HENKILÖSTÖN TIETOTURVAOPAS

Lokakuu 2013

SISÄLLYSLUETTELO

Miksi tietoturvallisuus on tärkeää sinulle ja yliopistolle.....1
Käytä vahvoja salasanoja ja pidä ne salassa 2
Sähköpostin käyttö.....3
Varo kalasteluviestejä ja muita huijauksia.....4
Käytä internet-palveluja ja sosiaalista mediaa vastuullisesti.....5
Käytä työnantajasi tietokoneita vastuullisesti 7
Pidä kotikoneesi terveenä ja toimivana.....8
Pidä huolta muistitikuistasi.....8
Etäkäyttö – koneen käyttö työpaikan ulkopuolella
(kotona, matkoilla).....9
Varo avoimia langattomia verkkoja ja julkisia koneita.....10
Huolehdi myös mobiililaitteittesi turvallisuudesta.....10
Huomioi tekijänoikeudet ja ohjelmistolisenssit 11
Miten toimia työsuhteen päättyessä.....12
Epäiletkö haittaohjelmatartuntaa tai tietoturvarikkomusta? 13
Lisätietoja ja linkkejä.....14

Tämä tietoturvaopas on tarkoitettu ensisijaisesti yliopistojen henkilökunnan käyttöön. Opas on tuotettu yliopistojen tietoturva-asiantuntijoiden yhteistyönä ja siitä on pyritty tekemään kaikkien yliopistojen käyttöön sopiva.

Työryhmä: Olavi Manninen, Itä-Suomen yliopisto, Mari Karjalainen, Oulun yliopisto, Matti Levänen, Jyväskylän yliopisto, Ulf Pensar, Svenska Handelshögskolan, Jan Wennström, Åbo Akademi.
Kuvat: Raija Törrönen, Itä-Suomen yliopisto
Taitto: Raija Sassi, Helsingin yliopisto

Osa oppaan tekstistä on peräisin 2009 julkaistusta opiskelijan tietoturvaoppaasta, jonka tekijät ovat Kenneth Kahri (Helsingin yliopisto), Olavi Manninen (Kuopion yliopisto), Kaisu Rahko (Oulun yliopisto).

Tietoturvaopas on laadittu Helsingin yliopiston, Itä-Suomen yliopiston, Jyväskylän yliopiston, Oulun yliopiston, Svenska handelshögskolanin sekä Åbo Akademin työnä, ja on lisensoitu Creative Commons Nimeä-Epäkaupallinen-JaaSamoin-lisenssin mukaisesti: http://creativecommons.org/licenses/by-nc-sa/1.0/fi/

Työryhmä on lisäksi laatinut kaksi tietoturvaopasta täydentävää ohjetta: tietoturvan pikaohjeessa on oppaan keskeisimmät asiat tiivistetysti ja mobiiliturvaohje sisältää ohjeita mobiililaitteiden käytöstä.

MIKSI TIETOTURVALLISUUS ON TÄRKEÄÄ SINULLE JA YLIOPISTOLLE

- Olet varmasti huomannut tiedotusvälineissä erilaisia tietoturvaan liittyviä uutisia. Oletko koskaan miettinyt millaisia tietoturvauhkia liittyy päivittäiseen tietojen-käsittelyysi?

- Esimerkiksi verkkokalastelulla pyritään hankkimaan käyttäjien salasanoja, joita käytetään taloudellisen hyödyn tavoitteluun.

- Verkkojen ja sähköpostin kautta leviävät haittaohjelmat ovat myös vakava uhka. Ne voivat esimerkiksi varastaa tai tuhota tiedostoja, välittää tunnus- ja salasanatietojasi haittaohjelman tekijälle tai hidastaa tietoverkkojen toimintaa.

- On myös syytä kiinnittää huomiota omiin toiminta-tapoihisi. Esimerkiksi pilvipalveluja ja sähköpostia käytettäessä voit epähuomiossa jakaa yliopiston kannalta suojattavaa tietoa.

- Työhösi liittyvien tietojen vuotaminen vääriin käsiin voi vahingoittaa yliopiston toimintaa ja mainetta sekä aiheuttaa taloudellisia menetyksiä. Yliopiston merkittävin pääoma on tieto – suojaa tiedot asianmukaisesti.

- Jokaisella on velvollisuus huolehtia tietoturvallisuudesta noudattamalla viestinnästä annettua lainsäädäntöä sekä yliopiston tietoturvasääntöjä ja -ohjeita.

- Tämän tietoturvaoppaan ohjeet auttavat sinua suojaa-maan käsittelemiäsi tietoja, työasemia ja tietoverkkoja tietoturvauhkilta.

- Jos epäilet, että käyttämässäsi koneessa on haittaohjel-matartunta tai tunnuksesi on joutunut vääriin käsiin, lue oppaan loppuosassa olevat ohjeet.

KÄYTÄ VAHVOJA SALASANOJA JA PIDÄ NE SALASSA

- Yliopiston järjestelmiin kirjaudutaan henkilökohtaisella käyttäjätunnuksella ja salasanalla. Käsittele käyttäjätunnustasi ja salasanaasi yhtä huolellisesti kuin pankkikorttiasi ja tunnuslukuasi.

- Olet henkilökohtaisesti vastuussa tunnuksesi käytöstä. Älä luovuta salasanaasi kenellekään toiselle. Edes järjestelmän ylläpitäjien ei tule tietää sitä. Jos joku tiedustelee salasanaasi, hän on poikkeuksetta väärällä asialla.

- Vaihda salasana riittävän usein yliopistosi ohjeistuksen mukaisesti ja heti, jos epäilet sen joutuneen jonkun muun käsiin.

- Jos saat uuden salasanan käyttäjätuesta, vaihda se heti sellaiseksi, jonka vain sinä tiedät.

- Valitse salasanasi huolellisesti. Hyvä salasana on sellainen, jonka muistat itse helposti, mutta jota ulkopuoliset eivät pysty murtamaan. Älä käytä salasanoina jokapäiväisiä tai sinuun liittyviä sanoja. Vältä salasanan kirjoittamista muistiin sellaisenaan. Tutustu yliopistosi ohjeisiin hyvän salasanan valitsemiseksi.

- Älä käytä missään yliopiston ulkopuolisessa palvelussa samaa salasanaa kuin yliopiston palveluissa, jotta ulkopuolisen palvelun salasanan murtaminen ei mahdollista pääsyä yliopiston järjestelmiin.

SÄHKÖPOSTIN KÄYTTÖ

- Yliopiston antamaa sähköpostiosoitetta tulee käyttää sähköpostiosoitteena kaikissa työasioissa. Yliopiston ulkopuolisen sähköpostipalvelun käyttö työasioihin on kielletty. Myös työsähköpostin automaattinen ohjaaminen ulkoisiin palveluihin on kielletty.

- Palveluja tarjottaessa ja virallisia hallintotehtäviä hoidettaessa tulee ensisijaisesti käyttää erillisiä organisaatiosähköpostiosoitteita, esimerkiksi kirjaamo@yliopisto.fi.

- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ilmoita lähettäjälle väärästä osoitteesta. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä. Kuitenkin hallintotehtäviä koskeva viesti tulee hallintolain mukaan ensisijaisesti lähettää eteenpäin oikealle taholle, jos se on tiedossa.

- Huolehdi sähköpostin käsittelystä myös poissaolosi aikana. Käytä tarvittaessa automaattivastauksia esimerkiksi loman aikana kertomaan kuka hoitaa asioita poissaollessasi.

- Erota saamasi ja lähettämäsi yksityiset viestisi selvästi työsähköpostiviesteistä (erillisiin sähköpostikansioihin).

- Kirjoittaessasi viestejä ota huomioon, että vastaanottaja saattaa lähettää luottamukselliseksi merkitsemäsi viestin eteenpäin aiottua laajemmalle piirille.

- Sähköpostiviestit voivat sisältää haittaohjelmia tai voivat ohjata sinut haittaohjelmia sisältävälle sivulle. Älä avaa viestiä, jos et ole varma viestin alkuperästä tai jos sen lähettämisestä ei ole sovittu. Tarvittaessa voit kysyä lisäohjeita tietotekniikkatuesta.

- Sähköpostiviestit liikkuvat verkossa yleensä salaamattomina ilman mitään suojausta, joten suojaamista edellyttävät tiedot ja aineistot on salakirjoitettava ennen lähettämistä yliopiston ulkopuolelle.

- Suojattavia tietoja ovat yliopiston toimintaan liittyvien luottamuksellisten tietojen lisäksi esimerkiksi henkilö- ja yhteystiedot, pankkiyhteystiedot ja terveystiedot.

- Harkitse, kenelle luovutat sähköpostiosoitteesi tai missä julkaiset sen. Vältä yliopiston sähköpostiosoitteen käyttämistä nettifoorumeilla ja yhteisöpalveluissa (esim. Facebook) ja hanki yksityiskäyttöösi erillinen sähköpostiosoite. Käyttäessäsi yliopiston sähköpostiosoitetta edustat aina myös yliopistoa.

VARO KALASTELUVIESTEJÄ JA MUITA HUIJAUKSIA

- Ole terveen epäluuloinen sähköpostiviestin luotettavuudesta. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Myös haittaohjelmat voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä.

- Varo kalasteluviestejä, joissa sinua pyydetään luovuttamaan tunnuksesi ja salasanasi tai kirjoittamaan ne jollekin verkkosivulle. Ylläpitäjät eivät koskaan kysy salasanaasi.

- Tarkista linkin todellinen kohdeosoite aina ennen klikkaamista. Ole erityisen varovainen, jos olet saanut linkin viestissä.

- Opettele erottamaan asialliset verkko-osoitteet huijareiden käyttämistä. Tutustu oman yliopistosi ohjeisiin.

- Ilman vastaanottajan lupaa lähetetyt mainokset ja ketjukirjeet ovat roskapostia. Älä vastaa niihin, vaan tuhoa ne heti. Jos jokin tarjous tuntuu liian hyvältä ollakseen totta, älä tartu siihen.

- Yliopistot käyttävät roskaposti- ja haittaohjelmasuodatuksessa erilaisia menetelmiä, jotka voivat vaikuttaa sähköpostin perilletuloon. Selvitä oman yliopistosi käytännöt.

- Sähköpostin lisäksi sinua voidaan yrittää harhauttaa myös muilla keinoin, esimerkiksi puhelimessa tai sosiaalisessa mediassa. Varo yllättäviä laskuja, tekaistuja viestejä ylläpidon nimissä ja tuttaviesi nimissä lähetettyjä yllättäviä pyyntöjä.

- Mikäli epäilet joutuneesi huijauksen tai huijausyrityksen kohteeksi, voit kysyä toimintaohjeita tietotekniikkatuelta tai poliisilta.

KÄYTÄ INTERNET-PALVELUJA JA SOSIAALISTA MEDIAA VASTUULLISESTI

- Monet internet-palvelut ovat pilvipalveluita, joissa käyttäjien palveluun syöttämät tiedot talletetaan ainoastaan palveluntarjoajan palvelimille ja usein Suomen ulkopuolelle. Palveluiden käyttöehdoista kannattaa tarkistaa jo ennen palvelun käyttöönottoa ainakin tiedon omistajuuden säilyminen ja ettei tietoja luovuteta eteenpäin.

- Perehdy yliopistosi ohjeistukseen sosiaalisessa mediassa esiintymisestä. Muista, että vain tietyillä tahoilla on oikeus esiintyä virallisesti yliopiston nimissä julkisissa medioissa.

- 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.

- Käytä opetuksessa ensisijaisesti yliopiston tarjoamia palveluja. Yleensä opiskelijoita voi edellyttää käyttämään yliopiston ulkopuolista, kirjautumista edellyttävää palvelua vain jos palvelu on yliopiston virallisesti hyväksymä.

- Jos harkitset pilvipalvelujen käyttöä, tarkista palvelun soveltuvuus käyttötarkoitukseen korkeakoulujen yhteisestä pilviarviointisivustosta (linkki liiteluettelossa oppaan lopussa). Mikäli pilvipalvelussa käsitellään luottamuksellisia tietoja, käytä ainoastaan riittävän turvallisiksi arvioituja palveluja.

- Selvitä etukäteen, kuinka voit poistaa kurssimateriaalin verkosta kurssin päätyttyä.

- Käyttäessäsi erilaisia verkkopalveluita (Facebook, kuvienjakopalvelut ym.) harkitse, mitä tietoja niihin viet. Kerran verkkoon laitettua tietoa (esim. dokumentit, valokuvat, henkilötiedot, mielipiteet) voi olla myöhemmin mahdoton saada kokonaan poistettua.

- Sähköposti- ja verkkoviestinnässä kannattaa noudattaa ns. netikettiä. Liian kärkevä kirjoittaminen esimerkiksi keskusteluryhmässä voi vaikuttaa sinun ja yliopiston maineeseen.

- Varo ponnahdusikkunoita sekä verkkosivuilla olevia mainoksia. Haittaohjelmat leviävät tehokkaasti sosiaalisessa mediassa ja verkkopalveluissa – älä klikkaile varomattomasti.

- Tarkista käyttämiesi verkkopalvelujen käyttäjäprofiilisi yksityisyyden suojaan vaikuttavat asetukset (kuka pääsee katsomaan tietoja) ja säädä niitä tarvittaessa. Muista, että palveluntarjoaja saattaa vaihtaa käyttöehtoja useasti.

- Verkkoyhteisöissä on helppo tekeytyä toiseksi tai toisenlaiseksi henkilöksi. Älä suhtaudu liian sinisilmäisesti kaikkeen lukemaasi.

- Älä tallenna paikkatietoja verkkopalveluihin lataamiisi kuviin. Ota kameran GPS-ominaisuus pois päältä tai poista paikkatiedot kuvista ennen niiden julkaisemista.

KÄYTÄ TYÖNANTAJASI TIETOKONEITA VASTUULLISESTI

- Kirjaudu koneelle aina omilla tunnuksillasi.
- Jos käytät yliopistolla yhteisessä käytössä olevaa konetta, käytön päätyttyä hävitä koneelle mahdollisesti tallentamasi väliaikaistiedostot ennen uloskirjautumista.
- Lukitse kone aina kun poistut sen luota, myös silloin kun poistut vain hetkeksi (Windows-koneissa: Win+L). Tämä estää tietojärjestelmien ja tiedostojen luvattoman käytön tunnuksellasi.

- Tallenna kaikki tärkeät aineistot verkkolevylle tai kotihakemistoosi. Tällöin yliopisto huolehtii aineistojen 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.
- Jos tulostat yhteiskäytössä olevalle kirjoittimelle, nouda tuloste heti tulostamisen jälkeen.
- Hävitä luottamukselliset tulosteet ja paperiasiakirjat asiakirjatuhoojalla tai laita ne lukittuun tietosuojasäilöön.
- Ohjelmistojen asennus yliopiston koneisiin on yleensä kielletty ja usein myös teknisesti estetty. Jos tarvitset jotakin tiettyä ohjelmistoa, ota yhteyttä tietotekniikkatukeen.
- Jos sinulla on käytössä yliopiston tietokone, johon sinulla on ylläpito-oikeudet, noudata allaolevia kotikoneiden ylläpidosta esitettyjä periaatteita.

PIDÄ KOTIKONEESI TERVEENÄ JA TOIMIVANA

Olet kotitietokoneesi ylläpitäjä. Seuraa koneesi toimintaa ja huolehdi sen tietoturvasta noudattamalla seuraavia ohjeita.

- Pidä verkossa oleva kone aina palomuurilla ja haittaohjelmatorjunnalla suojattuna.
- Älä asenna yhtään ohjelmaa, jota et oikeasti tarvitse. Asenna ohjelmistojen tietoturvapäivitykset. Poista tarpeettomaksi käyneet ohjelmat.
- Tee koneelle henkilökohtaiset tunnukset (ilman ylläpito-oikeuksia) jokaiselle käyttäjälle, myös itsellesi. Ylläpitotunnuksia ei tule käyttää kuin ylläpitotehtäviin (ohjelmistojen asennus, muiden tunnusten teko).
- Ota koneen tiedostoista varmuuskopiot säännöllisesti. Säilytä varmuuskopiot erillään tietokoneesta ja mahdollisuuksien mukaan lukitussa paikassa.
- Käytöstä poistettuja tietokoneita, älypuhelimia ja muistitikkuja ei tule heittää roskiin. Tiedot tuhotaan päällekirjoittamalla tai murskaamalla väline, paperiaineistot silppuamalla.

PIDÄ HUOLTA MUISTITIKUISTASI

- Älä käytä muistitikkua tiedostojen ensisijaisena tai ainoana tallennuspaikkana, vaikka se onkin kätevä väline tietojen siirtoon ja varmuuskopiointiin. Muistitikku voi hävitä helposti.
- Jos tallennat tikuille arkaluonteista materiaalia, hanki tiedot salakirjoittava muistitikku tai suojaa tiedot salakirjoittamalla ne.

- Suhtaudu varoen muiden käyttäjien muistitikkuihin. Tikulla voi olla automaattisesti käynnistyvä haittaohjelma, joka saastuttaa sinun koneesi.

- Jos löydät yliopistolta toisen käyttäjän muistitikun, toimita se yliopiston tietotekniikkatukeen tutkimatta sen sisältöä.

ETÄKÄYTTÖ – KONEEN KÄYTTÖ TYÖPAIKAN ULKOPUOLELLA (KOTONA, MATKOILLA)

- Selvitä yliopistosi ohjeista (etätyöohje, tietojen luokitteluohje, jne.) mitä työaineistoja saa käsitellä kotona ja matkoilla.

- Käytä työtehtävien hoitamiseen ensisijaisesti työnantajan laitteita.

- Työnantajan kone on tarkoitettu vain sinun käyttöösi. Älä lainaa sitä edes perheenjäsenille.

- Käytä VPN-yhteyttä, jonka avulla saat suojatun yhteyden yliopiston palveluihin.

- Matkoilla ollessasi suojaa tietokoneesi varastamiselta. On suositeltavaa, että kovalevy on suojattu teknisellä salauksella.

- Mikäli käsittelet luottamuksellisia paperiaineistoja kotona, huolehdi niiden asianmukaisesta säilyttämisestä ja hävittämisestä.

VARO AVOIMIA LANGATTOMIA VERKKOJA JA JULKISIA KONEITA

- Käyttäessäsi avoimia langattomia verkkoja käytä vain sellaisia sähköposti- ja verkkopalveluja, jotka salaavat tietoliikenteen (osoitteen alussa on https://) tai suojattua VPN-yhteyttä.

- Tietokoneen ja ohjelmien käytöstä jää aina sinua ja tekemisiäsi koskevaa tietoa. Opettele etukäteen, kuinka tyhjennät selaimen välimuistin ja poistat muut tyypillisimmät käytöstäsi jääneet jäljet.

- Nettikahvila-, kirjasto- ja yleisökoneiden turvallisuuteen ei kannata luottaa, koska niissä voi olla käyttäjätietoja keräävä ohjelma. Harkitse, onko tarpeen kirjautua esimerkiksi omaan sähköpostiisi tällaiselta koneelta.

HUOLEHDI MYÖS MOBIILILAITTEITTESI TURVALLISUUDESTA

- Puhelimet, taulutietokoneet ja muut mobiililaitteet tulee suojata vastaavin keinoin kuin tietokoneet.

- Älä avaa tuntemattomalta lähettäjältä tulleita tai muuten epäilyttäviä tekstiviestejä. Ne voivat sisältää haittaohjelmia, jotka lähettävät viestejä nimissäsi tai aiheuttavat muuten lisäkustannuksia.

- Suojaa mobiililaitteesi varastamiselta. Suojaa laite lukituskoodilla (PIN-koodin lisäksi), jotta muut eivät pääse käsiksi sen tietoihin. Ota selvää, pystyykö laitteen tarvittaessa etätyhjentämään.

- Sulje langattomat yhteydet (Bluetooth ja WLAN) aina kun et tarvitse niitä.

- Huolehdi myös mobiililaitteiden tietojen varmuuskopioinnista. Tyhjennä tiedot laitteista käytöstä poiston yhteydessä.
- Älä asenna yhtään ohjelmaa, jota et oikeasti tarvitse. Lataa ja asenna ohjelmistoja vain virallisista kauppapaikoista.
- Ulkomailla dataliikennekustannukset ovat korkeita, käytä datayhteyttä harkiten.
- Harkitse julkaisetko sijaintitietojasi verkkopalveluissa.

HUOMIOI TEKIJÄNOIKEUDET JA OHJELMISTOLISENSSIT

- Varmista, että sinulla on käyttöoikeus ohjelmistoihin, joita asennat laitteisiisi. Älä asenna laittomia kopioita.
- Yliopistosi kautta saat käyttöoikeuden joihinkin ohjelmistoihin, tiedot löydät oman yliopistosi ohjeista.

- Yleensä käyttäjällä ei ole ylläpito-oikeutta yliopiston hallinnoimiin laitteisiin. Pyydä tietotekniikkatukea asentamaan tarvitsemasi ohjelmat.

- Selvitä kirjastojen sähköisten aineistojen käyttöehdot tutustumalla kirjastojen antamaan ohjeistukseen.

- Tekijänoikeus suojaa mm. elokuvia ja musiikkiaineistoja. Älä kopioi niitä verkosta tai jaa niitä verkkoon ilman oikeudenomistajan erillistä lupaa.

MITEN TOIMIA TYÖSUHTEEN PÄÄTTYESSÄ

- Oikeus käyttää yliopistosi tietotekniikkapalveluja on sidottu työsuhteeseesi.

- Kun työsuhteesi päättyy, yliopisto sulkee käyttäjätunnuksesi, ja poistaa tietyn ajan kuluttua sähköpostikansiosi ja muut tiedostosi pysyvästi. Ennen käyttäjätunnuksesi sulkeutumista huolehdi seuraavista asioista:

  - Ilmoita yhteyskumppaneillesi sähköpostiosoitteen muuttumisesta.

  - Sovi hyvissä ajoin esimiehesi kanssa yliopistolle tarpeellisten työaineistojen luovuttamisesta.

  - Kopioi yliopiston palvelimilta itsellesi ne yksityiset tiedostosi, jotka haluat säilyttää, ja poista muut.

  - Kopioi itsellesi yksityiset sähköpostiviestisi tai lähetä ne eteenpäin toiseen sähköpostiosoitteeseesi.

  - Poista omilta laitteiltasi ne yliopiston kautta saamasi ohjelmistot, joihin sinulla ei enää ole käyttöoikeutta.

EPÄILETKÖ HAITTAOHJELMATARTUNTAA TAI TIETOTURVARIKKOMUSTA?

- Torjuntaohjelmistot eivät pysty antamaan täydellistä suojausta, sillä haittaohjelmia tulee jatkuvasti lisää. Jos epäilet, että jollakin käyttämälläsi koneella on tai on ollut haittaohjelma, toimi seuraavasti:

  1. Vaihda heti toisella koneella kaikki ne salasanat, joita olet haittaohjelman saastuttamalla koneella käyttänyt tai jotka ovat samoja kuin kyseisellä koneella käyttämäsi. Väärinkäytön selvittämiseksi ilmoita haittaohjelma-epäilystä ja tunnuksesi mahdollisesta kaappaamisesta tärkeimpien käyttämiesi palveluiden asiakaspalveluun.

  2. Jos kone on yliopiston, ota yhteyttä tietotekniikka-tukeen. Jos kone on omasi, älä käytä sitä ennen kuin selvität kuinka pystyt poistamaan haittaohjelman. Oman koneesi puhdistamiseen voit saada rajoitetusti apua yliopistosi tietotekniikkatuelta tai virustorjunta-ohjelmasi valmistajan kotisivuilta.

- Jos epäilet tietoturvarikkomusta tai järjestelmän väärin-käyttöä, ota yhteyttä palvelusta vastaavaan. Jos palvelu on yliopiston tai käytit palvelua yliopiston antamalla tunnuksella, ota yhteyttä yliopiston tietotekniikkatukeen. Muiden palveluiden kohdalla lähetä ilmoitus organisaa-tion abuse-osoitteeseen (esim. abuse@[toimialue]) tai soita organisaation 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.
  » Perehdy oman yliopistosi tietoturvaohjeisiin ja käytäntöihin

- Ohjeita turvalliseen nettikäyttöön.
  » http://www.tietoturvaopas.fi

- Tietoja tietoturvauhkista ja ohjeita niitä vastaan suojautumiseen.
  » http://www.tietosuoja.fi

- Netti-etiketti: hyvien tapojen noudattaminen verkkoviestinnässä.
  » http://www.fi.wikipedia.org/wiki/Netiketti

- Ohjeita viestinnän suojaamiseen, tiedotuksia tietoturvauhkista.
  » http://www.cert.fi

- Kuluttajaviraston ohjeet huijauksien tunnistamisesta
  » http://www.kuluttajavirasto.fi/fi-FI/huijaukset/

- Tietoturvaohjeita mobiililaitteiden käyttöön.
  » http://www.fucio.fi/tietoturva/mobiiliturvaohje.pdf

- Korkeakoulujen yhteinen pilviarviointisivusto.
  » http://pilviohje.eduuni.fi

- Tekijänoikeudet opettajan näkökulmasta
  » http://www.opettajantekijanoikeus.fi