Tietoturvaohje

Ohjeita tietoturvallisiin toimintatapoihin

Jokainen voi vaikuttaa omilla toimintatavoillaan oleellisesti siihen, miten tietoturva toteutuu. Vaikka verkko ja työasemat olisi suojattu virustorjuntaohjelmistoilla ja sovelluspalomuureilla, väärät toimintatavat voivat heikentää tietoturvaa oleellisesti.

Yleiset toimintatavat

- ✓ Jos mahdollista, työskentele niin, että salassa pidettävät tiedot eivät näy sivullisille. On hyvä, jos sinulla on näköyhteys ovelle tai huoneen kulkuaukolle.
- ✓ Älä pidä salasanoja ja tunnuslukuja paperille tulostettuna tai kirjoitettuna työpisteesi läheisyydessä.

- ✓ Jos tulostat järjestelmistä henkilötietolomakkeita, hävitä tulostetut tiedot käytön jälkeen viemällä ne lukittuun tietosuoja-astiaan. Älä säilytä henkilötietoja työpisteelläsi siten, että tiedot eivät säily salattuna. Siirrä paperiset listat lukittuun kaappiin tai muuhun suojattuun paikkaan.

- ✓ Lukitse työasemasi aina, kun poistut sen luota. Pikakomento työaseman lukitsemiselle on Windows-painike + L.

- ✓ Kun työstät Office-dokumentteja, tee säännöllisin väliajoin välitallennuksia. Vaikka ohjelmistot tekevät nykyään automaattisia välitallennuksia, niihin ei pidä luottaa sokeasti. Välitallennuksia kannattaa tehdä säännöllisesti itse.

Salasanat ja käyttäjätunnukset

- ✓ Valitse mahdollisimman pitkä, mutta vähintään 14 merkkiä sisältävä salasana. Käytä erikoismerkkejä tai numeroita sekä pieniä ja isoja kirjaimia.

- ✓ **Muodosta salasanasi lauseista tai niiden lyhenteistä, jolloin ne on helpompi muistaa ja salasanasta tulee riittävän pitkä.**

- ✓ Älä käytä samaa salasanaa useissa eri palveluissa ja järjestelmissä. Jos salasana saadaan selville yhdessä palvelussa, vaarantuu myös muiden palveluiden tietoturvan.

- ✓ Vaihda salasanasi säännöllisesti myös muihin järjestelmiin, kuin tietokoneellesi. Muuta koko salasanan rakenne, äläkä käytä juoksevaa numerointia salasanan perässä.

- ✓ Älä säilytä listaa käyttäjätunnuksista ja salasanoista työasemasi lähettyvillä. Tallenna salasanat esim. salasanan hallintasovellukseen.

Sähköpostin tietoturvallinen käyttö

- ✓ **Käytä työsähköpostiasi vain työasioihin. Älä anna työsähköpostin osoitetta esimerkiksi verkko-ostoksia tehdessäsi.**

- ✓ Älä kirjoita sähköpostiosoitettasi kokonaisuudessaan julkisille Internet-sivuille. Jos kirjoitat osoitteen, korvaa @-merkki esimerkiksi seuraavasti: (at). Internet-sivustoja skannataan sähköpostiosoitteiden löytämiseksi ja oikeinkirjoitettuna sähköposti voi päätyä roskapostittajien listoille.

- ✓ Älä avaa tuntemattomilta lähettäjiltä saapuneita liitetiedostoja, sillä ne voivat sisältää haitallisia ohjelmia. Jos viestin lähettäjä on tuntematon ja viesti otsikon perusteella epäilyttävä, on syytä harkita, kannattaako viestiä avata ollenkaan. Jos viesti on selkeästi mainos, tai roskaposti, poista viesti heti ja estä lähettäjä.

- ✓ Jos saat epäilyttävän, tai selkeän roskapostiviestin, älä missään tapauksessa vastaa viestiin. Jos vastaat, roskapostittaja saa vahvistuksen sähköpostilaatikon aktiivisuudesta ja ohjaa sinne roskapostiliikennettä entistä enemmän.

- ✓ Älä käsittele sähköpostissa henkilötietoja, käyttäjätunnuksia tai salasanoja. Jos kuitenkin lähetät henkilötietoja sähköpostitse, lähetä viesti salattuna. Viestinnässä OAJ:n suuntaan käytä yhteydenottolomakkeita aina, kun se on mahdollista.

- ✓ Älä avaa tuntemattomilta lähettäjiltä saapuneita linkkejä. Vaikka linkki näyttäisi vievän turvalliselle sivustolle, se voi todellisuudessa ohjata huijaussivustolle. Hyperlinkin tekstissä voi lukea mitä tahansa, mutta sen sisältämän kohdeosoitteen saa näkyviin viemällä hiiren linkin päälle.

Mobiililaitteiden tietoturva

- ✓ Suojaa puhelimesi ja tablettisi asettamalla näytön suojakoodi. Näytön suojakoodin ansiosta varastetun laitteen tietoihin on käytännössä mahdotonta päästä käsiksi.

- ✓ Vaihda myös SIM-kortin oletus PIN-koodi. Jos laite varastetaan ja SIM-kortin PIN-koodi on esim. 1234 tai 0000, varas voi käyttää liittymää, kunnes se saadaan suljetuksi.

- ✓ **Varmuuskopioi puhelimesi ja tablettisi säännöllisesti!** Varmuuskopiointi on ainoa tapa taata henkilökohtaisten ja arvokkaiden tietojesi, kuten valokuviesi säilyminen, jos laite hajoaa tai se varastetaan.

- ✓ Asenna laitteen tarjoamat ohjelmistopäivitykset. Ohjelmistopäivitykset korjaavat käyttöjärjestelmän virheitä ja paikkaavat tietoturva-aukkoja, joten ne ovat oleellinen osa mobiililaitteen tietoturvaa. **Huom! Muista ottaa varmuuskopio ennen ohjelmistopäivityksen asentamista!** Jos ohjelmistopäivitys epäonnistuu, voidaan laite joutua palauttamaan tehdasasetuksiin, jolloin kaikki sen sisältämät tiedot katoavat, jos niitä ei ole varmuuskopioitu.

- ✓ Älä vastaa outoihin tekstiviesteihin tai tarjouksiin, sillä niihin vastaaminen saattaa aiheuttaa kalliin laskun.

- ✓ Mieti tarkkaan, mitä sovelluksia puhelimessasi tarvitset ja lataa vain sellaisia sovelluksia, jotka ovat yleisesti turvallisiksi tunnettuja. Kaikki verkkokaupasta saatavat sovellukset eivät välttämättä ole turvallisia. Turhat sovellukset myös hidastavat laitettasi ja taustalla pyöriessään vievät paljon virtaa akusta.

Turvallinen verkkoselaaminen

- ✓ Harkitse tarkoin, mitä Internet-linkkejä avaat. Älä lataa linkeistä löytyviä tiedostoja, joiden sisällöstä et ole varma. Jos et ole varma ladatun tiedoston turvallisuudesta, älä avaa/suorita sitä.

- ✓ Älä tallenna eri järjestelmien/verkkopalveluiden salasanoja selaimen muistiin. Kun salasanat on tallennettu selaimeen, kenellä tahansa tietokoneelle pääsevällä on suora pääsy käyttämiisi palveluihin. Jos selain tarjoaa salasanan tallennusta, vastaa ilmoitukseen "Ei koskaan tälle sivustolle".

- ✓ Älä jaa henkilötietojasi tai käyttäjätunnuksia/salasanoja Internetissä, äläkä anna tunnuksiasi, vaikka pyytäjä esittäytyisi järjestelmänvalvojana. Mikään oikea palveluntarjoaja ei pyydä sinulta tunnuksia ja salasanoja.

- ✓ Jos käytät verkkopankkia tai vierailet muissa kirjautumista vaativissa palveluissa, tarkista, että selainyhteys on suojattu. Suojatun selainyhteyden tunnistat lukon kuvasta osoiterivillä ja osoitteen HTTPS-alusta.

- ✓ Älä avaa selaimeen ilmestyviä pop-uppeja (ponnahdusikkunoita). Epäilyttävät ponnahdusikkunat ilmoittavat esimerkiksi, että olet voittanut palkinnon tai että tietokoneesi on vaarassa. Näin houkutellaan käyttäjää vierailemaan haitallisilla sivustoilla.

- ✓ Mieti tarkkaan, mitä tietoja annat itsestäsi Internetissä. Älä jaa liian henkilökohtaisia tietoja itsestäsi, jotta et joudu identiteettivarkauden kohteeksi. Verkkorikollisuuden yleistymisen vuoksi identiteettivarkaudet ovat nykyään arkipäivää. Identiteettivarkaudella tarkoitetaan tilannetta, jossa varas käyttää

toisen henkilön nimeä tai henkilötunnusta hyväksi tavoitteenaan yleensä rahallinen hyöty.

Tietoaineiston turvallisuus ja varmuuskopiointi

- ✓ Säilytä henkilökohtaisia työdokumenttejasi omalla varmennetulla asemallasi. Älä säilytä näitä tiedostoja tietokoneesi työpöydällä tai C-asemalla. Jos tietokoneen kovalevy hajoaa, kaikki C-asemalla tai esim. työpöydällä olevat tiedostot menetetään.

- ✓ Älä säilytä tiedostoja ainoastaan muistitikulla. Kopioi tiedostot muistitikun lisäksi myös omalle varmennetulle levyasemallesi siltä varalta, että muistitikku häviää tai rikkoutuu.

- ✓ Älä säilytä muistitikulla luottamuksellista aineistoa. Jos muistitikku häviää, sillä olevaa aineistoa pääsee käyttämään kuka tahansa, myös väärin.

- ✓ Jos siirrät muistitikulta dokumentteja vieraalle tietokoneelle esim. koulutusta varten, poista dokumentit tallentamastasi tiedostosijainnista ja tyhjennä myös roskakori. Pelkkä tiedostojen poistaminen ei estä muita käyttäjiä selaamasta tallentamiasi tiedostoja. Siksi myös roskakori pitää tyhjentää.

- ✓ Jos havaitset, että tietokoneeseesi on liitetty tuntematon muistitikku, irrota se heti. Pienille huomaamattomille muistitikuille asennetaan ns. key loggereita, joiden tarkoituksena on tallentaa kaikki käyttäjän tekemät näppäimistön painallukset ja näin tallentaa mm. salasanoja ja pankkitunnuksia. Älä myöskään käytä tuntematonta, pöydältä löytynyttä muistitikkua.

- ✓ Voit suojata yhteisissä hakemistoissa säilyttämäsi Office-asiakirjan salasanalla, jos haluat, etteivät muut pääse muokkaamaan asiakirjaa. Jos asiakirjasi sisältää henkilötietoja tai henkilökohtaista ja arkaluontoista materiaalia, voit suojata koko tiedoston salasanalla niin, etteivät muut voi avata ja tarkastella asiakirjaa.