Opiskelijan tietoturvan pikaopas

Metropolia

Mitä on tietosuoja ja, miten minun on otettava se huomioon?

- Tietosuoja tarkoittaa järjestelyjä, joilla varmistetaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen. Tietosuoja on eri asia kuin tietoturva.
- Henkilötieto viittaa kaikkeen yksityishenkilöön liittyvään tietoon, joista hänet tunnistaa tai voi tunnistaa, esimerkiksi yhdistelemällä tietoja toisiinsa.
- Arkaluonteiset henkilötiedot muodostavat henkilötietojen erityisryhmän, joiden käsitteleminen on kiellettyä paitsi tietyissä tilanteissa.
- Tietosuojaa koskevan lainsäädännön tarkoituksena on turvata kaikille kuuluvat perusoikeudet, kuten oikeus yksityiselämän suojaan.

Metropolia

Mitä on henkilötieto?

Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti, esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Henkilö voidaan tunnistaa, esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.

- **Kotiosoite**
- **Ajokortti**
- **Valokuva**
- **IP-osoite**
- **Työhakemus**
- **Passi**

Henkilötieto

Arkaluonteinen Henkilötieto

Näitä tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille

Lisätietoa erityisten henkilötietoryhmien käsittelystä.

- Terveystiedot
- Tiedot sosiaali- ja/tai terveyspalveluiden asiakkuudesta,
- Julkisuuslain mukaan salassapidettävät tiedot (kuten opiskelijan koesuoritus ja/tai henkilön sanallinen henkilöarviointi)

- Uskonnollinen tausta
- Etninen alkuperä,
- AY-liikkeen jäsenyys,
- Henkilön taloudelliseen tilanteeseen liittyvät tiedot,
- Biometriset henkilötiedot yksiselitteisessä tunnistamistarkoituksessa, kuten kasvokuva

Tietosuoja-asetus suojaa henkilötietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään, tai että tapahtuuko tietojen käsittely manuaalisesti tai sähköisesti. Tietojen säilytystavalla ei myöskään ole merkitystä. Tietoja voidaan säilyttää, esimerkiksi IT-järjestelmässä, videovalvontajärjestelmässä tai paperiarkistossa.

Lähde: Tietosuojavaltuutetun toimisto

Metropolia

Suostumus käsittelyperusteena

1. Jos tietojenkäsittely perustuu suostumukseen, **rekisterinpitäjän on pystyttävä osoittamaan**, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn.

   Hanki suostumus kirjallisesti ennen kuin ryhdyt henkilötietojen käsittelytoimiin-

2. Jos rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka koskee myös muita asioita, *suostumuksen antamista koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.*

   Huomioi erityisesti, että suostumus tutkimukseen osallistumiseen on eri asia kuin suostumus henkilötietojen käsittelyyn.

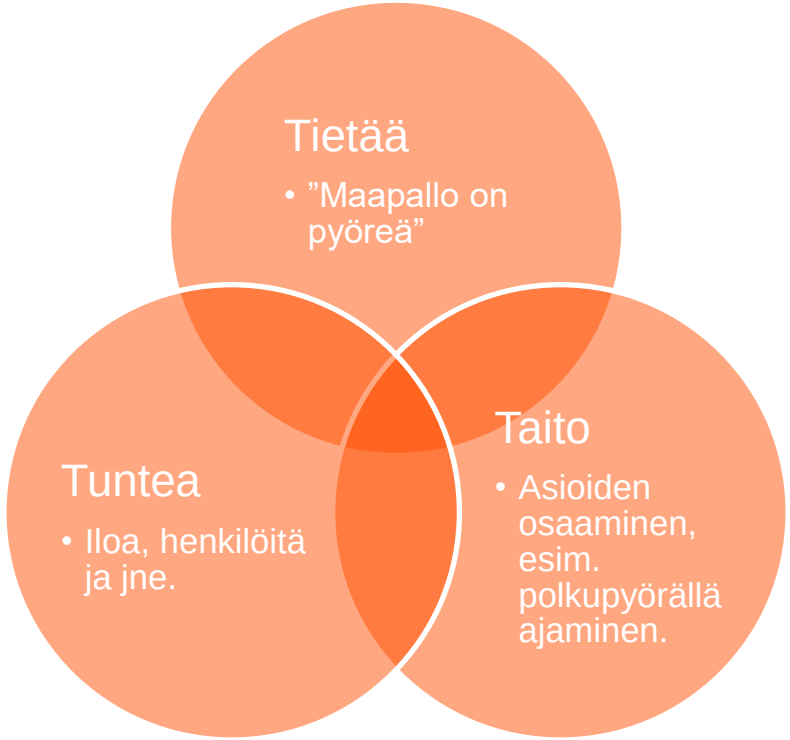
3. **Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa.** Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Ennen suostumuksen antamista rekisteröidylle on ilmoitettava tästä. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen.

4. Arvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten.

Metropolia

Mitä tieto on?

- Tietoturvalla (information security) suojataan tietoa, joka on eri muodossa ja asteissa.
- Tiedon asteet ja arvo vaihtelevat ihmisille:
  - Data = symbolit ja merkit, esim. aakkoset.
  - Informaatio = kuvailevaa ja tulkitaan datasta, esim. paperilta luettuna.
  - Tieto = informaatiolle annetaan konteksti ja on ihmisten välillä jaettua. Organisaation tuottama lisäarvo syntyy tästä.



Metropolia

Mitä on tietoturva?

- Tietoturva tarkoittaa järjestelyjä, joilla varmistetaan tiedon saatavuus, eheys ja luottamuksellisuus.
- Tietoturvassa tieto ymmärretään kokonaisvaltaisesti, joka voi olla monenlaisessa muodossa eri paikoissa:
  - Elektronisessa ja fyysisessä muodossa.
  - Aineellisena, esim. paperilla.
  - Aineettomana, esim. ihmisten oppimina tietona asioista.
- Suojaaminen tapahtuu hallinnollisilla, henkilöstöllisillä, organisatorisilla ja teknisillä toimilla.
  - Hallinnolliset toimet ovat organisatorisia käytäntöjä, kuten salasanapolitiikka ja tietoturvakoulutukset.
  - Tekniset toimet ovat taustalla toimivia suojatoimenpiteitä, kuten palomuurit tai identiteetinhallinta.
- Tietoturva-asiat tulisi ensisijaisesti nähdä liiketoiminnallisina asioina eikä teknologisina ongelmina ainoastaan.

- Tietoturva rakentuu kolmesta osasta (ns. CIA-kolmio), jotka voidaan määritellä, esimerkiksi seuraavalla tavalla:
  1. Metropoliassa opiskelijana teet kurssitehtäviä. Kurssitehtävien äärelle asiattomien ei tulisi päästä, josta tietoturvassa käytetään termiä tiedon **luottamuksellisuusvaatimus** (Confidentiality, C)**.**
  2. Opiskelijana Metropolian opettajat arvioivat kurssisuorituksiasi. Kurssisuorituksia koskevan tiedon on oltava tarkkaa ja turmelematonta läpi tiedon elinkaaren tietoturvan **eheysvaatimuksen mukaisesti** (Integrity, I).
  3. Kun opiskelijana teet ryhmätöitä, niin todennäköisesti työstät yhteistä dokumenttia muiden opiskelijoiden kanssa. Työdokumentilla on silloin **käytettävyysvaatimus** (Availability, A) opiskelijoiden näkökulmasta.

Metropolia

Tietoturvan perussanastoa

Henkilötietosuoja; tietosuoja	Järjestelyt, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.
Tietoturvallisuus	Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.
Kyberturvallisuus	Tavoitetila, jossa kyberympäristöön voidaan luottaa ja jossa sen toiminta turvataan.
Tietoturvapoikkeama; tietoturvahäiriö	Yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti.
Kyberympäristö; kybertoimintaympäristö	Digitaalisen informaation käsittelyyn tarkoitettu, toisiinsa yhteydessä olevista tietokoneista ja muista laitteista sekä tietoverkoista muodostunut ympäristö.
Identiteettivarkaus	Rikollista toimintaa, jossa henkilö esiintyy luvattomasti toisena henkilönä huijatakseen kolmatta osapuolta.
Varmuuskopiointi	Tarkoitetaan tärkeän tiedon kopiointia alkuperäisen tallennuspaikan lisäksi yhteen tai useampaan paikkaan. Onnettomuuden sattuessa voit palauttaa tiedot varmuuskopiosta.
VPN	Virtual Private Network, eli virtuaalinen erillisverkko. Tapa salata ja luoda yksityinen ja tietoturvallinen Internet-yhteys.

Salasanakäytäntö

Turvallisen salasanan luomisessa on muistettava muutama nyrkkisääntö.

- Salasanan on oltava pitkä, suosittelemme 15 merkkistä. Sisällytä myös isoja kirjaimia, numeroita ja erikoismerkkejä.

- **Älä käytä Metropolian palveluissa samaa salasanaa, jota käytät jossakin muussa palvelussa.** Pahimmillaan toisen palvelun tietomurto voi johtaa Metropolian tietotuvan vaarantumiseen.

- Hyvä salasanakäytäntö on, että salasana vaihdetaan tarpeeksi usein, kuten kahdesti vuodessa. Ethän säilytä salasanaasi sähköpostissa, puhelimessa tai tietokoneen työpöydällä.

- Tapauksissa jossa epäilet, että tietosi ovat joutuneet vääriin käsiin, vaihda Metropolian salasanasi välittömästi. Salasanan voi vaihtaa verkossa vahvalla tunnistautumisella. Sen jälkeen ota aina yhteyttä HelpDeskin puhelinpalveluun, joka ohjeistaa tapauksen mukaisesti Puh. 09 7424 6777.

Metropolia

Löydät turvapostista lisätietoa OMA:sta ja Tietohallintopalveluiden Wiki-sivuilta kirjautumalla Metropolia-tunnuksellasi järjestelmään.

Turvataso	Kuvaus	Esimerkit käytöstä	Osoitteen formaatti
”Kirje”	Salattavaksi haluttuihin viesteihin lisätään vastaanottajan osoitteen perään .s	Tarjoukset, hintatiedot, kyselyt, raportit ja talousraportit, henkilöturvatunnukset, yritysyhteistyökumppaneiden luottamukselliset tiedot, osa viranomaisyhteistyöstä (jossa ei arkaluonteisia henkilötietoja), julkisuuslain mukaan salassa pidettävät asiakirjat (esim. opinnäytetyön tutkimussuunnitelma)	nimi@yritys.fi.**s**
”Kirjattu kirje”	Lähettäjä voi varmistua vastaanottajasta, kun lisätään vastaanottajan sähköpostin perään vastaanottajan puhelinnumero ja .s	Terveystiedot tai tieto terveyspalvelujen käytöstä, lautakuntaviestintä, kaikki arkaluonteiset henkilötiedot (tiedot henkilön taloudellisesta asemasta, työttömyydestä, perheolosuhteista, yksityiselämän piiriin kuuluvat asiat), organisaation salassa pidettävät tiedot, taloudelliset ja oikeudelliset sitoumukset, luottamukselliset tiedot ja päätökset	nimi@yritys.fi**.0401234567.s**

HUOM: ”Kirjattu kirje” -taso on käytössä ainoastaan Metropolian henkilökunnalla, mutta opiskelija voi lähettää salatun viestin lisäämällä osoitteen perään S-kirjaimen.

- ”Kirjattu kirje” -tasolla vastaanottaja tunnistetaan lisäksi **SMS-autentikoinnin** avulla. Käytännössä vastaanottajan avatessa viestin, järjestelmä kysyy PIN-koodia, joka lähetetään samanaikaisesti tekstiviestinä vastaanottajan matkapuhelimeen.

Metropolia

Tietoturvallinen etäopiskelu

Etäopiskelulla tarkoitetaan muualla kuin Metropolian kampuksilla tapahtuvaa opiskelua.

Seuraavin keinoin parannat digiturvaasi arjessasi!

1. **Käyttäydy fiksusti tietokoneellasi vapaa-ajallasi ja opinnoissasi**
   - Kun käytät tietokonettasi, niin asioi luotettavilla sivuilla ja käytä turvallisia maksuyhteyksiä verkkomaksujen tekemiseksi.
2. **Käytä luotettavaa verkkoyhteyttä - opinnoissa hyödynnä Eduroam-verkkoa aina, kun voit**
   - Julkiset avoimet verkkoyhteyden eivät ole luotettavia kampuksen ulkopuolella. Pääset Eduroam-verkkoon omilla käyttäjätunnuksillasi vieraillessasi muissa Eduroam-jäsenorganisaatioissa ja päinvastoin. Kun työskentelet sensitiivisen datan kanssa käytä VPN-yhteyttä. Ohessa ohje VPN-yhteyden muodostamiseksi.
3. **Mieti, mitä jaat verkossa ja kunnioita yksityisyyden suojaa**
   - Kun julkaiset jotain verkossa, niin sisältö ei katoa sieltä, vaikka poistaisit julkaisun ja hakukoneet rajoittaisivat sen näkyvyyttä. Kunnioita muiden yksityisyyttä, esimerkiksi sosiaalisen median käytössäsi.
4. **Tarkista etätyö- ja opiskelupisteesi sijainti**
   - Jos teet opintojen ohessa töitä, niin noudata työnantajasi tietoturvaohjeita, esimerkiksi kampuksella työskentelemisen suhteen. Kysy työnantajaltasi ohjeistusta etätöiden toimintaperiaatteista, ettet vaaranna työnantajasi tietoturvaa.
5. **Varo huijauksia**
   - Opintojen digitalisaation yhteydessä myös huijauspuhelut, tietojenkalastelu ja käyttäjämanipulaatio ovat kasvaneet. Rikolliset hyödyntävät tätä haavoittuvaisuutta. Ole siis valppaana, kun toimit digitaalisessa ympäristössä.
6. **Sinulla on mahdollisuus käyttää F-Securen palveluita etuhintaan opiskellessasi Metropolialla**
   - F-Secure TOTAL on kokonaisvaltainen tietoturvapaketti, joka yhdistää yhteen tilaukseen tietoturvan, yksityisyydensuojan ja VPN:n, sekä identiteettisuojan ja salasanamanagerin.
7. **Opiskellessasi toisessa korkeakoulussa, kunnioita toisen korkeakoulun tietoturvan toimintaperiaatteita – kysy neuvoa tarvittaessa kohdekorkeakoulun käyttäjätuesta**
   - Kunnioita kohdekorkeakoulun tietoturvaa, jos olet vaihdossa tai suoritat Joo-opintoja.

Metropolia

Älä opiskele suojaamattomassa verkossa

- Suojatut verkot tunnistat HTTPS-tekstistä tai osoiterivin lukkosymbolista.
- Myös avoimet ilmaiset verkot (esim. VR:n junaverkko tai kahvilan julkinen verkko) ovat salaamattomia.
- Periaatteessa avoimessa verkossa kuka tahansa keinot hallitseva henkilö voi kaapata ja lukea tällaista liikennettä selkokielisenä.
- Älä jaa ikinä luottamuksellista ja salattua tietoa suojaamattoman verkon tai ilmaisverkon kautta.
- Älä koskaan mene verkkopankkiisi, mobiilipankkiisi tai muulle sivustolle, jolle joudut syöttämään henkilötietojasi suojaamattomassa verkossa.

Metropolia

Suojaa matkapuhelimesi – sinä olet puhelimesi tärkein tietoturvan lenkki

Puhelimen pääsykoodilla estät ulkopuolisen pääsemisen laitteellesi

- Käytä monimutkaista pääsykoodia ja PIN-koodia.
- Älä käytä peräkkäisiä numeroita tai syntymäaikaa koodinasi.

Käytä automaattista lukitusta ja etälukitusta varkauksien varalle

- Käytä puhelimen lukitusasetuksissa automaattista lukitusta, esim. vaihtaessasi SIM-kortin tai, jos puhelinta ei käytä muutamaan minuuttiin.
- Puhelimen etälukitus mahdollistaa puhelimen lukitsemisen, vaikka menettäisit tai kadottaisit puhelimen.

Rajaa puhelimen ilmoituksien näkyvyyttä

- Puhelimen näytölle voi ilmestyä arkaluonteista tai salassa pidettävää tietoa.
- Hallitse laitteesi sovelluksien ilmoitusasetuksia liiallisen informaatiotulvan välttämiseksi.

Päivitä puhelinta

- Pidä huoli sovelluksien ja käyttöjärjestelmien päivityksien ajantasaisuudesta.
- Sovelluksia päivitetään puhelimen sovelluskaupassa.
- Järjestelmäpäivitykset päivitetään puhelimen asetuksista laitteesi ohjeiden mukaisesti, joista puhelin tiedottaa käyttäjää.

Ilmoita menetetystä laitteesta Poliisille

- Vakuutus- ja takuukorvaus voi edellyttää rikosilmoituksen tekemistä.
- Jos puhelimesi muistaa käyttäjätunnuksen ja/tai salasanasi, kuten Metropolia-tunnuksesi, niin vaihda salasanasi välittömästi.

Ole varuillaan haittaohjelmien ja viruksien varalle

- Vältä Bluetooth-yhteyden pitämistä turhaan päällä viruksien ja haittaohjelmien leviämisen estämiseksi.
- Älä kytke puhelinta laitteeseen, jonka turvallisuudesta tai luotettavuudesta et ole varma.

Metropolia

TT-poikkeaman käsittelyprosessin vaiheet pääpiirteittäin

1. TT-poikkeaman havaitseminen
   - Ilmoita tarvittaville tahoille: käyttäjätuelle (HelpDesk), tietosuojavastaavalle ja tietoturva-asiantuntijalle.
   - Kiireettömät tapaukset: Metropolian palvelupyyntöjärjestelmässä.
2. Poikkeaman rajoittaminen
   - Estetään lisävahinkojen syntyminen ja minimoidaan vaikutukset.
3. Poikkeaman laajuuden arviointi
   - Mitä tietoja on vuotanut?
   - Mitä, missä, miten, kuka/ketkä ja miksi?
4. Poikkeamaan johtaneen tilanteen korjaaminen ja palautuminen
   - Siirtyminen poikkeamaan edeltäneeseen normaaliin olotilaan.
   - Kriisikestävyyden eli resilienssin vahvistaminen.
5. Poikkeamatilanteen jälkiselvitys
   - Oppiminen tulevaisuutta varten – ohjeistuksen parantaminen.
   - Dokumentointi.
   - Tietotekniikkarikkomuksen mahdollinen selvittäminen.

Metropolia

Fyysinen turvallisuus Metropoliassa

- Tietoturvaan kuuluu myös tiedon fyysisestä turvallisuudesta huolehtiminen.
- Fyysisillä hallintakeinoilla huolehditaan työtilojen turvallisuudesta, kulunvalvonnasta ja jopa opiskelijoista. Ilman opiskelijoita ei Metropoliaakaan voisi olla olemassa.
- Keinoja ovat, muun muassa lukitukset, savu- ja palovaroittimet, kamerat, vartiointi ja jäähdytysjärjestelmät .

Metropoliassa fyysinen turvallisuus huomioidaan, muun muassa:

- Huolehtimalla ovien ja ikkunoiden lukituksista poistuessa tilasta. Atk-laitteita sisältävät tilojen ovet on pidettävä lukittuina.
- Estämällä työaseman luvattoman käytön lukitsemalla työaseman. Työasemissa tehdään ns. lukitus painamalla WINDOWS -näppäintä ja L -kirjainta.
- Henkilökunnan jäsenet saattavat Metropolian vieraat pois korkeakoululta.
- Säilyttämällä opinnoissa käytettävää konetta asianmukaisesti kotona, matkoilla ja julkisissa tiloissa.
- Käsittelemällä fyysisiä asiakirjoja oikeaoppisesti, esim. opinnäytetyötäprosessin aikana.
- Metropolian henkilökunta pitää esillä kulkutunnistetta.
- Rajaamalla ei-henkilökuntaa kuuluvien pääsyoikeuksia fyysisissä tiloissa.

Metropolian tietoturvaohje sisältää tarkemman listauksen tietoturvallisuuden perusasioista. Niitä noudattamalla huolehdit osaltasi tunnuksesi, tietojesi ja käyttämiesi järjestelmien suojaamisesta.

Metropolia

Fyysisten asiakirjojen käsittely Metropoliassa

- Kaikki luottamuksellinen paperi- ja muu salassa pidettävä aineisto on laitettava tietoturvaroskikseen, kuten henkilötietoja sisältävät tulosteet ja kurssisuorituksiin liittyvät materiaalit.

- Jos sinulla on tarvetta tulostaa, hae tulosteet välittömästi monitoimilaitteelta.

- Mikäli käyttäjä saa toiselle henkilölle (esimerkiksi kaimalle) tarkoitetun sähköpostiviestin, vastaanottajan on lähetettävä alkuperäiselle lähettäjälle tieto epäonnistuneesta toimituksesta ja hävitettävä saapunut viesti.

- Tietojärjestelmien ja ohjelmistojen käyttö- ja ylläpitosäännöt ovat luettavissa Tietohallintopalveluiden sivuilta.

Metropolia

Tiedon hyödyntämisessä on huomioitava tiedon elinkaari

- Tiedon elinkaarisuunnittelulla hallitaan organisaation tieto-omaisuutta kustannustehokkaasti.

- Tiedonhallinnassa tulisi miettiä seuraavia asioita:
  - Mitä tietoa suojataa? (suojattava tieto-omaisuus)
  - Mihin tietoja käytetään? (tieto-omaisuuden käyttötarkoitus)
  - Minne tietoja tallennetaan? (tallentamispolitiikka)
  - Mikä on tiedon tai järjestelmän elinkaari vastuineen? (säilytysaika ja vastuutahot)

- Tiedon elinkaarisuunnittelua ohjaavat käytössä olevat prosessit, politiikka, käytännöt ja työkalut.

- Tiedonhallinnassa on tiedettävä minne tietoa tallentaa.
- Esimerkiksi arkaluonteista tietoa ei käsitellä pilvipalveluissa.

- Tietoa syntyy nykyisin kaikessa toiminnassa, kuten opinnäytetyön tekemisen yhteydessä.

- Tiedon elinkaarimalli koostuu neljästä vaiheesta
  1. Tiedon luomisesta ja vastaanottamisesta
  2. Säilyttämisestä ja käytöstä
  3. Jakamisesta ja siirtämisestä
  4. Tiedon arkistoinnista ja luokittelusta

Metropolia

Tiedon luokittelu

Asiakirjojen ja tietojen jakaminen luokkiin salassa pidettävyyden perusteella on tärkeä osa tiedon elinkaaren turvallisuutta. Kun tietoa luokitellaan, voidaan tieto tallentaa ja julkaista sille sopivassa tallennuskohteessa, kuten verkkolevyllä, tietokoneen paikallislevyllä, ulkoisella tallentimella, tietojärjestelmässä tai pilvipalvelussa. Tiedon luokittelu perustuu pilvipalveluehtoihin, lainsäädäntöön tai sopimuksiin.

Tieto-omaisuuden omistaja ja/tai käsittelijä vastaavat tiedon asianmukaisesta luokittelusta.

Metropoliassa on käytössä seuraavat tiedon luokitteluluokat:

Julkinen tieto

- Tiedon katseluun ei ole rajoituksia. Tähän kategoriaan kuuluvat kurssi- ja lehdistötiedotteet.

Sisäinen tai rajoitettu käyttöön tarkoitettu tieto

- Tietoa voi katsella Metropolian henkilökunta ja opiskelijat. Tähän luokkaan kuuluvat intratiedotteet ja opetusmateriaalit.

Luottamuksellinen tieto

- Tietoja voivat katsella ja käsitellä jokainen asianomaisen ryhmän jäsen. Tähän luokkaan kuuluvat hankkeissa ja projekteissa syntyneet tiedot. Kun kirjoitat opinnäytetyötäsi, niin sen yhteydessä syntynyt tieto on usein luottamuksellista ennen kuin se julkaistaan Metropolian kirjastossa.

Salassa pidettävä tieto

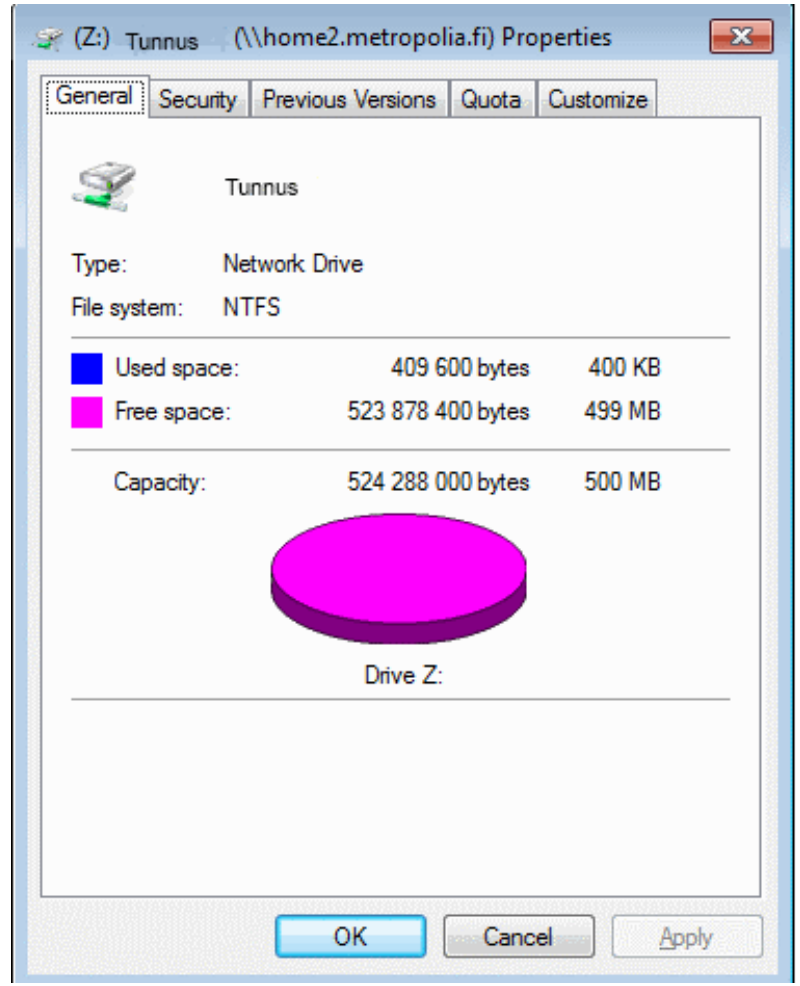
- Tietoa saavat käsitellä vain tietyt henkilöt. Lainsäädäntö asettaa tiettyjä velvoitteita tiedon käsittelemiseksi. Taloustieto ja arkaluonteiset henkilötiedot kuuluvat tähän luokkaa.

Lisätietoa tiedon luokittelusta löydät luokittelumallista.

Metropolia

Verkkolevyt Metropoliassa

Metropoliassa on käytössä useita eri verkkolevyjä, joiden käyttötarkoitukset tukevat eri tilanteiden tarpeita. Verkkolevyt ovat täysin Metropolian hallinnassa ja niistä otetaan varmuuskopioinnit tietohallintopalveluiden toimesta (pl. S-levy). Verkkolevyjen käytössä on kiinnitettävä huomiota seuraaviin asioihin: verkkolevyn käyttötarkoitus, tiedon luokitteluluokka ja tiedon käyttötarkoitus.



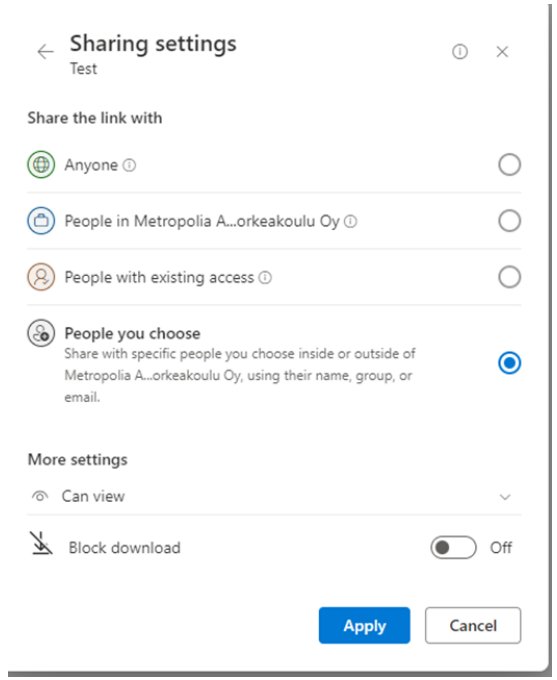
Z-levy on jokaisen opiskelijan henkilökohtainen kotihakemisto

- Levyllä saa käsitellä salassa pidettävää tietoa.
- Kansiossa on valmiiksi luotu Public html -kansio, joka on tarkoitettu julkiseen verkkoon julkaisemiseen. Älä käytä tätä kansiota tiedoston tallennuskansiona, vaan luo verkkolevylle uusi kansio henkilökohtaisia tiedostoja varten.
- Kun teet opinnäytetyötäsi Metropoliassa, niin hyödynnä tätä verkkolevyä, esimerkiksi haastattelujen tallentamiseksi ennen kuin olet anonymisoinut haastateltavien henkilötiedot.

Seuraavalla sivulla on tarkempi kooste verkkolevyjen käyttötarkoituksista.

Metropolia

Pilvipalveluiden



Metropolialla on käytössä Google Workspace for Education (esim. Google Drive ja Google Meet) & Microsoft Office 365 Education (esim. Microsoft OneDrive, SharePoint, Teams ja Stream) pilvipalvelut. Pilvipalveluiden käytössä tulee huomioida pilvipalveluiden käyttöehdot, jotka määrittävät palveluiden tallennuskäytännöt ja käyttötarkoitukset. Käyttäjät noudattavat pilvipalveluiden toimintaperiaatteita.

Muuta huomioitavaa

Kun jaat tiedostoja Googlen tai Microsoftin pilvipalveluista, niin noudata seuraavia käytänteitä.

- Kun jaat tiedoston tai kansion metropolialaiselle (henkilökunta, opiskelija, sidosryhmät yms.), käytä hänen Metropolian pilvipalvelutiliänsä, äläkä ulkopuolista sähköpostiosoitetta. Käyttöoikeus pilvipalveluihin on jokaisen metropolialaisen saatavilla.

- Kun jaat tiedoston tai kansion Metropolian ulkopuoliselle yhteistyökumppanille, käytä hänen oman organisaationsa (työpaikkansa tai oppilaitoksensa) sähköpostiosoitetta kuin vastaanottajan Gmail-osoitetta tai muuta henkilökohtaiseen käyttöön tarkoitettua sähköpostia.

- Älä jaa tiedostoja tai kansioita niin, että kuka tahansa linkin haltija pääsee niihin käsiksi (esim. Microsoftin pilvipalveluissa älä valitse Anyone with the link -toimintoa, vaan käytä Specific people tai People in Metropolia Ammattikorkeakoulu Oy with the link -toimintoja).

- Käytä Microsoftin pilvipalveluissa "Expiration date -toimintoa", jolla voi päättää linkin voimassaoloajan.

Metropolia

Tietoturvan yleisimmät uhkatermit

Käsite	Määritelmä
Uhka	Mahdollinen haitta tai kehityskulku, jota käytetään tietoisesti hyväksi. Uhka esitetään turvallisuudessa usein muodossa: *uhka = kyky + tahto*.
Tietoturvauhka	Uhka kohdistuu tietoon ja voi vaarantaa sen, kun haavoittuvaisuutta käytetään hyväksi.
Kyberuhka	Uhka kohdistuu kyberympäristöön ja voi vaarantaa sen, kun haavoittuvaisuuttaa käytetään hyväksi.
Haavoittuvaisuus	Alttius uhkille. Kuvaa mitä tahansa heikkoutta, jota tietoisesti voidaan käyttää hyödyksi. Haavoittuvaisuuksia on tietojärjestelmissä, prosesseissa ja ihmistoiminnassa.
Nollapäivähaavoit-tuvaisuus	Tietojärjestelmän haavoittuvaisuus ei ole palvelun tarjoajan tiedossa, mutta hyökkääjä tietää haavoittuvaisuudesta.
Hakkeri	Henkilö, joka tunkeutuu tai vaikuttaa tietoverkkoon, tietojärjestelmään tai niiden sisältämään tietoon ja käyttää ohjelma, palvelua tai muita resursseja. **Huomaa tarkoituksellinen haavoittuvaisuuden hyväksikäyttö!**

Mitä on tietojenkalastelu?

- Tietojenkalastelu eli verkkourkinta (eng. phishing) on tietotekniikassa esiintyvää rikollista toimintaa.
- Sen avulla pyritään saamaan haltuun luottamuksellisia tietoja, kuten henkilö- tai tilitietoja, esiintymällä tiedonsaantiin oikeutettuna tahona.
- Saatujen tietojen avulla voidaan pyrkiä saavuttamaan taloudellista hyötyä rikostoiminnassa.

Metropolia

Tyypillinen tietojenkalasteluoperaatio

1. Rikollinen lähettää tietojenkalasteluviestin sähköpostitse.

2. Vastaanottajaa avaa viestin ja seuraa linkkiä huijaussivustolle.

3. Linkki ohjaa hujaussivustolle, joka pyytää syöttämään käyttäjätunnukset ja salasanan.

4. Huijaussivustolta saadut käyttäjätunnus ja salasana ovat rikollisella.

5. Rikollisella pääsy organisaation sisäiseen tietoliikenteeseen.

6. Rikollinen pääsee käsiksi organisaation tieto-omaisuuteen, esim. näkemään laskutusliikennettä tai lukemaan käyttäjän sähköpostikeskustelua.

Metropolia

7. Rikollinen voi etsiä, esim. aitoja laskuja, joiden avulla muotoillaan aidon tuntuinen lasku, joka lähetään organisaatiolle —> uhri maksaa rikolliselle toivomansa summan huomaamattaan.

Tietojenkalastelumenetelmiä

Menetelmä	Määritelmä
Huijausviesti tai verkkourkinta (phishing)	Luottamuksellisen tiedon hankkimista sähköpostin tai väärien tietojen avulla.
Kohdistettu huijausviesti (spear phishing)	Suunnitelmallisempaa luottamuksellisten tietojen urkintaa sähköpostin välityksellä tai väärien tietojen avulla. Henkilö on tarkoituksella valikoitunut huijausviestin kohteeksi, esim. laajempien käyttöoikeuksien vuoksi.
Ylempien toimihenkilöiden huijaaminen (whaling)	Merkittävämpiin toimijoihin kohdistuneet tietojenkalastelut, esim. organisaation ylin johto tai yhteiskunnan merkkihenkilöt.
Palkinnolla houkuttelu (baiting)	Uhria houkutellaan käyttämään saastunutta kohdetta, joka voi olla muistitikku tai applikaatio.

Näin voit tunnistaa tietojenkalasteluviestin

Tietojenkalastelijat yrittävät painostaa kiireellisyyteen ja nopeaan reagoimiseen. Esimerkiksi tässä viestissä huomautetaan salasanan vanhenemisesta tänään.

1.

2.

Tässä esimerkissä tietojenkalastelun tunnistaa lähettäjän sähköpostista. Silti on huomioitava, että joskus tietojenkalastelija onnistuu lähettämään sähköpostin niin, että jopa lähettäjän osoite näyttää oikealta tai viesti on voinut tulla murretulta sähköpostitililtä. Siksi lähettäjän osoite voi näyttää myös aidolta, vaikka kyseessä olisi huijausviesti.

Viestin sisällön tarkastelu on tärkeätä Jos viestin sisällössä on jotain epäilyttävää, on noudatettava varovaisuutta.

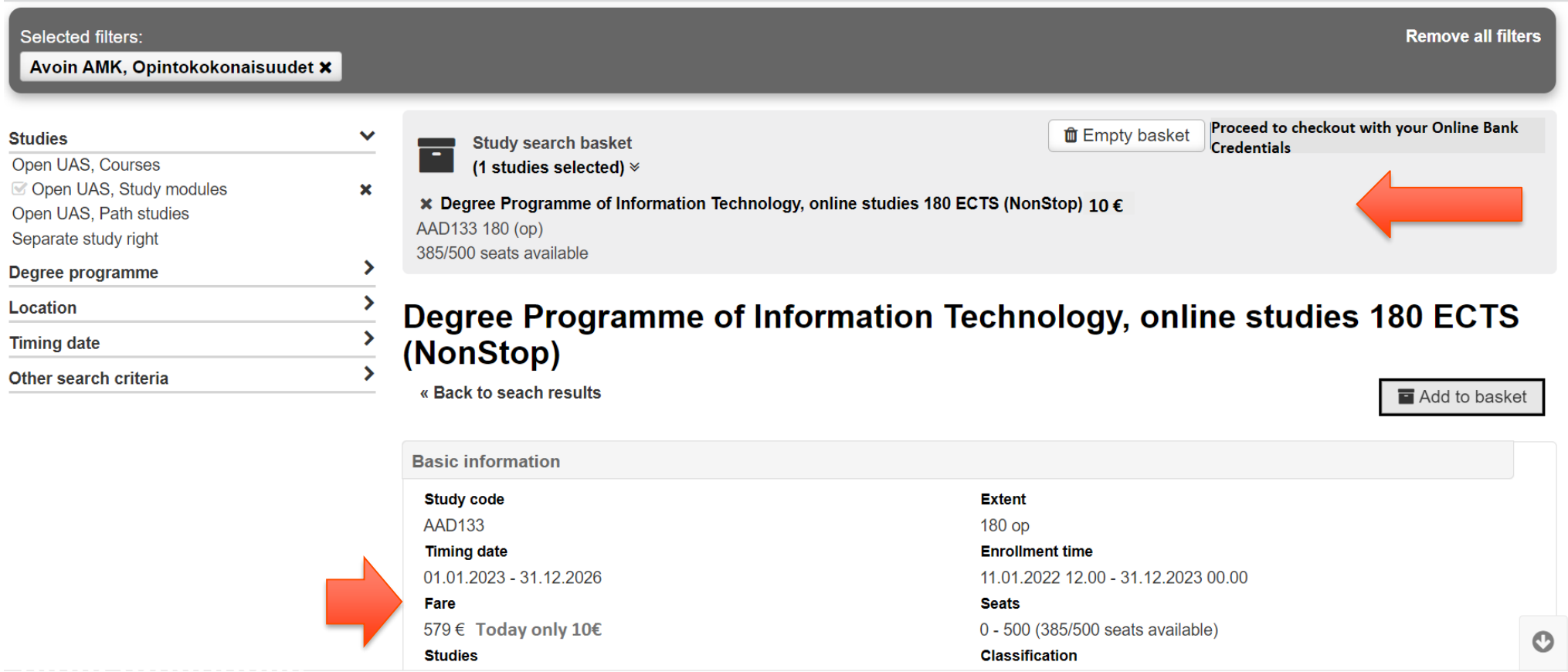
3.

4.

Hyvin usein tietojenkalasteluviestissä yritetään houkutella uhria klikkaamaan viestissä olevia linkkejä tekemällä niistä helposti huomattavia.

Metropolia

Kuinka suojautua nettihuijauksilta ja tietojenkalastelulta?



- Tutustu esimerkiksi verkkokaupan tarjouksen ehtoihin ja itse sivustoon. Älä syötä luottokorttitietojasi tai verkkopankkitunnuksiasi epäilyttävän oloiselle sivustolle harkitsematta.

Metropolia

Haittaohjelmat ja kyberhyökkäykset

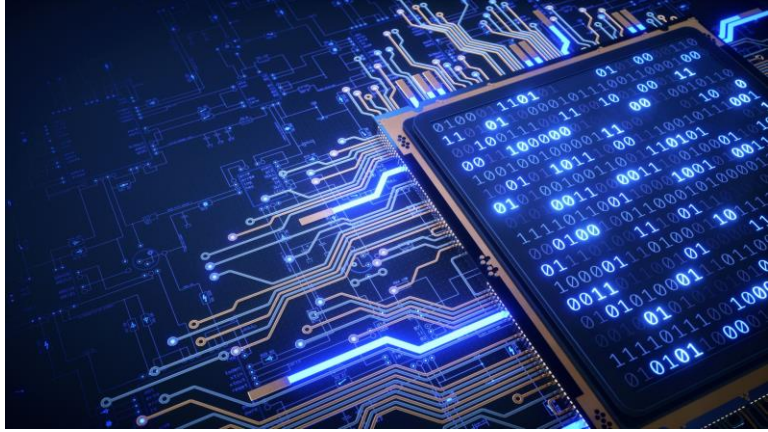
- Haittaohjelmalla hyökkääjä yrittää asentaa pahantahtoisen ohjelman organisaation tietotekniikkaa hyödyntävään järjestelmään.
- Haittaohjelmat nimensä mukaisesti viittaavat haitallisiin ohjelmistoihin (malicious software), jotka ovat tarkoituksella suunniteltu aiheuttamaan harmia organisaation tieto-omaisuudelle.
- Myös haittaohjelmia on eri tasoisia ja laatuisia.
- Tietojenkalastelua ja haittaohjelmia hyödynnetään kyberhyökkäyksessä, jotka kohdistuvat hyökkääjän havittelemaan tieto-omaisuuteen.
- Kyberhyökkäys tarkoittaa toimintaa, jolla pyritään verkkoympäristön tieto-omaisuuden oikeudettomaan käyttöön (esim. tunkeutumalla tietojärjestelmään) tai vahingoittamiseen (esim. tuhoamalla laitteita tai estämällä palvelun käyttö, esimerkiksi kuormittamalla verkkoliikennettä).
- Usein kohteeseen tunkeudutaan hyödyntämällä useita erilaisia kyberhyökkäysmenetelmiä, kuten tietojenkalastelua ennen haittaohjelman asentamista.
- Suunnitelmallisemmista kyberhyökkäyksistä puhutaan myös tietomurto-operaationa, jolla tarkoitetaan harkittua toimintaa tunkeutumisen tekemiseksi.
- Hyökkäys koostuu pääasiassa kolmesta vaiheesta:
    - Kohteen tiedustelusta
    - Kohteeseen tunkeutumisesta
    - Kohteen tieto-omaisuuden hyödyntämisestä

Metropolia

Haittaohjelmat ja niiden selitykset

Haittaohjelma	Määritelmä	Esimerkkejä
Virus (Virus)	Ohjelma, joka leviää tietokoneiden välillä ja monistaa itsensä ilman automaatiota.	*Brain, Iloveyou*
Mato (Worm)	Ohjelma, joka leviää tietokoneiden välillä ja monistaa itseään automaattisesti.	*Conficker, Slammer*
Vakoiluohjelma (Spyware)	Kerää ja lähettää tietoa käyttäjän huomaamatta kolmannelle osapuolelle.	*DaVinci, FinFisher*
Piilohallintaohjelma (Rootkit)	Ottaa verkon tai koneen hallintaansa.	*Uroburos*
Bottiverkko (Botnet)	Saastuneiden tietokoneiden muodostama verkko, jota hyökkääjä käyttää verkon kuormittamiseksi.	*Mirai*
Troijalainen (Troijans)	Naamioitu ohjelma, joka tekee tunkeutujan haluamia komentoja.	*Keymarble, Bandcall*
Kiristyshaittaohjelma (Ransomware)	Lukitsee tietokeen sisällön, niin ettei käyttäjä voi käyttää konetta. Kiristäjä pyytää lunnaita koneen vapauttamiseksi käyttäjältä.	*Petya, WannaCry*

Informaatiovaikuttaminen – tiedon ja tietämyksen muokkaamista



- Ihmiset haluavat vaikuttaa tietoon eli informaatioon joka voi olla hyvän- tai pahantahtoista.
  - Mainostamisella ja valistamisella yritetään muokata ihmiskäyttäytymistä, esim. liikkumaan enemmän tai syömään terveellisemmin.
- Verkottunut maailma on suonut myös uusia tapoja viestiä toiselle.
  - Pahantahtoisesta vaikuttamisesta puhutaan informaatiovaikuttamisena, jossa vaikutetaan kansalaisiin, päätöksentekijöihin ja toimintakykyyn ohjailemalla saatavilla olevaa informaatiota ja sen kulkua, esimerkiksi kansalaismielipiteen muokkaamiseksi.
- Perinteisellä medialla ei ole enää viestinnällistä monopolia – internet ja sosiaalinen media mahdollistavat laaja-alaisen levikin kenelle tahansa.

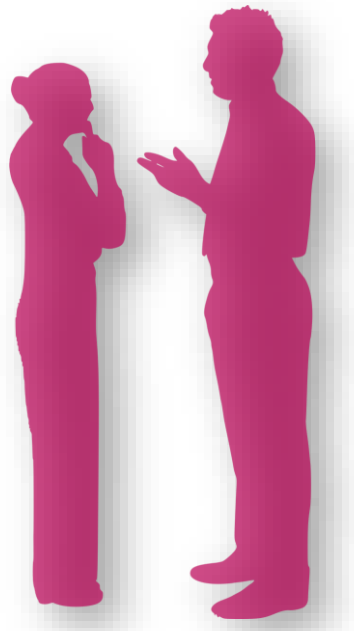
Metropolia

Sosiaalinen manipulointi ihmisten hakkeroimisena

- Social Engineering = käyttäjämanipulointi, sosiaalinen manipulointi, vaikuttaminen ja hämääminen —> tekniikka tai huijaus, jolla ihminen saadaan luovuttamaan tietoja vaikuttajalle.

- Huijaukset onnistuvat ihmisten erehdyksien ja hyväntahtoisuuden vuoksi.
  - Hyökkäyksen edellytyksenä on ihmiskäyttäytymisen ja psykologian ymmärtäminen.

- Miten käyttäjämanipulointia tehdään?
  - Kohde tunnistetaan ja hänestä kerätään tietoa.
  - Uhria lähestytään väärennetyllä henkilöllisyydellä ja keksityllä tarinalla.
  - Hyökkääjä yrittää saavuttaa uhrin luottamuksen ja toteuttaa hyökkäyksen.
  - Hyökkäys lopetetaan ja uhrin tietoa hyväksikäytetään.



Metropolia

Näin torjut eri manipulointitilanteita

Rauhoita tilanne

- Jos tilanne vaikuttaa kiireelliseltä tai sinua painostetaan, on tärkeätä pysähtyä hetkeksi harkitsemaan seuraavaa toimenpidettä. Huijarit pyrkivät kiireellisyyteen, jotta sinulla ei olisi aikaa miettiä asiaa perusteellisesti.

Tarkista oikeinkirjoitus

- Suurin osa kalasteluviesteistä, jotka ovat suomen kielellä, on käännetty käännösohjelman avulla. Silloin tekstistä voi löytyä kirjoitusvirheitä tai viestin rakenne voi olla huonosti kirjoitettua. Tämä voi viitata huijaukseen.

Mitä tietoa yhteydenottajalla on sinusta?

- Yhteydenotossa on hyvä huomioida mitä tietoa yhteydenottajalla on sinusta. Jos yhteydenottajalta puuttuu tieto, mikä hänellä ehdottomasti pitäisi olla, voi kyseessä olla tekaistu yhteydenotto.
- Harkitse, mitä jaat sosiaalisessa mediassa. Ammattilaiset hyödyntävät sosiaalista mediaa ja avoimia lähteitä kyberhyökkäyksen tiedusteluvaiheessa.

Pyydä yhteydenottajaa todistamaan henkilöllisyytensä

- Jos tuntematon henkilö yrittää rakennukseen sisään, esimerkiksi kantaen tikkaita, niin on häneltäkin varmistettava henkilöllisyys. Tikkaan kantaja voi yrittää hyödyntää ihmisten avuliaisuutta.

Onko tilanne realistinen?

- Realistisella ajattelulla tarkoitetaan sitä, että ymmärrät, mikä voisi oikeasti olla mahdollista ja, miksi se tapahtuisi.
    - Saat yllättävän työsähköpostin – mieti kuuluisiko minun saada sellainen?
    - Sinulle sanotaan, että voit lotossa– tiedät ettet ole kuitenkaan lotonnut viime aikoina.
    - Sinulle soittaa viranomainen ja pyytää tilitietojasi – viranomaiset lähettävät usein ilmoituksen asiakkaalle eivätkä soita suoraan hänelle ellei ole erikseen sovittu.

Metropolia

Metropolia-yhteisön ohjeet verkkomaailman uhkia vastaan 10 + 1 ohjetta

1. Ole terveen epäluuloinen – kysy riittävän usein miksi.
2. Harkitse, mitä tietoja jaat verkossa - kerran verkossa aina verkossa.
3. Varmista linkkien ja viestijän aitous – tiedä kommunikoijan identiteetti.
4. Huolehdi laitteidesi päivityksestä ja tietoturvasta – älypuhelimiin ja tietokoneisiin pätevät samat ohjeet pitkälti.
5. Laske kymmeneen raha-asioissa – rikolliset havittelevat pankki- ja henkilötietojasi.
6. Julkiset ja avoimet verkot ovat aina turvattomia – käytä VPN-yhteyttä, kun et ole tutussa verkossa.
7. Muista varmuuskopiointi – Älä kytke tuntemattomia laitteita, kuten USB-tikkua koneeseesi.
8. Käytä hyviä salasanoja ja salasanahallintasovellusta – ota käyttöön kaksivaiheinen tunnistautuminen, kun se on mahdollista.
9. Muista realistisuus kaikessa - jos jokin kuulostaa liian hyvältä ollakseen totta, se ei yleensä ole totta.
10. Verkkomaailmaa antaa enemmän kuin ottaa – älä pelkää siis turhaan.

+1 Huolehdi mahdollisuuksien mukaan muiden tietoturvasta esimerkiksi lastesi ja vanhempiesi.

Metropolia