TIETOJENKALASTELULTA SUOJAUTUMINEN

opsec
www.opsec.fi

TUNNISTA SÄHKÖPOSTIIN TULLUT HUIJAUSVIESTI

- **Epäile sähköpostiviestiä huijaukseksi, jos viestin sisältö on kirjoitettu huonolla kielellä tai viesti sisältää kiristykseen tai uhkailuun liittyvää sisältöä.**
- **Ole erityisen tarkkana, jos viestin sisältöön liittyy raha (esim. lasku-, palkka- tai tilitiedot).**
- **Huijausviestin sisältö voi olla kohdennettu sinulle työtehtäviesi tai aikaisempien viestiesi perusteella, joten varmista viestin aitous, jos epäilet sen sisältöä.**

KYSEENALAISTA LÄHETTÄJÄN TIEDOT

- **Suhtaudu epäilevästi myös viestin lähettäjätietoihin, jos viestissä on jotain epäilyttävää. Huijausviestit voivat tulla tutun henkilön nimissä, joten tutun henkilön yhteystiedot voivat löytyä niin sähköpostiosoitteesta kuin allekirjoituksestakin.**

EPÄILE LINKKEJÄ, LIITTEITÄ JA SIVUSTOJA

- **Epäile viestissä saamaasi linkkiä tai liitettä, jos sen kautta avattava hyperlinkki poikkeaa hiemankin aidosta url-osoitteesta. Epäile myös linkistä avattavaa sivustoa, jos sivuston ulkoasu poikkeaa aidosta sivustosta.**
- **Älä koskaan kirjoita tunnuksiasi sivustolle, jos et ole varma sivuston luotettavuudesta. Kirjaudu palveluihin ja järjestelmiin vain niiden linkkien kautta, joita yleensä käytät.**

PANOSTA SALASANOIHIN

- **Käytä eri salasanaa eri palveluissa ja järjestelmissä. Näin varastetuilla tunnuksilla ei voi kirjautua useampaan palveluun tai järjestelmään.**
- **Panosta salasanojen laatuun. Käytä salasanoja, jotka ovat tarpeeksi pitkiä ja sisältävät erikoismerkkejä ja numeroita.**

TUNNUKSET VAARASSA?

- **Jos epäilet joutuneesi tietojenkalastelun uhriksi tai epäilet omien tunnusten joutuneen vääriin käsiin, kirjaa ylös, mitä on tapahtunut.**
- **Ota aina välittömästi yhteyttä oman organisaation tietoturvasta vastaavaan tahoon:**