PC-KEISARI

🎣 Huijausviestit – tunnista ja toimi -pikaopas

Näin tunnistat viranomaisen, pankin tai kuljetusyhtiön nimissä tulevan huijausviestin – ja näin toimit, jos ehdit jo antaa tietojasi.

👥 Itseopiskeluun · Taso: ei ennakkotietoja · ⏱ n. 15–20 min lukuaikaa

🎭 Tunnista huijaus ajoissa

Huijausviestit näyttävät nykyään usein aidoilta: logot ovat oikeat ja kieli voi olla täysin virheetöntä. Siksi kannattaa katsoa ennen kaikkea sitä, **mitä viesti pyytää sinua tekemään**.

📋 Näistä merkeistä tunnistat huijauksen

1. **Kiire tai pelko:** "tilisi suljetaan", "maksu on maksamatta", "paketti jää toimittamatta".
2. **Luotettava nimi:** lähettäjä esiintyy pankkina, viranomaisena tai muuna tuttuna tahona ja pyytää tietojasi.
3. **Linkki tai painike:** sen kautta pitäisi kirjautua verkkopankkitunnuksilla tai antaa henkilö- tai maksutietoja.
4. **Lähettäjän osoite** näyttää ensisilmäyksellä oikealta, mutta on tarkemmin katsottuna jotain muuta.
5. **Liian hyvä tarjous** – se ei todennäköisesti ole totta.

💡 **Muista:** kömpelö kieli voi paljastaa huijauksen, mutta *virheetön* kieli ei todista, että viesti on aito. Nykyään huijausviestit kirjoitetaan usein täydellisellä suomella.

🔁 **Muistatko: viesti on kirjoitettu virheettömällä suomella ja siinä on pankin logo. Onko se siis aito?**

Ei välttämättä. Logon ja hyvän kielen voi kopioida. Ratkaisevaa on, pyydetäänkö sinua toimimaan kiireellä, avaamaan linkki tai antamaan tunnuksia – silloin kyse on lähes varmasti huijauksesta.

🏛️ Esimerkki: viesti "Suomi.fi-palvelusta"

Suomi.fi-palvelun nimissä liikkuu toistuvasti uskottavan näköisiä huijaussähköposteja. Niissä kerrotaan, että Suomi.fi-viesteihisi on tullut uusi viesti – esimerkiksi päätös verottajalta – ja kehotetaan painamaan **Avaa viesti** -painiketta. Painike vie huijaussivulle.

📋 Näin tarkistat lähettäjän

1. **Älä paina viestin painiketta tai linkkiä.**
2. Katso lähettäjän nimeä. Huijausviestissä siinä voi lukea uskottavasti esimerkiksi "Viestipalvelu".
3. Paina tai napauta lähettäjän **nimeä**. Nyt näet koko sähköpostiosoitteen.
4. Lue osoite loppuun asti. Jos se on jonkin aivan muun organisaation – esimerkiksi ulkomaisen yliopiston – osoite, viesti on huijaus.

💡 **Näin tunnistat aidon Suomi.fi-ilmoituksen:** Suomi.fi-viestien sähköposti-ilmoituksessa **ei ole koskaan linkkiä**. Siinä vain kerrotaan, että palvelussa odottaa viesti. Suomi.fi-viestit ei myöskään koskaan lähetä ilmoituksia **tekstiviestillä**.

🔁 **Kokeile: sähköpostissa lukee "Sinulle on uusi viesti Suomi.fi-palvelussa" ja alla on sininen *Avaa viesti* -painike. Aito vai huijaus?**

Huijaus. Aidossa Suomi.fi-ilmoituksessa ei ole linkkejä eikä painikkeita. Jos haluat varmistaa, onko sinulle tullut viesti, kirjoita selaimeen itse **suomi.fi** tai avaa Suomi.fi-sovellus ja kirjaudu sitä kautta.

🔐 Asioi aina turvallista reittiä

Paras suoja on yksinkertainen tapa: **et koskaan kirjaudu viestissä olevan linkin kautta**. Menet palveluun aina itse.

📋 Näin teet sen

1. Kirjoita palvelun virallinen osoite (esim. **suomi.fi** tai pankkisi osoite) itse selaimen osoiteriville.
2. Tallenna sivu **kirjanmerkiksi**. Seuraavalla kerralla avaat sen kirjanmerkistä.
3. Jos palvelulla on virallinen **mobiilisovellus**, käytä sitä.
4. Älä mene palveluun myöskään **hakukoneen tulosten** kautta – huijarit voivat ostaa mainospaikkoja hakutulosten yläpuolelta.
5. Jos epäilet yhteydenottoa, soita yrityksen tai viranomaisen asiakaspalveluun numerosta, jonka olet **itse etsinyt** – älä viestissä annetusta numerosta.

💡 **Vinkki:** kirjautumiseen muihin kuin pankkipalveluihin voit käyttää **mobiilivarmennetta**. Silloin pankkitunnuksesi eivät ole vaarassa.

❓ Entä jos puhelimeen pyydetään asentamaan ohjelma?

Älä asenna mitään, jonka todellista tarkoitusta et tiedä – vaikka pyytäjä esittäytyisi pankin tai viranomaisen edustajaksi. Lopeta puhelu tai keskustelu heti, kun jokin epäilyttää.

🔁 Muistatko: mitkä kolme turvallista reittiä verkkopalveluun on?

1) Kirjoitat osoitteen itse osoiteriville, 2) avaat palvelun tallentamastasi kirjanmerkistä tai 3) käytät palvelun virallista sovellusta.

🚨 Jos pahin tapahtui – älä viivyttele

Jos painoit linkkiä ja annoit tietojasi, toimi heti. Nopeus vähentää vahinkoja. Huijatuksi joutuminen ei ole häpeä – huijaukset ovat taitavasti tehtyjä.

📋 Näin toimit, tässä järjestyksessä

1. **Soita heti omaan pankkiisi.** Numero löytyy pankkikortin takaa tai pankin omilta sivuilta.
2. **Annoitko korttitiedot?** Sulje kortti: korttien sulkupalvelu palvelee ympäri vuorokauden numerossa **020 333** (ulkomailta **+358 20 333**).
3. **Annoitko salasanan?** Vaihda se heti – sekä kyseiseen palveluun että kaikkiin muihin, joissa käytät samaa tunnusta ja salasanaa.
4. **Tee rikosilmoitus** poliisille (poliisi.fi).
5. **Seuraa tilitapahtumiasi** lähipäivinä ja ilmoita oudoista veloituksista heti pankkiin.

💡 **Vinkki:** tallenna numero **020 333** puhelimesi yhteystietoihin nimellä "Korttien sulku". Hätätilanteessa sitä ei tarvitse etsiä.

🔁 **Muistatko: kenelle soitat ensimmäisenä, jos annoit verkkopankkitunnuksesi huijarille?**

Omaan pankkiisi – heti. Korttitiedoista soitat lisäksi korttien sulkupalveluun 020 333. Rikosilmoituksen voi tehdä vasta sen jälkeen.

🤝 Älä jää yksin – apua ja ilmoitus

Huijauksen jälkeen moni tuntee häpeää tai ahdistusta. Siitä kannattaa puhua – läheiselle tai ammattilaiselle.

📋 Mistä saat apua

1. **Rikosuhripäivystys** auttaa rikoksen uhreja ja heidän läheisiään numerossa **116 006**: ma–to klo 9–18 ja pe klo 9–16. Palvelu on maksuton.
2. **Kerro läheiselle.** Samalla varoitat häntä samanlaisesta viestistä.
3. **Ilmoita huijausviestistä** Kyberturvallisuuskeskukselle: **kyberturvallisuuskeskus.fi** → Ilmoita. Ilmoitusten avulla viranomaiset voivat varoittaa muita.

🔁 **Muistatko: mihin numeroon voit soittaa, jos huijaus jää vaivaamaan mieltä?**

Rikosuhripäivystykseen numeroon **116 006** (ma–to 9–18, pe 9–16).

🧭 Muistilista koottuna

Tilanne	Toimi näin
Viestissä on linkki tai painike kirjautumiseen	Älä paina. Mene palveluun itse kirjoittamalla osoite.

Lähettäjä näyttää viralliselta	Paina lähettäjän nimeä ja lue koko osoite.
"Uusi viesti Suomi.fi-palvelussa" + Avaa viesti -painike	Huijaus – aidossa ilmoituksessa ei ole linkkejä.
Soittaja pyytää tunnuksia tai asentamaan ohjelman	Lopeta puhelu. Soita itse virallisesta numerosta.
Annoit verkkopankkitunnukset	📞 Oma pankki heti
Annoit korttitiedot	📞 Korttien sulku **020 333** (24/7)
Tarvitset tukea	📞 Rikosuhripäivystys **116 006**

✅ Mitä osaan nyt?

Käy mielessäsi läpi, osaatko jo nämä asiat. Jos jokin kohta epäilyttää, palaa sen aiheen kohdalle ja lue se vielä kerran.

- [ ] Tunnistan huijauksen merkit: kiire, luotettava nimi, linkki ja tietojen pyytäminen.
- [ ] Tiedän, että virheetön kieli ja oikea logo eivät todista viestiä aidoksi.
- [ ] Osaan tarkistaa lähettäjän koko sähköpostiosoitteen.
- [ ] Tiedän, ettei aidossa Suomi.fi-ilmoituksessa ole linkkejä.
- [ ] Menen verkkopalveluihin aina itse: osoiterivi, kirjanmerkki tai virallinen sovellus.
- [ ] Tiedän, että tunnuksista soitan heti pankkiin ja korttitiedoista numeroon 020 333.
- [ ] Tiedän, mistä saan tukea (116 006) ja minne voin ilmoittaa huijausviestistä.