DIGI- JA VÄESTÖTIETO-VIRASTO

Digitaalinen luottamus on kääntymässä parempaan suuntaan

– ensimmäistä kertaa barometrin historiassa

Digiturvabarometri 2026

Sisällysluettelo

Digiturvabarometri on Digi- ja väestötieto-viraston vuosittain tuottama digiturvallisuutta käsittelevä tutkimus.

Tutkimus on julkaistu vuodesta 2020 alkaen.

Tutkimuksen kohderyhmänä ovat Suomessa asuvat täysi-ikäiset henkilöt.

Vuoden 2026 kyselyyn vastasi 1 250 henkilöä heinäkuussa 2026.

LISÄTIETOJA

Kimmo Rousku
VAHTI-pääsihteeri, johtava erityisasiantuntija
etunimi.sukunimi@dvv.fi tai digiturva@dvv.fi
Puh. 0295 536 000 (vaihde)

Tiivistelmä

Digiturvabarometri 2026 osoittaa, että kansalaisten näkökulmasta digiturvallisuudessa on tapahtunut merkittävä käänne. Ensimmäistä kertaa barometrin historiassa useat keskeiset mittarit kehittyvät samaan aikaan myönteiseen suuntaan:

- luottamuksen pitkään jatkunut lasku on pysähtynyt,
- turvallisuuden tunne on vahvistunut ja
- kansalaiset ryhtyvät aiempaa useammin konkreettisiin suojatoimiin.

Muutos ei johdu siitä, että uhat olisivat väistyneet, vaan siitä, että suomalaisten kyky toimia niiden keskellä on parantunut.

Luottamus digipalvelujen ja -laitteiden turvallisuuteen on kääntynyt nousuun. Luottamusindeksi parani vuodessa seitsemän pistettä lukemaan −20 ja on jo lähellä vuoden 2023 tasoa. Luottamuksensa heikentyneeksi kokevien osuus laski 38 prosentista 29 prosenttiin.

Muutos on suurin vanhimmissa ikäryhmissä, joissa luottamus digipalvelujen ja -laitteiden turvallisuuteen on parantunut eniten: 65–74-vuotiailla indeksi nousi 22 pistettä ja 75–99-vuotiailla 18 pistettä.

Arkeaan digitaalisessa ympäristössä pitää turvallisena 86 prosenttia vastaajista, neljä prosenttiyksikköä enemmän kuin vuotta aiemmin.

Kotimaisuus on valttia

Tunnettuus ja kotimaisuus lisäävät luottamusta digitaaliseen maailmaan. Suomen digitaalista toimintaympäristöä pitää turvallisena 70 prosenttia, ja 54 prosenttia arvioi kyber- ja digiturvan toteutuvan täällä paremmin kuin useimmissa EU-maissa.

Viranomaisiin ja finanssialan toimijoihin luottaa tietojensa käsittelyssä 87 prosenttia. Ero kotimaisen ja ulkomaisen välillä on jyrkkä: kotimaisiin verkkokauppoihin luottaa 70 ja ulkomaisiin 20 prosenttia.

Suomessa myös luottamus viranomaisten tuottamaan sisältöön on vahva: 88 prosenttia vastaajista luottaa viranomaisten sisältöihin. Tämä luku on pysynyt samalla tasolla vuodesta 2023 saakka. Kotimaisiin uutismedioihin luottaa 66 prosenttia suomalaisista ja ulkomaisiin uutismedioihin 50 prosenttia.

Luottamus keskittyy toimijoihin, joiden vastuut ovat selkeät ja jotka koetaan osaksi suomalaista yhteiskuntaa.

Suomessa on vahva luottamus viranomaisten tuottamaan sisältöön.

Luottamus tekoälyyn laahaa käytön jäljessä

Tekoäly yleistyy nopeammin kuin siihen luotetaan. Vähintään kuukausittain tekoälyä käyttävien osuus on kasvanut kahdessa vuodessa 20 prosentista 47 prosenttiin ja päivittäiskäyttäjien 4 prosentista 16 prosenttiin. Käyttö ei enää painotu nuoriin.

Luottamus tekoälypalveluja kohtaan laahaa selvästi jäljessä: vain 23 prosenttia luottaa vahvasti tekoälypalvelujen tietoturvaan tai niiden tuottamaan sisältöön. Tekoälylukutaidosta onkin tulossa keskeinen digiturvataito.

Suomalaiset arvioivat oman digiturvaosaamisensa paremmaksi kuin mitä heidän käyttäytymisensä antaa odottaa.

Digiturvataitonsa arvioi hyviksi 89 prosenttia suomalaisista. Silti 12 prosenttia kirjautuisi verkkopankkiin puhelun aikana pankin edustajaksi esittäytyvän henkilön pyynnöstä, 6 prosenttia klikkaisi pankin tai viranomaisen nimissä lähetettyä kirjautumislinkkiä ja 22 prosenttia on vuoden aikana reagoinut johonkin, joka osoittautui huijausyritykseksi.

Kehityssuunta on kuitenkin oikea: useat osaamismittarit paranivat 6–8 prosenttiyksikköä ja 48 prosenttia on parantanut maksuvälineidensä turvallisuutta.

Tekoälylukutaidosta on tulossa keskeinen digiturvataito.

Huijaukset yleisiä, vaikutukset laskussa

Huijaukset ovat Suomessa yleisiä, mutta niiden vaikutus on pienenemässä. Digihuijauksen tai huijausyrityksen on kohdannut 81 prosenttia suomalaisista, joka viides kohtaa niitä vähintään viikoittain. Samalla vertailukelpoisten uhkamittareiden keskiarvo laski vuodessa 34 prosentista 30 prosenttiin.

Lasku näkyy kaikissa keskeisissä kanavissa – voimakkaimmin tekstiviesteissä. Tähän vaikuttaa muun muassa se, että Suomessa verkkorikollisten toimintaa on pystytty rajoittamaan teknisin keinoin laajalla viranomaisten ja elinkeinoelämän yhteistyöllä.

Finanssiala, teleoperaattorit ja viranomaiset ovat kehittäneet ratkaisuja, joilla voidaan esimerkiksi estää pääsyä rikollisten perustamille huijaussivustoille sekä vaikeuttaa SMS-tekstiviestien lähettäjätunnusten väärentämistä ja hyödyntämistä huijauksissa.

Vaikka huoli huijauksista on kasvanut, huijausten koetaan vaikuttavan omaan arkeen ja luottamukseen digimaailmaa kohtaan hieman aiempaa vähemmän. Tämä viittaa siihen, että suomalaisten digitaalinen kriisinkestävyys on vahvistumassa. Onnistuneiden huijausten hinta pysyy silti korkeana. Kymmenen prosenttia kertoo menettäneensä rahaa vuoden aikana – heistä 9 prosenttia yli tuhat euroa. Suuruusluokaltaan tämä tarkoittaa noin 450 000 henkilöä ja arviolta 128 miljoonan euron vuosittaisia menetyksiä pelkästään yksityishenkilöille. Lisäksi 30 prosenttia arvioi huijausten aiheuttavan merkittäviä taloudellisia huolia. Organisaatioiden kokemat vahingot tulevat tämän päälle.

Rahallisten menetysten lisäksi huijaukset tekevät ihmisistä varovaisempia ja heikentävät luottamusta digitaalisiin palveluihin.

Kymmenen prosenttia kertoo menettäneensä rahaa vuoden aikana – heistä 9 prosenttia yli tuhat euroa.

Ilmoitushalua pitää lisätä

Barometrin tulosten perusteella suomalaisilla on eniten parannettavaa digihuijauksista ilmoittamisessa.

Huijauksen tunnistaneista 43 prosenttia ei kerro asiasta kenellekään; palveluntarjoajalle asiasta ilmoittaa 17 prosenttia, pankille 12 prosenttia ja poliisille 7 prosenttia vastaajista. Rikokseen johtaneissa tapauksissakin 42 prosenttia jättää rikosilmoituksen tekemättä. Digihuijatuksi tulemista ei kuitenkaan pidä hävetä, sillä myös alan huippuammattilaiset tulevat huijatuksi ja menettävät rahaa.

Ilmoittamattomuus heikentää viranomaisten, pankkien ja operaattoreiden tilannekuvaa digihuijauksista ja hidastaa niiden torjuntaa.

Suomalaisten vahvuus ei ole huijausten vähäisyys vaan kasvava kyky toimia niiden keskellä.

Kansalaisten digiturvaosaaminen on parantunut, ja sen kehittämistä on tärkeää jatkaa. Turvallisuus ei kuitenkaan voi perustua siihen, että jokaisen käyttäjän pitäisi tunnistaa yhä uskottavammat ja teknisesti kehittyneemmät huijaukset. Seuraava kehitysaskel on vahvistaa turvallisuutta entisestään palvelujen rakenteissa, prosesseissa ja teknisissä suojauksissa. Käyttäjän pitäisi pystyä helposti varmistamaan yhteydenoton aitous, ilmoittamaan epäilyttävästä toiminnasta ja saada suojaa myös silloin, kun hän ei itse tunnista huijausta.

Samalla tarvitaan nykyistä saumattomampaa yhteistyötä ja selkeämpää vastuunjakoa viranomaisten, finanssialan, teleoperaattoreiden, digitaalisten alustojen ja palveluntarjoajien välillä. Tavoitteena on digiympäristö, jossa turvallinen toiminta on käyttäjälle helpoin ja oletusarvoinen vaihtoehto.

Turvallisuuden on toimittava
myös silloin, kun ihminen erehtyy.

Tutkimuksen toteutus ja käyttö

Digi- ja väestötietoviraston Digiturvabarometri-tutkimuksella selvitetään täysi-ikäisten suomalaisten kyber- ja digiturvaosaamista, asenteita sekä kokemuksia digitaalisen toimintaympäristön turvallisuudesta.

Tavoitteena on muodostaa kokonaiskuva siitä, miten suomalaiset käyttävät digitaalisia palveluja, millaiseksi he kokevat oman osaamisensa ja turvallisuutensa sekä miten he suhtautuvat digitaalisen maailman ajankohtaisiin ilmiöihin ja uhkiin.

Digiturvabarometria on toteutettu vuodesta 2020 lähtien. Tutkimuksen konsepti uudistettiin syksyllä 2022, jolloin tutkimuksen toteuttajaksi valittiin tutkimustoimisto Vastakaiku Oy. Tutkimusaineisto kerätään Bilendi Oy:n ylläpitämän M3-paneelin avulla.

Tämä raportti käsittelee Digiturvabarometrin tuloksia vuodelta 2026. Näitä tuloksia verrataan osin aikaisempiin Digibarometrien tuloksiin vuosilta 2023–2025.

Tutkimuksen kohderyhmänä ovat Suomessa asuvat täysi-ikäiset henkilöt. Vuoden 2026 kyselyyn vastasi 1 250 henkilöä heinäkuussa 2026. Tulokset on painotettu siten, että aineisto muodostaa valtakunnallisesti edustavan otoksen sukupuolen, iän ja asuinalueen mukaan. Vuoden 2026 tutkimuksen virhemarginaali on noin ±3,0 prosenttiyksikköä 95 prosentin luottamustasolla.

Tutkimuksen avulla voidaan tarkastella muun muassa sitä, kuinka merkittävä osa digitaalinen maailma on suomalaisten arkea ja kuinka aktiivisesti erilaisia digipalveluja ja -laitteita käytetään. Barometri tuottaa tietoa myös kansalaisten tekoälyn käytöstä ja siihen liittyvästä luottamuksesta sekä siitä, millaiseksi suomalaiset arvioivat kyber- ja digiturvallisuuden tilanteen Suomessa.

Tutkimuksessa tarkastellaan lisäksi suomalaisten omaa arviota digiturvaosaamisestaan, heidän kokemaansa turvallisuuden tunnetta arjessa sekä heidän kohtaamiaan digitaalisia uhkia. Samalla selvitetään, kuinka paljon suomalaiset luottavat eri toimijoihin ja digitaalisiin palveluihin henkilötietojen ja muiden tärkeiden tietojen turvallisessa käsittelyssä.

Vuonna 2026 tutkimukseen on myös lisätty uusia kysymyksiä, joilla voidaan verrata esimerkiksi Suomen sijoittumista kansainvälisesti.

Raportin loppuosassa listaamme digikäyttäjille kymmenen ohjetta siitä, miten voi välttää digihuijauksia ja miten toimia, jos joutuu huijatuksi. Lisäksi listaamme suosituksia organisaatioille ja järjestöille turvallisuuden lisäämiseksi digipalveluissa ja -asioinnissa.

Digi- ja väestötietovirasto hyödyntää Digiturvabarometrin tuloksia kyber- ja digitaalisen turvallisuuden kehittämisessä, Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) toiminnassa sekä viraston omissa hankkeissa ja palveluissa.

Barometrin pitkittäisaineisto mahdollistaa myös digiturvallisuuteen liittyvien asenteiden, osaamisen, käyttäytymisen ja luottamuksen muutosten seuraamisen vuodesta toiseen.

Lisätietoa VAHTI-toiminnasta
https://dvv.fi/vahti

Ylläpidämme ja kehitämme myös kansalaisia varten **Henkilötietojani on viety tai vuotanut** -opasta
https://www.suomi.fi/oppaat/tietovuoto

Luottamus digimaailmaan vahvistuu

Vuoden 2026 Digiturvabarometrin merkittävin viesti on positiivinen muutos. Ensimmäistä kertaa barometrin historiassa useat tärkeät mittarit ovat kääntyneet samanaikaisesti parempaan suuntaan. Luottamus digitaaliseen maailmaan ei enää heikkene kuten edellisinä vuosina, vaan turvallisuuden tunne on vahvistunut, ja suomalaiset ovat ryhtyneet aiempaa useammin konkreettisiin toimiin oman turvallisuutensa parantamiseksi.

Luottamus on saatu kääntymään parempaan suuntaan, mutta vielä on paljon kehitettävää.

Digihuijauksen vahingot voivat olla merkittäviä ja vaikuttaa uhrin talouteen haitallisesti.

Organisaatioiden tulisi kehittää ja harjoitella digihuijausten käsittelyyn liittyvän prosessin toimintaa.

Digipalvelut- ja laitteet nostivat luottamusta

Selkein muutos näkyy luottamuksessa digipalvelujen ja -laitteiden turvallisuuteen.

Luottamusindeksi parani vuodesta 2025 vuoteen 2026 seitsemän pistettä: lukemasta −27 lukemaan −20. Indeksi muodostuu luottamuksensa vahvistuneeksi ja heikentyneeksi kokevien erotuksesta.

Luottamuksensa heikentyneeksi tuntevien osuus laski 38 prosentista 29 prosenttiin. 62 prosenttia kertoo luottamuksensa pysyneen ennallaan ja 9 prosenttia vahvistuneen.

Vuoden 2026 tulos on jo hyvin lähellä vuoden 2023 tasoa, jolloin indeksi oli −19.

Vastaajat perustelevat luottamuksen vahvistumista suojauskeinojen, tunnistautumisen, valvonnan ja huijausten estämisen kehittymisellä, lisääntyneellä digiturvaviestinnällä sekä pankkien, operaattoreiden ja viranomaisten toimilla. Myös oman osaamisen ja varovaisuuden nähdään lisääntyneen.

Luottamusta heikentävät puolestaan huijausten määrän ja uskottavuuden kasvu, tekoälyn mahdollistamat entistä kehittyneemmät huijaukset sekä kokemus siitä, että vastuu turvallisuudesta jää paljon käyttäjälle itselleen.

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

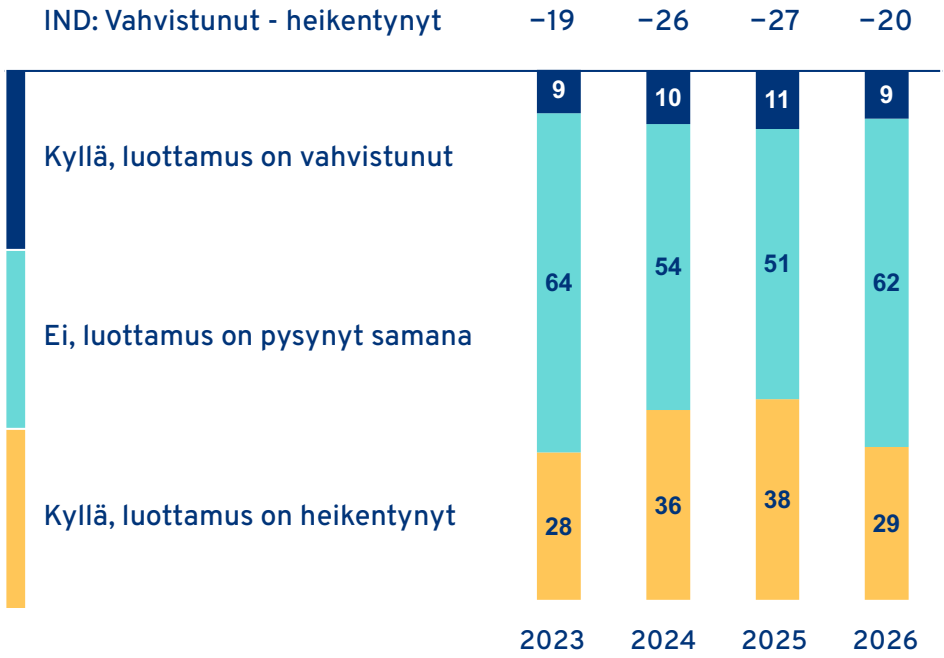
+7

Luottamusindeksi on kahden vuoden pudotuksen jälkeen kääntynyt nousuun.

Vuonna 2026 lähes kaksikolmasosaa (62 %) kokee, että luottamus on pysynyt samana, kun se oli vuonna 2025 vain noin puolet (51 %).

29 %

Arvioi luottamuksen heikentyneen viime vuodesta, kun vuonna 2025 vastaava luku oli 38 %.



Vuosien 2023 ja 2024 välillä luottamus heikkeni voimakkaasti. Asiaa voi osaltaan selittää keväällä 2024 laajasti julkisuutta saanut tietomurto, joka kohdistui Helsingin kaupungin kasvatuksen ja koulutuksen toimialaan. Barometriaineisto ei kuitenkaan itsessään osoita syy-yhteyttä yksittäisen tapahtuman ja luottamuksen muutoksen välillä.

	Luottamusindeksi	Muutos edelliseen vuoteen
2023	−19	
2024	−26	−7
2025	−27	−1
2026	−20	+7

Suuri muutos vanhimmissa ikäryhmissä

Luottamus digipalvelujen ja -laitteiden turvallisuuteen on kasvanut erityisesti 25–34-vuotiaiden ja yli 64-vuotiaiden keskuudessa. Esimerkiksi 65–74-vuotiaiden luottamusindeksi nousi vuodessa lukemasta −42 lukemaan −20 eli 22 pistettä ja 75–99-vuotiaiden luottamusindeksi lukemasta −49 lukemaan −31 eli 18 pistettä.

86 prosenttia suomalaisista pitää päivittäistä toimintaansa digitaalisessa toimintaympäristössä melko tai erittäin turvallisena. Tämä on neljä prosenttiyksikköä enemmän kuin vuotta aiemmin. Turvattomaksi toimintansa kokee 10 prosenttia.

18–24-vuotiaiden keskuudessa turvallisuuden tunne kasvoi vuodessa kahdeksan prosenttiyksikköä ja 75–99-vuotiaiden keskuudessa yhdeksän prosenttiyksikköä.

Miten turvalliseksi tunnet päivittäisen toiminnan digitaalisessa toimintaympäristössä?

86 %

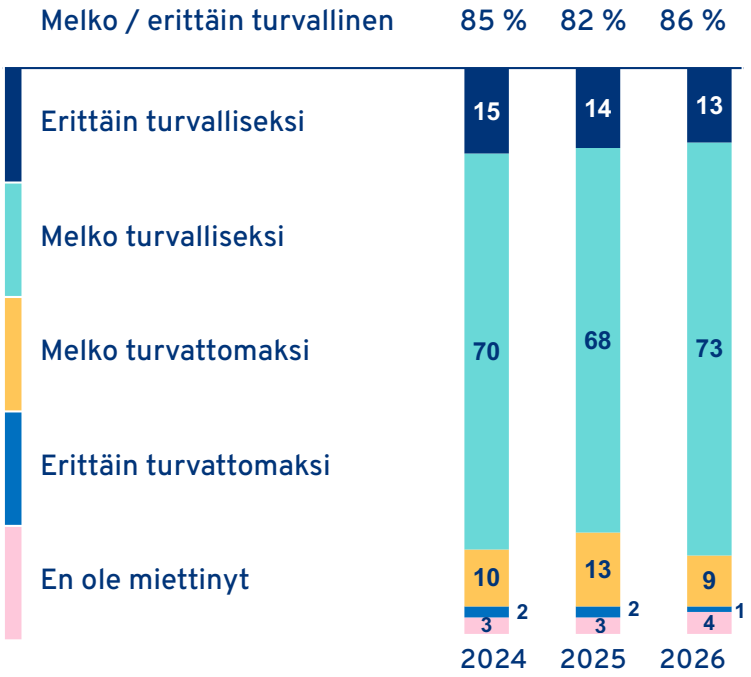
Tuntee päivittäisen toiminnan digitaalisessa toimintaympäristössä melko tai erittäin turvalliseksi.

+4 % vs. 2025

+1 % vs. 2024

10 %

Kokee päivittäisen toiminnan digitaalisessa toimintaympäristössä melko tai erittäin turvattomaksi.



Kivijalkana viranomaiset, finanssiala ja kotimaisuus

Vuonna 2026 barometriin otettiin mukaan uusia kysymyksiä, joihin saadut vastaukset vahvistavat kuvaa Suomesta turvallisena digitaalisena yhteiskuntana.

70 prosenttia vastaajista pitää Suomen digitaalista toimintaympäristöä turvallisena, ja vain 3 prosenttia on asiasta täysin eri mieltä. Lisäksi 54 prosenttia arvioi, että Suomessa kyber- ja digiturvaa toteutetaan paremmin kuin useimmissa muissa EU-maissa. Väitteestä on eri mieltä 17 prosenttia, mutta lähes kolmannes ei osaa ottaa siihen kantaa. Tämä kertoo osin kysymyksen haastavuudesta.

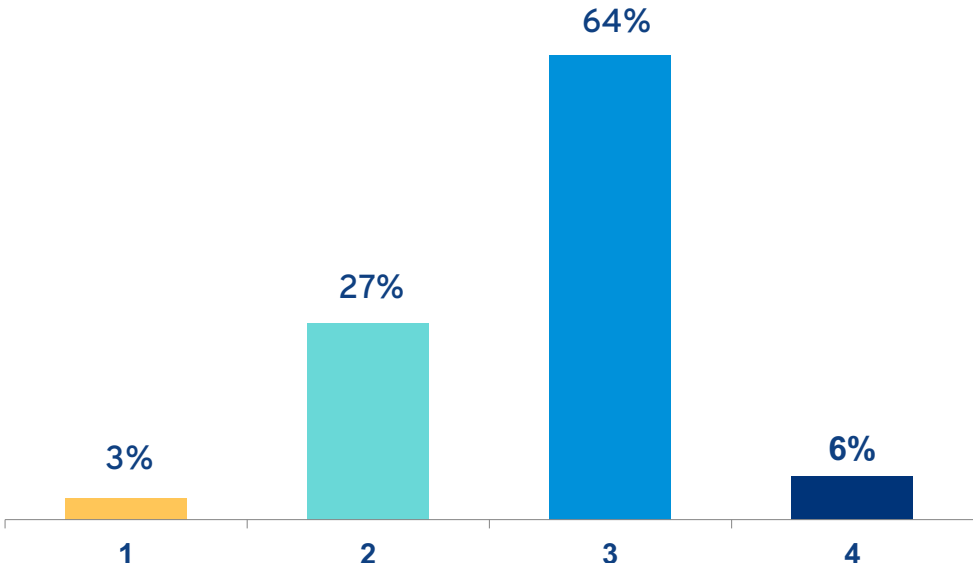
Kuinka turvalliseksi tunnet tällä hetkellä digitaalisen toimintaympäristön Suomessa?

70 %

Yli kaksi kolmasosaa (70 %) kokee tällä hetkellä digitaalisen toimintaympäristön Suomessa turvalliseksi (arviot 3–4).

30 %

Vajaa kolmasosa (30 %) ei koe digitaalista toimintaympäristöä turvalliseksi (1–2). Ääripään vastauksia ”En lainkaan turvalliseksi” on vain 3 %.



Asteikolla 1–4, jossa 1=en lainkaan turvalliseksi ja 4=erittäin turvalliseksi

Luottamus yhteiskunnan keskeisiin toimijoihin on erityisen vahvaa.

Finanssialan toimijoihin ja viranomaisiin luottaa henkilötietojen ja muiden tärkeiden tietojen turvallisessa käsittelyssä 87 prosenttia suomalaisista. Molempien tulos on pysynyt samalla korkealla tasolla kuin vuotta aiemmin. Työnantajaansa luottaa 81 prosenttia vastaajista.

Suomessa luotetaan yhteiskunnan instituutioihin ja kotimaisiin toimijoihin.

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

87 %

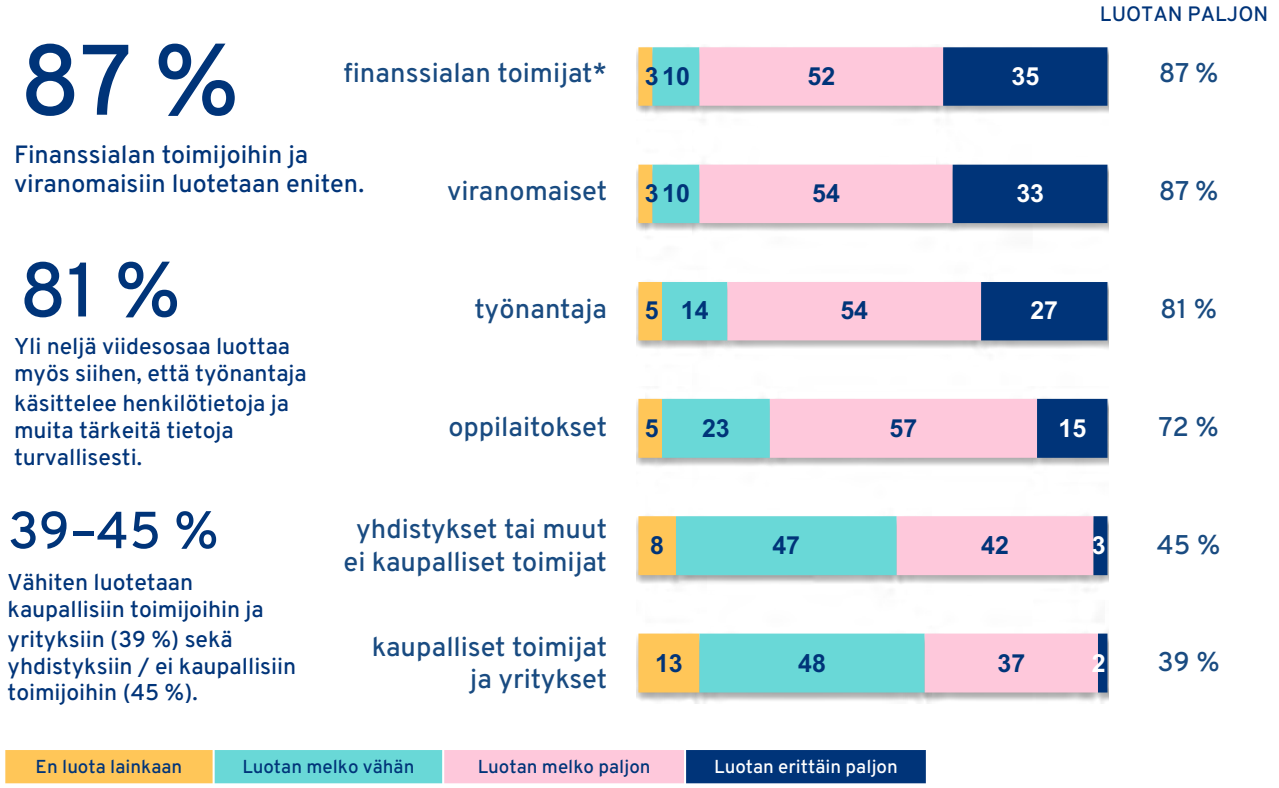
Finanssialan toimijoihin ja viranomaisiin luotetaan eniten.

81 %

Yli neljä viidesosaa luottaa myös siihen, että työnantaja käsittelee henkilötietoja ja muita tärkeitä tietoja turvallisesti.

39–45 %

Vähiten luotetaan kaupallisiin toimijoihin ja yrityksiin (39 %) sekä yhdistyksiin / ei kaupallisiin toimijoihin (45 %).



*finanssialan palvelut (pankki-, maksu- ja vakuutuspalvelut)

Kotimaisiin verkkokauppoihin ja sisältöihin luotetaan

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

82 %

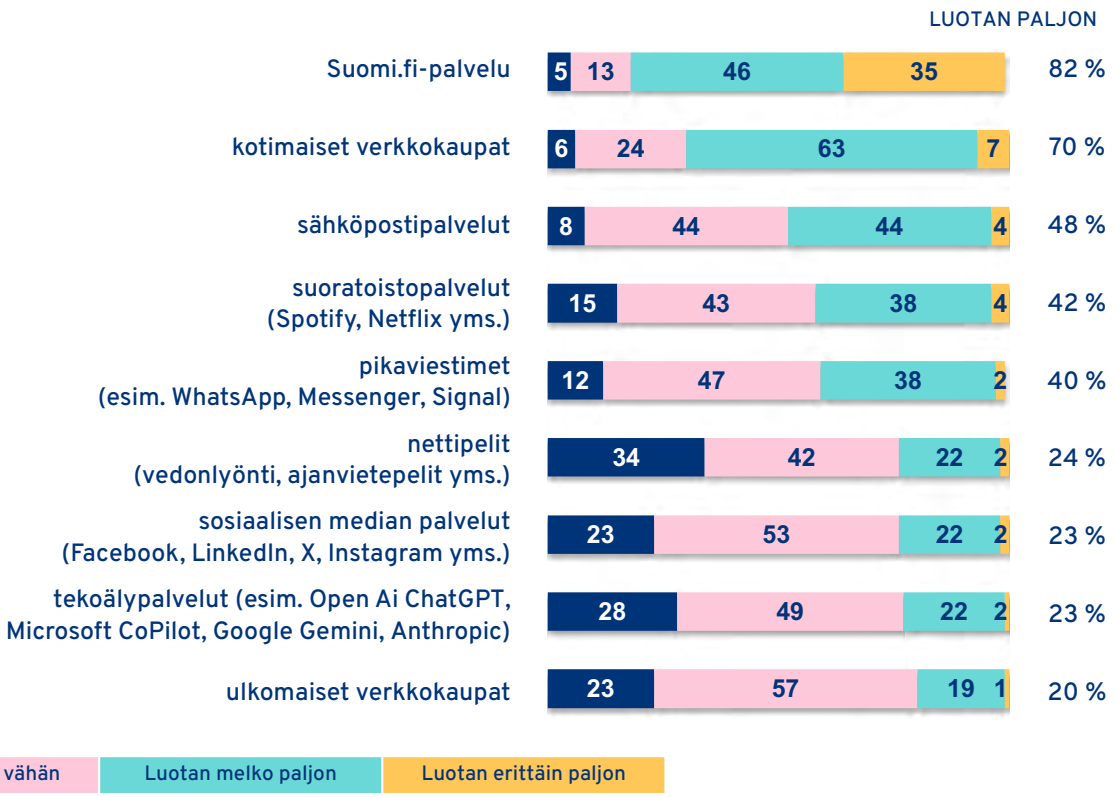
Suomi.fi-palveluun luotetaan eniten.

70 % vs 20 %

Yli kaksi kolmasosaa luottaa paljon kotimaisten verkkokauppojen henkilötietojen käsittelyyn, kun taas vain joka viides luottaa paljon ulkomaisiin verkkokauppoihin.

23 %

Sosiaalisen median palveluihin ja tekoälypalveluihin luottaa vain reilu neljäsosa.



Myös kotimaisuus näyttää lisäävän luottamusta. Uutena kysymyksenä kysyimme luottamuksesta Suomi.fi-palvelua kohtaan. Vastaajista 82 prosenttia luottaa Suomi.fi-palveluun paljon. Kotimaisiin verkkokauppoihin puolestaan luottaa 70 prosenttia ja ulkomaisiin verkkokauppoihin vain 20 prosenttia vastaajista.

Verkkokauppoihin liittyvä luottamus on kuitenkin laskenut: kotimaisissa kaupoissa 75 prosentista 70 prosenttiin ja ulkomaisissa 23 prosentista 20 prosenttiin. Syynä ovat todennäköisesti vale-verkkokauppoihin ja muut maksamiseen liittyvät huijaukset.

Huomionarvoista on, että samaan aikaan vale-verkkokaupassa rahaa menettäneiden osuus on pienentynyt 10 prosentista 7 prosenttiin. Luottamus on siis laskenut, vaikka huijausten kokonaismäärä on vähentynyt.

Kotimaisuuden merkitys näkyy myös sisällöissä. 88 prosenttia suomalaisista luottaa paljon viranomaisten tuottamaan sisältöön, täsmälleen yhtä moni kuin vuotta aiemmin. Tunnettuihin kotimaisiin uutismedioihin luottaa 66 prosenttia, kun vastaava osuus tunnetuissa ulkomaisissa uutismedioissa on 50 prosenttia.

Kokonaisuutena luottamus digitaaliseen maailmaan ei siis jakaudu tasaisesti. Luottamus on voimakkainta siellä, missä toimija tunnetaan, sen vastuut ovat selkeät ja se koetaan osaksi suomalaista yhteiskuntaa.

Kuinka moni suomalainen luottaa paljon seuraavien tahojen tai palvelujen tuottamaan sisältöön?

	2023	2024	2025	2026
viranomaiset	88 %	89 %	88 %	88 %
tunnetut kotimaiset uutismediat (YLE, HS, Iltalehti yms.)	67 %	69 %	69 %	66 %
yritykset	61 %	64 %	65 %	59 %
tunnetut ulkomaiset uutismediat (Reuters, BBC, New York Times yms.)	54 %	57 %	55 %	50 %
yhdistykset tai muut ei kaupalliset toimijat	52 %	55 %	54 %	48 %
tekoälypalvelut (esim. Open Ai ChatGPT, Microsoft CoPilot, Google Gemini, Anthropic)	15 %	19 %	21 %	23 %
sosiaalisen median palvelut (Facebook, LinkedIn, X, Instagram yms.)	20 %	24 %	25 %	21 %

Sosiaalisen median sisällöt ovat pudonneet vähiten luotetuksi sisällöksi.

Tekoälyn käyttö kasvaa luottamusta nopeammin

Tekoälypalvelujen käyttöönotto on yksi barometrin voimakkaimmista muutoksista.

Kun tekoälystä kysyttiin ensimmäisen kerran vuonna 2024, suomalaisista 20 prosenttia käytti tekoälyä vähintään kuukausittain. Vuonna 2025 osuus oli 31 prosenttia ja vuonna 2026 jo 47 prosenttia. Tekoälypalvelujen säännöllinen käyttö on siis yli kaksinkertaistunut kahdessa vuodessa.

Päivittäin tai lähes päivittäin tekoälyä käyttävien osuus on noussut kahdessa vuodessa 4 prosentista 16 prosenttiin.

Tekoälyn säännöllinen käyttö on yli kaksinkertaistunut kahdessa vuodessa.

Yhteenveto tekoälystä

2024	2025	2026		18–24 vuotta	25–34 vuotta	35–49 vuotta	50–64 vuotta	65–74 vuotta	75–99 vuotta
TEKOÄLYPALVELUJEN KÄYTÖN LAAJUUS									
55 %	39 %	27 %	ei ole käyttänyt lainkaan tekoälypalveluja	10 %	18 %	15 %	26 %	42 %	56 %
20 %	31 %	47 %	käyttää tekoälypalveluja kuukausittain tai useammin	66 %	59 %	59 %	43 %	31 %	26 %
TEKOÄLYYN LIITTYVÄ OSAAMINEN JA TIETÄMYS									
27 %	36 %	38 %	on saanut melko/erittäin paljon tietoa tekoälyn turvallisesta hyödyntämisestä	62 %	49 %	43 %	32 %	27 %	20 %
LUOTTAMUS TEKOÄLYPALVELUJEN TURVALLISUUTEEN JA SISÄLTÖÖN									
22 %	20 %	23 %	luottaa melko/erittäin paljon, että tekoälypalvelut käsittelevät omia tietoja turvallisesti	24 %	32 %	23 %	20 %	23 %	20 %
19 %	21 %	23 %	luottaa melko/erittäin paljon tekoälypalvelujen tuottamaan sisältöön	28 %	26 %	23 %	22 %	20 %	15 %

Tekoälypalvelut (esim. Open Ai ChatGPT, Microsoft CoPilot, Google Gemini, Anthropic)

Samalla tekoälyä kokonaan käyttämättömien osuus on pudonnut 55 prosentista 27 prosenttiin. Kasvu ei enää rajoitu nuoriin. Kuukausittain tai useammin tekoälyä käyttää 66 prosenttia 18–24-vuotiaista, 59 prosenttia 25–49-vuotiaista, 43 prosenttia 50–64-vuotiaista, 31 prosenttia 65–74-vuotiaista ja jo 26 prosenttia 75–99-vuotiaista. Vuodessa suurimmat muutokset näkyvät 35–49-vuotiaiden sekä 65–74-vuotiaiden keskuudessa.

Tekoälysisällöt somea luotettavampia

Luottamus tekoälyyn kasvaa kuitenkin huomattavasti käyttöä hitaammin. Vain 23 prosenttia luottaa paljon siihen, että tekoälypalvelut käsittelevät henkilötietoja ja muita tärkeitä tietoja turvallisesti. Vuotta aiemmin osuus oli 20 prosenttia. Samoin vain 23 prosenttia suomalaisista luottaa paljon tekoälyn tuottamaan sisältöön.

Tekoälyn tuottamaan sisältöön luotetaan nyt kuitenkin enemmän kuin sosiaalisen median sisältöön, johon luottaa paljon 21 prosenttia vastaajista. Luottamus tekoälyn tuottamaan sisältöön nousi vuodessa kaksi prosenttiyksikköä, kun taas luottamus sosiaalisen median sisältöön laski neljä prosenttiyksikköä.

Vuoden 2026 kuva onkin kaksijakoinen: tekoälyn hyödyntämisestä tulee nopeasti normaalia, mutta luottamus siihen ei kasva samaa tahtia. Tämä nostaa tekoälyn lukutaidon ja turvallisen hyödyntämisen yhdeksi lähivuosien keskeisistä digiturvataidoista.

Tekoälyn lukutaito ja turvallinen hyödyntäminen ovat lähivuosien keskeisiä digiturvataitoja.

Digipalveluita käytetään paljon ja niiden tärkeys on tunnistettu

Digipalvelut ovat vakiintuneet osaksi suomalaisten arkea, sillä 77 prosenttia pitää digipalveluja ja -sovelluksia tärkeinä. Tulos on pysynyt käytännössä samalla tasolla jo viiden vuoden ajan. Alle 35-vuotiailla merkitys on vuonna 2026 korkeimmillaan: 88–93 prosenttia pitää palveluja tärkeinä.

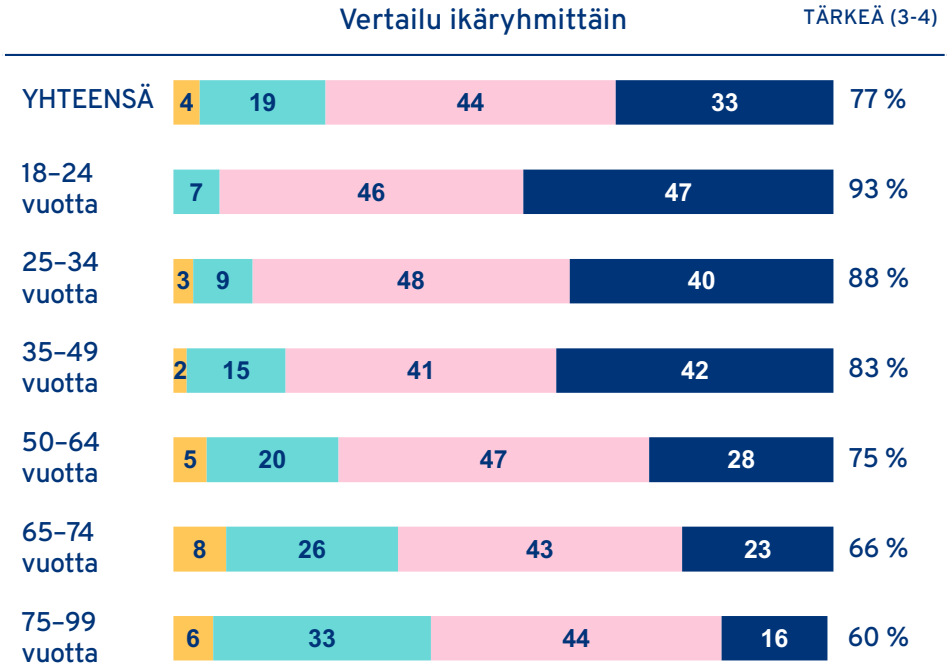
Kuinka tärkeäksi koet erilaiset digipalvelut ja -sovellukset omassa arjessasi?

77 %
Yli kolme neljäsosaa suomalaisista kokee erilaiset digipalvelut ja -sovellukset tärkeäksi (arviot 3–4) omassa arjessaan.

88–93 %
Alle 35-vuotiailla sama luku on noin 90 %.

75–83 %
35-64-vuotiaista vähintään kolme neljäsosaa pitää digipalveluja ja -sovelluksia tärkeänä (3-4).

60–66 %
Yli 64-vuotiaistakin vähintään kolme viidesosaa arvioi samoin.



Myös digipalvelujen käyttö on runsasta. 72 prosenttia suomalaisista käyttää digipalveluja päivän aikana paljon, ja alle 50-vuotiaista jopa 81–91 prosenttia. Vanhimmassakin 75–99-vuotiaiden ryhmässä puolet käyttää digipalveluja paljon.

Minkä verran käytät erilaisia digipalveluita ja -sovelluksia tyypillisesti päivän aikana?

72 %

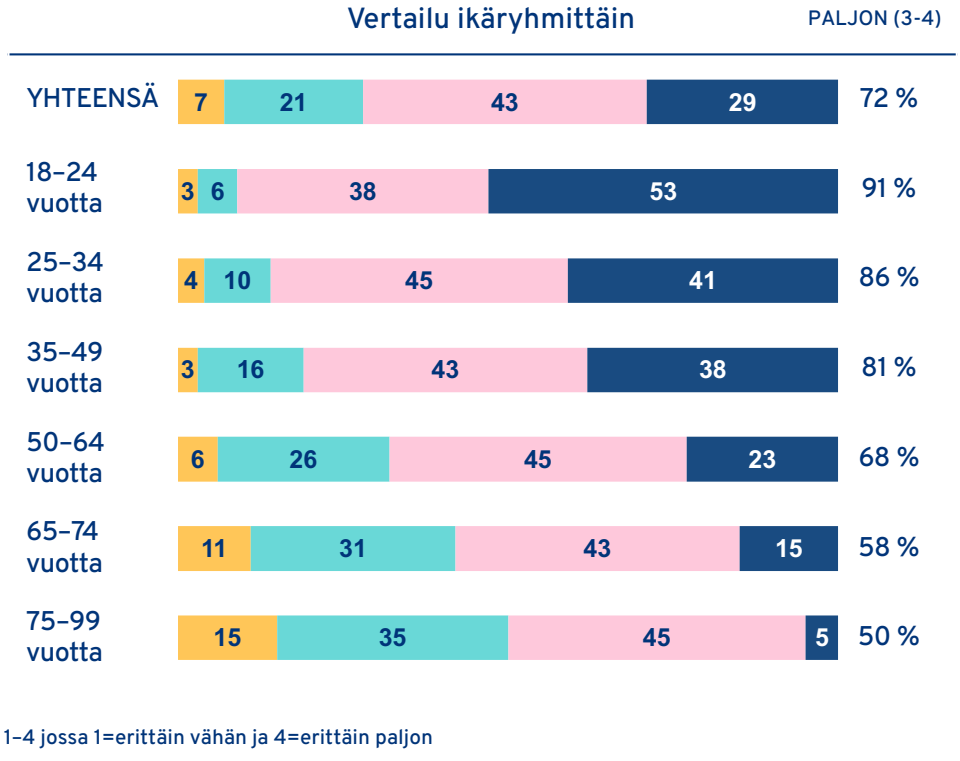
Lähes kolme neljäsosaa käyttää paljon (3–4) erilaisia digipalveluja ja -sovelluksia.

81–91 %

Alle 50-vuotiaista vähintään neljä viidesosaa käyttää digipalveluita ja -sovelluksia paljon.

50–68 %

50. ikävuoden jälkeen aktiivinen käyttö putoaa selvästi. Silti kaikissa ikäryhmissä, myös 75–99-vuotiaissa, vähintään puolet käyttävät digipalveluja ja -sovelluksia paljon.



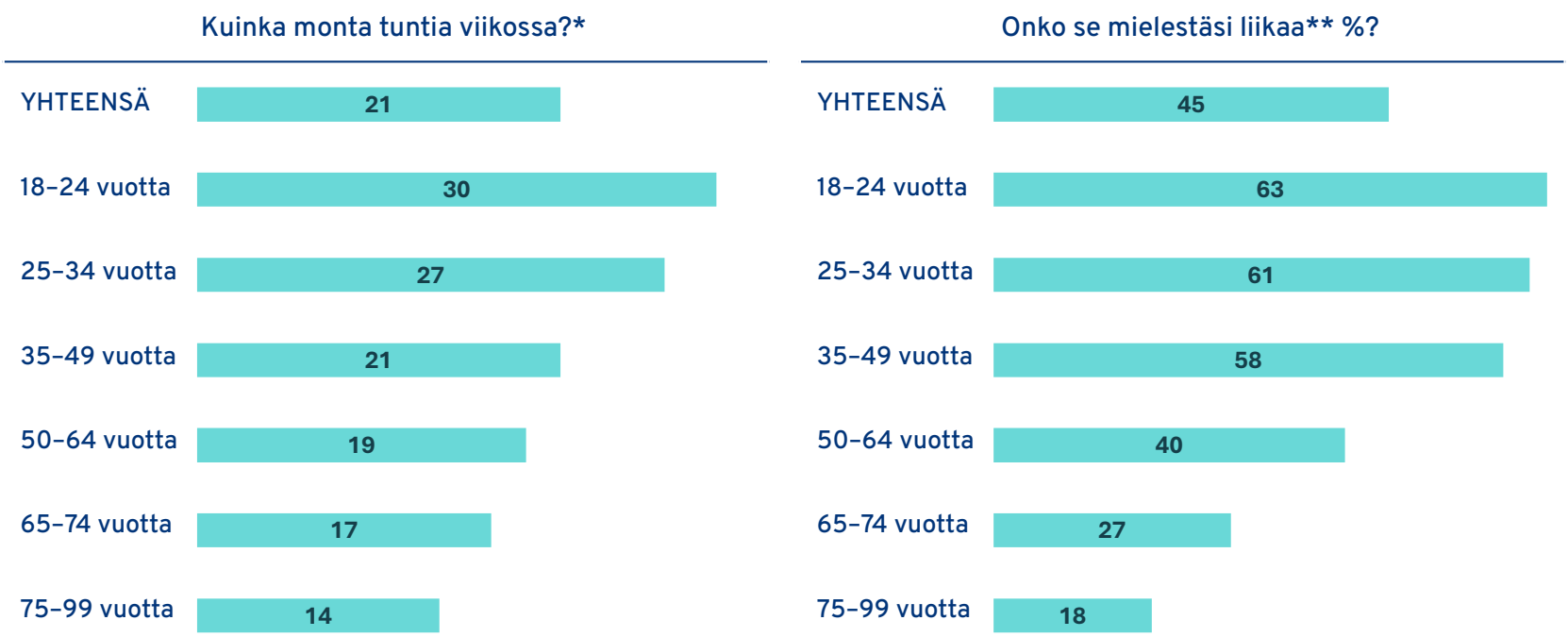
Suomalaisten keskimääräinen vapaa-ajan ruutuaika on 21 tuntia viikossa. Tämä on noin tunti enemmän kuin vuotta aiemmin. Alle 35-vuotiailla ruutuaikaa kertyy 27–30 tuntia viikossa. Vähiten aikaa ruudun ääressä viettävät 75–99-vuotiaat, mutta heilläkin määrä on 14 tuntia eli keskimäärin kaksi tuntia päivässä.

Ruutuaika tunnistetaan itsekin ongelmaksi. 45 prosenttia pitää omaa vapaa-ajan ruutuaikaansa liian suurena tai aivan liian suurena. Alle 50-vuotiaista näin ajattelee 58–63 prosenttia.

Digitaalisuus ei ole enää erillinen toimintaympäristö vaan merkittävä osa tavallista elämää. Samalla myös digiturvallisuudesta tulee yhä selvemmin osa arjen turvallisuutta.

45 % käyttää mielestään liikaa aikaa ruudun ääressä.

Viikoittainen ruutuaika ja sen määrän arviointi



*Asioihin, jotka eivät liity työsi hoitamiseen tai opintoihin (ns. vapaa-ajan ruutuaika)

**Kysymykseen on vastattu LIIKAA tai AIVAN LIIKAA

Oma näkemys turvataidoista ei vastaa todellisuutta

Peräti 89 prosenttia suomalaisista antaa itselleen arvion hyvä tai erittäin hyvä digipalvelujen ja -laitteiden turvallisessa käyttämisessä. Tulos on korkea, vaikka se on laskenut kahdella prosenttiyksiköllä kolmen lähes identtisen vuoden jälkeen.

Vanhimmassa ikäryhmässä 76 prosenttia kokee osaamisensa hyväksi, kun 35–49-vuotiaista näin kokee peräti 95 prosenttia.

Oma näkemys osaamisesta on kuitenkin osin ristiriidassa todellisen käyttäytymisen kanssa.

Kuinka hyvin osaat omasta mielestäsi käyttää turvallisesti digitaalisia palveluita* ja digilaitteita**?

89 %

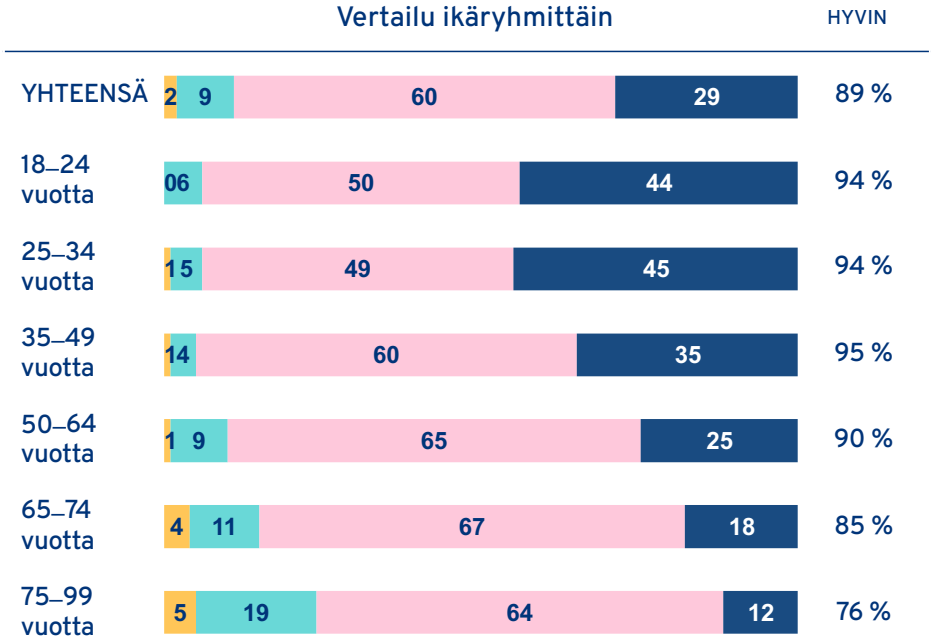
Suomalaisista arvioi osaamisensa hyväksi tai erittäin hyväksi digitaalisten palvelujen ja digilaitteiden turvallisessa käytössä.

29 %

arvioi oman osaamisensa erittäin hyväksi.

12 % / 45 %

18–34-vuotiaista 44–45 % arvioi osaamisensa erittäin hyväksi, kun taas yli 64-vuotiailla luvut ovat 12–18 %.



*esim. verkkopankki, viranomaispalvelut, suoratoistopalvelut
**esim. tietokone, älypuhelin, tabletti, älytelevisio, älykello/aktiivisuusranneke

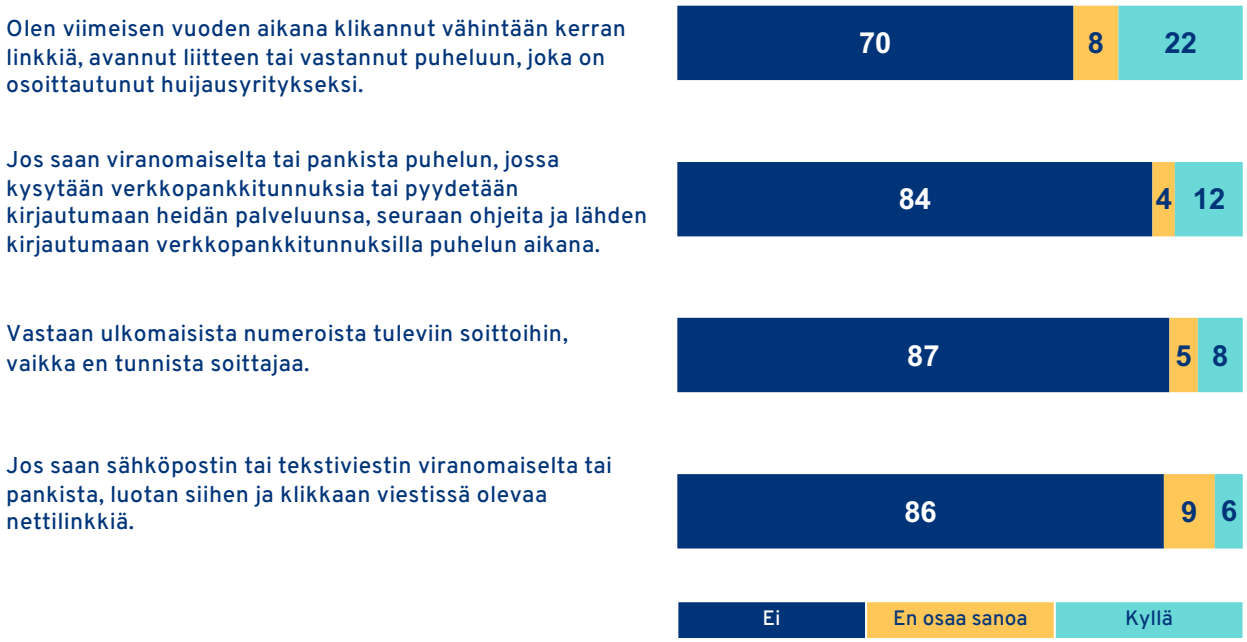
12 prosenttia vastaajista lähtisi kirjautumaan verkkopankkiin puhelun aikana, jos soittaja esiintyisi pankin tai viranomaisen edustajana. Pankin tai viranomaisen nimissä lähetettyä linkkiä klikkaisi sähköpostista tai tekstiviestistä 6 prosenttia vastaajista, ja 8 prosenttia vastaa tuntemattomista ulkomaisista numeroista tuleviin puheluihin.

Peräti 22 prosenttia kertoo viimeisen vuoden aikana klikanneensa linkkiä, avanneensa liitteen tai vastanneensa puheluun, joka osoittautui huijausyritykseksi.

Tässä näkyy yksi barometrin kiinnostavimmista ristiriidoista: pidämme itseämme turvallisempina digikäyttäjinä kuin käyttäytymisemme antaa ymmärtää.

Pidämme itseämme turvallisempina digikäyttäjinä kuin käyttäytymisemme antaa ymmärtää.

Väittämät: tietämys digiturvasta ja osaaminen toimia turvallisesti



12 % lähtisi kirjautumaan verkkopankkitunnuksilla viranomaiselta tai pankista tulevan puhelun aikana.

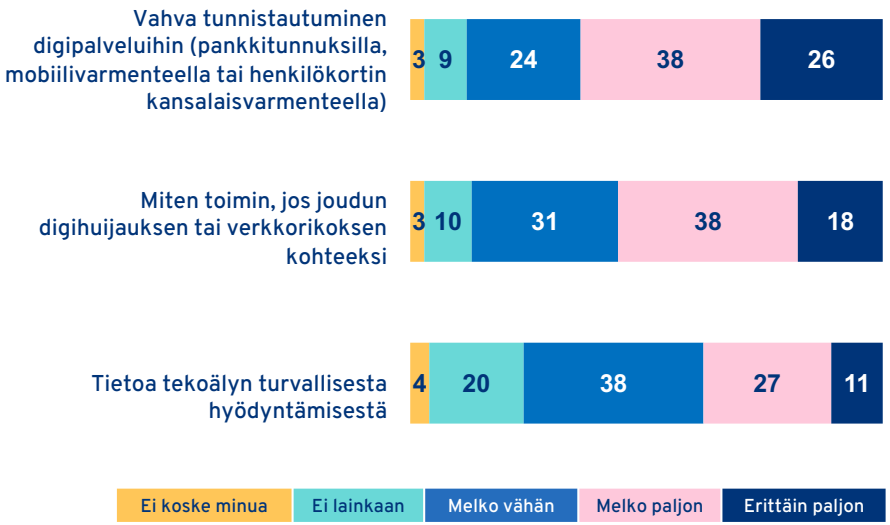
Sähköpostin tai tekstiviestin kohdalla vastaava luku on 6 %.

Parannusta huijausyrityksiin varautumisessa

Samaan aikaan osaamisessa näkyy kuitenkin myös selviä myönteisiä muutoksia. Yhä useampi tietää, mitä tehdä epäillessään verkkohuijausta, osaa tarkistaa verkkosivuston tai verkkokaupan turvallisuuden ja käyttää eri palveluissa eri salasanoja. Nämä taidot ovat parantuneet 6–8 prosenttiyksikköä vuodessa.

Vahvaan tunnistautumiseen saatu koulutuksen ja tiedon määrä on pudonnut poikkeuksellisen paljon vuodesta 2025: - 10 %. Asiaan voi vaikuttaa viranomaispostin muuttuminen ensisijaisesti digitaaliseksi. Muutoksen myötä Suomi.fi-viestien käyttäjämäärä on kasvanut keväästä 2025 yli 2,4 miljoonalla käyttäjällä. Suomi.fi-viestit, kuten yhä useampi muu digiasiointipalvelu, edellyttää vahvaa tunnistautumista.

Minkä verran olet saanut tietoa ja/tai koulutusta* seuraavista tilanteista ja niissä toimimisesta?



*esim. työpaikalla, oppilaitoksessa, mediasta

	2023	2024	2025	2026
Vahva tunnistautuminen digipalveluihin (pankkitunnuksilla, mobiilivarmenteella tai henkilökortin kansalaisvarmenteella)	75 %	72 %	74 %	64 %
Miten toimin, jos joudun digihuijauksen tai verkkorikoksen kohteeksi	51 %	55 %	55 %	56 %
Tietoa tekoälyn turvallisesta hyödyntämisestä	27 %	27 %	36%	38 %

MELKO / ERITTÄIN PALJON

Vahvaan tunnistautumiseen saatu koulutuksen ja tiedon määrä on pudonnut poikkeuksellisen paljon vuodesta 2025: - 10 %

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

48 %

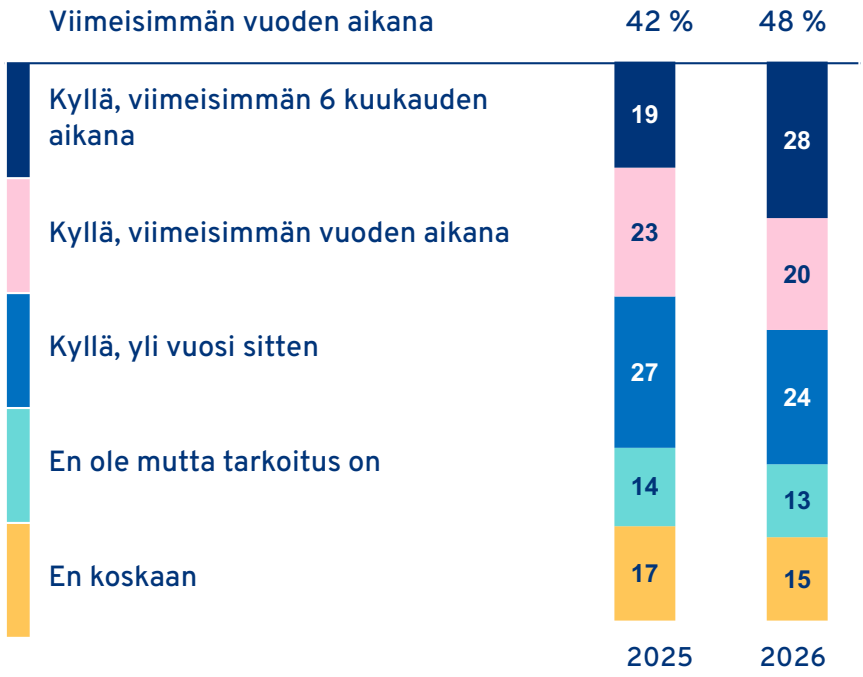
Lähes puolet suomalaista on parantanut maksukorttien ja tilien käyttöön liittyvää turvallisuutta viimeisen vuoden aikana.

+6 % vs. 2025

28 %

Reilu neljäsosa ei ole vielä tehnyt tätä. Luvussa on pientä pudotusta vuodesta 2025, jolloin luku oli 31 %.

−3 % vs. 2025



*esim. aikamäärä tai summakohtaisia nosto- tai siirtorajoituksia tai alue-/maakohtaisia rajoituksia

Myös konkreettisten suojatoimien käyttö on lisääntynyt. 48 prosenttia suomalaisista on parantanut maksukorttiensa ja tiliensä käyttöön liittyvää turvallisuutta viimeisen vuoden aikana, kuusi prosenttiyksikköä enemmän kuin vuonna 2025. Suurinta kasvu on 75–99-vuotiaiden, 18–24-vuotiaiden ja 50–64-vuotiaiden keskuudessa.

Huoli huijauksista kasvaa, mutta resilienssi paranee

Suomalaiset ovat selvästi aiempaa huolestuneempia digihuijauksista. 69 prosenttia on niistä melko tai erittäin huolissaan. Tämä on peräti kymmenen prosenttiyksikköä enemmän kuin vuotta aikaisemmin. Myös henkilötietojen väärinkäyttö huolestuttaa 75 prosenttia suomalaisista.

Keskeinen syy näin merkittävään kasvuun liittyy todennäköisesti siihen, että aihe on ollut eri medioissa esillä aiempaa enemmän. Myös omat ja lähipiirin, sukulaisten, ystävien ja tuttavien kokemukset vaikuttavat asiaan.

Mitä mieltä olet kansalaisiin kohdistuvista digihuijauksista?

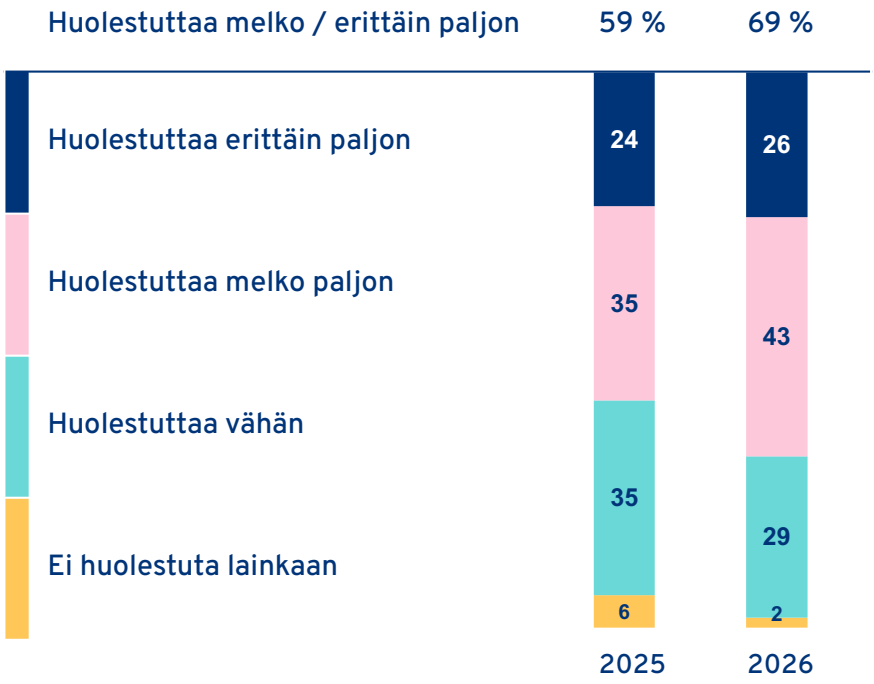
69 %

Kansalaisiin kohdistuvat digihuijaukset huolestuttavat yli kahta kolmasosaa suomalaisista melko tai erittäin paljon.

+10 % vs. 2025

31 %

Vajaan kolmasosan (31 %) mielestä kansalaisiin kohdistuvat digihuijaukset huolestuttavat vähän (29 %) tai ei lainkaan (2 %).



Kuinka paljon kansalaisiin kohdistuvilla digihuijauksilla on ollut vaikutusta omaan arkeesi?

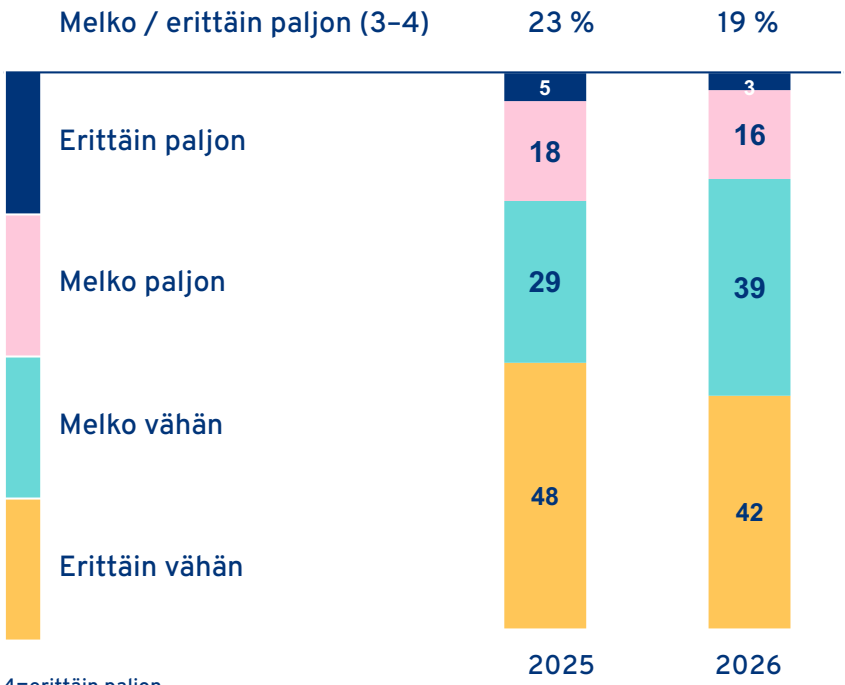
19 %

Vain vajaa viidesosa (19 %) kokee, että kansalaisiin kohdistuvilla digihuijauksilla on ollut melko tai erittäin paljon vaikutusta omaan arkeen. Luku on vähentynyt 4 % viime vuodesta.

−4 % vs. 2025

81 %

Yli neljä viidesosaa kokee, että kansalaisiin kohdistuvat digihuijaukset ovat vaikuttaneet omaan arkeen vähän (1–2).



Asteikolla 1–4, jossa 1=erittäin vähän ja 4=erittäin paljon

Huolen kasvu ei kuitenkaan näy negatiivisena kehityksenä kaikissa mittareissa. 19 prosenttia vastaajista sanoo, että digihuijaukset ovat vaikuttaneet paljon heidän omaan arkeensa. Tämä on neljä prosenttiyksikköä vähemmän kuin viime vuonna.

Kuinka paljon kansalaisiin kohdistuvilla digihuijauksilla on ollut vaikutusta luottamukseesi digitaalista yhteiskuntaa kohtaan?

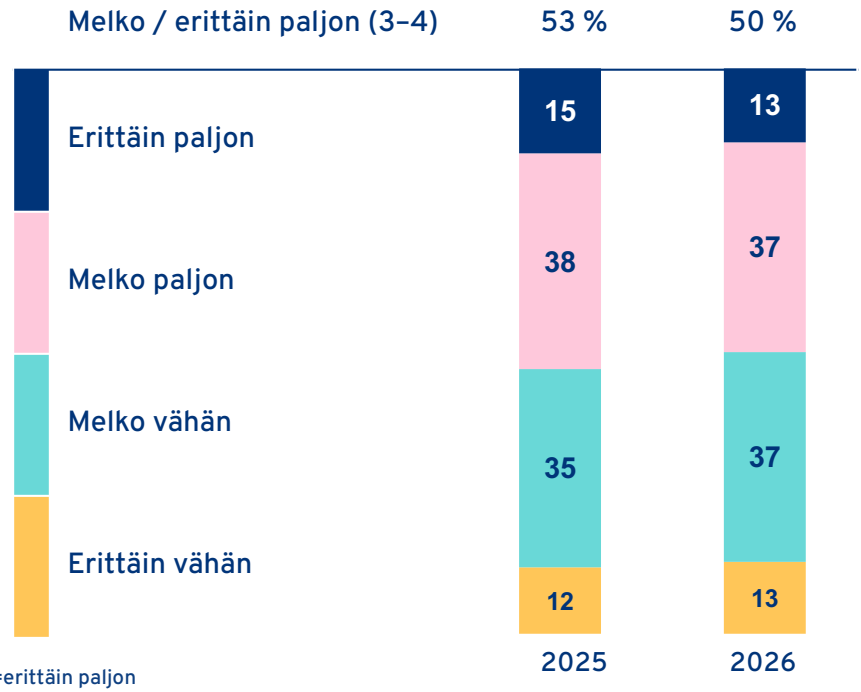
50 %

Puolet suomalaisista kokee, että kansalaisiin kohdistuvat digihuijaukset ovat vaikuttaneet paljon (3–4) luottamukseen digitaalista yhteiskuntaa kohtaan.

−3% vs. 2025

50 %

Toisaalta puolet kokee, että kansalaisiin kohdistuvilla digihuijauksilla on ollut vain vähän (1–2) vaikutusta luottamukseen digitaalista yhteiskuntaa kohtaan.



Asteikolla 1–4, jossa 1=erittäin vähän ja 4=erittäin paljon

Puolet vastaajista katsoo huijausten vaikuttaneen paljon luottamukseensa digitaalista yhteiskuntaa kohtaan, mutta tässäkin osuus on pienentynyt kolmella prosenttiyksiköllä edellisestä vuodesta.

Miten suomalainen yhteiskunta on mielestäsi varautunut digihuijausten estämiseen ja torjumiseen?

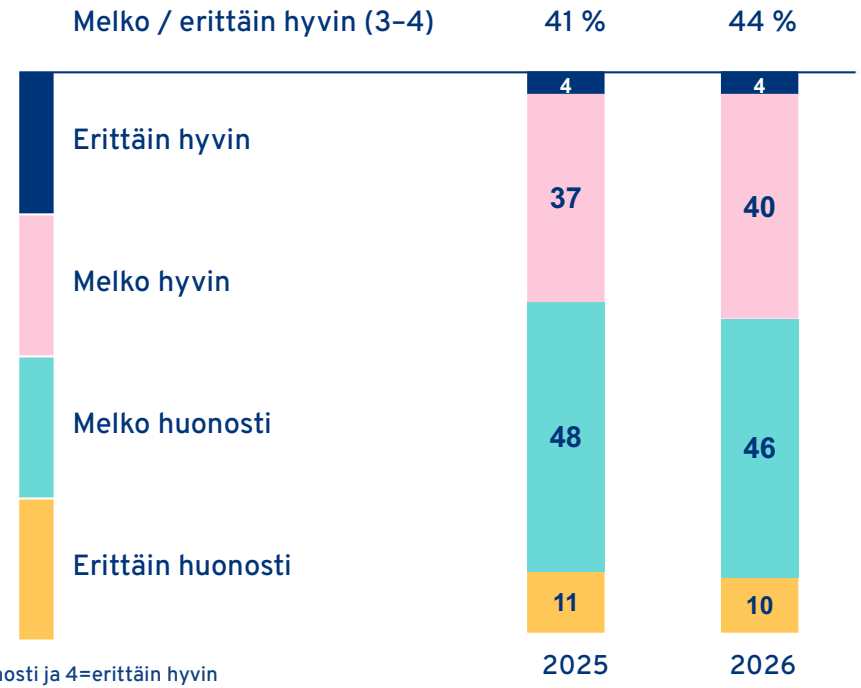
44 %

Arvioi, että suomalainen yhteiskunta on varautunut hyvin (3–4) digihuijausten estämiseen ja torjumiseen.

+3% vs. 2025

56 %

Toisaalta yli puolet kokee, että suomalainen yhteiskunta on varautunut huonosti (1–2).



Asteikolla 1–4, jossa 1=erittäin huonosti ja 4=erittäin hyvin

Myös yhteiskunnan varautuminen arvioidaan hieman aiempaa paremmaksi. 44 prosenttia suomalaisista pitää Suomen varautumista digihuijausten estämiseen ja torjumiseen hyvänä. Tämä on kolme prosenttiyksikköä enemmän kuin viime vuonna. Enemmistö eli 56 prosenttia arvioi sen silti edelleen huonoksi.

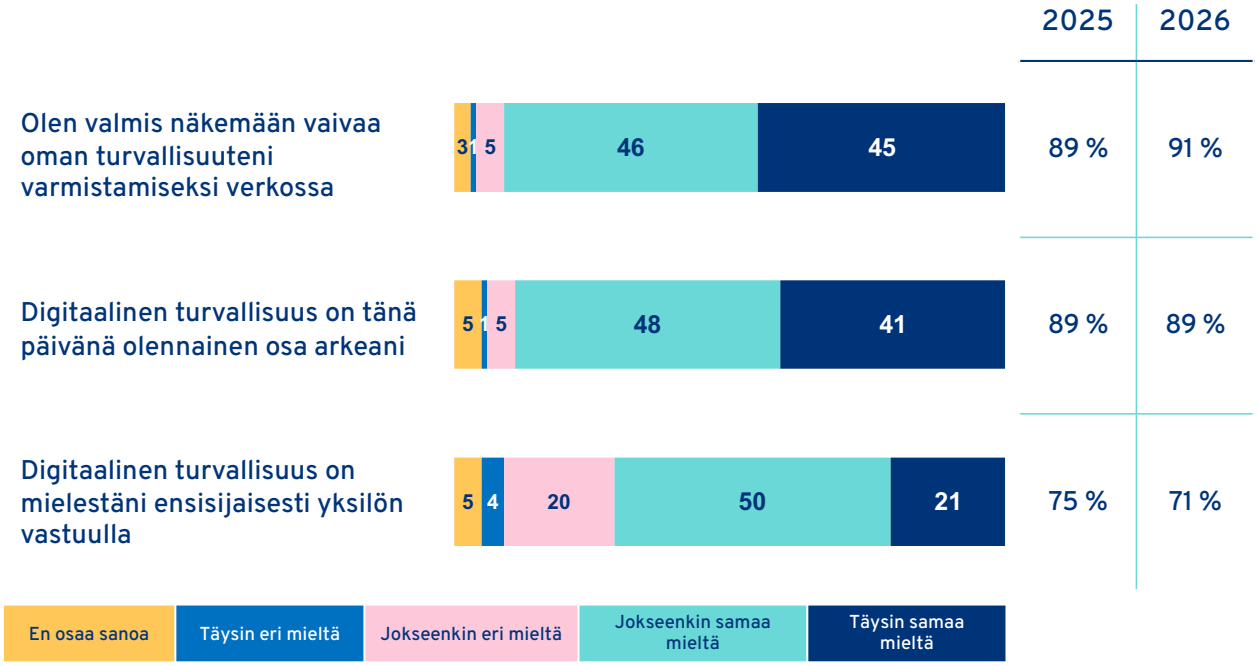
Samaan aikaan 91 prosenttia vastaajista on valmis näkemään vaivaa oman turvallisuutensa varmistamiseksi verkossa. Luku on parantunut vuodessa kaksi prosenttiyksikköä.

Digiturvallisuutta ei kuitenkaan nähdä yhtä voimakkaasti yksilön tehtävänä kuin aiemmin. Digiturvallisuutta ensisijaisesti yksilön vastuuna pitävien osuus on laskenut 75 prosentista 71 prosenttiin.

Tulos voi viitata siihen, että ajattelussa on syntymässä uudenlainen tasapaino: ihmiset ovat valmiita kantamaan vastuuta omasta turvallisuudestaan, mutta digiturvallisuutta ei enää nähdä pelkästään yksilön tehtävänä.

91 % on valmis näkemään vaivaa turvallisuutensa varmistamiseksi.

Suhtautuminen digiturvaan



Digitaalisen turvallisuuden eteen ollaan valmiita näkemään entistä enemmän vaivaa (91 %).

Suomalaiset uskovat tunnistavansa huijaukset

Suomalaisten luottamus omaan kykyynsä tunnistaa huijaukset on kansainvälisesti korkea. 82 prosenttia arvioi olevansa melko tai erittäin varma siitä, että tunnistaa digihuijauksen.

Global Anti Scam Alliancen (GASA) Euroopan-vertailussa vuonna 2026 vastaava luku on 71 prosenttia, eli ero Suomen hyväksi on 11 prosenttiyksikköä.

Kuinka varma olet siitä, että tunnistat digihuijauksen tai huijausyrityksen esimerkiksi sähköpostissa, tekstiviestissä, puhelussa tai verkkopalvelussa?

82 %

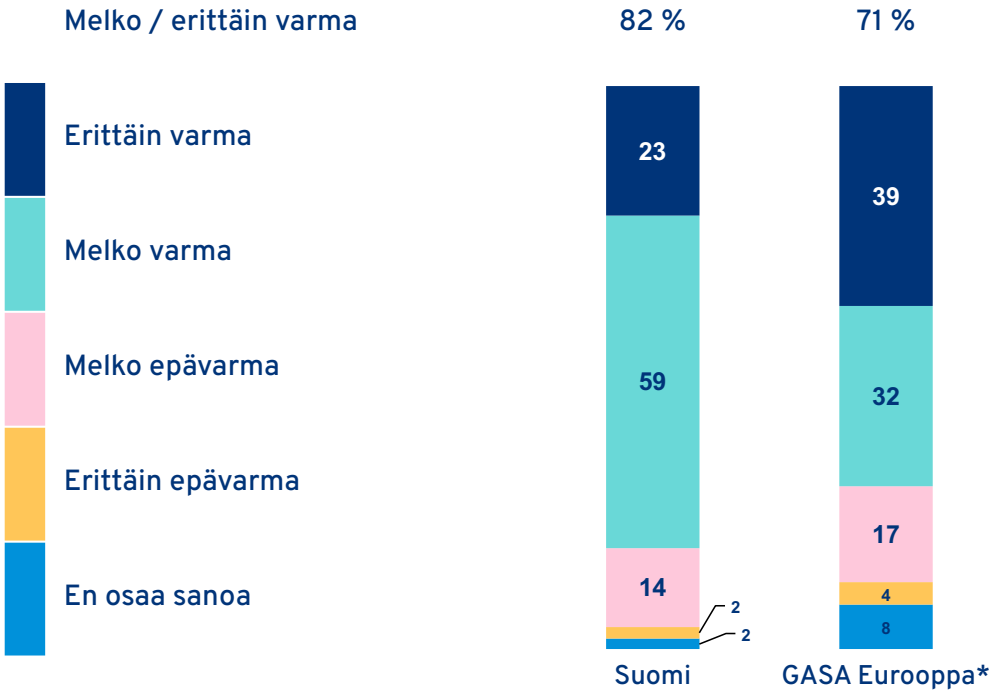
Suomessa ollaan selkeästi varmempia tunnistamaan digihuijauksia kuin muualla Euroopassa.

+11 % vs. Eurooppa

23 %

on erittäin varmoja, kun taas Euroopassa on selkeästi enemmän niitä, jotka ovat erittäin varmoja.

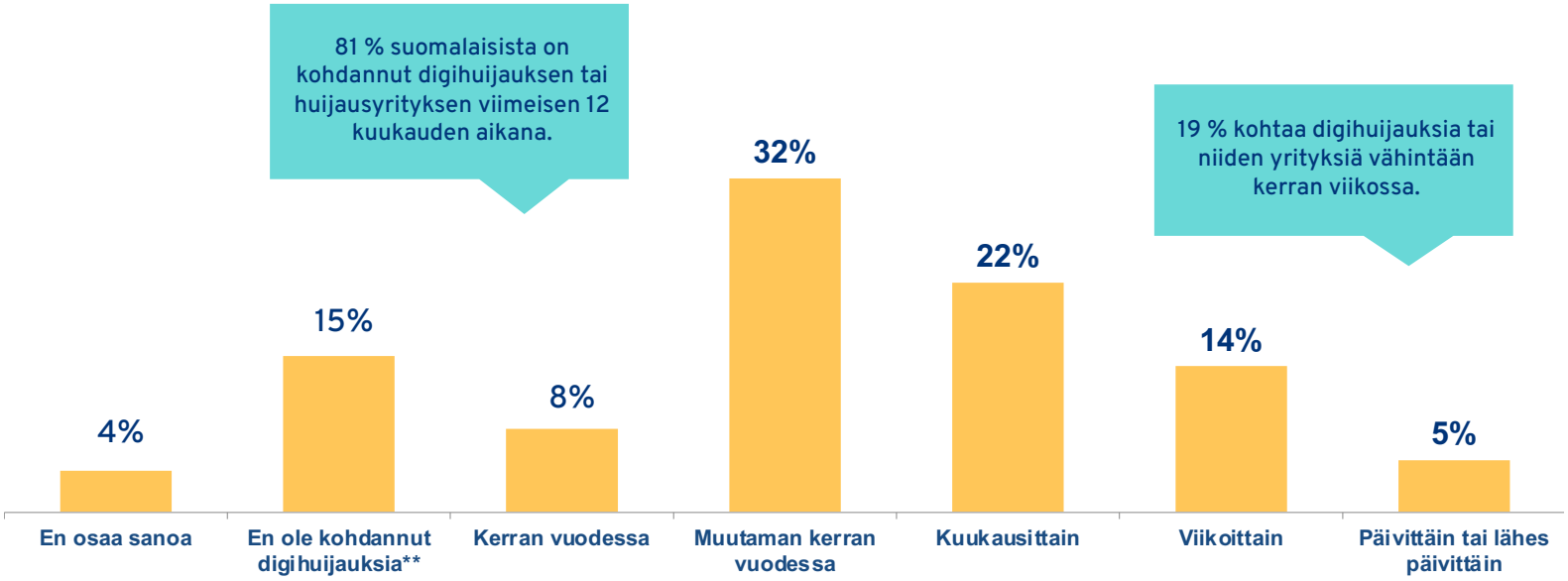
-16 % vs. Eurooppa



* Global Anti Scam Alliance (GASA): State of Scams in Europe 2026

Vahva luottamus omaan tunnistuskykyyn ei kuitenkaan tarkoita, ettei digihuijauksille altistuttaisi. 81 prosenttia suomalaisista on kohdannut digihuijauksen tai huijausyrityksen viimeisen 12 kuukauden aikana, kun eurooppalainen vertailuluku on 75 prosenttia.

Kuinka usein olet viimeisen 12 kuukauden aikana kohdannut digihuijauksia* tai huijausyrityksiä?



*esim. huijausviestejä, kalasteluviestejä, huijauspuheluita tai valeverkkokauppoja
**tai huijausyrityksiä

Joka viides suomalainen kertoo kohtaavansa huijauksia vähintään viikoittain, ja 5 prosenttia jopa päivittäin tai lähes päivittäin.

Digihuijausten yleisyyttä Suomessa voi selittää osin yhteiskuntamme korkea digitalisaatioaste: meillä on kattava ja hyvin toimiva digitaalinen infrastruktuuri, sähköiset palvelut ja maksujärjestelmät ovat laajasti käytössä ja lähes kaikilla on käytössään jokin älylaite. Lisäksi väestön kielitaito on hyvä. Nämä tekijät tekevät Suomesta houkuttelevan kohteen myös kansainväliselle verkkorikollisuudelle.

Tekoälyaikana kieli ei enää toimi suojana

Samalla on saattanut säilyä ajatus Suomesta eräänlaisena digitaalisen maailman ”Muumilaaksona”, Pohjolan perukoilla sijaitsevana turvallisena yhteiskuntana, jota suojaavat maantieteellinen sijainti ja kansainvälisesti harvinainen suomen kieli. Tälle turvallisuuden tunteelle on entistä vähemmän perusteita.

Verkkorikollisuus on globaalia, eikä maantiede anna suojaa siltä. Tekoälyn nopea kehitys vaikuttaa myös kielen tarjoamaan suojaan: laadukkaiden suomenkielisten huijausviestien, keskustelujen, puheen ja videoiden tuottaminen on aiempaa helpompaa.

Kuinka usein olet viimeisen 12 kuukauden aikana kohdannut digihuijauksia tai huijausyrityksiä?

81 %

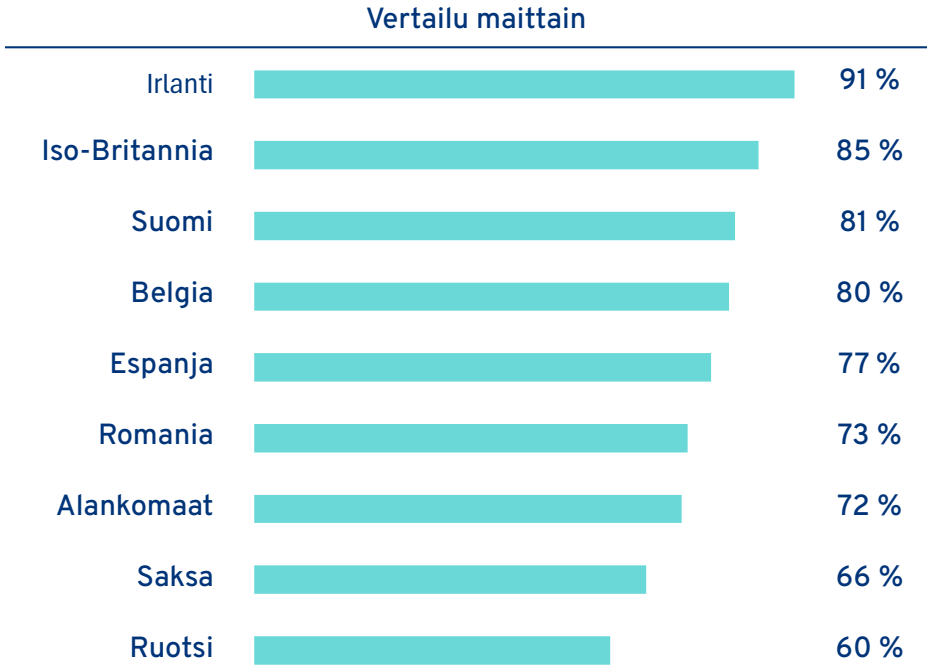
81 % suomalaisista on kohdannut digihuijauksen tai huijausyrityksen viimeisen 12 kuukauden aikana.

75 %

GASA Eurooppa –tutkimuksen* mukaan vastaava eurooppalainen luku on 75 %.

80–91 %

Irlannissa, Isossa-Britanniassa, Suomessa ja Belgiassa vähintään neljä viidesosaa on kohdannut digihuijauksia tai huijausyrityksiä.



*Global Anti Scam Alliance (GASA): State of Scams in Europe 2026

Tekoäly mahdollistaa yhä uskottavampien ääni-, kuva- ja videosyväväärennösten tuottamisen. Tämä vaikeuttaa aidon ja tekoälyllä tuotetun tai manipuloidun synteettisen sisällön erottamista toisistaan.

2.8.2026 sovellettavaksi tullut EU:n tekoälyasetus toi uusia velvoitteita muun muassa tekoälyn käytöstä kertomiseen sekä deepfake- ja muun tekoälyllä tuotetun tai muokatun sisällön merkitsemiseen.

Useita uhkia laskusuunnassa

Toinen vuoden 2026 merkittävistä myönteisistä signaaleista on toteutuneiden uhkien kehitys. Vertailukelpoisten uhkamittareiden kokonaiskeskiarvo laski vuodessa 34 prosentista 30 prosenttiin.

Sähköposti on edelleen yleisin huijauskanava: huijaus- tai kalasteluviestejä on saanut 71 prosenttia vastaajista. Tekstiviestihuijauksia on kohdannut 48 prosenttia, huijauspuheluita 47 prosenttia, sosiaalisen median huijausyrityksiä 42 prosenttia ja pikaviestisovellusten huijauksia 33 prosenttia.

Huijaus- ja kalastelu-viestejä tulee vastaan aiempaa harvemmin.

Digiturvallisuuteen liittyvien uhkien toteutuminen itselle vimeisen vuoden aikana

	2022	2023	2024	2025	2026
Olen saanut huijaus- tai kalasteluviestejä sähköpostiini	83 %	83 %	84 %	78 %	71 %
Olen saanut huijaus- tai kalasteluviestejä tekstiviestinä (SMS)	-	66 %	72 %	62 %	48 %
Olen saanut huijaus- tai kalastelupuhelinsoittoja	64 %	61 %	61 %	54 %	47 %
Olen kohdannut huijausyrityksiä sosiaalisen median kanavissa (Facebook, Instagram, LinkedIn yms.)					42 %
En ole pystynyt hoitamaan haluamaani asiaa digitaalisesti, koska palvelutarjoajan digipalvelu ei ole ollut toiminnassa	42 %	39 %	32 %	33 %	36 %
Olen saanut huijaus- tai kalasteluviestejä pikaviestisovelluksiini (esim. WhatsApp, Messenger, Signal)	-	30 %	43 %	42 %	33 %
Olen huomannut, että työhöni tai mielipiteisiini on yritetty vaikuttaa joko digimaailmassa tai henkilökohtaisella kontaktoinnilla	16 %	14 %	15 %	14 %	13 %
Olen menettänyt rahaa tekemällä ostoksen valeverkkokaupasta	-	-	9 %	10 %	7 %
Olen menettänyt rahaa kiristyksen tai digihuijauksen takia	9 %	12 %	8 %	7 %	6 %
Olen joutunut identiteettivarkauden kohteeksi	5 %	6 %	6 %	6 %	5 %

Laskenut | Noussut

Uhkien toteutumisen kokonaiskeskiarvossa (vertailukelpoiset mittarit)

−4 % pudotus vuodesta 2025:
2025: 34 %
2026: 30 %

Monen uhan toteutuminen on ollut laskusuunnassa viimeisen kahden tai kolmen vuoden aikana.

Erityisesti huijaus- ja kalasteluviestit (SMS): −14 %
sekä vastaavat pikaviesti-sovellukset: −9 %.

Useiden keskeisten huijausmuotojen määrät ovat laskeneet. Sähköpostin huijaus- ja kalasteluviestejä kohdanneiden osuus laski 78 prosentista 71 prosenttiin, tekstiviesteissä 62 prosentista 48 prosenttiin ja huijauspuheluissa 54 prosentista 47 prosenttiin. Pikaviestisovelluksissa osuus laski 42 prosentista 33 prosenttiin.

Tekstiviestihuijauksissa muutos on siis peräti −14 prosenttiyksikköä ja pikaviestihuijauksissa −9 prosenttiyksikköä.

Digipalvelujen häiriöt ja käyttökatkot vaikuttavat siihen, miten ihmiset pystyvät hoitamaan asioitaan digitaalisesti: vastaajista 36 % sanoo asioiden hoitamisen estyneen häiriöiden vuoksi. Luku on kasvanut vuodesta 2025 kolme prosenttiyksiköä.

Rahaa valeverkkokaupassa menettäneiden osuus laski 10 prosentista 7 prosenttiin, kiristyksen tai digihuijauksen seurauksena 7 prosentista 6 prosenttiin ja identiteettivarkauden takia 6 prosentista 5 prosenttiin.

Suomen vahvuus ei siis ole se, että huijauksia olisi vähän. Vahvuus näyttää pikemminkin olevan siinä, että kansalaiset tunnistavat niitä suhteellisen hyvin ja oppivat toimimaan niiden keskellä.

Suomessa huijauksia riittää, mutta niiden määrää on saatu laskettua ja niitä tunnistetaan paremmin.

Verkkorikollisuutta vastaan yhteistyöllä ja valppaudella

Suomessa on viimeisen vuoden aikana otettu käyttöön useita uusia teknisiä keinoja digihuijausten torjumiseksi.

Estolista rajoittaa pääsyä haitallisiin osoitteisiin

Yksi keino torjua digihuijauksia on finanssialan, teleoperaattoreiden ja viranomaisten yhteistyössä toteuttama niin sanottu estolistapalvelu, jonka avulla pääsyä verkkorikollisten käyttämiin haitallisiin verkko-osoitteisiin voidaan rajoittaa nopeasti.

Kun uusi huijaussivusto tai muu haitallinen osoite tunnistetaan ja ilmoitetaan palveluun, sen estäminen voi tapahtua parhaimmillaan minuuteissa ja tyypillisesti muutamien tuntien kuluessa.

Estolista on tehokas työkalu, mutta sen toiminta edellyttää, että haitalliset verkko-osoitteet havaitaan ja ilmoitetaan nopeasti. Uusien huijaussivustojen ja haitallisten linkkien ilmoittaminen on siis edelleen tärkeää.

Tekstiviestien lähettäjätunnukset hyväksytettävä etukäteen

Suomi vaikeutti tekstiviestihuijauksia merkittävästi toukokuussa 2026, kun uudet velvoitteet lähettäjien tunnistamiselle tulivat voimaan (Traficomin uudistettu määräys 28 L/2025 M Viestintäverkkojen ja palvelujen yhteentoimivuudesta).

Organisaatioiden tekstiviesteissään käyttämät suomalaiset puhelinnumerot ja nimimuotoiset lähettäjätunnukset on hyväksytettävä etukäteen. Vaatimus koskee SMS-viestien lisäksi myös MMS- ja RCS-viestejä. Lupavaatimuksen ansiosta esimerkiksi pankin, viranomaisen tai muun tunnetun organisaation lähettäjätunnuksen väärentäminen on Suomessa pääsääntöisesti estetty.

Ilman lupaa lähetetyt viestit näkyvät vastaanottajalle tunnuksella ”Tuntematon” ja 2.11.2026 alkaen tunnuksella ”Roskaposti” tai ne estetään kokonaan.

Tekniset ratkaisut eivät poista tekstiviestihuijauksia kokonaan. Verkkorikolliset voivat edelleen lähettää huijausviestejä omista tai muista käytössään olevista numeroista ja ohjata vastaanottajia esimerkiksi haitallisille verkkosivuille.

Siksi teknisten suojausten rinnalla tarvitaan käyttäjien valppautta ja kykyä tunnistaa huijausyrityksiä.

Onnistuneiden huijausten seuraukset edelleen merkittäviä

Huijauksen kohdanneista 8 prosenttia on luovuttanut huijauksen seurauksena jotakin suojattavaa tietoa. Useimmiten kyse on henkilötiedoista tai pankki- ja maksukorttitiedoista, joita 4 prosenttia huijauksen kohdanneista on luovuttanut.

Käytännössä rikollinen on samassa yhteydessä tyypillisesti saanut haltuunsa myös muita henkilöä koskevia tietoja käytetystä digihuijauskanavasta riippuen.

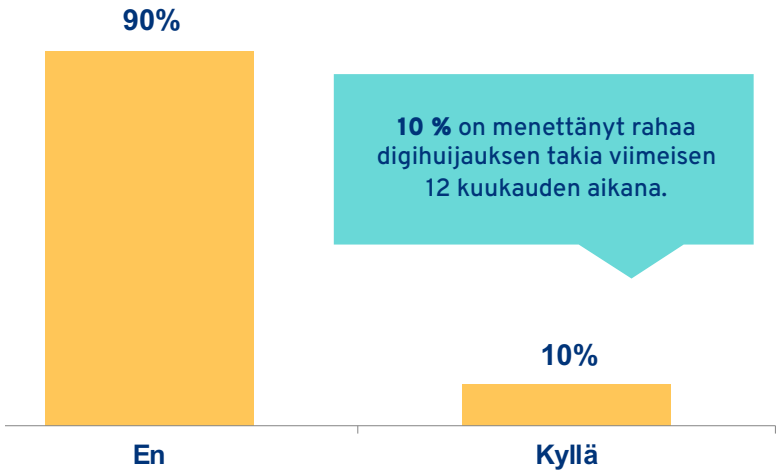
Oletko viimeisen 12 kuukauden aikana luovuttanut digihuijauksen seurauksena jotain seuraavista?

8 % on luovuttanut jotain näistä tiedoista.

Eniten on luovutettu henkilötietoja (4 %) ja pankki- tai maksukorttitietoja (4 %).

Rahan menettäminen digihuijauksen takia

Oletko menettänyt rahaa digihuijauksen, kiristyksen tai valeverkkokauppaostoksen takia?



Kuinka monta erillistä digihuijausta johti siihen, että menetit rahaa viimeisen 12 kuukauden aikana?

Suomalaisista 10 prosenttia kertoo menettäneensä viimeisen 12 kuukauden aikana rahaa digihuijauksen, kiristyksen tai valeverkkokauppaostoksen seurauksena.

Erityisen huolestuttavana voidaan pitää sitä, että näistä noin joka kuudes (16 %) on menettänyt rahaa useammin kuin kerran.

9 % digihuijauksen uhreista menetti yli 1 000 euroa.

Rahaa menettäneistä 69 prosenttia menetti 1–100 euroa, 19 prosenttia 101–500 euroa, 3 prosenttia 501–1 000 euroa ja 9 prosenttia yli 1 000 euroa.

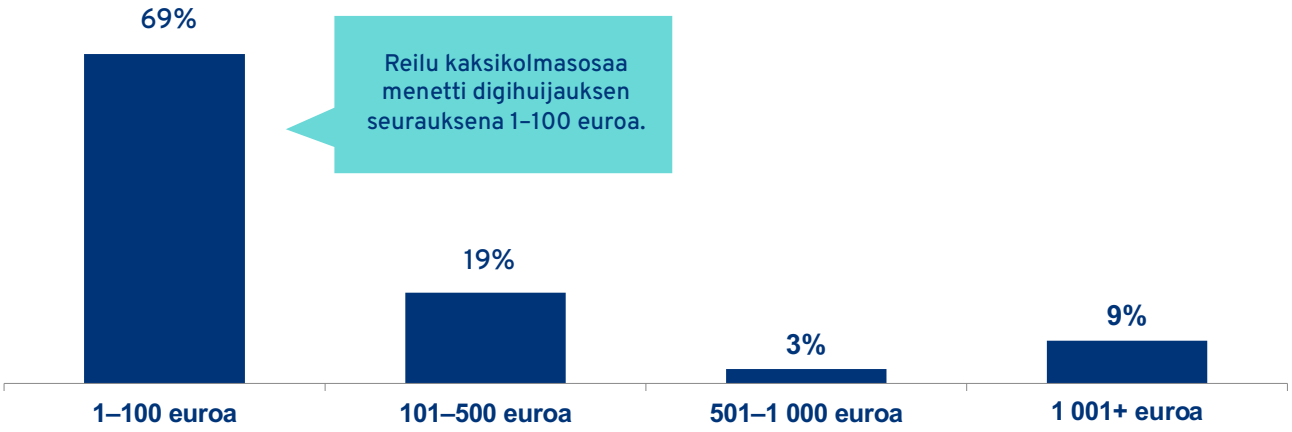
Jos Suomessa on Tilastokeskuksen arvion mukaan noin 4,5 miljoonaa aktiivista digikäyttäjää ja 10 prosenttia heistä on menettänyt rahaa digihuijauksen seurauksena, kyse olisi noin 450 000 suomalaisesta.

Kun menetysluokille käytetään varovaisia keskimääräisiä euromääriä, rahallisten menetysten kokonaismääräksi voidaan arvioida noin 128 miljoonaa euroa vuodessa. Arvio on suuruusluokaltaan linjassa esimerkiksi poliisin ja Finanssiala ry:n julkaisemien vuosittaisten tietojen kanssa.

On tärkeää huomata, että arvio koskee vain yksityishenkilöiden menetyksiä. Sen lisäksi taloudellisia vahinkoja aiheutuu muun muassa yrityksiin ja muihin organisaatioihin kohdistuvista digihuijauksista, maksuliikennepetoksista ja kiristyksistä sekä maksu- ja luottokorttipetoksista.

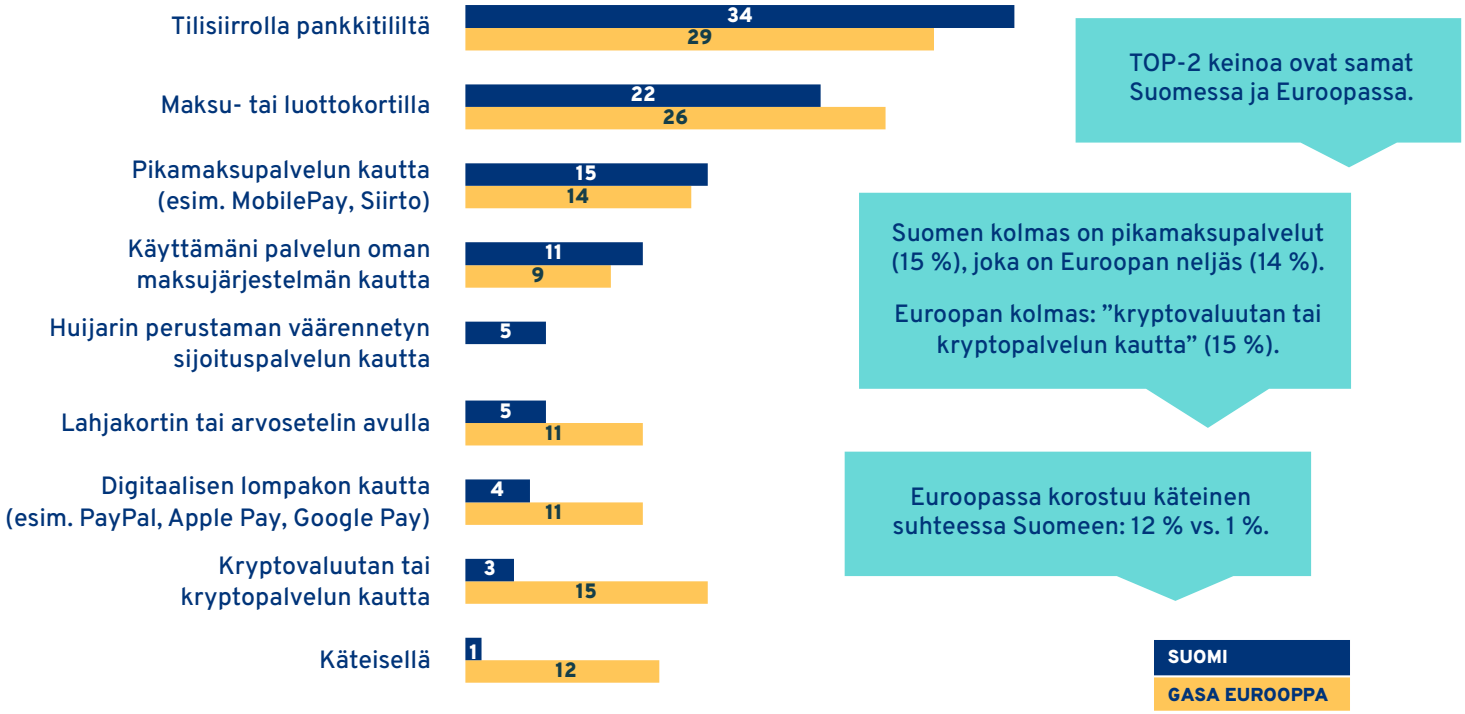
Digirikollisuuden aiheuttamien suorien taloudellisten menetysten kokonaismäärä Suomessa on siten merkittävästi suurempi, mutta sen luotettava arviointi on vaikeaa. Tämän vuoksi ilmoittaminen on erityisen tärkeää etenkin tilanteissa, joissa rikoksen seurauksena menetetään rahaa.

Kuinka paljon rahaa menetit yhteensä digihuijauksen seurauksena viimeisen 12 kuukauden aikana?



Joukko: Digihuijauksen takia viim. 12 kuukauden aikana rahaa menettäneet 10 %

Millä tavalla huijari sai rahasi?



Joukko: Digihuijauksen takia viim. 12 kuukauden aikana rahaa menettäneet

Kun rikollinen saa haltuunsa henkilön pankkitilin tai pystyy vaikuttamaan henkilön tekemään maksuun, reilussa kolmanneksessa (34 %) digihuijauksista huijari sai rahat tilisiirrolla. Noin viidesosassa (22 %) rahat siirrettiin maksu- tai luottokortilla ja 15 prosentissa rahat siirrettiin niin sanottujen pikamaksupalvelujen kautta.

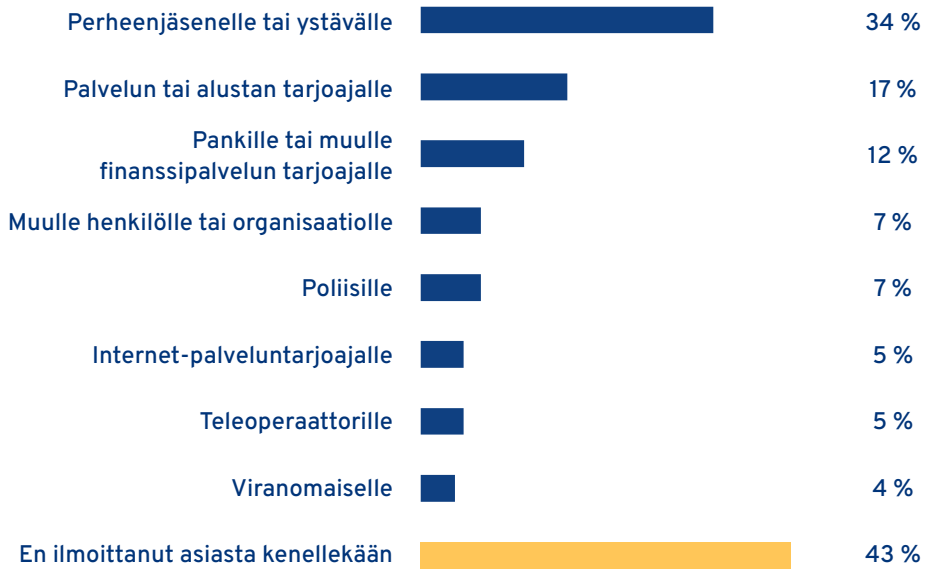
Kannattaa huomata, että esimerkiksi kaupoista hankittavat lahjakortit ja arvosetelit ovat olleet käytössä viidessä prosentissa ja kryptovaluutta ainoastaan kolmessa prosentissa huijauksia.

Etenkin graafin neljässä alimmassa kohdassa Suomi poikkeaa merkittävästi GASA Eurooppa -tutkimuksen tuloksista. Tulos korostaa, että Suomen maksuliikenne on keskittynyt perinteisten finanssialan toimijoiden palveluihin ja käteisen rahan käyttö on vähäistä.

Digihuijauksista kerrotaan harvoin niille, jotka voisivat toimia

Yksi vuoden 2026 tuloksista nousee erityisen vahvasti kehittämiskohteeksi: huijauksista ilmoitetaan liian vähän.

Kenelle ilmoitit viimeisen 12 kuukauden aikana kohtaamastasi digihuijauksesta?



Joukko: on kohdannut digihuijauksen viimeisen 12 kk aikana 81 %

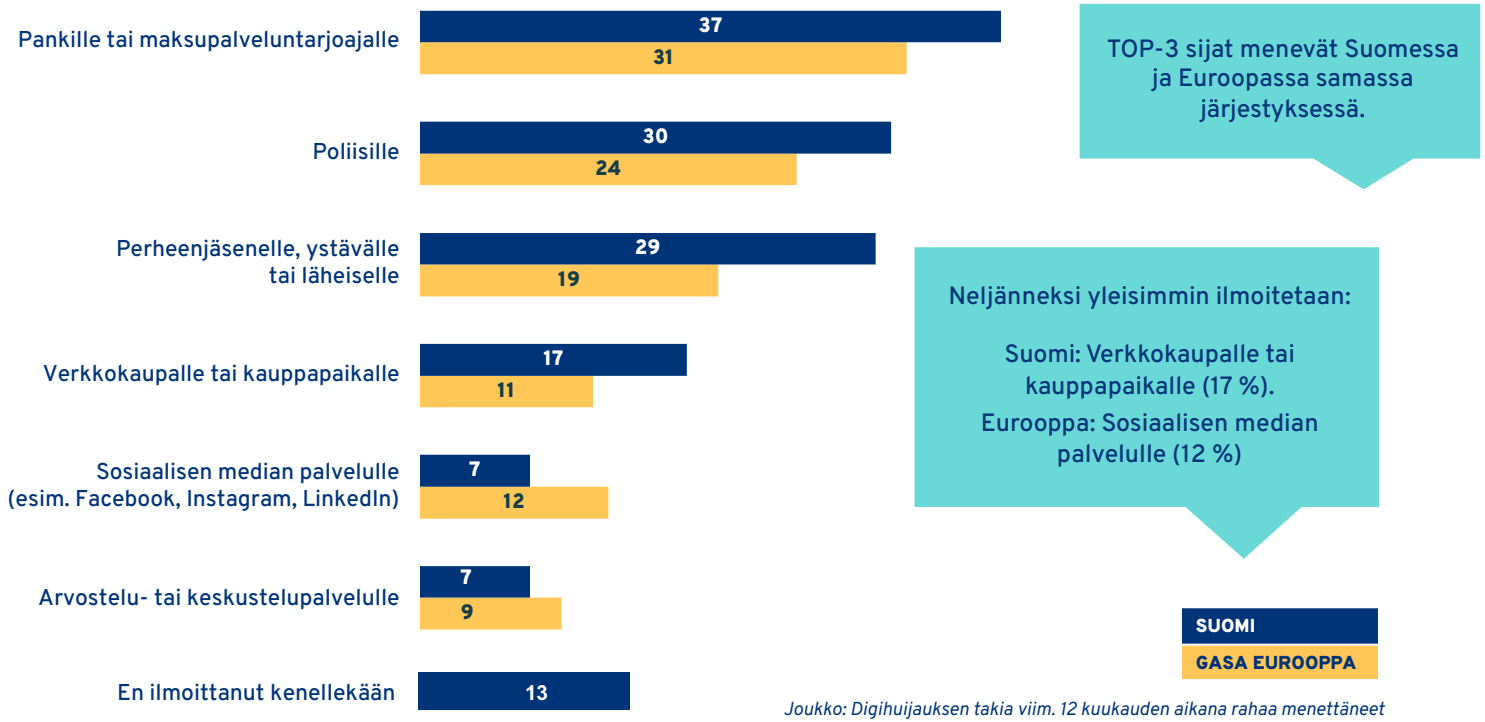
Kolmasosa (34 %) ilmoittaa kohtaamastaan digihuijauksesta perheenjäsenelle tai ystävälle.

17 % ilmoittaa palvelun tai alustan tarjoajalle ja 12 % pankin tai muun finanssipalvelun tarjoajalle.

43 % ei ole ilmoittanut asiasta kenellekään.

Huijauksen tai huijausyrityksen kohdanneista 43 prosenttia ei ilmoittanut asiasta kenellekään. 34 prosenttia kertoo tapauksesta perheenjäsenelle tai ystävälle, kun taas palvelun tai alustan tarjoajalle ilmoittaa 17 prosenttia, pankille tai muulle finanssipalvelulle 12 prosenttia ja poliisille vain 7 prosenttia.

Kun menetit rahaa, kenelle ilmoitit digihuijauksesta tai kerroit tapahtuneesta?

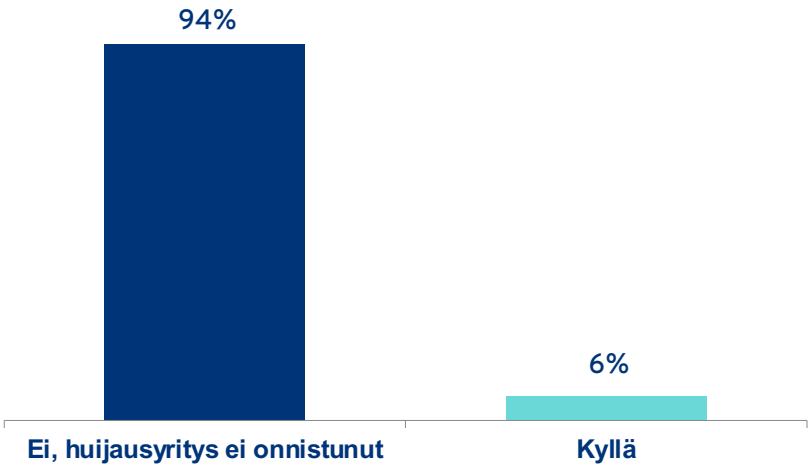


Joukko: Digihuijauksen takia viim. 12 kuukauden aikana rahaa menettäneet

Tilanne muuttuu olennaisesti, kun huijauksessa menetetään rahaa. Tällöin 37 prosenttia kertoo ilmoittavansa pankille tai maksupalveluntarjoajalle ja 30 prosenttia poliisille. Silti 13 prosenttia rahaa menettäneistä ei ilmoita tapahtuneesta kenellekään. Suomi poikkeaa myös tässä positiivisesti euroopanlaajuisesti: Euroopassa näistä asioita ilmoitetaan vähemmän kuin meillä Suomessa.

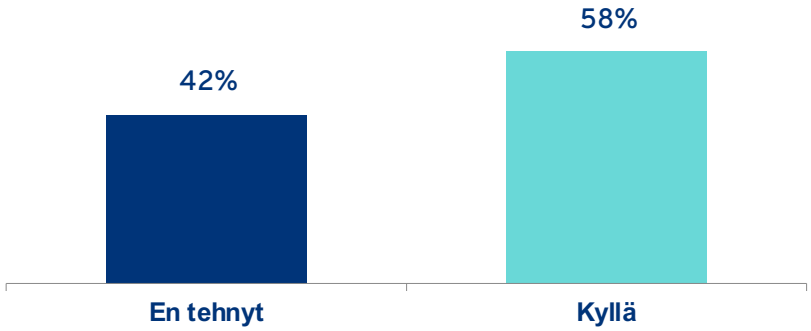
Rikoksen kohtaaminen

Johtiko kohtaamasi digihuijaus tai sen yritys rikokseen tai petokseen viimeisen 12 kuukauden aikana (esim. menetit rahaa tai henkilötietojasi)?



Joukko: ”on kohdannut digihuijauksen viimeisen 12 kk aikana” 81 %

Teitkö rikosilmoituksen tästä digihuijauksesta, petoksesta tai rikoksesta?



Joukko: ”on joutunut rikoksen tai petoksen uhriksi” 6 %

Vielä selvemmin ilmoittamisen aukko näkyy toteutuneissa rikoksissa. Huijauksen kohteeksi joutuneista kuudella prosentilla tapaus johti rikokseen, esimerkiksi petokseen tai rahan tai henkilötietojen menetykseen. Näistä uhreista 58 prosenttia teki rikosilmoituksen, 42 prosenttia ei.

Tämä on järjestelmätason ongelma. Jos huijauksista ei ilmoiteta, viranomaiset, pankit, teleoperaattorit ja palvelualustat eivät saa hyvää tilannekuvaa huijausten määrästä, menetelmistä ja kehityksestä. Samalla myös rikollisen toiminnan tunnistaminen, tekijöiden kiinni saaminen ja heidän toimintansa estäminen vaikeutuvat.

Ilmoittamisen tekeminen helpoksi, ymmärrettäväksi ja hyödylliseksi pitäisi nostaa yhdeksi seuraavista digiturvallisuuden kehityskohteista.

Huijauksista ilmoittaminen pitää tehdä helpoksi, ymmärrettäväksi ja hyödylliseksi.

Mikä sai sinut epäilemään huijausta tai lopettamaan tilanteen viimeisen 12 kuukauden aikana kohtaamissasi tilanteissa?

	Suomi	Eurooppa*
Lähettäjä tai yhteydenottaja vaikutti epäluotettavalta	1	na.
Linkki, liite tai verkkosivusto vaikutti epäilyttävältä tai virheelliseltä	2	5
Viestissä tai yhteydenotossa oli ristiriitoja tai epäloogisuuksia	3	3
Tarjous tai viesti vaikutti liian hyvältä ollakseen totta	4	2
Viesti tai pyyntö ei vastannut sitä, miten kyseinen organisaatio normaalisti toimii	5	3
Rahan, maksun tai henkilötietojen pyytäminen vaikutti epäilyttävältä	6	1

Suomessa kiinnitetään selkeästi enemmän huomiota lähettäjään, linkkiin, liitteeseen tai verkkosivustoon. (sijat 1-2)

Euroopassa painottuu rahan, maksun tai henkilötietojen pyytämiseen liittyvät epäilyt tai itse tarjouksen epäilyttävyys (”vaikutti liian hyvältä ollakseen totta”).

Joukko: Ei ole menettänyt rahaa eikä ole luovuttanut henkilötietoja digihuijausyrityksissä

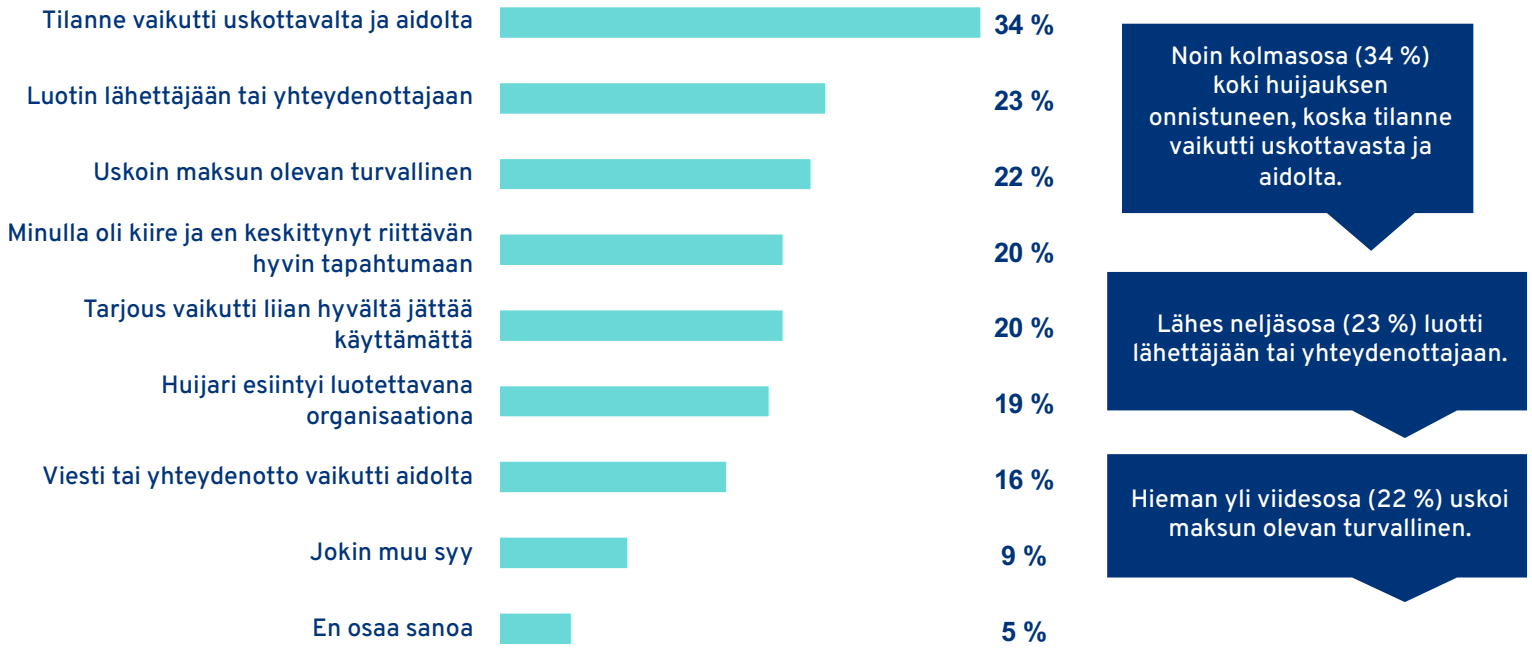
Kun huijausyritys havaitaan ajoissa, sen keskeiset signaalit ovat yleensä inhimillisiä. Epäluotettavalta vaikuttava lähettäjä herättää epäilyn 56 prosentilla, epäilyttävä linkki tai verkkosivusto 54 prosentilla ja viestin ristiriitaisuus tai epäloogisuus 51 prosentilla. Liian hyvältä vaikuttava tarjous tunnistetaan varoitusmerkiksi 43 prosentissa tapauksista.

Viestintä ja selkeät toimintamallit ovat tärkeimmät suojakeinot

Barometrin tärkein laadullinen havainto koskee sitä, miksi huijaukset onnistuvat tai epäonnistuvat.

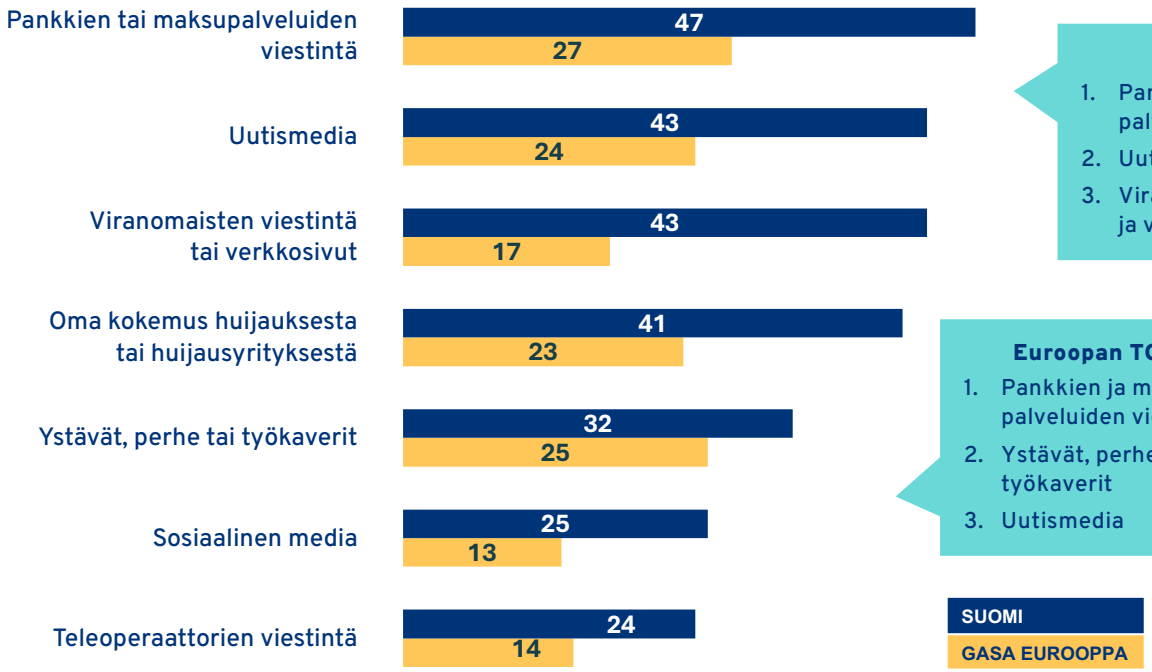
Rahaa menettäneistä 34 prosenttia kertoo huijauksen onnistuneen siksi, että tilanne vaikutti uskottavalta ja aidolta. 23 prosenttia luotti lähettäjään tai yhteydenottajaan, ja 22 prosenttia uskoi maksun olevan turvallinen. Kiire ja liian hyvältä vaikuttanut tarjous vaikutti 20 prosentilla ja huijarin esiintyminen luotettavana organisaationa vaikutti 19 prosentilla.

Miksi uskot huijauksen onnistuneen?



Joukko: Digihuijauksen takia viim. 12 kuukauden aikana rahaa menettäneet

Mitkä seuraavista ovat auttaneet sinua tunnistamaan tai välttämään digihuijauksia?



Suomen TOP-3

1. Pankkien ja maksupalveluiden viestintä
2. Uutismedia
3. Viranomaisten viestintä ja verkkosivut

Euroopan TOP-3

1. Pankkien ja maksupalveluiden viestintä
2. Ystävät, perhe tai työkaverit
3. Uutismedia

Suomen yksi etu on erittäin laaja-alainen tiedottaminen kansalaisille ja eri toimijoiden välinen yhteistyö.

Ikä vaikuttaa siihen, mistä tietoa saadaan. Pankkien, maksupalvelujen ja viranomaisten viestintä korostuu erityisesti yli 64-vuotiaiden vastaajien keskuudessa. Sosiaalinen media puolestaan on merkittävämpi nuorille vastaajille, ja sen merkitys vähenee tasaisesti iän mukana.

Tulokset kertovat myös, mikä kansalaisia käytännössä auttaa. Pankkien ja maksupalvelujen viestintä on tärkein yksittäinen huijausten tunnistamista tai välttämistä tukeva tekijä, jonka nimeää 47 prosenttia. Seuraavina ovat uutismediat 43 prosentilla, viranomaisten viestintä ja verkkosivut 43 prosentilla sekä oma kokemus huijauksista 41 prosentilla.

Näistä asioista viestitään Suomessa erittäin laajasti, ja suomalaiset keskiarvot ovat monilta osin merkittävästi korkeampia kuin muualla Euroopassa.

Millaisia vaikutuksia digihuijauksella on ollut sinuun?

Vajaa kolmasosa luottaa aiempaa vähemmän digitaalisiin palveluihin ja verkkoympäristöihin.

Lähes puolet (49 %) on aiempaa varovaisempi digipalvelujen käytössä, koska on kokenut digihuijauksen tai sen yrityksen.

Vajaa kolmasosa (29 %) kokee, että digihuijauksilla ei ole ollut merkittäviä vaikutuksia.

Huijauksilla on vakavia seurauksia myös silloin, kun rahaa tai henkilötietoja ei menetetä.

Huijauksen kohdanneista 49 prosenttia on muuttunut varovaisemmaksi digipalvelujen käyttäjäksi ja 30 prosenttia luottaa digitaalisiin palveluihin aiempaa vähemmän. 15 prosenttia jakaa enemmän varoituksia muille, 14 prosenttia pelkää joutuvansa uudelleen huijauksen kohteeksi ja 8 prosenttia kertoo huijausten aiheuttaneen stressiä tai ahdistusta.

Rahaa menettäneillä seuraukset voivat olla huomattavasti vakavampia: 15 prosentilla on ollut vaikeuksia maksaa välttämättömiä menoja, 12 prosenttia on joutunut vähentämään normaalia kulutustaan, 10 prosenttia on tarvinnut läheisiltään taloudellista tukea ja 6 prosenttia on joutunut ottamaan lainaa tai velkaantumaan.

Digiturvallisuus on kääntymässä parempaan

Digiturvallisuudessa on nähtävissä myönteistä kehitystä, mutta käytännössä turvallisuus rakentuu ihmisen arjessa. Digiturvabarometri 2026 ei anna kuvaa riskittömästä digitaalisesta Suomesta, vaan päinvastoin: huijausyrityksiä kohtaa neljä viidestä suomalaisesta, joka viides kohtaa niitä vähintään viikoittain ja huoli digihuijauksista on kasvanut voimakkaasti.

Vuoden 2026 ratkaiseva ero aiempiin vuosiin on kuitenkin se, että uhkien kasvu ei enää automaattisesti tarkoita luottamuksen heikkenemistä.

- Luottamusindeksi on kääntynyt parempaan suuntaan.
- Turvallisuuden tunne on kasvanut.
- Useiden huijaustyyppien kohtaaminen on vähentynyt.
- Kansalaiset ryhtyvät aiempaa enemmän konkreettisiin suojatoimiin.
- Digiturvallisuuden eteen ollaan valmiita näkemään enemmän vaivaa.
- Viranomaisiin, finanssialaan ja keskeisiin suomalaisiin digitaalisiin palveluihin luotetaan vahvasti.

Tekoäly muuttaa toimintaympäristöä ennen näkemättömällä nopeudella. Sen käyttö kasvaa paljon nopeammin kuin siihen kohdistuva luottamus. Tekoäly samaan aikaan sekä vahvistaa kansalaisten mahdollisuuksia suojata itseään että mahdollistaa entistä uskottavampia huijauksia ja muita verkkorikoksia.

Turvallisuus on rakennettava palveluihin sisään

Barometrin keskeinen viesti on, että suomalainen digiyhteiskunta näyttää vuonna 2026 ensimmäisiä merkkejä vahvistuvasta digitaalisesta kriisinkestävyydestä. Luottamus ei enää heikkene ja turvallisuuden tunne on noussut, vaikka uhat eivät ole poistuneet eikä luottamus ole vielä palautunut.

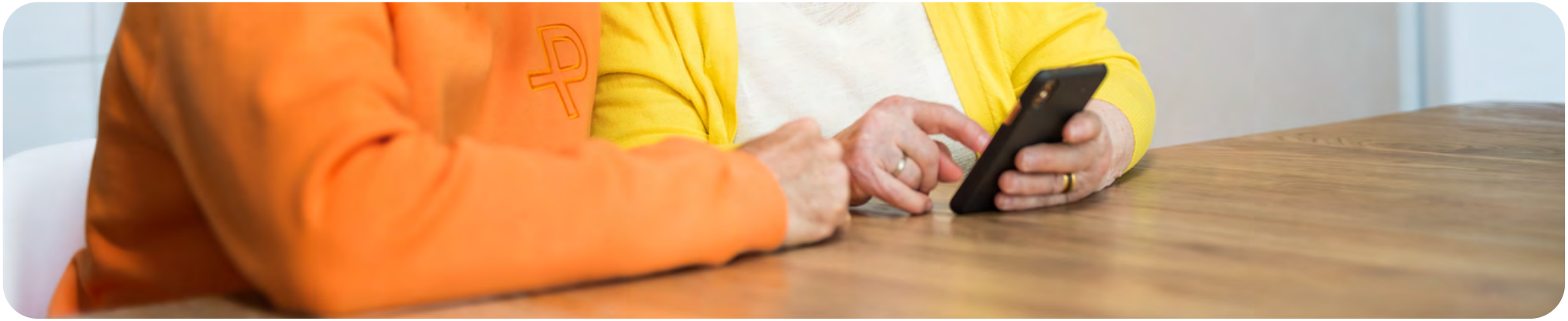
Seuraava askel ei ole vain parempi teknologia eikä valistuneempi kansalainen, vaan turvallisuus, joka on rakennettu palveluihin sisään: helppo tapa varmistaa yhteydenoton aitous, matala kynnys ilmoittaa ongelmista, viestinnän edelleen kehittäminen ja selvä vastuunjako pankkien, viranomaisten, operaattorien ja alustojen kesken.

Kansalaisen osaaminen on kokonaisuuden osa, ei sen korvike.

12 keskeistä mittaria seurattavaksi

Mittari	2026	Muutos
Luottamusindeksi (vahvistunut – heikentynyt)	−20	+7 pistettä
Kokee arjen digiympäristön turvalliseksi	86 %	+4 %-yks.
Luottaa tekoälypalveluiden tuottamaan sisältöön	23 %	+ 2 %
Käyttää tekoälypalveluja vähintään kuukausittain	47 %	+16 %-yks.
Arvioi osaavansa käyttää digipalveluja turvallisesti	89 %	−2 %-yks.
Digihuijaukset huolestuttavat melko tai erittäin paljon	69 %	+10 %-yks.
Uhkien toteutuminen, kokonaiskeskiarvo	30 %	−4 %-yks.
On kohdannut digihuijausyrityksiä	81 %	•
On menettänyt rahaa digihuijauksen takia	10 %	•
Pitää Suomen digitaalista toimintaympäristöä turvallisena	70 %	•
Teki rikosilmoituksen digihuijauksesta, petoksesta tai rikoksesta	58 %	•
Ei ilmoittanut kohtaamastaan huijauksesta kenellekään	43 %	•

Kymmenen ohjetta digikäyttäjille
– näin vältät digihuijauksia ja toimit, jos joudut huijatuksi



1. Pysähdy aina, kun sinua hoputetaan

Kiire, pelottelu ja painostaminen ovat digihuijareiden tavallisia keinoja. Jos sinua vaaditaan toimimaan heti, maksamaan nopeasti tai pitämään asia salassa, pysähdy ja mieti ennen kuin teet mitään.

2. Älä luota pelkkään nimeen, numeroon tai ulkonäköön

Puhelu, viesti tai verkkosivu voi näyttää tulevan pankilta, viranomaiselta, yritykseltä tai jopa tutulta ihmiseltä. Varmista yhteydenotto itse toisesta kanavasta käyttämällä ennestään tuntemaasi numeroa, sovellusta tai verkkosivustoa. Tai kilauta kaverille!

3. Älä tunnistaudu tai maksa toisen ohjeiden mukaan

Älä kirjaudu pankkiin, hyväksy tunnistautumista tai tee maksua yllättävän puhelun tai viestin perusteella. Avaa pankin tai muun palvelun sovellus tai verkkosivu aina itse. Jos käytät selainta, kirjoita verkko-osoite itse selaimen osoiteriville. Älä koskaan siirry palveluun saamastasi linkistä tai hakukoneen tuloksien kautta.

Rikollinen ei yleensä pysty aiheuttamaan merkittävää vahinkoa, ellei hän saa haltuunsa tunnuksiasi, pääse tunnistautumaan palveluihin puolestasi tai kaappaa identiteettiäsi.

4. Tarkista ennen kuin klikkaat, ostat tai maksat

Katso lähettäjä, verkkosivun osoite, maksunsaaja ja se, onko viestissä jotakin epäloogista. Jos tarjous vaikuttaa liian hyvältä ollakseen totta tai jokin siinä epäilyttää muuten, älä jatka ennen kuin olet varmistanut asian.

5. Suojaa tilisi ja laitteesi etukäteen

Käytä eri palveluissa laadukkaita eri salasanoja ja ota käyttöön monivaiheinen tunnistautuminen aina kun mahdollista. Päivitä laitteet ja sovellukset sekä hyödynnä pankin tarjoamia maksu-, kortti- ja käyttörajoja. Pieni vaiva etukäteen voi estää suuren vahingon.

6. Jos epäilet huijausta, keskeytä tilanne heti

Älä jatka keskustelua, klikkaa uusia linkkejä tai lähetä lisää tietoja. Sulje puhelu tai viestiyhteys ja selvitä rauhassa, mitä on tapahtunut. Huijauksen voi vielä pysäyttää, vaikka olisit jo ehtinyt tehdä jotakin, esimerkiksi luovuttaa tietojasi.

7. Jos annoit tietoja tai rahaa, toimi nopeasti

Ota heti yhteyttä pankkiin tai maksupalveluun, jos olet maksanut, luovuttanut pankki- tai korttitietoja tai hyväksynyt epäilyttävän maksutapahtuman tai tilisiirron. Sulje tarvittaessa kortit ja tunnukset sekä vaihda vaarantuneet salasanat.

Mitä nopeammin toimit, sitä paremmat mahdollisuudet vahinkojen rajoittamiseen on.

8. Ilmoita tapahtuneesta – älä jää yksin

Tallenna viestit, puhelinnumerot, verkkosoitteet, kuitit ja muut tapahtumaan liittyvät tiedot. Ilmoita tapauksesta tilanteen mukaan pankille, palveluntarjoajalle ja poliisille sekä tarvittaessa muille viranomaisille.

9. Suojaa yksityisyyttäsi – pidä digitaalinen jalanjälkesi hallinnassa

Mieti ennen julkaisemista, mitä tietoja jaat itsestäsi, läheisistäsi tai arjestasi verkossa. Vältä tarpeettomien henkilötietojen, valokuvien, sijaintitietojen, matkasuunnitelmien tai arkaluonteisten tietojen julkaisemista. Tarkista myös säännöllisesti sovellusten ja palveluiden yksityisyysasetukset sekä se, mitä tietoja sinusta löytyy julkisesti verkosta.

Huijatuksi joutumista ei tarvitse hävetä: ilmoittamalla autat estämään muita joutumasta saman huijauksen kohteeksi. Pienikin digitaalinen johtolanka voi auttaa saamaan rikollisia kiinni!

10. Hyödynnä tekoälyä digihuijausten tunnistamisessa

Voit kysyä tekoälyltä esimerkiksi:
”Vaikuttaako tämä sivusto digihuijaukselta?”. Liitä tai kopioi kysymyksen perään tarkistettava verkko-osoite.

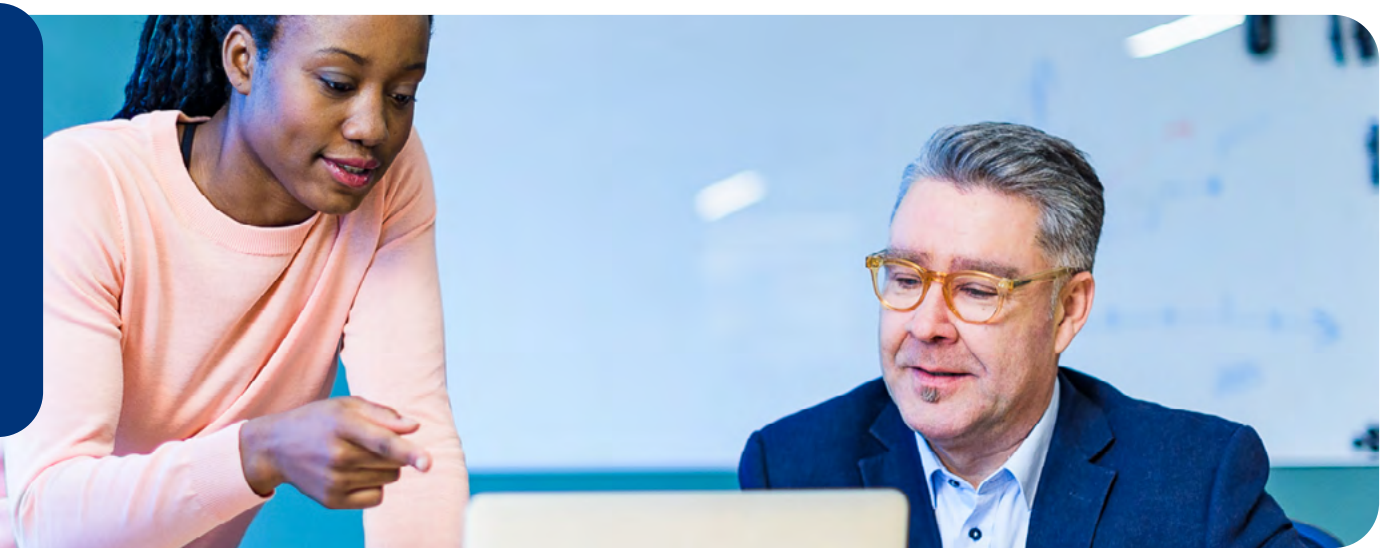
Voit myös ottaa viestistä näyttökuvan tai valokuvan ja pyytää tekoälyä arvioimaan, näkyykö siinä huijauksen merkkejä.

Muista kuitenkin: tekoäly voi erehtyä. Vaikka se arvioisi sivun tai viestin turvalliseksi, tarkista silti osoite, lähettäjä ja muut varoitusmerkit ennen kuin kirjaudut, maksat tai annat henkilötietoja. Tekoäly on hyvä toinen silmäpari, ei lopullinen totuus.

12 suositusta organisaatioille ja järjestöille

Vuoden 2026 Digiturvabarometrissa näkyvä luottamuskäänne voidaan muuttaa pysyväksi suunnaksi, jos

- turvallisuus näkyy käyttäjälle,
- turvallinen toiminta tehdään helpoksi ja
- organisaatiot ottavat vielä aktiivisemman roolin digihuijausten ehkäisemisessä.



1. Mahdollista digihuijauksista ilmoittaminen yhdeltä luukulta ja tarkista oma prosessisi

Rakenna asiakkaalle selkeä ilmoitus- ja palvelupolku tilanteisiin, joissa hän epäilee joutuneensa digihuijauksen kohteeksi. Organisaation on osattava käynnistää omat suojaavat toimenpiteensä sekä ohjata asiakas tarvittaessa esimerkiksi poliisin, Kyberturvallisuuskeskuksen, tietosuojavaltuutetun toimiston, pankin tai muun toimivaltaisen tahon palveluihin.

Testaa samalla, että oma henkilöstö tuntee prosessin ja osaa toimia oikein ja viivyttelemättä.

2. Harjoittele digiuhkia aidontuntuisilla tilanteilla

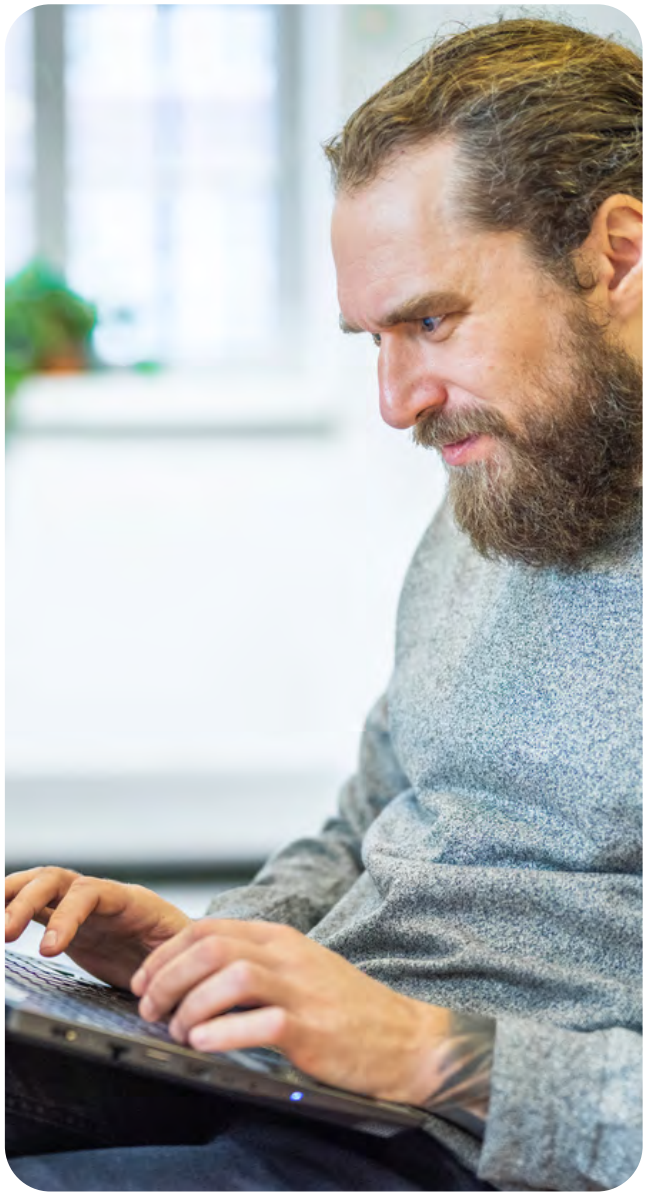
Älä jätä koulutusta pelkkien ohjeiden ja verkkokurssien varaan. Pidä harjoituksia esimerkiksi huijauspuheluista, tietojenkalastelusta, tilisiirroista, pikamaksuista, kiireeseen perustuvista pyynnöistä sekä pankkina, viranomaisena, johtajana tai muuna luotettuna tahona esiintymisestä.

Harjoituta organisaatiossa erityisesti tilanteen pysäyttämistä, yhteydenoton tarkistamista toisesta kanavasta sekä nopeaa ilmoittamista. Testaa samalla, toimivatko organisaation omat ilmoituskanavat käytännössä.

3. Korjaa vahvan tunnistautumisen koulutusvaje

Vahva tunnistautuminen ei itsessään estä huijausta, jos käyttäjä saadaan hyväksymään rikollisen käynnistämä tapahtuma. Opeta käyttäjiä aina tarkistamaan, mitä he ovat hyväksymässä ja missä palvelussa tunnistautuminen tapahtuu.

Korosta erityisesti, ettei yllättävän puhelun, viestin tai muun yhteydenoton perusteella pidä automaattisesti tunnistautua pankkitunnuksilla tai mobiilivarmenteella. Ohjeista keskeyttämään tilanne ja avaamaan oikea palvelu itse tunnetusta osoitteesta tai sovelluksesta.



4. Panosta tekoälyn turvallisen käytön perustaitoihin

Opeta henkilöstölle, mitä tietoja tekoälypalveluihin voidaan syöttää ja mitä ei. Järjestä harjoituksia henkilötietojen ja luottamuksellisten tietojen käsittelystä, tekoälyn tuottamien vastausten tarkistamisesta, lähdekritiikistä sekä tekoälyavusteisten huijausten, kuten uskottavien viestien, kuvien, äänen ja videoiden, tunnistamisesta.

Ohjaa henkilöstö käyttämään työtehtävissä organisaation hyväksymiä ja tietoturvallisesti hallinnoituja tekoälypalveluja, mutta kannusta opiskelemaan näitä myös vapaa-ajalla.

5. Hyödynnä viestinnässä luotettuja viestinviejiä

Digihuijausten torjunta ei onnistu yhden organisaation viestinnällä. Pankkien, viranomaisten, teleoperaattorien, uutismedian, työpaikkojen, oppilaitosten, järjestöjen ja läheisten viestit voivat täydentää ja vahvistaa toisiaan.

Kohdenna viestit eri käyttäjäryhmille ja niihin kanaviin, joissa he asioivat. Toista keskeisiä toimintamalleja riittävän usein ja reagoi nopeasti uusiin huijausilmiöihin.

6. Mittaa osaamista käyttäytymisen, ei vain itsearvion perusteella

Älä arvioi digiturvaosaamista pelkästään kysymällä, kuinka hyvinä ihmiset itse pitävät taitojaan. Täydennä kyselyitä tilannepohjaisilla tehtävillä, simulaatioilla ja harjoituksilla.

Seuraa esimerkiksi, osaavatko käyttäjät keskeyttää epäilyttävän tilanteen, tarkistaa lähettäjän tai yhteydenoton toisesta kanavasta, varmistaa maksupyynnön ja ilmoittaa epäilyttävästä tapahtumasta. Mittaa ennen kaikkea turvallista toimintaa käytännössä.

7. Tue huijauksen kohteeksi joutunutta ilman syyllistämistä

Tarjoa nopeasti apua maksujen pysäyttämiseen, tunnusten ja henkilötietojen suojaamiseen, rikosilmoituksen tekemiseen sekä tarvittaessa talous- ja velkaneuvonnan sekä henkisen tuen tai kriisiavun löytämiseen. Kuuntele rauhallisesti ja vältä kysymyksiä, jotka voivat lisätä häpeää tai syyllisyyttä.

Huijaukset on tietoisesti rakennettu hyödyntämään kiirettä, pelkoa, luottamusta ja auktoriteetteja. Keskity siihen, mitä voidaan vielä estää, suojata, palauttaa ja ilmoittaa. Kiitä kertomisesta – nopea ilmoittaminen voi ehkäistä muiden joutumista saman huijauksen kohteeksi.

8. Rakenna huijausten torjunta palveluihin sisään

Älä jätä turvallisuutta vain käyttäjän tarkkaavaisuuden ja huijausten tunnistamiskyvyn varaan. Hyödynnä palveluissa poikkeavien kirjautumisten, maksujen ja käyttäytymisen tunnistamista, riskiperusteista lisävarmistusta sekä tarkoituksenmukaisia rajoituksia ja viiveitä.

Suunnittele käyttöliittymät niin, että poikkeuksellinen tai riskialtis toiminta herättää käyttäjän huomion ennen hyväksymistä. Turvallisen vaihtoehdon pitää olla käyttäjälle myös helpoin vaihtoehto.

Pyri hyödyntämään turvallisuutta edistävien tekoälypalveluiden hyödyntämistä 24/7 -tyyppisesti.

9. Tee organisaation yhteydenottojen aitouden tarkistamisesta helppoa

Tarjoa asiakkaalle yksinkertainen tapa varmistaa, onko viesti, puhelu tai muu yhteydenotto todella organisaatioltasi. Suosi tunnettuja asiointikanavia, sovellusten sisäisiä viestejä ja selkeitä takaisinsoittomenettelyjä.

Vältä toimintatapoja, jotka totuttavat asiakkaita kirjautumaan palveluihin yllättävien viestien linkeistä. Kerro selkeästi myös, mitä organisaatiosi ei koskaan pyydä asiakasta tekemään puhelimessa, viestillä tai sähköpostilla.

10. Suojaa erityisesti maksut ja muut vaikeasti peruttavat toimenpiteet

Tunnista palveluistasi tilanteet, joissa huijauksen seuraukset voivat muuttua nopeasti merkittäviksi: tilisiirrot, uuden maksunsaajan lisääminen, tilinumeromuutokset, käyttöoikeuksien myöntäminen, henkilötietojen luovuttaminen ja vahvan tunnistautumisen hyväksyminen.

Käytä riskin mukaan riippumatonta varmennusta, kahden henkilön hyväksyntää, maksurajoja, lisävahvistusta tai lyhyttä viivettä. Tavoitteena on luoda viimeinen mahdollisuus pysäyttää huijaus ennen peruuttamatonta toimenpidettä.

11. Torju oman organisaatiosi nimissä tehtäviä huijauksia aktiivisesti

Seuraa, miten organisaatiosi nimeä, verkkotunnuksia, logoja, puhelinnumeroita ja henkilöstön nimiä käytetään verkossa. Huolehdi sähköpostin teknisistä suojauksista, kuten SPF-, DKIM- ja DMARC-määrityksistä.

Seuraa samankaltaisia verkkotunnuksia, valeprofiileja sekä huijaussivustoja ja luo toimintamalli niiden nopeaan ilmoittamiseen ja alasajoon. Kerro myös asiakkaille nopeasti, jos organisaatiosi nimissä on käynnissä huijauskampanja.

12. Jaa huijaustietoa nopeasti organisaatiorajojen yli

Yksi havaittu huijaus voi olla osa kampanjaa, joka kohdistuu samanaikaisesti tuhansiin ihmisiin ja useisiin organisaatioihin. Luo toimintamalli, jolla haitalliset verkkotunnukset, URL-osoitteet, puhelinnumerot, tilinumerot, maksunsaajat ja muut tunnistetiedot voidaan välittää nopeasti niitä tarvitseville toimijoille.

Tee yhteistyötä viranomaisten, pankkien, teleoperaattoreiden, teknologiayritysten ja muiden kumppaneiden kanssa. Tavoitteena on lyhentää ketjua havainnosta ilmoitukseen, estoon ja tarvittaessa järjestelmien alasajoon.

Suosittelemme organisaatioita

- osallistumaan maksuttomaan vuosittaiseen Taisto kyber- ja digiturvaharjoitukseen: dvv.fi/taisto
- tutustumaan “OrganisaatioItani on viety tai vuotanut tietoja” -oppaaseen: www.suomi.fi/oppaat/tietomurto

DIGI- JA VÄESTÖTIETO-VIRASTO