Ammatillisen oppilaitoksen henkilöstön kyber-turvallisuustietoisuus oppilaitoksen arjessa

Sami Kiiskinen

2023 Laurea

Laurea-ammattikorkeakoulu

Ammatillisen oppilaitoksen henkilöstön kyberturvallisuustietoisuus oppilaitoksen arjessa

Sami Kiiskinen
Turvallisuusjohtamisen ylempi amk
Opinnäytetyö
Toukokuu 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtamisen koulutusohjelma

Tradenomi (Ylempi AMK)

Sami Kiiskinen

Ammatillisen oppilaitoksen henkilöstön kyberturvallisuustietoisuus oppilaitoksen arjessa

Vuosi 2023 Sivumäärä 107

Tämä opinnäytetyö on tehty osana Laurea ammattikorkeakoulun turvallisuusjohtamisen opintoja. Työn tavoitteena on kehittää Hyria konsortion kyberturvallisuutta henkilöstön toimintaan liittyen. Ammatillisella oppilaitoksella on useita lakisääteisiä velvoitteita kerätä ja tallentaa tietoa. Kerättyyn tietoon liittyen organisaatiolla on lakisääteisiä tietosuojavelvoitteita. Tämän lisäksi ammatillisella oppilaitoksella on useita muita syitä suojata tietojärjestelmiään, sillä suuri osa toiminnasta ja osa opetuksesta tapahtuu tietoverkkojen ja -järjestelmien välityksellä ja niitä hyödyntäen. Näiden järjestelmien toimintakatkokset voivat haitata merkittävästi oppilaitoksen ydintoimintaa.

Tämä kehittämistehtävä toteutettiin nojautuen aikaisempaan tutkimukseen organisaatioiden henkilöstön kyberturvallisuustietoisuudesta. Osana kehittämistehtävää tehty tapaustutkimus toteutettiin hyödyntäen laadullisia tutkimusmenetelmiä. Aineisto kerättiin kyselylomakkeen ja teemahaastatteluiden avulla. Aineisto analysointiin fenomenologisen tutkimusstrategian periaatteiden mukaisesti sekä kyselyn osalta lisäksi tilastollisia menetelmiä hyödyntäen. Työn tuloksena muodostui käsitys henkilöstön kyberturvallisuustietoisuudesta, sen ilmenemisestä oppilaitoksen arjessa sekä ehdotus toiminnan kehittämiseksi.

Toimeksiantajan henkilöstön kyberturvallisuustietoisuus on yleisesti hyvällä tasolla. Henkilöstö koki kyberturvallisuuden ja tietoturvallisuuden tärkeänä oppilaitosympäristössä, omassa arjessaan sekä yhteiskunnassa yleisesti. Oppilaitoksen arjessa tämä näkyi hieman vaihtelevasti. Henkilöstö on valpas ja pyrkii havaitsemaan mahdollisia haitallisia pyrkimyksiä. Kuitenkaan heidän osaamisensa ei täysin tue tätä pyrkimystä. Lukuisten eri järjestelmien ja ohjelmistojen keskellä valppaus ja huolellisuus saattaa arjen kiireissä joskus herpaantua. Keskeinen epävarmuutta herättävä tekijä on etätyön kyberturvallisuus. Havaintojen perusteella toimeksiantajan henkilöstön kyberturvallisuustietoisuuden kehittämiseksi on ehdotettu aihealueen perehdytyksen tehostamista, kyberturvallisten toimintatapojen implementointia tietojärjestelmiin ja tietoteknisiin laitteistoihin liittyvään perehdytykseen ja laiteluovutuksiin sekä kyberturvallisten toimintatapojen lisäämistä henkilöstön opiskelijoille pitämien orientaatioiden sisältöön.

Asiasanat: kyberturvallisuus, kyberturvallisuustietoisuus, kyberturvallisuusosaaminen, turvallisuuskulttuuri

Laurea University of Applied Sciences **Abstract**

Security Management

Master of Business Administration

Sami Kiiskinen

Cybersecurity Awareness of Vocational Institution Personnel in the Daily Life of the Institution

Year 2023 Pages 107

This thesis conducted as part of the studies in Security Management at Laurea University of Applied Sciences. The objective of this thesis was to enhance the cybersecurity of the client, Hyria Consortium, regarding to the actions of their personnel. A vocational educational institution has several legal obligations to collect and store information. In relation to the collected data, the organization has legal data protection obligations. In addition to this, the oganization has several reasons to protect their information systems, as a significant portion of their operations and some of the teaching activities take place through computer networks and systems. Disruptions in the functioning of these systems can significantly hinder the core activities of the educational institution.

This development task was based on previous research on the cybersecurity awareness of educational institution personnel. As part of the development task, a case study was conducted using qualitative research methods. Data were collected through a questionnaire and thematic interviews. The data were analyzed following the principles of phenomenological research strategy, supplemented with statistical methods for the survey data. The outcome of the work was an understanding of personnel's cyber security awareness, its manifestation in the daily life of, and a proposal to improve it.

The cybersecurity awareness of the Hyria personnel is generally at a good level. The personnel see cybersecurity and information security important in their work environment, everyday lives, and in society in general. However, this awareness is reflected somewhat variably in the daily operations of the institution. The personnel are vigilant and strive to detect possible malicious activities. However, their knowledge and skills do not fully support this effort. Amidst numerous different systems and software, vigilance and diligence may sometimes wane due to the pressures of everyday tasks. The cybersecurity is causing uncertainty in remote work environment. Based on the results, it has been suggested to enhance the familiarizations to improve the cybersecurity awareness of the client’s personnel. This includes implementing cyber secure practices in all orientations related to information systems and IT hardware, as well as incorporating cyber secure practices into the content of orientations conducted for both staff and students.

Keywords: cybersecurity, cybersecurity awareness, cybersecurity knowledge, security culture

Sisällys

1 Johdanto

Tietojärjestelmiin ja -verkkoihin liittyvässä toimintaympäristössämme on useita uhkakuvia, jotka kohdistuvat organisaatioiden keskeisiin toimintoihin sekä suojattaviin arvoihin. Nykyään lähes kaikki tieto on tallennettuna digitaalisesti ja saatavilla etänä tietoverkkojen kautta. Ammatillinen oppilaitos joutuu käsittelemään ja tallentamaan lakisääteisistä (Laki ammatillisesta koulutuksesta 2017/531) velvoitteistaan johtuen opiskelijoiden tietoja, myös EU:n tietosuoja-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) tarkoittamia arkaluonteisia henkilötietoja. Henkilö- ja yhteystietojen lisäksi opiskelijoista tallennetaan terveystietoja liittyen esimerkiksi tuen ja ohjauksen tarpeeseen. Tietoverkkojen ja -järjestelmien luotettava toiminta on keskeistä opetuksessa sillä suurin osa tiedosta, opetuksesta ja materiaaleista sijaitsee verkkolevyasemilla, sähköisissä oppimisympäristöissä ja pilvipalveluiden, kuten Microsoft Office365 palvelussa. Toimivat verkot, pilvipalvelut ja työasemat ovat siis ehdoton edellytys oppilaitoksen ydintoiminnalle, opetukselle. Ammatillisen oppilaitoksen Keudan järjestelmiin kohdistui 28.11.2022 epäilyttävää verkkoliikennettä, ja he joutuivat estämään pääsyn järjestelmiinsä. Tämän johdosta järjestelmät olivat pois käytöstä 9 päivää ja vielä pitkään senkin jälkeen toiminnassa oli katkoksia järjestelmän palauttamiseen liittyvistä toimenpiteistä johtuen. Tapahtumien aikaisten tietojen mukaan opiskelijoiden ja työntekijöiden tietoja ei kuitenkaan olisi päätynyt ulkopuolisten haltuun. (Keuda 2022.) Maaliskuussa 2023 Keuda julkaisi raportin tapahtumasta. Tuolloin selvisi, että järjestelmiin oli tunkeuduttu Bitlock ohjelmistoa käyttäen. Ohjelmisto oli saastuttanut noin 60 % oppilaitoksen verkossa olevista työasemista. Raportin mukaan oppilaitoksella on edelleen palautumisen toiminnot kesken ja joitakin haittoja toiminnalle on odotettavissa ainakin kesään 2023 asti. Suorat kustannukset ovat olleet yli 100 000 euroa ja epäsuoria kustannuksia on odotettavissa merkittävästi. (Keuda 2023.) Helmikuussa 2023 uutisoitiin Vaasassa tapahtuneesta tietomurrosta jossa 50 oppilaan tiedot Wilmassa olivat päätyneet ulkopuolisten käsiin. Joulukuussa 2022 tapahtuneen tietomurron syyksi paljastui palvelua tuottavan Visma Enterprise Oy:n selvityksen mukaan opetushenkilöstöön kuuluvan henkilön käyttäjätunnusten joutuminen vääriin käsiin. Tämän mahdollisti opetushenkilöstöllä yleisesti käytössä ollut kolmannen osapuolen tuottama epävirallinen sovellus. Sovelluksen mahdollistamana kirjautuminen järjestelmään oli jäänyt aktiiviseksi antaen tunkeutujalle pääsyn Wilmaan tallennettuihin opiskelijoiden tietoihin. (YLE 2023.)

Oppilaitoksen tietoturvavelvoitteiden kannalta keskeinen ja realistinen uhka on, että joku pääsee tunkeutumaan oppilaitoksen hallinnoimiin järjestelmiin varastaen ja/tai estäen pääsyn tietoihin. Tietojen tuhoutuminen, vääristyminen tai arkaluonteisten henkilötietojen päätyminen kiristäjien käsiin ja keskustelupalstoille olisi toiminnan kannalta monin tavoin haitallista. Vuoden 2022 helmikuussa julkisuuteen tuli tieto Savonia ammattikorkeakoulun kohdistuneesta tietomurrosta. Poliisin julkaisemien tietojen mukaan tietomurto oli kohdistunut Savonia ammattikorkeakoulun serverille. Tietomurrossa on Poliisin tietojen mukaan käytetty

LockBit 2.0 nimistä kiristyshaittaohjelmaa. (Poliisi 2022.) Tapauksen alkuvaiheessa Savonia ammattikorkeakoulun rehtori ehti jo tiedottaa, ettei henkilötietoja vuotanut lainkaan vaan hyökkääjä olisi ainoastaan lukinnut joitakin tiedostokansioita, jotka sijaitsivat henkilökunnan omassa käytössä olevilla verkkolevyasemilla. Lukitsemisen avaamisen vastineeksi hyökkääjä oli vaatinut lunnaita. Myöhemmin Savonia ammattikorkeakoulussa havaittiin lukittujen ja vuotaneiden tietojen joukossa opiskelijoiden tietoja. (Rytkönen 2022.) Poliisin tiedottaessa esitutkinnan lopettamisesta kerrottiin tietomurrossa vuotaneen 700 entisen ja nykyisen opiskelijan nimiä ja henkilötunnuksia (Remes 2022).

Tämän opinnäytetyön tekijä oli itse edellisessä kappaleessa kuvatun tapahtuman aikaan opiskelemassa Savonian avoimen ammattikorkeakoulun kurssilla ja joutui yhdessä muiden noin 7000 opiskelijan kanssa päivittämään salasanansa ja pohtimaan olisivatko henkilökohtaiset tiedot vuotaneet ja jopa julkaistu jossain anonyymin Tor-verkon keskustelupalstalla. Tästä ja yleisesti aihetta kohtaan koetusta mielenkiinnosta johtuen on opinnäytetyön aiheeksi valikoitunut kyberturvallisuus ja erityisesti henkilöstön osaaminen päivittäiseen tietojärjestelmien käyttämiseen liittyen. Aiheen alustavia keskusteluja käytiin kehittämistyön toimeksiantajan, Hyria koulutuksen turvallisuusasioiden johtajan Matti Kymäläisen, kanssa. Näiden keskustelujen ja aiempien kyberturvallisuuden johtamiseen liittyvien opintojen sekä työssä tietoturvallisuuden opetustehtävissä, opinnäytetyön tekijälle on muodostunut käsitys henkilöstön tietoturvaosaamisen merkityksestä kyberturvallisuuden kokonaisuudelle. Limnéll, Majewski & Salminen (2014, 13–15) kuvaavat kirjan Kyberturvallisuus johdannossa kyberturvallisuuden olevan erinomainen esimerkki tilanteesta, jossa kokonaisturvallisuuden ajattelumalli on keskeinen ja olevan virhe ajatella kyberturvallisuuden koskevan vain teknisiä järjestelmiä. Heidän mukaansa kyberturvallisuus ei ole vain pienen asiantuntijajoukon asia, vaan jokainen organisaation jäsen on omalta osaltaan vastuussa sen onnistumisesta.

Kyberturvallisuuden kannalta organisaatioita voi kohdata muutkin kuin mainehaitat. Tämän sai kokea yhdyskuntateknologiaan ja talotekniikkaan erikoistunut Uponor, joka joutui loppuvuodesta 2022 kyberhyökkäyksen kohteeksi. Hyökkäyksestä johtuen Uponor joutui ajamaan koko tuotannon alas noin viikon ajaksi. Tästä johtuen yhtiön liikevaihto loka-joulukuussa jäi toissa vuoden vastaavasta ajasta jopa 53 miljoonaa euroa. (Helsingin Sanomat 2023.) Vaikka organisaatioissa ja yhteiskunnassa on lisääntyvässä määrin ymmärretty kyberturvallisuuden merkitys, on aiheeseen liittyvä perustietous edelleen heikohkolla tasolla. Organisaatioiden henkilöstöllä tulisi tulevaisuudessa olla vähintään kyberturvallisuuden perustaidot hallinnassa. Euroopan kyberturvallisuuskeskusten ECHO (European network of cybersecurity and competence hub for innovation and operations) yhteishankkeen tarkoituksena on ollut kehittää Euroopan Unionin kyberpuolustuskykyä mittavan neljävuotisen hankkeen avulla. Hankkeessa on koottu yhteen monipuolinen asiantuntijaverkosto, joka on tuottanut erilaisia työkaluja kyberturvallisuuden kehittämiseen. (Laurea 2019.) Ling, L., Hea, Xua, Asha, Anwarb & Yuanb (2019, 8) mukaan organisaation kyberturvallisuuden onnistumisessa on tärkeää johdon

sitoutuminen, hyvät toimintamallit ja henkilöstön osaamisen ja taitojen kehittäminen. Ensimmäinen askel perustaitojen kehittämisessä on kartoittaa ja selvittää nykyisen osaamisen taso. Tähän tämän opinnäytetyönä tehtävän tutkimuksellisen kehittämistyön on tarkoitus tuoda vastaus soveltamalla jo olemassa olevia työkaluja, tutkimusta ja tutkimuksellisia menetelmiä ammatillisen oppilaitoksen kyberturvallisuuden kehittämisen tarpeisiin.

1.1 Työn toimeksiantaja

Tämän opinnäytetyön toimeksiantaja on Kanta- ja Päijät-Hämeen sekä Uudenmaan alueella toimiva Hyria konsortio, joka koostuu kahdesta konsernista: Hyria Koulutus Oy konsernista ja Hyria Säätiö konsernista. Hyvinkään ja Riihimäen kaupunkien, Lopen ja Hausjärven kuntien sekä Hyria säätiö omistama Hyria Koulutus tarjoaa koulutus- ja valmennuspalveluita, konserni – ja liiketoimintapalveluita sekä johdon palveluita. Hyria Business Institute tarjoa erilaisia kasvu- ja koulutuspalveluita, jotka on kohdistettu työelämän ja aikuisen työväestön tarpeisiin. Hyria säätiö konserni toimii Kanta-Hämeen ja Keski-Uudenmaan alueilla palvellen vuosittain jopa 2000 asiakasta. Hyria Säätiön tarjoamat palvelut pitävät sisällään erilaisia työllistymisen ja muun tukemisen palveluita kuten etsivä nuorisotyö, työhönvalmennus, työpajatoiminta sekä tarjoaa erilaisia valmennusympäristöjä kuten kierrätyskeskus-, kahvila-ravintola- ja kuljetustoimintaa. Hyria Säätiön on ovat perustaneet Hyria koulutuksen omistajat: Hausjärven ja Lopen kunnat sekä Riihimäen ja Hyvinkään kaupungit. Hyria Konsortiossa on henkilöstöä noin 520 josta opettavaa henkilöstöä hieman alle 400. Vuosittain Hyriassa opiskelee lähes 10 000 tutkinto- ja osatutkinto-opiskelijaa sekä 1500 valmentautujaa. Hyrian valtionosuusrahoitus oli 36,2 miljoonaa euroa vuonna 2021. (Hyria 2022.)

Tämä opinnäytetyö tehtiin Hyrian turvallisuusasioiden johtajan Matti Kymäläisen sekä Hyrian ICT-palveluiden päällikön Janne Lehtisen toimeksiannosta ja ohjauksessa Matti Kymäläisen toimiessa yhteyshenkilönä opinnäytetyöprosessiin liittyen. Kyselytutkimusta varten haettiin tutkimuslupaa organisaation toimitusjohtajalta. Hakemus hyväksyttiin ja tutkimuslupa (VaiPek / A 4 / 2023) opinnäytetyön osana tehtävälle tutkimukselle annettiin 22.1.2023 (Liite 1).

1.2 Toimeksiantajan lakisääteiset tietosuojavelvoitteet

Laki ammatillisesta koulutuksesta (2017/531) mukaisen ammatillisen oppilaitoksen osalta Oppilas- ja opiskelijahuoltolaki (1287/2013) pykälä 21 velvoittaa oppilaitosta ylläpitämään yksilökohtaista rekisteriä, johon on kirjattu pykälän 20 mukaiset asiat kuten opiskelijan:

- nimi, henkilötunnus ja kotikunta sekä alaikäisen tai muutoin vajaavaltaisen opiskelijan huoltajan tai muun laillisen edustajan nimi ja yhteystiedot;
- asian aihe, tausta ja vireille panija;
- tiedot asian käsittelystä monialaisen asiantuntijaryhmän kokouksessa, kokoukseen osallistuvat henkilöt ja heidän asemansa;

- suunnitelma toimenpiteistä opiskelijan yksilökohtaisen opiskeluhuollon järjestämiseksi ja niiden toteuttamisesta ja seurannasta vastaavat tahot;
- opiskelijaa koskeva välttämätön tieto liittyen opiskeluhuollossa toteutettuihin ja toteutettaviin toimenpiteisiin;
- kirjauksen päivämäärä sekä kirjauksen tekijä ja hänen ammattinsa tai virka-asemansa. (Oppilas- ja opiskelijahuoltolaki 1287/2013, §20)

Oppilas- ja opiskelijahuoltolaki (1287/2013) §22 mukaan oppilaitoksella on velvoite pitää salassa aiemmin mainitut lakisääteisesti tallennettavat ja kirjattavat tiedot. Tästä salassapidosta on oikeus poiketa vain opiskelijan opiskelijahuollon järjestämiseen liittyvistä syistä tai opiskelijan vaihtaessa oppilaitosta hänen tai hänen huoltajansa luvalla. Lisäksi tietoja voidaan ilmoittaa poliisille vakavaan henkeen ja terveyteen kohdistuvan rikoksen ennaltaehkäisemiseksi. Laki ammatillisesta koulutuksesta (2017/531) luku 11 määrittelee samankaltaiset salassapitovelvollisuudet opiskelijan terveystiedoille sekä henkilökohtaisen osaamisen kehittämissuunnitelmille. Kyseiset lait määrittelevät tarkasti tilanteet ja henkilöt, joille opiskelijan tietoja voidaan luovuttaa.

Euroopan parlamentin ja neuvoston asetus (EU) (2016/679) (niin sanottu tietosuoja-asetus) ja sitä täydentävä kotimainen tietosuojalaki (2018/1050) määrittelevät yleisellä tasolla kaikkia toimijoita koskevat ehdot tietojen käsittelylle ja niiden salassapidolle. Näiden lakien mukaisesti ammatillinen oppilaitos voi lakisääteisistä velvoitteistaan johtuen kerätä ja tallentaa tietoa opiskelijoistaan. Tietosuoja-asetuksessa määritellään tietojen käsittelyssä ja suojauksessa epäonnistuneelle organisaatiolle mahdollisesti hyvinkin tuntuva rangaistus. Rikoslaki 1889/39 (luku 38 §9) määrittelee tietosuojarikoksen kohdalla tietosuojalain tai muiden henkilötietojen käsittelystä määräävien lakien mukaisten toimenpiteiden laiminlyönnin yhtenä täyttyneen rikoksen tunnusmerkkinä.

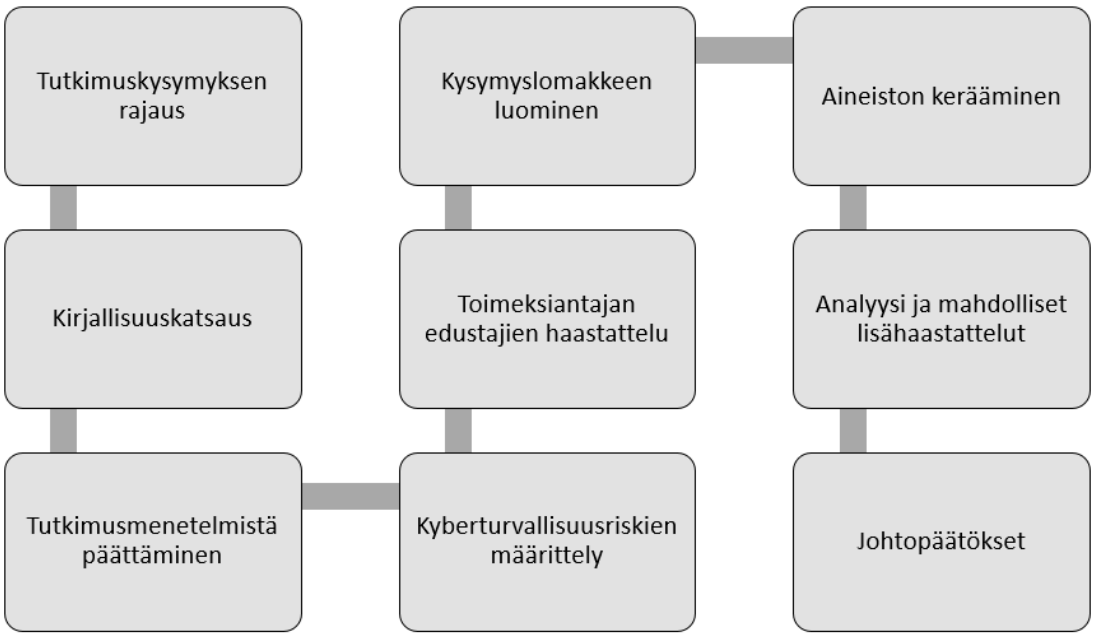
Laki yksityisyyden suojasta työelämässä (2004/759) määrittelee tietoja, joita työnantaja saa käsitellä, ketkä työnantajan organisaatiossa saavat käsitellä ja mistä rekrytointiin liittyvät tiedot tulee hankkia. Tämän lain mukaan työntekijän tietoja saa käsitellä vain työsuhteen tai muiden etujen kannalta oleellisten päätösten tekijä ja valmistelija.

1.3 Työn tavoitteet

Tämän opinnäytetyönä tehtävän kehittämistyön tavoitteena on selvittää Hyria Konsortion henkilöstön kyberturvallisuuteen liittyvää tietoisuutta ja osaamista sekä kyberturvallisuuskoulutuksen tarvetta tulevaisuudessa. Tähän tarkoitukseen luotiin ammatillisen oppilaitoksen ympäristöön soveltuva kysely, jonka avulla on mahdollista kartoittaa henkilöstön subjektiivinen kyberturvallisuuteen liittyvä tietoisuuden, osaamisen ja perehdyttämisen riittävyyden kokemus. Joidenkin aihealueiden kohdalla kyselyyn on sisällytetty osaamisen tasoa mittaavia kysymyksiä keskeisten kyberturvallisuusriskien osalta. Kyselyn avulla henkilöstön on mahdollista

saada hieman käsitystä tavoista, joilla heidän oma toimintansa voisi vaarantaa organisaation kyberturvallisuutta. Usein intuitiivisesti ihmiset saattavat ajatella ymmärtävänsä kokonaisuuksia paremmin kuin todellisuudessa ymmärtävätkään. Intuition on todettu toimivan paremmin tilanteissa, joissa olosuhteet ovat kohtalaisen samankaltaiset ja palaute omista päätöksistä on saatu suhteellisen nopeasti. Tilanteissa, joissa päätöksen teon ympäristö on monimutkaisempi, tähtää pidemmälle tulevaisuuteen tai palaute omista päätöksistä saadaan pidemmällä viiveellä, tai ei lainkaan, on intuition todettu toimivan huonommin. Esimerkiksi lääkäri, joka ei diagnoosin jälkeen useinkaan tapaa potilastaan, todetakseen diagnoosin ja hoidon onnistumisen, ei tilastollisesti onnistu diagnoosissaan erityisen hyvin. Edellinen esimerkki kuvaa hyvin palautteen merkitystä intuition luotettavuudelle. (Kahneman, 2011. 236–244.) Intuitio toimii lähes yhtä hyvin kuin strukturoidut ja tarkkaan pohditut analyysimenetelmät mikäli intuitiolla on käytössään vastaukset oikeisiin kysymyksiin. Puhtaasti intuitiolla tehty arvio ilman oikeita kysymyksiä ja vastauksia ei useinkaan ole kovin tarkka. Tilastollisesti jokin arvioista kuitenkin aina osuu oikeaan. (Kahneman, 2011. 229–232.)

Opinnäytetyön suunnitelman mukaisesti opinnäytetyöprosessi (Kuvio 1) jakautui yhdeksään vaiheeseen: tutkimuskysymyksen rajaus, kirjallisuuskatsaus, tutkimusmenetelmistä päättäminen, kyberturvallisuusriskien määrittäminen, toimeksiantajan edustajien haastattelut, kysymyslomakkeen luominen, aineiston kerääminen, aineiston analyysi ja lisähaastattelut ja johtopäätökset.

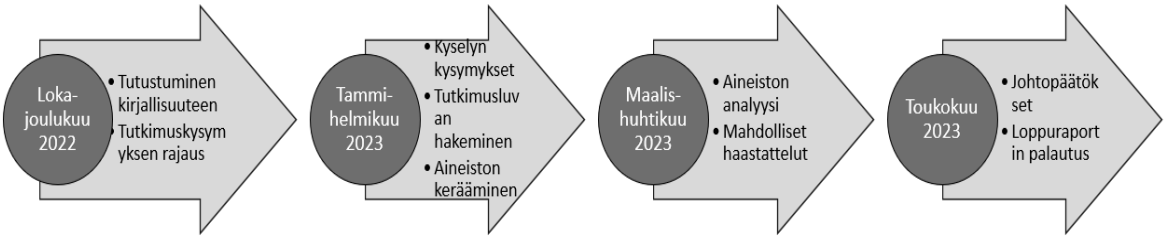


Kuvio 1 Opinnäytetyöprosessin suunnitelma

Tutkimuskysymykset:

1. Millainen on henkilöstön kyberturvallisuustietoisuus?
2. Miten kyberturvallisuustietoisuus näkyy arjessa?
3. Miten henkilöstön tietoisuutta voidaan kehittää?

Toteutussuunnitelman aikataulun (Kuvio 2) mukaisesti loka- joulukuun 2022 aikana toteutettiin kirjallisuuteen tutustuminen, tutkimuskysymyksen ja apukysymysten rajaus sekä tutkimussuunnitelma, tutkimusluvan hakeminen tammikuussa 2023. Asiantuntijahaastattelut sekä kyselyn kysymyspatteriston valmistelut toteutettiin helmikuussa 2023. Aineisto kerättiin maaliskuun 2023 alkupuoliskolla, aineiston analyysi ja tarvittavat haastattelut toteutettiin maalis-huhtikuussa sekä johtopäätökset ja lopullinen raportti valmistui toukokuussa 2023. Opinnäytetyö esiteltiin opinnäytetyöseminaarissa toukokuussa 2023.



Kuvio 2 Opinnäytetyöprosessin suunniteltu aikataulu

2 Tutkimusmenetelmät ja toteutus

Tämän opinnäytetyönä tehtävän kehittämistyön toteuttaminen tapahtui laadullisten tutkimusmenetelmien mukaisesti niiden periaatteita noudattaen. Puusa & Juuti (2020, luku 6) mukaan laadullisessa tutkimuksessa on kyse lähestymistavasta, jolla tutkimusongelmaa on tarkoitus pyrkiä ratkaisemaan. Tutkija voi pyrkiä haastamaan tutkittavien todellisuutta, jolloin tämä tulee huomioida tutkimusmenetelmien valinnassa. Tällöin menetelmät ovat erilaiset kuin tutkittaessa ilmiötä, jossa tutkittavien maailmankuvassa ei ole merkittävää ristiriitaa odotettavissa. Vilkka (2021, luku 5) mukaan laadullisten tutkimusmenetelmien avulla tarkastellaan ihmisten sosiaalista maailmaa merkityksien ja merkityskokonaisuuksien kautta. Merkitykset ilmenevät erilaisina käsityksinä, toimintana, ajatuksina tai päämäärinä. Tutkittavan

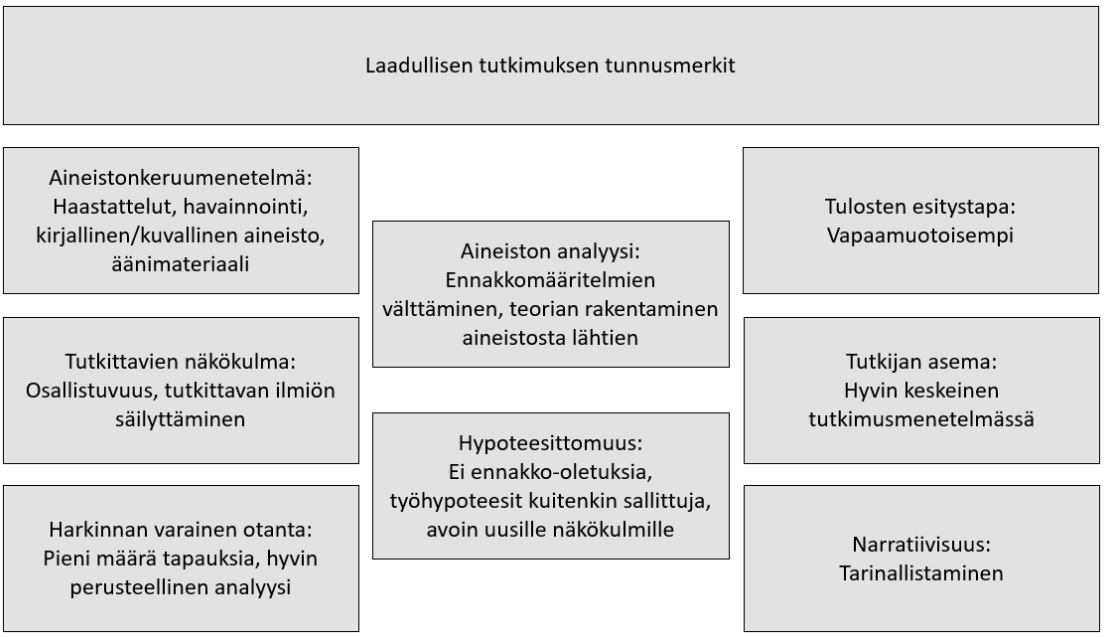
kokemukset ovat aina omakohtaisia, ja siten henkilökohtaisia, kun taas käsitykset ovat jonkin yhteisön tai organisaation ihmisille yhteisiä tapoja ajatella asioista.

Laadullisessa tutkimuksessa tutkimusasetelma on joustava ja tutkimusprosessi etenee tutkijan esiymmärryksen kautta kirjallisuuskatsauksella aikaisempaan teoriaan, jonka jälkeen hänen on mahdollista arvioida uudelleen aikaisempaa käsitystään. Aineistonkeruuvaiheessa voi tutkija törmätä tilanteeseen, jossa tutkimuksen tavoitetta tai rajausta on tarkennettava. (Puusa ym. 2020, luku 4.) Laadullisen tutkimuksen tavoitteena on tutkimuksen aikana löytää ja havaita ilmiöitä, jotka ovat eivät ole toiminnasta heti havaittavissa. Tavoitteena on kerätyn aineiston avulla löytää ilmiön syvällisempi merkitys. Tästä johtuen tutkijan tulisi pyrkiä toimimaan vapaana omista ennakkokäsityksistään. (Vilkka 2021, luku 5.)

Eskola & Suoranta (1998, luku 1) esittävät, että tutkimusta tehdessä tulisi valita tutkittavaan ongelmaan sopiva tutkimusmenetelmä menetelmäkeskeisyyden sijaan. Kallinen & Kinnunen (2021) mukaan laadullista tutkimusta tehdessä tulee suhtautua tutkimukseen sekä sen kohteeseen ennakkoluulottomasti ja avoimin mielin oma arkitieto unohtaen, vaikka ilmiö itsessään olisikin tutkijalle tuttu. Tutkimusta tehdessä tapahtumia tulisi havainnoida ikään kuin näkisi ne ensimmäistä kertaa. Tällöin on mahdollista havaita ilmiöitä, jotka eivät tulisi muutoin havaituksi. Laadullisessa tutkimuksessa tarkoituksena on kerätä ja käyttää empiirisiä aineistoja kuten haastatteluita, havaintoja, kuvia ja tekstejä. Kerättyjä aineistoja ei analysointivaiheessa muuteta numeeriseen muotoon. Laadullisessa tutkimuksessa tutkittavien subjektiivisuuden hyväksyminen on tärkeää ja heitä tuleekin kohdella sen edellyttämällä tavalla. Tällöin ihmisten kokemukset pääsevät esille. Tutkija muodostaa uusia näkökulmia tulkitessaan aineistoa ja yrittäessään kuvata tutkittavaa ilmiötä tutkittavien näkökulmasta käsin. Puusa ym. (2020, johdanto) mukaan laadullisessa tutkimuksessa tutkittavaa ilmiötä tyypillisesti lähestytään tutkittavien näkökulmasta heidän kokemuksiansa, ajatuksiansa ja tunteitaan tarkkaillen ja tutkittavien näille asioille antamia merkityksiä selvittäen. Laadullisia ja määrällisiä tutkimusmenetelmiä voidaan hyödyntää samassa tutkimuksessa (Alasuutari 2011, luku 2).

Laadullisessa tutkimuksessa ihmisten näkemykset ja kokemukset eivät välttämättä mahdollista suorien syy-seuraus-suhteiden tunnistamista. Tällöin tutkimuksen tuloksena ei välttämättä synny pelkistettyjä johtopäätöksiä. Vaikka laadullinen tutkimus usein mielletään aineistovetoiseksi, on tässä opinnäytetyössä teoriavetoisuus siten läsnä, että kyberturvallisuus- ja henkilöstön osaamisen teoria on se, josta tässä tutkimuksessa lähdetään liikkeelle ja empiirinen aineisto analysoidaan aikaisempaan teoriaan verraten. (Kallinen ym. 2021.) Eskola ym. (1998, luku 1) esittävät laadullisen tutkimuksen tunnusmerkistöksi (Kuvio 3) seuraavia kokonaisuuksia: aineistonkeruumenetelmä, tutkittavien näkökulma, otanta, aineiston analyysi, hypoteesittomuus, tutkimustyyli, tulosten esitystapa, tutkijan asema sekä narratiivisuus. Aineistonkeruumenetelmillä kerätään erilaista aineistoa esimerkiksi haastatteluilla, havainnoimalla tai hyödyntämällä muuhun tarkoitukseen tehtyä kirjallista-, kuva- tai äänimateriaalia.

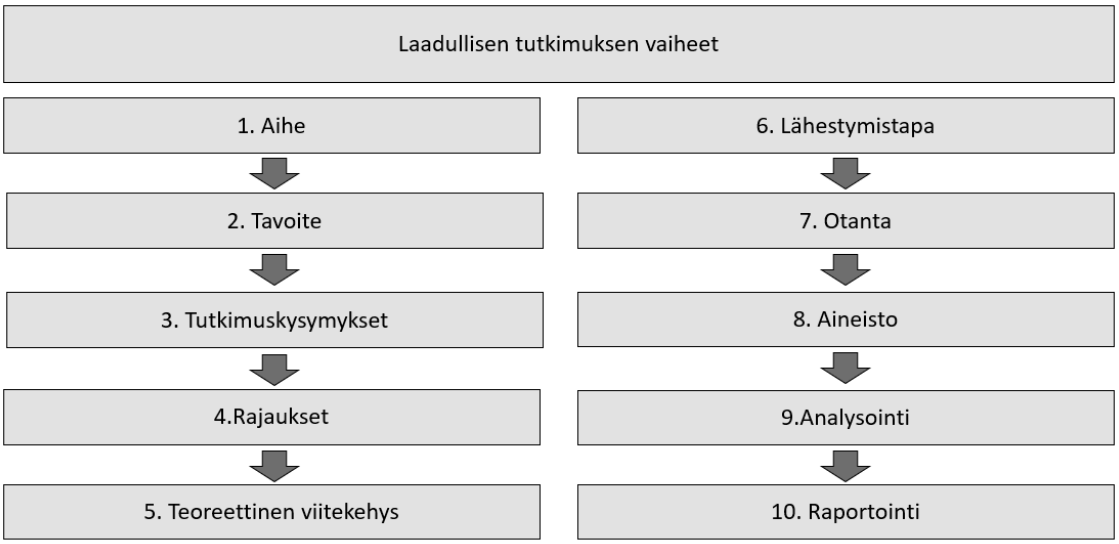
Tutkittavan näkökulman selvittämisessä laadulliseen tutkimukseen kuuluu yleensä tutkittavien osallistuminen. Kenttätyön avulla tutkija pyrkii pääsemään mahdollisimman lähelle tutkittavaa kohdetta sekä tutkittavaa ilmiötä, jotta tutkittavasta ilmiöstä muodostuisi mahdollisimman autenttinen kuva. Laadullisessa tutkimuksessa keskitytään yleensä pienempään harkinnanvaraiseen otantaan. Tähän suppeampaan tapausmäärään pyritään keskittymään hyvin perusteellisesti. Tällöin teoria rakennetaan empiirisestä aineistosta lähtien. Aineiston, eli korpuksen, rajaus vaikuttaa merkittävästi analyysiin laatuun. Vaikka laadullisessa tutkimuksessa tutkijan asema on tärkeä ja hyvin keskeinen, tulisi tutkijan silti pyrkiä välttämään hypoteesien tekemistä tutkimustuloksen vääristymisen välttämiseksi.



Kuvio 3 Eskola ym. (1998, luku 1) mukaillen laadullisen tutkimuksen tunnusmerkit.

Puusa ym. (2020, johdanto) mukaan laadulliseen tutkimukseen kuuluu useita vaiheita (Kuvio 4). Tutkimusprosessi alkaa aiheesta, jonka tutkija kokee vaativan tutkimista. Perustelu aiheelle voi löytyä tutkijan omista havainnoista tai esimerkiksi kirjallisuudesta esiin nousseesta ilmiöstä, jonka jotain näkökulmaa ei ole vielä tutkittu. Tällainen tutkimaton näkökulma on nimeltään tutkimusaukko. Aiheen valinnan jälkeen tutkijan tulee määrittää tutkimukselle tavoite, joka on riittävän selkeä, jotta voidaan määritellä tutkimuskysymykset, joilla lähdetään aihetta selvittämään. Kun tutkimuskysymykset on rajattu hyvin, jää jäljelle yleensä kaksi tai kolme keskeisintä kysymystä. Tutkimuksen onnistumisen kannalta on tässä vaiheessa tärkeää muistaa, että tutkimusmenetelmän ei tule mennä tutkimuskysymysten edelle. Optimitilanteessa tutkimuskysymykset ovat tiedossa jo ennen tutkimusmenetelmän ja aineiston keruun suunnittelua. Tutkimusprosessin tässä vaiheessa tutustutaan aihetta käsittelevään kirjallisuuteen ja pyritään löytämään tutkittavalle aiheelle teoreettinen viitekehys. Tämä on aikaa vievä vaihe, jonka edetessä saattaa tutkimuskysymyksetkin vielä tarkentua tai jopa muuttua.

Tutkimuskysymykset tulisi kuitenkin olla lopullisesti päätetty ennen aineiston keruuta, jotta kerätty aineisto olisi soveltuvaa tutkimuksen onnistumisen kannalta. Lähestymistavan valintaan vaikuttaa se, onko tarkoitus kuvata jotain tiettyä tapahtumaa vai ymmärtää tarkemmin kyseisestä tapahtumaa tai ilmiötä.



Kuvio 4 Puusa ym. (2020, johdanto) mukaillen laadullisen tutkimuksen vaiheet

Harrison, Birks, Franklin, & Mills (2017, 1) mukaan tapaustutkimuksen menetelmät ovat kehittyneet erittäin paljon viimeisen 40 vuoden aikana. Tämän johdosta tapaustutkimusta pidetään tehokkaana menetelmänä pyrittäessä tutkimaan ja ymmärtämään todellisen maailman monimutkaisia asioita. Tapaustutkimuksen menetelmiä käytetäänkin nykypäivänä laajasti eri tieteenaloilla, erityisesti sosiaalitieteissä, koulutuksessa, talous-, oikeus- ja terveystieteissä. Usein tapaustutkimuksesta puhuttaessa mielletään sen koskevan yksittäisen ihmisen käyttäytymisen ja kokemisen tutkimusta. Tämä juontaa juurensa tutkimusmenetelmän historiasta sosiologian tutkimuksessa. Tapaustutkimus voi olla määrällinen tai laadullinen. Yksittäisen organisaation, yrityksen tai valtion tarkastelu yksittäisenä tutkimuskohteena ei välttämättä kuitenkaan tarkoita, että kyseessä olisi tapaustutkimus. Toisaalta ei myöskään voida todeta, että yksittäisen organisaation toimintaa tutkittaessa tutkimuksen laatu ja onnistuminen kaatuisi yleistettävyyden puutteeseen otannan pienuuden johdosta. Tähän vaikuttaa enemmän tuloksien tarkastelussa ja raportoinnissa valittu näkökulma. Käsitelläänkö organisaatiota yksilönä vai yhteisönä. (Puusa ym. 2020, luku 6.) Tutkimusta suunnittelevalla on oltava pohdittavana riittävä määrä aineistoa. Kuitenkin laadullisessa tutkimuksessa aineiston määrää tärkeämpää on käytössä olevan aineiston laatu. (Vilkka 2021, luku 5.) Harrison ym. (2017, 12) mukaan käyttämällä useampia tapoja kerätä aineistoa sekä analysoida sitä, voidaan synergiaa hyödyntämällä saada kokonaisvaltaisempi käsitys tutkittavasta aiheesta. Tutkimusmenetelmien käyttötavat voivat vaihdella tutkimuksen luonteesta riippuen. Yleisimmin käytetyt menetelmät

voivat käsittää haastatteluja, kohderyhmien havainnointia tai esineiden ja muiden artefaktien tarkastelua. Muitakin menetelmiä voidaan hyödyntää tapaustutkimuksen osalta.

2.1 Tutkimusaineiston kerääminen

Tutkimusaineiston kerääminen voi laadullisessa tutkimuksessa tapahtua monin erilaisin tavoin. Yleisimpiä aineiston keruumenetelmiä ovat yksilö- ja ryhmähaastattelut, sekä erilaisten dokumentaatioiden tai havaintojen kerääminen. Mikäli tarvetta ilmenee, voidaan tutkimuksen kannalta oleellista aineistoa hankkia lisää vielä analyysivaiheen ollessa käynnissä. Tutkimustuloksien raportoinnissa tulee huomioida riittävän, mutta ei liian, yksityiskohtainen aineiston kuvaus, jotta tutkimuksen johtopäätökset tulevat perusteltua. Puusa ym. (2020, johdanto.) Tutkimushaastattelussa tavoitteena on kerätä tutkittava aineisto puheen muodossa. Puhe voidaan dokumentoida kirjallisesti tai esimerkiksi tallentaen haastattelu video- tai äänimuodossa. Tallenteen puheosuuden purkamista kirjalliseen muotoon kutsutaan litteroinniksi. Haastattelu voidaan tehdä myös lomakehaastatteluna, jolloin haastattelun rakenne on strukturoitu ja se etenee tutkijan ennalta päättämien kysymysten ja niiden muotoilun ehdoilla. Tämän toteutustavan lopputuloksena on tutkijan taustatyön perusteella tehtyihin kysymyksiin saadut vastaukset. Kun lomakehaastattelu toteutetaan paperilla haastateltava voi valita vastausjärjestyksen, sähköisessä lomakkeessa usein edetään tutkijan valitsemassa järjestyksessä. Näin toteutetussa haastattelussa tutkijan perehtyminen aiheen teoriaan sekä oman objektiivisuuden muistaminen ovat hyvin tärkeitä sillä tässä metodissa lopputuloksena syntyy tutkittavan reagointi tutkijan valitsemiin asioihin. Avoimessa henkilöhaastattelussa, tutkijan pyrkiessä välttämään tutkittavan ohjailua, saatetaan todennäköisemmin löytää merkityksiä, joita tutkija ei välttämättä osannut huomioida haastattelukysymyksiä valmistellessaan. Ryhmähaastattelu on laadullinen tutkimusmenetelmä, jolla voidaan tutkia jonkin yhteisön yhteistä käsitystä tutkittavasta asiasta. Tällöin haasteena on haastattelutilanteen säilyttäminen sellaisena, että tutkittavasta asiasta muodostuu oikeanlainen yhteisön yhteinen käsitys, eikä esille tule vain muutaman vahvan yksilön esiin nostamat asiat. Lomakehaastattelua tehdessä tulee huomioida asioita tutkittavan mielenkiinnon säilyttämiseksi. Taustatietojen osalta tutkijan täytyy tarkkaan pohtia mitkä ovat tutkimuksen kannalta oleellisia asioita ja pyrkiä pitämään taustatietojen määrä mahdollisimman pienenä, jotta tutkittavalla riittää vielä motivaatiota vastata tutkimuksen kannalta oleellisempiin kysymyksiin. Tulkinta tulee niillä taustatiedoilla mitä on saatu järkevästi kerättyä. Ylitulkintaa tulee välttää, jotta tutkimustulos ei sen johdosta vääristyisi. (Vilkka 2021, luku 5.)

2.2 Kyselylomake

Kyselylomakkeella tehtävä lomaketutkimus on hyvin yleinen ja pitkään käytössä ollut tapa kerätä tutkimusaineistoa. Aikaisemmin kyselytutkimus toteutettiin paperisella kyselylomakkeella. Nykyään tämän rinnalle on noussut erilaisten ohjelmistojen tai verkkosivujen, kuten

sosiaalisten median palvelujen avulla tehdyt verkkokyselyt. Kyselylomake on 1900-luvun alkupuoliskolta alkaen yleistyneiden tilastollisten tutkimusmenetelmien johdosta suosittu tapa kerätä aineistoa esimerkiksi taloustieteissä. (Alasuutari 2011, luku 2; Valli 2018, osa 1.) Kyselylomakkeiden alkuun yleensä sijoitetaan kysymykset, joiden tarkoituksena on kartoittaa vastaajan taustan kannalta oleellisia asioita, kuten ikä tai koulutus. Nämä kysymykset toimivat eräänlaisena lämmittelynä seuraavassa vaiheessa eteen tuleviin aiheeseen liittyviin helppoihin kysymyksiin. Mikäli kyselyssä on arkoja aiheita käsitteleviä kysymyksiä, olisi ne hyvä sijoittaa helppojen kysymysten jälkeen. Lopuksi voidaan vielä kysyä muutamia jäähdyttelykysymyksiä. Taustakysymykset voidaan sijoittaa loppuun kysymysmäärän ollessa suuri, kun voidaan olettaa vastaajan keskittymiskyvyn jo ehtineen hieman herpaantua. (Valli 2018, osa 1.)

Valli (2018, osa1) mukaan kyselylomake voidaan jakaa kolmeen vaiheeseen. Ensimmäisessä vaiheessa pyrkimyksenä on saada vastaaja vakuutettua aiheen tärkeydestä sekä luoda luottamuksellinen suhde tutkijaan. Seuraavissa vaiheissa tulee huomioida tutkittavan aihepiirin merkitys vastaajille ja sen vaikutus vastausinnokkuuteen ja -motivaatioon. Liian pitkä kysely saattaa jäädä kesken. Aihepiirin tuttuus vaikuttaa kysymysten asetteluun sekä valittuihin käsitteisiin ja kieliasuun. Kysymysten muotoilu vastaajalle henkilökohtaisesti kohdistettuun muotoon saattaa vaikuttaa luonnollisemmalta ja vastaajan motivaatiota lisäävästi. Kysymyksiä pohtiessa tulee pyrkiä sellaisiin sanamuotoihin, joiden johdosta ei vastaajalle pääsisi syntymään väärinkäsityksiä kysymyksen sisällöstä, jotta saadaan vastauksia asetettuihin tutkimuskysymyksiin. Vastausvaihtoehtoja pohdittaessa kannattaa miettiä aineiston analyysitapoja. Mikäli aineistoa tullaan käsittelemään tilasto-ohjelmassa, on vastausvaihtoehdot hyvä numeroida valmiiksi, mikäli se on ohjelmiston kannalta tarpeellista.

Kyselylomakkeella tehdyt kyselyt on perinteisesti toteutettu paperisena. Muitakin tapoja on. Tutkijan lomake kerrallaan keräämä tapa lienee se työläin, kun taas valmiilla ohjelmistolla internetin kautta kerätty lienee aineiston keräämisen kannalta helpoin tapa. Vastausprosenttiin toteutustavalla on merkitystä, mikäli tutkittavia ei ole velvoitettu vastaamaan esimerkiksi työnantajan toimesta. Kyselylomake saattaa vastaajalle tuntua työläämmältä kuin internetin kautta lomakkeeseen vastaaminen. Sähköinen lomake voidaan toteuttaa niin ettei lomakkeessa pääse eteenpäin vastaamatta kaikkiin kysymyksiin. Paperisen lomakkeen osalta vastaavaa mahdollisuutta ei ole. Otantamenetelmiä on useita ja otannan valinnalla sekä koolla on paljon merkitystä tutkimuksen onnistumiselle. Mikäli tutkimuksen on tarkoitus edustaa tasapuolisesti tiettyjä ihmisryhmiä, tulee tämä tietysti huomioida otantaa pohdittaessa. (Valli 2018, osa1.)

2.3 Puolistrukturoitu haastattelu - teemahaastattelu

Hirsjärvi & Hurme (2015, luku 3) mukaan haastattelu menetelmänä soveltuu monenlaisiin tutkimustarkoituksiin. Haastattelun vuorovaikutuksellista luonteesta johtuen sen aikana voidaan

kohdistaa tiedonhankintaa ilmi tulleisiin avoinna oleviin kysymyksiin. Haastattelun aikana on mahdollista saada ymmärrys vastauksista ja niiden takana olevista motiiveista. Tähän tutkimusmenetelmään tulisi kuitenkin suhtautua tiedostaen vapaamuotoisen tai puolistrukturoitujen haastattelujen osalta mahdolliset esiin nousevat ongelmat. Haastattelun avulla voidaan selventää vastauksia ja saada syventävää tietoa. Haastattelussa tutkimusmenetelmänä on haasteena siihen vaadittu aika, joka jakautuu itse haastattelun lisäksi myös haastattelutulosten litterointiin, mikäli kyseessä on vapaamuotoinen haastattelu. Menetelmänä haastattelussa on mahdollisuus moniin virhelähteisiin, joita voivat aiheuttaa sekä haastattelija, että haastateltava.

Hirsjärvi ym. (2015, luku 4) mukaan teemahaastattelussa, jota myös puolistrukturoiduksi kutsutaan, kysymykset ovat samat kaikilla haastateltaville, mutta vastauksille ei tarjota vaihtoehtoja. Tällöin haastateltavilla on mahdollisuus sanoittaa vastaus omin sanoin. Teemahaastattelussa haastattelu kohdistuu tiettyihin teemoihin. Menetelmänä se ei ole sidottu kvalitatiivisiin tai kvantitatiivisiin menetelmiin. Teemahaastattelussa kysymyksiä oleellisempaa on teemoittain etenevä haastattelu. Tällöin haastateltavan tulkinnat tulevat esille eikä tutkijan näkökulmat kysymyksien kautta liiaksi määrää vastauksien suuntaa. Teemahaastattelu on lähempänä strukturoimatonta kuin strukturoitua haastattelua. Haastattelu tutkimusmenetelmänä edellyttää kielen huomioimista. Kielellisten kommunikaatiotapojen on todettu vaihtelevan eri tilanteessa olevien ihmisten kesken ja tämä tulee huomioida haastattelua tehtäessä. Haastattelussa on huomioitava, mikäli tarpeellista, arkielämän tilanteissa käytettävä kieli ja käytettävä sen mukaisia ilmaisuja. Haastateltavien henkilöiden määrään liittyen ei ole olemassa tarkkaa oikeaa lukua. Kaikki riippuu tutkimuksen tarkoituksesta, tutkittavasta kokonaisuudesta, sekä mitä ja miksi tutkitaan. Hirsjärvi ym. (2015, luku 5) mukaan jo muutama henkilö haastattelemalla on mahdollista kerätä merkittävä määrä tietoa. Kun selvitetään yritys- ja organisaatiotason asioita, on haastateltavat hyvä jakaa ryhmiin hierarkkisen aseman mukaisesti. Joissain tapauksissa voidaan kokeilla saturaatio nimellä kulkevaa menetelmää, jossa haastatellaan niin monta haastateltavaa, kunnes uudet haastateltavat eivät enää tuo uutta tutkimuksen kannalta merkittävää tietoa.

Ennen haastattelua tulee teemat olla pohdittuna hyvin etukäteen. Näiden teemojen alle voidaan vielä lisätä joitakin tarkentavia asioita. Pääsääntöisesti teemahaastattelu kuitenkin etenee vapaamuotoisesti haastattelijan ohjatessa keskustelua teemoittain, ajoittain tehden tarkentavia kysymyksiä sellaisen tarpeen esiintyessä. (Hirsjärvi ym. 2015, luku 5.)

Laadullisen tutkimuksen analyysissä aineistoa pyritään käsittelemään yleensä kokonaisuutena. Tällöin argumentaatioita ei perusteta eri yksiköiden välisiin eroihin, vaan tavoitteena on muodostaa käsitys ilmiöstä kokonaisuutena. Laadullisen tutkimuksen analyysissä pyrkimyksenä on havaintojen pelkistäminen sekä tutkimuskysymykseen vastaaminen. (Alasuutari 2011, luku 2.)

Tämän opinnäytteenä tehdyn tapaustutkimuksen tutkimusstrategia on luonteeltaan fenomenologinen, sillä tutkimuksen tarkoituksena on pyrkiä ymmärtämään kohdeorganisaation ihmisten kokemusta kyberturvallisuuden aihealueesta. Tämän tutkimusstrategian luonteesta johtuen aihetta on pyritty lähestymään ilman liian vahvoja ennakko-odotuksia, vaikka aihealueen taustatutkimuksen pohjalta onkin muodostunut jonkinlainen teoreettinen viitekehys. Fenomenologisen tutkimusstrategian mukaisesti tutkimuksen johtopäätökset ovat opinnäytteen tekijän pohdintoja, ja pyrkimystä ymmärtää kohdeorganisaation henkilöstön kokemusta. (Jyväskylän Yliopisto 2015.) Fenomenologia käsitteen kirjaimellinen merkitys tarkoittaa jäsentämistä. Käsite on johdettu kreikan kielen sanoista ilmiö, ilmenevä, järki, käsitteellisyys, tarkoittaen oppia ilmenevästä. Käsitteenä fenomenologia on hyvin laaja ja saattaa eri tutkijoille tarkoittaa hieman eri asiaa. Fenomenologisen liikkeen perustajan pidetään Edmund Husserlia, joka 1800-luvulla poimi käsitteen käyttöön omista filosofian opinnoistaan. Hänen mukaansa tutkimuksen alkuun panijana tulisi olla asiat ja ongelmat. Tutkijan pitäisi pyrkiä ymmärtämään näiden todellisuutta puhtaasti filosofisten asioiden sijaan. (Backman & Himanka 2007, 2–6.)

2.4 Aikaisempi tutkimus

Kyberturvallisuuteen liittyviä kokonaisuuksia on tutkittu viime vuosina huomattavasti enemmän kuin aikaisemmin. Taustateorian keräämisvaiheessa tietokantahakuja tehtiin useilla eri hakusanoilla. Opinnäytetyöhön parhaiten soveltuvat tutkimukset löytyivät hakusanoilla cybersecurity, cybersecurity awareness, cyber awareness, cybersecurity knowledge ja information security awareness. Tietokantahaut tehtiin EBSCOhost, Proquest Central ja ScienceDirect tietokannoista koska opinnäytetyön tekijällä on opintojensa johdosta käyttöoikeus kyseisiin tutkimustietokantoihin. Hakujen jälkeen käytiin tiivistelmätasolla läpi merkittävä määrä tutkimuksia, joista poimittiin opinnäytetyön kannalta olennaisimmat tarkempaa analyysiä ja taustateoriaa varten (Taulukko 1). Aikavälillä 2012–2022 tehdyistä kyberturvallisuustietoisuuteen keskittyvistä tutkimuksista suuri osa oli tehty eri maiden yliopistojen opiskelijoille. Opettajien, varsinkaan ammatillisten oppilaitosten, kyberturvallisuuden tietoisuuden osalta tutkimusta ei juurikaan löytynyt. Tietoturvallisuustietoisuus otsikon alla tutkimusta on tehty enemmän myös muille kuin opiskelijoille. Viime vuosien osalta näissä julkaistuissa ja vertaisarvioiduissa tutkimuksissa käsiteltiin käytännössä myös kyberturvallisuutta tietoturvallisuusotsikon alla.

Taulukko 1 Työhön valittujen tutkimusten valinta- sekä poissulkukriteerit

Hakusanat	Tietokannat	Sisäänottokriteerit	Poissulkukriteerit
cybersecurity, cybersecurity awareness, cyber awareness, cybersecurity knowledge ja information security awareness.	EBSCOhost, Proquest Central ja ScienceDirect	Vertaisarvioitu ja julkaistu tutkimus. Tutkimuksen aiheena henkilöstön kyberturvallisuustietoisuus opetus- ja oppilaitosympäristössä. Tutkimus tehty vuosina 2012–2022	Tutkimuksen kohteena kyberturvallisuuden ammattilaiset. Tutkimus keskittyy tekniseen kyberturvallisuuteen. Tutkimus ei ole sovellettavissa oppilaitosmaailmaan. Tutkimus tehty halutun ajan ulkopuolella. Tutkimusta ei vertaisarvioitu ja julkaistu.

Ramlo & Nicholas (2021, 362–363) mukaan ihmisten henkilökohtainen käyttäytyminen on merkityksellinen kyberturvallisuuden kannalta. Q-menetelmän mukaisessa tutkimuksessa tutkittavat henkilöt jakautuivat suhtautumisen perusteella neljään erilaista asennetta kuvaavaan ryhmään: kyberturvallisuuden parhaisiin käytänteisiin uskoviin, naiiveihin, huolestuneisiin, mutta ei valppaisiin sekä kyberturvallisuuden tärkeyttä kyseenalaistaviin. Tämän tutkimuksen perusteella vain kyberturvallisuuden parhaisiin käytänteisiin uskovat ymmärsivät näiden toimintatapojen merkityksen sekä toimivat erittäin tietoisena ja valppaana näiden toimintatapojen ja ohjeiden mukaisesti. Kolmen muun suhtautumistyypin osalta voitiin todeta, että ne kaikki ovat työnantajan kannalta ei toivottua suhtautumista. Suhtautumistyyppien keskeiset tyypit kuviossa 5.

Kuvio 5 Ramlo ym. (2021, 362–363) mukaillen suhtautuminen kyberturvallisuuteen

Aljohni, Elfadil, Jarajreh & Gasmelsied (2021, 280) mukaan opiskelijoiden kyberturvallisuustietoisuudessa on usein puutteita. Saudi-Arabiassa yliopisto-opiskelijoiden kyberturvallisuustietoisuuden taso oli kohtuullisella tasolla eikä suurempia eroja ollut esimerkiksi sukupuolien välillä. Tietotekniikan opiskelijoiden osalta osaamisen taso oli muita opiskelijoita parempaa. Opiskelijat yleisesti olivat sitä mieltä, että kyberturvallisuustietoisuuden lisäämiseksi olisi tarpeellista järjestää koulutusta myös yliopistossa ja tutkimuksen johtopäätöksenä olikin vahva suositus kyberturvallisuustietoisuutta lisäävän koulutuksen järjestämisestä jo opiskelijoiden opintojen alkuvaiheessa.

Alammary, Alshaik & Pratama (2022, 4–16) tutkivat yliopiston opetushenkilöstön kyberturvallisuustietoisuutta opetettaessa videosovelluksen välityksellä. Tutkimuksen alussa oletuksena oli, että tutkittavat suhtautuisivat työssään yksityisyyteen ja tietoturvaan samalla vakavuudella kuin omien tietojensa suojaamiseen henkilökohtaisissa sovelluksissa. Hieman yllättäen näin ei kuitenkaan ollut. Yleisesti turvallisuus- ja tietoturvatietoisuus oli heikolla tasolla. Tietoisuuden tasoon nostavasti vaikuttivat käytetyn ohjelmiston tuttuus, verkko-opetuskokemus sekä opetettavan alan tietoteknisyys. Tietoisuuden tasoon vaikutti virkaikä organisaatiossa

siten, että yli 10 vuotta opetustyössä olleiden osalta kyberturvallisuustietoisuuden taso oli alhaisempi.

Khader, Karam & Fares (2021, 1–5) kirjalliskatsauksessaan toteavat kyberturvallisuus tietoisuuden osoittautuneen useissa tutkimuksissa organisaation kyberturvallisuuden heikoksi lenkiksi. Hieman organisaatiosta ja toimialasta riippuen haasteena on voinut ollut esimerkiksi tietoisuuden ja osaamisen taso. Joissain kohderyhmissä, kuten yliopisto-opiskelijoissa, haasteena ei niinkään ollut tietämättömyys vaan se ettei osaamista hyödynnetty käytännössä.

Pósa & Grossklags (2022, 491–506) tutkivat työelämässä olevien tietotekniikkaa yliopistossa opiskelevien henkilöiden työ- ja opiskelukokemuksen vaikutusta kyberturvallisuuden riskitietoisuuteen. Tutkimuksessa selvitettiin lisäksi missä kyberturvallisuuden osa-alueissa tämä erityisesti korostuu positiivisesti ja minkä aiheiden osalta vaikutus on negatiivinen. Yleisellä tasolla havaittiin työkokemuksen korreloivan positiivisesti tietoisuudessa etätyö- ja kyberturvallisuusohjeista, sovellusten turvallisuudesta, sosiaalisen manipuloinnin mahdollisuudesta ja kodissa tai muussa vieraassa paikassa sijaitsevaan langattomaan verkkoon kiinnitettyjen laitteiden turvallisuuden huomioimisessa. Omien laitteiden käytön riskit työkäytössä olivat paremmin tiedossa enemmän työkokemusta omaavilla opiskelijoilla.

Sulaiman, Muhammad, Hussain, & Wider (2022, 2–3) ovat tutkineet Malesian valtion työntekijöiden kyberturvallisuustietoisuutta PMT-teoriaa (protection motivation theory) hyödyntäen käyttäjien erilaisia kyberturvallisuuskäyttäytymiseen liittyviä taustoja. PMT-teoriassa on kyse yksilön suhtautumisesta uhkia kohtaan. Yksilön arvioidessa uhan kokonaisvaikuttavuutta hän arvioi uhan vakavuutta sekä omaa haavoittuvuuttaan ja kykyään selvitä tilanteesta. Kokiessaan uhan vakavana, yksilö saattaa olla motivoituneempi osallistumaan esimerkiksi organisaation kyberturvallisuuskoulutukseen, tai todennäköisemmin noudattaa annettuja ohjeita ja opetettuja toimintatapoja. Haavoittuvuustietoisuus vaikuttaa esimerkiksi yleiseen pelkoon kyberhyökkäyksestä sekä tietoisuuteen mahdollisesti puuttuvista turvallisuustoimista ja -toimenpiteistä. Sopeutumisen mallit on jaettu kolmeen osaa. Aikaisempi kokemus kyberhyökkäyksen kohteeksi joutumisesta vaikuttaa kyberturvallisuusohjeiden noudattamiseen motivaatiota lisäävästi. Vastatoimenpiteen tehokkuuteen uskomisen on todettu vaikuttavan toimintaan. Omaan kyvykkyyteen luottavat uskovat osaavansa toimia oikein ja kyberturvallisesti sekä tietävät toimintamallit uhan realisoituessa. Sulaiman ym. (2022, 12) havaitsivat, että tietoisuus uhan olemassaolosta vaikuttaa positiivisesti yksilön kokemukseen uhan vakavuudesta. Tietoisuus kyberturvallisuusuhkista ei kuitenkaan vaikuttanut tutkittavien kokemukseen haavoittuvuudesta. Tietoisuudesta huolimatta käyttäjät saattavat käyttää heikkoja salasanoja tai noudattaa riskialttiita toimintatapoja. He havaitsivat, että kyberturvallisen toimintatavan omaksuneet kokivat matalampaa estettä toimintatapojen ja ohjeiden noudattamiselle. Käyttäjän kokiessa kyberturvalliset toimintatavat työlääksi, on hän myös alttiimpi olemaan noudattamatta kyseisiä ohjeita ja toimintatapoja. Tapojen muuttamisen, ajankäytön ja

epämukavuuden havaittiin olevan esteenä käyttäjien kyberturvallisuusohjeiden ja -toimintatapojen noudattamiselle.

Andronache (2021, 15–16) mukaan tutkimuksessa haastatteluista rahoitussektorin edustajista lähes 31 prosenttia vastasi olevansa huolissaan ihmisten kyvystä tunnistaa ongelmia ja heidän kyvystään välttää virheitä. Tämä on linjassa muun tutkimuksen kanssa. Ihmisen toiminnasta johtuvissa riskeissä kaksi keskeistä tekijää oli puutteelliset kyberturvallisuustaidot sekä kyberturvallisuustietoisuuden taso. Haastateltujen mukaan hyvin usein kyberturvallisuustoimenpiteiden pettäessä taustalla on ihmisestä johtuvat edellä mainitut syyt, jotka voivat vaikuttaa negatiivisesti organisaation kykyyn reagoida nopeasti ja tehokkaasti kyberturvallisuutta vaarantavassa tilanteessa. Turvallisuuskulttuurilla havaittiin olevan tässä suuri merkitys, joten PMT- menetelmän hyödyntämiselle kyberturvallisuustietoisuuden kehittämishankkeissa on vahvat perusteet (Andronache 2021, 17; Sulaiman ym. 2022, 3).

3 Käsitteet

3.1 Tietoturvallisuus

ISO 27000:2020 standardi määrittelee tietoturvallisuuden sellaiseksi tilaksi, jossa organisaation hallussa oleva tieto säilyy eheänä, luotettavana sekä on tarvittaessa organisaation saatavilla. Limnéll ym. (2014, 31) mukaan tietoturvallisuus tarkoittaa olemassa olevan tiedon turvaamista.

Tietoturvallisuus pitää sisällään erilaiset prosessit ja menettelytavat, joilla varmistetaan organisaation toiminnan jatkuminen tietoturvallisena (ISO 27000:2020). Limnéll ym. (2014, 35) mukaan turvallisuuden keskeisenä osana voidaan nähdä sietokyvyn, resilienssin, vaatimus. Toiminnan jatkuvuuden kannalta on oleellista säilyttää toimintakyky häiriön sattuessa.

> Jatkuvuus on organisaation kyky jatkaa tuotteiden ja palveluiden toimittamista hyväksyttävissä olevalla aikavälillä ja ennalta määritellyllä kapasiteetilla häiriön jälkeen. (ISO 22301:2019)

3.2 Kyberturvallisuus

Limnéll ym. (2014, 30–31) mukaan fyysisen ja digitaalisen maailman rajapinnasta johtuen kyberturvallisuus käsitteenä on kehitetty tarkoittamaan näiden yhdessä muodostamaan kokonaisuuteen vaikuttamista hallitusti. Aikaisemmin käytössä olleeseen käsitteeseen, tietoturvallisuuteen, on erona tiedon liikkumisen eri järjestelmissä sisällyttäminen samaan käsitteeseen. Hopkin (2018, 292) toteaa turvallisuuden kannalta keskeisenä kaikkien turvallisuustoimintojen sekä -ajattelun implementoimista kaikkeen organisaation toimintaan. Näin ollen

kyberturvallisuuskin tulisi huomioida kaikessa toiminnassa. Sulaiman ym. (2022, 1) kuvaa kyberturvallisuutta laajaksi tietojärjestelmäkokonaisuudeksi, jossa yhdistyy teknologia- ja ihmiselementti.

Andronache (2021, 9–10) mukaan turvallisuustietoisuus on tarpeellista tietovuotojen ehkäisemiseksi sekä henkilöstön valppauden ylläpitämiseksi. Organisaatioilla on erilaisia ohjeita, toimintatapoja, joiden avulla pyritään pienentämään ihmisistä aiheutuvaa riskiä tavoitteena suojata tiedon eheys, saatavuus ja luotettavuus. Tämä onnistuu varmistamalla henkilöstön tietoisuus kyberturvallisuuteen liittyvistä riskeistä ja vastuistaan.

Vaikka kyberkiusaamisen ei ole todettu vaikuttavan suoranaisesti lisääntyneenä kyberturvallisuusriskinä on sen tunnistaminen ja siihen liittyvän tietoisuuden levittäminen kouluympäristössä tarpeellista (Khader ym. 2021, 4).

3.3 Organisaatio- ja turvallisuuskulttuuri

Organisaatio on ryhmä henkilöitä, joka pyrkii pääsemään yhteiseen tavoitteiseen erilaisten valtaan ja vastuuseen liittyvien toimintojen avulla. Organisaatioita voivat olla esimerkiksi yritykset ja muut yhteisöt, julkishallinnon toimijat kuten viranomaiset sekä hyväntekeväisyysjärjestöt. (ISO 27000:2020.) Reiman, Pietikäinen & Oedewald (2008, 3–16) mukaan turvallisuuskulttuuri on monitasoinen ilmiö ja muodostuu organisaation ihmisten asenteista, uskomuksista, kokemuksista sekä organisaatiossa käytössä olevista prosesseista. On mahdollista, että organisaatiokulttuurin kaikilla osa-alueilla ei ole merkitystä turvallisuuden ja riskien näkökulmasta.

Kansainvälisen atomienergiajärjestön IAEA:n (1991) mukaan turvallisuuskulttuuri on kokoelma yksilöiden ja yhteisön luonteenpiirteitä ja asenteita, joiden avulla toiminnan turvallisuuden kannalta keskeiset osa-alueet tulevat huomioiduksi niiden vakavuuden mukaisesti. Kyseisen ajattelutavan mukaan turvallisuuskulttuuri on asenteellista sekä rakenteellista. Näihin molempiin voidaan vaikuttaa organisaation toimintaperiaatteiden sekä johtamisen menetelmien kautta. Andronache (2021, 12) mukaan turvallisuuskulttuuriin vaikuttavat keskeisesti strategiset ja sosiaaliset vaikutteet sekä yksilön omat näkemykset yhdessä lainsäädännön ja sääntöjen kanssa (Kuvio 6).

Kuvio 6 Andronache (2021, 12) mukaillen turvallisuuskulttuurin vaikutteet

Organisaation toimintakulttuurilla on todettu olevan paljon vaikutusta siihen, kuinka yksilöt suhtautuvat riskin ottoon. Logg & Tinsley (2023) mukaan havaitessaan toisten henkilöiden rikkovan sääntöjä tai ottavan riskejä ilman seuraamuksia ovat ihmiset taipuvaisia itsekin ottamaan isompia riskejä. Samaa pätee organisaatiossa ja yhteiskunnassa yleisesti. Tästä johtuen toimintakulttuuri ja omavalvonta vaikuttavat paljon yksilön toimintaan. Mikäli henkilö toimii tietoturvallisuuden kannalta riskiä aiheuttaen ja siitä ei seuraa mitään tai järjestelmä ei huomaa asiaa, tulee henkilö todennäköisesti toistamaan käytöstään. Lisäksi on erittäin todennäköistä, että henkilö ottaa jatkossa useammin ja isompia riskejä.

3.4 Tietoturvan poikkeama

ISO 27000:2020 standardi määrittelee poikkeaman tilanteeksi, jossa vaatimukset jäävät täyttymättä.

> Häiriö on odotettu tai odottamaton häiriötilanne, joka aiheuttaa suunnittelemattoman negatiivisen poikkeaman tuotteiden ja palveluiden organisaation tavoitteiden mukaisessa toimittamisessa. (ISO 22301:2019)

Haavoittuvuus on heikkous, jota hyökkääjä tai kilpailija voi hyödyntää vaarantaen resurssin luotettavuuden, saatavuuden tai salassapidon. Tällainen heikkous tai virhe voi vaarantaa tietojärjestelmän tai -verkon, sovelluksen tai protokollan toiminnan (Varbanov 2021, 26.) Nämä heikkoudet voivat olla järjestelmään sisään tahallisesti asennettuja takaportteja tai rakentamisvaiheessa vahingossa järjestelmään jääneitä (Limnéll ym. 2014, 236).

Haittaohjelma on ohjelmisto, jota hyökkääjä hyödyntää saadakseen pääsyn kohteena olevaan järjestelmään. Hyökkääjän tavoitteena saattaa olla varastaa tietoa, dataa tai rahaa ihmisiltä ja organisaatioilta. Erilaisia haittaohjelmia voivat olla virukset, vakoiluohjelmat,

madot/troijalaiset, takaovet, kiristysohjelmat, saastutetut mobiililaitteiden sovellukset ja mobiililaitteiden haittaohjelmat. (Varbanov 2021, 23–40; Limnéll ym. 2014, 236.)

4 Kyberturvallisuuteen henkilöstön kautta kohdistuvat keskeiset uhat

Tietoverkkojen ja -järjestelmien teknisen suojauksen kehittyessä ovat rikolliset ja muut toimijat havainneet helpommaksi kohdistaa järjestelmien tunkeutumiseen tähtäävän toiminnan näitä järjestelmiä käyttävään henkilöstöön vaikuttamiseen. On havaittu, että dataan luvatta pääsy on helpompaa hyödyntämällä ihmisten hyväuskoisuutta ja taipumusta auttaa kanssa ihmisiä. Näin ollen yritysten ja organisaatioiden tulee tunnistaa nämä vaikutuksille alttiit tavat ja taipumukset voidakseen vaikuttaa riskiä pienentävästi, esimerkiksi henkilöstön kyberturvallisuustietoisuutta lisäämällä. (Khader ym. 2021, 1.) Suurin osa turvallisuusvuodoista on todettu tapahtuneen käyttäjän huonosta arviointikyvystä, virheestä tai näiden yhdistelmästä johtuen. Huonosti toimivat yksilöt voivat näin vaarantaa koko organisaation. Tietojärjestelmiin tunkeutumiset usein johtuvat käyttäjien tietoisuuden puutteesta, välinpitämättömyydestä, tietämättömyydestä, vastarinnasta, apatiasta tai huonosta käyttäytymisestä. Organisaatio saattaa olla hyvinkin kyberturvallisuustietoinen ja voi käyttää suuria summia tietojärjestelmien tekniseen turvallisuuteen. Tästä huolimatta käyttäjät ovat heikoin lenkki ja altis virheille ja epäonnistumisille. (Suleiman 2022, 1–2.)

Ruoslahti, Coburn, Trent & Tikanmäki (2021, 40) kirjallisuuskatsauksessaan toteavat organisaatioiden kyberturvallisuuden yleisimmin vaarantuneen ihmisten tekemien virheiden tai puutteellisten kyberturvallisuustaitojen ja -tietoisuuden johdosta. Mikäli johto ei ole tunnistanut riskien hallintamenetelmiä oikein, ja ne ovat ristiriidassa organisaation henkilöstön käsitysten kanssa, eivät suunnitellut toimenpiteet mahdollisesti toimi. Tämä johtuu siitä, että tavat toimia eivät todellisuudessa laajene koko organisaatioon, eikä monen turvallisuustoiminnon onnistumisen kannalta tarpeellinen riskitietoisuus saa riittävää jalansijaa henkilöstön keskuudessa. (Reiman ym. 2008, 16.)

Organisaation kyberturvallisuuteen kohdistuu monenlaisia uhkia, joiden hallinnassa turvallisuuskulttuurilla, henkilöstön osaamisella ja kyberturvallisuustietoisuudella on keskeinen rooli. Limnéll ym. (2014, 47) toteaa, että kyberturvallisuudessa kyse on yhden kolmasosan verran teknologiasta ja kahden kolmasosan verran muusta, kuten henkilöstöstä ja ihmisen toiminnasta. Helsingin seudun kauppakamarin Suomalaisissa yrityksissä tekemän kyselyn mukaan 29 prosenttia yrityksistä kokee oman henkilöstön olevan suurin uhka yrityksen kyberturvallisuudelle. 41 prosenttia yrityksistä koki suurimpana kyberturvallisuudessa onnistumisen esteenä käyttäjien piittaamattomuuden tieto- ja kyberturvallisuutta vaarantavista uhista. (Vesterinen & Korslow 2022, 4–5.) Samassa kyselyssä 61,8 prosenttia vastanneista yrityksistä kertoi, ettei heillä ole harjoiteltu kyberturvallisuussuunnitelmien toimivuutta lainkaan vaikka 76 prosenttia

kertoikin henkilöstön tietävän kuinka toimia tunkeutumista epäiltäessä (Vesterinen ym. 2022, 17–19).

4.1 Etätyö

Kolomoets (2022, 1–2) mukaan tietovuotojen riski kasvaa työntekijöiden siirtyessä etätöihin. Tämä johtuu siitä, että työntekijät ovat poissa työnantajan valvomista tiloista, joissa työnantajalla on mahdollisuus valvoa ja ohjata toimintaa. Arvioiden mukaan tietovuodot jopa kaksin- tai kolminkertaistuvat, kun työntekijät työskentelevät kotikoneiltaan, jotka eivät ole työkoneiden tavoin suojattuja tai kun he siirtävät tiedostoja pikaviestipalveluiden ja sosiaalisen median välityksellä. Nwankpa ym. (2023, 11) mukaan etätyökulttuurilla voi olla positiivinen vaikutus organisaation kyberturvallisuuteen, mikäli organisaation perehdytys, koulutus ja toimintamallit ovat kyberturvallisuutta tukevia.

Kotiolosuhteissa kyberturvallisuuden kannalta tärkeää olisi työntekijöiden tiedostaa langattoman verkon reitittimen oikeat suojausasetukset sekä palomuurin ja päivityksien ajantasaisuudesta huolehtiminen. Työnantajan tarjoamien mobiililaitteiden ja omien laitteiden osalta tulisi huomioida ohjeiden mukaiset toimintatavat riskien pienentämiseksi. Työntekijän tulisi osata huomioida kotiverkkoon liitettyjen muiden laitteiden turvallisuus. Näistä varsinkin halvimmissa on usein kustannussyistä jätetty pois monia kyberturvallisuuden kannalta keskeisiä ominaisuuksia. Tästä johtuen laitteiden laadulla ja valmistajalla on kyberturvallisuuden kannalta merkitystä. Kodeissa usein on käytössä laitteita, joissa on mahdollisuus äänikomentoihin. Tällaisissa laitteissa tämä ominaisuus saattaa olla päällä oletusasetuksena tai sen poistaminen on jopa mahdotonta. Etätyöaikana sosiaalinen manipulointi on helpompaa työntekijöiden ollessa pois työyhteisöstään. Työyhteisön läsnäololla on sosiaalisen manipulaation riskiä pienentävä vaikutus. Usein pelkästään siksi, että asioita voidaan hoitaa, ja yhteydenottojen oikeellisuutta varmistaa kasvotusten. (Pósa ym. 2022, 4–7.) Kolomoets (2022, 2) mukaan muissa kuin oman organisaation tietoverkoissa tapahtuva työskentely lisää riskiä. Varsinkin mikäli tietoverkot ovat julkisia, suojaamattomia ja mahdollisesti jopa toisessa maassa.

4.2 Jututtaminen

Organisaatioiden salassa pidettäviä tai pitämiä tietoja voidaan urkkia henkilökohtaisesti ottamalla yhteyttä organisaation työntekijään, jolla voi olla tärkeitä tietoja urkkijan näkökulmasta. Halutut tiedot eivät välttämättä ole juuri niitä lopullisia tietoja, joita urkkiva osapuoli tai jututtaja tavoittelee. Kohteena voi olla tietoja, joiden avulla on mahdollista ottaa yhteyttä toiseen henkilöön tai muutoin tietoja yhdistelemällä päätellä haluttuja asioita. Erilaisin psykologian keinoin urkkijan tavoitteena on herättää tunne luottamuksellisesta vuorovaikutustilanteesta, jolloin kohdehenkilö saadaan avautumaan asioista, joita hän ei muutoin tulisi paljastaneeksi. Erilaisia tilanteita ja tapoja, joissa jututtaja voi ottaa yhteyttä ja pyrkiä avaamaan vuorovaikutussuhde ovat esimerkiksi: valetyöhaastattelut ja -

rekrytointiyhteydenotot, kyselylomakkeet, kohtaaminen harrastuksissa, messuilla tai muutoin työhön liittyen. (Vesterinen 2021, 1–3.) Sosiaalisen manipuloinnin avulla tapahtuvat hyökkäykset ovat kalastelusähköpostien ohella yleisimpiä organisaatioiden kohtaamia hyökkäysmenetelmiä. Hyökkääjät hyödyntävät työntekijöiden tietämättömyyttä tietoturvasta sekä samoja etäyhteysohjelmistoja kuin yrityksen omakin tietojärjestelmää hallinnoiva henkilöstö (Ruoslahti ym. 2021, 40; Kolomoets (2022, 4.) Tähän samaan kategoriaan kuuluvat ns. toimitusjohtajahuijaukset sekä sosiaaliseen mediaan tehtyjen valetilien avulla aikaan saatu valheellisen luottamuksen tunne (Varbanov 2021, 39).

4.3 Kalastelusähköpostit

Haittaohjelmien ja kalasteluviestien avulla tehtyjä hyökkäyksiä pidetään monessa yrityksessä merkittävimpänä yrityksensä kohtaamana uhkana (Vesterinen ym. 2022, 4; Ruoslahti ym. 2021, 40). Kahneman (2012, 350–351) mukaan usein ihmisten toiminta on vaistonvaraista. Tämä ilmenee tilanteissa siten, etteivät ihmiset malta ottaa selvää asioista ennen kuin toimivat. Voi tulla eteen tilanne, jossa he arvioivat riskiä virheellisin perustein ja saattavat seurauksen pelossa tulla valinneeksi toimintatavan, joka on todellisuudessa seurauksiltaan tekemättömyyttä vakavampi. Näitä ajattelun vinoumia ja ominaisuuksia hyökkääjät usein hyödyntävät kalasteluposteja lähettäessään. Kun sähköposti on muotoiltu tärkeäksi ja kiireelliseksi vastaanottajalle muodostuu paine reagoida linkki tai liite avaamalla, jotta ei joutuisi kärsimään mahdollisesta asian viivästymisestä tai hoitamattomuudesta aiheutuvista seurauksista. Kiireessä ihmiset eivät jaksa lukea viestejä ja lähettäjien osoitteita kunnolla eivätkä pohdi rauhassa onko viesti aiheellinen. He tulevat helposti avanneeksi haitalliselle sivustolle johtavan linkin tai liitteenä olevan haittaohjelman sisältävän tiedoston. (Kahneman 2012, 412–413.)

4.4 Hakutulosten ja mainosten turvallisuus

FINE (2022) raportoi joulukuussa 2022 heille tulleen suuri määrä yhteydenottoja liittyen asiakkaiden ohjautumisesta huijareiden hallinnoimille verkkopankkien tai muiden tunnistautumista edellyttävien palveluiden sivuilta näyttäville sivuille. Yleisimpiä huijaustapoja on mainokset ja kalastelusähköpostit, mutta näille sivuille joudutaan myös huolimattomien verkkohakujen johdosta. Hakemalla esimerkiksi Google-haun avulla pankin tai muun palvelun nimellä voi hakutuloksien joukkoon nousta huijaussivustoja, joiden mainoksia rikolliset ovat saaneet nostettua hakutulosten kärkeen. Samanlaisesta ongelmasta Keskusrikospoliisi varoitti vuonna 2021 Omakanta palvelun käytön lisääntyessä Covid19 rokotustodistusten latausten tarpeesta johtuen. (IS 2021.) Varbanov (2021, 39–40) mukaan tämä on yksi varteen otettava hyökkäystie järjestelmiin.

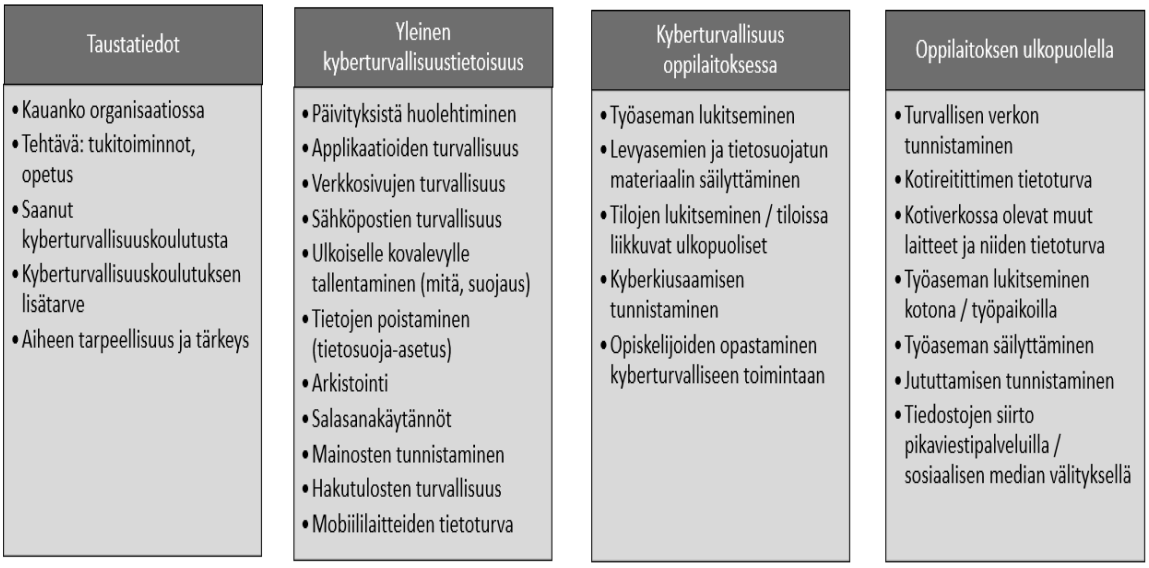
Internetin kautta tapahtuvissa hyökkäyksissä mainosten ja pop-up ikkunoiden avulla on saatu houkuteltua henkilöstö avaamaan hyökkääjän haluama sivusto. Tältä sivustolta on

organisaation järjestelmään saatu ladattua esimerkiksi haitta- tai kiristysohjelma tai muuten aikaan saatu pääsy järjestelmään. (Khader ym. 2021, 3.)

4.5 Salasanakäytännöt

Khader ym. (2021, 2) kirjallisuuskatsauksen mukaan useissa tutkimuksissa havaittiin tutkittavilla esiintyneen taipumusta salasanakäytäntöjen ja ohjeistusten välttämiseen. Tällöin henkilöt pyrkivät pitämään salasanansa mahdollisimman yksinkertaisena ja käyttivät samaa salasanaa monessa palvelussa sekä välttelivät 2-vaiheisen tunnistautumisen käyttämistä, mikäli se oli mahdollista. Salasanoihin on havaittu päästyn käsiksi sosiaalisen manipuloinnin ja vaikuttamisen, kuten jututtamisen, keinoin (Varbanov 2021, 38). Älypuhelinten osalta olisi hyvä muistaa suojausasetukset ja salasanat sekä suojata älypuhelin pääsykoodilla (Limnéll ym. 2014, 51).

Kirjallisuuskatsauksen johtopäätösten pohjalta aihealueet voisi jakaa neljään osaan: taustatiedot, yleiset kyberturvallisuustietoisuuteen liittyvät kysymykset, kyberturvallisuus oppilaitoksessa ja kyberturvallisuus oppilaitoksen ulkopuolella (Kuvio 7).



Kuvio 7 Kyselyn osa-alueet kirjallisuuskatsauksen pohjalta

5 Asiantuntijahaastattelut

Ennen kyselylomakkeen kysymysten suunnittelua oli tarpeellista haastatella organisaation tietoteknisistä järjestelmistä vastaavaa päällikköä sekä organisaation turvallisuusasioista vastaavaa johtajaa. Haastattelut toteutettiin Teams:in välityksellä. Haastatteluilla varmistettiin

kirjallisuuskatsauksesta esille nousseiden asioiden oleellisuus toimeksiantajan organisaation kannalta ja, että kaikki kohdeorganisaation kyberturvallisuuden kannalta keskeiset asiat tulevat varmasti huomioitua kyselyssä.

Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina siten, että ennen haastattelua haastattelija valmisteli aiemmasta tutkimuksesta nousevien kysymysten perusteella kokonaisuuksia, joihin kaivattiin tarkennusta. Lisäksi haastatteluissa pyrittiin löytämään kohdeorganisaation toiminnalle tyypillisiä osa-alueita, joita ei aikaisemman tutkimuksen perusteella mahdollisesti tullut esille. Haastattelutilanteessa aihealueiden sisällä edettiin tarpeen mukaan sinne, minne vastaukset keskustelua johdattelivat.

5.1 Tietoteknisistä järjestelmistä vastaavan päällikön haastattelu

Haastattelussa käsiteltiin organisaation kyberturvallisuuden nykytilanne, jonka todettiin olevan hyvällä tasolla. Teknisten järjestelmien ominaisuuksista johtuvia ongelmia tai haavoittuvuuksia ei ole tähän mennessä havaittu omissa, eikä ulkopuolisten tekemissä analyyseissä. Teknisten järjestelmien päivitykset ja teknisen tietoturvallisuuden kannalta olennaisten ominaisuuksien todettiin olevan ajan tasalla ja vaatimuksia vastaavat. Näiden toiminnan kannalta olennaista on yhteistyökumppanien ja ohjelmistojen toimittajien nopea reagointi havaittuihin mahdollisiin haavoittuvuuksiin sekä päivityksien tuottaminen riittävän nopeasti. Näistä tiedottaminen on tärkeää. (Lehtinen 2023.)

Henkilöstön toiminnan suurimpana haasteena haastateltava toi esille erilaiset huijausviestit. Näiden viestien viimeaikainen kehittyminen on herättänyt huolta henkilöstön kyvystä havaita ja tunnistaa kyseisiä viestejä jatkossakin. Jonkin verran ilmoituksia henkilöstöltä on aiheista kuitenkin tullut. Se osoittaa jonkinlaista asiaan liittyvää valveutuneisuutta organisaation työntekijöillä jo olevan. Näiden niin sanottujen phishing- tai kalasteluviestien tarkoitus on pyrkiä hankkimaan viestin lähettäjälle pääsy organisaation järjestelmään hyödyntämällä työntekijän kiirettä tai muuta syytä, ettei huijausviestiä tunnisteta. Näiden viestien avulla tunkeutujat ovat pyrkineet saamaan työntekijältä käyttäjätunnukset järjestelmään. Jonkin verran on liikkeellä viestejä, joilla on pyritty saamaan työntekijä avaamaan viestin liitteenä oleva tiedosto, joka sisältää tunkeutumisen mahdollistavan haittaohjelman. Näitä viestejä ei tule pelkästään sähköpostitse ja tekstiviestinä vaan niihin henkilöstö törmää myös Whatsappissa, Facebookissa ja muissa sosiaalisen median palveluissa. (Lehtinen 2023.)

Haastattelun aikana muita henkilöstön toiminnasta nousevia mahdollisia riskejä todettiin olevan mobiililaitteiden suojaus. On mahdollista, että pin-koodina saattaa olla oletusasetuksena oleva, mobiililaitteessa ei välttämättä ole lainkaan lukitusta tai käytetään samaa oletuskoodia kuin sim-kortissa. Vieraiden tai julkisten tietoverkkojen käytön osalta havaittiin jonkinlaisen riskin mahdollisuus, mutta organisaatiossa käytössä olevien kannettavien työasemien suojaus on teknisesti hyvällä tasolla ja kaikki verkkoliikenne on suojattu, joten tämän ei todettu

sellaisenaan olevan erityisen korkea riski. Samaan johtopäätökseen tultiin kotiverkoissa työn tekemisen osalta. Aikaisempi kirjautuminen esimerkiksi johonkin tunnettuun julkiseen verkkoon mahdollistaa koneen automaattisen yhdistymisen johonkin toiseen langattomaan verkkoon, jolla on sama SSID-tunniste. (Lehtinen 2023.)

Työaseman säilyttäminen organisaation tiloissa ja niiden ulkopuolella todettiin olevan jonkinlainen riski johtuen opetushenkilöstön liikkuvasta työstä yrityksissä ja eri oppilaitosyksiköissä. On mahdollista, että työasemia säilytetään väliaikaisesti esimerkiksi ajoneuvoissa julkisella paikalla tai työnantajien tiloissa. Ammatilliset oppilaitokset ovat lainsäädännöstä johtuen avoimia tiloja, ja opetustakin pääsee seuraamaan jokainen niin pyytäessään. Tämän todettiin muodostavan mahdollisen riskin, mikäli tiloissa liikkuvia henkilöitä pyrkisi esimerkiksi henkilöstön työtiloihin tai tekniseen tilaan. Mahdollisesti käytössä olevat ulkoiset levyasemat ja muistitikut muodostavan riskin henkilöstön tallentaessa niihin tietosuoja-asetuksen alaista materiaalia. Opetus- ja lähdemateriaalien joutumien ulkopuolisten käsiin ei muodosta riskiä. Mikäli henkilöstö ei ole ohjeistuksien vastaisesti tallentanut suoraan työasemalla mitään tietosuojan kannalta olennaista, ei työaseman joutuminen vääriin käsiin välttämättä muodosta riskiä kaksivaiheisen tunnistautumisen ansiosta. (Lehtinen 2023.)

Haastattelussa kysyttiin jututtamisesta riskinä ja mitä seurauksia tällaisesta voisi olla. Organisaatiossa on tietoturvaselvityksen yhteydessä testattu jututtamisen mahdollisuutta sekä edellisessä kappaleessa mainittua ulkopuolisen liikkumista luvatta tiloissa. Tuolloin tilanteen todettiin olevan hyvällä tasolla. Tiloissa kulkemiseen liittyen kulunvalvontatunnisteiden oikeaoppinen kuittaaminen sekä vain henkilökohtaiseen käyttöön luovuttaminen todettiin tärkeäksi. Opetushenkilöstö liikkuu paljon eri toimipisteiden välillä ja oppilaitoksen tiloissa työskentelee tuntiopettajia sijaisena. Henkilöstön tulisi aina varmistaa oleskelun oikeellisuus tavatessaan oppilaitoksen suljetuista tiloissa tuntemattoman henkilön tai tuntemattoman henkilön sellaiseen tilaan pääsyä pyytäessä. (Lehtinen 2023.)

Viimeisenä kokonaisuutena haastattelussa aiemmin mainitun kulunvalvontatunnisteiden lainaamisen lisäksi tuli ilmi oppilaitosympäristön avoimuuden ja yleisen luottamuksen oletusarvoisuuden muodostama mahdollisuus sille, että työasemia jaetaan käytössä sekä opiskelijoiden, että kollegoiden kanssa. Tämä ei suoranaisesti muodosta riskiä, mikäli työasema ei ole avattu henkilöstön edustajan henkilökohtaisilla tunnuksilla. Toimintamalli saattaa kuitenkin olla mahdollinen ja yhdessä huonon työaseman käytön valvonnan kanssa saattaa muodostaa riskin. Lisäksi käyttäjätunnuksia ja salasanoja saatetaan jakaa, jotta mahdollisuus päästä järjestelmiin saadaan hetkellisestä tarpeesta johtuen annettua jollekin toiselle henkilölle. (Lehtinen 2023.)

5.2 Turvallisuusasioiden johtajan haastattelun tulokset

Haastateltava totesi organisaation tieto- ja kyberturvallisuuden olevan yleisesti hyvällä tasolla. Hyria konsortiossa on käynnissä kyberturvallisuuden kehittämisprojekti, jonka osana on käyty lävitse kyberturvallisuuden johtamiseen liittyviä prosesseja sekä poikkeustilanteen johtamista. Organisaatiossa on harjoiteltu kyberturvallisuutta vaarantavaan tilanteen johtamista. Yleisestä tilanteesta johtuen on jouduttu varautumaan tilanteisiin sähkökatkojen sattuessa ja näiden osalta on tehty suunnitelmat sekä ohjeistettu henkilöstöä toimimaan oikein ja turvallisesti. Kyberturvallisuus on huomioitu sähkönjakelun häiriön sattuessa. (Kymäläinen 2023.)

Haastateltava totesi yhdeksi haasteeksi moniympäristötyön, jossa työntekijät työskentelevät työn tekemisen paikkaa vaihdellen. Tämä koskee isoa osaa opetushenkilöstöstä, jotka tekevät työtä oppilaitoksen eri toimipisteissä, opiskelijoiden työnantajilla, kotona sekä muissa etätyöpaikoissa. Tämä osaltaan muodostaa haasteita ja riskejä sillä organisaatio ei pysty varmistamaan muiden kuin omien tilojensa verkkojen turvallisuuden. Riskinä on langattomat verkot muualla kuin työnantajan toimitiloissa sekä näihin verkkoihin liittyneet muut laitteet, joiden tietoturva usein ei vastaa työkäytössä olevien laitteiden vaatimuksia. Kotona töitä tehdessä samaan langattomaan verkkoon voi olla liittyneenä monenlaisia kodin laitteita kuten televisioita, pelikonsoleita, tulostimia sekä esimerkiksi musiikin toistoon tarkoitettuja laitteita. Samaa verkkoa voi usein käyttää muutkin kuin työntekijä itse. Esimerkiksi tämän lapset ja lasten ystävät. (Kymäläinen 2023.)

Työnantajan työkäyttöön tarjoamien laitteiden osalta todettiin ohjelmistojen olevan ajan tasalla ja automaattisesti päivittyviä, mutta riski voi muodostua, kun käytetään ristiin työ- ja omia laitteita. Ristiin käyttöä voi tapahtua kumpaan suuntaan vain, joko omia asioita työlaitteilla tai omilla laitteilla työasioita hoidettaessa. Omista sähköposteista työasioiden hoitamista ei ohjeistuksen mukaisesti pitäisi tapahtua. Henkilöstön toimiessa ohjeiden mukaan pienenee riski esimerkiksi sähköpostitse tapahtuviin huijauksiin. Tiedostojen ja liitteiden lähettäminen laitteelta ja käyttäjätililtä toiselle saattaa muodostaa jonkinlaisen riskin, vaikka järjestelmät hyvin havaitsevat ja torjuvat jo tiedossa olevat haittaohjelmat. Ulkoisille kovalevyille ja muistitikuille tallentamisen osalta riski on haastateltavan mielestä olemassa ja tähän asiaan liittyen lisäselvitys tarpeellinen. Työasemille tallentaminen verkkoyhteyden puuttumisen, sähkönjakelun häiriön tai muun syyn johdosta todettiin olevan ohjeistuksesta huolimatta asia, jonka yleisyydestä olisi hyvä saada jonkinlainen käsitys. Sekä varmistus sille, että tietosuojattua materiaalia ei tallennettaisi organisaation ohjeistamien sijaintien ulkopuolelle. (Kymäläinen 2023.)

Haastattelun aikana esiin nousi oppilaitosten avoimuus, joka mahdollistaa tiloissa liikkumisen ilman siihen oikeuttavaa asiaa tai kulkulupaa. Näihin tilanteisiin liittyy riski, että ulkopuolinen pääsee käsiksi työasemiin tai organisaation verkkoon. Tästä johtuen työasemien ja

henkilöstön työtilojen lukituksesta huolehtiminen sekä hyvien salasanakäytäntöjen mukaisten toimintatapojen noudattaminen on tärkeää. Yksi näkökulma on opiskelijoiden kyberturvallisuustaidot, niiden opettaminen sekä merkitys oppilaitoksen kyberturvallisuudelle myös osoituksena opettajien kyberturvallisuustaidoista ja -tietoisuudesta. Henkilöstön keskuudessa on suuri vaihtelu tietoteknisten järjestelmien ja ohjelmistojen käyttöön käytetyn työajan osalta. Joidenkin henkilöiden osalta kyseessä on käytännössä joitakin tunteja viikossa ja toisten osalta suurin osa työajasta kuluu näiden järjestelmien ja ohjelmistojen parissa. Tämä on asia joka haastateltavan näkemyksen mukaan tulisi huomioida kyselyä tehtäessä. Muita toimeksiantajan näkemyksen mukaan kiinnostavia taustatietoja on vastaajien työuran pituus sekä työuran pituus Hyriassa, aikaisemmin saatu kyberturvallisuuskoulutus sekä vastaajan kokemus sen tarpeesta. Haastattelussa tuli ilmi oletus kyberturvallisuuskäsitteen käytön mahdollisesta negatiivisesta vaikutuksesta vastausprosenttiin. Tietoturvallisuus käsitteenä saattaisi olla helpommin lähestyttävä eikä kuitenkaan vaikuttaisi tutkimuksen lopputulokseen. (Kymäläinen 2023.)

5.3 Asiantuntijahaastatteluiden yhteenveto

Organisaation tietoturvallisuudesta vastaavien henkilöiden haastatteluiden perusteella vahvistui aikaisemman kirjallisuuskatsauksen kanssa samankaltainen kuva haasteista, joita ammatillisen oppilaitoksen kyberturvallisuus kohtaa oman henkilöstön toiminnasta johtuen. Näiden tietojen pohjalta kyselyn keskeisiksi osa-alueiksi (Kuvio 8) valikoitui taustatiedot, yleinen kyberturvallisuustietoisuus sekä toiminta työtehtävissä.

Taustatiedot	Yleinen tietoisuus	Toiminta työssä
• Sukupuoli-identiteetti • Sijainti organisaatiossa • Työsuhteen pituus • Aikaisempi kyberturvallisuuskoulutus • Hyrian perehdytyksessä saatu kyberturvallisuuskoulutus • Kokemus aiheen tärkeydestä • Kokemus taitojen riittävyydestä • Lisäkoulutuksen tarve • Kokemus, että omassa organisaatiossa tietoturvallisuusosaaminen on hyvällä tasolla	• Tietoinen kyberturvallisuuteen liittyvistä asioista • Tietojärjestelmien käytön määrä työtehtävissä • Tallentaa mobiililaitteen pin-koodeja ja salasana tms. • Tietoturvallisuuden huomiointi työajan ulkopuolella • Virusturva omissa laitteistoissa • Jos työnantaja olisi valmis tarjoamaan tietoturvaa omiin laitteisiin olisiko valmis • Olen pohtinut kodissani käytössä olevan langattoman tietoverkon tietoturvaa • Varmuus omaan verkkoon yhdistettyjen laitteiden tietoturvasta • Internet sivuille navigointitapa • Sähköpostin lähettäjän oikeellisuuden varmistaminen	• Tapana käyttää samaa salasanaa useassa laitteessa/ohjelmistossa • Työasemien jakaminen muiden kanssa • Käyttäjätunnusten jakaminen muiden kanssa • Työaseman lukitseminen koneelta poistuessa • Työpaikoilla, messuilla, työmatkoilla tms. henkilökohtainen työasema mukana vai erikseen matkatarkoitukseen • Ulkoisten kovalevyjen ja usb-tikkujen käyttö • Suoraan työasemalle tallentaminen • Voin yhdistää mihin tahansa langattomaan verkkoon tietoturvallisesti • Huomioin tietoturvan perehdyttäessäni opiskelijoita tietojärjestelmien ja ohjelmistojen käyttöön

Kuvio 8 Kyselyllä selvitettävät aihealueet

6 Aineiston kerääminen

Alammary ym. (2022, 8–9) tekemä kyberturvallisuuden tietoisuutta koskeva tutkimus toteutettiin verkossa kyselylomakkeella, jossa kysymykset oli jaettu kolmeen osaan yleisiin taustatietoihin kuten sukupuoli, ikä, pohjakoulutus, työkokemus organisaatiossa, opetuskokemus. Toisessa osiossa tutkittiin vastaajien yleistä asennetta tietoteknisiä järjestelmiä kohtaan sekä heidän digilukutaitoaan. Kolmannessa osiossa kyberturvallisuustietoisuutta mitattiin erilaisilla tilannekuvauksilla, joiden perusteella vastaajat saivat valita mielestään osuvimmin heidän toimintatapaansa kuvaavan vaihtoehdon.

ECHO hankkeen osana on kehitetty kyberturvallisuusosaamisen viitekehys ECHO Cybersecurity framework (E-CSF). E-CSF on työkalu, jonka avulla organisaation on mahdollista arvioida henkilöstön kyberturvallisuusosaamisen puutteita. Tämä niin sanottu gap-analyysityökalu on kehitetty erityisesti terveydenhuollon, liikenteen ja energiahuollon toimialoille tunnistamaan henkilöstön osaamisvaatimuksen ja nykyosaamisen väli (englanniksi gap). E-CSF työkalu on tarkoitettu teknisen kyberturvallisuuden parissa työskentelevän henkilöstön osaamisen kartoittamiseen, joten ei sellaisenaan käy tähän työhön. Työkalu toimii kuitenkin monipuolisen haavoittuvuuslistauksensa puolesta tässä työssä hyvänä lisälähteenä kyselyn kysymyksiä tuotettaessa. (Varbanov 2021, 4–5.)

6.1 Kyselyn toteutus

Aineiston keräystavaksi valikoitui verkon kautta tehtävä kysely henkilöstön työn liikkuvasta luonteesta johtuen. Hyrian toimipisteitä on usealla paikkakunnalla, jonka lisäksi henkilöstö kiertää työpaikoilla sekä hybridityömallin mukaisesti työskentelee myös muualla kuin Hyrian toimitiloissa. Verkossa toteutettavan kyselyn tarkoituksena oli varmistaa mahdollisimman suuri osallistujamäärä jakamalla kyselylomake henkilöstölle sähköpostin välityksellä. Kysely toteutettiin Webropol alustalla, johon opinnäytteen tekijällä on työnsä puolesta käyttöoikeudet olemassa. Toisena vaihtoehtona oli Google Forms palvelu, mutta Webropol valikoitui käytettävyyden sekä analyysiominaisuuksiensa johdosta. Vastausajaksi valittiin kaksi viikkoa, jotta kaikilla olisi varmasti aikaa vastata, mikäli näin halusivat. Kyselyn toteutusajaksi valittiin ajankohta, jolloin oppilaitoksen päätoimialueella (Hyvinkää-Riihimäki) ei ole talviloma-viikkoa, sillä tuohon ajankohtaan ajoittuu henkilöstön enemmistön vapaajaksot. Kysely ajoittui ajalle 28.2.-14.3.2023. Linkki Webropol kyselyyn jaettiin sähköpostilla (Liite 2) koko Hyria konsortion henkilöstölle. Viisi päivää ennen kyselyn sulkeutumista aiheesta muistutettiin Hyrian Yammerissa, jonka viestit näkyvät organisaation sisäisen verkon aloitussivulla. Kyselyn sulkeutumista edeltävänä päivänä lähetettiin vielä sähköpostimuistutus koko konsortion henkilöstölle.

Kyselyä varten kysymykset (Liite 3) valikoituivat kirjallisuudessa sekä haastatteluista esiin nousseiden haavoittuvuuksien pohjalta. Kysymykset pyrittiin jakamaan siten, että niistä

muodostuisi kokonaisuuksia, jolloin vastaajan on helpompi keskittyä yhteen aihepiiriin kerrallaan. Yksittäisten kysymysten muotoilussa painotettiin selkeyttä ja ymmärrettävyyttä, jotta vastauksilla saadaan tavoiteltua tietoa ilman väärin ymmärryksiä. Joidenkin kysymysten osalta niiden muotoilun valintaan vaikutti aineiston keruun lisäksi ajatus niiden tietoisuutta lisäävästä vaikutuksesta.

Taustatiedoissa päädyttiin kysymään sukupuoli-identiteetistä tutkimuksellisestä näkökulmasta, vaikka yhteyshenkilöiden mukaan kohdeorganisaation näkökulmasta tällä tiedolla ei ole merkitystä. Tutkimuksen kannalta se saattaa kuitenkin tuoda esille ilmiöitä, joilla voi olla merkitystä asiaa tarkastellessa. Samasta syystä vastaajien ikäryhmää päädyttiin kysymään. Kuitenkin karkeasti kolmeen ryhmään jakaen. Taustatietojen osalta jätettiin kysymättä tarkkoja osastotietoja, sillä se saattaa vaarantaa tutkittavien anonymiteetin pienempien osastojen vastausprosentin mahdollisesti vaihdellessa. Hyria Konsortion sisällä työskentelyn osalta kysyttiin, työskenteleekö vastaaja Hyria Koulutus Oy:ssä vai Hyria Business Institutessa tai Hyria säätiössä. Työsuhteen pituutta Hyriassa kysyttiin, jotta voitiin selvittää sen merkitys kyberturvallisuusosaamisen kokemuksen ja tietoisuuden kannalta. Viikoittainen työaika tietojärjestelmien parissa on olennainen tieto arvioitaessa osaamisen ja riskin suhdetta. Näiden lisäksi koulutusaste valittiin taustatietoihin aikaisemman tutkimuksen esiin nostamien havaintojen pohjalta.

Ennen kyselyn julkaisua kyselylomaketta koekäytettiin kolmeen eri kertaan 10 henkilön toimesta. Jokaiselta koekäyttäjältä kerättiin palautteet, joiden perusteella lomaketta sekä kysymysten muotoiluja muokattiin ymmärrettävyyden ja käytettävyyden lisäämiseksi. Lopuksi kyselylomake vielä koekäytettiin toimeksiantajan yhteyshenkilön toimesta, jonka jälkeen kyselyn toteuttamiselle saatiin lopullinen lupa.

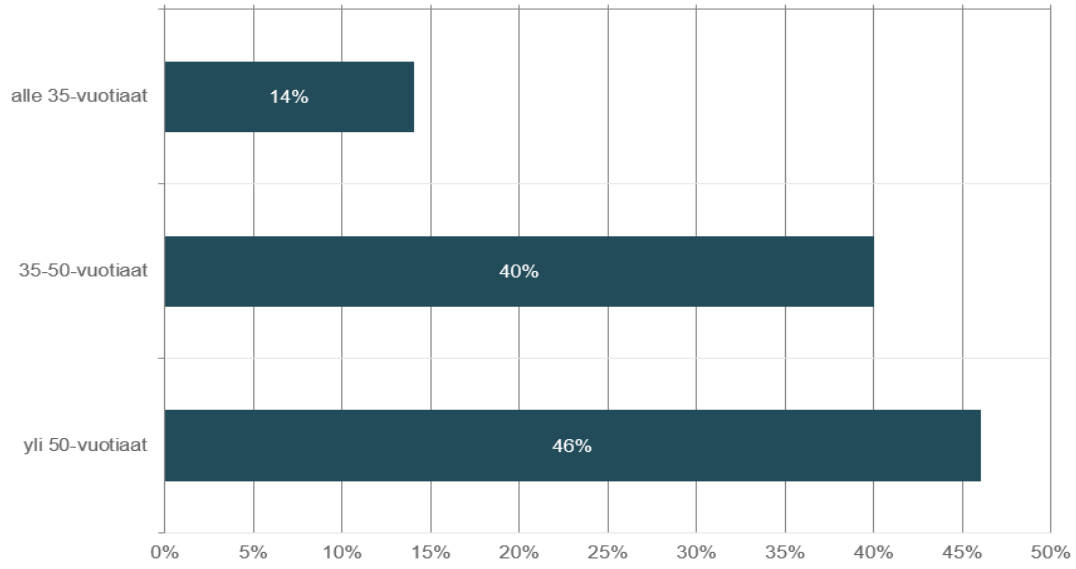
6.2 Haastattelujen toteutus

Kyselyn jälkeen toteutettiin teemahaastattelut (Liite 4), joissa haastateltiin Microsoft Teams:in välityksellä Hyrian henkilöstöstä vapaaehtoisesti haastateltavaksi ilmoittautuneita henkilöitä. Haastateltavat jakautuivat koko organisaation henkilöstörakennetta mukaillen henkilöstöraportin mukaisesti. Haastattelut tallennettiin sekä litteroitiin Microsoft Office365 osana olevan tekstinkäsittelyohjelma Wordin litterointiominaisuuden avulla. Haastatteluiden teemat jakautuivat tutkimuskysymysten mukaisesti: minkälainen on henkilöstön kyberturvallisuustietoisuus, miten kyberturvallisuustietoisuus näkyy arjessa ja miten henkilöstön tietoisuutta voidaan kehittää?

7 Tulokset

Tutkimuksen pääaineistona toimivaan kyselyyn vastasi 252 (n=252) henkilökunnan jäsentä. Henkilöstön kokonaismäärän ollessa noin 520 voidaan vastausprosenttia pitää hyvänä ja siltä osin tuloksia organisaation henkilöstön näkemyksiä kuvaavana. Taustatietoja vastaajilta kerättiin kysymyksillä 1–8. Vastaajat jakautuivat sukupuoli-identiteetin mukaan miehet 31,3 % (n=79), naiset 65,5 % (n=165) ja kysymykseen ei halunnut vastata 3,2 % (n=8) vastaajista. Tämä noudattaa hyvin Hyrian (2023) henkilöstöraportin mukaista sukupuolijakaumaa, jossa naisia on 67 % ja miehiä on 33 %.

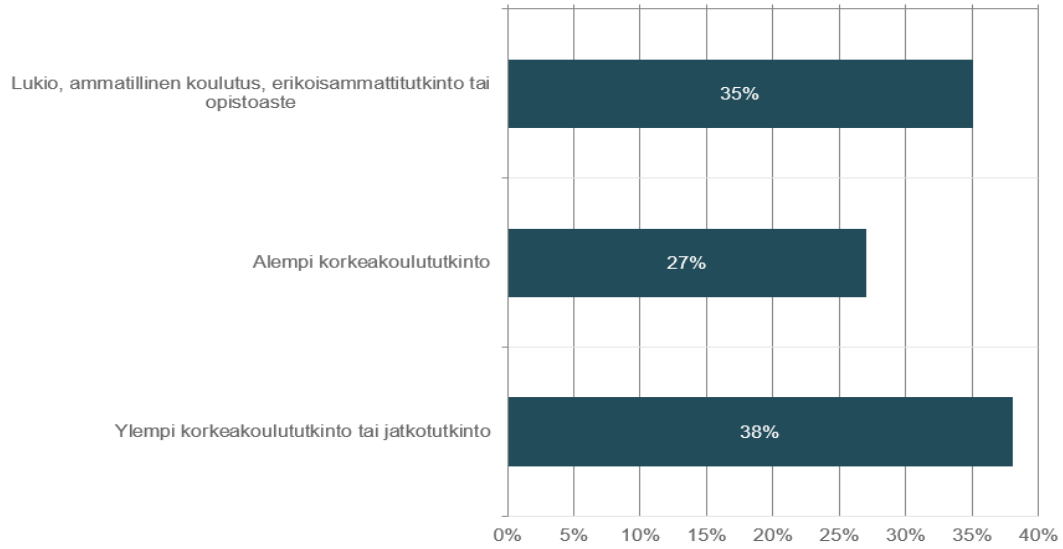
Vastaajat jakautuvat (Kuvio 9) iän puolesta siten, että alle 35-vuotiaita vastaajissa on pienin ryhmä (n=36), 35-50-vuotiaita toiseksi suurin ryhmä (n=100) ja yli 50-vuotiaita vastaajista edustaa suurin ryhmä (n=116). Henkilöstön keski-iän ollessa 47 vuotta (Hyria, 2023) on vastaajien ikäjakauma organisaation henkilöstön ikäjakauman kaltainen.



Kuvio 9 Kyselyyn vastanneen henkilöstön (n=252) ikäjakauma

Ylimmän koulutusasteen osalta vastaajat jakautuivat (Kuvio 10) siten, että suurimman ryhmän muodostaa vastaajat, joiden ylin koulutusaste on ylempi korkeakoulututkinto tai jatkotutkinto (n=94). Toiseksi suurimman ryhmän muodostavat vastaajat, joiden ylin koulutus on opistoaste tai alempi (n=88). Pienintä ryhmää vastaajista edustaa alempi korkeakoulutus (n=68). Koska kysely koski koko oppilaitoksen henkilöstöä on koulutusjakaumassa huomioitava erilaiset organisaation itse omalla henkilöstöllä toteuttamat tukipalvelut sekä opetus- ja ohjaushenkilöstön koulutusvaatimuksien erilaisuus. Esimerkiksi ammatillisten aineiden opettajan kelpoisuuteen

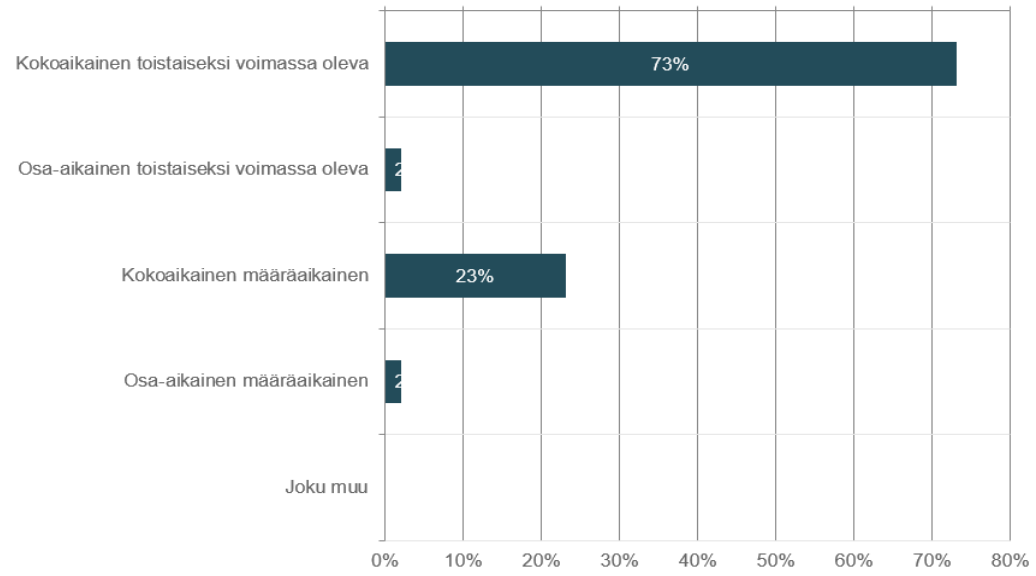
saattaa joillakin koulutusaloilla riittää erikoisammattitutkintotasoinen koulutus ja yleisten tutkinnon osien opettajan koulutusvaatimuksena on vähintään ylempi korkeakoulututkinto.



Kuvio 10 Vastaajien ylin koulutusaste (n=250)

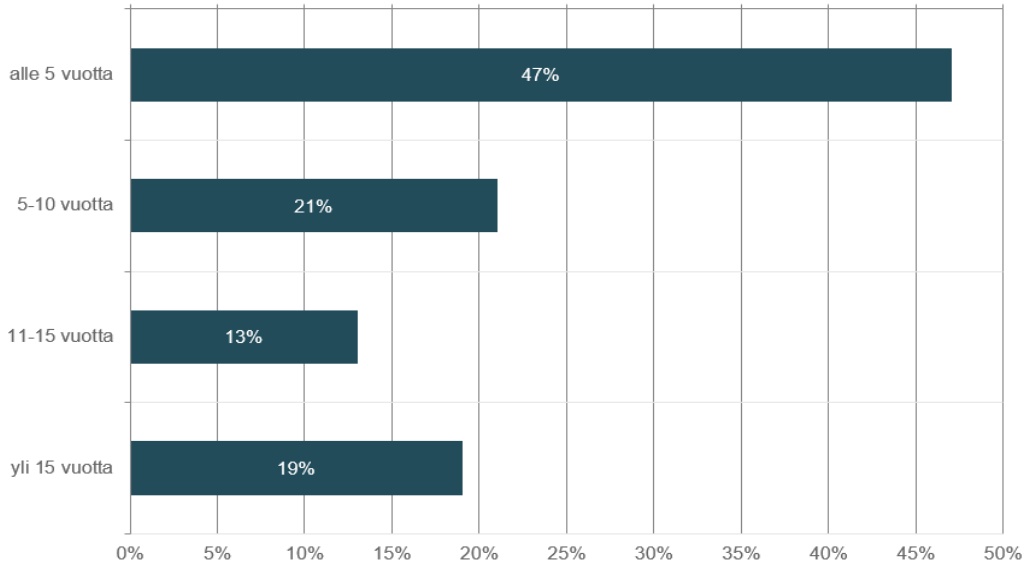
Koko konsortion sisällä isoimman vastaajien ryhmän muodostivat Hyria Koulutus Oy:n palveluksessa olevat (n=204). Hyria säätiön ja Business-palveluiden työntekijät muodostivat pienemmän (n=48) ryhmän vastaajista. Opetus- ja ohjaushenkilöstöä on vastaajien enemmistö (n=140) muun henkilöstön muodostaessa pienemmän (n=112) vastaajaryhmän. Hyrian (2023) henkilöstöraportin mukaan 70 prosenttia henkilöstöstä on opetus- ja ohjaushenkilöstä ja 30 prosenttia työskentelee hallinto- ja tukipalvelujen tehtävissä. Kyselyn kysymysten asettelulla saattaa olla vaikutusta hieman poikkeavaan jakaumaan vastaajien osalta. Vastaajista 91 % (n=229) toimii työntekijän roolissa ilman esihenkilövastuita ja esihenkilön roolissa työskentelee 9 % (n=23) kyselyn vastaajista.

Vastaajista selkeä enemmistö (n=183) työskentelee toistaiseksi voimassa olevassa työsuhteessa (Kuvio 11) täyttä työaikaa tehden. Määräaikaisella työsopimuksella työskentelee hieman vajaa neljännes (n=58) vastaajista. Tätä selittää osittain lainsäädäntö, jonka mukaan ammatillinen oppilaitos ei voi palkata ammatillista opettajaa tai kouluttajaa toistaiseksi voimassa olevaan työsuhteeseen, mikäli henkilö ei ole suorittanut ammatillisen opettajan pätevyyttä. Tästä johtuen vakiintuneena käytäntönä on usein aloittaa työsuhde määräaikaisella työsopimuksella samalla ammatillisen opettajan opintoja suorittaen. Osa-aikaiset toistaiseksi voimassa olevat (n=5) ja osa-aikaiset määräaikaiset (n=4) muodostavat pienen osan vastaajien joukosta. Hyrian henkilöstöraportin mukaan toistaiseksi voimassa olevassa työsuhteessa työskentelee 74 prosenttia henkilöstöstä ja määräaikaisessa 26 prosenttia henkilöstä (Hyria 2022).



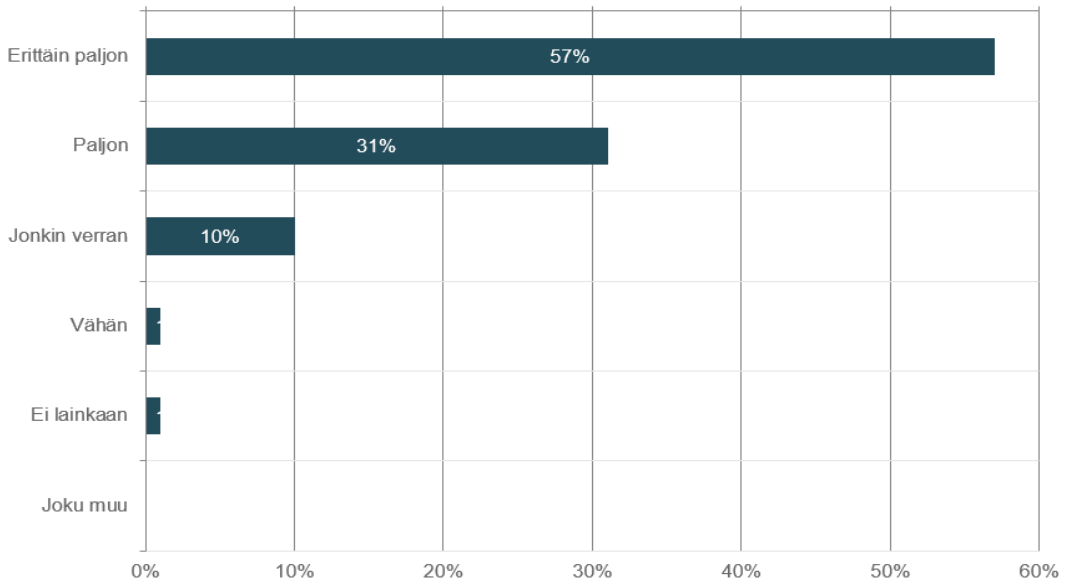
Kuvio 11 Vastaajien (n=252) työsuhdemuoto

Hyriassa kertyneen työkokemuksen (Kuvio 12) osalta suurin vastaajaryhmä oli alle 5 vuotta työsuhteessa olleet, heidän edustaessa lähes puolta (=118) vastaajista. Seuraavaksi suurimpana ryhmänä (n=54) olivat Hyriassa 5–10 vuotta työskennelleet. Lähes yhtä suuren vastaajajoukon (n=48) muodostavat yli 15-vuotta työskennelleet, 11-15 vuotta työskennelleiden edustaessa pienintä (n=32) ryhmää vastaajista. Määräaikaisessa työsuhteessa olevista henkilöistä yli yhdeksän kymmenestä (n=59) oli työskennellyt Hyriassa alle 5 vuotta, 4 henkilöä 5–10 vuotta ja yksi henkilö yli 10 vuotta. Kaikissa kysymyksissä verrattaessa määräaikaisten ja alle 5 vuotta työskennelleiden vastauksia olivat vastaukset hyvin lähellä toisiaan ja mahtuivat yhden tai kahden henkilön vastauksen aiheuttamaan vaihteluun. Tästä johtuen määräaikaisten osalta ei suurempaa painoarvoa annettu työsuhteen muodolle vaan raportoinnissa huomioitiin alle 5 vuotta Hyriaan työsuhteessa olleet (n=118).



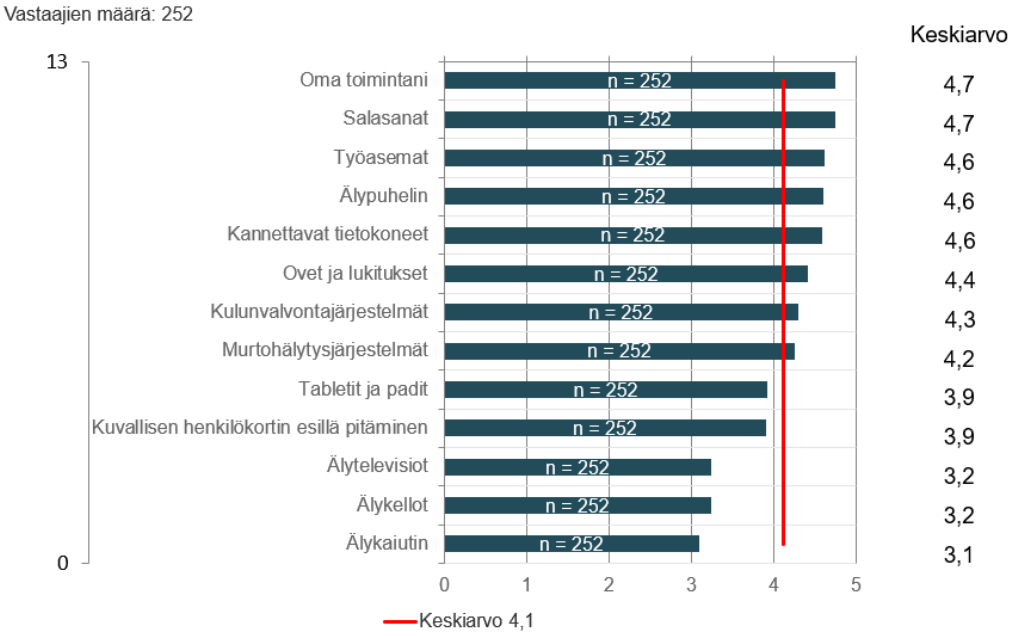
Kuvio 12 Vastaajien (n=252) työkokemus Hyria konsortion palveluksessa

Vastaajat kokivat tietoturvallisuuden tärkeyden lisääntyneen yhteiskunnassa viime aikoina (Kuvio 13) pääsääntöisesti erittäin paljon (n=143) tai paljon (n=78). Jonkin verran tärkeyden koki lisääntyneen (n=25) joka kymmenes vastaaja. Vähän (n=2) tai ei lainkaan (n=3) aiheen tärkeäksi kokeneet olivat hyvin pieni otos. Tulos antaa kuvan henkilöstöstä, joka seuraa aikamme ajankohtaisia aiheita eri medioissa. Kaikki vastaajat kertoivat huomioivansa tietoturvallisuuteen liittyviä asioita omassa elämässään työn ulkopuolella joko usein (n=194) tai joskus (=58). Tämä antaa vaikutelman henkilöstöstä, joka on tietoinen kyberturvallisuudesta ainakin jonkinlaisella tasolla. Taustatiedoilla verratessa esille nousi Hyria säätiön ja Business-palveluiden henkilöstön osalta selvästi matalammat prosentit. Heistä hieman alle puolet totesi tietoturvallisuuden merkityksen lisääntyneen yhteiskunnassa merkittävästi ja hieman yli kaksi viidesosaa totesi sen lisääntyneen paljon.



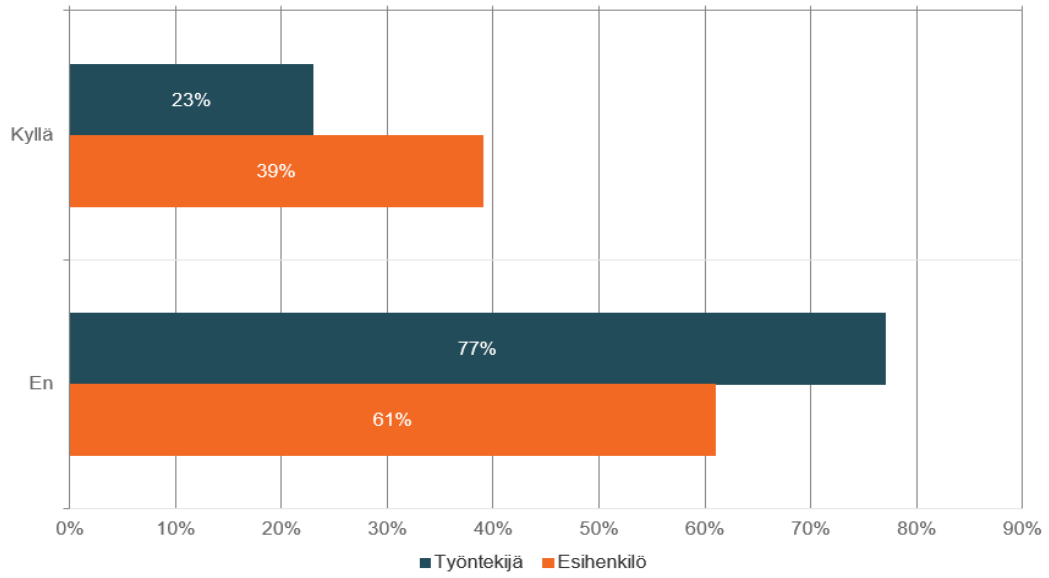
Kuvio 13 Vastaajien (n=252) kokemus tietoturvallisuuden tärkeyden lisääntymisestä

Vastaajilta kysyttiin heidän arvioitaan erilaisten kyberturvallisuuteen liittyvien elementtien merkityksestä tietoturvallisuuden kannalta (Kuvio 14). Pääsääntöisesti kaikki kyselyyn valitut elementit koettiin jollain tasolla tärkeiksi kaikkien vastauksien keskiarvon asettuessa 4,1 tasolle. Arvioissa tärkeimmiksi koettiin oma toiminta ja salasanat (ka=4,7). Heti näiden perässä kannettavat tietokoneet, työasemat ja älypuhelimet (ka=4,6). Tabletteja ja iPadeja ei koettu samalla tavalla tärkeäksi (ka=3,9). Tässä ei mahdollisesti ole tiedostettu kyseisen laitteen toimivan saman kaltaisella periaatteella kuin älypuhelimet. Verkkoon liitettävien laitteiden osalta ei koettu älykelloa (ka=3,2), älytelevisiota (ka=3,2) eikä älykaiutinta (ka=3,1) yhtä tärkeäksi kuin muita laitteita. Ovet ja lukitukset (ka=4,4) sekä kulunvalvontajärjestelmät (ka=4,3) ja murtohälytysjärjestelmät (ka=4,2) koettiin tärkeiksi. Sen sijaan kuvallisen henkilökortin esillä pitämistä ei koettu yhtä tärkeäksi (ka=3,9). Tässä kohtaa vastaajat eivät mahdollisesti ole tunnistaneet tiloissa kulkemisen ja tunnistautumisen merkitystä osana tietoturvallisuutta tukevaa toimintakulttuuria. Tämän kysymyksen osalta vertailussa korrelaatiota oli siten, että henkilöt, jotka pitivät ovia ja lukituksia tietoturvallisuuden kannalta tärkeinä kokivat samoin myös murtohälytysjärjestelmien (R=0,47) ja kulunvalvontajärjestelmien osalta (R=0,46). Nämä osa-alueet kulkevat käsi kädessä pohdittaessa tiloissa tapahtuvaa luvallista ja luvatonta liikkumista, joten samat henkilöt ovat selvästi mieltäneet nämä toimitilaturvallisuuden elementit osaksi tietoturvallisuutta. Mielenkiintoinen havainto oli kulkukorttien ja kulunvalvontajärjestelmien välinen positiivinen korrelaatio (R=0,49) joka ei kuitenkaan vaikuttanut ovet ja lukitukset ja murtohälytysjärjestelmät vastausvaihtoehtojen osalta vastaavalla tavalla.



Kuvio 14 Kyberturvallisuuteen liittyvien elementtien merkityksen kokemus vastaajien keskuudessa (n=252)

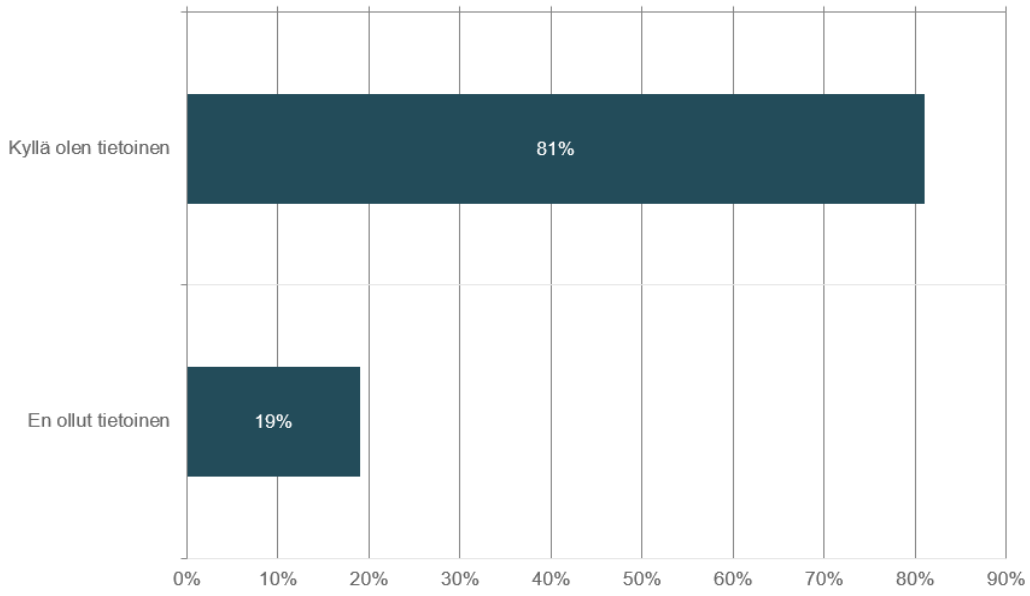
Älypuhelimen tietoturvallisuuden tärkeyden olivat monet ymmärtäneet aikaisemman kysymyksen perusteella ja vastaajista kolmen neljäsosan (n=191) enemmistö kertoi, ettei esimerkiksi talleta älypuhelimen yhteystietoihin salasanoja, pin-koodeja, tunnuslukuja tai muita vastaavia tietoja. Toisaalta vastaajista noin neljännes (n=61) kertoi näin tekevänsä. Vertailtaessa vastauksia (Kuvio 15) esihenkilöiden ja työntekijöiden välillä havaitaan tämän toimintamallin olevan suhteellisesti tarkasteltuna huomattavasti yleisempää esihenkilöiden keskuudessa. Lähes kaksi viidennestä (n=9) esihenkilöistä vastasi toimivansa näin. Määrällisesti kuitenkin työntekijöiden määrä on suurempi (n=52). Jatkotutkimuksen aiheena voisi tutkia mistä tämä johtuu. Koulutuksen ja perehdytyksen kohdistaminen esihenkilöihin ei välttämättä ole huono investointi, kun vielä huomioimme heillä olevan työntekijöitä laajemmat pääsyoikeudet järjestelmiin sekä tietoturvallisuuden ja -suojan kannalta tärkeisiin tietoihin. Lisäksi esihenkilöiden koulutukseen panostamalla on mahdollista siirtää kyberturvallisuudenkin kannalta parempia toimintamalleja organisaatiossa eteenpäin.



Kuvio 15 Älypuhelimeen tallennetut salasanat, pin-koodit ja tunnusluvut verratuna aseman mukaan (n=252)

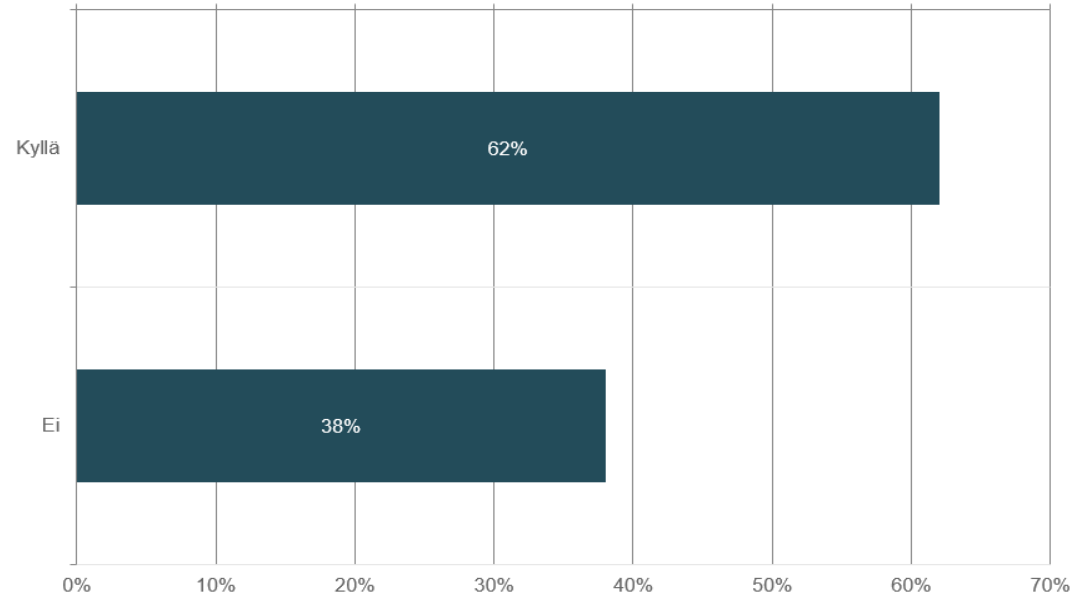
Älypuhelimet ja mobiililaitteet koettiin tietoturvallisuuden kannalta tärkeiksi. Siitä huolimatta oli havaittavissa toimintatapa, joka saattaa vaarantaa salasanakäytännöt (Kuvio 15). Noin viidennes (n=48) vastaajista ei ollut tietoinen (Kuvio 16) vaarantavansa salasanojensa ja koodiensa tietoturvan jakaessaan applikaatioille pääsyn näihin. Hyria säätiön ja Business-palveluiden henkilöstöstä suuremmalla osalle asia tuli uutena tietona. Heistä hieman yli kahden kolmanneksen (n=34) vastatessa tienneensä tämän etukäteen ja hieman alle kolmannekselle (n=14) tämän tullessa uutena tietona. Kun ottaa huomioon applikaatioiden kysyvän erikseen pääsyä yhteystietoihin on mahdollista, että kaikki vastaajat eivät ole pysähtyneet pohtimaan mihin tietoon sovellus oikeasti pääsyn haluaa. Osa vastaajista selvästi oli kuitenkin asiaa pohtinut.

> On jo pidemmän aikaa mietityttänyt Hyrian linja esim. tiktok, facebook, ja instagram sovelluksiin työpuhelimessa. Toivoisin yleistä linjausta näihin asioihin. (Kyselyyn vastaaja)



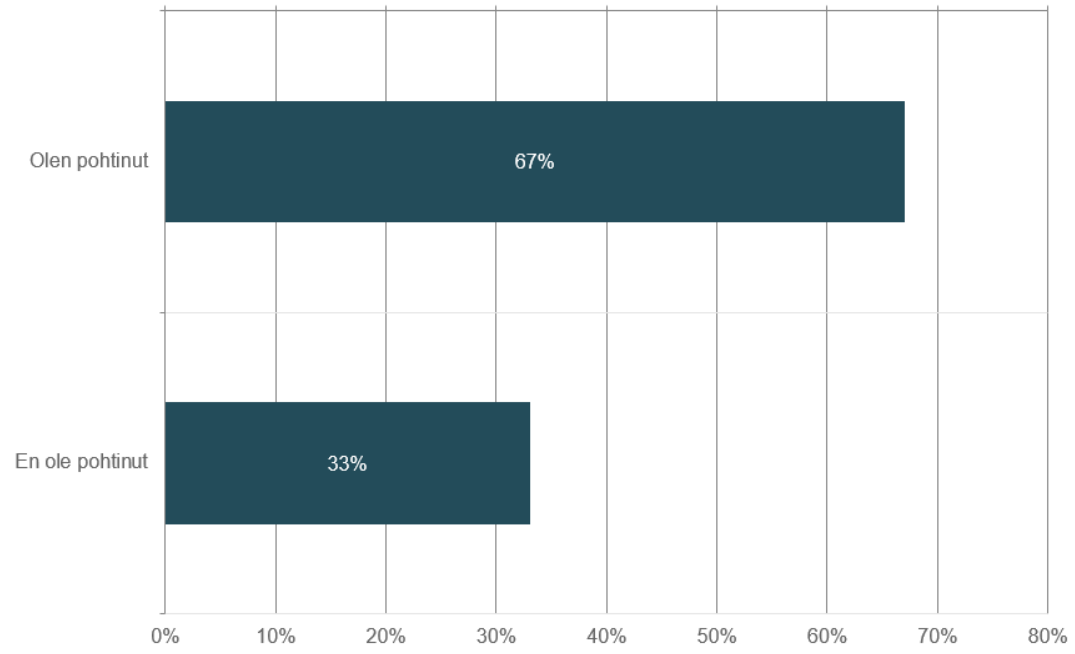
Kuvio 16 Olen tietoinen, että antaessani applikaatiolle pääsyn yhteystietoihini tulen antaneeksi pääsyn kaikkiin yhteystietoihin tallennettuihin tietoihin (n=252)

Omaa henkilökohtaista kyberturvallisuutta mobiililaitteiden osalta oli nähnyt tarpeelliseksi parantaa jonkinlaisella tietoturvaohjelmistolla, kuten virusturva tai vpn, enemmistö (n=157) vastaajista (Kuvio 17). Hyvin merkittävä osa (n=95) vastaajista ei ole tietoturvaohjelmistoja omiin mobiililaitteisiinsa hankkinut. Pankki- ja muita palveluita, kuten sähköpostia, ihmiset nykyään käyttävät hyvin paljon, joten mobiililaitteiden haavoittuvuudet saattavat olla merkityksellisiä esimerkiksi sosiaalisen median kautta saadun haittaohjelman sisältävän viestin saajalle. Monet nykyaikaiset haittaohjelman torjuntaan käytetyt palvelut tunnistavat haitalliset applikaatiot, liitteet ja toiminnot myös mobiililaitteessa. Mobiililaitteet kuitenkin ovat, sovellukset eristävän toimintaperiaatteensa ansiosta, lähtökohtaisesti tietokoneita turvallisempia käyttää.



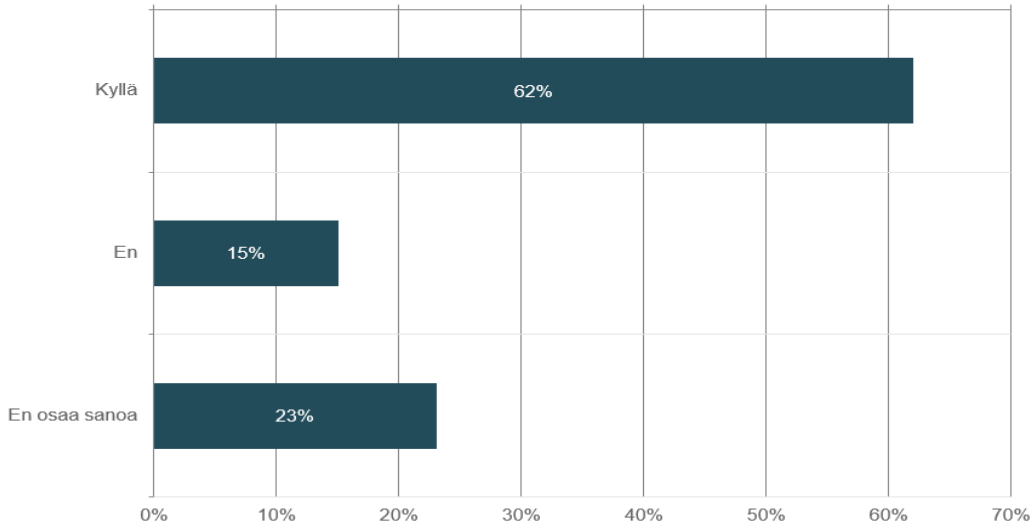
Kuvio 17 Henkilökohtaisessa mobiililaitteessa jonkinlainen tietoturvaohjelmisto (n=252)

Kodeissaan käytössä olevien langattomien tietoverkkojen tietoturvaa kertoi pohtineensa kaksi kolmasosaa (n=168) vastaajista (Kuvio 18). Merkille pantavaa on kuinka iso osa (n=84) vastaajista ei ole tällaista asiaa pohtinut. Nykyisen hybridityömallin aikana hyvin suuri osa henkilöstöstä tekee töitä kotona kotiverkkoon liittyneenä. Tällöin kyseisen verkon tietoturvan tasolla on merkitystä työnantajankin kannalta.



Kuvio 18 Olen pohtinut kotini langattoman verkon tietoturvaa (n=252)

Mikäli työnantajan kautta saisi alennettuun hintaan haittaohjelmien torjuntaan ja verkkoyhteyden suojaamiseen soveltuvan ohjelmiston henkilöstöstä enemmistö (n=155) olisi valmis sellaisen hankkimaan (Kuvio 19). Vastaajista 39 ei ole halukas näin tekemään ja hieman yllättäen vastaajista 58 ei osaa sanoa kuinka toimisi tällaisen mahdollisuuden kohdalla. Tässä on yksi mahdollisuus työnantajan vaikuttaa etätyön mukanaan tuomiin tietoturvallisuushaasteisiin työntekijöiden kotiverkkojen ja -laitteiden tietoturvaa parantamalla. Esimerkiksi varmistamalla, että laitteet, joiden kautta saatetaan kirjautua työsähköpostiin (joka siis ohjeistuksen mukaan kielletty) tai joilla esimerkiksi tehdään opetusmateriaalia, ovat mahdollisimman hyvin suojattuja.



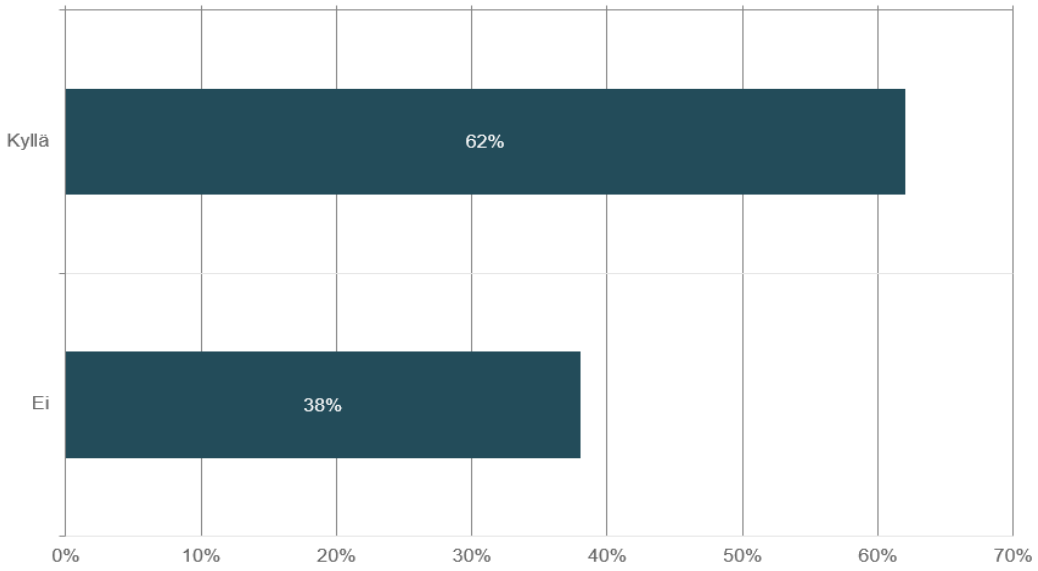
Kuvio 19 Halukkuus hankkia tietoturvaohjelmisto alennettuun hintaan (n=252)

Vastausten perusteella lähes puolet (n=116) henkilöstöstä on käyttänyt jotain internetissä tarjolla olevaa ilmaista käännöspalvelua tai ChatGPT tyyppistä tekoälypalvelua. Tästä ryhmästä noin kolmannes (n=39) ei ole huomioinut tietoturvaa näin tehdessään. Vaikka tämä joukko edustaa vain noin 15,5 prosenttia vastaajien kokonaismäärästä on huomion arvioista todeta, että todellinen luku organisaation tasolla voi olla suurempi sillä jatkokysymys kohdistettiin vain henkilöille, jotka kertoivat käyttäneensä kyseisiä palveluita aikaisemmin. Tietosuojan osalta tässä on yksi mahdollinen kehittämisen ja ohjeistuksen parantamisen mahdollisuus. Ainakin mikäli vastaavia palveluita käytetään sellaisen tiedon toiselle kielelle kääntämiseen, joka pitää sisällään salassa pidettäviä tietoja. Tämä kysely ei kuitenkaan vastaa minkälaisen tiedon kääntämiseen kyseisiä palveluita on käytetty.

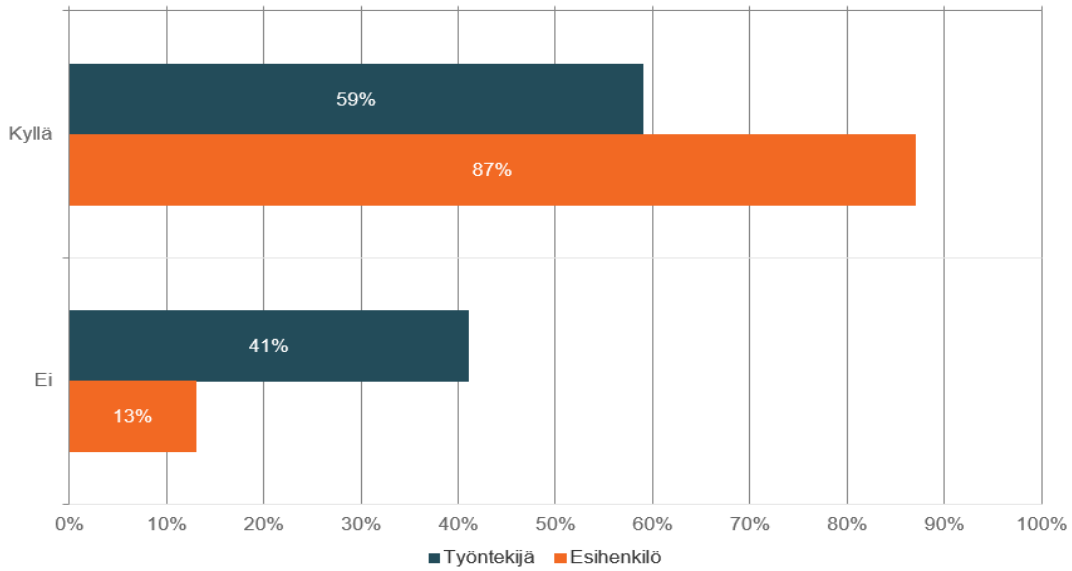
Hieman yli kolme neljäsosaa (n=194) vastaajista (n=252) kertoi huomioivansa usein tietoturvallisuuteen liittyviä asioita työnsä ulkopuolella. Samat henkilöt kokivat myös pohtineensa oman kotiverkkonsa tietoturvaa sekä sitä käyttävien muiden henkilöiden ja laitteiden vaikutusta verkkonsa tietoturvalle. Hieman alle neljännes vastaajista (n=58) kertoi huomioivansa

tietoturvallisuuteen liittyviä asioita työn ulkopuolella joskus. Yksikään vastaaja ei vastannut, ettei olisi koskaan huomioinut tietoturvaa työnsä ulkopuolella.

Samaa salasanaa useammassa kuin yhdessä verkkopalvelussa tai sovelluksessa (Kuvio 20) kertoi käyttävänsä enemmistö vastaajista (n=156). Tämä oli suhteellisesti yleisempää (Kuvio 21) esihenkilöiden (n=20 vs. n=3) kuin työntekijöiden (n=136 vs. n=93) keskuudessa. Saman salasanan käyttäminen useammassa palvelussa oli hieman yleisempää Hyria säätiön ja Business-palveluiden henkilöstön kuin Hyria Koulutus Oy:n henkilöstön keskuudessa. Vaikka yleisellä tasolla tätä käytäntöä voidaan pitää tietoturvallisuuden kannalta riskiä lisäävän, ei kyselyn avulla kuitenkaan selvitetty minkälaisissa sovelluksissa tai verkkosivuilla henkilöstöllä on ollut tapana käyttää samaa salasanaa. Jatkotutkiminen on tarpeellista, mikäli halutaan selvittää, onko ilmiö jalkautunut kaikenlaisten palveluiden pariin vai onko kyseinen käytäntö käytössä vain lievempää tietoturvaa vaativien palveluiden kirjautumisessa. Tämän kysymyksen kohdalla on mahdollista pieni sekaannus myös työnantajan tarjoamien Office 365 ja muiden palveluiden yhtenäisestä kirjautumisesta johtuen.



Kuvio 20 Kertoi käyttävänsä samaa salasanaa useammassa kuin yhdessä palvelussa (n=252)



Kuvio 21 Sama salasana useammassa palvelussa, työntekijä esihenkilö vertailu (n=252)

Haastatteluissa tuli ilmi, että salasanojen kohdalla on tapahtunut asenteessa muutosta vaikkakin salasanojen keksiminen useampiin palveluihin koettiin työlääksi kuten haastateltava kuvaa alla:

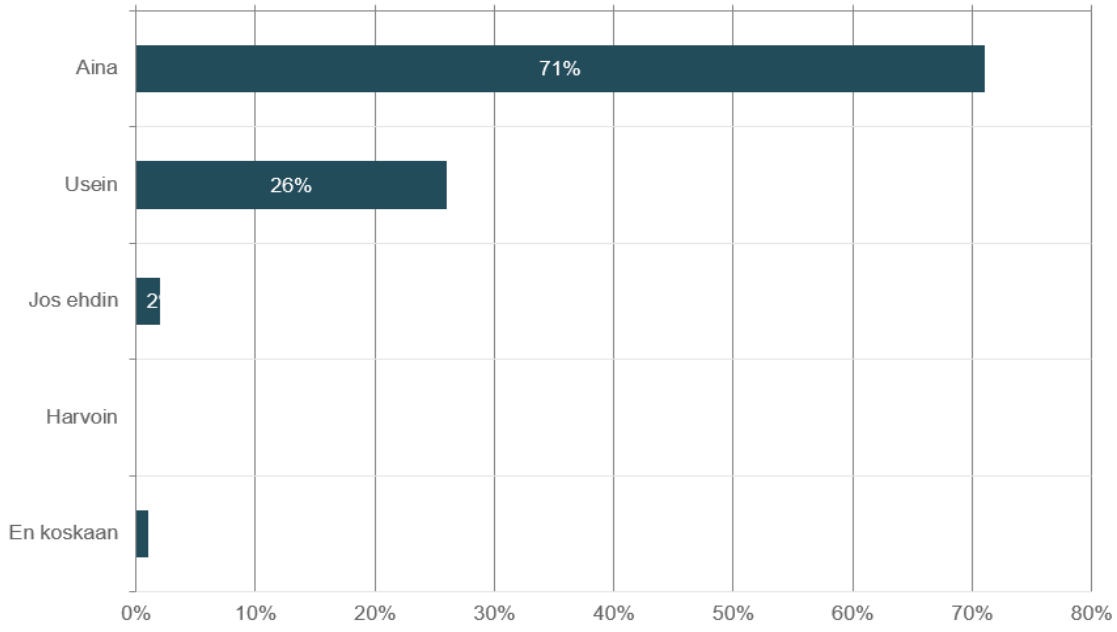
> Niiden keksiminen on vähän tuskallista välillä ja ja mäkin niinku saatan käyttää samaa. Mä muutan ehkä yhtä merkkiä siellä. Ja toki kirjoitankin isolla jonkun tai jotain tämmöistä näin, että en nyt ihan tällä hetkellä. Jossain vaiheessa mulla oli sama salasana useammassakin paikassa, mutta oon nyt sitten vaihtanut ne. (Haastateltava 5)

Lisäksi tuli ilmi, että haastateltavat käyttivät samaa salasanaa sellaisissa palveluissa, joiden eivät kokeneet olevan niin kriittisiä tietoturvan kannalta.

> Toki itsekin samoja salasanoja käytän jossain tällaisessa ns. huviluonteisessa palveluissa missä se käyttö ei ole ehkä niin vakavaa ja sille on sitten omat sähköpostinsa luotuna sitä varten ja niin edespäin. Mutta sitten taas tällaisessa työkäytössä niin pyrkimys kyllä on mahdollisimman paljon niin kun käyttää sellaisia salasanoja, jotka nyt ainakaan ei ihan liian lähellä toisiansa ole. (Haastateltava 1)

Saadessaan linkkejä sisältäviä viestejä mihin tahansa sovellukseen tai palveluun (Kuvio 22) lähes kaikki vastaajista pyrkivät varmistumaan viestin lähettäjän oikeellisuudesta joko aina (n=178) tai usein (n=66). Hyvin harva vastasi pyrkivänsä tähän vain silloin kun ehtii (n=6) tai ei lainkaan (n=2). Tässä tietoisuudessa varmasti vaikutti yleisesti mediassa käyty keskustelu

linkkien haitallisuudesta sekä Hyriassa sisäisen tiedottamisen kautta tulleista viesteistä, joissa on varoitettu haitallisia linkkejä sisältävistä sähköposteista.



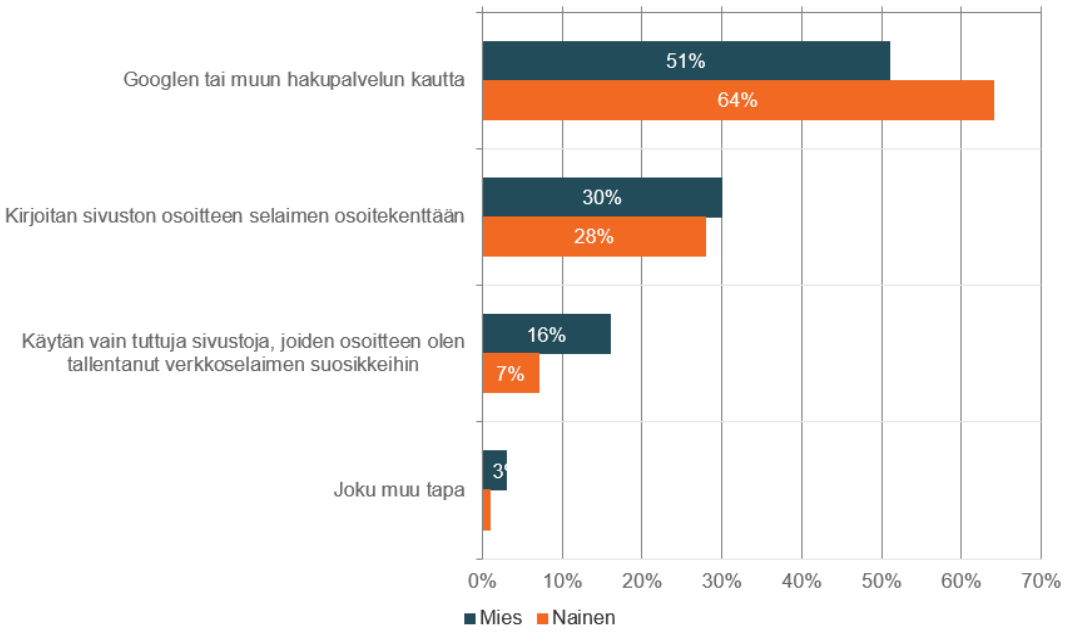
Kuvio 22 Pyrin varmistumaan linkin lähettäjän oikeellisuudesta (n=252)

Internetissä verkkosivustolle pääsääntöisesti Googlen tai vastaavan hakukoneen kautta koko vastaajajoukosta (n=252) kertoi hakeutuvansa lähes kolme viidennestä (n=149). Osoitteen selaimen osoitekenttään vastasi kirjoittavansa alle kolmannes (n=74) ja tallennetun osoitteen kautta sivustoille kertoi suunnistavansa kymmenesosa (n=26) vastaajista. Joku muu kohtaan yksi vastaaja oli vastannut käyttävänsä Googlea normaalisti, mutta tunnistautumista edellyttäviin palveluihin hän kertoi siirtyvänsä kirjoittamalla verkkosivun osoitteen osoite kenttään sekä varmistavansa vielä lukon kuvasta olevansa turvallisessa sivustolla.

Hieman yllättäen sivustolle hakeutumisessa oli havaittavissa sukupuolikohtainen (Kuvio 23) ero, joka ei haastatteluiden avulla ollut selitettävissä. Kuitenkin työtehtävien sukupuolija-kauma organisaatiossa saattaa vaikuttaa tähän tulokseen. Organisaatiossa vähemmän aikaa työskennelleet ja nuorin ikäryhmä olivat myös taipuvaisempia navigoimaan verkkosivuille Googlen tai vastaavan hakukoneen kautta. Haastatteluissa vastaajat johdonmukaisesti vastasi-vat menevänsä esimerkiksi pankkien sivuille kirjoittamalla osoitteen tai kirjanmerkin kautta, mutta muuten kertoivat käyttävänsä Googlen hakukonetta.

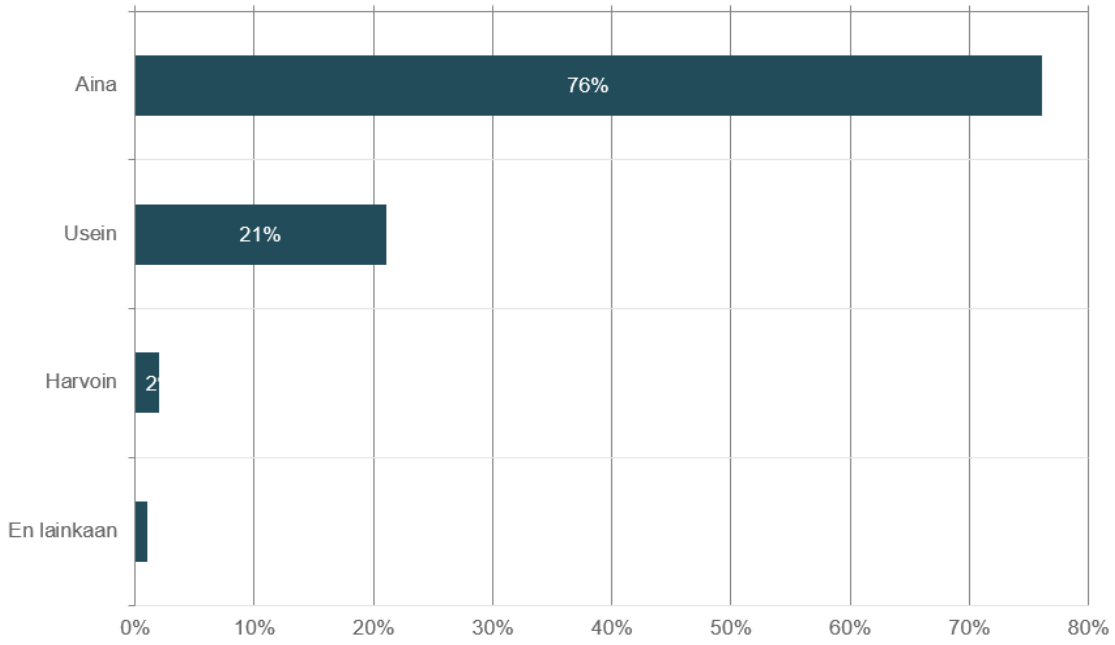
Pankkisivuille en mene koskaan Googlen kautta. (Haastateltava 4)

Tosiaan niin en mene hakukoneen kautta, että sitten niinku kirjoitan sen osoitteen kokonaisuudessaan. (Haastateltava 2)



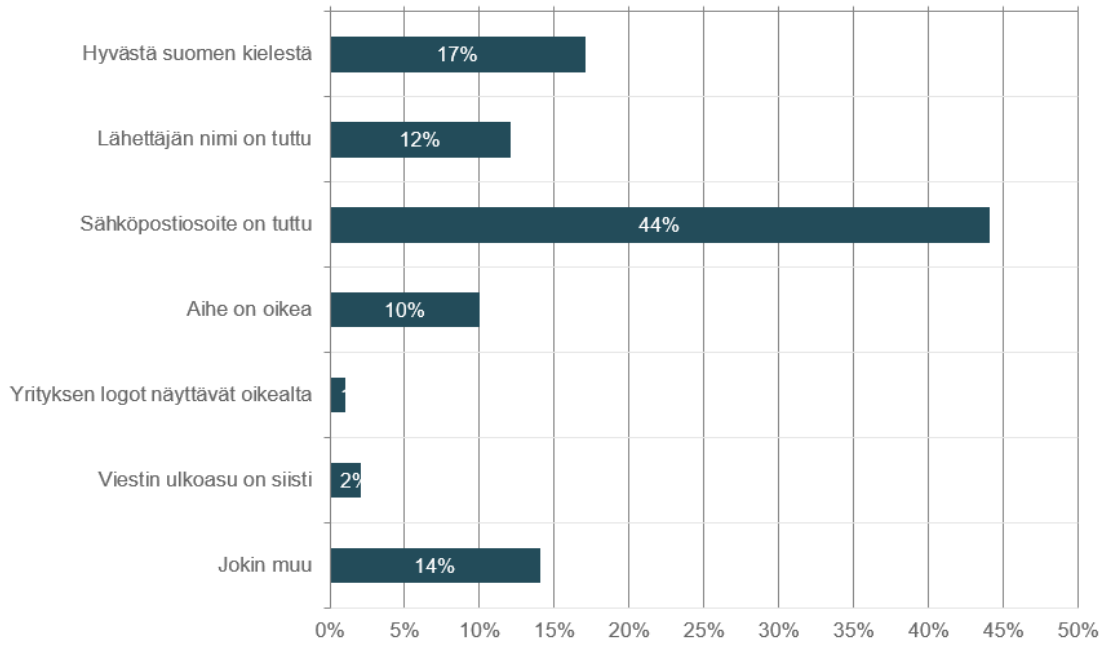
Kuvio 23 Kuinka hakeutuu internetin sivustoille (n=244)

Saadessaan liitetiedostoja sähköpostiin tai muuhun palveluun (mukaan lukien sosiaalisen median palvelut), lähettäjän oikeellisuuden pyrkii aina varmistamaan (Kuvio 24) suurin osa (n=193) henkilöstöstä. Usein oikeellisuuden pyrkii varmistamaan noin viidennes (n=52) ja harvoin (n=5) tai ei lainkaan (n=2) muodostavat hyvin pienen osan vastaajista. Luotettavalta lähettäjältä saatua linkkiä tai liitetiedostoa ei myöskään pidetä turvallisena (n=228). Sen sijaan moni (n=15) ei osannut vastata kysymykseen sekä jokunen (n=9) vastaaja oli sitä mieltä, että luotettavan henkilön lähettämä viestin liitetiedosto tai viestissä oleva linkki olisi luotettava.



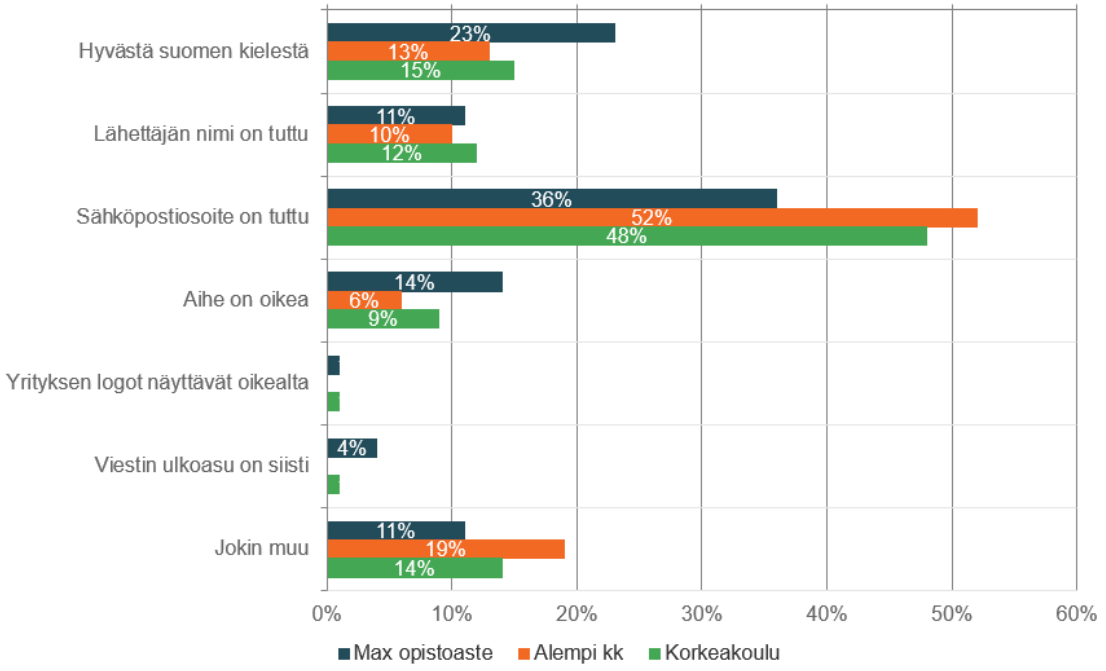
Kuvio 24 Pyrkii varmistamaan liitetiedoston tai linkin lähettäjän luotettavuuden (n=252)

Kysyttäessä mistä henkilö voisi tunnistaa sähköpostin olevan luotettava jakautuivat vastaukset useamman vaihtoehdon kesken (Kuvio 25). Tässä kysymyksessä oli mahdollista valita vain mielestään paras vaihtoehto tai vastata avoimeen kohtaan. Vastaajista suurin ryhmä (n=112) piti tuttua sähköpostiosoitetta luotettavan sähköpostin tunnistamiseen parhaana tapana. Toiseksi suurin vastaajien ryhmä (n=43) piti parhaana tapana tunnistaa viestissä käytettyä hyvää suomen kieltä. Kolmanneksi suurin ryhmä (n=36) oli vastannut avoimeen kohtaan. Lähes kaikki avoimet vastaukset pitivät sisällään toteamuksen, ettei mistään yllä olevista voi päätellä täysin varmasti ja suurin osa vastasi, että kaikki tai monet yllä olevista yhdessä sekä odotettu sähköposti voisivat yhdessä antaa suuntaa viestin luotettavuudesta. Neljänneksi (n=30) suurin vastaajaryhmä piti parhaimpana luotettavuuden osoittajana tuttua lähettäjän nimeä ja viides (n=25) ryhmä oikeaa aihetta. Yrityksen logoa (n=2) ja viestin ulkoasua (n=4) piti parhaimpana vain muutama vastaaja.



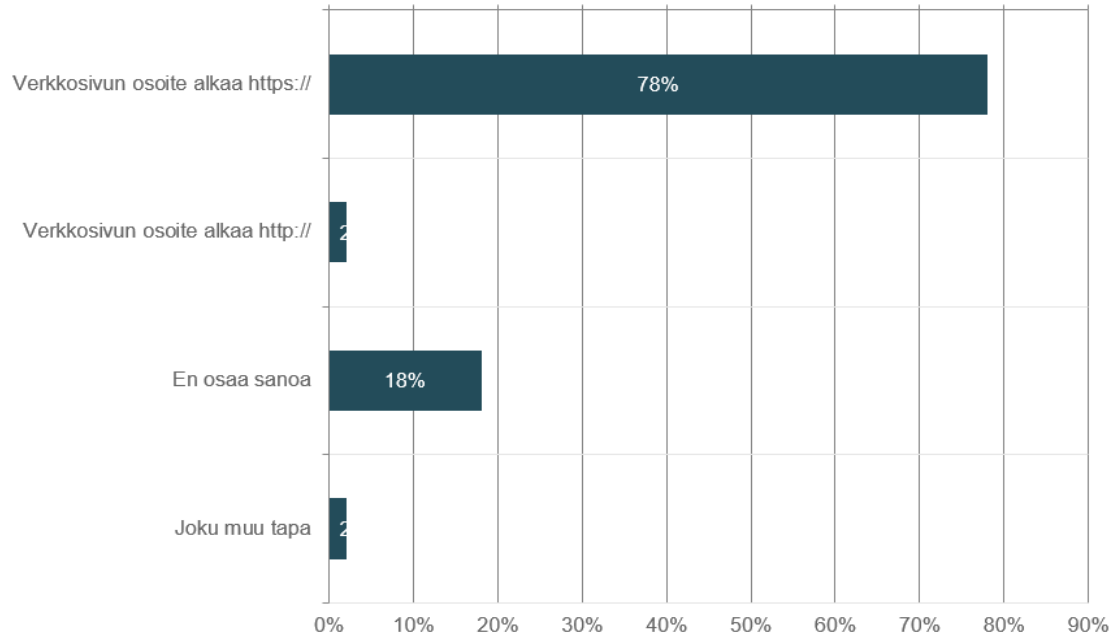
Kuvio 25 Mistä tunnistaa luotettavan sähköpostin (valitse paras vaihtoehto) (n=252)

Kysymyksen kohdalla koulutustaustalla (Kuvio 26) tuntui olevan merkitystä, sillä alimman koulutustausta ryhmästä jopa 23 prosenttia totesi tunnistavansa luotettavan sähköpostin parhaiten hyvästä suomen kielestä. Kyseinen vastaajaryhmä erottautui hieman muidenkin vaihtoehtojen kohdalla.



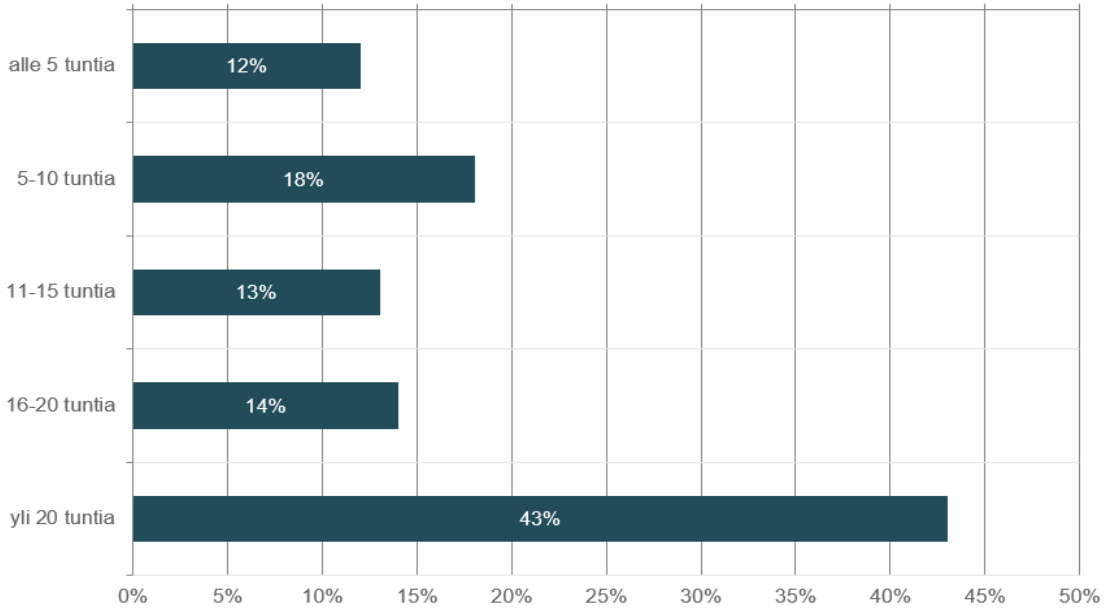
Kuvio 26 Sähköpostin luotettavuuden tunnistaminen koulutustaustan mukaan (n=252)

Suojatun verkkosivun osoitteen (Kuvio 27) tunnistaa noin kolme neljännestä (n=198) vastaajista. Kysymykseen ei osannut vastata melkein viidennes (n=45) vastaajista, mitä voidaan pitää kohtalaisen suurena osuutena kokonaismäärästä. Neljä (n=4) vastaajaa vastasi suojatun verkkosivun osoitteen alkavan http:// ja viisi (n=5) vastaajaa vastasi avoimeen kenttään. Avoimeen kenttään vastanneista yksi vastaaja oli vastannut, ettei tiedä ja neljä vastaajaa vastasi, että suojatun verkkosivun tunnistaa tarkastamalla varmennetiedot tai osoitekentän vieressä olevasta lukon kuvasta.



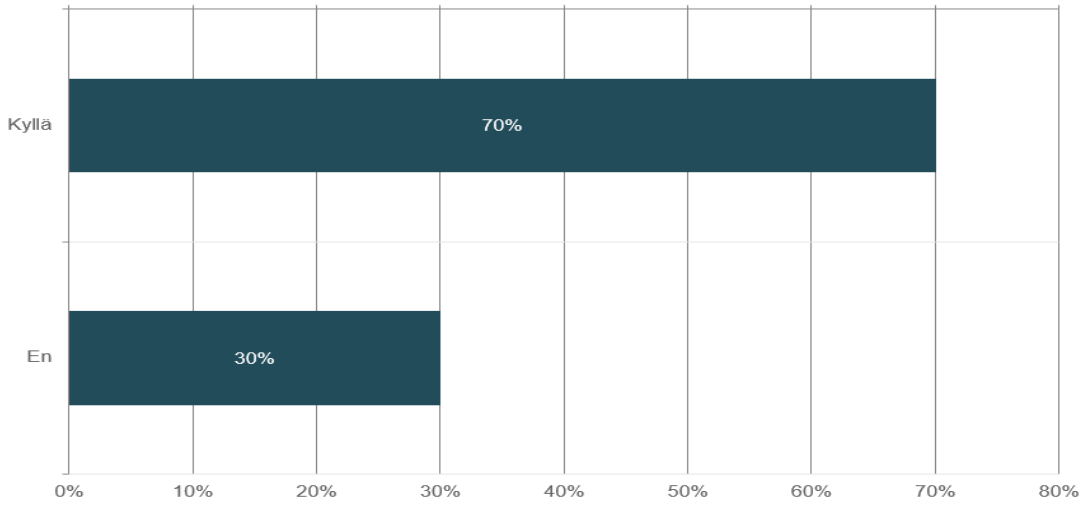
Kuvio 27 Miten tunnistaa suojatun verkkosivun osoitteen (n=252)

Yli 20 tuntia tietoteknisiä järjestelmiä työviikon aikana käyttävät henkilöt (Kuvio 28) muodostivat suurimman (n=108) ryhmän vastaajista. Toiseksi suurimman (n=47) ryhmän muodostivat 5–10 tuntia työviikon aikana tietoteknisiä järjestelmiä käyttävät henkilöt. Kolmanneksi suurin (n=35) vastaajaryhmä oli 16–20 tuntia työviikon aikana käyttävät ja neljänneksi suurimpana (n=32) ryhmänä 11–15 tuntia käyttäjät sekä pienimpänä (n=30) ryhmänä alle 5 tuntia työviikon aikana tietoteknisiä järjestelmiä käyttävät vastaajat. Kun tätä kysymystä tarkastellaan suodatettuna eri taustatekijöillä, on esihenkilöistä yli 20 tuntia viikossa tietoteknisiä järjestelmiä käyttäviä noin 70 prosenttia (n=16). Tämä saattaa olla huomion arvoista, kun vertaa aikaisempiin kysymyksiin, joiden kohdalla esihenkilöiden osalta oli hieman parannettavaa toimintatavoissa.



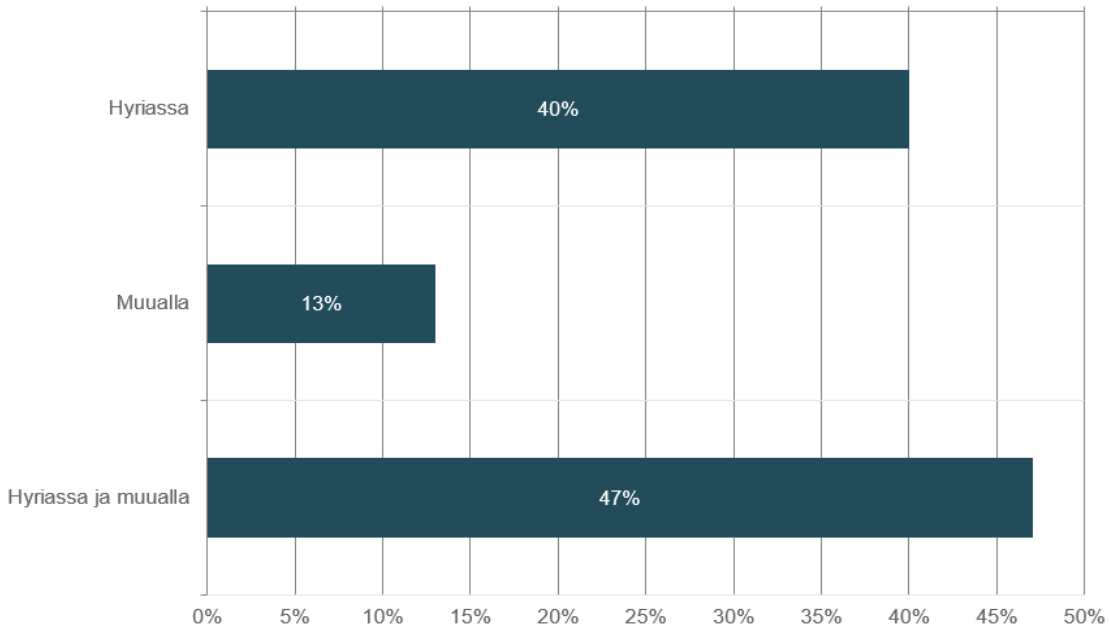
Kuvio 28 Tietoteknisten järjestelmien käyttö työviikon aikana (pl. opetustilanteet) (n=252)

Tietojärjestelmien ja -laitteiden tietoturvalliseen käyttöön liittyvää koulutusta (Kuvio 29) kertoi saaneensa (n=176) enemmistö vastaajista. Hieman vajaa kolmannes (n=76) koko vastaajajoukosta (n=252) ei ole saanut aikaisemmin kyseistä koulutusta. Lähes kolmanneksen osuus henkilöstöstä ei ole saanut koulutusta, joka on kohtalaisen suuri luku. Varsinkin kun otetaan huomioon tietoteknisten järjestelmien ja -laitteiden jo pitkään jatkunut käyttö osana lähes kaikkia työtehtäviä. Tämän luvun pitäisi olla lähellä nollaa henkilöä, mikäli organisaatioiden tietoturvallisuus ja perehdytys on hoidettu tietoturvallisuuden hyvien käytänteiden mukaisesti.



Kuvio 29 Saanut koulutusta tietojärjestelmien ja -laitteiden tietoturvalliseen käyttöön (n=252)

Tietojärjestelmien tietoturvalliseen käyttöön koulutusta saaneiden (Kuvio 30) osalta (n=176) lähes yhdeksän kymmenestä (n=153) oli saanut kyseistä koulutusta Hyriassa. Tästä vastaajajoukosta melkein puolet (n=82) vastasi saaneensa Hyriassa ja muualla koulusta. Hieman yli kymmenesosa (n=23) on saanut koulutusta jossain muualla kuin Hyriassa. Koulutusta saaneiden osalta Hyria on onnistunut tavoittamaan koulutuksella henkilöstöään hyvin. Mikäli laskemme mukaan vastaajat, jotka eivät ole saaneet (n=76) koulutusta on vastaajista kaksi viidesosaa (n=99) henkilöitä, jotka eivät ole lainkaan saaneet koulutusta tietojärjestelmien ja -laitteistojen tietoturvalliseen käyttöön. Luku on merkittävä.



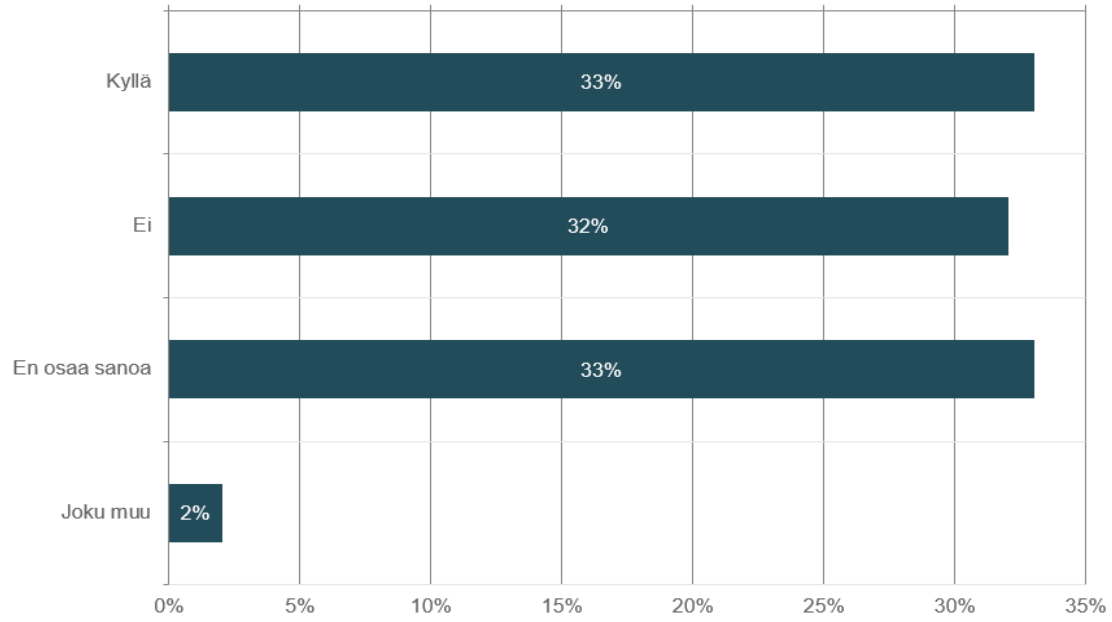
Kuvio 30 Missä saanut koulutusta tietojärjestelmien tietoturvalliseen käyttöön (n=176)

Kun koko vastaajajoukolta (n=252) kysyttiin kokemusta Hyrian perehdytyksen riittävyydestä tietojärjestelmien, työasemien ja älypuhelimien tietoturvalliseen käyttöön (Kuvio 31), totesi noin kolmannes (n=83) sen olleen riittävästi huomioitu. Lähes samansuuruisen vastaajajoukon muodostivat vastaajat, joiden mielestä perehdytyksessä ei ollut riittävästi huomioitu (n=81) ja vastaajat, jotka eivät osanneet sanoa (n=82) oliko riittävästi huomioitu. Kuusi vastaajaa vastasi kohtaan joku muu, Nämä vastaukset pitivät sisällään vastausvaihtoehtojen kaltaiset vastaukset ja kaksi vastaajaa totesi myös tarpeelliseksi jatkuvan osaamisen päivittämisen.

> Perehdytystä on ollut, mutta mielestäni asioista pitäisi muistuttaa useammin koko henkilöstöä. (Vastaaja 1)

> Voisi olla säännöllisin väliajoin päivitys. (Vastaaja 4)

> Olisi hyvä päivittää henkilökunnan taitoja käyttää laitteita ja tietojärjestelmiä turvallisesti ja oikein (Vastaaja 5)



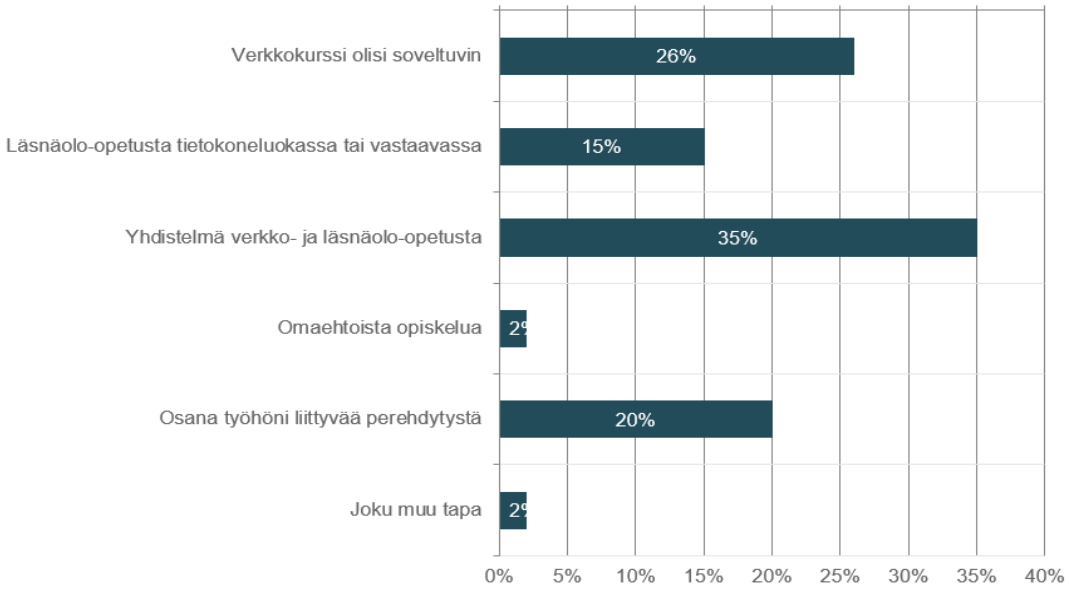
Kuvio 31 Onko Hyrian perehdytyksessä huomioitu riittävästi tietojärjestelmien, työasemien ja älypuhelimien tietoturvallinen käyttö (n=252)

Toimiakseen työtehtävissään tietoturvallisesti vastaajista (n=252) neljä viidesosaa (n=204) koki tietojensa ja taitojensa olevan riittävällä tasolla. Viidennes (n=48) ei näin kokenut. Aiheeseen liittyvää koulutusta tästä vastaajajoukosta koki kaipaavansa lähes kaikki (n=46) vastaajat. Tältä joukolta (Kuvio 32) kysyttiin mieluisinta koulutustapaa aiheeseen liittyen. Vastaajista suurin (n=16) ryhmä halusi yhdistelmän verkko- ja läsnäolo-opetusta, toiseksi suurimmalle ryhmälle mieluisen koulutustapa (n=12) olisi verkkokurssi, viidenneksen (n=9) mielestä heille mieluisin tapa olisi liittää koulutus osaksi perehdytystä. Pienin (n=7) ryhmä tästä joukosta koki läsnäolo-opetuksen mieluisimpana koulutuksen toteuttamistapana. Tuloksia tarkastellessa heräsi epäilys kyselyn rakenteen heikkoudesta sillä koulutuksen tarpeeseen ja koulutusmuotoon vastausta kysyttiin vain vastaajilta, jotka eivät kokeneet osaamisensa riittävän. Tästä johtuen aihe oli yksi teemahaastattelun teemoista. Näiden tulosten perusteella voisi olla syytä olettaa koulutuksen tarpeen ja halukkuuden koulutukseen olevan hieman kyselyn antamaa tulosta suurempi. Haastatelluista kaikki kokivat osaamisensa riittäväksi suoriutuakseen tietoturvallisesti työtehtävistään. Siitä huolimatta he kaikki kokivat tarvetta koulutukselle.

> Tietoturvallisuuteen liittyvät seikat kehittyvät ja muuttuu koko ajan niin tota sillä ehkä ajatellaankin sitten, että myös sitä perehdytystä ja koulutustakin

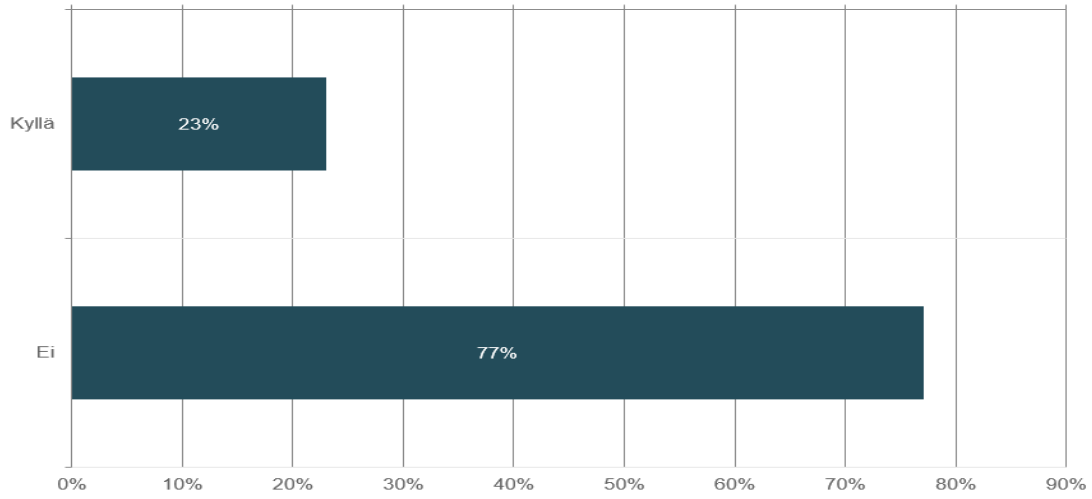
siihen kuitenkin tarvitaan, vaikka tilanne tällä hetkellä olisikin ihan OK. (Haastateltava 1)

Niin, ei niitä ehkä tule sitten omatoimisesti niitä tietoja päivitettyä. Voisi olla ihan hyvä, että vaikka kerran kahdessa vuodessa olisi joku tämmöinen päivän kurssi, mikä olisi kaikille pakollinen. Asiat muuttuvat eli niitä on hyvä muistutella. (Haastateltava 4)



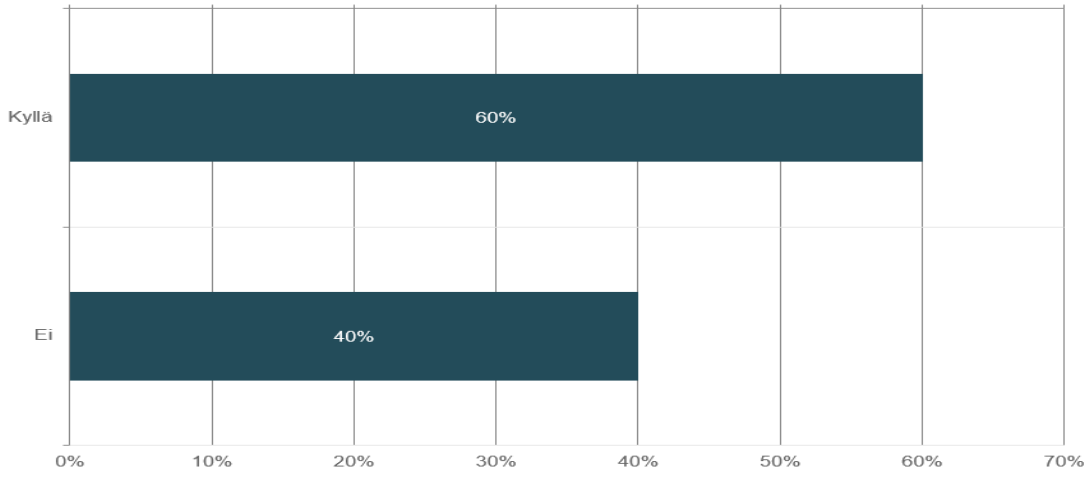
Kuvio 32 Osaamisensa riittämättömäksi kokeneille (n=48) mieluisin koulutustapa

Työskennellessään etänä kotitoimistolla (Kuvio 33), noin neljäsosalla (n=58) vastaajista työasemansa kanssa samassa tietoverkossa on yhdistettynä laite tai laitteita, joiden tietoturvasta tai ohjelmistojen päivityksen ajantasaisuudesta he eivät ole varmoja. Kolme neljäsosaa (n=194) vastasi, että heidän kotiverkossaan ei tällaisia laitteita ole liittyneenä.



Kuvio 33 Kotiverkossa liittyneenä laitteita, joiden tieturvasta ei varma (n=252)

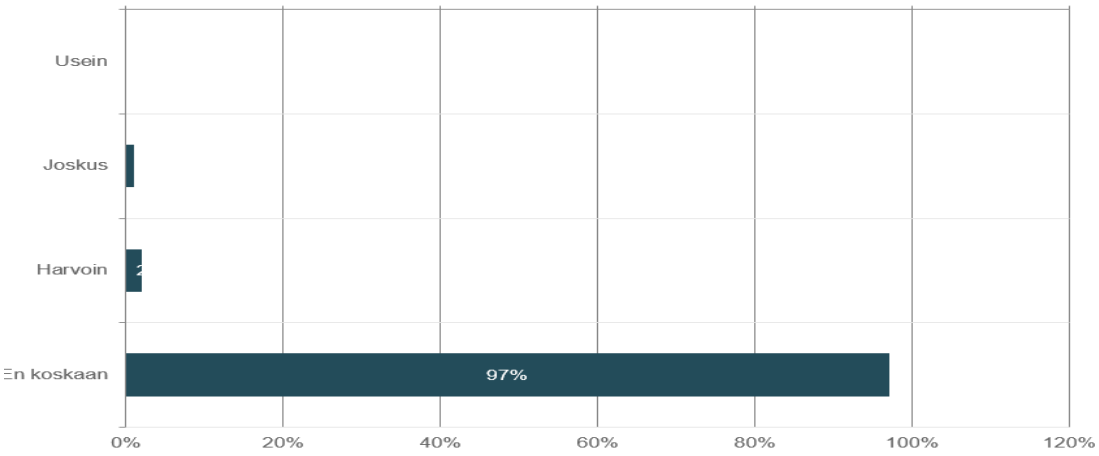
Kolme viidesosaa (n=152) kertoi saman langattoman verkon olevan myös muiden henkilöiden käytössä (Kuvio 34). Noin neljä kymmenesosaa (n=100) vastaajista vastasi, että työkäytössä olevaa kotiverkkoa ei käytä muut henkilöt. Edelliseen kysymykseen kyllä vastanneista (n=152) kertoi yli kaksi kolmannesta (n=103) huomioineensa muiden henkilöiden vaikutuksen verkkonsa tietoturvalle. Melkein kolmannes (n=49) tästä joukosta ei kertonut tätä huomioineensa.



Kuvio 34 Langatonta kotiverkkoa käyttävät muutkin henkilöt (n=252)

Työkonettaan välillä muiden henkilöiden kanssa samanaikaisesti on käyttänyt tai hetkeksi jopa koneensa toisen käyttöön lainannut kymmenesosa (n=25) kaikista vastaajista (n=252). Tämä on kohtalaisen suuri luku, joka mahdollistaa kyberturvallisuuden kannalta haitallisia tapahtumaketjuja, mikäli konetta lainataan esimerkiksi asiakkaan tai opiskelijan käyttöön. Tämä toimintamalli oli huomattavasti yleisempää Hyria säätiön ja Business-palveluiden vastaajaryhmässä neljänneksen osuudella ja Hyria Koulutus Oy:n palveluksessa olevista vastaajista vain hieman yli yksi kahdestakymmenestä toimii näin. Tähän varmasti vaikuttaa Säätiön

osalta monenlaiset asiakkuudet, joissa tukitoimien tarvitsijoiden osalta voi tulla tarvetta käyttää henkilökunnan henkilökohtaisia työasemia esimerkiksi kyselyn tai hakemuksen täyttämiseen. Haastattelun mukaan näitä tilanteita on ollut joitakin, mutta työntekijät ovat olleet aina vieressä samassa tilassa. Tämä ei ole kyberturvallisuuden kannalta haluttu tilanne. Vastaajista (n=252) lähes kaikki (n=245) vastasivat, etteivät missään tilanteessa jaa omia tunnuksiaan opiskelijoiden tai työkavereidensa kanssa (Kuvio 35). Joskus (n=2) tai harvoin (n=5) näin kertoi tekevänsä alle 3 prosenttia vastaajista.



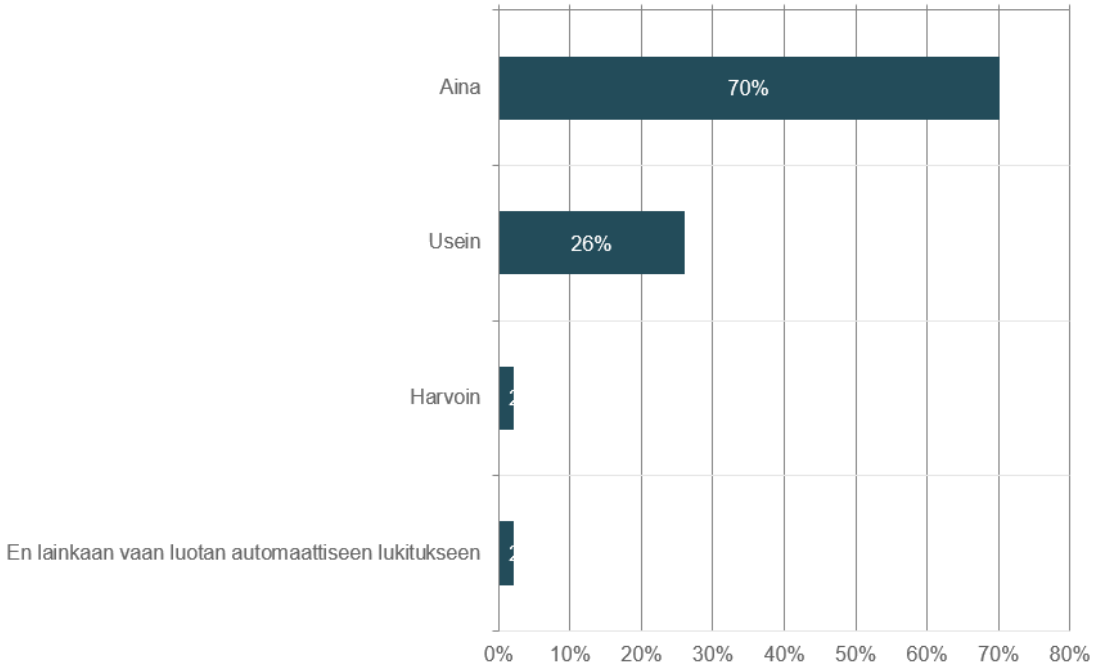
Kuvio 35 Jaan käyttäjätunnuksen toisen henkilön kanssa (n=252)

Työaseman läheisyydestä poistuessaan sen muistaa aina lukita suurin osa (n=175) vastaajista (Kuvio 36). Noin yksi neljäsosa (n=66) muistaa usein tehdä tämän. Automaattiseen lukitukseen luottaa noin kaksi ja puoli prosenttia (n=6) ja harvoin (n=5) työaseman lukitsee kaksi prosenttia vastaajista. Kyberturvallisuuden kannalta paras, koko henkilöstöllä käytössä oleva toimintatapa, olisi työasemien lukitseminen aina niiden luota poistuttaessa. Haastateltavien osalta ilmeni jonkin verran havaintoja organisaatiossa auki olevista työasemista varsinkin opetustiloissa. Niin sanotussa edu-verkossa olevat työasemat eivät samanlaista riskiä muodosta kyberturvallisuudelle, ellei siellä ole auki esimerkiksi opettajan kirjautumisia muihin tietosuojan kannalta tärkeisiin järjestelmiin. Haastatteluissa kävi ilmi, että henkilökunnan käytössä olevissa työtiloissa saattaa olla tapana jättää työasema lukitsematta niiltä poistuttaessa. Tämä lisää riskiä tiloissa, joihin saattaa päästä muitakin henkilöitä kuten opiskelijoita, asiakkaita tai yhteistyökumppaneita kuten työnantajien edustajia. Lisäksi tällainen toimintatapa lisää riskiä organisaation sisäisiin väärinkäytöksiin.

> Itse joskus ehkä jätän lukitsematta, kun poistun tästä (henkilökunnan työtilasta) vähäksi aikaa niin niin... (Haasteltava 4)

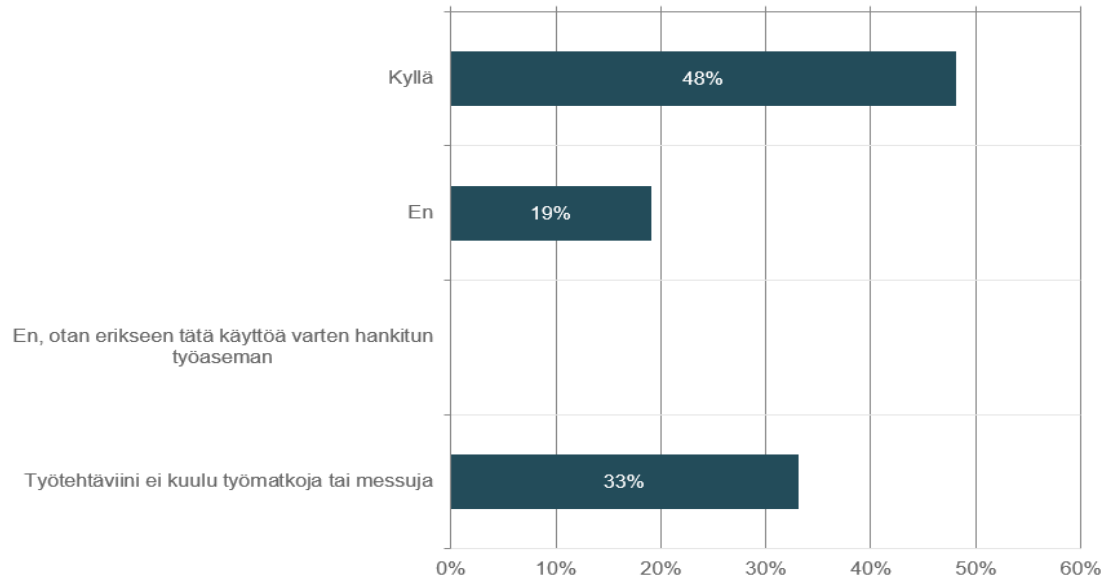
Esihenkilöt olivat suhteessa huolellisempia työasemien lukitsemisen osalta sillä heistä yli neljä viidestä (n=19) muistaa lukita aina, hieman yli yksi kymmenestä (n=3) joskus ja vain yksi ei

koskaan. Hyria säätiön ja Business-palveluiden henkilöstöstä vain hieman yli puolet vastasi lukitsevansa työasemansa aina (n=26) ja kaksi neljännestä usein (n=19) koneelta poistuessaan.



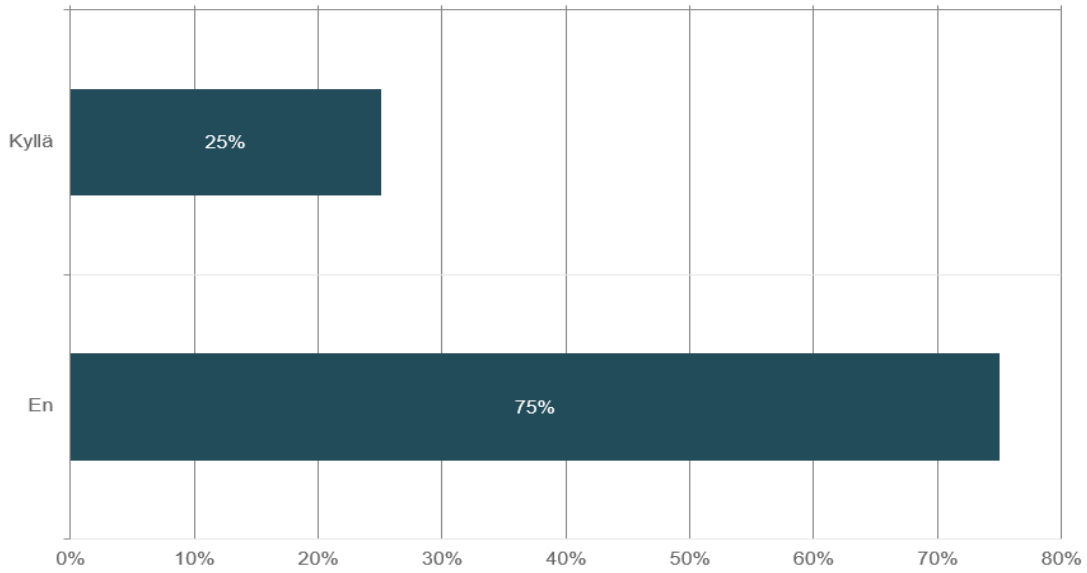
Kuvio 36 Muistaa lukita työaseman aina poistuessaan koneen läheisyydestä (n=252)

Työmatkoille ja messuille henkilökohtaisessa käytössä olevan työnantajan omistaman työasemansa ottaa mukaan lähes puolet (n=120) vastaajista (Kuvio 37). Toiseksi suurimman (n=83) ryhmän muodostavasta vastaajat, joiden työtehtäviin ei kuulu työmatkat tai messut. Kolmanneksi suurin (n=48) ryhmä vastasi, että ei ota mukaan henkilökohtaisessa käytössä olevaa työasemaansa. Yksi (n=1) vastaaja vastasi ottavansa erikseen tätä käyttöä varten hankitun työaseman. Tässä kysymyksessä vastauksien jakautumiseen vaikutti varmasti työnantajan käytännöt, joihin ei varsinaisesti kuulu erilliset työasemat työmatkojen ajaksi. Messuilla ja muualla on ollut käytössä muitakin kuin työntekijöiden henkilökohtaisessa käytössä olevia työasemia. Huomioitavaa kuitenkin on, että mikäli messuilla on työasemalle kirjautuneena omilla tunnuksilla, koneeseen on hyvin helppo ja nopea asentaa esimerkiksi haittaohjelma koneen haltijan huomion kiinnittyessä hetkellisesti toisaalle. Etenkin ulkomaille suuntautuvilla työmatkoilla tulisi kiinnittää huomiota työaseman koskemattomuuden varmistamiseen. Erillisen työaseman mukaan ottaminen on asia jota kyberturvallisuuden kannalta on syytä pohtia varsinkin esihenkilöiden osalta sillä heistä kolme neljästä (n=17) kertoi ottavansa henkilökohtaiseen käyttöön luovutetun työasemansa mukaan työmatkoille.

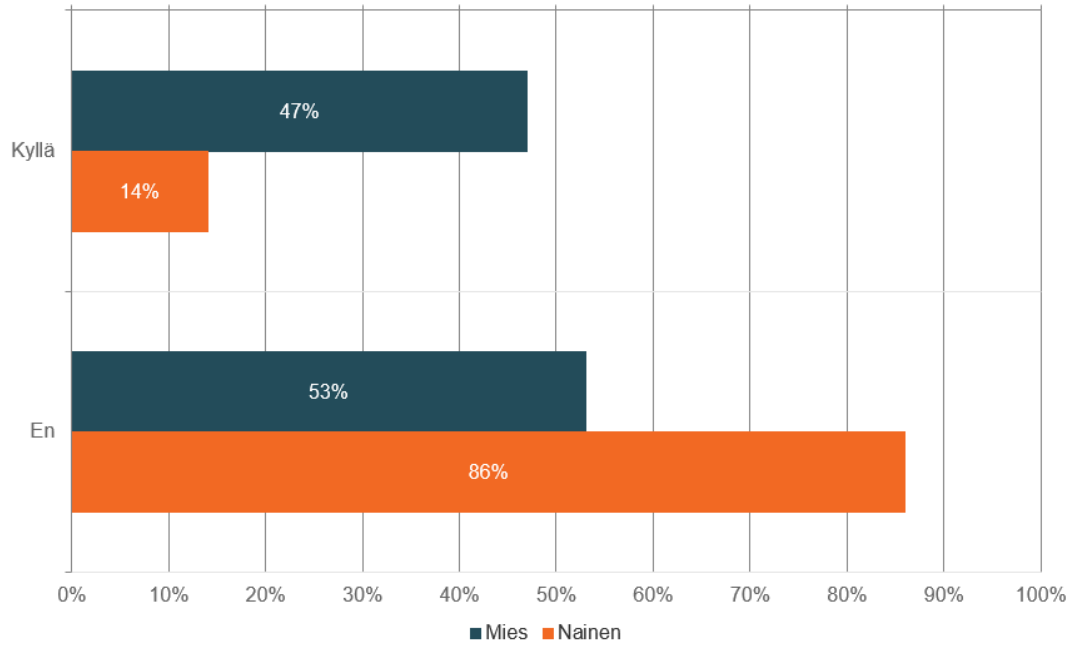


Kuvio 37 Otan henkilökohtaisen työasemani työmatkoille ja messuille (n=252)

Työhön liittyen ulkoisia kovalevyjä ja/tai usb-muistitikkuja tiedostojen siirtämiseen ja säilyttämiseen (Kuvio 38) kertoi käyttävänsä noin yksi neljäosa (n=62) vastaajista. Enemmistö (n=190) ei käytä näitä ulkoisia tallennusasemia työtehtäviinsä liittyen. Sukupuolen havaittiin korreloivan tämän kysymyksen kohdalla hyvinkin vahvasti R= 0,31 mikä suoraan näkyikin verrattaessa vastauksia vastaajan sukupuolen (Kuvio 39) mukaan. Tästä voidaan mahdollisesti tehdä jotain tulkintaa alakohtaisista toimintatavoista.



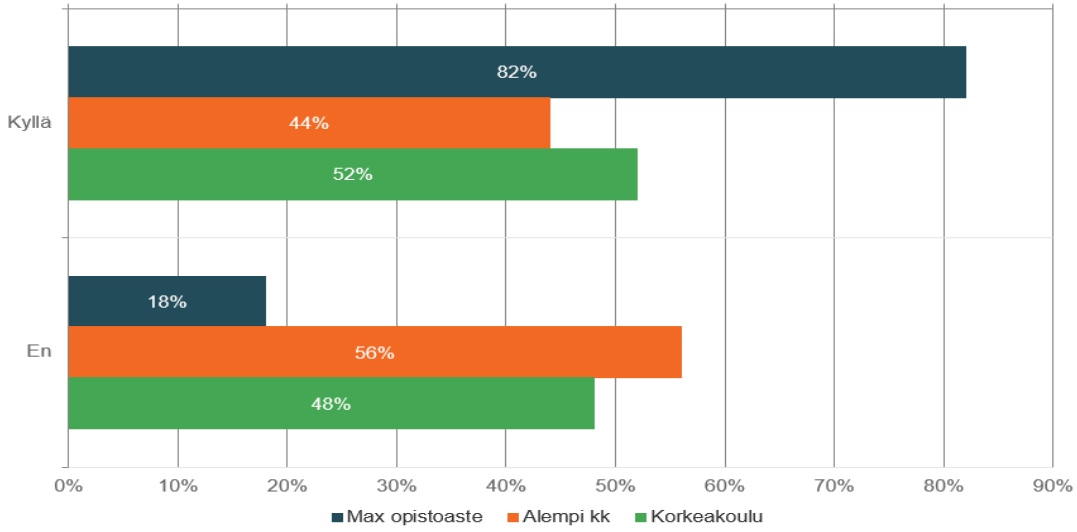
Kuvio 38 Käyttää ulkoisia tallennusasemia tiedostojen siirtämiseen ja säilytykseen (n=252)



Kuvio 39 Käyttää ulkoisia kovalevyjä tai usb-muistitikkuja (n=252) sukupuolen mukaan verrattuna (R=0,31)

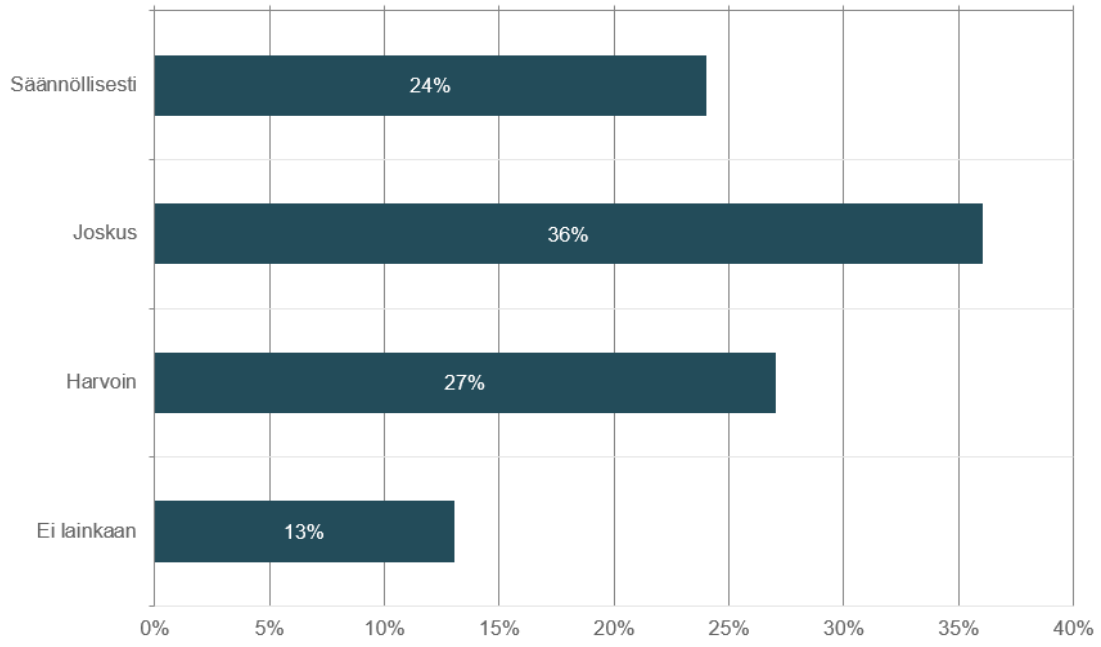
Edelliseen kysymykseen kyllä-vastauksen vastanneille esitettiin kolme jatkokysymystä. Ensimmäisessä kysymyksessä kysyttiin ovatko vastaajat huomioineet tietosuojan ulkoisia tallennusasemia käyttäessään. Vastaajista lähes neljä viidesosaa (n=49) kertoi huomioineensa ja noin viidennes (n=13) ei ollut huomioinut tietosuojaa. Ulkoisia tallennusmuotoja (n=62) käyttävistä lähes neljännes (n=24) kertoi käyttävänsä samaa usb-muistitikkua tai kovalevyä muissa kuin työnantajan hallinnoimissa laitteissa. Tämä vastaajajoukko on hieman suurempi kuin olisi tavoiltevaa tietosuojan huomiotta jättäneiden osalta. Kuitenkin tietosuojan huomioinut vastaaja ei mahdollisesti ole osannut huomioida haittaohjelmien leviämisen vaikutuksia tietoturvallisuudelle ja -suojalle. Kolmannella ulkoisten tallennusasemien käyttäjille kohdistetulla kysymyksellä pyrittiin selvittämään, onko vastaajilla tietoa mahdollisuudesta salata usb-muistitikulla olevat tiedosto siten, ettei niitä ole mahdollista avata ilman salasanaa. Tästä vastaajien joukosta (n=62) salausmahdollisuudesta oli tietoisia hieman alle kolme viidesosaa (n=36). Uutena tämä mahdollisuus tuli yli kahdelle viidesosalle (n=26) vastaajista. Koulutustaustan vaikutus (Kuvio 40) tässä kysymyksessä oli merkittävä siten, että suhteellisesti suurimman ryhmän muodostivat alemman koulutustaustan vastaajien parissa kyllä (n=14) vastanneet, jotka olivat selkeästi isompi ryhmä kuin ei (n=3) vastanneet. Muiden korkeakoulutettuja osalta vastaukset jakautuivat tasaisesti. Yleisesti nämä puutteet toimintatavoissa eivät muodosta riskiä, mikäli tallennettu materiaali on opetusmateriaalia eikä esimerkiksi opiskelijoiden tietoja. Ainoan riskin tässä tapauksessa muodostaa ryhmä, joka käyttää samaa tallennusasemaa myös muissa kuin Hyrian hallinnoimissa laitteissa. Näiden laitteiden osalta Hyrialla ei ole

samanlaista mahdollisuutta vaikuttaa esimerkiksi haittaohjelmien torjuntaan kuin hallinnoimillaan laitteilla.



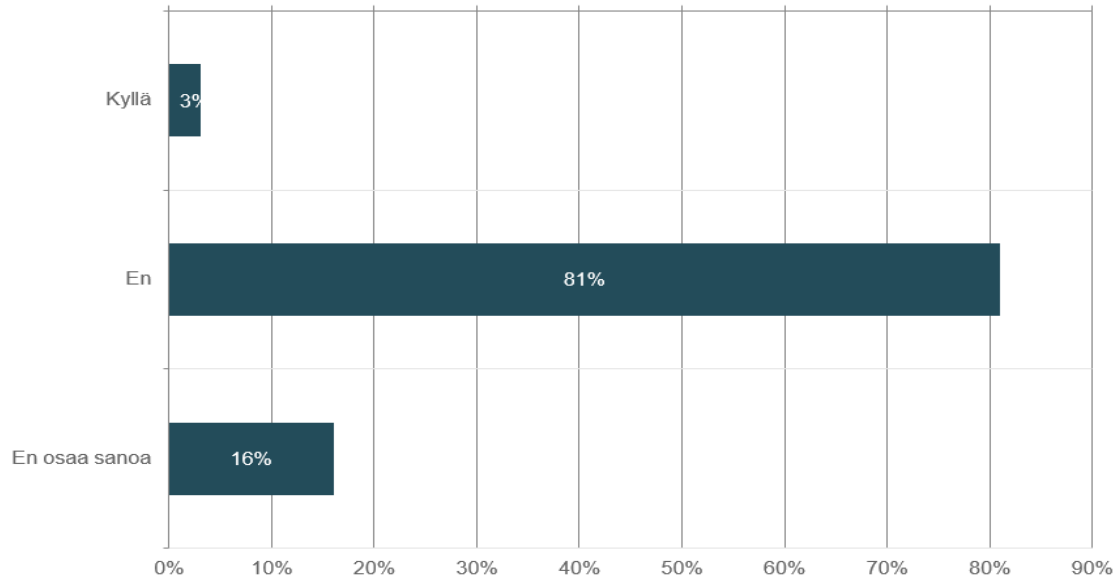
Kuvio 40 Tiedossa usb-tikun salausmahdollisuus verrattuna koulutustaustan mukaan (n=62)

Vastaajilta (n=252) kysyttiin tallentavatko he tiedostoja suoraan työasemalle henkilökohtaisen verkkoaseman tai OneDriven sijaan (Kuvio 41). Suurimman vastaajajoukon (n=91) muodostivat vastaajat, jotka vastasivat toimivansa joskus näin. Toiseksi suurimman (n=67) ryhmän muodostivat harvoin näin toimivat. Kolmanneksi suurimman (n=60) ryhmän muodostivat säännöllisesti työasemalle verkkoasemien sijaan tallentavat. Pienin vastaajajoukko (n=34) oli ei lainkaan työasemalle tallentavat. Tietoturvallisuuden kannalta olisi parempi toimintatapa tallentaa verkkoasemille työaseman sijaan. Lähtökohtaisesti työasemalle tallentaminen ei ole hyvä toimintatapa sillä työasemalle murtautuminen on nopea ja asiantuntijalle helppo toimenpide. Tällaisessa tilanteessa murtautujalle aukeaa pääsy työasemalle tallennettuihin tiedostoihin. Tähän kokonaisriskiin tietysti vaikuttaa tallennettujen tiedostojen laatu. Mikäli kyseiset tiedostot ovat opetusmateriaalia tai opetusmateriaalin tekemiseen tarvittavaa aineistoa, ei suurta vahinkoa tapahdu työaseman anastuksen tai siihen murtautumisen yhteydessä.



Kuvio 41 Tallentaa tiedostoja suoraan työasemalle (muualle kuin verkkoasemalle) (n=252)

Vastaajista (n=252) hieman yli neljä viidesosaa (n=205) vastasi etteivät voi yhdistää työkonettaan tietoturvan vaarantumatta julkisella paikalla olevaan langattomaan verkkoon (Kuvio 42). Toiseksi suurimman (n=40) vastaajajoukon muodostivat henkilöt, jotka eivät osanneet sanoa tämän toiminnan vaikutusta tietoturvaansa. Pienimpänä ryhmänä oli vastaajat, joiden mielestä tietoturva ei vaarantuisi, mikäli he yhdistäisivät työkoneensa mihin tahansa julkisella paikalla olevaan langattomaan verkkoon.

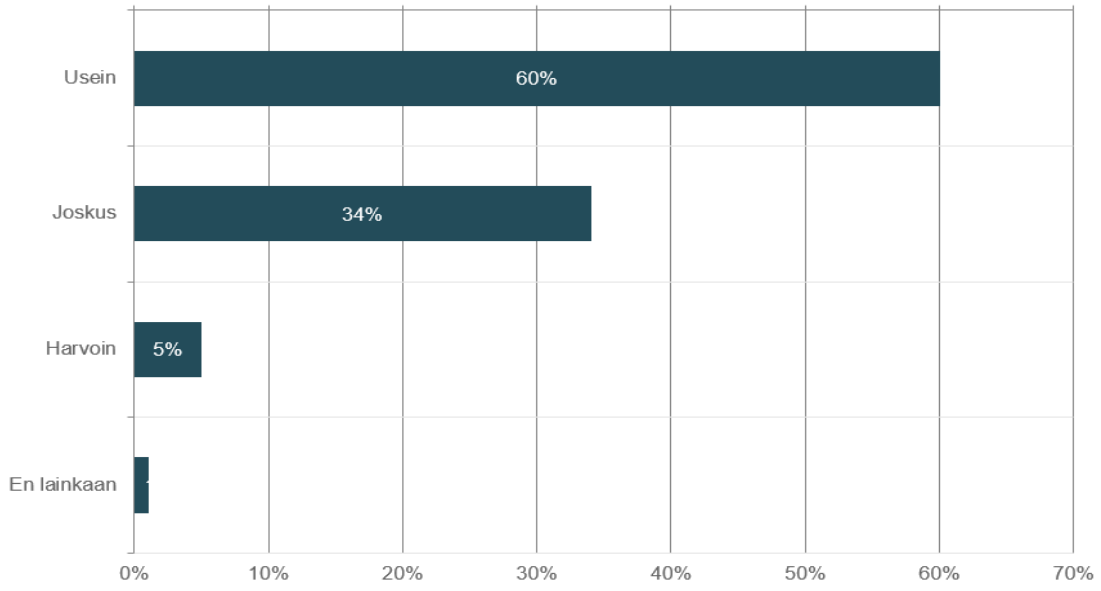


Kuvio 42 Voin yhdistää työkoneeni mihin tahansa julkisella paikalla olevaan langattomaan verkkoon tietoturvan vaarantumatta (n=252)

Työssään liitetiedostoja joutuu usein vastaanottamaan ja lähettämään (Kuvio 43) kolme viidesosaa (n=151) vastaajista (n=252). Toiseksi suurimman ryhmän, hieman yli kolmanneksen (n=86) kaikista vastaajista, muodostivat henkilöt, jotka joutuivat joskus lähettämään ja vastaanottamana liitetiedostoja. Harvoin (n=12) tai ei lainkaan (n=3) lähettävät ja vastaanottavat olivat hyvin pieni ryhmä vastaajien kokonaismäärästä. Tämän perusteella suuri osa henkilöstöstä joutuu työtehtävissään paljon vastaanottamaan ja lähettämään viestejä, joissa on mukana liitetiedostoja. Liitetiedostojen laatua ei kyselyssä pyritty selvittämään, mutta haastattelujen perusteella nämä liitteet pitävät sisällään myös tietosuojan kannalta suojattavaa materiaalia, kuten opiskelijoiden ja asiakkaiden henkilö- ja terveystietoja.

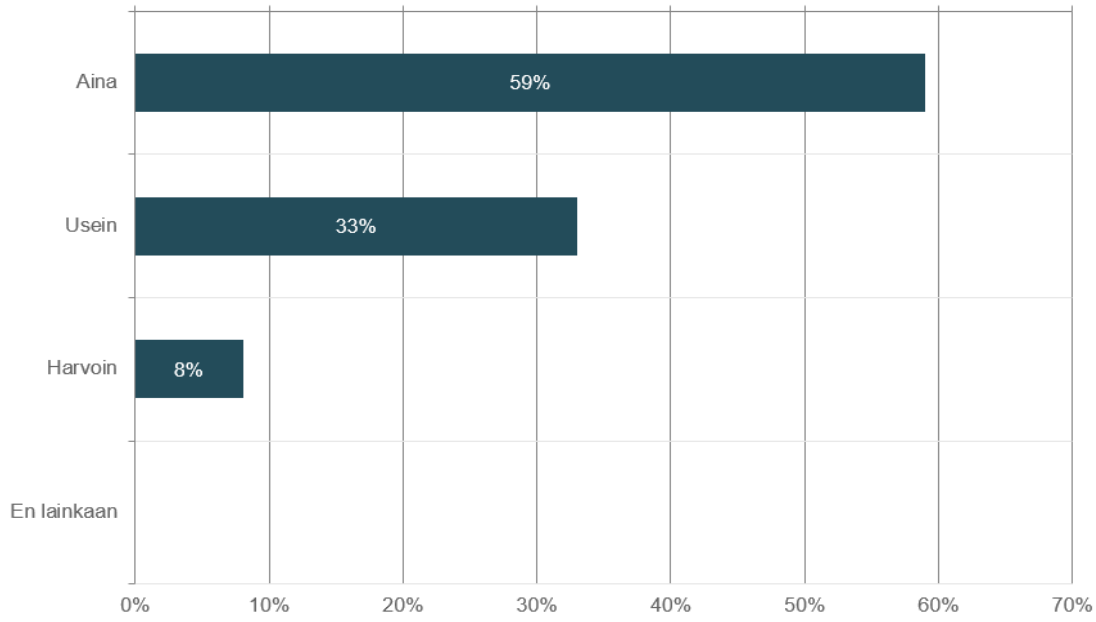
> Ihmisten tietojen kanssa toimitaan, että niiden kanssa pitää olla tosi tarkka. Ja me käytämme paljon sitä turvasähköpostia. (Haastateltava 5)

> Jos me lähetetään oppilaan tiedot jonnekin ja jos on oppilaan hetu niin todellakin lähetetään se turvapostilla. (Haastateltava 4)



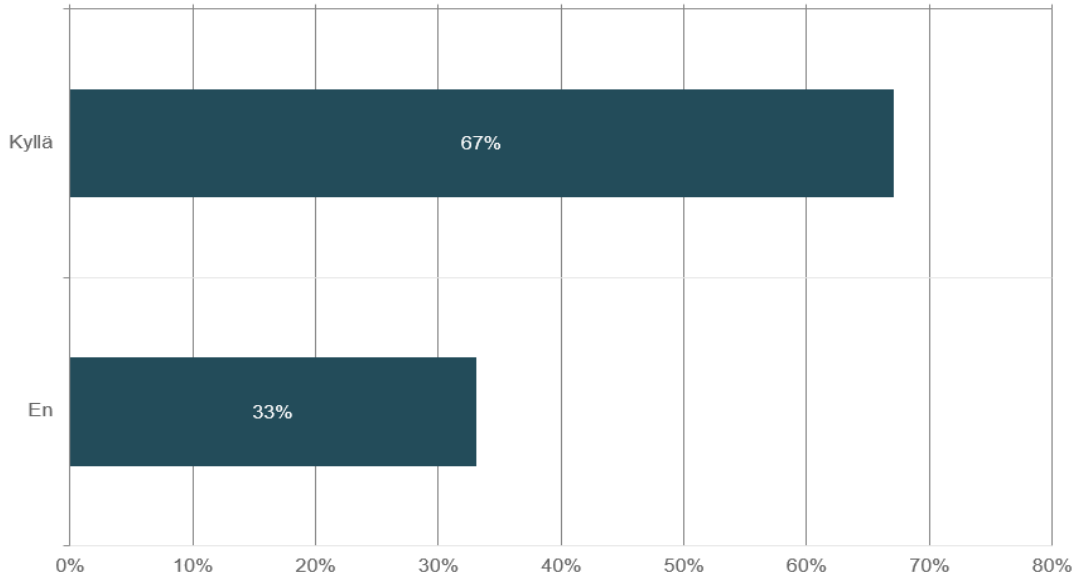
Kuvio 43 Työssään lähettää ja vastaanottaa liitetiedostoja (n=252)

Vastaajista (n=252) noin kolme viidesosaa (n=150) vastasi aina varmistavansa, mistä on kysymys, mikäli saa työsähköpostiinsa viestin itselleen tuntemattoman organisaation sähköpostista (Kuvio 44). Usein näin vastasi tekevänsä noin kolmannes (n=83) vastaajista. Kolmanneksi (n=19) suurimman ryhmän muodostivat vastaajat, jotka vastasivat harvoin toimivansa näin. Yksikään vastaaja ei vastannut, ettei lainkaan pyri varmistamaan mistä on kysymys.

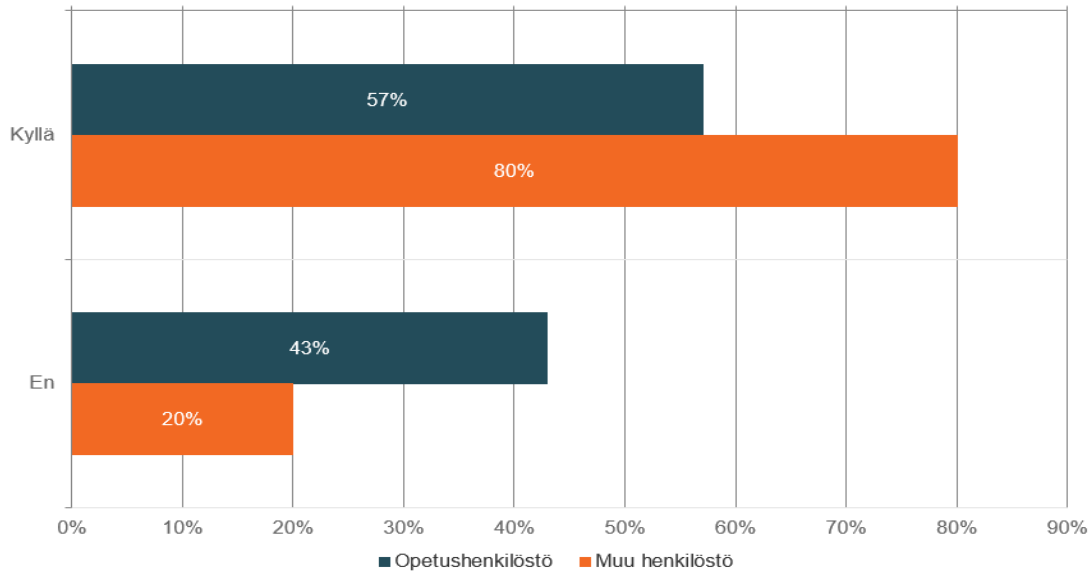


Kuvio 44 Mikäli saa työsähköpostiin viestin muusta, kuin itselleen tutun organisaation sähköpostista, varmistaa mistä on kysymys ennen avaamista (n= 252)

Työhönsä liittyvät sähköpostit (Kuvio 45) osaa tarvittaessa salata noin kaksi kolmasosaa (n=170) vastaajista. Noin yksi kolmannes (n=82) vastasi, ettei osaa työsähköpostinsa salaustoimintoa käyttää. Hyvin suuri osa henkilöstöstä ei siis osaa käyttää työsähköpostin salaustoimintoa. Joukossa varmasti on henkilöstöä, joka ei lähetä mitään arkaluontoista tai tietosuojan alaista materiaalia, mutta hyvin suurella todennäköisyydellä suuri osa tästä vastaajamäärästä kuitenkin näin toimii. Tehtävä organisaatiossa vaikutti merkittävästi sähköpostien salaamisen taitoihin (Kuvio 46). Muusta henkilöstöstä hieman yli neljä viidestä (n=90) vastasi osaavansa salata työhön liittyvän sähköpostin tarvittaessa ja alle viidennes (n=22) ei. Opetushenkilöstön osalta hieman alle kaksi kolmannesta (n=80) vastasi osaavansa ja hieman yli kolmannes (n=60) koki ettei osannut. Koulutustaustan vaikutus teki eroa vastaajien välillä vastausten jakaantuessa siten, että alemman korkeakoulutuksen saaneista (n=43) hieman alle kaksi kolmasosaa ja enintään opistotasoisen koulutuksen saaneista vastaajista kolme neljäsosaa (n=66) vastasi osaavansa käyttää salaustoimintoa. Korkeakoulutetuista hieman alle kaksi kolmasosaa (n=60) vastasi osaavansa käyttää työsähköpostin salaustoimintoa. Salaustoimintoa kuitenkin tulisi osata käyttää jokaisen, joka lähettää työsähköpostissa tietosuoja- tai muista syistä salassa pidettäviä tietoja. Henkilön omiakin tietoja sisältävät viestit olisi hyvä salata, vaikka lähettäjä ei itse kokisi tietojaan tärkeiksi.



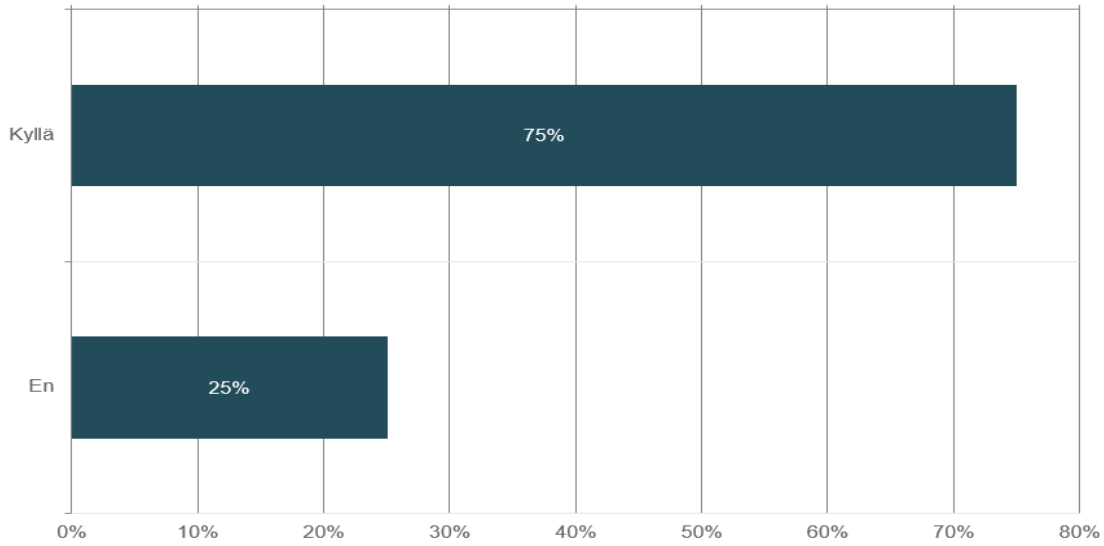
Kuvio 45 Osaa salata työhönsä liittyvät sähköpostit tarvittaessa (n=252)



Kuvio 46 Osaa salata työhönsä liittyvät sähköpostit tarvittaessa, tehtävän mukaan (n=252)

Vastaajista (n=252) kolme neljännestä (n=188) tietää missä tilanteessa työhön liittyvät sähköpostit tulisi salata (Kuvio 47). Yksi neljännes (n=64) vastasi ettei tiedä. Tämä luku on melko suuri ottaen huomioon tiedot mitä organisaatiossa säännöllisesti käsitellään. Vastaajajoukko pitää sisällään henkilöitä, joiden työtehtäviin ei kuulu opiskelijoiden, asiakkaisen, yhteistyökumppaneiden tai muun henkilöstön tietojen käsittelyä, joten tämä vastaajien määrä ei välttämättä anna aihetta erityisen suureen huoleen. Tämän kysymyksen kohdalla esihenkilöt

olivat muuta henkilöstöä valveutuneempia, sillä heistä kahdeksankymmentäseitsemän prosenttia kertoi tietävänsä missä tilanteessa työsähköpostit tulee salata. Tämä lienee heidän työtehtävänsä huomioiden ihan odotettavissa oleva vastausprosentti. Kun pohditaan minkälaisia tietoja esihenkilöt käsittelevät, toivoisi tämän luvun kuitenkin olevan jopa täydet sata prosenttia. Hieman pohdittavaa herätti myös se, että isompi osa vastaajista tiesi missä tilanteessa työsähköposti tulee salata kuin tiesi kuinka se tehdään. Kysely ei anna vastausta siihen johtuuko tämä siitä, että osa vastaajista käyttää näissä tilanteissa turvasähköpostia eikä täten ole ollut tarpeen perehtyä sähköpostin salaustoimintojen käyttöön.

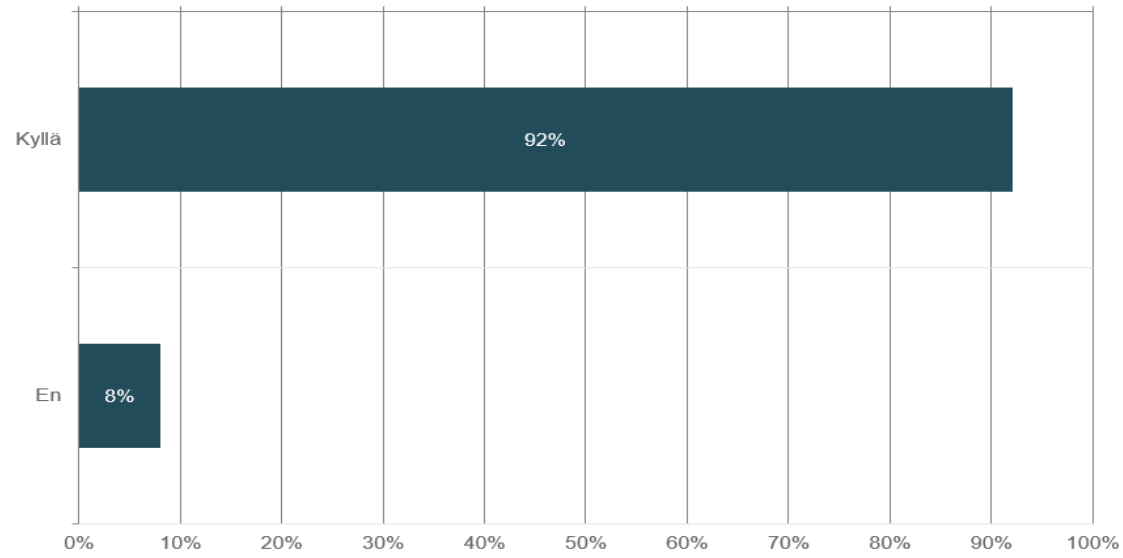


Kuvio 47 Tietää missä tilanteessa työsähköpostit tulee salata (n=252)

Vastaajista yli yhdeksän kymmenestä (n=231) vastasi tiedostavansa mahdollisesti jakavansa eteenpäin viestejä, joita viestin alkuperäinen lähettäjä ei ole tarkoittanut eteenpäin jaettavaksi (kuvio 48). Vastaajista alle kymmenesosa (n=21) kertoi ettei ole tätä tiedostanut. Tämä on mielenkiintoinen tulos, kun huomioi sen, että haastatteluissa sekä arkielämän tilanteissa on tullut ilmi organisaatiossa olevan yleinen tapana lähettää eteenpäin viestejä varmistamatta lupaa viestin alkuperäiseltä lähettäjältä. Tämä kysymys saattaakin olla huonosti muotoiltu eikä anna oikeaa kuvaa todellisesta toimintatavasta näissä tilanteissa. Mahdollisesti parempi muotoilu kysymykselle olisi ollut, että edelleen lähettäessään viestiä varmistaako henkilö viestin alkuperäiseltä lähettäjältä suostumuksen viestin edelleen lähettämiseksi. Tämä aihe nousi esiin jo asiantuntijahaastatteluissa sekä myöhemmin kyselylomakkeen vapaan vastauksen kentässä.

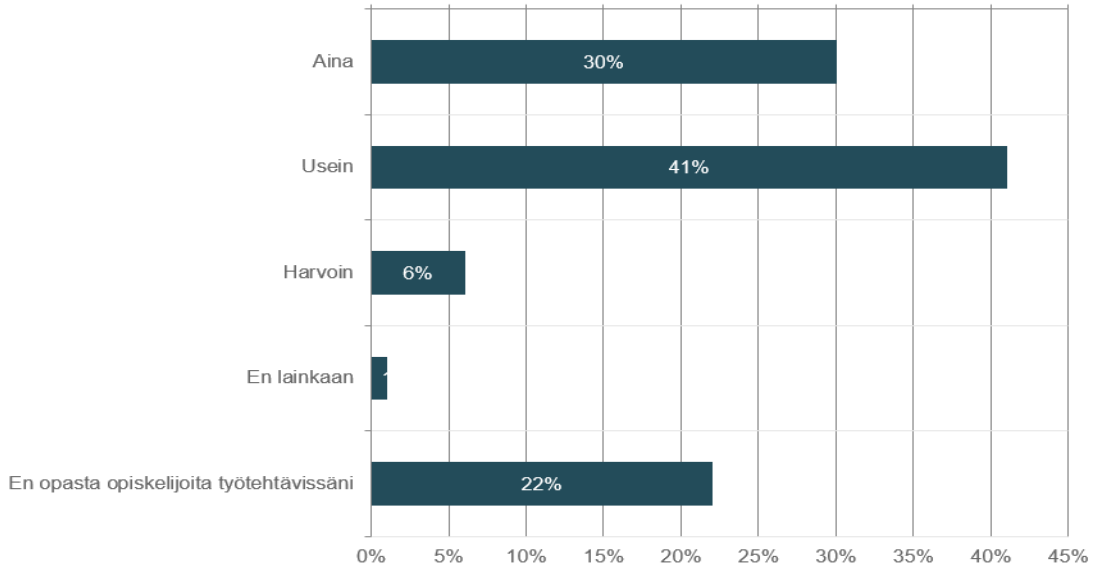
> Usein minun lähettämä sähköposti lähetetään eteenpäin ilman, että olen tarkoittanut sitä jaettavaksi. Sisällön tai muun takia. Olen vuosien aikana huomannut tämän käytännön olevan todella yleistä ja täten jätän paljon kirjoittamatta asioita viestiin. (Kyselyyn vastaaja)

Tässä kysymyksessä esihenkilöt olivat jokainen (n=23) vastanneet tiedostavansa mahdollisesti jakavansa jotain mitä ei viestin alkuperäinen lähettäjä ole mahdollisesti tarkoittanut edelleen jaettavaksi.



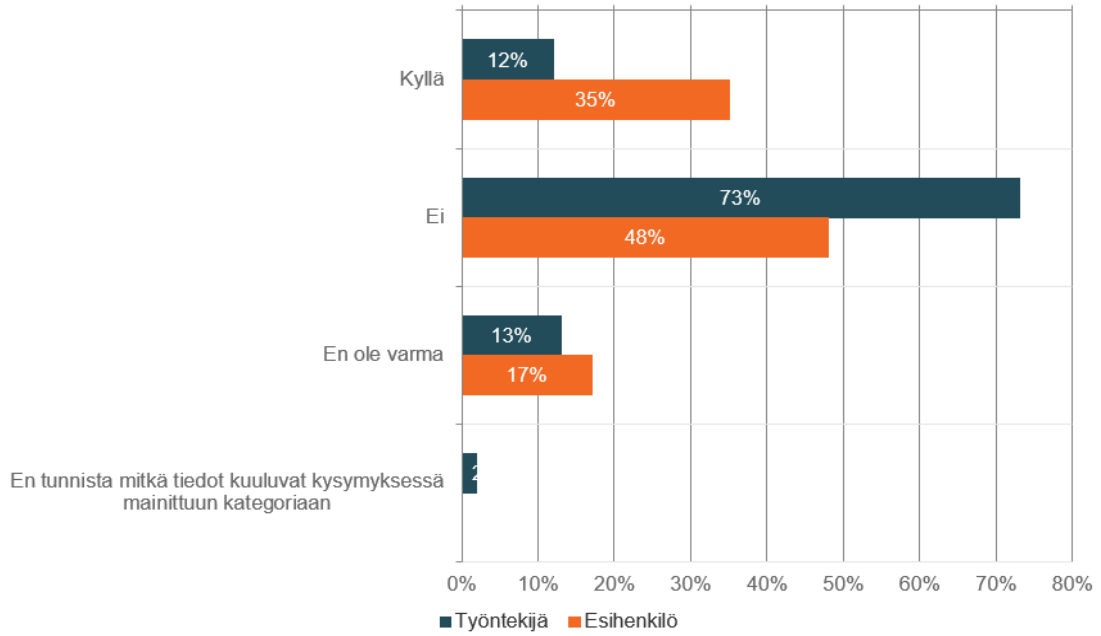
Kuvio 48 Tiedostaa, että viestin välittämällä saattaa tulla lähettäneeksi eteenpäin tietoja, joita viestin alkuperäinen lähettäjä ei ole tarkoittanut eteenpäin jaettavaksi (n=252)

Yleistä kiinnostusta kyber- ja tietoturvallisuuteen pyrittiin selvittämään myös kysymällä huomioivatko vastaajat tietoturvalliset toimintatavat opastaessaan opiskelijoita ja asiakkaita uusien tietojärjestelmien käyttöön (Kuvio 49). Näistä ei ole suoraan ohjetta henkilöstölle olemassa, mutta tämän kysymyksen perusteella voitaneen arvioida ainakin sitä, kuinka tärkeänä henkilöstö pitää tietoturvallisuuden aihepiiriä. Vastaajista suurimman ryhmän, hieman yli kaksi viidesosaa (n=103) muodosti vastaajat, jotka usein toimivat näin. Toiseksi suurimman (n=75) vastaajajoukon muodostivat vastaajat, jotka vastasivat aina huomioivansa tietoturvalliset toimintatavat opiskelijoita ja asiakkaita opastaessaan. Kolmanneksi suurin (n=55) ryhmä oli vastaajat, joiden työtehtäviin ei kuulu opiskelijoiden tai asiakkaiden perehdyttäminen tietojärjestelmiin. Harvoin tietoturvallisuuden huomioivat olivat pieni ryhmä (n=16) ja ei lainkaan vastanneita (n=3) ei ollut juuri lainkaan.

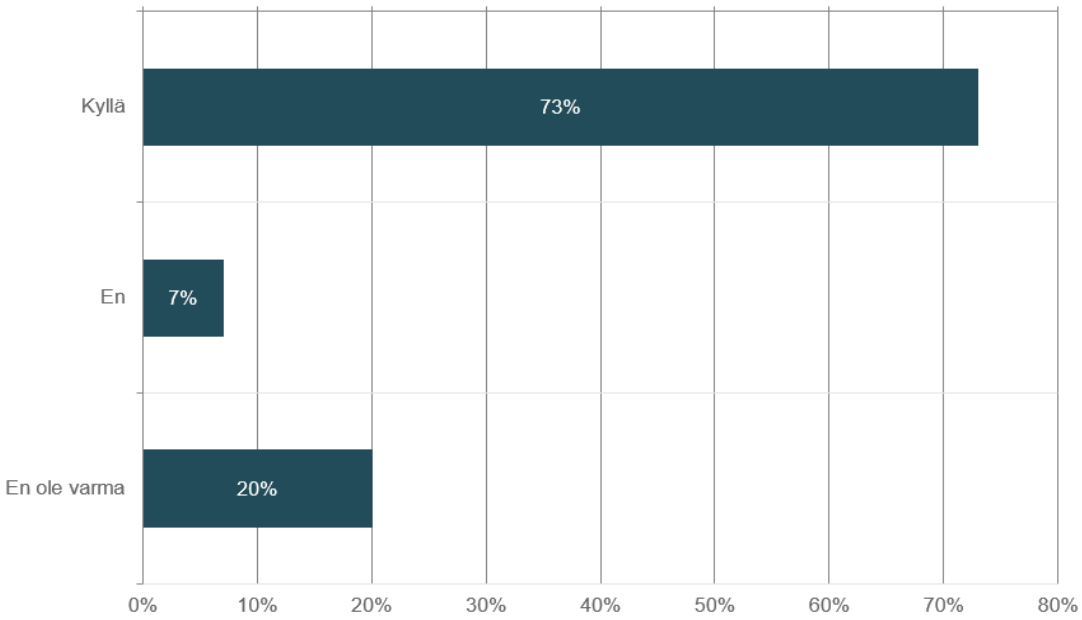


Kuvio 49 Huomioi tietoturvalliset toimintatavat opastaessaan asiakkaita ja opiskelijoita uusien tietojärjestelmien käytössä (n=252)

Hyriassa työskentelyn aikana urkinnan kohteeksi joutuneita oli yhteensä 36 vastaajaa. Tämä muodostaa 14,3 prosenttia koko vastaajajoukosta (n=252). Vastaajien suurin ryhmä (n= 178) on henkilöt, jotka ovat vastanneet, etteivät he ole joutuneet urkinnan kohteeksi. Kolmanneksi suurin ryhmä (n=33) on vastaajat, jotka eivät ole varmoja ovatko joutuneet urkinnan kohteeksi. Pienin ryhmä (n=5) on vastaajat, jotka eivät tunnista mitkä tiedot kuuluvat kysymyksessä mainittuihin tietosuojan ja tietoturvallisuuden kannalta merkittäviin tietoihin. Kyllä vastanneiden ryhmässä painottuu esihenkilöiden osuus (Kuvio 50). Vastaajista suurin ryhmä lähes kolmen neljänneksen (n=184) osuudella on kuitenkin henkilöitä, jotka kokevat tietävänsä kuinka tulee toimia, mikäli joutuisivat urkinnan kohteeksi (Kuvio 51). Toiseksi suurin ryhmä (n=51) ovat vastaajat, jotka eivät ole varmoja, kuinka toimia kuvatun laisessa tilanteessa. Pienimmän ryhmän (n=17) vastaajien joukossa muodostavat henkilöt, jotka vastasivat, etteivät tiedä kuinka tulisi toimia joutuessaan urkinnan kohteeksi. Hieman yli neljäsosa (n=68) vastaajista ei joko tiennyt kuinka toimia tai eivät olleet varmoja tietävätkö kuinka toimia, mikäli joutuvat urkinnan kohteeksi. Tämä on lukuna sellainen, joka antaa aihetta pohtia olisiko perehdytyksissä ja tietoturvallisuuskoulutuksissa aiheellista käsitellä myös tätä näkökulmaa.



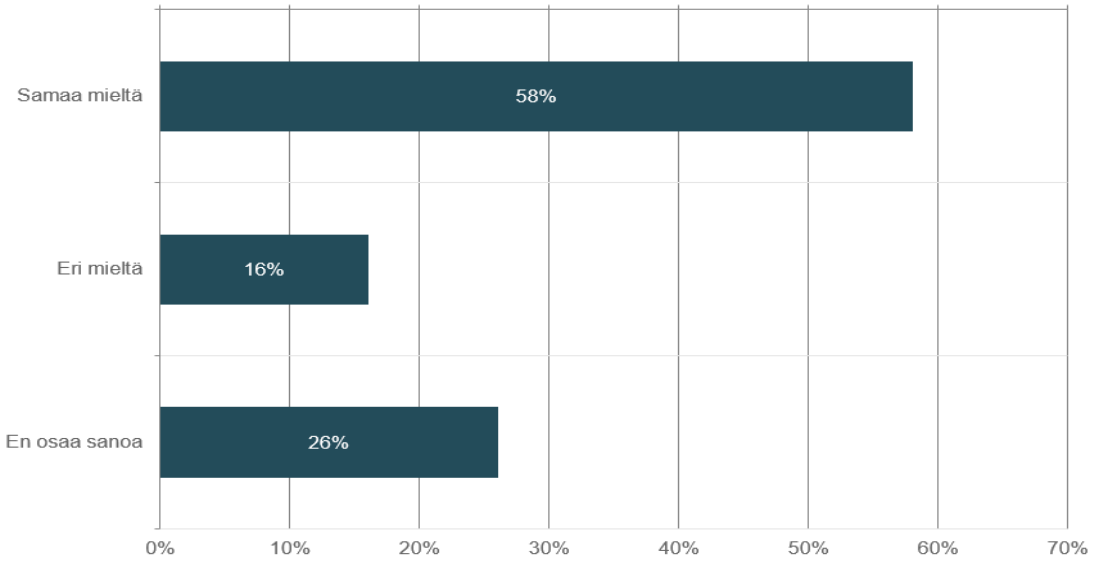
Kuvio 50 Hyriassa työskentelyn aikana yritetty urkkia tietoturvallisuuden ja tietosuojan kannalta tärkeitä asioita. Esihenkilöt ja työntekijät eriteltynä (n=252)



Kuvio 51 Tietää kuinka toimia urkinnan kohteeksi joutuessaan (n=252)

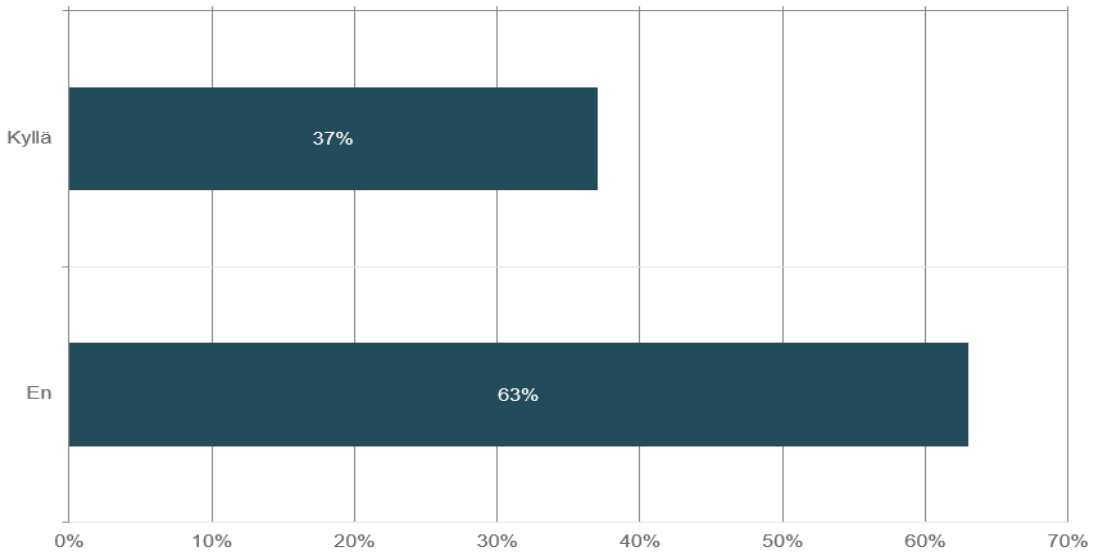
Yleisesti työyhteisössä tietoturvallisuuden kokee olevan hyvällä tasolla (Kuvio 52) melkein kolme viidesosaa (n=147) vastaajista. Toiseksi suurin (n=65) vastaajajoukko muodostuu vastaajista, jotka eivät osaa sanoa tietoturvallisuuden tasosta. He muodostavat hieman yli

neljänneksen koko vastaajajoukosta. Pienin ryhmä (n=50) oli vastaajat, joiden mielestä heidän työyhteisössään ei ole tietojärjestelmiin liittyvä tietoturvallisuusosaaminen hyvällä tasolla. Tämän kysymyksen kohdalla koulutustausta aiheutti eroavaisuuksia siten, että alemman korkeakoulun ylimpänä koulutusasteena ilmoittaneet olivat muun vastaajajoukon kanssa eri näkemyksen omaavia. Heistä vain hieman yli kaksi viidesosaa oli sitä mieltä, että tietojärjestelmiin liittyvä tietoturvallisuus oli hyvällä tasolla ja hieman yli neljännes heistä oli sitä mieltä, ettei näin olisi.



Kuvio 52 Kokee työyhteisön tietoturvallisuusosaamisen olevan hyvällä tasolla (n=252)

Kun vastaajilta (n=252) kysyttiin (Kuvio 53) kokevatko he huolta muiden työyhteisönsä työntekijöiden tietoturvallisuusosaamisesta vastasi hieman yli kolme neljäsosaa (n=159) etteivät he koe huolta. Kuitenkin hieman alle kaksi viidesosaa (n=93) kokee huolta muiden työntekijöiden tietoturvallisuusosaamisesta. Tämän kysymyksen kohdalla tehtävän ja koulutustaustan osalta vastaajaryhmät erosivat siten, että esihenkilöistä 48 prosenttia ja alemman korkeakoulun ylimpänä koulutusasteena ilmoittaneista 49 prosenttia vastasi olevansa huolissaan muiden työntekijöiden tietoturvallisuusosaamisesta. Mielestäni tuota lukua voidaan kokonaisuutena pitää korkeana ja huomiota kannattaa kohdistaa siihen, että käytännössä joka toinen esihenkilö koki huolta työntekijöiden tietoturvallisuusosaamisen tasosta. Vertailussa nousi esille työsuhteessa alle 5-vuotta olleet sekä alle 35-vuotiaat. Molemmat ryhmät kokivat tietojärjestelmiin liittyvän tietoturvallisuuden olevan hieman alemmalla tasolla kuin keskiarvovastaaja. He kuitenkin kokivat huolta muiden osaamisesta suhteessa vähemmän. Alle 5 vuotta työskennelleistä hieman alle kolme kymmenystä ei osannut vastata organisaation tietojärjestelmien tason kokemukseen. Heistä seitsemän kymmenestä ei ollut huolissaan muiden osaamisesta.



Kuvio 53 Kokee huolta muiden työntekijöiden tietoturvallisuusosaamisesta (n=252)

Kysymyksessä 56 kysyttiin yleisesti kyselyn aihealueen vastaajassa herättämiä ajatuksia ja havaintoja. Tähän kysymykseen vastasi 54 vastaajaa (n=252).

> Etenkin mobiililaitteiden ja -sovellusten käytöstä ei ole olemassa työnantajan puolesta selkeitä ohjeita. Epäilen vahvasti, ettei työnantajan puolella edes ymmärretä, mitkä palvelut ovat säännöllisesti ja oleellisesti osalle organisaation työntekijöille tarpeellisia ja tärkeitä työvälineitä. Siihen kuuluu monia sovelluksia, joiden tietoturvallinen käyttö on työntekijän oman osaamisen varassa. (Vastaaja 2)

> Aihe on tärkeä ja ajankohtainen. Organisaatioiden tietojärjestelmiin kohdistuva vaikuttaminen lisääntyy ja myös koulutusorganisaatiot ovat olleet vaikuttamisen kohteena, tämä kehityssuunta jatkuu varmasti myös tulevaisuudessa. Kuitenkin käytännön arjessa ihmiset usein unohtavat oman toimintansa ja valintojensa vaikutukset tietoturvalle. Oppilaitokset perinteisesti avoimina ympäristöinä ovat alttiita fyysiselle vaikuttamiselle ja tietojen urkinnalle, mutta henkilöstö ei tätä välttämättä aina ymmärrä. (Vastaaja 4)

> Tietoturvaan tulisi kiinnittää Hyriassa enemmän huomiota. Teknologia kehittyy niin nopeasti, että vuosia sitten pidetty perehdytys voi olla vanhentunutta tai unohtunut. Myös etätyötä tekeville pitäisi olla opastusta tietoturvaan liittyen. (Vastaaja 5)

> Hyvä olisi opejen tiedostaa se, että ovien, joiden kuuluu olla lukossa, kiinniolon varmistaminen on helpointa tietoturvaa. (Vastaaja 6)

Koen tietäväni perusasiat aiheesta, mutta välillä huomaan tietäväni kuitenkin huolestuttavan vähän asiasta. Minun ei tule aina ajateltua tietoturvallisuusasioita töitä tehdessäni. Asia johtuu ehkä siitä, etten ole ennen ollut sellaisessa työssä, jossa käsiteltäisiin henkilökohtaisia tietoja aivan tällä tavalla, joten en ole tottunut asioita ajattelemaan. (Vastaaja 11)

Lisää koulutusta henkilöstölle! (Vastaaja 12)

Minusta olisi hyvä käydä koko henkilöstön kanssa läpi esimerkiksi, että wifin kautta komennettava pesukone voi urkkia tietoja ja esimerkiksi asiakasjärjestelmiä jne. ei todellakaan pitäisi avata suojaamattomassa verkossa ja huomioida myös, että huoltoaseman toimistossa huomioidaan tietoturvaseikat. Turvapostin pitäisi olla laajemmin käytössä. (Vastaaja 18)

Tietotekniikan tietoturva tärkeää, mutta myös esim. papereiden tietoturvallinen hävittäminen on tärkeää. (Vastaaja 19)

Tärkeä ja ajankohtainen aihe, jota arjen kiireessä ei aina ole aikaa pysähtyä miettimään sen vaatimalla tavalla. (Vastaaja 21)

Mielestäni on tärkeää käsitellä tietoturvaa ja kartoittaa työyhteisön sisäisiä tietoturva ja tiedonkäsittely taitoja. (Vastaaja 23)

Kaikki työyhteisön jäsenet eivät suhteudu aiheeseen kovin vakavasti. Myös itselle tapahtuu kiireessä ajattelemattomuudesta aiheutuvia riskitilanteita. (Vastaaja 25)

Huolta herätti se miten vähän Hyria on opastanut/kouluttanut/tiedottanut aiheeseen liittyen. Se pieni perehdytyksen yhteydessä käyty tietoturvallisuuskoulutus ei ole mielestäni tarpeeksi kattava ja unohtuu helposti arjen kiireissä. (Vastaaja 26)

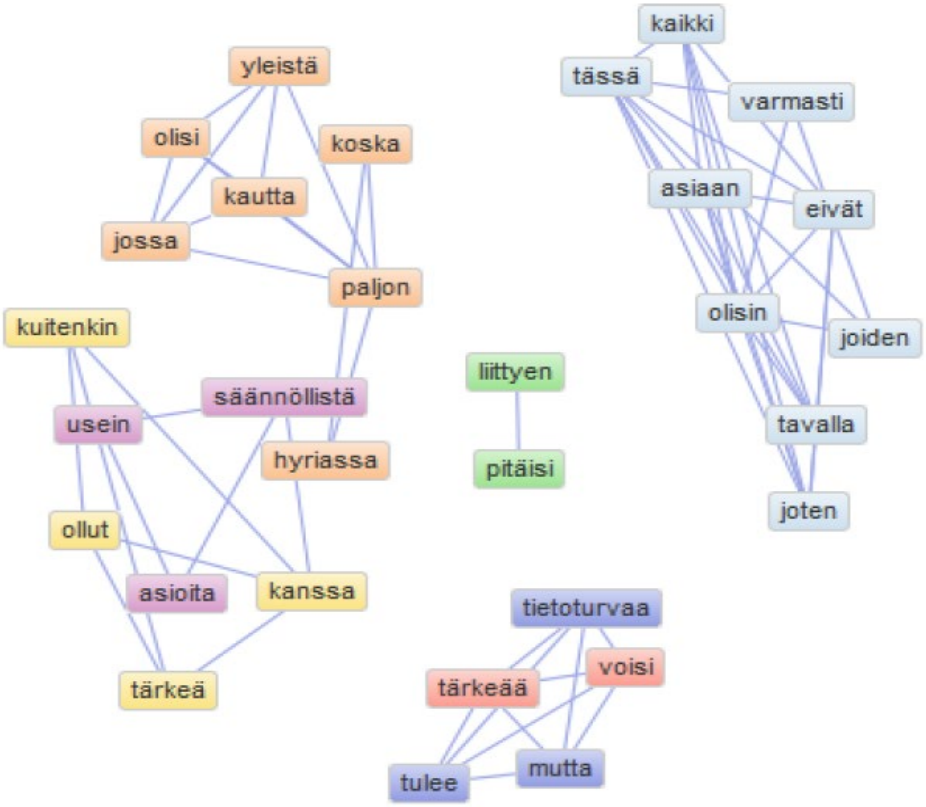
Ehkä jokin "pakollinen" tietoturva-asioiden kertaus olisi paikallaan koko työtiimilleni. (Vastaaja 27)

Tärkeä ja laaja aihe, joka vaatii paneutumista ja säännöllistä koulutusta. (Vastaaja 29)

Tietoturvakoulutuksia tarvittaisiin paljon enemmän osastokohtaisesti, vaikka jokaisen työntekijän tulisikin tunnistaa oma vastuunsa. (Vastaaja 31)

> Vallitsevassa maailmantilanteessa voisi tietoturva-asioista olla enemmänkin yleistä keskustelua. (Vastaaja 37)
>
> Tuntuu, että täytyisi olla jatkuvasti hereillä ja seurata asioita ja ohjeita. Pelkään, etten tee niin. (Vastaaja 39)
>
> Kysymykset osoittivat, että tietoturvallisuus-asioissa olisi paljon opittavaa. (Vastaaja 41)
>
> Tärkeä asia. Voi olla, että perehdytyksessä tietoturva-asiat tulevat nykyisin hyvin esille. Voisi olla kuitenkin fiksua huolehtia myös siitä, että vuosia talossa olleet osaisivat nämä asiat myös. (Vastaaja 46)
>
> Olen huolestunut tietoturvallisuudesta nykytilanteessa ja pyrin olemaan mahdollisimman huolellinen. Lisätieto ja selkeät toimintamallit eivät olisi pahitteeksi. (Vastaaja 49)
>
> Tarpeellinen aihe ja varmasti mukana eritasoista osaajaa. (Vastaaja 52)

Avoimissa vastauksissa toistui muutamat aihepiirit ja sanat (Kuvio 54) joiden perusteella muodostui kuva vastaajista, jotka kokevat tietoturvallisuuden tärkeänä asiana. Avoimen kysymyksen vastauksissa vahvistui kyselyn perusteella saatu kuva henkilöstöstä, joka pitää tietoturvallisuutta ja tietojärjestelmien turvallista käyttöä tärkeänä asiana. He toivovat säännöllistä koulutusta, selkeitä ohjeistuksia ja toimintaohjeita sillä he pelkäävät aiheuttavansa omalla toiminnallaan tietoturvan vaarantumisen. Kohtalaisen vahvana vastaajien keskuudessa oli huoli muiden työntekijöiden osaamisesta kyberturvallisuuteen liittyen.



Kuvio 54 Avoimien vastausten sanakartta (n=54)

Haastatteluissa esille nousivat samat havainnoit kuin kyselyn avoimissa vastauksissa noudattaen samaa yleistä kuvaa mikä kyselyn vastauksissa jo muotoutui. Tietoisuus aiheen tärkeydestä oli vahvasti läsnä haastateltavien mielipiteissä ja näkemyksissä. Oman osaamisen osalta haastateltavat tiedostivat mahdolliset puutteensa, vaikka jokainen piti itseään keskimääräistä Hyrian työntekijää paremmin aiheeseen perehtyneenä. Tämä saattoi johtua ihmisillä yleisesti olevasta harhasta tai vain siitä, että haastatteluun vapaaehtoisesti tarjoutuivat ne henkilöt, jotka kokivat aiheen tärkeänä. Kaksi haastateltavaa kertoi myös ilmoittautuneensa haastatteluun voidakseen oppia aihepiiristä mahdollisesti jotain uutta.

Haastateltavien kyberturvallisuustietoisuudessa oli hieman vaihtelua hyvin epävarmasta käyttäjästä tietojärjestelmien kanssa kokeneeseen henkilöön. Yleisesti haastateltavien kertomuksista välittyi kiinnostus aihepiiriin. Haastateltavien omaan toimintaan liittyen oli havaittavissa asioiden priorisointi turvallisuuden kannalta esimerkiksi siinä, kuinka he menivät joillekin verkkosivuille tai minkälaisia salasanoja he käyttivät itselleen tärkeissä palveluissa. Kiireestä ja muusta johtuen he olivat kokeneet ajoittain ottaneensa riskejä salasanoja tai muita toimintatapoja valitessaan. Salasanojen osalta haastateltavat olivat pohtineet erilaisia tarpeita salasanoille ja kertoivat käyttävänsä eri salasanoja eri tarkoitukseen. Turvallisemmaksi koettuja käytettiin tietosuojan kannalta tärkeämpien sivustojen osalta. Kuitenkin jokainen haastateltava kertoi, ettei ollut itsekään ihan täysin tyytyväinen siihen, miten on salasanoja

käyttänyt. Syyksi haastateltavat kokivat pääsääntöisesti kiireessä tehdyt tunnukset sekä erilaisten kirjautumista vaativien palveluiden määrän.

> No siis henkilökohtaisessa elämässä käytän kyllä samaa salasanaa monessa jutussa koska muistini on huono. Vanha ihminen. Mutta olen pyrkinyt siihen töissä, että mulla on joka paikkaan eri salasana. (Haastateltava 4)

> Joka paikkaan pitää kirjautua, niin sitten varmaan aika helposti menee niin, että sitten on joku semmoinen yleissalasana, jota tulee käyttäneeksi sitten. (Haastateltava 2)

Opetustiloissa olevat työasemat ovat liittyneenä niin sanottuun edu-verkkoon ja näiden työasemien osalta usein saattaa olla, että koneet ovat auki, vaikka opettaja ei ole paikalla tai koneissa on selkeästi kirjautumistunnukset merkitty koneeseen. Tämä ei lähtökohtaisesti muodosta ongelmaa, mikäli esimerkiksi selaimen kautta opetushenkilöstö ei ole kirjautunut johonkin tietosuojattavaa materiaalia sisältävään palveluun kuten oppilastietojärjestelmä Wilmaan.

> Ihmisten olisi syytä muistaa se, että kun he ovat kirjautuneena vaikkapa eduverkon koneelle, niin hehän ovat saattaneet sitten avata Wilmaa tai jotain muuta vastaavaa omilla tunnuksillaan kuitenkin. (Haastateltava 1)

Työyhteisössään he kokivat toiminnan olevan pääsääntöisesti hyvällä tasolla. Kuitenkin vuosien varrella haastateltavat olivat toistuvasti havainneet avaimia ovissa, ovia lukitsematta ilman, että opettajaa paikalla, työasemia lukitsematta myös tiloissa missä opiskelijoita ja asiakkaita vierailemassa. Joitakin tilanteita oli myös havaittu, joissa oli kirjoitettu tai lähetetty tietoja, joita ei kuuluisi salaamatta lähettää. Haastateltavien havaintojen mukaan tietosuojan alaisista asioista oli keskusteltu haastateltavien mielestä varomattomasti. Jonkinasteista urkintaa oli kohdattu, mutta sen koettiin olevan enemmän uteliaisuudesta johtuvaa eikä niinkään ammattimaista tai muuten pahoin aikein toteutettua. Tiloissa liikkumisen osalta haasteltavat totesivat avoimen oppilaitosympäristön muodostavan haasteen tietoturvallisuuden kannalta. Haastateltavat kokivat, että henkilökunta ei välttämättä kiinnitä huomioita tiloissa liikkuviin heille tuntemattomiin henkilöihin.

> Tässä suhteessa kyllä vaikkapa henkilökortin käyttäminen, niin itse kyllä näkisin, että olisi suotavaa, jos useampi henkilöstön jäsen sitä oikeasti pitäisi esillä. Olisi kyllä tärkeää, että sitten pystyisi helposti ja nopeasti, niin kun ainakin suurin piirtein tunnistamaan, että onko se nyt oikealla asialla se kaveri siellä vai ei. (Haastateltava 1)

Mobiililaitteisiin ja applikaatioiden käyttöön liittyen pääsääntöisesti oli käsitys, että turhia applikaatioita ei kannata latailla. Kuitenkin liittyen applikaatioiden vaatimiin oikeuksiin oli haastateltavilla hieman enemmän tietämättömyyttä esimerkiksi sen suhteen mihin kaikkiin tietoihin applikaatiot pääsyä pyytävät ja mistä tämän tiedon voisi mahdollisesti tarkistaa. Kaikkia ehtoja haastateltavat eivät kertoneet lukevansa ennen applikaation asentamista ja oikeuksien antamista. Työpuhelimen suhteen kuitenkin oltiin varovaisia, mutta se ei kuitenkaan täysin ollut vaikuttanut siihen mitä sosiaalisen median palveluita esimerkiksi työpuhelimiin ladattiin ja miten niitä käytettiin.

> Varmaan niinku jengi luottaa siihen, että ikään kuin ICT hoitaa niin mun ei tarvitse tätä asiaa tietää. (Haastateltava 3)

Jokainen haastateltava koki vahvasti, että aiheeseen liittyvää koulutusta tulisi olla enemmän. He myös kokivat ohjeistuksien olevan kyberturvallisuuden osalta puutteellisia tai ohjeita ei ainakaan ole nostettu esille riittävän vahvasti. Joitakin ohjeita he kertoivat kuitenkin nähneensä. Vahvasti nousi toive siitä, että hybridityöhön liittyvien toimintamallien osalta olisi hyvä olla saatavilla selkeä perehdytys ja ohjeistus, jonka perusteella työntekijät voisivat turvallisin mielin toimia myös etänä omalla kotitoimistolla tai esimerkiksi opiskelijoiden ja asiakkaiden työpaikoilla.

> Mutta tavallaan siis ohjeistukseen kuuluu selittää se auki, että sitten voi olla joku valveutunut käyttäjä, joka oikeasti miettii sitä ja sitten se ei saa oikein vastausta tavallaan. Niinku vaikka nyt meikäläinen, että en mä, sanotaan rehellisesti, pysty tietää. Mutta jos mulla on ICT:n laatimat ohjeet, että se on turvallista, niin silloinhan se on niinku selvä. (Haastateltava 3)

> Ehkä ne ohjeistukset ovat semmoisia mihin voisi jotenkin satsata. Kun tämmöisiä mun kaltaisia ihmisiä täällä kuitenkin on töissä aika paljon, joille nää ei ole niin itsestään selviä. (Haastateltava 4)

Epävarmuus oman toiminnan turvallisuuden osalta oli selkeästi vaivannut heitä työtehtäviä tehdessään. Haastatteluissa ja avoimissa vastauksissa nousi myös esille niin sanotun tietosuojakalvon saaminen kannettavan työaseman näyttöihin. Yhden haastateltavan toiveena oli, että nämä tulisivat jopa automaattisesti työasemien mukana työasemia ict-palveluista luovutettaessa. Kaikki haastateltavat kokivat esihenkilöiden pääsääntöisesti ottavan tietoturvahuolet vakavasti.

Haastattelujen yleinen teema oli koulutusmyönteinen suhtautuminen ja koulutusta toivottiin tietoteknisten järjestelmien tietoturvalliseen käyttöön. Koulutuksen toivottiin olevan säännöllistä ja huomioivan muuttuvat järjestelmät sekä erilaiset uhat, joita nykyään järjestelmiin kohdistuu. Haastatteluissa kysyttiin haastateltavilta mielipidettä

tietoturvallisuuskoulutuksesta henkilöstöpäivien yhteydessä. Jonkinlainen rasti näihin päiviin liittyen koettiin hyvänä vaihtoehtona. Näin kattavuus henkilöstön parissakin saataisiin korkeammaksi kuin pelkästään ohjeita julkaisemalla.

> Ei niitä ehkä tule sitten omatoimisesti niin tietoja päivitettyä. Voisi olla ihan hyvä, että vaikka kerran kahdessa vuodessa olisi joku tämmöinen päivän kurssi mikä olisi kaikille pakollinen. Asiat muuttuvat eli niitä on hyvä muistutella. (Haastateltava 4)

Haastateltavat kaipasivat itsenäisempiä koulutusmuotoja kuten tietoturvallisuuden verkkokurssi. Vastaavanlainen kurssi kuin henkilöstöllä on tällä hetkellä It's Learningissä menossa ilmastovastuulliseen toimintaan liittyen. Haastateltavat toivat esiin arjen haasteita kuten kiireet ja muut aihealueet, joihin tarvitaan lisää koulutusta. Kaikkea ei kuitenkaan haluttu samaan aikaan arjen kiireiden keskelle. Se on varmasti hyvä huomioida, jotta aiheeseen liittyvä kiinnostus ja uteliaisuus ei käänny negatiiviseksi.

> Puolen tunnin info tai vajaan tunnin info asiasta. Ihan koko henkilöstölle, että sinne voisi vaan tulla kuuntelemaan se asia. (Haastateltava 5)

Mahdollisesti tuleviin koulutuksiin toivottiin esimerkkejä erilaisista tilanteista hahmottamaan asioita käytännön tasolla.

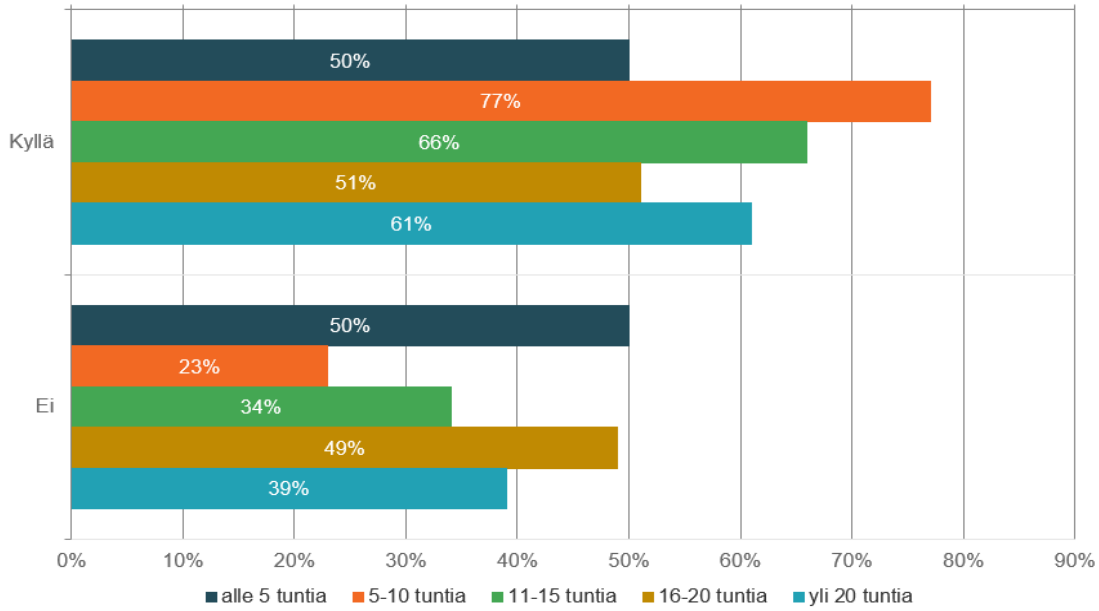
> Esimerkiksi keissejä, semmoisia, että niiden kautta sitä sitten ymmärtää ja ehkä muistaa paremmin ne asiat. Kun kuulee jonkun keissin ja sitä voi sitten toistaa sitä keissiä. Ja ne tarinat jäävät parhaiten mieleen ihmisille. (Haastateltava 5)

8 Johtopäätökset

Opinnäytetyönä tehty kehittämistyö nosti esille joitakin osa-alueita, joiden perusteella toimeksiantajan organisaatio voi kehittää henkilöstönsä kyberturvallisuusosaamista ja -tietoisuutta. Lisäksi tehty tutkimus nosti esille joitakin tarpeita jatkotutkimukselle, mikäli havaintoihin halutaan tarkennus ja varmuus. Esimerkkinä salasanakäytäntöjen osalta jäi selvittämättä todellinen tilanne samojen salasanojen käytön suhteen. Hieman on viitteitä, että mahdollisesti samoja salasanoja käytetään muutenkin kuin turvallisuusvaatimuksiltaan lievempien palveluiden ja verkkosivujen kohdalla. Kohdeorganisaation kannalta tämä ei tietenkään ole niin merkittävä tekijä, mikäli aiheeseen puututaan suunnitellusti perehdytyksen, koulutuksen, ohjeistamisen ja tiedottamisen keinoin.

Organisaatiojaon kannalta Hyria Koulutus Oy:n henkilöstön kyberturvallisuustietoisuus oli kautta linjan hieman paremmalla tasolla kuin Hyria säätiön ja Business-palveluiden. Tämä näkyi siinä, kuinka tärkeänä asiat koettiin ja miten kokemus heijastui arjen toimintaan. Ainoa osa-alue, jossa Hyria Koulutus Oy:n henkilöstön toiminta oli heikommalla tasolla, liittyi sähköposteihin, niiden liitteisiin ja linkkeihin. Tämä on mielenkiintoinen havainto sillä Hyria säätiön ja Business-palveluiden henkilöstö on hieman, mutta ei merkittävästi, paremmin koulutettua, ja selkeästi nuorempia. Heistä suurempi osa on määräaikaisessa työsuhteessa ja heidän työsuhteensa on kestänyt vähemmän aikaa kuin Hyria koulutus Oy:n palveluksessa olevien henkilöiden. Kyselyssä ei anonymiteetin säilyttämisen turvaamiseksi eritelty säätiön ja Business-palveluiden henkilöstöä toisistaan.

Esihenkilöt kokivat pääsääntöisesti kyberturvallisuuteen liittyvät asiat tärkeämpinä kuin työntekijät. He olivat saaneet vähemmän perehdytystä tietojärjestelmien tietoturvallisuuteen ja olivat muuta henkilöstöä enemmän sitä mieltä, että aihetta ei ole riittävästi huomioutu organisaation perehdytyksessä. Esihenkilöistä hieman alle kolmannes koki, ettei oma osaaminen ollut riittävällä tasolla ja heistä melkein puolet oli huolissaan työyhteisön muiden jäsenten tietojärjestelmään liittyvästä tietoturvallisuusosaamisesta. Tämä siitäkin huolimatta, että esihenkilöillä oli muuta henkilöstöä selkeästi positiivisempi käsitys organisaation tietoturvallisuuden tasosta. Esihenkilöiden tietoisuuden kokemuksesta huolimatta toiminta ei näkynyt kaikessa arjessa. He esimerkiksi tallensivat salasanoja ja pin-koodeja mobiililaitteiden yhteystietoihin muuta henkilöstöä enemmän ja olivat pohtineet oman kotinsa langattoman tietoverkon tietoturvaa työntekijöitä vähemmän. Suhteessa muuhun henkilöstöön esihenkilöistä huomattavasti suurempi osa vastasi käyttävänsä samoja salasanoja useammassa palvelussa sekä hieman suurempi osa kertoi tallentavansa tiedostoja suoraan työasemalle verkkoaseman sijaan. Tämä on varmasti sellainen asia mihin kannattaa ohjeistuksessa, ja koulutuksissa kiinnittää huomioita, kun ottaa huomioon, että esihenkilöt viettävät työntekijöitä enemmän aikaa työasemalla työskennellen, he käyvät työmatkoilla työasemat mukanaan enemmän sekä heillä on laajemmat pääsyoikeudet useampaan tietojärjestelmään työntekijöihin verrattuna. Pääsääntöisesti yli 16 tuntia viikossa työasemalla työskentelevät ovat paremmin kyberturvallisuustietoisia sekä heidän toimintansa oli kyberturvallisuuden vaatimuksien kannalta toivottavampaa. Tähän ryhmään joidenkin kysymyksien kohdalla toivat poikkeuksen esihenkilöt joista 16 työskenteli yli 20 tuntia viikossa työasemalla. Kuviossa 55 on esimerkkipoikkeama esihenkilöihin liittyen. Heistä lähes yhdeksän kymmenestä vastasi käyttävänsä samaa salasanaa useammassa palvelussa. Kun vähennetään esihenkilöiden osuus, tulee yli 20 tuntia viikossa työskentelevien osalta kyllä ja ei vastausten suhteeksi lähes sama (54 % vs.46 %) kuin 16–20 tuntia viikossa työskentelevillä.



Kuvio 55 Käyttää samaa salasanaa useammassa palvelussa, työajan mukaan (n=252)

Organisaation henkilöstöllä on yleisesti kokemus kyberturvallisuuden tärkeydestä. Tästä osoituksena kyselyn saama suosio. 100 vastaajan raja rikkoutui jo ensimmäisen työpäivän aikana kyselyn avauduttua kyseisen työpäivän aamuna. Tämä siitäkin huolimatta, että yksi haastateltava kertoi, ettei ollut vastannut ensimmäiseen kyselykutsuun johtuen siitä, että johdon assistentin nimissä tulleessa sähköpostissa oli turvallisuusasioiden johtajan viesti ja allekirjoitus. Oman toiminnan tärkeys on siis huomioitu, mutta osaaminen ei ole vielä sellaisella tasolla, että luottamus riittäisi oman arviointikyvyn osalta. Kirjallisuudesta nousi erilaisia tuloksia kyberturvallisuustietoisuudesta tehdyissä tutkimuksissa. Pósa ym. (2022, 491–506) havaitsivat tutkimuksessaan pidemmän opetuskokemuksen ja työsuhteen korreloivan itse asiassa kyberturvallisuustietoisuutta nostavasti. Havainto on yhteneväinen tässä opinnäytetyössä tehdyn tutkimuksen osalta, joskaan ei täysin selvästi. Alammary ym. (2022, 8–9) tekivät päinvastaisen johtopäätöksen omassa tutkimuksessaan. Hyrian henkilöstön vastauksia analysoitaessa iän kautta suodatettuna joidenkin kysymysten kohdalla alle 35-vuotiaiden toiminta oli heikommalla tasolla kuin 35–50-vuotiaiden. Joidenkin osa-alueiden osalta yli 50-vuotiaat olivat hieman paremmin selvillä oikeista toimintamalleista. Nuorin ikäryhmä ja alle 5 vuotta Hyriassa työskennelleet esimerkiksi kokivat vähemmän viimeaikaista tietoturvan tärkeyden lisääntymistä yhteiskunnassa. Syitä voi olla monia. Iän mukanaan tuoma perspektiivi saattaa vaikuttaa ajalliseen kokemukseen. Kysymyksen asettelun sana valinta (viime aikoina) saattaa siten vaikuttaa tulokseen.

Merkittävä huomio kuitenkin on se, että henkilöstöstä lähes neljäkymmentä prosenttia ei ole saanut tietojärjestelmien tietoturvalliseen käyttöön koulutusta Hyriassa. Kolmannes henkilöstöstä ei ollut saanut lainkaan. Koulutukselle siis on selkeästi tarvetta jo numeroita

tarkastellen. Aineistosta nousi toistuvasti esille tarve perehdytykselle, koulutukselle ja toimintaohjeille. Näiden avulla on mahdollista lisätä myös henkilöstön tietoisuutta osaamisen ja aiheen esillä pysymisen kautta. Opiskelijoitaan ja asiakkaitaan henkilöstö ohjeistaa kyberturvalliseen toimintaan jonkin verran. Uusien opiskelijoiden ja asiakkaiden orientaatioihin voisi kehittää sisältöä, jossa opetetaan kyberturvalliset toimintatavat oppilaitoksen toimintaympäristössä. Tässä mallissa henkilöstöstä suuri osa joutuisi perehtymään aiheeseen riittävällä tarkkuudella voidakseen opettaa ja perustella ohjeita opiskelijoille ja asiakkaille. Kyberturvallisuustietoisuuden- ja osaamisen lisäämiseksi olisi tarpeellista kehittää hybridityöhön liittyvää osaamista. Hea ym. (2019, 8) mukaan johdon sitoutumisen lisäksi oikeat toimintamallit, ohjeet ja koulutus lisää henkilöstön kyberturvallisuustietoisuutta.

Nwankpa & Datta (2023, 10–11) mukaan etätyöskentely ei välttämättä muodosta organisaation kyberturvallisuudelle riskiä, mikäli henkilöstön osaaminen, ohjeet ja organisaation toimintamallit ovat kunnossa. Tällä hetkellä merkittävällä osalla Hyrian henkilöstöstä tuntui olevan haasteita tunnistaa turvallinen tietoverkko tai onko kotona käytössä oleva langaton verkko riittävän tietoturvallinen työn tekemistä varten. Aineistosta välittyi kuva henkilöstöstä, joka ei tiennyt kuinka heidän tulisi toimia kyberturvallisuuden kannalta. Koulutuksessa olisi hyvä käydä ne toimintamallit sekä toimenpiteet, joita henkilöstön tulisi noudattaa ja toteuttaa jotta heillä on tieto, kuinka hoitaa oma osuutensa organisaation kyberturvallisuudesta. Epävarmuuden vähentämiseksi olisi hyvä kertoa ne tilanteet, joissa organisaation tietoturvaohjelmistot ja salatut verkkoyhteydet tuovat riittävän suojan. Johtopäätöksenä työskentelyn kyberturvallisuuteen oppilaitoksen ulkopuolella tulee kiinnittää huomiota. Kannettavia työasemia luovutettaessa olisi hyvä kerrata tietoturvallisen etätyöskentelyn ohjeet yhdessä organisaation asiantuntijoiden kanssa. Työasemat olisi hyvä varustaa lähtökohtaisesti etätyön vaatimuksien mukaisesti kuulokkeilla ja tietosuojakalvoilla.

Kuvio 56 Tapaustutkimuksen keskeiset havainnot tiivistetysti

Tehty opinnäytetyö tuloksineen ja kehitysehdotukseen on esitetty toimeksiantajan edustajille, joilta työ on saanut hyvän ja innostuneen palautteen. Turvallisuusasioiden johtajan ja tietojärjestelmistä vastaavan päällikön mukaan tehdyt havainnot ja kehitysehdotukset tulevat huomioiduksi tulevissa kyberturvallisuuden kehittämistoimissa. Kyberturvallisten toimintatapojen ohjeistuksia, perehdytyksiä ja koulutuksia tullaan parantamaan jatkossa kehittämistyön havaintojen perusteella. Tietoturvallisuustaitoja kehittävän verkkokurssin kehittäminen on tällä hetkellä suunnitteluvaiheessa. Opinnäytetyön tekijä on nimetty yhdeksi verkkokurssin tekijöistä.

9 Pohdintaa

Opinnäytetyön suunnitteluvaiheessa työn tekijä teki päätöksen hyödyntää pääsääntöisesti laadullisia tutkimusmenetelmien. Perusteluna oli, että tutkimusaiheesta ja -kohteesta johtuen kyseisen tutkimuksen tulokset eivät olisi yleistettävissä laajemmalti yhteiskuntaan tai edes ammatillisiin oppilaitoksiin. Mikäli olisi valittu tutkittavaksi aiheeksi jokin aihe, jonka jokainen organisaatio kohtaisi samalla tavalla, olisi voitu jotain johtopäätöksiä tehdä. Tutkittaessa asioita, jotka ovat hyvin sidonnaisia organisaation toimintakulttuuriin, perehdytykseen sekä järjestelmiin ei tuloksien osalta yhteiskunnallista yleistettävyyttä voida saavuttaa. Vaikka opinnäytteenä tehtyä kehittämistyötä ja sen kyselyosuutta ei ollut suunniteltu määrällisten tutkimusmenetelmien analyysejä silmällä pitäen oli näistä työkaluista kuitenkin jonkin verran hyötyä. Joidenkin vertailujen kohdalle ne nopeuttivat aineiston analyysiä, nostaen sieltä esiin selkeästi asioita, jotka korreloivat keskenään positiivisesti tai negatiivisesti. Kyselyn rakenne

kuitenkin oli sellainen, että varsinaisesti määrällisiä analyysimenetelmiä pystyi hyödyntämään vain joidenkin kysymysten kohdalle siten, että niistä voisi jotain yleistettävää todeta. Joidenkin aiheiden tulosten osalta lievää yleistettävyyttä voi siis olla havaittavissa. Laajempaan yleistettävyyteen ammatillisten oppilaitosten osalta pyrittäessä olisi tarpeen ollut tutkia useamman oppilaitoksen henkilökunnan kokemuksia.

Opinnäytetyön tekijä työskentelee itse kohdeorganisaatiossa, joten tutkimustyötä tehdessä oli kiinnitettävä huomioita objektiivisuuden säilyttämiseen. Työn tekijän tarkempi ymmärrys kuitenkin rajoittuu yhden koulutusosaston toimintatapoihin ja -kulttuuriin eikä koko organisaation toiminnan tasosta ole sellaista ymmärrystä, jonka perusteella voisi juurikaan hypoteeseja esittää. Tämä näkyi esimerkiksi kyselyn kysymyksien kohdalla siten, että selvitettävät asiat valikoituivat taustateorian perusteella silloinkin kuin tiedossa oli kyseisen toimintamallin oletettu yleisyys tai ohjeistus organisaatiossa. Osa selvitettävistä taustatiedoista valikoitui kyselyyn siitä huolimatta, ettei kohdeorganisaation edustajien mukaan tiedoilla ollut merkitystä. Jälkikäteen tarkasteltuna nämä olivat oikeita ratkaisuja tuoden lisää tietoa käsiteltävästä aihepiiristä sekä ymmärrystä ilmiön luonteesta. Täysin objektiivinen ei varmastikaan voi tutun organisaation kohdalla olla, mutta pyrkimyksenä on ollut hyödyntää organisaation tuntemusta vain joidenkin analyysiin liittyvien tulosten tulkitsemisessa.

Kyselyn kysymyksiä laadittaessa osa ohjaava ajatusta oli kyselyn perehdyttävän ja kouluttavan luonteen hyödyntäminen. Kysely, jossa toimintatapoja selvitetään, herättää vastaajissa ajatuksia jo kysymyksiin vastatessa. Anonyymin kyselyn ja haastatteluiden ansiosta opinnäytetyön tekijälle syntyi vaikutelma rehellisesti annetuista vastuksista eikä tulosten vääristymistä seurausten pelosta johtuen ainakaan tullut ilmi. Yleisen työyhteisössä saadun palautteen, toimeksiantajalta saadun palautteen, kyselyn avoimissa vastauksissa saatujen palautteiden sekä haastatteluissa esiin nousseiden palautteiden perusteella opinnäytetyön aihe todettiin tärkeäksi, kysely hyväksi ja tarpeelliseksi sekä monen vastaajan mielestä jo itsessään osaamista kehittäväksi.

Opinnäytetyön lopputuloksena syntynyt kehittämisehdotus kyberturvallisten toimintamallien mukaan ottamisesta kaikkeen tietojärjestelmiin, tietoteknisiin laitteisiin, ohjelmistoihin tai verkko-oppimisympäristöihin liittyvään perehdytykseen on saanut hyvän vastaanoton toimeksiantajan organisaatiossa. Tutkimuksen esiin nostamat havainnot henkilöstön toiminnan kehityskohteista huomioidaan organisaation kyberturvallisuuskoulutuksissa sekä ohjeistuksissa. Opinnäytetyönä tehty kehittämistyön voidaankin todeta vastaavan toimeksiantajan ja työn tekijän työlle asettamia tavoitteita.

Opinnäytetyön tekijälle työ oli ensimmäinen laatuaan, joten oppimista tapahtui aiheanalyysistä viimeiseen johtopäätökseen ja raportin tarkastettavaksi luovuttamiseen asti. Kyselyn kysymyksien asettelun onnistuminen selvisi vasta analyysivaiheessa. Esimerkiksi ilmaisu, viime

aikoina, osoittautui analyysivaiheessa heikoksi valinnaksi. Tämä ilmaisu ei huomioinut ajallisen kokemuksen perspektiivin vaihtelua kokijan ikäryhmän mukaan. Kyselylomakkeessa kaikkia kysymyksiä ei esitetty jokaisella vastaajalle kyselyn pitämiseksi kohtuullisen pituisena. Käytännössä joidenkin kysymysten vastauksien perusteella avautui tietyn vastausvaihtoehdon valinneille vastaajille uusia kysymyksiä. Tämä oli pääsääntöisesti hyvä toimintamalli, joskin jotkin kysymykset olisi ollut parempi esittää koko vastaajajoukolle. Tämä selvisi vasta aineistoa analysoidessa. Tätä puutetta onnistuttiin paikkaamaan haastatteluvaiheessa. Yksittäisen organisaation osalta kyberturvallisuustietoisuuden kaltaisen ilmiön tutkiminen oli mielenkiintoinen matka organisaation toiminta- ja turvallisuuskulttuuriin. Seuraava askel olisi henkilöstön kyberturvallisuustietoisuuden tutkiminen ammattioppilaitoksissa valtakunnallisesti.

Lähteet

Painetut

Hopkin, P. 2018. Fundamentals of Risk Management. Pondicherry: KoganPage

Kahneman, D. 2012. Thinking, Fast and Slow. Penguin Random House UK.

Limnéll, J., Majewski, K., & Salminen, S. 2014. Kyberturvallisuus. Saarijärvi: Docendo Oy.

Sähköiset

Alammary, A., Alshaik, M. & Pratama, A.R., 2022. Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic. PeerJ Computer Science. Viitattu 12.12.2022. https://www.proquest.com/scholarly-journals/awareness-security-privacy-settings-video/docview/2685808779/se-2

Alasuutari, P. 2011. Laadullinen tutkimus 2.0. E-kirja. Tampere: Vastapaino 2011

Aljohni, W., Elfadil, N., Jarajreh, M. & Gasmelsied, M. 2021. Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. International Journal of Advanced Computer Science and Applications, 12(3) Viitattu 26.11.2022. https://www.proquest.com/scholarly-journals/cybersecurity-awareness-level-case-saudi-arabia/docview/2655119311/se-2

Andronache, A. 2021. Increasing Security Awareness Through Lenses of Cybersecurity Culture. Journal of Information Systems & Operations Management, 15(1), pp. 7-22. Viitattu 31.12.2022. https://www.proquest.com/scholarly-journals/increasing-security-awareness-through-lenses/docview/2571982600/se-2?accountid=12003

Backman, J. & Himanka, J. 2007. Fenomenologia. Helsingin Yliopisto 2007. Viitattu 22.4.2023. https://helda.helsinki.fi/handle/10138/160881

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. E-kirja. Tampere: Vastapaino.

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) Viitattu 16.11.2022. Viitattu 26.12.2022. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679

FINE Vakuutus- ja rahoitusneuvonta 2022. Asiakkaita huijataan verkkopankeilta näyttäville valesivustoille. Viitattu 15.12.2022. https://www.fine.fi/ajankohtaista/2022/asiakkaita-huijataan-verkkopankilta-nayttaville-valesivustoille.html

Harrison, H., Birks, M., Franklin, H. & Mills, J. 2017. Case Study Research: Foundations and Methodological Orientations. Forum Qualitative Sozialforschung Forum: Qualitative Social Research Vol. 18, Viitattu 25.2.2023. https://www.qualitative-research.net/index.php/fqs/article/view/2655

Helsingin Sanomat 2022. Kyber-hyökkäys leikkasi Uponorin liikevaihtoa kymmenillä miljoonilla. Viitattu 20.2.2023. https://www.hs.fi/talous/art-2000009395531.html

Hirsjärvi, S. & Hurme, H. 2015. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. E-kirja. Gaudeamus Oy.

Hyria 2022. Organisaatio. Viitattu 16.11.2022. https://www.hyria.fi/hyria/organisaatio

IAEA 1991. Safety culture. Safety Series 75-INSAG-4. Vienna: IAEA. Viitattu 10.12.2022. https://www-pub.iaea.org/mtcd/publications/pdf/pub882_web.pdf

Ilta-Sanomat 2021. KRP varoittaa ovelasta Omakanta-huijauksesta – toimi näin suojautuaksesi. Viitattu 15.12.2022. https://www.is.fi/digitoday/tietoturva/art-2000008285667.html

ISO/IEC 27001:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki. Suomen standardoimisliitto.

Jyväskylän yliopisto 2015. Menetelmäpolkuja humanisteille. Viitattu 22.4.2023. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/fenomenologinen-tutkimus

Kallinen, T. & Kinnunen, T. 2021.Laadullisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto. Viitattu 17.11.2022. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/

Keuda 2022. Keudaan kohdistunut kyberhyökkäys. Viitattu 10.12.2022. https://www.keuda.fi/2022/12/07/keudaan-kohdistunut-kyberhyokkays/

Keuda 2023. Keudan loppuraportti kyberhyökkäyksestä on valmistunut. Viitattu 13.3.2023. https://www.keuda.fi/2023/03/10/keudan-loppuraportti-kyberhyokkayksesta-on-valmistunut/

Khader, M., Karam, M. & Fares, H. 2021. Cybersecurity Awareness Framework for Academia. Information, 12(10), pp. 417. Viitattu 14.12.2022. https://www.proquest.com/scholarly-journals/cybersecurity-awareness-framework-academia/docview/2584398462/se-2

Kolomoets, E. 2022. Ensuring information security in the field of remote work. Journal of Physics: Conference Series, 2210(1), pp. 012008. Viitattu 12.12.2022. https://www.proquest.com/scholarly-journals/ensuring-information-security-field-remote-work/docview/2645193830/se-2

Laki ammatillisesta koulutuksesta 2017/531 Viitattu 16.11.2022. Viitattu 26.12.2022. https://www.finlex.fi/fi/laki/ajantasa/2017/20170531

Laki yksityisyyden suojasta työelämässä 2004/759 Viitattu 26.12.2022. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Laurea 2019. ECHO - European network of Cybersecurity centres and competence Hub for innovation and Operation. Viitattu 13.11.2022. https://www.laurea.fi/hankkeet/e/echo---european-network-of-cybersecurity-centres-and-competence-hub-for-innovation-and-operations/

Ling, L., Hea, W., Xua, L., Asha, I., Anwarb, M. & Yuanb, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, Volume 45, April 2019, Pages 13-24. Viitattu 26.12.2022. Viitattu 22.5.2023. https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S0268401218302093

Logg, J M. & Tinsley, C H. 2023. Research: How Risky Behaviour Spreads. Harvard Business Review. Viitattu 21.2.2023. https://hbr.org/2023/02/research-how-risky-behavior-spreads

Nwankpa, J K. & Datta, P M. 2023. Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security, Volume 130, 2023. Viitattu 20.5.2023. https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S0167404823001761?via%3Dihub

Oppilas- ja opiskelijahuoltolaki 1287/2013 Viitattu 26.12.2022. https://www.finlex.fi/fi/laki/ajantasa/2013/20131287

Poliisi 2022. Poliisi jatkaa Savonia-ammattikorkeakouluun kohdistuneen tietomurron tutkintaa. Viitattu 12.11.2022. https://poliisi.fi/-/poliisi-jatkaa-savonia-ammattikorkeakouluun-kohdistununeen-tietomurron-tutkintaa

Pósa, T. & Grossklags, J. 2022. Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students. Journal of Cybersecurity and Privacy, 2(3), pp. 490. Viitattu 13.12.2022. https://www.proquest.com/scholarly-journals/work-experience-as-factor-cyber-security-risk/docview/2716552025/se-2

Puusa, A. & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. E-kirja. Gaudeamus Oy.

Pöyhönen, J., Nuojua, V., Lehto, M. & Rajamäki, J. 2019, "Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations", Information & Security, vol. 43, no. 1, pp. 236-256. https://www.researchgate.net/publication/335995107_Cyber_Situational_Awareness_and_Information_Sharing_in_Critical_Infrastructure_Organizations

Ramlo, S. & Nicholas, J.B. 2021. The human factor: assessing individuals' perceptions related to cybersecurity. Information and Computer Security, 29(2), pp. 350–364. Viitattu 26.11.2022 ja 13.12.2022. https://www.proquest.com/scholarly-journals/human-factor-assessing-individuals-perceptions/docview/2557138292/se-2?accountid=12003

Reiman, T., Pietikäinen, P. & Oedewald, P. 2008. Turvallisuuskulttuuri – Teoria ja arviointi. 2008. VTT Publications. Viitattu 10.12.2022. https://www.vttresearch.com/sites/default/files/pdf/publications/2008/P700.pdf

Remes, M. 2022. Poliisi on keskeyttänyt Savonia-ammattikorkeakoulun tietomurron tutkinnan – henkilötietoja vietiin helmikuussa noin 700 opiskelijalta. YLE Uutiset 2022. Viitattu 12.11.2022. https://yle.fi/uutiset/3-12442864

Rikoslaki 1889/39 Viitattu 26.12.2022. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Ruoslahti, H., Coburn, J., Trent, A. & Tikanmäki, I. 2021. Cyber Skills Gaps – A Systematic Review of the Academic Literature. Connections: The Quarterly Journal, 20(2), pp. 33–45. Viitattu 26.11.2022 https://www.proquest.com/scholarly-journals/cyber-skills-gaps-systematic-review-academic/docview/2654407696/se-2?accountid=12003

Rytkönen, A-P. 2022. Tietomurrossa uusi käänne: Savonian opiskelijoiden tietoja julkaistiin Tor-verkossa. YLE Uutiset 2022. Viitattu 12.11.2022 https://yle.fi/uutiset/3-12319469

SFS-EN ISO/IEC 27000:2020 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki. Suomen Standardoimisliitto.

SFS-EN ISO 22301:2019 Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset. Helsinki. Suomen Standardoimisliitto.

Sulaiman, N.S., Muhammad, A.F., Hussain, S. and Wider, W., 2022. Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, 13(9), pp. 413. Viitattu 27.12.2022. https://www.proquest.com/scholarly-journals/cybersecurity-behavior-among-government-employees/docview/2716552017/se-2

Tietosuojalaki 2018/1050 Viitattu 26.12.2022. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Varbanov, P. 2021. D2.6 ECHO CYBERSKILLS FRAMEWORK. Viitattu 13.11.2022. https://ec-honetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf

Vesterinen, P. 2021. Pidä yritystiedot turvassa! Helsingin seudun kauppakamari. Viitattu 25.11.2022. https://view.taiqa.com/helsinki.chamber/yritysturvallisuus-pida-yritystiedot-turvassa

Vesterinen, P. & Korslow, P. 2022. Yrityksiin kohdistuvat kyberuhat. Helsingin Seudun Kauppakamari. Viitattu 24.11.2022. https://view.taiqa.com/helsinki.chamber/yrityksiin-kohdistuvat-kyberuhat--selvitys-2022#/page=1

Valli, R. 2018. Ikkunoita tutkimusmetodeihin. 5.painos. E-kirja. Jyväskylä: PS-kustannus 2018

Vilkka, H. 2021. Tutki ja kehitä. E-kirja. Jyväskylä: PS-kustannus 2021

YLE 2023. Vaasassa Wilmasta vuosi 50 oppilaan henkilötiedot, eikä kyseessä ole ensimmäinen tietoturvaloukkaus – kehittäjä kiistää tietosuojariskin. Viitattu 20.2.2023. https://yle.fi/a/74-20018090

Julkaisemattomat

Hyria koulutus Oy 2023. Tasa-arvo ja yhdenvertaisuussuunnitelma 2023. Hyrian intranet

Kymäläinen, M. 2023. Turvallisuusasioiden johtajan haastattelu 31.1.2023. Hyria. Teams-haastattelu.

Lehtinen, J. 2023. ICT-päällikön haastattelu 27.1.2023. Hyria. Teams-haastattelu.

Kuviot

Taulukot

Liitteet

Liite 1: Tutkimuslupa

Hyria
Hyria koulutus Oy
toimitusjohtaja

Päätös
19.1.2023

1 / 1
VaiPek / A 4 / 2023

Tutkimusluvan myöntäminen / Ammatillisen oppilaitoksen henkilöstön kyberturvallisuustietoisuus oppilaitoksen arjessa

Laurea ammattikorkeakoulussa turvallisuusjohtamisen koulutusohjelmassa (YAMK) tutkintoa suorittava ja opinnäytetyötä tekevä tekevä Sami Kiiskinen pyytää lupaa tutkia Hyrian henkilöstön kyberturvallisuustietoisuuden tasoa.

Tutkimuksen aineistonkeruumenetelmänä ovat verkkokysely henkilöstölle ja haastattelut vapaaehtoisille henkilöstöön kuuluville. Tutkimus toteutetaan kevään 2023 aikana.

Päätös

Koska tehtävä tutkimus tukee Hyrian kyberturvallisuuden suunnittelun kehittämistä sekä ko. koulutuksen kohdentamista henkilöstölle paremmin, päätän myöntää Sami Kiiskiselle tutkimusluvan oheisen tutkimuslupahakemuksen mukaisesti.

Pekka Vaittinen
toimitusjohtaja

Liitteet

Tutkimuslupahakemus

Tiedoksi

Sami Kiiskinen
Laurea / Hanna-Miina Sihvonen
Hyria / hallitus, johtoryhmä, turvallisuusasioiden johtaja Matti Kymäläinen, turvallisuusalan koulutuspäällikkö Mikko Rasimus, ICT-järjestelmäpäällikkö Janne Lehtinen

SÄHKÖISESTI ALLEKIRJOITETTU
Vaittinen Pekka, Toimitusjohtaja/johtava rehtori 22.1.2023 17:39

Liite 2: Kyselyn saatekirje

Tervehdys Hyrian heimon jäsen,

Opiskelen Laurea ammattikorkeakoulussa turvallisuusjohtamisen koulutusohjelmassa (ylempi AMK). Opinnäytetyössäni tutkin tietojärjestelmien tietoturvallista käyttöä. Tämän johdosta toivotan sinut tervetulleeksi osallistumaan Hyrian henkilöstölle suunnattuun, tietojärjestelmien turvalliseen käyttöön liittyviä toimintatapoja ja tietoisuutta selvittävään kyselytutkimukseen. Tutkimuksen tuloksia tullaan hyödyntämään Hyrian tietoturvallisuuden kehittämisessä.

Kyselyyn vastaaminen vie aikaa noin 10 minuuttia. Luethan kysymykset huolellisesti. Valitse sen jälkeen tilannettasi parhaiten kuvaava vastausvaihtoehto. Vastausaikaa on 14.3.2023 (mukaan lukien) asti.

Linkki kyselyyn

Tutkimukseen liittyen tarkoitus on haastatella joitakin vapaaehtoisia. Teams:issa toteutettava haastattelu kestää noin 30 minuuttia. Haastattelut toteutetaan maaliskuun puolesta välistä alkaen. Mikäli haluat osallistua tutkimukseen, ja näin tukea Hyrian turvallisuuskulttuurin kehittämistä, voit ilmoittautua haastatteluun kyselyn lopussa olevan linkin kautta tai tästä.

Tutkimukselle on myönnetty tutkimuslupa VaiPek / A 4 / 2023

Aikaasi ja panostasi arvostaen,

Sami kiiskinen

Turvallisuusala

040 673 2272

sami.kiiskinen@hyria.fi

Liite 3: Kysymyslomake

Tietoturvallisuuskysely

☐ Pakolliset kysymykset merkitty tähdellä (*)

Tämän kyselytutkimuksen tarkoitus on selvittää tietoturvallisuustietoisuutta. Kysely muodostuu kolmesta osa-alueesta:

- taustatiedot
- ajatukset tietoturvallisuudesta yleisesti
- työhön liittyvä toiminta

Luethan kysymykset huolellisesti. Valitse sen jälkeen mielestäsi parhaiten kuvaava vastausvaihtoehto. Kaikkiin kysymyksiin tulee vastata, jotta voit siirtyä seuraavalle sivulle.

Taustatiedot

1. Olen*

- ○ Mies
- ○ Nainen
- ○ En halua vastata

2. Ikä *

- alle 35vuotiaat
- 35–50-vuotiaat
- yli 50-vuotiaat

3. Ylin koulutusaste

- Lukio, ammatillinen koulutus, erikoisammattitutkinto tai opistoaste
- Alempi korkeakoulututkinto
- Ylempi korkeakoulututkinto tai jatkotutkinto

4. Työskentelen *

- Hyria Koulutus Oy
- Hyria säätiö tai Hyria Business-palvelut

5. Työsuhdemuoto *

- Kokoaikainen toistaiseksi voimassa oleva
- Osa-aikainen toistaiseksi voimassa oleva
- Kokoaikainen määräaikainen
- Osa-aikainen määräaikainen
- Joku muu _____

6. Työtehtävä *

- Opetushenkilöstö (opettajat, kouluttajat, ohjaajat)
- Muu henkilöstö (muut kuin edellisessä vaihtoehdossa mainitut)

7. Toimin *

- Työntekijänä
- Esihenkilönä

8. Työsuhteeni pituus Hyriassa *

- ○ alle 5 vuotta
- ○ 5–10 vuotta
- ○ 11–15 vuotta
- ○ yli 15 vuotta

Seuraavat kysymykset koskevat yleisesti ajatuksia tietoturvallisuuteen liittyen

9. Kokemukseni mukaan viime aikoina tietoturvallisuuden merkitys yhteiskunnassa on lisääntynyt *

- ○ Erittäin paljon
- ○ Paljon
- ○ Jonkin verran
- ○ Vähän
- ○ Ei lainkaan
- ○ Joku muu _____

10. Arvioi seuraavien asioiden merkitys tietoturvallisuuden kannalta. 1 = ei merkityksellinen, 5 =erittäin merkityksellinen. *

	1	2	3	4	5
Ovet ja lukitukset	○	○	○	○	○
Työasemat	○	○	○	○	○
Älypuhelin	○	○	○	○	○
Kulunvalvontajärjestelmät	○	○	○	○	○
Kuvallisen henkilökortin esillä pitäminen	○	○	○	○	○
Salasanat	○	○	○	○	○
Murtohälytysjärjestelmät	○	○	○	○	○
Oma toimintani	○	○	○	○	○
Älykellot	○	○	○	○	○
Tabletit ja padit	○	○	○	○	○

	1	2	3	4	5
Älytelevisiot	○	○	○	○	○
Kannettavat tietokoneet	○	○	○	○	○
Älykaiutin	○	○	○	○	○

11. Olen tallentanut mobiililaitteen (älypuhelin/kännykkä) yhteystietoihin salasanoja, pin-koodeja, tunnuslukuja tai muita vastaavia tietoja. *

○ Kyllä

○ En

12. Olen tietoinen, että annettuani mobiililaitteeseen asennetulle sovellukselle (Facebook, Whatsapp, Instagram tms.) pääsyn laitteen yhteystietoihin, tulen antaneeksi pääsyn myös yhteystiedoissani olevien henkilöiden kaikkiin osoitekirjassa oleviin tietoihin. Tämä koskee myös sinne mahdollisesti tallentamiani koodeja ja salasanoja. *

○ Kyllä olen tietoinen

○ En ollut tietoinen

13. Olen käyttänyt Googlen tai muun vastaavan palveluntarjoajan verkossa olevaa ilmaista käännöspalvelua tai ChatGPT tyyppistä tekoälypalvelua. *

○ Kyllä

○ En

14. Jatkoa edelliseen kysymykseen: Näin tehdessäni olen huomioinut tietosuojan, sekä sen, että kyseiseen palveluun kopioitua tietoa voidaan käyttää johonkin muuhun tarkoitukseen. Lisäksi palveluun syötetyt tiedot voivat olla yhdistettävissä minuun ja työnantajaani. *

○ Kyllä olen huomioinut

○ En ole huomioinut

15. Huomioitko tietoturvallisuuteen liittyviä asioita omassa elämässäsi työn ulkopuolella? *

- Usein
- Joskus
- En lainkaan

16. Minulla on omassa henkilökohtaisesti omistamassani mobiililaitteessa jonkinlainen erikseen hankittu tietoturvaohjelmisto (virusturva, vpn). *

- Kyllä
- Ei

17. Olen pohtinut kodissani käytössä olevan langattoman verkon tietoturvaa. *

- Olen pohtinut
- En ole pohtinut

18. Minulla on käytössä sama salasana useammassa kuin yhdessä palvelussa, sovelluksessa tai verkkosivustolla. *

- Kyllä
- Ei

19. Saadessani linkkejä sisältäviä viestejä (mihin tahansa sovellukseen tai palveluun), pyrin varmistumaan viestin ja lähettäjän oikeellisuudesta. *

- Aina
- Usein
- Jos ehdin
- Harvoin
- En koskaan

20. Pääsääntöisesti menen internetissä verkkosivulle
*

- Googlen tai muun hakupalvelun kautta
- Kirjoitan sivuston osoitteen selaimen osoitekenttään
- Käytän vain tuttuja sivustoja, joiden osoitteen olen tallentanut verkkoselaimen

suosikkeihin
Joku muu tapa

21. Saadessani liitetiedostoja sähköpostiin tai muuhun palveluun (sosiaalisen median palvelut), pyrin varmistamaan, että lähettäjä on oikea tai muuten tuttu.*

Aina
Usein
Harvoin
En lainkaan

22. Luotettavalta lähettäjältä saatu linkki tai liitetiedosto on aina turvallinen. *

Kyllä
Ei
En osaa sanoa

23. Luotettavan sähköpostin tunnistaa (valitse mielestäsi paras vaihtoehto).

Hyvästä suomen kielestä
Lähettäjän nimi on tuttu
Sähköpostiosoite on tuttu
Aihe on oikea
Yrityksen logot näyttävät oikealta
Viestin ulkoasu on siisti
Jokin muu

24. Miten tunnistan suojatun verkkosivun osoitteen?

Verkkosivun osoite alkaa https://
Verkkosivun osoite alkaa http://
En osaa sanoa
Joku muu tapa

25. Jos työnantajan kautta saisi alennetulla hinnalla haittaohjelmien torjuntaan ja verkkoyhteyden suojaamiseen soveltuvan ohjelmiston, olisin valmis asentamaan ja käyttämään kyseistä sovellusta omissa henkilökohtaisissakin laitteissani (työasemat, älypuhelin, tabletit)? *

- ○ Kyllä
- ○ En
- ○ En osaa sanoa

Työtehtäviin liittyvää tietoturvallisuutta koskevat kysymykset

26. Työviikon aikana, työtehtävissäni (pl. esitystekniikka opetustilanteessa), käytän tietoteknisiä järjestelmiä (työasemat, mobiililaitteet) keskimäärin *

- ○ alle 5 tuntia
- ○ 5–10 tuntia
- ○ 11–15 tuntia
- ○ 16–20 tuntia
- ○ yli 20 tuntia

27. Olen saanut Hyriassa tai/ja muualla koulutusta tietojärjestelmien ja -laitteiden tietoturvallisesta käytöstä. *

- ○ Kyllä
- ○ En

28. Missä olen saanut edellisessä kysymyksessä mainittua koulutusta? *

- ○ Hyriassa
- ○ Muualla
- ○ Hyriassa ja muualla

29. Hyriassa saamassani perehdytyksessä on mielestäni huomioitu riittävästi tietojärjestelmien (mukaan lukien työasemat ja älypuhelimet) tietoturvallinen käyttö. *

- Kyllä
- Ei
- En osaa sanoa
- Joku muu

30. Toimiakseni työtehtävissäni tietoturvallisesti koen, että tietoni ja taitoni ovat riittävällä tasolla. *

- Kyllä
- Ei

31. Koen kaipaavani lisää aiheeseen liittyvää koulutusta. *

- Kyllä koen
- En koe

32. Minkälaista koulutusta koet tarvitsevasi? *

- Verkkokurssi olisi soveltuvin
- Läsnäolo-opetusta tietokoneluokassa tai vastaavassa
- Yhdistelmä verkko- ja läsnäolo-opetusta
- Omaehtoista opiskelua
- Osana työhöni liittyvää perehdytystä
- Joku muu tapa

33. Työskennellessäni etänä kotitoimistolla, työasemani kanssa samaan tietoverkkoon on yhdistettynä laite tai laitteita, joiden tietoturvasta tai ohjelmistojen päivityksen ajantasaisuudesta en ole varma. *

- Kyllä
- Ei

34. Kotini langatonta verkkoa (jota käytän myös työkäytössäni olevalla työasemalla), käyttävät muutkin henkilöt. *

- ○ Kyllä
- ○ Ei

35. Olen huomioinut tämän mahdollisen vaikutuksen verkkoni tietoturvallisuudelle. *

- ○ Kyllä
- ○ En

36. Käytän työkonettani välillä muiden henkilöiden kanssa samanaikaisesti, tai lainaan työasemani hetkeksi toisen henkilön käyttöön? *

- ○ Kyllä
- ○ En

37. Käytän yhteisesti omia tunnuksiani ja salasanojani työkavereiden ja/tai opiskelijoiden kanssa. *

- ○ Usein
- ○ Joskus
- ○ Harvoin
- ○ En koskaan

38. Muistan lukita henkilökohtaisessa työkäytössä olevan työasemani, kun poistun koneen läheisyydestä. *

- ○ Aina
- ○ Usein
- ○ Harvoin
- ○ En lainkaan vaan luotan automaattiseen lukitukseen

39. Kun käyn messuilla tai työmatkoilla, otan mukaani henkilökohtaisessa työkäytössä olevan, työnantajan omistaman kannettavan tietokoneen. *

- ○ Kyllä
- ○ En

- ○ En, otan erikseen tätä käyttöä varten hankitun työaseman
- ○ Työtehtäviini ei kuulu työmatkoja tai messuja

40. Käytän työhöni liittyen ulkoisia kovalevyjä ja/tai usb-muistitikkuja tiedostojen siirtämiseen ja säilyttämiseen.*

- ○ Kyllä
- ○ En

41. Jatkoa edelliselle kysymykselle: Olen huomioinut tietosuojan näin tehdessäni. *

- ○ Kyllä
- ○ En

42. Käytän samaa usb-muistitikkua ja/tai kovalevyä myös muissa, kuin työnantajan hallinnoimissa laitteissa.*

- ○ Kyllä
- ○ En

43. Olen tietoinen, että usb-muistitikulla olevat tiedostot on mahdollista salata, jolloin sen päätyessä vääriin käsiin tiedostoja ei voi avata ilman salasanaa.

- ○ Kyllä
- ○ En

44. Minulla on tapana tallentaa tiedostoja suoraan työasemalla (muualle kuin verkkokansioon tai OneDriveen).*

- ○ Säännöllisesti
- ○ Joskus
- ○ Harvoin
- ○ Ei lainkaan

45. Voin yhdistää työkoneeni mihin tahansa julkisella paikalla käytössä olevaan langattomaan (wifi/wlan) verkkoon ilman, että tietoturvani vaarantuu? *

- Kyllä
- En
- En osaa sanoa

46. Joudun työssäni lähettämään ja vastaanottamaan liitetiedostoja *

- Usein
- Joskus
- Harvoin
- En lainkaan

47. Mikäli saan työsähköpostiini viestin jostain muusta, kuin itselleni tutun organisaation sähköpostista, varmistan ensin mistä on kysymys, ennen kuin avaan viestin?*

- Aina
- Usein
- Harvoin
- En lainkaan

48. Osaan salata työhöni liittyvät sähköpostit tarvittaessa?*

- Kyllä
- En

49. Tiedän missä tilanteessa työhöni liittyvä sähköposti tulee salata? *

- Kyllä
- En

50. Tiedostan, että edelleen lähettämällä (viestin välittäminen) saatan tulla lähettäneeksi eteenpäin tietoja, joita viestin alkuperäinen lähettäjä ei ole

tarkoittanut eteenpäin jaettavaksi. *

- Kyllä
- En

51. Opastaessani opiskelijoita tai aakkaita uusien tietojärjestelmien käytössä, huomioin myös tietoturvalliset toimintatavat. *

- Aina
- Usein
- Harvoin
- En lainkaan
- En opasta opiskelijoita työtehtävissäni

52. Minulta on Hyriassa työskentelyn aikana yritetty urkkia tietoturvallisuuden ja tietosuojan kannalta tärkeitä asioita. *

- Kyllä
- Ei
- En ole varma
- En tunnista mitkä tiedot kuuluvat kysymyksessä mainittuun kategoriaan

53. Mikäli joutuisin tällaisen urkinnan kohteeksi, tiedän, miten minun tulee toimia. *

- Kyllä
- En
- En ole varma

54. Yleisesti koen, että työyhteisössäni tietojärjestelmiin liittyvä tietoturvallisuusosaaminen on hyvällä tasolla. *

- Samaa mieltä
- Eri mieltä
- En osaa sanoa

55. Koen huolta työyhteisöni muiden työntekijöiden tietoturvallisuusosaamisesta. *

- ◯ Kyllä
- ◯ En

56. Mitä muita ajatuksia ja havaintoja tämä aihealue sinussa herätti?

Tarkoituksena on haastatella joitakin vapaaehtoisia kyselystä nousevien ilmiöiden lähempää tarkastelua varten. Osallistumalla haastatteluun pääset tuomaan esille havaintojasi tähän aiheeseen liittyen. Haastattelun muistiinpanot käsitellään anonyymisti eikä niitä yhdistetä haastateltuun henkilöön. Haastattelu tapahtuu Teams:in välityksellä ja vie noin 30 minuuttia.

Painettuasi Lähetä painiketta, vastauksesi tallennetaan. Seuraavalla sivulla on linkki haastatteluun ilmoittautumista varten.

Liite 4: Teemahaastattelu

Taustatiedot:
Koulutustausta:
Työkokemus Hyriassa:
Tehtävä: opetushenkilöstö / muu henkilöstö
Teema 1: Millainen on henkilöstön kyberturvallisuustietoisuus?
Miten kokee oman tietojärjestelmiin liittyvän tietoturvallisuusosaamisen?
Näkyykö tutkimuksen esiin nostama ilmiö työyhteisössä? Verkkosivuille googlen kautta? Luotto omiin kykyihin, mutta vahva tarve lisäkoulutukselle?
2/3 Kertoi käyttävänsä samaa salasanaa useammassa kuin yhdessä palvelussa. Miten kokee tämän näkyvän henkilöstön tietoisuudessa? Mistä uskoo tämän toimintatavan johtuvan? Tärkeät / vähemmän tärkeät.
Miten henkilöstön tietoisuus näkyy mobiililaitteiden käytössä? Esimerkiksi applikaatioiden osalta. Tuleeko päätöksiä olla lataamatta, jos vaatii liikaa oikeuksia?
Teema 2: Miten kyberturvallisuustietoisuus näkyy arjessa?
Kuinka tietojärjestelmien tietoturvallisuus näkyy työyhteisössä?
Minkälainen tietoturvallisuuden taso mielestäsi työyhteisössäsi on? 58 % oli sitä mieltä, että hyvällä tasolla 37 % koki huolta muiden työntekijöiden tietoturvallisuusosaamisesta
Miten kannettavien työasemien käyttö oppilaitoksen ulkopuolella on ohjeistettu?
Näkyykö tutkimuksen esiin nostamat ilmiöt työyhteisössä: Käytetäänkö sähköpostien salausta? Ohjeistus? Miten usb-muistitikkujen käyttöä näkyy työyhteisössä? Ohjeistus? Koneinen yhteiskäyttöä samoilla tunnuksilla?
Onko etätyön asettamat tietoturvallisuuden haasteet huomioitu ohjeistuksessa?
Onko havainnut nykyistä suurempaa tarvetta turvasähköposteille?
Onko havainnut tietotuvallisuuteen liittyviä puutteita?
Kokeeko, että esihenkilö ottaa tietoturvallisuuteen liittyvät huolet vakavasti?
Onko havainnut ovien lukitsemisen käytäntöihin liittyen parannettavaa?
Onko työyhteisössä kukaan joutunut urkinnan kohteeksi? Onko osaamista tunnistamiseen?
Teema 3 Miten henkilöstön tietoisuutta voidaan kehittää?
Onko Hyriassa ollut tarpeeksi koulutusta aiheeseen liittyen? Minkä tyyppistä koulutusta? Miten koulutus on toteutettu?
Mitä kehitettävää henkilöstön tietoturvallisuustietoisuudessa olisi?
Miten henkilöstön tietoisuutta voidaan kehittää? Minkälaista koulutusta haluaisi? Haluaako osaamisen seurantaa? Kuinka usein tällaista tarvitaan? Sopisiko tällainen aihe henkilöstöpäivään?
Mitä muuta aiheesta haluaa sanoa?