

# HAITALLISESTA TAI EPÄILYTTÄVÄSTÄ SÄHKÖPOSTIVIESTITÄ ILMOITTAMINEN

Aalto-yliopiston tietotekniikkapalveluiden tietoturvaryhmä pyytää malliviestejä liittyen haitalliseen tai epäilyttävään sähköpostiviestintään. Nämä viestit ovat normaalisti huijaus- tai urkintaviestejä, ja ne saattavat myös sisältää liitteisiin piilotettuja haittaohjelmia. Tietoturvaryhmän tavoitteena on sekä estää pääsy viestien mukana välitettävien linkkien osoittamiin mahdollisiin haitallisiin palveluihin että opettaa roskapostin suodatuksen käytettävää järjestelmää tunnistamaan ja varoittamaan näistä viesteistä. Liitetiedostot tarkastetaan haittaohjelmien varalta, ja toimitamme tarvittaessa näytteitä haittaohjelmatorjuntaohjelmistojen valmistajille. Näihin tarkoituksiin viestit tarvitaan täydellisinä, eli kaikkine otsikkokenttineen, linkkeineen ja liitteineen. Helpoimmin tämä onnistuu lähettämällä epäilyttävä viesti sähköpostin liitteenä suoraan tietoturvaryhmälle (security@aalto.fi) seuraavassa kuvattavien (kuvaukset Aallossa tuetulle postiohjelmistolle) toimintamallien avulla.

Viestin lähettäminen liitteenä tapahtuu **Outlookissa** seuraavasti:

- aloita uuden viestin lähettäminen osoitteella: security@aalto.fi
- kirjoita lyhyt vapaamuotoinen saateviesti sekä otsikko
- vedä ja pudota (drag & drop) viestilistasta malliviesti tämän uuden viestin päälle
- lähetä viesti

Viestin lähettäminen liitteenä tapahtuu **Outlook Web App:issa (OWA)** seuraavasti:

- viestilistalla klikataan hiiren oikealla malliviestiä
- valitaan "forward as attachment" tai "välitä liitteenä"
- kirjoita lyhyt vapaamuotoinen saateviesti sekä otsikko
- vastaanottajaksi merkitään security@aalto.fi
- lähetä viesti

Viestin lähettäminen liitteenä tapahtuu Thunderbirdissä seuraavasti:

- viestilistalla klikataan hiiren oikealla malliviestiä
- valitaan "forward as" ja edelleen "attachment"
- kirjoita lyhyt vapaamuotoinen saateviesti sekä otsikko
- vastaanottajaksi merkitään security@aalto.fi
- lähetä viesti

Mikäli viestin otsikon alkuun on jo leimattu merkintä "possible spam" ja viesti on ohjautunut roskapostikansioon, on suodatus toiminut oikein, eikä mallia tarvitse lähettää. Mallin voi tässäkin tapauksessa lähettää, mikäli epäilee viestin olevan väärin merkitty roskaksi. Viesti(t) analysoidaan ja tuloksesta tiedotetaan lähettäjää. Analyysin aikana viestin linkkejä ei tule klikkailla, eikä mahdollisia liitetiedostoja avata.