MOBIILITURVAOHJE HENKILÖSTÖLLE JA OPISKELIJOILLE

Mobiililaitteet (älypuhelimet ja taulutietokoneet eli tabletit) ovat helposti varastettavia ja hukattavia laitteita. Tällöin on vaarana, että luvaton käyttäjä pääsee käsiksi henkilökohtaisiin tai yliopiston tietoihin. Hän voi myös esiintyä laitteen omistajana lähettämällä sähköposteja nimissäsi. On siis tärkeää, että tiedät laitteisiin liittyvät riskit ja toimit ohjeiden mukaisesti.

LAITTEEN KÄYTTÖÖNOTTO

- Hanki ensisijaisesti sellainen mobiililaite, jota yliopistosi suosittelee.
- Kirjoita muistiin laitteesi sarjanumero, puhelimen IMEI-koodi ja liittymän tunnustiedot. Laita tiedot sellaiseen paikkaan, että löydät ne tarvittaessa helposti.
- Merkitse laitteesi esimerkiksi tarralla ja nimikirjaimilla, jotta pystyt erottamaan sen muista vastaavista laitteista esimerkiksi kokouksissa tai lentokentän turvatarkastuksessa.
- Laite on ehdottomasti suojattava salasanalla tai suojakoodilla. Älä käytä syntymäaikoja tai helposti arvattavia sanoja tai numerosarjoja.
- Muista laitteen suojakoodi. Jos unohdat asettamasi suojakoodin, menetät laitteessa olevat tiedot, koska tällöin laitteen saa käyttöön ainoastaan palauttamalla se alkuperäisasetuksiin.
- Selvitä, voiko mobiililaitteesi tarvittaessa etätyhjentää ja kuinka se tapahtuu.
- Selvitä, mitä yliopiston palveluja voit laitteellasi käyttää ja on luvallista käyttää.
- Harkitse haittaohjelmatorjunnan ja palomuurin hankkimista: tarjolla on monia hyviä ilmaisiakin ohjelmia.

LAITTEEN TURVALLINEN KÄYTTÖ

- Älä lainaa mobiililaitettasi muille.
- Lukitse laitteesi silloin kun se ei ole käytössä. Monissa laitteissa on mahdollista käyttää automaatti-lukitusta, joka lukitsee laitteen kun sitä ei ole käytetty vähään aikaan.
- Laitetta avatessasi varmista, että muut eivät pysty näkemään kirjoittamaasi suojakoodia tai salasanaa. Vaihda koodi, jos epäilet sen tulleen ulkopuolisten tietoon.
- Joihinkin taulutietokoneisiin on saatavissa ns. tietoturvakalvo, joka estää laitteen näytön näkyvyyden sivuille.
- Älä avaa tuntemattomalta lähettäjältä tulleita tai muuten epäilyttäviä teksti- ja multimediaviestejä. Ne voivat sisältää haittaohjelmia, jotka lähettävät viestejä nimissäsi tai aiheuttavat muuten lisäkustannuksia.
- Älä asenna yhtään ohjelmaa, jota et oikeasti tarvitse. Lataa ja asenna ohjelmistoja vain virallisista kauppapaikoista.
- Huolehdi laitteen ohjelmistojen säännöllisestä päivittämisestä tietoturvallisuuden varmistamiseksi.
- Huolehdi mobiililaitteessa olevien tietojen varmuuskopioinnista (tai synkronoinnista).
- Käytä synkronoinnissa ensisijaisesti yliopiston hyväksymiä palveluita esimerkiksi kalenterin ja osoitekirjan synkronointiin.
- Harkitse, mitä laitteessasi olevia tietoja voit synkronoida ulkoiseen verkkopalveluun.
- Harkitse, onko tarpeen julkaista laitteesi sijaintitietoja verkkopalveluissa.
- Sulje langattomat yhteydet (Bluetooth ja WLAN), aina kun et tarvitse niitä.
- Ulkomailla ollessasi vältä www-selailua ja sähköpostin automaattista synkronointia korkeiden dataliikennekustannusten vuoksi.

3.12.2013

LAITTEEN KADOTESSA

- Etätyhjennä laitteessa olevat tiedot ja sulje matkapuhelinliittymä. Laitteen etätyhjennys ei onnistu, jos liittymä on suljettu. Liittymää ei siis kannata välttämättä sulkea heti, vaan vasta sitten kun etätyhjennys on suoritettu.
- Ota yhteys tietotekniikkatukeen ja ilmoita laitteen katoamisesta.
- Jos laite varastetaan, tee siitä ilmoitus poliisille.

MOBIILILAITTEEN POISTAMINEN KÄYTÖSTÄ

- Siirrä laitteessa olevat tiedot uuteen laitteeseesi tai ota tiedot muuten talteen.
- Tyhjennä laitteen muisti ennen laitteen poistoa.
- Mikäli laitteessa on erillinen muistikortti, joka ei jää käyttöösi, tyhjennä myös se.