

Tietoturva

Miten seniorit voivat välttää digihuijauksia?



Pekka Tynkkynen
Enter ry
13.2.2026



ENTER ry

- Henkilökohtaista ja maksutonta digiopastusta sekä tietoisuuksia.
- Kohderyhmänä seniorit
- Toiminta perustuu pääosin vapaaehtoistoimintaan
 - 200 opastajaa
 - 5 palkattua työntekijää koordinoi toimintaa.
- Toiminta-alue Uusimaa
- Perustettu vuonna 1997
- Jäseniä hieman yli 1000
- Opastuspaikat <https://www.entersenior.fi/opastus/>



Huijausten muodot - eräs jaottelu

Romanssihuijaukset

Rakkaushuijaus voi tehdä syvää henkistä ja taloudellista vahinkoa

Nettikauppahuijaukset

Verkon kauppapaikoilla tapahtuu jatkuvasti huijauksia

Sijoituspetokset

Sijoitushuijari houkuttelee lupauksilla poikkeuksellisen suurista tuotoista.

Identiteettivarkaudet

Varastettuja henkilötietoja käytetään luvattomiin tarkoituksiin.

Tietojenkalastelu

Rikollinen urkkii henkilökohtaisia tietojasi esimerkiksi puhelimessa, sähköpostilla tai viesteillä

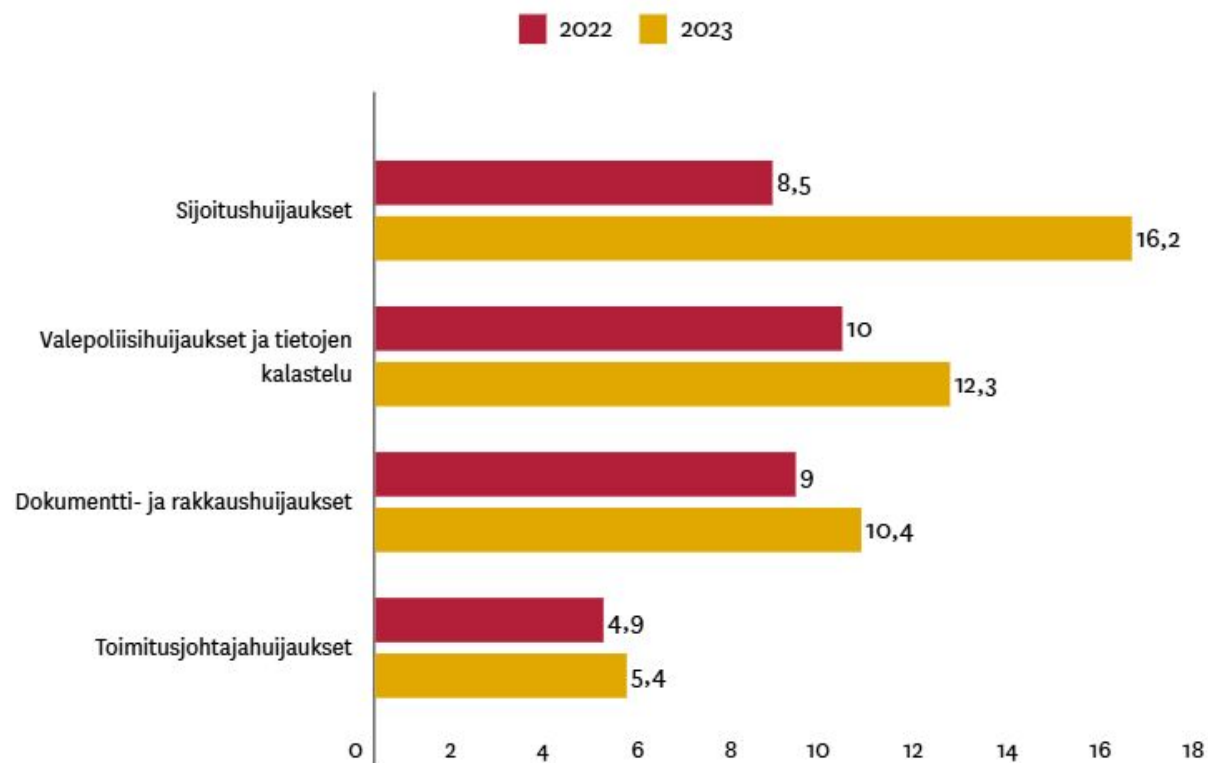
Tietomurrot ja -vuodot

Arkaluontoisten tietojen vuotaminen voi vaarantaa ihmisten ja yritysten turvallisuuden.

Rahalliset menetykset nettihuujauksiin Suomessa

Rahat katosivat huijareiden taskuihin

Pankkien tietoon tulleiden huijausten rahalliset arvot Suomessa, miljoonaa euroa



Lähde: Talouselämä
2/2025

Tärkein tietosuoja olet sinä itse



”Tietoturvasta 20 prosenttia on tekniikkaa ja 80 % ihmisen käytöstä.”

Panu Moilanen

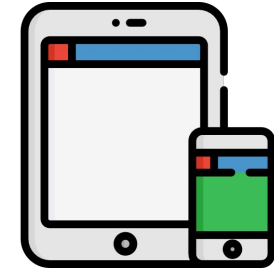
lehtori

Kyberturvallisuus, Jyväskylän yliopisto

Tietoturva - tekniikka päätelaitteet

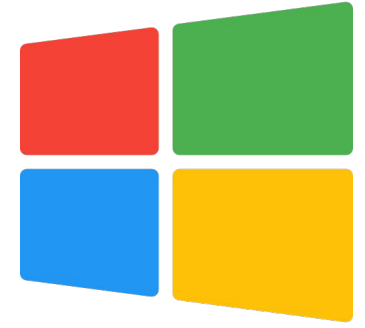


Älypuhelimet ja tabletit - toimenpiteet



- Vaihda SIM-kortin ja päätelaitteen PIN-koodi
 - ilman muutosta ne ovat esim 0000 tai 1234 (painettu käyttöohjeisiin)
- Kirjaudu laitteeseen Google tilillä/Apple ID:llä
- Ota käyttöön kaksivaiheinen tunnistus - tekstiviesti tai sähköposti
- Ota käyttöön näytön automaattinen lukitus (suositus 2...10..30 min)
- Asenna AINA järjestelmä- ja sovelluspäivitykset
- Varmista että varmuuskopiointi pilveen on päällä (Google, iCloud) myös mobiilidatalla, laiterikkoontumisia tapahtuu
- Hanki sovelluksia vain virallisesta sovelluskaupasta (Google Playkauppa tai Applen AppStore)
- Erilliset tietoturvaohjelmistot ei ole välttämättömiä
 - Androidissa riittää Google Play protect - ota käyttöön
 - iPhone ei tarvitse virustorjuntaa

Windows tietoturva



- Käytä Microsoft-tiliä
- Kirjaudu koneeseesi salasanalla tai PIN-koodilla
- Käytä tietoturvaohjelmaa - Win10/11:ssä valmiina MS Defender
- Pidä palomuuuri käytössä – sisältyy MS Defenderiin
- Pidä päivitykset ajan tasalla
- Huolehdi omien tietojesi ts. kirjoittamiesi ja vastaanottamiesi tiedostojen varmuuskopioinnista joko ulkoiselle levyille tai pilveen (laiterikkoontumisiakin tapahtuu)
- Lataa sovelluksia vain luotettavista lähteistä, ei viestin linkistä



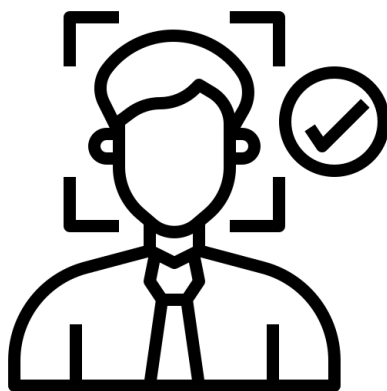
Mac tietoturva



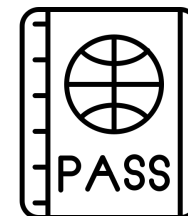
- Pidä palomuuuri käytössä
- Pidä päivitykset ajan tasalla
- Huolehdi omien tietojesi ts. kirjoittamiesi ja vastaanottamiesi tiedostojen varmuuskopioinnista (laiterikkoontumisiakin tapahtuu)
- Käytä virusturvaa tarvittaessa
- Lataa sovelluksia vain luotettavista lähteistä



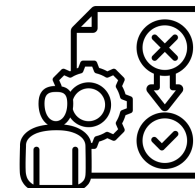
Turvallinen tunnistautuminen digipalveluihin



Mikä on vahva tunnistus?



Vahva tunnistautuminen on **henkilöllisyyden todistamista palveluun**, yleensä verkkopankkiin, muuhun maksutapaan, tai viranomaispalveluihin käyttäen **kaksivaiheista tunnistautumista**.



Kaksivaiheinen tunnistautuminen pyytää käyttäjältä jotain tietoa jonka vain käyttäjä tietää ja jotain mitä vain käyttäjä omistaa. Käytännössä PIN ja puhelin tai puhelimen sovellus.

Sähköinen vahva tunnistautuminen - vaihtoehdot

Mobiilivarmenne

- Suomalaisten puhelinyhtiöiden kehittämä vahva tunnistautumispalvelu.
- Saat omalta operaattorilta
- Toimii puhelimessa SIM-kortilla
- Hinta 0-3€/kk
- Suositus: *käytetään kaikki muihin kuin pankkipalveluihin*



Verkkopankkitunnistus

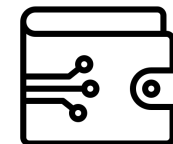
- Vahva tunnistautuminen suomalaisiin verkkopankkeihin
- Suositus: käytetään ainoastaan pankkipalveluissa

3. vaihtoehto: Kansalaisvarmenne henkilökortti ja kortinlukija



<https://dvv.fi/kansalaisvarmenne>

Eurooppalainen digitaalinen identiteettilompakko



- Digi- ja väestötietovirasto (DVV) rakentaa suomalaisten käyttöön digitaalisen *identiteettilompakon*.
- Jokaisen kansalaisen perussovellus, jota käytetään *älypuhelimella*.
- Lompakko edistää turvallista digitaalista asiointia Suomessa ja Euroopassa.
- Sovellus tulee saataville vuoden 2026 loppuun mennessä
 - Ominaisuuksia on tarkoitus laajentaa vaiheittain.
- Ensimmäisessä vaiheessa lompakkoa voi käyttää ainakin
 - Vahvan sähköisen tunnistautumisen välineenä
 - Sähköiseen allekirjoitukseen



Tietoturva



Oman toiminnan merkitys



Huijausten yleisiä periaatteita

- Henkilön oma innostus saada jotain erityistä
 - Liiallinen luottaminen saatuun sähköpostiin, Facebook viestintään tai tekstiviestiin
 - Lähettäjän valheellisuuden huomaamattomuus jonkin erityisen saamisen innossa
- Innostus voi olla
 - Erityistä voittomahdollisuutta vain sinulle, ainutkertaista tavaraa, peliä, suurta alennusta, jne
 - Henkilökohtaisesta kertomuksesta lähtevää auttamishalua

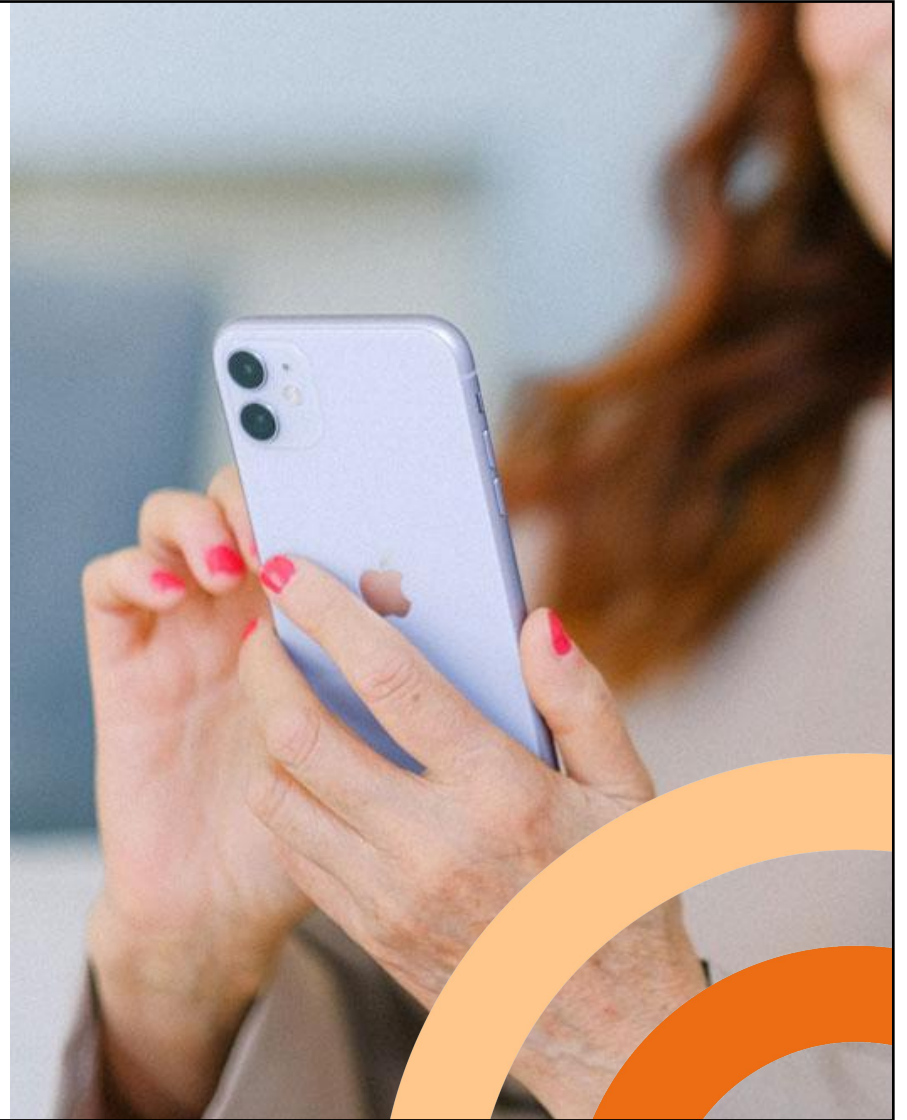
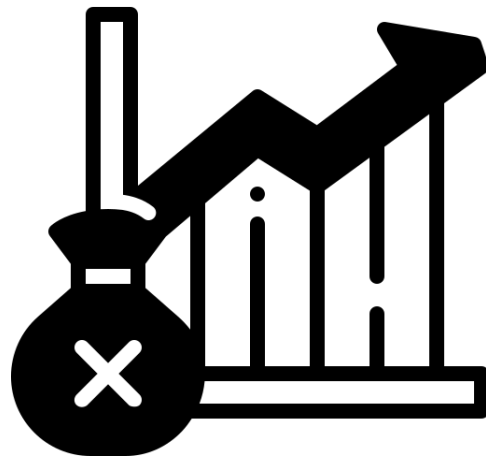
Huijaus: kauppa

- Myös avoin kauppatoiminta voi olla eritasoisia huijauksia
 - Tarpeettoman palvelun myynti
 - Olemattoman esineen myynti
- Tarjoavan myyjän suurin tarve on tehty kauppa
 - Myyjä pyrkii aina esittämään palvelun olevan välttämätön ostajalle
 - Ostaja ei aina kehtaa myöntää osaamattomuuttaan, vaikka pitäisi todeta ”en ymmärrä tuon välttämättömyyttä, en osta”
- Puhelimessa sovitun kaupan voi myös peruuttaa



Sijoitushuijaukset

Miten välttää?



Jossain on vielä hunajaa

Näyttelijä Jarmo Koski haaveili huolettomista eläkevuosista. Sitten hän uppoutui vuosiksi sijoitushuijaukseen ja menetti kaikki säästönsä – ja enemmänkin.

Roosa Oksanen HS, teksti

Outi Pyhäranta HS, kuvat ja videot

Julkaistu 1.10.2025

💎 Tilaailla



Varoitusmerkkejä sijoitushuijauksista

Tuotot

- Jos joku vaikuttaa liian hyvältä ollakseen totta, se todennäköisesti ei ole totta

Lähestyminen

- Vain huijarit tarjoavat tavallisille ihmisille sijoitusvinkkejä puhelimesta

Aktiivisuus

- Vastapuoli vastaa viesteihin mihin vuorokauden aikaan tahansa

Monimutkaisuus

- Älä sijoita kohteeseen, jota et ymmärrä



Ahneus!

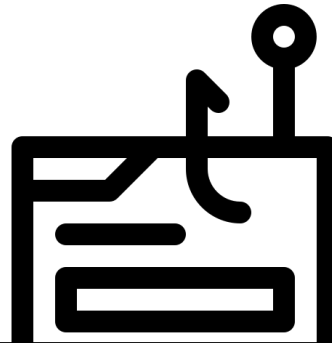


Tietojen kalastelu



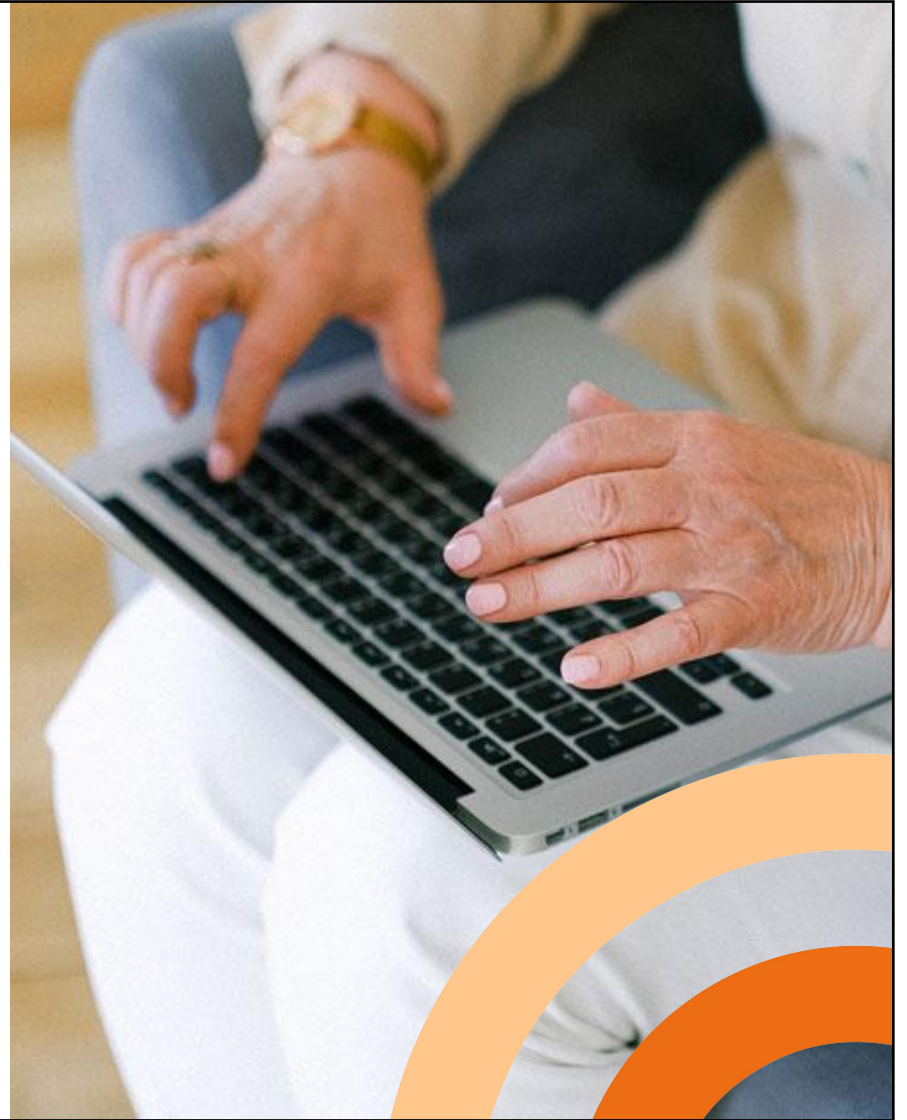
Tietojen kalastelu - Phishing

- Sait tuntemattomalta lähettäjältä sähköpostiviestin tai tekstiviestin, jossa sinulle annetaan linkki
- Kyse on usein **tietojen kalastelusta** (Phishing), joka vie pankin oikeita nettisivuja muistuttavalle valesivulle
- Kun syötät sinne tietosi, ne päätyvät ulkopuolisten käyttöön ja tietoon.
- **Älä koskaan klikkaa sähköpostin tai tekstiviestin linkkiä, jos et ole varma lähettäjästä**





Turvallinen pankkiasiointi



Pankit

- Mene verkkopankkiin kirjanmerkeistä ta itse kirjoittamasi pankin nettiosoite, ***ei koskaan hakukoneen tuloksista***
- Kirjaudu pankin internetsivujen kautta TÄRKEÄÄ: Älä koskaan mene verkkopankkiin painamalla linkkiä, joka sinulle on tullut sähköpostissa tai tekstiviestissä.
- Tarkasta, että yhteys pankkiin on suojattu: Selaimen osoiterivillä osoitteen alussa pitää lukea **https://**, ei **http://**



Verkkopankin turvallinen käyttö tietokoneen selaimella

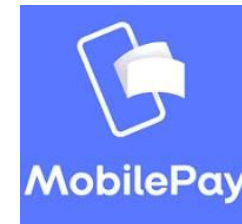
- Varmista, että tietokoneen tietoturva on kunnossa (Windows Defender riittää).
- Pankki ei koskaan kysele pankkitunnuksia tai turvalukuja sähköpostilla tai puhelimella.
- Pankkihuujauksissa saatetaan kysyä useampaa peräkkäistä turvalukua. Älä syötä niitä
- Lopeta istunto Kirjaudu ulos-linkistä.
- Yhteiskäyttöiseltä koneelta tyhjennä lopuksi selaimen selaushistoria.
- Tarkista tiliotteesi (tilitapahtumasi), ettei niissä ole sinulle kuulumattomia rahasiirtoja.



Mobiilipankki kännykässä tai tabletissa

- Älykännykässä tai tabletissa oleva pankin sovellus on turvallisempi kuin selaimen kautta kulkeva liikenne, koska
 - Pankin tietojärjestelmä tarkastaa aina sovelluksen eheyden
 - Sovelluksen liikennettä ei voi kaapata
- Älykännykässä tai tabletissa pitää olla näytön lukitusasiat kunnossa
- Käytä ainakin 6 osaista salanumeroa, muu kuin syntymäaikasi
- Rahasiirtoihin myös mobiilisovellukset
 - Mobilepay
 - Siirto-maksu (OP&Nordea käyttäjien välillä)

Suositus!



Turvatilihuijaus

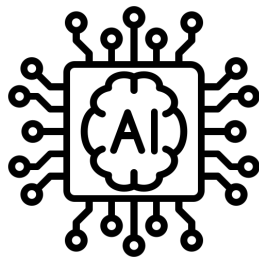
Miten ne toimivat

- Huijari ottaa uhriin yhteyttä puhelimella tai viestillä esiintyen pankin pankin henkilönä.
- Väittää uhrin tilillä olevan epämääräistä toimintaa
- Pyytää uhrin pankkitunnuksia, jotta rahat voidaan siirtää *turvatilille*

Miten välttää

- Rauhoitu, ota hetki aikaa
- Mitää turvatilijä ei ole olemassa!!
- Pankin henkilö tai viranomainen ei koskaa kysy pankkitunnuksia netissä tai puhelimesta

Suomen pankin ex-pääjohtajan Erkki Liikasen epäillään menettäneen 40000 euroa huijareille



Yleisimmät tekoälyhuijaukset ja niiden välttäminen

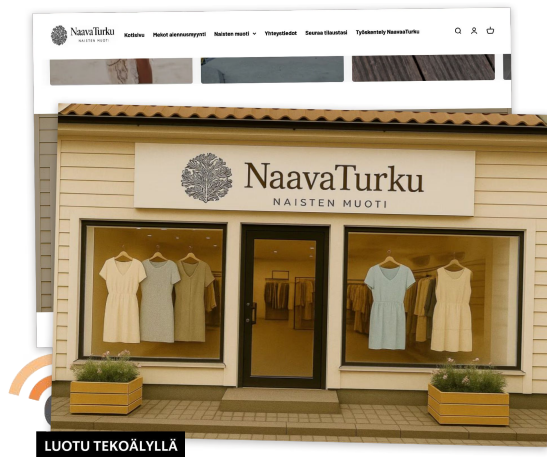


Väärennetty nettikaupat



Miten ne toimivat?

- Tekoälyllä voidaan tehdä nettikauppa, joka näyttää (lähes) aidolta



Miten välttää?

- Kaupan sivulta ei löydy kunnon yhteystietoja
- Tarjoukset ovat “liian hyviä” ollakseen totta
- Käytä vain hyväksihavaittuja nettikauppoja

Väärennetyt tekoälytuotteet ja palvelut

- **Miten ne toimivat?**

Tarjotaan tekaistuja tai toimimattomia tekoälypohjaisia tuotteita, kuten ekirjoja tai vääriä sijoitusneuvonantajia



Verkkokauppa Amazonista löytyy lukuisia tekoälyllä luotuja kirjoja Sanna Marinista ja Alexander Stubbista. Kuva: Amazon.com

- **Miten välttää?**

- Tutki tekijän/yrityksen taustat ja käyttäjäarviot ennen ostamista.



Yhteenveto - huijausten välttäminen



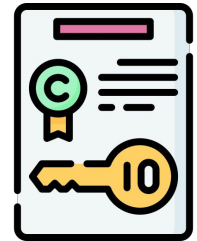
Yleinen neuvo: **Jos jokin kuulostaa epäilyttävältä, liian hyvältä ollakseen totta, se ei todennäköisesti ole totta!**

- Tarkista asia kahdesti
- Käytä arkijärkeä.

Huijaukset perustuvat usein kiireeseen ja tunteisiin – älä anna niiden hämätä!

Yhteenveto II - huijausten välttäminen

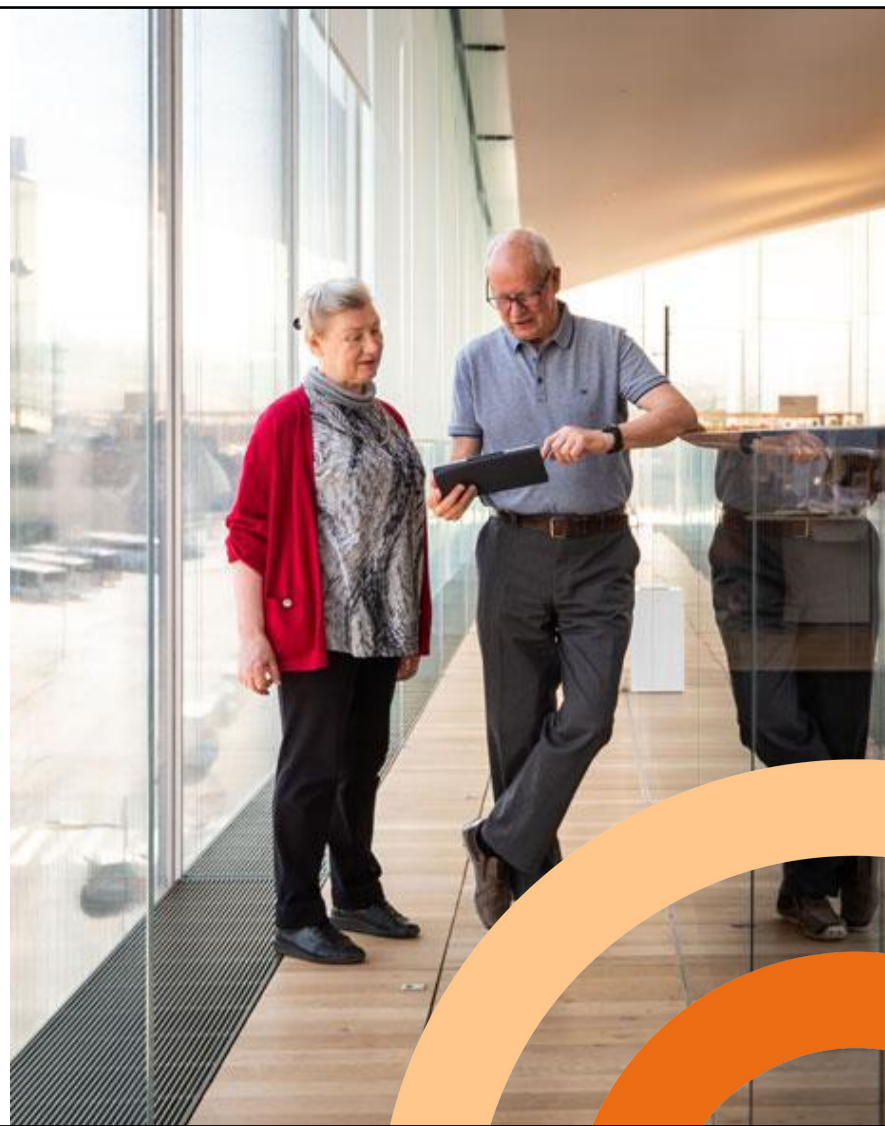
- **Älä jaa pankki ym. tunnuksia kenellekään**
 - Pankit ja viranomaiset eivät koskaan kysy niitä puhelimesta tai viesteissä
- **Älä avaa tuntemattomilta lähettäjiltä sähköposteissa tai tekstiviesteissä tulleita linkkejä**
- Käytä pankkitunnuksia ainoastaan omaan pankkiin kirjautuessasi
- Tekniikka ja laitteet
- Pidä laitteiden ohjelmistopäivitykset ajan tasalla
- Ota käyttöön kaksivaiheinen tunnistus
 - Asenna uusia ohjelmistoja ainoastaan virallisista kaupoista: Apple App Store, Microsoft Store ja Google Play



Käytännön apua tietoturva-asioihin



 **enter** www.entersenior.fi/opastus/



Valtakunnallinen SeniorSurf etäopastus -palvelu

- Apua ilman, että tarvitsee poistua kotoa!
- Vertaisopastajat neuvovat puhelimitse. Tarvittaessa voidaan käyttää myös video- ja etäyhteysohjelmia.
- Voit kysyä neuvoa laitteen hankintaan, ohjelmien ja palvelujen käyttöön tai laiteasetuksiin
- Täytä pyyntölomake www.etaopastus.fi tai puhelimitse 044 700 7101 - voit soittaa milloin vain!
 - Kuuntele nauhoite loppuun, niin sinulle soitetaan takaisin kahden arkipäivän kuluessa.

