



OPISKELIJAN TIETOTURVAOPAS

Kesäkuu 2009

SISÄLLYSLUETTELO

Tietoturvallisuuden ja tietosuojan merkitys opiskelijalle	1
Käyttöoikeudet ja salasanat	2
Verkko ja sähköposti	3
Yksityisyyden suojaaminen	5
Yliopiston tietokoneiden käyttö	6
Oman tietokoneen käyttö ja ylläpito	7
Julkisten tietokoneiden ja langattomien verkkojen käyttö	9
Kannettavat muistivälineet ja varmuuskopiot	10
Tekijänoikeudet ja ohjelmistolisenssit	11
Opinto-oikeuden päätyessä	12
Miten toimit, jos epäilet haittaohjelmatartuntaa tai tietoturvarikkomusta	13
Lisätietoja ja linkkejä	takakansi

Tämä tietoturvaohje on tuotettu yliopistojen tietoturva-asiantuntijoiden yhteistyönä ja se on tarkoitettu ensisijaisesti yliopisto-opiskelijoiden käyttöön. Ohjeesta on pyritty tekemään kaikkien yliopistojen käyttöön sopiva.

Työryhmä: Kenneth Kahri (Helsingin yliopisto), Olavi Manninen (Kuopion yliopisto), Kaisu Rahko (Oulun yliopisto)

Taitto ja kuvat: Katja Koppinen ja Raija Törrönen (Kuopion yliopisto)

TIETOTURVALLISUUDEN JA TIETOSUOJAN MERKITYS OPISKELIJALLE

- Tietokoneet ja verkko ovat tärkeitä välineitä niin opiskelussa kuin vapaa-ajalla. Verkon käyttöön liittyy kuitenkin erilaisia vaaroja, ja vahinkojen ehkäisemiseksi sinun tulee tietää joitakin asioita tietoturvallisuudesta ja tietosuojasta.
- **Tietoturvallisuus** käsittää kaikki ne asiat, joilla pyritään siihen, että palvelut ja järjestelmät toimivat oikein, luotettavasti ja ovat turvallisia käyttää.
- **Tietosuoja** käsittää kaikki ne toimenpiteet, joilla pyritään suojelemaan ihmisten yksityisyyttä henkilötietojen käsitteilyssä.
- Yksityisyyden suojaamiseksi on oleellista huomioida tietosuoja käyttämissäsi palveluissa ja omassa toiminnassasi. Suojaa sekä omat tietosi että hallussasi olevat muiden henkilöiden tiedot. Kaikilla on joitakin ulkopuolisilta suojattavia tietoja, esimerkiksi henkilö- ja yhteystietoja, pankkiyhteystietoja, terveystietoja, sähköpostiviestejä tai kuvia.
- Tietoturvallisuutta pidetään usein vaikeana asiana, mutta käyttämällä tervettä järkeä ja noudattamalla ohjeita selvität suurimman osan tietoturvakysymyksistä.
- Jokaisella on velvollisuus huolehtia tietoturvallisuudesta. Yliopiston tietoturvapoliittikka määrittelee opiskelijalle muun muassa vastuun noudattaa annettuja ohjeita itsensä ja toisten suojelemiseksi. Tietoturvaloukkauksista voi olla seuraamuksia esimerkiksi viestinnästä annetun lainsäädännön perusteella.
- Jos toimit opiskelun ohessa luottamustehtävissä, sinulla on laajemmat vastuut kuin opiskelijalla. Perehdy näihin vastuisiin.

KÄYTTÖOIKEUDET JA SALASANAT

- Yliopiston tietojärjestelmien käyttöoikeus on henkilökohtainen ja se on tarkoitettu vain sinun käyttöösi.
- Yliopiston tietokoneisiin ja järjestelmiin kirjaudutaan yleensä käyttäjätunnuksella ja salasanalla. Käsittele käyttäjätunnustasi ja salasanaasi yhtä huolellisesti kuin pankkikorttiasi ja tunnuslukuasi.
- Joissakin yliopistoissa voidaan tunnistautumiseen tai kulunvalvontaan käyttää älykorttia (opiskelijakortti Lyyra), ja myös siitä tulee pitää hyvää huolta. Älä lainaa korttia toisille, sillä kortin omistaja vastaa sen kaikesta käytöstä.
- Olet vastuussa tunnuksesi käytöstä. Älä luovuta käyttäjätunnustasi, salasanaasi tai älykorttiasi kenellekään toiselle. Edes järjestelmän ylläpitäjien ei tule tietää salasanaasi. Jos joku tiedustelee tunnuksesi ja salasanaasi, hän on poikkeuksetta väärällä asialla.
- Yliopiston sinulle tarjoamat sähköposti- ja muut palvelut on tarkoitettu ensisijaisesti opiskelukäyttöön. Voit käyttää palveluja kohtuullisessa määrin myös yksityistarkoituksiin, jos se ei haittaa palvelujen ensisijaista käyttötarkoitusta.
- Yliopiston järjestelmien kaupallinen käyttö on yleisesti ottaen kielletty. Myös käyttö yliopiston ulkopuoliseen poliittiseen toimintaan, kuten vaalimainontaan, on kielletty.
- Hyvä salasana on sellainen, jonka muistat itse helposti, mutta jota ulkopuoliset eivät pysty arvaamaan. Vältä salasanan kirjoittamista muistiin.
- Älä käytä salasanoina jokapäiväisiä tai sinuun liittyviä sanoja. Valitse salasana, jossa on pieniä ja isoja kirjaimia,

numeroita ja jopa erikoismerkkejä. Erikoismerkit eivät kuitenkaan käy kaikkiin järjestelmiin, tarkista tämä yliopistosi ohjeista.

- Jos olet saanut uuden salasanan yliopistosi tietotekniikkapalveluista, vaihda se heti sellaiseksi, jonka vain sinä tiedät.
- Vaihda salasanat riittävän usein yliopistosi ohjeistuksen mukaisesti ja heti, jos epäilet niiden joutuneen jonkun muun käsiin. Älä käytä missään yliopiston ulkopuolisessa palvelussa samaa salasanaa kuin yliopiston palveluissa.

VERKKO JA SÄHKÖPOSTI

- Internet-verkossa tiedot liikkuvat usein salaamattomina ilman mitään suojausta. Ole siis huolellinen sähköpostin ja verkon käytössä.
- Jokainen opiskelija saa yliopiston käyttäjätunnuksen ja sähköpostiosoitteen. Yliopiston antamaa osoitetta tuleekin käyttää ensisijaisena sähköpostiosoitteena yliopiston palveluissa ja järjestelmissä, muun muassa opintorekisterissä ja oppimisympäristöissä (Oodi, Optima, Moodle, Blackboard jne.).
- Sähköposti- ja muussa viestinnässä kannattaa perehtyä ns. netikettiin ja noudattaa sitä. Liian kärkevä kirjoittaminen esimerkiksi keskusteluryhmässä on epäkohteliasta, ja loukkaavan nettikirjoittelun perusteella on annettu oikeustuomioitakin.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia. Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä. Tarvittaessa voit kysyä lisäohjeita tietotekniikkaneuvonnasta.

-
- Ilman vastaanottajan lupaa lähetetyt mainokset ja ketjukirjeet ovat roskapostia. Älä vastaa niihin tai välitä niitä eteenpäin, vaan tuhoa ne heti. Roskapostiviestit saattavat sisältää haittaohjelmia tai ohjata käyttäjän haittaohjelmia sisältäville sivuille.
 - Yliopistot käyttävät roskapostisuodatuksessa erilaisia menetelmiä. Joissakin järjestelmissä roskapostisuodatus on automaattisesti päällä, joissakin järjestelmissä käyttäjän pitää itse laittaa torjunta päälle. Pehdy oman yliopistosi käytäntöihin.
 - Ole terveen epäluuloinen sähköpostiviestin luotettavuudesta. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Myös virukset voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä.
 - Varo erityisesti ns. kalasteluviestejä, joissa sinua pyydetään luovuttamaan tunnuksesi ja salasanasi tai pankkipalvelun tunnuksesi eteenpäin jollakin asiallisen tuntuisella perusteella.
 - Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ilmoita lähettäjälle väärästä osoitteesta. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
 - Viestejä lähettäessäsi varmista, että tiedät viestin vastaanottajien oikeat sähköpostiosoitteet ja tarkista osoitteet kirjoitusvirheiden varalta ennen viestin lähettämistä.
 - Harkitse, kenelle luovutat sähköpostiosoitteesi tai missä julkaiset sen. Hanki itsellesi ilmaissähköpostiosoite (esim. Hotmail, Gmail) ja vältä yliopiston sähköpostiosoitteen käyttämistä nettifoorumeilla ja yhteisöpalveluissa (esim. Facebook, MySpace).
 - Käytä vain tunnettuja ja asialliseksi tiedettyjä verkkopalveluita.

-
- Jos käytät yliopiston ulkopuolisen tarjoajan sähköpostipalvelua, valitse sellainen palvelu, joka salaa tietoliikenteen (selainkäyttöisessä palvelussa osoitteen alussa on <https://> ja selaimen alakulmassa näkyy suljetun lukon kuva).
 - Älä koskaan käytä verkkopalveluja tunnuksella, jolla on ylläpito-oikeudet (Administrator, root).

YKSITYISYYDEN SUOJAAMINEN

- Käytä harkintaa henkilötietojen käsittelyssä: harkitse, mitä tietoja voit luovuttaa ja kenelle.
- Omien tietojesi luovutukseen sinulla on harkintavalta. Toisen henkilön tietojen luovutukseen pitää olla tämän lupa tai muu oikeutus.
- Harkitse myös, mitä omia tai muiden tietoja laitat verkko-yhteisöihin (kuten Facebook, MySpace) tai muihin web-palveluihin. Kerran verkkoon laitettua henkilökohtaista tietoa kuten valokuvaa tai kotiosoitetta voi olla mahdoton myöhemmin saada kokonaan poistettua.
- Verkko-yhteisöissä on helppo tekeytyä toiseksi tai toisenlaiseksi henkilöksi. Älä suhtaudu liian sinisilmäisesti kaikkeen lukemaasi.
- Jos käytät matkapuhelinta julkisilla paikoilla, joku voi kuulla puheesi ja lisäksi tunnistaa sinut. Älä siis keskustele kovaan ääneen.



YLIOPISTON TIETOKONEIDEN KÄYTTÖ

- Pyri suojaamaan tietokoneen näppäimistö ja näyttö muiden katseilta kirjautuessasi koneelle ja aina, kun käsittelet suojattavaa aineistoa.
- Kirjautu koneelle aina omilla tunnuksillasi. Käytön päätyttyä kirjautu ulos ja siivoa jälkesi:
 - Tyhjennä selaimen tallentamat väliaikaistiedostot ja muut tiedot.
 - Hävitä muut koneelle mahdollisesti tallentamasi väliaikaistiedostot.
 - Ota muistitikkuasi ja paperit mukaasi.
- Jos poistut väliaikaisesti koneelta, ota muistitikkuasi ja muut aineistosi mukaan ja lukitse kone, jottei kukaan pääse käyttämään tunnuksiasi tai näkemään tiedostoja. Huomioi kuitenkin, että koneen lukitseminen pidemmäksi aikaa saattaa olla kiellettyä, koska tällöin kone jää varatuksi.



Windows -tietokoneen lukitseminen (Win+L).

- Tallenna kaikki tärkeät aineistosi verkkolevyillesi tai palvelimelle kotihakemistoosi käyttäessäsi yliopiston verkossa olevaa konetta. Tällöin yliopisto huolehtii aineistosi varmuuskopioinnista.

-
- Tallenna muutokset tasaisin väliajoin (monissa Windows-ohjelmissa Ctrl-S), jos muokkaat tekstiä tai muuta aineistoa pidemmän aikaa. Tällöin et menetä kaikkea tekemääsi työtä teknisen häiriön sattuessa.
 - Ennen kuin tulostat yhteiskäytössä olevalle kirjoittimelle, varmista sen sijainti. Nouda oma tulosteesi kirjoittimelta mahdollisimman pian. Lukitse koneesi tulosteen noutamisen ajaksi.
 - Yliopiston koneet on tarkoitettu ensisijaisesti opiskeluun ja työntekoon. Älä varaa yliopiston koneita pitkäksi aikaa yksityiskäyttöön, jos muut käyttäjät jonottavat koneille.
 - Ohjelmistojen asennus yliopiston koneisiin on yleensä kielletty ja usein myös teknisesti estetty. Jos tarvitset jotakin tiettyä ohjelmistoa, ota yhteyttä tietotekniikkatukeen. Ohjelma voi jo olla toisen atk-tilan koneissa, tai se on mahdollista hankkia.
 - Jos olet saanut kulkukortillasi tai -avaimellasi käyttöoikeuden yliopiston lukittuina pidettäviin atk-luokkiin, sulje ovi jälkeesi äläkä päästä asiattomia käyttäjiä luokkaan.

OMAN TIETOKONEEN KÄYTTÖ JA YLLÄPITO

- Yliopisto vastaa omien tietokoneidensa tietoturvallisuudesta. Jos sinulla on oma kone, vastaat itse sen tietoturvallisuudesta. Pyri siis noudattamaan hyvää ylläpitotapaa.
- Hyvä ylläpitotapa edellyttää, että koneessa on ajantasaisena ylläpidetyt palomuur- ja virustorjuntaohjelmistot, automaattiset käyttöjärjestelmäpäivitykset (esim. Windows Update -toiminnolla) ja myös muiden ohjelmistojen tietoturvapäivityksistä huolehditaan.

-
- Käytä ylläpito-oikeuksin varustettua käyttäjätunnusta (esim. Administrator, root) vain ylläpitotehtäviin: ohjelmien asennukseen ja muiden käyttäjätunnusten hallintaan.
 - Tee normaalia käyttöä varten itsellesi ja kaikille muille koneen käyttäjille henkilökohtaiset tunnukset ilman ylläpito-oikeuksia. Tämä parantaa käyttäjien yksityisyyden suojaa ja vähentää haittaohjelmatartunnan mahdollisuutta.
 - Asenna koneellesi vain ne ohjelmat, joita välttämättä tarvitset. Jokainen turha ohjelmistoasennus lisää haittaohjelmatartunnan vaaraa. Asenna ohjelmia vain tunnetuista ohjelmistopankeista.
 - Huolehdi myös tiedostojen säännöllisestä varmuuskopiointista – mieti mitä tietoja menetät, jos koneesi kovalevy vikaantuu yllättäen tai haittaohjelma tuhoaa tiedostoja.
 - Kannettavan koneen kuljettaminen ja säilyttäminen edellyttää huolellisuutta. Kone tulee suojata iskuilta, pölyltä ja kosteudelta. Koneita ei kannata jättää autoon, tai ainakin se kannattaa pitää pois näkyviltä.
 - Jos sinulla on oma langaton verkko, ota sen suojausasetukset käyttöön, jotteivät muut pääse väärinkäyttämään verkko-yhteyttäsi tai seuraamaan, mitä teet verkossa. Ohjeet löydät langattoman verkon laitteittesi käyttöohjeista.
 - Jos sinulla on käytössä oma laajakaistaliittymä, selvitä päätelaitteen käyttöohjeista, sisältääkö se palomuuriminaisuuksia ja ota ne käyttöön.
 - Pyri säännöllisesti seuraamaan ohjelmistojen tietoturvaongelmista annettuja varoituksia (esim. www.cert.fi).

JULKISTEN TIETOKONEIDEN JA LANGATTOMIEN VERKKOJEN KÄYTTÖ

- Erilaiset nettikahvila-, kirjasto- ja yleisökoneet ovat matkoilla käteviä sähköpostin lukemiseen, tiedonhakuun ja sosiaalisten verkkopalvelujen käyttöön. Niiden turvallisuuteen ei kuitenkaan kannata luottaa, haittaohjelma voi hyvinkin vaania edellisten käyttäjien jäljiltä.
- Mieti etukäteen mitä aiot tehdä, onko sinun välttämätöntä kirjautua verkkopalveluihin omalla tunnuksellasi ja millaisia tietoja aiot käsitellä näillä koneilla.
- Tietokoneen ja ohjelmien käytöstä syntyy aina jälkiä; väli-aikaistiedostoja, evästeitä, selainistuntoja ja muita sinua ja tekemisiäsi koskevaa tietoa. Opettele etukäteen, kuinka tyhjennät selaimen välimuistin ja poistat muut tyyppillisimmät käytöstäsi jääneet jäljet yleisessä käytössä olevilta koneilta.
- Käyttäessäsi langattomia verkkoja kiinnitä huomiota siihen, onko verkkoyhteys suojattu vai ei. Yleisessä käytössä olevissa verkoissa, esimerkiksi kahviloissa ja lentoasemilla, yhteys on tavallisesti suojaamaton ja verkkoliikennettäsi voi seurata helposti. Tällaisissa verkoissa kannattaa käyttää vain sellaisia sähköposti- ja verkkopalveluja, jotka salaavat tietoliikenteen (osoitteessa on <https://> ja selaimen alakulmassa lukon kuva).

KANNETTAVAT MUISTIVÄLINEET JA VARMUUSKOPIOT

- Yliopisto huolehtii tiedostojesi varmuuskopioinnista, jos tallennat ne verkkolevyillesi tai palvelimelle kotihakemistoosi.
- USB-muistitikut ovat käteviä välineitä tietojen siirtoon ja varmuuskopiointiin – älä kuitenkaan käytä niitä tiedostojen ensisijaisena tai ainoana tallennuspaikkana. Muistitikku myös häviää helposti – älä tallenna tikuille arkaluonteista materiaalia.
- Suhtaudu varoen muiden käyttäjien USB-muistitikkuihin. Tikulla voi olla haittaohjelma, joka käynnistyy automaattisesti, kun tikku liitetään koneeseen, ja saastuttaa myös sinun koneesi.
- Jos löydät yliopistolta toisen käyttäjän muistitikun, toimita se yliopiston tietotekniikkaneuvontaan tutkimatta sen sisältöä.
- Jos sinulla on oma tietokone, ota sen tiedostoista säännöllisesti varmuuskopioita. Sopivia varmuuskopiointivälineitä ovat mm. ulkoiset USB-kiintolevyt, muistitikut sekä kirjoitettavat DVD- tai CD-levyt. Merkitse varmuuskopiot (mitä tietoja kopio sisältää, milloin otettu). Testaa varmuuskopioiden luettavuutta säännöllisesti.
- Säilytä varmuuskopiot erillään tietokoneesta ja mahdollisuuksien mukaan lukitussa paikassa.
- Opettele pitämään aineistosi hyvässä järjestyksessä sekä tietokoneella, muistivälineillä että paperimuodossa, jolloin on helpompi huolehtia niiden suojaamisesta.
- Käytöstä poistettuja kovalevyjä, muistitikkuja ja muita muistivälineitä sekä luottamuksellisia tietoja sisältäviä paperiaineistoja ei tule heittää roskiin. Aineistot pitää tuhota

asianmukaisesti: muistitikuilla, kovalevyllä ja muilla sähköisillä välineillä olevat tiedot tuhotaan päällekirjoittamalla tai murskaamalla väline, paperiaineistot silppuamalla.

TEKIJÄNOIKEUDET JA OHJELMISTOLISENSSIT

- Asenna tietokoneellesi vain sellaisia ohjelmistoja, joihin olet hankkinut käyttöoikeuden (lisenssin) tai jotka ovat maksuttomia ja ovat yleisessä jakelussa. Älä asenna laittomia kopioita tai ohjelmistoja, joiden käyttöoikeudesta et ole varma.
- Yliopistosi kautta saat joidenkin ohjelmistojen käyttöoikeuden, tarkempia tietoja tästä löydät oman yliopistosi antamista ohjeista.
- Muista kuitenkin, että yliopiston kautta saatujen ohjelmien käyttö on usein rajoitettu opiskelutarkoituksiin ja oikeutesi käyttää niitä lakkaa kun opinto-oikeutesi päättyy. Käyttöoikeuden päättyessä olet velvoitettu poistamaan ohjelmistot kaikilta niiltä koneilta, joille asensit niitä.
- Kirjastojen sähköisten aineistojen käyttöehdot rajoittavat sitä, kuka niitä saa käyttää ja mihin tarkoitukseen. Selvitä nämä käyttöehdot itsellesi tutustumalla kirjastojen ja aineistopalvelujen antamaan ohjeistukseen.
- Tekijänoikeus suojaa elokuvia ja musiikkiaineistoja. Älä kopioi niitä verkosta, äläkä myöskään jaa niitä verkkoon ilman oikeudenomistajan erillistä lupaa. Nykyinen tekijänoikeuslaki ei salli tietokoneohjelmistojen kopiointia omaan käyttöön ja rankaisee kaikesta luvattomasta levittämisestä.
- Lainaa tekstiä omiin harjoitustöihisi ja opinnäytteisiisi vain sitaattioikeuden antamassa laajuudessa. Jos lainaat tekstiä, kerro mitkä osat lainasit ja keneltä. Selvitä aina aineiston käyttöoikeus ennenkuin lainaat aineistoa tai linkität sen omaan aineistoosi.

OPINTO-OIKEUDEN PÄÄTTYESSÄ

- Oikeus käyttää yliopistosi tietotekniikkapalveluja on sidottu opinto-oikeuteesi.
- Kun valmistut tai opinto-oikeutesi päättyy, päättyy myös palvelujen käyttöoikeus, ja käyttäjätunnukseksi sulkeutuu yleensä automaattisesti. Tietyn ajan päästä käyttöoikeuden päättymisestä yliopisto poistaa käyttäjätunnukseksi, sähköpostikansiosi ja muut tiedostosi pysyvästi. Ennen käyttäjätunnukseksi sulkeutumista huolehdi seuraavista asioista:
 - Ilmoita yhteyskumppaneillesi sähköpostiosoitteen muuttumisesta.
 - Kopioi yliopiston palvelimilta itsellesi ne omat tiedostosi, jotka haluat säilyttää, ja poista muut.
 - Kopioi itsellesi omat sähköpostiviestisi tai lähetä ne eteenpäin toiseen sähköpostiosoitteeseesi.
 - Poista omalta koneeltasi ne yliopiston kautta saamasi ohjelmistot, joihin sinulla ei enää ole käyttöoikeutta.

MITEN TOIMIT, JOS EPÄILET HAITTAOHJELMA-TARTUNTAA TAI TIETOTURVARIKKOMUSTA

- Jos epäilet, että jollakin käyttämälläsi koneella on tai on ollut haittaohjelma, toimi seuraavasti:
 1. Vaihda heti toisella koneella kaikki ne salasanat, joita olet kyseisellä koneella käyttänyt tai jotka ovat samoja kuin kyseisellä koneella käyttämäsi. Jos olet käyttänyt koneelta verkkopankkiasi, ota yhteyttä pankkiisi ja kerro heille, että pankkitunnuksesi on mahdollisesti kaapattu.
 2. Jos kone on omasi, lakkaa välittömästi käyttämästä sitä ja selvitä kuinka pystyt pääsemään eroon haittaohjelmasta. Jos koneen omistaa joku muu, ota yhteyttä siitä vastaavaan henkilöön tai tahoon ja kerro haittaohjelmaepäilystäsi.
- Oman koneesi puhdistamiseen voit saada rajoitetusti apua yliopistosi tietotekniikkatueltä, aloita etsimällä heidän antamia ohjeita virustartuntojen käsittelystä. Virustorjuntaohjelmasi valmistajan kotisivut opastavat myös eteenpäin haittaohjelmien etsinnässä ja poistamisessa.
- Jos sinulla on syytä epäillä jonkinlaista tietoturvarikkomusta tai järjestelmän väärinkäyttöä, ota yhteyttä kyseisestä palvelusta tai järjestelmästä vastaavaan. Jos kyse on omasi yliopistostasi, ota yhteyttä tietotekniikkatukeen, muiden organisaatioiden kohdalla soita vaihteeseen ja pyydä ohjaamaan tietoturva-asioita käsittelevälle henkilölle. Kerro selkeästi mitä olet havainnut ja milloin havaitsemasi tapahtui. Jätä myös nimesi ja yhteystietosi, jotta sinulta voidaan pyytää tarvittaessa lisätietoja.

LISÄTIETOJA JA LINKKEJÄ

- Oman yliopistosi tietoturvasivusto
 - » Pehdy oman yliopistosi tietoturvaohjeisiin ja käytäntöihin
- Ohjeita turvalliseen nettikäyttöön
 - » www.tietoturvaopas.fi
 - » www.tietoturvakoulu.fi
- Ohjeita henkilötietojen käsittelystä ja yksityisyyden suojaamisesta
 - » www.tietosuoja.fi
- Netti-etiketti: hyvien tapojen noudattaminen verkkoviestinnässä
 - » fi.wikipedia.org/wiki/Netiketti
- Ohjeita viestinnän suojaamiseen, tiedotuksia tietoturvaauhkista
 - » www.cert.fi
- Matkapuhelinten käytön turvallisuusohjeita
 - » www.ficora.fi/mobiiliturva
- Valtion säädöstietopankki
 - » www.finlex.fi
- Helsingin yliopiston TVT-ajokortti-aineisto
 - » www.helsinki.fi/tvt-ajokortti/materiaali.htm