Tunnista nettihuijaus

Tietoa nettihuijauksista
lyhyesti ja selkeästi.

huijausinfo.fi

KULUTTAJALIITTO
KONSUMENTFÖRBUNDET

Nettihuijaus tarkoittaa,
että ihmistä huijataan tietokoneen,
puhelimen tai tabletin avulla.
Huijaus voi tapahtua
esimerkiksi Facebookissa tai sähköpostilla.
Rikollinen yrittää saada rahaa tai tärkeitä tietoja.

Tämä opas kertoo

- kuinka tunnistat huijauksen
- mitä teet, jos sinua huijataan
- miten toimit turvallisesti netissä.

Ole varovainen netissä!

Kuluttajaliitto, toukokuu 2026

ISBN 978-952-9787-94-4 (painettu)
ISBN 978-952-9787-95-1 (pdf)

Sisältö

1. Mikä on nettihuijaus?

Nettihuijaukset ovat petoksia,
joita rikolliset tekevät digilaitteiden avulla
(esimerkiksi tietokone, tabletti, puhelin).
Ihmistä voidaan huijata monella tavalla,
kuten Facebookissa tai tekstiviestillä.

Rikolliset yrittävät saada rahaa tai tärkeitä tietoja.
Näitä tietoja ovat esimerkiksi luottokortin tiedot,
pankkitunnukset, henkilötunnus ja salasanat.

Jos rikollinen saa tiedot.
hän voi tehdä ostoksia ja sijoituksia toisen ihmisen nimissä.
Silloin tämä ihminen menettää rahaa.
Rikollinen voi myös toimia netissä tämän ihmisen nimellä
ja huijata muita ihmisiä somessa.
Some tarkoittaa sosiaalista mediaa, kuten Facebookia.

Huijaukset tehdään usein ulkomailta käsin.
Taustalla on yleensä järjestäytynyt rikollisuus.

Rikolliset yrittävät saada

- **pankkikorttien ja luottokorttien tietoja**
- **henkilötietoja, kuten henkilötunnus**
- **käyttäjätietoja, kuten sähköpostin tunnus ja salasana.**

Lue ensin tämä

- Älä vastaa vieraan ihmiseen viestiin,
  jos se on outo tai yllättävä.
  Poista viesti.
- Älä avaa outoa tai yllättävää linkkiä.
  Linkki vie usein rikollisten verkkosivuille.
- Älä usko kaikkea, mitä luet tai näet netissä.
  Kuvia ja videoita on helppo väärentää.
- Muista, että rahaa ei tule mistään ilmaiseksi
  rehellisellä tavalla.
- Rikolliset osaavat tehdä huijauksia,
  jotka näyttävät aidoilta.
- Ole varovainen,
  jos saat ilmoituksen voitosta.
  Jos et osallistu lottopeleihin,
  et voi voittaa niissä.
- Älä koskaan lähetä tilinumeroita, passitietoja
  tai muita henkilötietoja vieraille ihmisille.
- Epäile aina tarjousta,
  jos hinta on liian halpa.
- Älä lähetä rahaa luottokortin numeron
  tai rahansiirtokoodin avulla.
- Selvitä yrityksen sähköpostiosoite.
  Luotettavat yritykset eivät käytä
  ilmaisia postiosoitteita, kuten gmail.

Lähde mukaillen: Suomen poliisi

2. Huijausviestit

Erilaiset huijausviestit ovat hyvin yleisiä.
Melkein kaikki saavat huijausviestejä.

Huijausviesti voi tulla sähköpostilla,
tekstiviestinä tai somen kautta, kuten Facebookissa.

Usein näyttää,
että viestin lähettäjä on viranomainen,
kuten poliisi tai Kela.
Viestissä voi lukea, että palvelussa on

- uusi viesti
- asiakirja, joka täytyy allekirjoittaa
- lasku, joka täytyy maksaa.

Yhteistä huijausviesteille on,
että sinua pyydetään toimimaan.
Usein viestissä lukee, että asialla on kiire.

Muista nämä ohjeet:

Älä avaa huijausviestin linkkiä.
Linkki vie yleensä sivulle,
joka kalastelee tietoja eli varastaa tietosi.
Voit myös saada haittaohjelman laitteellesi.
Älä avaa viestin liitteitä.

Rikolliset lähettävät viestejä myös pankkien nimissä.
Viestissä lukee esimerkiksi,
että pankkikorttisi suljetaan,
jos et päivitä tietojasi.
Viestin mukana on linkki,
jolla tiedot täytyy päivittää.

Älä avaa linkkiä.
Linkki vie huijaussivulle,
joka näyttää verkkopankilta.
Sivun tarkoitus on varastaa pankkitunnuksesi.

Pankit eivät koskaan pyydä,
että päivität tietosi tekstiviestillä tai sähköpostilla.
Vain huijarit tekevät niin!

Rikolliset voivat lähettää tekstiviestin pankin nimissä. Kuva: Magnific.

Huijausviestejä lähetetään esimerkiksi
Postin, kauppojen ja puhelinoperaattoreiden nimissä (esimerkki 4).
Voi myös näyttää siltä,
että viestin lähettäjä on lääkäriasema,
kuten Terveystalo tai Mehiläinen (esimerkki 3).
Viestissä lukee usein,
että asialla on kiire
ja että sinulle tulee ongelmia,
jos et toimi heti.

WhatsApp-huijaukset ovat myös hyvin yleisiä.
Viesteissä voidaan esimerkiksi tarjota työtä,
jossa on hyvä palkka.
Huijari voi myös esittää,
että hän on ihastunut sinuun.

Kiristyshuijausviestit

Rikolliset yrittävät myös kiristää ihmisiä
huijausviestien avulla.
Rikollinen voi väittää,
että hän on kuvannut sinua salaa
tietokoneesi kameralla.
Rikollinen uhkaa julkaista kuvat,
jos et maksa hänelle rahaa.

Viesti on huijaus.
Älä maksa rahoja,
joita rikollinen vaatii.
Tee rikosilmoitus poliisille,
ja säilytä rikollisen viestit.

Alla esimerkkejä siitä, millaisia huijausviestit voivat olla:

Esimerkki 1: Vero-huijausviestit

Rikollinen lähettää viestin verottajan nimissä.
Viestissä lukee, että olet saanut veronpalautusta
tai veronpalautus on peruttu.
Mukana on usein linkki.
Älä avaa linkkiä.

Esimerkki huijausviestistä.
Rikollinen on lähettänyt sen verottajan nimissä.

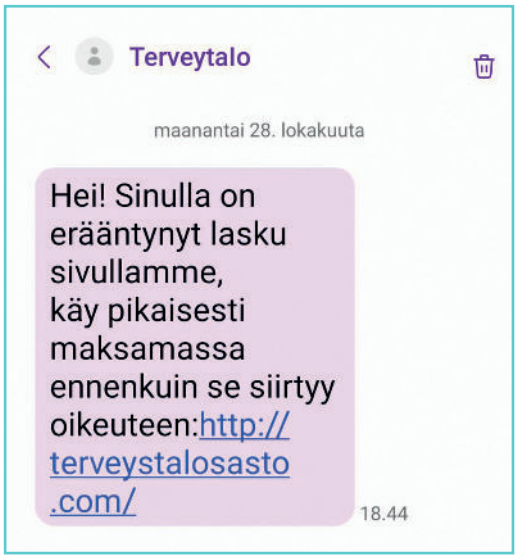
Esimerkki 2: Kanta-huijausviestit

OmaKanta-sivuilta voit katsoa terveystietosi.
Palvelun nimissä lähetetään
kuitenkin paljon huijausviestejä.
Viestissä väitetään, että tilisi on poistettu käytöstä.
Sähköpostin osoite tai linkin verkko-osoite ei ole oikea.
Suomen kieli voi olla huonoa.

Verottaja tai OmaKanta ei lähetä tai pyydä tietoja tekstiviestillä.
Oikeat viestit löytyvät OmaVero- ja OmaKanta-palveluista.

Esimerkki 3: Terveystalo-huijausviestit

Terveystalon nimissä lähetään viestejä,
joissa lukee,
että sinun täytyy maksaa lasku heti.
Lääkäriasemat eivät lähetä tekstiviestejä,
joissa on mukana lasku tai maksumuistutus.



Esimerkki huijausviestistä.
Rikollinen on lähettänyt sen Terveystalon nimissä.

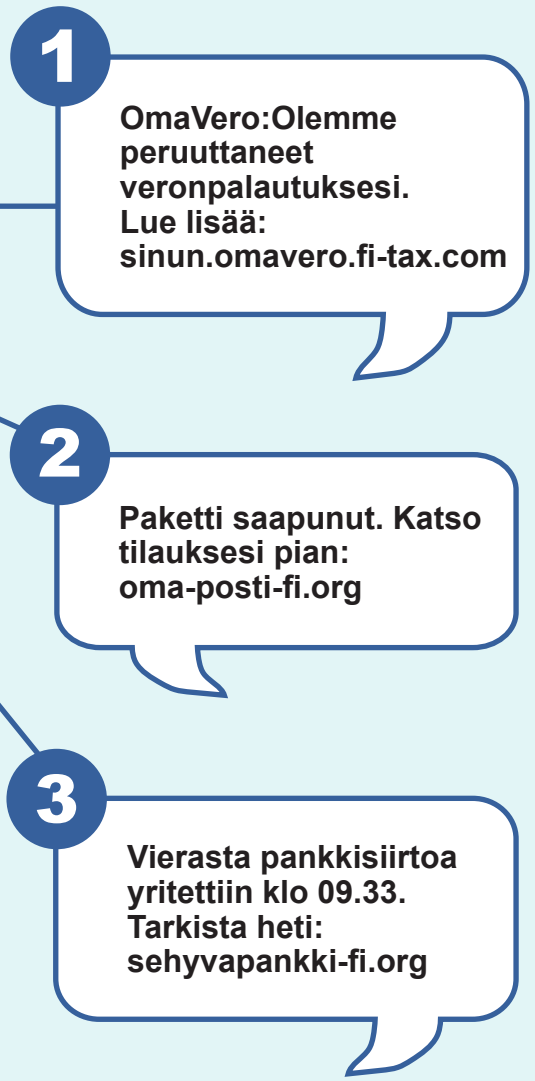
Esimerkki 4: Posti-huijausviestit

Ihmisiä huijataan myös Postin
ja kuljetusyritysten nimissä.
Viestissä lukee,
että olet saanut paketin,
ja mukana on linkki.
Älä avaa linkkiä.
Tarkista, onko viesti aito.
Voit tarkistaa asian esimerkiksi
OmaPosti-sovelluksesta
tai kuljetusyrityksen sivuilta.

Esimerkki huijausviestistä.
Rikollinen on lähettänyt sen Postin nimissä.

Tunnistatko tietojen kalastelun eli varastamisen?

1. Rikolliset lähettävät viestejä esimerkiksi pankin, postin ja viranomaisen nimissä.
2. Viestissä on linkki huijaussivulle.
3. Viesti koskee usein ongelmaa, jolla on kiire.
4. Huijaussivu näyttää oikealta kirjautumissivulta.
5. Huijaussivun voi tunnistaa verkko-osoitteesta. Osoite ei ole oikea.
6. Kirjaudu palveluihin vain virallisten sivujen tai sovellusten kautta.



Toimi näin, jos saat oudon viestin

1. Älä avaa viestin linkkiä.

Älä kirjaudu linkin kautta esimerkiksi verkkopankkiin
tai viranomaisen palveluun.

2. Mene viestin lähettäjän palveluun turvallisesti.

Kirjoita osoite internet-selaimen osoiteriville.
Osoiterivi on sivun yläreunassa.

Voit mennä palveluun myös virallisen sovelluksen kautta.
Sovellus tarkoittaa ohjelmaa eli appia,
joka ladataan puhelimen sovelluskaupasta.

Tarkista palvelusta, onko viesti aito.

3. Voit myös soittaa lähettäjän asiakaspalveluun.

Kysy, onko viesti aito.
Älä vastaa viestiin suoraan,
vaan etsi asiakaspalvelun yhteystiedot netistä.

**4. Jos saat ilmoituksen voitosta,
tarkista, onko kilpailu todellinen.**

Kilpailuista kerrotaan yleensä järjestäjän nettisivuilla.

3. Huijauspuhelut

Huijari voi myös soittaa.
Muista, että pankki, poliisi tai viranomainen
ei koskaan pyydä pankkitunnuksia puhelimessa.

Erilaisia huijauspuheluita

- Huijari soittaa ja esittää **pankin työntekijää.**
  Hän voi sanoa, että tililläsi on outoja maksuja
  ja pyytää siirtämään rahat turvatilille.
- Huijari esittää **lainayrityksen työntekijää.**
  Hän sanoo, että joku on hakenut nimelläsi lainaa.
  Sitten huijari pyytää sinulta pankkitunnuksia.
  Hän väittää, että tunnuksien avulla
  voi estää lainahakemuksen.
- Huijari esittää **poliisia.**
  Hän voi kertoa,
  että pankkitililläsi on outoja maksuja.
  Huijari pyytää pankkitunnuksia,
  jotta asia voidaan selvittää.
- Huijari esittää **perintätoimiston työntekijää.**
  Hän väittää esimerkiksi,
  että sinulla on myöhästynyt lasku,
  joka täytyy maksaa.
- Huijari esittää **hyvinvointialueen työntekijää.**
  Hän voi esimerkiksi yrittää myydä vitamiineja
  ja pyytää henkilökohtaisia tietoja.
- Joskus puhelin soi vain hetken.
  Tavoite on, että soitat takaisin numeroon,
  joka voi olla maksullinen tai siellä vastaa huijari.

Älä soita takaisin tuntemattomaan numeroon,
jos et tiedä kuka on soittanut.

IT-tukihuijaukset

IT-tukihuijaus tarkoittaa,
että huijari soittaa ja esittää tukihenkilöä,
joka auttaa tietokoneen kanssa.
Oikeasti hän haluaa varastaa pankkitietosi ja rahasi.
Huijari puhuu yleensä englantia.

Huijari väittää esimerkiksi näin:

- Soitan Microsoftin toimistosta,
  koska tietokoneessasi on ongelma
  (esimerkiksi virus).
- Ongelma täytyy korjata heti.
  Vain minä voin pelastaa koneesi.

Yleensä huijari pyytää,
että lataat ohjelman,
jonka avulla hän voi käyttää konettasi etänä.

Muista nämä vinkit

- Oikea IT-tukihenkilö ei soita yllättäen,
  vaan soittaja on aina huijari.
- Älä koskaan lataa ohjelmia koneellesi,
  jos joku soittaa ja pyytää niin.
- Älä anna puhelimessa
  pankkitunnuksia tai henkilötunnuksia.
  Niitä ei kysy pankki tai poliisi.
  Niitä kysyy huijari!
- Lopeta puhelu, joka tuntuu oudolta.
- Estä huijarin numero.
  Voit myös estää puhelut,
  jotka tulevat ulkomailta.
  Apua saat puhelinoperaattoriltasi.
- Älä soita takaisin tuntemattomaan numeroon,
  jos soitto tulee yllättäen.

4. Romanssihuijaukset

Netin kautta voi löytää puolison tai ystävän.
Netissä on kuitenkin
paljon romanssihuijareita.
Huijari teeskentelee rakkautta tai ystävyyttä,
mutta haluaa oikeasti rahaa.
Romanssihuijaus voi kestää monta vuotta.
Ihminen voi menettää kaikki rahansa
ja ottaa jopa lainaa.

Huijari vetoaa tunteisiin

Huijari osaa vedota tunteisiin taitavasti.
Hän voi kehua sinua ja olla kiinnostunut elämästäsi.
Huijari voi myös kertoa,
että hänellä on vaikeaa.
Huijari voi kertoa esimerkiksi,
että hänen läheisensä kuolee,
jos et lähetä rahaa sairaalan maksuihin.
Älä usko surullista tarinaa.

Älä myöskään usko,
jos tarina on liian hyvä.
Huijari voi kertoa,
että hän on hyvin rikas.
Hän voi myös kertoa,
että hän on rakastunut sinuun,
vaikka ei edes tunne sinua.

Miten romanssihuijaus toimii?

1. Huijari laittaa viestin somessa
   (kuten Facebook tai Instagram)
   tai deittisovelluksessa (kuten Tinder).

2. Huijari esittää usein,
   että hän on rikas amerikkalainen sotilas,
   komea lääkäri tai kaunis näyttelijä.
   Kuva ja tiedot on keksitty tai varastettu netistä.

3. Huijari kertoo, että hän haluaa tavata sinut,
   mutta matka peruuntuu aina.

4. Huijari pyytää rahaa,
   lahjakortteja tai kalliita tavaroita.
   Hän voi pyytää myös
   kryptovaluuttaa eli virtuaalirahaa.

5. Usein huijari voi lähettää rahaa sinun tilillesi
   ja pyytää,
   että siirrät rahat toisen ihmisen tilille.

6. Jos et lähetä rahaa, huijari voi suuttua.
   Hän voi myös syyllistää ja uhkailla sinua.

7. Huijari yrittää todistaa,
   että hän on luotettava.
   Hän voi esimerkiksi lähettää kuvia,
   joissa hän on lasten kanssa.
   Hän voi myös lähettää linkkejä yrityksensä nettisivuille.

Mieti, onko nettirakkaasi luotettava

Onko sinulla nettirakas?
Jos epäilet, että rakkaasi on huijari,
mieti seuraavia asioita:

- Tiedätkö oikeasti, kuka nettirakkaasi on?
- Oletko koskaan tavannut rakastasi?
- Pyytääkö hän sinulta rahaa esimerkiksi matkaa varten?
- Onko rahoilla kiire?
  Tuntuuko sinusta, että rakkaasi painostaa tai kiristää sinua?

Näin voit estää romanssihuijauksen

- Ole varovainen,
  kun tutustut uusiin ihmisiin netissä.
  Ole varovainen etenkin,
  jos saat vieraalta ihmiseltä viestin.
  Älä vastaa viestiin,
  jos epäilet ihmistä huijariksi.
  Älä hyväksy huijarin kaveripyyntöä.
- Älä usko kaikkea,
  mitä uusi ihminen kertoo sinulle.
- Yritä varmistaa uuden tuttusi henkilöllisyys.
  Voit esimerkiksi etsiä hänestä tietoa netistä.
- Älä lähetä uudelle tutullesi rahaa, lahjakortteja tai tavaroita.
  Älä myöskään lähetä mitään tietojasi
  tai kuvia passistasi.
- Jos olet jo antanut rahaa,
  lopeta se heti.
  Ilmoita huijauksesta omaan pankkiisi
  ja tee rikosilmoitus poliisille
- Pyydä tapaamista ja sitä,
  että ihminen maksaa itse matkansa.
  Huijari ei maksa matkaa ja peruu tapaamisen.
- Puhu läheisesi kanssa uudesta tutustasi,
  vaikka huijari kieltäisi sen.

5. Nettikaupassa huijaus

Nykyään netistä voi ostaa melkein kaikkea.
Netissä on myös kirpputoreja,
joista voi ostaa käytettyjä tavaroita
(esimerkiksi Tori.fi ja Facebook Marketplace).

Joskus nettikaupoissa huijataan.
Silloin asiakas maksaa tavaran tai palvelun,
mutta ei saa sitä.
Huijaus voi koskea esimerkiksi vaatetta,
puhelinta tai vuokramökkiä.
Rikollinen saa rahat.

Rikolliset tekevät huijausmainoksia
ja sivuja, jotka näyttävät oikeilta nettikaupoilta.
Netin kirpputoreilla rikolliset
esittävät ostajaa tai myyjää,
mutta henkilötiedot on keksitty.

Älä osta kiireellä!
Harkitse ostosta rauhassa.
Tarkista myös,
onko nettikauppa luotettava.

Näin voit estää huijauksen nettikaupassa

Muista, että mikään ei ole ilmaista!
Liian hyvä tarjous on huijaus.
Älä kiirehdi, vaan harkitse ostosta rauhassa.

Tee ostoksia vain luotettavilla sivuilla.
Käytä tuttuja nettikauppoja
tai lue muiden kokemuksia kaupasta
(käytä Googlea tai muuta hakukonetta).
Katso myös, että kaupan sivuilla on nämä tiedot:
katuosoite, sähköposti, puhelinnumero.

Maksa aina luottokortilla, jos voit.
Luottokortti (credit) tarjoaa paremman suojan
kuin pankkikortti (debit).
Voit saada rahasi takaisin pankilta,
jos sinulle tulee ongelmia.

Lue tilausehdot huolellisesti.
Säilytä kaikki kaupan viestit,
tilausvahvistus ja kuitti.

Nettikirpputorilla muista nämä asiat:

- Tarkista myyjän tiedot ja tuotteen kuvat.
  Onko kuva itse otettu vai kuvakaappaus?
- Mieti, onko hinta liian halpa tai liian kallis.
- Mieti, onko tuote aito.
  Voit pyytää todisteita, esimerkiksi ostokuitin.
- Jos mahdollista, sovi tapaaminen.
  Silloin voit tutustua tavaraan.
- Käytä turvallisia maksutapoja
  (kuten pankit, MobilePay, PayPal).
- Pyydä myyjältä yhteystiedot ennen maksua.

Esimerkki valenettikaupasta:

Suomen kielen seassa on vieraskielisiä sanoja.

Tarjous on voimassa vain vähän aikaa.

Alennukset ovat suuria.

Kuvat näyttävät siltä, että ne on otettu kuvapankista tai tehty tekoälyllä. Kuvat voivat olla myös keskenään erityylisiä.

Kuvassa on esimerkki valenettikaupasta, jonka Kuluttajaliitto on tehnyt.

Tarjoukset ovat voimassa vain vähän aikaa. Ostaja yritetään saada toimimaan nopeasti.

Valenettikauppa myy usein hyvin erilaisia tavaroita. Esimerkiksi vaatekaupassa voidaan myydä myös perämoottoreita ja ruokaa.

Tarkista aina ennen ostamista, että yrityksen sivuilla on nämä tiedot

- Yrityksen nimi, osoite, puhelin ja sähköposti.
- Tuotteen tai palvelun sisältö ja hinta.
- Toimitusmaksu ja muut maksut.
- Tieto siitä, miten ja milloin saat tuotteen.
- Onko tilaus kertatilaus vai kestotilaus.
  (Kestotilaus jatkuu automaattisesti.)
- Miten tilauksen voi peruuttaa tai palvelun sulkea.
- Miten maksu tapahtuu ja millä ehdoilla.
- Miten voit tehdä valituksen eli reklamaation.

Tarkista yrityksen tiedot ennen kuin ostat tuotteita nettikaupasta. Kuva: Magnific.

6. Sijoitushuijaukset

Sijoitushuijaus tarkoittaa,
että ihminen huijataan sijoittamaan
tai antamaan rahaa asiaan,
jota ei ole olemassa
Huijaus voi koskea esimerkiksi
osakkeita, joukkolainaa tai kryptovaluuttaa.
(Kryptovaluutta on virtuaalista rahaa,
kuten Bitcoin).

Usein huijari väittää, että

- tämä erikoistarjous on juuri sinulle
- voit rikastua nopeasti ja helposti
- tarjous päättyy pian – toimi heti.

Netissä voi olla valeuutisia ja valemainoksia,
joissa on julkisuuden henkilöitä.
Uutisessa voi olla kuva näyttelijästä tai poliitikosta,
joka on saanut paljon rahaa Bitcoin-sijoituksen avulla.
Uutinen ei ole totta.

Sijoitushuijarit mainostavat myös somessa
ja hakukoneissa (kuten Facebook, Tinder ja Google).
Huijari voi myös soittaa tai lähettää viestejä.

Sijoitushuijauksen uhri voi menettää paljon rahaa,
jopa satoja tuhansia euroja.

Näin voit estää sijoitushuijauksen

- Muista, että vain huijari tarjoaa puhelimessa ilmaisia sijoitusneuvoja, joiden avulla saa paljon rahaa.
- Älä sijoita rahaa mainosten perusteella. Esimerkiksi Facebookissa on valemainoksia.
- Varmista, että sijoituskohde on luotettava. Saat apua esimerkiksi pankista, jos et tiedä, onko kohde aito vai huijausta.
- Älä sijoita rahaa kohteisiin, joita et ymmärrä. Ole varovainen etenkin kryptovaluutan eli virtuaalisen rahan kanssa. Siihen liittyy paljon huijauksia ja riskejä.

Esimerkki sijoitushuijauksesta

Sijoitushuijausta varten tehdään usein huijaussivu, jota mainostetaan somessa.
Kuvan huijaussivulla on otsikko, joka vetoaa tunteisiin.
Sivulla annetaan tarkat tiedot sijoittamisesta.
Sivulla on käytetty Ylen toimittaja Tommy Fräntin ja presidentti Sauli Niinistön kuvaa.

7. Tekoälyn käyttö huijauksissa

Tekoälystä on paljon hyötyä,
mutta sitä käytetään myös huijauksiin.

Tekoäly osaa tehdä tekstiä, kuvia, videoita ja ääntä.
Rikolliset tekevät tekoälyn avulla
esimerkiksi valeuutisia,
jotka eivät ole totta.
Rikolliset tekevät myös huijauksia,
joissa kalastellaan eli varastetaan henkilötietoja.

Esimerkki videosta, jonka tekemiseen on käytetty tekoälyä

Kuvakaappaus Ilta-Sanomien nettisivuilta.

Rikolliset tekivät tekoälyn avulla huijausvideon
pääministeri Petteri Orposta.
Orpo ei oikeasti esiinny videolla,
vaan video on syväväärennös.
Videota käytettiin sijoitushuijauksessa.

Esimerkkejä huijauksista, jotka on tehty tekoälyllä

Puhelut:
Huijari voi soittaa tekoälyn avulla puhelun,
jossa hän käyttää väärää ääntä.
Esimerkiksi voi kuulostaa siltä,
että oma lapsi soittaa ja pyytää rahaa.

Työntekijälle voidaan soittaa puhelu,
jossa huijari käyttää toimitusjohtajan ääntä.
Johtaja pyytää siirtämään rahaa nopeasti.

Videot:
Tekoälyn avulla voi tehdä videoita,
jotka näyttävät todella aidoilta.
Videon nimi on syväväärennös eli deepfake.
Videolla voi esiintyä julkisuuden henkilö,
mutta se on huijausta.

Myös videopuheluissa huijataan.
Huijari voi soittaa Whats App -videopuhelun,
jossa hän esittää tuttua ihmistä ja pyytää rahaa.
Ihmisen ääni ja kuva on otettu
esimerkiksi somen videosta.

Viestit:
Tekoäly osaa kirjoittaa viestejä,
jotka näyttävät aidoilta.

Valokuvat:
Tekoäly osaa tehdä valokuvia,
jotka näyttävät oikeilta.
Huijarit käyttävät kuvia
esimerkiksi romanssihuijauksissa.

Näin voit estää tekoälyhuijaukset

- **Sovi läheistesi kanssa tunnussana.**
  Kysy tunnussanaa,
  jos saat soiton tai viestin,
  jossa läheinen pyytää jotain, kuten rahaa.
  Jos tunnussanaa ei ole sovittu,
  kysy tietoja, joita huijari ei voi tietää.
  Yritä aina varmistaa, onko soitto tai viesti huijaus.

- **Älä koskaan anna tärkeitä tietojasi puhelimessa, viestissä tai netissä.**
  Älä kerro henkilötietoja, pankkitietoja
  tai luottokortin numeroita.
  Älä myöskään lähetä rahaa.
  Tietoja ei kysy poliisi, pankki tai viranomainen.
  Niitä kysyy huijari!

- **Jos sinua yritetään kiristää, ota yhteyttä poliisiin.**
  Säästä kaikki viestit tai videot.
  Älä anna rahaa huijarille!

- **Älä usko kaikkea.**
  Esimerkiksi kun näet uutisen tai videon netissä,
  mieti, onko se totta.

- **Älä kiirehdi.**
  Huijari yrittää saada sinut toimimaan nopeasti.
  Ole varovainen,
  jos saat yllättäviä pyyntöjä tai viestejä.

8. Vinkkejä laitteiden ja käyttäjätilien suojaamiseen

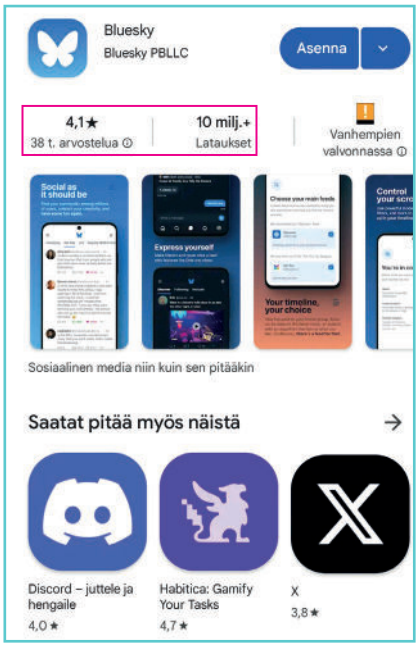
Monet laitteet ovat yhteydessä nettiin,
kuten puhelin, tietokone ja televisio.

Kun suojaat laitteesi,
voit paremmin estää
esimerkiksi käyttäjätilisi varastamisen.
Käyttäjätili on henkilökohtainen tunnus,
jolla voit kirjautua verkkopalveluihin ja sovelluksiin
(esimerkiksi Google-tili, Facebook-tili ja Netflix-tili).

Suojaa laitteesi näin

- Tutustu laitteen tietoturva-asetuksiin.
- Vaihda laitteeseen turvallinen salasana.
  Älä käytä salasanaa,
  joka on helppo arvata (esimerkiksi 1234).
- Lataa sovelluksia puhelimeen tai tablettiin
  vain virallisesta sovelluskaupasta
  (esimerkiksi App Store ja Google Play).
- Päivitä laite, ohjelmistot ja sovellukset tarpeeksi usein.
  Päivitä sovellukset vain virallisen sovelluskaupan kautta.
- Jos myyt tai kierrätät puhelimen,
  tallenna ensin tärkeät tiedot,
  kuten kuvat ja yhteystiedot.
  Tyhjennä sitten puhelin eli palauta tehdasasetukset.
  Lopuksi poista SIM-kortti.
- Etsi muiden laitteiden kierrätysohjeet netistä.

Muista nämä vinkit, kun lataat uutta sovellusta



Sovellus on ohjelma eli appi,
joka ladataan puhelimeen tai tablettiin.

1. Lataa sovelluksia vain virallisista sovelluskaupoista (esimerkiksi App Store ja Google Play).
2. Katso tarkasti sovelluksen nimi, kuvake ja julkaisija.
3. Katso myös latausten määrä.
   Jos suuri määrä ihmisiä on ladannut sovelluksen, se on luultavasti turvallinen.

Suojaa käyttäjätilisi näin

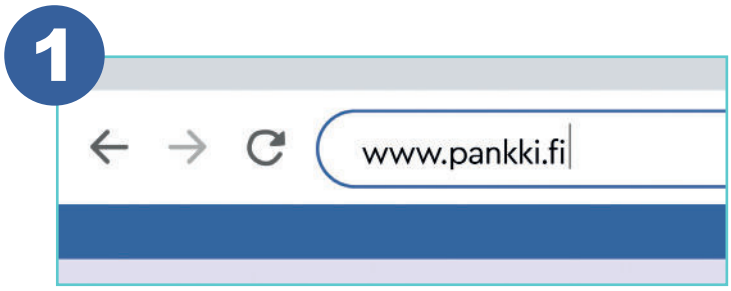
- Käytä joka paikassa eri salasanaa.
- Älä käytä helppoja salasanoja, kuten 123456.
- Käytä turvallisia salasanoja:
  - vähintään 12 merkkiä
  - isoja ja pieniä kirjaimia
  - numeroita ja erikoismerkkejä.
- Voit käyttää myös salasanalauseita (esimerkiksi OmaLapsiLukee3).
- Tallenna salasanat turvalliseen paikkaan selkeästi.
- Vaihda salasanat tarpeeksi usein.
- Jos mahdollista,
  valitse kaksivaiheinen tunnistautuminen.
  Se tarkoittaa,
  että salasanan lisäksi kysytään koodi tai numerosarja,
  joka toimii vain kerran.

9. Turvavinkkejä pankkiasioihin

Mene pankin tai viranomaisen palveluun turvallisesti.

Nämä kolme tapaa ovat turvallisia:

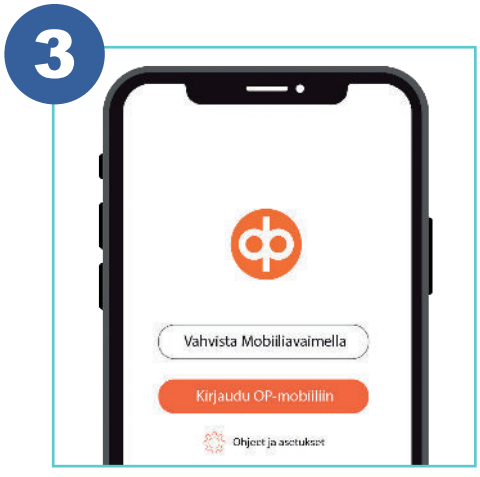
1. Kirjoita osoite nettisivun yläreunaan kokonaan alusta loppuun. Älä valitse valmiita vaihtoehtoja, joita internet tarjoaa.
2. Käytä omaa kirjanmerkkiä.
3. Kirjaudu virallisen sovelluksen kautta, jos käytät puhelinta tai tablettia.



Kirjoita osoite nettisivun yläreunaan.

2

Tallenna pankin sivu itsellesi **kirjanmerkiksi eli suosikiksi.** Silloin pääset sivulle helposti ja turvallisesti.



Pankin virallinen sovellus on turvallinen.

Älä mene palveluun Googlen
tai muiden hakukoneiden kautta.
Muuten voit joutua huijaussivulle.
Huijarit osaavat tehdä sivuja,
jotka näyttävät oikeilta pankin sivuilta.

Käytä pankkitunnuksiasi vain silloin,
kun kirjaudut pankin palveluihin.
Muissa paikoissa käytä mobiilivarmennetta.
Saat sen puhelinoperaattoriltasi.
Mobiilivarmenne on turvallinen tapa tunnistautua.

Lisää vinkkejä rahojen suojaamiseen

- Kysy pankista, voitko tehdä maarajoituksen.
  Silloin kortilta tai tililtä
  voi tehdä maksuja vain maihin,
  jotka valitset (esimerkiksi vain Suomi).
- Aseta maksukorteillesi turvarajat.
  Silloin voit päättää,
  kuinka paljon kortilla voi maksaa
  tai nostaa rahaa päivässä.
  Jos rikollinen varastaa tietosi,
  hän ei voi tyhjentää tiliäsi heti.
- Aseta turvaraja myös tilillesi.
- Jos haluat suojata säästösi,
  avaa toisessa pankissa tili,
  johon ei ole verkkopankkitunnuksia.
  Siirrä säästöt sinne.
  Silloin rikollinen ei voi varastaa tunnuksiasi
  ja tyhjentää tiliäsi.

Näin suojaat tietosi rikollisilta

Toimi näin, jos henkilötietosi varastetaan.
Näin voit myös suojata tietosi etukäteen.

- Tee muuttosuojaus Postille
  ja Digi- ja väestötietovirastoon.
- Harkitse vakavasti luottokieltoa.
  Silloin kukaan ei saa lainaa sinun tiedoillasi.
  Lue lisää sivulta 33.
- Tee rekisteröintikielto
  Patentti- ja rekisterihallitukselle.
- Tee tietojen luovuttamisen kielto
  Väestötietojärjestelmään.
- Muuta puhelinnumerosi salaiseksi tarpeen mukaan.
- Poista tietosi laskutuspalveluista,
  joita olet käyttänyt (kuten Klarna).
  Kiellä palveluiden käyttö.
- Käytä turvallisia salasanoja.
- Valitse kaksivaiheinen tunnistautuminen,
  jos mahdollista.
  Silloin kysytään salasanan lisäksi
  koodi tai numerosarja,
  joka toimii vain kerran.

Lue lisää:
www.riku.fi/toimi-nain-jos-tietojasi-on-vuodettu-verkkoon

10. Mistä saat apua?

Toimi näin, jos olet menettänyt rahaa, henkilötietoja tai pankkitunnukset

1. Ilmoita huijauksesta pankkisi asiakaspalveluun.
   Toimi nopeasti.
   Pankki voi sulkea tilisi ja maksukortit.
2. Tee rikosilmoitus poliisille: www.poliisi.fi

Hae apua muualta

- Älä jää yksin – puhu asiasta läheistesi kanssa.
  Sinun ei tarvitse tuntea häpeää,
  sillä jokaista voidaan huijata.
- **Rikosuhripäivystys** neuvoo ja antaa tukea.
  Soita numeroon 116 006 tai keskustele chatissa.
  Lisää tietoa: www.riku.fi
- **Kilpailu- ja kuluttajavirasto** auttaa,
  jos sinua huijaa suomalainen yritys.
  Lisää tietoa: www.kkv.fi/kuluttajaneuvonta
- Jos sinulla on ongelmia
  ulkomaisen nettikaupan kanssa,
  saat apua **Euroopan kuluttajakeskuksesta**.
  Keskus toimii Suomessa.
  Lisää tietoa: www.ecc.fi

Apua netin käyttöön

Saat apua turvalliseen netin käyttöön
esimerkiksi kirjastosta ja Eläkeliitosta.
Voit kysyä apua myös
puhelinoperaattoriltasi tai pankiltasi.

SeniorSurf-toiminta tarjoaa opastusta ikäihmisille.
Lisää tietoa: www.seniorsurf.fi/seniorit/opastuspaikat

Vapaaehtoinen luottokielto

**Vapaaehtoinen luottokielto suojaa rahasi,
jos henkilötietosi varastetaan.**

- Voit suojata rahasi,
  jos teet itsellesi luottokiellon.
  Silloin rikolliset eivät voi saada
  tiedoillasi luottoa eli lainaa.
  Voit keskeyttää luottokiellon milloin haluat.
- Lisää tietoa löydät Suomi.fi-palvelusta.

Näin teet reklamaation eli valituksen

Voit tehdä pankille reklamaation,
jos sinua on huijattu ja menetit rahaa.
Joissakin tapauksissa
pankki voi maksaa sinulle korvauksen.

Ota yhteyttä omaan pankkiisi,
ja tee huijauksesta kirjallinen reklamaatio.
Suullinen reklamaatio ei riitä.
Varmista, että saat asiasta kirjallisen vastauksen.

Jos et ole tyytyväinen pankin vastaukseen,
voit ottaa yhteyttä FINEen
eli Vakuutus- ja rahoitusneuvontaan.
Voit soittaa tai kysyä asiasta chatissa.
Lue lisää: www.fine.fi

11. Lisää tietoa huijauksista ja neuvontaa

Kuluttajaliiton tietopankki huijauksista
www.huijausinfo.fi

Poliisi
www.poliisi.fi/petosrikokset

Rikosuhripäivystys
www.riku.fi/erilaisia-rikoksia/nettihuijaus

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
www.kyberturvallisuuskeskus.fi

Kilpailu- ja kuluttajaviraston kuluttajaneuvonta
www.kkv.fi/kuluttajaneuvonta

Euroopan kuluttajakeskus Suomessa
www.ecc.fi

Suomi.fi-palveluiden neuvonta
puhelin 0295 000

Huijauksista varoitetaan esimerkiksi näissä somekanavissa ja nettisivuilla:

- **Huijausinfo**
  Facebook @huijausinfo
  Instagram @huijausinfo
- **Poliisi**
  Facebook @Suomenpoliisi
  Viestipalvelu X @Suomenpoliisi
- **Kyberturvallisuuskeskus**
  Facebook @NCSC-FI
  Viestipalvelu X @CERTFI

Yle Oppimisen Digitreenit -sivuilla voit oppia suojautumaan huijauksilta.
www.yle.fi/aihe/digitreenit

SeniorSurf-toiminta antaa vinkkejä puhelimen, tietokoneen ja netin käyttöön.
www.seniorsurf.fi

Kuluttajaliiton YouTube-kanavalla on videoita, joissa opit tunnistamaan huijauksia.
www.youtube.com/@kuluttajaliittory

Tietoisku

Tiesitkö?
WhatsAppissa voit estää vieraita ihmisiä lisäämästä sinua ryhmiin.

Tee näin:

1. Avaa WhatsApp.
2. Klikkaa kolmea pistettä oikeassa yläkulmassa.
3. Valitse **Asetukset.**
4. Valitse **Tietosuoja.**
5. Valitse **Ryhmät.**
6. Valitse **Yhteystietoni.**

Tietoisku

Tiesitkö?
Jos et halua puheluita ja viestejä joltakin ihmiseltä,
voit estää hänen numeronsa.

Tee näin, jos sinulla on Android-puhelin
(kuten Samsung tai OnePlus):

1. Klikkaa puhelimen kuvaa.
2. Valitse numero, jonka haluat estää.
3. Klikkaa kolmea pistettä tai i-kuvaketta.
4. Valitse **Estä yhteyshenkilö.**