

Tunnista nettihuijaus



Tämän oppaan avulla voit oppia lisää nettihuijauksista. Luettuasi oppaan tunnet yleisimmät huijaustyytit, osaat tunnistaa niitä ja tiedät, miten toimia, jos joudut huijatuksi. Oppaan tavoitteena on tukea ja kannustaa turvalliseen netin käyttämiseen.

Voit käyttää opasta itseopiskeluun tai neuvoa sen avulla muita. Opasta saa jakaa eteenpäin myös omille verkostoille.

Tämä opas on toteutettu osana Kuluttajaliiton Huijarit kuriin! -hanketta (STEA 2019–2021) ja päivitetty Huijausinfo selkeällä kielellä -hankkeessa (STEA 2024–2026).

Lisätietoja hankkeesta ja huijauksista löydät osoitteesta www.huijausinfo.fi

Kuluttajaliitto ry on Suomen ainoa yleinen ja kaikille avoin kuluttajien, asukkaiden, potilaiden ja sote-asiakkaiden edunvalvonta-, koulutus- ja neuvontajärjestö.

Puolustamme kohderyhmiemme etua yhteiskunnallisessa päätöksenteossa ja autamme arjen valinnoissa neuvomalla ja kouluttamalla.

Lue lisää www.kuluttajaliitto.fi

ISBN 978-952-9787-70-8 (nidottu)

ISBN 978-952-9787-71-5 (pdf)

3. päivitetty versio (maaliskuu 2025)

Sisältö

1. Mikä on nettihuijaus?	4
2. Huijausviestit	6
3. Huijauspuhelut	12
4. Romanssihuijaukset	15
5. Nettikauppahuijaukset	19
6. Sijoitushuijaukset	23
7. Tekoälyn käyttö huijauksissa	27
8. Turvavinkit laitteiden ja käyttäjätilien suojaamiseen	32
9. Pankkiasioinnin turvavinkkejä	34
10. Kysy rohkeasti apua	37
11. Lisätietoa huijauksista	40
Tietoisku	42





1. Mikä on nettihuijaus?

Nettihuujaukset ovat rikollisten tekemiä erityyppisiä petoksia, joissa hyödynnetään digilaitteita (esim. tietokone, tabletti, kännykkä).

Nettihuujauksissa huijarit pyrkivät saamaan rahaa, henkilötietoja tai käyttäjätunnuksia ja salasanoja.

Huijausten tavoitteena on saada taloudellista hyötyä joko heti tai hyödyntämällä huijatulta saatuja tietoja myöhemmin.

Huijausten taustalla on usein kansainvälinen järjestäytynyt rikollisuus. Vaikka huijauksessa käytettäisiin suomen kieltä, se ei tarkoita, että se olisi tehty Suomessa. Iso osa huijauksista toteutetaan Suomen rajojen ulkopuolella.



Rahan huijaamisen lisäksi meitä voidaan yrittää huijata myös esimerkiksi valeuutisilla, joilla pyritään vaikuttamaan ihmisten ajatteluun ja päätöksentekoon. Varmista epäilyttävän tiedon aitous useammasta eri lähteestä.

Lue ensin tämä:

- Epäilyttäviin ja tuntemattomilta tulleisiin kirjeisiin, teksti- tai sähköpostiviesteihin ei ole syytä vastata. Viestit voi hävittää kuten muunkin roskapostin.
- Rahaa ei tule mistään ilmaiseksi rehellisellä tavalla. Älä usko kaikkea mitä kerrotaan, kirjoitetaan tai näytetään vaikka kuvana tai videona.
- Rikolliset osaavat tehdä aidon näköisiä huijauksia hyödyntäen nykyaikaista teknologiaa ja internetissä jo olevaa sisältöä.
- Mikäli ei ole osallistunut lottopeleihin, ei niissä voi voittaakaan.
- Tilinumeroita, passitietoja tai muita henkilötietoja ei pidä lähettää tuntemattomille.
- Epäilyttävän edullisen tarjouksen rehellisyyttä on aina syytä epäillä.
- Rahojen lähettäminen luottokorttinumeroiden ja erilaisten rahansiirtokoodien avulla on arveluttavaa.
- Sähköpostiosoitteet on syytä selvittää: vakavasti otettavat yritykset eivät käytä internetin ilmaispostiosoitteita.

Lähde mukailten: Suomen poliisi



Rikolliset tavoittelevat pankki- ja luottokorttitietoja, henkilötietoja (mm. henkilötunnus) sekä käyttäjätietoja (esim. sähköpostin tunnus ja salasana).

2. Huijausviestit

Huijarit lähestyvät kaikilla käytössä olevilla viestialustoilla. Lähes jokainen saa huijausviestejä.

Tunnistatko kalastelun?

1 OmaVero: Olemme peruuttaneet veronpalautuksen. Lue lisää: <https://omavero.fi-taxi.net>

Saapuva maksu kelasta pysäytetty puutteellisten tietojen vuoksi, tarkista asia <https://kela.soumi-fi-.net>

Paketti saapunut. Katso tilauksesi pian: <https://om-posti-fi.org>

2

sehyvapankki-fi.org
Vierasta pankki siirtoa yritettiin klo 09.33.

3

TIEDOKSENNE Kelasta
Tukeanne on vähennetty 50 %
kirjau: ke . soumi-fi.xyz

4 Kalastelusivujen ulkoasu on usein uskottava kopio aidosta kirjautumissivusta.

5 Huijaussivun voi tunnistaa verkko-osoitteesta.

6 Kirjaudu palveluihin vain niiden virallisten sivujen tai applikaatioiden kautta.

1 Kalasteluviestejä lähetetään esimerkiksi pankkien, postin ja viranomaisten nimissä.

2 Viestissä on linkki huijaussivustolle.

3 Viesti koskee usein kiireellistä häiriötä tai ongelmaa. Näin vastaanottaja yritetään saada hätiköimään ja luovuttamaan tietonsa kalastelijoille.

Oma Pankkini

Tunnus
Salasana
LOG IN

Oma Pankkini

Tunnus
Salasana
LOG IN

<https://ompankkini.fi>

<https://turvallisuus-ompankkini.fi>

<https://ompankkiini-fi.org>

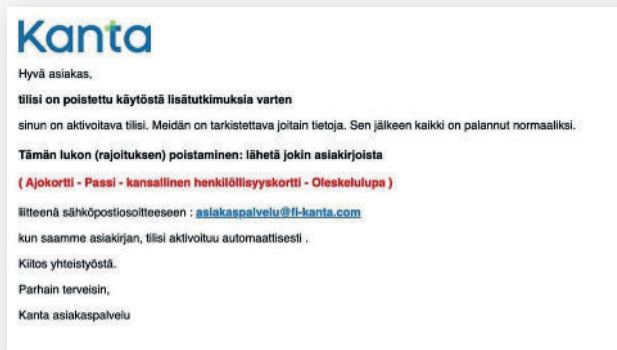
Huijausviestejä lähetetään muun muassa viranomaisten nimissä. Näissä viesteissä väitetään esimerkiksi, että palvelussa on uusi viesti tai allekirjoitettava asiakirja tai maksamaton lasku.

ESIMERKKI



Verohallinnon nimissä lähetetyissä huijausviesteissä kerrotaan usein, että viestin vastaanottaja on saanut veronpalautusta tai veronpalautus on peruttu.

Veroasioita ei hoideta tekstiviesteillä. Oikeat viranomaisen lähettämät viestit löytyvät verottajan verkkopalvelusta OmaVerosta.

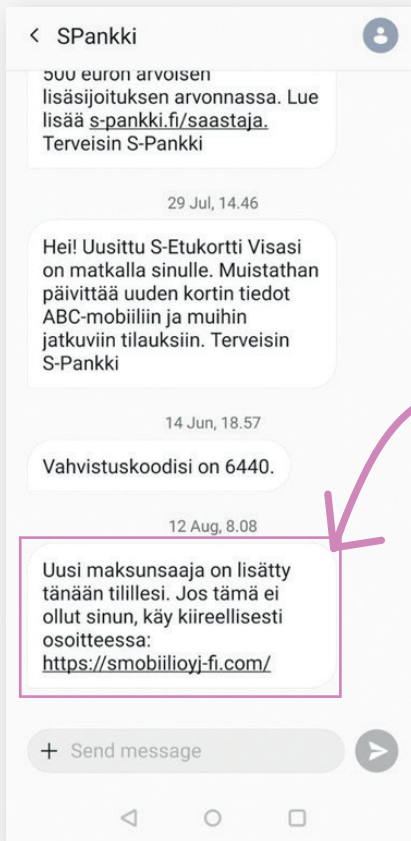


Kanta-palvelun nimissä on lähetetty lukuisia huijausviestejä, joissa väitetään muun muassa, että viestin vastaanottajan tili on poistettu käytöstä. Viesteissä suomen kieli ei ole välttämättä sujuvaa, ja sähköpostiosoitteet tai linkkien verkko-osoitteet eivät ole oikean tahon mukaisia.

Suomalaisten pankkien nimissä lähetetään viestejä, joissa uhataan esimerkiksi pankkikortin tai verkkopankin sulkemisella, jos vastaanottaja ei päivitä tietojaan viestin mukana tulleella linkillä. Linkki johtaa verkkopankilta näyttävälle huijaussivulle, jossa kalastellaan pankkitunnuksia.

Pankit eivät pyydä asiakkaitaan päivittämään mitään tietoja tekstiviestillä tai sähköpostilla – vain huijarit pyytävät!

ESIMERKKI



Tekstiviestillä lähetetty huijausviesti saattaa mennä älypuhelimessa samaan ketjuun aitojen viestien kanssa.

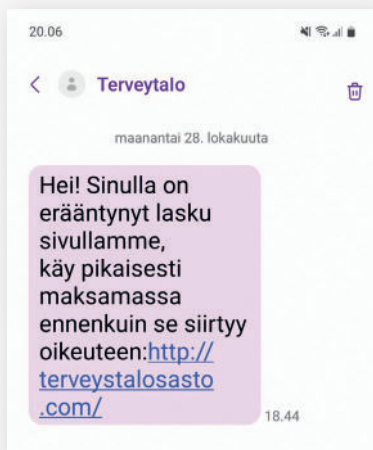
Älä avaa sähköposti- tai tekstiviestin mukana tullutta linkkiä, lataa outoa viestin liitetä tai anna pankkitunnuksia tai henkilötietoja!



Huijausviestien linkit johtavat pääsääntöisesti tietojenkalastelusivuille. Linkin kautta saattaa myös ladata laitteelleen haittaohjelman. Viestin liitteitä ei myöskään kannata avata.

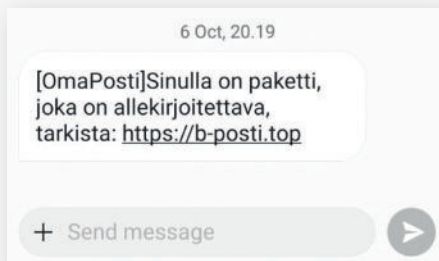
Huijausviestejä lähetetään esimerkiksi terveyspalveluita tarjoavien tahojen (mm. Terveystalo, Mehiläinen), Postin, kuljetusyritysten, kauppojen ja operaattoreiden nimissä. Viesteissä painostetaan aina kiireellä ja uhataan seurauksilla.

ESIMERKKI



Terveystalon nimissä lähetetyissä viesteissä väitetään yleensä, että vastaanottajalla on erääntynyt lasku, joka on maksettava välittömästi.

Terveyspalveluita tarjoavat tahot eivät lähetä laskuja tai maksumuistutuksia tekstiviestillä.

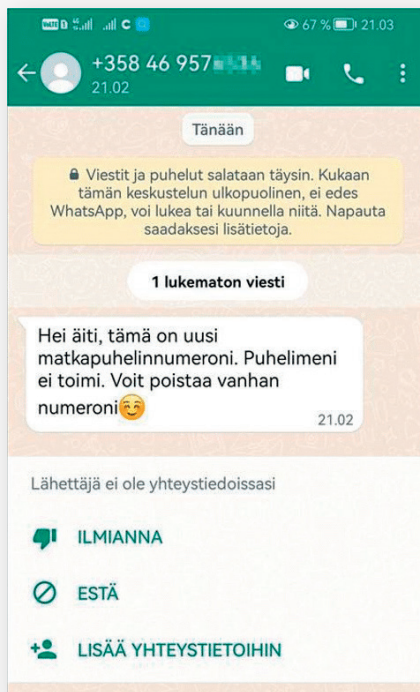


Postin ja kuljetusyritysten nimissä tulleissa huijausviesteissä kerrotaan usein paketista, jonka saaminen edellyttää toimenpiteitä.

Aidot saapumisilmoitukset edellyttävät tilausta netistä ja ne voi tarkistaa esimerkiksi OmaPosti-sovelluksesta tai kuljetusyrityksen sivuilta.

WhatsApp-sovelluksen kautta lähetetään useita erityyppisiä huijausviestejä, joissa tarjotaan muun muassa työpaikkaa hyvällä palkalla, kerrotaan huipputuottavia sijoitusvinkkejä tai lähestytään seuranhakumielessä.

ESIMERKKI



“Hei äiti”- tai “Hei isä” -huijauksessa viestin vastaanottajan lapsena esiintyvä huijari kertoo lapsen numeron vaihtuneen.

Huijarin tarkoituksena on yleensä saada vastaanottaja lähettämään rahaa ”lapsen uudelle tilille”, joka on syystä tai toisesta vaihtunut.

Jos saat tämänkaltaisen viestin, voit tarkistaa asian oikeellisuuden soittamalla lapsen vanhaan numeroon.

Kiristyshuijausviestit

Huijausviesteillä voidaan yrittää myös kiristää viestin saajaa. Usein lähettäjä väittää kaapanneensa huijauksen kohteena olevan henkilön tietokoneen tai sähköpostitilin ja salakuvan-neensa tätä koneen kameralla.

Viestillä huijari yrittää kiristää rahaa (yleensä kryptovaluuttaa, kuten bitcoineja) ja uhkaa julkaista ”arkaluontoisia” kuvia kohteen työkavereille ja muulle lähipiirille.

Kyseessä on huijaus, eikä konetta ole hakkeroitu tai kaapattu. Älä maksa kiristysviesteissä vaadittuja rahoja. Tee rikosilmoitus poliisille ja säilytä saamasi viestit.

Toimi näin, jos sait epäilyttävän viestin

1. Älä avaa viestissä olevaa linkkiä tai kirjaudu verkkopankkiin, viranomaisten palveluihin tms. viestien mukana tulneiden linkkien kautta.
2. Mene viestissä väitetyn lähettäjän palveluun omilla tunnuksillasi virallisen mobiilisovelluksen kautta tai kirjoittamalla osoite internet-selaimen osoiteriville.



3. Jos et tiedä, onko viesti huijausta vai ei, voit kysyä asiasta soittamalla viestin lähettäneen tahon asiakaspalveluun. Älä kuitenkaan vastaa viestiin suoraan, vaan etsi erikseen asiakaspalvelun yhteystiedot.
4. Arvonnoista ja kilpailuista kerrotaan yleensä järjestäjän nettisivuilla. Sivuilta kannattaa tarkistaa, onko viestissä väitetty kilpailu tai arvonta todellinen.



3. Huijauspuhelut



Joskus puhelimiin soitetaan vain parin hälytyksen ajan – tällöin tarkoituksena on yleensä saada huijauksen kohteena oleva soittamaan takaisin maksulliseen numeroon.



Pankin virkailijana esiintyvä huijari voi esimerkiksi varoittaa epäilyttävästä maksuliikenteestä pankkitilillä ja kehottaa siirtämään rahat turvatilille.



Lainaa tarjoavan yrityksen työntekijäksi tekeytynyt soittaja saattaa sanoa puhelun vastaanottajan nimellä tehdyn lainahakemuksia, jotka voi estää antamalla pankkitunnuksensa. Soittaja voi jopa ohjata puhelun pankin työntekijänä esiintyvälle toiselle huijarille, joka pyytää tunnuksia.



Huijarit voivat esiintyä myös poliisinä ja kertoa pankin hävittyneen rahaliikennettä vastaan tilillä. Asiaa tutkiva ”poliisi” vaatii pankkitunnuksia asian selvittämiseksi.



Sijoitushuijauksia tehtailevat rikolliset esiintyvät usein puhelimesta sijoitusasiantuntijoina tarjoten huippuhyvää sijoitusmahdollisuutta esimerkiksi kryptovaluuttoihin. Huijarit saattavat esittää itse tekemiään infograafeja ”tuottojen” kehityksestä. Tarkoituksena on saada huijauksen kohde sijoittamaan yhä enemmän rahaa olemattomiin kohteisiin.



Perintätoimiston työntekijänä esiintyvä soittaja saattaa kertoa mm. olemattomasta myöhästyneestä laskusta, joka täytyy maksaa.



Hyvinvointialueen työntekijänä esiintyvä soittaja voi yrittää myydä esimerkiksi ikäihmiselle vitamiinilisiä ja vaatia henkilökohtaisia tietoja.



Joskus huijarit laittavat robotit tekemään puheluita eri numeroihin tarkistaakseen, ovatko kyseiset puhelinnumerot toiminnassa.

IT-tukihuijaukset

IT-tukihuijauksessa on kyse siitä, että rikollinen soittaa ja esiintyy nettitukihenkilönä ja väittää, että henkilön tietokone on uhattuna. Yleensä englantia puhuva huijari sanoo soittavansa Microsoftin IT-tuesta ja väittää, että:

1. hän soittaa Microsoftin pääkonttorilta, jossa henkilön konetta on tarkkailtu
2. henkilön kone lähettää jotain signaalia viasta, joka pitää korjata
3. tietokone on saastunut haittaohjelmilla ja mahdollisesti tilit on kaapattu
4. asialla on kiire ja vain hän voi auttaa pelastamaan henkilön koneen.

Soittaja haluaa antaa vaikutelman, että kyseessä on erittäin kiireellinen asia ja että hänen ohjeitaan on välttämätöntä kuunnella ja noudattaa.

Yleensä huijari pyytää lataamaan laitteelle etähallintaohjelman, jonka avulla soittaja voi auttaa koneen pelastamisessa.



**IT-tukihuijari yrittää
päästä käsiksi tieto-
koneeseesi ja sitä kautta
pankkitiliisi.**



Muista nämä vinkit

- Muista, että kuluttajille ei ole olemassa yleistä IT-tukea, joka soittaa ja varoittaa ongelmista laitteessa – kyseessä on aina huijari. Mikään laite ei myöskään lähetä tietoja koneen tilasta ulkopuolisille tahoille.
- Älä ikinä lataa etähallintaohjelmia tai muita sovelluksia laitteellesi yllättäen soittaneen henkilön pyynnöstä.
- Älä koskaan anna puhelimesta kyselijöille pankki- tai henkilötunnuksia. Niitä ei kysele pankki, poliisi tai viranomainen – vain huijarit!
- Jos saat oudon tuntuksen puhelun esimerkiksi pankilta, poliisilta tai muulta viranomaiselta, lopeta puhelu. Voit varmistaa puhelun aitouden esimerkiksi soittamalla suoraan kyseisen tahon asiakaspalveluun tai kirjautumalla mobiilisovellukseen. Poliisiin saat yhteyden soittamalla neuvontapalveluun: www.poliisi.fi/neuvontapalvelu
- Estä numero oman puhelimesi asetuksista. Ulkomaisista numeroista tulevien puheluiden estosta voit kysyä omalta operaattoriltasi.
- Älä soita takaisin täysin yllättäen tuntemattomista numeroista tullessiin puheluihin.
- Jos esimerkiksi sijoitusvinkki kuulostaa liian hyvältä ollakseen totta, se todennäköisesti ei ole sitä. Oikeat sijoitusvälittäjät eivät tarjoa vinkkejä puhelimitse.



4. Romanssihuijaukset

Romanssihuijauksessa huijari esiintyy kuviteltuna henkilönä tavoitteenaan luoda romanssi tai ystävyssuhde tämän olemattoman hahmon ja huijauksen kohteen välille. Aikaansaatua romanssia hyödyntämällä huijarin tarkoituksena on saada kohteelta rahaa.

Rikoksen tekijät käyttävät häikäilemättömästi hyväksi ihmisten luonnollista tarvetta löytää seuraa tai elämäkumppani.

Taitavasti tunteisiin vetoamalla voidaan saada huijattua suuriakin summia rahaa. Romanssihuijaus saattaa kestää jopa vuosia. Ihmiseltä saatetaan viedä kaikki säästöt ja saada kohde ottamaan jopa lainaa. Moni romanssihuijauksen kohteena oleva menettää kymmeniä tai jopa satoja tuhansia euroja.



Romanssihuijaus saattaa muuttua sijoitushuijaukseksi, kun huijari ehdottaa houkuttelevia sijoitusmahdollisuuksia.



Romanssihuijauksen kulku

1. Huijari lähestyy kohdetta yleensä sosiaalisen median (esim. Facebook tai Instagram) tai deittisovellusten (esim. Tinder) tai muiden seuranhakupalveluiden kautta.
2. Yhteyttä pidetään pääsääntöisesti eri viestisovellusten kautta (WhatsApp, Hangouts, Messenger).
3. Huijari saattaa kertoa työskentelevänsä esimerkiksi kriisialueella tai öljynporauslautalla. Yleensä hän kertoo olevansa varakas ja hyvässä työssä.
4. Huijarin sosiaalisessa mediassa oleva profiili esittää usein komeaa ja varakasta upseeria tai kaunista näyttelijää esimerkiksi Amerikasta tai Itä-Euroopasta. Kuvat, henkilön nimi ja titteli elämäntarinaoineen on joko keksitty tai varastettu toisen ihmisen sometileiltä netistä.
5. Huijari kertoo usein tietävänsä paljon Suomesta ja haluavansa tulla käymään. Matkat Suomeen peruuntuvat kuitenkin aina erilaisten epäonnisten sattumien vuoksi.
6. Usein huijari kertoo saaneen hiljattain perinnön tai suuren summan rahaa muusta syystä tai on valmiiksi rikas. Huijari on kuitenkin jostain syystä estynyt käyttämään rahojaan ja pyytää kohdetta sen takia ”lainaamaan” rahaa.
7. Rahan sijaan huijari saattaa pyytää myös lahjakortteja tai kalliita tavaroita.
8. Huijari saattaa pyytää rahansiirtoa pankkisiirron sijaan kryptovaluuttana tai kansainvälisen välityspalvelun kautta.
9. Huijari voi myös yrittää saada kohteena olevan henkilön sijoittamaan rahansa olemattomiin sijoituskohteisiin, esimerkiksi kryptovaluuttaan.



Jos sinulle lähetetään rahaa yllättäen, älä käytä sitä tai lähetä eteenpäin. Ilmoita asiasta heti oman pankkisi asiakaspalveluun.

10. Rahansiirtoja pyydetään tekemään jonkun toisen tilille, ei huijariille itselleen. Rahapyynnöt saattavat liittyä myös johonkin hätään, kuten sairaalakuluihin, palkkojen maksamiseen, tullimaksuihin, työttömyyteen, eroon tai läheisen kuolemaan.
11. Huijari saattaa syyllistää tai uhkailla kohdetta, jos tämä ei suostu tai pysty tekemään pyydettyjä rahansiirtoja. Jos rahaa pyytäneen luotettavuutta epäilee, saattaa huijari esittää loukkaantunutta ja suuttua.
12. Huijari todistelee omaa luotettavuuttaan ja aitouttaan esimerkiksi lähettämällä kuvia itsestään, joissa hän on eläinten tai lasten kanssa tai luottamusta herättävässä työssä. Huijari saattaa esitellä myös linkkejä yrityksensä verkkosivuille.

Jos epäilet nettituttavasi luotettavuutta, kysy itseltäsi nämä kysymykset

- Miksi juuri minua lähestytään?
- Tiedänpö oikeasti, kuka nettirakkaani on?
- Olenko koskaan tavannut nettirakastani?
- Pyytääkö hän minulta rahaa vedoten mahdollisiin matkakuluihin, passin hankintaan tai erilaisiin dramaattisiin tapahtumiin ja tarinoihin?
- Onko rahanpyynnöissä painostuksen, kiireen tai kiristyksen maku?

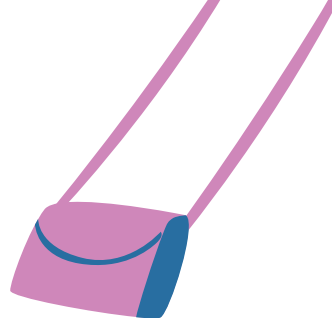


Näin voit välttyä romanssihuijaukselta

- Ole varovainen tutustuessasi uusiin ihmisiin netissä, varsinkin jos täysin vieras henkilö lähettää yllättäen viestin.
- Älä usko liian helposti kaikkiin tarinoihin, joita uusi tuttavasi kertoo.
- Pyri varmistamaan tuttavan henkilöllisyys esimerkiksi etsimällä hänestä tietoa netistä.
- Älä lähetä uudelle tuttavalle rahaa, lahjakortteja tai tavaroita. Älä myöskään lähetä henkilökohtaisia tietojasi tai kuvia passistasi.
- Älä nouda sinulle yllättäen lähetettyjä paketteja.
- Vaadi tapaamista ja sitä, että henkilö kustantaa itse matkansa luoksesi.
- Puhu läheisesi kanssa uudesta tuttavastasi, vaikka huijari kieltäisi sen.



**Jos jokin asia vaikuttaa
liian hyvältä tai liian
pahalta ollakseen totta,
se ei yleensä ole totta!**



5. Nettikauppahuijaukset

Nykyisin netistä voi ostaa lähes mitä tahansa. Luotettavien nettikauppojen lisäksi netistä löytyy myös huijaussivuja ja -mainoksia. Myös netin kirpputoreilla, kuten Tori.fi-palvelussa ja Facebookissa on huijareita, jotka saattavat esiintyä käytetyn tavarán ostajana tai myyjänä.

Nettikauppahuijauksissa rikolliset luovat aidon nettikaupan näköisiä sivuja verkkoon huijatakseen ihmisiltä rahaa. Netti-kirpputoreilla huijarit esiintyvät keksityillä henkilötiedoilla.

Huijausnettikaupoissa kaupataan mitä tahansa palveluita ja tavaroita, joita ihmiset hankkivat muutenkin (esim. vaatteet, lomaosakkeet, vuokramökit, puhelimet).



Älä tee ostopäätöstä kiireellä! Harkitse ja tarkista verkkokaupan luotettavuus esim. hakukoneen avulla.

Näin voit välttää nettikauppahuijauksen

- Muista, ettei mikään netissä ole ilmaista! Myyntitilanteessa huijari yrittää hämätä uskomattoman hyvillä tarjouksilla ja sydäntäsärkevillä tarinoilla ja ohjata nopeaan ostopäätökseen kiireellä painostaen.
- Tee ostoksia tuttujen yritysten sivuilla tai varmista verkkokaupan luotettavuus ja maine: etsi hakukoneella (esim. Google) keskustelupalstoilta muiden käyttäjien kommentteja yrityksestä ja tarkista, että verkkokaupan sivulla annetaan riittävästi tietoa yrityksestä.
- Älä osta, jos olet epävarma nettikaupan luotettavuudesta. Huijauksissa voidaan esiintyä myös tuttuina suomalaisina yrityksinä.
- Maksa aina luottokortilla, jos mahdollista. Luottokortilla maksettua voit kääntyä luottokortin myöntäneen pankin puoleen, jos joudut huijatuksi, eikä asian selvittely verkkokaupan kanssa onnistu.
- Lue tilausehdot huolellisesti, aina myös pienellä kirjoitettu teksti. Säilytä tilausvahvistukset, kaikki viestinvaihto myyjän kanssa ja kauppiaan kuittaus maksun hyväksynnän jälkeen.
- Nettikirpputoreilla kannattaa kiinnittää huomiota tuotteen kuviin ja hintaan sekä myyjän tietoihin. Onko kuva itse otettu vai kuvakaappaus? Onko hinta liian edullinen tai turhankin kallis? Ovatko muut antaneet myyjästä arvioita? Tarkkaile tai pyydä todisteita tuotteen aitoudesta. Jos mahdollista, sovi myyjän kanssa tapaaminen, jossa voit tutustua tavaraan ennen maksamista.
- Nettikirpputoreilla maksuun kannattaa käyttää tunnettuja toimijoita (esim. pankit, MobilePay, PayPal). Vastapuolen yhteystiedot on hyvä saada itselleen puolin ja toisin ennen maksusuoritusta.

Suomen kielen seassa on vieras-kielisiä sanoja.

Alennukset ovat suuria.



Tarjous on voimassa vain lyhyen ajan.

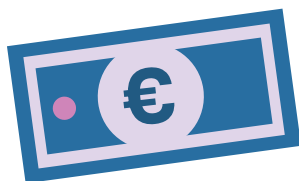
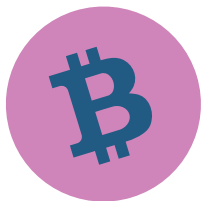
Kuvat näyttävät kuvapankista otetuilta tai tekoälyllä tehdyiltä. Kuvat voivat olla myös keskenään erityyppisiä.

Kuvassa on Kuluttajaliiton tekemä esimerkki valeverkkokaupasta. Kuluttajaa painostetaan toimimaan nopeasti houkuttelevilla tarjouksilla, jotka ovat voimassa vain lyhyen ajan.

Valeverkkokaupoissa on usein myynnissä tuotteita hyvin laajalla skaalalla: esimerkiksi vaatekaupassa voidaan myydä myös perämoottoreita ja ruokaa.

Tarkista aina ennen ostamista, että yritys antaa verkkosivuillaan selkeästi seuraavat tiedot, varsinkin jos kyseessä on sinulle aiemmin tuntematon verkkokauppa

- Yrityksen tiedot ja yhteystiedot (yrityksen virallinen nimi, maantieteellinen osoite, puhelinnumero ja sähköpostiosoite).
- Tuotteen tai palvelun sisältö ja hinta.
- Toimitus- ja muut kulut tai niiden määräytyminen sekä toimitustapa ja -aikataulu.
- Toimitusehdot ja niissä mahdollisesti mainittavat tuotteeseen liittyvät rajoitukset tai yllättävät ehdot.
- Onko kyseessä kertatilaus vai sitoutuuko ostaessa kestopäätökseen.
- Miten maksu tapahtuu ja millä ehdoilla.
- Miten tilauksen voi peruuttaa tai palvelun sulkea ostamisen jälkeen.
- Miten valituksen eli reklamaation voi tehdä.
- Maininta myyjän tai palveluntarjoajan lakisääteisestä virhevastuusta.
- Tieto mahdollisuudesta ja tavoista saattaa riita kuluttajariitalautakuntaan tai vastaavalle taholle.



6. Sijoitushuijaukset

Sijoitushuijauksessa houkutellaan huipputuottavan sijoitus-
tarjouksen varjolla hankkimaan esimerkiksi osakkeita, jouk-
kolainoja tai kryptovaluuttaa.

Usein ainutlaatuista huippusijoitusta tarjotaan erikoistar-
jouksena juuri sinulle. Tarjouksen kerrotaan olevan voimassa
lyhyen ajan ja luvataan äkkirikastumista.

Huijarit tehtailevat nettiin erilaisia valeuutisia ja -mainoksia,
joissa käytetään suomalaisten luotettaviksi koettujen jul-
kisuuden henkilöiden, kuten näyttelijöiden, poliitikkojen ja
yritysjohtajien kuvia ja väitetään heidän rikastuneen virtuaa-
livaluuttaan sijoittamalla tai suosittelevan Bitcoin-sijoituksia.

Sijoitushuijarit mainostavat myös sosiaalisessa mediassa,
kuten Facebookissa, Tinderissä ja hakukoneissa (esim. Goo-
gle). Huijarit voivat myös ottaa suoraan yhteyttä WhatsAp-
pissa tai muissa viestipalveluissa tai soittamalla.

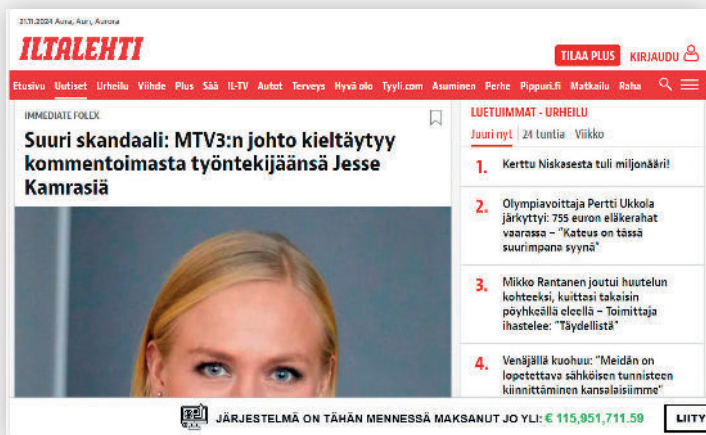
Sijoitushuijauksissa huijauksen kohteena olevien rahanme-
netykset ovat usein suuria, jopa kymmeniä ja satoja tuhansia
euroja.

Sijoitushuijauksen kulku

1. Sijoitushuijaus käynnistyy yleensä sosiaalisessa medias-
sa nähdystä valemainoksesta, jossa mainostetaan hyvin
tuottavia sijoituskohteita. Niihin kehoitetaan sijoittamaan
heti, sillä tilaisuus on voimassa vain hetken.
2. Mainos johtaa huijaussivulle, joka voi olla tehty näyttä-
mään esimerkiksi uutissivustolta. Sivulla ohjeistetaan
tarkasti, miten sijoitus tapahtuu. Kun huijauksen kohde
antaa yhteystietonsa, alkavat huijareiden painostavat
yhteydenotot, joiden tavoitteena on saada kohteelta
mahdollisimman paljon rahaa.
3. Huijauksen kohde huijataan sijoittamaan rahaa sijoitus-
kohteeseen, jota ei todellisuudessa ole olemassa.
4. Tämän jälkeen huijauksen kohteelle soitellaan ja lähete-
lään sähköpostia ja pyydetään lisäsijoitusta ulkomaiselle
pankkitilille tai virtuaalivaluutan vaihtopalveluun.
5. ”Todisteeksi” esitellään kuvia tekaistuista pörssikaaviois-
ta tai verkkosivuista, joiden mukaan sijoitukset tuottavat
hyvin. Huijarit voivat myös aluksi lähettää pieniä rahasum-
mia muka todisteeksi sijoitusvoitoista.
6. Huijauksen kohdetta saatetaan pyytää asentamaan tie-
tokoneeseen etähallintaohjelma, jolla sijoitusmyyjä va-
kuuttaa pystyvänsä antamaan parempaa palvelua. Todel-
lisuudessa huijari tekee kohteen pankkitililtä luvattomia
siirtoja tyhjentäen mahdollisesti koko tilin.
7. Yhteydenpito voi olla hyvin tiivistä ja aggressiivista, eikä
omia rahoja saa pois vaikka haluaisi nostaa sijoituksensa
tai saamansa ”voitot”.
8. Huijauksen paljastuttua huijarit voivat myöhemmin soit-
taa huijauksen kohteelle lakimiehinä esiintyen ja tarjota
apua huijauksen selvittämiseksi rahaa vastaan.

Sijoitushuijauksia varten tehdään usein uutissivu, jolla mainostetaan huijausta tutun suomalaisen julkisuuden henkilön kasvoilla. Sivut on usein naamioitu näyttämään esimerkiksi Yle uutisten sivuilta ja niissä on tarkat ohjeet sijoituksen tekemiseen ja mainoksia kryptovaluutoista. Usein sivuilla on kirjoitusvirheitä ja sivuilla olevat linkit muihin artikkeleihin eivät yleensä toimi. Huijaussivuja mainostetaan esimerkiksi Facebookissa ja Googlessa.

ESIMERKKI



Sijoitushuijausta varten tehdään usein huijaussivu, jota mainostetaan sosiaalisessa mediassa. Kuvassa olevalla huijaussivulla on luotu tunteisiin vetoava otsikko ja siinä annetaan yksityiskohtaiset tiedot sijoittamisesta. Sivulla on käytetty toimittaja Jesse Kamrasin nimeä sekä ulkoministeri Elina Valtonen kuvaa.



Huijauksissa on käytetty myös pääministeri Petteri Orpon kuvaa ja nimeä markkinoimaan olematonta sijoituskohdetta. Helsingin Sanomien sivuksi naamioidulla huijaussivulla väitetään, että Orpon määräyksestä suomalaiset alkavat saada veroista tuloja, mikä on tosiasiassa huijausta.

Jos epäilet sijoitushuijausta

- Muista, että kukaan ei tarjoa ilmaiseksi hyvin tuottavia sijoituskohteita tai sijoitusvinkkejä tavalliselle ihmiselle puhelimitse – ainoastaan huijarit tekevät näin.
- Älä sijoita rahojasi netissä (esim. Facebookissa) nähdyn mainoksen perusteella.
- Varmista sijoituskohteen ja sitä hoitavan yrityksen tausta ja luotettavuus. Apua voit kysyä esimerkiksi omasta pankistasi, jos et itse tiedä onko kohde aito vai huijausta.
- Älä sijoita kohteisiin, joita et ymmärrä. Varsinkin kryptovaluuttoihin sijoittamisessa kannattaa olla varovainen, sillä niihin liittyy paljon huijauksia ja riskejä.



Tekoäly on lähtökohtaisesti hyödyllinen arjen työkalu, jota voidaan käyttää esimerkiksi hakukoneissa, lääketieteessä ja valeutisten tunnistamisessa.

7. Tekoälyn käyttö huijauksissa

Tekoälystä on kuluttajalle paljon hyötyä, mutta kuten mitä tahansa työkalua, myös tekoälyä voidaan käyttää pahoissa aikeissa. Tekoälyn yleistymisen vaatii kuluttajilta ajantasaisia mediataitoja, kuten kriittistä medialukutaitoa.

Verkkorikolliset hyödyntävät erityisesti tekoälyä, joka tuottaa uutta sisältöä, kuten tekstiä, kuvia, videoita tai ääntä. Tekoälyä voidaan hyödyntää esimerkiksi henkilötietojen kalaste-luun erilaisten huijausten avulla. Tekoälyn avustuksella voidaan luoda myös esimerkiksi valheellista uutissisältöä, kuten uutiskuvia ja -videoita.

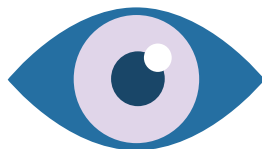
Suomen kieli on aiemmin karsinut suomalaisiin kohdistuvia huijausyrityksiä, mutta tekoälyn kehityksen myötä huijausyritysten kohdentaminen meille on entistä helpompaa. Huijauksia ei myöskään voi enää yhtä helposti tunnistaa esimerkiksi kielioppivirheistä, koska tekoäly mahdollistaa entistä vakuutavampien käännösten tekemisen.

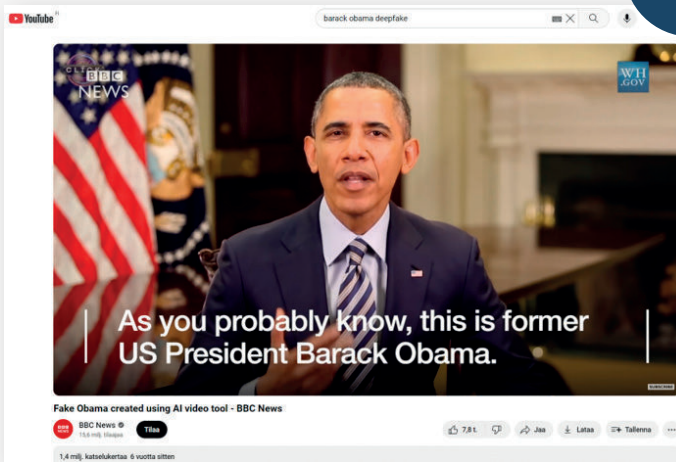
Esimerkkejä tekoälyhuijauksista

- **Huijaussoittot:** Tekoälyä voidaan käyttää esimerkiksi huijaussoittoihin, joihin väärennetään vaikkapa perheenjäsenen ääni. Väärennetyn äänen avulla soitetaan puhelu, jossa läheinen pyytää rahaa ”häätätilanteesta” selvittääkseen. Työntekijöihin voidaan kohdistaa huijaussoitto, jossa toimitusjohtaja pyytää kiireellisesti siirtämään rahaa.
- **Videot:** Tekoälyn avulla voidaan tehdä ”syväväärennöksiä” (deepfake) eli erittäin aidon ja realistisen näköisiä videoita, joilla näyttää esiintyvän esimerkiksi julkisuudesta tuttu henkilö. Tämä on kuitenkin huijausta. Ääntä voidaan poimia mm. sosiaalisessa mediassa julkaistuista videoista. Syväväärennöksen avulla on tehty mm. WhatsApp-videopuheluhuijauksia, joissa huijari on soittanut tutuksi henkilöksi naamioituneena ja pyytänyt rahaa.
- **Viestit:** Tekoälyn avulla huijarit pystyvät muotoilemaan viestejä aiempaa tehokkaammin. Tekoäly osaa tuottaa tekstiä, jonka kieli on sujuvampaa kuin esimerkiksi automaattisesti ohjelmoitujen ”spämmibottien”. Ne lähettävät saman sähköpostiviestin usealle henkilölle tai useaan uutisryhmään, jotka eivät niitä ole tilanneet tai halunneet.
- **Valokuvat:** Tekoälyn avulla voidaan luoda myös realistisia valokuvia. Tällaisia kuvia voidaan käyttää esimerkiksi romanssihuijauksissa. Tekoälyn luomat kuvat eivät välttämättä löydy käänteisellä kuvahauulla, mikä vaikeuttaa huijauksen tunnistamista.



Erilaiset sisällöntunnistustyökalut voivat auttaa erottamaan ihmisen tuottaman sisällön tekoälyn tekemästä (esim. Smodin).





Ison-Britannian yleisradioyhtiö BBC teki tekoälyn avulla syvävääärennös-esimerkkivideon Yhdysvaltain presidentti Barack Obamasta. Barack Obama ei kuitenkaan oikeasti esiinny videolla, vaan video on koostettu hänen aiemmista julkisista esiintymisistään.

Miten varautua tekoälyhuijauksiin?

1. Sovi läheistesi kanssa ”tunnussanasta”. Voit tiedustella tunnussanaa, jos saat läheisen nimissä viestin tai puhelun, jossa sinulta esimerkiksi pyydetään rahaa. Mikäli tunnussanaa ei ole sovittu, kysele yhteydenottajalta sellaisia tietoja, joita tekoäly ei voi tietää. Pyri aina varmistamaan soittajan tai viestin todenperäisyys.
2. Älä koskaan luovuta yhteydenottajalle henkilökohtaisia tietojasi, kuten pankkitietoja. Älä myöskään lähetä rahaa. Muista, että mikään viranomainen, poliisi, pankki tai posti ei soita ja pyydä henkilötietojasi, pankkitietojasi tai luotokortin numeroita.
3. Jos sinua yritetään kiristää, säilytä kaikki viestit tai videot ja ole yhteydessä poliisiin. Älä anna rahaa huijarille!

4. Ole kriittinen ja tietoinen. Tekoälyn räjähdysmäinen yleistyminen vaatii kriittisiä medialukutaitoja. Perehdy esimerkiksi valeutisten tunnusmerkkeihin ja tekoäyllä luodun sisällön tunnistamiseen.
5. Huijari pyrkii usein vetoamaan kiireeseen ja saamaan uhrin ohittamaan tavalliset prosessit. Maltti on valttia. Suhtaudu aina varauksella yllättäviin pyyntöihin ja poikkeuksiin.

Opi tunnistamaan tekoäyllä luotujen kuvien ja videoiden piirteitä

Tekoäyllä tehdyn kuvan tai videon voi tunnistaa aidosta kiinnittämällä huomiota yksityiskohtiin, kuten:

- Montako sormea kuvan ihmisellä on?
- Onko kuvan ihmisellä tai eläimellä kaikki raajat tallessa tai ylimääräisiä raajoja?
- Näyttävätkö ihmisen hiukset, kulmakarvat ja/tai parta pehmeiltä ja utuisilta?
- Onko ihmisen iho kuin muovailuvahaa?
- Jos kyseessä on video, liikkuvatko ihmisen suu ja silmät luonnollisesti?
- Onko kuvassa elementtejä, jotka muistuttavat siveltimen-vetoja?

Voit opetella tunnistamaan tekoälyn piirteitä esimerkiksi Ylen verkkosivuilta löytyvillä testeillä: www.yle.fi

Huom! Tekoäly kehittyy nopeasti. Tämä opas on tehty helmikuussa 2025. Tulevaisuudessa tekoäly saattaa osata luoda entistä aidompia kuvia ja videoita.



Tekoälyn avulla voidaan luoda realistisen näköisiä valokuvia. Viereinen kuva on tehty Midjourney 5.2. -tekoälyä käyttäen.



Tekoälyn avulla voidaan luoda myös taiteellisia kuvia. Viereinen "maalaus" on tehty ChatGPT:n GPT-4-palvelun avulla. Tunnistaisitko sen tekoälyn tekemäksi?



8. Turvavinkit laitteiden ja käyttäjätilien suojaamiseen

Useimmilla meistä on käytössään erilaisia digilaitteita, jotka ovat yhteydessä nettiin. Suojaamalla laitteesi pystyt paremmin estämään esimerkiksi käyttäjätiliesi kaappauksen tai laitteesi hyödyntämisen palvelunestohyökkäyksissä.

- Tutustu oman laitteesi tietoturva-asetuksiin.
- Vaihda laitteen oletussalasana. Esim. oletuksena usein olevat admin, 0000 tai 1234 ovat helposti arvattavissa.
- Pidä laitteiden, ohjelmistojen ja sovellusten päivitykset ajan tasalla.
- Päivitä sovellukset ainoastaan virallisen sovelluskaupan kautta.
- Jos haluat myydä tai kierrättää puhelimesi, ota ensin talteen puhelimella olevat tarpeelliset tiedot, kuten kuvat, videot, viestit ja yhteystiedot. Palauta sitten puhelimen tehdasasetukset ja poista SIM-kortti. Näin varmistat, että laitteella olevat tiedot eivät päädy väärin käsiin.
- Tietokoneen ja muiden laitteiden myymisen tai kierrättämisen osalta katso tarkemmat ohjeet googlaamalla esim. ”äly- ja digilaitteetkin kuuluvat kierrätykseen”

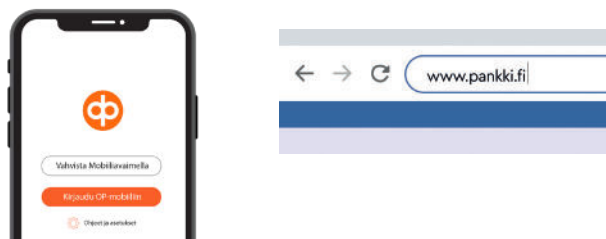
- Luo jokaiseen palveluun ja laitteeseen eri salasana.
- Vältä helppoja salasanoja, kuten 123456 tai ”salasana”.
- Käytä tarpeeksi turvallisia salasanoja: vähintään 12 merkkiä, isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.
- Harkitse salasanalauseiden käyttöä.
- Tallenna salasanat omaan käyttöösi selkeällä menetelmällä.
- Vaihda salasanat riittävän usein.
- Valitse mahdollisuuksien mukaan monivaiheinen tunnistautuminen. Monivaiheisessa tunnistautumisessa henkilöllisyytesi varmistetaan salasanan lisäksi ylimääräisellä todennuksella, joka on kertakäyttöinen numerosarja tai koodi. Monivaiheista tunnistautumista kannattaa aina käyttää etenkin sellaisissa palveluissa, joissa on henkilö- tai maksutietoja.
- Harkitse, onko laitetta pakko yhdistää nettiin.



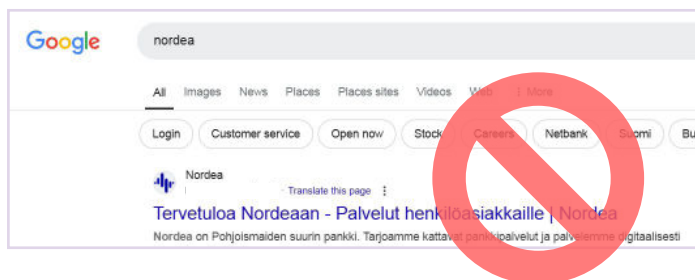
Monet puhelinoperaattorit ja tietoturvayritykset tarjoavat erilaisia palveluita, joiden tarkoitus on parantaa laitteiden tietoturvaa. Maksulliset palvelut voivat tarjota lisäturvaa tietyissä tilanteissa, mutta ne eivät ole aina välttämättömiä kaikille käyttäjille. Hyvät tietoturvataidot kantavat pitkälle!

9. Pankkiasioinnin turvavinkkejä

- Pankkiin ja viranomaistahojen palveluihin on turvallisinta kirjautua ainoastaan kyseisen tahon virallisen mobiilisovelluksen tai omien tallennettujen kirjanmerkkien kautta tai kirjoittamalla osoite suoraan nettiselaimen osoiteriville.



- Pankin, viranomaisen tai muun vastaavan tahon palveluun ei kannata kirjautua hakukoneen (esim. Google) hakutuloksiin nousseiden linkkien kautta. Huijarit tehtailevat aitojen sivujen näköisiä valesivustoja ja ostavat niille näkyvyyttä hakukoneissa.



- Käytä pankkitunnuksiasi vain pankin omassa sovelluksessa tai nettisivulla. Suosi muissa paikoissa tunnistautumiseen esimerkiksi mobiilivarmennetta, jonka voit saada omalta puhelinoperaattoriltasi. Mobiilivarmenteen käyttö saattaa olla maksullista. Kysy lisää omalta operaattoriltasi.

- Ainakin jotkut pankit tarjoavat mahdollisuuden asettaa maksukortteillesi ja tilisiirroille maarajoituksia. Tällöin kortilta tai tililtä voi tehdä maksusuorituksia vain valitsemiisi maihin, esim. ainoastaan Suomessa.
- Voit asettaa vuorokausikohtaisen käyttörajan maksukorttien käteisnostoille, maksuille maksupäätteellä ja maksuille verkossa sekä sovelluksissa. Myös tileille voi asettaa rajoituksia.
- Maksuraja voi olla järkevää asettaa mahdollisimman matalaksi kortteille, joilla teet esim. paljon verkko-ostoksia.

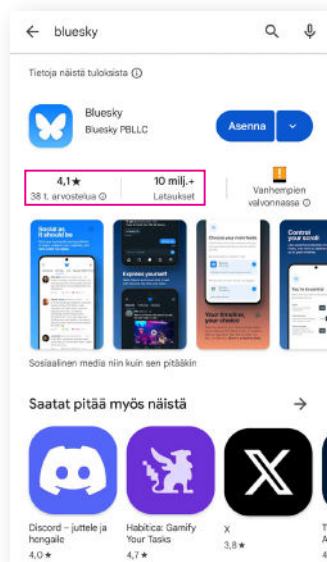
Käytännöt voivat vaihdella pankkikohtaisesti. Kysy lisää pankiltasi tai tutustu asiaan verkkopankissasi.

- Jos haluat turvata säästösi pankkitunnusten kalastelulta, avaa esimerkiksi toisessa pankissa tili, johon ei ole netti-pankkitunnuksia ja siirrä säästösi sinne.



Muista nämä vinkit, kun lataat uutta sovellusta

1. Lataa sovelluksia vain virallisista sovelluskaupoista (esim. App Store, Google Play).
2. Tutustu huolellisesti sovelluksen nimeen, kuvakkeeseen ja julkaisijaan.
3. Tarkastele, kuinka moni muu on jo ladanut sovelluksen. Mitä enemmän sovellusta on ladattu sitä parempi.



Lue tämä, jos olet joutunut tietomurron uhriksi tai epäilet tietojesi väärinkäyttöä

Pikavinkit tietomurron uhreille ja tietojen väärinkäytön vähentämiseen ennakolta

- Tee muuttosuojaus Postille sekä Digi- ja väestötietovirastoon
- Harkitse vakavasti luottokieltoa
- Tee rekisteröintikielto Patentti- ja rekisterihallitukselle
- Tee tietojen luovuttamisen kiello Väestötietojärjestelmään
- Muuta tarvittaessa puhelinnumerosi salaiseksi
- Poista tietosi käyttämisestä laskutuspalveluista (esim. Klarna) ja kiellä niiden käyttö
- Huolehdi turvallisista salasanoista ja kaksivaiheisesta tunnistautumisesta

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



10. Kysy rohkeasti apua

Jos olet menettänyt rahaa, henkilötietoja tai pankkitunnukset

1. Ole mahdollisimman nopeasti yhteydessä oman pankkisi asiakaspalveluun ja kerro huijauksesta. Pankki voi sulkea pankkitilisi ja pankki- ja luottokorttisi, jos tiedot ovat päätyneet huijarille.
2. Tee rikosilmoitus poliisille, www.poliisi.fi. Ilmoittaminen kannattaa aina, sillä poliisi voi päästä ilmoituksen avulla rikollisten jäljille.

Hae apua muualta

3. Älä jää yksin! Puhu huijauksesta läheistesi kanssa. Lisäksi voit keskustella huijauksesta ottamalla yhteyttä Rikosuhri-
riipäivystykseen: www.riku.fi
4. Huijauksen selvittämisessä auttaa Kilpailu- ja kuluttajavirasto, jos kotimainen yritys on huijannut: www.kkv.fi/kuluttajaneuvonta
5. Neuvoja tai sovitteluapua maiden rajat ylittävän kaupan ongelmatilanteissa antaa Euroopan kuluttajakeskus Suomessa: www.ecc.fi

Omaehtoinen luottokielto

Jos olet menettänyt henkilötietosi rikollisille huijauksen seurauksena, voit ottaa omaehtoisen luottokiellon

- Oma luottokielto estää tekemästä mitään luotollisia ostoksia. Sen voi itse keskeyttää tarvittaessa.
- Omaehtoisen luottokiellon voi tehdä kaikkiin olemassa oleviin rekistereihin:
 - » Verohallinnon positiivinen luottotietorekisteri (maksuton)
 - » Suomen Asiakastieto Oy (maksullinen)
 - » Dun & Bradstreet Oy (maksullinen).
- Lisätietoa omaehtoisesta luottokiellosta löydät Suomi.fi-palvelusta.

Huijatun kokeman häpeän käsittely ja huijauksen uhrin auttaminen

Huijattu on petosrikoksen uhri, eikä huijatuksi joutumista tarvitse hävetä. Huijatuksi tuleminen voi aiheuttaa suurta häpeän tunnetta ja kohde saattaa syyttää itseään tapahtuneesta.

Häpeän käsittelyssä tärkeintä on puhua huijauksesta ja hakea tarvittaessa ammattiapua. Kun ihminen kokee valmiiksi häpeää, häntä kannattaa kohdella ymmärtäväisesti.

Apua digiasioinnissa

Digiasioissa apua voi kysyä esimerkiksi kirjastoilta, alueellisilta digitukiyhdistyksiltä sekä Eläkeliiton paikallisyhdistysten vertaisohjaajilta. Voit kysyä apua myös omalta operaattoriltasi tai pankiltasi.

SeniorSurf-toiminta tarjoaa digiopastusta senioreille.

Katso: www.seniorsurf.fi/seniorit/opastuspaikat

Reklamaation tekeminen

Jos olet tullut huijatuksi ja menettänyt rahaa, voit tehdä pankille reklamaation.

Ota yhteyttä omaan pankkiisi ja tee asiastasi kirjallinen reklamaatio eli vaatimus. Huomioi, että suullinen reklamaatio ei ole riittävä. Varmista, että saat asiastasi kirjallisen päätöksen.

Mikäli olet tyytymätön pankin kirjalliseen vastaukseen tai haluat lisätietoja asiastasi, voit olla yhteydessä FINE Vakuutus- ja rahoitusneuvontaan puhelimitse tai chatin kautta: www.fine.fi

Mikäli asiasi ei ratkea neuvonnan keinoin, voidaan asia käsitellä riita-asiana joko toimistomenettelyssä tai Pankkilautakunnassa. FINE antaa riita-asiasta kirjallisen ratkaisusuosituksen.

Ratkaisusuositukset ovat nimensä mukaisesti suosituksia, eikä niitä ole pakko noudattaa. Palveluntarjoajat ovat kuitenkin noudattaneet niitä lähes poikkeuksetta. Koska FINEn ratkaisut ovat suosituksia, niistä ei voi erikseen valittaa. FINEn osalta asian käsittely päättyy ratkaisusuosituksen antamiseen.

Jos olet FINEn ratkaisun jälkeen asian lopputulokseen edelleen tyytymätön, voit nostaa tuomioistuimessa kanteen vastapuolena olevaa palveluntarjoajaa vastaan kanneajan puitteissa. Asian käsittelyä varten asiakas voi tarkistaa mahdollisuutensa saada yleistä oikeusapua ja tarkastaa mahdollisen oikeusturvavakuutuksensa kattavuuden.

Lähde: www.fine.fi

11. Lisätietoja huijauksista

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

**Huijauksista varoitetaan esimerkiksi
Huijausinfon ja Kyberturvallisuuskeskuksen sekä
poliisin sosiaalisen median kanavissa ja netti-
sivuilla**

Huijausinfo

Facebookissa ja Instagramissa @huijausinfo

Kyberturvallisuuskeskus

Viestipalvelu X:ssä @CERTFI ja Facebookissa @NCSC-FI

Poliisi

Viestipalvelu X:ssä ja Facebookissa @Suomenpoliisi

**Yle Oppimisen Digitreenien materiaalit
huijauksista**

www.yle.fi/aihe/digitreenit

**SeniorSurf-toiminnan vinkit mm. digilaitteiden
käyttöön ja netissä toimimiseen**

www.seniorsurf.fi

**Kuluttajaliiton YouTube-kanavalla on useita
huijauksiin liittyviä koulutusvideoita**

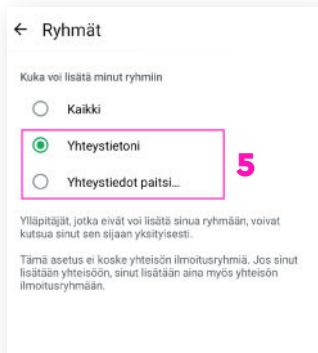
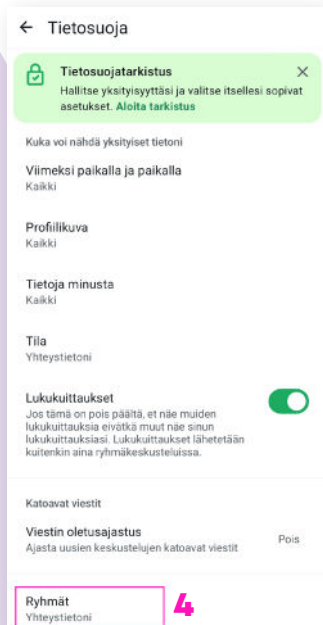
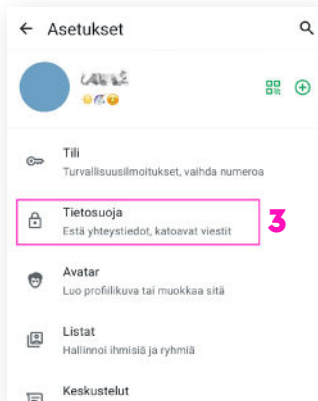
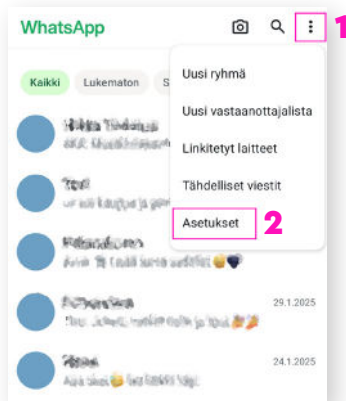
www.youtube.com/@kuluttajaliittory



Tietoisku

Tiesitkö, että voit estää WhatsAppissa yhteystietojesi ulkopuolisia henkilöitä lisäämästä sinua ryhmiin?

Toimi näin: Klikkaa sovelluksen oikeassa ylänurkassa kolmea pistettä > Asetukset > Tietosuoja > Ryhmät.

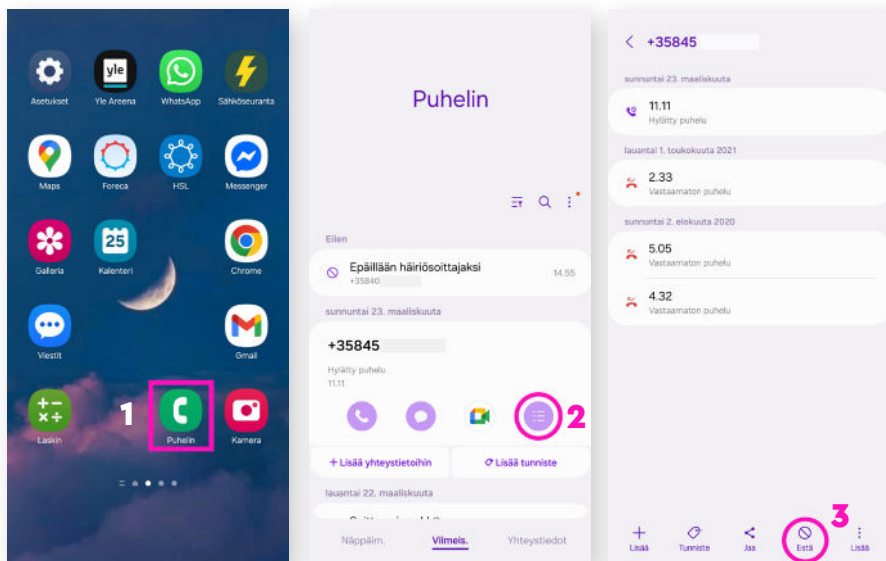


Tietoisku

Jos saat puheluita ja viestejä henkilöltä, jolta et halua yhteydenottoja, voit estää häntä ottamasta jatkossa sinuun yhteyttä. Alla näet esimerkin, miten estää epätoivottu numero Android-puhelimella.

Toimi näin: Klikkaa puhelinkuvaketta > Valitse numero, jonka haluat estää > Klikkaa kolmea pistettä tai ”i”-kuvaketta > Klikkaa ”estä”.

Eston voi halutessaan poistaa samalla tavalla.



Operaattorit ja muut telealan toimijat tarjoavat erilaisia palveluita tuntemattomien soittajien ja häirikköpuheluiden tunnistamiseen. Tutustu eri vaihtoehtoihin.

huijausinfo.fi



**KULUTTAJALIITTO
KONSUMENTFÖRBUNDET**