



Vipuvoimaa
EU:lta
2014–2020

Virtuaalisten kohtaamisten tietoturva

Luotettu verkko, ohjelmistopäivitysten asentaminen, palomuuuri ja virustarjonta ovat tietoturvallisuuden peruselementtejä. Kun osallistut tapahtumaan, on muun valmistautumisen ohella hyvä ottaa huomioon myös oma ja muiden tietoturva. Muistathan, että viime kädessä vastuu omien tai muiden tietojen jakamisesta on sinun vastuullasi. Harkitse siis aina tilannekohtaisesti kenelle, miten ja mitä tietoa jaat.

Kokosimme avuksesi kolme tärkeintä käytännön vinkkiä tietoturvan varmistamiseksi tapahtuman aikana:

1. Ympäristö

Jakaessasi luottamuksellista tietoa varmista, että olet hiljaisessa ja yksityisessä ympäristössä niin, ettei tilassa ole muita henkilöitä, eikä kukaan ulkopuolinen voi kuulla keskustelua tai nähdä näyttöäsi. Mikäli ympäristösi ei anna täyttä näkösuojaa koneesi näytölle, voit käyttää sen suojana tietoturvakalvoa.

2. Henkilötietojen jakaminen

Mieti jo etukäteen, mitä asioita haluat eri tilanteissa jakaa itsestäsi tietoturva huomioiden. Esimerkiksi henkilötietojen, puhelinnumeroiden, sähköpostiosoitteiden yms. tarpeetonta julkista jakamista tulee välttää. Hyödynnä yksityisviestien mahdollisuutta harkinnan mukaan.

3. Tiedostojen jakaminen

Jos haluat jakaa tiedostoja Zoom tai Adobe Connect -istuntojen aikana, käytä mieluiten näytön jakamisen toimintoa sen sijaan, että lataisit tiedostot suoraan käytössä olevaan sovellukseen. Varmista kuitenkin, ettet näyttöä jakaessasi tule jakaneeksi jotain sellaista, mitä ei ollut tarkoitus. Esimerkiksi pikaviestimien ja sähköpostin ponnahdusikkunat kannattaa estää tilaisuuden ajaksi esimerkiksi sulkemalla sovellukset.

Tapahtumanjärjestäjä poistaa työtilan käytöstä kesäkuun 2019 aikana.