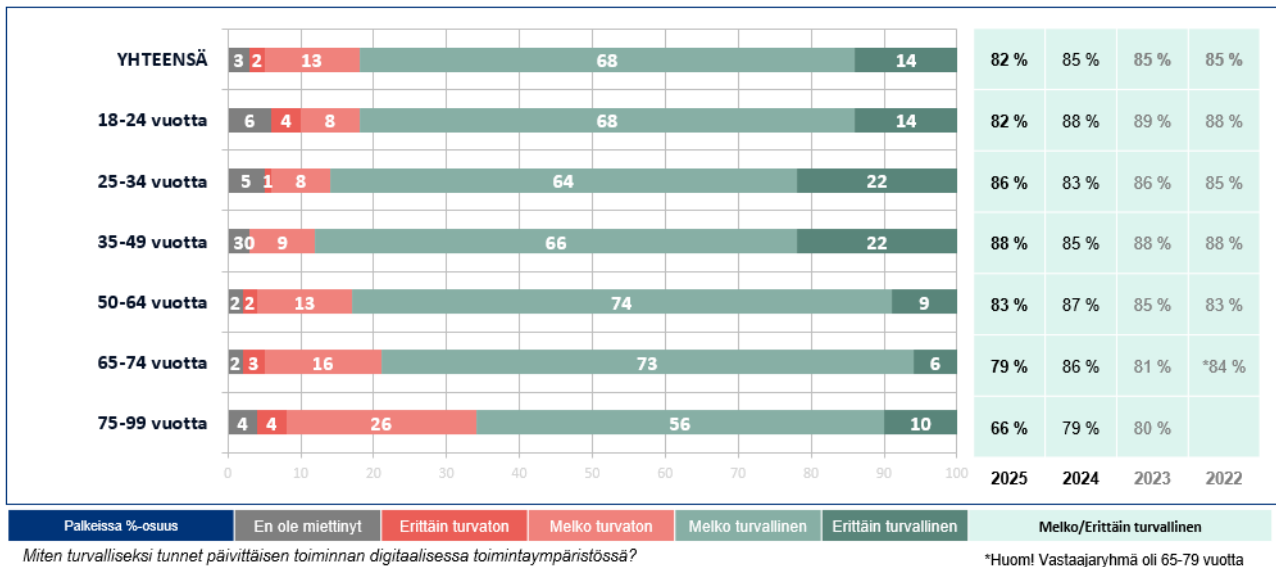
6.10.2025

Nämä kolme kategoriaa muodostavat jatkumon: luottamus vahvistunut → pysynyt samana → heikentynyt.

Henkilöt, joiden luottamus on vahvistunut, kokevat ympäröivän maailman ja oman osaamisensa tukevan turvallisuutta. Samalla luottamuksen tasolla pysyneet luottavat itseensä ja kokemukseensa. Heikentynyttä luottamusta tuntevat kokevat ympäristön muuttuvan nopeammin kuin oma osaaminen, mikä luo epävarmuutta ja pelkoa.

Luottamus digitaaliseen turvallisuuteen ei siis riipu vain todellisista uhkista, vaan myös siitä, millaista oma osaaminen on suhteessa niihin. Jos ihmiset kokevat, että osaavat toimia oikein, luottamus säilyy tai vahvistuu. Jos taas uhat koetaan ylivoimaisiksi, luottamus heikkenee, vaikka konkreettisia vahinkoja ei olisikaan vielä tapahtunut.

3.3.2 Turvallisuuden tunne digitaalisessa toimintaympäristössä – ikävertailu Miten turvalliseksi tunnet päivittäisen toiminnan digitaalisessa toimintaympäristössä?



Analyysi

Yhteensä 82 % kokee arjen digitoimintaympäristön vähintään melko turvalliseksi. Taso laski vuodesta 2024 (85 %).

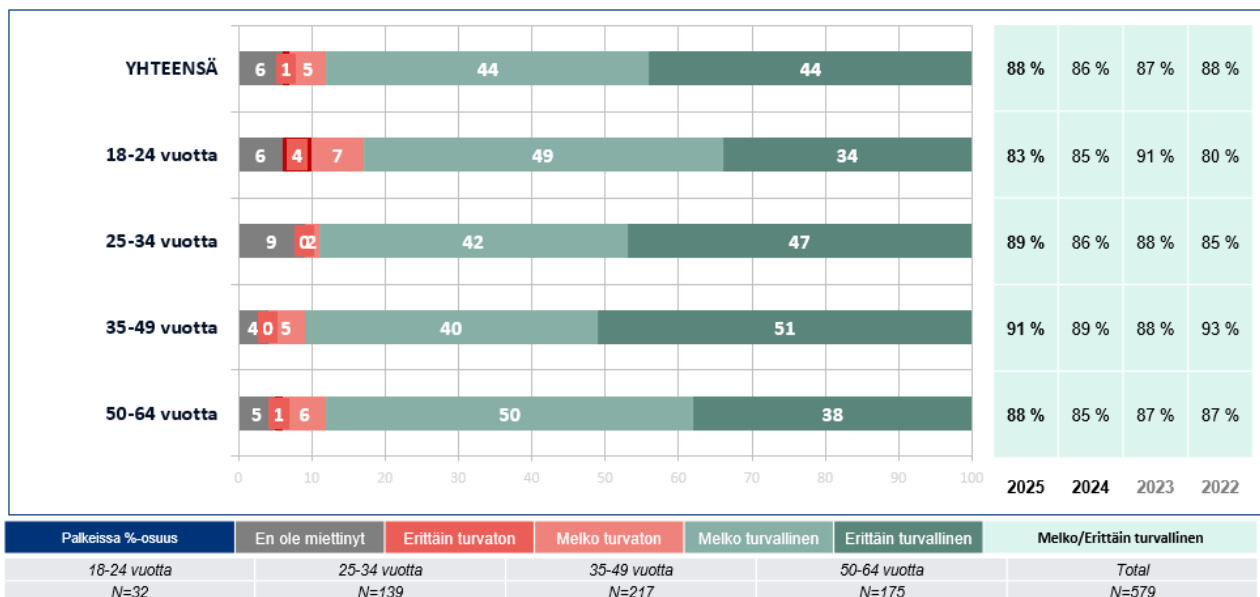
Lasku näkyy etenkin nuorimmissa (18–24-vuotiaat: 88 % → 82 %) ja vanhimmissa (75–99-vuotiaat: 79 % → 66 %). Keskimmaisissä ikäryhmissä suunta on päinvastainen (25–34-vuotiaat: 83 % → 86 %, 35–49-vuotiaat: 85 % → 88 %). Erittäin turvalliseksi olonsa tuntevien osuus on suurin 25–49-vuotiailla (22 %).

Havainnot

6.10.2025

Tuloksessa kannattaa huomioida etenkin vanhimpien ikäryhmien merkittävä lasku, sekä selvästi muita korkeampi turvattomuuden tunne (26 % kokee olonsa melko turvattomaksi 75–99-vuotiaissa). Lisäksi näkyi lievää epävarmuutta nuorissa (“en ole miettinyt” vastausten määrä on 6 %). Kokonaisvarmuus on yhä korkea, mutta vastausten jakautuminen kasvaa erityisesti ääripäissä. Tämä on osa yleistä muutaman prosentin laskusuuntaa useissa suoraan tai välillisesti turvallisuuteen liittyvässä kysymyksissä.

3.3.3 Turvallisuuden tunne digitaalisessa toimintaympäristössä töissä



Analyysi

Selkeä enemmistö kokee olonsa turvalliseksi. 44 % vastasi ”melko turvallinen” ja 44 % ”erittäin turvallinen”, eli yhteensä 88 % (2025). Tämä taso on pysynyt vakaana viime vuosina (86–88 %). Vaikka prosentuaalinen osuus tämän (88 %) ja edellisen kysymyksen (82 %) osalta ovat lähellä toisiaan melko ja erittäin turvallisten vastausten välillä, työpaikalla olonsa erittäin turvalliseksi kokevien osuus on merkittävästi suurempi (44 %) verrattuna yleisesti (14 %). Samoin turvallisuuden tunne on jopa noussut kaksi prosenttiyksikköä.

Ikäryhmäerot

- 18–24-vuotiaat: yhteensä 83 % vastasi kokevansa olonsa melko tai erittäin turvalliseksi. Nuorin ryhmä on hieman muita epävarmempi: sekä ”melko turvaton” että ”erittäin turvaton” vastausten osuudet ovat korkeammat kuin vanhemmissa ikäryhmissä.
- 25–34-vuotiaat: 89 % eli suhteellisen korkea turvallisuudentunne.
- 35–49-vuotiaat: 91 % eli korkein turvallisuudentunne.

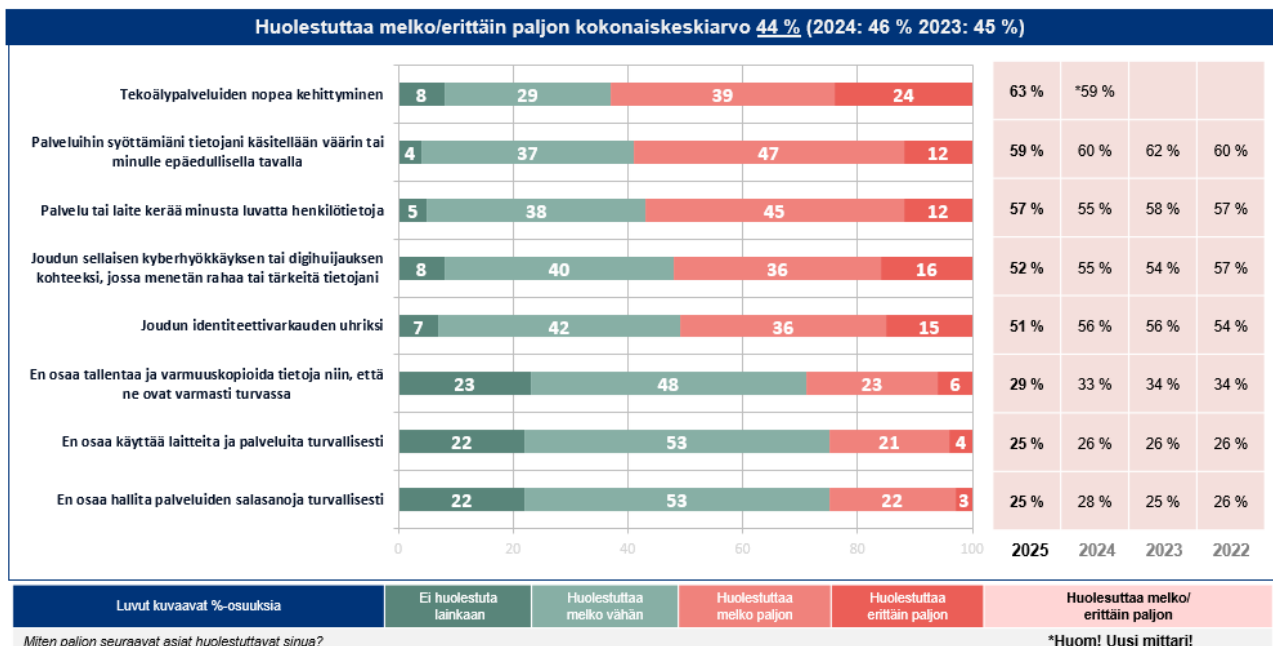
6.10.2025

- 50–64-vuotiaat: 88 % kokee olonsa turvalliseksi, mikä on hyvin linjassa kokonaistason kanssa.
- Negatiivisten osuudet: pieni, mutta merkittävä joukko koki tilanteen negatiivisesti. Yhteensä noin 6 % ei ole miettinyt asiaa, noin 1–4 % kokee olonsa erittäin turvattomaksi ja noin 2–7 % melko turvattomaksi riippuen ikäryhmästä.
- Trendit: vuosien 2022–2025 melko ja erittäin turvallisten vastausten osuus on pysynyt korkeana ja vakiona. Siinä ei ole merkittävää heikkenemistä tai paranemista.

Havainnot

Luottamus on työpaikoilla vahvaa, mutta ei aivan kaikilla. Suurin osa tuntee olonsa turvalliseksi, mutta silti nuorten (18–24-vuotiaat) pienempi turvallisuudentunne kannattaa huomioida. He ovat usein alttiimpia uusille ilmiöille (informaatiovaikuttaminen, sovellukset, some, pelit) ja huomaavat tai tulkitsevat riskit eri tavalla.

3.3.4 Digiturvallisuuteen liittyvät huolestuttavat asiat Miten paljon seuraavat asiat huolestuttavat sinua?



Analyysi

On positiivista havaita, että keskiarvo on pienentynyt kaksi prosenttiyksikköä. Ei ole yllättävää, että viime vuonna toisella sijalla ollut tekoälypalveluiden nopea kehittyminen on noussut huolenaiheista korkeimmaksi. Viime vuoden eniten huolestuttanut aihe (palveluihin syötettyjä tietoja käsitellään



6.10.2025

väärin) on pudonnut toiseksi.

- Tekoälypalveluiden nopea kehittyminen: 63 % huolestuneita (39 % melko paljon, 24 % erittäin paljon).
- Palveluihin syöttämiäni tietoja käsitellään väärin tai minulle epäedullisesti: 59 huolestuneita % (47 % + 12 %).
- Palvelu tai laite kerää minusta luvatta henkilötietoja: 57 % huolestuneita (45 % + 12 %).
- Joudun kyberhyökkäyksen tai digihuijauksen kohteeksi ja menetän rahaa/tärkeitä tietoja: 52 % huolestuneita (36 % + 16 %).
- Joudun identiteettivarkauden uhriksi: 51 % huolestuneita (36 % + 15 %).
- Vähiten huolta herättävät tekniset ja osaamiseen liittyvät seikat: varmuuskopiointi 29 %, laitteiden turvallinen käyttö 25 %, salasanojen hallinta 25 % (yhteensä melko tai erittäin paljon -vastaukset).
- Koko mittariston keskiarvo (melko tai erittäin paljon): 44 % huolestuneita. Vuodesta 2024 on tapahtunut pientä laskua 46 prosentista 44 prosenttiin.

Havainnot

Luottamuksen ytimessä on data ja sen käyttö. Vastaajat pelkäävät eniten sitä, mitä palvelut tekevät niihin syötetyille tiedoille, ja miten laitteet keräävät tietojamme. Tämä on selkeä merkki tietosuojan, tiedonhallinnan ja läpinäkyvyyden merkityksestä.

Tekoäly nousee erilliseksi huolenaiheeksi. Tekoälyn nopea yleistyminen koetaan erikseen niin merkittävänä, että se on korkeimmalla sijalla huolenaiheista. Osa huolesta voi liittyä automaatioon, väärän tiedon levitykseen, verkkorikollisuuden kehittymiseen, päätöksenteon selittämättömyyteen ja yksityisyyteen.

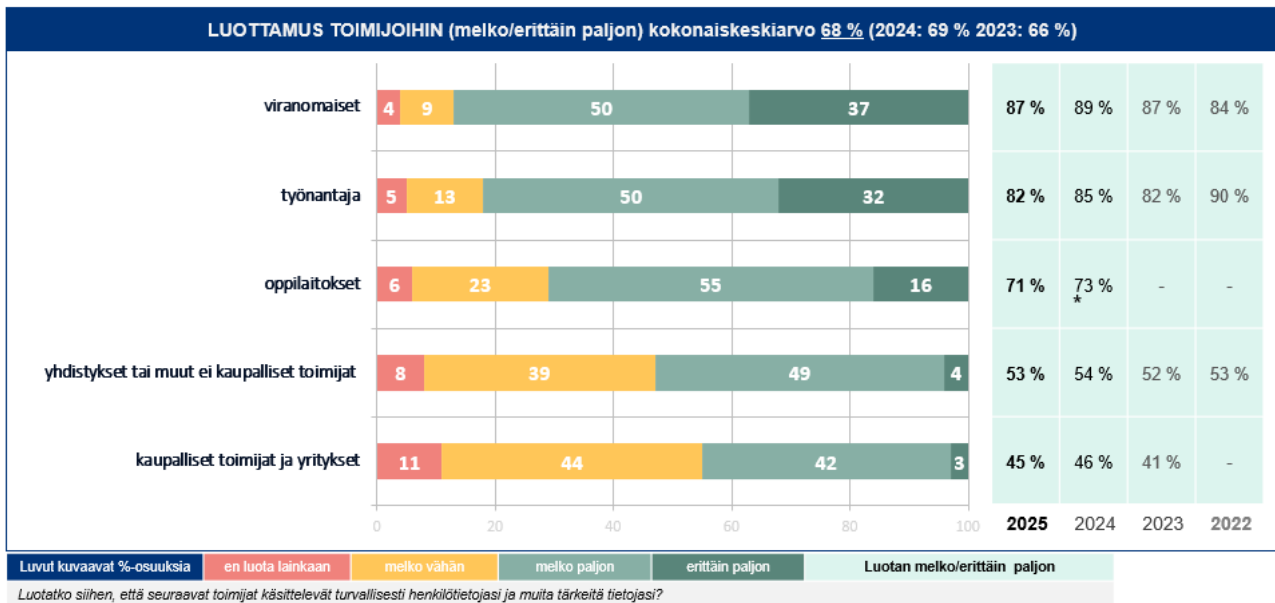
Osaamis- ja käytännölliset ongelmat näyttäytyvät pienimpinä (varmuuskopiointi, salasanat). Tämä voi tarkoittaa sitä, että ihmiset aliarvioivat näiden merkityksen riskeihin nähden, tai että osaamisen puute on piilossa.

Turvallisuushat ja identiteettivarkaudet ovat konkreettisia pelkoja. Ne ovat suoraan sidoksissa taloudelliseen ja henkilökohtaiseen vahinkoon, minkä vuoksi ne aiheuttavat paljon huolta.

6.10.2025

3.4 Luottamus tietojen käsittelyyn ja sisältöihin

3.4.1 Luottamus siihen, että omia tietoja käsitellään turvallisesti Luotatko siihen, että seuraavat toimijat käsittelevät turvallisesti henkilötietojasi ja muita tärkeitä tietojasi?



Analyysi

Tämä on yksi digiturvabarometrin keskeisimmistä kysymyksistä.

Julkiset toimijat ovat luottamuksen kärjessä, kaupalliset toimijat ja yritykset häntäpäässä. Viranomaisiin luottaa 87 % (joista 37 % “erittäin paljon”), kun yrityksissä vastaava osuus on 45 % (vain 3 % “erittäin paljon”). Työnantaja on toisella sijalla 82 prosentilla, mutta trendi on loivasti laskeva vuodesta 2024 (85 %) ja selvästi alempi kuin vuonna 2022 (90 %).

Oppilaitoksiin luottaa 71 %. Luottamuksen taso oppilaitoksiin on kohtalainen, mutta “erittäin paljon” -vastausten osuus jää matalaksi (16 %). Yhdistyksissä/ei-kaupallisissa toimijoissa luottamus on jakautunut. 47 % on varauksellisia (8 % ei luota lainkaan, 39 % melko vähän), vaikka 53 % luottaakin vähintään melko paljon.

Vuosivertailuna kokonaiskuva heikkeni aavistuksen (69 % → 68 %). Laskua tuli erityisesti viranomaisiin (–2 prosenttiyksikköä) ja työnantajiin (–3 prosenttiyksikköä). Yritykset taas nousivat vuoden 2023 tasosta (41 % → 45 %), mutta jäivät jälkeen vuoden 2024 tasosta. Pienet muutokset voivat kertoa esimerkiksi, että luottamus reagoi nopeasti uutisvirtaan, poikkeamiin ja näkyviin tietoturvatapauksiin.

Havainnot

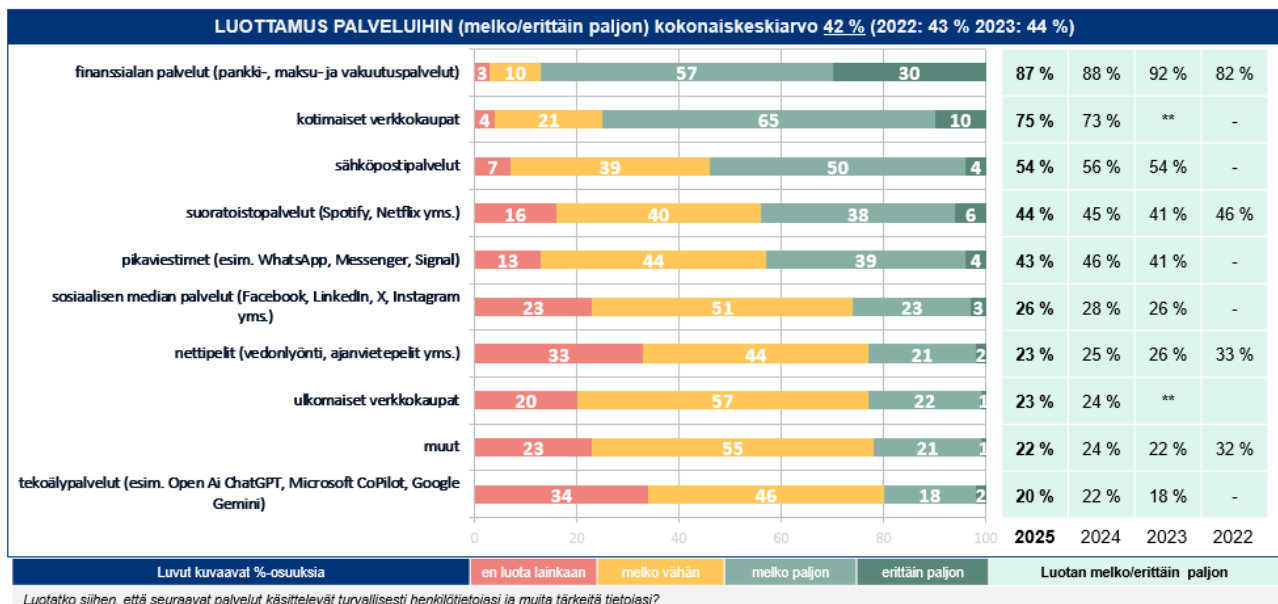


6.10.2025

Verkkorikollisuuteen ja muuhun turvattuuteen liittyvä uutisointi on kasvanut viimeisen vuoden aikana. Kansalaisten luottamus on laskenut vähemmän, kuin etukäteen kenties odotettiin. Viimeisen vuoden aikana on useiden viranomaisten, mutta myös yritysten ja etenkin finanssialan nimissä on lähetetty paljon erilaisia kalasteluviestejä. Osa kalasteluviesteistä on johtanut kansalaisiin kohdistuneisiin rikoksiin. Tämä laskeva suuntaus on huolestuttava trendi.

Saman kysymyksen toisessa osassa on esillä muita keskeisiä toimijoita ja myös digitaalisia palveluita.

Luottamus siihen, että omia tietoja käsitellään turvallisesti



Tämän osion ensimmäisellä sijalla ovat edelleen finanssialan palvelut (87 %), vaikka laskua vuoden 2023 huipusta (92 %) on tapahtunut. Vahva tunnistautuminen, sääntely (PSD2/DORA) ja pitkän linjan riskikuri näkyvät luottamusta ylläpitävinä tekijöinä. Verkkorikollisuus ja näiden toimijoiden nimissä verkkorikollisten lähettämät (kymmenet) miljoonat kalasteluviestit ja puhelinsoitot ovat kuitenkin aiheuttaneet asiakkaille merkittävää taloudellista vahinkoa.

Toisella sijalla ovat kotimaiset verkkokaupat (75 %). Parannusta vuoteen 2024 verrattuna on tapahtunut kahden prosenttiyksikön verran.

Keskitasolla ovat sähköposti (54 %), suoratoisto (44 %) ja pikaviestimet (43 %). Viestikanavissa luottamusta syövät huijaukset (phishing, tilikaappaukset) ja pikaviestimien osalta huoli esimerkiksi tietosuojasta.

Luottamus sosiaaliseen mediaan (26 %) on pysyvästi matala. Kaupallistettu datatalous ja jatkuvat väärinkäyttöuutiset pitävät luottamuksen pohjalla. Luottamus nettipeleihin (23 %) on laskenut pitkään (vuonna 2022: 33 %). Ulkomaisten

6.10.2025

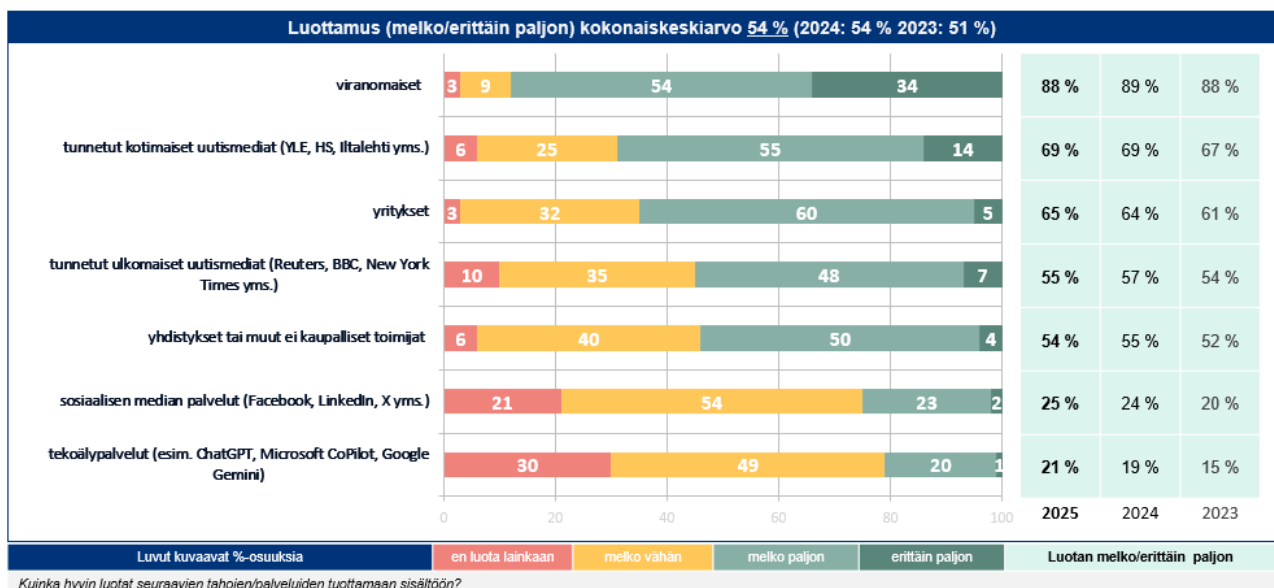
verkkokauppojen luottamuksen tason laskuun (23 %) vaikuttavat valeverkkokauppojen yleistyminen, halpatuotekauppojen laatuongelmat sekä EU-rajat ylittävän kuluttajansuojan epäselvempi tilanne.

Luottamus tekoälypalveluihin kasvoi lievästi vuodesta 2023 (18 %) vuoteen 2024 (22 %), mutta laski taas vuonna 2025 (20 %). Tekoälypalveluiden nopeaan kehittymiseen yhdistetään useita erilaisia riskejä. Näitä ovat esimerkiksi tekoälypalveluiden työelämään ja koko yhteiskuntaan aiheuttamat muutokset, niiden tarjoamat uudet mahdollisuudet verkkorikillisille ja väärinkäyttäjille, sekä palveluiden tuottamat virheet.

Luottamus palveluihin kokonaisuutena laski loivasti (44 % → 42 %). Kärkipäässä pysyi rahoitus- ja finanssiteknologia. Kaikkein sosiaalisimmat ja eniten dataa käyttäjistään keräävät palvelut kärsivät mainehaitoista.

Jakautuminen tuntuu kasvavan: suomalainen vs. ulkomainen, säännelty vs. villimpi ekosysteemi, sekä "infra" (pankki, kotimaiset kaupat) vs. "viihde/kanavat" (some, pelit). Ero luottamuksessa näihin on iso.

3.4.2 Luottamus tahojen/palvelujen tuottamaan sisältöön Kuinka hyvin luotat seuraavien tahojen/palveluiden tuottamaan sisältöön?



Analyysi

Vastauksissa näkyy selkeä luottamuksen hierarkia. Viranomaiset, kotimaiset uutismediat ja yritykset ovat luotetuimpien joukossa. Sosiaalinen media ja tekoälypalvelut taas jäävät selvästi jälkeen.

Perusluottamus instituutioihin pysyi vakaana. Viranomaisten luottamus on korkea ja pysynyt vakaana (n. 88–89 %), mikä antaa hyvän pohjan julkiselle kriisiviestinnälle.



6.10.2025

Perinteinen media piti asemansa. Kotimaiset uutismediat säilyttivät korkean luottamuksen. Ulkomaiset mediat herättivät hieman vähemmän luottamusta, mutta myös niiden luotettavuus oli yli 50 %.

Yritykset ovat nouseva luottamustaho. Yritysten luottamus on kasvussa (61 % → 65 %), mikä kertoo yritysten viestinnän ja vastuullisuusviestien vaikutuksesta.

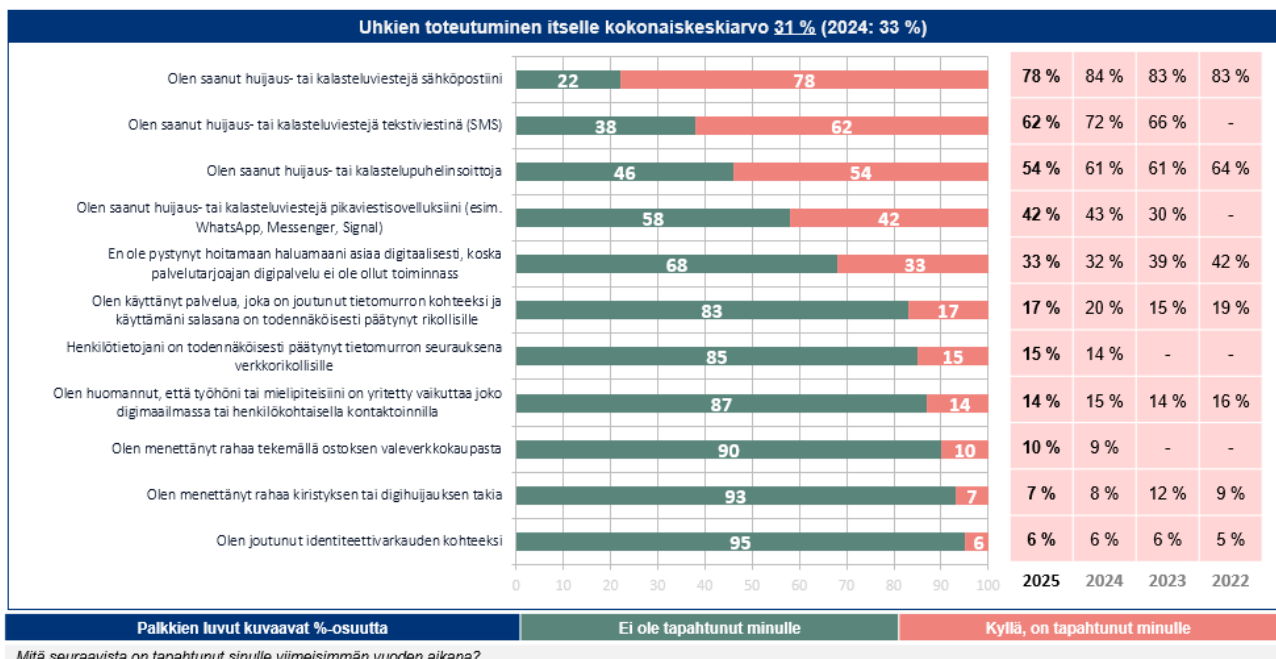
Sosiaalinen media ja tekoälypalvelut ovat kansalaisten luottamuksessa selvästi heikoimmalla tasolla, mutta molemmat osoittavat pientä kasvua (sosiaalinen media 20 % → 25 %, tekoäly 15 % → 21 %). Näiden hyödyntäminen saattaa nostaa luottamusta vähitellen.

Etenkin sosiaalisen median osalta luotettavuuden parantamista olisi mahdollista toteuttaa panostamalla sisältopolitiikkaan, faktantarkistukseen ja helpoksi tehtäviin luotettavuustyökaluihin (lähdeviitteet, merkinnät).

Näiden molempien osalta tarvitaan edelleen kansalaisten mediataitojen kehittämistä. Media- ja digitaalinen lukutaito (lähdekritiikki, lähdetarkastus, miten tunnistaa tekoälytuotoksia) on edelleen tärkeä ennaltaehkäisevä toimi.

3.5 Digiturvallisuus arjessa

3.5.1 Digiturvallisuuteen liittyvien uhkien toteutuminen itselle Mitä seuraavista on tapahtunut sinulle viimeisimmän vuoden aikana?





6.10.2025

Analyysi

Kokonaiskeskiarvo laski 31 prosenttiin (2024: 33 %), eli raportoitujen uhkien kokeminen on hieman vähentynyt. Selvin muutos on eniten käytössä olevissa kanavissa:

- Sähköpostissa (–6 prosenttiyksikköä) ja huijauspuheluissa (–7 prosenttiyksikköä) tapahtumat vähenivät.
- SMS-huijaukset putosivat voimakkaasti (–10 prosenttiyksikköä), mutta pysyivät silti korkeina (62 %).
- Pikaviestimet ovat lähes entisellään (–1 prosenttiyksikköä). 42 % kertoi altistuneensa.
- Vaikutukset ja vahingot eivät katoa. Rahan menetys verkkokaupassa nousi 10 prosenttiin (+1 prosenttiyksikköä). Kiristyksestä tai huijauksesta kärsineitä on yhä 7 %, ja identiteettivarkauden kohteeksi oli joutunut 6 %. Palvelukatkokset osuivat kolmannekseen (33 %), mutta trendi on pidemmällä aikavälillä laskeva (42 % → 33 %).

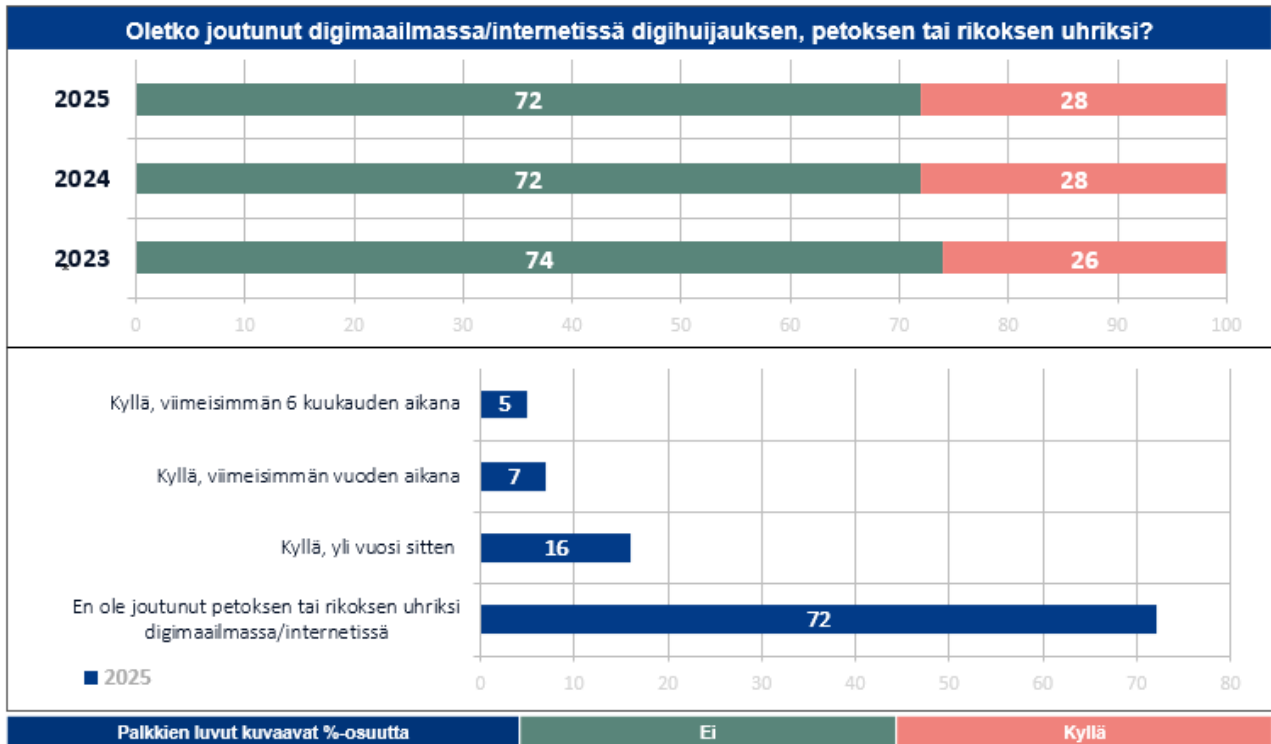
Havainnot

Operaattoreiden ja organisaatioiden tietoturvaluotteiden kehittäminen, suodatus, valvonta ja arjen varovaisuus ovat todennäköisesti pienentäneet altistusta peruskanavissa. Vahinkotapausten osuus ei laske vastaavasti. Tämä viittaa siihen, että harvemmat, mutta laadukkaammat kampanjat osuvat yhä, tai että kansalaiset eivät tunnista hyökkäyksiä yhtä hyvin kuin aikaisemmin.

6.10.2025

3.5.2 Rikoksen uhriksi joutuminen digimaailmassa/internetissä ja rikosilmoituksen tekeminen

Oletko joutunut digimaailmassa/internetissä digihuijauksen, petoksen tai rikoksen uhriksi?



Analyysi

Riskitaso on pysynyt vakaana. Uhriksi joutuneiden osuus pysyi samana 2024–2025 (28 %). Luku on hieman korkeampi kuin vuonna 2023 (26 %).

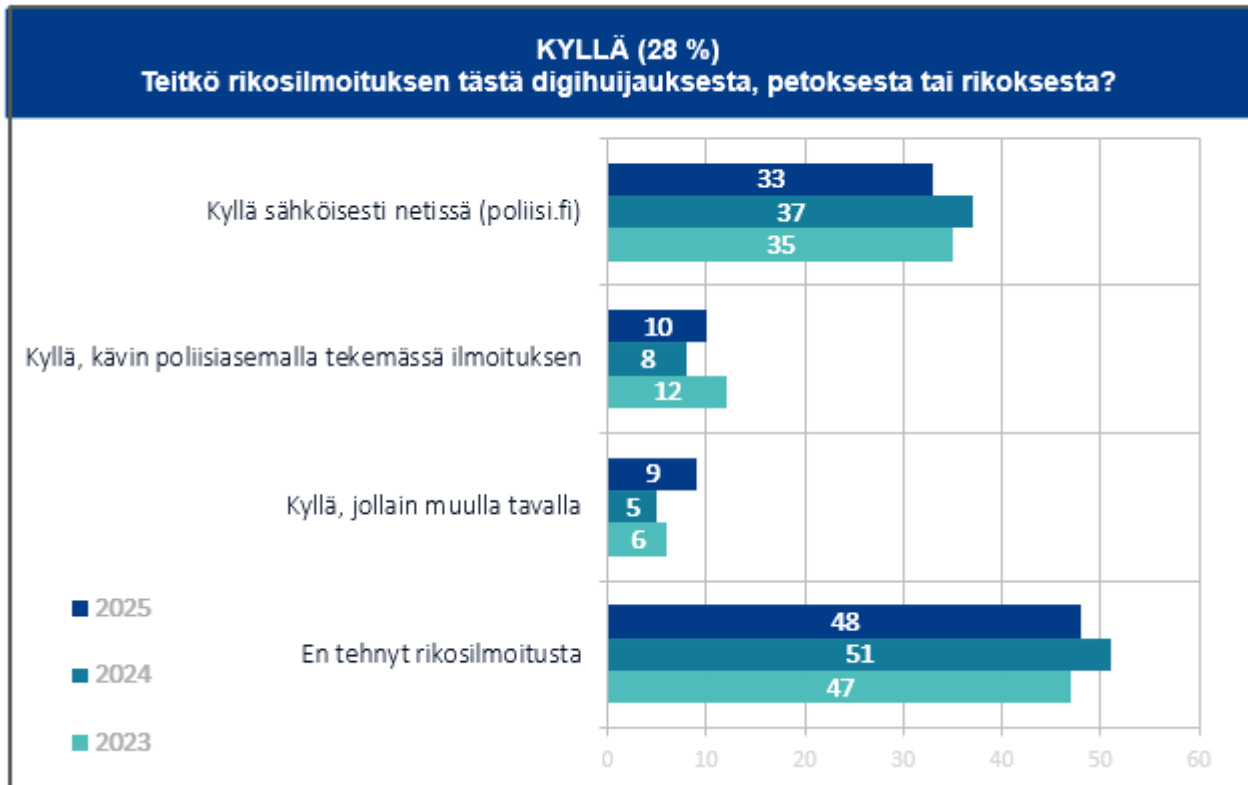
Uusia tapauksia on vuodessa 12 %. 5 % viimeisen 6 kuukauden aikana ja 7 % 6–12 kuukautta sitten. Noin 4/10 uhria (12/28 ≈ 43 %) on joutunut huijauksen tai rikoksen kohteeksi viimeisen vuoden sisällä, ja 16/28 ~ 57 % aiemmin yli vuosi sitten.

Enemmistö (72 %) ei ole joutunut uhriksi, mutta taso ei parane. Uhkakenttä pysyy mukana arjessa.

6.10.2025

3.5.3 Rikoksen uhriksi joutuminen digimaailmassa/internetissä ja rikosilmoituksen tekeminen

Teitkö rikosilmoituksen tästä digihuijauksesta, petoksesta tai rikoksesta?



Analyysi

28 % täysi-ikäisistä suomalaisista on joutunut digimaailmassa/internetissä digihuijauksen, petoksen tai rikoksen uhriksi. 52 % on tehnyt ylipäättään koskaan rikosilmoituksen. 40 % näistä rikosilmoituksista on tehty viimeisimmän vuoden aikana. Tämä tarkoittaa, että noin 6 % täysi-ikäisistä suomalaisista on kyselyn perusteella tehnyt viimeisen vuoden aikana rikosilmoituksen digimaailman rikoksesta tai petoksesta.

Havainnot

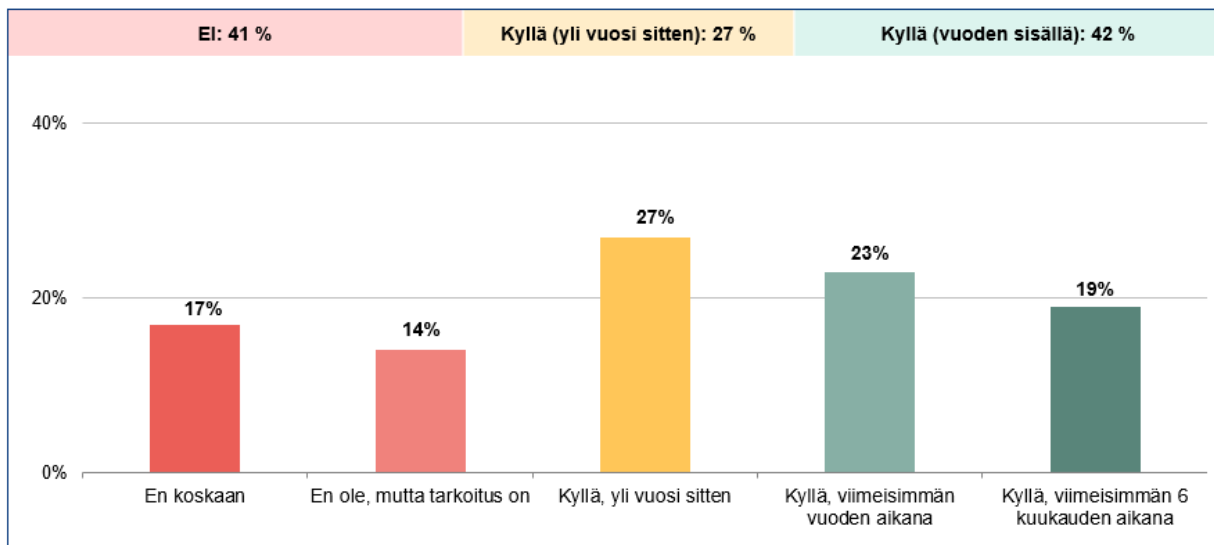
Valitettavasti viranomaiset eivät saa kaikkea sitä tietoa, mitä kansalaisten ja organisaatioiden tulisi heille ilmoittaa. Tämän takia emme saa selville verkkorikollisuuden kokonaiskuvaa tai heidän saamaansa taloudellista rikoshyötyä.

Mitä enemmän Poliisi saa ilmoituksia, sitä parempi tilannekuva saadaan verkkorikollisuuden tilanteesta Suomessa. Jokainen, ilmoittajasta itsestään kenties merkityksetön tieto, voi edesauttaa verkkorikollisen kiinnisaamisessa (digitaalinen sormenjälki).

6.10.2025

3.5.4 Maksukorttien ja tilien turvallisuuden parantaminen

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



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

Analyysi

69 % on tehnyt turvatoimia jossain vaiheessa ja 42 % on tehnyt niitä viimeisen vuoden aikana. Tämä viittaa siihen, että pankkien viestintä ja turvatarkistukset, mobiilisovellusten asetukset sekä julkinen keskustelu näkyvät vastaajien käyttäytymisessä.

Kriittisesti kolmannes (31 %) ei ole vielä parantanut suojausta. Tässä on samalla merkittävä riskiryhmä. Passiivisuus on usein altistava tekijä (esim. sama kortti/tili käytössä kaikkialla, ei hälytyksiä, korkeat oletusrajat).

On ilahduttavaa havaita, että 19 % on tehnyt näitä toimenpiteitä viimeisen 6 kuukauden aikana. Tämä lähiaikoina tapahtunut korjaus on yleensä reaktiivista (läheltä piti -tilanne, kaverin kokemus, pankin viesti, mediassa esillä olleet uutiset).

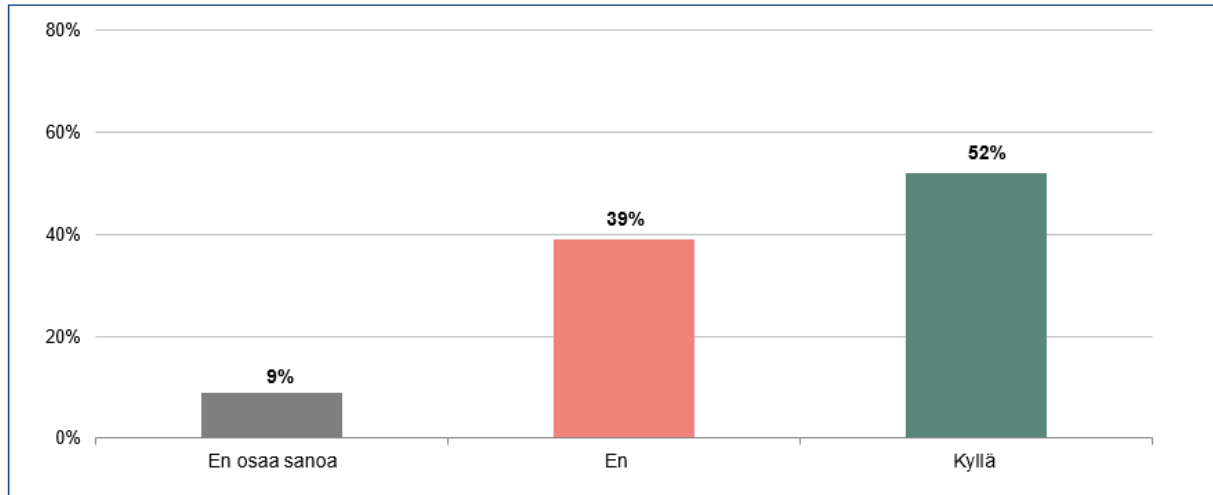
Lisäksi 14 % vastasi aikovansa ryhtyä toimenpiteisiin. Tämä ryhmä pitäisi saada aktivoitua tekemään suunnittelemansa toimenpiteet.

Havainnot

Turvataso on menossa oikeaan suuntaan. Yli kaksi kolmesta on jo toiminut, ja lähes puolet viimeisen vuoden aikana. Kolmannes on vielä lähtökuopissa. Sekä finanssialan toimijat, että media ovat nostaneet esille lokakuussa 2025 käyttöönotettavan EU-alueen pikamaksuasetuksen, joka varoittaa, jos saajan tilinumeron nimi ei vastaa maksajan syöttämää nimeä. Tämä toivottavasti kannustaa myös kansalaisia tarkistamaan asetuksiaan ja miettimään turvallisempia käyttötapoja.

6.10.2025

3.5.5 Käytän jokaisessa eri verkkopalveluissa eri salasanaa - uusi



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.

Analyysi

Yli puolet (52 %) ilmoitti käyttävänsä eri salasanaa jokaisessa palvelussa, mikä on hyvä lähtökohta. 39 % kuitenkin myönsi salasanojen kierrätyksen. Tämä joukko on alttiina tietomurroissa paljastuneille salasananhyökkäyksille (vuotanutta salasanaa testataan muihin palveluihin). 9 % "en osaa sanoa" -vastauksia viittaa siihen, ettei omaa salasanojen käyttöä hahmoteta (ei hallintatyökalua, ei näkyvyyttä).

Havainnot

Eri salasanan käyttö eri palveluissa ei vielä takaa turvaa, koska salasanoja voidaan toteuttaa myös heikkolaatuisesti. Tällaisia ovat:

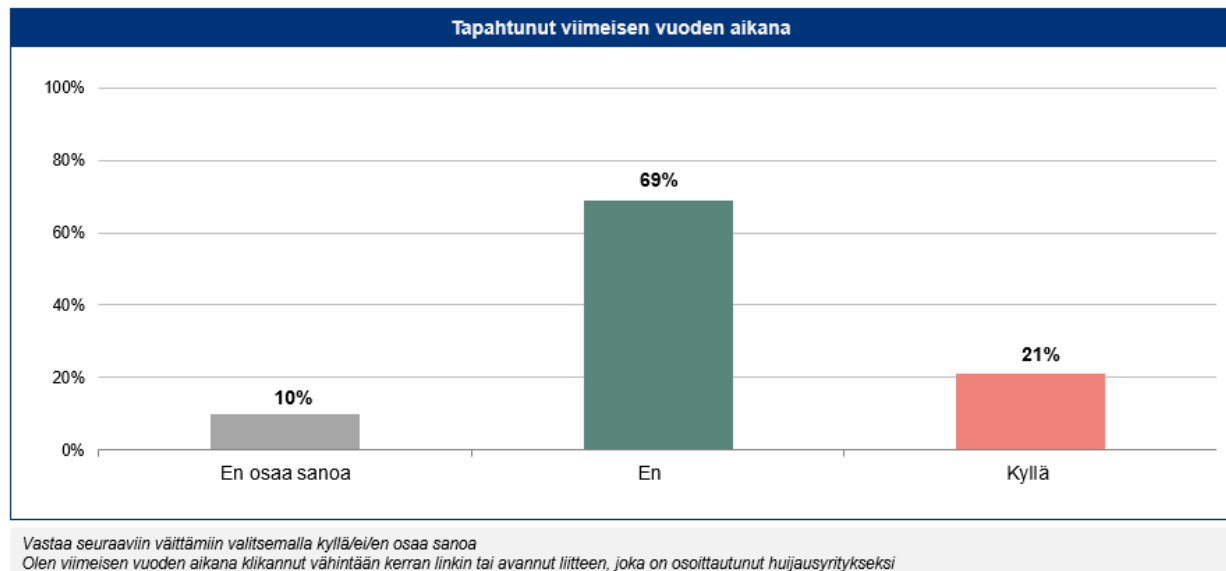
1. Heikot salasanat (lyhyet, ennustettavat lauseet)
2. Toistuvat kaavat (sama runko + vaihtuva loppu: Kesä2024!, Kesä2025!)
3. Ilman toista tekijää (kaksivaiheinen tunnistautuminen eli MFA/2FA puuttuu)

"Kyllä" -vastausten ryhmässä on todennäköisesti salasananhallinnan käyttäjiä (selaimen tai erillisen sovelluksen holvi). "En" -vastausten ryhmän keskeinen ajuri on muistikuorma. Ilman holvia ja automaattista täyttöä ihminen optimoi muistettavuutta, ei turvallisuutta. "En osaa sanoa" -vastaus on usein merkki sekavasta käytännöstä (selaimen muistamat, muistilistat ja muistilaput).

6.10.2025

3.5.6 Olen klikannut linkkiä, joka osoittautui huijausyritykseksi - uusi

Olen viimeisen vuoden aikana klikannut vähintään kerran linkin tai avannut liitteen, joka on osoittautunut huijausyritykseksi - uusi



Analyysi

Joka viides suomalainen (21 %) on klikannut huijauslinkkiä tai avannut huijausliitteen viimeisen vuoden aikana. Tämä osoittaa, kuinka yleisiä digihuijaukset ovat ja kuinka vaikeita niitä on tunnistaa. Ikäryhmien välillä ei ole tässä havaittavissa eroa.

Tämä on iso arjen riski, sillä yksi väärä klikkaus riittää käynnistämään salasanojen kalastelun, haittaohjelman latauksen tai maksuhuijauksen. Lisäksi 10 % ei osaa sanoa, mikä viittaa heikkoon tilannetietoisuuteen. Osa vastaajista voi olla klikannut linkkiä huomaamattaan (esim. puhelimessa esikatselu aukeaa napsautuksesta).

Havainnot

Kun tätä peilaa muihin tuloksiin (sähköpostihuijauksia sai 78 %, SMS-huijauksia 62 % ja pikaviestihuijauksia 42 %), suuntaa antava tulkinta on, että altistumisesta seuraa klikkaus varsin usein. Vähintään joka neljäs–kolmas altistuksista johtaa ainakin yhteen klikkaukseen (kanavat sekoittuvat, joten tämä on karkea arvio).

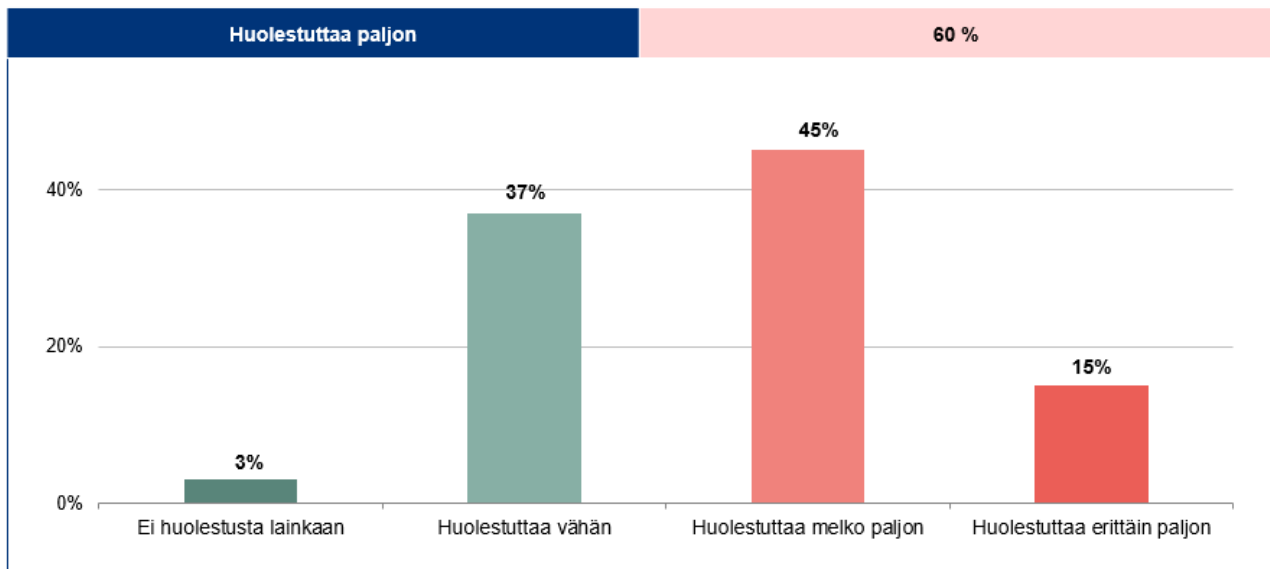
Mitä tämä kertoo käyttäytymisestä? Puhelimissa linkit aukeavat herkemmin (pieni ruutu, esikatselut), ja yhteys maksamiseen on lyhyt (Apple/Google Pay, mobiilipankki). Huijausten laatu on parantunut (aidon näköiset nettiosoitteet, tekoälyllä tehdyt tekstit ja grafiikka). Digihuijausta ei enää tunnista pelkästään kirjoitusvirheen perusteella, kuten aiemmin.

“En osaa sanoa” -vastauksen antanut ryhmä on usein se, jolla ei ole systemaattisia rutiineja linkkien tarkistamiseen.

6.10.2025

3.6 Kyberhyökkäykset, digihuijaukset ja suhtautuminen digiturvaan

3.6.1 Huoli suomalaisen yhteiskuntaan kohdistuvista kyberhyökkäyksistä ja digihuijauksista - uusi



Mitä mieltä olet suomalaisen yhteiskuntaan kohdistuvista kyberhyökkäyksistä ja digihuijauksista?

Analyysi

Suomalaisten perushuoli on korkea ja laajasti jakautunut. Kuusi kymmenestä kokee vähintään merkittävää huolta, ja vain kolme prosenttia ei koe huolta lainkaan. Paino on ”melko paljon” -vastausten kategoriassa (45 %), mikä kertoo pikemminkin jatkuvasta, arkeen ulottuvasta riskitietoisuudesta kuin paniikista.

Yhteiskunnallinen näkökulma on vahva. Huoli ei rajaudu yksilön asiointiin, vaan kohdistuu koko palveluekosysteemiin (pankit, viranomaiset, terveydenhuolto, energia, viestintä).

Suurin määrä on ”melko paljon” -vastauksia (45 %). Tämä viittaa siihen, että ihmiset pitävät riskiä todellisena, mutta eivät koe tilannetta hallitsemattomaksi.

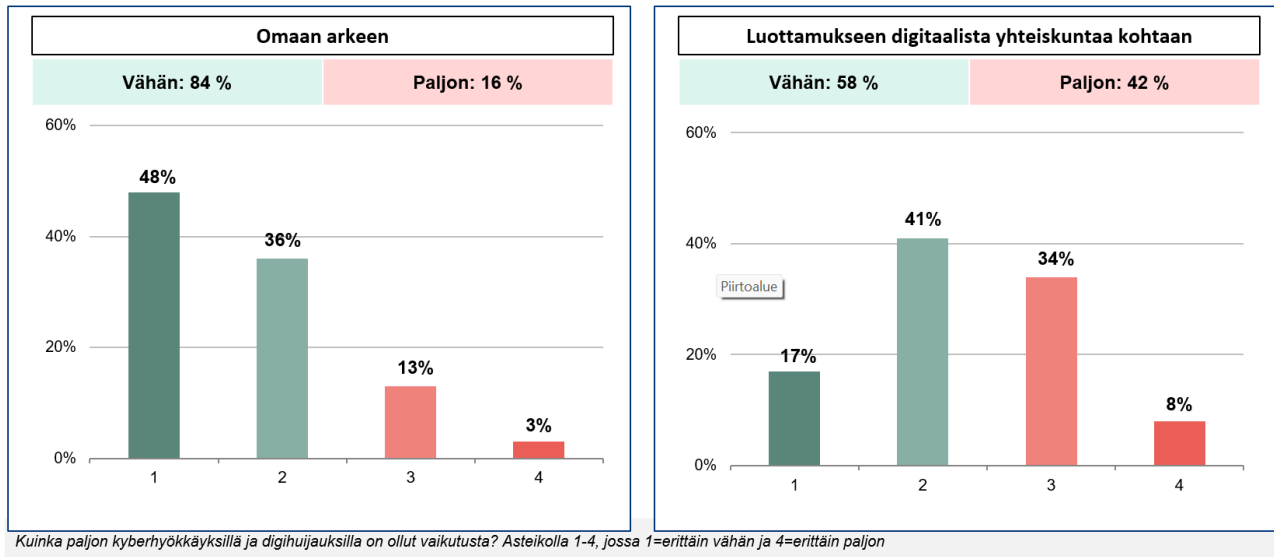
Havainnot

Huoli on korkea, mutta rakentava. Suomalaiset odottavat konkreettisia, näkyviä suojatoimia ja selkeitä ohjeita. Seuraava parannus syntyy läpinäkyvyydestä, selkeistä ohjeista ja harjoituksista sekä arjen digihygieniasta, ei pelottelusta.

6.10.2025

3.6.2 Kyberhyökkäyksien ja digihuijauksien vaikutus

Kuinka paljon kyberhyökkäyksillä ja digihuijauksilla on ollut vaikutusta? Uusi



Analyysi

Kyberhyökkäykset ja digihuijaukset vaikuttavat arkeen vähän. 84 % kokee, että ne ovat vaikuttaneet vain vähän omaan arkeen kuluneena vuotena. Keskimääräinen vaikutus omaan arkeen on matala.

Luottamukseen digitaalista yhteiskuntaa kohtaan vaikutus on selvästi suurempi. 42 % raportoi paljon vaikutusta luottamukseensa digitaalista yhteiskuntaa kohtaan. Vaikutus on selvästi suurempi arjen vaikutukseen nähden.

Ero "paljon" -vastauksen antaneiden kokemuksessa on 26 prosenttiyksikköä (16 % vs. 42 %). Häiriöt eivät useimmiten pysäytä arkea, mutta nakertavat järjestelmätason luottamusta.

Havainnot

Resilienssi arjessa toimii kohtuullisesti. Palvelukatkokset ja huijausyritykset näkyvät, mutta useimmat ihmiset pystyvät jatkamaan arkeaan vähin häiriöin (varajärjestelyt, useampi tunnistautumispalvelu).

Luottamus on herkempi muuttuja. Näyttävät tapaukset, mediahuomio ja ketjuvahingot (tietovuodot, henkilötietojen väärinkäyttö) heijastuvat nopeasti luottamukseen, vaikka omaan arkeen ei olisi tullut suurta konkreettista haittaa.

Mielipiteiden jakautumisesta on olemassa riski: pieni vähemmistö (8 %) koki erittäin paljon vaikutusta luottamukseen. Jos tätä ryhmää ei kohdata avoimesti ja konkreettisesti, heistä tulee narratiivin kantajia lähipiireissään.

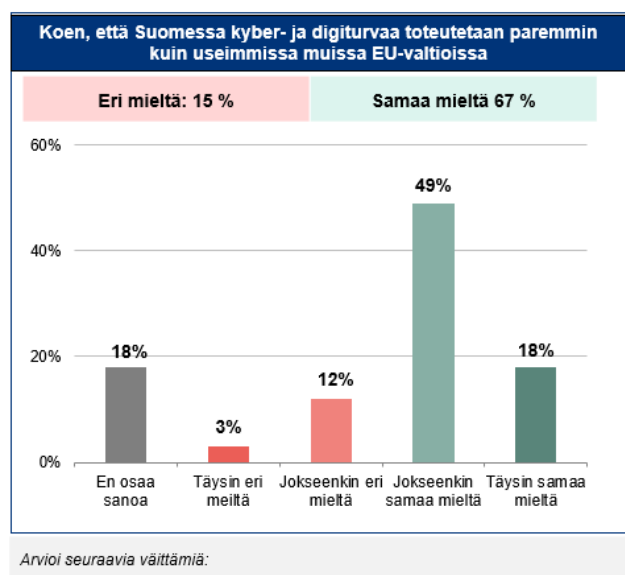
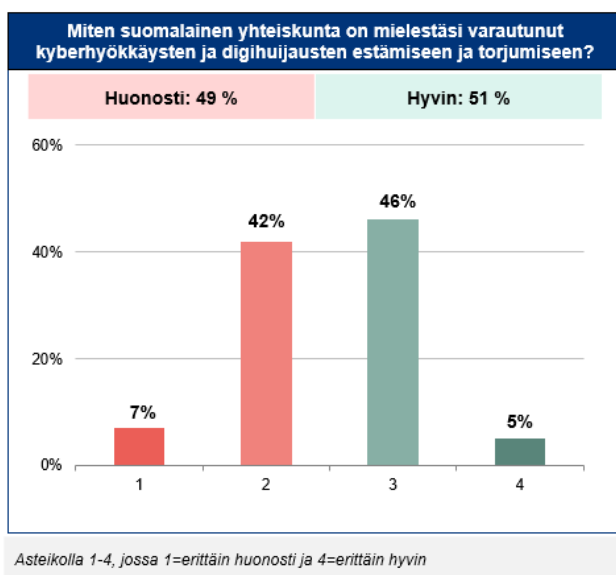
6.10.2025

Suomalaisten arki on yllättävän resilientti, mutta luottamus järjestelmätasolla on haavoittuvampi. Parannus syntyy kolmella tavalla: läpinäkyvä resilienssi, käyttäjälle näkyvät oletusturvat ja harjoiteltu ensivaste. Kun nämä ovat kunnossa, "paljon"-kokemukset kääntyvät kohti "vähän"-kokemuksia sekä arjessa, että luottamuksessa.

3.6.3 Yhteiskunnan varautuminen digiturvaan

Miten suomalainen yhteiskunta on mielestäsi varautunut kyberhyökkäysten ja digihuijausten estämiseen ja torjumiseen? Uusi

Koen, että Suomessa kyber- ja digiturvaa toteutetaan paremmin kuin useimmissa muissa EU-valtioissa - uusi



Analyysi

51 % valmiusarvio on riittävä, mutta ei edes hyvä.

Vain 5 % antaa arvosanan erittäin hyvin. Suurin osa keskittyy arvoon 3 (46 %), mikä viestii koetusta perusvalmiudesta, mutta huipputason (ennakointi, varautumisharjoitukset, palautumiskyky) kuilu näkyy.

Kokonaisjakauma jakautuu lähes tasan. "Hyvin" -vastauksen antoi 51 % ja "Huonosti" -vastauksen 49 %. Tämä kertoo jakautuneesta kokemuksesta. Pienikin negatiivinen uutisvirta voi vaikuttaa kokonaiskuvaan.

Suomen suhteellinen asema nähdään selvästi positiivisena. 67 % koki, että Suomessa kyber- ja digiturvaa toteutetaan paremmin kuin useimmissa EU-maissa. Vain 15 % oli eri mieltä. Nettosaldo + 52 prosenttiyksikköä on vahva.

18 % "en osaa sanoa" -vastauksia paljastaa tietovajeen. Kaikilla ei ole näkyvyyttä vertailukelpoisiin mittareihin, tai he eivät ole ajatelleet asiaa.

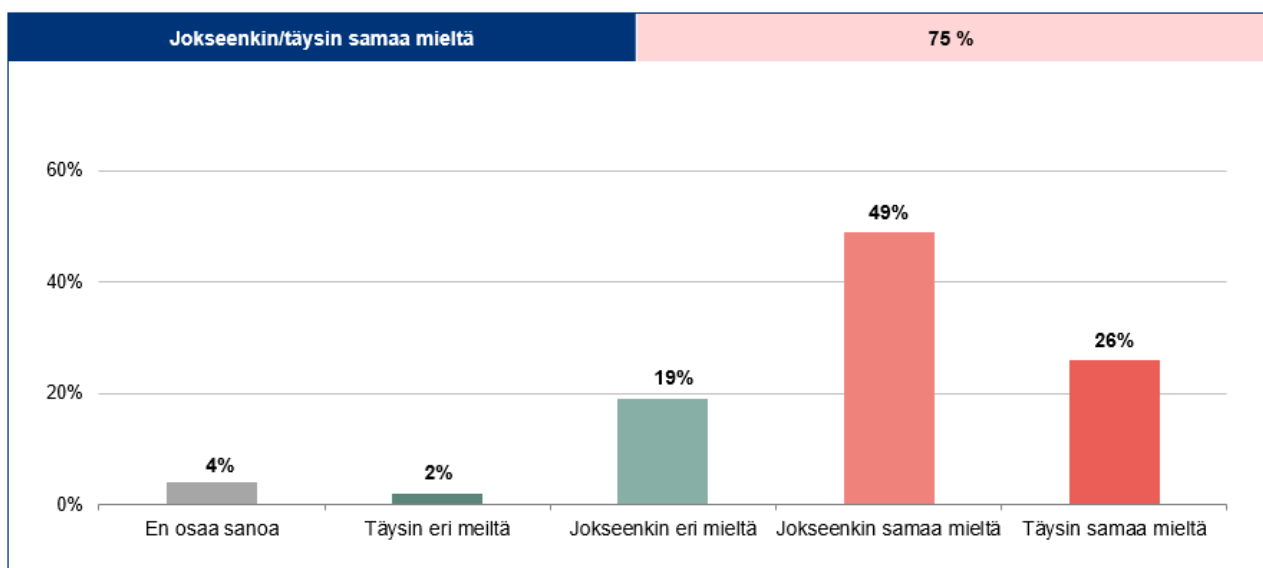
Havainnot

6.10.2025

Luottamuksen ja valmiuden välillä on jännite. Ihmiset ajattelevat Suomen pärjäävän suhteellisesti hyvin, mutta absoluuttinen varmuus puuttuu (vain 5 % vastasi “erittäin hyvin”). Suomen ajatellaan olevan muita edellä, mutta ei omalla tavoitetasollamme.

Viestintä ratkaisee seuraavan pisteen. Kun puolet kokee valmiuden vain välttäväksi, läpinäkyvät todisteet ovat tehokkain keino siirtää vastaajia seuraavaan arvoon eli 3→4.

3.6.4 Olen huolissani henkilötietojeni väärinkäytöstä verkossa - uusi



Arvioi seuraavia väittämiä: Olen huolissani henkilötietojeni väärinkäytöstä verkossa

Asteikko: täysin eri mieltä, jokseenkin eri mieltä, jokseenkin samaa mieltä, täysin samaa mieltä, en osaa sanoa

Analyysi

Kolme neljästä (75 %) on vähintään jokseenkin huolissaan henkilötietojensa väärinkäytöstä. Kyse on laajasta ja korkean tason huolesta, ei marginaalisesta ilmiöstä.

Asiasta vallitsee vahva konsensus. Vain 21 % on eri mieltä. Nettosaldo on +54 prosenttiyksikköä.

4 % “en osaa sanoa” -vastauksia on pieni, mutta merkityksellinen ryhmä, joka usein jää ilman selkeitä ohjeita tai näkyvyyttä oman datan käsittelyyn.

Havainnot

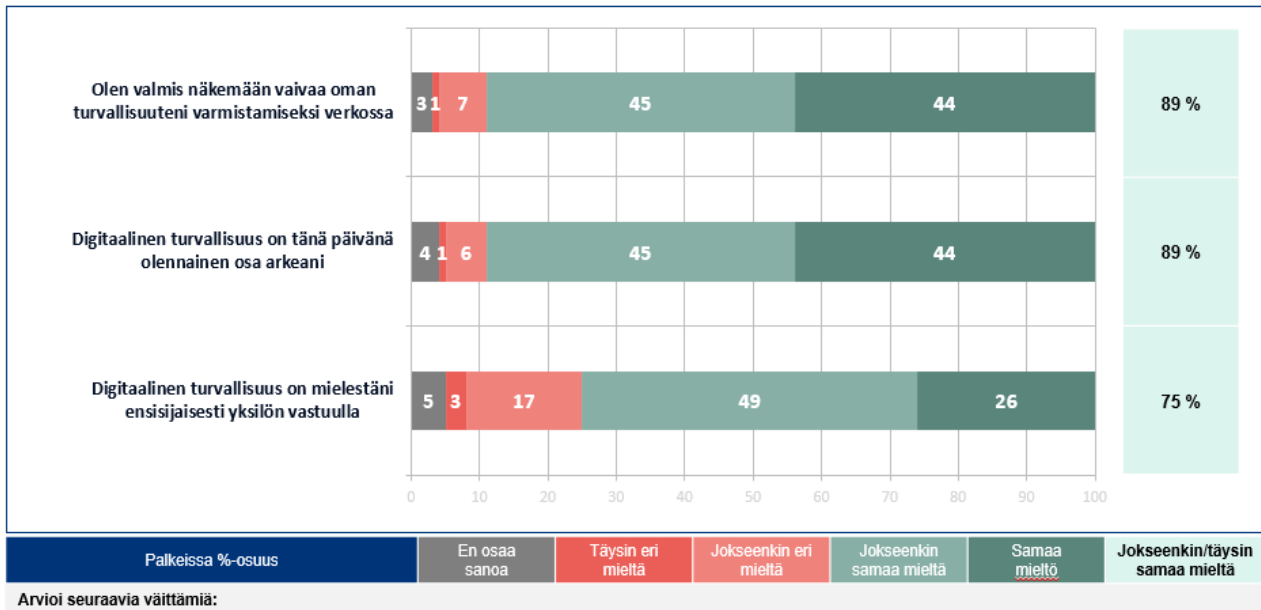
Tulokset ovat linjassa muun havaintoaineiston kanssa. Aiemmin nähty korkea altistuminen huijausviesteille sekä jatkuvat tietomurto uutiset rakentavat pysyvää riskitietoisuutta.

Huoli kohdistuu sekä valvontakykyyn (mitä dataa kerätään, mihin sitä käytetään) että toimijuuteen (kuinka helposti voi nähdä, hallita ja poistaa omia tietoja).

6.10.2025

Luottamuksen rakentuminen edellyttää todisteita, ei vain vakuutteluja. Tällaisia ovat läpinäkyvä lokitus, selkeät poistopolut, viestintä, EU-rajauksen kaltaiset kontrollit ja nopea reagointi poikkeamiin.

3.6.5 Suhtautuminen digiturvaan - uusi



Analyysi

Motivaatio on korkea. 89 % vastaajista on valmiita näkemään vaivaa oman verkkoturvallisuutensa eteen. Tämä on harvinaisen vahva signaali käyttäytymisen muutoksen mahdollistajille. Kun motivaatio on olemassa, on ratkaisevaa tehdä oikea teko helpoksi.

89 % kokee digitaalisen turvallisuuden olennaiseksi osaksi arkea. Turvallisuus ei ole erillinen kurssi, vaan osa jokapäiväisiä valintoja (kirjautuminen, maksaminen, viestintä).

Vastuukäsitys on jaettu, ei yksioikoinen. 75 % näkee digiturvan ensisijaisesti yksilön vastuuna, mutta samalla viidennes (20 %) on vähintään jokseenkin eri mieltä. Tämä kertoo, että kansalaiset odottavat paljon myös palveluntarjoajilta ja viranomaisilta.

Havainnot

Sanoista tekoihin siirtyminen on seuraava haaste. Korkea valmius ei automaattisesti muutu teoiksi. Sama aineisto osoitti aiemmin mm., että kolmannes ei ole vielä parantanut kortti- ja tiliturvaansa ja 39 % kierrättää salasanoja. Motivaatio on kunnossa, mutta asioita ei kuitenkaan toteuteta turvallisesti. "Yksilö ensin" -asenne ei saa johtaa "yksin vastuussa" -tilaan. 25 % ei näe vastuuta ensisijaisesti yksilöllä, ja



6.10.2025

he odottavat oletusturvaa ja selkeää ohjausta. Tämä on järkevää, sillä järjestelmätason suojat kompensoivat inhimillisiä erehdyksiä.

Operatiivinen viesti kannattaa rakentaa toiminnaksi. Tarvitaan selkeitä toimintaohjeita, joilla voidaan myös pienentää mahdollisia pelkoja ja ylläpitää arkimotivaatiota.

3.6.6 Suhtautuminen tekoälyyn - uusi

2024	2025		18-24 vuotta	25-34 vuotta	35-49 vuotta	50-64 vuotta	65-74 vuotta	75-99 vuotta
TEKOÄLYPALVELUIDEN KÄYTÖN LAAJUUS								
55 %	39 %	ei ole käyttänyt lainkaan tekoälypalveluita	17 %	24 %	26 %	42 %	68 %	63 %
20 %	31 %	käyttää tekoälypalveluita kuukausittain tai useammin	49 %	43 %	38 %	28 %	11 %	15 %
TEKOÄLYYN LIITTYVÄ OSAAMINEN JA TIETÄMYS								
27 %	36 %	on saanut melko/erittäin paljon tietoa tekoälyn turvallisesta hyödyntämisestä	60 %	47 %	44 %	30 %	23 %	17 %
LUOTTAMUS TEKÖÄLYPALVELUIDEN TURVALLISUUTEEN JA SISÄLTÖÖN								
59 %	63 %	tekoälypalveluiden nopea kehittyminen huolestuttaa melko/erittäin paljon	59 %	56 %	58 %	66 %	72 %	65 %
22 %	20 %	luottaa melko/erittäin paljon, että tekoälypalvelut käsittelevät omia tietoja turvallisesti	26 %	23 %	25 %	20 %	14 %	13 %
32 %	34 %	ei luota lainkaan siihen, että tekoälypalvelut käsittelevät omia tietoja turvallisesti	23 %	33 %	28 %	32 %	47 %	40 %
19 %	21 %	luottaa melko/erittäin paljon tekoälypalveluiden tuottamaan sisältöön	31 %	27 %	27 %	18 %	14 %	12 %
30 %	30 %	ei luota lainkaan tekoälypalveluiden tuottamaan sisältöön	16 %	31 %	23 %	30 %	42 %	41 %

Tekoälypalveluilla viitataan tässä esimerkiksi: esim. Open Ai ChatGPT, Microsoft CoPilot, Google Gemini

Tähän taulukkoon on koottu keskitetysti kaikki digiturvabarometrissä mukana olevat tekoälyyn liittyvät kysymykset. Tämä on tehty siksi, että tekoälyn merkitys tulee säilymään sekä kasvamaan lähivuosien aikana.

Tekoälyn käyttö laajenee nopeasti, mutta jakautuu kahtia

Tekoälyä käyttämättömien osuus pieneni 16 prosenttiyksikköä ja säännöllinen käyttö kasvoi 11 prosenttiyksikköä. 39 % ei käytä tekoälyä lainkaan. Syntyy kahtia jakautunut AI-arki: vahvistuva aktiivien joukko ja iso passiivisten joukko.

Säännöllinen käyttö oli korkeinta 18–24-vuotiailla (49 %) ja 25–34-vuotiailla (43 %). Se laski tasaisesti vanhemmissa ikäryhmissä (50–64-vuotiailla 28 %, 65–74-vuotiailla 11 %, 75–99-vuotiailla 15 %). Passiivisuus kasvoi jyrkästi 50+-vuotiaiden ikäryhmissä (ei käytä lainkaan: 42–68 %).

Tietous kasvaa, mutta ei kuro umpeen luottamuskilua

Turvallisen hyödyntämisen koulutusta tai tietoa “melko/erittäin paljon” saaneiden määrä nousi 36 prosenttiin (+ 9 prosenttiyksikköä). Luottamus datan käsittelyn turvallisuuteen pysyi kuitenkin matalana (20 %) ja jopa heikkeni. Tieto lisääntyy,





6.10.2025

mutta skeptisyys ei katoa. Tämä on rationaalista ottaen huomioon uutisoinnin tekoälyyn liittyvistä ilmiöistä ja ongelmista.

Tietoisuus on suurinta nuorilla (18–24-vuotiaat: 60 %) ja hiipuu vanhemmissa ikäryhmissä (75–99-vuotiaat: 17 %). Tämä korreloi käytön kanssa.

Huoli kehitysvauhdista kasvaa

63 % kokee tekoälyn nopean kehityksen huolestuttavaksi (+4 prosenttiyksikköä). Huoli on selvästi suurempi iäkkäämmissä ryhmissä (50–64-vuotiaat: 66 %, 65–74-vuotiaat: 72 %, 75–99-vuotiaat: 65 %). Signaali on, että uudet kyvykkyudet (agenttitoiminnot, generointi työvälineissä) ylittävät vielä monen riskinsietorajan.

Luottamus dataan ja sisältöön

Luottamus datan käsittelyyn turvallisesti on matala ja laskeva. Nuorilla luottamusta oli enemmän (18–24-vuotiaat: 26 %), vanhemmilla selvästi vähemmän (65–74-vuotiaat: 14 %, 75–99-vuotiaat: 13 %). “Ei luota lainkaan” -vastausten määrä nousi vanhemmissa ikäryhmissä 23 % → 47 %.

Tekoälyn tuottaman sisällön luottamuksessa oli lievää nousua 19 % → 21 %, mutta 30 % ei luota lainkaan. Iän merkitys on voimakas: luottamus sisältöön 31 % (18–24-vuotiailla) → 12 % (75–99-vuotiailla). Ei-luottavat kasvavat nuorimmasta 18-24-vuotiaiden ikäryhmän 16 % → 42 % luottamuspulaan 65-74-vuotiaiden ikäryhmässä.

3.6.7 Yhteenveto tekoälystä: vertailu tekoälyn käytön mukaan - uusi

TEKOÄLYN KÄYTTÖ	Ei käytä Lainkaan 39 %	On vähän kokeillut 30 %	Kuukausittain tai useammin 31 %	KAIKKI VASTAAJAT
TEKOÄLYN KEHITTÄMISEEN LIITTYVÄ HUOLI				
Tekoälypalveluiden nopea kehittyminen huolestuttaa melko/erittäin paljon	70 %	62 %	53 %	63 %
LUOTTAMUS TEKÖÄLYN SISÄLTÖIHIN JA OMIEN TIETOJEN KÄSITTELYYN				
Luottaa melko/erittäin paljon, että tekoälypalvelut käsittelevät omia tietoja turvallisesti	9 %	18 %	37 %	20 %
Luottaa melko/erittäin paljon tekoälypalveluiden tuottamaan sisältöön	10 %	20 %	36 %	21 %

Tekoälypalveluilla viitataan tässä esimerkiksi: esim. Open Ai ChatGPT, Microsoft CoPilot, Google Gemini

Analyysi

Tekoälyn käyttö laskee huolta, mutta ei poista sitä. Huolestuneiden osuus putosi





6.10.2025

selvästi, kun siirryttiin ei-käyttäjistä (70 %) satunnaiskäyttäjiin (62 %) ja säännöllisiin käyttäjiin (53 %).

Säännöllisistä käyttäjistä puolet (53 %) on yhä huolissaan kehitysvauhdista. Tulkinta on, että käytön myötä pelko muuttuu konkreettiseksi varovaisuudeksi, mutta ei katoa kokonaan.

Luottamus kasvaa käytön myötä, mutta jää matalaksi kokonaisuudessa

Omien tietojen käsittelyyn luottaminen yli nelinkertaistui: 9 % (ei-käyttäjät) → 37 % (kuukausittain tai useammin käyttävät).

Sisältöön luottaminen liki kolminkertaistui: 10 % → 36 %.

Havainnot

Kokonaistaso on matala. Kaikkien vastaajien keskiarvot ovat 20–21 %. Tässä näkyy luottamuskuilu; käyttökokemus parantaa luottamusta, mutta suuri yleisö pysyy epäilevänä.

”Ei käytä” -vastauksen antaneilla (39 %) on korkea huolen ja hyvin matala luottamuksen taso. Tälle ryhmälle tekoäly näyttäytyi riskinä, ei hyötynä. Vähän kokeilleet (30 %) ovat siirtymävaiheessa. Huoli laski ja luottamus nousi, mutta kumpikaan ei ole vielä vahva. Kuukausittain tai useammin (31 %) käyttävät näkevät käytännön hyödyt. Luottamus kasvoi selvästi, mutta enemmistö on silti varovaisia.