Yliopisto-organisaation toimijoiden tietoturvatietoisuus

Lomaketutkimus Lapin yliopiston opiskelijoiden ja henkilöstön tietoturvatietoisuudesta ja tietoturvatietoisuuden tasojen eroista

Nooa Sarkkinen
Pro gradu -tutkielma
luokanopettajakoulutus
Lapin yliopisto
Kevät 2025

Yliopisto-organisaation toimijoiden tietoturvatietoisuustutkimus – Lomaketutkimus Lapin yliopiston tietoturvatietoisuudesta ja tietoturvatietoisuuden tasojen eroista

Nooa Sarkkinen
Kasvatustiede, luokanopettajakoulutus
Lapin yliopisto

Pro gradu -tutkielma, 72 sivua, 1 liite
Toukokuu 2025

Tutkielmassa selvitettiin Lapin yliopiston opiskelijoiden ja henkilöstön tietoturvatietoisuuden tasoa sekä tarkasteltiin rooli- ja tiedekuntakohtaisia eroja. Tutkimus on määrällinen ja aineisto kerättiin verkkokyselylomakkeella ja siihen vastasi 78 henkilöä. Tutkimus pohjautuu Parsons ym. (2013) kehittämään HAIS-Q tietoturvatietoisuusmittariin. HAIS-Q perustuu KAB-malliin, jonka perusteella tutkittavaa ilmiötä lähestytään tiedon, asenteen ja käyttäytymisen näkökulmista. Tieto, asenne ja käyttäytyminen toimivat myös tämän tutkimuksen keskeisinä tutkittavina muuttujina.

Aineiston vastaukset pisteytettiin ja niiden avulla muodostettiin tasoa kuvaavat prosenttiluvut. Alle 60 % tulos tarkoitti riittämätöntä tasoa, 60–80 % tulos tarkoitti riittävää tasoa ja yli 80 % tulos tarkoitti hyvää tasoa. Tutkimuksen vertailtavia vastaajaryhmiä olivat koko aineisto, tiedekunnat, opiskelijat, henkilöstö, tiedekunnan opiskelijat ja tiedekunnan henkilöstö. Tiedon, asenteen ja käyttäytymisen tuloksia ja niiden tunnuslukuja vertailtiin myös vastaajaryhmien välisesti.

Asenne oli tutkimuksen selvästi vahvin osa-alue ja käyttäytyminen selvästi heikoin. Koko aineiston asennemuuttujan keskiarvotulos oli 86,5 % eli hyvä, tietomuuttujan keskiarvotulos oli 69 % eli riittävä ja käyttäytymismuuttujan keskiarvotulos oli 59 % eli riittämätön. Henkilöstön tulokset olivat korkeammat kuin opiskelijoilla erityisesti asenteen ja käyttäytymisen osalta. Tietotaso oli henkilöstön ja opiskelijoiden välisesti sama. Tiedekuntien välisesti oikeustieteiden ja taidetieteiden tiedekunnat saavuttivat korkeimmat tulokset ja kasvatustieteiden tiedekunta oli selvästi heikoin. Yhteiskuntatieteiden tietoturvatietoisuuden taso oli matalampi kuin oikeustieteiden ja taiteiden tiedekunnilla, mutta korkeampi kuin kasvatustieteillä.

Tulokset viittaavat yleiseen tarpeeseen kehittää suurelta osin puutteelliseksi osoittautunutta tietoturvakäyttäytymistä. Koska tiedekuntien välisesti ilmeni suuria eroja, myös tiedekuntien tietoturvatietoisuuden tasoja tulisi kehittää kohdennetusti tiedekuntiin, joissa tietoturvatietoisuus oli selvästi heikompi. Tutkimusta voidaan hyödyntää yliopiston tietoturvakoulutuksen suuntaamisessa, seurannassa tai suunnittelussa. Jatkotutkimuksissa voisi selvittää tarkemmin syitä tietoturvatietoisuuden eroja ja kehittää kohdennettuja toimenpiteitä tietoturvakäyttäytymisen parantamiseksi.

Avainsanat:
tietoturvatietoisuus, HAIS-Q, yliopisto, käyttäytyminen, asenne, tieto, tietoturva

Sisällysluettelo

1. Johdanto

Yhteiskunta on digitalisaation ja teknologian kehityksen myötä muutostilassa, jossa toiminta ja apuvälineet ovat sitoutuneet osittain tai kokonaan tieto- ja viestintäteknologiaan. Kouluissa esimerkiksi opetusmateriaalit, kommunikaatio, johtaminen ja monet muut organisaation toiminnot perustuvat enenevissä määrin tieto- ja viestintäteknologiaan nojautuviin ratkaisuihin. Asioiden siirtyessä sähköisiin ratkaisuihin tietoturva nousee merkittäväksi osaksi jokaisen arkea.

Tietoturvan korostuneesta merkityksestä merkkejä ovat maailmanlaajuisesti kasvanut tietoturvauhka, uudet lainsäädännöt, määräykset tietosuojan ja tietoturvallisuuden parantamiseksi sekä yhdenmukaistamiseksi EU:ssa ja sen jäsenmaissa. Tietoturvaa käsitteleviä lakeja ja määräyksiä ovat esimerkiksi EU-komission määräämä NIS2-direktiivi, Suomen laki julkisen hallinnon tiedonhallinnasta (906/2019) ja EU:n GDPR-tietosuojalaki. NIS2-direktiivi on tämän tutkielman kirjoittamisen aikana ollut siirtymävaiheessa. Direktiivin alaisten organisaatioiden ja instituutioiden siirtymä on ollut määrä tulla valmiiksi syksyllä 17.10.2024.

Tutkielman aihe sai alkunsa tutkielman tekijän tietoturvakiinnostuksesta, mutta toisaalta myös tietoturvan ajankohtaisuudesta ja sen kasvaneesta merkityksestä. Motivaatio tutkielman tekemiseen perustui haluun perehtyä tietoturvaan tarkemmin ja lisätä ymmärrystä siitä koulutuksen kontekstissa. Tämä opinnäytetyö ei ollut pelkästään akateeminen suoritus, vaan samalla henkilökohtainen oppimisprosessi.

Tutkielman lähtökohdat rakentuivat korona-aikana alkaneen ohjelmointikiinnostuksen pohjalta, joka johti vaihto-opintoihin Norjaan opiskelemaan aihetta. Tietotekniikkakurssien joukkoon valikoitui kyberturvallisuuden kursseja ja koulun harrastustoiminnan kautta tarjoutui mahdollisuus osallistua kyberturvallisuuden *Capture The Flag* -tapahtumiin. Vaihto-opintojen aikaiset kokemukset, kyberturvallisuuskurssit ja kyberturvallisuuden harrastustoiminta loivat lähtökohdat tutkimukselle ja tutkijan positiolle.

Oppilaitoksen kyberturvaa käsitellään usein tietoturvan ja tietosuojan käsitteiden kautta ja siksi tutkielman keskeinen termi kyberturvallisuus tarkentui asteittain tietoturvaksi. Tietoturva ja kyberturva ovat käsitteinä lähellä toisiaan ja molemmat perustuvat

kolmelle periaatteelle, joita ovat tiedon luotettavuus, eheys ja saatavuus. Tietoturvan käsite päätettiin ottaa tutkielman keskeiseksi lähtökohdaksi kyberturvallisuuden sijaan.

Pro gradu -tutkielmassa tarkastellaan Lapin yliopiston (LAY) opetus- ja tutkimushenkilökunnan ja opiskelijoiden tietoturvatietoisuutta tiedon, asenteen ja käyttäytymisen näkökulmasta. Tutkimus on määrällinen ja siihen osallistuneiden vastaukset pisteytetään ja niistä muodostetaan tutkimuksen keskeiset tieto-, asenne- ja käyttäytymismuuttujat.

Tutkielman teemojen valintaan vaikutti digitalisoituvassa yhteiskunnassa tietoturvallisuuden merkityksen korostuminen. Kyse ei ole vain digitaalisen omaisuuden ja tiedon suojaamisesta, vaan kasvavasta vaatimuksesta kouluttaa organisaation henkilöitä ymmärtämään yksilön vastuu osana tietoturvan toteutumista. Organisaatioiden ja yhteiskunnan lisätessä digitaalisia ja tietoteknisiä palveluita tietoturvallisuuden riskit lisääntyvät ja tietoturvallisuuden vaatimukset laajenevat ja muuttuvat.

Tutkimus tukeutuu vahvasti Parsons ym. (2013) tietoturvatietoisuuden mittauksen *Human Aspect of Information Security Questionnaire* -apuvälineeseen (HAIS-Q). Oppilaitoksen tietoturvaa käsittelevä teoriarunko on rakennettu organisaation tietoturvaa ja tarkemmin oppilaitoksen tietoturvaa käsittelevästä kirjallisuudesta ja lähdeaineistosta. Tutkimuksen keskeisinä lähteinä on käytetty alan kirjallisuuden lisäksi yliopisto-organisaatioiden julkisia tietoturvadokumentteja, tietoturvalakeja ja asetuksia.

Tutkimuksesta saatua tietoa voidaan hyödyntää tulevaisuudessa tietoturvakoulutuksen suunnittelun ja suuntaamisen tukena. Toisena pyrkimyksenä on tuottaa tietoa tietoturvan arvioinnin ja sen seurannan tueksi.

2. Tietoturva oppilaitosorganisaatiossa

Tämän luvun alaluvuissa määritellään tietoturvan perusteet, jotka toimivat tutkielman aiheen pohjana. Näitä ovat luotettavuus, eheys ja saatavuus, joita käsitellään alaluvussa 2.1. Tietosuojaa ja tietoturvaa käsitellään usein rinnakkain, mutta niiden painopisteet eroavat toisistaan. Näiden käsitteiden eroavaisuuksista ja samankaltaisuuksista on kirjoitettu samassa alaluvussa. Organisaatioiden tietoturva on aina yksikkökohtaista riippuen sen ympäristöstä ja esimerkiksi käsiteltävän tiedon luonteesta. Oppilaitoksen tietoturva muistuttaa yleisesti organisaation tietoturvaa ja tätä aihetta avataan alaluvussa 2.2, jonka jälkeen alaluvussa 2.3 avataan tarkemmin yliopiston tietoturvan erityispiirteitä.

2.1 Tietoturvan perusteet

Tietoturvan käsite perustuu turvallisuuden käsitteeseen, joka tarkoittaa olotilaa, jossa turvallisuuden riskit ovat poissa tai hallinnassa. Sen saavuttamiseksi tietoturvallisuuteen sisältyy riskienhallintaa, joka tarkoittaa organisaatioon kohdistuvien uhkien ja haavoittuvuuksien tunnistamista, niiden todennäköisyyden ja vaikutuksen arviointia sekä toimenpiteiden suunnittelua riskien pienentämiseksi hyväksyttävälle tasolle. (Whitman & Mattord 2018, 255.) Riskienhallinnassa tulee huomioida sekä tekniset että inhimilliset tekijät, joka tarkoittaa esimerkiksi henkilöstön toiminnan ja ympäristön olosuhteiden huomioimista. Viimevuosina inhimilliseen tekemiseen on alettu kiinnittämään entistä enemmän huomiota (Sasse, Borstoff & Weirich 2001, 122).

Tietoturvan keskeiset elementit ovat luotettavuus (*confidentiality*), eheys (*integrity*) ja saatavuus (*availability*). Tiedon luotettavuuden, eheyden ja saatavuuden turvaaminen tarkoittaa tietojärjestelmien suojaamista luvattomalta pääsyltä, käytöltä, häirinnältä, paljastumiselta, muuttamiselta tai hävittämiseltä. (Turvallisuuskomitea 2018, 10 & 15.) Tietoturvan luotettavuus, eheys ja saatavuus toimivat keskeisenä viitekehyksenä tietoturvapolitiikan ja tietoturvatyön lainsäädännön, standardien ja käytänteiden suunnittelun ja arvioinnin perustana. Niiden näkökulmasta tietoturvaa voidaan lähestyä systemaattisesti. (Turvallisuuskomitea 2018, 10 & 15; Helsingin yliopisto.)

Tiedon luotettavuus tarkoittaa tiedon saatavuutta vain valtuutetuille ja luvan omaaville henkilöille, eikä tieto ole levinnyt valtuuttamattomalle toimijalle tai henkilölle, jolle tieto ei ole tarkoitettu. Salaaminen, käyttöoikeuksien hallinta ja käyttäjien tunnistaminen ovat esimerkkejä tietoturvaratkaisuista, joilla luottamuksellisuuden toteutumista tuetaan. Eheys tarkoittaa tiedon alkuperäisyyttä ja yhteneväisyyttä alkuperäisen tiedon kanssa koko tiedon elinkaaren ajan. Saatavuus tarkoittaa tiedon saumatonta hyödynnettävyyttä aikaan ja paikkaan katsomatta. Se tarkoittaa, että valtuutetuilla käyttäjillä on pääsy tietoon ja järjestelmiin silloin kun sille on tarve. (Turvallisuuskomitea 2018, 10 & 15; Whitman & Mattord 2018, 15–17.)

Tietoturva on näkökulma, jonka tavoite on suojata tietoaineistojen ja tietojärjestelmien eheyden, luotettavuuden ja saatavuuden lisäksi tietosuojan tavoitteita. (Tietosuojavaltuutetun toimisto; Turvallisuuskomitea 2018, 15 & 20). Tietosuoja on tietoturvaan lukeutuva osa-alue ja näkökulma, jonka painopisteet ovat yksilöiden tietosuojaoikeuksien toteutuminen ja henkilötietojen turvaaminen luvattomalta pääsyltä, käytöltä, käsittelyltä, paljastumiselta ja häviämiseltä. Tietosuojan näkökulma painottuu yksilön oikeuksiin henkilötietojen yksityisyydestä ja sen tarkoituksena on varmentaa henkilötietojen oikeutettu käsittely, kerääminen ja prosessointi sekä säilyttäminen asiaankuuluvasti. (Doering 2024.)

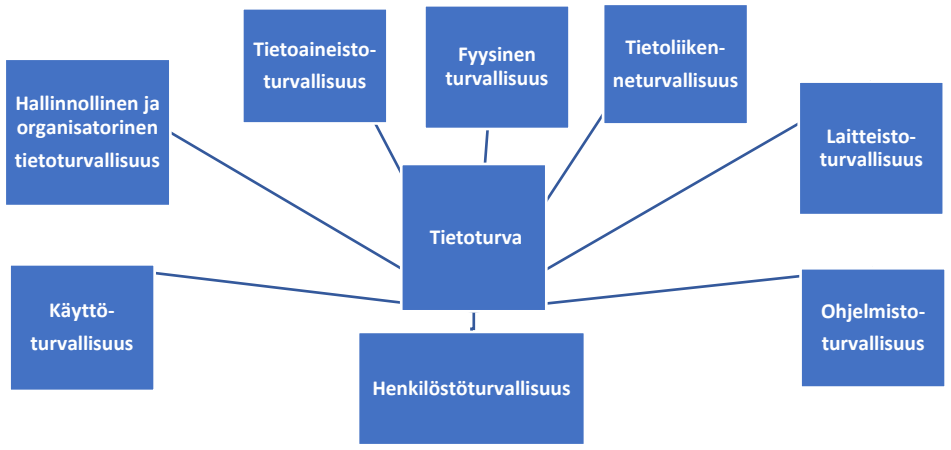
Tietosuoja on myös perusoikeus ja se pohjautuu jokaisen oikeuteen henkilötietojen suojasta. Suojattavia henkilötietoja ovat esimerkiksi tiedot, jotka voidaan liittää tunnistettavaan tai tunnistettuun luonnolliseen henkilöön. Henkilötietoja voi olla tallennettuna papereille, sähköisinä tiedostoina, kortistossa, mapeissa ja kuva- tai äänitallenteena. (Doering 2024; Tietosuojavaltuutetun toimisto.)

Tietoturvan ollessa kokonaisvaltainen näkökulma tiedon ja tietojärjestelmien suojaamiseksi, tietosuoja on puolestaan käytännön teknisiä, hallinnollisia ja fyysisiä toimintoja tietoturvauhkan pienentämiseksi tai poistamiseksi. Tietoturva huomioi esimerkiksi organisaatiodatan, immateriaaliomaisuuden ja yhtiösalaisuudet ilman yksilöllistä painotusta rekisteröidyn tietosuojasta. (Doering 2024.)

2.2 Yliopisto-organisaation tietoturvaympäristö

Opetushallituksen verkkosivujen mukaan oppilaitoksen tietoturva muistuttaa vahvasti organisaation tietoturvaa (Opetushallitus) ja se perustuu myös aikaisemmin mainittuihin tietoturvan kolmeen peruselementtiin, eli luotettavuuteen, eheyteen ja saatavuuteen. Tietoturvaan kohdistuvat uhat ovat ajan kuluessa kehittyneet laajoiksi tapahtumien ketjuiksi, eivätkä tietoturvan kolme periaatetta kykene yksinään vastaamaan nykypäivän muuttuviin tietoturvauhkiin. (Whitman & Mattord 2018, 11.)

Vastatakseen tietoturvauhkien muodostamiin riskeihin organisaation tietoturvan rakenne on kuvattu Jason ym. (2011, 17) teoksen Managing information security mukaan seuraavasti: organisaation tietoturvan osa-alueet koostuvat fyysisestä turvallisuudesta, dataturvallisuudesta, järjestelmä- ja verkkoturvallisuudesta, kommunikaatioturvallisuudesta, langattomasta turvallisuudesta, verkko- ja ohjelmistoturvallisuudesta, turvallisuuskäytänteistä ja -toiminnasta ja henkilöstöturvallisuudesta. Opetushallituksen verkkosivuilla sen osa-alueet on esitetty kuvan 1 mukaisesti.



Kuva 1. Organisaation tietoturva (Opetushallitus)

Tietoturvan merkitys on suuri organisaatiolle ja sen toiminnalle. Tietoturvan vaarantumisella voi olla monenlaisia suoria ja epäsuoria vaikutuksia kuten organisaatiotiedon vaarantuminen tai paljastuminen, henkilötietojen tai muun tiedon paljastuminen ja leviäminen valtuuttamattomille toimijoille, mutta merkittävänä vaikutuksena on myös,

että se heikentää organisaation julkista kuvaa, luotettavuuden perustaa ja voi keskeyttää tai estää toiminnan kokonaan. Korkea turvallisuuden taso voidaan saavuttaa motivoituneen ja hyvinvoivan henkilöstön avulla. (Valtionvarainministeriö 2007, 9.)

Organisaation suojattavat kohteet (*assets*) ovat mitä tahansa, jolla on jotakin arvoa tiedon omistajalle (Andress ym. 2014, 5). Suojattavat kohteet ovat yleisesti organisaation tai yhteiskunnan kannalta merkitykselliset kohteet, joita ovat niiden tietojärjestelmät, tieto, prosessit, fyysiset tilat, yksittäiset asiakirjat tai työasemat. (Turvallisuuskomitea 2018, 12).

Organisaatio turvaa tietonsa erilaisilla ehkäisytoimenpiteillä ja pyrkii estämään tiedon paljastumisen, väärän käytön, häiriköinnin, vahingollisen tai tahallisen tuhoutumisen tai peukaloinnin estämiseksi. Turvallisuuskomitean määritelmän mukaan tietoturvajärjestelyitä ovat myös esimerkiksi fyysisten tilojen lukitus, kulunvalvonta, asiakirjojen turvallinen hävitys ja säilytys, tiedon varmennustoimet, tiedon salaaminen, virustorjunta, palomuuri ja varmennekäytänteet. (Turvallisuuskomitea 2018, 11.)

Oppilaitosturvallisuuden näkökulmasta osa-aluejaottelut eivät ole yksiselitteisiä, sillä niissä ilmenee päällekkäisyyksiä, kuten henkilöstöturvallisuuden, tietoturvallisuuteen ja muiden osa-alueiden kesken. Koululaitoksille on suuri merkitys kriittisen data ja digitaalisen infrastruktuurin suojaaminen, koska koululaitokset ovat niistä erityisen riippuvaisia. (Rikander 2021, 49 & 51.)

Tietoturvakulttuuri on yksilöiden uskomusten, asenteiden ja tiedon vuorovaikutus, jonka tuloksena organisaation tietoturvallisuuden käyttäytymismallit rakentuvat. Toisin sanoen tietoturvakulttuurin luominen tarkoittaa organisaation tietoturvakäytänteiden sisältymistä osaksi automaattisia toimintatapoja. (Da Veiga, Eloff & Martins 2007, 149.)

Tietoturvakäytänteet ovat johdon määrittämiä tietoturvaohjeita ja tietoturvavaatimuksia organisaation työntekijöille (Koohang ym. 2022, 7). Tietoturvakäytänteet ovat dokumentti, jossa määritellään säännöt, odotukset ja kokonaisvaltainen lähestymistapa, jolla pyritään ylläpitämään yrityksen datan luottamuksellisuus, eheys ja saatavuus. Tietoturvakäytänteet esiintyvät yleisellä tai yksityiskohtaisella tasolla. Yksityiskohtaisesta tasosta esimerkkinä on langattoman verkon käyttöön liittyvät ohjeet ja käytänteet.

Tietoturvakäytänteiden voidaan ajatella vastaavan kysymyksiin “mitä” ja “miksi”. (Varonis.)

Tietoturvakäytänteet ja tietoturvakulttuuri ovat välittömässä yhteydessä tutkimuksen keskiössä olevan tietoturvatietoisuuden käsitteen kanssa. Tietoturvatietoisuus on riippuvainen yksilöllisistä tekijöistä, mutta myös organisaation tietoturvakäytänteistä ja organisaation tietoturvakulttuurista. (Parsons ym. 2017).

2.3 Yliopiston tietoturvan erityispiirteet

Yliopiston tietoturvallisuuden tehtävänä on huolehtia tietoturvan ja tietosuojan toteutumisesta. Henkilötietojen käsittelyn on lähes poikkeuksetta perustuttava lakiin. (Tampereen yliopisto.) Tieto on yliopistoille merkittävä voimavara. Yksi yliopiston perustehtävistä on tiedon tuottaminen ja tiedon tuottamisen lisäksi yliopisto käsittelee, säilyttää ja jakaa tietoa erilaisiin tarpeisiin organisaation sisäisesti sekä yhteiskunnallisesti. Sen takia tietoturva ja tietosuoja ovat yliopistolle erityisen tärkeitä. (Helsingin yliopisto.)

Suomen laissa määritellään yleiset reunaehdot tietotekniikkapalveluiden toteutukselle, ylläpidolle ja sen käyttäjille. Laeissa määritellään myös velvollisuudet ja oikeudet koskien palvelun tuottajia, ylläpitäjiä ja käyttäjiä. Lakien reunaehtojen lisäksi yliopisto määrittää tarkemmin yliopiston tärkeimmät strategiset painopisteet ja linjaukset tietoturvan osalta. (Helsingin yliopisto.)

Tiedon käsittely edellyttää tietotekniikkaa, johon liittyviä palveluita tietotekniikkakeskus yliopistolle tuottaa. Tietosuoja ja tietoturva on tästä huolimatta koko organisaation vastuu, johon henkilöstö ja opiskelijat toiminnassaan sitoutuvat. Tietoturvaa koskevia sääntöjä ja ohjeita noudattamalla edistetään koko organisaation erilaisten tietojen turvaamista. (Helsingin yliopisto.)

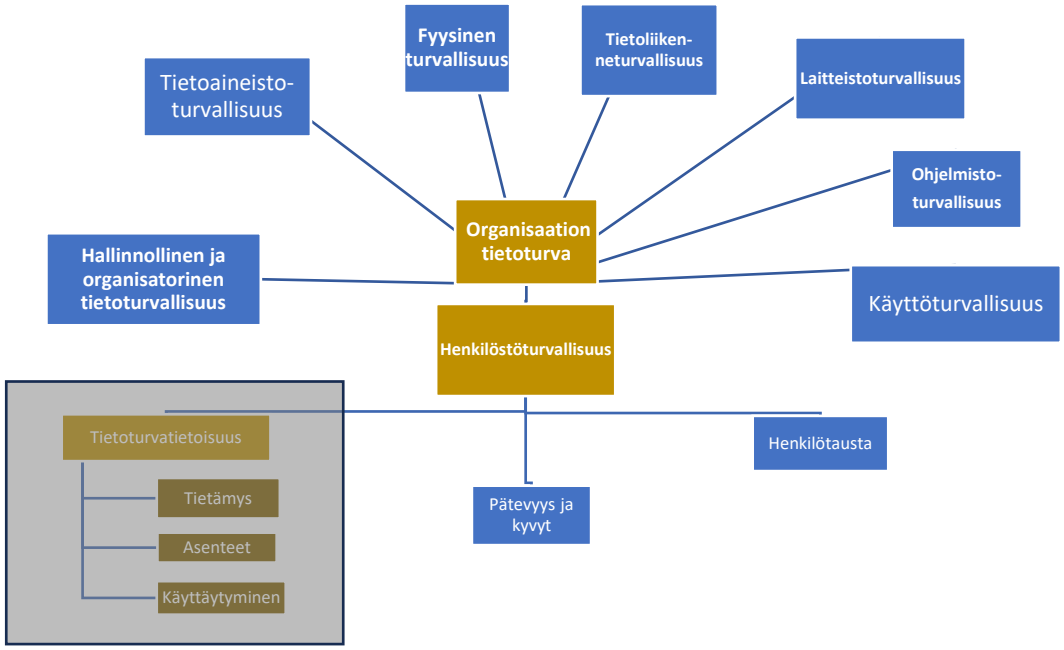
Tietoturvasta on huolehdittava koko tiedon elinkaaren ajan ja tietoturvasta tulee huolehtia tiedon olomuodosta ja käsittelyvaiheesta riippumatta aina. Tietosuojasta huolehtimalla edistetään koko yliopisto-organisaation yksityisten tietojen ja henkilötietojen suojaamista. (Helsingin yliopisto.)

Yliopistoja koskevia tietoturvallisuuden riskejä ovat yleisesti tietojärjestelmien, tietoaineistojen ja palveluiden luottamuksellisuuden vaarantuminen, jolloin tietojärjestelmien ja tietojen käyttö paljastuu valtuuttamattomille ja käyttöoikeuksien ulkopuolisille henkilölle tai toimijoille. Sivullisten mahdollisuus tietojen käsittelyyn, muuttamiseen tai poistamiseen tulee olla estetty. (Tampereen yliopisto.)

Tietojen ja järjestelmien oikeutettujen käyttäjien tulee toimia asianmukaisesti tehtäviinsä nähden. Järjestelmien, tietojen ja palveluiden on oltava luotettavia, oikeita ja ajan tasalla. Tieto ja tietojärjestelmät eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, laitteisto- tai ohjelmistovikojen, haittaohjelmien tai muiden vahinkojen, häiriötilanteiden tai tapahtumien seurauksena. (Tampereen yliopisto.) Toisin sanoen tietojärjestelmät ja tietoaineistot tulee olla suojattuna tahattomilta ja tahallisilta uhilta.

3. Henkilöstöturvallisuus ja tietoturvatietoisuus

Tämän luvun alaluvuissa perehdytään tarkemmin organisaation tietoturvan henkilöstöturvallisuuden osa-alueeseen ja henkilöstöturvallisuuden osalta painopisteenä on tietoturvatietoisuus. Kuva 2 esittää henkilöstöturvallisuuden asemaa osana organisaation tietoturvaa. Kuvassa on eriteltynä ja korostettuna tälle tutkielmalle tärkeä käsite eli tietoturvatietoisuus, joka on osa henkilöstöturvallisuutta. Tietoturvatietoisuuden lisäksi henkilöstöturvallisuuteen kuuluvat myös henkilötausta sekä pätevyys ja kyvyt.



Kuva 2. Organisaation tietoturva, henkilöstöturvallisuus ja tietoturvatietoisuus (Parsons ym. 2017, 47-48; Opetushallitus)

Kuvan 2 tarkoituksena on auttaa ymmärtämään tutkielman tietoturvatietoisuuden painopistettä ja sen osuutta organisaation tietoturvan aihealueella. Tietoturvatietoisuutta voidaan määritellä monella eri tavalla, mutta tutkielmassa tietoturvatietoisuuden tutkimisen näkökulmana käytetään Parsons ym. (2013) käyttämää tiedon, asenteen ja käyttäytymisen näkökulmaa ja se on korostettu kuvassa harmaalla värillä.

3.1 Ihmisperäinen turvallisuuselementti

Ihmisperäinen turvallisuus on koulutuksen kontekstissa tärkeässä roolissa henkilöstön työkuvien sisältäessä erilaisten tietojen käsittelyä ja hallinnointia, kuten esimerkiksi henkilötietoja ja tutkimustietoa. Edellä mainitut tekijät muodostavat tietoturvaa koskevat vaatimukset organisaation henkilöstölle tietoturvatietoisuudesta ja sen osaamisesta. Kouluttamalla ja ohjeistamalla henkilöstöä tietoturvatietoisuuteen voidaan ehkäistä ihmisperäistä turvallisuusriskiä (Andress 2011, 120 & 121; Kyberturvallisuus 1, inhimilliset tekijät).

Henkilöstön taustat, kyvyt, toiminta ja niistä johtuvat turvallisuustekijät lukeutuvat ihmisperäiseen turvallisuuselementtiin, joka on yksi merkittävimmistä riskitekijöistä (Valtionvarainministeriö 2008, 12; Andress 2011, 120). Tietomurroista 23 % johtuu ihmisperäisestä virheestä ja Verizonin tietomurtoraportin mukaan tietomurroista 85 % koski ihmisperäistä turvallisuutta (Varonis; Verizon). Ihmisen rooli on aina ollut ja tulee aina olemaan merkittävin tekijä tietomurroissa (Gardner & Thomas 2014, 1).

Ihmisperäisen turvallisuuselementin riskejä ovat organisaation sisäinen inhimillinen virhe (*unintentional*), organisaation sisäinen vahingollinen toiminta (*intentional*), käyttäjän manipulointi (*social engineering*), tietojenkalastelu (*phishing*), ja muu (*other*) (Malinen 2021, 6). Turvallisuusalan ammattilaiset käyttävät merkittävän määrän aikaa rakentaakseen turvallisuuden tasoja. Sähköpostifiltterit, välitinpalvelimet, palomuurit ja muut teknologiat säädetään ympäristöjen turvallisuuden optimoimiseksi. Yksittäisen henkilön toiminta voi mitätöidä koko turvallisuusjärjestelyn yhdellä klikkauksella. Tätä turvallisuuden riskiä ja turvallisuuden osa-aluetta kutsutaan ihmisperäiseksi turvallisuuden elementiksi. (Andress 2011, 120; Kyberturvallisuus 1, Inhimilliset tekijät.)

Henkilöstöturvallisuus tarkoittaa henkilöstöstä johtuvien riskien hallintaa. Se koostuu työntekijöiden suojaamisesta rikoksilta ja onnettomuuksilta, toiminnalle kriittisten henkilöresurssien varmistamisesta ja toiminnan ennakoivasta suojaamisesta (Elinkeinoelämän keskusliitto 2016, 10 & 11). Henkilöstöturvallisuuden riskit voivat olla tahallisen tai tahattoman toiminnan riskejä. Tahallisen toiminnan riskiä pyritään hallitsemaan turvallisuustarkastusten ja auditointien avulla, kun taas tahattoman ihmisperäisen tietoturvariskin hallinta tapahtuu henkilöstön tietoturvatietoisuuden lisäämisen

kautta. (Andress 2011, 120.) Henkilöstöturvallisuus vaikuttaa tietoturvaan konkreettisesti, koska henkilöstö toimii tiedon välittömässä läheisyydessä. Henkilöstö käsittelee tietoa muokkaamalla, vastaanottamalla, tallentamalla, välittämällä ja tuhoamalla sitä, sekä vastaa kollektiivisesti tietojärjestelmien ja tietovarastojen ylläpidosta. (Valtionvaraministeriö 2008, 12.)

3.2 Tietoturvatietoisuus

Tietoturvatietoisuus on suomen kielen käännös englanninkielisestä käsitteestä (*information security awareness, ISA)* ja se lukeutuu osaksi henkilöstöturvallisuutta aikaisemmin esitetyn kuvan 2 osoittamalla tavalla. Se ilmentää tietoturvatietoisuuden lisäksi myös koko tutkielman aihealueen kontekstia.

Tietoturvatietoisuutta määritellään pääsääntöisesti kahden näkökulman mukaan. Merkityksellistä on, missä viitekehyksessä määrittely tapahtuu ja millaisia vaatimuksista siihen sisältyy. (Parsons ym. 2017, 41; Mäkinen 2022, 15.) Näkökulmien eroavaisuutena on, nähdäänkö tietoturvatietoisuus kykynä ymmärtää tietoturvan merkitystä ja siihen liittyviä käytänteitä, vai sisältyykö tietoturvatietoisuuteen myös käyttäytymistä. (Wilson & Hash 2003, 28–29; Hadlington, Popovac, Janicke, Yevseyeva & Jones 2019, 41–48.)

Tietoturvatietoisuus tarkoittaa huomion suuntaamista tietoturvaan. Se on tila, jossa yksilö on tietoinen tietoturvallisuudesta ja on sitoutunut toteuttamaan tietoturvallisuuden tavoitteita. Tietoturvatietoisuuteen vaikuttamalla vahvistetaan ymmärrystä hyvistä turvallisuuskäytänteistä ja turvallisista toimintatavoista. Käytänteet ja toimintatavat koskevat esimerkiksi tietokoneen ja internetin käyttöä, etätyökäytänteitä ja muita käytänteitä, joiden tavoitteena on hallita ja suojata organisaation tietoja (NIST 800-50 2003, 8–9; Gardner & Thomas 2014, 1; Kruger & Kearney 2006, 289–290.) Heikko tietoturvatietoisuus voi aiheuttaa uhkaa koko organisaatiolle.

Jotta organisaatiot kykenevät suojaamaan tiedon luottamuksellisuutta, eheyttä ja saatavuutta, kaikkien on osallistuttava tietotekniikan turvalliseen käyttämiseen ja hallinnointiin. NIST SP 800-50 standardissa käsitellään tietoturvatietoisuuden vaatimuksia

kolmessa osassa. Ensimmäinen on oman roolin ja vastuun ymmärtäminen organisaation tehtävässä. Toinen on tietoturvakäytänteiden, -toimintojen ja proseduurien ymmärtäminen ja riittävä tietämys vaadittavista ja saatavilla olevista hallinnointikäytänteistä. Kolmas osa on ymmärrys toiminnallisista käytänteistä ja teknisistä kontrollointimenetelmistä tietotekniikan resurssien suojaamiseksi, joista itse on vastuussa. (NIST SP 800-50.)

Tietoturvatietoisuuden vaatimukset määrittyvät organisaatiokohtaisesti. Tietoturvadokumentit määrittävät organisaation omat tietoturvavaatimukset tarkemmin. Asiakirjoja, joissa vaatimuksia määritellään ovat tietoturvasuunnitelmat, tietoturvapolitiikka, tietoturvakäytänteet ja tietoturvaohjeistukset. Kansainvälisen tietoturvastandardin (ISO/IEC 27001, 2013) mukaan organisaation henkilöstön ja sidosryhmien tulee olla tietoisia tietoturvakäytänteistä, yksilön vastuusta tietoturvan toteutumisessa ja tietoturvan ja tiedonhallinnan vaatimusten noudattamatta jättämisen seurauksista. Tietoturvakäytänteiden tulee olla saatavilla dokumentoituna, käytänteet tulee välittää organisaation sisäisesti ja niiden on oltava saatavilla asiaankuuluville henkilöille ja toimijoille. (ISO/IEC 27001, 2013.)

3.3 Tietoturvatietoisuuden mittari HAIS-Q

Human Aspect of Information Security questionnaire (HAIS-Q) on mittari, jonka avulla voidaan mitata tietoturvallisuuden kontekstissa ihmisperäistä tietoturvan ulottuvuutta. Alkujaan se kehitettiin tietoturvatietoisuuden mittausvälineeksi mittaamaan yksilöiden välisiä eroja tietoturvaa koskevista tiedoista (*knowledge*), asenteista (*attitude*) ja käyttäytymisistä (*behaviour*). (Butavicius ym. 2016, 3.)

HAIS-Q on apuvälineenä rakennettu KAB-kyselymallin pohjalta, joka on lähtöisin terveysalan tutkimuksesta. KAB-kyselytutkimuksen tarkoituksena on olla edustava tutkimus, jonka tavoitteena on tuoda tietoisuuteen mitä tiedetään, mitä uskotaan ja miten toimitaan valitun tutkimusaiheen kontekstissa. KAB-mallissa tietoa kerätään itse hallinnoiduilla tai tiedon kerääjän hallinnoimilla puolistrukturoiduilla tai strukturoiduilla kyselylomakkeilla. (Andrade, Menon, Ameen & Praharaj 2020).

HAIS-Q:n ydinkomponentit ovat kuvan 3 mukaisen KAB-mallin tieto, asenne ja käyttäytyminen. Tieto tarkoittaa tietoturvallisuuden kontekstissa yksilön ymmärrystä periaatteista, käytänteiden, sääntöjen, ohjeiden ymmärtämistä ja tietoisuutta mahdollisista uhista ja vaaroista. Asenne tarkoittaa yksilön uskomuksia, suhtautumista ja ennakkooletuksia tietoturvaa ja sen käytänteitä kohtaan. Käyttäytyminen tarkoittaa ulkoisesti havaittavaa toimintaa, kuten tietoturvakäyttäytymistä ja tietoturvan noudattamista yksilötasolla. Tiedot vaikuttavat asenteisiin ja käyttäytymiseen, jolloin hyvän tietämyksen omaavat yksilöt tekevät parempia päätöksiä tietoturvallisuutta koskien. (Parsons, ym. 2014, 166 & 167; Schrader & Lawless 2004, 10; Parsons ym. 2017, 48.)

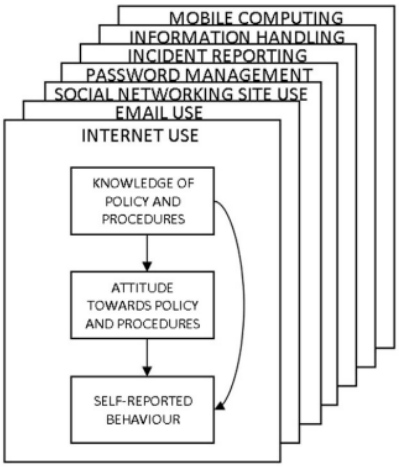
Kuva 3. KAB-mallin soveltaminen HAIS-Q tietoturvatietoisuus kyselyyn (Parsons ym. 2017, 48)

Parsons ym. (2017, 48) mukaan yksilön tietoturvatietoisuuteen vaikuttavat kolme rakenteellista tekijää. Näitä ovat yksilölliset muuttujat (*individual factors*), organisatoriset muuttujat (*organisational factors*) ja välilliset muuttujat (*intervention factors*) ja ne on esitetty osana kuvaa 3. Yksilölliset tekijät tarkoittavat psykologisia ja demografisia tekijöitä, kuten persoonallisuutta, aikaisempia kokemuksia tietojärjestelmistä, yleistä tietoturvatietoisuutta ja minäpystyvyyttä. Organisatoriset tekijät tarkoittavat organisaatiokulttuuria, esimerkiksi palkitsemista tai rangaistusta, sekä sosiaalisia normeja, kuten kollektiivista tietoturva-asennoitumista ja -käyttäytymistä. Välilliset tekijät tarkoittavat

tietoturvakoulutusta, organisaation viestintää ja tietoturvaharjoituksia. (Parsons ym. 2017, 48; Mäkinen 2022, 27 & 42.)

HAIS-Q:n avulla voidaan saada kokonaisvaltaisempi ymmärrys ihmisperäisen tietoturvaelementin heikkouksista ja vahvuuksista turvallisuusjärjestelmän sisällä. HAIS-Q:a voidaan käyttää apuvälineenä määrittämään organisaation henkilöstön tietoturvaosaamisen tasoa, tunnistamaan koulutustarpeita, arvioimaan kehittymistä ja ymmärtämään laajempaa turvallisuuden kehityksen suuntaa. (Parsons ym. 2014, 34.) HAIS-Q korostaa ihmisperäistä turvallisuuden näkökulmaa kasvavan tietoturvauhan alueella.

HAIS-Q mittaa seitsemää tietoturvatietoisuuden osa-aluetta, jotka on esitetty kuvassa 4. Mitattavia tietoturvatietoisuuden osa-alueita ovat salasanan hallinta, sähköpostin käyttö, internetin käyttö, sosiaalisen median käyttö, mobiililaitteet, tiedonkäsittely ja tapaturmaraportointi. (Butavicius ym. 2016, 3.) Kategoriat jaetaan edelleen KAB-mallin mukaisesti, jolloin ihmisperäisestä turvallisuuselementtistä saadaan tietoa eri näkökulmista. (Parsons ym. 2013, 34.)



Kuva 4. HAIS-Q mittarin osa-alueet ja jaottelu KAB-mallin mukaisesti (Parsons ym. 2017, 49)

HAIS-Q mittari vaatii soveltamista käytettävään ympäristöön. Tutkielmassa tietoturvasääntöjen, -käytänteiden ja -ohjeiden perustana toimivat HAIS-Q apuvälineen valmiit kysymykset ja Lapin yliopiston omat tietoturvaa käsittelevät julkiset dokumentit. Näitä

dokumentteja ovat henkilöstön tietoturvaopas, henkilöstön tietoturvan pikaohje, henkilöstön mobiiliturvaohje, opiskelijan tietoturvaopas, opiskelijan tietoturvan pikaohje, opiskelijan mobiiliturvaohje, Lapin yliopiston IT-palveluiden käyttösäännöt, Lapin korkeakoulukonsernin tietoaineistojen käsittelyohje, tietoaineistojen turvaluokitus IT-järjestelmissä, Lapin yliopiston sähköpostisäännöt ja Lapin yliopiston tietoturvapolitiikka. Lisäksi tietoturvakysymyksiä on rakennettu Tampereen yliopiston pakollisen kurssin ”Korkeakouluyhteisön tietoturva- ja tietosuojakoulutus” sisällöstä.

Mittarin tuottamia tietoja prosessoidaan taulukko-ohjelmilla ja lopuksi esitetään grafiikoina. Tuloksia jaotellaan kolmeen kategoriaan Kruger & Kearney (2019, 293) käyttämän asteikon hyvä, riittävä ja riittämätön mukaan. Tietoturvatietoisuuden skaala on luotu tietoturva-asiantuntijoiden näkemysten ja heidän toteuttaman tietoturvatietoisuustutkimuksen pohjalta. (Kruger & Kearney 2019, 293-294.)

4. Tutkimuksen toteutus

Tässä luvussa esitetään tutkimuksen toteutuksen osat kokonaisuuksittain. Luku alkaa tutkimuksen tarkoituksen ja tutkimuskysymyksien esittelystä, jonka jälkeen esitetään tutkimuksen filosofista taustaa ja siihen perustuvia metodologisia valintoja. Aineiston keruu toteutettiin kyselylomakkeella, jonka rakenteista ja rakentamisesta on kerrottu alaluvussa 4.3. Kyselylomakkeella kerätty aineisto kuvataan alaluvussa 4.4 ja aineiston analyysi ja sen perusteet avataan alaluvussa 4.5. Alaluvut on pyritty rakentamaan siten, että sen avulla lukija saa tarkan käsityksen tutkimuksen perusteista, rakenteista, valinnoista ja tutkimuksen etenemisestä.

4.1 Tutkimuksen tarkoitus ja tutkimuskysymykset

Tutkimusongelman rajaaminen alkoi kysymyksestä, onko tietoturvatietoisuus objektiivinen mitattavissa oleva ilmiö vai onko se kontekstisidonnainen ja ihmisten rakentama käsite. Tässä tutkimuksessa tietoturvatietoisuus on määritelty objektiiviseksi, kontekstisidonnaiseksi, olemassaolevaksi ja mitattavaksi ilmiöksi.

Tutkimuksen tarkastelun kohteeksi on valittu Lapin yliopiston (LAY) opetus- ja tutkimushenkilöstö ja sen opiskelijat. Tietoturvatietoisuuden tarkastelussa on käytetty tiedon, asenteen ja käyttäytymisen näkökulmaa. Tarkastelun painopisteeksi muodostettiin tietoturvatietoisuudesta rakennetut tasot ja niiden erot ja yhtäläisyydet vastaajaryhmien välillä. Lisäksi tutkimuksella pyritään tuottamaan käyttökelpoista tietoa, jota voidaan hyödyntää organisaation tietoturvatietoisuuden kehittämisessä. Toissijaisena tavoitteena on pyrkimys tuottaa tietoa tietoturvatietoisuuden arvioinnin ja seurannan tueksi. Tietoturvatietoisuuden kehityksen arvioimiseksi tietoturvatietoisuutta tulee mitata systemaattisesti ja on oleellista tarkastella sen muutosta.

Opiskelijat ja henkilöstö määrittyvät tässä tutkimuksessa henkilöstöturvallisuuden näkökulmasta organisaation sisäisiksi yksilöiksi. Keskeisin ero opiskelijoiden ja henkilöstön välillä on eriävät tietoturvavaatimukset. Henkilöstön työtehtävät sisältävät opiskelijoihin verrattuna poikkeavasti tiedon käsittelyä ja arvosanojen ja postituslistojen hallinnointia. Vastuu työpaikan tarjoamista henkilökohtaisista työlaitteista kuuluvat sen

käyttäjille. Edellä mainitut esimerkit ilmentävät, että henkilöstöön kohdistuvat tietoturvavaatimukset ovat myös yleisesti laajemmat kuin opiskelijoilla.

Tutkimuksella pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Millainen on tietoturvatietoisuuden taso Lapin yliopistossa?
  - Millainen tietoturvatietoisuuden taso Lapin yliopiston opiskelijoilla ja henkilöstöllä on?
  - Millaisia eroja ja yhtäläisyyksiä tietoturvatietoisuuden tasoissa ilmenee Lapin yliopistossa roolien ja tiedekuntien välillä?

Ensimmäisen tutkimuskysymyksen tarkoituksena on rakentaa lähtökohdat tietoturvatietoisuuden tarkastelemiseksi. Toinen ja kolmas tutkimuskysymys on suunniteltu tarkastelemaan ensimmäisen tutkimuskysymyksen avulla tuotettua dataa tietoturvatietoisuudesta suhteessa vastaajien taustamuuttujiin. Tiedekunta ja organisaatiorooli on valittu tutkimukselle tärkeiksi taustamuuttujiksi.

4.2 Tutkimusfilosofia ja metodologiset valinnat

Tutkimuksen metodologia vaatii tiedon ja todellisuuden luonnetta koskevien tieteellisen maailmankatsomuksen ja näkökulmien rajaamisen, joiden pohjalle tutkimuksen menetelmälliset valinnat perustuvat. Tieteessä samanaikaisesti voi vaikuttaa jopa toisilleen vastakkaiset tieteenfilosofiat. (Jyväskylän yliopisto.) Tutkimus nojautuu suurelta osin postpositivismiin, jolle luonteenomaista ovat määrällisyys ja oletus siitä, että tutkittava ilmiö on objektiivisesti mitattavissa.

Tutkimuksen tutkimusongelma perustuu postpositivistiseen näkökulmaan, jolloin tutkittavan ilmiön ajatellaan olevan luonteeltaan välittömästi ja objektiivisesti mitattavissa oleva asia. Postpositivismissa, kuten tässä tutkimuksessa, pyritään ilmiön objektiiviseen tarkasteluun. Postpositivistisessa tieteen suuntauksessa kuitenkin tunnistetaan, että tutkijan arvot, hypoteesit, teoriat ja taustatiedot vaikuttavat siihen, mitä tutkimuksessa havaitaan. Postpositivismi perustuu kriittiselle tarkastelulle ja tutkimusprosessin toistettavuudelle. Se mahdollistaa tilastollisen analyysin, hypoteesien testaamisen ja tiedon luotettavuuden arvioinnin. (Guba & Lincoln 1994, 110; Jyväskylän yliopisto.)

Postpositivismin lisäksi tutkimuksella on yhtymäkohtia relativismin eli suhteellisuusajattelun kanssa, jolloin tietoon ja totuuteen vaikuttaa ympäristö, jossa ilmiötä tarkastellaan. Tutkimuksessa ympäristön vaikutus otetaan huomioon rakentamalla mittarin sisältö tutkittavan organisaation ympäristön vaatimuksien pohjalta. (Guba & Lincoln 1994, 110; Jyväskylän yliopisto.)

Määrälliselle tutkimukselle tyypillisiä piirteitä ovat esimerkiksi mittaaminen, tiedon strukturointi, tiedon esittäminen numeroilla, objektiivisuus ja vastausten suuri lukumäärä. Näiden piirteiden tavoite on vertailla ja selittää tutkittavaa ilmiötä. (Vilkka 2007, 13 & 21.) Vertailevalle tutkimukselle soveltuvia aineistonkeruumenetelmiä ovat postikyselyt, internetkyselyt, haastattelulomake tai havainnointi, kun taas selittävälle tutkimukselle sopivia tutkimustapoja ovat strukturoitu postikysely tai internetkysely. (Vilkka 2007, 11, 19 & 25.) Näiden ominaisuuksien takia verkossa toteutettava kyselylomake soveltuu tämän tutkimuksen aineistonkeruumenetelmäksi ja se soveltuu laajan kohderyhmän tavoittamiseen ajasta ja paikasta riippumatta (Vilkka 2007, 28).

Lomaketutkimus on tyypillinen menetelmä määrälliselle tutkimukselle ja se soveltuu aineistonkeruumenetelmäksi suurelle vastaajajoukolle (Dillman 2000). Lomaketutkimus rakentuu strukturoiduista ja suljetuista kysymystyypeistä. Havainnointi ja mittaaminen tapahtuu suoraan tai välillisesti, jolloin voidaan puhua empiirisestä tutkimuksesta (Luokkanen & Turunen 2019, 32).

Lomaketutkimusta käytetään laajasti tietoturvatietoisuusmittauksen menetelmänä. Kyselytutkimus perustuu ilmiöiden, tapahtumien tai ominaisuuksien esiintymisen, yleisyyden, jakautumisen tai vuorovaikutuksen selvittämiseen. Kyselytutkimuksen avulla kerätystä aineistosta muodostetaan yleinen kuva muuttujista ja niiden välisistä suhteista. (Jyväskylän yliopisto.) Kyselytutkimukselle tyypillisiä kohteita ovat henkilöt ja heidän mielipiteensä, asenteet, ominaisuudet ja käyttäytyminen. (Vilkka 2007, 28.)

Kyselytutkimuksessa mittari merkitsee väitteiden ja kysymysten joukkoa, joiden tarkoituksena on mitata moniulotteisia ja erilaisia ilmiöitä. Mittareina voidaan käyttää valmiita mittareita, niitä voidaan rakentaa itse tai aiemmin käytettyjä ”valmiita” mittareita voidaan soveltaa. Valmiin mittarin käyttäminen ei ole itsestään selvyys, sillä mittari ei välttämättä toimi samalla tavalla uuden tutkimuksen asiayhteydessä. Mitattavat ilmiöt eivät

usein pysy täysin muuttumattomina, vaan ne voivat muuttua ajan kuluessa tai ilmetä eri ympäristössä eri tavalla. (Vilkka 2007, 12.) Tässä tutkimuksessa sovelletaan valmista HAIS-Q tietoturvatietoisuusmittaria, joka on esitelty tarkemmin alaluvussa 3.3.

4.3 Kyselylomakkeen rakenne

Kysymysten sisällöt perustuvat yliopistojen julkisiin tietoturvalähteisiin kuten yliopisto-organisaatioiden verkkosivuihin, ohjeisiin, ohjeistuksiin ja tietoturvadokumentteihin. Tietoturvaohjeista ja ohjeistuksista painotetaan Lapin ja Tampereen yliopistojen julkisia tietoturvadokumentteja. Muita yliopistoja, joiden verkkosivuja ja ohjeita on hyödynnetty ovat Aalto-yliopisto ja Helsingin yliopisto.

Aineiston keruuta varten kyselylomake suunnitellaan Parsons ym. (2013 & 2017) luoman tietoturvatietoisuuden mittaamiseen apuvälineen HAIS-Q perustalta. Apuvälineen rakenteelliset osat muodostavat kyselylomakkeen rakenteet ja lisäksi on luotu uusi osio, joka on yleinen tietoturvatietoisuus. Tietoturvatietoisuuden kyselyn osiot ovat:

1. Yleinen tietoturvatietoisuus
2. Käyttäjä- ja salasanaturvallisuus
3. Sähköpostiturvallisuus
4. Internet-turvallisuus
5. Sosiaalisen median ja internetpalveluiden tietoturva
6. Etätyöskentely, etälaitteet ja mobiililaitteet
7. Tietoturvapoikkeamat ja tietoturvatapahtumat
8. Tiedonkäsittely

Kyselytutkimuksen ensimmäisen osion lisääminen tutkimukseen perustuu ajatukseen konstruktivistisesta oppimiskäsityksestä, jonka mukaan uusi tieto kiinnittyy aikaisemmin opittuun tai osattuun. Uudella osiolla selvitetään lyhyesti vastaajien yleistietoa tietoturvasta ja kysymykset suunnitellaan koskemaan tietoturvan perusasioita. Kysymyksillä saadaan tietoa vastaajien tietoturvatietoisuuden lähtökohdista. Tietoturvatietoisuus pohjautuu ymmärrykseen tietoturvauhista, mistä uhat johtuvat ja mitä ne voivat olla.

Kyselyn ja sen osien lisäksi kysymykset luokitellaan suunnitteluvaiheessa HAIS-Q:ssa käytetyn mallin mukaisesti tiedon, asenteen ja käyttäytymisen alakategorioihin. HAIS-Q-apuvälineen valmiita kysymyksiä käytetään mallina, mutta kyselylomakkeen kysymykset ja kysymysten sisältö rakennetaan sopimaan yliopistoympäristöön.

Kysymysten sisältöjen perustana toimivat ensisijaisesti Lapin yliopiston omat tietoturvaa käsittelevät julkiset dokumentit. Niitä ovat henkilöstön tietoturvaopas, henkilöstön tietoturvan pikaohje, henkilöstön mobiiliturvaohje, opiskelijan tietoturvaopas, opiskelijan tietoturvan pikaohje, opiskelijan mobiiliturvaohje, Lapin yliopiston IT-palveluiden käyttösäännöt, Lapin korkeakoulukonsernin tietoaineistojen käsittelyohje, tietoaineistojen turvaluokitus IT-järjestelmissä, Lapin yliopiston sähköpostisäännöt ja Lapin yliopiston tietoturvapolitiikka. Lisäksi tietoturvaohjeita on rakennettu Tampereen yliopiston pakollisen tietoturvakurssin ”Korkeakouluyhteisön tietoturva- ja tietosuojakoulutus” sisällöstä.

Kysymyslomakkeen rakentamista varten kerätään raakatietoa tietoturvadokumenttien sisällöistä luokittelemalla ohjeita, määräyksiä ja tavoitteita HAIS-Q apuvälineen mukaan osioihin 1.–7. Tietoturvadokumenttien sisällöistä kerätty raakatieto muodostaa Lapin yliopiston opiskelijoita ja henkilöstöä koskevien tietoturvatietoisuuskysymysten sisällöllisen perustan. Kysymykset operationalisoidaan siten, että yksittäinen kysymys tuottaa kerätyillä vastauksilla tietoa yksilön tietoturvatiedosta, tietoturva-asenteesta tai tietoturvakäyttäytymisestä. Operationalisoidut kysymykset jaotellaan HAIS-Q apuvälineen seitsemän osa-alueen ja yleisen tietoturvaosion mukaan osioihin 1–8.

Kyselyssä hyödynnetään monivalintakysymyksiä, valintakysymyksiä ja Likert-asteikkokysymyksiä. Eri kysymystyypeillä pyritään saamaan monipuolista tietoa vastaajien tietoturvatietoisuudesta ja välttämään kyselyn yksitoikkoisuutta. Yksitoikkoisuuden kompastuskivenä voi olla, että kysely käy vastaajalle liian raskaaksi. Kysely pyritään rakentamaan vastaajaystävällisyys edellä, jotta se olisi vastaajalle mahdollisimman kevyt.

Kysymysten ideoinnissa, luonnostelussa ja operationalisoinnin tukena hyödynnetään tekoälyä. Tekoälylle annetuissa kehotteissa, eli prompteissa, annetaan tarkat ohjeet kysyttävästä asiasta ja tietoturvakysymys kohdennetaan tarkasti käyttäjätasolle

tarkkaan määritellyistä aiheista. Ulkoasu pyritään muodostamaan käyttäjän näkökulmasta ymmärrettäväksi ja arkipäiväiseksi. Tekoälyn tukea käytetään erityisesti kysymysten ulkoasun muotoiluun ja kysymysten ideointiin, jonka jälkeen kysymykset tarkistetaan ja muotoillaan manuaalisesti. Kysymysten tärkein vaatimus on, että niiden sisältö löytyy tietoturvadokumenteista tai -materiaaleista.

4.4 Aineiston kuvaus

Tutkielman aineistonkeruun perustui validioituun tietoturvamittauksen apuvälineeseen. Mittaria sovellettiin yliopistoympäristöön ja kyselylomakkeen sisällöt muokattiin vastaamaan Lapin yliopiston tietoturvakäytänteitä sekä organisaation sisäisiä sääntöjä. Mittarin soveltaminen tutkimusympäristöön on edellytys sen validiteetille. Vaikka mittarin sisältö suunniteltiin tarkasti tutkimusympäristöön, on tärkeä tiedostaa, että kysymysten tulkinnan yhdenmukaisuus voi vaihdella vastaajien välillä ja voi siten vaikuttaa mittarin ja tulosten validiteettiin.

Aineistonkeruuprosessi aloitettiin pyytämällä tukea Lapin yliopiston tiedekuntien kanslioilta kyselyn levittämiseksi. Kyselytutkimuksen välittäminen tiedekuntien kautta saatiin koko laajuudessaan toteutettua 25.5.2024 mennessä. Aineisto kerättiin noin kolmessa kuukaudessa vuoden 2024 kevään ja kesän taitteessa. Kyselyn avanneita oli 253 kappaletta. Kyselyn avanneista henkilöistä 96 olivat aloittaneet vastaamisen ja lopulta kyselytutkimukseen vastasi 78 henkilöä.

Kyselytutkimuksen kohdentamisessa ja rakentamisessa onnistuttiin halutulla tavalla. Sen rakennusvaiheen suurin haaste oli kyselyn pituuden ja laajuuden paisuminen. Rajaamisen haasteiden takia kysely muodostui pitkäksi, joka puolestaan vaikutti todennäköisesti kyselytutkimukseen vastanneiden lopulliseen lukumäärään. Tästä merkkinä olivat 253 kyselyn avannutta vastaajaa, joista 78 lopulta olivat täyttäneet kyselyn loppuun.

Taulukko 1. Vastaajien taustamuuttujat

	LKM	***%***
Sukupuoli		
Mies	15	19,5
Nainen	56	72,7
Muu	3	3,9
En halua vastata	3	3,9
Tiedekunta		
Kasvatustieteiden tiedekunta	18	23,7
Oikeustieteiden tiedekunta	18	23,7
Yhteiskuntatieteiden tiedekunta	11	14,5
Taiteiden tiedekunta	29	38,2
Ikä		
20–29-vuotiaita	30	38,9
30–39-vuotiaita	19	24,7
40-vuotias tai yli	28	36,4
Rooli		
Opiskelija	60	76,9
Henkilöstö	17	22,1

Aineisto on kuvattu taulukossa 1, jonka mukaan miesten osuus oli noin viidesosa ja naisten osuus kolme neljäsosaa. Henkilöstön osuus aineiston vastauksista oli neljäsosa ja loput vastaajista olivat opiskelijoita. Tiedekuntakohtaisesti vastaajista noin kaksi viidesosaa kuului taiteiden tiedekuntaan, kasvatustieteiden ja oikeustieteiden tiedekunnan osuus vastaajista oli molemmilla noin neljäsosa. Vähiten vastaajia tavoitettiin yhteiskuntatieteiden tiedekunnasta hieman alle 15 prosentin osuudella. Noin kolme neljäsosaa vastaajista oli opiskelijoita ja loput henkilöstöä. Vastaajien Ikäjakauma oli tutkimuksessa tasaisimmin jakautunut. Vastaajista suurin osa oli 20–29-vuotiaita neljänkymmenen prosentin osuudella. Toiseksi suurin ikäryhmä vastaajista oli 40 tai yli vuotiaat, joiden osuus oli hieman yli kolmasosan vastaajista ja vähiten vastaajia oli 30–39-vuotiaita, joiden osuus vastaajista oli noin neljäs osa.

4.5 Aineiston analysointi

Webropolilla kerätty aineisto tallentui verkkopalveluun numeerisena datana. Se tarkoitti, että kyselyn vastausvaihtoehdot olivat kyselylomakkeessa sanallisia, mutta vastaukset tallentuivat Webropoliin numeroina. Ennen aineiston käsittelyä numeroina tallentuneet vastaukset valmisteltiin luettavaan muotoon lisäämällä numeerisille tiedoille sanalliset vastineet. Sanallisten vastausvaihtoehtojen korjaamisen ohella numeeriset arvot säilytettiin, koska niitä hyödynnettiin analyysissa. Kerätyn aineiston valmistelu analyysia varten sisälsi myös kysymysten kategorisoinnin tieto, asenne tai käyttäymiskysymyksiksi. Aineiston valmistelu toteutettiin käyttämällä SPSS-ohjelmistoa. Valmistelulla helpotettiin aineiston muuttujien, kysymysten, vastausten ja kategorisoinnin hallinnointia.

Tutkimuksessa hyödynnettiin laajalti keskiarvoja, mediaaneja ja vastausten keskihajontaa. Keskiarvo voidaan laskea summaamalla mittausarvot ja jakamalla tulos havaintojen lukumäärällä. Keskiarvo kuvaa, kuinka paljon kukin havainto eroaa keskimäärin keskiarvosta. Keskiarvo soveltuu esimerkiksi suhdelukuasteikolla kuvattujen jakaumien kuvaamiseen. Joskus keskiarvo kertoo vain vähän aineistosta ja se saattaa olla aineistossa jopa poikkeava arvo eikä välttämättä kerro luotettavasti mistä on kyse. (Tilastokeskus.)

Mediaani tarkoittaa pistettä, jossa aineisto jakautuu tasaisesti puoliksi. Mediaani toimii hyvin tilanteeseen, jossa asia on vahvasti polarisoitunut ja keskiarvo ei kykene kuvaa tilanteen mitattavia arvoja ja siinä esiintyviä havaintoja. Erot syntyvät polarisoituneissa tilanteissa ääripäiden suuresta etäisyydestä. Kun havainnot keskittyvät jakauman toiseen päähän ja osa havainnoista poikkeaa selvästi keskimääräisestä, mediaani kuvaa keskiarvoa paremmin jakauman keskikohtaa (Tilastokeskus.)

Tutkimusaineiston operationalisoinnin ja analysoinnin kannalta keskeistä oli rakentaa tiedon, asenteen ja käyttäytymisen muuttujat. Tietomuuttuja kuvaa sitä, mitä henkilö tietää tietoturvasta, asennemuuttuja kuvaa tietoturvaa koskevaa asennetta ja tunnetta ja käyttäytymismuuttuja kuvaa sitä, miten henkilö käyttäytyy tietoturvan osalta (Parsons ym. 2017).

Tieto, asenne ja käyttäytymismuuttujat rakennettiin siten, että vastaukset pisteytettiin. Pisteytettyjen vastausten pohjalta tieto, asenne ja käyttäytymismuuttujille muodostettiin summamuuttujat. Tietomuuttuja rakentui valintakysymyksistä, monivalintakysymyksistä ja Likert-asteikkokysymyksistä. Asenne- ja käyttäytymismuuttujat muodostuivat Likert-asteikkokysymyksistä. Taulukossa 2 on esitetty tieto-, asenne- ja käyttäytymismuuttujien kysymysnumerot, kysymysten kohdat ja maksimipisteet.

Taulukko 2. Tietoturvamuuttujien rakentaminen

	LIKERT (Kysymys nro. [kysymyskohdat])	**Monivalintak.** (Kysymys nro)	**Valintakysym.** (Kysymys nro.)	Max
Tietomuuttuja	5. [1–4], 8. [1–3], 12. [1, 3], 13. [1–3], 15. [1–5], 18. [3], 21. [1]	2, 6, 14, 16, 17, 19, 21	1, 3, 7, 9, 12	31 p
Asennemuuttuja	4. [1], 5. [6], 8. [4], 13. [4], 15. [6], 18. [1], 21. [3]	-	-	7 p
Käyttäytymismuuttuja	4. [2], 5.[5], 8. [5–7], 12.[2, 4-6], 13. [5], 15.[7], 18. [2], 21.[2]	-	-	13

Valintakysymykset pisteytettiin etenemisjärjestyksessä ensimmäisenä, jonka jälkeen pisteytettiin monivalintakysymykset ja viimeisenä pisteytettiin LIKERT-kysymykset. Valintakysymyksen oikea vastaus oli arvoltaan +1 p. pistettä ja väärä vastaus +0 pistettä. Monivalintakysymykset pisteytettiin siten, että yhden monivalintakysymyskokonaisuuden maksimipistemäärä oli +1 p. Monivalintakysymykset pisteytettiin siten, että valitut oikeat vastaukset jaettiin ennalta määriteltyjen oikeiden vastausten lukumäärällä. Likert-kysymykset perustuivat viisi portaiseen asteikkoon ja sisälsivät vastausvaihtoehdot väliltä täysin samaa mieltä - täysin erimieltä. Riippuen kysymyksen asettelusta +1 p. voi saada vastaamalla täysin samaa mieltä tai täysin eri mieltä. Vastausvaihtoehdot kaksi tai neljä olivat kysymyksenasettelun mukaan arvoltaan +0,5 p. Neutraali vastausvaihtoehto (3) ja väärä vastaus olivat arvoltaan +/- 0p. Vastaus numero 6. ”en tiedä” käsiteltiin vääränä vastauksena +/- 0 p.

Tieto-, asenne- ja käyttäytymismuuttujien yhteissummasta muodostettiin lisäksi kokonaispistemuuttuja. Kokonaispistemuuttuja sisälsi kyselyn kaikkien kysymysten pisteiden summan. Tietomuuttujan maksimipisteet olivat 31 pistettä, asennemuuttuja maksimipisteet olivat 7 pistettä ja käyttäytymismuuttujan maksimipisteet olivat 13 pistettä. Kokonaispisteiden suurin mahdollinen pistemäärä oli 51. Kyselylomake sisälsi eri määrän tieto-, asenne- ja käyttäytymiskysymyksiä ja niiden maksimipisteiden määrät ovat erit.

Tietoturvamuuttujille laskettiin myös keskiarvoon perustuva prosenttiluku. Prosenttilukumuunnoksen laskentakaavat on esitetty taulukossa 3. Prosenttilukuja käytettiin analyysissa vertailuarvoina ja tasokuvaajina. Niiden avulla toteutettiin vastaajaryhmien välistä vertailua.

Taulukko 3. Tietoturvamuuttujien laskentakaavat

Pistetulos	**Muunnos prosenttiluvuksi**
K_pisteet = tiedon pistetuloksen	K_prosentti = (K_pisteet / maksimipisteet_K) * 100 %
A_pisteet = asennekysym. pistesumma	A_prosentti = (A_pisteet / maksimipisteet_A) * 100 %
B_pisteet = käyttäytymiskysym. pistesumma	B_prosentti = (B_pisteet / maksimipisteet_B) * 100 %
K_A_B_ pisteet = K+A+B yhteistulos	*KAB_prosentti = (K_A_B_pisteet / maksimipisteet) * 100 %*

Tietoturvamuuttujien analysointiin sovelletaan tilastollisia menetelmiä ja kuvailevaa analyysia. Kuvailevan analyysin tavoite on kuvata ja tiivistää määrällisten muuttujien jakautumista tai useampien muuttujien yhteisjakaumia välttämällä kuitenkin tässä vaiheessa yleistyksiä tulosten perusteella. (Tietoarkisto)

Tietoturvamuuttujien tuloksia luokitellaan kuvailevan analyysin lisäksi Krugerin ja Kearneyn (2006, 293) määrittelemien hyvä, keskiverto ja riittävä tietoturvatietoisuuden tasojen mukaan. Tietoturvatietoisuuden tasot on esitetty taulukossa 4. Kurger & Kearneyn määritelmän mukaan 60 % toimii tietoturvatietoisuuden tavoitetason alarajana. Alle 60 prosentin tulos tarkoittaa riittämätöntä tietoturvatietoisuuden tasoa ja, että koulutusta ja ohjeistusta tulisi lisätä. Tietoturvatietoisuuden taso on keskiverto 60–79 % tuloksella ja 80–100 % tulos tarkoittaa, että yksilö ymmärtää tietoturvaa ja yksilö suhtautuu aktiivisesti tietoturvakäytäntöihin. (Kruger & Kearney 2006, 293 & 294.)

Taulukko 4. Kruger & Kearney (2006, 293) tasojen luokittelu

	Awareness	Measurement (%)
Hyvä	(Good)	80—100 %
Keskiverto	(Average)	60—79 %
Riittämätön	(Poor)	59 % tai vähemmän

Kruger & Kearneyn määrittelemiä tietoturvatietoisuuden tasoja käytetään tulosten luokitteluun ja tason tulkintaan. Koska tutkimuksessa ei ollut käytettävissä aikaisempaa tietoa tietoturvatietoisuuden tasosta, tärkeänä raja-arvona tutkimuksessa toimi erityisesti 60 %. Tätä raja-arvoa tarkastelemalla voitiin toteuttaa selkeää tulosten kahtiajakoa. Tasoluokat keskiverto ja hyvä tuottivat riittävä-riittämätön-luokitteluun tarkentavaa ja arvokasta lisätietoa kun vastaajaryhmien tuloksia vertailtiin.

5. Tulokset

5.1 Koko aineiston tulokset

Luvussa kuvataan tutkimusaineiston tulokset yhtenä joukkona. Laskettuja keskiarvoja, keskihajontoja ja mediaaneja käytetään vertailuarvoina aineistosta muodostetuille ryhmille. Vertailun avulla saadaan tietoa eroista ja samankaltaisuuksista.

Taulukossa 5 on esitetty koko aineiston tieto-, asenne- ja käyttäytymismuuttujien tunnuslukuja. Pisteiden keskiarvo tarkoittaa kaikkien vastaajien pistemäärästä laskettua keskiarvoa. Keskiarvo prosentteina tarkoittaa tietoturvatietoisuuden tasoa, jota peilataan taulukon 4 esitettyihin tasoihin ja käytetään vastaajaryhmien tulosten vertailussa. Taulukossa kuvataan myös pisteiden mediaani sekä keskihajonnat.

Taulukko 5. Koko aineiston tietoturvatietoisuuden tuloksia

		Tieto	**Asenne**	**Käyttäyt.**	**Kokonaisp.**
Maksimipisteet		31 p.	7 p.	13 p.	51 p.
Pisteiden keskiarvo	(pisteet)	21,4	6,1	7,7	35,1
(Tietoturvatietoisuuden taso) **Keskiarvo prosentteina**	(%)	69	86,5	59	67,5
Keskihajonta	(pisteet)	4,5	1,09	2,6	7,1
Keskihajonta	(%)	14,5	15,6	19,6	13,7
Mediaani	(%)	71,4	92,9	61,5	69,4

Koko aineiston tuloksista asennemuuttujan keskiarvo on paras tuloksella 86,5 %, ylittäen ainoana hyvän tason rajan. Toiseksi vahvin muuttuja on tieto keskiarvolla 69 % ylittäen riittävän tason rajan. Käyttäytymismuuttuja on selvästi heikoin muuttuja tuloksella 59 % jääden juuri riittävän tason alapuolelle.

Käyttäytymismuuttujan keskihajonta on lähes 20 % ja se vahvistaa sitä tulosta, että käyttäytyminen on heikoin osa-alue. Tietomuuttujan ja asennemuuttujan keskihajonnat ovat 5 prosenttiyksikköä pienemmät. Pieni keskihajonta tarkoittaa, että osaaminen on tasaisempaa.

Tieto-, asenne- ja käyttäytymismuuttujien mediaanit ovat yli niiden keskiarvon ja se tarkoittaa, että aineistossa on enemmän keskiarvoa parempia tuloksia. Tietomuuttujan keskiarvo on selkeästi yli riittävän tason, asennemuuttujan keskiarvo on yli hyvän tason rajan keskiarvotuloksella 86,5 % ja käyttäytymismuuttujan keskiarvo on alle 60 %, eli puutteellinen.

5.2 Henkilöstön ja opiskelijoiden tietoturvatietoisuustulokset

Organisaatiorooli käsitellään tutkimuksessa kaksijakoisesti. Opiskelijoiden ja henkilöstön tuloksia vertaillaan yhtäältä keskenään ja toisaalta suhteessa koko tutkimusaineiston keskiarvoihin. Roolimuuttujan kautta tarkasteltuna asennemuuttuja on opiskelijoiden ja henkilöstön vahvin tietoturvatietoisuuden osa-alue. Toiseksi vahvin muuttuja on tietomuuttuja ja selkeästi heikoin osa-alue on käyttäytyminen.

Taulukossa 6 on esitetty opiskelija- ja henkilöstövastaajaryhmien tieto-, asenne- ja käyttäytymismuuttujien tunnuslukuja. Pisteiden keskiarvo tarkoittaa vastaajaryhmän pistemäärästä laskettua keskiarvoa. Keskiarvo prosentteina tarkoittaa tietoturvatietoisuuden tasoa, jota verrataan taulukon 4 esitettyihin tasoihin ja käytetään vastaajaryhmien tulosten vertailussa. Taulukossa kuvataan myös vastaajaryhmien pisteiden mediaanit sekä keskihajonnat.

Taulukko 6. Henkilöstön & opiskelijoiden tulokset

			Tieto	Asenne	Käyttäyt.	Kokonaisp.
Maksimipisteet			31p	7p	13p	51p
Opiskelijat:	Ka	(pisteet)	21,3	5,6	7,6	34,8
Henkilöstö:	Ka	(pisteet)	21,9	6,5	8,3	36,7
Opiskelijat:	Ka	(%)	68,9 %	85,0 %	58,1 %	67,0 %
Henkilöstö:	Ka	(%)	70,5 %	93,3 %	63,6 %	70,5 %
Opiskelijat:	Kh	(pisteet)	4,9	1,1	2,6	7,6
Henkilöstö:	Kh	(pisteet)	2,7	0,7	2,4	4,3
Opiskelijat:	Kh	(%)	15,7 %	16,2 %	19,8 %	14,7 %
Henkilöstö:	Kh	(%)	8,6 %	9,6 %	18,2 %	8,2 %
Opiskelijat:	M.	(%)	71,7 %	89,3 %	57,7 %	68,6 %
Henkilöstö:	M.	(%)	71,5 %	100 %	65,4 %	71,9 %

Ka = keskiarvopisteet, Kh = keskihajonta M. = mediaani

Henkilöstön ja opiskelijoiden tietomuuttujan keskiarvo on noin 70 %. Henkilöstön tietomuuttujan keskihajonta on noin puolet pienempi kuin opiskelijoilla. Henkilöstön ja opiskelijoiden tietomuuttujan mediaaniarvot ovat lähes samat ja vain hieman yli koko aineiston keskiarvon. Vaikka tietomuuttujan tulokset ovat muuten yhtenevät, voidaan tuloksista nostaa esille, että henkilöstön tiedon tasossa on vähemmän heittelevyyttä.

Henkilöstön asennemuuttujan keskiarvo on korkea (noin 93 %). Se on 8,3 prosenttiyksikköä suurempi kuin opiskelijoilla. Myös opiskelijoiden asenteen keskiarvo ylittää hyvän tason rajan. Henkilöstön asennemuuttujan keskihajonta on 9,6 % ja huomattavasti pienempi kuin opiskelijoilla. Molempien vastaajaryhmien asennemuuttujan mediaani on yli oman vastaajaryhmän keskiarvotuloksen ja henkilöstön mediaani on erityisen korkea, jopa 100 %. Korkea keskiarvo ja mediaani tarkoittavat, että henkilökunnan asenne on kauttaaltaan erinomainen. Opiskelijoiden kesken on paljon hyviä tuloksia, mutta myös joitakin heikkoja tuloksia. Asennemuuttuja on opiskelijoiden ja henkilöstön vahvin tietoturvamuuttuja.

Henkilöstön käyttäytymismuuttujan keskiarvo on 63,1 % ja 5,5 prosenttiyksikköä korkeampi kuin opiskelijoilla. Molemmilla vastaajaryhmillä käyttäytymismuuttujan keskihajonta on erityisen suuri, noin 19 %. Käyttäytymismuuttujan mediaani on opiskelijoilla alle oman vastaajaryhmän keskiarvotuloksen ja henkilöstöllä yli oman keskiarvotuloksen. Henkilökunnan käyttäytymismuuttuja on keskiarvon, keskihajonnan ja mediaanin mukaan selvästi parempi kuin opiskelijoilla. Käyttäytymismuuttuja on opiskelijoiden ja henkilöstön heikoin tietoturvatietoisuusmuuttuja.

5.3 Tiedekuntien tulokset

Tässä alaluvussa käsitellään aineiston tuloksia muodostamalla vastauksista tiedekuntakohtaiset ryhmät. Tarkoituksena on saada yksityiskohtaisempaa tietoa tietoturvatietoisuuden kolmesta osa-alueesta tiedekuntien näkökulmasta tarkasteltuna.

Taulukossa 7 on tiedekuntien tieto-, asenne- ja käyttäytymismuuttujien tunnuslukuja. Pisteiden keskiarvo tarkoittaa vastaajaryhmän pistemäärästä laskettua keskiarvoa. Keskiarvo prosentteina tarkoittaa tietoturvatietoisuuden tasoa, jota verrataan taulukon 4 esitettyihin tasoihin ja käytetään vastaajaryhmien tulosten vertailussa. Taulukossa kuvataan myös vastaajaryhmien pisteiden mediaanit sekä keskihajonnat.

Taulukko 7. Tiedekuntien tulokset

	Tiedot				Asenne				Käyttäyt.				Kokonaisp.			
	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)
KTK	19,5	63,1	14,4	61,3	6,1	87,7	13,6	89,3	7,3	56	13,6	59,6	33	63,4	13,6	66,5
OTK	22,3	71,9	14,9	75,2	6,2	88,1	15,3	92,9	8,3	63,9	20	65,4	36,7	70,7	13,8	73,7
YTK	22,5	72,5	14	72,6	6	85,7	16,1	85,7	7,3	55,8	21,8	57,7	35,7	68,7	14	69,9
TTK	21,4	69	10,5	67,8	6,3	90,3	11,6	92,9	8,7	66,8	14,8	73,1	36,4	70	10	69,3
Koko aineisto	21,4	68,6	14,5	71,4	6,1	86,5	15,6	92,9	7,7	59	19,6	61,5	35,1	67,5	13,7	69,4

Ka = keskiarvopisteet, Kh = keskihajonta, M = mediaani

Tietomuuttujan korkeimman keskiarvotuloksen (noin 72 %) saivat yhteiskuntatieteet ja oikeustieteet. Taidetieteiden tietomuuttujan keskiarvo on noin 2 prosenttiyksikköä ja kasvatustieteillä 9,5 prosenttiyksikköä matalampi kuin taidetieteillä ja oikeustieteillä. Kasvatustieteiden tietomuuttuja eroaa keskiarvolta muista tiedekunnista huomattavasti heikommilla tuloksilla.

Taiteiden tiedekunnan tietomuuttujan keskihajonta 10,5 % on pienin ja eroaa siinä muista tiedekunnista. Muiden tiedekuntien keskihajonnat ovat 14–15 %. Suurimman ja pienimmän keskihajonnan ero on 4,4 prosenttiyksikköä. Oikeustieteiden mediaani on selvästi korkeampi kuin oikeustieteiden keskiarvo ja se vahvistaa oikeustieteiden hyvää tietomuuttujan tulosta. Kasvatustieteiden mediaani on muutaman prosentin pienempi kuin tiedekunnan oma keskiarvotulos ja heikentää kasvatustieteiden tulosta. Yhteiskuntatieteiden mediaani ei eroa merkittävästi omasta keskiarvosta.

Asennemuuttujan on tiedekuntien vahvin osa-alue, jonka osalta kukin tiedekunta saavutti vähintään keskiarvotuloksen 85 %. Taiteiden tiedekunnalla oli vahvin keskiarvo 90,3 % ja yhteiskuntatieteiden matalin 85,7 %. Vain yhteiskuntatieteiden asennemuuttujan keskiarvotulos on alle koko aineiston keskiarvon. Huomioitavaa on, että parhaan keskiarvotuloksen lisäksi taiteidentiedekunnalla keskihajonta oli selkeästi pienin ja omaa keskiarvoa korkeampi mediaani vahvistaa tiedekunnan tulosta.

Käyttäytymismuuttuja on tiedekuntien heikoin tietoturvamuuttuja. Taiteiden tiedekunnan keskiarvo on 66,8 % ja oikeustieteellisen keskiarvo on 64 %. Ne ylittävät riittävän tason rajan. Kasvatustieteet ja yhteiskuntatieteet jäävät riittävän tason alapuolelle noin 56 % keskiarvoilla. Taiteiden tiedekunnan käyttäytymismuuttujan pieni keskihajonta ja suuri mediaani vahvistavat taiteiden tiedekunnan tulosta suhteessa muihin tiedekuntiin. Myös oikeustieteiden keskiarvo on korkea ja mediaani yli keskiarvon, mutta keskihajonta on huomattavasti suurempi kuin taiteiden tiedekunnalla.

5.4 Tiedekuntakohtaiset opiskelijoiden ja henkilöstön tulokset

Tiedekuntaroolin näkökulma tarkoittaa, että tuloksia tarkastellaan tiedekuntakohtaisesti henkilöstöryhminä ja opiskelijaryhminä. Kappaleen tulokset sisältävät yksityiskohtaisempia tuloksia verrattuna edellisiin tiedekunta ja rooli kappaleisiin. Tuloksien tarkastelua syvennetään yhdistämällä edellisten lukujen taustamuuttujat yhdeksi näkökulmaksi.

Tiedekuntaroolijaottelun yhteydessä henkilöstön tiedekuntakohtaiset vastaajamäärät ovat kooltaan pienet määrällisen tutkimuksen aineistoksi. Tiedekuntaroolin tarkastelu päätettiin kuitenkin ottaa mukaan osaksi tutkimusta, koska se tuotti merkityksellisiä havaintoja ja mielenkiintoisia huomioita tutkittavasta ilmiöstä.

Taulukoissa 7 ja 8 on esitetty tiedekunnittain niiden opiskelijoiden ja henkilöstön tieto-, asenne- ja käyttäytymismuuttujien tunnuslukuja. Pisteiden keskiarvo tarkoittaa vastaajaryhmän pistemäärästä laskettua keskiarvoa. Keskiarvo prosentteina tarkoittaa tietoturvatietoisuuden tasoa, jota verrataan taulukon 4 esitettyihin tasoihin. Keskiarvoprosenttia käytetään myös vastaajaryhmien tulosten vertailussa. Taulukoissa kuvataan myös vastaajaryhmien pisteiden mediaanit sekä keskihajonnat.

Taulukko 8. Opiskelijoiden tiedekuntakohtaiset tulokset

	Tiedot				Asenne				Käyt.				Kokonaisp.				
	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	LKM
KTK	18,1	58,5	15,6	61,1	5,6	80,5	12,8	78,6	6,4	49,3	17,8	50	30,2	58,1	14,5	62,4	11
OTK	22,1	71,1	16,2	74,9	6,1	87,6	16,3	92,9	7,9	61,0	19,8	61,5	36,1	69,5	14,8	73,1	15
YTK	22,7	73,1	14,3	72,6	6,0	85,4	17,	92,9	7,5	57,4	21,6	57,7	36,1	69,5	14,5	69,3	25
TTK	21,3	68,8	12,0	66,3	6,3	90,2	10,8	92,9	8,8	67,3	15,2	71,2	36,4	70,0	11,1	68,8	8
Koko aineisto	21,4	68,9	14,5	71,4	6,1	86,4	15,6	92,9	7,7	59,0	19,6	61,5	35,1	67,5	13,7	69,4	

Ka = keskiarvopisteet, Kh = keskihajonta, M = mediaani

Taulukko 9. Henkilöstön tiedekuntakohtaiset tulokset

	Tieto				asenne				Käyttäytyminen				kokonaispisteet				
	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	Ka (p)	Ka (%)	Kh (%)	M (%)	LKM
KTK	21,7	70,1	9,0	71,1	6,9	99,0	2,7	100	8,6	66,5	10,3	69,2	37,3	71,8	6,1	74,1	7
OTK	23,4	75,5	16,2	75,5	6,3	90,5	10,9	92,9	10,2	78,2	17,3	76,9	39,9	76,7	5,0	79,1	3
YTK	21,2	68,3	12,8	72,4	6,1	87,5	9,0	85,7	6,0	46,2	23,1	50	33,3	64,0	10,9	67,6	4
TTK	21,6	69,5	6,5	67,8	6,3	90,5	16,5	100	8,5	65,4	16,8	73,1	36,4	70,0	8,4	69,9	3
Koko aineisto	21,4	68,9	14,5	68,6	6,1	86,4	15,6	92,9	7,7	59,0 %	19,6	61,5	35,1	67,5	13,7	69,4	

Ka = keskiarvopisteet, Kh = keskihajonta, M = mediaani

Taulukot 7 ja 8 sisällytettiin kappaleen alkuun, jotta tulkitsemattomat tulokset olisivat helposti saatavilla ja tarkasteltavissa niitä käsittelevän tekstin yhteydessä. Valinnalla haluttiin helpottaa tulosten välitöntä saatavuutta. Taulukon oleellisimpia arvoja ovat tietoturvatietoisuusmuuttujien keskiarvo prosentteina -tulokset.

Kasvatustieteiden tiedekunta

Kasvatustieteen opiskelijoiden tietomuuttujan keskiarvo on 12 prosenttiyksikköä matalampi kuin kasvatustieteiden henkilöstöllä ja noin 10 prosenttiyksikköä alle koko aineiston keskiarvon. Henkilöstön tietomuuttujan keskiarvotulos on yli koko aineiston keskiarvon ja kaikista vastaajaryhmistä kolmanneksi suurin. Henkilöstön tietomuuttujan keskihajonta on merkittävän pientä ja opiskelijoiden keskihajonta on keskimääräistä hieman suurempaa. Tulokset viittaavat vahvasti henkilöstön korkeampaan tietoturvatietoisuuden tasoon kasvatustieteiden tiedekunnassa.

Opiskelijoiden asennemuuttujan keskiarvo ylittää hyvän tason raja-arvon. Kasvatustieteiden opiskelijoiden asennemuuttujan keskiarvo 80,5 %, mutta se on tutkimuksen heikoin asenteen tulos. Se on 5,9 prosenttiyksikköä matalampi kuin koko aineiston keskiarvo ja 18,5 prosenttiyksikköä heikompi kuin kasvatustieteiden henkilöstön keskiarvo. Kasvatustieteiden henkilöstön asennekeskiarvo on 99 % ja koko tutkimuksen

vahvin. Kasvatustieteen opiskelijoiden asenteen keskihajonta on pienempi kuin koko aineiston asennemuuttujan keskihajonta, mutta selkeästi suurempi kuin henkilöstön keskihajonta. Kasvatustieteen opiskelijoiden mediaani on 2 prosenttiyksikköä alle oman asennekeskiarvon, kun taas henkilöstön mediaani on täydet 100 %. Tulosten mukaan kasvatustieteiden opiskelijoiden asenne on hyvällä tasolla, mutta koko tutkimuksen muihin vastaajaryhmiin huomattavasti heikompi.

Kasvatustieteen opiskelijoiden käyttäytymismuuttujan keskiarvo on 49,3 %, joka on noin 10 prosenttiyksikköä matalampi kuin koko aineiston keskiarvo ja 16,7 prosenttiyksikköä henkilöstön asennekeskiarvoa matalampi. Opiskelijoiden käyttäytymismuuttujan keskihajonta on 7,5 prosenttiyksikköä korkeampi kuin henkilöstöllä. Opiskelijoiden käyttäytymisen mediaani on vain hieman oman keskiarvon yläpuolella ja henkilöstöllä mediaani on noin 3 % korkeampi kuin oma keskiarvo. Tiedekunnan henkilöstön käyttäytymismuuttuja on selvästi yli riittävän tason, sen keskihajonta on pieni ja tulos on koko tutkimuksen muihin tuloksiin verrattuna suhteellisen korkea.

Kasvatustieteiden opiskelijoiden tietomuuttujan ja asennemuuttujan keskiarvot ovat tutkimuksen heikoimmat. Kasvatustieteiden opiskelijoiden asennemuuttujan mediaani on ainoa, joka jää merkittävästi alle oman keskiarvotuloksen. Opiskelijoiden käyttäytymismuuttujan tulos on koko tutkimuksen käyttäytymiskeskiarvoon verraten yli 10 prosenttiyksikköä heikompi. Heikko keskiarvo ja mediaani vahvistava tulosta siitä, että kasvatustieteiden käyttäytymisen heikko tulos korostuu.

Kasvatustieteen henkilöstön tieto, asenne ja käyttäytymismuuttujien keskiarvot ovat systemaattisesti korkeammat kuin kasvatustieteiden opiskelijoilla. Kasvatustieteen henkilökunta voidaan nostaa kokonaispisteiden, matalan keskihajonnan ja tasaisen keskiarvotulosten mukaan tutkimuksen toiseksi vahvimmaksi vastaajaryhmäksi. Kasvatustieteiden henkilöstön tieto-, asenne- ja käyttäytymismuuttujien keskiarvotulokset ylittävät poikkeuksetta koko tutkimuksen keskiarvotuloksen ja keskihajonta on erityisen pientä.

Kasvatustieteiden henkilöstön ja opiskelijoiden tulosten tarkastelu viittaa, että tiedekunnan matala tietoturvatietoisuuden taso on yhteydessä opiskelijoiden heikkoihin tuloksiin.

Oikeustieteiden tiedekunta

Oikeustieteellisen tiedekunnan opiskelijoiden tietoturvatietoisuuden tulokset olivat kokonaisvaltaisesti vahvat. Tieto-, asenne- ja käyttäytymismuuttujien osalta oikeustieteen opiskelijoiden tietoturvatietoisuuden tulokset olivat opiskelijoiden kesken parhaat. Opiskelijoiden keskiarvot ovat korkeat, mediaanit ovat kaikkien tietoturvamuuttujien osalta yli oman vastaajaryhmän keskiarvon. Oikeustieteiden opiskelijoiden keskihajonta on suurta kaikkien tietoturvamuuttujien kohdalla.

Oikeustieteiden opiskelijoiden ja henkilöstön tietomuuttujan keskiarvot ovat riittävällä tasolla ja tutkimuksen muihin tuloksiin verrattuna korkeat. Henkilöstön keskiarvo on koko tutkimuksen korkein ja opiskelijoiden keskiarvo on koko tutkimuksen vastaajaryhmien osalta kolmanneksi korkein. Oikeustieteiden henkilöstön tietomuuttujan keskihajonta on huomattavasti pienempi kuin tiedekunnan opiskelijoilla. Vaikka opiskelijoiden tietomuuttujan keskihajonta on korkea, sen mediaani vahvasti yli oman keskiarvotuloksen. Oikeustieteen tietomuuttujan tulokset ovat kauttaaltaan vahvemmat kuin opiskelijoilla.

Oikeustieteellisen tiedekunnan opiskelijoiden ja henkilöstön asennemuuttujan keskiarvotulokset ovat yli koko aineiston keskiarvon ja selvästi hyvän tason yläpuolella. Oikeustieteen opiskelijoiden keskihajonta on asennemuuttujan kohdalla suuri ja mediaani merkittävästi yli oman keskiarvotuloksen. Henkilöstön asennemuuttujan keskiarvo on parempi kuin oikeustieteen opiskelijoilla, mutta opiskelijoiden mediaani on lähes yhtä korkea kuin henkilöstön keskiarvo- ja mediaanitulokset.

Koko tutkimuksen heikoimman tietoturvamuuttujan – käyttäytyminen - osalta oikeustieteiden henkilöstön tulos on poikkeava huomattavan korkealla keskiarvotuloksella. Oikeustieteen henkilöstön käyttäytymismuuttujan tulos on koko tutkimuksen paras ja ylittää muut tutkimuksen käyttäytymisen keskiarvotulokset vähintään 11 prosenttiyksiköllä ja on melkein yli hyvän tason. Oikeustieteen opiskelijoiden käyttäytymismuuttujan keskiarvotulos ylittää koko tutkimuksen keskiarvon ja on riittävän rajan yläpuolella.

Muista vastaajaryhmistä eroten oikeustieteiden henkilökunnan käyttäytymismuuttuja ei ole tulosten mukaan heikoin tietoturvatietoisuuden osa-alue.

Tiedekunta-rooli tarkastelussa oikeustieteiden henkilöstö nousee koko tutkimuksen vahvimmaksi vastaajaryhmäksi. Oikeustieteen opiskelijoiden tietoturvatietoisuuden taso on kokonaispisteiden mukaan taiteiden tiedekunnan opiskelijoiden kanssa vahvimmat.

Myös oikeustieteiden tiedekuntakohtaisten henkilöstön ja opiskelijoiden tulosten perusteella voidaan todeta, että henkilöstön tietoturvatietoisuus on vahvempaa kuin opiskelijoilla. Oikeustieteellisen tiedekuntakohtaiset tulokset osoittavat myös, että oikeustieteellisen tiedekunnan tietoturvatietoisuus on vahva.

Yhteiskuntatieteiden tiedekunta

Yhteiskuntatieteet opiskelijoiden tietomuuttuja on tiedekuntien opiskelijoiden selvästi paras ja koko tutkimuksen toiseksi paras ja on selvästi yli koko tutkimuksen keskiarvon. Yhteiskuntatieteiden opiskelijoiden tietomuuttujan keskiarvo on noin 5 prosenttiyksikköä yhteiskuntatieteiden henkilöstöä parempi ja siksi poikkeaa muista tuloksista.

Yhteiskuntatieteiden henkilöstön asennemuuttujan keskiarvo on hieman opiskelijoiden keskiarvoa parempi, mutta on lähes sama. Opiskelijoiden asennemuuttujan keskihajonta on tutkimuksen suurin ja 8,1 % suurempi kuin yhteiskuntatieteiden henkilöstöllä.

Yhteiskuntatieteiden henkilöstön käyttäytymismuuttujan vertaaminen on merkityksetöntä, koska henkilöstön keskiarvo on epäilyttävän pieni. On syytä olettaa, että yhteiskuntatieteen henkilöstön käyttäytymismuuttujan kysymysten vastaukset eivät ole todenmukaisia, vaan vastaajat ovat lopettaneet vastaamisen. Henkilöstön käyttäytymisen keskiarvo on tästä syystä heikoin keskiarvolla 46,3 % ja 11,2 prosenttiyksikköä heikompi kuin opiskelijoiden 57,4 %.

Yhteiskuntatieteiden tulosten osalta voidaan todeta, että henkilöstön osaaminen ei ollut merkittävästi parempaa, mutta keskihajonta on pienempää. Opiskelijoiden asenteen keskihajonta on 8,1 % suurempi ja lähes kaksinkertainen verrattuna henkilöstöön.

Yhteiskuntatieteiden opiskelijoiden suoriutuminen on kokonaispisteiden mukaan lähes yhtä vahvalla tasolla kuin oikeustieteiden ja taiteiden tiedekunnan opiskelijoilla. Tuloksen tulkinnassa on otettava huomioon tietomuuttujan suuri osuus ja sen vaikutus kokonaispisteisiin. Tietomuuttujan pisteiden osuus koko tutkimuksessa on suuri. Hyvän tietomuuttujan ohella yhteiskuntatieteiden opiskelijoiden asenne ja käyttäytyminen jäävät oikeustieteellisen- ja taiteiden tiedekunnan opiskelijoiden tulosta heikommaksi. Se on otettava huomioon arvioidessa tuloksen merkitystä ja siksi yhteiskuntatieteiden opiskelijoiden tulos on lopulta heikompi kuin oikeustieteiden ja taiteiden tiedekunnan opiskelijoilla.

Taiteiden tiedekunta

Taiteiden tiedekunnan henkilöstön ja opiskelijoiden tiedon keskiarvotulokset ovat lähes samat, mutta henkilöstön keskiarvo on marginaalisesti opiskelijoita korkeampi. Henkilöstön tietomuuttujan keskihajonta on puolet pienempi kuin opiskelijoilla. Taiteiden tiedekunnan opiskelijoiden tietomuuttujan mediaani on pienempi kuin henkilöstöllä ja keskihajonta suurempi.

Taiteiden tiedekunnan opiskelijoiden ja henkilöstön asennemuuttujan keskiarvo on sama, mutta henkilöstön keskihajonta on noin 6 prosenttiyksikköä suurempi. Taiteiden tiedekunnan opiskelijoiden ja henkilöstön keskiarvot ovat yli koko aineiston keskiarvon.

Taiteidentiedekunnan opiskelijoiden käyttäytymisen keskiarvo on hieman parempi kuin henkilöstöllä. Kokonaisuudeltaan opiskelijoiden ja henkilöstön keskihajonnan määrät ovat lähes samat ja vastaajaryhmien keskiarvot ovat selkeästi yli koko aineiston keskiarvotuloksen.

Taiteiden tiedekunnan tuloksien mukaan henkilöstön ja opiskelijoiden tulosten ero on kaikilta osin pieni. Taiteiden tiedekunnan opiskelijoiden ja henkilöstön tulokset ovat

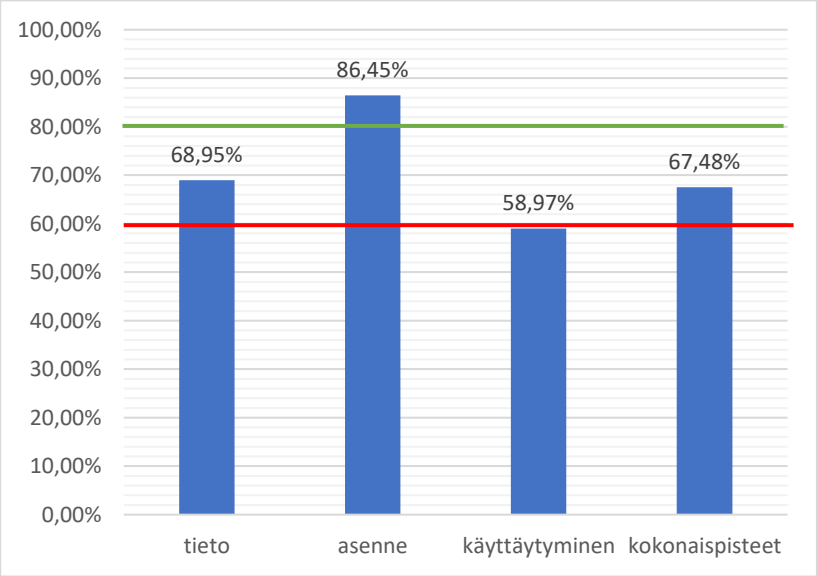
kaikkein tasaisimmat verrattuna muihin tiedekuntiin. Taidetieteiden opiskelijoiden ja henkilöstön tuloksista suurimpana havaintona ilmenee henkilöstön pieni keskihajonta ja taiteiden tiedekunnan opiskelijoiden vahva tietoturvatietoisuuden taso suhteessa tutkimuksen muden tiedekuntien opiskelijoiden tuloksiin.

6. Johtopäätökset ja yhteenveto

Tutkimusaineiston vastaajista noin kolme neljäsosaa oli opiskelijoita ja siksi tutkimuksen koko aineistoa kuvaavat tiedon, asenteen ja käyttäytymisen keskiarvot myötäilivät vahvemmin opiskelijoiden tuloksia. Henkilöstön pienempi osuus aineistossa voi vaikuttaa tuloksiin pelkistämällä niitä. Opiskelijoiden ja henkilöstön tiedekuntakohtaiset tulokset haluttiin henkilöstön pienestä lukumäärästä huolimatta sisällyttää osaksi tutkimustuloksia, koska niiden tulokset tuottivat tutkimuksen kannalta oleellisia ja mielenkiintoisia havaintoja.

Koko aineisto

Koko aineiston tulokset osoittivat, että asenne oli tietoturvatietoisuuden vahvin osa-alue ja sen keskiarvotulos ylitti hyvän tason rajan. Tieto oli riittävällä tasolla ja toiseksi vahvin osa-alue. Käyttäytyminen puolestaan oli tulosten mukaan heikoin osa-alue ja se jää koko tutkimusaineiston keskiarvotuloksen osalta alle riittävän tason. Tulokset osoittavat, että yliopiston tietoturvatietoisuuden taso oli pääsääntöisesti riittävällä tasolla. Ainoana poikkeuksena oli käyttäytyminen, joka jäi koko aineiston keskiarvotulokselta alle riittävän tason.



Kuva 5. Koko aineiston keskiarvotulokset. Punainen = riittävän tason raja, vihreä = hyvän tason raja

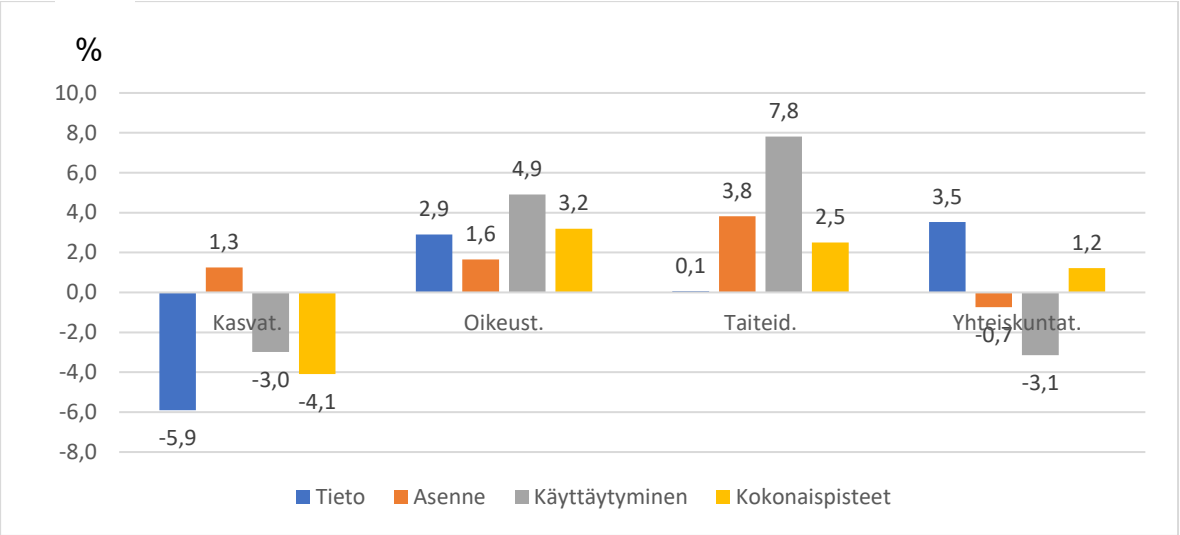
6.1 Tiedekuntien väliset erot

Tiedekuntien tulokset osoittivat, että oikeus- ja taidetieteiden tietoturvatietoisuuden tasot olivat korkeimmat, kun taas kasvatustieteiden tulokset jäivät kaikilla osa-alueilla selvästi alle keskiarvon. Yhteiskuntatieteiden tietoturvatietoisuuden taso oli matalampi kuin oikeus- ja taidetieteillä, mutta selvästi vahvempi kuin kasvatustieteillä.

Tietomuuttujan osalta yhteiskuntatieteiden keskiarvo oli heikompi kuin oikeus- ja taidetieteiden tiedekunnilla, mutta siitä huolimatta riittävällä tasolla. Kasvatustieteiden tietomuuttujan tulos oli selvästi heikoin ja erosi muista tiedekunnista. Kaikkien tiedekuntien asennemuuttujan keskiarvo oli hyvällä tasolla. Kasvatustieteiden ja yhteiskuntatieteiden käyttäytymisen keskiarvotulokset jäivät selvästi alle riittävän tason, kun taas oikeustieteiden- ja taidetieteiden tiedekunnilla käyttäytymisen keskiarvo oli yli riittävän tason. Kasvatustieteiden ja yhteiskuntatieteiden tietoturvatietoisuusmuuttujien keskiarvot olivat heikommat kuin oikeustieteiden ja taidetieteiden tiedekunnilla.

Oikeustieteiden, taidetieteiden ja yhteiskuntatieteiden kokonaispisteiden keskiarvotulokset olivat korkeammat kuin koko aineiston keskiarvotuloksen, kun taas kasvatustieteiden kokonaispisteiden keskiarvo oli ainoana sitä pienempi. Tiedon, asenteen ja käyttäytymisen tulosten tarkempi tulkinta osoitti, että yhteiskuntatieteiden asenteen ja käyttäytymisen tulokset olivat oikeustieteiden ja taiteiden tiedekuntaan verrattuna huomattavasti heikommat, vaikka kokonaispisteet olivat lähes samantasoiset. Taiteiden- ja oikeustieteiden tiedekuntien tulosten keskiarvot olivat tasaisemmin jakautuneet kuin yhteiskuntatieteillä ja siksi paremmat.

Tiedekuntien tulokset on esitetty kuvassa 6 suhteessa koko aineiston keskiarvotuloksiin. Kuva antaa yleiskuvan tiedekuntien tuloksista. Kuva ilmentää yhteiskuntatieteiden heikompaa tietoturvatietoisuuden tulosten kokonaisuutta verrattuna taidetieteiden -ja oikeustieteiden tiedekuntiin. Kuva ilmentää myös kasvatustieteiden muita tiedekuntia heikompaa tasoa.



Kuva 6. Tiedekuntien keskiarvot suhteessa koko aineiston keskiarvoon

Taiteiden tiedekunnan keskihajonta oli kokonaisuudessaan erityisen pieni ja tulosten mediaanit olivat omaa keskiarvoa hieman korkeampia. Pienen keskihajonnan voidaan ajatella olevan taiteiden tiedekunnan osalta merkki osaamisesta. Osaamiselle tyypillistä on tasainen suoriutuminen ja erojen tasapäistyminen.

Oikeustieteellisen tiedekunnan tulos oli tiedekuntien välisesti vahvin. Sen keskihajonta oli suuri, mutta mediaani oli korkea ja merkittävästi oman keskiarvotuloksen yläpuolella. Oikeustieteiden korkea keskihajonta tulkitaan korkean mediaanitulosten kanssa tiedekunnan tulosta vahvistavaksi tekijäksi.

Kasvatustieteiden ja yhteiskuntatieteiden asenne- ja käyttäytymismuuttujien keskiarvotulokset olivat samantasoiset. Molempien tiedekuntien asenteen keskiarvo ylitti hyvän tason rajan ja keskiarvotulos oli tiedekuntien kesken lähes sama. Molempien tiedekuntien asenteen ja käyttäytymisen tulokset olivat heikommat verrattuna oikeustieteiden ja taidetieteiden tuloksiin.

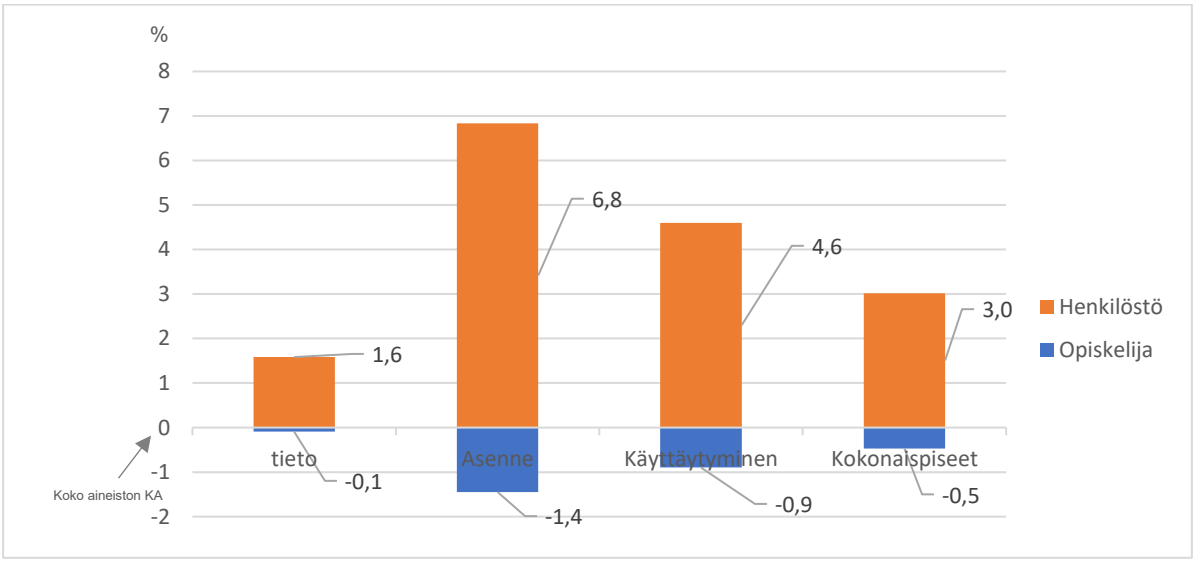
Kasvatustieteiden ja yhteiskuntatieteiden suurimpana erona oli tietomuuttujan keskiarvo. Yhteiskuntatieteiden tietomuuttujan keskiarvo oli erittäin korkea, kun taas kasvatustieteillä se oli hieman yli riittävän tason rajan. Kasvatustieteiden ja yhteiskuntatieteiden keskihajonnat olivat koko aineistoon verrattuna keskimääräiset ja tiedekuntien mediaanit painottuivat kaikin osin hieman oman keskiarvotuloksen yläpuolelle.

6.2 Henkilöstön ja opiskelijoiden väliset erot

Henkilöstön tiedon, asenteen ja käyttäytymisen keskiarvotulokset olivat yli koko aineiston keskiarvon ja korkeammat kuin opiskelijoilla. Opiskelijoiden tietomuuttujan keskiarvo oli lähes sama kuin koko aineiston keskiarvo. Asenteen ja käyttäytymisen keskiarvotulokset jäivät opiskelijoilla alle keskiarvon.

Henkilöstön ja opiskelijoiden tulokset osoittivat, että asenne oli tietoturvatietoisuuden vahvin osa-alue. Molempien vastaajaryhmien asenteen keskiarvotulokset olivat yli hyvän tason ja tiedon keskiarvotulokset ylittivät selvästi riittävän tason ollen samansuuruiset. Henkilöstön ja opiskelijoiden tulokset erosivat eniten käyttäytymisen osalta.

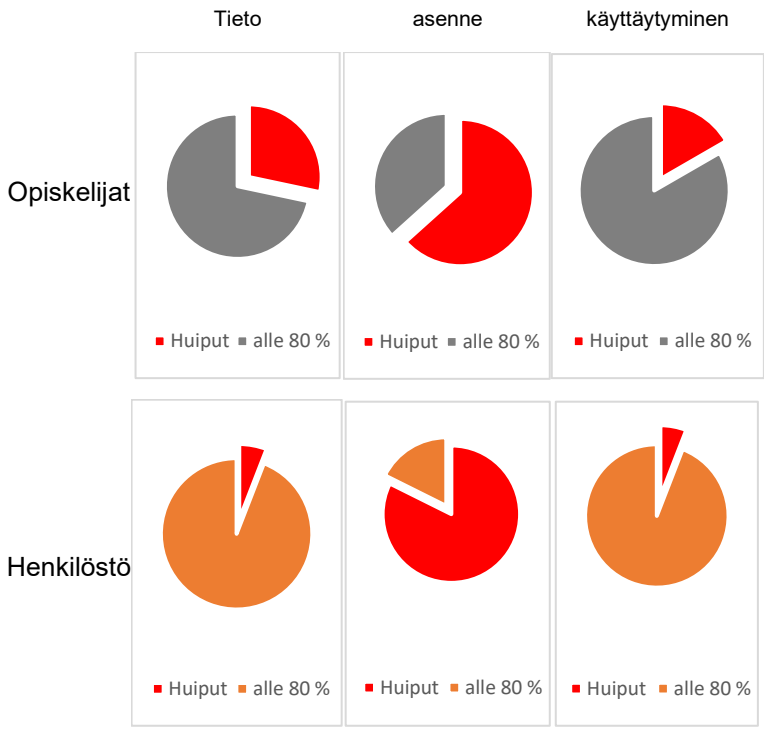
Kuva 7 ilmentää henkilöstön ja opiskelijoiden tuloksia suhteessa koko aineiston tuloksiin. Kuvasta voidaan havaita, että henkilöstön tietoturvamuuttujien keskiarvot ylittivät poikkeuksetta koko aineiston keskiarvotulokset. Opiskelijoiden vastaajaryhmän keskiarvotulokset jäivät puolestaan kaikilta osin alle koko aineiston keskiarvotulosten.



Kuva 7. Opiskelijoiden ja henkilöstön keskiarvo suhteessa koko aineiston keskiarvoon

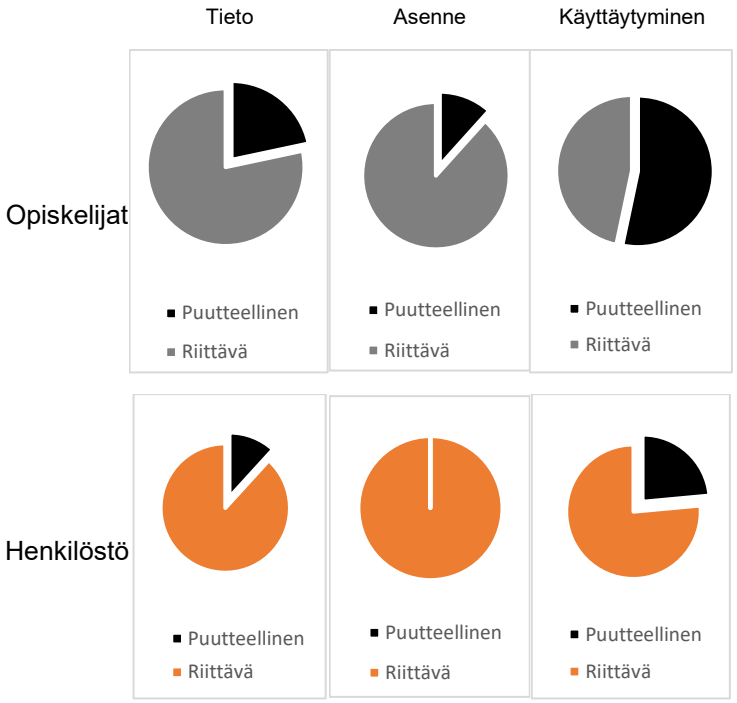
Henkilöstön -ja opiskelijoiden vastaajaryhmien tulosten mediaanien perusteella henkilöstön tiedon, asenteen ja käyttäytymisen tulokset painottuivat selvästi oman keskiarvon yläpuolelle ja keskihajonnat olivat pienemmät. Henkilöstön tieto, asenne ja käyttäytymisen keskihajonnat ja mediaanit tukevat havaintoa henkilöstön vahvemmasta tietoturvatietoisuuden tasosta. Opiskelijoiden tulosten keskiarvot olivat pienemmät, keskihajonnat suuremmat ja vastaukset eivät painottuneet samalla tavalla oman keskiarvotuloksen yläpuolelle kuin henkilöstöllä.

Poikkeavana havaintona roolien välisesti oli opiskelijoiden tietomuuttujan korkeampi mediaani, vaikka tietomuuttujan keskiarvo oli matalampi. Se tarkoittaa, että opiskelijoiden joukosta löytyi huomattavan paljon omaa keskiarvoa korkeampia tuloksia. Kuva 8 ja 9 havainnollistavat roolien puutteellisten tulosten ja huipputulosten osuuksia vastaajaryhmissä.



Kuva 8. Opiskelijoiden ja henkilöstön huipputulosten osuudet

Kuvasta 8 voidaan nähdä, että opiskelijoiden joukossa on enemmän huipputuloksia tiedon ja asenteen osalta kuin henkilöstön vastaajaryhmässä. Henkilöstön vastaajaryhmässä asenteen huipputuloksien osuus oli suurempi kuin opiskelijoilla. Kuva 9 puolestaan ilmentää, että myös puutteellisten tulosten osuus oli opiskelijoilla suurempi kuin henkilöstöllä.



Kuva 9. Opiskelijat ja henkilöstö puutteellisten tulosten osuudet

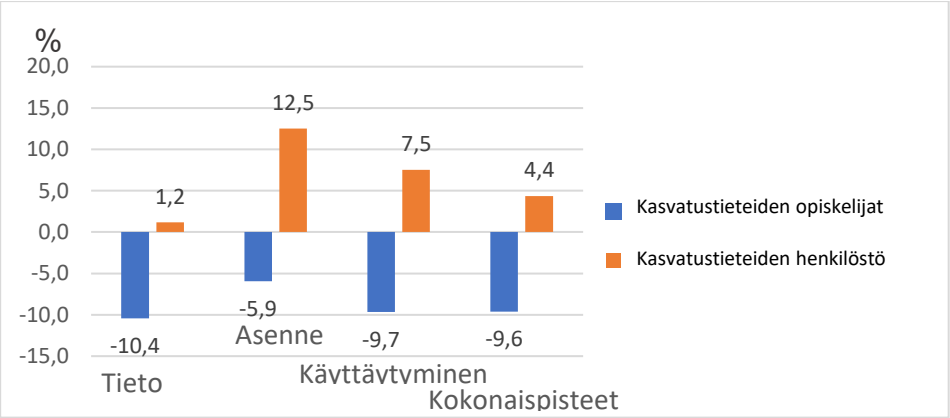
Kuvat 8 ja 9 kertovat henkilöstön ja opiskelijoiden erilaisesta tietoturvatietoisuuden jakautumisesta vastaajaryhmän sisällä. Henkilöstön tietoturvatietoisuus on tasaisempaa ja opiskelijoiden tietoturvatietoisuudessa ilmenee suuria eroja.

6.3 Henkilöstön ja opiskelijoiden väliset erot eri tiedekunnissa

Tiedekuntakohtaisten henkilöstön ja opiskelijoiden tulosten tarkastelu tuotti tietoa roolien välisistä eroista tiedekuntien sisällä. Oikeustieteiden ja kasvatustieteiden henkilöstön ja opiskelijoiden tuloksien mukaan henkilöstön tietoturvatietoisuus on selvästi vahvempi. Yhteiskuntatieteiden ja taidetieteiden tiedekuntien opiskelijoiden tulokset olivat puolestaan osittain korkeammat kuin tiedekuntien henkilöstöllä**.** Tulokset osoittivat, että henkilöstön korkeampi tietoturvatietoisuuden taso ei ole yksiselitteistä ja siinä ilmenee poikkeuksia.

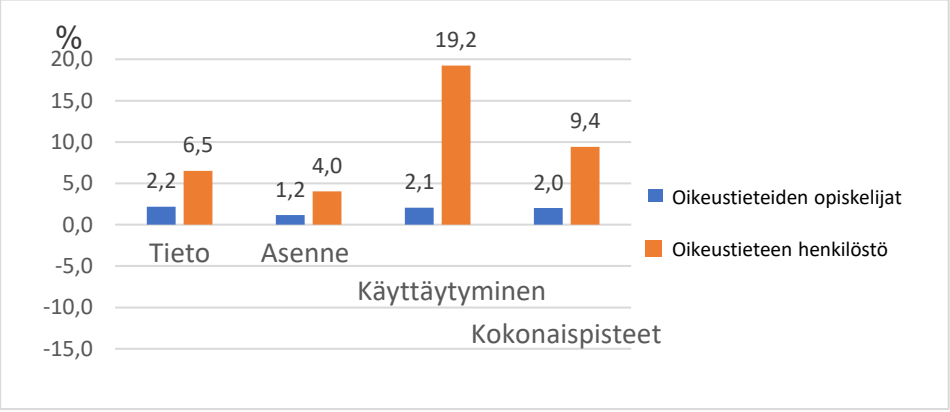
Kasvatustieteiden tiedekunnan henkilöstön tulokset olivat selvästi vahvemmat kuin tiedekunnan opiskelijoilla. Henkilöstön keskiarvot olivat korkeat, niiden keskihajonnat olivat pieniä ja tulokset painottuivat mediaanin mukaan oman keskiarvon yläpuolelle. Kasvatustieteiden henkilöstön asennemuuttujan tulos oli koko tutkimuksen vahvin. Kasvatustieteiden opiskelijoiden kokonaispisteiden keskiarvo jäi alle riittävän tason rajan. Kuva 10 havainnollistaa kasvatustieteiden opiskelijoiden selkeästi heikompia keskiarvoja suhteessa keskiarvoon ja tiedekunnan henkilöstöön. Kasvatustieteiden opiskelijat olivat tutkimuksen heikoin vastaajaryhmä.

Kasvatustieteiden tulokset olivat tiedekuntana heikoimmat. Opiskelijoiden ja henkilöstön tiedekuntakohtaiset tulokset osoittivat, että kasvatustieteiden heikko tulos painottui merkittävästi tai kokonaan tiedekunnan opiskelijoihin. Kuva 10 havainnollistaa henkilöstön ja opiskelijoiden keskiarvotulosten suuria eroja suhteessa koko aineiston keskiarvoon ja toisiinsa.



Kuva 10. Kasvatustieteiden opiskelijoiden ja henkilöstön keskiarvot suhteessa koko aineiston keskiarvoon

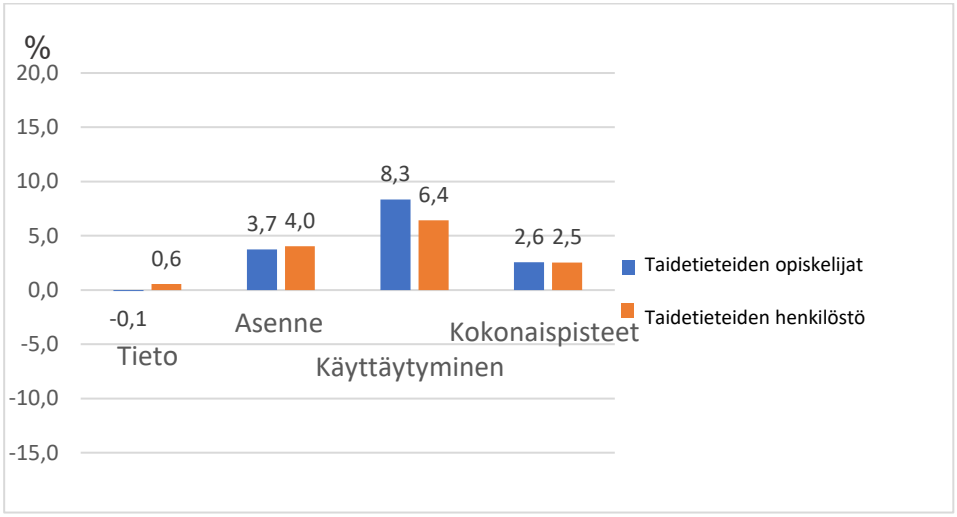
Oikeustieteiden tiedekunnan tuloksista havaittiin saman suuntaisia tuloksia kuin kasvatustieteiden tiedekunnan henkilöstön ja opiskelijoiden tuloksista. Oikeustieteiden henkilöstön keskiarvotulokset olivat korkeammat ja keskihajonta oli pienempää. Oikeustieteiden henkilöstön tulokset olivat tutkimuksen vahvimmat. Oikeustieteiden opiskelijoiden mediaanit olivat korkeat ja sen mukaan opiskelijoiden tulos painottui vahvasti yli oman keskiarvon. Opiskelijoiden tulokset olivat tiedekunnan henkilöstöä heikommat, mutta muiden tiedekuntien opiskelijoihin verrattuna tulokset olivat vahvimmat. Kuva 11 ilmentää oikeustieteiden henkilöstön ja opiskelijoiden tulosten eroja suhteessa koko aineiston tuloksiin.



Kuva 11. Oikeustieteiden henkilöstön ja opiskelijoiden tulokset suhteessa koko aineiston keskiarvoon

Oikeustieteiden opiskelijoiden ja henkilöstön tulokset olivat myös tiedekuntien välisesti korkeimmat. Vahvat henkilöstön ja opiskelijoiden tulokset osoittavat, että tiedekunnan tietoturvatietoisuus on muista tiedekunnista positiivisesti poikkeava. Oikeustieteiden henkilöstön tuloksien erityisenä havaintona oli käyttäytymismuuttujan korkein keskiarvotulos. Sen keskiarvotulos oli merkittävästi korkeampi kuin koko tutkimuksen muut käyttäytymisen tulokset ja ylsi lähes 80 % hyvään tasoon.

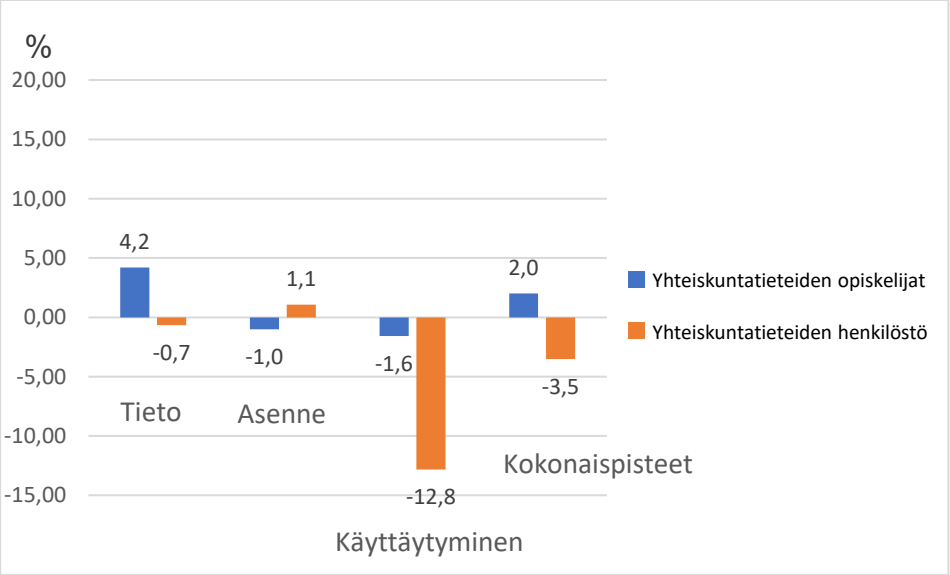
Taiteiden tiedekunnan henkilöstön tietomuuttujan kokonaispisteiden keskiarvotulos oli hieman opiskelijoita korkeampi ja keskihajonta oli merkittävästi pienempi. Opiskelijoiden ja henkilöstön asenteen keskiarvot olivat yhtä suuret. Tiedekunnan henkilöstön asenteen tulosta vahvisti korkea mediaani, joka selitti myös sen korkeampaa keskihajontaa. Opiskelijoiden käyttäytymismuuttujan keskiarvo oli henkilöstöä korkeampi. Henkilöstön käyttäytymisen mediaani oli merkittävästi yli oman keskiarvotuloksen ja oli opiskelijoiden mediaania korkeampi. Kuva 12 ilmentää taidetieteiden opiskelijoiden ja henkilöstön tasaisia tietoturvatietoisuuden tuloksia.



Kuva 12. Taiteiden tiedekunnan henkilöstön ja opiskelijoiden tulokset suhteessa keskiarvoon

Taiteiden tiedekunnan opiskelijoiden ja henkilöstön tietoturvatietoisuuden erot olivat pieniä. Henkilöstön pääsääntöisesti korkeampien mediaanitulosten ja pienemmän keskihajonnan mukaan voidaan kuitenkin todeta, että tiedekunnan henkilöstön tulokset viittaavat korkeampaan tietoturvatietoisuuden tasoon.

Yhteiskuntatieteiden opiskelijoiden tieto ja käyttäytymismuuttujien keskiarvot olivat henkilöstöä korkeammat, mutta henkilöstön asenteen tulos oli korkeampi kuin tiedekunnan opiskelijoilla. Opiskelijoiden tietoturvatietoisuuden taso oli kokonaispisteiden keskiarvolta henkilöstöä korkeampi. Kuva 13 ilmentää yhteiskuntatieteiden tietoturvatietoisuuden tuloksia suhteessa koko aineiston tulokseen.



Kuva 13. Yhteiskuntatieteiden henkilöstön ja opiskelijoiden tulokset suhteessa keskiarvoon

Yhteiskuntatieteiden opiskelijoiden tietomuuttujan keskiarvo oli poikkeuksellisen korkea. Se oli tiedekunnan henkilöstöä korkeampi ja muiden tiedekuntien opiskelijoihin verrattuna korkein. Vaikka opiskelijoiden tietomuuttujan keskiarvo oli henkilöstöä korkeampi, henkilöstön ja opiskelijoiden tiedon mediaanit olivat lähes samat. Yhteiskuntatieteiden henkilöstön käyttäytymisen tulos oli poikkeuksellisen matala ja tutkimuksen heikoin.

7. Pohdinta

Tutkielman tavoitteena oli tutkia Lapin yliopiston opiskelijoiden ja henkilöstön tietoturvatietoisuutta sekä tarkastella, miten tieto, asenne ja käyttäytyminen eroavat vastaajaryhmien välisesti. Tutkimuksen tuloksista havaittiin, että tietoturvatietoisuuden taso oli pääsääntöisesti riittävällä tasolla, mutta erityisesti tietoturvakäyttäytymiseen liittyi haasteita. Pohdintaluvussa tarkastellaan tulosten keskeisiä havaintoja, niiden merkitystä sekä tutkimuksen luotettavuutta ja jatkotutkimusmahdollisuuksia.

Tietoturvatietoisuuden haasteena käyttäytyminen

Tutkimuksen tulokset ilmentävät aikaisempien raporttien tuloksia siitä, että ihminen on tietoturvan heikoin lenkki (Sasse, Brostoff & Wairich 2011, 122; Crossler, Johnston, Lowry, Qing Hu, Warkentin & Baskerville 2013, 91; Security today). Suurin osa onnistuneista tietoturvaan kohdistuneista hyökkäyksistä ovat seurauksia toimijoiden sosiaalisesta manipuloinnista (Mitcnick & Simon 2022, 4).

Vastaajat suhtautuvat asenteeltaan tietoturvaan positiivisesti ja tiedon taso on riittävä. Hyvä asenne ja riittävä tieto eivät suoraan näy käyttäytymisessä, mutta tulosten perusteella vastaajat siis tietävät ja ymmärtävät tietoturvan merkityksen, vaikka eivät välttämättä noudata turvallisia toimintatapoja käytännössä. Heikko tietoturvakäyttäytyminen voi johtua useista syistä, kuten käyttäytymisen automatisoitumattomuudesta, huolimattomuudesta, ajattelemattomuudesta, kiireestä tai organisaation tietoturvakulttuurin puutteista (Carpenter 2023).

Tutkimuksen merkittävimmät havainnot olivat opiskelijoiden yleisesti heikompi tietoturvatietoisuuden taso ja tietoturvatietoisuuden tasojen erot tiedekuntien välisesti. Opiskelijat ovat tietoturvatietoisuudeltaan heikompia kuin henkilöstö ja jäävät joltain osin riittävän tason alapuolelle. Kasvatustieteiden opiskelijoiden tulos on selvästi heikoin ja osittain alle riittävän tason. Tulokset antoivat viitteitä siitä, että opiskelijoiden tietoturvatietoisuus kaipaa vahvistamista.

Jatkoa ajatellen on perusteltua selvittää tiedekuntien välisille eroille tarkempia syitä ja kehittää tietoturvatietoisuutta tulosten mukaan. Henkilöstön tuloksista ilmenee yksittäisiä heikkouksia, kuten yhteiskuntatieteiden henkilöstön käyttäytymisen taso. Tietoturvatietoisuutta on syytä mitata ja ylläpitää systemaattisesti, eikä tällä tutkimuksella ei voida tuottaa faktapohjaista tietoa tietoturvatietoisuuden riittämättömyydestä tai riittävyydestä, mutta tutkimus viittaa siihen, että tietoturvakäyttäytymisessä esiintyy puutteita sekä henkilöstöllä että opiskelijoilla erityisesti käyttäytymisen osalta.

Henkilöstöllä korkeampi tietoturvatietoisuuden taso kuin opiskelijoilla

Henkilöstöön kuulumisella voitiin tulosten mukaan todeta olevan vaikutusta tietoturvatietoisuuden korkeampaan tasoon. Henkilöstön tietoturvatietoisuuden tiedon, aseteen ja käyttäytymisen tasot olivat yleisesti korkeammat kuin opiskelijoilla, ja erityisesti heidän asenteensa ja käyttäytymisensä olivat paremmalla tasolla. Henkilöstön korkeammat asenteen ja käyttäytymisen tasot viittaavat, että työtehtävien vastuut, vaadittava tietoturvakoulutus ja organisaation käytänteet yhtenäistävät ja vahvistavat henkilöstön tietoturvatietoisuuden tasoa.

HAIS-Q apuvälineessä esitetään tietoturvatietoisuuden taustalla vaikuttavia tekijöitä, joita olivat yksilölliset-, organisatoriset- ja välilliset tekijät. Opiskelijoiden vastaajaryhmässä ilmentyneet suuremmat tietoturvatietoisuuden tasoerot saattavat perustua siihen, että taso on vahvasti riippuvainen yksilön omista kyvyistä. Se tarkoittaa, että opiskelijoiden tietoturvatietoisuus on vahvemmin riippuvainen yksilöiden omista henkilökohtaisista tiedoista, taidoista ja kokemuksista. Yksilöllisiin tekijöihin perustuva osaaminen ei tällöin perustu yhtenäisiin toimintatapoihin, käytänteisiin ja koulutuksiin. Yksilöllisten tekijöiden voidaan ajatella olevan syy suurempaan hajontaan vastaajaryhmän yksilöiden välillä. Organisatoristen tekijöiden ja välillisten tekijöiden vaikutus on todennäköisesti opiskelijoilla vähäisempää ja se voi selittää opiskelijoiden tuloksien pääsääntöisesti heikompien tasojen ja erojen syitä.

Myös henkilöstön tietoturvatietoisuuden korkeaan ja tasaiseen tulokseen vaikuttavat yksilölliset tekijät, mutta sen lisäksi organisatoriset ja välilliset tekijät vahvemmin kuin opiskelijoilla. Henkilöstön tietoturvatietoisuuden taso perustuu opiskelijoita vahvemmin yhteisiin lähtökohtiin, kuten tiukempiin tietoturvavaatimuksiin, pakolliseen tietoturvakoulutukseen ja organisaation tietoturvaa edistäviin kampanjoihin. Ne yhtenäistävät ja parantavat vastaajaryhmän tuloksia.

Opiskelijoiden tulokset ovat jakautuneet epätasaisemmin ja ääripäihin. Mielenkiintoisena havaintona on, että opiskelijoilla huipputuloksien osuus on tieto ja käyttäytymismuuttujien osalta suurempi kuin henkilöstöllä. Tämä viittaa myös siihen, että opiskelijoiden tulokset ovat riippuvaisia yksilön omista tiedoista, taidoista ja kokemuksista.

Oikeustieteiden ja taiteiden tiedekunnilla tietoturvatietoisuudet vahvimmat

Oikeustieteellisen tiedekunnan tietoturvatietoisuus oli tutkimuksen tulosten mukaan korkein ja riittävällä tasolla. Taiteiden tiedekunnan tietoturvatietoisuuden taso oli myös riittävällä tasolla ja viittasi pienellä keskihajonnalla ja keskivertoa korkeammilla keskiarvotuloksilla tasaisenvahvaan tietoturvatietoisuuden tasoon. Yhteiskuntatieteiden tietoturvatietoisuuden taso oli heikompi kuin oikeustieteillä ja taidetieteillä, mutta selvästi vahvempi kuin kasvatustieteillä. Kasvatustieteiden tulokset jäivät kokonaispisteiden osalta alle riittävän tason. Kasvatustieteiden tiedekunnan heikon tuloksen osalta olisi kiinnostavaa tietää, että löytyykö heikkoon tietoturvatietoisuuden tasoon syy ammatin rakenteissa vai onko kasvatustieteiden tiedekunnan tietoturvaopetus erilaista.

Yhteiskuntatieteiden tietomuuttujan tulos oli poikkeuksellisen korkea. Yhteiskuntatieteiden tietomuuttujan korkea tulos on erityinen myös siitä syystä, että tutkimuksen kysymyspatteristo painottui yli 60 % osuudella tietoaiheisiin kysymyksiin. Mielenkiintoista olisi selvittää miksi yhteiskuntatieteiden tietomuuttujan tulos oli niin korkea, mutta asenteen tulos oli keskivertainen ja käyttäytymisen tulokset olivat matala.

Tiedekuntien tulosten ja niiden välisten erojen syytä on haasteellista selittää tarkasti ilman yksityiskohtaisempaa tutkimusta erojen syistä. Tiedekuntien välisesti voitiin havaita vahvimmat ja heikoimmat tiedekuntakohtaiset tietoturvatietoisuuden tasot, mutta sen syytä ei tässä tutkimuksessa tutkittu tarkemmin. Mielenkiintoista olisi etsiä tarkempia vastauksia siihen, löytyykö selittäviä tekijöitä esimerkiksi ammattikunnasta, opetuskulttuurista tai jostain muualta. Toisin sanoen, mielenkiintoista olisi tutkia opetuskulttuurin ja kohdeammatin vaikutusta tietoturvatietoisuuden tasoon kaikissa tiedekunnissa tai jopa eri yliopistojen välillä.

Kasvatustieteiden ja oikeustieteiden henkilöstön tulokset vahvemmat kuin tiedekunnan opiskelijoilla

Tiedekuntakohtaisen roolien välisten tulosten tarkastelun tärkeinä havaintoina olivat kasvatustieteiden tiedekunnan opiskelijoiden heikko taso verrattuna tiedekunnan henkilöstöön**.** Oikeustieteiden henkilöstön tulosten taso oli selvästi korkeampi kuin opiskelijoilla. Oikeustieteiden erona kasvatustieteisiin oli, että molempien - henkilöstön ja opiskelijoiden – vastaajaryhmien tulokset olivat suhteellisen korkeat.

Oikeustieteiden tiedekunnan henkilöstön tulokset olivat koko tutkimuksen vahvimmat. Oikeustieteellisen tiedekunnan henkilöstön ja opiskelijoiden korkea tietoturvatietoisuuden taso on looginen, koska tietoturvan korostuminen nyky-yhteiskunnassa näkyy vahvasti lainsäädännössä. Esimerkkejä tietoturvan vaikutuksesta lainsäädäntöön ovat tuore NIS2 direktiivi ja laki julkisen hallinnon tiedonhallinnasta. Lait ja asetukset ovat esimerkkejä siitä, että tietoturva ja siihen liittyvät säädökset ovat olleet ja ovat edelleen näkyviä ja ajankohtaisia aiheita oikeustieteiden ammatissa.

Taiteiden tiedekunnan opiskelijoiden ja henkilöstön välillä ei ollut merkittäviä eroja tietoturvatietoisuuden tasoissa. Se viittaa siihen, että tiedekunnan opiskelijoiden ja henkilöstön tietoturvakulttuuri ja toimintatavat ovat yhtenäiset. Syy tähän voi olla taiteiden tiedekunnan koulutuksen suurempi riippuvuus tietotekniikasta, ja se nostaa tietoturvan konkreettiseksi ja tärkeäksi osaksi jokapäiväistä toimintaa.

Yhteiskuntatieteiden henkilöstön ja opiskelijoiden tulokset olivat poikkeukselliset, koska opiskelijoiden tietoturvatietoisuuden taso oli korkeampi kuin henkilöstöllä. Tiedekunnan opiskelijoiden tietomuuttuja oli opiskelijoista muodostettujen tiedekuntakohtaisten vastaajaryhmien tuloksista keskiarvoltaan korkein. Korkea tietomuuttujan ohella käyttäytymismuuttuja oli heikko ja asennemuuttuja keskiarvoinen. Yhteiskuntatieteiden henkilöstön tuloksista merkittävänä huomiona oli heikko käyttäytymismuuttujan tulos. Henkilöstön käyttäytymisen keskiarvo oli niin heikko, että tuloksen luotettavuutta on syytä epäillä.

Tutkimuksen luotettavuus ja haasteet

Verkkokyselyyn liittyy luotettavuuteen vaikuttavia haasteita, jotka on syytä tunnistaa. Aineistossa esiintyi vahvaa vastaajien jakautumista ja kyselyyn vastanneiden aktiivisuus oli suhteellisen vähäistä. Näiden tekijöiden seurauksena tutkimuksen luotettavuus voi heikentyä. Tutkimuksessa 77 % oli opiskelijoita ja vain 23 % henkilöstöä. Epätasainen jakautuminen voi vaikuttaa tulosten yleistettävyyteen ja vinouttaa tuloksia. Erityisesti tiedekuntakohtaiset henkilöstön vastaajaryhmät muistuttivat kooltaan laadullisen tutkimuksen kokoluokkaa ja niiden tuloksia on tulkittava harkiten ja suuntaa antavasti.

Verkkokysely on tehokas aineistonkeruumenetelmä ja se soveltui hyvin tämän tutkimuksen aineistonkeruumenetelmäksi hajautuneen kohderyhmän tavoittamiseksi ajasta ja paikasta riippumattomasti. Kyselytutkimukset voivat kuitenkin olla vastaajille epämieluisia ja vastausaktiivisuus saattaa jäädä pieneksi. Tutkimusaineiston kerääminen aloitettiin myöhään keväällä ja kyselyä pidettiin auki heinäkuun loppupuolelle asti. Ajankohta on haasteellinen, koska opiskelijat irtautuvat opinnoistaan lomalle ja töihin kesän ajaksi ja henkilöstöstä suuri osa oli mahdollisesti kesälomalla. Aineistonkeruun ajankohta on saattanut vaikuttaa osaltaan kyselyn vastaajien aktiivisuuteen sekä henkilöstön että opiskelijoiden osalta. Vastausaktiivisuus oli tämän tutkimuksen osalta suhteellisen pieni.

Aineiston keruu toteutettiin sähköpostilistoja hyödyntämällä tiedekuntakontaktien kautta. Tiedekuntia pyydettiin jakamaan kyselytutkimus opiskelijoille ja henkilöstölle. Sähköpostilistoista ja jakamisen laajuudesta päättivät lopulta tiedekunnan virkailija, eikä jakamista kontrolloitu tarkemmin. Kyselytutkimuksen jakamisen vaikutusta on vaikea arvioida yksityiskohtaisesti. Kyselytutkimuksen jakamista olisi ollut hyvä kontrolloida tarkemmin esimerkiksi seuraamalla tietoja vastaanottajien lukumääristä. Voi olla epärealistista ajatella, että tiedekunnilta olisi saatu tietoa myös henkilöstön ja opiskelijoiden lukumääristä, mutta näillä tiedoilla olisi voitu saada tarkempaa tietoa vastaajien aktiivisuudesta.

Kyselytutkimuksen luotettavuuteen saattaa vaikuttaa myös itsevalikoitumisharha. Vastaamisen perustuessa vapaaehtoisuuteen, se saattaa johtaa vastaajien valikoitumiseen tietoturvasta keskimääräisesti kiinnostuneempiin yksilöihin. Tietoturvasta kiinnostuneiden yksilöiden valikoituminen tutkimukseen puolestaan voi nostaa vastaajien keskiarvoja suhteessa perusjoukkoon ja vääristää todellisuutta.

Kyselytutkimuksen luotettavuuteen liittyy vahvasti myös vastaajien motivaatio ja huolellisuuden vaihtelu. Kyselylomake muodostui pitkäksi, vaikka sen pituutta pyrittiin lyhentämään suunnitteluvaiheessa. Kysymystyyppejä pyrittiin keventämään vastaajaystävällisiksi suunnittelemalla kysymystyypit monipuolisiksi. Kyselylomakkeen pituus on saattanut vaikuttaa vastaajien keskittymiseen ja huolellisuuteen etenkin kyselyn loppupuolella.

Tutkimuksessa käytetty HAIS-Q-mittari on aiemmissa tutkimuksissa validoitu apuväline tietoturvatietoisuuden mittaamiseen. Tässä tutkimuksessa mittaria sovellettiin yliopistoympäristöön, ja kysymykset muokattiin vastaamaan Lapin yliopiston tietoturvakäytänteitä. Mittarin sovellettavuus vahvistaa tutkimuksen luotettavuutta. Mittariston soveltaminen korkeakoulukontekstiin voisi jatkotutkimuksissa kaivata lisävalidointia.

Jatkotutkimusehdotukset

Tutkimus herätti useita jatkokysymyksiä, joihin eri jatkotutkimuksilla voitaisiin tarjota vastauksia. Ensinnäkin havainto siitä, että käyttäytyminen oli heikoin tietoturvatietoisuuden osa-alue, kaipaa tarkempaa tutkintaa. Aihetta voitaisiin lähestyä laadullisella tutkimuksella, jossa opiskelijoita ja henkilöstöä haastateltaisiin siitä, miten he noudattavat tietoturvakäytäntöjä.

Toinen jatkotutkimusidea liittyy tiedekuntakohtaisiin eroihin tietoturvatietoisuudessa, jota olisi hyödyllistä tarkastella tiedekuntien tietoturvakoulutuksen, opetuksen, perehdytyksen ja painotuksen näkökulmasta. Tutkimuksessa voitaisiin selvittää tietoturvakäytänteiden eroja eri oppialojen, tiedekuntien tai oppilaitosten välillä.

Kolmantena jatkotutkimusehdotuksena on tietoturvakoulutuksen vaikutuksien tutkiminen. Tutkimus voitaisiin toteuttaa interventiona, jossa osa vastaajista saa lisäkoulutusta tietoturvaan. Vastaajajoukkojen käyttäytymistään seurattaisiin ennen koulutusta ja sen jälkeen, jotta mahdolliset muutokset voitaisiin tunnistaa.

Neljäs jatkotutkimusaihe muodostuu ajatuksesta, että miksi tieto ei johda toimintaan? Tämä kysymys tarjoaa kiinnostavan tutkimusnäkökulman ja liittyy siihen, miten yksilöiden tietoturvakäyttäytymistä voidaan muuttaa tehokkaammin.

Viidennes jatkotutkimusehdotus koskee tutkimusotantaa, jota olisi hyvä laajentaa. Suuremmalla vastaajajoukolla saataisiin tarkempaa tietoa siitä, miten esimerkiksi roolit ja tiedekunnat vaikuttavat tietoturvatietoisuuden tasoon. Tämä lisäisi tutkimuksen yleistettävyyttä ja tarjoaisi mahdollisuuden tehdä tarkempia vertailuja eri taustamuuttujien välillä.

Jatkotutkimusehdotusten osalta tärkeää olisi laajentaa aineistoa tai kerätä kokonaan uusi aineisto. Suuremmalla ja laajemmalla aineistolla voitaisiin testata tämän tutkimuksen tuloksia ja varmentaa tutkimuksen poikkeavien tuloksien validiteettia. Laajemmalla aineistolla tietoturvatietoisuuden erojen tarkastelua voitaisiin toteuttaa tarkemmin ja tarkastella ilmiötä uusista näkökulmista.

Tutkimusta tehdessä osaamisen käsite nousi usein esille. Tämä tutkimus ei tutkinut osaamista, koska osaamisen mittaamiseksi tarvitaan huomattavasti tarkempaa tietoa. Kasvatustieteissä usein käytetyn osaamisen käsitteen ja sen teorian liittäminen tietoturvatietoisuuden tutkimukseen voisi tuottaa merkittävää lisäarvoa tietoturvatietoisuuden tutkimuksen aihealueelle. Kasvatustieteellisestä ammattitaidosta voitaisiin hyötyä tietoturvatietoisuuden aihepiirin tutkimuksessa.

Lähteet

Andrade C, Menon V, Ameen S, Kumar Praharaj S. Designing and Conducting Knowledge, Attitude, and Practice Surveys in Psychiatry: Practical Guidance. Indian Journal of Psychological Medicine. 2020;42(5):478-481. doi:10.1177/0253717620946111

Ardner, B & Thomas, V. 2014. c Defending Against Social Engineering and Technical Threats. E-kirja. Rockland, MA: Elsevier Science & Technology Books.

Andress, J. (2011). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice. Syngress.

Ashenden, D. 2008, Information Security management: A human challenge? Information Security Technical Report, 13(4), 195–201. http://www.sis.pitt.edu/jjoshi/courses/IS2621/Spring2014/Paper1.pdf

Butavicius, M., Calic, D., McCormac, M., Parsons, K., Pattinson, M. & Zwaans T. (2017) Individual differences and information security awareness. Computers in human behaviour. 151

Carpenter, P. 2023. The Knowledge, Intention and Behavior Gap in Cybersecurity: How to Close It. *Security Today*, 22.8.2023. Saatavilla: https://securitytoday.com/articles/2023/08/22/the-knowledge-intention-and-behavior-gap-in-cybersecurity.aspx. Viitattu 24.03.2025

Crossler R., Johnson A., Lowry P., Qing H., Warkentin M. & Baskerville R. (2013) Future directions for behavioural information security research. Computers & Security, 91. Saatavilla: https://daneshyari.com/article/preview/6884336.pdf

Doering, J. (2024, October 14). *What is the difference between information security and data protection*. Secfix. Saatavilla: https://www.secfix.com/post/what-is-the-difference-between-information-security-and-data-protection Luettu 9.4.2025

Elinkeinoelämän keskusliitto. 2016. *Elinkeinoelämän yritysturvallisuusmalli*. Saatavilla: https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf. Luettu 23.04.2023.

Grimmick R. (2023) What is a Security Policy? Definition, Elements, and Examples. Saatavilla: https://www.varonis.com/blog/what-is-a-security-policy#definition Luettu 12.06.2023.

Guba, E. G. & Lincoln, Y. S. 1994. Competing paradigms in qualitative research. Teoksessa N. K. Denzin & Y. S. Lincoln (toim.), *Handbook of qualitative research*, 105–117. Thousand Oaks, CA: Sage Publications. Saatavilla: https://miguelangelmartinez.net/IMG/pdf/1994_Guba_Lincoln_Paradigms_Quali_Research_chapter.pdf. Luettu 10.4.2025.

Helsingin yliopisto. 2025. *Tietoturva yliopistolla*. Tietotekniikkakeskus. Saatavilla: https://www.helsinki.fi/fi/tietotekniikkakeskus/tietoturva-yliopistolla. Luettu 24.11.2023.

Helsingin yliopisto. 2022. *Yliopiston tietoturvapolitiikka*. Tietotekniikkakeskus. Saatavilla: https://www.helsinki.fi/fi/tietotekniikkakeskus/tietoturva-yliopistolla/tietoturva-ja-tietosuoja/yliopiston-tietoturvapolitiikka. Luettu 24.11.2023.

ISO/IEC 27001. Saatavilla: https://cdn.standards.iteh.ai/samples/82875/726bcf58250e43d9a666b4d929c8fbdb/ISO-IEC-27001-2022.pdf

ISO/IEC 27002. https://www.trofisecurity.com/assets/img/ISO-IEC_27002-.pdf

Jyväskylän yliopisto 2025. *Survey*. Jyväskylän yliopisto. Saatavilla: https://sites.app.jyu.fi/mehu/fi/menetelmapolku/tutkimusstrategiat/survey. Luettu 30.08.2023.

Jyväskylän yliopisto 2025. *Tieteenfilosofiset suuntaukset*. Jyväskylän yliopisto. Saatavilla: Saatavilla: https://sites.app.jyu.fi/mehu/fi/menetelmapolku/tieteenfilosofiset-suuntaukset. Luettu 10.4.2025.

Karvi T. 2011, Tietoturvan perusteet, luku 1: yleistä tietoturvasta. Helsingin yliopisto. verkkolähde: https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_11.pdf

Koohang A., Springer Sargent C., Horn Nord J. & Paliszkiewicz J. (2022) International Journal of Information Management, Internet of Things (IoT): From awareness to continued use, volume 62. Saatavilla: https://www.sciencedirect.com/science/article/pii/S0268401221001353

Kruger, H. A. & Kearney, W. D. 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296. Saatavilla: https://www.researchgate.net/publication/222422461_A_prototype_for_assessing_information_security_awareness. Luettu 10.4.2025.

Malinen, L. M. 2021. *The Human Element in IT Security*. Bachelor's Thesis. Degree Programme in Business Information Technology. Haaga-Helia ammattikorkeakoulu. Saatavilla: https://www.theseus.fi/bitstream/handle/10024/495843/The%20Human%20Element%20in%20IT%20Security.pdf. Luettu 10.4.2025.

Mitcnick K. & Simon W. (2011) The art of deception: controlling human element of security. John Wiley & Sons. Saatavilla: https://books.google.fi/books?hl=fi&lr=&id=rmvDDwAAQBAJ&oi=fnd&pg=PR7&dq=mitnick+%26+Simon+2002+.pdf&ots=_fy0QB3-S9&sig=P_qI7Q1zF7zrzy0JF_CyoUPoyVw&redir_esc=y#v=onepage&q&f=false

Mäkinen A. (2022) Tietoturvatietoisuuden kehittäminen finanssialan organisaatiossa. Pro gradu -tutkielma. Turun yliopisto. Saatavilla: https://www.utupub.fi/bitstream/handle/10024/173006/Makinen_Aliisa_opinnnayte.pdf?sequence=1

National Institute of Standards and Technology (2003) Building an Information Technology Security Awareness and Training Program. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Nilivaara, P., Saarnio, M., Vainikainen, M., Aitto-oja, A., & Hienonen, N. (2022). Laaja-alainen osaaminen koulussa: Ajattelijana ja oppijana kehittyminen. Gaudeamus.

Opetushallitus. *Tietoturva ja -suoja koulussa*. Saatavilla: https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa Luettu 9.4.2025

Opintokeskus Sivis, Osaamisen tunnistaminen. Saatavilla: https://www.ok-sivis.fi/tunnista-ja-tunnusta-osaaminen/osaamisen-tunnistaminen.html Luettu 23.04.2023.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T. (2017) The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers and Security, 66, 40–51

Parsons, Kathryn & McCormac, Agata & Butavicius, Marcus & Pattinson, Malcolm & Jerram, Cate. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security. 42. 10.1016/j.cose.2013.12.003. Saatavilla: https://www.researchgate.net/publication/259991932_Determining_Employee_Awareness_Using_the_Human_Aspects_of_Information_Security_Questionnaire_HAIS-Q/citation/download

Sanastokeskus ry, Security, viitattu 30.01.2023. https://termipankki.fi/tepa/fi/haku/security

Sanastokeskus ry, Turva, viitattu 30.01.2023. https://termipankki.fi/tepa/fi/haku/turva

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Schrader, P.G. & Lawless, Kimberly. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. Performance Improvement. 43. 8 - 15. 10.1002/pfi.4140430905. https://www.researchgate.net/publication/229542766_The_knowledge_attitudes_behaviors_approach_how_to_evaluate_performance_and_learning_in_complex_environments

Sobers S. 89 Must-Know Data Breach Statistics 2022. Viitattu 24.04.2023. https://www.varonis.com/blog/data-breach-statistics

Tampereen korkeakouluyhteisö. 2023. *Tietoturva lyhyesti*. Saatavilla: https://www.tuni.fi/fi/it-palvelut/kasikirja/tietoturva/tietoturva-lyhyesti. Viitattu 10.4.2025.

Tampereen yliopisto 2023. kyberturvallisuus 1: inhimmilliset tekijät.

Tietoarkisto. 2025. *Tilastollinen päättely*. Tampereen yliopisto. Saatavilla: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/paattely/paattely/. Luettu 06.11.2024.

Tilastokeskus. 2025. *Peruskäsitteet tutuiksi*. Tilastojen lukutaito -opas. Saatavilla: https://guides.stat.fi/c.php?g=686459&p=4906523. Luettu 27.03.2025

Tietosuojavaltuutetun toimisto. *Tietosuoja*., Saatavilla: https://tietosuoja.fi/tietosuoja Luettu 9.4.2025

Toth P. & Klein P. (2014) A Role-Based Model for Federal Information Technology/ Cybersecurity Training. NIST Special publication, 800-16, Revision 1 (3rd Draft) https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf

Turvallisuuskomitea, kyberturvallisuussanasto, 2018. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Tietoturvallisuudella tuloksia – yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007. Saatavilla: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2008.pdf

Valtiovarainministeriö, Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008. Saatavilla: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2008.pdf

Veiga, Adéle & Martins, N. & Eloff, Jan. (2007). Information security culturevalidation of an assessment instrument. South. African Bus. Rev. 11. 146-166. https://www.researchgate.net/publication/313639012_Information_security_culturevalidation_of_an_assessment_instrument

Vilkka, H. 2007. Tutki ja mittaa: määrällisen tutkimuksen perusteet. Helsinki: Tammi.

Wilson, M. – Hash, J. 2003, Building an Information Technology Security Awareness and Training Program. NIST Special publication, 800(50), 1–39. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Zoto E., Cybersecurity and Computer Networks IIKG1001, Norwegian University of Science and Technology, 26.09.2022.

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security* (6th ed.). Cengage Learning.

Liitteet

Liite 1. Kyselylomake

Kysely tietoturvatietoisuudesta

Tämän kyselyn keskiössä on tietoturvatietoisuus eli se, millainen tietämys sinulla on tietoturvasta, tietoturvakäytänteistä ja tietoturvaohjeista. Kysely on kohdennettu Lapin yliopiston nykyisille opiskelijoille ja henkilöstölle.

Kysely on rakennettu pedagogisella otteella, jolloin kysely myös perehdyttää vastaajia Lapin yliopistoa koskevaan tietoturvaan käyttäjän näkökulmasta.

Joidenkin käsitteiden määritelmät avautuvat, kun osoitat katkoviivalla alleviivattua sanaa. Esim. tietoturva. (huom. Ei toimi kosketusnäytöllä). Jokaisen osion alussa on käsitteiden määritelmiä yhteisen ymmärryksen tueksi.

Käytän kyselyn tuloksia aineistona opinnäytetyössäni. Kerään aineiston anonyymina eikä vastaajia voida tunnistaa vastausten perusteella. Vastaamalla tähän kyselyyn annat luvan käyttää vastauksiasi aineistona opinnäytetyössäni.

Kiitos, että vastaat kyselyyni! Ystävällisin terveisin,

Nooa Sarkkinen
Kasvatustieteiden tiedekunta - Kasvatustieteiden maisteriohjelma,
luokanopettajakoulutus
nsarkkin@ulapland.fi

Osio 1. Yleinen tietoturva

Riski (tietoturva) = Omiin tärkeisiin tiedostoihin tai henkilötietoihin kohdistuva yleinen uhka tai käsittelemiisi toisten henkilötietoihin tai tärkeisiin tiedostoihin kohdistuva uhka. esim. Häviäminen, tuhoutuminen, katoaminen ja väärinkäyttö

1. Mikä seuraavista on **suurin** tietoturvaan kohdistuva riski?

Valitse yksi vaihtoehto

Ihmisperäinen virhe / käyttövirhe
Ohjelmistoperäinen vika tai haavoittuvuus
Järjestelmän/laitteen vika tai haavoittuvuus
Hakkerit ja tarkoitukselliset toimijat

2. Mitkä seuraavista vaihtoehdoista ovat tietoturvaan kohdistuvia uhkia?

Valitse vähintään yksi vaihtoehto

Kahvin kaatuminen tietokoneelle ja laitteen tuhoutuminen
Vahinkoperäinen tiedoston poistaminen tai kadottaminen
Luonnonkatastrofi tai luonnonilmiö
Laitteesta tai ohjelmistosta johtuva bugi
Tarkoituksellisen toimijan toimittama haittaohjelma tai tietojen kalastelu
Käyttäjän oma virhe tai vahinko

3. Kuinka suuri vaikutus yksilöiden tietoturvakäyttäytymisellä on koko organisaation tietoturvan osalta?

Valitse yksi vaihtoehto

1. Ei vaikutusta
2. Pieni vaikutus
3. Kohtalainen vaikutus
4. Suuri vaikutus
5. Erittäin suuri vaikutus
   En osaa sanoa

4. Vastaa yleistä tietoturvaa koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-Tietoturvallisuus on minulle tärkeää
1 | 2 | 3 | 4 | 5 | 6
-Luen LUC:n lähettämiä tietoturvaa käsitteleviä sähköposti-ilmoituksia
1 | 2 | 3 | 4 | 5 | 6

Osio 2. Käyttäjätunnus- ja salasanaturvallisuus

5. Vastaa yleistä tietoturvaa koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

- Yliopistotunnuksen salasanaa ei tule käyttää missään muissa palveluissa
  1 | 2 | 3 | 4 | 5 | 6
- Salasanaa ei ole suositeltavaa säilöä tekstitiedostona
  1 | 2 | 3 | 4 | 5 | 6
- Yliopistotunnuksen salasanan jakaminen luotetulle henkilölle on turvallista
  1 | 2 | 3 | 4 | 5 | 6
- Saan antaa minun yliopiston palveluiden salasanan toiselle henkilölle
  1 | 2 | 3 | 4 | 5 | 6

6. Mitkä ovat vahvan salasanan piirteitä?

Voit valita useita vaihtoehtoja

Salasana on muistettava

Salasana ei sisällä käyttäjään yhdistettäviä tietoja tai sanoja.

Salasana on uniikki tai käyttämätön uusi salasana

Mitä pitempi salasana, sitä turvallisempi.

Salasana ei saa olla yksittäinen sana.

Salasana ei saa olla yleisimmin käytettyjen sanojen joukossa.

7. Lapin yliopiston ohjeiden mukaan sinun tulisi käsitellä työ- tai opiskelutunnusta samalla huolellisuudella kuin _____.

Valitse yksi vaihtoehto

… Osoitetietojasi

… puhelinnumeroasi

… Tunnuslukuasi tai pankkikorttiasi

Osio 3. Sähköpostiturvallisuus

8. Vastaa seuraaviin sähköpostiturvallisuutta koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta.

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-On turvallista avata tuntemattomalta lähettäjältä saapuneen viestin linkki.
1 | 2 | 3 | 4 | 5 | 6
-On turvallista avata tuntemattomalta lähettäjältä saapuneen viestin liitetiedosto.
1 | 2 | 3 | 4 | 5 | 6
-Pelkästä sähköpostilinkin avaamisesta ei voi tapahtua mitään vahingollista.
1 | 2 | 3 | 4 | 5 | 6
-On tärkeää olla jatkuvasti "*sopivan valppaana*" sähköpostin lähettäjän tai sisällön luotettavuudesta.
1 | 2 | 3 | 4 | 5 | 6
-Harkitsen sähköpostiviestin linkkien klikkaamista, vaikka ne tulisivat tunnetulta lähettäjältä.
1 | 2 | 3 | 4 | 5 | 6
-En klikkaa tuntemattomalta lähettäjältä saapuneen sähköpostiviestin linkkejä.
1 | 2 | 3 | 4 | 5 | 6
-Olen "*terveen epäileväinen*" sähköpostiviestien linkkien luotettavuudesta.
1 | 2 | 3 | 4 | 5 | 6

9. Miten yliopiston ohjeiden mukaan tulee toimia, jos saat toiselle henkilölle tarkoitetun sähköpostin?

Valitse alta yksi vaihtoehto.

Välitän viestin oikealle vastaanottajalle ja ilmoitan väärästä sähköpostiosoitteesta lähettäjälle.
Poistan viestin ja jätän sen huomioimatta.
Teen ilmoituksen tietoturvatapoikkeuksesta.
Ilmoitan lähettäjälle väärästä osoitteesta. En välitä viestiä oikealle vastaanottajalle.
Poistan viestin, koska sitä ei ole tarkoitettu minulle luettavaksi. En ilmoita kenellekään erikseen.
Olen hallinnollisessa tehtävässä, minulla on eri toimintaohjeet.

10. Osaatko tarkastella *sähköpostiviestin* linkin luotettavuutta tai turvallisuutta?

En
Kyllä
|
|_____ (Jos kyllä)

11. Miten tarkastat tai tarkastelet linkin turvallisuutta?

Osio 4. Internet-turvallisuus

Luottamuksellinen tieto = Tieto, joka on vain sallittujen ja oikeutettujen henkilöiden käytettävissä ja nähtävissä.
Julkinen verkko = avoin langaton verkko on radioteitse toimiva tiedonsiirtoverkko, joka on avoimesti yleisön käytettävissä.

12. Vastaa seuraaviin internet-turvallisuutta koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta.

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-Luottamuksellisen tiedon tai sähköpostin lähettäminen kahvilan julkisessa wifi-verkossa voi olla riskialtista.
1 | 2 | 3 | 4 | 5 | 6
-Olen "terveen epäluuloinen" ennen kuin syötän tietojani verkkosivulle.
1 | 2 | 3 | 4 | 5 | 6
-Ohjelmistojen ja tiedostojen lataaminen verkkosivuilta ei sisällä riskiä.
1 | 2 | 3 | 4 | 5 | 6
-Pyrin lataamaan työ- tai opiskelukoneelleni ohjelmistoja vain ohjelmistokaupan kautta.
1 | 2 | 3 | 4 | 5 | 6
-Vältän verkossa mainosten ja ponnahdusikkunoiden ajattelematonta klikkaamista.
1 | 2 | 3 | 4 | 5 | 6
-Klikkaan verkkomainoksia ja ponnahdusikkunoita.
1 | 2 | 3 | 4 | 5 | 6

Osio 5. Sosiaalisen median ja internetpalveluiden tietoturva

Some = sosiaalinen media, kuten Facebook, LinkedIn, Instagram ym.
Verkkopalvelu = Verkon välityksellä toimiva palvelu. (esim. google drive, youtube, X, Tori.fi, Dropbox, muut pilvipalvelut, ResearchPortal, ChatGPT ym.)

13. Vastaa seuraaviin sosiaalista mediaa ja internetpalveluita koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta.

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-Kerran verkkoon laitettua kuvaa tai tietoa voi olla mahdotonta saada poistettua.
1 | 2 | 3 | 4 | 5 | 6
-On mahdollista, että sosiaalisesta mediasta kerättyjä tietojani voitaisiin käyttää minua vastaan.
1 | 2 | 3 | 4 | 5 | 6
-Henkilökohtaisella tietoturvalla ei ole vaikutusta työ- tai opiskelupaikan tietoturvan näkökulmasta.
1 | 2 | 3 | 4 | 5 | 6
-Minulle on merkityksellistä mitä tietoja ja asioita julkaisen sosiaalisessa mediassa.
1 | 2 | 3 | 4 | 5 | 6
-Olen tarkastanut sosiaalisen median yksityisyysasetukset.
1 | 2 | 3 | 4 | 5 | 6

14. Valitse alta *asetukset, jotka on* ***suositeltava tarkistaa*** ennen verkkopalvelun käyttöönottoa.

Valitse yksi tai useampi vaihtoehto

Palveluun antamieni tietojen omistajuuden säilyminen (nimi, osoite, työ ym.)
Tietojen luovutusoikeudet
Käyttäjänimi
Profiilin julkisuus
Profiilin toiminnan julkisuus
Profiilin tietojen julkisuus
Palveluun ladattujen tiedostojen omistajuus (kuvat, videot, tiedostot)
Palveluun ladattujen tiedostojen julkisuus (kuvat, videot, tiedostot)
Profiilin lähipiirin julkisuus (Ystävät, tuntemani ihmiset ym.)

Osio 6. Etätyöskentely, etälaitteet, mobiililaitteet

Omatietokone = Omistamani laite

Julkinen tietokone = Yleisessä käytössä oleva tietokone (esim. kahvila, kirjasto ym.)

Toisen omistama = Lapin yliopiston yhteiset tietokoneet, ystävän tietokone ym.

Ylläpito-oikeudet = Ylläpito-oikeudet antavat kyvyn **muuttaa** turvallisuusasetuksia, ***tehdä muutoksia*** toisille käyttäjille ja **asentaa** ohjelmistoja ja laitteita. Ylläpito-oikeudet mahdollistavat **toisiin käyttäjiin vaikuttavat muutokset**.

15. Vastaa seuraaviin etätyöskentelyä, etälaitteita ja mobiililaitteita koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta.

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-Olen yksin vastuussa omistamani tietokoneen tietoturvasta.
1 | 2 | 3 | 4 | 5 | 6
-Ylläpito-oikeuksille on suositeltavaa luoda erillinen käyttäjä omalla tietokoneella tai kotikoneella.
1 | 2 | 3 | 4 | 5 | 6
-Työ- tai opiskelukone tulee pitää valvottuna julkisilla paikoilla.
1 | 2 | 3 | 4 | 5 | 6
-Julkisen tietokoneen käyttämiseen ei sisälly erillistä tietoturvariskiä.
1 | 2 | 3 | 4 | 5 | 6
-Kahvilan verkkoyhteyden käyttäminen omalla koneella on yhtä turvallista kuin kotiverkon tai yliopiston eduroam-verkon käyttäminen.
1 | 2 | 3 | 4 | 5 | 6
-Tietokoneen tai mobiililaitteen säännöllinen varmuuskopiointi on tärkeää.
1 | 2 | 3 | 4 | 5 | 6
-Olen varautunut siihen, jos laitteeni varastettaisiin.

16. Mitkä ovat oman tietokoneen suojaamisen vähimmäisvaatimukset Lapin yliopiston ohjeiden mukaan.

Valitse vähintään yksi vaihtoehto

Palomuuri

Haittaohjelmantorjunta

Pääsykoodilla tai salasanalla suojaaminen

Säännöllinen varmuuskopiointi

Säännöllinen ohjelmiston ja käyttöjärjestelmän päivittäminen

Säännöllinen tietokoneen käyttäminen

17. Valitse alta Lapin yliopiston mobiililaitetta koskevat tietoturvaohjeet.

Valitse vähintään yksi vaihtoehto

Älä avaa tuntemattomia tai epäilyttäviä tekstiviestejä.

Suojaa mobiililaitteesi varastamiselta

Sulje langattomat yhteydet aina kun et tarvitse niitä.

Varmuuskopioi mobiililaitteen tiedostot.

Lataa vain tarvittavat ohjelmistot.

Lataa ohjelmistot vain virallisista kauppapaikoista.

Suojaa mobiililaitteesi vähintään pääsykoodilla.

Päivitä ohjelmistot ja käyttöjärjestelmä säännöllisesti.

Selvitä voiko mobiililaitteesi tarvittaessa etätyhjentää ja kuinka se tapahtuu.

Osio 7. Tietoturvapoikkeamat ja tietoturvatapahtumat

18. Vastaa seuraaviin tietoturvapoikkeamia ja tietoturvatapahtumia koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta.

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-**On tärkeää** ilmoittaa tietoturvapoikkeamasta tai haitallisesta viestistä tietoturvavastaaville.
1 | 2 | 3 | 4 | 5 | 6
-**Ilmoitan** tietoturvapoikkeamista tai haitallisista viesteistä matalalla kynnyksellä tietoturvavastaaville.
1 | 2 | 3 | 4 | 5 | 6
-Minulla on **ilmoitusvelvollisuus** tietoturvarikkomuksista ja epäilyksistä tietoturvavastaavalle.
1 | 2 | 3 | 4 | 5 | 6

19. Miten tulee toimia Lapin yliopiston ohjeiden mukaan, jos epäilet haittaohjelmatartuntaa ***omistamallasi*** tietokoneella?

valitse vähintään yksi vaihtoehto

Epäilys ei ole vielä riittävä syy erityistoimiin.

Lopetan tietokoneen käytön välittömästi

Hanki apua ja selvitä miten haittaohjelma poistetaan

20. Mistä voit saada apua haittaohjelman poistamiseksi ***omistamaltasi*** koneelta?

Valitse vähintään yksi vaihtoehto.

Voin saada rajallista apua omalta yliopistolta.
Virustorjuntaohjelman kotisivuilta.
Yliopisto poistaa haittaohjelman ja varmistaa saastuneen tietokoneen turvallisuuden.

Osio 8. Tiedonkäsittely

Tiedonkäsittely = esim. tiedon avaaminen, lukeminen, muokkaaminen, tallentaminen, kopiointi, lähettäminen ja hallinnointi.
Julkinen tietokone = Yleisessä käytössä oleva tietokone (esim. kahvila, kirjasto ym.)

21. Vastaa seuraaviin tiedonkäsittelyä koskeviin väittämiin oman tietosi tai näkemyksesi pohjalta.

(1. Täysin erimieltä–5. Täysin samaa mieltä, 6 EOS)

-Toisen henkilötietoja sisältävän tiedoston avaaminen julkisella tietokoneella on sallittua.
1 | 2 | 3 | 4 | 5 | 6
-Varmuuskopioin laitteeni tai tiedostoni säännöllisesti.
1 | 2 | 3 | 4 | 5 | 6
-Minulle on tärkeää käsitellä henkilötietoja turvallisesti ja asianmukaisesti.
1 | 2 | 3 | 4 | 5 | 6

22. Mitä käytöstä poistettavan tietokoneen, älypuhelimen tai muistitikun muistille tulee tehdä?

Valitse alta yksi vaihtoehto

Tuhota digitaalisesti päällekirjoittamalla tai fyysisesti murskaamalla.
Pyyhkimällä muisti palauttamalla laitteen tehdasasetukset.
Pyyhkimällä tiedostot ja ohjelmat siirtämällä ne roskakoriin ja tyhjentämällä roskakori.
Tuhota formatoimalla tai alustamalla muisti uudelleen.
Ei toimenpiteitä. Laitteen muistia ei voi avata ilman käyttöoikeuksia tai salasanaa.
Kierrättää laite elektroniikkaromuna.
En tiedä.

23. Mihin suojausluokkiin mainitut asiat sisältyvät käsityksesi mukaan?

-Yliopiston turvaohjeet
Julkinen tieto | perussuojaustaso | korkea suojaustaso
-Puhelinnumero
Julkinen tieto | perussuojaustaso | korkea suojaustaso
-Henkilötunnus
Julkinen tieto | perussuojaustaso | korkea suojaustaso
-Henkilökohtainen muistiinpano
Julkinen tieto | perussuojaustaso | korkea suojaustaso
-opinnäytetyön ja tieteellisen tutkimuksen suunnitelma
Julkinen tieto | perussuojaustaso | korkea suojaustaso
-Tiedot henkilön terveydentilasta
Julkinen tieto | perussuojaustaso | korkea suojaustaso
-Opintosuoritusote
Julkinen tieto | perussuojaustaso | korkea suojaustaso