jamk

Kyberturvallisuusosaaminen ja -suhtautuminen sosiaali- ja terveysalan opiskelijoiden keskuudessa

Kyselytutkimus

Teemu Maliniemi

Opinnäytetyö, AMK
Toukokuu 2021
Tietojenkäsittely ja tietoliikenne
Tieto- ja viestintätekniikka, insinööri (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Maliniemi, Teemu

Kyberturvallisuusosaaminen ja -suhtautuminen sosiaali- ja terveysalan opiskelijoiden keskuudessa, Kyselytutkimus

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 39 sivua.

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikka. Opinnäytetyö, AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Digitalisaation ja teknologian nopea kehitys on saanut yhteiskunnan integroimaan järjestelmiä ja ympäristöjä tietoverkkoihin. Tämä laitteiden verkostoituminen on auttanut yhteiskuntaa parantamalla ja helpottamalla yleisiä toimintoja, mutta samanaikaisesti lisännyt tarvetta kyberturvallisuudelle isomman hyökkäyspinta-alan johdosta. Yksi tärkeimpiä alueita tieto- ja kyberturvallisuutta huomioitaessa on laitteiden käyttäjät. Terveydenhuoltoala on yksi hyökätyimmistä aloista. Erilaisissa ympäristöissä, jotka käsittelevät kriittisiä tietoja, on tärkeää pystyä kouluttamaan laitteiden käyttäjät toimimaan erilaisissa tieto- ja kyberuhkatilanteissa.

Opinnäytetyössä tutkittiin Jyväskylän ammattikorkeakoulun sosiaali- ja terveydenhuoltoalan opiskelijoiden tieto- ja kyberturvallisuusosaamista. Tutkimuksen tavoitteena oli tuottaa mahdollisia parantamiskeinoja, joilla kehittää tieto- ja kyberturvallisuusosaamista erityisesti sosiaali- ja terveysalan opetuksessa. Tutkimuksen aineisto koottiin verkkokyselylomakkeella, joka toteutettiin Webropol-työkalulla. Tutkimuskysely jaettiin taustatietojen lisäksi neljään pääosaan: Vapaa-aika ja koti, koulu, työympäristö ja suhtautuminen. Tutkimuksen tulokset analysoitiin käyttäen kvantitatiivisia eli määrällisiä tutkimusmenetelmiä.

Tutkimuksen tuloksista selvisi, että vastaajien tieto- ja kyberturvaosaaminen on hyvällä tasolla ja heidän osaamisnäkemyksensä on erityisen hyvä. Huomiota tuloksista herätti vastaajien salasanojen ylläpito, jossa esiintyi puutteita. Toisena huomiona löytyi eroavaisuudet koulu- ja työympäristöjen kyber- ja tietoturvaohjeistuksien välillä. Työympäristössä on vastauksien perusteella ohjeistettu kyber- ja tietoturvallisuutta paremmin, kuin koulussa. Tutkimuksen pääpaino siirtyi analysointivaiheessa tarkastelemaan opiskelijoiden osaamisnäkemystä, sillä tutkimuskysely oli rakennettu siten, että siitä saatiin paremmin tietoa vastaajien osaamisnäkemyksestä, kuin oikeasta tieto- ja kyberturvaosaamisesta. Pääkehitysehdotukseksi esitettiin tulosten pohjalta henkilökohtaisesti relevantimpi ohjaus, joka mukautuu osaamistasoon ja tiedon määrään.

Avainsanat (asiasanat)

Kyberturvallisuus, tietoturvallisuus, kyselytutkimus, opiskelijat

jamk

Description

Maliniemi, Teemu

Cybersecurity competence and attitudes among Social Service and Healthcare students

Jyväskylä: JAMK University of Applied Sciences, September 2020, 39 pages.

Technology, Information and Communication Technology, Bachelor’s thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Progress in technology has enabled society to integrate systems and environments into different networks. Increased networking has helped society by improving and making everyday things and functions as well as making them easier to use. At the same time, this has made systems more vulnerable by increasing potential attack targets. When designing secure digital environments, it is essential to pay attention to device users. Social Services and Health Care are among the most attacked fields in this regard. In an environment where critical information is handled, it is important to be able to instruct users to act correctly in different cyberthreat situations.

The main goal of this bachelor's thesis was to survey JAMK University of Applied Sciences' Social Services and Health Care students' level of competence in cyber security and based on the results suggest development proposals to improve student’s overall level of competence. The research material was collected via an online survey that was made using Webropol. In addition to including background information, the research survey was divided into four main parts: home, school, work environment and attitude. During analysis, the focus of the study shifted from outlining students' actual cybersecurity competence towards examining students' perception of their own proficiency. This change was made due to the survey providing better information on perceived skill levels. The results of the study were analyzed using quantitative research methods.

The results of the survey showed that the respondents’ cyber security skills are generally at a high level, and they perceive their own skills as particularly good. One of the biggest shortcomings in terms of cyber security was respondent’s password maintenance habits. Furthermore, there was a distinct difference between cybersecurity guidelines in school and work environments: Based on the data, workplaces have better instructions for cybersecurity than schools do. Considering the study, the gauging of individual skill and the provision of personalized guidance was deemed as the primary suggestion for improving the development of instruction material and teaching.

Keywords or tags (subjects)

Cyber security, Information security, Survey, Students

Sisältö

Kuviot

1 Johdanto

Vuoden 2020 lokakuussa Tor-verkossa levinneet luottamukselliset tiedot, jotka olivat peräisin Psykoterapiakeskus Vastaamoon tehdyistä tietomurroista marraskuussa 2018 ja maaliskuussa 2019, herättivät keskustelua yksityisten tietojen turvallisuudesta digitaalisissa ympäristöissä. (Yle seurasi Vastaamon tietomurtoa 2020.) Terveydenhuoltoala on jatkuvan digitaalisen kehityksen alla, mikä helpottaa sekä yritysten että ihmisten arkea ja elämää. Samanaikaisesti digitalisaation seurauksena syntyy uusia mahdollisuuksia rikollisille varastaa ja myydä tietoa. Terveystoimiala oli jo vuonna 2015 kyberhyökkäysten top-5 listalla ensimmäisenä, jolloin myös varastettiin yli 100 miljoonaa potilastietoa. (Lehto, M & Limnéll & Innola & Pöyhönen & Rusi & Salminen 2017, 18).

Limnéllin, Majewskin ja Salmisen mukaan (2014, 15) “kyberturvallisuus on tasapainottelua mahdollisuuksien ja uhkien välillä”. Tämä dynaamisuus aiheuttaa omanlaisia ongelmia digitaalista turvallisuutta suunnitellessa. Mikäli infrastruktuurin suunnitteluvaiheessa on huomioitu digitaalinen turvallisuus, laitteiden turvallisuuden ylläpito helpottuu ja useimmiten onnistuu pitämällä laitteiden päivitykset ajan tasalla. Suurempi haaste ilmenee toteutettaessa henkilöstön valmistautumista ja taitoa toimia useita erilaisia uhkia vastaan.

Tämän opinnäytetyön tavoite on pyrkiä auttamaan edellä mainittua henkilöstön valmistautumista erilaisiin kyberuhkiin kartoittamalla tieto- ja kyberturvaosaamista tulevien sosiaali- ja terveysalan ammattilaisten kohdalla sekä ehdottamalla mahdollisia tapoja parantaa ja ohjeistaa nykyisiä opiskelijoita tieto- ja kyberturvan osalta.

2 Tietoperusta

Tässä tutkimuksessa tarkastellaan opiskelijaa ja työntekijää henkilönä, joka toimii fyysisessä ympäristössä ja on vuorovaikutuksessa niin fyysisen kuin digitaalisen maailman kanssa. Tarkemmin tutkitaan henkilön osaamista ja suhtautumista kybertoimintaympäristössä ja minkälainen mahdollinen vaikutus tällä on kyberturvallisuuteen. Tutkimuksen teoreettinen tausta perustuu täten tietoturvaan, kyberturvallisuuteen sekä tietosuojaan.

Tietoturvaa ja kyberturvallisuutta voidaan tutkia useasta eri näkökulmasta, ja monesti kyseiset termit saattavat merkitä eri asioita riippuen lähteestä. Tämän tutkimuksen osalta kyberturvallisuus käsitellään pääkäsitteenä, jonka alle tietoturva ja tietosuoja sijoittuvat.

2.1 Tietoturva

Tietoturva on käsitteenä vanhempi kuin kyberturvallisuus. Erona näillä termeillä on muun muassa se, että kyberturvallisuus kuvaa paremmin sitä kokonaisuutta, missä nyky-yhteiskunta elää ja toimii (Limnéll & Majewski & Salminen, 2014). Tietoturva kuvataan Kyberturvallisuuden sanastossa (2018) seuraavasti: “Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.” Tiedolla tarkoitetaan kyseisessä tapauksessa fyysisesti ja elektronisesti säilöttävää tietoa. Saatavuus, eheys ja luottamuksellisuus muodostavat sen kehyksen, jonka mukaisesti tätä tietoa pyritään turvaamaan mahdollisilta riskeiltä ja uhkilta. (Tietoturva 2020.)

Saatavuus

Saatavuudella tarkoitetaan, että valtuutettu henkilö pääsee tietoihin käsiksi ja Internetin välityksellä käytettävien palveluiden tiedot tulee olla saatavilla ajasta tai paikasta riippumatta (Gil 2018). Sähköisten palveluiden yleistyessä voidaan olettaa, että saatavuuden tarve lisääntyy.

Eheys

Tiedon eheyden varmistaminen tarkoittaa, että järjestelmät ja niillä olevien tietojen muuttumattomuus, luotettavuus ja ajantasaisuus on varmistettu. Eheyttä ylläpitävät järjestelyt turvaavat tietoa sekä tahalliselta tietojen muuttamiselta että vahingoilta, kuten laitteisto- tai ohjelmistovioilta.

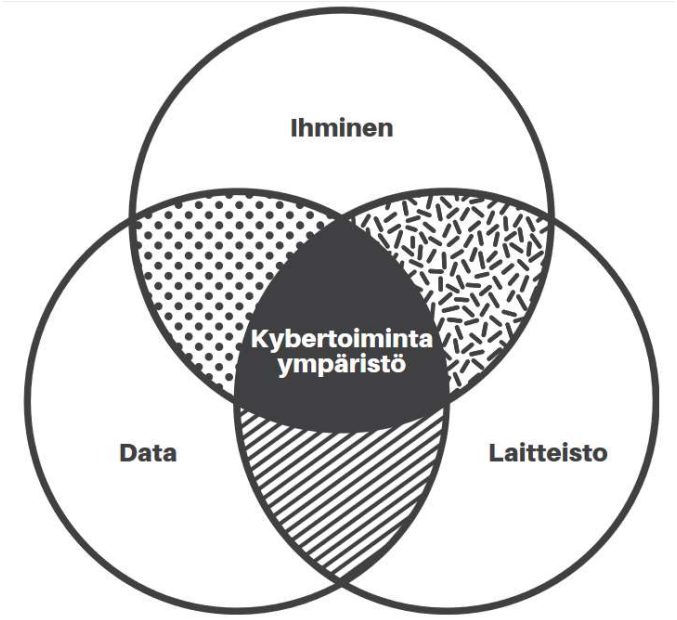
Luottamuksellisuus

Luottamuksellisuuden varmistamiseksi tieto on muodossa, johon vain valtuutettu henkilö pääsee käsiksi. Yleisin esimerkki tästä on, että tieto tai järjestelmä on salasanasuojattu ja salasana on vain

valtuutetun henkilön käytössä. Molemmat puolet aiemmasta esimerkistä lisäävät kohteen luottamuksellisuutta. Henkilöstön tietoturvaohje (2013) sisällyttää luottamuksellisuuteen myös sen, että valtuutetut henkilöt käyttävät tietoa ja järjestelmiä vain asianmukaisesti työtehtävissään.

2.2 Kybertoimintaympäristö

Kybertoimintaympäristö on tärkeä konsepti kyberturvallisuutta määrittäessä, koska kyberturvallisuuden yksinkertaisimpana tarkoituksena on turvata digitaalisen ympäristön toiminta. Viime vuosina kybertoimintaympäristö -termiä on käytetty kuvaamaan metafyysistä ajatusrakennelmaa, joka kuvaa ihmisen, laitteiston ja datan vuorovaikutusta (ks. Kuvio 1. Ihminen luo ja käyttää dataa, jota hän hyödyntää ja säilyttää laitteiston avulla. (Edgar & Manz 2017, 35.) Tässä ja Limnéllin ym. (2014, 47) määrittelemässä kybertoimintaympäristössä, jossa bittien maailma kohtaa fyysisen, on tärkeää huomioida se, että ihminen on yhtä lailla osa dynaamista ympäristöä.



Kuvio 1 Kybertoimintaympäristön ajatusrakennelma (Edgar & Manz 2017, 36, muokattu)

Kybertoimintaympäristö voidaan tulkita ympäristönä, joka muodostuu joko yhdestä tai useammasta tietojärjestelmästä (Kyberturvallisuuden sanasto 2018, 21). Kybertoimintaympäristö -termiä ei käytetä usein kuvaamaan pienempiä ympäristöjä vaan se usein kuvaillaan valtion tai sotilaallisen toiminnan näkökulmasta suureksi digitaaliseksi ympäristöksi, joka yhdistää useita valtioita ja näiden osa-alueita.

2.3 Kyberturvallisuus

Julkisen hallinnon digitaalinen turvallisuus (2020) kuvaa kyberturvallisuuden vastaavasti: “Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Kyberturvallisuutta suunnitellessa usein aluksi määritellään kyberturvallisuusympäristö, jota halutaan turvata erilaisilta kyberuhkilta ja niiden seuraamuksilta. Kyberturvallisuus mielletään usein vain “bittien” maailmassa tapahtuviin ilmiöihin. Limnéll ja muut (2014, 47) muistuttavat, että vähintään kaksi kolmasosaa kyberturvallisuudesta sijoittuu teknologian ulkopuolelle ympäristöissä, joissa suurempi osa sähköisistä laitteista on verkossa. Tämä ajatusmalli on olennainen toimivan kyberturvallisuusohjeistuksen kehittämisprosessissa.

Kyberturvallisuus seuraa pääasiallisesti samaa eheyden, saatavuuden ja luottamuksellisuuden muodostamaa kehystä, johon tietoturva perustuu. Edgar ja Manz kuitenkin tähdentävät, että näillä pääominaisuuksilla määrittely on liian karkea ja jättää pois kyberturvallisuuden tarkemmat näkökohdat. Heidän mukaansa kyberturvallisuudessa on lisäksi otettava huomioon autenttisuus ja kiistämättömyys. (Edgar & Manz 2017, 37). Kyseiset alueet esiintyvät myös täydennyksinä useissa tietoturvan määrittelyyn keskittyvissä lähdeaineistoissa.

Autenttisuus

Autenttisuus tai todennus tarkoittaa kyberympäristössä toimivien tahojen identiteettien varmistuksen. Kyberympäristössä toimitaan fyysisen maailman kautta ja autenttisuudella pyritään varmistamaan, että digitaalinen projektio kuuluu oikealle ihmiselle tai laitteelle. (Edgar & Manz 2017, 38). Autenttisuus pätee myös toimintoihin ja dataan kyberympäristössä. Tietyt toiminnot tai datat halutaan todentaa tulleen tietyltä käyttäjältä tai laitteelta (Kauppi 2019.)

Kiistämättömyys

Kiistämättömyydellä tarkoitetaan menetelmiä, joilla voidaan seurata ja tarkastaa tarvittaessa kybertoimintaympäristössä tapahtuvia muutoksia ja tapahtumia. Menetelmiä kuten tapahtumien kirjaamista lokitietoihin pystytään käyttämään hyödyksi, mikäli halutaan todistaa ympäristön aiempia turvallisuusnäkökohtia. Kyberturvallisuuden varmistaminen on mahdollista vain, jos pystytään tarjoamaan todisteita turvausmenetelmistä. (Edgar & Manz 2017, 38-39).

2.4 Tietosuoja

Tietosuojan merkitys ja sisältö ovat kasvaneet digitalisaation yhteydessä, minkä vuoksi henkilötietolaki on korvattu uudella tietosuojalailla. (Tietosuojalaki 1050/2018.) Uusi laki tarkentaa ja täydentää tietosuojaa ottamalla huomioon käyttäjän oikeudet, rekisterinpitäjän ja rekisteröidyn velvollisuudet, sekä mahdolliset poikkeustapaukset. Muutoksen tarkoituksena on mukailla EU:n yleistä tietosuoja-asetusta (A 2016/679/EU) ja varmistaa henkilötietojen laaja-alaisempi suojaus nyky-yhteiskunnassa.

Tietosuoja mielletään helposti vain tietojen salaamiseksi, mutta kuten Andreasson, Riikonen ja Ylipartanen kuvailevat, tietosuojassa kyse on asiakkaan luottamuksesta ja henkilöstön kyvykkyydestä käsitellä asiakkaan informaatiota koko sen elinkaaren aikana. Kyseisen kaaren aikaisia vaiheita ovat esimerkiksi asiakastietojen keräys, tallennus, käyttö, säilytys ja hävittäminen. (Andreasson, Riikonen & Ylipartanen 2017, 19)

3 Tutkimus

3.1 Tutkimuskysymys

Tutkimuksen tarkoituksena on selvittää ja kartoittaa kyber- ja tietoturvaosaamista Jyväskylän ammattikorkeakoulun sosiaali- ja terveysalan opiskelijoiden keskuudessa. Kyselyllä pyritään saamaan tuloksia, joitten pohjalta voidaan parantaa ja kehittää opiskelijoiden ja tulevien sosiaali- ja terveysalan ammattilaisten kyber- ja tietoturvaosaamista kyberuhkien välttämiseksi. Sivukysymyksenä on tarkoitus saada tietoa mitkä mittausmenetelmät ovat parhaita mittaamaan kyber- ja tietoturvaosaamista ja onko elämäntilanteella vaikutusta kyber- ja tietoturvaosaamiseen.

3.2 Kohderyhmä

Tutkimuksen kohderyhmänä ovat Jyväskylän ammattikorkeakoulun sosiaali- ja terveysalan opiskelijat. Kohderyhmän valintaan vaikutti kyberuhkien jatkuva lisääntyminen kyseisellä alalla ja toimeksiantaja halusi mahdollisten tuloksien pohjalta parantaa sosiaali- ja terveysalan kurssia ja tapoja, jolla pyritään opettamaan kyber- ja tietoturvaosaamista.

Tutkimukseen otettiin mukaan sekä AMK- että YAMK-koulutustyypit. AMK ja YAMK sisällytettiin kyselyyn, jotta nähtäisiin, onko mahdollisia eroja kyber- ja tietoturvaosaamisessa, jos vastaaja on ollut jo työelämässä pidempään.

3.3 Tutkimusmenetelmät

Tutkimuksen tuloksia analysoitaessa käytettiin hyödyksi kvantitatiivisia eli määrällisiä tutkimusmenetelmiä. Tutkimuksen tavoitteena oli kartoittaa kohderyhmän tieto- ja kyberturvaosaamista ja tämän pohjalta esittää mahdollisia kehitysehdotuksia parantamaan osaamistasoa. Tähän kvantitatiiviset tutkimusmenetelmät soveltuvat hyvin. Päätyökaluna hyödynnettiin Webropolin Professional Statistics -työkalua.

Tutkimuskyselyn asenneväittämäjoukkojen reliabiliteetin mittaamiseen käytettiin Cronbachin α (alpha) -arvoa. Tällä pyritään varmistamaan, että summamuuttujan mittarit ovat yhtenäisiä ja mittaavat samaa ilmiötä. Alfa-arvon parantamiseksi voidaan jättää asenneväittämäjoukosta kohdat pois, jotka alentavat alfa-arvoa. Tämä kuitenkin voi alentaa mittarin validiteettia. (KvantiMotv 2008.) Alfa-arvon laskemiseksi käytettiin Webropolin omaa Professional Statistics -työkalua ja arvo myös laskettiin käsin, jolla varmistettiin, ettei ohjelman automaatio tekisi virheitä. Muutamassa kohdassa esiintyi eroja käsin lasketun ja työkalun tuloksen välillä, mutta tarkemmin katsottuna nämä eroavaisuudet johtuivat siitä, miten työkalu huomioi laskussa kohdat missä vastaaja on jättänyt yhden tai useamman kohdan tyhjäksi.

3.4 Tutkimuksen toteuttaminen

Tutkimuskysely toteutettiin Internet-kyselynä. Kyseinen kyselymuoto valittiin helppouden ja vähäisten resurssivaatimusten takia. Internet-kysely verrattuna muihin kyselymuotoihin on lisäksi nopeampi jakaa. Kysely suoritetaan koronaviruksen aikana, joten myös turvallisuussyistä kontaktivapaa kyselymuoto oli suotava.

Kyselyn luontiin, jakeluun ja analysointiin käytettiin Webropol-kyselytyökalua. Tutkimuskysely jaettiin taustatietojen lisäksi neljään pääkohtaan: Vapaa-aika ja koti, koulu, työympäristö ja suhtautuminen. Kysyttäviksi taustatiedoiksi valittiin: sukupuoli, ikä, suoritettava tutkinto ja elämäntilanne.

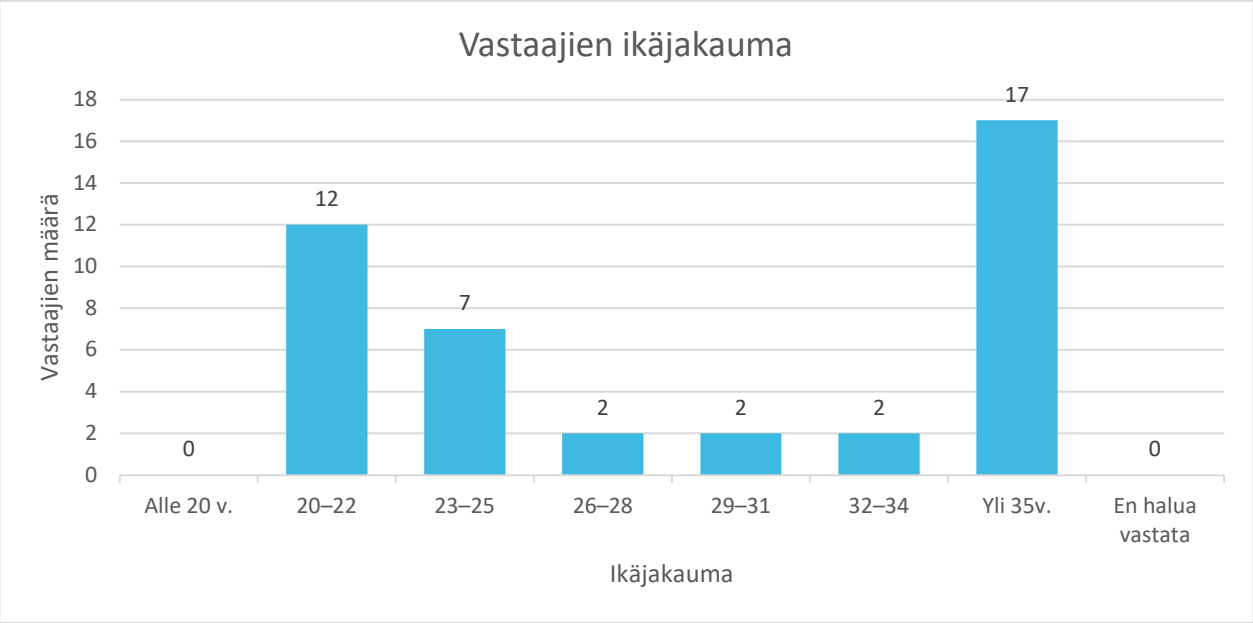
Tutkimuksen vastausaika alkoi 24.02.2021 ja kesti 19.03.2021 asti. Tutkimuskyselyä varten lähetettiin myös muistutusviesti kaksi kertaa vastausajan sisällä vastausprosentin ja reliabiliteetin parantamiseksi. Webropol mahdollisti muistutusviestin lähetyksen anonyymisti vain henkilöille, jotka eivät olleet vielä vastanneet kyselyyn. Taustatekijöiden kysyminen vaihdettiin viimeisen muistutusviestin jälkeen kyselyn loppuosioon. Tällä pyrittiin nostamaan vastausprosenttia sillä taustatekijöiden kysely ensimmäisessä osiossa saattaa vaikuttaa vastaajasta tungettelevalta (Vehkalahti 2008, 25).

4 Tutkimuksen tulokset

4.1 Taustatiedot

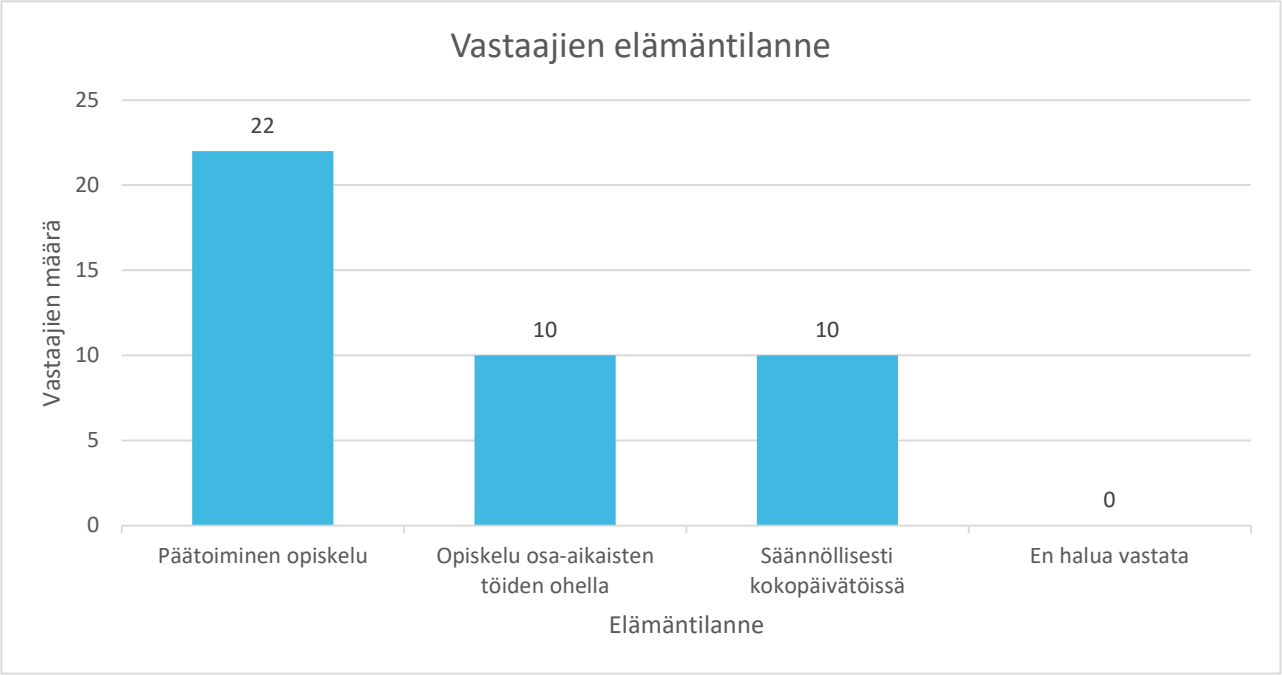
Tutkimuskysely lähetettiin 301:lle Jyväskylän ammattikorkeakoulun opiskelijalle, joista 42 vastasi kyselyyn. Kyselyn vastausprosentti oli 14.

Taustatekijöistä ensimmäisenä vastaajilta kysyttiin heidän sukupuoltaan. Vastaajista 88,1 prosenttia (n=37) oli naisia, miehiä oli 9,5 prosenttia (n=4) ja yksi vastaajista ei halunnut vastata. Vastaajien ikäjakaumassa yli 35-vuotiaat muodostivat 40,5 prosenttia (n=17), mikä näkyi myös muissa tuloksissa. Kuviossa 2 esitellään ikäjakauma kokonaisuudessaan.



Kuvio 2. Tutkimuskyselyn vastaajien ikäjakauma

Vastaajien suoritettava tutkinto jakautui siten, että AMK-tason opiskelijoita oli 61,9 prosenttia (n=26) vastaajista ja ylemmän YAMK-tason opiskelijoita oli 35,7 prosenttia (n=15). Yksi vastaajista vastasi suoritettavaksi tutkinnoksi vaihtoehdon ”muu” ilman tarkennusta avoimeen kenttään. YAMK-opiskelijoista 73,3 prosenttia (n=11) kuuluivat aiemmin mainittuun yli 35-vuotiaiden ryhmään. Kuviossa 3 näkyy vastanneiden elämäntilanteet. Tässä tapauksessa korrelaatiota ilmeni vahvasti siinä, että iäkkäämmät vastaajista olivat suuremmalla todennäköisyydellä kokopäivätöissä tai opiskelemassa osa-aikaisten töiden ohella.



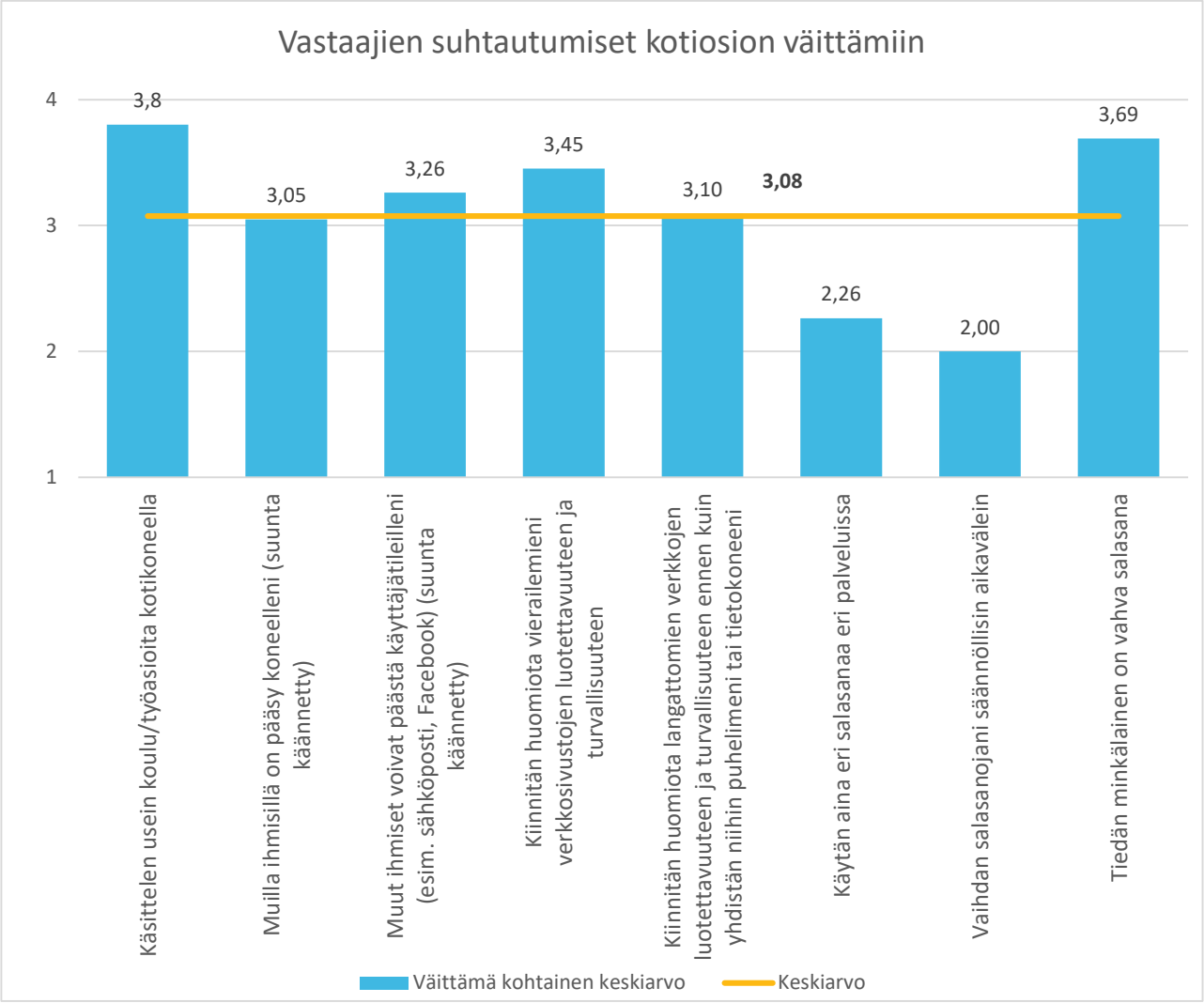
Kuvio 3. Kyselyyn vastanneiden elämäntilanne

4.2 Tietoturvallisuus kotona

Ensimmäisessä pääosiossa pyrittiin kartoittamaan opiskelijoiden kyber- ja tietoturvaosaamista kotona. Vastaajista kaikilla on käytössään kotikone. Jokaisessa pääosiossa kartoitettiin myös tieto- ja kyberturvaosaamista yhdellä asenneväittämäjoukolla. Asenneväittämäjoukkojen numeeriset arvot tarkoittavat vastaajien mielipiteitä eri väittämiin 4-asteisellä Likert-asteikolla. Asteikon numeerinen arvo 4 tarkoittaa vastaajan olevan täysin samaa mieltä väittämän kanssa ja numeerinen arvo 1 tarkoittaa vastaajan olevan täysin eri mieltä.

Kuvion 4 väittämien ”Muilla ihmisillä on pääsy koneelleni” ja ” Muut ihmiset voivat päästä käyttäjätileilleni (esim. sähköposti, Facebook)” vastauksien suunnat on käännetty analysointivaiheessa, jotta ne olisivat yhteneväisiä muiden väittämien kanssa. Toisin sanoen vastauksien neloset on muunnettu ykkösiksi, kolmoset kakkosiksi, ja niin edespäin. Kuten Vehkalahti (2008, 65) mainitsee, kääntäjien suunnan muuttaminen auttaa tulkitsemista ja muuttujien suunnat ovat jotakuinkin samantekeviä.

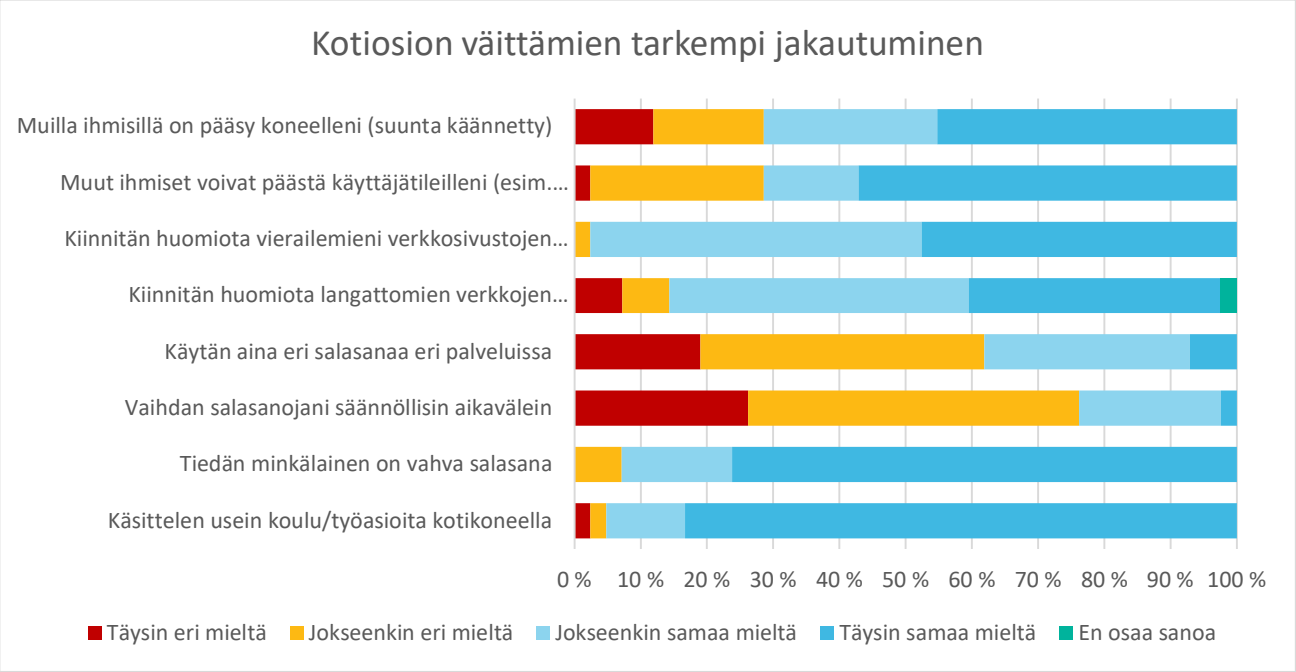
Kotiosion asenneväittämäjoukon reliabiliteettia mitattiin käyttäen Cronbachin α (alpha) -arvoa. Kaikkien kysymyksien kanssa summamuuttujan alpha-arvo jäi noin 0,61:een, jota voidaan pitää tietyissä tapauksissa liian alhaisena. Alpha-arvon nostamiseksi summamuuttujaa laskettaessa jätettiin väittämä ”käsittelen usein koulu-/työasioita kotikoneella” pois. Tämän ansiosta alpha-arvo saatiin nostettua 0,66:een. Patteriston vastauksien keskiarvot ja näiden yhteinen keskiarvo esitetään kuviossa 4, ja kuviossa 5 tuodaan esille vastauksien tarkempi jako. Molempiin kuvioihin on jätetty aiempi väittämä ja keskiarvo kuviossa 4 ilman pudotettua väittämää on 2,97.



Kuvio 4. Kotiosion asenneväittämäjoukon summamuuttuja

Keskiarvo 2,97 kertoo asteikolla 1-4:ään hyvästä yleisestä tieto- ja kyberturvaosaamisesta, mutta on tärkeää muistaa eri tilanteiden tärkeys erilaisissa kyberuhkaskenaarioissa. Tästä johtuen onkin mielekkäämpää keskittyä puutteisiin, joita tässä tapauksessa ilmenee vastaajien salasanojen käsittelytavoissa. Opiskelijoilta kysyttiin myös käyttävätkö he salasanojen hallintaan minkäänlaista salasanojen hallintaohjelmaa, johon 100 prosenttia (n=41) vastaajista vastasi kieltävästi, joka mahdollisesti viittaa huonolaatuiseen salasanakäytäntöön. Vastaajat kuitenkin näyttävät ymmärtävän heidän oman näkemyksensä puolesta, millainen on vahva salasana. (Ks. Kuvio 5.) Moni ei silti vastannut vaihtavansa salasanaa tai käyttävänsä eri salasanaa eri palveluissa, mikä on tieto- ja kyberturvallisuuden puolesta sekä kybertoimintaympäristöstä riippumatta ongelmallista. Mikäli vastaajat eivät käytä useita salasanoja eri palveluissa sen takia, että se vaikeuttaa heidän näkökulmastansa asioiden saatavuutta, olisi tämä erittäin selkeä korjattava epäkohta. Esimerkiksi

koulun puolesta ratkaisua voisi hakea esittelemällä erilaisia salasanan hallintaohjelmia opiskelijoille. On myös mahdollista, että ongelmaa ei koeta niin tärkeäksi, että siitä voitaisiin tiedottaa ja ohjeistaa.



Kuvio 5 Kotiosion asenneväittämäjoukon vastausten tarkempi jakautuminen

Kyselyä analysoitaessa ilmeni, että useissa kohdissa olisi voitu kysyä mahdollisia tarkentavia kysymyksiä. Esimerkiksi jos muilla ihmisillä on pääsy vastaajan koneelle, tarkoittaako tämä vain fyysistä pääsyä kyseiselle koneelle vai pääsevätkö muut käyttämään konetta vastaajan tunnuksilla ilman salasanan syöttämistä?

Yhtenä tavoitteena analysoitaessa oli yrittää selvittää vastaajien ”oikeaa” tieto- ja kyberturvaosaamista. Vastaajia ei esimerkiksi pyydetty antamaan esimerkkiä vahvasta salasanasta, vaan heiltä kysyttiin yleisemmin, tietävätkö he vahvan salasanan ominaisuuksia tai millainen se on. Tämä antoi enemmän tietoa vastaajien omasta osaamisnäkemyksestä kuin siitä, mitä heidän osaamisensa oikeasti on.

Kyberturvallisuudessa on yhtenä tekijänä tiedon eheys, johon vastaajien tiedon säilytystavat vaikuttavat. Vastaajista 83,3 prosenttia (n=35) kertoi käyttävänsä tiedostojen säilyttämiseen pilvipalveluita, kun taas loput 16,7 prosenttia (n=7) ilmoittivat, etteivät ne ole heillä käytössä. Tässä tapauksessa olisi ollut hyvä kysyä myös vastaajien varmuuskopiointitapoja, mutta pelkällä pilvipalveluiden käytölläkin saadaan vaikutettua tiedon eheyteen ja saatavuuteen. Tästä huolimatta pilvipalvelujen hyödyntäminen voi vastaajien keskuudessa johtaa entistä huonompaan tietosuojaan: saman salasanan käyttö eri sivustoilla on vastaajille yleistä, minkä perusteella he saattavat käyttää kyseistä salasanaa myös pilvipalvelun suojaamiseen.

Opiskelijoilta kysyttiin erilaisten ohjelmistojen käytöstä kotikoneella (ks. Kuvio 6). Vastauksista ilmeni, että opiskelijoilla on selkeästi hallussa ja tiedossa niin sanottujen perusohjelmistojen, kuten virustorjuntaohjelmien, käyttö. Toisaalta VPN-ohjelmistot eivät olleet heille läheskään yhtä tuttuja. Tuloksista on vaikea tulkita, onko termi kokonaan outo ja ovatko he esimerkiksi käyttäneet Windowsin omaa VPN-tukea yhdistäessään koneitaan omiin kouluhakemistoihinsa.

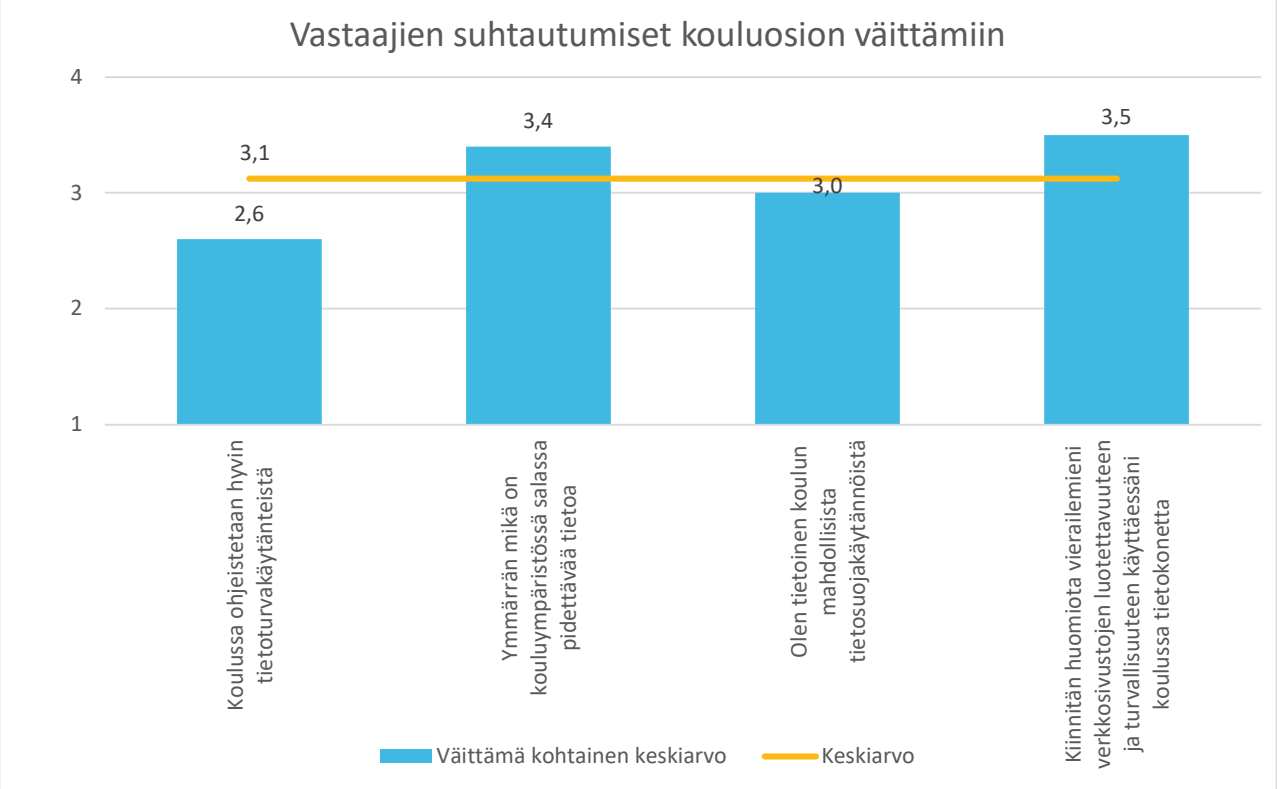
Kuvio 6. Opiskelijoiden eri ohjelmistojen käyttö kotikoneella

Tietoturvallisuuden puolesta olisi ollut mielekästä kysyä vastaajilta, jotka käyttävät automaattisia päivityksiä, antavatko he näiden päivitysten toteutua automaattisesti vai siirtävätkö he päivitysten ajankohtaa myöhemmäksi. Usein on törmätty käyttäytymiseen, jossa ihmiset eivät halua laittaa töitään tauolle päivitysten ajaksi, mikä saattaa viivästyttää päivityksiä muutamilla päivillä. Tämä kuitenkin perustuu anekdoottiseen tietoon.

Yleisesti vastaajien tieto- ja kyberturvakäyttäytyminen vaikuttaa olevan hyvällä tasolla, mutta aiemmin esitetty pohdinta siitä, miten vastaajien oma näkemys ja todellisuus saattaa erota toisistaan, on edelleen relevantti.

4.3 Tietoturvallisuus koulussa

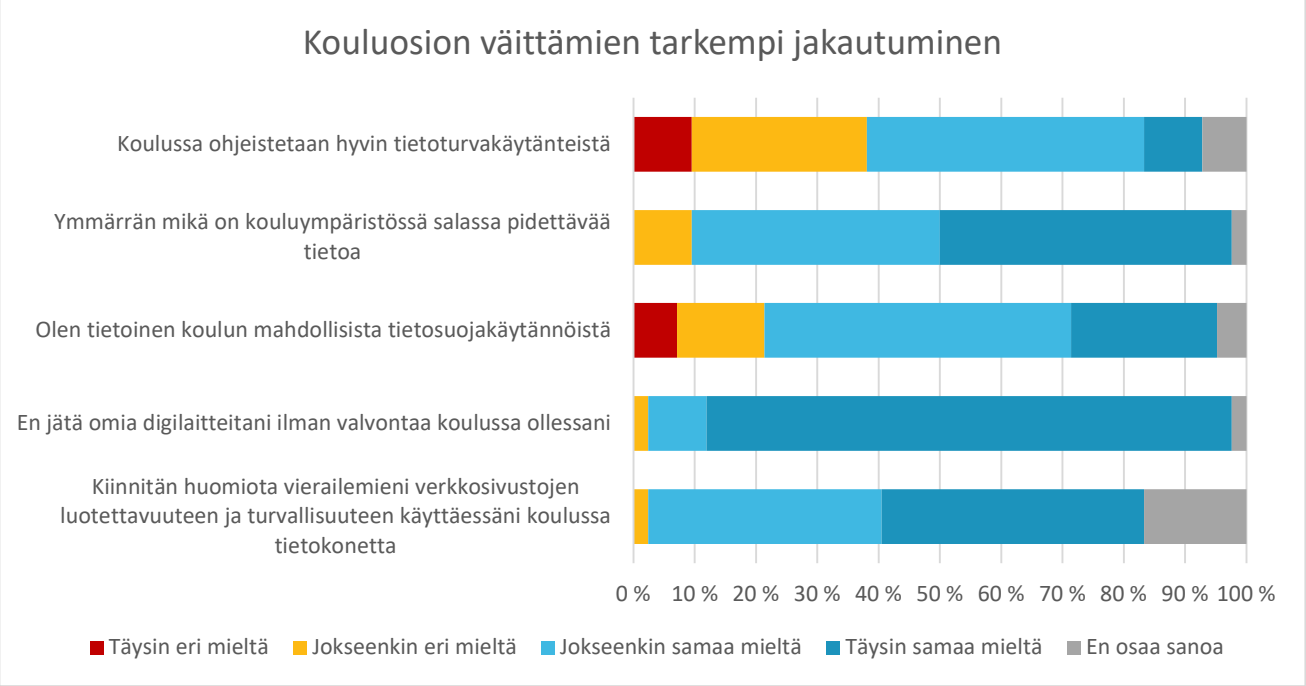
Kotiosion asenneväittämäjoukon reliabiliteettia mitatessa kaikkien väittämien kanssa alpha-arvo jäi 0,59:een. Jättämällä väite ”En jätä omia digilaitteitani ilman valvontaa koulussa ollessani” pois saatiin alpha-arvo nostettua 0,66:een. Ilman kyseistä väittämää keskiarvoksi väittämille tuli 3,125, kuten kuviossa 7 on esitetty.



Kuvio 7 Kouluosion asenneväittämäjoukon summamuuttuja

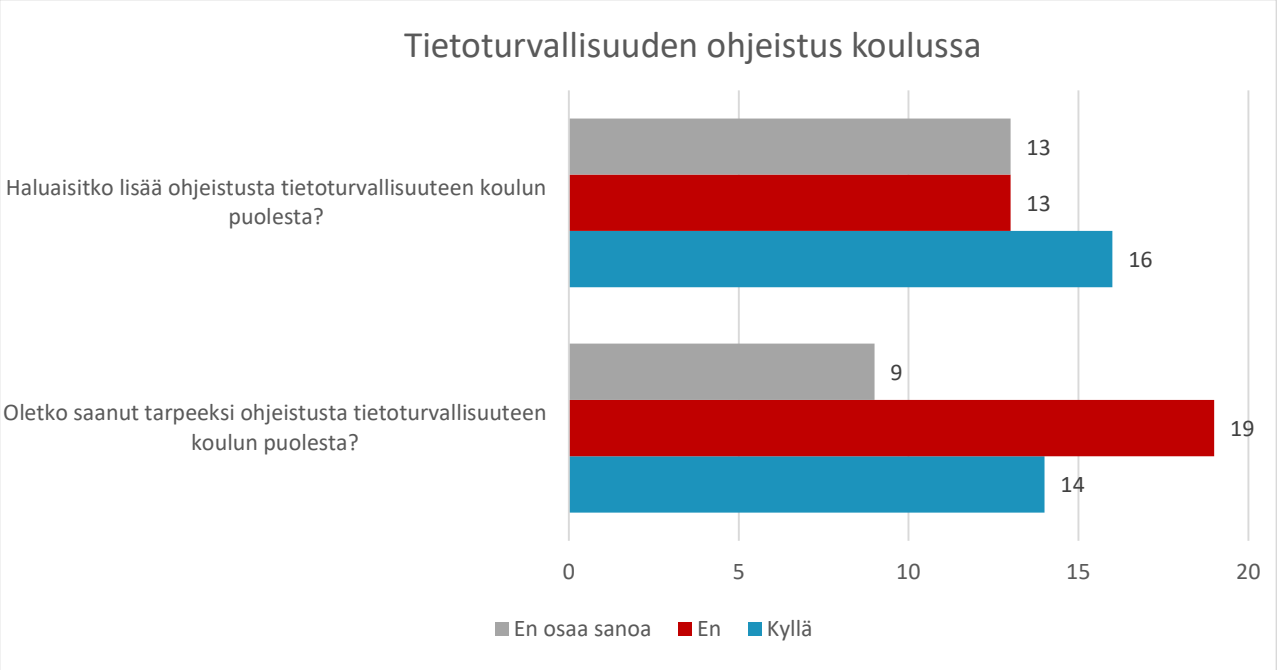
Kuten kotiosiossa, tulokset viittaavat hyvään tietoturvaosaamiseen ja -tietoisuuteen. Mahdollisena mielenkiinnon kohteena ilmenee se, että valtaosa vastaajista tietävät, mikä on salassa pidettävää tietoa kouluympäristössä ja kiinnittävät huomiota verkkosivustojen turvallisuuteen. Silti vastaajista 45,3 prosenttia (n=19) valitsi vaihtoehdon “jokseenkin eri mieltä”, “täysin eri mieltä” tai “ei osannut sanoa” väittämän ”koulussa ohjeistetaan hyvin tietoturvakäytänteistä” kohdalla. (Ks. Kuvio 8.) Yhtenä kysymyksenä herääkin se, mitä kautta vastaajat ovat saaneet aiempaa tietoa esimerkiksi juuri salassa pidettävistä tiedoista, jos he pystyvät vastaamaan tietävänsä, mitä se on.

Monessa kysymyksessä on spesifioitu kontekstin sijoittuvan kouluympäristöön, mutta on mahdollista, että vastaajat ovat ymmärtäneet kysymykset enemmän yleisinä tai vastanneet maalaisjärjen pohjalta. Esimerkiksi käsitys siitä, mitä salassa pidettävä tieto kouluympäristössä on, voi perustua tämänkaltaiseen yleistietoon. Kysymysvalintojen takia myös tässä osiossa on vaikea mitata vastaajien oikeaa osaamista. Mahdollisuutena on kuitenkin se, että vastaajat ovat saaneet tietoa muiden lähteiden kautta, kuten työpaikan puolesta.



Kuvio 8 Kouluosion asenneväittämäjoukon vastausten tarkempi jakautuminen

Opiskelijoiden kyber- ja tietoturvaosaamisen kehittämiseksi oli myös tärkeää kysyä vastaajilta, saavatko he koulun puolesta tarpeeksi ohjeistusta tietoturvallisuuteen ja millaista ohjeistusta he mahdollisesti haluaisivat. Vastaajista 45,3 prosenttia (n=19) oli sitä mieltä, että he eivät saaneet tarpeeksi ohjeistusta. Huomattava osa, 21,4 prosenttia (n=9), ei osannut vastata (Ks. Kuvio 9.) Opiskelijoilta kysyttiin tämän jälkeen, haluaisivatko he lisää ohjeistusta tietoturvallisuuteen koulun puolesta. Opiskelijoista 38,1 prosenttia (n=16) vastasi kyllä ja 30,9 prosenttia (n=13) vastasi kieltävästi. Kuten aiemmassa kysymyksessä, tässäkin tapauksessa huomattava osa, 31 prosenttia (n=13), ei osannut vastata. Vastaajilta tiedusteltiin myös avoimella kysymyksellä, millaista mahdollista ohjausta he haluaisivat.



Kuvio 9 Tietoturvallisuuden ohjeistuksen halu ja saanti koulussa

Molempien kysymysten vastauksista merkittävä osa oli ”en osaa sanoa”, mikä voisi antaa viitteitä siitä, että koulun tietoturvaohjeistus on ollut epäselvää tai sitä ei enää muisteta. Vastaajat ovat voineet olla myös epävarmoja siitä, ovatko yleiset infopaketit niin sanottua ohjeistusta. Avoimista vastauksista ilmeni, että osa opiskelijoista ei ole vielä ollenkaan käynyt koululla koronatilanteen vuoksi, mikä voi myös selittää epävarmuuden aiemmissa kysymyksissä. Vastaajien käytökseen on myös voinut vaikuttaa ”kyllä” -valinnan jälkeen ilmestyvä avoin kenttä, jonka pyytämä tarkennus on saatettu nähdä lisätyönä vastausprosessissa. Tutkimuksessa ei kuitenkaan tutkittu kyselykäyttäytymistä, joten tämä jätettiin sivuhuomioksi.

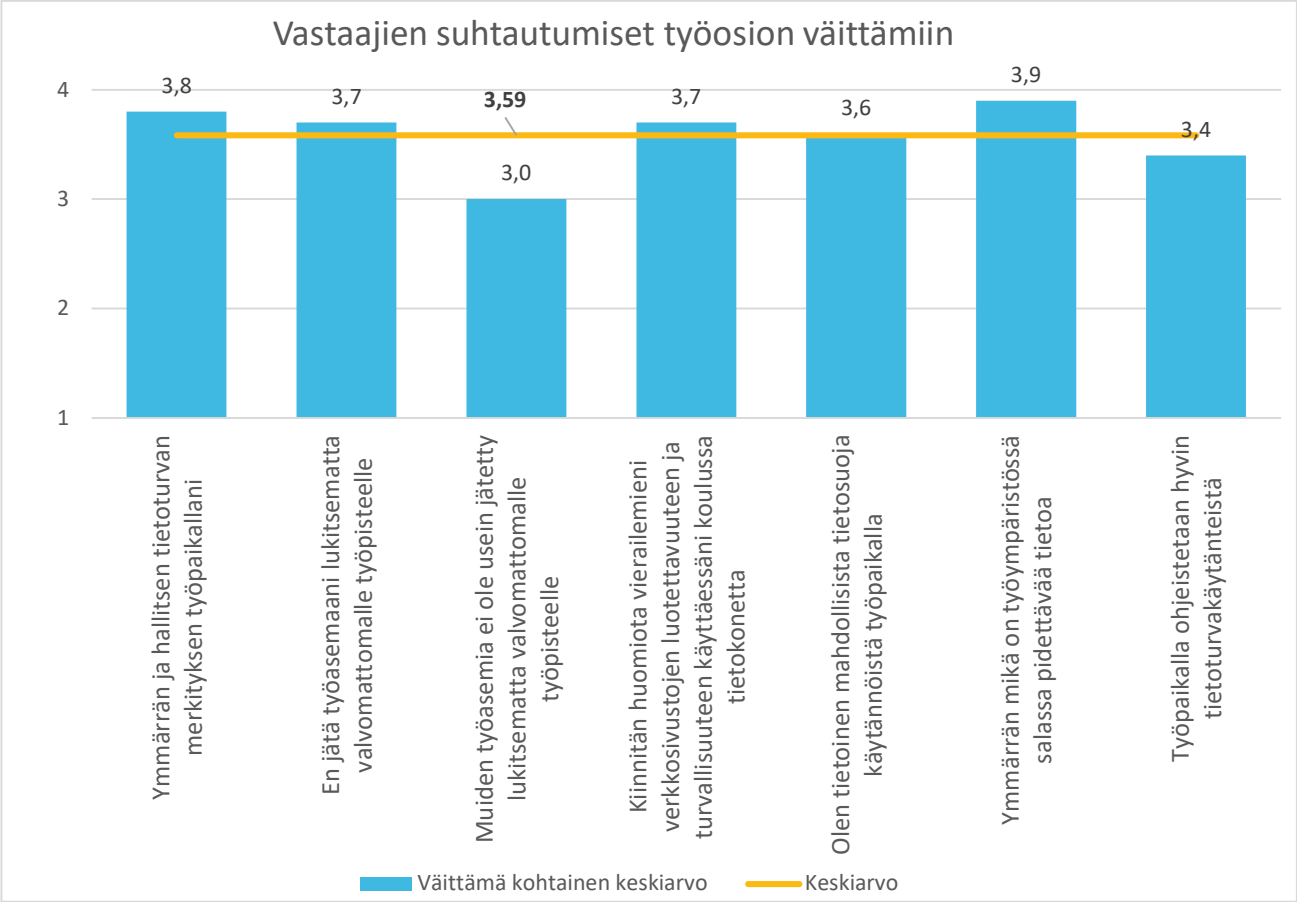
Avoimeen kysymykseen annetuista vastauksista tuli päällimmäisenä ilmi, että opiskelijat haluaisivat niin sanottua perustietoa tietoturvallisuuteen liittyen. Moni myös ilmaisi halun saada tietoa siitä, kuinka kotikonetta voi suojata. Pienempänä osuutena esiintyi opiskelijoiden halu saada säännöllisiä tietoiskuja ja/tai muistutuksia siitä, mitä tulee huomioida, sekä siitä, millaiset sivut ovat turvallisia ja mitkä eivät.

Viimeiseksi, kyselyn kouluosiossa, vastaajilta kysyttiin, käyttävätkö he koulun tarjoamaa langatonta verkkoa omilla henkilökohtaisilla laitteillaan. 73,8 prosenttia (n=31) valitsi myöntävän vastauksen ja 19,1 prosenttia (n=8) kieltävän. Loput 7,1 prosenttia (n=3) vastaajista eivät osanneet sanoa.

4.4 Tietoturvallisuus töissä

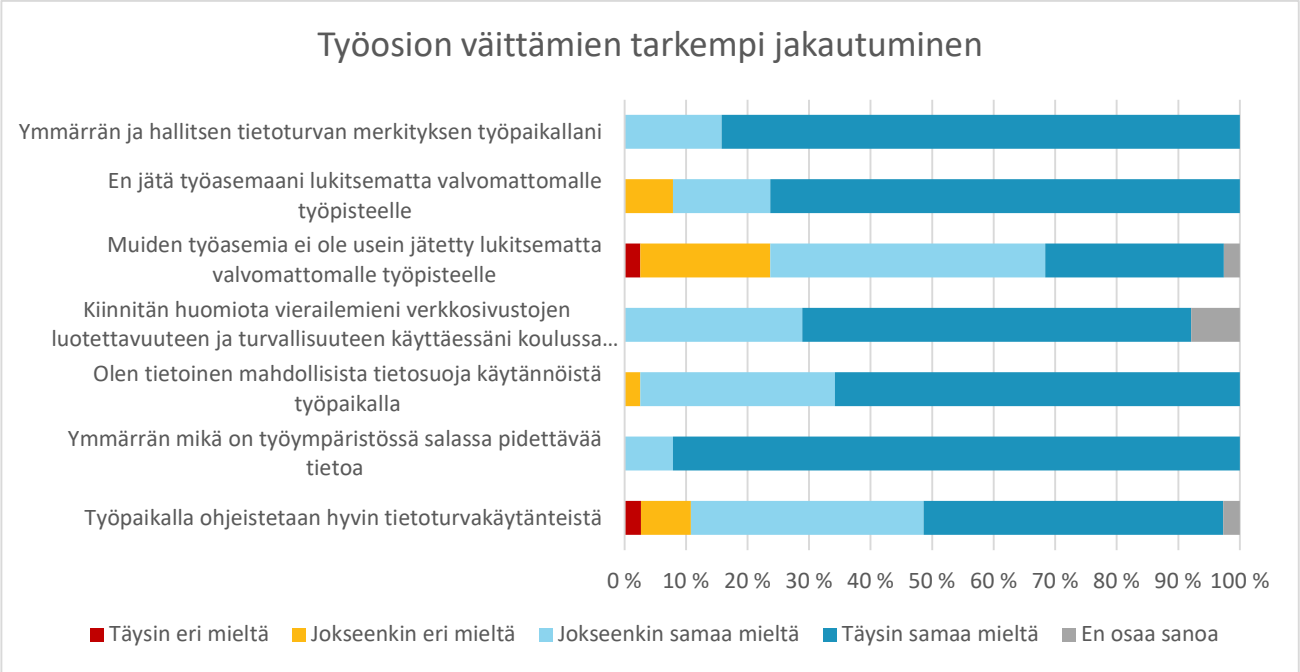
Seuraavassa pääosiossa kysely siirtyi tieto- ja kyberturvaosaamiseen työympäristössä. Ensimmäisenä opiskelijoilta kysyttiin, ovatko he olleet työsuhteessa ja/tai osallistuneet työharjoitteluun. Mikäli vastaus oli kielteinen, lomake ohjasi vastaajan suoraan seuraavaan pääosaan. Vastaajista 90 prosenttia (n=38) vastasi kyllä.

Kyselyn työosion väittämäpatteriston summamuuttujan alpha-arvo jäi arvoon 0,56. Tulos kyseenalaistaa reliabiliteetin, mutta tästä huolimatta tiettyjä väittämiä on kyetty käyttämään muiden kohtien analysoinnissa. Kyseinen patteristo on havainnollistettu kuviossa 10 Kysymyksiä tiputtamalla ei pystytty millään kombinaatiolla nostamaan alpha-arvoa korkeammalle kuin 0,58:aan. Tarkempi vastauksien jakautuminen on esitetty kuviossa 11



Kuvio 10 Työosion asenneväittämäjoukon summamuuttuja

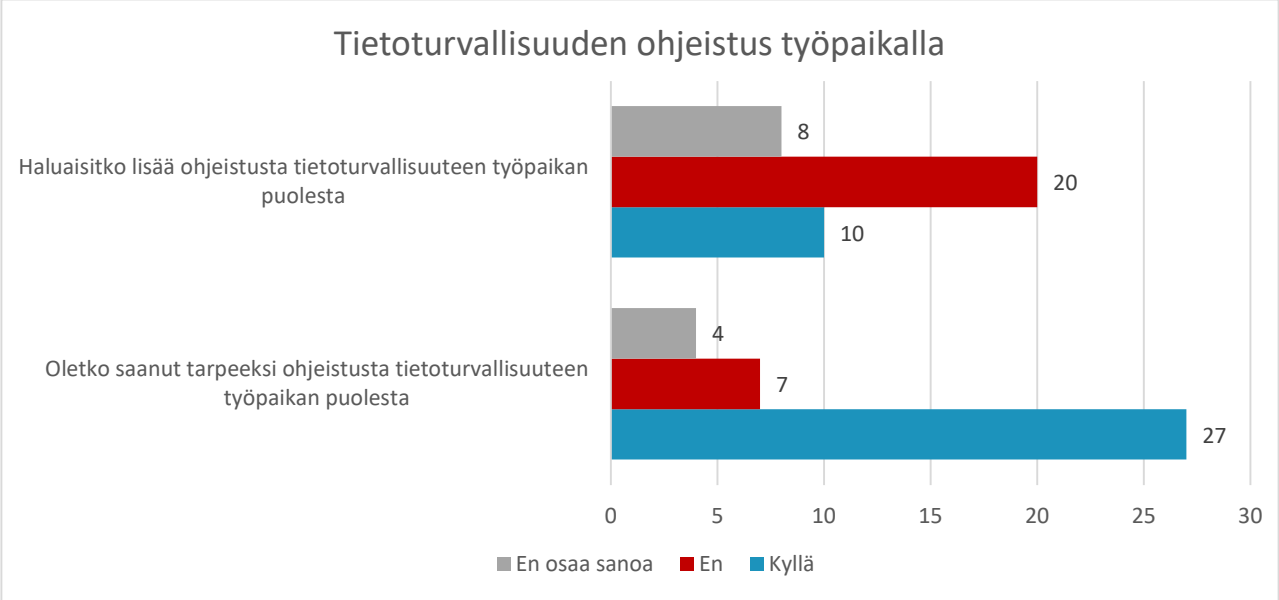
Kuviosta 9 nähdään, että työosion summamuuttujan keskiarvo 3,59 viittaa todella hyvään tietoturvaosaamiseen ja -taitoihin. Vaikuttava tekijä voi olla työpaikkojen parempi ohjeistus tietoturvaasioissa ja työympäristöissä: sosiaali- ja terveysalalla on erityisen tärkeää ylläpitää hyvää tietoturvallisuutta arkaluotoisten tietojen takia. Vastaajilta olisi voitu kysyä, kuinka pitkään he ovat olleet työelämässä. Tätä kautta pystyisi havainnollistamaan mahdollista yhteyttä siihen, kuinka itsevarmaksi vastaajat kokevat oman tietoturvaosaamisen ympäristössä, jossa he ovat olleet jo pidemmän aikaa, mikäli sellaista yhteyttä on.



Kuvio 11 Työosion asenneväittämäjoukon vastausten tarkempi jakautuminen

Samaan tapaan kuin kouluosiossa, vastaajilta kysyttiin, ovatko he saaneet tarpeeksi ohjeistusta työpaikan puolesta ja haluaisivatko he lisää ohjeistusta tietoturvallisuuteen työpaikan puolesta. Kuviosta 12 nähdään molempien kysymysten vastauksien jakautuminen. Tästä ilmenee selvästi, että vastaajat ovat kokeneet saavansa paremmin ohjeistusta työpaikalta kuin koululta. Tämän selittää mahdollisesti se, että työympäristössä ohjeistetaan tiettyyn tarkoitukseen ja toimintaan verrattuna kouluun, missä on hyödyllisempää ohjeistaa yleisemmällä tasolla. Tarkempi ohjeistus saattaa tuntua vastaajista laadukkaammalta ja tärkeämmältä.

Vaikka työympäristön ohjeistukseen ollaan tyytyväisempiä, on hyvä huomioida, että merkittävä osa – 26,3 prosenttia (n=10) – haluaisi silti lisää ohjeistusta tietoturvallisuuteen työpaikan puolesta. Myös usea vastaaja ei osannut sanoa haluaisivatko he lisää ohjeistusta, mikä ilmeni myös kouluosion samassa kysymyksessä. Työosion asenneväittämäjoukon tulos viittaisi vastaajien luottavan omaan tietoturvaosaamiseensa, mutta epävarmuus ohjeistuksen halussa on ristiriidassa tämän kanssa. Monella vastaajalla voi olla myös se mentaliteetti, että tietoturvasta voi aina oppia lisää. Sana “ohjeistus” ei myöskään saata kuvata sitä oppimistapaa, mitä vastaajat haluaisivat. Esimerkiksi tietoturvasta voidaan tiedottaa pienemmissä tietopaketeissa laajemman ohjaamisen sijasta.



Kuvio 12 Tietoturvallisuuden ohjeistuksen halu ja saanti työpaikalla

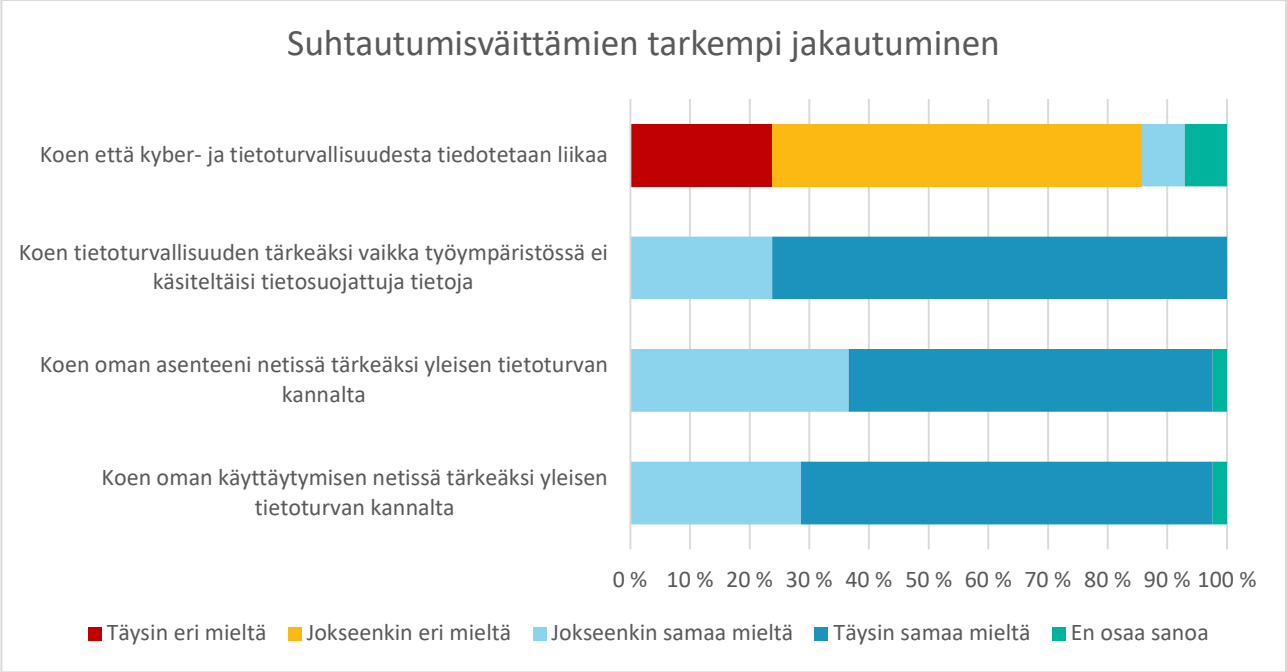
Opiskelijoilta kysyttiin, käyttävätkö he työpaikan tarjoamaa langatonta verkkoa. 26,3 prosenttia (n=10) vastasi myöntävästi ja 65,8 prosenttia (n=25) kieltävästi. 7,9 prosenttia (n=3) ilmoitti, että työpaikalla ei ole käytössä langatonta verkkoa. Verrattuna vastauksiin koulun langattoman verkon käytöstä, joista 73,8 prosenttia (n=31) olivat myönteisiä, tämä kontrasti työpaikan langattoman verkon käytössä on mielenkiintoinen. Vastaajille on mahdollisesti voitu ohjeistaa työpaikan puolesta, että langattoman verkon käyttöä tulisi välttää enemmän henkilökohtaisilla laitteilla. Vastaajilla voi myös olla vähemmän aikaa ja tarvetta käyttää henkilökohtaisia laitteita työpaikalla. Vastaajille on mahdollisesti myös tärkeämpi ylläpitää tietoturvaa työympäristössä, jossa käsitellään paljon arkaluontoista tietoa. Kyseinen kysymyksen esittäminen maissa, joissa mobiililaajakaistatarjonta on huonompi suhteessa Suomeen, tuottaisi todennäköisesti erilaisia ja mielenkiintoisia tuloksia.

4.5 Suhtautuminen

Tutkimuskyselyn viimeinen pääosio sisälsi vain yhden asenneväittämäjoukon, jolla selvitettiin vastaajien suhtautumista tietoturvan tärkeyteen ja sen tiedottamiseen. Asenneväittämäjoukossa oli

neljä väittämää, jotka osittain eivät sopineet muihin osioihin. Kyseisillä väittämillä myös pyrittiin löytämään mahdollisia negatiivisia näkemyksiä tietoturvallisuudesta tai sen tarpeesta.

Kuviosta 16 näkee selkeästi, että vastaajat kokevat tietoturvallisuuden tärkeäksi ja heidän oma käyttäytymisensä on tärkeä osa tietoturvallisuutta. Kyber- ja tietoturvallisuuden tiedottamisesta 7,2 prosenttia (n=3) oli jokseenkin sitä mieltä, että sitä tehdään liikaa. 7,2 prosenttia (n=3) ei osannut sanoa, miten he suhtautuvat kyseiseen väittämään. 61,9 prosenttia (n=26) olivat jokseenkin eri mieltä siitä, että tietoturvasta tiedotetaan liikaa. Tämä tulos voi viestiä siitä, että kyseiset vastaajat pitävät tiettyjä osia ohjeistuksesta turhina tai liian painotettuina, vaikka ohjeistus on kokonaisuudessaan määrällisesti sopivaa. Tässä tapauksessa vastaajien halu saada itselle relevanttia tiedotusta saattaa vaikuttaa tulokseen.



Kuvio 13 Suhtautumisosion asenneväittämäjoukon vastausten tarkempi jakautuminen

5 Yhteenveto

Opinnäytetyön tutkimuskysymyksenä oli selvittää kyber- ja tietoturvaosaamisen tasoa Jyväskylän ammattikorkeakoulun sosiaali- ja terveysalan opiskelijoiden keskuudessa ja kehittää tämän pohjalta mahdollisia tapoja parantaa heidän nykyistä osaamistaan. Kehitysehdotukset esitellään luvussa 6. Tutkimuskyselyprosessissa oli myös tarkoitus selvittää, miten kyseistä kyber- ja tietoturvaosaamista olisi järkevä kartoittaa.

Yhteen vedettynä opiskelijoiden kyber- ja tietoturvaosaaminen näyttää olevan tulosten perusteella hyvällä tasolla. Suurimpana puutteena osaamisessa ilmeni opiskelijoiden salasanakäytännöt, ja tähän liittyen myös kaikki vastaajat ilmoittivat, etteivät käytä salasanan hallintaohjelmia. Lisäksi tuloksista ilmeni muita pienempiä huomioita: esimerkiksi monen opiskelijan kotikoneelle ja käyttäjille on muilla ihmisillä pääsy. Kyselyssä ei kuitenkaan selvitetty, onko ulkopuolisilla pääsy salasanalla suojattuihin vai suojaamattomiin ympäristöihin. Lisäksi aineistosta löytyi selkeä ero työpaikan ja koulun tietoturvallisuuden ohjeistuksen välillä, joka ei suoranaisesti liity nykyiseen kyber- ja tietoturvaosaamiseen, mutta on hyvin olennainen mietittäessä opetus- ja kehitystapoja. Vastaajat todennäköisesti kokevat työpaikan tietoturvaohjeistuksen olennaisemmaksi kuin koulun vastaava ohjeistus, ja työpaikoilla on voitu myös panostaa enemmän tietoturvallisuuteen.

Opinnäytetyön tuloksien analysointivaiheessa ilmeni, että kysymykset oli rakennettu mittaamaan paremmin vastaajien omaa näkemystä heidän osaamisestansa. Tämä vuoksi analyysin keskiö siirtyi hieman pääkysymyksestä ja painoa lisättiin tieto- ja kyberturvan kehittämiselle sosiaali- ja terveysalalla. Tästä huolimatta tutkimuksen tuloksia voidaan kuitenkin hyödyntää esimerkiksi muokkaamaan opetusta ja ohjausta siihen suuntaan, mikä pienemmällä todennäköisyydellä esimerkiksi turhauttaisi opiskelijoita. Tuloksista selvisi selkeä itsevarmuus opiskelijoiden omaan tietoturvatietoisuuteen. Myös 35-vuotiaat ja vanhemmat näkyivät tuloksissa itsevarmempina verrattuna muihin ikäryhmiin. Näiden tulosten pohjalta on vaikea tehdä varmoja johtopäätöksiä siitä, viittaako kyseinen itsevarmuus hyvään vai huonoon suuntaan kokonaisturvallisuuden näkökulmasta. Jatkotutkimuksissa olisi hyvä selvittää tarkemmin samankaltaisen ryhmän oikeaa kyber- ja tietoturvatietämystä ja testata heidän osaamistaan sen kautta.

6 Kehittämisehdotukset

Tulosten pohjalta parhain kehitysehdotus on henkilökohtaisesti relevantimpi ohjaus, joka mukautuu osaamistasoon ja tiedon määrään. Opiskelijat ja varsinkin vanhemmat ikäryhmät näyttäisivät olevan itsevarmoja omasta osaamisestaan, mikä viestii siitä, että he myös tietävät omat ongelmakohtansa kyberturvallisuuden osalta. Ohjeistuksen määrä nähtiin osittain liiallisena, mihin keskitetympi ja räätälöidympi ratkaisu voi auttaa.

Käytännössä tämä kehitysehdotus voitaisiin toteuttaa, paloittelemalla ohjeistus aihealueisiin, josta ohjeistettava, ohjeistaja tai kurssinpitäjä voi valita relevantteja osioita. Yleisesti myös salasanojen ylläpidosta voidaan lisätä ohjeistusta, joka oli yksi puutteellisimmista osioista.

Huomionarvoista tässä on kuitenkin se, että kysely ei anna viitettä siitä, ovatko itsevarmat vastaajat oikeasti osaavia, mikä johtaa siihen, että heidän kyvystään itseohjautua relevanttiin ohjeistukseen ei saa varmuutta. Taipumus huonoihin salasanakäytäntöihin myös viestii siitä, että vastaajien oma näkemys osaamisesta ei välttämättä perustu hyviin kyberturvallisuusperiaatteisiin. Asiaa voi korjata osaamistesteillä, mutta yleisesti ottaen henkilökohtaisemman ohjeistuksen antaminen on jo tämän näkökohdan valossa monimutkaisempaa. Henkilökohtaistaminen vaatii myös enemmän resursseja: ohjeistukseen pitäisi laatia valmis materiaalipankki, josta voi poimia kurssiryhmälle sopivia täydennyksiä ja kurssit vaatisivat osaamiskartoituksen laatimisen.

7 Pohdinta

Heti opinnäytetyöprosessin alussa isoimmaksi ongelmaksi ilmeni työn rajaus, joka esiintyi hieman eri muodossa pitkin työtä. Kyberturvallisuuden mittaus on uusi ala (Edgar & Manz 2017, 33), mikä tuotti vaikeuksia sitä määriteltäessä ja rajatessa. Tietoturvallisuus ja kyberturvallisuus termien määritelmä vaihtui usein lähdettä vaihtaessa. Teoriaperustaa tehdessä päädyttiin kyberturvallisuuden määritelmään, jossa se sisältää mm. tietoturvallisuuden, tietosuojan allensa ja on hyvin olennainen osa kokonaisturvallisuutta. Tämä muistuttaa vahvasti Julkisen hallinnon kuvausta digitaalisen turvallisuuden viitekehyksestä (Julkisen hallinnon digitaalinen turvallisuus 2020, 16).

Rajausongelma jatkui osittain tutkimuskyselyn rakentamisvaiheessa, jossa suurimpana ongelmana oli mittareiden valitseminen ja kysymysten rakentaminen. Jälkeenpäin tarkasteltaessa kyselyä olisi

voitu parantaa monella tapaa. Esimerkiksi tietoa vastaajien elämäntilanteesta ei koettu tarpeelliseksi ja koko kysymys olisi voitu todennäköisesti jättää pois. Osa mittareista olisi voitu määrittää mittaamaan vastaajien todellista tietoturvaosaamista, josta on mainittu useaan kertaan analysointiosiossa. Kyselyn mittarit eivät ole myös niin koherentteja keskenään kuin ehkä olisi haluttu, mutta tätä ja aiempia puutteita pyrittiin lieventämään analysointivaiheessa keskittymällä siihen, kuinka tieto- ja kyberturvaohjeistusta voitaisiin kehittää näiden tulosten pohjalta. Nämä seikat kuitenkin väistämättä vaikuttivat tutkimustulosten käyttökelpoisuuteen.

Tutkimuskysely suoritettiin aikana, jolloin koronatilanne vielä vaikutti yhteiskunnallisiin normeihin ja tätä seikkaa oli vaikea sivuuttaa analysoitaessa tilanteen erikoisuuden vuoksi. On myös vaikea sanoa, kuinka moneen kohtaan tällä erityistilanteella oli vaikutusta tai kuinka paljon esimerkiksi etätöiden lisääntyminen vaikuttaa vastaajien tietoturvakäyttäytymiseen.

Analysointivaiheessa mielenkiintoa herätti varsinkin tietoturvallisuuden ohjeistuksen saannin ja halun ero koulu- ja työympäristön välillä. Tietoturvan kehittämisen kannalta tämä oli myös tärkeä kohta selvittää, mihin analysoinnin paino oli jo siirretty. Tähän liittyen tutkimuskyselyssä olisi voitu kysyä esimerkiksi tarkemmin millaista ohjeistusta vastaajat olivat jo saaneet.

Lähteet

A 2016/679/EU. Euroopan parlamentin ja neuvoston asetus henkilötietojen käsittelystä. Viitattu 15.03.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504.

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Opas tietosuojavastaavalle uudesta tietosuoja-asetuksesta. Tallinna: Tietosanoma Oy.

Edgar, T. W. & Manz, D. O. 2017. Research methods for cyber security. Cambridge, England: Syngress.

Gil, A. 2018. Data security – Confidentiality, integrity & availability. KVA:n sivustolle tehty nettiartikkeli. Viitattu 18.02.2021. https://www.kvausa.com/data-security-confidentiality-integrity-and-availability/.

Tietoturva. 2020. Opiskelijan digitaidot -kurssi. Helsingin Yliopisto. Viitattu 18.02.2021. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/.

Henkilöstön tietoturvaohje. 2013. VAHTI:n (Valtiohallinnon tietoturvallisuuden johtoryhmä) tietoturvaohje henkilöstölle. Viitattu 18.02.2021. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet .

HeTiL 523/1999. Henkilötietolaki. Viitattu 15.03.2021. https://www.finlex.fi, säädökset alkuperäisinä.

Kauppi, J. 2019. Mitä on tietoturva?. Blogi-kirjoitus Leijona Security Oy:n sivustolle. Viitattu 13.03.2021. https://www.leijonasecurity.fi/2019/07/26/tietoturva/.

KvantiMOTV. 2008. Mittaaminen: Mittarin luotettavuus. Menetelmäopetuksen tietovaranto -verkkojulkaisu. Yhteiskuntatieteellinen tietoarkisto. Viitattu 13.04.2021. https://www.fsd.tuni.fi/menetelmaopetus/mittaaminen/luotettavuus.html#reliabiliteetti.

Julkisen hallinnon digitaalinen turvallisuus. 2020. Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta. Viitattu 13.01.2021. https://julkaisut.valtioneuvosto.fi/handle/10024/162169.

Kyberturvallisuuden sanasto. 2018. Turvallisuuskomitean vuosina 2017–2018 laadittu projekti Sanastokeskus- sivustolle. Viitattu 4.2.2021. https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Kyberturvallisuus ja kybertoimintaympäristö. N.d. Ulkoministerion ulko- ja turvallisuuspolitiikka -artikkeli. Ulkoministeriö. Viitattu 19.02.2021. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto/.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J. Rusi, T. & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja. Valtioneuvoston kanslia. Viitattu 13.01.2021.

https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nyky-tila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Limnéll, J., Majewski, K. & Salminen, M. 2014. *Kyberturvallisuus*. Jyväskylä: Docendo.

Tietosuojalaki 1050/2018. Tietosuojalaki. Viitattu 15.03.2021. https://www.finlex.fi, ajantasainen lainsäädäntö.

Yle seurasi Vastaamon tietomurtoa. 2020. Ylen seuranta Vastaamon tieto-murtoa koskien. Viitattu 13.01.2021. https://yle.fi/uutiset/3-11612399

Vehkalahti, K. 2008. Kyselytutkimuksen mittarit ja menetelmät. Vammala: Tammi.

Liitteet

Liite 1. Saatekirje kyselylomakkeelle

Hei!

Olen tieto- ja viestintätekniikan opiskelija Jyväskylän Ammattikorkeakoulussa ja teen osana opinnäytetyötäni tutkimuskyselyä. Kyselyllä selvitetään osaamista ja suhtautumista kyber- ja tietoturvallisuuteen Jyväskylän Ammattikorkeakoulun sosiaali- ja terveysalan opiskelijoiden keskuudessa.

Kyselyn vastaukset tullaan käsittelemään nimettöminä ja luottamuksellisesti. Vastauksia käsittelee ja analysoi opinnäytetyön tekijä Maliniemi Teemu. Kyselytulokset säilötään vuoden ajan opinnäytetyön valmistumisesta.

Vastaaminen on helppoa ja kestää noin 5–15 minuuttia.

Pyydän vastaamaan kyselyyn viimeistään 9.3.2021 avaamalla oheinen osoite [SurveyLinkText] tai kopioimalla kyseinen osoite ja liittämällä se Internet-selaimen osoitekenttään.

Jokainen vastaus auttaa kyber- ja tietoturvallisuuden kartoittamista ja kehittämistä.

Lisätietoa tutkimuksesta ja kyselylomake asioista saa Teemu Maliniemeltä (k8434@student.jamk.fi).

Etukäteen vastauksistanne kiittäen
Teemu Maliniemi

Liite 2. Muistutuskirje

Hei,

Muistutan vastaamisesta “Opiskelijoiden kyber- ja tietoturvaosaaminen” -kyselyyn.

Kyselyllä selvitetään osaamista ja suhtautumista kyber- ja tietoturvallisuuteen Jyväskylän Ammattikorkeakoulun sosiaali- ja terveysalan opiskelijoiden keskuudessa. Kyselyn vastaukset tullaan käsittelemään nimettöminä ja luottamuksellisesti.

Tämänhetkinen kyselyn vastausprosentti on 6 %. Vastauksien avulla voidaan mahdollisesti kehittää kyber- ja tietoturvallisuutta, joka on erityisen tärkeää alalla, joka käsittelee usein luottamuksellisia tietoja.

Vastaaminen on helppoa ja kestää noin 5–10 minuuttia.

Pyydän vastaamaan kyselyyn viimeistään 17.3.2021 avaamalla oheinen osoite [SurveyLinkText] tai kopioimalla kyseinen osoite ja liittämällä se Internet-selaimen osoitekenttään.

Lisätietoa tutkimuksesta ja kyselylomakeasioista saa Teemu Maliniemeltä (k8434@student.jamk.fi).

Kiittäen vastauksistanne
Teemu Maliniemi

Liite 3. Toinen muistutuskirje

Hei,

Muistutan vielä vastaamisesta “Opiskelijoiden kyber- ja tietoturvaosaaminen” -kyselyyn.

Vastauksia on jo tullut kivasti, mutta vielä tarvitsisin lisää luotettavamman tutkimustuloksen aikaansaamiseksi. Jokaisella vastauksella saadaan koottua erittäin arvokasta tietoa opiskelijoiden mielipiteistä ja tavoista. Vastauksenne on tärkeä.

Kyselyssä pyritään selvittämään kyber- ja tietoturva osaamista Jyväskylän Ammattikorkeakoulun sosiaali- ja terveysalan opiskelijoiden keskuudessa. Kyselyn vastaukset tullaan käsittelemään nimettöminä ja luottamuksellisesti. Kysely on osa opinnäytetyötä.

Kyselyn vastausaikaa on pidennetty perjantaihin 19.03.2021 asti, joten pyytäisin vastaamaan siihen mennessä avaamalla oheinen osoite [SurveyLinkText] tai kopioimalla kyseinen osoite ja liittämällä se Internet-selaimen osoitekenttään.

Lisätietoa tutkimuksesta ja kyselylomakeasioista saa Teemu Maliniemeltä (k8434@student.jamk.fi).

Kiittäen vastauksistanne
Teemu Maliniemi

Liite 4. Tutkimuskysely

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Opiskelijoiden kyber- ja tietoturvaosaaminen

Pakolliset kentät merkitään asteriskilla (*) ja ne tulee täyttää lomakkeen viimeistelemiseksi.

Tervetuloa vastaamaan opiskelijoiden kyber- ja tietoturvaosaamiskyselyyn

Kyselyllä selvitetään osaamista ja suhtautumista kyber- ja tietoturvallisuuteen Jyväskylän ammattikorkeakoulun sosiaali- ja terveysalan opiskelijoiden keskuudessa. Kyselyn vastaukset käsitellään nimettömänä ja kysely on jaettu 5 eri osioon: Vapaa-aika, koulu, työympäristö, suhtautuminen ja taustatiedot. Kysely on osa opinnäytetyötä, jossa tutkitaan opiskelijoiden kyber- ja tietoturvaosaamista ja millainen vaikutus sillä on kokonais- kyberturvallisuuteen ja kuinka sitä voisi mahdollisesti kehittää. Ohessa on muutamia vastaamisohjeita.

Vastaamisohjeet:
1. Vastaa kysymyksiin omien olemassa olevien tietojesi perusteella.
2. Valitse kysymyksissä se vaihtoehto, joka on parhaiten sopiva, jollei kysymyksen ohjeissa muuten mainita.
3. Lue kukin kysymys, vastausvaihtoehdot ja mahdollinen ohjeteksti huolellisesti.
4. Jokaisen sivun lopussa on kenttä, johon voit halutessasi tarkentaa yhtä tai useampaa vastausta
5. Vastaaminen kestää noin 5-15 minuuttia

Taustatieto

1. Sukupuoli *

- ○ Mies
- ○ Nainen
- ○ Muu
- ○ En halua vastata

2. Ikäjakauma *

- ◯ Alle 20 v.
- ◯ 20–22
- ◯ 23–25
- ◯ 26–28
- ◯ 29–31
- ◯ 32–34
- ◯ Yli 35v.
- ◯ En halua vastata

3. Suoritettava tutkinto *

- ◯ AMK
- ◯ YAMK
- ◯ Muu

4. Mikä seuraavista sopii elämäntilanteeseesi *

- ◯ Päätoiminen opiskelu
- ◯ Opiskelu osa-aikaisten töiden ohella
- ◯ Säännöllisesti kokopäivätöissä
- ◯ En halua vastata

5. Tarkennus (vapaaehtoinen)

Voit merkitä alapuolella olevaan kenttään tarkennuksen ja kysymyksen numeron mitä tarkennus koskee (esim. Kysymys 4: "Tarkennus")

Vapaa-aika

6. Käytössäni on kotikone (kannettava tietokone/tabletti, pöytäkone)

- ◯ Kyllä
- ◯ Ei

7. Vapaa-ajalla / kotona

Seuraavassa kysymyksessä on sarja väittämiä. Valitse oikealta mikä kuvaa parhaiten omaa mielipidettäsi

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Käsittelen usein koulu/työasioita kotikoneella	◯	◯	◯	◯	◯
Muilla ihmisillä on pääsy koneelleni	◯	◯	◯	◯	◯
Muut ihmiset voivat päästä käyttäjätileilleni (esim. sähköposti, Facebook)	◯	◯	◯	◯	◯
Kiinnitän huomiota vierailemieni verkkosivustojen luotettavuuteen ja turvallisuuteen	◯	◯	◯	◯	◯
Kiinnitän huomiota langattomien verkkojen luotettavuuteen ja turvallisuuteen ennen kuin yhdistän niihin puhelimeni tai tietokoneeni	◯	◯	◯	◯	◯
Käytän aina eri salasanaa eri palveluissa	◯	◯	◯	◯	◯

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Vaihdan salasanojani säännöllisin aikavälein	◯	◯	◯	◯	◯
Tiedän minkälainen on vahva salasana	◯	◯	◯	◯	◯

8. Käytätkö tiedostojen säilyttämiseen pilvipalveluita esim. OneDrive, Google Drive, Dropbox.

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa

9. Käytätkö salasanojen hallintaohjelmaa? (esim. Lastpass, Dashlane)

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa

10. Kotikoneen ohjelmistot

	Kyllä	En	En osaa sanoa	En omista kotikonetta
Käytätkö Virustorjuntaohjelmistoa kotikoneellasi?	◯	◯	◯	◯
Käytätkö palomuuria kotikoneellasi?	◯	◯	◯	◯
Käytätkö virustentorjuntaohjelmaa kotikoneellasi?	◯	◯	◯	◯
Käytätkö VPN-ohjelmistoa kotikoneellasi?	◯	◯	◯	◯
Onko kotikoneellasi käytössä automaattiset päivitykset	◯	◯	◯	◯

	Kyllä	En	En osaa sanoa	En omista kotikonetta
Käytätkö kotikoneellasi automaattista näytön lukitsemista, jonka jälkeen kone vaatii tunnistautumisen esim. salasanan syöttämisen	○	○	○	○

11. Tarkennus (vapaaehtoinen)

Voit merkitä alapuolella olevaan kenttään tarkennuksen ja kysymyksen numeron mitä tarkennus koskee (esim. Kysymys 4: "Tarkennus")

Koulu

12. Koulu

Seuraavassa kysymyksessä on sarja väittämiä. Valitse oikealta mikä kuvaa parhaiten omaa mielipidettäsi

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Kiinnitän huomiota vierailemieni verkkosivustojen luotettavuuteen ja turvallisuuteen käyttäessäni koulussa tietokonetta	○	○	○	○	○
En jätä omia digilaitteitani ilman valvontaa koulussa ollessani	○	○	○	○	○
Olen tietoinen koulun mahdollisista tietosuojakäytännöistä	○	○	○	○	○
Ymmärrän mikä on kouluympäristössä salassa pidettävää tietoa	○	○	○	○	○
Koulussa ohjeistetaan hyvin tietoturvakäytänteistä	○	○	○	○	○

13. Oletko saanut tarpeeksi ohjeistusta tietoturvallisuuteen koulun puolesta?

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa

14. Haluaisitko lisää ohjeistusta tietoturvallisuuteen koulun puolesta?

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa

16. Käytätkö koulun tarjoamaa langatonta (wi-fi)verkkoa omilla henkilökohtaisilla laitteillasi (puhelin, läppäri, tabletti)

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa
- ◯ Koulussa ei ole tarjolla langatonta verkkoa

17. Tarkennus (vapaaehtoinen)

Voit merkitä alapuolella olevaan kenttään tarkennuksen ja kysymyksen numeron mitä tarkennus koskee (esim. Kysymys 4: "Tarkennus")

Työympäristö

18. Oletko ollut työsuhteessa tai osallistunut työharjoitteluun

- ◯ Kyllä

- ◯ En

19. Työ

Seuraavassa kysymyksessä on sarja väittämiä. Valitse oikealta mikä kuvaa parhaiten omaa mielipidettäsi

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Ymmärrän ja hallitsen tietoturvan merkityksen työpaikallani	◯	◯	◯	◯	◯
En jätä työasemaani lukitsematta valvomattomalle työpisteelle	◯	◯	◯	◯	◯
Muiden työasemia ei ole usein jätetty lukitsematta valvomattomalle työpisteelle	◯	◯	◯	◯	◯
Kiinnitän huomiota vierailemieni verkkosivustojen luotettavuuteen ja turvallisuuteen käyttäessäni koulussa tietokonetta	◯	◯	◯	◯	◯
Olen tietoinen mahdollisista tietosuoja käytännöistä työpaikalla	◯	◯	◯	◯	◯
Ymmärrän mikä on työympäristössä salassa pidettävää tietoa	◯	◯	◯	◯	◯
Työpaikalla ohjeistetaan hyvin tietoturvakäytänteistä	◯	◯	◯	◯	◯

20. Käytätkö työpaikan tarjoamaa langatonta verkkoa (wi-fi) omilla henkilökohtaisilla laitteillasi (puhelin, läppäri, tabletti)

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa
- ◯ Työpaikalla ei ole käytössä langatonta verkkoa

21. Oletko saanut tarpeeksi ohjeistusta tietoturvallisuuteen työpaikan puolesta

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa

22. Haluaisitko lisää ohjeistusta tietoturvallisuuteen työpaikan puolesta

- ◯ Kyllä
- ◯ En
- ◯ En osaa sanoa

23. Tarkennus (vapaaehtoinen)

Voit merkitä alapuolella olevaan kenttään tarkennuksen ja kysymyksen numeron mitä tarkennus koskee (esim. Kysymys 4: "Tarkennus")

Suhtautuminen

24. Suhtautuminen

Seuraavassa kysymyksessä on sarja väittämiä. Valitse oikealta mikä kuvaa parhaiten omaa mielipidettäsi

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Koen oman käyttäytymisen netissä tärkeäksi yleisen tietoturvan kannalta	◯	◯	◯	◯	◯
Koen oman asenteeni netissä tärkeäksi yleisen tietoturvan kannalta	◯	◯	◯	◯	◯

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Koen tietoturvallisuuden tärkeäksi vaikka työympäristössä ei käsiteltäisi tietosuojattuja tietoja	◯	◯	◯	◯	◯
Koen että kyber- ja tietoturvallisuudesta tiedotetaan liikaa	◯	◯	◯	◯	◯

25. Tarkennus (vapaaehtoinen)

Voit merkitä alapuolella olevaan kenttään tarkennuksen ja kysymyksen numeron mitä tarkennus koskee (esim. Kysymys 4: "Tarkennus")