OPISKELIJAN TIETOTURVAOPAS

Syyskuu 2017

lokalisoitu joulukuussa 2017

päivitetty helmikuussa 2019

Tämä tietoturvaopas on tarkoitettu ensisijaisesti yliopisto-opiskelijoiden 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 ja Jan Wennström, Åbo Akademi.

Kuvat: Raija Törrönen, Itä-Suomen yliopisto

Opas on päivitetty versio 2009 julkaistusta opiskelijan tietoturvaoppaasta, tekijät Kenneth Kahri, Helsingin yliopisto, Olavi Manninen, Kuopion yliopisto ja Kaisu Rahko, Oulun yliopisto.

SISÄLLYSLUETTELO

MIKSI TIETOTURVALLISUUS ON SINULLE TÄRKEÄÄ

- Päivittäiseen tietojenkäsittelyyn liittyy erilaisia tietoturvauhkia.
- Yksi vakava uhka on verkkojen ja sähköpostin kautta leviävät haittaohjelmat. Ne voivat esimerkiksi varastaa tai tuhota tiedostojasi, välittää tunnus- ja salalausetietojasi haitta-ohjelman tekijälle tai hidastaa tietoverkkojen toimintaa. Torjuntaohjelmistot eivät pysty suojaamaan kaikilta haittaohjelmilta, sillä niitä tulee jatkuvasti lisää. Muita vakavia uhkia ovat identiteettivarkaudet sekä taloudellisen hyödyn tavoittelu käyttäjän tietojen avulla.
- Käyttämällä tervettä järkeä ja noudattamalla ohjeita voit suojata tietojasi, käyttämiäsi työasemia ja tietoverkkoja tietoturvauhkilta. Suojaa omien tietojesi lisäksi hallussasi olevat muiden henkilöiden tiedot. Ulkopuolisilta suojattavia tietoja ovat esimerkiksi henkilö- ja yhteystiedot, pankkiyhteystiedot, terveystiedot ja sähköpostiviestit.
- Jokaisella on velvollisuus huolehtia tietoturvallisuudesta noudattamalla viestinnästä annettua lainsäädäntöä sekä yliopiston tietoturvasääntöjä. Niiden noudattamatta jättäminen saattaa johtaa seuraamuksiin.

KÄYTÄ VAHVOJA SALASANALAUSEITA JA PIDÄ NE SALASSA

- Yliopiston järjestelmiin kirjaudutaan henkilökohtaisella käyttäjätunnuksella ja salasanalauseella(salasanalla). Käsittele käyttäjätunnustasi ja salasanalausettasi yhtä huolellisesti kuin pankkikorttiasi ja tunnuslukuasi.
- Saatuasi uuden salasanalauseen käyttäjätuesta, vaihda se heti sellaiseksi, jonka vain sinä tiedät. Vaihda salasanalause riittävän usein yliopistosi ohjeistuksen mukaisesti ja heti, jos epäilet sen joutuneen jonkun muun käsiin.
- Olet vastuussa tunnuksesi käytöstä. Älä luovuta salalausettasi kenellekään toiselle. Edes järjestelmän ylläpitäjien ei tule tietää sitä. Jos joku tiedustelee salalausettasi, hän on poikkeuksetta väärällä asialla.
- Valitse salasanalauseesi huolellisesti. Hyvä salasanalause on sellainen, jonka muistat itse helposti, mutta jota ulkopuoliset eivät pysty murtamaan. Älä käytä salasanalauseina jokapäiväisiä tai sinuun liittyviä sanoja tai sanontoja. Vältä salasanalauseen kirjoittamista muistiin sellaisenaan. Tutustu yliopistosi ohjeisiin hyvän salasanalauseen valitsemiseksi.
- Älä käytä missään yliopiston ulkopuolisessa palvelussa samaa salasanalausetta kuin yliopiston palveluissa, jotta ulkopuolisen palvelun salasanalauseen murtaminen ei mahdollista pääsyä yliopiston järjestelmiin. Ota käyttöön salasanojen hallintaohjelmisto salasanalauseiden hallinnan helpottamiseksi.

SÄHKÖPOSTIN KÄYTTÖ

- Yliopiston antamaa sähköpostiosoitetta on syytä käyttää ensisijaisena sähköpostiosoitteena yliopiston sisäisessä viestinnässä ja palveluissa, muun muassa opintorekisterissä ja oppimisympäristöissä. Käyttämällä yliopiston sähköpostipalveluita voit parantaa viestinnän turvallisuutta.
- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ilmoita lähettäjälle väärästä osoitteesta. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.

- 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 tietotekniikkaneuvonnasta (origo helpdesk).
- Sähköpostiviestit liikkuvat verkossa yleensä salaamattomina ilman mitään suojausta, joten suojaamista edellyttävät tiedot on salakirjoitettava ennen lähettämistä.
- Harkitse, kenelle luovutat sähköpostiosoitteesi tai missä julkaiset sen. Vältä yliopiston sähköpostiosoitteen käyttämistä nettifoorumeilla ja yhteisöpalveluissa (esim. Facebook) ja hanki yksityiskäyttöösi erillinen sähköpostiosoite.

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 salalauseesi tai kirjoittamaan ne jollekin verkkosivulle. Ylläpitäjät eivät koskaan kysy salalausettasi.
- 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 ja tekaistuja viestejä ylläpidon nimissä ja tuttaviesi nimissä lähetettyjä yllättäviä pyyntöjä.

KÄYTÄ VERKKOPALVELUJA JA SOSIAALISTA MEDIAA VIISAASTI

- Käyttäessäsi erilaisia verkkopalveluita (Facebook, kuvienjakopalvelut ym.) harkitse, mitä omia tai muiden tietoja niihin viet. Kerran verkkoon laitettua henkilökohtaista tietoa kuten valokuvaa tai kotiosoitetta voi olla myöhemmin mahdoton saada kokonaan poistettua.
- Varo ponnahdusikkunoita sekä verkkosivuilla olevia mainoksia. Haittaohjelmat leviävät tehokkaasti sosiaalisessa mediassa ja verkkopalveluissa - älä klikkaile varomattomasti.
- Älä käytä verkkopalveluja, jotka eivät tunnu luotettavilta.
- Monet verkkopalvelut ovat pilvipalveluita, jolloin käyttäjien palveluun syöttämät tiedot ovat ainoastaan palveluntarjoajan palvelimilla, usein Suomen ulkopuolella. Pilvipalveluihin liittyy useita tietoturvariskejä, jotka on hyvä tiedostaa. Palveluiden

käyttöehdoista kannattaa tarkistaa jo ennen palvelun käyttöönottoa ainakin tiedon omistajuuden säilyminen ja ettei tietojasi luovuteta eteenpäin.

- Tarkista käyttäjäprofiilisi yksityisyyden suojaan vaikuttavat asetukset (kuka pääsee katsomaan tietoja) ja säädä niitä tarvittaessa.
- 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.
- Verkkoyhteisöissä on helppo tekeytyä toiseksi tai toisenlaiseksi henkilöksi. Älä suhtaudu liian sinisilmäisesti kaikkeen lukemaasi.
- Sähköposti- ja verkkoviestinnässä kannattaa noudattaa ns. netikettiä. Liian kärkevä kirjoittaminen esimerkiksi keskusteluryhmässä voi vaikuttaa maineeseesi esimerkiksi työnhaussa.
- Älä tallenna paikkatietoja verkkopalveluun lataamiisi kuviin. Ota kameran GPS-ominaisuus pois päältä tai poista paikkatiedot kuvista ennen niiden julkaisemista.

PIDÄ OMA TIETOKONEESI TERVEENÄ JA TOIMIVANA

- Olet oman tietokoneesi ylläpitäjä. Seuraa koneesi toimintaa ja huolehdi sen tietoturvasta noudattamalla seuraavia ohjeita.
- Verkossa oleva kone tulee aina suojata palomuurilla ja haittaohjelmatorjunnalla.
- Älä asenna yhtään ohjelmaa, jota et oikeasti tarvitse. Asenna ohjelmistojen tietoturvapäivitykset.
- Tee kotikoneelle henkilökohtaiset tunnukset (ilman ylläpito-oikeuksia) jokaiselle käyttäjälle. Ylläpitotunnuksia ei tule käyttää kuin ylläpitotehtäviin (ohjelmistojen asennus, muiden tunnusten teko).
- Ota kotikoneen 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.

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. Vaihda myös SIM-kortin PIN-koodi. 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 harkiten.
- Harkitse julkaisetko sijaintitietojasi verkkopalveluissa.

KÄYTÄ YLIOPISTON TIETOKONEITA VASTUULLISESTI

- Kirjaudu koneelle aina omilla tunnuksillasi. 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 tunnuksesi ja tiedostojesi luvattoman käytön. Huomioi kuitenkin, että koneen lukitseminen pidemmäksi aikaa saattaa olla kiellettyä, koska tällöin kone jää varatuksi.

- Tallenna kaikki tärkeät aineistosi verkkolevylle tai kotihakemistoosi. Tällöin yliopisto huolehtii aineistosi varmuuskopioinnista.
- Jos tulostat yhteiskäytössä olevalle kirjoittimelle, nouda tuloste heti tulostamisen jälkeen.
- 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.
- Ohjelmistojen asennus yliopiston koneisiin on yleensä kielletty ja usein myös teknisesti estetty. Jos tarvitset jotakin tiettyä ohjelmistoa, ota yhteyttä tietotekniikkatukeen(origo helpesk).

VARO AVOIMIA LANGATTOMIA VERKKOJA JA JULKISIA KONEITA

- Nettikahvila-, kirjasto- ja yleisökoneiden turvallisuuteen ei kannata luottaa, niissä voi olla käyttäjätietoja keräävä ohjelma. Harkitse, onko tarpeen kirjautua esimerkiksi omaan sähköpostiisi tällaiselta koneelta.
- Tietokoneen ja ohjelmien käytöstä jää aina sinua ja tekemisiäsi koskevaa tietoa. Opettele etukäteen, kuinka tyhjennät selaimen välimuistin ja poistat muut tyypillisimmät käytöstäsi jääneet jäljet.
- Käyttäessäsi langattomia verkkoja käytä vain sellaisia sähköposti- ja verkkopalveluja, jotka salaavat tietoliikenteen (osoitteen alussa on https://).

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 salakirjoittamalle ne (esimerkiksi Windows BitLocker).
- Suhtaudu varoen muiden käyttäjien muistitikkuihin. Tikulla voi olla automaattisesti käynnistyvä haittaohjelma, joka saastuttaa sinun koneesi.
- Jos löydät yliopistolta toisen käyttäjän muistitikun, toimita se yliopiston tietotekniikka-neuvontaan (origo helpdesk) tutkimatta sen sisältöä.

HUOMIOI TEKIJÄNOIKEUDET JA OHJELMISTOLISENSSIT

- Varmista, että sinulla on käyttöoikeus ohjelmistoihin, joita asennat koneeseesi. Älä asenna laittomia kopioita.
- Yliopistosi kautta saat käyttöoikeuden joihinkin ohjelmistoihin, tiedot löydät oman yliopistosi ohjeista.
- Selvitä kirjastojen sähköisten aineistojen käyttöehdot tutustumalla kirjastojen antamaan ohjeistukseen.
- Tekijänoikeus suojaa elokuvia ja musiikkiaineistoja. Älä kopioi niitä verkosta tai jaa niitä verkkoon ilman oikeudenomistajan erillistä lupaa.

MITEN TOIMIA OPINTO-OIKEUDEN PÄÄTTYESSÄ

- Oikeus käyttää yliopistosi tietotekniikkapalveluja on sidottu opinto-oikeuteesi.
- Kun valmistut tai opinto-oikeutesi päättyy, yliopisto sulkee käyttäjätunnuksesi, ja poistaa tietyn ajan kuluttua sähköpostikansiosi ja muut tiedostosi pysyvästi. Ennen käyttäjätunnuksesi 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 omilta laitteiltasi ne yliopiston kautta saamasi ohjelmistot, joihin sinulla ei enää ole käyttöoikeutta.

EPÄILETKÖ HAITTAOHJELMATARTUNTAA TAI TIETOTURVARIKKOMUSTA?

- Jos epäilet, että jollakin käyttämälläsi koneella on tai on ollut haittaohjelma, toimi seuraavasti:

    1. Vaihda heti toisella koneella kaikki ne salalauseet, joita olet haittaohjelman saastuttamalla koneella käyttänyt tai jotka ovat samoja kuin kyseisellä koneella

käyttämäsi. Väärinkäytön selvittämiseksi ilmoita haittaohjelmaepäilystä ja tunnuksesi mahdollisesta kaappaamisesta tärkeimpien käyttämiesi palveluiden asiakaspalveluun.

2. Jos kone on omasi, älä käytä sitä ennen kuin selvität kuinka pystyt poistamaan haittaohjelman. Jos koneen omistaa joku muu, ota yhteyttä siitä vastaavaan henkilöön tai tahoon ja kerro tilanteesta. Oman koneesi puhdistamiseen voit saada rajoitetusti apua yliopistosi tietotekniikkatuelta tai virustorjuntaohjelmasi valmistajan kotisivuilta.

3. Jos epäilet tietoturvarikkomusta tai järjestelmän väärinkäyttöä, ota yhteyttä palvelusta vastaavaan. Jos palvelu on yliopiston tai käytit palvelua yliopiston antamalla tunnuksella, ota yhteyttä yliopiston tietotekniikkatukeen. Muiden palveluiden kohdalla lähetä ilmoitus organisaation abuse-osoitteeseen (esim. abuse(at)lut.fi) 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

- Perehdy oman yliopistosi tietoturvaohjeisiin ja käytäntöihin.
  » Oman yliopistosi tietoturvasivusto

- Yliopiston Salasanalauseohjeistus
  » https://id.lut.fi/guidelines_fi.html

Ohjeita turvalliseen nettikäyttöön.
» https://turvalistit.fi/

- Tietosuojavaltuutetun toimisto
  » https://tietosuoja.fi/etusivu

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

- Ohjeita viestinnän suojaamiseen, tiedotuksia tietoturvauhkista.
  » https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

- Kuluttajaviraston ohjeet huijauksien tunnistamisesta
  » https://www.kkv.fi/Tietoa-ja-ohjeita/Ostaminen-myyminen-ja-sopimukset/huijaukset/

- Korkeakoulujen yhteinen pilviarviointisivusto.
  » https://wiki.eduuni.fi/display/pilviohje/