KUINKA TUNNISTAN HAITALLISEN SÄHKÖPOSTIVIESTIN - TOP-10 VINKIT

Yliopistomme roskapostin suodatukseen hankkimaa ja käyttämää järjestelmää opetetaan tunnistamaan yhä tehokkaammin erilaisia huijaus-, urkinta- yms. haitallisia sähköpostiviestejä tavallisen roskapostin lisäksi. Valitettavasti mikään tekninen järjestelmä ei kuitenkaan voi taata 100%:sta suojaa, ja viime kädessä ratkaisun viestin ja liitteiden avaamisesta tekee aina sen vastaanottaja. Tästä syystä on hyvä opetella tunnistamaan tavallisimmat vaaran merkit. Seuraavassa on kuvattu top-10 vinkit tunnistamisen avuksi. Yksikin saattaa riittää, mutta mitä useampi ehdoista täyttyy, sitä varmemmin viesti on huijausta sekä useimmiten myös vaarallinen.

1. Onko viesti roskapostikansiossa ja leimattu ”possible spam” merkinnällä otsikon alussa?
   - Nämä viestit on tarkastettu ja epäilyttäviksi havaittu. Virheitä tapahtuu, mutta ne ovat harvinaisia tai niille on selkeä syy (esim. linkki epäilyttävään palveluun).
2. Kysytäänkö viestissä salasanoja tai tunnuksia (esim. Aalto, luottokortit, pankit)?
   - Tunnuksia EI kysytä. Jos kysytään, on se huijausta tai urkintaa ja esim. Aalto sekä pankit eivät lähetä sähköpostilla kirjautumispyyntöjä tai -linkkejä.
3. Onko lähettäjän osoite järkevä ja oletko viestin ainoa sekä oikea vastaanottaja?
   - Katso onko lähettäjän osoite järkevä ja mieti miksi viestillä on useita vastaanottajia tai miksi ne piilotetaan.
4. Onko viestissä käytetty kieli väärä ja/tai onko siinä paljon kirjoitusvirheitä?
   - Yritykset ja organisaatiot tietävät oikean palvelukielen kohdallasi. Kansainvälisessä viestinnässä englanti on standardikieli, ei ruotsi, saksa, puola, tms. Useat kirjoitusvirheet viesteissä ovat harvinaisia ja aina vaaran merkki.
5. Kirjautumista vaativien linkkien tulee aina olla salattuja (https) eli ei http!
   - Älä koskaan syötä mitään salasanaa, jos sivusto ei ole salattu eli https.
6. Uhataanko viestissä jollakin kovalla toimella (tunnuksen sulkeminen, postin katkaisu)?
   - Uhkailu on aina vaaran merkki! Anna tunnuksen mieluummin sulkeutua kuin lankeat kiireessä urkintaan.
7. Kiirehditäänkö vastaanottajaa tiukalla aikarajalla (12/24/36/48h)?
   - Jos tunnuksellasi on ongelmia, ei sen kanssa odoteta edes 12 tuntia. Aalto sulkee tunnukset heti ja soittaa perään. Kiire on aina vaaran merkki!
8. Onko viestissä liitetiedostoja ja kuuluisiko siinä olla moisia?
   - Liitteissä välitetään paljon haittaohjelmia ja niillä kierretään roskapostin suodatusta. Mieti ja varmista mikä liite on ennen kuin avaat sen.
9. Ovatko mahdolliset liitetiedostot pakattuja (zip, gz, cab) tai muuten tyypiltään outoja?
   - Pakkaamista käytetään haittaohjelmatorjunnan ja roskapostin suodatuksen kiertämiseen sekä käyttäjän harhauttamiseen. Tunnista aina liitteen tyyppi ennen avaamista!
10. Toimitetaanko viestissä linkki tiedostoon verkossa?
    - Tiedosto verkossa ei kulje sähköpostin suodatuksen ja analyysin läpi. Kysy aina, miksi sinulle toimitettava tiedosto on verkossa eikä suoraan postin liitteenä?

Epäselvissä tapauksissa on parasta kääntyä tietoturvan puoleen (security@aalto.fi) ja varmistaa asia. Lisäksi on hyvä muistaa Aallon toimintamalli: ”me emme varoita, me suljemme ja soitamme teille”.

Turvallista sähköpostiviestintää toivottaa: Aalto ITS / tietoturvaryhmä