Ohjeita ja neuvoja

Näiden ohjeiden ja neuvojen avulla osaat toimia turvallisesti verkossa. Tämä osio on laadittu yhteistyössä Yhdistyneessä kuningaskunnassa toimivan Get Safe Online -hankkeen ja Yhdysvaltojen turvallisuusministeriön (Department of Homeland Security) kanssa.

- Suojaa tietokoneesi ja kannettavat laitteesi
- Suojaa henkilötietosi ja henkilöllisyytesi
- Suojaa yritystiedot organisaation ulkopuolella
- Toimi verkossa huolellisesti
- Ole verkkoviisas

Suojaa tietokoneesi ja kannettavat laitteesi

Tietokone

- Käytä palomuuria. Palomuurit suojaavat verkkoasi joiltakin viruksilta ja hakkereilta.
- Asenna virustentorjuntaohjelma. Virustentorjuntaohjelma estää viruksia leviämästä tietokoneellesi.
- Hanki uusimmat turvallisuuspäivitykset. Pidä sovellukset ja käyttöjärjestelmä kunnossa, puhtaina viruksista ja haittaohjelmista ja päivitettyinä.
- Estä vakoiluohjelmat. Älä päästä tuntemattomia koneellesi välttämällä epäilyttäviä sähköposteja ja liitetiedostoja.
- Ota säännöllisesti varmuuskopioita: suojaa tietosi tuhoutumiselta.

Kannettavat tietokoneet

- Katkaise langattomat yhteydet, kun niitä ei käytetä tai tarvita.
- Yhdistä kannettava tietokoneesi säännöllisin väliajoin luotettavaan verkkoon päivittääksesi turvajärjestelmät.
- Ota kannettavaan tietokoneeseen tallennetuista tiedostoista varmuuskopiot.
- Älä jätä kannettavaa tietokonettasi vartioimatta.

USB-muistit

- Käytä salattuja USB-muisteja.
- Aseta USB-muisti lukutilaan katkaisimesta välttääksesi virusten leviämisen. Joissakin USB-muisteissa on katkaisin, josta muisti saadaan lukutilaan, jossa tietokonetta estetään tallentamasta tiedostoja tai muuttamasta muistissa olevia tiedostoja.
- Skannaa USB-muisti kopioituasi tiedostoja epäluotettavalta tai ei-hyväksytyltä koneelta virusten leviämisen välttämiseksi.

- Poista USB-muistista kaikki tiedostot, joita ei sillä hetkellä tarvita, ennen kuin kiinnität muistin jonkun toisen tietokoneeseen.
- Ota USB-muistiin tallennetuista tiedoista varmuuskopiot tietojen palauttamiseksi siltä varalta, että muistissa olevat tiedot sattuvat tuhoutumaan.
- Kiinnitä USB-muistit avaimenperään tai nauhaan, jottei se katoa. USB-muisti katoaa helposti ja se on helppo varastaa pienen kokonsa vuoksi. Lisäksi koska sen tallennuskapasiteetti on suuri, suurempi tietomäärä on vaarassa joutua väärin käsiin. USB-muisteja säilytetään yleensä laukuissa, repuissa, tietokonelaukuissa tai takkien ja housujen taskuissa. Ne jäävät myös usein lojumaan työpisteisiin. Viime aikoina yhä useampia USB-muisteja on kadonnut, joutunut väärään paikkaan, lainattu ilman lupaa tai varastettu.

Matkapuhelimet ja kämmentietokoneet

Kämmentietokoneissa, kuten Windows Mobile -, Palm-, iPhone-, Android- ja Blackberry-laitteissa, on internetyhteys ja suurten tietomäärien tallennuskapasiteetti. Niiden kannettavuus tarkoittaa, että niitä on käsiteltävä erityisen huolellisesti.

- Katkaise langattomat yhteydet (eli Bluetooth ja WLAN), kun niitä ei käytetä. Bluetooth-tekniikan avulla elektroniset laitteet voivat olla yhteydessä keskenään käyttämällä lyhyen kantaman radioyhteyttä.
- Älä jätä matkapuhelintasi tai kämmentietokonettasi vartioimatta. Muutoin on vaara, että tietoja häviää.
- Käytä salasanatoimintoa estääksesi älypuhelimeesi murtautumisen etäältä.

Suojaa henkilötietosi ja henkilöllisyytesi

- **Käytä tehokasta salasanaa.** Salasanasi vastaa internetissä kotisi lukkoa ja avainta. Salasanat ovat tärkein puolustautumiskeino, ja hyvien salasanakäytäntöjen kehittäminen auttaa pitämään tärkeät henkilötietosi ja henkilöllisyytesi paremmin suojattuina. Tietokoneesi salasana on avain kaikkeen tietokoneellesi ja verkkotileillesi tallentamaasi tietoon – sekä yritystä koskevaan että yksityiseen. Suojaa tietosi tehokkaalla salasanalla: käytä monimuotoista merkkijoukkoa, yhdistele (isoja ja pieniä) kirjaimia, numeroita ja muita merkkejä. Mitä enemmän salasanasi merkit vaihtelevat, sitä vaikeampi salasanaa on arvata. Älä käytä salasanana henkilökohtaisia tietoja – omaa nimeäsi tai lastesi nimeä, syntymäpäiviä tms. – jotka joku saattaisi tietää tai saada helposti tietoonsa. Vältä myös yleisiä sanoja, sillä osa hakkereista käyttää ohjelmia, jotka kokeilevat jokaista sanakirjassa olevaa sanaa.
- **Vaihda salasanaasi säännöllisesti.** Jos epäilet, että järjestelmään on murtauduttu, vaihda salasanasi välittömästi.
- **Pidä salasanasi salassa.** Salasanasi on ainutlaatuinen, eikä sitä pidä kertoa kenellekään. Luota salasanan suhteen muistiisi aina kun mahdollista. Kehitä itsellesi strategia salasanojen muistamiseksi. Jos kirjoitat salasanasi ylös, talleta se huolellisesti. Älä jätä

salasanamerkintöjäsi sellaiseen paikkaan, johon et jättäisi salasanojesi suojaamia tietojakaan.

- **Jokaiselle tilille oma salasana.** Käytä eri salasanaa jokaisella verkkotililläsi (tai ainakin muutamia eri salasanoja). Jos käytät samaa salasanaa monilla tileillä, yhdelle tilille murtautuva pääsee kaikille muillekin tileillesi.
- **Suojaa tilisi.** Monet tilien ylläpitäjät käyttävät lisäkeinoja varmistaakseen, kuka olet, ennen kuin pystyt hoitamaan asioita kyseisellä sivustolla.
- **Päätä omasta verkko-osallistumisestasi.** Jos mahdollista, aseta verkkosivuston yksityisyyttä ja tietosuojaa koskevat asetukset haluamallesi tietojenjaon tasolle. On suositeltavaa rajoittaa henkilöitä, joiden kanssa jaat tietojasi.
- **Käytä yhteisöpalvelusivuja varovaisesti.** Tiedosta, että yhteisöpalvelusivuilla voivat yhdistyä monet internetiin liittyvät riskit: verkkokiusaaminen, yksityisten tietojen paljastuminen, verkkoahdistelu, ikään sopimattomaan sisältöön pääsy ja ääritapauksissa verkkohoukuttelu ja lasten hyväksikäyttö.

Suojaa yritystiedot organisaation ulkopuolella

- **Varmista, että arkaluonteiset tiedot ovat suojassa.** Kun olet organisaation ulkopuolella, varmista, että pidät arkaluonteiset tiedot ja välineet suojassa koko ajan varkauden tai katoamisen estämiseksi. Käsittele tietoja erityisen huolellisesti julkisilla paikoilla.
- **Pidä yritystiedot salassa.** Muista, että joku saattaa kuulla keskustelusi. Älä anna organisaation luottamuksellisia tietoja kaikkien saataville.
- **Varo olan yli kurkkimista.** Huolehdi matkustaessasi tai etätyötä tehdessäsi, ettei kukaan pääse kurkkimaan olkasi yli.
- **Käytä selainsähköpostia viisaasti.** Sähköpostin lukemisessa verkkoselaimen kautta on noudatettava samaa varovaisuutta kuin sähköpostiohjelmissa, ja lisäksi siihen liittyy muutamia muitakin turvallisuusriskejä.

Toimi verkossa huolellisesti

- **Katkaise langattomat yhteydet, kun niitä ei käytetä tai tarvita.**
- **Käytä maalaisjärkeä Wi-Fi-verkoissa.** Käyttäessäsi Wi-Fi-verkkoa rajaa hoidettavien asioiden tyyppiä ja aseta laitteesi suojausasetukset rajoittamaan pääsyä koneellesi.
- **Suojaa rahasi.** Hoitaessasi pankkiasioita tai tehdessäsi ostoksia verkossa tarkista, että sivustot ovat suojattuja. Katso, alkaako sivuston osoite kirjainyhdistelmillä ”https://” tai ”shttp://”. Ne tarkoittavat, että tietojasi suojataan sivustolla ylimääräisin keinoin. ”Http://”-alkuiset sivustot eivät ole suojattuja.
- **Poista oudot sähköpostit.** Roskaposti on turvallisuusuhka. Älä avaa tuntemattomia sähköposteja tai liitetiedostoja.
- **Kun epäilyttää, älä epäröi poistaa.** Kun sähköposteissa, twiiteissä, viesteissä ja verkkomainoksissa olevat linkit vaikuttavat epäilyttäviltä, vaikka tuntisit lähteen, on parasta poistaa viesti tai tarvittaessa merkitä se roskapostiksi.

- **Välitä sähköpostiviesti eteenpäin vain, jos se on asianmukaista.** Harkitse ensin, pitäisikö aiempien vastaanottajien ketju poistaa.
- **Surffaa netissä varoen.**
- **Älä lataa asiakirjoja ja materiaalia epäluotettavilta tahoilta.**
- **Käytä yleisiä tietokoneita varoen.** Ota yhteys yleisellä tietokoneella vain, jos yhteytesi on suojattu (ilmoitetaan riippulukolla selaimen oikeanpuoleisessa alareunassa ja kirjaimilla ”https://” verkkosivuston osoitteen alussa).
- **Käytä tunnettujen ja luotettavien yhtiöiden selainsähköposteja.**

Ole verkkoviisas

- **Pysy ajan tasalla.** Pidä itsesi ajan tasalla uusista tavoista suojautua internetissä. Tarkista luotettavilta sivustoilta uusimmat tiedot ja jaa ne perheen, ystävien ja kollegojen kesken. Kannusta heitä olemaan verkkoviisaita. Tee selaimestasi turvallinen.
- **Älä toimi suin päin.** Ole varovainen sellaisten viestien kanssa, joissa sinua pyydetään toimimaan välittömästi; joissa sinulle tarjotaan jotain, joka on liian hyvää ollakseen totta, tai joissa pyydetään henkilötietoja.
- **Varmuuskopioi.** Suojaa työsi, musiikkisi, valokuvasi ja muut digitaaliset tietosi tekemällä sähköiset kopiot ja tallettamalla ne turvallisesti.