jamk

Jyväskylän ammattikorkeakoulun harjoittelun suorittaneiden terveydenhuollon opiskelijoiden käsityksiä tietoturvasta

Otto Karppinen

Opinnäytetyö, AMK
Toukokuu 2022
Tekniikan ala
Tieto- ja viestintätekniikka, insinööri (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Karppinen, Otto

Jyväskylän ammattikorkeakoulun harjoittelun suorittaneiden terveydenhuollon opiskelijoiden käsityksiä tietoturvasta

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu, 2022, 40 sivua.

Kyberturvallisuus, Tieto- ja viestintätekniikka, Opinnäytetyö AMK

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Digitalisaation ja informaatioteknologian nopea kehittyminen on muokannut maailmasta verkostoituneen yhteisön. Sille on asetettu suuret odotukset ihmisen mm. vuorovaikutuksen lisääjänä, työtehokkuuden optimointia sekä terveyden ja hyvinvoinnin edistäjänä. Monista hyödyistään huolimatta teknologian edistyminen on tuonut mukanaan isomman verkkorikollisuuden aallon. Mitä enemmän maailmassa digitalisoidaan asioita, sitä enemmän kaikki muut turvallisuuden osa-alueet ovat yhteydessä kyberturvallisuuteen. Osa-alueista haavoittuvimpia on ihmisten oma käyttäytyminen tietoturvan kokonaisuudessa. Terveydenhuoltosektori on tämän hetken yksi hyökätyimmistä aloista. Tavoitteena ei ole tehdä järjestelmistä täydellisiä vaan ihmisistä kokonaisvaltaisesti osaavampia tietoturvallisuuden parissa.

Tutkimus toteutettiin harjoittelun suorittaneiden terveydenhuollon opiskelijoiden tietoturvallisuuden osaamisesta. Tavoiteltiin tietoa tietoturvaosaamisen nykytasosta ja tunnistaa eroavaisuuksia opiskelijoihin, jotka ei vielä harjoittelua olleet suorittaneet. Haluttiin myös etsiä keskeisiä kehityskohteita, joita kouluttamisella voitaisiin parantaa. Työ tehtiin sähköisellä kyselyalustalla, joka lähetettiin opiskelijoille ja kerättiin vastauksista analysoitava materiaali. Tutkimuksen tekeminen kyselyllä mahdollisti tutkimuksen tavoitteisiin pääsemisen ja tutkimuskysymyksiin vastaamisen.

Tulokseksi saatiin keskeisiä keinoja, joilla tietoturvallisuutta voidaan parantaa terveydenhuollon opiskelijoiden keskuudessa. Vastausten perusteella moni käyttää omia laitteita työasioiden hoitoon, joka on aina turvallisuus riski yritykselle. Havainnoitiin selkeää eroavaisuutta itseluottamuksessa tietoturvaan liittyvissä asioissa harjoittelun tehneiden ja harjoittelua vaille olevien kohderyhmien välillä. Harjoittelun tehneet kokivat enemmän epäilystä omasta ja vertaistensa tietoturvaosaamisessa. Kolmanneksi kyselyssä raportoitiin tärkeistä harjoittelun tietoturvaa parantavista seikoista. Kuten fyysisen ympäristön turvallisuus sekä tietosuojaosaamisen parantamisen keinot nähtiin suurimmiksi kehityskohteiksi. Lähdettiin käsittelemään kysymyksiä eri näkökulmasta ja tekemään johtopäätöksiä vastauksista. On mahdollista, että omia laitteita käytetään esimerkiksi sähköpostien vastaamiseen. Myös työolosuhteiden muutokset voivat vaikuttaa harjoittelijoiden yleiseen tietoturvaosaamiseen.

Avainsanat (asiasanat)

Tietoturva, digitalisaatio, kyselytutkimus, opiskelija, tietosuoja

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Karppinen Otto

Perceptions of information security among health care students who have completed an internship at Jyvaskyla University of Applied Sciences

Jyvaskyla: JAMK University of Applied Sciences, May 2022, 40 pages

Engineering and technology. Degree Program in Information and communication technology. Bachelor´s thesis.

Permission for open access publication: yes

Language of publication: Finnish

Abstract

The rapid development of digitalisation and information technology has transformed the world into a networked community. High expectations have been set for it, especially in promotion of health and well-being. Despite its many benefits, advances in technology have brought with it a larger wave of cybercrime. The more things are digitised in the world, the more all other aspects of security are linked to cybersecurity. The most vulnerable of these areas is people's own behaviour in terms of information security as a whole. The health care sector is currently one of the most attacked sectors. The goal is not to make the systems completely secure however, to make people more competent in information security.

A study was conducted on the information security skills of health care students who completed the internship. The aim was to find out about the current level of information security skills and to identify differences for students who had not yet done an internship. There was also a desire to look for key areas for development that could be improved through training. The work was done on an electronic questionnaire, which was sent to the students and the material to be analysed was collected from the answers. Conducting a survey with a survey made it possible to reach the objectives of the survey and answer the research questions.

As a result there were key ways to improve information security among health care students. Based on the answers, many use their own equipment to handle work matters, which is always a security risk for the company. There was a clear difference in self-confidence between the target groups who had practised in matters related to information security and those who did not. Those who did the internship felt more doubt about their own and their peers' security skills. The survey reported important aspects of improving the security of internships. Such as the security of the physical environment and the means to improve data protection expertise were seen as major areas for development. We started to address the questions from a different perspective and draw conclusions from the answers. It is possible that your own devices are used, for example, to reply to emails from home. Changes in working conditions can also affect trainees' general security skills.

Keywords/tags (subjects)

Information security, digitisation, survey research, student, data protection

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Termit ja lyhenteet

AMK ammattikorkeakoulututkinto

CIA-triad Confidentiality Integrity Availability

EU European Union

GDPR General Data Protection Regulation

IoT Internet of Things

IP Internet Protocol

ICT Information and Communication Technology

IT Information Technology

JAMK Jyväskylä University of Applied Sciences

VPN Virtual Private Network

WLAN Wireless Local Area Network

WIFI IEEE 802.11

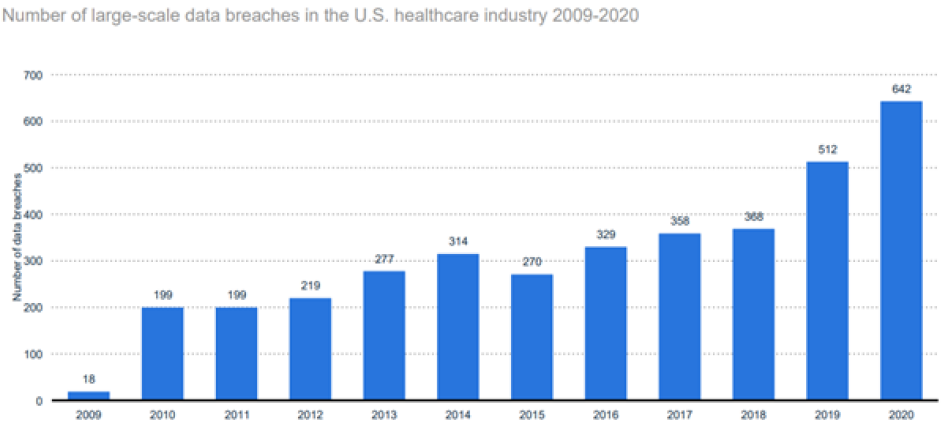
YAMK ylempi ammattikorkeakoulututkinto

1 Johdanto

Kyberturvallisuus on noussut maailmalla kasvavaksi huolenaiheeksi yhteiskunnan digitalisoitumisen myötä. Myös suomessa yhteiskunta digitalisoituu vauhdilla, joka aiheuttaa kasvavan resurssipulan alan osaajista. (Susi 2021). Kybertoimintaympäristöstä on tullut osa jokaisen kansalaisen elämää ja kuka tahansa voi joutua kyberongelmiin. Xetnet (2021) määrittelee kyberturvallisuuden opetuksen ja osaamisen puutteen korkeimmaksi kyberuhaksi yrityksille.

Opinnäytetyössä käsitellään Jyväskylän ammattikorkeakoulun harjoittelun suorittaneiden sosiaali- terveysalan opiskelijoiden tietoturvaosaamista. Aihe on ajankohtainen ei vain maailmalla mutta myös Suomessa kasvavien tietoturvamurtojen aikakautena. (Huusko 2020). Mattila, Ali-Yrkkö ja Seppälä (2020) määrittelee tietovuotojen tuottavan kotimaisille yrityksille tavattoman paljon haasteita. Vaikka suomessa ollaan kyberturvallisuudessa Euroopan keskitasoa korkeammassa asemassa. On suomi jäämässä kehityksessä lukuisilla muilla mittareilla jälkeen, kun verrataan muiden pohjoismaiden kehitystä. Kailio (2021) täsmentää että EU:n tietosuoja-asetuksen voimaantulosta lähtien on yrityksillä ollut pakollista ilmoittaa kaikista tietovuodoista. Etenkin terveydenhuolto- ja rahoitusalojen sektoreilta raportoidaan eniten tietoturvaloukkauksia.

Rikolliset ovat siirtäneet huomiotaan finanssialasta terveydenhuoltoon sen sisältämien henkilötietojen ja arkaluonteisen datan vuoksi. Potilastietojen taloudellinen merkitys voi olla jopa suurempi kuin luottokorttitiedot, lisäksi niistä rikolliset voivat saada jopa paremmalla todennäköisyydellä lunnaita ja niillä on helpompi kiristää. Terveydenhuoltoon lisääntyvää rikollisuutta voi osittain selittää myös se, miten sitä pidetään heikosti kyberhyökkäyksiin varautuneena eli ns. ”pehmeänä” kohteena. Yleisesti ottaen organisaatiot käyttävät IT-kustannuksistaan 5–15 % kybertuvallisuuteen, kun taas sosiaaliterveysalalla kustannukset ovat noin 3 % luokkaa. (Martti 2019)



Kuvio 1. Yhdysvalloissa yli 500 asiakirjan tietovuoto terveydenhuollossa vuosilta 2009–2020 (Johnson 2021)

JAMK:n blogi (2021) korostaa että kyberturvallisuusosaamista olisi hyvä lisätä semmoisilla toimialoilla, joiden ydinosaamista se ei luonnostaan ole. Terveydenhuoltoalan sektorilla kasvavien tietovuotojen määrä viime vuosien aikana Yhdysvalloissa (ks. kuvio 1). Koronakriisin aikana lisääntyneistä tietojenkalastelu ja kiristyshaittaohjelmista hyökkäyksistä on kohdistunut merkittävästi myös terveydenhuoltoon.

2 Tietoperusta

Kyberturvallisuutta ja tietoturvaa ylläpidetään lukuisten eri tietoteknisten toimenpiteiden, kuten palomuurien, salausten ja virustorjuntaohjelmistojen avulla. Tärkeämpää on kuitenkin se, miten ihminen on tässä kokonaisuudessa heikoin lenkki. Lehto, M ja muut toteavat että, työntekijöiden piittaamattomuus tai puolihuolimaton suhtautuminen tietoturvaan ja lisääntynyt sosiaalisen manipuloinnin (engl. Social engineering) keinot ovat keskeisin kyberhyökkäyksien myötävaikuttava tekijä. Maailmalla ja suomessa on uutisoitu hyökkäyksistä terveydenhuoltoon kohdistuneista kyberhyökkäyksistä koronakriisin ajan, tätä myöten rikollisuus terveydenhuoltoalalla on lisääntynyt ja toimintaa haittaavia hyökkäyksiä tapahtuu yhä useammin. (Huoltovarmuuskeskus 2021) Terveydenhuoltoala oli kyberhyökkäyksien viiden korkeimman listalla jo 2015, jolloin varastettiin yli 100 miljoonaa potilastietoa. (Lehto 2017). Lisääntyneet tietomurrot näkyvät varsinkin Yhdysvalloissa. Myös sairaaloissa ovat kyberhyökkäykset lisääntyneet Aasiassa, Lähi-idässä ja Euroopassa. (Huusko 2020)

Kasperskyn (N.d) selvityksessä Yhdysvalloissa ja Kanadassa terveydenhuolto organisaatioiden työntekijöillä ei ole tarvittavaa koulutusta tai tietoisuutta tietoturvallisuudesta. Kysely paljastaa muutamia hälyttäviä huomioita, jotka korreloivat kasvavien hakkerointi ja it-hälytyksien taustalla. Lausunnossa käy ilmi, että on selkeitä tietoisuuden puutteita Kanadan liittovaltion asetuksessa pitää potilastietojärjestelmä tietoturvallisena. (Lagasse 2019) Yhdysvalloista leviävät huolestuttavat trendit voivat tulla samanlain suomeen, jos emme ota terveysalan opiskelijoiden kouluttamista jo oppilaitoksessa yhtä vakavasti kuin työpaikan harjoitteluissa. Andreasson (2014) toteaa että, jokaisesta ei tietenkään voida saada tietoturvan ammattilaista mutta kaikilla on oltava peruskäsitys organisaatiossa käsittelemästään tiedon merkityksestä, koska organisaation tietoturva on yhtä kuin sen heikoin osa-alue. Onnistunut tietoturvan kehittäminen vaatii jatkuvaa koulutusta ja viestintää, jotta dataa voidaan huolellisesti käsitellä sen vaatimalla luottamuksellisuudella.

2.1 Tietoturva

Usein ihmetellään kyberturvallisuuden ja tietoturvan eroa. Käsitteet linkittyvät vahvasti toisiinsa mutta niissä löytyy tärkeitä eroja, jotka tullaan ottamaan huomion tässä tutkimuksessa. Kyberturvallisuudessa perinteisesti otetaan huomioon tietotuvan elementit teknisen laitteiston, palomuurien ja systeemien näkökulmasta. Tietoturvallisuudessa tärkeätä on tiedon saatavuuden, eheyden ja luottamuksellisuuden täyttyminen. Molempiin käsitteisiin kuuluu saatavuus, eheys ja luottamuksellisuus. Olcott (2017) kuitenkin osoittaa, että kyberturvallisuus on käsitteenä teknillisesti kompleksisempi kuin tietoturva.

Tietoturva tarkoittaa tiedon luottamuksellisuuden, saatavuuden ja eheyden säilyttämistä (ks. kuvio 2). Jokaisella organisaatiolla on hallussaan tietoja, jotka ovat heille tärkeitä suojattavia voimavaroja. Toimenpiteitä, joilla näitä suojataan, kutsutaan tietoturvaksi. (Lundgren. 2017) Yleisesti tietoturva tarkoittaa tietojen, järjestelmien, palveluiden ja tietoliikenteen suojaamista ulkopuolisilta uhkilta. Yksittäisen ihmisen kohdalla tämä tarkoittaa tämän ihmisen tietoja sisältävien järjestelmien ja palveluiden tietoturvaa.

Kuvio 2. CIA-triad

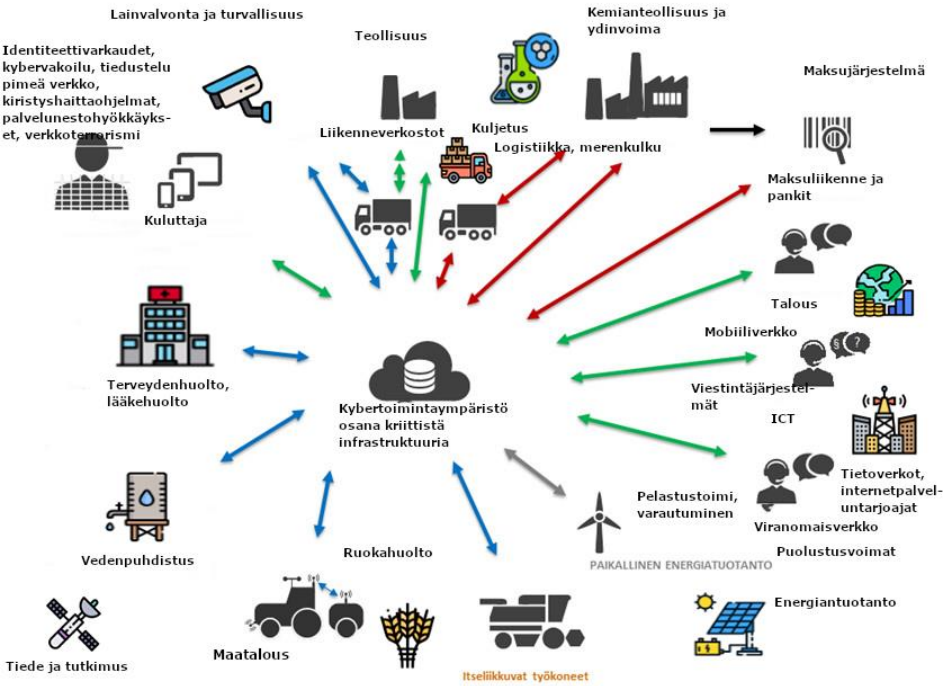
Tietoturvan kolminaisuuteen kuuluu luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuudella tarkoitetaan että, tieto on käytettävissä vain sille henkilölle, laitteelle tai prosessille, joka on valtuutettu käyttämään sitä. Yksinkertaisimmillaan tarkoittaa sitä, että järjestelmä on salasanasuojattu ja sinne pääsee vain se henkilö, jolla salasana on. (Andress 2011) Hieman monimuotoisemmassa ympäristössä, voidaan määritellä käyttäjälle vain katseluoikeudet ja toiselle suoritusoikeudet, joten työtehtävät jakautuvat henkilöille heidän omien työtehtävien mukaan. Henkilötietojen identiteetin- ja pääsynhallinta pohjautuvat luottamuksellisuuteen ja eheyteen. Käyttäjänhallinnan tarkoituksena on varmistaa, että tieto ei ole saatavissa käyttäjille, prosesseille, tai laitteille ellei heillä ole valtuuksia käyttää tietoja.

Eheydellä tarkoitetaan tilaa, jossa tieto on pysynyt muuttumattomana siitä pisteestä, jonka lähettäjä tai lähde on sen laittanut liikkeelle ja tullut perille vastaanottajalle. Tieto on siis pysynyt muuttumattomana siirron tai tallennuksen aikana ja sen luotettavuus on varmistettu. (Andress 2011) Järjestelmät, jotka ylläpitävät eheyttä varmistavat tiedon muuttumattomuuden laitteisto- tai ohjelmistovioilta. (NICCS 2022)

Saatavuudella tarkoitetaan tiedon välitöntä käytettävyyttä siitä hetkestä alkaen, kun sitä tarvitaan. Tieto on käytettävissä ajasta ja paikasta riippumatta valtuutetuille henkilöille. Lääketieteellistä ympäristöissä järjestelmien saatavuudelle on äärimmäisiä vaatimuksia. Näiden systeemien täytyy olla kykyisiä vastustamaan kyberuhkia, sähkökatkoksia tai laitteiston vikaantumista. Kyberturvallisuudessa saatavuus liitetään yleensä voimavaroihin kuten tietoon tai tietojärjestelmiin. (DNV N.d)

Ulkoministeriön (N.d) määritelmän mukaan kybertoimintaympäristöllä tarkoitetaan ihmisien luomaa digitaalista rinnakkaistodellisuutta, jossa sekä fyysinen että digitaalinen ovat läsnä. Kyse on monimutkaisesta maailmanlaajuisesta informaatioverkostosta. Informaatioteknologia, sosiaalinen media, automatisoidut järjestelmät sekä internet yhdistää meitä globaalisti. Kriittinen infrastruktuuri vesi- energiahuolto- pankki järjestelmä-, terveydenhuolto sekä liikenne ovat kaikki riippuvaisia digitaalisesta ympäristöstä (ks. kuvio 3). Tietotekniikan nopea kehittyminen on tuonut uusia haasteita, esimerkiksi kyberrikollisuuden, joka uhkaa tätä uudistunutta kybertoimintaympäristöä.

Esineiden internet (IoT) on monimutkainen käsite, minkä vuoksi on vaikea tarkentaa mitä se tarkalleen ottaen pitää sisällään. Voidaan kuitenkin todeta, että esineiden internet on fyysisten laitteiden verkko, jotka voivat todentaa itsensä toisten laitteiden avulla. Kybertoimintaympäristö on osa esineiden internetiä ja yksi vaikeimmista kyberturvallisuuden haasteista seuraavalla vuosikymmenellä. (Barajas 2014)



Kuvio 3. Kybertoimintaympäristö kriittisessä infrastruktuurissa

Liikenne- ja turvallisuusviraston (2020) määritelmän mukaan kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus on

toiminto, jolla suojataan järjestelmiä verkkoja ja ohjelmia digitaalisilta hyökkäyksiltä. Kyberturvallisuus on myös varautumista mahdollisiin uhkiin sekä jatkuvaa valvontaa niiden ehkäisemiseksi. Holmes (2022) toteaa että kyberturvallisuus on teknisten keinojen avulla tietoteknisten laitteiden ja voimavarojen puolustamista haitallisilta digitaalisilta hyökkäyksiltä. Kyberturvallisuus ottaa huomioon organisaation sisä- ja ulkopuolelta tulevien hyökkäyksen mahdollisuuden. Näiden hyökkäysten tarkoituksena on yleensä päästä käsiksi, muuttaa tai tuhota arkaluonteista tietoa. Hyökkäyksille tyypillistä on kiristää käyttäjiä rahalla tai keskeyttää liiketoimintaprosessit. Laitteita, laitteistoja ja tietokoneohjelmistoja on nykyisin niin paljon, että kyberturvallisuuden toteuttaminen onkin muuttunut entistä haastavammaksi. (CISCO 2021)

2.2 Tietosuoja

Tietosuoja turvaa oikeuden henkilötietoja käsiteltäessä. Työpaikkojen on tarjottava työntekijöilleen ja asiakkailleen yksityisyydensuojaa. Tarkoittaa siis ihmisistä kerättyä henkilökohtaista tietoa, jota yrityksen kuuluu suojella. Henkilötietojen käsittely pohjautuu siis aina lakiin. Henkilötietoja voidaan säilöä tiedostoissa, tietokannoissa, paperilla, äänitiedostoissa, kuvissa tai mapeissa. Henkilötietoja voivat olla nimi, kotiosoite, sähköpostiosoite, puhelinnumero, henkilökortin numero, auton rekisterinumero, paikannustiedot, IP-osoite, potilastiedot, lemmikin eläinlääkäritiedot ja edesmenneiden sukulaisten perinnöllisiä sairauksia koskevat tiedot. (Tietosuojavaltuutetun Toimisto. 2020)

Euroopan yleinen tietosuoja-asetus Asetus (EU) 2016/679 tuli voimaan 2016 ja sitä on sovellettu suomessa 2018, yleisesti tämä tunnetaan käsitteellä GDPR. Suomessa on 2018 lähtien tarkennettu tietosuojalakia 5.12.2018/1050 ottamalla huomioon rekisteröidyt eli luonnolliset henkilöt, rekisterinpitäjät eli viranomaiset, jotka määrittelevät säännöt henkilötietojen käsittelyyn sekä henkilötietojen käsittelijät eli ulkopuoliset tahot, jotka käsittelevät henkilötietoja rekisterinpitäjien lukuun. (Tietosuojavaltuutetun Toimisto 2020)

Yritysten vastuulla on hallussa olevien henkilötietojen lainmukainen käsittely ja suojaaminen. Valitettavan usein organisaatioissa sivuutetaan tietosuojariskien ennaltaehkäisevää toimintaa. Tämä voi johtua tietosuojavastaavan puuttumisesta yrityksessä. Yritysten hallinnollinen johto ei tällöin hoida lain edellyttämää velvoitettaan. Ennaltaehkäisevien toimenpiteiden puuttumisesta voi näin seurata rikosoikeudellisia seuraamuksia yrityksille. (Andreasson 2014). Pahimmassa tapauksessa

yrityksellä elintärkeät tietokannat voivat olla tietomurtojen kohteena puutteellisen suojauksen vuoksi. Finlexin päätöksessä 1150/161/2021 kerrotaan marraskuussa 2018, Psykoterapiakeskus Vastaamon potilastietokantaan kohdistui ensimmäinen tietomurto. Toinen murto tapahtui maaliskuussa 2019, ja koko tapahtuneesta seurasi lähes 25 000 rikosilmoitusta.

3 Tutkimus

3.1 Tutkimuskysymys

Tutkimuksen aihe saatiin Jyväskylän ammattikorkeakoululta. Tutkimuksen alkuvaiheessa määriteltiin seuraavat kysymykset, jotka johdattelivat kirjoittamaan opinnäytetyötä näiden kysymysten näkökulmasta. Tutkimuksen tarkoituksena oli selvittää, mikä vaikutus harjoittelulla tai harjoitteluilla on Jyväskylän ammattikorkeakoulun sosiaaliterveysalan opiskelijoiden tietoturvaosaamiseen. Sivukysymyksenä pyrittiin löytämään vastaus, miten eroavat Jyväskylän ammattikorkeakoulun harjoittelun tai harjoitteluita suorittaneet sosiaaliterveysalan opiskelijat tietoturvaosaamiseltaan ei lainkaan harjoittelua suorittaneista sosiaaliterveysalan opiskelijoista. Selkeyden vuoksi opinnäytetyön edetessä tulen viittamaan harjoittelun suorittaneisiin opiskelijoihin tutkimusjoukkona (1), ja ei lainkaan harjoittelua suorittaneita opiskelijoita tutkimusjoukkoon (0). Vastausten pohjalta verrataan tutkimusjoukkoa (1) tutkimusjoukkoon (0) ja tehdään näiden pohjalta vertailua, jolla vastataan hankkeessa määriteltyyn kysymykseen.

3.2 Kohderyhmät

Tutkimuksen kohteena olivat Jyväskylän ammattikorkeakoulun sosiaaliterveysalan opiskelijat. Toimeksiannon pohjalta kohderyhmään valittiin sekä alemman että ylemmän korkeakoulututkinnon suorittaneita opiskelijoita. Kohderyhmän valintaan vaikutti aiheen rajaus, tutkimuskysymykset sekä sosiaaliterveysalalla lisääntyvät tietomurrot. Tulosten perusteella voidaan myös tarvittaessa määritellä uusia kurssikuvauksia ja lisätä tietoturvakoulutusta opiskelijoille.

3.3 Tutkimusmenetelmät

Tutkimus toteutettiin hyödyntäen määrällisiä eli kvantitatiivisia tutkimusmenetelmiä. Kyselytutkimus on usein laadultaan kvantitatiivinen koska ollaan kiinnostuneita numeerisiin tuloksiin perustuvasta ilmiöstä ja tullaan vertailemalla selittämään niitä tilastollisella analyysimenetelmällä. (N.a 2015)

Tutkimuksessa oli tarkoitus käyttää myös haastatteluja tutkimusmenetelmänä, mutta kyselyssä olleeseen kysymykseen ”haluatko haastatteluun” ei vastannut yksikään opiskelija myöntävästi. Tutkimuksessa on yhden anonyymin valmistuneen sairaanhoitajaopiskelijan kertomuksia sairaalaympäristössä työskentelystä. Kertomuksesta on poimittu tutkimuskyselyyn osittain kysymyksiä ja vastausvaihtoehtoja.

3.4 Tutkimuksen toteutus

Tutkimus toteutettiin sähköisenä kyselynä opiskelijoille käyttäen Webropolin Professional Statistics -työkalulla. Kysely lähetettiin 579 opiskelijalle koulun sähköpostiosoitteeseen. Kaikki tutkimukseen liittyvä data kerättiin anonyymisti ja kerätty tieto tuhotaan opinnäytetyön valmistumisen jälkeen.

Kyselyn kysymykset jaettiin kuuteen eri aihealueeseen, jotka jaettiin opiskelijan taustatiedot, tietoturvan tarkastelu, asenteisiin, uskomuksiin, todellisiin uhkakuviin, sekä opinnollisiin tarpeisiin. Vastausaikaa opiskelijoilla oli 22.3–12.4.2022.

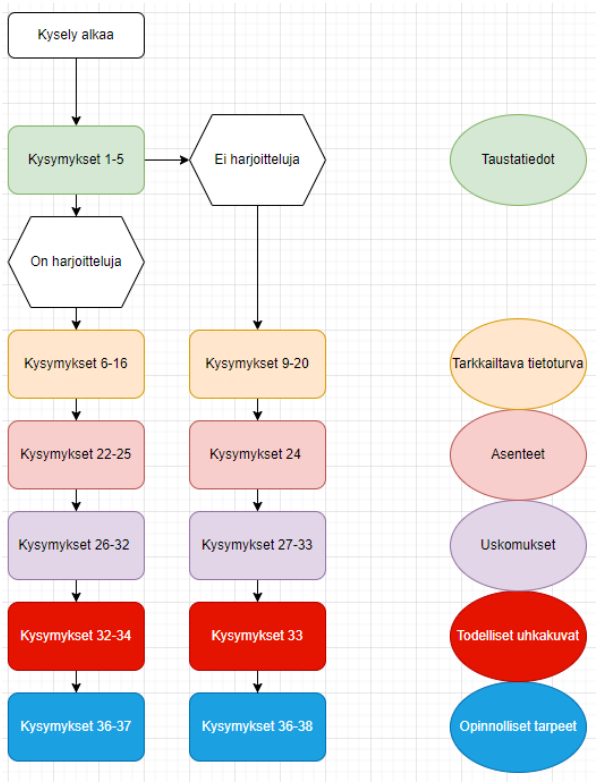
4 Tutkimuskysely

4.1 Kyselyn tiedot

Tutkimuksen kysely lähetettiin 579 opiskelijan sähköpostiosoitteeseen. Vastausprosentti oli noin kahdeksan, sillä 51 henkilöä vastasi kyselyyn. Vastanneiden määrä on todellisuudessa vielä vähemmän, kun kyselyn edetessä osa vastaajista jätti kyselyn kesken tai ei halunnut vastata tiettyihin kohtiin. Lähestulkoon kaikissa kyselyn kysymyksissä oli kohdat ”en tiedä”, ”en halua vastata kysymykseen”. Kysymykset olivat myös kaikki valinnaisia lukuun ottamatta yhtä oleellista kysymystä.

Viidennessä kysymyksessä selvitettiin, onko vastaaja harjoittelun tehnyt opiskelija vai ei. Tutkimuksessa oli tarkoitus olla opiskelijoiden haastatteluja kanssa mutta koronapandemia sekä vastaajien kielteinen päätös vaikutti siihen, ettei haastatteluja pidetty.

Kysely jaettiin kuuteen eri kategoriaan taustatiedot, tarkkailtava tietoturva, asenteet, uskomukset, todelliset uhkakuvat sekä opinnolliset tarpeet. Taustatietokysymysten jälkeen kysymyksessä viisi jakoi vastaajat omiin kohderyhmiin (0) ja (1), joille suunnattiin kohderyhmäkohtaiset kysymykset.



Kuvio 4. Kyselyn rakenne

Todelliset uhkakuvat -kategoriaa ei käytetty kohderyhmän (0) kysymyksissä. Jako kahteen eri kohderyhmään selkeytti kyselyn luomista ja mahdollisti tavan verrata kyselyn vastauksia kohderyhmittäin. Kyselyn jakaminen kategorioihin samoin selkeytti kyselyn tekemistä. Kuvio 4 havainnollistaa kyselyn rakenteesta vuokaavion eri kategorioittain värikoodattuna.

4.2 Kyselyn tulokset ja tarkastelu

4.2.1 Taustatiedot

Taustatiedoilla selvitettiin vastaajilta harjoittelujen määrä ja yleisesti heidän taustastaan vähän enemmän, jotta voitaisiin tehdä tarkempi analyysi. Lähes kaikki kysymykset taustatiedoissa olivat valinnaisia tämä tarkoituksellisesti koska pakollisina ne olisivat voineet vaikuttaa vastausten tuloksiin. Taustatiedoissa ensimmäiseksi selvitettiin vastaajalta halusiko hän osallistua haastatteluun kyselyn sijasta. Tuloksena kukaan ei halunnut osallistua haastatteluun. Taulukossa 1 toisena kysymyksenä selvitettiin, minkä tutkinnon opiskelija on vastaamassa. Suurin osa vastaajista kuului sairaanhoitajien (AMK) koulutusohjelmaan (31 %) (n=15), toiseksi ja kolmanneksi eniten vastauksia saatiin toimintaterapian (AMK) koulutusohjelmasta (12,5 %) (n=6), sekä sairaanhoitajien (YAMK) koulutusohjelmasta (12,5 %) (n=6).

Taulukko 1. Vastaajien tutkinnot

Tutkinto	n	Prosentti
Sairaanhoitaja (AMK)	15	31 %
Fysioterapeutti (AMK)	4	8 %
Sosionomi (AMK)	4	8 %
Kätilö (AMK)	4	8 %
Toimintaterapia (AMK)	6	12 %
Sairaanhoitaja (YAMK)	6	12 %
Fysioterapeutti (YAMK)	1	2 %
Sosionomi (YAMK)	2	4 %
Kätilö (YAMK)	0	0 %
Toimintaterapia (YAMK)	2	4 %
Kuntoutuksen ohjaaja (YAMK)	5	10 %

Taulukoissa 2–3 selvitettiin vastaajien ikää ja sukupuolta. Vastaajista (23 %) (n=11) oli yli 41-vuotiaita, YAMK:n mukaan ottaminen tutkimukseen vaikutti tähän jonkin verran. Oletettavasti suurimääräisin vastausten joukko saatiin 18–24-vuotiailta (31 %) (n=15). Tutkimukseen vastanneista 92 % oli naisia (n=45).

Taulukko 2. Vastaajien ikäjakauma

Ikä	n	Prosentti
18–24	15	31 %
25–30	10	20 %
31–35	8	16 %
36–40	5	10 %
41 -	11	23 %

Taulukko 3. Vastaajien sukupuolet

Sukupuoli	n	Prosentti
Nainen	45	92 %
Mies	3	6 %
En halua vastata	1	2 %

Taulukossa 4 taustatietojen viidennessä kysymyksessä ja kyselyn ainoassa pakollisessa kysymyksessä selvitettiin vastaajien taustaa siitä, onko hänellä harjoitteluja suoritettu vai ei. Tuli vasta pitkälle kyselyä luodessa selväksi, että joihinkin koulutusohjelmiin (YAMK) ei kuulu harjoittelua laisinkaan. Tämä hiukan vaikeutti tutkimuskysymyksiin vastaamista siitä näkökulmasta, että jotkin vastaajat (ei harjoittelua suorittaneet) ovat oletettavasti olleet työelämässä jo jonkin aikaa ja todennäköisesti siellä saaneet kokemusta ja näin ollen käsitystä tietoturvasta ja tietosuojasta. He tällöin sekoittuvat (ei yhtään harjoittelua suorittaneisiin) jotka oletettavasti ovat vielä tietoturva käsitykseltään jäljessä niistä, jotka ovat harjoittelun tehneet. Muussa tapauksessa harjoittelun suorittaneiden ja ei ollenkaan harjoittelua suorittaneiden kyselyyn vastaajat menivät aika tasaisesti, joka on positiivista tutkimuksen kannalta.

Taulukossa 4 harjoittelun suorittaneita vastaajia oli yhteensä 55 % (n=27), joista enemmistö oli 1–2 harjoittelua suorittaneita 33 % (n=16). Ei yhtään harjoittelua suorittaneita vastaajia oli yhteensä 45 % (n=22), joista 27 % (n=13) harjoittelu ei kuulunut laisinkaan tutkinto-ohjelmaan. Viidennen kysymyksen pakollisuus oli perusteltu sen takia koska kysely jatkui tämän jälkeen suuntaan (1) tai

suuntaan (0), riippuen siitä oliko harjoittelua tehty vai ei. Toisen haaran kysymykset oli piilotettu vastaajilta.

Taulukko 4. Vastanneiden harjoitteluiden määrä

Harjoittelut	n	Prosentti
En yhtään harjoittelua vielä	9	18 %
1–2	16	33 %
3–4	9	18 %
5–6	1	2 %
7–8	1	2 %
Tutkintooni ei kuulu harjoittelua	13	27 %

4.2.2 Tietoturvan tarkastelu

Kysymykset 6–8 oli suunnattu vain harjoittelun suorittaneille. Kuudennessa kysymyksessä selvitettiin harjoittelupaikan kokoa kysymällä sen henkilöstömäärää. Koska suomessa sosiaaliterveysalan työvoiman jakautuminen on yli 70 % julkiseen sektoriin painottuva, jako näin pieniin henkilöstömäärin ei ollutkaan niin olennaista. Yllättävää kuitenkin oli, että 78 % (n=21) vastaajista oli alle 50 hengen harjoittelupaikassa. Suomen yrittäjät (2019) määrittelee pienyrityksiksi alle 50 työntekijän yritykset ja mikroyrityksiksi alle 10 hengen yritykset.

Taulukko 5. Harjoittelun suorittaneiden harjoittelupaikan henkilöstömäärät

Henkilöstömäärä	n	Prosentti
1–4	1	4 %
5–9	2	7 %
10–19	8	30 %
20–49	10	37 %
50–99	1	4 %
100-	5	19 %

Kysymyksissä 6–8 harjoittelun suorittaneista selvitettiin vastaajan roolia harjoittelussa sekä minkälaisella laitteistolla töitä tehdessä käytettiin internetiä. Taulukossa 6 havainnollistaa miten harjoittelijaksi luokitteli itsensä 93 % vastaajista. Pöytätietokoneet nousivat ykköseksi harjoittelupaikan käytetyimmäksi verkkoon kiinnitetyksi laitteeksi 89 % (n=24), seuraavana kannettavat tietokoneet 74 % (n=20).

Internetin käyttö erottui vastaajien kesken selkeämmin kysymyksissä 8-9. Taulukossa 7 harjoittelua vaille kohderyhmän vastaajat kokivat internetin käytön parhaaksi välineeksi kannettavan tietokoneen 82 % (n=18). Ylempi vertailukysymys harjoittelun suorittaneille nousi pöytäkoneet ykköseksi internetin käytön suhteen 89 % (n=24).

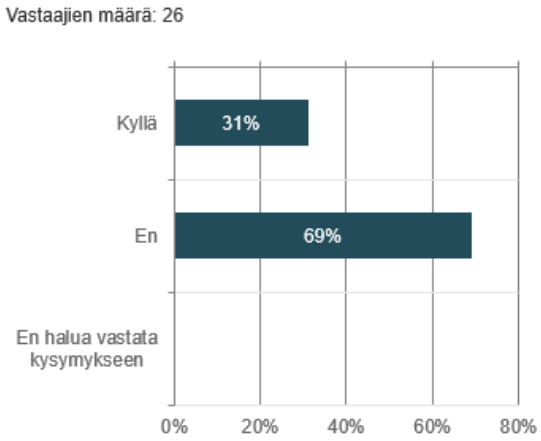
Taulukko 6. Harjoittelussa olleiden yleisin verkkoon kiinnitetty laitteisto

Laitteisto harjoittelussa	n	Prosentti
Pöytätietokone	24	89 %
Kannettava tietokone	20	74 %
Tabletti	3	11 %
Älypuhelin	17	63 %
Jollain muulla, millä?	1	4 %

Taulukko 7. Ei harjoittelua kohderyhmän yleisin laitteisto verkon käyttöön

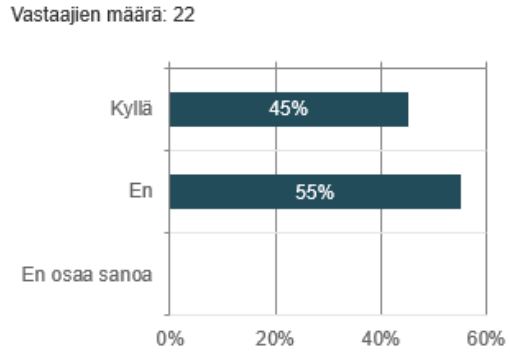
Laitteisto yleensä	n	Prosentti
Pöytätietokone	5	23 %
Kannettava tietokone	18	82 %
Tabletti	4	18 %
Älypuhelin	17	77 %
Jollain muulla, millä?	0	0 %

Kysymyksissä 10–11 selvitettiin harjoittelun suorittaneiden tottumuksista käyttää työasioihin puhelinta ja verrattiin sitä harjoittelua ei vielä suorittaneisiin JAMK:n langattoman verkon käyttämiseen omilla laitteilla (ks. kuvio 5). Vastanneista 31 % eli n=8 oli käyttänyt omia laitteitaan työasioiden hoitamiseen. Vastausten perusteella AMK vastaajat käyttivät vähemmän omia laitteita työasioihin kuin YAMK vastaajat. YAMK vastaajilla vastauksia oli tosin vähemmän mikä saattaa vaikuttaa tulokseen.



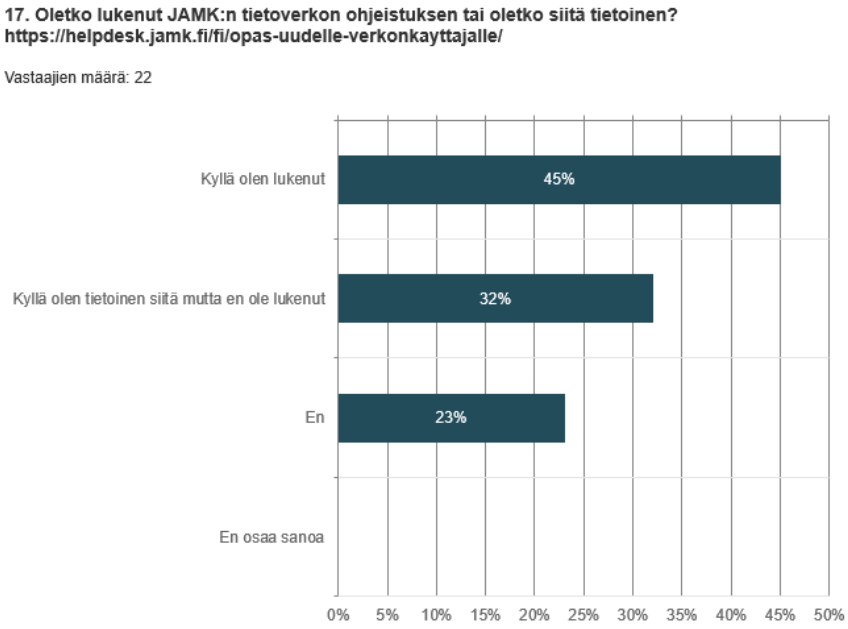
Kuvio 5. Kysymys 10 harjoittelun suorittaneiden omien laitteiden käyttäminen työasioihin

Omien laitteiden käyttö koulun langattomassa verkossa, ja harjoittelupaikan verkossa on eri asioita mutta toisaalta tässä tapauksessa työpaikalla on käytetty omia henkilökohtaisia laitteita vähemmän vastausten perusteella. JAMK:n Dynamon kampuksella pöytätietokoneet sijaitsevat toisen kerroksen sosiaaliterveysalan käytävällä. Vastauksista voidaan päätellä, että moni opiskelija hyödyntää koneiden käyttömahdollisuutta (ks. kuvio 6).



Kuvio 6. Kysymys 11 ei harjoittelua suorittaneiden omien laitteiden käyttö JAMK:n verkossa

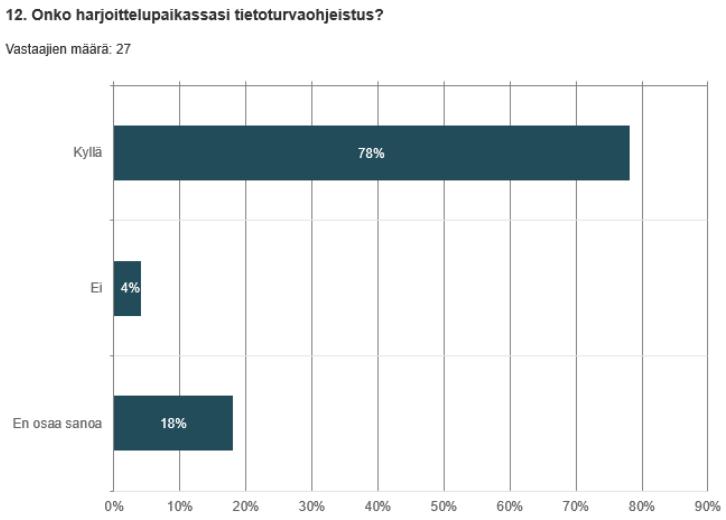
Sosiaaliterveysalan harjoittelijoilla tulee olla tietotekniset perustaidot, joita ovat mm. potilastietojärjestelmien tuntemus sekä yleiset tieto- ja viestintätekniikkataidot, myös sähköpostin käyttäminen. Kyselyn kysymyksissä 12 ja 17 kartoitettiin molempien kohderyhmien tietoturvaohjeistuksen tunnistamista. Saatiin selville, että valtaosa vastauksista kohderyhmässä harjoittelun suorittaneet olivat sitä mieltä, että harjoittelupaikassa on tietoturvaohjeistus 78 % (n=21). Kohderyhmän ei harjoittelua suorittaneet kuviossa 7, kysymyksessä lisäksi selvitettiin opiskelijoiden kiinnostusta ohjeeseen, jossa ilmeni, että vain niukka enemmistö oli lukenut ohjeen.



Kuvio 7. Kysymys 17 ei vielä harjoittelua suorittaneiden tietoturvaohjeistuksen sisäistäminen

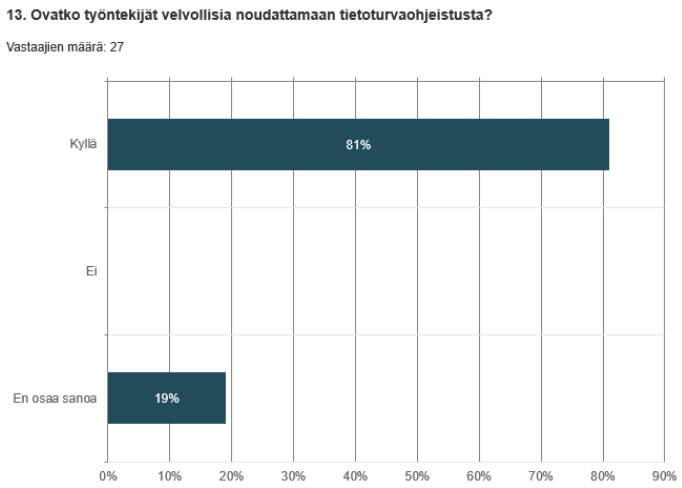
JAMK:n Helpdeskin tietoturvaohjeistuksessa on kattavat ohjeet uudelle verkonkäyttäjälle kampuksilla asioidessa. Se sisältää ohjeet salasanan, sähköpostin, kotihakemiston, www-sivujen, tulostimen, yleisimpien verkkopalvelujen sekä etätyöskentelyn käytöstä.

Osa vastanneista 22 % ei tiennyt tai harjoittelupaikassa ei ollut tietoturvaohjeistusta (ks. kuvio 8). Kyse on lähes neljäsosaa kysymykseen vastanneista, joten prosenttiosuus on kohtuullisen korkea aika olennaisesta asiasta tietoturvan kannalta harjoittelupaikoissa. Tietoturvaohjeistus tulisi oletuksena olla selkeästi osoitettu uusille harjoittelijoille jokaisella työpaikalla.



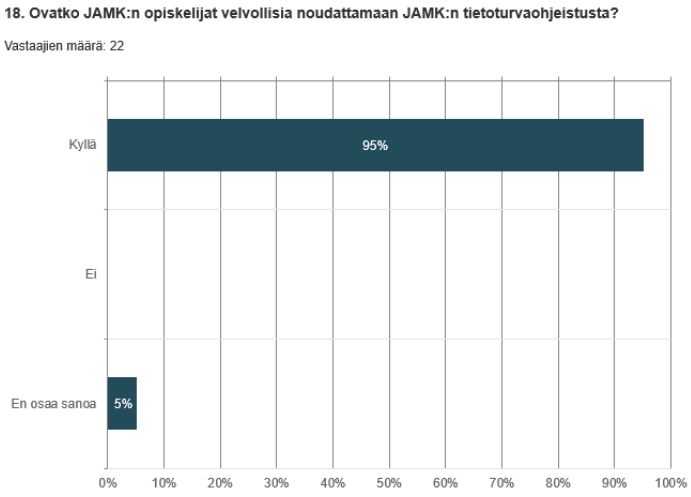
Kuvio 8. Kysymys 12 harjoittelun suorittanut onko harjoittelupaikassasi ollut tietoturvaohjeistus

Kysymyksissä 13 ja 18, molemmille kohderyhmille tarkennettiin, oliko heillä velvollisuus noudattaa tietoturvaohjeistusta. Molemmissa kohderyhmissä lähes vastaava enemmistö kertoi, että noudattaminen on velvollista.



Kuvio 9. Kysymys 13 harjoittelun suorittaneet ovatko työntekijät velvollisia noudattamaan tietoturvaohjeita

Melkein viidesosa harjoittelun suorittaneista vastaajista ei tiennyt pitääkö harjoittelupaikassa noudattaa tietoturvaohjeistusta (ks. kuvio 9). Ei harjoittelua suorittaneissa vastasivat samaan kysymykseen (ks. kuvio 10). He vastasivat melkein täysin 95 % ”Kyllä”.



Kuvio 10. Kysymys 18 ei harjoittelua suorittaneiden velvollisuus noudattamaa JAMK:n tietoturvaohjeistusta

Kohderyhmälle harjoittelun suorittaneet, pyydettiin tarkentamaan, mitä harjoittelupaikan tietoturvaohjeistus sisälsi, jotta saataisiin peruskäsitys Jyväskylässä terveydenhuollon harjoittelijoille suun-

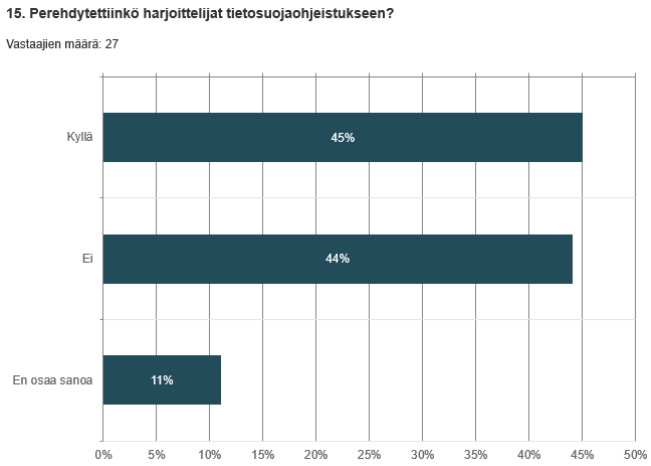
natusta ohjeistuksesta käyttäjille (ks. kuvio 11). Kysymyksessä saatiin selville että, luottamuksellinen materiaalin tuhoaminen 89 %, työsähköpostin käyttö 78 %, rajoitettu toimitiloihin kulkeminen 70 % ja salasanoihin 70 % liittyvät ohjeet olivat korkeimmaksi valituimmat.

Vastauksissa ilmeni myös, että tietoturvaohjeet vaihtelevat työpaikkakohtaisesti, joten kysymykseen oli siinä mielessä vaikea vastata, jos oli suorittanut useamman harjoittelun eri paikoissa. Suuremmissa työpaikoissa on todennäköisesti valtuutettu IT-tuki, joka pitää huolta järjestelmien päivittämisestä 52 % sekä varmuuskopioinnista 22 %. Ja sosiaaliterveysalalla harvemmin on mahdollisuus etätöihin niin VPN-ohjeen 30 % pieni prosenttiosuus voi osittain selittyä sillä. Vain yhdessä harjoittelupaikassa 4 % ei ollut harjoittelijalle tullut ilmi, että työpaikalla olisi tietoturvaohjeistusta. Tämä hiukan eroaa kysymyksestä 12 jossa 22 % ei tiennyt ohjeista.

Mitkä seuraavista kuuluvat harjoittelupaikkasi tietoturvaohjeistukseen?	n	Prosentti
Harjoittelupaikassa on käytössä salasanojenhallintaohjelmisto	9	33 %
Sosiaalisen median käyttö, (esimerkiksi kielto käyttää sosiaalista mediaa työajalla)	6	22 %
Työsähköpostin käyttö, (esimerkiksi työsähköpostin käyttö vain työasioihin)	21	78 %
Toimitiloihin kulkeminen, (esimerkiksi työtietokoneiden valvominen tai pitäminen lukittujen ovien takana)	19	70 %
Erillinen tietosuojaohjeistus	12	44 %
Etätyöohje, (esimerkiksi VPN:n käyttö, VPN:n käytön ohjeet, mitä työkoneelle saa verkosta ladata)	8	30 %
Järjestelmien tai työtietokoneiden salasanat, (esimerkiksi niiden voimassaoloaika on rajoitettu ja on pakotettu vaihtamaan n-ajan välein	19	70 %
Virustorjunta työkoneella ja sen säännöllinen päivittäminen	14	52 %
Varmuuskopiointi, (esimerkiksi onko työkoneilla Onedrive/Dropbox käytössä, onko jokin muu backup työtietokoneessa?	6	22 %
Luottamukselinen materiaali, (esimerkiksi paperilla olevien potilastietojen/talousasiakirjojen laittaminen erilliseen lukittuun astiaan?	24	89 %
Työaseman ja kannettavan työtietokoneen käyttö, (esimerkiksi kun omalta työasemalta poistutaan, työkoneen lukitseminen	16	59 %
Internetin käyttö työpaikalla, (esimerkiksi työtietokoneella ei ole pääsyä joillekin nettisivuille)	6	22 %
Vieraat, (esimerkiksi onko vierailla vapaa pääsy tuontatotiloihin)	7	26 %
Jotain muuta, mitä?	1	4 %
Työpaikalla ei ollut tietoturvaan liittyvää ohjeistusta	1	4 %
Ei mitään näistä	0	0 %

Kuvio 11. Kysymys 14 harjoittelun suorittaneet mitkä seuraavista kuuluvat tietoturvaohjeisiin

Kysyttiin ensimmäiseltä kohderyhmältä, sisältyikö harjoitteluun myös erillinen tietosuojaohjeistus, johon vain 44 % otti kantaa (n=12) (ks. kuvio 12). Eli suhteellinen enemmistö harjoittelutyöpaikoista liittävät tietosuojaohjeen samaan tietoturvaohjeistukseen. Tai ohjeet sekoitetaan keskenään. Tulos oli vastaavanlainen erillisellä kysymyksellä. Myöntävästi 45 % (n=12) otti kantaa.



Kuvio 12. Kysymys 15 harjoittelun suorittaneet perehdytettiinkö erilliseen tietosuojaohjeistukseen

Kysyttiin tietosuojaohjeen sisällöstä, johon saatiin seuraavat vastaukset (ks. kuvio 13). Potilastietojen lainmukainen käsittely 96 %, salassapito- ja vaitiolovelvollisuus 100 % saivat suurimmat valinnat. Virheellisen tiedon päivittäminen 73 %, henkilötietojen saatavuus 69 %, ja asiakkaiden oikeus tietojen saantiin 88 % olivat kanssa iso enemmistö valinnoista.

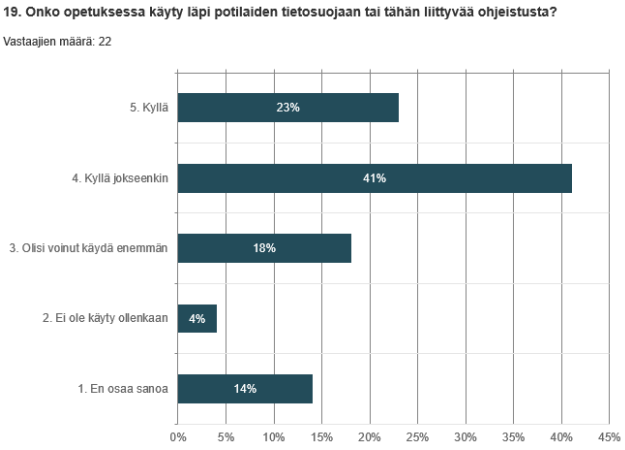
Mitä seuraavista on otettu huomioon harjoittelupaikkasi tietosuojaohjeistuksessa?	n	Prosentti
Potilastietojen ja henkilötietojen lainmukainen käsittely, (esimerkiksi henkilötietoja kerätään asianmukaisesti)	25	96 %
Salassapito- ja vaitiolovelvollisuus, (esimerkiksi henkilötietoja käsitellään luottamuksellisesti ja turvallisesti)	26	100 %
Virheellisen tiedon päivittäminen, (esimerkiksi epätarkat tai virheelliset tiedot poistetaan tai oikaistaan heti)	19	73 %
Henkilötietojen saatavuus, (esimerkiksi kerättävä henkilötieto on vain nimenomaista tarkoitusta varten ja sitä kerätään vain tarpeellinen määrä)	18	69 %
Oikeus saada tietoja, (esimerkiksi potilailla tai asiakkailla oikeus saada tieto siitä mitä, miksi ja miten häntä koskevia henkilötietoja käsitellään)	23	88 %
Oikeus tietojen poistoon, (esimerkiksi rekisteröidyillä asiakkailla on oikeus poistattaa kaikki heidän henkilötiedot rekisteristä)	7	27 %
Oikeus saada tieto tietoturvaloukkauksesta, (esimerkiksi harjoittelupaikan on ilmoitettava tietoturvaloukkauksesta rekisteröidyille)	8	31 %
Henkilötietojen säilyttäminen, (henkilötietoja säilytetään ainoastaan niin kauan kuin se on välttämätöntä tietojenkäsittelyn tarkoitusta varten)	15	58 %
Ei mitään näistä	0	0 %
Jotain muuta, mitä?	2	8 %
Työpaikalla ei ollut tietosuojaan liittyvää ohjeistusta	1	4 %

Kuvio 13. Kysymys 16 harjoittelun suorittaneet tietosuojaohjeiden sisältö

Vertailun vuoksi kysyttiin kohderyhmältä, ei harjoittelua suorittaneet, mitä JAMK:n kursseilla on otettu huomioon tietosuoja-aiheesta. Kyseisen kohderyhmän vastauksista saatiin seuraavat tulokset (ks. kuvio 14). Aihealueet tarkennetusta kysymyksestä 20, eli potilas- ja henkilötietojen käsittelyn valitsi 77 % (n=17) sekä salassapito- ja vaitiolovelvollisuus arkaluonteiseen tietoon 77 % (n=17). Myös asiakirjojen salassapito oli korkea 68 % (n=15). Väittämiä ei voitu pitää täysin samanlaisina kuvion 13 kysymysten kanssa sillä ei ollut täysin tiedossa mitä koulun opetuksessa käydään läpi tietosuojaan liittyen kohderyhmän opiskelijoille. Valittiin kuvion 14 väittämiin tietosuojan yläkäsitteitä.

Kuvio 14. Kysymys 20 ei harjoittelua JAMK:n tietosuojaan liittyvät aihealueet

Kysyttiin ei harjoittelua suorittaneiden vastaajilta, ovatko saaneet opetusta asiakkaiden tietosuojaan liittyen (ks. kuvio 15). Kyllä tai jokseenkin myönteisiä vastauksia tuli yhteensä 64 % (n=13). Päättelemällä vastauksista voisi todeta, että tietosuoja otetaan viimeistäänkin harjoittelussa esille, jos sitä ei ole vielä koulussa ilmaistu.



Kuvio 15. Kysymys 19 ei harjoittelua suorittaneiden tietosuojaan liittyvä opetus

4.2.3 Asenteet

Selvitettiin kohderyhmältä harjoittelun suorittaneet kuviossa 16, heidän asenteitaan väittämiin tietoturvasta. Keskiarvo väittämissä oli (3.7). Esiin nousi jälleen tärkeimmäksi asiakas- ja potilastietojen tietoturvallinen käsittely (4.0). Myös laitteiston ja henkilökunnan tilojen suojaaminen ulkopuoliselta pääsyltä (3.9) nousi keskiarvon yläpuolelle. Omien tietojen ja taitojen kehittäminen oli tässä kysymyksessä kanssa keskiarvon yläpuolella (3.8).

Kuvio 16. Kysymys 22 harjoittelun suorittaneiden asenteet tietoturvaväittämiin

Seuraavat asenneväittämät kysyttiin molemmilta kohderyhmiltä. Tarkoitus oli selvittää mitkä asenteet vaikuttavat olevan harjoittelussa olleille korostettuna. Lisäksi selvittää mitkä asenteet kohderyhmällä ei harjoittelua suorittaneet olivat vastaavissa kysymyksissä. Kohderyhmän harjoittelun suorittaneet selvityksessä keskiarvosta muodostui (2,1) (ks. kuvio 17). Kyberhyökkäyksestä aiheutuvaa tietovuotoa (2,5) pidettiin huomattavana huolena jo harjoittelun tehneiden opiskelijoiden mielestä. Samoin laitteistojen ja järjestelmien vanhuus (2,8) aiheutti epäilystä.

Mitä seuraavista pidät todennäköisinä tietoturvauhkina harjoittelupaikassasi?	1-5
Kyberhyökkäyksestä aiheutuva sähkökatkos, medisiinisen laitteen toimintahäiriö tai vikatilanne	2,5
Kyberhyökkäyksestä aiheutuva tietosuojavuoto, (potilas- tai henkilötiedon paljastuminen)	2,2
Työpaikan henkilöstön heikkojen salasanojen johdosta aiheutunut hyökkääjän luvaton pääsy järjestelmiin	2,1
Arkaluonteisten tietojen vuotaminen sosiaalisen median kautta, (esimerkiksi työkaverin käyttäjä-ID leviää somessa)	1,5
Poistuessa työpisteeltä, työaseman auki ja valvomatta jättäminen	2,3
Työpaikalla puhelinsoiton yhteydessä arkaluonteisen tiedon leviäminen	2,2
Työntekijöiden äänekkään keskustelun seurauksena arkaluonteisen tiedon leviäminen	2,4
Työsähköpostiin tulleen haitallisen linkin klikkaaminen	2,0
Laitteistojen tai järjestelmien vanhuudesta johtuva toimintahäiriö (esimerkiksi pävityksiä ladattaessa laitteiston jumittaminen)	2,8
Työpaikan henkilöstön aiheuttama tahallinen vandalisointi järjestelmiin	1,4
Työpaikan henkilöstön tahaton tietojen poistaminen vahingossa (esimerkiksi kirjatessa tietoja, vanhojen tietojen poistaminen.)	1,9
Työpaikan henkilöstön luvaton arkaluonteisten tietojen selaaminen, (esimerkiksi tylsyyden aiheuttama satunnaisten potilastietojen surffailu.)	1,5
Jotain muuta, mitä?	4,1

Kuvio 17. Kysymys 23 kohderyhmä harjoittelun suorittaneiden asenteet tietoturvauhkiin

Kohderyhmällä ei harjoittelua suorittaneilla oli lähes vastaavat asenteet mahdollisista tietoturvauhista (ks. kuvio 18). Keskiarvo väittämissä oli (2,2) Ennen harjoittelujen alkamista mahdollisesti korostetaan työasemalta poistumisen hyviä toimenpiteitä (2,9). Molemmat kohderyhmät uskoivat laitteiston vanhuuden (2,7) olevan korkea tietoturvariski. Myös kohderyhmän ei harjoittelua suorittaneiden näkökanta salasanojen heikkoudesta harjoittelijoiden kesken voi olla tietoturvariski. Edelleen on hyvä mainita, että sama kohderyhmä arvelee työntekijöiden äänekkään keskustelun (2,4) ja puhelinsoiton (2,3) olevan mahdollisia tietoturvariskejä. Lisämainintana pidettiin merkittävänä uhkana tilannetta, jossa henkilökunnan tiedot kuten puhelinnumero voisi levitä asiakkaille.

Mitä seuraavista pidät todennäköisinä tietoturvauhkina tulevassa työ- tai harjoittelupaikassasi?	1-5
Kyberhyökkäyksestä aiheutunut sähkökatkos, medisiinisen laitteen toimintahäiriö tai vikatilanne	2,0
Kyberhyökkäyksestä aiheutunut tietosuojavuoto, (esimerkiksi potilas- tai henkilötiedon paljastuminen)	2,1
Työpaikan henkilöstön heikkojen salasanojen johdosta aiheutunut hyökkääjän luvaton pääsy järjestelmiin	2,3
Arkaluonteisten tietojen vuotaminen sosiaalisen median kautta, (esimerkiksi kulkukortin käyttäjä-ID leviää somessa)	2,2
Poistuessa työpisteeltä, työaseman auki ja valvomatta jättäminen	2,9
Työpaikalla puhelinsoiton yhteydessä arkaluonteisen tiedon leviäminen	2,4
Työntekijöiden äänekkään keskustelun seurauksena arkaluonteisen tiedon leviäminen	2,3
Työsähköpostiin tulleen haitallisen linkin klikkaaminen	2,1
Laitteistojen tai järjestelmien vanhuudesta johtuva toimintahäiriö, (esimerkiksi pävityksiä ladattaessa laitteiston jumittaminen)	2,7
Työpaikan henkilöstön aiheuttama tahallinen vandalisointi järjestelmiin	1,4
Työpaikan henkilöstön tahaton tietojen poistaminen vahingossa, (esimerkiksi kirjatessa tietoja, vanhojen tietojen poistaminen.)	1,9
Työpaikan henkilöstön luvaton arkaluonteisten tietojen selaaminen, (esimerkiksi tylsyyden aiheuttama satunnaisten potilastietojen surffailu.)	1,8
Jotain muuta, mitä?	4,8

Kuvio 18. Kysymys 24 kohderyhmä ei harjoittelua suorittaneiden asenteet tietoturvauhkiin

Harjoittelun suorittaneille asetettiin kysymys tietoturvan kehittämisestä harjoittelupaikassa taulukossa 8. Kysymyksistä nousi suurimmaksi kehitysehdotuksiksi esille fyysisen ympäristön turvaaminen 63 % (n=17) sekä poikkeustilanteiden ja ongelmatapahtumien hallinta 59 % (n=16). Osa oli

myös lisännyt tietoturvakoulutuksen osaksi kehitystarpeita harjoittelussa, jotain muuta, mitä -osioon. Mielenkiintoisesti tietosuojaohjeiden päivittäminen oli kolmanneksi eniten valittu kehitystarve 48 % (n=13).

Taulukko 8. Kysymys 25 kohderyhmä harjoittelun suorittaneiden kehitystarpeet harjoittelussa

Kehitettävää harjoittelupaikan tietoturvaosaamisessa	n	Prosentti
Salasanaohjeiden päivittäminen	11	41 %
Tietosuojaohjeiden päivittäminen	13	48 %
Pääsynhallinta	8	30 %
Tietojärjestelmien kehitys, testaaminen ja ylläpito	12	44 %
Fyysisen ympäristön turvallisuus	17	63 %
Henkilöstöturvallisuus	9	33 %
Tietoturvapolitiikka	9	33 %
Poikkeustilanteiden ja ongelmatapahtumien hallinta	16	59 %
Omaisuuden ja tieto-omaisuuden (suojattavat tiedot) hallinta	4	15 %
Tietojärjestelmien käytön ja tiedonvälityksen turvallisuuden hallinta	6	22 %
Ei mitään näistä	1	4 %
Jotain muuta, mitä?	2	7 %

4.2.4 Uskomukset

Taulukossa 9 valtaosa harjoittelun suorittaneiden vastaajista uskoi omaan havainnointikykyynsä tiedostaa mahdollisia tietoturvauhkia 56 % (n=15). Jokseenkin moni oli kuitenkin sitä mieltä, etteivät ole niin varmoja kyvystään tunnistaa tietoturvauhkia 37 %. Kohderyhmä ei harjoittelua suorittaneiden tulokset vastaavaan kysymykseen taulukossa 10. Kaikki vastaajat kokivat olevansa tietoisia tai jokseenkin tietoisia 100 % tietoturvauhista tulevassa harjoittelu- tai työpaikassa. Huomattavasti siis enemmän vastaajista ei uskonut kykyynsä verrattuna ei harjoittelua suorittaneisiin taulukossa 10.

Taulukko 9. Kysymys 26 harjoittelun suorittaneiden usko tiedostaa tietoturvauhkia työpaikalla

Tietoinen mahdollisista tietoturvauhista organisaa-tiossa	n	Prosentti
Kyllä	15	56 %
En	2	7 %
En tiedä	10	37 %

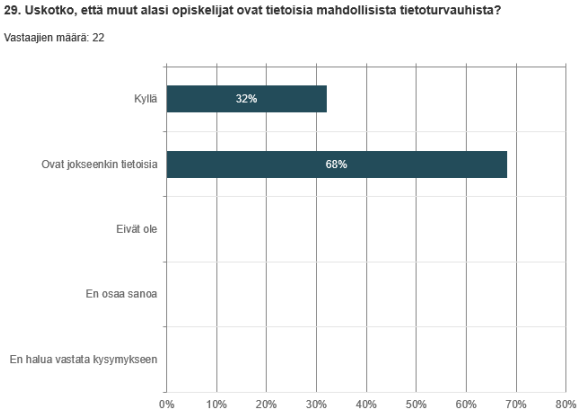
Taulukko 10. Kysymys 27 ei harjoittelua suorittaneiden usko tiedostaa tietoturvauhkia tulevassa harjoittelussa

Tietoinen mahdollisista tietoturvauhista organisaatiossa	n	Prosentti
Kyllä	2	22 %
Olen jokseenkin tietoinen	7	78 %
En	0	0 %
En tiedä	0	0 %

Kohderyhmän harjoittelun suorittaneiden uskomukset kollegoidensa kyvystä tunnistaa tietoturvauhkia organisaatiossa (ks. kuvio 19). Tuloksena enemmän epävarmuutta harjoittelussa kollegoiden kykyyn tunnistaa tietoturvaan liittyviä uhkia kuin ei harjoittelua suorittaneiden ryhmässä.

Kuvio 19. Kysymys 28 kohderyhmä harjoittelun suorittaneiden usko työkavereiden kykyyn tiedostaa tietoturvauhkia

Vastaavanlainen kysymys tehtiin kohderyhmään ei harjoittelua suorittaneet. Kysyttiin uskovatko he kanssaopiskelijoidensa kykyä tunnistaa mahdollisia tietoturvauhkia organisaatiossa. Ilmeni 100 % luottamus kohderyhmän ei harjoittelua koulukavereidensa kykyyn tunnistaa tietoturvauhkia (ks. kuvio 20). Ei vielä harjoittelua suorittaneilla vaikuttaa olevan enemmän itsevarmuutta omaan tietoturvakykyynsä kuin harjoittelun suorittaneilla opiskelijoilla.



Kuvio 20. Kysymys 29 kohderyhmä ei harjoittelua suorittaneiden usko koulukavereiden kykyyn tiedostaan tietoturvauhkia

4.2.5 Todelliset uhkakuvat

Kyseisellä kategorialla pyrittiin selvittämään, mitä tarkalleen ottaen kohderyhmät kokivat kriittiseksi tietoturvan voimavaraksi harjoitteluissa. Kyseessä on laajempi väittämien joukko, jossa selvitettiin uskoa todellisista tietoturvauhista seuraavien vuosien aikana harjoittelupaikassa tai tulevassa harjoittelupaikassa. Vastaajien uhkakuvat muistuttivat molemmissa kohderyhmissä hyvin samantyyppiseltä, joissa oli samat korkeimmalle sijoittuneet uhkakuvat.

Mikä seuraavista tietoturvauhista uskot todennäköisimmin realisoituvan seuraavien vuosien aikana harjoittelupaikassasi?	Pro
Väärien tietojen kirjaaminen inhimillisen virheen takia, (esimerkiksi työkiireiden aiheuttamana)	89 %
Väärien tietojen saanti organisaation ulkopuolelta, (esimerkiksi potilaalta itseltään)	48 %
Inhimillisestä virheestä johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi vainajien tietojen jääminen järjestelmään tai entisten työntekijöiden tietojen jääminen järjestelmään)	59 %
Ohjelmiston toiminnasta johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi tilanne jossa järjestelmä on niin monimutkainen)	15 %
Tietoliikenneongelmista aiheutunut väärien tai puutteellisten tietojen kirjautuminen tietojärjestelmään, (esimerkiksi myrskyn aiheuttama sähkökatkos)	33 %
Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen valtuutetun henkilön toimesta (esimerkiksi lääkäri tai hoitaja)	4 %
Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen hoitajan itsensä toimesta, (esimerkiksi helpottaakseen omaa työtään tai muu välinpitämättömyys)	15 %
Valtuuttamattoman henkilön tekemä tietojen tahallinen väärentäminen tietojärjestelmään, (esimerkiksi pääsy järjestelmiin työpaikan tietokoneilla)	0 %
Tietoliikenneyhteyksien vikaantumisesta tai katkoksesta aiheutunut pääsyn estyminen kaikkiin tai osaan tietojärjestelmästä tarvittavista potilastiedoista, (Kuten kyberhyökkäys kriisitilanteessa)	30 %
Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin johtuen tietojärjestelmän vikaantumisesta, (esimerkiksi laitteiston vanhuus tai päivittämättömyys)	44 %
Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin väärin määriteltyjen käyttövaltuuksien takia, (esimerkiksi lääkäri ei pääse tarkastelemaan hoitajan tekemiä kirjauksia)	22 %
Jotain muuta, mitä?	0 %
Ei mitään näistä	0 %
En osaa sanoa	4 %

Kuvio 21. harjoittelun suorittaneiden epäilys todennäköisimmin toteutuvista tietoturvauhista seuraavien vuosien aikana harjoittelupaikassa.

Molemmissa kohderyhmissä samat pääasialliset uhat, joissa on enemmistö valintoja. Kohderyhmässä harjoittelun suorittaneet, väärien tietojen kirjaaminen inhimillisen virheen takia 89 % (n=24), väärien tietojen saaminen asiakkaalta 48 % (n=13) ja inhimillisestä virheestä johtuvat vanhentuneet merkinnät tietojärjestelmässä 59 % (n=16) (ks. kuvio 21). Kohderyhmässä ei harjoittelua, väärien tietojen kirjaaminen inhimillisen virheen takia 86 % (n=18), väärien tietojen saaminen asiakkaalta 62 % (n=13) ja inhimillisestä virheestä johtuvat vanhentuneet merkinnät tietojärjestelmässä 76 % (n=16). (ks. kuvio 22).

Mitä seuraavista tietoturvauhista uskot todennäköisimmin realisoituvan seuraavien vuosien aikana tulevissa harjoittelupaikoissasi?	Prose
Väärien tietojen kirjaaminen inhimillisen virheen takia, (esimerkiksi työkiireiden aiheuttamana)	86 %
Väärien tietojen saanti organisaation ulkopuolelta, (esimerkiksi potilaalta itseltään)	62 %
Inhimillisestä virheestä johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi vainajien tietojen jääminen järjestelmään tai entisten työntekijöiden tietojen jääminen järjestelmään)	76 %
Ohjelmiston toiminnasta johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi tilanne jossa, järjestelmä monimutkainen ja ylivoimainen tehtävä johon ei työkiireen takia nähdä vaivaa)	48 %
Tietoliikenneongelmista aiheutunut väärien tai puutteellisten tietojen kirjaaminen tietojärjestelmään, (esimerkiksi myrskyn aiheuttama sähkökatkos)	52 %
Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen valtuutetun henkilön toimesta (esimerkiksi lääkäri tai hoitaja)	5 %
Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen hoitajan itsensä toimesta, (esimerkiksi helpottaakseen omaa työtään tai muu välinpitämättömyys)	10 %
Valtuuttamattoman henkilön tekemä tietojen tahallinen väärentäminen tietojärjestelmään, (esimerkiksi pääsy järjestelmiin työpaikan tietokoneilla)	19 %
Tietoliikenneyhteyksien vikaantumisesta tai katkoksesta aiheutunut pääsyn estyminen kaikkiin tai osaan tietojärjestelmästä tarvittavista potilastiedoista, (Kuten kyberhyökkäys kriisitilanteessa)	52 %
Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin johtuen tietojärjestelmän vikaantumisesta, (esimerkiksi laitteiston vanhuus tai päivittämättömyys)	52 %
Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin väärin määriteltyjen käyttövaltuuksien takia, (esimerkiksi lääkäri ei pääse tarkastelemaan hoitajan tekemiä kirjauksia)	52 %
Jotain muuta, mitä?	0 %
En mitään näistä	0 %
En tiedä	5 %

Kuvio 22. Kysymys 33 ei harjoittelua suorittaneiden epäilys todennäköisimmin toteutuvista tietoturvauhista seuraavien vuosien aikana harjoittelupaikassa

Uhkakuvien viimeisenä kysymyksenä selvitettiin kohderyhmältä harjoittelun suorittaneet taulukossa 11, mitä tietoja he uskoivat pahantekijän tavoittelevan sosiaaliterveysalan harjoittelupaikasta. Asiakas- ja potilastiedot nousivat jälleen korkeimmaksi valituksi uhkakuvaksi 81 % (n=22).

Taulukko 11. Kysymys 34 harjoittelun suorittaneiden epäilys siitä mitä rikollinen tavoittelee työpaikalta.

Harjoittelijoiden usko siitä mitä tietoja pahantekijä tavoittelee organisaatiosta	n	Prosentti
Työpaikan järjestelmien salasanoja	6	22 %
Asiakas- ja/tai potilastietoja	22	82 %
Henkilökunnan tietoja	7	26 %
Rajoitettua palvelutietoa	2	7 %
Työpaikan verkkoon liittyvää rajoitettua tietoa ja siihen kiinnitettyjä laitteistoja	5	19 %
En osaa sanoa	7	26 %
Jotain muuta, mitä?	0	0 %

4.2.6 Opinnolliset tarpeet

Kategorialla haluttiin selvittää, mitä opiskelijat kokivat tarpeelliseksi oppia ennen harjoitteluun siirtymistä. Lisäksi mitä yhtäläisyyksiä kohderyhmillä on. Esimerkiksi mitä harjoittelun suorittaneet kokevat tarpeelliseksi parantaa tietoturvaosaamisessaan harjoittelun päätteeksi. Tulokset saattavat kertoa vastaajien itseluottamuksesta ja kyvystä tiedostaa tietoturvaan liittyvien asioiden tunnistamista. Taulukot 12 ja 13 havainnollistaa molempien kohderyhmien vastaukset.

Taulukko 12. Kysymys 35 harjoittelun suorittaneiden henkilöstön tietoturvakoulutus viimeisen vuoden aikana

Henkilöstön tietoturvakoulutus harjoittelun suorittaneet	n	Prosentti
Kyllä	5	19 %
Ei	3	11 %
En osaa sanoa	19	70 %

Taulukko 13. Kysymys 36 kohderyhmän ei harjoittelua suorittaneiden lisäkoulutustarve

Tutkintoon kuuluva tietoturvakoulutus	n	Prosentti
Kyllä	6	17 %
On jokseenkin	25	69 %
Ei	4	11 %
En osaa sanoa	1	3 %

Selvitimme taulukossa 14, mitä harjoittelun suorittaneet ovat mieltä tietoturva- ja tietosuojakoulutuksesta JAMK:ssa. Tietosuoja 44 % ja turvallisen etätyönohje 48 % nousivat halutuimmiksi koulutustarpeiksi harjoittelun suorittaneiden ryhmässä. Erikoinen tulos kun terveysalalla harvemmin uskoisi olevan etätyölle mahdollisuutta. Tietosuojaan liittyvät vastaukset taulukossa 14 lisää miettimisen aihetta onko harjoittelussa tarpeeksi tietosuojaan perehdytystä.

Taulukko 14. Kysymys 37 kohderyhmä harjoittelun suorittaneet lisäkoulutustarve valikkopohjainen

Mistä osa-alueista haluaisit lisäkoulutusta	n	Prosentti
Salasanat	4	15 %
Turvallisten ja haitallisten nettisivujen tunnistaminen	10	37 %
Tietosuoja	12	44 %
Turvallisten ja haitallisten sähköpostilinkkien tunnistaminen	8	30 %
Somen käyttöopas	6	22 %

Turvallisen etätyön ohje	13	48 %
Lainsäädäntö liittyen tietosuojaan ja tietotekniikkarikoksiin	12	44 %
Jotain muuta, mitä?	0	0 %
En osaa sanoa	3	11 %
En tarvitse lisäkoulutusta	2	7 %

Kohderyhmän ei harjoittelua suorittaneet lisäkoulutustarve laajempi valikkopohjainen selvitys. Kysymykseen sama vastaus etätyöstä kuin harjoittelun suorittaneilla. Korona-ajalla voi olla näihin vastauksiin jonkin verran vaikutusta miksi etätyö koetaan nyt tärkeäksi. Jälleen taulukossa 15 huomattavasti enemmän vastaajista (ei harjoittelua suorittaneissa) kokevat yleisesti lisäkoulutustarpeen vähemmän tärkeämmäksi. Ei harjoittelua suorittaneilla on enemmän itseluottamusta tietoturvaosaamiseen kuin harjoittelun suorittaneilla.

Taulukko 15. Kysymys 38 kohderyhmä ei harjoittelua lisäkoulutustarve valikkopohjainen

Millä osa-alueella haluat lisäkoulutusta	n	Prosentti
Salasanat	0	0 %
Turvallisten ja haitallisten nettisivujen tunnistaminen	6	29 %
Tietosuoja	4	19 %
Turvallisten ja haitallisten sähköpostilinkkien tunnistaminen	6	29 %
Somen käyttöopas	2	10 %
Lainsäädäntö liittyen tietosuojaan ja tietotekniikkarikoksiin	6	29 %
Turvallisen etätyön ohje	12	57 %
En tarvitse lisäkoulutusta	4	19 %
En osaa sanoa	1	5 %
Jotain muuta, mitä?	0	0 %

5 Yhteenveto

Tutkimuksessa selvitettiin Jyväskylän ammattikorkeakoulun harjoittelun suorittaneiden sosiaaliterveysalanopiskelijoiden tietoturvaosaamista. Haluttiin selvittää harjoittelun vaikutusta tähän tietoturvaosaamiseen. Halusimme lisäksi selvittää miten tietoturvaosaamista olisi mahdollista kehittää

ennen harjoittelun aloittamista. Kyselyyn vastausten perusteella on syytä kyseenalaistaa tutkimuksen laadukkuutta, sillä vastauksia kyselyyn saatiin aika hyvin, mutta vastausten jakautuminen kysymysnumeroiden mukaan vaihteli suuresti. Varsinkin kyselyn loppua kohden vastaajia oli noin puolet verrattuna alkukysymysten vastausten määrään. Tämä seikka on syytä ottaa huomioon, jos tästä tutkimuksesta meinaa tehdä johtopäätöksiä tulevaisuudessa. Kyselyssä oli paljon hyviä kysymyksiä ja ne oli lähtökohtaisesti hyvin jaoteltu kategorioittain. Harmillisesti kyselyssä oli myös muutama liian isoja kysymyksiä, joissa mahdollisten vastauksien määrä oli liian iso ja joissa väittämät vain pintapuolisesti koskivat aihealueen rajausta. Isommat kysymykset olivat laadittaessa mielenkiintoisen kuuloisia mutta vaikeasti analysoitavissa jälkeenpäin. Liian isot kysymykset myös karkottivat vastaajia pois kyselystä tai hyppäämään yli niistä kysymyksistä. Jos isot kysymykset olisi tehty pakolliseksi, olisi toki voinut olla teoriassa mahdollista saada eri suuruinen vastausten lukumäärä.

Tiivistetysti opiskelijoilla, jotka eivät ole olleet harjoittelussa on enemmän uskoa omaan ja vertaistensa tietoturva- ja tietosuojaosaamiseen kuin heillä, jotka ovat olleet harjoittelussa. Vaikuttaa että näin ollen harjoittelulla on tapana aiheuttaa epäilystä omaan ja vertaisten kyvykkyyteen tietoturvaosaamisessa. Syitä tähän voi olla alalla vallitsevat heikot työolosuhteet. Suurin osa kyselyyn vastanneista olivat sairaanhoitaja harjoittelun käyneitä (n=15) 31 %. Anonyymin sairaanhoitajan kommenttien sekä ”jotain muuta, mitä”-osioon vastausten perusteella, sairaanhoitajan työssä tehdään tietojärjestelmiin merkintöjä jokaisesta palveluun kuuluvasta tilanteesta. Osastolla kiireiden vuoksi merkintöjä ei aina keretä tehdä ja data järjestelmiin jää puutteelliseksi. Kuviossa 21 havainnollistaa harjoittelussa käyneiden suurimmaksi tietoturvariskiksi inhimillisen virheen takia aiheuttaman väärän kirjauksen järjestelmään 89 %. Toisena vanhentuneiden tietojen jääminen järjestelmään 59 %. Väärien tietojen merkitseminen tietojärjestelmiin on siis merkittävä tietoturvariski harjoittelun suorittaneilla.

Suurena osaamisen puutteena voidaan pitää yleistä tietoisuutta tietoturvaan liittyviin asioihin etenkin omien laitteiden käyttämistä työasioiden hoitamiseen. Moni ilmoitti kysymyksissä, miten he käyttävät omia henkilökohtaisia laitteitaan työasioiden hoitamiseen, joka viestii merkittävästä tietoturvaongelmasta terveydenhuollolle. On myös huomioitava, että kotiolosuhteissa perheenjäsenet saattavat käyttää satunnaisesti työpuhelinta mikä saattaa johtaa rajoitetun sisällön paljastu-

miselle. Aikaisemmassa tutkimuksessa, jossa on käsitelty saman alan opiskelijoiden tietoturva-osaamista, Maliniemi (2021) kertoo että, isoimpana osaamisen puutteena pidetty salasanojenhallintaa. Samassa tutkimuksessa on huomattu, että opiskelijoille on mahdollisesti ohjeistettu, ettei työpaikan langatonta verkkoa kannata käyttää omilla laitteilla. Eli langattoman verkon käyttö on työpaikalla jo tutkitusti matalaa. Eli on siis todennäköisempää, että vastaajat käyttävät henkilökohtaisia laitteitaan työpaikan ulkopuolella. Esimerkiksi työsähköposteihin vastaamiseen. On myös oleellista huomioida, että muut perheenjäsenet käyttävät ja saattavat tietää tunnukset jopa työtietokoneille. Koska kyseinen huomio tehtiin harjoittelun tehneiden kohderyhmään niin harjoittelulla ei näin ole ollut siihen osaamiseen vaikutusta.

Yhteenveto taulukoista 6–7 tarkoittaisi, että monissa harjoittelupaikoissa on käytössä langalliset tietoverkot verkon kytkentään. Kannettavat tietokoneet olivat kuitenkin molemmissa kohderyhmissä suosittu valinta. Voidaan siis tehdä johtopäätös, että WLAN-verkkoon kirjaudutaan pääsääntöisesti langattomalla yhteydellä langallisen verkon sijasta, joka yleisesti nostaa käyttäjien tietoturvariskiä. (Badman 2021)

Älypuhelinten korkea käyttöaste molemmissa kohderyhmissä voi viitata tottumukseen käyttää esimerkiksi työsähköpostien lukemiseen omaa henkilökohtaista älypuhelinta tai työpaikan tarjoamaa puhelinta. Vastaavasti ei harjoittelua suorittaneilla esimerkiksi oppilaitoksen sähköposteja luetaan omalla älypuhelimella. Voidaan arvella, että harjoittelun suorittaneilla on tietoturvaohjeistuksessa sääntönä käyttää työpaikalla pöytätietokoneen kautta nettiyhteyttä tai sitä vähintäänkin kuuluu suosia tietyissä työtehtävissä. Kannettavan tietokoneen suosiota voidaan pitää edelleen tavallisena toimintatapana mikä mahdollistaa paremman liikkuvuuden työtehtävissä. Tutkimuksen kannalta tärkeintä on että, otetaan huomioon kaikki tilanteet, joissa tietoturvallisempaan käyttäytymiseen pyritään ohjaamaan. Tietoturvan toteutuminen kotona sekä työelämässä on opinnäytetyön hyödynnettävyyden kannalta vähemmän olennaista kuin se, miten itse harjoittelulla on vaikutusta opiskelijoiden tietoturvakäsitykseen.

Ero kohderyhmän harjoittelussa olleiden käsityksestä noudattaa ohjeita on hiukan huolestuttava. Lähes 1/5 vastanneista ei osannut sanoa pitääkö ohjeistusta noudattaa. Tietysti tietoturvaohjeet

voi esittää erilaisena ohjeena eri työpaikoissa ja käsitteet voivat vaihdella. Selkeämpi käsitys tietoturvaohjeeseen kohderyhmän (ei harjoittelua suorittaneet) vastauksissa viittaa miten harjoittelupaikoissa saattaa olla epäselvemmät ohjeet tietoturvaohjeita laadittaessa.

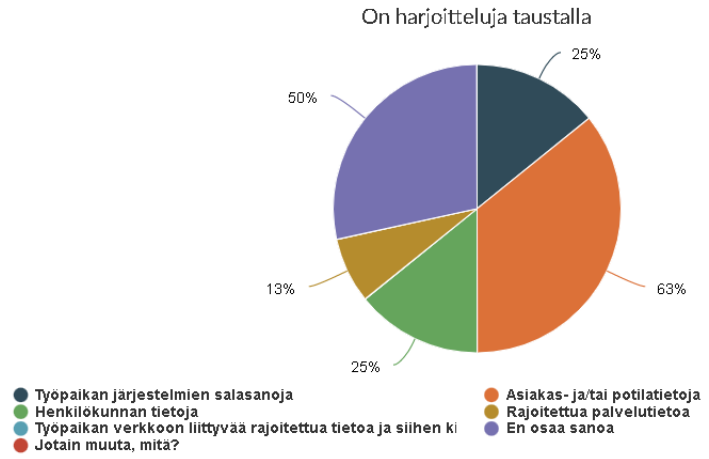
Fyysisen ympäristön turvallisuus terveydenhuollon organisaatiossa muodostaa korvaamattoman kokonaisuuden sen tietoturvan kannalta. Siihen kohdistuu monimuotoisia uhkia, joita Tammisalon (2005) raportista nostan esille muutamia:

a) Tiloissa säilytetään sinne kuulumatonta materiaalia tai tavaroita
b) Ulkopuolisia henkilöitä pääsee organisaation tiloihin vastaanottotiskin tai turvatarkastuksen ohi
c) Ovia ei pidetä lukittuna henkilökunnan tiloihin
d) Työympäristössä ei ole kulunvalvontaa
e) Tiloihin kuuluvilla henkilöillä ei ole näkyviä tunnisteita tai työvaatteita, kuuluuko hän organisaatioon vai onko hän vierailija
f) Arkaluonteisia tietoja jätetään työhuoneisiin tai neuvottelutiloihin lukitsematta ja/tai näkyville
g) Vierailijoilla ei ole saattajaa
h) Ohikulkijat näkevät heille kuulumatonta materiaalia työpöydiltä, näytöltä tai kuulee tietoja puhelusta
i) Työkoneisiin on asennettu niihin kuulumattomia ohjelmistoja tai liitännäisiä selaimeen
j) Laitteisto vikaantuu puutteellisen puhdistamisen takia
k) Henkilökunta ei huolehdi riittävällä tasolla avaimistaan tai kulkukorteistaan
l) Tietojärjestelmät ovat sijoitettu tiloihin joihin ulkopuolisilla on teoriassa mahdollisuus niitä käyttää
m) Organisaation tietokoneet ovat mahdollista varastaa, kun ne eivät ole lukittuna työpisteisiin fyysisesti

Harjoittelun suorittaneet kokevat fyysisen ympäristön kehittämisen suurimmaksi kehitystarpeeksi harjoitteluorganisaatiossa. Tämä sama tulos osoittautui korkeimmaksi molemmissa AMK ja YAMK vastaajissa. Toinen merkittäväksi koettu tietoturvallisuuden puute organisaatiossa oli poikkeustilanteiden ja ongelmatapahtuminen hallinta. Merkittävintä tietoturvaan liittyvissä ongelmatilanteissa olisi se, miten terveydenhuoltohenkilöstö reagoi niihin. Eli miten havaituista tietoturvapoikkeamista tai loukkauksia raportoidaan eteenpäin asianmukaiselle vastaavalle tai tuelle. Eikä niitä jäädä pohtimaan pienen henkilöstön kesken liian pitkäksi aikaa. Tarkoittaako kyselyn tulos sitä, etteikö henkilöstölle ole ollut tiedossa kenelle mahdollisista tietoturvaan liittyvistä ongelmatilanteista ole kuuluu raportoida tai onko raportointi jäänyt kiireen tai muun syyn johdosta tekemättä. Muutamia poimintoja Tammisalon (2005) raportista liittyen poikkeustilanteiden uhkista terveydenhuollon organisaatiossa:

a) Tietoturvapoikkeamista tai havaituista loukkauksista raportoiminen ylemmälle toimihenkilölle on jäänyt tekemättä määrittelemättömästä syystä
b) Henkilöille havaitsemille rikkeille ei ole sovittu käytäntöä tai niistä ei ole merkintää tietoturvaohjeistuksessa
c) Puutteellisen valtuuttamisen johdosta terveydenhuollon henkilökunta pääsee muuttamaan tapahtumatietoja järjestelmässä
d) Vanhoja tapahtumatietoja ei säilytetä riittävän tietoturvallisesti
e) Seurannasta ei synny hälytyksiä
f) Hälytykset eivät käynnistä korjaustoimenpiteitä eikä muita seuraamuksia
g) Organisaation henkilöstö on työolosuhteiden johdosta ylikuormitettu eikä aikaa jää pohtia tietoturvaan liittyviä poikkeustilanteita
h) Organisaation kulttuurissa ei pidetä riittävän tärkeänä tieturvapoikkeamiin liittyviä asioita
i) Henkilökunnalle ei ole tiedossa minkälainen tietoturvapoikkeama voisi olla
j) Henkilökunnalle ei ole informoitu mahdollisista tietoturvaan liittyvistä poikkeamista tarpeeksi
k) Henkilökunta ei ole saanut tarpeellista koulutusta tietoturvaan liittyvissä asioissa

Verrattiin kysymystä 34. niihin, jotka vastasivat kysymykseen 10 käyttävänsä henkilökohtaisia laitteitaan työasioihin. Suodatetulla vastaajilla ”Kyllä” kysymykseen 10 vastasivat kysymyksessä 34. (ks. kuvio 23)



Kuvio 23. Kysymykseen 10 kuviossa 5 vastannut "kyllä". Kysymys 34 epäilys siitä mitä pahantekijä tavoittelee työpaikalta.

Merkittävästi enemmän vastaajia ei osannut sanoa 50 % mitä pahantekijät tavoittelevat työpaikan ympäristöstä. Ilman suodatusta vastanneissa 26 % ei osannut sanoa mitä rikollinen tavoittelee harjoitteluympäristössä. On siis isompi todennäköisyys vastaajalla olla tietämätön harjoittelussa mah-

dollisista tietoturvauhkista, jos hän käyttää omia laitteitaan työasioihin. Korostaa joko tietämättömyyttä tai tietoturvaan tai osaamisen puutetta. Kokonaisuudessaan merkittävä riski työorganisaatiolle.

6 Kehittämisehdotukset

Kyselyssä otettiin selvää opiskelijoiden omasta näkemyksestä kehitettäviin asioihin, joista saatiin kerättyä seuraavanlainen kehityslista. Opiskelijat kokivat turvallisen etätyöohjeen kaikista merkittävimmäksi tietoturvaosaamista lisääväksi aihealueeksi. Tämä sama huomio tehtiin molempien kohderyhmien kysymyksissä. Toiseksi harjoittelun suorittaneet kokivat kehitystarpeiksi tietosuojan sekä tietosuojalainsäädännön toisin kuin ei harjoittelua suorittaneet. Vastanneilla esiintyi epätietoisuutta niin tietoturvan perusteissa kuin tietoturvalainsäädännössä. Vastaavanlainen huomio on tehty Tiittanen (2013) opinnäytetyössä. Eli joko organisaation tietosuojaohjeistuksessa on puutteita tai siitä halutaan lisäohjeita. Voi myös olla, ettei tietosuojaohjeistusta ole riittävästi läpikäyty harjoittelussa opiskelijoille. Fyysisen ympäristön turvallisuus sekä poikkeustilanteisiin reagoiminen pidettiin harjoittelijoiden ryhmässä isoimpina kehitystä vaativina osa-alueina. Tietosuojaohjeiden päivittäminen oli myös yksi valituimmista aiheista.

Edellisissä tutkimuksissa Maliniemi (2021), jossa sama aihealue on tehty huomio vanhempien ikäryhmien opiskelijoiden olevan itsevarmempia omasta osaamisestaan tietoturvassa. Myös ohjeistuksen määrää on pidetty liiallisena. Lisäksi salasanojen ylläpitoa on pidetty puutteellisena samassa tutkimuksessa. Maliniemen (2021) tutkimuksessa ei selvinnyt onko itseluottamus ja tietoturvaosaamisen oikeaa osaamista vai onko se itseluottamus puutteellista osaamista. Vastaavaan ilmiöön törmättiin tässäkin tutkimuksessa, kun kysymykset eivät mitanneet opiskelijoiden oikeaa osaamista vaan uskoa, asenteita, uhkakuvia ja omia näkemyksiä kehitysehdotuksista. Olisikin tulevaisuudessa hyvä kartoittaa terveydenhuollon opiskelijoiden osaamista mittaava tutkimus tietoturva-asioihin, joihin he saattavat törmätä työelämässä.

Tutkimuksessa nousseita asioita voidaan käyttää hyödyksi mahdollisia uusia opetussuunnitelmia laadittaessa. On mahdollista, että vastanneiden omat näkemykset osaamisestaan ei vastaa tietoturvan periaatteisiin kuviossa 2. Olisikin mielekästä tehdä tutkimus vastanneiden oikeasta osaamisesta tulevissa tutkimuksissa. Mahdollisia kehityskohteita opiskelijoiden osaamiseen parantamiseen voisi olla omien laitteiden käytöstä työasioihin koituvien tietoturvariskien kouluttaminen.

Myös langattoman verkon käytöstä koituvia riskejä olisi syytä kouluttaa. Sekä yleisesti järjestelmien kirjaamiseen liittyvistä riskeistä, jos data jää puutteelliseksi tietojärjestelmään. Mahdollisesti myös organisaatioiden vanhojen tietoturvaohjeiden läpikäyminen oppilaitoksessa ennen harjoittelua.

7 Pohdinta

Tutkimuksen yhtenä tarkoituksena oli tarkastella, onko harjoittelulla vaikutusta tietoturvaosaamiseen. Tähän pyrittiin löytämään vastauksia kyselylomakkeen eri kategorioilla sekä vertaamalla opiskelijoihin, joilla ei ollut harjoittelukokemusta. Parhaimmaksi kategoriaksi tässä osoittautui uskomusten osio. Huomasimme että harjoittelun suorittaneilla oli enemmän epäilyksiä itsensä sekä vertaistensa tietoturvaosaamisesta, kuin niillä ketkä eivät olleet suorittaneet harjoittelua. Huomattavaa oli myös, että ennen harjoittelua opiskelijoilla oli tunnollisempi osaaminen verkon JAMK:n tietoturvaohjeistuksesta, kuin niillä ketkä olivat harjoittelussa perehtyneet työpaikan tietoturvaohjeisiin. Jos katsomme tuloksia, suoraa vastausta emme löytäneet tähän kysymykseen muissa osioissa mutta viitteitä kriittisistä tietoturvapuutteista löydettiin molemmissa kohderyhmissä.

Tutkimuksen toisena tarkoituksena oli selvittää terveydenhuollon harjoittelun suorittaneiden opiskelijoiden tietoturvaosaamista. Tässä mielestäni onnistuttiin paremmin ja löydettiin heikkouksia osaamisessa. Kuten omien laitteiden käyttämistä työasioihin sekä tietosuojaohjeiden ymmärtämisen puutetta. Positiivisena asiana huomasimme, miten molemmat kohderyhmät pitivät potilas- ja asiakastietoja tärkeimpinä suojeltavina voimavaroina harjoittelupaikassa. Molemmat kohderyhmät suhtautuivat myös hyvin vakavasti yleisimpiin tietoturva- ja tietosuojariskeihin. Negatiiviseksi asiaksi muodostui opiskelijoiden omat näkemykset harjoittelupaikan tietoturvapuutteista. Kuten fyysisen ympäristön turvallisuus sekä poikkeustilanteisiin reagoiminen harjoittelussa.

Kyselyn luominen itsessään on hyvä tehdä monen henkilön toimesta. Useamman on hyvä ottaa siihen kantaa ennen kuin sen lähettää liikkeelle. Kyselyn laittaminen eteenpäin on myös lopullinen valinta sillä vastaajia voi olla vain rajattu määrä niin eivät jaksa uudestaan vastata samanlaiseen kyselyyn. Mielestäni jäi olennaisia ja muuten hyviä kysymyksiä kyselystä pois koska ne tulivat mieleen vasta jälkeenpäin. Muutamia mielestäni kelvollisia kysymyksiä mitä olisi voinut käyttää tutkimuskyselyssä:

- Yleisesti on tuntemuksesi siitä, onko oma tietoturva- tai tietosuojaosaamisesi parantunut harjoittelun johdosta.
- Vaikuttaako alan yleinen terveysalan palkkataso motivaatioosi tiedostaa tietoturvaan tai tietosuojaan liittyviä asioita?
- Käytän lähes vastaavanlaista salasanaa pakollisen 3kk salasanavaihdon yhteydessä, muutan siihen vain jonkun tietyn numeron tai ison kirjaimen. Kyllä/Ei.
- Mikä on työyhteisösi suhtautuminen tietoturva- tai tietosuojatyyppisiin asioihin?
- Vaikuttaako työyhteisön ilmapiiri negatiivisesti tietoturva- tai tietosuojasuhtautumiseen?
- Mikä on oma, arvioisi tietoturva- ja tietosuojaosaamisen tasostasi harjoittelun päätteeksi?
- Onko JAMK:n tietoturvakoulutuksella ollut vaikutusta tietoturvaosaamiseesi harjoittelussa?
- Onko tietoturvaosaamisesi mielestäsi riittävä harjoittelun läpikäymiseen?
- Ymmärrätkö tietoturvan merkityksen omassa työssäsi?

Olisi ollut mielekästä kysellä kohderyhmiltä heidän motivaatioonsa vaikuttavia seikkoja tietoturvaosaamisessa. Myöskin heidän mielipiteensä itse kokemastaan tietoturvaosaamisen tasosta harjoittelussa ja sen jälkeen. Vielä parempi jos samoilta henkilöiltä olisi voinut saada vastauksen ennen harjoittelua ja sen päätteeksi. Jälkimmäisessä tapauksessa olisi pitänyt aikatauluttaa tutkimusta huomattavasti pidemmäksi.

Työssä mielestäni onnistuttiin löytämään puutteita osaamisessa, joita pystytään tulevaisuudessa kehittämään esimerkiksi koulutusta parantamalla. Selkein ero tämän tutkimuksen nojalla harjoittelulla on aiheuttaa terveydenhuollon opiskelijoissa epävarmuutta tietoturvaosaamisessa. Hyödylliseksi asiaksi osoittautui keskustelu JAMK:n opettajan kanssa, jossa otettiin selvää CampusOnlinen kurssitarjonnasta. Digitaalinen turvallisuus ja kyberuhat terveysalalla -kurssi on tällä hetkellä vapaasti valittavissa opinnoissa terveysalan opiskelijoille. JAMK:lla on tällä hetkellä yhdellä ICT-valmiudet kurssilla tietoturvaan tai tietosuojaan liittyvää opetusta. Jos CampusOnlinen kurssi tulee osaksi pakollisia kursseja sillä voisi olla merkittävää vaikutusta terveydenhuollon opiskelijoiden tietoturvaosaamisessa.

Lähteet

1150/161/2021. Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen. Viitattu 05.05.2022. https://finlex.fi/fi/viranomaiset/tsv/2021/20211183?search%5Btype%5D=pika&search%5Bpika%5D=vastaamo

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Tallinna: Tietosanoma.

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Andress, J. 2011. The Basics of Information Security, 1–16

Badman L. 2021. What is the difference between WLAN and Wi-Fi? Viitattu 17.04.2022. https://www.techtarget.com/searchnetworking/answer/Wireless-vs-Wi-Fi-What-is-the-difference-between-Wi-Fi-and-WLAN

Barajas, O. 2014. How the Internet of Things (IoT) Is Changing the Cybersecurity Landscape. Viitattu 04.04.2022. https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/

CISCO, 2021. The modern cybersecurity landscape: Scaling for threats in motion. Viitattu 30.04.2022. https://learn-umbrella.cisco.com/technical-paper-library/the-modern-cybersecurity-landscape-scaling-for-threats-in-motion , pdf.

DNV. N.d. The three-pillar approach to cyber security: Data and information protection. Viitattu 30.4.2022. https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683

Huoltovarmuuskeskus. 2021. Organisaation verkkosivut. Viitattu 27.11.2021. https://www.huoltovarmuuskeskus.fi/organisaatio/huoltovarmuuskeskus/

Holmes, R. 2022. Cybersecurity Vs. Information Security: Is There A Difference? Viitattu 05.04.2022. https://www.bitsight.com/blog/cybersecurity-vs-information-security

Huusko, J. 2020. Terveydenhuoltoon kohdistuvat tietomurrot lisääntyvät, Yhdysvallat varoittaa – Tietoturva-yhtiön mukaan ainakin 400 sairaalaan tehty tietomurtoja viime viikkojen aikana. Viitattu 27.11.2021. HS tilaajille. https://www.hs.fi/ulkomaat/art-2000006707701.html

Johnson, J. 2021. Number of healthcare data breaches involving the loss of 500 or more records in the United States from 2009 to 2020. Statista. Viitattu 27.11.2021. https://www-statista-com.ezproxy.jamk.fi:2443/study/50995/health-care-and-cyber-security/ Statista Dossier, dia-15.

Kailio, A. 2021. Milloin tietovuodosta pitää kertoa myös potilaalle? Tietosuojavaltuutettu antoi ohjeen. Viitattu 10.01.2022. https://www.tivi.fi/uutiset/milloin-tietovuodosta-pitaa-kertoa-myos-potilaalle-tietosuojavaltuutettu-antoi-ohjeen/64a2bb65-4bf3-4480-b8e5-ff4980d1adec

Kaspersky. N.d. What is Cyber Security? Viitattu 16.01.2022. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lagasse, J. 2019. Close to one-third of healthcare employees have never received cybersecurity training, report shows. healthcarefinancenews.com. Viitattu 27.11.2021. https://www.healthcarefinancenews.com/news/close-one-third-healthcare-employees-have-never-received-cybersecurity-training-report-shows

Lehto, M., Kari, M. Sederholm, T. & Laitinen, T. 2019. Terveydenhuolto ja kyberuhkat. Jyväskylän yliopisto, Informaatioteknologian tiedekunta. Viitattu 27.11.2021. https://www.researchgate.net/publication/331659598_Terveydenhuolto_ja_kyberuhkat

Lehto, M., Limnéll, J. Innola, E. Pöyhönen, J. Rusi, T. & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Viitattu 27.11.2021. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja. Valtioneuvoston kanslia. https://valtioneuvosto.fi/-//10616/suomen-kyberturvallisuuden-nykytila-tavoitetila-ja-tarvittavat-toimenpiteet-tavoitetilan-saavuttamiseksi

Lehto, M., Pöyhönen, J. & Lehto, M.2019. Kyberturvallisuus sosiaali- ja terveydenhuollossa. Viitattu 05.12.2021. https://jyx.jyu.fi/handle/123456789/63325

Liikenne- ja turvallisuusvirasto (TRAFICOM). 2020. SUOSITUS KYBERTURVALLISUUDEN EDISTÄMISESTÄ RAIDELIIKENTEESSÄ. Viitattu 30.04.2022. https://www.traficom.fi/fi/saadokset/suositus-kyberturvallisuuden-edistamisesta-raideliikenteessa

Liikenne- ja turvallisuusvirasto (Kyberturvallisuuskeskus). Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 30.04.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Lundgren, B. & Möller, N. 2017. Defining Information Security. Viitattu 16.01.2022. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6450831/

Maliniemi, T. 2021. Kyberturvallisuusosaaminen ja -suhtautuminen sosiaali- ja terveysalan opiskelijoiden keskuudessa. Viitattu 07.05.2022. Opinnäytetyö. Jyväskylän ammattikorkeakoulu. https://www.theseus.fi/handle/10024/503262

Mattila, J., Ali-Yrkkö, J. & Seppälä T. 2020. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? Viitattu 05.12.2021. https://www.etla.fi/julkaisut/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/

N.a. 2015. Määrällinen tutkimus. Viitattu 27.11.2021. Koppa Jyväskylän yliopisto. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus

NICCS. 2022. Explore Terms: A Glossary of Common Cybersecurity Words and Phrases. Viitattu 30.04.2022. https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C

Saarimäki, J. 2019. TOP 5 tietoturvauhat ja -ratkaisut organisaatioille. Viitattu 23.11.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/top-5-tietoturvauhat-ja-ratkaisut-organisaatioille

Susi, M & Taipalkoski, J. Kyberturvallisuuden maailmaan on syytä tutustua jo pienenä. Viitattu 20.8.2021. https://teknologiateollisuus.fi/fi/ajankohtaista/kyberturvallisuuden-maailmaan-syyta-tutustua-jo-pienena

Tammisalo, T. 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Viitattu 04.05.2022. Raportteja 5/2005. https://www.julkari.fi/bitstream/handle/10024/76288/Ra5-2005.pdf?sequence=1&isAllowed=y

Tietosuojavaltuutetun Toimisto. 2020. TIETOSUOJA. Viitattu 16.01.2022. https://tietosuoja.fi/tietosuoja

Tiittanen, A. 2013. Terveysalan opiskelijoiden käsitykset tietoturvasta ensimmäisen opiskeluvuoden jälkeen. Viitattu 02.05.2022. Opinnäytetyö, s43. https://www.theseus.fi/handle/10024/53957

Tilastokeskus, Yritysrekisteri. 2019. Suomen yrittäjät. Viitattu 05.05.2022. https://www.yrittajat.fi/yrittajajarjesto/tietoa-yrittajista/yrittajyys-suomessa/

Ulkoministeriö. N.d. Kyberturvallisuus ja kybertoimintaympäristö. Viitattu 30.04.2022. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

Xetnet. 2021. Kyberuhat vuonna 2021–7 yleistä uhkaa yrityksille. Viitattu 04.05.2022. https://www.xetnet.fi/kyberuhat-vuonna-2021-7-yleista-kyberuhkaa-esittelyssa/

Äijö, E. 2018. Tietosuojavaltuutetun työmäärä räjähti kasvuun: terveysalalla tietovuoto-ongelmia ilmoitetaan erityisen paljon. Viitattu 05.12.2021. https://yle.fi/uutiset/3-10299263

Liitteet

Liite 1. Kyselylomakkeen sisältö vastausvaihtoehtoineen kohderyhmittäin

Kohderyhmä 0 (ei harjoittelua)	*Kohderyhmä 1 (Vähintään harjoittelussa)*
1. Jos haluat osallistua kahdenkeskiseen haastatteluun tämän kyselyn sijasta niin, vastaa 'Kyllä' ja jätä tähän yhteystietosi. Haastattelu toteutetaan puhelimitse ja kestää n. 15–30 minuuttia. (Jos vastaat 'Kyllä' ja klikkaat 'Seuraava' ohjaudut automaattisesti kyselyn loppuun yhteystietojen antamista varten.) Vastausvaihtoehdot: - Kyllä - En	**1. Jos haluat osallistua kahdenkeskiseen haastatteluun tämän kyselyn sijasta niin, vastaa 'Kyllä' ja jätä tähän yhteystietosi. Haastattelu toteutetaan puhelimitse ja kestää n. 15–30 minuuttia. (Jos vastaat 'Kyllä' ja klikkaat 'Seuraava' ohjaudut automaattisesti kyselyn loppuun yhteystietojen antamista varten.)** Vastausvaihtoehdot: - Kyllä - En
2. Minkä tutkinnon opiskelija olet? Vastausvaihtoehdot: - Sairaanhoitaja (AMK) - Fysioterapeutti (AMK) - Sosionomi (AMK) - Kätilö (AMK) - Toimintaterapia (AMK) - Sairaanhoitaja (YAMK) - Fysioterapeutti (YAMK) - Sosionomi (YAMK) - Kätilö (YAMK) - Toimintaterapia (YAMK) - Kuntoutuksen ohjaaja (YAMK)	**2. Minkä tutkinnon opiskelija olet?** Vastausvaihtoehdot: - Sairaanhoitaja (AMK) - Fysioterapeutti (AMK) - Sosionomi (AMK) - Kätilö (AMK) - Toimintaterapia (AMK) - Sairaanhoitaja (YAMK) - Fysioterapeutti (YAMK) - Sosionomi (YAMK) - Kätilö (YAMK) - Toimintaterapia (YAMK) - Kuntoutuksen ohjaaja (YAMK)
3. Mikä on ikäsi? Vastausvaihtoehdot: - 18–24 - 25–30 - 31–35 - 36–40 - 41 -	**3. Mikä on ikäsi?** Vastausvaihtoehdot: - 18–24 - 25–30 - 31–35 - 36–40 - 41 -
4. Mikä on sukupuolesi? Vastausvaihtoehdot: - Nainen - Mies - En halua vastata	**4. Mikä on sukupuolesi?** Vastausvaihtoehdot: - Nainen - Mies - En halua vastata
5. Montako harjoittelua olet suorittanut? **(Jos suoritat parhaillaan ensimmäistä harjoittelua niin vastaus = '1–2')** Vastausvaihtoehdot: - En yhtään harjoittelua vielä - 1–2 - 3–4	**5. Montako harjoittelua olet suorittanut?** **(Jos suoritat parhaillaan ensimmäistä harjoittelua niin vastaus = '1–2')** Vastausvaihtoehdot: - En yhtään harjoittelua vielä - 1–2 - 3–4

- 5–6 - 7–8 - Tutkintooni ei kuulu harjoittelua **9. Minkälaisella laitteistolla käytät yleisesti internetiä?** Vastausvaihtoehdot: - Pöytätietokone - Kannettava tietokone - Tabletti - Älypuhelin - Jollain muulla, millä? **11. Käytätkö joskus omia henkilökohtaisia laitteitasi JAMK:n langattomassa verkossa (WIFI)?** Vastausvaihtoehdot: - Kyllä - En - En osaa sanoa **17. Oletko lukenut JAMK:n tietoverkon ohjeistuksen tai oletko siitä tietoinen?** **https://helpdesk.jamk.fi/fi/opas-uudelle-verkon-kayttajalle/** Vastausvaihtoehdot: - Kyllä olen lukenut - Kyllä olen tietoinen siitä mutta en ole lukenut - En - En osaa sanoa **18. Ovatko JAMK:n opiskelijat velvollisia noudattamaan JAMK:n tietoturvaohjeistusta?** Vastausvaihtoehdot: - Kyllä - Ei - En osaa sanoa **19. Onko opetuksessa käyty läpi potilaiden tietosuojaan tai tähän liittyvää ohjeistusta?** Vastausvaihtoehdot: - Kyllä - Kyllä jokseenkin - Olisi voinut käydä enemmän - Ei ole käyty ollenkaan - En osaa sanoa **20. Onko koulun kursseilla otettu huomioon seuraavia tietosuojaan liittyviä aiheita?** Vastausvaihtoehdot: - Potilastietojen ja henkilötietojen käsittely - Salassapito- ja vaitiolovelvollisuus arkaluonteiseen tietoon - Asiakirjojen salassapito - Salassapidosta poikkeaminen	- 5–6 - 7–8 - Tutkintooni ei kuulu harjoittelua **6. Mikä on tai oli harjoittelupaikkasi henkilöstömäärä?** Vastausvaihtoehdot: - 1–4 - 5–9 - 10–19 - 20–49 - 50–99 - 100- **7. Mikä oli työroolisi harjoittelussa?** Vastausvaihtoehdot: - Harjoittelija - Työntekijä - Esimies **8. Minkälaisella laitteistolla harjoittelupaikassasi käytetään tai käytettiin internetiä?** Vastausvaihtoehdot: - Pöytätietokone - Kannettava tietokone - Tabletti - Älypuhelin - Jollain muulla, millä? **10. Oletko joskus käyttänyt omia laitteitasi työasioiden hoitoon?** Vastausvaihtoehdot: - Kyllä - En - En halua vastata kysymykseen **12. Onko harjoittelupaikassasi tietoturvaohjeistus?** Vastausvaihtoehdot: - Kyllä - Ei - En osaa sanoa **13. Ovatko työntekijät velvollisia noudattamaan tietoturvaohjeistusta?** Vastausvaihtoehdot: - Kyllä - Ei - En osaa sanoa **14. Mitkä seuraavista kuuluvat harjoittelupaikkasi tietoturvaohjeistukseen?** Vastausvaihtoehdot: - Harjoittelupaikassa on käytössä salasanojenhallintaohjelmisto - Sosiaalisen median käyttö, (esimerkiksi kielto käyttää sosiaalista mediaa työajalla) - Työsähköpostin käyttö, (esimerkiksi työsähköpostin käyttö vain työasioihin)

- Oikeus saada tietoja
- Ei mitään näistä
- Jotain muuta, mitä?

24. Mitä seuraavista pidät todennäköisinä tietoturvauhkina tulevassa työ- tai harjoittelupaikassasi?

Vastausvaihtoehdot:

1. Epätodennäköinen
2. Mahdollinen
3. Todennäköinen
4. Lähes varma
5. En osaa vastata

Kysymykset:
- Kyberhyökkäyksestä aiheutunut sähkökatkos, medisiinisen laitteen toimintahäiriö tai vikatilanne
- Kyberhyökkäyksestä aiheutunut tietosuojavuoto, (esimerkiksi potilas- tai henkilötiedon paljastuminen)
- Työpaikan henkilöstön heikkojen salasanojen takia aiheutunut hyökkääjän luvaton pääsy järjestelmiin
- Arkaluonteisten tietojen vuotaminen sosiaalisen median kautta, (esimerkiksi työkaveri ottaa työajalla someen kuvan, jossa vahingossa näkyy kollegan kulkukortin käyttäjä-ID)
- Poistuessa työpisteeltä, työaseman auki ja valvomatta jättäminen
- Työpaikalla puhelinsoiton yhteydessä arkaluonteisen tiedon leviäminen
- Työntekijöiden äänekkään keskustelun seurauksena arkaluonteisen tiedon leviäminen
- Työsähköpostiin tulleen haitallisen linkin klikkaaminen
- Laitteistojen tai järjestelmien vanhuudesta johtuva toimintahäiriö, (esimerkiksi päivityksiä ladattaessa laitteiston jumittaminen)
- Työpaikan henkilöstön aiheuttama tahallinen vandalisointi järjestelmiin
- Työpaikan henkilöstön tahaton tietojen poistaminen vahingossa, (esimerkiksi kirjatessa tietoja, vanhojen tietojen poistaminen.)
- Työpaikan henkilöstön luvaton arkaluonteisten tietojen selaaminen, (esimerkiksi tylsyyden aiheuttama satunnaisten potilastietojen surffailu.)
- Jotain muuta, mitä?

27. Uskotko olevasi tietoinen mahdollisista tietoturvauhista tulevassa harjoittelu- tai työpaikassasi?

Vastausvaihtoehdot:
- Kyllä
- Toimitiloihin kulkeminen, (esimerkiksi työtietokoneiden valvominen tai pitäminen lukittujen ovien takana)
- Erillinen tietosuojaohjeistus
- Etätyöohje, (esimerkiksi VPN:n käyttö, VPN:n käytön ohjeet, mitä työkoneelle saa verkosta ladata)
- Järjestelmien tai työtietokoneiden salasanat, (esimerkiksi niiden voimassaoloaika on rajoitettu ja on pakotettu vaihtamaan n-ajan välein; onko salasanojen sisältöä ohjeistettu; jos salasana unohtuu?)
- Virustorjunta työkoneella ja sen säännöllinen päivittäminen
- Varmuuskopiointi, (esimerkiksi onko työkoneilla OneDrive/Dropbox käytössä, onko jokin muu varmuuskopio työtietokoneessa?
- Luottamuksellinen materiaali, (esimerkiksi paperilla olevien potilastietojen/talousasiakirjojen laittaminen erilliseen lukittuun astiaan, josta ne hävitetään turvallisesti)
- Työaseman ja kannettavan työtietokoneen käyttö, (esimerkiksi kun omalta työasemalta poistutaan, työkoneen lukitseminen; tietoturvasuojien käyttö näytöissä; kannettavan koneen jättäminen autoon tai muuten lojumaan huolettomasti.)
- Internetin käyttö työpaikalla, (esimerkiksi työtietokoneella ei ole pääsyä joillekin nettisivuille)
- Vieraat, (esimerkiksi onko vierailla vapaa pääsy tuotantotiloihin)
- Jotain muuta, mitä?
- Työpaikalla ei ollut tietoturvaan liittyvää ohjeistusta
- Ei mitään näistä

15. Perehdytettiinkö harjoittelijat tietosuojaohjeistukseen?

Vastausvaihtoehdot:
- Kyllä
- Ei
- En osaa sanoa

16. Mitä seuraavista on otettu huomioon harjoittelupaikkasi tietosuojaohjeistuksessa?

Vastausvaihtoehdot:
- Potilastietojen ja henkilötietojen lainmukainen käsittely, (esimerkiksi henkilötietoja kerätään asianmukaisesti, lainmukaisesti ja rekisteröityjen kannalta läpinäkyvästi)
- Salassapito- ja vaitiolovelvollisuus, (esimerkiksi henkilötietoja käsitellään luottamuksellisesti ja turvallisesti)
- Virheellisen tiedon päivittäminen, (esimerkiksi epätarkat tai virheelliset tiedot poistetaan tai oikaistaan heti)

- Olen jokseenkin tietoinen - En - En tiedä - En halua vastata kysymykseen **29. Uskotko, että muut alasi opiskelijat ovat tietoisia mahdollisista tietoturvauhista?** Vastausvaihtoehdot: - Kyllä - Ovat jokseenkin tietoisia - Eivät ole - En osaa sanoa - En halua vastata kysymykseen **33. Mitä seuraavista tietoturvauhista uskot todennäköisimmin realisoituvan seuraavien vuosien aikana tulevissa harjoittelupaikoissasi?** Vastausvaihtoehdot: - Väärien tietojen kirjaaminen inhimillisen virheen takia, (esimerkiksi työkiireiden aiheuttamana) - Väärien tietojen saanti organisaation ulkopuolelta, (esimerkiksi potilaalta itseltään) - Inhimillisestä virheestä johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi vainajien tietojen jääminen järjestelmään tai entisten työntekijöiden tietojen jääminen järjestelmään) - Ohjelmiston toiminnasta johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi tilanne jossa, järjestelmä on niin kulunut [huonosti koodattu] että vanhojen tietojen poistaminen on ylivoimainen tehtävä, johon ei työkiireen takia nähdä vaivaa) - Tietoliikenneongelmista aiheutunut väärien tai puutteellisten tietojen kirjaaminen tietojärjestelmään, (esimerkiksi myrskyn aiheuttama sähkökatkos) - Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen valtuutetun henkilön toimesta (esimerkiksi lääkäri tai hoitaja) - Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen hoitajan itsensä toimesta, (esimerkiksi helpottaakseen omaa työtään tai muu välinpitämättömyys) - Valtuuttamattoman henkilön tekemä tietojen tahallinen väärentäminen tietojärjestelmään, (esimerkiksi pääsy järjestelmiin työpaikan tietokoneilla) - Tietoliikenneyhteyksien vikaantumisesta tai katkoksesta aiheutunut pääsyn estyminen kaikkiin tai osaan tietojärjestelmästä tarvittavista potilastiedoista, (esimerkiksi ulkopuolinen vaikuttaja, kuten kyberhyökkäys kriisitilanteessa)	- Henkilötietojen saatavuus, (esimerkiksi kerättävä henkilötieto on vain nimenomaista tarkoitusta varten ja sitä kerätään vain tarpeellinen määrä) - Oikeus saada tietoja, (esimerkiksi potilailla tai asiakkailla oikeus saada tieto siitä mitä, miksi ja miten häntä koskevia henkilötietoja käsitellään) - Oikeus tietojen poistoon, (esimerkiksi rekisteröidyillä asiakkailla on oikeus poistattaa kaikki heidän henkilötietonsa rekisteristä) - Oikeus saada tieto tietoturvaloukkauksesta, (esimerkiksi harjoittelupaikan on ilmoitettava tietoturvaloukkauksesta rekisteröidyille ilman aiheetonta viivytystä) - Henkilötietojen säilyttäminen, (henkilötietoja säilytetään ainoastaan niin kauan kuin se on välttämätöntä tietojenkäsittelyn tarkoitusta varten) - Ei mitään näistä - Jotain muuta, mitä? - Työpaikalla ei ollut tietosuojaan liittyvää ohjeistusta **22. Kuinka tärkeänä pidät seuraavien asioiden turvaamista?** Vastausvaihtoehdot: 1. En ollenkaan tärkeänä 2. Jokseenkin tärkeänä 3. Tärkeänä 4. Erittäin tärkeänä 5. En osaa sanoa **Kysymykset:** - Asiakas- ja tai potilastietojen tietosuojaperiaatteiden mukainen käsittely - Työpaikan tuotteet, tiedot ja järjestelmät - Työpaikan talousasiakirjat - Omien tietojen ja taitojen kehittäminen - Tutkimus- ja kehitystiedot - Tietoteknisen laitteiston ajantasainen päivittäminen - Laitteiston ja henkilökunnan tilojen suojaaminen ulkopuoliselta pääsyltä **23. Mitä seuraavista pidät todennäköisinä tietoturvauhkina harjoittelupaikassasi?** Vastausvaihtoehdot: 1. Epätodennäköinen 2. Mahdollinen 3. Todennäköinen 4. Lähes varmana 5. En osaa sanoa **Kysymykset:** - Kyberhyökkäyksestä aiheutuva sähkökatkos, medisiinisen laitteen toimintahäiriö tai vikatilanne - Kyberhyökkäyksestä aiheutuva tietosuojavuoto, (potilas- tai henkilötiedon paljastuminen)

- Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin johtuen tietojärjestelmän vikaantumisesta, (esimerkiksi laitteiston vanhuus tai päivittämättömyys) - Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin väärin määriteltyjen käyttövaltuuksien takia, (esimerkiksi lääkäri ei pääse tarkastelemaan hoitajan tekemiä kirjauksia) - Jotain muuta, mitä? - En mitään näistä - En tiedä **36. Onko tutkintoosi kuulunut riittävästi tietoturva- ja tietosuojakoulutusta** Vastausvaihtoehdot: - Kyllä - On jokseenkin - Ei - En osaa sanoa **38. Millä tietoturvaa tai tietosuojaa koskevalla osa-alueella haluaisit lisäkoulutusta?** Vastausvaihtoehdot: - Salasanat - Turvallisten ja haitallisten nettisivujen tunnistaminen - Tietosuoja - Turvallisten ja haitallisten sähköpostilinkkien tunnistaminen - Somen käyttöopas - Lainsäädäntö liittyen tietosuojaan ja tietotekniikkarikoksiin - Turvallisen etätyön ohje - En tarvitse lisäkoulutusta - En osaa sanoa - Jotain muuta, mitä?	- Työpaikan henkilöstön heikkojen salasanojen takia aiheutunut hyökkääjän luvaton pääsy järjestelmiin - Arkaluonteisten tietojen vuotaminen sosiaalisen median kautta, (esimerkiksi työkaveri ottaa työajalla someen kuvan, jossa vahingossa näkyy kollegan kulkukortin käyttäjä-ID) - Poistuessa työpisteeltä, työaseman auki ja valvomatta jättäminen - Työpaikalla puhelinsoiton yhteydessä arkaluonteisen tiedon leviäminen - Työntekijöiden äänekkään keskustelun seurauksena arkaluonteisen tiedon leviäminen - Työsähköpostiin tulleen haitallisen linkin klikkaaminen - Laitteistojen tai järjestelmien vanhuudesta johtuva toimintahäiriö (esimerkiksi päivityksiä ladattaessa laitteiston jumittaminen) - Työpaikan henkilöstön aiheuttama tahallinen vandalisointi järjestelmiin - Työpaikan henkilöstön tahaton tietojen poistaminen vahingossa (esimerkiksi kirjatessa tietoja, vanhojen tietojen poistaminen.) - Työpaikan henkilöstön luvaton arkaluonteisten tietojen selaaminen, (esimerkiksi tylsyyden aiheuttama satunnaisten potilastietojen surffailu.) - Jotain muuta, mitä? **25. Mitä harjoittelupaikassasi voitaisiin kehittää tietoturvaosaamiseen liittyen?** Vastausvaihtoehdot: - Salasanaohjeiden päivittäminen - Tietosuojaohjeiden päivittäminen - Pääsynhallinta - Tietojärjestelmien kehitys, testaaminen ja ylläpito - Fyysisen ympäristön turvallisuus - Henkilöstöturvallisuus - Tietoturvapolitiikka - Poikkeustilanteiden ja ongelmatapahtumien hallinta - Omaisuuden ja tieto-omaisuuden (suojattavat tiedot) hallinta - Tietojärjestelmien käytön ja tiedonvälityksen turvallisuuden hallinta - Ei mitään näistä - Jotain muuta, mitä? **26. Uskotko olevasi tietoinen mahdollisista tietoturvauhista organisaatiossasi?** Vastausvaihtoehdot: - Kyllä - En - En tiedä **28. Uskotko, että työkaverisi ovat tietoisia mahdollisista uhista organisaatiossasi?**

	Vastausvaihtoehdot: - Kyllä - Ovat jokseenkin tietoisia - Eivät ole - En osaa sanoa - En halua vastata kysymykseen **30. Kuinka todennäköisenä pidät tietovuodon riskiä organisaatiossasi seuraavan viiden vuoden aikana?** Vastausvaihtoehdot: 1. Epätodennäköisenä 2. Mahdollisena 3. Todennäköisenä 4. Lähes varmana 5. En osaa sanoa **Kysymykset:** - Kuinka todennäköisenä pidät tietovuodon riskiä organisaatiossasi seuraavan vuoden aikana? **32. Mikä seuraavista tietoturvauhista uskot todennäköisimmin realisoituvan seuraavien vuosien aikana harjoittelupaikassasi?** Vastausvaihtoehdot: - Väärien tietojen kirjaaminen inhimillisen virheen takia, (esimerkiksi työkiireiden aiheuttamana) - Väärien tietojen saanti organisaation ulkopuolelta, (esimerkiksi potilaalta itseltään) - Inhimillisestä virheestä johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi vainajien tietojen jääminen järjestelmään tai entisten työntekijöiden tietojen jääminen järjestelmään) - Ohjelmiston toiminnasta johtuvat tietojärjestelmässä olevat vanhentuneet tiedot, (esimerkiksi tilanne jossa, järjestelmä on niin kulunut [huonosti koodattu] että vanhojen tietojen poistaminen on ylivoimainen tehtävä, johon ei työkiireen takia nähdä vaivaa) - Tietoliikenneongelmista aiheutunut väärien tai puutteellisten tietojen kirjautuminen tietojärjestelmään, (esimerkiksi myrskyn aiheuttama sähkökatkos) - Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen valtuutetun henkilön toimesta (esimerkiksi lääkäri tai hoitaja - Tietojärjestelmässä tapahtunut tietojen tahallinen väärentäminen hoitajan itsensä toimesta, (esimerkiksi helpottaakseen omaa työtään tai muu välinpitämättömyys) - Valtuuttamattoman henkilön tekemä tietojen tahallinen väärentäminen tietojärjestelmään, (esimerkiksi pääsy järjestelmiin työpaikan tietokoneilla)

	- Tietoliikenneyhteyksien vikaantumisesta tai katkoksesta aiheutunut pääsyn estyminen kaikkiin tai osaan tietojärjestelmästä tarvittavista potilastiedoista, (esimerkiksi ulkopuolinen vaikuttaja, kuten kyberhyökkäys kriisitilanteessa) - Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin johtuen tietojärjestelmän vikaantumisesta, (esimerkiksi laitteiston vanhuus tai päivittämättömyys) - Pääsyn estyminen tietojärjestelmästä tarvittaviin potilastietoihin väärin määriteltyjen käyttövaltuuksien takia, (esimerkiksi lääkäri ei pääse tarkastelemaan hoitajan tekemiä kirjauksia) - Jotain muuta, mitä? - Ei mitään näistä - En osaa sanoa **34. Mitä tietoja uskot rikollisen tavoittelevan harjoittelupaikastasi?** Vastausvaihtoehdot: - Työpaikan järjestelmien salasanoja - Asiakas- ja/tai potilastietoja - Henkilökunnan tietoja - Rajoitettua palvelutietoa - Työpaikan verkkoon liittyvää rajoitettua tietoa ja siihen kiinnitettyjä laitteistoja - En osaa sanoa Jotain muuta, mitä? **35. Onko harjoittelupaikan henkilöstö osallistunut tietoturvakoulutukseen viimeisen vuoden aikana?** Vastausvaihtoehdot: - Kyllä - Ei - En osaa sanoa **36. Onko tutkintoosi kuulunut riittävästi tietoturva- ja tietosuojakoulutusta?** Vastausvaihtoehdot: - Kyllä - On jokseenkin - Ei - En osaa sanoa 37. Mistä osa-alueista haluaisit lisäkoulutusta? - Salasanat - Turvallisten ja haitallisten nettisivujen tunnistaminen - Tietosuoja - Turvallisten ja haitallisten sähköpostilinkkien tunnistaminen - Somen käyttöopas - Turvallisen etätyön ohje - Lainsäädäntö liittyen tietosuojaan ja tietotekniikkarikoksiin - Jotain muuta, mitä? - En osaa sanoa

	- En tarvitse lisäkoulutusta

Liite 2. Kyselyn saatekirje

Hei!

Olen tieto- ja viestintätekniikan opiskelija Jyväskylän Ammattikorkeakoulussa ja teen osana opinnäytetyötäni tutkimuskyselyä. Kyselyllä selvitetään harjoittelun vaikutusta sosiaaliterveysalan opiskelijoiden tietosuoja- ja tietoturvaosaamiseen. Kyselytulokset tuhotaan opinnäytetyön valmistumisen jälkeen arviolta kesällä 2022. Vastaaminen on helppoa ja kestää noin 5–15 minuuttia. Pyydän vastaamaan kyselyyn viimeistään 05.04.2022 avaamalla oheinen osoite:

https://link.webropolsurveys.com/R/C4E4AFC1C92C7623

tai kopioimalla kyseinen osoite ja liittämällä se Internet-selaimen osoitekenttään. Jokainen vastaus auttaa tietoturvallisuuden kartoittamista ja kehittämistä.

Etukäteen kiittäen vastauksistanne.

https://link.webropolsurveys.com/R/C4E4AFC1C92C7623

Liite 3. Kyselyn toinen saatekirje

Hei!

Olen tieto- ja viestintätekniikan opiskelija Jyväskylän Ammattikorkeakoulussa ja teen osana opinnäytetyötäni tutkimuskyselyä. Tämä on muistutusviesti, vastausaikaa on pidennetty 12.04 asti. Kyselyllä selvitetään harjoittelun vaikutusta sosiaaliterveysalan opiskelijoiden tietosuoja- ja tietoturvaosaamiseen. Kyselytulokset tuhotaan opinnäytetyön valmistumisen jälkeen arviolta kesällä 2022. Vastaaminen on helppoa ja kestää noin 5–15 minuuttia. Pyydän vastaamaan kyselyyn viimeistään 12.04.2022 avaamalla oheinen osoite:

[SurveyLinkText]

tai kopioimalla kyseinen osoite ja liittämällä se Internet-selaimen osoitekenttään. Jokainen vastaus auttaa tietoturvallisuuden kartoittamista ja kehittämistä.

Etukäteen kiittäen vastauksistanne.