Tieto- ja Digiturva

Wellamo-opisto


Tietosuoja
• Lainmukaisuus ja yksilön oikeudet
• Onko tiedon keruu perusteltua?
Digiturva
• Turvallinen digikäyttäytyminen
• Huijausten tunnistus
Henkilötietojen turvallinen käsittely
Yhteinen tavoite:
Suojaa tietoja ja ihmisiä
Tietoturva
• Tekninen suojaus
• Salaus ja varmuuskopiot

Tietoturva

Tietoturva suojaa tietoa

- Luottamuksellisuus (vain oikeat henkilöt pääsevät tietoihin
- Eheys (tietoa ei muuteta luvatta)
- Saatavuus (tieto on käytettävissä silloin kun sitä tarvitaan)

Tietoturva, esimerkkejä

Ennen kaikkea teknistä ja hallinnollista suojaamista

- Viranomaisen henkilörekisteri on suojattu salasanalla ja käyttöoikeudet on rajattu vain tietylle henkilöstölle -> *Luottamuksellisuus*
- Tiedosto tallennetaan pilvipalveluun ja siitä otetaan automaattinen varmuuskopio -> *Tiedon saatavuus ja eheys*
- Virustorjuntaohjelmisto estää kiristysohjelman pääsyn tietokoneelle -> *Suojataan tiedon eheys ja saatavuus*
- Käyttöjärjestelmä- ja sovelluspäivitykset
- Vahvojen salasanojen ja kaksivaiheisen tunnistautumisen käyttäminen

Tietosuoja

Keskittyy ihmisen oikeuksiin suhteessa hänen henkilötietoihinsa

Minulla on oikeuksia – en ole vain datan lähde

Perustuu EU:n yleiseen tietosuoja-asetukseen eli General Data Protection Regulation (GDPR).

Ydinkohdat:

- Henkilötietojen käsittelylle tulee olla laillinen peruste
- Kerätään vain tarpeellinen määrä tietoa
- Informoidaan rekisteröityä miksi tietoja kerätään
- Säilytetään tietoa vain niin kauan kuin on tarpeen
- Rekisteröidyn oikeudet (tarkastus, oikaisu, poistaminen)

Tietosuoja, esimerkkejä

Kameravalvonta

- Onko laillinen peruste
- Onko asiasta ilmoitettu
- Kauanko tallenteita säilytetään

Puhelimen sovellus pyytää käyttölupaa

- Taskulamppusovellus pyytää pääsyä yhteystietoihin?
- Kartta-sovellus pyytää lupaa sijaintiin?

Digiturva

- Digiturvassa keskiössä on ihminen ja hänen toimintansa, ei pelkkä tieto.
- Digiturva liittyy **käyttäytymiseen, osaamiseen ja riskiymmärrykseen** sisältäen:
  - Turvallisen verkkokäyttäytymisen
  - Huijausten tunnistamisen
  - Digihyvinvoinnin
  - Identiteetin ja yksityisyyden suojaamisen

Digiturva, esimerkkejä

- Seniori tunnistaa pankin nimissä tulleen huijausviestin eikä klikkaa linkkiä → kyky toimia turvallisesti
- Some-käyttäjä säätää yksityisyysasetukset niin, etteivät kaikki näe hänen kuviaan → Yksityisyyden suoja
- Henkilö ei jaa verkossa henkilötunnustaan tai tarkkoja matkasuunnitelmiaan julkisesti → Identiteettisuoja
- Lapselle opetetaan, etteivät kaikki verkossa kohdatut ihmiset ja väitteet ole luotettavia.
  → digihyvinvointi, turvallisuus digitaalisessa ympäristössä

Digiturva

Tietoturva on osa digiturvaa. Ilman tietoturvaa ei ole digiturvaa, mutta pelkkä tietoturva ei riitä.

Esimerkki: Pankkitunnukset

- Tietoturva: Pankki suojaa järjestelmänsä, käyttää vahvaa tunnistautumista ja salattua yhteyttä.
- Digiturva: Asiakas ei anna pankkitunnuksiaan kenellekään

Molempia tarvitaan

Tietojen kalastelu

- verkkohuijaukset

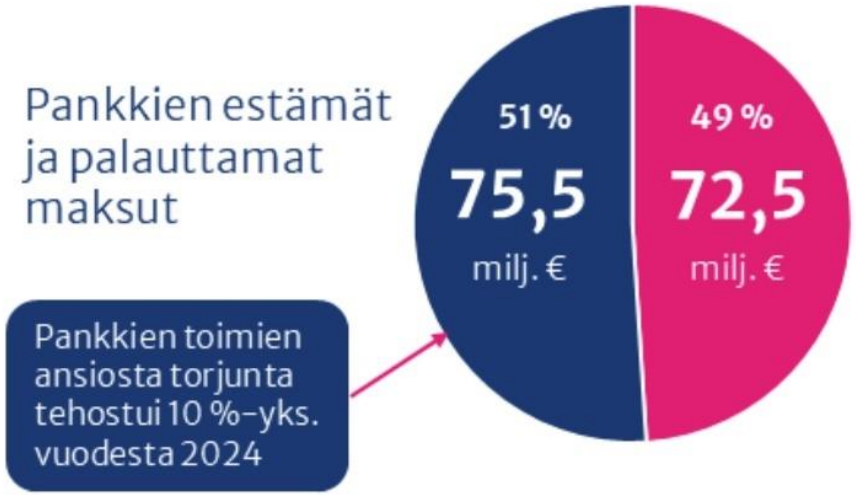
HUIJAUKSET JA PETOKSET

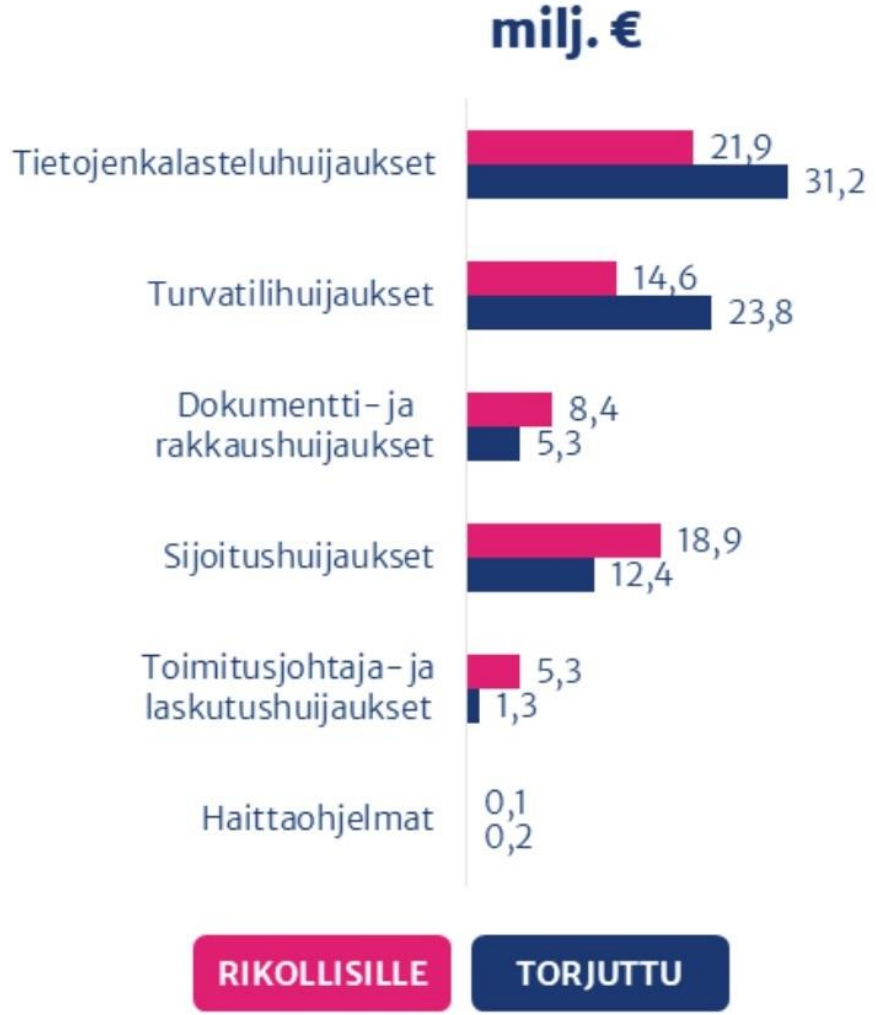
Pankkien tietoon tulleet huijaukset 2025

Huijauksia yhteensä 2025

148,0 milj. €

+38 % vrt. 2024





Lähde: FA Finanssiala ry

Mitä tietoja halutaan?

Esimerkkejä halutuista tiedoista

Tunnistautumistiedot

- Käyttäjätunnukset, salasanat, pinkoodit…

Henkilötiedot

Kaikki tiedot, jotka liittyvät henkilön tunnistamiseen mm:

- Nimi, puhelinnumero, sotu, sähköpostiosoite, osoite, sijainti

Tiedot sosiaalisista suhteista, sukulaisista

- Melkein mitä vain, mitä voi hyödyntää muiden tietojen kanssa tai luotaessa uskottavaa tarinaa isompaan huijaukseen

Mihin tietoja käytetään?

Taloudellinen hyöty

- Verkkopankkihuijaus
- Sijoitushuijaukset
- Lahjoitus/avustushuijaukset
- Väärillä henkilötiedoilla tehdyt tilaukset ja tavaran myyminen
- Henkilötietojen hyödyntäminen osana muita rikoksia
- Myyminen toisille rikollisille

Identiteettivarkaus
Rikollinen esiintyy sinuna

- Tuotteiden tilaus osamaksusopimuksella sinun laskuusi, rikollisen ilmoittamaan pakettiautomaatti/poste restante –osoitteeseen
- Tori.fi-, Huuto.net yms. huijaukset sinun identiteetilläsi
- Erilaiset viranomaisilmoitukset: Etuudet, puhtaan identiteetin hankkiminen esim. luottotiedot…
- Myös pikavippien/lainojen saaminen voi onnistua. Kaikki pikavippien tarjoajat eivät toimi säädösten mukaan (sotu voi riittää).

Miten huijaus toimii?

Huijausten keinoja

Psykologiset vaikutuskeinot, manipulaatio

Ihminen saadaan toimimaan enemmän tunteella kuin järjellä

Psykologisia ja sosiaalisia vaikutusmekanismeja

- Tunteisiin vetoaminen
- Luodaan houkutteleva tilanne. Tarjotaan erityistä etua **vain** sinulle.
- Luodaan uhkaava tilanne, jossa uhrin tulee toimia **HETI!** Kiireen ja hädän tuntu
- Rakennetaan luottamusta pidemmällä suhteella, vedotaan haluun auttaa
- Rikollinen väittää edustavansa luotettavaa tahoa, esimerkiksi:
  - Pankki, poliisi, omakanta, posti…
  - Luotettava yritys: Tokmanni, Prisma…
  - Ystävä, oma lapsi…

Keinoja saada tietoja:

- **Huijausviestit joissa linkki/puh.nro huijaussivulle**
  - Sähköpostiviestit
  - Facebook-, Whatsap-, Tekstiviestit
- **Huijauspuhelut**
- Ovella kävijät ("poliisi, huoltomies")

Annat itse tiedot rikolliselle!
Luulet antavasi tietoja viranomaiselle tai hyväksymääsi tarkoitukseen.

- Tekniset keinot
  - Palveluihin murtautuminen (huonot salasanat yms.)

Missä muodossa huijaukset tulevat?

Esimerkkejä huijauksista tekstiviestillä tai sähköpostilla:

- ”Postista” on tullut lähetys jossa jotain epäselvyyttä, klikkaa tätä linkkiä ja tarkista…
- ”Tokmannin lahjakortti”. Olet valittu Tokmannin lahjakortin saajaksi, anna henkilötietosi niin saat 100€ lahjakortin…
- **Klikkaamalla linkkejä siirryt rikollisten tekemille oikean näköisille sivulle antamaan henkilötietojasi.**

- ”Hei äiti/isä! ” Lompakkoni ja puhelimeni ryöstettiin! Lähetän tämän viestin ystäväni puhelimesta. Laita rahaa tälle ystäväni tilille niin hän antaa ne minulle ja voin ostaa puhelimen…”
- **Viesti ei ole aito. Rahat menevät huijarin tilille**

”Pankista” soitetaan, turvatilihuijaus

- Väitetään, että olet tehnyt tilisiirron ulkomaille.
- Soitolla muka varmistettaan onko se totta
- Ehdotetaan uuden tilin avaamista, jonne rahat saadaan turvaan. ”Turvatili”
- Puhutaan tietojenkalasteluhuijauksista ja ettei kannata klikata epämääräisiä linkkejä. Rikollinen rakentaa uskottavuutta ja luottamusta varoittamalla huijauksista.
- Poliisikin mainitaan uskottavuutta ja auktoriteettia vahvistamaan
- videolinkki

Esimerkkejä huijauksista

- **Valeystävä. ”**Kaverisi kaveri” tai huijari joka on kopioinut ystäväsi Fb-tilin pyytää sinua ystäväksesi Facebookissa. Eräänä päivänä hän kertoo jonkin tunteisiin vetoavan tarinan ja pyytää voitko auttaa häntä rahallisesti.
- Valeystävä suosittelee upeaa sijoitusmahdollisuutta jolla hän on rikastunut
- **Romanssihuijaukset,** tunnesiteeseen pohjautuva hyväksikäyttäminen. Huijari jaksaa rakentaa suhdetta pitkään ennen iskua!

Kiristyksiä

- **Haittaohjelmauhkaus**. Jos et maksa rahaa, tietokone lukkiutuu ja menetät kaikki tietokoneen tiedostot
- Väitetään, että olet käynyt internetin ”epämääräisillä” sivustoilla. Yhteydenottaja väittää olevansa Europolin poliisi ja vaatii lisäselvityksiä

Miten välttää huijatuksi tuleminen?

Älä klikkaa epämääräisiä linkkejä

- Älä kirjaudu verkkopankkin tai palveluihin arveluttavassa yhteydenotossa saamasi linkin kautta.

- Älä kirjaudu verkkopankkiin jonkun toisen kehotuksesta.

Suojele tietojasi, terve epäluuloisuus

- Älä anna tai kerro henkilö- tai pankkitietojasi puhelimessa, sähköpostilla tai sosiaalisen median kanavissa.
- Älä anna kenenkään ottaa etäyhteyttä laitteeseesi, mikäli et ole täysin varma tahosta.
- Seuraa uutisointia huijauksista ja ole tietoinen huijareiden tavoista vaikuttaa ja manipuloida.

“Jos jokin on liian hyvää ollakseen totta – se ei todennäköisesti ole totta"

Teknisiä keinoja

➔**Pidä laitteet ja ohjelmat päivitettyinä**

➔**Käytä tarpeeksi pitkiä ja hyviä salasanoja**
(12 merkkiä, eri merkkejä Fa2#)

➔**Vaihda salasanat säännöllisesti**

➔**Eri salasanat eri palveluille**

➔**Ota käyttöön kaksi/monivaiheinen tunnistautuminen**
(varmennuskoodi puhelimelle)

Kirjaudu palveluihin niiden omien sivujen tai mobiilisovelluksen kautta

- Tallenna oikeaksi tarkistettu verkkopankin nettiosoite kirjainmerkiksi ja käytä sitä.
- Oikeat verkko-osoitteet ovat muotoa:

✓ op.fi nordea.fi s-pankki.fi

✗ op-pankki.fi omanordea.fi spankki.fi

- Monet **tietoturvaohjelmat** sisältävät työkaluja joilla tunnistaa tai estää huijaussivustot ja –linkit

- Hanki ja käytä **mobiilivarmennetta** (dna, elisa, telia)

”Pankkiasiointiin kannattaa käyttää pankkien tunnuksia. Kaikkeen muuhun digitaaliseen asiointiin suosittelen ottamaan käyttöön rinnalle myös Mobiilivarmenteen.”

TIETOTURVA-ASIANTUNTIJA MIKKO HYPPÖNEN, WITHSECURE

Mobiilivarmenne

Jos epäilet huijausta:

”Jäitä hattuun”

Katkaise puhelu

Pysähdy ja rauhoitu: Selvitä asiaa ja arvioi luotettavuutta

Selvitä oikeat yhteystiedot ja kysy sieltä

Pyydä apua luotettavalta taholta!

Jos tulit huijatuksi

- **Kuka vain voi tulla huijatuksi**
- Huijatuksi tuleminen aiheuttaa voimakasta häpeää, epätoivoa ja itsesyytöksiä.
- Älä syytä itseäsi! Sinä et ole hölmö vaan huijauksen uhri.
- Myönnä tapahtunut, älä hyssyttele ja jää odottelemaan, vaan toimi pian:

1. Ota yhteyttä pankkiin -> tilien ja korttien sulku
2. Ota yhteyttä poliisiiin, rikosilmoitus
3. **Puhu asiasta!**
   - Läheiset
   - Rikosuhripäivystys

nytvalppaana.fi

- Poliisiin, DVV:n ja Traficomin koostama sivusto

huijaamaton.fi

- Finanssiala ry