Miten työntekijän tulisi hallita tietoturvallisuuttaan?

Teemu Heinonen

Haaga-Helia ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
2022

Tiivistelmä

Tekijä(t)
Teemu Heinonen

Tutkinto
Tietojenkäsittely, tradenomi

Raportin/Opinnäytetyön nimi
Miten työntekijän tulisi hallita tietoturvallisuuttaan?

Sivu- ja liitesivumäärä
46 + 15

Tässä tutkimuksessa käsiteltiin työntekijän tietoturvallisuuden hallintaan liittyviä asioita. Tutkimus laadittiin ensisijaisesti toimeksiantajayritykselle, jolla pyrittiin organisaation henkilöstön tietoturvallisuuden ja tietoturvallisuusosaamisen kehittämiseen.

Työssä käytiin läpi työntekijän tietoturvallisuuteen kohdistuvia uhkia ja niistä aiheutuvia riskejä. Tavoitteena oli parantaa työntekijöiden tietoturvaosaamista ja tietoisuutta uhkiin liittyen. Uhkien pohjalta esitettiin useita keinoja, joilla kunkin osa-alueen uhilta voidaan suojautua, sekä niiden riskejä minimoida. Tutkimuksen tietoperusta pohjautui tietoturva-asioiden, tietoturvauhkien ja suojautumiskeinojen läpikäyntiin.

Tutkimuksen teoriaan pohjautuen luotiin tutkimuskysely, jolla kartoitettiin toimeksiantajan henkilöstön tietoturvallisuutta ja työntekijöiden käyttämiä käytäntöjä tietoturvallisuuden hallintaan liittyen. Kysely toteutettiin 2022 keväällä. Siihen osallistui toimeksiantajayrityksestä vapaaehtoisesti 65 työntekijää.

Tutkimus rajattiin koskemaan työntekijöiden tietoturvallisuuteen liittyviä asioita mobiililaitteiden, etätyön, sekä työtietokoneen osalta. Tutkimuksella haluttiin vastata työntekijälle tietoturvallisuuteen liittyviin kysymyksiin: Mitä työntekijän tulee hallita tietoturvastaan ja miksi? Millaisia uhkia ja riskejä tietoturvaan liittyy? Millä konkreettisilla keinoilla työntekijän tulisi suojautua tietoturvallisuuteen kohdistuvia uhkia vastaan?

Näihin kysymyksiin haettiin vastaukset laadullisella tutkimusmenetelmällä kirjallisuutta, sekä monipuolisia ja laadukkaita ohjeita hyödyntämällä.

Tutkimustulokset osoittivat, että työntekijöiden tietoturva on yleisesti hyvä, jos tietoturvaperehdytystä on annettu perusperehdytyksen tasolla. Tietojenkalastelu osoittautui suurimmaksi uhaksi työntekijöiden tietoturvalle ja siitä oli myös eniten kokemuksia. Käyttäjätilien suojaamiseen liittyvien käytäntöjen osalta työntekijöillä oli parannettavaa yksittäisillä osa-alueilla. Kyselyyn osallistuneet työntekijät arvostivat ja pitivät yleisesti tietoturvallisuutta hyvin tärkeänä asiana työarjessaan.

Asiasanat
Tietoturva, työntekijät, ohjeet, yritykset, digitalisaatio, tiedonhallinta, tietosuoja, riskienhallinta, tietoverkkorikokset, tietojärjestelmät, suojaus

Sisällys

1 Johdanto

Nykyisessä yhteiskunnassamme, jossa lähes kaikki on digitaalista ja yrityksien digitaalisia ratkaisuja kehitetään jatkuvasti entistä tehokkaimmiksi ja kilpailukykyisimmiksi, on työntekijälle asettunut entistä suurempi vastuu tietoturvallisuudestaan. Tämän kehityksen mukana työntekijästä on myös muodostunut keskeinen ja useasti helpoin portti hyökkääjille yrityksen sisälle pääsemiseen. Työntekijän ja tietoturvasta vastaavien henkilöiden on tärkeää analysoida ja hallita työntekijän tietoturvallisuutta jatkuvasti, koska ohjelmistot, työtehtävät, työntekijät ja tietotekninen infrastruktuuri ovat nopeasti muuttuvia ja vaihtuvia. Ohjelmistot ja tietotekninen infrastruktuuri muuttuu usein, esimerkiksi päivitysten ja yleisen kehityksen myötä. Tietoturvallisuutta vastaan hyökkäävät rikolliset keksivät ja löytävät jatkuvasti uusia sekä tehokkaampia keinoja tietoturvan rikkomiseen, joilla pyritään yleensä hankkimaan rahallista etua tai näyttämään omia taitoja. Tästä syystä on välttämätöntä tunnistaa omaan tietoturvallisuuteen kohdistuvat uhat, hallita omaa tietoturvallisuutta ja ylläpitää tietoturvaosaamisen tasoa työntekijänä. Pahimmassa tapauksessa työntekijästä aiheutuneet tietoturvariskit voivat johtaa pitkiin rikostutkintoihin ja oikeuskäsittelyihin, koska tietoturvarikollisten jäljittäminen on usein vaikeaa ja aikaavievää. Sivullisille uhreille eli mahdolliselle työntekijälle tai asiakkaalle tässä prosessissa voi aiheutua raskaita haittoja. Näiden seuraukset heijastuvat siten suoraan yrityksen liiketoimintaa haittaavina tekijöinä.

Tutkimuksessa käsitellään työntekijän tietoturvaan kohdistuvia uhkia ja työntekijään liittyviä tietoturvariskejä, jotka kuuluvat kokonaan tai osittain työntekijän vastuulle. Tutkimuksen teorian pohjana on hyödynnetty vuonna 2021 syksyllä tutkimusprosessi kurssilla toteutettua tutkimusraporttia samasta aiheesta. Käsiteltävän aiheen pääpisteenä on työntekijän henkilökohtainen tietokone, koska se on valtaosan työntekijöistä keskeisin työväline työpaikoilla. Tutkimuksen rajausta on hieman laajennettu aiemmasta käsittelemään lisäksi mobiililaitteiden tietoturvaan liittyviä asioita ja etätöihin liittyvien verkkolaitteiden tietoturvaa, joiden tietoturvan hallinta kuuluu osittain työntekijälle, ja on lisäksi merkittävä osa työntekijöiden tietoturvasta. Tutkimuksen pohjalta pyritään antamaan selkeitä keinoja ja neuvoja, joilla tietoturvallisuuteen kohdistuvia uhkia voidaan tunnistaa ja riskejä hallita itse työntekijän toimesta.

Tutkimuksen tietoperusta, eli luvut 2 ja 3 pohjautuvat sisällönanalyysiin. Tutkimuksen empiirinen osa käsittää luvut 4, 5 ja 6. Tutkimus on menetelmältään laadullinen, jossa systemaattisen aineiston analysoinnin lisäksi, käytetään tutkimuksen monipuolisuuden kannalta toimeksiantajayrityksen henkilöstölle luotua kyselytutkimusta teoriaan eli tietoperustaan pohjautuen. Tutkimuksen kyselytuloksia hyödynnetään myös toimeksiantajayrityksessä tietoturvakoulutusten järjestämiseen ja tietoturvan eri osa-alueiden kehittämiseen.

Käsiteltävä aihe on lähes aina tutkimisen arvoinen, koska se on nopeasti ja jatkuvasti muuttuva ja kansainvälinen aihe, joka on hyvin olennainen osa arkielämäämme ja myös yhteiskuntaamme yleisesti. Työntekijän tietoturvallisuuteen liittyen on olemassa monipuolisia ja laadukkaita ohjeita, mutta ne ovat usein useassa eri paikassa ja niiden sisältö on osittain puutteellista, joten tässä työssä pyritään kokoamaan oleellisimmat ohjeet ja tiedot yhdeksi asiakokonaisuudeksi. Tietoturvallisuutta ei tulisi missään tilanteissa laiminlyödä, ja usein ilmenneet laiminlyönnit eivät ole tarkoituksellisia, joten tietoturvaohjeistuksen avulla ja tietoturvallisuuteen kohdistuvia uhkia käsittelemällä, pyritään saamaan työntekijöiden osalta tähän ongelmaan ratkaisu. Näiden ongelmanratkaisua varten on myös listattu laajasti keinoja, joilla uhilta voidaan suojautua.

Tutkimustuloksilla pyritään muodostamaan monipuolinen, mutta selkeä tietopaketti, jonka avulla työntekijä pystyy kehittämään kriittisintä tietoturvaansa ja havaitsemaan mahdollisia epäkohtia omassa tietoturvallisuudessaan tai tietoturvaosaamisessaan. Asiaan käytännönläheisellä lähestymisellä ja erilaisilla esimerkeillä on tarkoitus motivoida työntekijää syventämään tietoisuuttaan tietoturvallisuuden tärkeydestä, sekä ajankohtaisiin tietoturvauhkiin ja -riskeihin liittyen. Tutkimuskysely toimii lisäksi tietoturvallisuuden hallintaa havainnollistavana tekijänä työntekijälle, sekä tässä työssä tutkittavien asioiden merkitystä todistavana. Tutkimus on toteutettu pääosin työn toimeksiantajan käyttöön, mutta tutkimuksen sisältö sopii varsin hyvin myös yleiseen käyttöön, koska se sisältää monipuolisesti ohjeita yleisiin ja myös ajankohtaisiin työntekijöihin kohdistuviin tietoturvauhkiin liittyen, sekä keinoja niiden riskien minimointiin. Tietyille aloille tai tehtäväalueille on yksityiskohtaisempia ja yleisistä laajempia tietoturvallisuusohjeita työnantajan tai muiden toimijoiden toimesta, jotka työntekijän tulee lisäksi ottaa huomioon. Tässä työssä ei käydä kyseisiä poikkeuksia läpi, vaan ohjeistaminen on yleisluonteisempaa. Vaikka tämä tutkimus keskittyy ensisijaisesti työntekijöihin kohdistuviin tietoturvauhkiin sekä -riskeihin, niin käydyistä asioista suurinta osaa voi hyödyntää myös työn ulkopuolella, koska uhkat ovat samankaltaisia.

Toimeksiantajayritys on keskisuuri yritys, joka työllistää yli 120 henkilöä ja jonka liikevaihto oli vuonna 2021 yli 120 miljoonaa euroa. Yrityksen toimiala ja liiketoiminnan luonne vaatii toimiakseen paljon henkilötietojen käsittelyä, joten laadukkaan tietoturvallisuuden ja tietosuojan ylläpitäminen on edellytys sujuvan liiketoiminnan kannalta. Toimeksiantajaa esitellään tarkemmin työn neljännessä luvussa. Tutkimusrajauksessa ja materiaalin valinnan pohjana työntekijällä tarkoitetaan yleisesti toimistotyöntekijöitä, tai muita työntekijöitä, jotka tekevät työnsä pääosin tietokoneella, sekä käyttävät mahdollisesti mobiililaitteita.

Taulukko 1. Peittomatriisi.

Alaongelma	**Teoreettinen viitekehys**	**Kyselylomakkeen kysymykset**	**Tutkimuksen tulokset**
Mitä työntekijän tulee hallita tietoturvastaan ja miksi?	2, 3	2, 2.2, 2.3	5.2, 5.5, 6
Millaisia uhkia ja riskejä työntekijän tietoturvaan liittyy?	2.1, 2.1.2, 2.1.3, 2.2, 2.3	2.1.1, 2.1.2, 2.1.3, 2.2, 2.3	5.3, 5.4, 6
Millä konkreettisilla keinoilla työntekijän tulisi suojautua tietoturvallisuuteen kohdistuvia uhkia vastaan?	3.1, 3.2, 3.3, 3.4, 3.5, 3.6	3.1, 3.2, 3.3, 3.4, 3.5, 3.6	5.2, 5.5, 6

Peittomatriisilla (taulukko 1), havainnollistetaan tutkimuksen alaongelmien yhteyttä teoreettiseen viitekehykseen, tutkimuksen alaongelmiin, sekä tutkimuksen tuloksiin.

Tutkimuksella pyritään siis vastaamaan työntekijälle kysymyksiin:

- Mitä asioita työntekijän tulee hallita tietoturvallisuudestaan ja miksi?
- Millaisia uhkia työntekijän tietoturvaan kohdistuu ja millaisia riskejä niistä muodostuu?
- Mitkä ovat ne konkreettiset keinot, joilla tietoturvauhkia vastaan voidaan suojautua, sekä riskejä minimoida?

1.1 Tutkimuksessa käytettyjä käsitteitä

Tietoturvallisuus (tietoturva) – Tarkoittaa tiedon luotettavuuden, eheyden ja saatavuuden ylläpitoa ja varmistusta.

Hakkerointi – Toimintaa, jossa vaikutetaan tai tunkeudutaan tietoverkkoon, tietojärjestelmään tai niiden sisältämään tietoon ja käytetään ohjelmaa, palvelua tai muuta resurssia hyväksi.

Tietojenkalastelu (phishing) – Toimintaa, jonka tavoitteena on saada rikollisten haltuun käyttäjätunnuksia ja salasanoja tai muita käyttäjälle tai organisaatiolle arvokkaita tietoja.

Varmuuskopio – Tietojen kopiointi useampaan tallennusmediaan ja niiden säilyttäminen toisistaan erillään turvallisessa paikassa. Mikäli alkuperäinen tiedosto tuhoutuisi, se voidaan palauttaa varmuuskopioinnin avulla.

VPN – Virtuaalinen erillisverkko (Virtual Private Network). Tapa salata ja luoda yksityinen ja tietoturvallinen internet-yhteys.

Sosiaalinen vaikuttaminen (social engineering) – Toimintaa, jolla rikollinen hyödyntää sosiaalisella vaikuttamisella tai manipuloinnilla kohteensa hyväuskoisuutta tai auttamishalua.

Päivitys – Päivitykset ovat prosesseja, joilla suojataan järjestelmiä ja sovelluksia. Niiden avulla paikataan tyypillisesti tietoturvahaavoittuvuuksia, korjataan muita virheitä tai parannetaan ominaisuuksia.

GDPR – General Data Protection Regulation, on yleinen tietosuoja-asetus. Tietosuoja-asetuksessa määritetään EU:n määräämät tietosuojavaatimukset (standardit) yrityksille ja organisaatioille henkilötietojen keräämiseen, säilytykseen ja käsittelyyn liittyen.

Salasananhallintaohjelma – Ohjelma, jota voidaan käyttää salasanojen hallintaan. Ohjelmaan voidaan tallentaa useita eri salasanoja, ja salasanojen hyödyntäminen tileissä edellyttää vain yhden vahvan salasanan muistamista kirjautuessa palveluun.

Palomuuri – Ohjelmisto tai laite, joka estää luvattomat yhteydenotot Internetistä tietokoneeseen. Se sallii vain luotettavat ja turvalliset yhteydenotot Internetistä.

(Kyberturvallisuuskeskus 2020a.)

Reititin – Verkkolaite, joka yhdistää tietoverkon osia toisiinsa ja jonka avulla voidaan muodostaa yhteys internetiin.

Kiristysposti – Kiristystapa, jolla hyökkääjä pyrkii yleensä saamaan rahaa käyttäjältä väittämällä murtautuneen käyttäjän tietokoneelle ja tietoihin. Liittyen esimerkiksi aikuisviihteen käyttöön tai muuhun arkaluonteiseen tietoon.

Salasana – Avain käyttäjätileihin tai laitteisiin, jolla pyritään varmistamaan, että pääsy säilyy vain tarkoitetulla taholla.

Kaksi- tai monivaiheinen tunnistautuminen (2FA/MFA) – Tekniikka, jolla pyritään varmentamaan henkilön identiteetti kahta tai useampaa tunnistautumismenetelmää käyttämällä. Tekniikalla pyritään estämään käyttäjätilien luvaton käyttäminen.

Tietoverkkorikollisuus – Tarkoittaa rikollisuutta, jonka toiminta tapahtuu sähköisissä toimintaympäristöissä ja tietoverkoissa.

Palvelunestohyökkäys (DoS) – tarkoittaa hyökkäystä, jossa kohteeseen tuotetaan suuri määrä liikennettä, jolla pyritään kaatamaan verkkopalvelu tai estämään sen käyttöä.

Kyberterrorismi – Toimintaa, jossa pyritään aiheuttamaan fyysistä vahinkoa hyödyntämällä kybertoimintaympäristöjä (tietoverkkoja).

Valtiollinen tiedustelu – Tiedustelua, jolla pyritään suojaamaan valtion kansallista etua sisältäviä tietoja ja keräämään valtiolle hyödyllistä tietoa muista maista.

Haavoittuvuus – Haavoittuvuudella tarkoitetaan tietoturva-aukkoa, eli virhettä jossain digitaalisessa palvelussa, sovelluksessa tai ympäristössä. Haavoittuvuuksia voidaan käyttää hyväksi vihamieliseen tarkoitukseen hakkerien toimesta.

Nollapäivähaavoittuvuus – Tämä haavoittuvuustyyppi tarkoittaa kriittistä tietoturva-aukkoa, jossain digitaalisessa palvelussa, sovelluksessa tai ympäristössä, jolle ei ole olemassa korjausta.

Laadullinen tutkimusmenetelmä – Kvalitatiivisella tutkimusmenetelmällä tarkoitetaan Tietoarkiston (s.a) mukaan menetelmää, jossa tutkimus koostuu monenlaisista lähestymistavoista, joilla pyritään vastaamaan asettamiin tutkimuskysymyksiin systemaattisesti. Koostuu yleensä aineiston tuottamisesta, aineiston analysoinnista, sekä johtopäätösten tekemisestä näiden pohjalta.

IT – (Information Technology) eli tietotekniikka tarkoittaa tietojenkäsittelyä digitaalisesti tietokoneiden ja tietoliikenteen avulla.

1.1.1 Haittaohjelmatyypit

Kiristyshaittaohjelma – Haittaohjelma, jolla pyritään tyypillisesti saamaan lunnaita käyttäjältä salaamalla tai manipuloimalla laitteen tietoja sekä estämällä tietokoneen käyttöä.

Virus – Haittaohjelma, joka käynnistyy käyttäjän toimesta ja leviää laitteesta ja tiedostoista toiseen.

Mato – Automaattisesti leviävä haittaohjelma, joka ei vaadi isäntäohjelmaa levitäkseen.

Troijalainen – Normaaliksi ohjelmaksi naamioitu haittaohjelma, joka käynnistää viruksen, haittaohjelman tai käyttää hyväksi kohteen haavoittuvuutta.

Takaovi/takaportti – Takaovi (haittaohjelma) kohdeympäristössä tai -tietokoneessa, jonka avulla hyökkääjä saa tietoverkon välityksellä hallinnan kohteeseen ohittamalla tietoturvamekanismit.

Vakoiluohjelma – Haittaohjelma, joka vakoilee käyttäjän toimia tietokoneella ja kerää ja lähettää ne automaattisesti kolmansille osapuolille. Kerää esimerkiksi tietoa web- selaamisesta. Tähän kategoriaan lukeutuu haitalliset mainosohjelmat, selainkaappaajat ja näppäimistönlukijat.
(IF 2017.)

2 Työntekijän tietoturvaan kohdistuvat uhat ja riskit

Ihmisillä saattaa olla usein käsitys, että heillä ei olisi tietoa, joka voisi kiinnostaa jotakin tahoa. Tämä on täysin harhakuva, joka voi kostautua pahasti yksityishenkilönä tai työntekijänä. Tietoverkkorikollisuus on globaali tietoturvaan kohdistuva uhka, jolla rikolliset ja rikollisorganisaatiot pyrkivät saamaan rahallista tai tiedollista hyötyä. Toiminta kohdistuu yleensä erilaisiin toimintoihin tai asioihin, jossa käsitellään rahaa ja rahanarvoisia tietoja, esimerkiksi henkilötietoja tai muita organisaatioille merkittäviä tietoja. Tietoverkkorikollisuuden lisäksi uhkia tietoturvalle aiheutuu kyberterrorismisista ja valtiollisesta tiedustelusta. Tietoturvallisuus on osa-alue, joka tulee nykyään ottaa huomioon kaikessa toiminnassa vapaa-ajalla ja työssä. Tietoturvallisuuteen liittyen perinteinen rikollisuus on muuttunut entistä enemmän tietoverkkorikollisuudeksi.
(Järvinen & Rousku 2017, luku 1.)

Työntekijöihin kohdistuvat tietoturvauhat ovat yleisiä ja ne ovat yrityksille vaarallisimmat, koska työntekijällä on jo pääsy yrityksen resursseihin. Kyseisen uhan vakavuutta ei vieläkään ymmärretä täysin, vaikka työntekijän kautta hyökkääjä saisi pääsyn suoraan yrityksen sisälle.
(Viskari 2017, 5-6.)

Tietoturvallisuuden säilyttämisen merkityksellisin tarkoitus on ylläpitää tietoaineistojen luottamuksellisuus, eheys ja saatavuus. Keskeisimmät tietoturvauhat pohjautuvat käyttäjän omaan toimintaan tai rikollisten ammattimaiseen suuniteltuun toimintaan. Näiden avulla rikollinen, rikollisryhmät tai valtiot pyrkii ottamaan haltuunsa henkilö- ja luottokorttitietoja, yrityssalaisuuksia tai valtiosalaisuuksia. Samat tahot voi vaihtoehtoisesti pyrkiä tahraamaan yritysten sekä ihmisten maineen, tai vaikuttamaan eri tahojen päätöksentekoon. (Valtiovarainministeriö 2010, 13.)

2.1 Tietoverkkorikollisuus ja tietoaineistoihin kohdistuvat uhat

Kun käytät Internetiä kotona tai työpaikalla ja sinulla on Internetiin yhteydessä olevia laitteita käytössä, niin olet mahdollinen tietoverkkorikollisuuden kohde. Rikolliset voivat esimerkiksi kaapata ja hyödyntää Internetiin yhdistettyjä laitteitasi tietokoneellesi ja organisaatiosi resursseihin pääsyyn tai muuhun rikolliseen toimintaan, kuten palvelunestohyökkäyksiin. (Järvinen & Rousku 2017, luku 1.)

Rikollisten hyödyntämät hyökkäykset voivat onnistuessaan mahdollistaa käyttäjän laitteen etähallinnan ja käyttämisen rikollisiin käyttötarkoituksiin osana suurempaa hyökkäystarkoitusta, kuten esimerkiksi roskapostipalvelinympäristönä, palveluihin salasanayhdistelmiä kokeilevana tai matemaattisesti murtavana resurssina, huijaus-verkkopalveluna tai kohdistettuja palvelunestohyökkäyksiä suorittavana verkkoalustana (Valtiovarainministeriö 2010, 13).

Aiemmin mainittu uhka voi aiheuttaa suurenkin riskin muiden työntekijöiden laitteille, koska yhden ”saastuneen” laitteen avulla voidaan suhteellisen yksinkertaisilla tavoilla saada yrityksen toisia laitteita hyökkääjien haltuun. Tästä voisi olla esimerkkinä niinkin yksinkertainen tapa kuin yrityksen viestintäkanavaan julkaisun tekeminen tai sähköpostin lähettäminen muulle henkilöstölle alkuperäisen uhrin tunnuksilla, jossa muille ehdotetaan ladattavaksi jotain uskottavaa liitetiedostoa, joka onkin oikeasti haittaohjelma. Vaihtoehtoisesti, kyseinen tiedosto voitaisiin piilottaa yrityksen dokumenttipankkiin tai muokata siellä olemassa olevia tiedostoja sisältämään haitallista ohjelmakoodia.

Tietoaineistoihin liittyvän uhkan aiheuttaa työntekijöiden sosiaalisen median käyttäminen, jos työntekijä julkaisee palveluihin salassa pidettäviä tietoja. Tämän osalta on myös otettava huomioon, että julkisen ja salassa pidettävän tiedon välillä voi joskus olla varsin pieni kynnys. Useampi julkista tietoa sisältävä julkaisu voikin kokonaisuutena muodostaa yhden tietokokonaisuuden, joka ei enää olisi julkinen tieto. Tämä uhka korostuu, jos kyseisten palveluiden käyttöön ei ole oikeanlaista politiikkaa määritelty yrityksessä. (Valtiovarainministeriö 2010, 29.)

Jos salassa pidettävää tietoa sisältäviä julkaisuja tai viestejä joutuu Internetiin, voi tieto levitä useampaan paikkaan ja jäädä sinne ikuisuudeksi. Palvelunpitäjä tai muu kolmas osapuoli ei välttämättä pysty poistamaan tietoja tarpeeksi ajoissa ennen kuin tiedot ovat jo vuotaneet muualle. Tietojen poistoyritykset voivat lisäksi vain ruokkia vuotaneen tiedon levittämistä. (Valtiovarainministeriö 2010, 14.)

Langattomat WIFI-verkot ovat luonteensa vuoksi lähtökohtaisesti turvattomia, koska ne mahdollistavat verkkoliikenteen kuuntelun. Liikenteestä voidaan pahimmassa tapauksessa varastaa käyttäjätunnuksia tai muuta arkaluonteista tietoa. Jos langatonta verkkoa ei ole salattu, niin käyttäjän istuntoa verkossa voidaan manipuloida ja liikennettä tarkastella selkokielellä. Bluetooth-ominaisuus voi myös aiheuttaa uhkia laitteille, jos toimintoa pidetään päällä jatkuvasti ja laitteita paritetaan usein bluetoothin avulla julkisilla paikoilla. (Doherty 2015, luku 6.)

2.1.1 Tietomurrot ja tietovuodot

Organisaatioille ja työntekijän tietoturvallisuudelle kriittisiä tietoverkkorikollisuuden uhkia ovat tietomurrot. Hyökkääjä tai rikollisorganisaatio pyrkii saamaan tietomurroista taloudellista hyötyä tai käytettäviä resursseja, esimerkiksi aiemmin mainittuihin palvelunestohyökkäyksiin. Rikollinen voi asettaa tietomurron kohteena olevaan ympäristöön kiristyshaittaohjelmia tai jakaa ympäristön avulla haitallista materiaalia. Tietomurroista saatuja tietoja voidaan lisäksi hyödyntää identiteettivarkauksissa.

Tietomurroista aiheutuu kohteena olevalle organisaatiolle mainehaittoja ja taloudellisia tappioita. Lisäksi tietomurroista palautuminen vaatii paljon aikaa ja korjauksia, joka vaikuttaa organisaation tavallisiin toimintoihin. (Kyberturvallisuuskeskus 2021c.). Tietomurron aiheuttamista negatiivista vaikutuksista hyvä esimerkki on Psykoterapiakeskus Vastaamon tapaus, joka tuli julkisuuteen vuonna 2020.

Kyseisessä murrossa kymmenien tuhansien Vastaamon asiakkaiden potilastiedot joutuivat vääriin käsiin tietomurron seurauksena, koska yrityksen potilastiedot olivat verkossa ilman tarvittavaa suojausta (ehkä jopa vuosia), joten rikolliset pääsivät käsiksi yrityksen tietokantaan. Tässäkin tietomurtotapauksessa kohteena olevalta yritykseltä ja uhreilta pyrittiin kiristämään rahaa. (Yle 2021.)

Työntekijä saattaa tietämättään sosiaalisessa mediassa aiheuttaa riskin organisaation muille työntekijöille tai koko yrityksen tietoturvallisuudelle. Sosiaalisen median käyttäjiin kohdistuvia uhkia ovat vakoilu ja tietojenkalastelu, joiden avulla voidaan pyrkiä saamaan pääsy yrityksen tietoihin. Sosiaalista mediaa voidaan käyttää alustana, josta kerätään tehokkaasti uhreihin liittyvää tietoa, jota voidaan myöhemmin hyödyntää organisaation vaarantamiseen. Sieltä voidaan etsiä tarvittavaa tietoa ja yhdistää sitä muihin jo saatuihin tietoihin. Useat sovellukset sisältävät haavoittuvuuksia, jotka voivat mahdollistaa käyttäjän laitteen etäkäytön haavoittuvuuden hyödyntäjän toimesta. Sosiaalisen median sovellukset eivät poikkea tästä. Kilpailu sosiaalisen median eri palveluntarjoajien välillä on lisännyt ja nopeuttanut niiden sovelluskehitystä, joka johtaa yleisesti siihen, että tietoturvallisuus ja sovellusten testaaminen kärsivät. Sovelluksiin liittyvät haavoittuvuudet ja unohtuneet päivitykset voivat aiheuttaa useita riskejä. Haavoittuvuuksista aiheutuu uhka tiedoille. (Valtiovarainministeriö 2010, 15-17.)

Mobiililaitteissa perinteinen arkkitehtuuri käyttöjärjestelmän osalta poikkeaa tietokoneiden arkkitehtuurista, joka tietokoneella mahdollistaa useille eri käyttäjille kirjautumisen. Mobiililaitteella sen sijaan olet yhdellä käyttäjällä, jossa kaikki tiedot ovat. Tämä tarkoittaa, että käyttämiesi sovellusten välillä ei ole samanlaista estettä. Mobiililaitteilla useat eri sovellukset kysyvät myös usein käyttöoikeuksia eri asioihin. Jos sovellus on haavoittunut tai vihamieliseen tarkoitukseen luotu, ja sille on myönnetty käyttöoikeudet tallennustilaan tai muualle, niin tämä voi aiheuttaa riskin koko laitteen tiedoille. (Dwivedi, Burns, Chung, Clark & Thiel, 2010, luku 1.)

2.1.2 Tietojenkalastelu ja verkkohuijaukset

Yleisiä työntekijöihin kohdistuvia tietoturvauhkia ovat tietojenkalastelu ja verkkohuijaukset, joihin työntekijät valitettavan usein lankeavat. Yksi syy tähän on perehdytyksen puute kyseisiin uhkiin ja niiden riskeihin liittyen. (Viskari 2017, 19.)

Yksi ajankohtaisista tietoturvauhista viime aikoina on ollut huijauspostit ja kiristyspostit, tarkemmin pornokiristykset. Tässä huijaustavassa hyökkääjä väittää viestissä saaneen käyttäjän kiinni aikuisviihteen katselusta haittaohjelman avulla. Kuten useissa huijauksissa, tässäkin huijauksessa yritetään aiheuttaa kiireen tuntu käyttäjälle arkaluonteisella teemalla ja kiristää rahaa. Viestit ovat olleet yleensä suomeksi ja viestien rakenne sekä kieliopin laatu on vaihdellut. Samantyyppisiä huijausyrityksiä ilmenee jatkuvasti eri teemoilla, mutta huijauksissa vaadittavia lunnaita ei tule missään nimessä maksaa. Joskus viestit vaikuttavat hyvinkin aidoilta ja niissä voidaan mainita oikeita haavoittuvuuksia tai tarkkaa tietoa kohteesta. (Kyberturvallisuuskeskus 2019a.)

Sosiaalinen media on tietojenkalastelulle oiva paikka, koska siellä henkilöihin lähestyminen ja tavoittaminen voi olla helpompaa kuin missään muualla. Näihin liittyen ollaan usein varomattomampia tuntemattomien kontaktipyyntöjen tai viestien osalta, eikä roskapostiviestien osalta kouluteta henkilöstöä tähän liittyen samalla tasolla kuin muihin palveluihin liittyen. Sosiaalisista medioista saaduista tiedoista voidaan lisäksi suorittaa tehokkaammin kohdistettuja tietojenkalasteluhyökkäyksiä eri kohderyhmiin. (Valtiovarainministeriö 2010, 15-16.) Kohdistetuissa kalasteluhyökkäyksissä kohderyhmän osalta voidaan olla kartoitettu muun muassa kohderyhmän kiinnostuksen kohteita tai kohteena olevan henkilön elämään liittyviä yksityiskohtia, joita voidaan käyttää hyväksi hyökkäyksen toteutuksessa, jotta uhri lankeaisi näihin suuremmalla todennäköisyydellä.

Tekstiviestien kautta toteutettavilla huijaus- ja kalasteluyrityksillä yritetään saada yhtä lailla käyttäjä klikkaamaan haitallisia linkkejä, jotta käyttäjä täyttäisi esimerkiksi tunnustietojaan johonkin palveluun liittyen. Puhelimien osalta uhkaa pahentaa se, että näyttökoko on pieni ja linkkien osalta pienten poikkeavuuksien tunnistaminen voi tästä syystä olla hankalaa. (Doherty 2015, luku 4.)

Tekstiviestien osalta kalasteluhyökkäyksiä on toteutettu esimerkiksi Postin saapumisilmoituksien sisältöä hyödyntämällä, joissa on mainittu, että postiin on tulossa paketti, joka vaatii vielä rahasumman suorittamisen tai palveluun kirjautumisen tietyn vääristetyn linkin kautta, ennen kuin paketti voidaan noutaa.

2.1.3 Haittaohjelmat

Tietokoneelle hyvin yleinen sekä vaarallinen uhka on haittaohjelmat. Riski haittaohjelmien kohteeksi joutumiselle kasvaa, jos tietokoneessa on paljon ylimääräisiä ohjelmia, ja jos ohjelmia tai selainlaajennuksia ei päivitetä ajallaan. Haittaohjelmat leviävät tyypillisesti selaimen tai sähköpostin kautta. Haittaohjelmia on monenlaisia, mutta näistä ehdottomasti ikävin ohjelmatyyppi on kiristyshaittaohjelma, jota levitetään usein esimerkiksi sähköpostitse hyödyntämällä oikeiden ohjelmien tiedostoliitteitä, kuten Microsoft Office -sovellusten tiedostoliitteitä.
(Järvinen & Rousku 2017, luku 3.)

Jos käytät tietokoneellasi vieraita USB-tikkuja, niin voit altistaa työkoneesi haittaohjelmille. Haittaohjelmien uhriksi saattaa joutua helposti myös eri verkkosivustojen kautta, kuten viihdeverkkosivujen kautta. Näistä aiheutuu riski myös työpaikan muihin järjestelmiin, koska haittaohjelmat voivat levitä laitteesta eteenpäin. (Kyberturvallisuuskeskus 2020b.)

Työntekijöiden käyttämät sosiaalisen median alustat aiheuttavat myös haittaohjelmien osalta työntekijään kohdistuvia uhkia. Hyökkääjät voivat tehokkaasti levittää haittaohjelmia kätkemällä esimerkiksi vihamielistä haittakoodia sisältäviä verkkosivuja uutispäivityksiin tai yksittäisiin keskusteluihin, esimerkiksi hyödyntämällä tuttuja verkko-osoitteita ja manipuloimalla oman haitallisen verkkosivun verkko-osoitettaan muistuttamaan näitä.
(Valtiovarainministeriö 2010, 17-18.)

Yleisimmät haittaohjelmatyypit olisi hyvä tuntea pääpiirteittäin, jotta mahdollisesti kohteeksi tai pahimmassa tapauksessa uhriksi joutuessaan voisi tunnistaa, että kyseessä on haittaohjelma. Yleisimpiä haittaohjelmia ja niiden toimintaa on listattu ja kuvattu tutkimuksen alussa johdannon jälkeen.

2.2 Fyysiset tietoturvauhat ja -riskit

Tietokonettasi koskevia fyysisiä tietoturvauhkia ovat esimerkiksi varkaudet, katoamiset, väärinkäyttö, sekä salakuuntelu tai -katselu fyysisten työkalujen avulla. Hyökkääjät voivat lisäksi hyödyntää erilaisia fyysisiä työkaluja tai muuttaa olemassa olevia fyysisiä oheislaitteita hyökkäystarkoituksiin. Näistä tyypillisimmät ovat USB-tikut, näppäimistökaapparit, fyysiset kaapparit, langattomat näppäimistöt ja web-kamerat. (Järvinen & Rousku 2017, luku 4.)

Tietokoneen ja oheislaitteiden turvallinen hallinta on tärkeää. Hyvä esimerkki, jossa hallintaa laiminlyödään, on poistuminen työskentelytilasta lukitsematta tietokonettasi. Tällä tavoin aiheutuu tarpeettomia riskejä, etenkin toimistolla tai julkisella paikalla työskennellessä.
(Järvinen & Rousku 2017, luku 6.)

Edellä mainittujen lisäksi tietokoneille ja muille laitteille uhkaa aiheuttava on sosiaalinen vaikuttaminen. Sosiaalista vaikuttamista voi tapahtua fyysisesti, verkon kautta tai muita reittejä. Fyysisessä vaikuttamisessa hyökkääjä voi esittäytyä toisena henkilönä hyvin uskottavasti ja yrittää päästä sisälle organisaatiosi tiloihin, josta hän voi päästä käsiksi laitteisiisi tai yrityksen laitteisiin. (Kyberturvallisuuskeskus 2020c.)

Etätöissä työskennellessä voi muodostua helposti uhka mahdollisten työpaikan salaisten tietojen osalta, jos perheenjäsen näkee tai pääsee käsittelemään hänelle kuulumatonta luottamuksellista tietoa. Jos perheenjäsen saa luottamuksellista tietoa, niin voi hän tahattomasti ja ajattelemattomuuttaan levittää tiedon eteenpäin. Sama koskee muualla työskenneltäessä. Mahdolliset ohikulkevat ihmiset voivat nähdä tietokoneen tai mobiililaitteen ruudun, kun käsittelet näytöllä luottamuksellista tietoa. Erilaisilla näyttökalvoilla voidaan vaikeuttaa tahallista tai tahatonta salakatselua. Samanlaisen uhan aiheuttaa salakuuntelu, jos puhut työasioista sellaisessa paikassa, jossa joku voi kuulla fyysisen keskustelun tai työpuhelun.
(Kyberturvallisuuskeskus 2020b.)

Mobiililaitteet voivat tulla varastetuksi tai hävitä, jolloin tietoturvalle suurimpana riskinä on niillä olevat tiedot. Yrityksen salassa pidettäviä tietoja voidaan saada mobiililaitteelta sähköpostisovelluksen avulla, jos laite päätyy taholle, jolla on motiivi hyödyntää tietoja. Mobiililaitteiden tietoihin voidaan myös päästä käsiksi, jos laitetta lainaa jollekin ulkopuoliselle vain puhelun soittamista varten. Tässä tilanteessa laitetta lainaava taho voi pahimmassa tapauksessa asettaa haittaohjelman laitteelle ja siten saada pääsyn laitteeseen ja sen tietoihin. (Dwivedi ym. 2010, luku 1.)

Mobiililaitteiden katoamisen tai varastamisen riskit ulottuvat myös laitteen ulkopuolelle laitteen omistajan käyttämiin verkkopalveluihin. Jos käyttäjä on tallentanut salasanojaan selaimeen tai muihin käyttämiin sovelluksiin, niin verkkopalveluiden kautta päästään käsittelemään laajempaa tietokokonaisuutta ja toimintoja. Kun kyse on organisaation laitteesta, voidaan laitteen avulla yrittää päästä käsiksi myös organisaation muihin laitteisiin ja palveluihin. (Suomidigi 2013, 24.)

2.3 Huolimattomuudesta aiheutuvat tietoturvauhat ja -riskit

Jos käsittelet tietoaineistoja tietokoneellasi ja etenkin salassa pidettäviä tietoja, esimerkiksi tietynlaiset henkilötiedot, niin tietojen suojaamisen ja luokittelun tärkeys korostuu entisestään, koska kyseiset tiedot kuuluvat rikollisten halutuimpien tietojen joukkoon. (Järvinen & Rousku 2017, luku 6.). Tämän lisäksi tietosuojalaissa on määritelty GDPR:n mukaiset vaatimukset kyseisten tietojen käsittelystä, keräämisestä ja säilytyksestä, joita tulee noudattaa.

Tärkeää on myös kiinnittää huomiota julkisilla paikoilla keskusteluun tai laitteiden käyttöön, ja varmistaa ettei keskustella salassa pidettävistä tiedoista tai käytetä laitteita niin että joku voi nähdä mitä niillä tehdään (Järvinen & Rousku 2017, luku 6).

Tähän samaan kategoriaan sijoittuu sosiaalisessa mediassa jaettavat tiedot ja julkaisut. Hyökkääjien ensiaskelia hyökkäyksissä on tiedustelu, ja sosiaalisista medioista tietoa irtoaa tyypillisesti paljon. Varmista yksityisyysasetuksesi käyttämistäsi sosiaalisista medioista ja kiinnitä erityistä huomiota, että mitä tietoa jaat itsestäsi tai työpaikkaasi liittyen. (Järvinen & Rousku 2017, luku 5.)

Huolimattomuus salasanojen osalta on riski käyttäjätileillesi ja tietokoneellesi. Heikkoja ja samoja salasanoja käyttämällä useissa palveluissa, voi hyökkääjä saada käyttäjätiliesi oikeudet käyttöön ja niille pääsyn. (Kyberturvallisuuskeskus 2020c.)

Koska hakkerit pyrkivät yleisesti tehokkaimpaan ratkaisuun hyökkäystapauksissa, niin tarkoittaa tämä salasanojen osalta sitä, että hakkeri voi pyrkiä valitsemaan hyökkäyksissään sellaisia käyttäjiä, joilla on useissa palveluissa sama salasana. Tämä helpottaa ja nopeuttaa huomattavasti hakkerin toimintaa. Hakkeri voi lisäksi käyttää tietovuodoissa vuotaneita käyttäjätietolistoja hyväkseen ja kokeilla niistä saatuja tunnuksia eri palveluihin, jolloin samaa salasanaa käyttävät ovat pulassa. (Speed, Nykamp, Anderson & Nampalli 2013, 129.)

Useilla hyökkääjillä on käytössään erilaisia ohjelmia salasanojen murtamiseen, joiden avulla helpoimmat salasanat murtuvat jopa sekunneissa. Hyökkääjät voivat käyttää joko sanalistoja apunaan tunnuksien murtamisessa tai yrittää murtaa niitä suoraan laskentateholla.
On siis erittäin tärkeää käyttää vahvoja salasanoja, sekä muuttaa niitä säännöllisesti.

Sosiaalinen vaikuttaminen aiheuttaa internetpalveluissa uhkaa, jos verkon käyttö ei ole huolellista. Hyökkääjät tekevät sivustoja oikeiden verkkosivujen pohjalta huijatakseen käyttäjää luulemaan, että hän olisi oikealla sivulla. Yleensä tämän paljastaa sivun verkko-osoite, jossa on siihen kuulumattomia sanoja tai merkkejä. Esimerkki huijaussivusto Ylen sivuista voisi olla muodossa www.yyle.fi, www.2.yle.fi tai muuta vastaavaa. (Kyberturvallisuuskeskus 2020c.)

3 Keinot tietoturvauhkilta suojautumiseen ja riskien hallintaan

Tietoverkkorikollisuuden uhkia vastaan ei ole mahdollista suojautua 100 prosenttisesti, paitsi sulkemalla tietokoneet kokonaan käytöstä. Tietoturvauhkia vastaan tulee kuitenkin pyrkiä suojautumaan parhaalla mahdollisella tavalla ja yksi oleellinen niistä on ymmärtää, että mitä hakkerit yleisesti ajattelevat tai toimillaan pyrkivät saavuttamaan.
(Esteves, Haro & Ramalho 2017, luku 2.)

Huijauksia on ollut aikojen alusta lähtien niin kauan kuin ihmisiäkin on ollut. Ei ole noloa joutua huijauksen kohteeksi ja sen mahdollisuuden pelosta ei tarvitse lopettaa tietokoneiden ja Internetin käyttöä, päinvastoin. Kuten monessa muussakin asiassa, harjoitus tekee mestarin.
Käytä monipuolisesti tietokonetta ja kerää varmuutta ja kokemusta sen käytöstä. Käytännön tapauksiin vertaaminen ja käytännön kautta oppiminen auttaa tietoturvallisuuden uhkien hahmotusta. Käytä maalaisjärkeä verkossa ja ole tarkka. Ethän jätä kotioveakaan rakoselleen lähtiessäsi töihin, koska jossain vaiheessa joku varmasti käyttää tilaisuuden hyödyksi. Sama pätee tietoturvallisuuteen. (Kyberturvallisuuskeskus 2021b.)

Jos tietoturvaa laiminlyödään niin voi menetettävänä olla sinun tai työpaikkasi maine, arkaluonteiset tiedot, raha tai identiteetti. Tämän lisäksi näiden pohjalta palautuminen on vaikeaa ja niistä voi jäädä pysyviä merkkejä. (Kyberturvallisuuskeskus 2020c.)

Tietoturvallisuuden tavoitteet eli luotettavuuden, eheyden ja saatavuuden varmistaminen perustuu juurikin keinoihin, joilla näitä ylläpidetään. Tiedon luottamuksellisuudella tarkoitetaan, että tiedot pysyvät näkymättöminä ulkopuolisille ja käytettävänä niille tarkoitetulla omistajalla, sekä määritetyillä tiedon käyttäjillä. Näistä tiedoista esimerkkejä ovat sähköpostiviestit, yrityssalaisuudet, työverkkoliikenne, sekä palkanmaksuun liittyvät tiedot. Eheydellä tarkoitetaan tietojen oikeellisuutta, sekä oikein määriteltyjä käyttöoikeuksia tietojen muuttamiseen.
Huoltomies ei saa päästä asiakkaan taloustietoihin käsiksi, eikä työntekijöiden pidä päästä muuttamaan omia palkkojaan HR-järjestelmiin. Tätä on eheys. Saatavuudella sen sijaan tarkoitetaan, että esimerkiksi tietojärjestelmien, verkkoyhteyksien, sekä laitteiden pitää toimia, jotta käyttäjät pääsevät tietoihin käsiksi. Tavoitteena siis ylläpitää vikasietoista tietoympäristöä, jotta tiedot ovat saatavilla. (Järvinen 2022, 13-14.)

3.1 Käyttäjätilien suojaus

Työpaikalla ja kotona käyttäjätileillesi parhaan suojan saat käyttämällä vahvoja salasanoja eli tarpeeksi pitkiä ja monimutkaisia. Jokaiseen käyttäjätiliin tulee lisäksi olla eri salasana, jotta monta tiliä ei ole saman salasanan varassa. Monien vahvojen eri salasanojen muistaminen voi olla haastavaa, joten eri tilien salasanoja varten on hyvä käyttöönottaa salasanojen hallintaohjelma. (Kyberturvallisuuskeskus 2020c.)

Vahvoilla salasanoilla tarkoitetaan sellaisia salasanoja, jotka ovat vähintään 8-merkkiä pitkiä, jo käytetyistä salasanoista poikkeavia, sekä isoja ja pieniä kirjaimia, numeroita, sekä näppäimistöltä löytyviä erikoismerkkejä (+-=![ ] { }/ \;”#%&( )?:_> < ^ | ’ ´ . @ $) sisältäviä. Salasana lasketaan heikoksi myös, jos se sisältää oman nimesi, käyttäjänimesi tai yrityksen nimen, tai jos se sisältää yksinkertaisia perusmuotoisa sanoja (esim. pöytä). Vahvan salasanan voi muodostaa vaikka itse keksimästä lauseesta, kuten ”koirani on jo kahdeksan vuotta”, voisi olla muotoa ”koir@n10NJOkahdek5ANvuoTT4!”.

Salasanojen säännöllinen päivittäminen on tärkeää, vaikka käyttäisitkin jo vahvoja salasanoja. Joskus käyttämiisi palveluihin voi kohdistua hyökkäyksiä, jolloin salasanoja saattaa vuotaa Internetiin. Salasanojen päivittämisellä minimoidaan tästä aiheutuva riski. Älä myöskään käytä suoraan salasanassasi sellaista tietoa, joka on helppo saada selville. Tästä esimerkkinä lapsen tai muun läheisen nimi tai syntymäaika. (Speed, ym. 2013, 131-133.)

On täysin ymmärrettävää, että monimutkaisten salasanojen muistaminen ja kirjoittaminen voi olla haastavaa tai työlästä. Palveluihin kirjautumisen helpon käytettävyyden kannalta on siis kannattavaa ottaa aiemmin mainittu salasananhallintaohjelma käyttöön, jos siihen on mahdollisuus, jotta tileille kirjautuminen helpottuisi.

Salasanojen hallintaohjelmia on paljon maksullisista ilmaisiin, joten valitse itsellesi niistä sopivin ja noudata ohjelman ohjeita tarkkaan ja kiinnitä erityistä huomiota ohjelman salasanan vahvuuteen, koska sen taakse tulevat muut salasanasi. Hyviä esimerkkejä salasanojen hallintasovelluksista on Bitwarden, Enpass ja F-Secure ID PROTECTION. (Kyberturvallisuuskeskus 2020d.)

Pyri käyttämään kaikissa käyttäjätileissäsi kaksi- tai monivaiheista tunnistautumista, jos vain mahdollista, koska tämä lisää huomattavasti käyttäjätilien tietoturvaa ja vaikeuttaa tilin väärinkäyttöä, jos hyökkääjä pääsisi salasanan läpi. (Kyberturvallisuuskeskus 2020c.)

3.2 Laitteiden sovellus- ja ohjelmistopäivitykset

Varmista, että tietokoneesi ja käyttämäsi ohjelmat tai järjestelmät ovat ajan tasalla päivitysten osalta. Suurin osa näistä päivittyy automaattisesti, mutta työpaikan IT-tuki saattaa vastata esimerkiksi tietokoneen ja kriittisten järjestelmien päivityksestä. Älä viivyttele päivitysten asennuksen suhteen, vaan suorita ne aina heti. Pyri pitämään työtietokoneella vain välttämättömiä sovelluksia, jotka liittyy työhösi. (Kyberturvallisuuskeskus 2020b.)

Vaikka päivitykset joskus ärsyttävätkin ja ne keskeyttävät laitteiden käyttöä, niin tulee ne tehdä ajoissa, koska joskus sovelluksissa saattaa olla todella kriittisiä tietoturva-aukkoja tai nollapäivähaavoittuvuuksia, joita hyökkääjät voivat pahimmillaan hyödyntää tuntien sisällä haavoittuvuuksien löytymisestä. Kriittisimpiä sovelluksia päivitysten tärkeyden osalta ovat muun muassa kaikki selaimet (esimerkiksi Google Chrome), verkkolaitteet (esimerkiksi reitittimet), sekä käyttöjärjestelmät, kuten Windows. Reitittimien laiteohjelmistoja päivittäessä tulee ottaa huomioon, että laitteen päivitystä ei saa keskeyttää, koska muuten verkkolaitteesta voi tulla käyttökelvoton. Ota laitteissasi automaattiset päivitykset käyttöön, jos mahdollista. Varmista, että laitteellasi on tallennustilaa päivityksille ja että sovellukset varmasti päivittyvät. Kiinnitä huomiota käyttämiisi sovelluksiin ja poista turhat sovellukset laitteesta, koska tämä vähentää päivitysten määrää ja parantaa myös tietoturvaa siinä sivussa. (Järvinen 2022, 36-40.)

3.3 Tiedonhallinta ja epäkohtien tunnistaminen

Varmista myös, että tietokoneellesi tallennetut, sinulle tai työpaikallesi arvokkaat tiedot ovat varmuuskopioituna säännöllisesti, jotta kyseiset tiedot ovat pahimman tapauksen varalta tallessa. (Kyberturvallisuuskeskus 2020b.)

Varmuuskopioita voit tallentaa ulkoiselle kovalevylle, USB-tikulle, pilvipalveluihin tai yrityksesi dokumenttipankkiin, jos sellainen löytyy. Pilvipalveluissa tulee varmistaa käytettävän palvelun tietoturvallisuus. Fyysisissä tallennustiloissa huonona puolena on luottamuksellisuudelle aiheutuva riski, jos niitä ei säilytetä oikein. Kiinnitä huomiota tietokoneesi käyttäjällä tai järjestelmien käyttäjänä sinun käytössä oleviin käyttöoikeuksiin. Jos huomaat, että pystyt tekemään tai näkemään asioita, joita sinun ei tarvitsisi, niin ilmoita tästä eteenpäin IT-osastolle, jotta käyttöoikeudet saadaan tarkastettua. Tämä parantaa sinun ja organisaatiosi tietoturvaa, sekä yleensä käytettävyyttä. Tämä ei kuitenkaan poissulje tietoturvariskejä. Peruskäyttäjänäkin voit joutua yhtä lailla haittaohjelmien tai muiden hyökkäysten uhriksi. (Järvinen 2022, 41-43.)

Pidä mielessä, että erilaisille tiedoille on omat turvaluokituksensa, joiden osalta tulee noudattaa luokittelun mukaista tallennus- tai käsittelytapaa. Tiedostoja ei voi tallentaa minne sattuu, vaan täytyy aina varmistaa, että voiko tietyn tiedoston tallentaa ajateltuun paikkaan. Turvaluokittelun tasoja ovat henkilökohtainen, julkinen, sisäinen, luottamuksellinen, ja salainen. Henkilökohtaiseen kuuluu nimensä mukaisesti työntekijän henkilökohtaiset tiedostot eli työhakemukset, todistukset tai muut vastaavat. Julkiseen tasoon kuuluu yrityksen julkiset uutiset, verkkosivuilla olevat hinnastot tai yhteystiedot. Sisäisellä tasolla on yrityksen sisäisiä tietoja, esimerkiksi hankkeisiin liittyviä tietoja tai sisäiseen jakoon jaettuja tiedotteita. Luottamuksellinen taso käsittää tiedot, jotka ovat salattavia ulkopuolisilta ja vain tiettyjen ihmisten nähtäväksi tarkoitettuja. Näistä esimerkkinä henkilötiedot, luottamukselliset raportit, palkkatiedot tai työntekijöihin liittyvät yksityiset HR-tiedot. Salainen taso on kaikista rajotetuin taso ja soveltuu asioihin, jonka suhteen laki määrää tarkat säännöt. Salaiselle tasolle asettuu esimerkiksi Puolustusvoimien tietyt tiedot, jotka ei ole kuin tietyille ihmisille nähtäväksi. (Järvinen 2022, 163-166.)

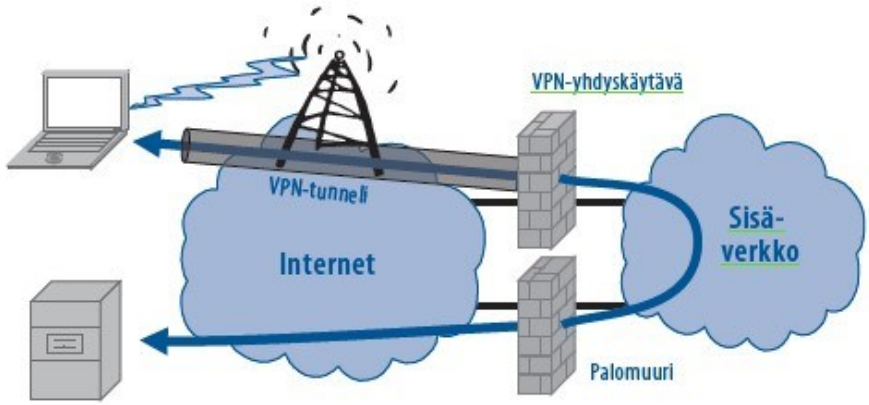
Arvioi jatkuvasti omaa tietoturvallisuutesi vahvuutta ja osaamistasoa. Mikäli havaitset epäkohtia osaamisessa, vaadi työpaikaltasi koulutusta ja kysy tarvittaessa apua. Huomioi myös työtehtäviesi luonne, esimerkiksi jos käsittelet työssäsi GDPR:n alaisia henkilötietoja, mutta et ole saanut niihin liittyen tietosuojakoulutusta toimintatavoista ja käytännöistä niin vaadi rohkeasti tähän muutosta työnantajaltasi. Pyri ilmoittamaan aina mahdollisista epäkohdista tai huomioista työnantajalle tai tietoturvasta vastaavalle taholle, koska huomiosi voivat olla hyvin arvokkaita ja tarvittavia, sekä joskus eliminoida yrityksen toiminnalle vaarallisen riskin.

3.4 Etätöiden tietoturvallisuus

Kiinnitä etätyöskennellessäsi huomioita, että asuntosi ovet ja ikkunat ovat kiinni, jos asuntosi jää valvomatta. Murtovarkauksia tapahtuu, eikä yrityksen laitteita tai mahdollisia luottamuksellisia asioita sisältäviä dokumentteja haluta missään nimessä menettää heille. Käytä myös kotona omiin asioihin eri konetta kuin työasioihin. Menee myös toiseen suuntaan, eli älä tee työasioita omilla laitteilla. Pidä myös työtietokone suljettuna, kun et käytä sitä ja mielellään poissa samasta verkosta, kun muut laitteesi. Jos työskentelet julkisilla paikoilla, niin älä koskaan jätä laitteitasi vartioimatta. Pyri lisäksi käyttämään kodin ulkopuolella julkisen langattoman verkon sijaan omaa verkkoa, esimerkiksi puhelimen jakamaa verkkoa. (Järvinen 2022, 186-192.)

Varmista, että tietokoneesi virustorjuntaohjelma on toimintakunnossa. Se suojaa viruksia, vakoiluohjelmia, kiristysohjelmia, sekä osaltaan tietojenkalastelua vastaan. Pidä huolta, että web-kamerasi on piilotettu tai USB-kameroiden osalta irrotettu tietokoneesta, kun et käytä sitä. Hakkerit voivat kaapata web-kamerasi ilman mitään ilmoituksia, jos he saavat tietokoneelle yhteyden. (Kaspersky s.a.)

Käytä aina salattua yhteyttä eli VPN-yhteyttä, kun siihen on mahdollisuus. VPN parantaa huomattavasti tietoliikenteesi tietoturvallisuutta salaamalla sen. Tämän tärkeys korostuu etenkin etätyöskentelyssä. VPN-yhdistää tietokoneesi yrityksen sisäverkkoon.



Kuva 1. VPN-tunneli (Suomidigi 2013).

Kuvassa 1 havainnollistetaan VPN-yhteyden muodostamista. Sisäverkolla tarkoitetaan työpaikan suojattua sisäverkkoa ja sisäverkon reunalla internetin välissä toimii palomuuri, kuten myös tietokoneessa ja verkkolaitteissa tulee olla.

Etätöihin liittyen tulee huomioida enemmän oman verkon tietoturvallisuutta. Pidä huolta, että kotireitittimesi ja siihen liitettyjen pääte- tai älylaitteiden päivitykset ovat ajantasalla ja että reititin on turvallinen salasanojen osalta. Nämä voivat vaikuttaa merkittävästi tietokoneesi tietoturvaan.

Varmista, että reitittimessä on vahva salasana, eikä esimerkiksi oletussalasana. Reitittimen tietoja pääsee yleensä päivittämään selaimessa osoitteesta (192.168.1.1.). Sivu kysyy reitittimen salasanaa kirjautuessa. Reitittimen kotisivulta voi myös vaihtaa reitittimen nimen eli SSID:n pois reitittimen oletusnimestä. Tämä on kannattavaa, jotta verkkolaitteesi merkki tai malli ei paljastu mahdolliselle väärinkäyttäjälle tai ulkopuolisille. Langattoman verkon salausasetukset kannattaa myös varmistaa, että käytössäsi on turvallisin salausvaihtoehto. Vahvin salaus on WPA3, mutta perusreittimet tukee todennäköisemmin vain WPA2-salausta (AES). Reitittimen laiteohjelmiston päivityksiä kutsutaan firmware-päivityksiksi. Kyseiset päivitykset kannattaa tarkastaa aiemmin mainitusta verkko-osoitteesta. Verkkolaitteiden käyttöohjeissa kerrotaan aina tarkemmin verkkolaitteen hallinnasta. (Kaspersky s.a.)

Noudata tietoturvallisuuden ja etätöiden osalta työpaikkasi ohjeistuksia (Kyberturvallisuuskeskus 2020b.).

3.5 Keinot fyysisiltä tietoturvauhilta suojautumiseen

Varkauksien, väärinkäytön ja salakatselun ja -kuuntelun osalta tulee olla tarkkana ja huolehtia omasta tietokoneesta, oheislaitteista ja työskentely-ympäristöstä huolellisesti. Jos huomaat poikkeavuuksia tai epäilet jotain asiaa, kysy matalalla kynnyksellä vastaavalta taholta asiasta. (Järvinen & Rousku 2017, luku 4.)

Työpaikkasi toimitiloissa työskennelläsi kiinnitä huomiota ympärillä tapahtuviin asioihin ja puutu mahdollisiin poikkeavuuksiin. Jos näet työpaikan tiloissa tuntemattoman henkilön tai muun henkilön, jolla kuuluisi olla kuvallinen henkilökortti niin varmista hänen käyntinsä tarkoitus henkilökorttia pyytämällä. Mikäli henkilöllä ei ole tiloihin vaadittuja vaatimuksia niin ilmoita asiasta vastaavalle taholle viipymättä. Tämä ei pelkästään koske tietoturvallisuutta vaan tämä on myös riski henkilöstöturvallisuudelle. (Järvinen & Rousku 2017, luku 2.)

Tietokoneen lukitseminen työpisteeltä poistuessa pitäisi olla täysin rutiininomaista ja itsestäänselvyys kaikille. Näin ei kuitenkaan valitettavasti ole, koska koneita jää lukitsematta, kun työntekijät lähtevät esimerkiksi kahvitauolle tai hakemaan tulostimelta jotain. Lukitse siis aina työpisteeltä poistuessasi koneesi manuaalisesti. Lukitseminen on helppoa ja nopeinta näppäinyhdistelmällä Windows-näppäin+L-kirjain, mutta se onnistuu myös painamalla Ctrl+Alt+Del, ja painamalla valikosta ”lukitse”. (Järvinen 2022, 183-184.)

Laitteiden mahdollisien varkauksien tai katomisten ehkäisyksi tulee olla erittäin huolellinen laitteiden kanssa. Kyseisien tapauksien varalle on kuitenkin olemassa myös teknisiä ominaisuuksia, joita hyödyntää näissä tilanteissa. Laitteesta kannattaa ottaa etsi laitteeni -toiminnallisuus käyttöön, jotta laitteen sijainnin voisi selvittää. Windows-tietokoneissa paikannuksen käyttöönotto vaatii, että sijaintitietojen käyttö on sallittu. Paikannustoiminnallisuus löytyy, kun siirtyy tietokoneella Asetukset > Päivittäminen ja suojaus > Etsi laitteeni. Tämän voi ottaa käyttöön vain järjestelmänvalvojan käyttöoikeuksilla. Kun toiminnallisuus on käytössä, niin laite voidaan paikantaa Microsoft-tilille kirjautumalla. (Järvinen 2022, 91-92.) Sama toiminnallisuus löytyy Android- ja iOS-laitteista, ja se kannattaa ottaa käyttöön. Paikannuspalvelun saa käyttöön asetuksista. Tähän liittyen saa varmasti tarvittaessa apua IT-osastolta.

Kiinnitä fyysisien dokumenttien hallintaan huomiota. Älä jätä tulostamiasi dokumentteja lojumaan tulostimelle, vaan lähde noutamaan niitä heti tulostumisprosessin aikana. Älä myöskään jätä niitä tai muistitikkuja lojumaan työpisteellesi tai muualle lukitsemattomaan paikkaan, vaan säilytä niitä lukitussa tilassa tai mukanasi. (Järvinen 2022, 51.)

3.6 Keinot huolimattomuuden aiheuttamien uhkien hallintaan

Verkossa selatessa tai sähköpostia luettaessa tulee aina olla huolellinen. Klikkaile harkiten verkkosivuilla, sosiaalisessa mediassa ja sähköpostissa sekä muissa viestintäpalveluissa. Epäilyttävissä tilanteissa varmista asia ja aitous. Usein asiat, jotka vaikuttavat liian hyvältä ollakseen totta, ovat huijausta. (Kyberturvallisuuskeskus 2020b.) Vaikka salasanoista ollaan mainittu aikaisemmin, niin tätä asiaa ei voida painottaa tarpeeksi. Pidä huoli, että salasanasi ovat laadukkaita ja monimutkaisia, jotka sisältävät erikoismerkkejä, numeroita ja isoja kirjaimia. Varmista myös jos säilöt salasanoja, että ne ovat turvallisesti tallessa.

Huolimattomuuden aiheuttamilta uhilta suojautumiseen tehokkain tapa on olla skarppina. Muista tauottaa työtäsi tarpeeksi ja antaa aivojen levätä välillä. Töissä on usein kiire, mutta pyri silti miettimään aina tarkkaan ennen kuin klikkaat epävarmoja asioita. (Kyberturvallisuuskeskus 2020d.)

Älä koskaan anna salasanojasi kenellekään. Edes IT-tuki ei tarvitse salasanaasi tukitehtävien suorittamista varten. Muista lisäksi aina työpäivän jälkeen sulkea tietokoneesi ja tallentaa keskeneräiset työt. Tallennusta kannattaa oppia tekemään säännöllisesti, jotta et joutuisi pahimmassa tapauksessa tekemään samoja asioita uudelleen. Päivitykset voivat joskus alkaa asentumaan automaattisesti ja pakottaa tietokoneen sammutuksen, jos tietokone jää yöksi päälle. Esimerkiksi Microsoft Office-työkaluissa saat tallennettua työsi nopeiten painamalla näppäinyhdistelmää Ctrl+S-kirjain. Vaihtoehtoisesti voit myös ottaa sovelluksista automaattisen tallennuksen käyttöön. (Järvinen 2022, 51-52.)

Kiinnitä huomiota, että mitä ohjelmia lataat internetistä tai sovelluskaupoista. Vaikka mobiililaitteiden sovelluskaupat olisivat Applen tai Androidin (Googlen) omassa hallinnassa, niin tämä ei tarkoita etteikö siellä olisi myös vihamielisiä tai haitallisia sovelluksia. Varmista, että ladattava sovellus on oikea ja turvallinen, ennen kuin lataat sen. Tämän osalta kannattaa lisäksi varmistaa, että mobiililaitteessa on virustorjuntaohjelma käytössä. (Speed, ym. 2013, 135-136.) Sosiaalista mediaa käytettäessä tulee kiinnittää erityistä huomiota julkaisemiseen ja palvelun yksityisyysasetuksiin, sekä valita tarkoin kenet hyväksyy verkostoon. Huolimattomat arkaluonteista tietoa sisältävät julkaisut aiheuttavat ikäviä seurauksia. Käytettävän profiilin osalta tulee tarkastaa, että mitä tietoa jakaa itsestään ja kenelle ne näkyvät. Yksityisyysasetukset ja omat tiedot kannattaa tarkastaa jokaisesta sosiaalisen median palvelusta. Yksityisyysasetuksista kannattaa katsoa, että julkaisut, kaverilista, sekä omat tiedot näkyvät vain kavereille. Linkedin voi hyödyllisyyden lisäksi pahimmillaan aiheuttaa uhkia ja helpottaa hyökkääjän tiedusteluprosessia. Sieltä voidaan nähdä organisaation työntekijät, kuvat ja työtehtävien jakautuminen. Näitä hyökkääjä voi hyödyntää kohdistettujen hyökkäysten suunnitteluun. (Järvinen 2022, 138-142.)

4 Tutkimuksen toteutus

Toteutettu tutkimus on laadullinen eli kvalitatiivinen tutkimus. Tutkimuksessa on kerätty kyselyaineistoa ennalta suunnitellulta kohderyhmältä ja kyselyn tuloksia on hyödynnetty teorian testaukseen systemaattisesti. Tuotettua teoriaa on kerätty eri ohjeita, kirjallisuutta ja alan ammattilaisten sisältöä analysoimalla. Materiaalin analysoimiseen ja pääkohtien tunnistamiseen hyödynsin tietoturva-osaamistani ja kokemustani materiaalin tukena. Tietoa ajankohtaisimmista uhista kerättiin analysoimalla materiaalia eri lähteistä, kuten Kyberturvallisuuskeskuksen sivuilta ja alan kirjallisuudesta. Valtion toimijana Kyberturvallisuuskeskus valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta jatkuvasti, joten tutkimuksessa on pyritty käyttämään laajasti heidän tuottamaa materiaalia, koska se on erittäin laadukasta ja ajankohtaista. Kyberturvallisuuskeskus seuraa jatkuvasti kansainvälisiä kyberturvallisuuteen ja tietoturvallisuuteen kohdistuvia uhkia yksityishenkilöihin, sekä yrityksiin liittyen. Valitut menetelmät olivat mielestäni sopivia käsiteltävään aiheeseen, koska menetelmillä saatiin monipuolista ja laadukasta tietoa tutkimukseen ja tiedonkeruu ja analysointi saatiin toteutettua tehokkaasti.

4.1 Tutkimuksen vaiheet

Ensimmäisessä tutkimusvaiheessa tutkimusmenetelmä ja tutkimustyyppi valittiin aihealueeseen ja toimeksiantajalle sopivaksi. Näiden toimenpiteiden jälkeen aineistoa työntekijän laitteisiin kohdistuvista ja liittyvistä tietoturvauhista kerättiin ja analysoitiin monipuolisesti ajankohtaisuutta ja aiheen rajausta silmällä pitäen. Toisessa vaiheessa sisällön keräys ja analysointi kohdistui keinoihin ja asioihin, joilla uhkia ja mahdollisia riskejä voitaisiin minimoida, tai joiden avulla niiltä voidaan suojautua parhaiten. Myös kysely toimeksiantajayrityksen henkilöstölle luotiin tässä vaiheessa ja se valmisteltiin tarkoitukseen sopivaksi toimeksiantajan edustajan palautteen pohjalta. Henkilöstölle toteutetulla tietoturvakyselyllä tutkittiin vastaajien tietoturvaosaamista ja tietoturvakokemuksia. Kyselystä kerrotaan lisää seuraavissa luvuissa. Teoriasisällön kokoamiseen hyödynnettiin ajatuskartan käyttöä ja keskeisten asioiden painoarvon ja kategorian jaottelua paperille. Tutkimusaiheen osa-alueet siis kategorisoitiin pienempiin osiin, jotta lähteiden kartoitus ja hyödyntäminen oli selkempää.

Seuraavassa vaiheessa tutkimuskyselyn kysymysten tarkoitusta avattiin ja yhteys tietoperustaan selitettiin. Kyselyn tuloksia oli tavoite esittää graafisesti, sekä selitettynä tekstimuodossa. Niistä oli tarkoitus muodostaa teoriaa ja tutkimusongelmia tukeva analyysi.

4.2 Tutkimuskysely työntekijöille tietoturvallisuuden hallinnasta

Toimeksiantajayrityksen henkilöstölle luotiin vapaaehtoinen kysely tietoturvan hallinnasta (ks. liite 3), joka julkaistiin Yammer-viestintäpalvelussa yrityksen yleisellä kanavalla 1.4.2022, josta koko henkilöstö näkee julkaisun ja saa siitä ilmoituksen. Julkaisussa (ks. liite 1) kerrottiin mihin tarkoitukseen kyselyn tuloksia käytetään, kauan kyselyyn vastaaminen kestää arviolta, ja että kysely on täysin anonyymi. Julkaisussa mainittiin myös, että kyselyyn tulisi vastata huhtikuun loppuun mennessä. Huhtikuun puolessa välissä kyselyyn oltiin vastattu jo 50 kertaa. Kyselyyn liittyen lähetettiin vielä 14.4.2022 muistutus sähköpostitse koko henkilöstölle (ks. liite 2), jossa kerrottiin mihin tarkoitukseen kyselyn vastauksia hyödynnetään, sekä painotettiin sen tärkeyttä ja vastausten anonymiteettia.

Muistutus sähköpostitse oli selkeästi tarpeellinen ja tehokas tapa, koska kyselyyn tuli 20 prosenttia lisää vastauksia hyvin lyhyessä ajassa muistutuksen jälkeen. Henkilöstöä muistutettiin vielä 20.4.2022 hieman eri tavalla kommentoimalla alkuperäistä julkaisua kyselystä (ks. liite 1), kertomalla tilannetietoa kyselyyn vastanneiden määrästä ja nostaakseen julkaisun Yammerissa ensimmäiseksi käyttäjille. Tällöin kyselyyn oli vastannut 60 henkilöä. Toukokuun lähestyessä kyselyyn vastaaminen hiipui selvästi, mutta tästä huolimatta huhtikuun loppuun mennessä kyselyyn oli sulkemishetkellä vastattu 65 kertaa, joka oli positiivinen tulos.

Kysely tavoitti Yammerissa 106 käyttäjää, ja voidaan olettaa sähköpostiviestinnän tavoittaneen vielä enemmän. Kyselyyn johtavaa linkkiä jaettiin pelkästään toimeksiantajayrityksen sisällä ja sitä markkinoitiin nimenomaan kyseisen yrityksen työntekijöille täytettäväksi, jotta kyselyyn johtava linkki pysyisi yrityksen sisällä. Tietoturvakyselyyn vastasi 65 henkilöä eli noin 55 prosenttia toimeksiantajayrityksen henkilöstöstä, joten kyselyn toteutusta voidaan pitää hyvin onnistuneena.

4.3 Kyselylomake ja kysymykset

Tutkimuksessa päädyttiin toteuttamaan kysely tutkittavaan aiheeseen liittyen, koska sillä voidaan konkreettisesti tukea tutkimuksen teoriaa ja siitä on tämän tutkimuksen lisäksi merkittävää hyötyä toimeksiantajayritykselle aiheeseen liittyviä koulutuksia ja ohjeistuksia varten. Toimeksiantajan toiveen lisäksi valintaa helpotti vallitsevat työkäytännöt koronapandemian vuoksi. Haastattelututkimuksen toteuttaminen vallitsevassa tilanteessa olisi ollut vaikeaa sekä myös tarpeetonta, koska kyseessä on arkaluonteinen aihe, johon liittyen anonymiteetin ylläpitäminen on tärkeää työntekijöiden suojaamiseksi. Haastattelutilanteissa haastattelija saa luonnollisesti tietoonsa vastaajan identiteetin, jota tässä tapauksessa ei haluttu. Kyselyn kysymykset luotiin pääosin tutkimuksen toteuttajan toimesta, mutta niitä korjattiin ja muokattiin toimeksiantajayrityksen edustajan palautteen pohjalta. Kyselystä tuli yhteensä noin viisi versiota, joista osaan lisättiin kysymyksiä tai korjattiin olemassa olevia kysymyksiä. Näistä viimeinen versio oli julkaistava versio. Kysely toteutettiin hyödyntämällä Google Forms kyselypalvelua.

Kyselyssä oli 45 kysymystä eli melko paljon, mutta tämän osalta otettiin riski, koska kyselyllä haluttiin kartoittaa mahdollisimman monipuolisesti aiheeseen liittyvät osa-alueet. Kysymyksiin vastaamiseen kuluva aika kellotettiin ja se oli noin 5 minuuttia, joka oli sopiva. Kysymyksien sisältö pyrittiin pitämään mielenkiintoisena ja sellaisena, että vastaaja kokee ne tärkeäksi normaalissa työarjessaan, joka motivoisi vastausten antamista. Osa kysymyksistä oli lisäksi tarkentavia kysymyksiä aiemmassa kohdassa esitettyihin kysymyksiin. Kysymykset ja vastausvaihtoehdot pyrittiin pitämään yksinkertaisina, jotta vastaajan on helppo tehdä kysely.

Vastanneiden taustatietoina kerättiin kysymyksissä koulutustaso ja ikä. Kyselyyn vastanneiden sukupuolta ei koettu tarpeelliseksi kysyä toteutetussa kyselyssä, koska sillä ei koettu olevan merkitystä tämän kyselyn tuloksien hyödyntämisessä. Kyselyn alussa kysyttiin vastaajan arviota omasta tietoturvallisuuden osaamistasostaan sekä tietoturvallisuuden tärkeyttä vastaajan työarjessaan asteikoilla 1-5. Vastaajalta kysyttiin alussa lisäksi, että mihin osa-alueeseen liittyen hän kaipaisi eniten tai lisää tietoturvaperehdytystä, mikäli kokee tarvitsevansa.
Tämän jälkeen alkoi tarkemmat kysymykset tietoturvallisuuden hallintaan ja tietoturvallisuuskokemuksiin ja -havaintoihin liittyen. Kyseiset tietoperustaan pohjautuvat kysymykset ovat jaettu viiteen kategoriaan, jotka listataan ja kuvataan seuraavaksi.

Kategoria 1. Tietoturvaosaaminen ja uhkien tunnistaminen

Tässä kategoriassa tietoturvaosaamisesta kysyttiin itsearviota, jotta voidaan kartoittaa vastaajien oma arviota sen tasosta, sekä heijastaa tämän kohdan vastauksien yhteyttä muihin vastauksiin. Kategoriassa tarkasteltiin myös vastaajan osaamistasoa siltä kantilta, että tunteeko ja tunnistaako työntekijä tietoturvauhkia työympäristössään muiden työntekijöiden osalta. Tässä pyrittiin lisäksi tutkimaan, että pitävätkö työntekijät tietoturvallisuutta tärkeänä arjessaan, jotta voitaisiin nähdä yleistä asennetta tietoturvaa kohtaan. Tämän kategorian kyselytulokset nähdään luvussa 5.2.

Kategoria 2. Tietojenkalastelu, verkkohuijaukset ja haittaohjelmat

Kategorian 2 kysymyksissä pyrittiin keräämään tietoa, että kuinka moni on joutunut tietojenkalastelun ja huijausyritysten kohteeksi, koska kyseiset tavat ovat yleisimpiä tapoja, joita hyökkääjät käyttävät näiden helppouden ja tehokkuuden vuoksi. Tietojenkalastelulta välttyminen tai siihen lankeaminen perustuu hyvin vahvasti huolellisuuteen, kuten tutkimuksen teoriassa ollaan nähty. Kohteeksi joutuneiden määrällä voi myös perustella, että tietojenkalasteluun liittyvä perehdyttäminen on tarpeellista ja hyödyllistä, jotta kohteet tunnistavat kalasteluyritykset tietojenkalasteluksi. Vastaajista pyrittiin lisäksi kartoittamaan, että onko kukaan joutunut valitettavan identiteettivarkauden uhriksi koskaan, koska tämä yleensä viittaa tietovuodon uhriksi joutumista. Haittaohjelmien osalta kerättiin tietoa, että onko vastaajien laitteista löytynyt näitä, jotta tiedetään onko aihe-alueesta kokemusta, ja että miten merkittävästi yrityksen koulutuksissa tulisi käydä tätä osa-aluetta läpi. Tämän kategorian kyselytulokset nähdään koottuna luvussa 5.3.

Kategoria 3. Fyysinen tietoturvallisuus ja huolimattomuudesta aiheutuvat tietoturvauhat

Fyysiseen tietoturvallisuuteen ja huolimattomuudesta aiheutuviin uhkiin liittyen pyrittiin arvioimaan vastaajien omaa tietoturvallisuuttaan työympäristössä fyysisiin laitteisiin ja fyysisiin uhkiin liittyen. Huolimattomuus liittyy olennaisesti fyysiseen tietoturvallisuuteen, jonka osalta tässä pyrittiin kartoittamaan vastaajan huolellisuutta fyysisisissä tietoturva-asioissa, esimerkiksi omiin laitteisiin ja työympäristössä mahdollisesti ilmeneviin poikkeavuuksiin liittyen. Tämän kategorian kyselytulokset nähdään luvusta 5.4.

Kategoria 4. Käyttäjätilien suojaus, laitteiden- ja tiedonhallinta, etätöiden tietoturvallisuus

Tämän kategorian osa-alueita kartoitettiin hyvin laajasti. Etenkin käyttäjätileihin liittyviä suojaustoimenpiteitä ja käytettyjä tapoja haluttiin tutkia mahdollisimman monelta kantilta, koska ne ovat hyvin kriittisiä. Kategoriaan liittyvien kysymysten pohjalta kartoitettiin myös koulutustarvetta. Käyttäjätileistä kysyttiin salasanojen ja käyttäjätilien hallintaan liittyviä asioita.
Laitteiden- ja tiedonhallintaan liittyen kerättiin tietoa työntekijöiden laitteiden käyttötarkoituksia tarkastelemalla, sekä laitteiden suojaukseen liittyen. Etätyön tietoturva-asioita kartoitettiin käytettävän VPN-yhteyden osalta ja mahdollisiin työntekijän kodin verkkolaitteisiin liittyen. Tämän kategorian tuloksia havainnollistetaan luvussa 5.5.

5 Tulokset

Tässä luvussa esitellään tutkimustuloksia. Tutkimuskyselyn vastaajien taustatiedot käydään ensimmäiseksi läpi, jonka jälkeen siirrytään tietoturvallisuuden hallintaan liittyvien kysymyksien vastausten esittelyyn. Tulokset on jaettu neljään kategoriaan, jotka on listattu aiemmassa luvussa. Seuraavaksi esitellään kyselyyn vastanneiden taustatiedot.

5.1 Vastaajien taustatiedot

Kyselyyn osallistuneilta kerättiin taustatieto koulutustasosta ja ikäluokasta.
Vastaajien ilmoittama koulutustaso jaettuna kolmeen ryhmään:

- Noin 35 prosentilla vastaajista oli koulutustasona peruskoulu, lukio tai ammattikoulu
- Noin 40 prosentilla vastaajista alempi korkeakoulututkinto eli kandidaattitason tutkinto
- Noin 25 prosentilla vastaajista ylempi korkeakoulututkinto eli maisteritason tutkinto

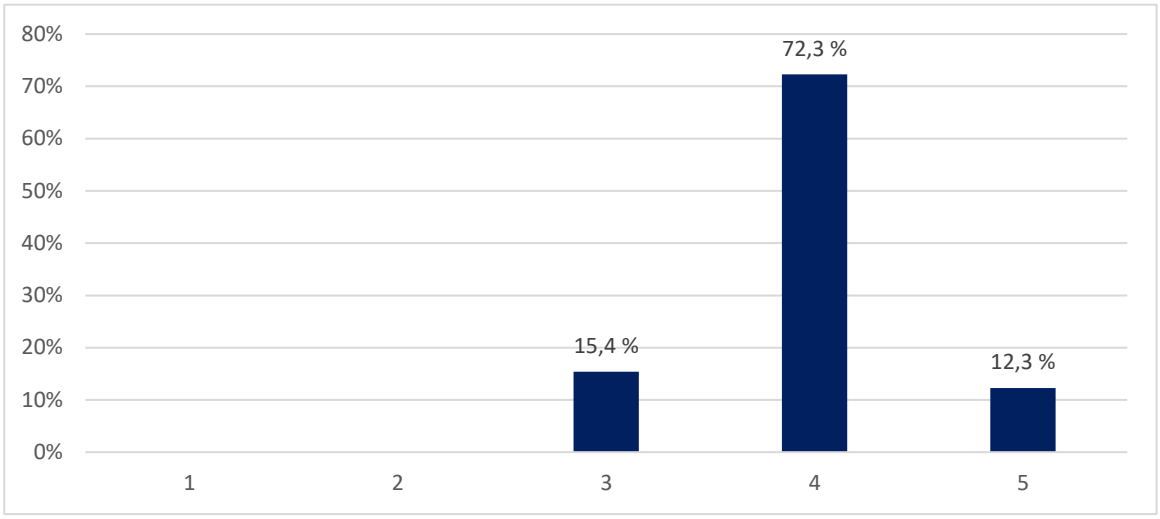
Vastaajien ilmoittama ikä jaettuna ikäluokkiin:

- Noin 20 prosenttia kuului ikäluokkaan 16-35-vuotiaat
- 20 prosenttia ikäluokkaan 35-45-vuotiaat
- Noin 35 prosenttia ikäluokkaan 45-55-vuotiaat
- Noin 20 prosenttia ikäluokkaan 55-60-vuotiaat
- Noin 5 prosenttia yli 60-vuotiaiden ikäluokkaan

Vastaajissa oli eniten alemman korkeakoulutason omaavia henkilöitä, joita oli 25 työntekijää. Toiseksi eniten lukio- ja ammattikoulutasolla olevia, joita oli 23 työntekijää. Kolmanneksi eniten ylemmän korkeakoulutason omaavia työntekijöitä, joita yhteensä 16 työntekijää. Kaikista vähiten oli työntekijöitä, joilla nykyisenä koulutustasona oli peruskoulu. Peruskoulutasolla olevia oli vain yksi työntekijä.

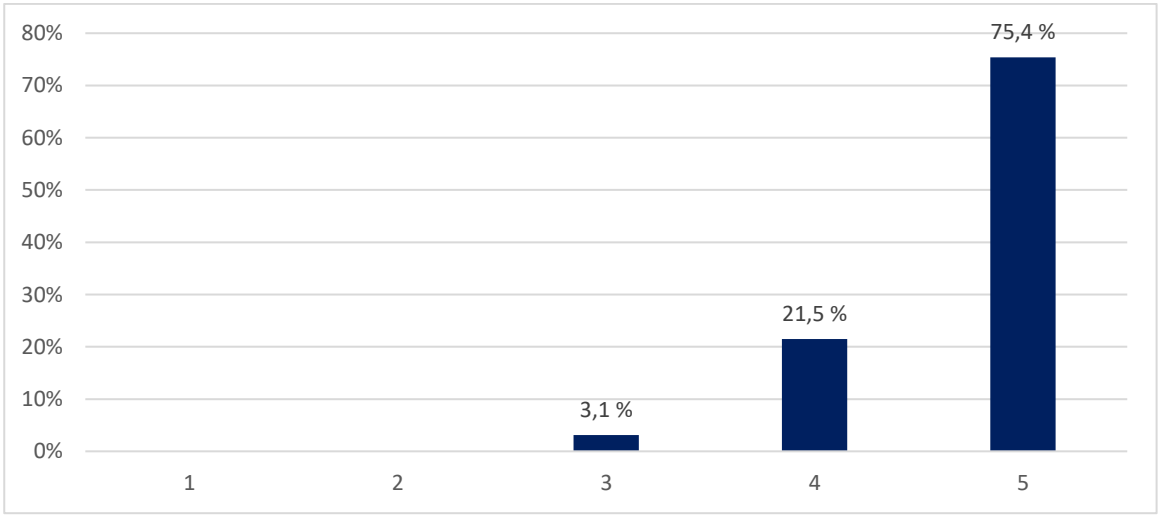
Ikäluokkien osalta eniten vastaajia oli luokassa 45-55-vuotiaat, johon kuului yhteensä 22 työntekijää. Toiseksi suurimpana ikäluokkana 55-60-vuotiaat, johon kuului 14 työntekijää. Vain yhden työntekijän erolla oli seuraavaksi 35-45-vuotiaat, johon kuului 13 työntekijää. Neljänneksi eniten työntekijöitä oli ikäluokassa 25-35-vuotiaat, joita oli 11. Seuraavaksi yli 60-vuotiaiden ikäryhmä, johon kuului 3 työntekijää. Vasta viimeisenä 16-25-vuotiaat, joita oli vain kaksi työntekijää.

5.2 Tietoturvaosaaminen ja uhkien tunnistaminen



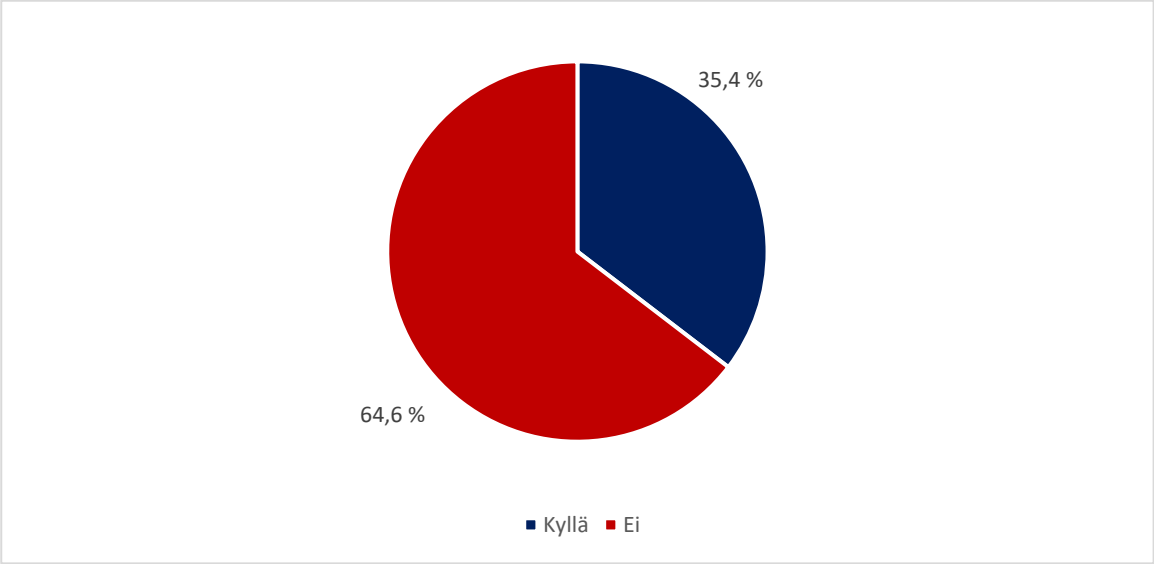
Kuva 2. Arvio tietoturvallisuuden osaamistasostani.

Vastaajat antoivat arvionsa omasta tietoturvallisuusosaamisen tasosta asteikolla 1-5 (kuva 2). 1 = En tunne tietoturvallisuuteen liittyviä asioita tai käytäntöjä, 5 = Tunnen tietoturvallisuusasiat ja käytännöt erinomaisesti. Eniten vastauksia asettui asteikolle 4, jonka vastanneita oli 47 työntekijää. Toisena 10 työntekijää, joiden arvio asteikolla 3. Viimeisenä vastausmäärältään oli parhaan osaamistason vastannut 8 työntekijää.



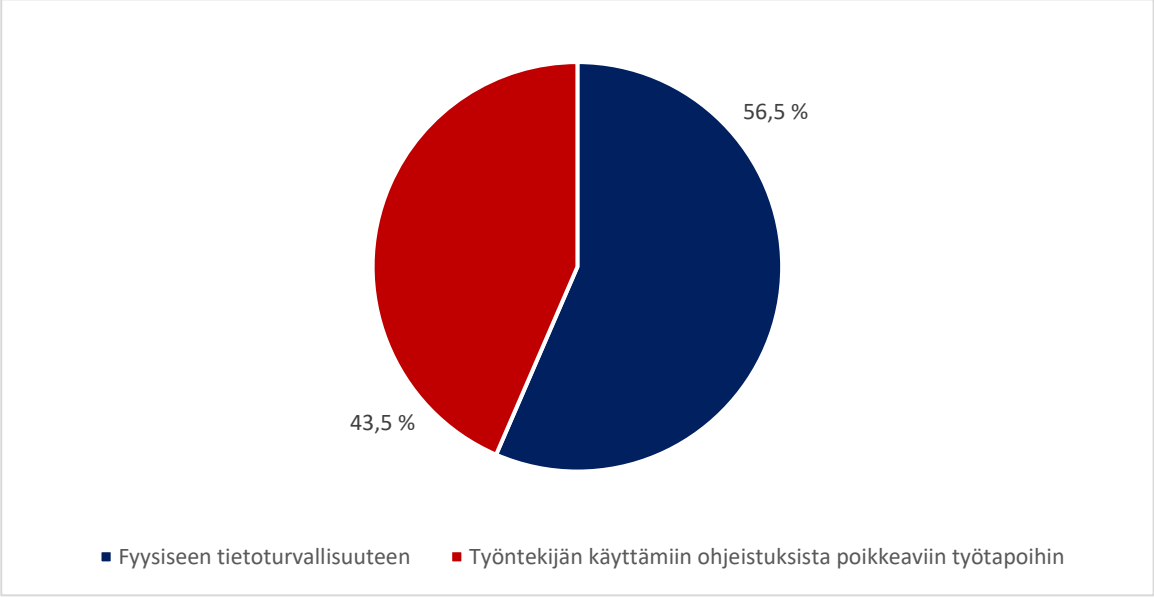
Kuva 3. Tietoturvallisuuden tärkeys minulle työarjessani.

Vastaajat ilmoittivat kuvassa 3 asteikolla 1-5, että kuinka tärkeänä he pitävät tietoturvallisuutta työarjessaan. 1 = Ei lainkaan tärkeä, 5 = Erittäin tärkeä. Valtaosa eli 49 työntekijää vastasi pitävänsä tietoturvallisuutta erittäin tärkeänä työarjessaan. Toisena tuli taso 4, jonka vastasi 14 työntekijää. Vähiten vastauksia sai taso 3, jonka vastasi 2 työntekijää.



Kuva 4. Olen havainnut tietoturvan laiminlyöntiä työympäristössäni työntekijöiden toimesta.

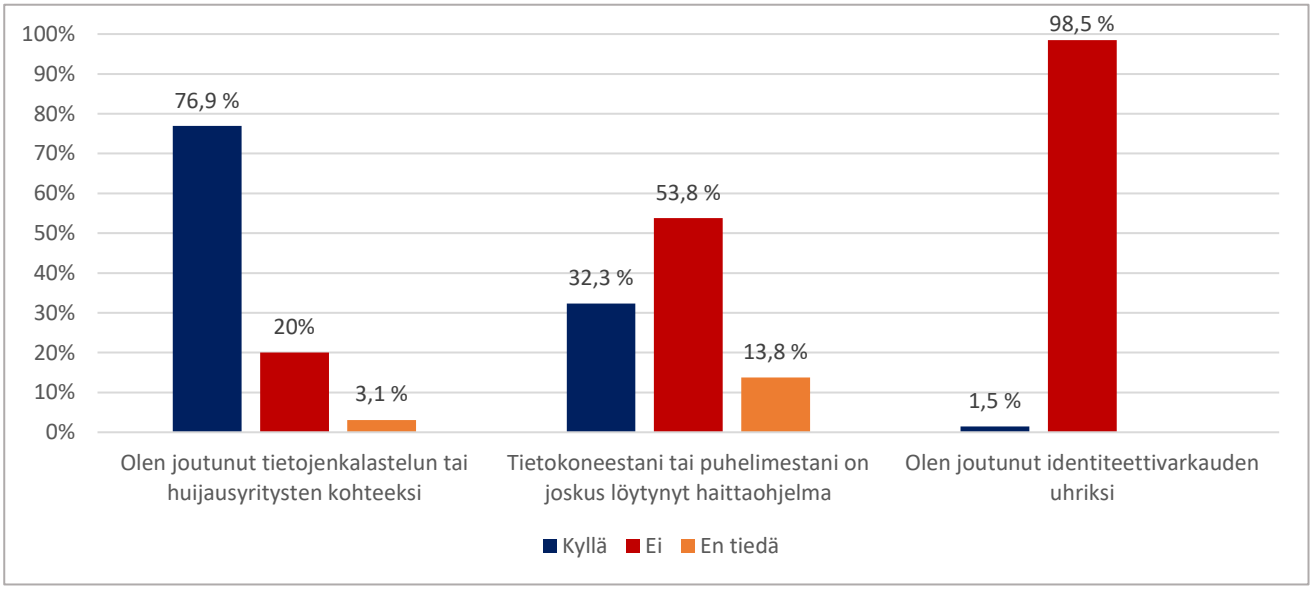
Kuvasta 4 nähdään, kuinka moni vastaajista on havainnut tietoturvallisuuden laiminlyöntiä työympäristössään. Suurin osa eli 42 työntekijää eivät olleet havainneet laiminlyöntiä. 23 työntekijää olivat havainneet laiminlyöntiä.



Kuva 5. Vastaa tähän, jos vastasit edelliseen kysymykseen myönteisesti. Mihin laiminlyönti pääosin liittyi?

13 edelliseen kysymykseen myönteisesti vastanneista työntekijöistä vastasi, että laiminlyönti liittyi fyysiseen tietoturvallisuuteen. 10 työntekijää vastasi, että laiminlyönti johtui ohjeista poikkeavista työtavoista.

5.3 Tietojenkalastelu, huijaukset, haittaohjelmat

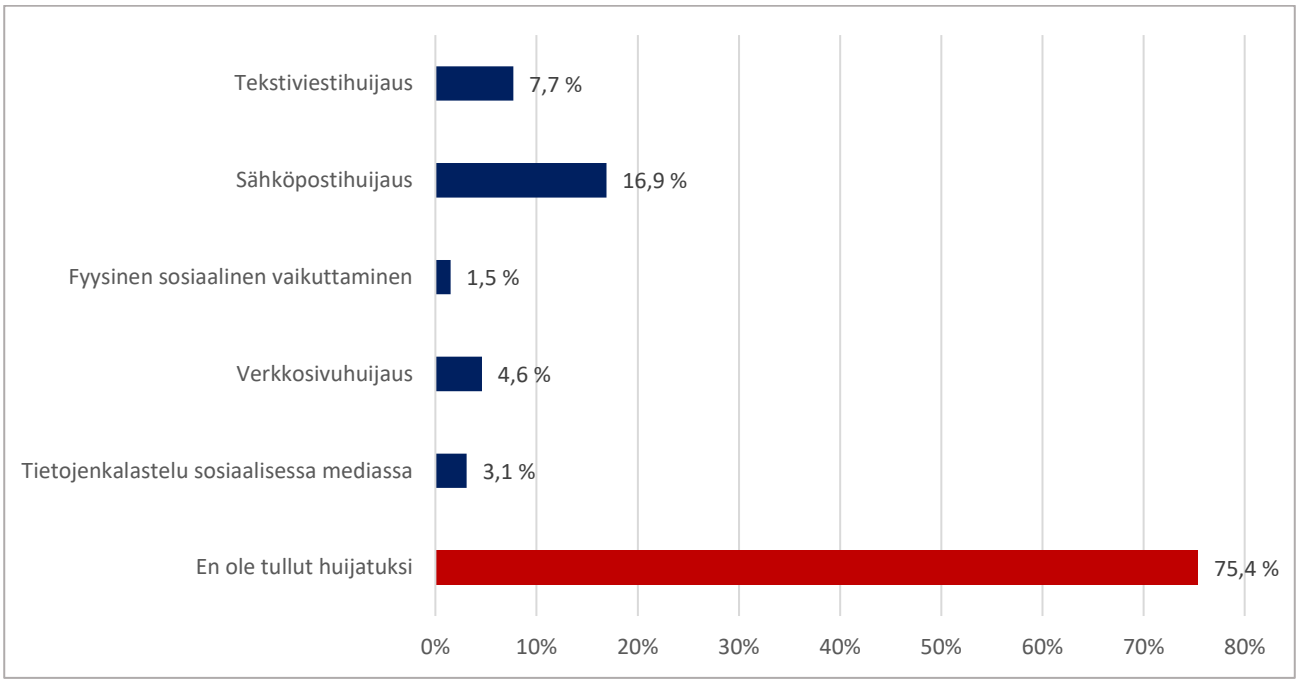


Kuva 6. Vastaukset tietojenkalastelusta ja huijausyrityksistä, haittaohjelmista, sekä identiteettivarkaudesta.

Tietojenkalastelun tai huijausyritysten kohteeksi töissä tai vapaa-ajalla, oli vastanneista joutunut 50 työntekijää. 13 työntekijää vastasi, että eivät olleet joutuneet kalastelun tai huijausyritysten kohteeksi. 2 työntekijää vastasivat, että eivät tiedä ovatko joutuneet kohteeksi (kuva 6).

Laitteista löytyneiden haittaohjelmien osalta vastaukset jakautuivat seuraavasti. Suurin osa eli 35 työntekijää vastasi, että laitteistaan ei ole koskaan löytynyt haittaohjelmaa. 21 työntekijää vastasi, että tietokoneesta tai puhelimesta on löytynyt haittaohjelma. Vähiten vastauksia saaneena oli vaihtoehto ”en tiedä”, jonka oli vastannut 9 työntekijää (kuva 6).

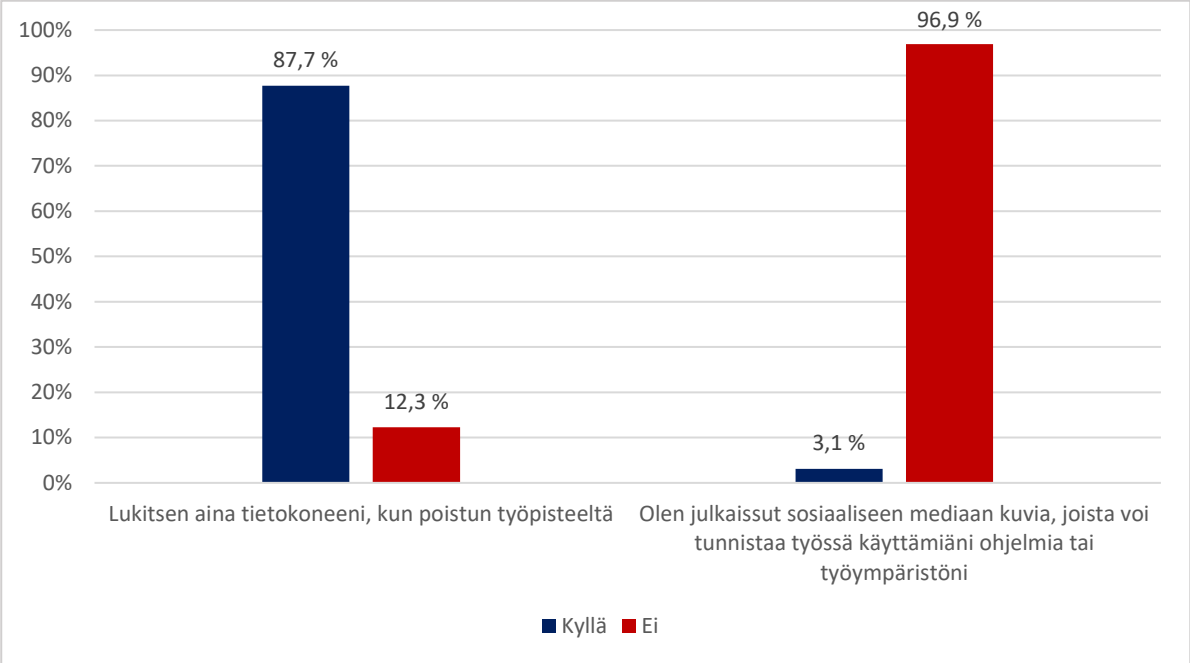
Viimeisessä kohdassa kartoitettiin identiteettivarkauden uhriksi joutuneita. Uhreja oli onneksi todella vähän. Uhriksi oli valitettavasti joutunut kuitenkin yksi työntekijä (kuva 6).



Kuva 7. Olen tullut huijatuksi jollain seuraavista keinoista.

Huijauksien osalta kartoitettiin huijaustapoja, joista suurin osa vastauksista oli ”en ole tullut huijatuksi”, jonka oli vastannut 49 työntekijää. Toiseksi eniten vastauksia oli saanut sähköpostihuijaus, jonka vastanneita oli 11 työntekijää. Kolmanneksi tekstiviestihuijaus, jonka vastanneita oli 5 työntekijää. Tämän jälkeen verkkosivuhuijaus, jonka oli vastannut 3 työntekijää. Seuraavaksi tietojenkalastelu sosiaalisessa mediassa. Tämän vastauksen valinneita vain 2 työntekijää. Viimeisenä ja vähiten vastauksia saaneena oli fyysinen sosiaalinen vaikuttaminen, jonka oli vastannut yksi työntekijä (kuva 7).

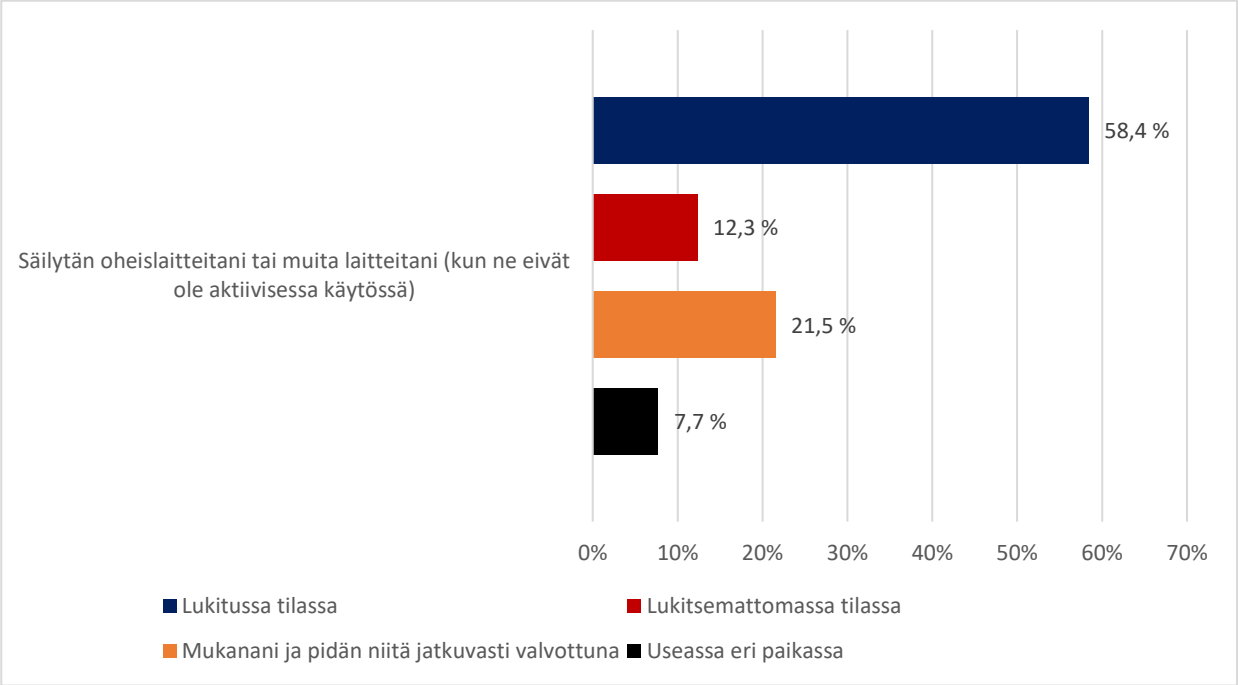
5.4 Fyysinen tietoturvallisuus ja huolimattomuudesta aiheutuvat uhat



Kuva 8. Tietokoneen lukitsemiseen ja sosiaalisen median julkaisuihin kohdistuvat kysymykset.

Kuvasta 8 nähdään vastausten jakautuminen tietokoneen lukitsemiseen ja sosiaaliseen median julkaisemiseen liittyen. Kyselyvastausten perusteella suurin osa lukitsee tietokoneensa lähtiessään työpisteeltä. Tämän vastanneita oli 57 työntekijää. Sen sijaan 8 työntekijää vastasi, että eivät lukitse tietokonetta poistuessaan työpisteeltä.

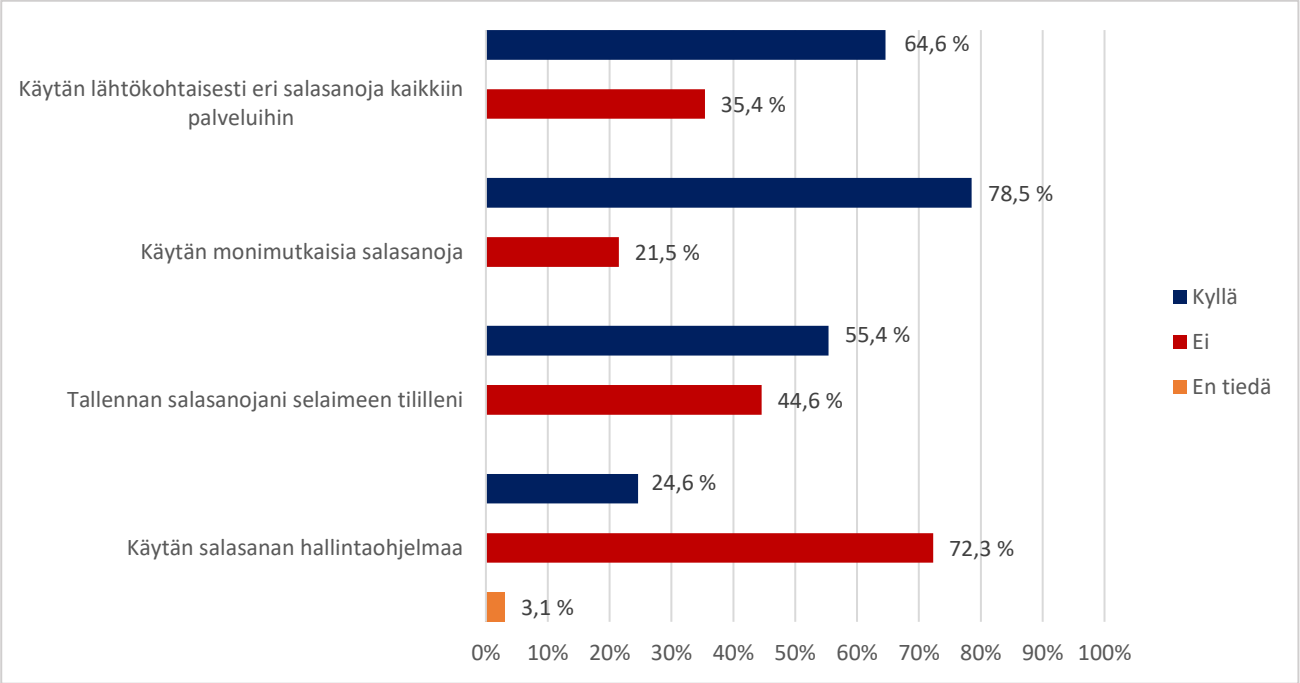
Suurin osa vastaajista eivät olleet vastausten perusteella julkaisseet sosiaaliseen mediaan kuvia, joista työssä käyttämiä ohjelmia tai työympäristö olisi tunnistettavissa. 63 työntekijää vastasi, että eivät olleet julkaisseet sellaisia kuvia. 2 työntekijää vastasi julkaisseen sellaisia kuvia.



Kuva 9. Vastaukset oheislaitteiden ja muiden laitteiden säilytykseen liittyen.

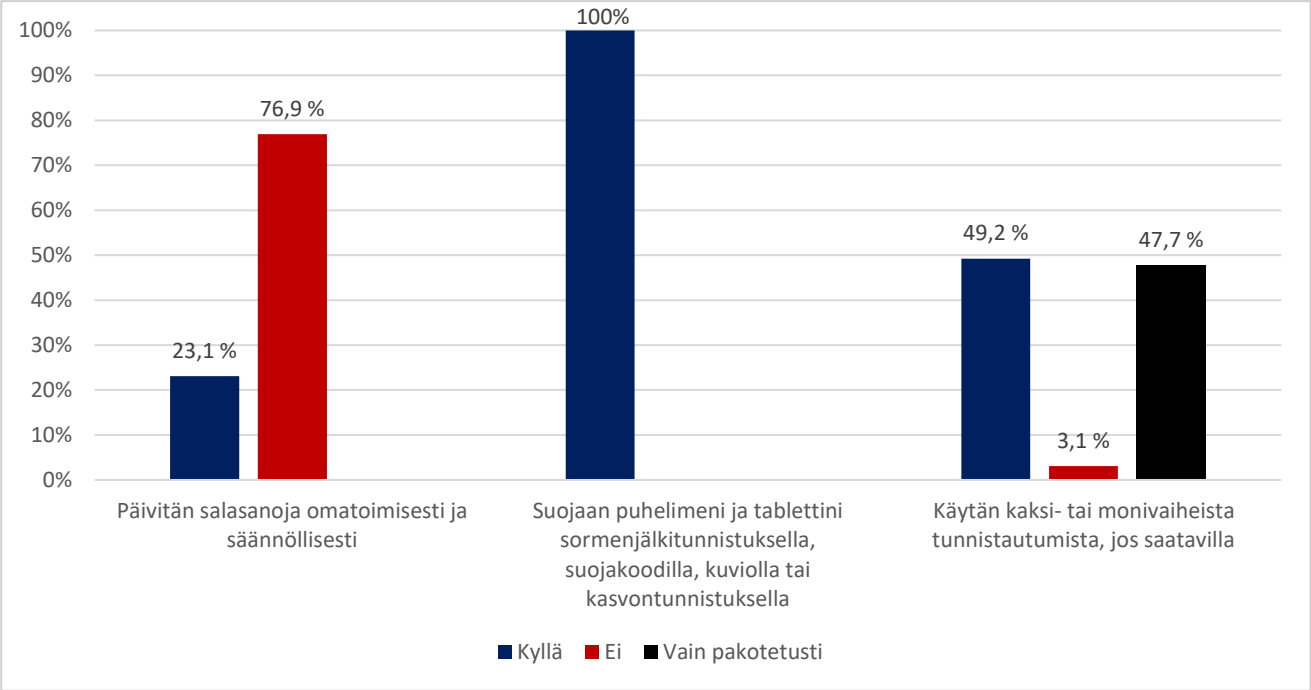
Kuvan 9 kysymykseen oheislaitteiden tai muiden laitteiden säilyttämisen osalta, vastasi suurin osa säilyttävänsä niitä lukitussa tilassa. Tämän vastauksen valinneita työntekijöitä oli 38. Seuraavaksi oli 14 työntekijää, jotka olivat vastanneet kantavansa niitä aina mukana ja pitävän niitä valvottuna. 8 työntekijää vastasivat, että säilyttävät laitteita lukitsemattomassa tilassa. 5 työntekijää, eli vähiten oli vastanneet säilyttävänsä niitä useassa eri paikassa.

5.5 Käyttäjätilien suojaus, laitteiden- ja tiedonhallinta, etätyöt



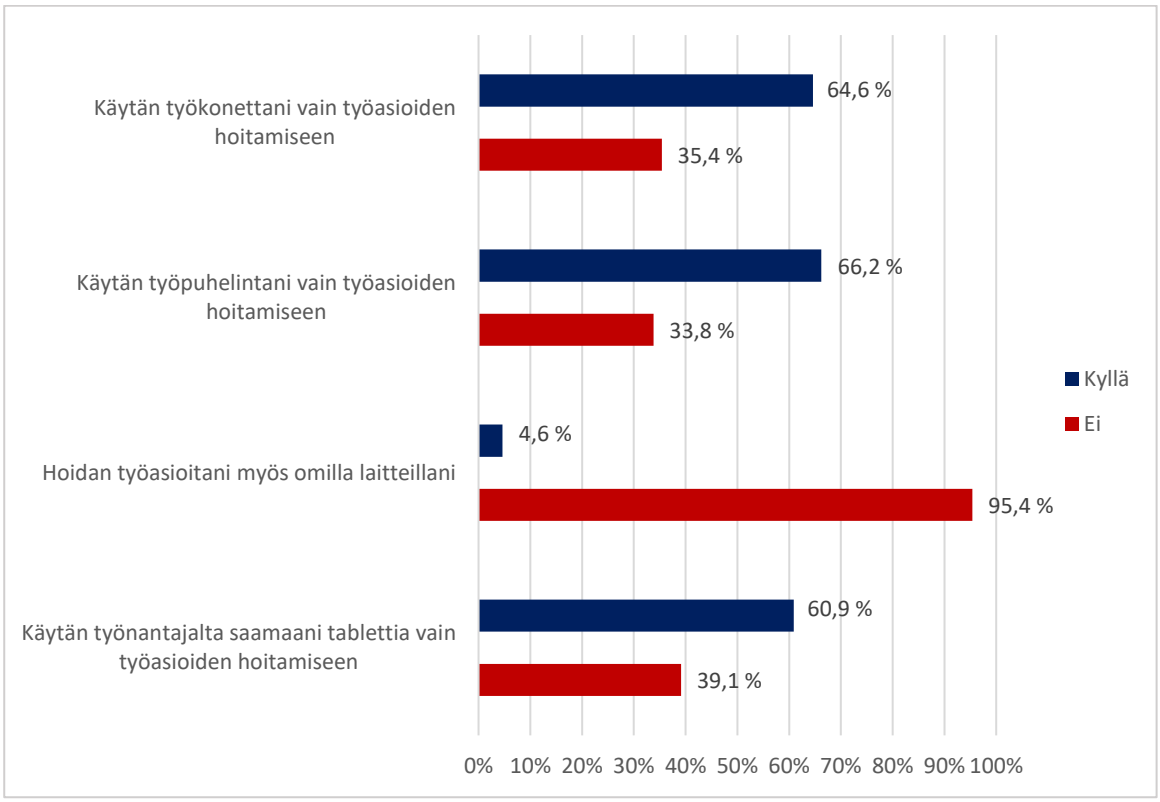
Kuva 10. Vastaukset salasanojen hallintaan liittyen.

Kuvassa 10, ylimmässä diagrammissa 42 työntekijää vastasi käyttävänsä eri salasanoja kaikkiin käyttämiinsä palveluihin. 23 työntekijää vastasi, että ei käytä eri salasanoja.
Toiseksi ylimmästä diagrammista nähdään, että suurin osa vastaajista käyttää monimutkaisia salasanoja. Tämän vaihtoehdon vastanneita oli 51 työntekijää. 14 työntekijää vastasi, että eivät käytä monipuolisia salasanoja. Kolmannessa diagrammissa tulokset olivat melko tasaisia, mutta enemmistö, eli 36 työntekijää vastasivat tallentavansa salasanoja selaimen tilille. Loput työntekijät, eli 29 vastasi, että eivät tallenna selaimelle salasanoja. Viimeisenä kysyttiin salasanojen hallintaohjelman käytöstä, johon 47 työntekijää vastasivat, että eivät käytä salasanoille hallintaohjelmaa. 16 vastasivat käyttävänsä sellaista. Vastaajista 2 työntekijää eivät tienneet, että käyttävätkö salasanojen hallintaohjelmaa.



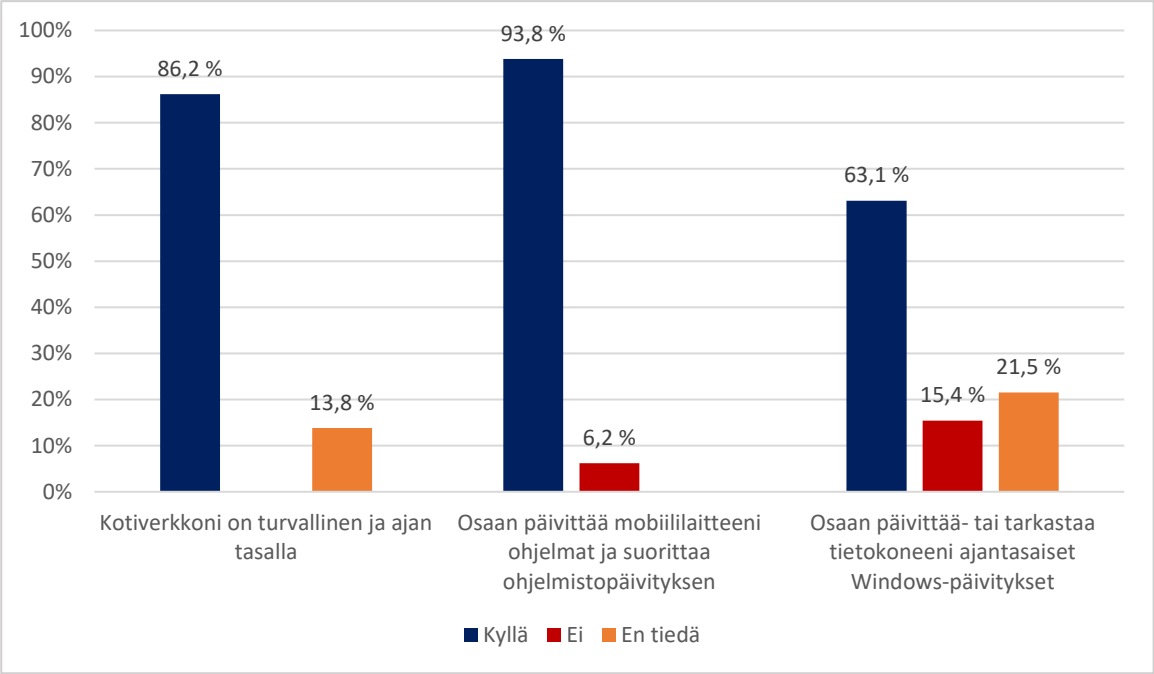
Kuva 11. Vastauksen käyttäjätilin suojaukseen ja laitteiden suojaukseen liittyen.

Kuvan 11 ensimmäisestä diagrammista nähdään, että suurin osa vastasi kielteisesti salasanojen päivittämiseen. 50 työntekijää vastasivat, että eivät päivitä salasanojaan omatoimisesti ja säännöllisesti. 15 työntekijää vastasivat päivittänsä niitä säännöllisesti. Toisesta diagrammista nähdään hyvin positiivinen tulos, eli kaikki 65 vastannutta työntekijää suojaa puhelimensa ja mahdollisen tablettinsa jollain kuvassa mainituista suojaustavoista. Viimeisen diagrammin osalta nähdään hieman negatiivinen tulos. 32 työntekijää vastasivat käyttävänsä kaksi- tai monivaiheista tunnistautumista, mutta jopa 31 työntekijää vastasivat, että käyttävät vain pakotetusti. Kaksi työntekijää vastasivat, että eivät käytä monivaiheista tunnistautumista.



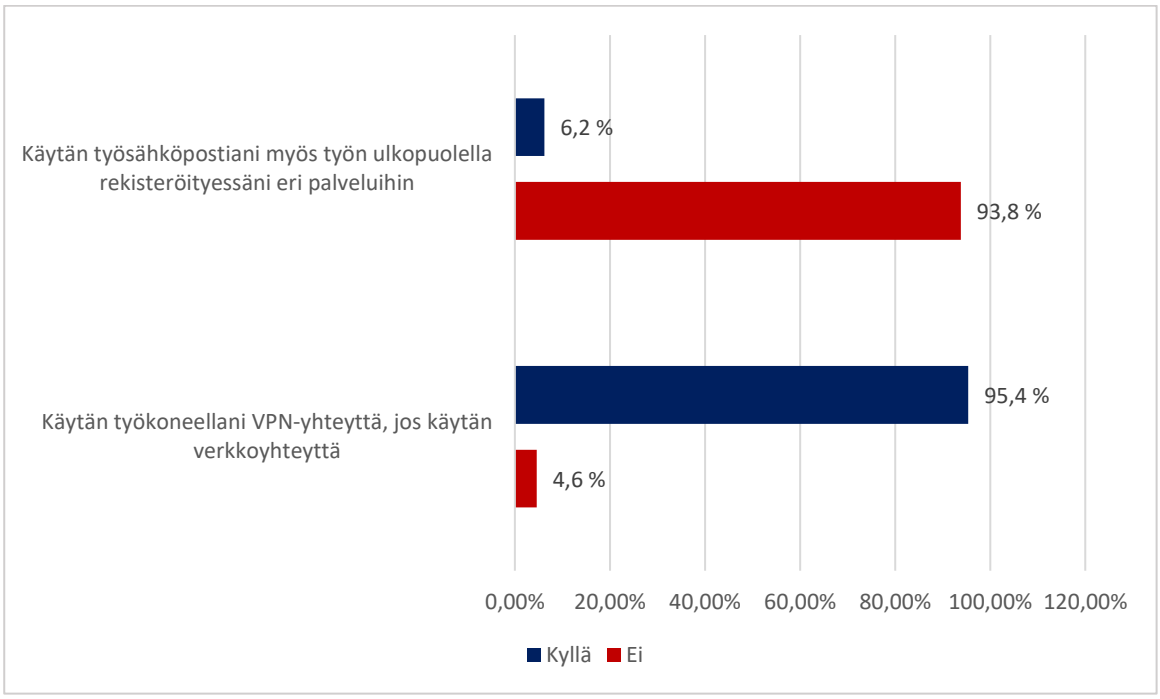
Kuva 12. Vastaukset työlaitteiden käyttöön ja työasioiden hoitamiseen liittyen.

Kuvassa 12 nähdään ensimmäisestä diagrammista, että suurin osa vastaajista, eli 42 työntekijää käyttää työkonetta vain työasioiden hoitamiseen. 23 työntekijää vastasivat käyttävänsä työkonetta myös muihin tarkoituksiin. Seuraavasta diagrammista nähdään, että suurin osa ja melkein sama määrä käyttää työpuhelinta vain työasioiden hoitamiseen, kuin mitä työkoneen käyttöön oli vastattu. 43 työntekijää vastasivat käyttävänsä työpuhelinta vain työasioiden hoitamiseen. 23 työntekijää vastasi käyttävänsä myös muuhun tarkoitukseen. Kolmannesta diagrammista nähdään työasioiden hoitamiseen liittyen, että valtaosa työntekijöistä, eli jopa 62 työntekijää ei hoida työasioita omilla laitteillaan. Vain kolme työntekijää vastasivat myönteisesti. Viimeisessä diagrammissa työnantajalta tabletin saaneista työntekijöistä vastasivat 14 työntekijää, että käyttävät tablettia vain työtarkoituksiin. Loput 9 työntekijää vastasivat käyttävänsä sitä myös muihin tarkoituksiin.



Kuva 13. Vastaukset laitteiden päivityksiin ja kotiverkkoon liittyen.

Kuvassa 13, suurin osa ensimmäisen diagrammin vastaajista vastasivat, että heidän kotiverkkonsa olisi turvallinen ja ajan tasalla. Tämän vastauksen antoivat 56 työntekijää. Yksikään ei vastannut tähän kohtaan kielteisesti, mutta 9 työntekijää vastasivat, että eivät tiedä onko heidän kotiverkkonsa turvallinen tai ajan tasalla. Seuraavassa diagrammissa mobiililaitteiden ohjelmien ja ohjelmiston päivityksestä vastasivat jopa 61 työntekijää, että osaavat suorittaa kyseiset päivitykset. Neljä työntekijää vastasivat, että eivät osaa tehdä kyseisiä päivityksiä. Viimeisessä diagrammissa Windows-päivityksien suorittamisesta ja tarkastamisesta vastasivat 41 työntekijää, että osaavat suorittaa tai tarkastaa päivitykset. 10 työntekijää eivät osanneet suorittaa tai tarkastaa päivityksiä. 14 työntekijää eivät olleet varmoja asiasta ja vastasivat vaihtoehdon ”en tiedä”.



Kuva 14. Vastaukset työsähköpostin ja VPN-yhteyden käyttämiseen.

Valtaosa vastaajista eivät käyttäneet työsähköpostiansa eri palveluiden rekisteröinteihin. 61 työntekijää vastasivat, että eivät käytä työsähköpostiansa rekisteröinteihin. Neljä työntekijää vastasivat käyttävänsä työsähköpostiansa tähän tarkoitukseen. VPN-yhteyden käyttöön liittyen valtaosa vastasi, että sitä käytetään. 62 työntekijää vastasivat käyttävänsä sitä, ja kolme työntekijää eivät vastausten perusteella käyttäneet ollenkaan VPN-yhteyttä.

6 Pohdinta ja johtopäätökset

Tutkimus osoitti keskeisimpiä ja kriittisimpiä työtekijän tietoturvallisuuteen kohdistuvia uhkia ja kuvasti myös näistä aiheutuvia riskejä. Tutkimuksella saatiin laajasti myös käytännön tietoa työntekijöiden tietoturvallisuuden hallintaan liittyen toteutetulla kyselyllä. Kyselyyn vastanneiden määrä oli hyvä ja sen vuoksi vastauksista saatiin laadukasta tietoa, jota peilata teoriaan. Suurin osa vastaajista oli ikäluokaltaan hieman vanhempia, mutta tuloksien perusteella tietoturvan taso pysyi normaalilla ja yleisesti katsottuna hyvällä tasolla. Tietoturvan tärkeyttä tarkastelevien kysymysten osalta vaikutti, että vastaajat pitävät tietoturvaa hyvin tärkeänä arjessaan niin kuin kuuluukin. Tietoturvan laiminlyöntiä oli havaittu työympäristössä erityisesti fyysisen tietoturvan osalta. Tämä havainto otetaan toimeksiantajayrityksessä varmasti koulutusten kannalta huomioon. Tietojenkalastelun kohteeksi joutuneita oli paljon, joka ei tänä päivänä yllätä, kun toteutustavat ovat helppoja ja tehokkaita. Huijatuksi tulemista kartoitettiin myös ja kysyttiin huijauksen tyyppiä. Tässä kärkeen meni arvatenkin sähköpostihuijaus, johon oltiin langettu. Tietojenkalastelun vaarallisuudesta ja uhista mainittiin tietoperustassa, joten tulos tukee teoriaa. Salasanoihin liittyen vastaajilla oli kehitettävää tietyiltä osa-alueilta, kuten salasanojen päivitykseen ja salasanojen hallintaohjelman käyttöön liittyen. Oli positiivista huomata, että mobiililaitteiden osalta kaikki vastaajat käyttivät jotakin laitteen suojauskeinoa, esimerkiksi suojakoodia. Monivaiheisen tunnistautumisen osalta pitäisi vastaajille osoittaa, kuinka tärkeä osa käyttäjätilien tietoturvaa se on, jotta kaikki käyttäisivät myös vapaaehtoisesti sitä. Tulokset eivät olleet hälyttäviä, vaan suurimmilta osin hyviä. Osa kysymyksistä poistettiin tutkimuksen virallisesta versiosta sen takia, koska niiden ei koettu tuovan tähän työhön lisäarvoa, mutta toimeksiantajayrityksen erilliseen käyttöön kyllä. Siksi niitä ei ole esitelty. Yksityiskohtaisia kohdeorganisaation tietoturvaan liittyviä parannusehdotuksia ei tässä voida kertoa, koska niitä voitaisiin pahimmillaan käyttää hyväksi. Tulosten pohjalta pyritään kuitenkin priorisoimaan tietoturvakoulutusten sisältöä kohdeorganisaatiossa, sekä mahdollisesti seuraamaan näihin osa-alueisiin liittyvää toimintaa arjessa tarkemmin.

Tutkimuksen kartoittamien uhkien pohjalta käytiin läpi useampia keinoja, joilla uhilta voidaan pyrkiä suojautumaan ja minimoida niistä aiheutuvia riskejä. Työntekijän tietoturvaan liittyvien toimien tai tietoturvaosaamisen ei ole oltava täydellistä, koska sellainen ei ole mahdollista. Niin kauan kun ihmiset toteuttavat tietoturvaratkaisuja, niin aina löytyy toisia ihmisiä, jotka pystyvät murtamaan tietoturvan, vaikka se olisi kuinka vahva tahansa. Kun tekee parhaansa ja huomioi nämä asiat, niin se riittää. Yleinen, mutta valitettava fakta on se, että tietoturvan osalta tulee pyrkiä olemaan parempi kuin joku toinen hyökkääjän potentiaalinen kohde. Tällöin hyökkääjä valitsee luonnollisesti helpoimman kohteen ja siirtyy sen pariin. Sama pätee käytännön rikollisuudessakin.

Murtovarkaat valitsevat yleensä hyötyä ja vaivaa punnitsemalla parhaan kohteen toimillensa. Tietoturvankin osalta tulee lisäksi muistaa, että tilaisuus voi tehdä varkaan.

Tutkimuksessa ilmenneiden uhkien ja oman kokemukseni pohjalta vaikuttaa selvästi siltä, että tietojenkalastelu ja huijausposti ovat tällä hetkellä merkittävin uhka työntekijöiden tietoturvalle. Tietojenkalastelutavat, hyökkäystoteutuksien kohdistusalueet, sekä sisältö kehittyvät jatkuvasti, joka vaatii vielä entistä enemmän tarkkuutta työntekijöiltä ja huomiota työntekijöiden tietoturvasta vastaavilta henkilöiltä. Näiden olemassaolon lisäksi riski suurenee huomattavasti, jos perustason tietoturva-asiat eivät ole kunnossa. Näistä tärkeimpiä esimerkkejä ovat käyttäjätilien suojaus, virustorjunta, palomuuri ja päivitykset.

Tutkimuksen tavoitteena oli vastata kysymyksiin:

- Mitä asioita työntekijän tulee hallita tietoturvallisuudestaan ja miksi?
- Millaisia uhkia työntekijän tieoturvaan kohdistuu ja millaisia riskejä niistä muodostuu?
- Mitkä ovat ne konkreettiset keinot, joilla tietoturvauhkia vastaan voidaan suojautua, sekä riskejä minimoida?

Tutkimuksella haluttiin saada kattava ja laadukas asiakokonaisuus luotua työntekijöille tietoturvallisuuden hallintaan liittyen. Tietokoneen ja muiden laitteiden tietoturvaa tulee hallita tutkimuksessa käytyjen tietojen ja keinojen pohjalta ja työpaikan, sekä yleisiä tietoturvallisuusohjeistuksia noudattamalla. Tiedostamalla uhat ja mahdolliset riskit, voidaan tunnistaa uhkia ja minimoida tietoturvariskejä. Tietoturvaa tulee hallita jatkuvasti arvioimalla sitä ja tekemällä jatkuvia toimia siihen liittyen. Hallinnan puuttuminen aiheuttaa merkittäviä riskejä, joista voi aiheutua itselle tai työpaikalle pysyviä haittoja ja raskaita seurauksia. Läpi koko tutkimuksen, päähavainto listattuja uhkia ja riskejä yhdistävästä tekijästä oli huolimattomuus. Huolellisuudella ja toimimalla hallitusti pärjää jo hyvin pitkälle. Työntekijän tietoturvaan kohdistuu paljon uhkia ja näitä tulee hallita rutiininomaisesti, sekä niiden riskit tiedostaa, kuten tutkimuksessa mainittiin.

Työntekijöiden tulee hallita tietoturvallisuuttaan, koska organisaation tietoturvallisuus on juuri niin vahva kuin sen heikoin lenkki. Tietoturvan keskiössä ovat tiedot ja ihmisten toiminta tietoihin liittyen, joten paras tulos saadaan, kun kaikki tekevät oman osansa parhaalla osaamisellaan. Keskeisimpiä ja hyödyllisimpiä konkreettisia suojautumiskeinoja listattiin kolmannessa kappaleessa ja käytännön keinojen lisäksi tähän kuuluu suuressa määrin perehtymistä tietoturvaan liittyviin asioihin.

Potentiaalisia jatkotutkimusaiheita tietoturvaa koskien olisi hyvä tehdä mobiililaitteista, kodin IoT-laitteista tai yrityksen tietoturvakartoituksen toteuttamisesta. IoT-laitteiden osalta olisi myös kiinnostavaa tietää, että kuinka monella on nykyään näitä kotona, koska ne vaikuttavat kotiverkon tietoturvaan olennaisesti.

Tietoturvallisuuden tärkeyttä painostetaan paljon, mutta ei syyttä. Sen säilyvyys on edellytyksenä toimivalle yhteiskunnalle tänä päivänä, kun useampi palvelu ja toiminto on digitalisoitu. Tämän lisäksi tietoturvallisuudelle aiheuttaa tällä hetkellä merkittävästi uhkaa vallitseva tilanne maailmalla. Sotakriisi Euroopan alueella on osoittanut, kuinka tärkeää on että tietoturvallisuus säilyy, ja että tietotekninen infrastruktuuri on kaikilta osa-alueilta suojattu hyvin. Tietoturvan varmistamisella pyritään suojelemaan ihmisiä ja yrityksiä, edellytyksenä tietojen luotettavuuden, eheyden ja saatavuuden ylläpito. Tutkimuksen pohjalta voidaan todeta, että myös työntekijän vastuu ja työntekijältä vaaditut asiat ovat lisääntyneet vuosien saatossa tietoturvaan liittyen digitalisaation johdosta ja tietotekniikan kehittyessä, sekä kiristyneen maailmantilanteen johdosta. Työhön saatiin koottua laajalti keskeisimpiä ja ajankohtaisia tietoturvauhkia ja -riskejä sekä toimia ja tietoa, joilla näitä voidaan tunnistaa ja hallita.

6.1 Tutkimuksen luotettavuus

Tutkimuksen luotettavuutta käsitellään pätevyyden eli validiteetin, sekä luotettavuuden eli reliabiliteetin avulla. Reliabiliteetilla arvioidaan tutkimusta kolmesta näkökulmista. Onko käytetty metodi luotettava ja johdonmukainen tarkoitetuissa olosuhteissa? Pysyyko havainnot ja tulokset olennaisina eri aikoina? Ovatko tulokset johdonmukaisia ja poikkeavatko ne mahdollisista uusista tuloksista samasta aiheesta? Validiteettia pidetään yleensä tärkeämpänä laadullisessa tutkimuksessa kuin luotettavuutta, koska sillä tutkitaan, että onko tutkimus pätevä, laadukkaasti ja perustellusti muodostettu, ja että ovatko saadut päätelmät oikeita. (Saaranen-Kauppinen & Puusniekka 2006.)

Laadullisessa tutkimuksessa luotettavuutta on myös hyvä arvioida, koska varsinkin kyselyn luomisessa, sekä tulosten keräämisessä voi tutkimuskohderyhmän käsitys ja ymmärrys aiheeseen liittyvistä kysymyksistä poiketa kyselyn toteuttajan kanssa. Tämä voi johtaa siihen, että vastaaja antaa vääriä vastauksia, koska ymmärtää kysymykset väärin. Tässä tutkimuksessa kyselyn luonnissa pyrittiin huomioimaan tällaiset asiat. Kyselystä luotiin useampi versio, joissa kysymyksiä pyrittiin mietittimään yleisestä näkökulmasta ilman oman IT-alan asiantuntijuuden tuomaa apua. Kysymyksiä selkeytettiin ja vaihdettiin toimeksiantajan edustajan palautteen pohjalta, sekä myös omien näkemysteni pohjalta. Kyselyn luomisessa kiinnitettiin huomiota, että kysymykset olisivat yksinkertaisia, kiinnostavia ja tärkeitä lukijalle. Kyselyn kesto pyrittiin myös pitää lyhyenä, jotta vastausten keskeytymisen tai keskittymisen menetyksen riskejä voitaisiin minimoida.

Tutkimuksessa käytetyt tiedonkeruu- ja tuottamismenetelmät olivat järjestelmällisiä ja lähteiden valintaan käytettiin aiheiden paino-arvon jaottelua avuksi, jotta tietoperustan eli lukujen 2 ja 3, sekä niiden alalukujen sisältö saataisiin mahdollisimman laadukkaaksi ja monipuoliseksi. Tietoturva aiheena on luonteeltaan sellainen, että on epätodennäköistä, että tässä tutkimuksessa käytetyn kyselyn tulokset olisivat esimerkiksi puolen vuoden jälkeen täysin samat, jos kysely toteutettaisiin uudelleen. Yksilöiden tietoturvaosaaminen ja yrityksien käytännöt muuttuvat usein nopeasti. Uskon kuitenkin, että vastauksissa olisi paljon yhtäläisyyksiä, jos kohderyhmä olisi sama. Kyselyn tuloksia selittäessä on myös poistettu sellaiset kysymykset tutkimuksesta, joista olisi voinut luoda harhaanjohtavia näkemyksiä. Näitä on esimerkiksi tietyt monivalintakysymykset.

Tutkimus ja sen tulokset vaikuttavat kokonaisuudessaan päteviltä, koska tietoa on monipuolisesti, se on perusteltua ja tarkoin valittua. Tutkimustuloksien vastaukset liittyvät myös vahvasti tietoperustaan, joka luo tärkeän yhteyden näiden välille.

6.2 Opinnäytetyöprosessin ja oman oppimisen arviointi

Tutkimus ja koko opinnäytetyöprosessi vahvisti omaa oppimistani työntekijöiden tietoturvan osalta, kun laadukasta lähdemateriaalia pääsi analysoimaan laajasti ja samalla vertaamaan havaintoja ja tietoa omiin kokemuksiini ja osaamiseeni. Tietoperustan tiedot vahvistivat myös omia kokemukseeni pohjautuvia päätelmiäni tietyistä tietoturvan osa-alueista, joten pystyn hyvin samaistumaan teoriaan ja tuloksiin. Tutkimukseen ja aiheeseen liittyen motivaatiota tuli huomattavasti lisää, kun sain tutkimusaiheeksi sellaisen, jolla voin auttaa työntekijöitä tai lisätä heidän tietoisuutta tietoturvallisuuteen liittyvien uhkien ja riskien osalta.

Sen lisäksi, että aihe kiinnosti minua prosessin alussa erittäin paljon, tuli sopivasti mieleen käyttötarkoitus tutkimukselle toimeksiantajayritykseen, sekä idea tutkimuskyselylle ja sen rakenteelle. Tutkimuksessa toteutettu kysely antoi merkittävää lisäarvoa tutkimuksessa. Kyselyvastausten analysointi antoi minulle hyvää osviittaa siitä, millä tasolla työntekijöiden tietoturvallisuus keskimäärin on, jos tietoturvaa on koulutettu heille perustasolla. Vastaukset antoivat myös hyvän kuvan siitä, kuinka tärkeänä työntekijät pitävät tietoturvaa ja sen eri osa-alueita työarjessaan. Opin paljon uutta tutkimusmenetelmien hyödyntämisestä, lähdemateriaalin analysoinnista, sekä akateemisesta kirjoittamisesta. Olisin voinut priorisoida työn, vapaa-ajan, sekä tämän opinnäytetyöprosessin välillä tarkemmin. Lisäksi asioita olisi voinut suunnitella vielä entistä enemmän, koska se olisi helpottanut ja nopeuttanut prosessia. Olen kokonaisuudessan kuitenkin hyvin tyytyväinen lopputulokseen ja uskon tutkimuksesta olevan hyötyä toimeksiantajayrityksessä, sekä muille työntekijöille. Voin myös itse palata tutkimukseen tulevaisuudessa ja virkistää työntekijöiden tietoturvan hallintaan liittyviä asioita, jos sille on tarvetta ja jos tietoturva-asiat eivät ole ehtineet muuttua liian merkittävästi.

Lähteet

Doherty, J. 2015. Wireless and Mobile Device Security. Luettu: 19.5.2022.

Dwivedi, H., Burns, J., Chung, C., Clark, C. & Thiel, David V., 2010.
Mobile Application Security. Luettavissa: https://learning.oreilly.com/library/view/Mobile-Application-Security/9780071633567/. Luettu: 19.5.2022.

Esteves, J., Haro, G. d. & Ramalho, E. 2017. To Improve Cybersecurity, Think Like a Hacker.
MIT Sloan Management Review. Luettavissa: https://learning.oreilly.com/library/view/to-improve-cybersecurity/53863MIT58314. Luettu: 19.5.2022.

IF 2017. Kyberterminologiaa. Luettavissa:
https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/kyberterminologiaa. Luettu: 19.5.2022.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit.
Helsinki: Alma Talent. Luettu: 19.5.2022.

Järvinen, P. 2022. Yrityksen tietoturvaopas. 1. painos. Helsinki: Kauppakamari.
Luettu: 19.5.2022.

Kaspersky s.a. Cyber Security Risks: Best Practices for Working from Home and Remotely.
Luettavissa: https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe.
Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2021a. Ohjeet ja oppaat yksityishenkilöille. Luettavissa:
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille. Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2020a. Kyberturvallisuuden perussanasto. Luettavissa:
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto. Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2020b. Tee etätyöstä turvallista vinkkiemme avulla. Luettavissa:
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tee-etatyosta-turvallista-vinkkiemme-avulla.
Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2020c. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla. Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2020d. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon. Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2019a. Pornokiristyksiä runsaasti liikkeellä. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pornokiristyksia-runsaasti-liikkeella-ala-usko-huijarien-vaitteita. Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2021b. Tietoturvataidot – äh mikä mörkö! Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvataidot-ah-mika-morko. Luettu: 19.5.2022.

Kyberturvallisuuskeskus 2021c. Näin suojaudut tietomurroilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta. Luettu: 19.5.2022.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto, reliabilititeetti. Luettavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_2.html. Luettu: 20.5.2022.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto, Validiteetti. Luettavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_1.html. Luettu: 20.5.2022.

Suomidigi 2013. VAHTI Päätelaitteiden tietoturvaohje. Luettavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-52013-paatelaitteiden-tietoturvaohje. Luettu: 19.5.2022.

Speed, T. N., Nykamp, D., Speed, T., Anderson, J. & Nampalli, J. 2013. Mobile Security: How to Secure, Privatize, and Recover your Devices. Packt Publishing. Luettu: 19.5.2022.

Tietoarkisto s.a. Johdatus laadulliseen tutkimukseen ja verkkokäsikirjaan. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/johdatus-laadulliseen-tutkimukseen-ja-verkkokasikirjaan/. Luettu: 19.5.2022.

Valtiovarainministeriö 2010. VAHTI Sosiaalisen Median Tietoturvaohje. Luettavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-42010-sosiaalisen-median-tietoturvaohje. Luettu: 15.5.2022.

Viskari, N. 2017. Työntekijät – uhka yrityksen tietoturvalle. AMK-opinnäytetyö. Haaga-Helia ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma. Luettavissa: http://urn.fi/URN:NBN:fi:amk-201705178780. Luettu: 19.5.2022.

Yle 2021. Uudet tiedot: Vastaamon potilaiden tiedot olivat ehkä jopa vuosia suojaamatta netissä. Luettavissa: https://yle.fi/uutiset/3-11750220. Luettu: 19.5.2022.

Liitteet

Liite 1. Kyselyn julkaisu ja muistutus Yammer-viestintäpalvelussa

All Company

Teemu Heinonen – April 1 at 11:12 AM

Kysely henkilöstölle

Hei! Teen opinnäytetyötäni työntekijän tietoturvallisuuden hallinnasta. Pyytäisin kaikkia vastaamaan alla olevaan **anonyymiin** kyselyyn 1.5.2022 mennessä. Kyselyyn kuluu n. 5 minuuttia. Kyselyn täyttäminen ei vaadi kirjautumista mihinkään. Kyselyn tuloksia hyödynnetään opinnäytetyössä tietoturvaohjeistuksen muodostamiseen, sekä organisaatiossamme tuleviin tietoturvakoulutuksiin ja ohjeistuksiin.

Iso kiitos kyselyn täyttäneille!

[redacted]

cc: [redacted]

[redacted] – April 5 at 11:24 AM

Hyvä kysely, toivottavasti mahdollisimman moni täyttää tämän.

UNLIKE REPLY SHARE ...

You, [redacted] reacted to this

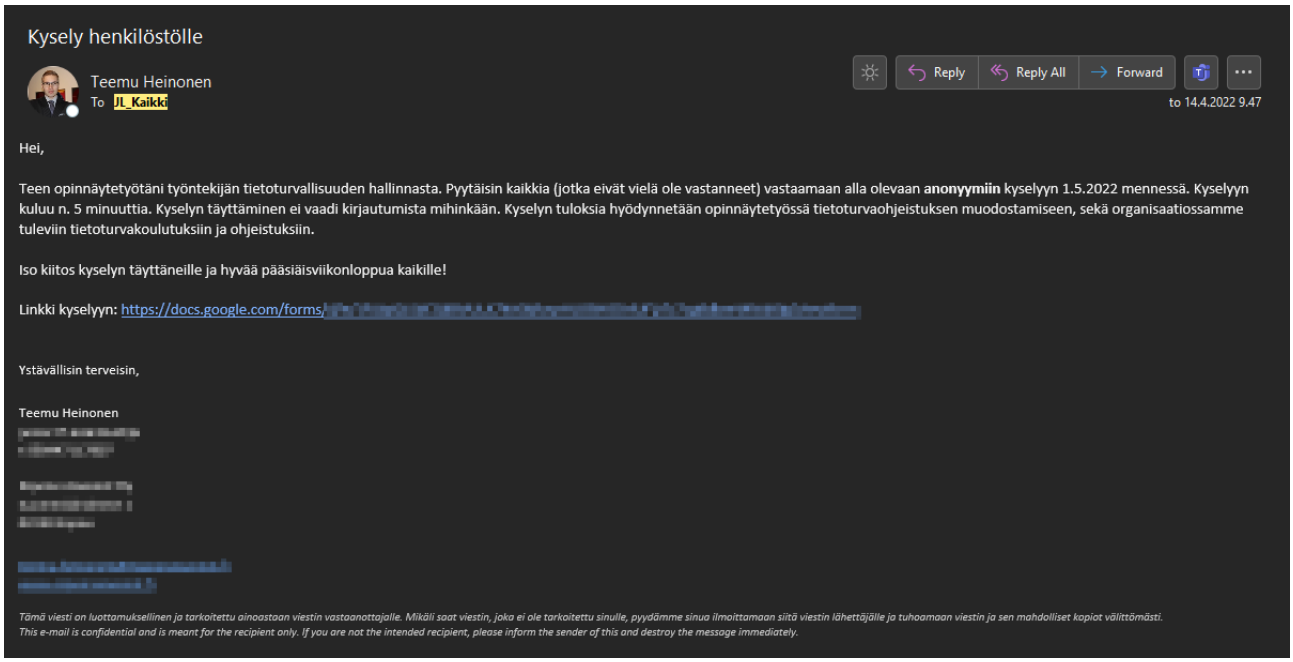
Teemu Heinonen – April 21 at 02:19 PM

Kyselyyn on vastannut nyt 60 henkilöä. Kiitos kaikille!
Vielä ehtii huhtikuun loppuun asti täyttämään kyselyn, mikäli ei vielä ole sitä tehnyt.

LIKE REPLY SHARE EDIT ...

[redacted] and 2 others reacted to this

Liite 2. Muistutusviesti sähköpostitse henkilöstölle



Kysely henkilöstölle

Teemu Heinonen
To JL_Kaikki

Reply | Reply All | Forward

to 14.4.2022 9.47

Hei,

Teen opinnäytetyötäni työntekijän tietoturvallisuuden hallinnasta. Pyytäisin kaikkia (jotka eivät vielä ole vastanneet) vastaamaan alla olevaan **anonyymiin** kyselyyn 1.5.2022 mennessä. Kyselyyn kuluu n. 5 minuuttia. Kyselyn täyttäminen ei vaadi kirjautumista mihinkään. Kyselyn tuloksia hyödynnetään opinnäytetyössä tietoturvaohjeistuksen muodostamiseen, sekä organisaatiossamme tuleviin tietoturvakoulutuksiin ja ohjeistuksiin.

Iso kiitos kyselyn täyttäneille ja hyvää pääsiäisviikonloppua kaikille!

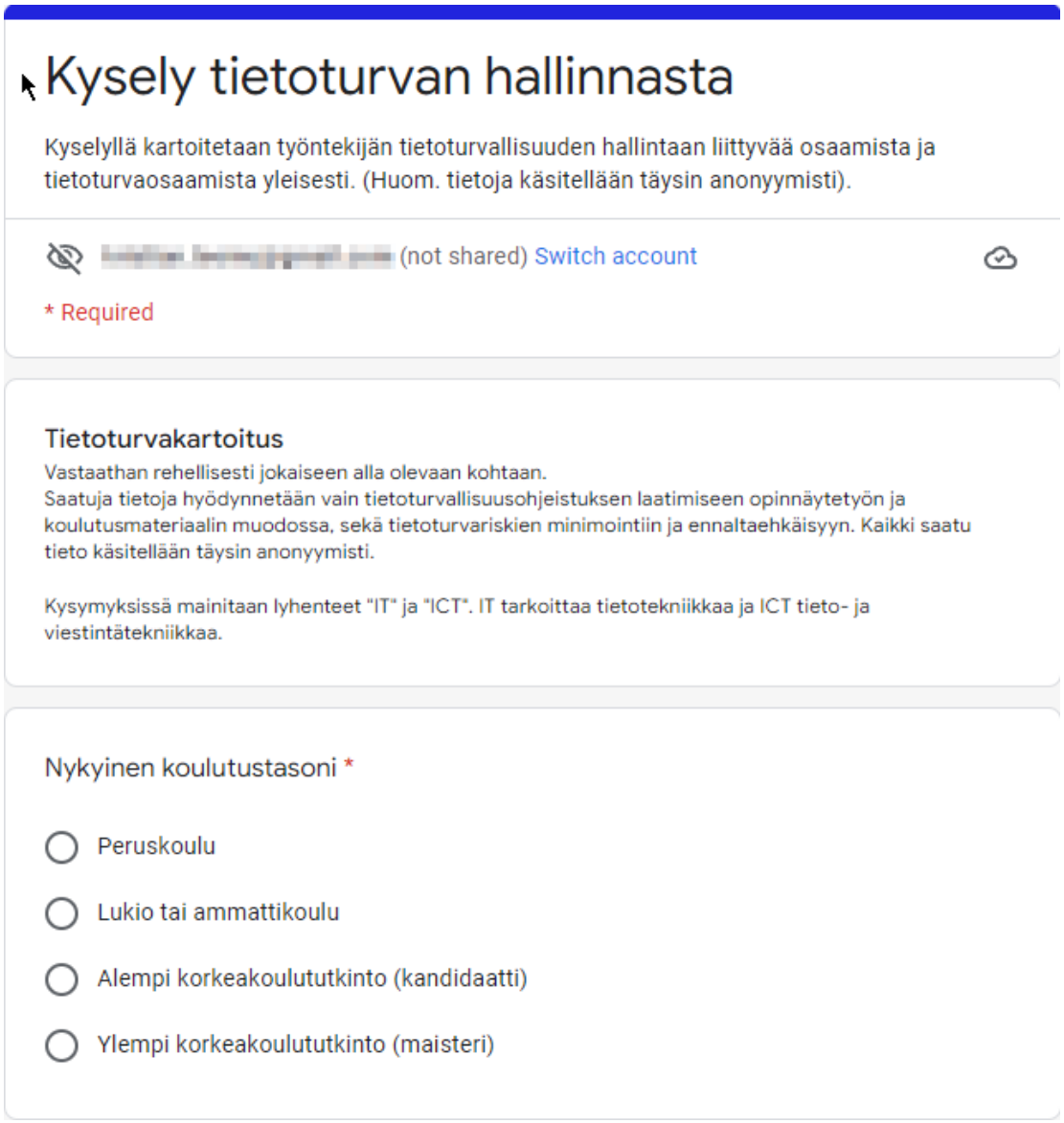
Linkki kyselyyn: https://docs.google.com/forms/

Ystävällisin terveisin,

Teemu Heinonen

Tämä viesti on luottamuksellinen ja tarkoitettu ainoastaan viestin vastaanottajalle. Mikäli saat viestin, joka ei ole tarkoitettu sinulle, pyydämme sinua ilmoittamaan siitä viestin lähettäjälle ja tuhoamaan viestin ja sen mahdolliset kopiot välittömästi.
This e-mail is confidential and is meant for the recipient only. If you are not the intended recipient, please inform the sender of this and destroy the message immediately.

Liite 3. Kyselylomake



Kysely tietoturvan hallinnasta

Kyselyllä kartoitetaan työntekijän tietoturvallisuuden hallintaan liittyvää osaamista ja tietoturvaosaamista yleisesti. (Huom. tietoja käsitellään täysin anonyymisti).

[redacted] (not shared) Switch account

* Required

Tietoturvakartoitus

Vastaathan rehellisesti jokaiseen alla olevaan kohtaan.
Saatuja tietoja hyödynnetään vain tietoturvallisuusohjeistuksen laatimiseen opinnäytetyön ja koulutusmateriaalin muodossa, sekä tietoturvariskien minimointiin ja ennaltaehkäisyyn. Kaikki saatu tieto käsitellään täysin anonyymisti.

Kysymyksissä mainitaan lyhenteet "IT" ja "ICT". IT tarkoittaa tietotekniikkaa ja ICT tieto- ja viestintätekniikkaa.

Nykyinen koulutustasoni *

- ○ Peruskoulu
- ○ Lukio tai ammattikoulu
- ○ Alempi korkeakoulututkinto (kandidaatti)
- ○ Ylempi korkeakoulututkinto (maisteri)

Olen *

- 16-25-vuotias
- 25-35-vuotias
- 35-45-vuotias
- 45-55-vuotias
- 55-60-vuotias
- Yli 60-vuotias

Tietoturvallisuuden tärkeys minulle työarjessani *

	1	2	3	4	5	
Ei lainkaan tärkeä	○	○	○	○	○	Erittäin tärkeä

Arvio tietoturvallisuuden osaamistasostani *

	1	2	3	4	5	
En tunne tietoturvallisuuteen liittyviä asioita tai käytäntöjä	○	○	○	○	○	Tunnen tietoturvallisuusasiat ja käytännöt erinomaisesti

Kaipaisin seuraavista osa-alueista eniten tai lisää tietoturvallisuusperehdytystä? *

- [ ] Tietokoneisiin liittyvä tietoturva
- [ ] Mobiililaitteisiin liittyvä tietoturva (puhelimet ja tabletit)
- [ ] Etätyöskentelyyn liittyvä tietoturva (etätyökäytännöt ja verkkolaitteiden tietoturva)
- [ ] Fyysinen tietoturvallisuus (salakuuntelu- tai katselu, varkaudet, sosiaalinen vaikuttaminen)
- [ ] Kaikki edellä mainitut tai tietoturvallisuus yleisesti
- [ ] En koe tarvitsevani lisää tietoturvaperehdytystä
- [ ] Other: _____

Olen joutunut tietojenkalastelun tai huijausyritysten kohteeksi työssä tai vapaa-ajalla (sähköposti, tekstiviesti, some tai nettisivut) *

- ( ) Kyllä
- ( ) Ei
- ( ) En tiedä

Olen joutunut identiteettivarkauden uhriksi *

- ( ) Kyllä
- ( ) Ei

Tietokoneestani tai puhelimestani on joskus löytynyt haittaohjelma *

- Kyllä
- Ei
- En tiedä

Suojaan puhelimeni ja tablettini sormenjälkitunnistuksella, suojakoodilla, kasvontunnistuksella tai kuviolla *

- Kyllä
- Ei

Käytän lähtökohtaisesti eri salasanaa kaikkiin palveluihin *

- Kyllä
- Ei

Käytän monimutkaisia salasanoja (yli 10 merkkiä pitkä, sis. isoja ja pieniä kirjaimia, erikoismerkkejä ja numeroita) *

- Kyllä
- Ei

Päivitän salasanoja omatoimisesti ja säännöllisesti *

- Kyllä
- Ei

Käytän kaksi- tai monivaiheista tunnistautumista, jos saatavilla *

- ◯ Kyllä
- ◯ Ei
- ◯ Vain pakotetusti

Käytän työkonettani vain työasioiden hoitamiseen *

- ◯ Kyllä
- ◯ Ei

Käytän työpuhelintani vain työasioiden hoitamiseen *

- ◯ Kyllä
- ◯ Ei

Vastaa vain jos olet saanut työnantajaltasi tabletin työkäyttöön* Käytän työtablettiani vain työasioiden hoitamiseen

- ◯ Kyllä
- ◯ Ei

Hoidan työasioitani myös omilla laitteillani *

- ◯ Kyllä
- ◯ Ei

Olen tullut huijatuksi jollain seuraavista keinoista työssä tai vapaa-ajalla *

- [ ] Tekstiviestihuijaus
- [ ] Sähköpostihuijaus
- [ ] Fyysinen sosiaalinen vaikuttaminen
- [ ] Verkkosivuhuijaus
- [ ] Tietojenkalastelu sosiaalisessa mediassa
- [ ] En ole tullut huijatuksi
- [ ] Other: _____

Lukitsen aina tietokoneeni, kun poistun työpisteeltä *

- ◯ Kyllä
- ◯ Ei

Säilytän salasanoja paperilla tai tekstitiedostoissa *

- [ ] Paperilla
- [ ] Tekstitiedostoissa
- [ ] Ei

Käytän salasanojen hallintaohjelmaa *

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

Tallennan salasanojani selaimeen tililleni *

- ◯ Kyllä
- ◯ Ei

Käytän työsähköpostiani myös työn ulkopuolella rekisteröityessäni eri palveluihin *

- ◯ Kyllä
- ◯ Ei

Olen saanut tietosuoja- ja tietoturvakoulutusta *

- ◯ Kyllä
- ◯ En
- ◯ En tiedä

Kotiverkkoni on turvallinen ja ajantasalla *

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

Osaan päivittää- tai tarkastaa tietokoneeni ajantasaiset Windows-päivitykset *

- ◯ Kyllä
- ◯ En
- ◯ En tiedä

Osaan päivittää mobiililaitteeni ohjelmat ja suorittaa ohjelmistopäivityksen *

- ◯ Kyllä
- ◯ En

Keskustelen salassa pidettävistä tiedoista julkisella paikalla tai julkisissa kulkuvälineissä *

- ◯ Kyllä
- ◯ Ei

Käsittelen salassa pidettäviä tietoja julkisella paikalla tai julkisissa kulkuvälineissä *

- ◯ Kyllä
- ◯ Ei

Jos vastasit edelliseen kysymykseen kyllä, niin miten varmistat, että salakatselua- tai kuuntelua ei tapahdu käsittelyyn liittyen?

- ☐ Käytän tietosuojakalvoa tietokoneessani
- ☐ Käytän VPN-yhteyttä
- ☐ Käytän vain omaa verkkoyhteyttä
- ☐ Valitsen sellaisen työpisteen, jossa fyysistä salakatselua ei voi tapahtua
- ☐ Kaikki edellä mainitut
- ☐ Käsittelen tietoja ilman verkkoyhteyttä
- ☐ En varmista
- ☐ Other: _____

Olen julkaissut sosiaaliseen mediaan työhöni liittyen kuvia, joista voi tunnistaa työssä käyttämiäni ohjelmia tai työympäristöni *

- ◯ Kyllä
- ◯ Ei
- ◯ Ehkä

Olen havainnut tietoturvan laiminlyöntiä työympäristössäni työntekijöiden toimesta *

- ◯ Kyllä
- ◯ Ei

Jos vastasit edelliseen kysymykseen "Kyllä" niin milloin havaitsit laiminlyöntiä? Voit jättää tämän kohdan tyhjäksi, jos et vastannut edelliseen myönteisesti.

- ☐ Viimeisen kuukauden sisällä
- ☐ Viimeisen vuoden sisällä
- ☐ 1-3 vuoden sisällä
- ☐ Yli kolme vuotta sitten

Vastaa tähän vain, jos vastasit edelliseen kysymykseen. Mihin laiminlyönti pääosin liittyi?

- ◯ Fyysiseen tietoturvallisuuteen (esim. laitteiden tai fyysisten dokumenttien hallinta, tai salassa pidettävistä tiedoista puhuminen)
- ◯ Sosiaalisen median sisältöön
- ◯ Työntekijän käyttämiin (ohjeistuksista poikkeaviin) työtapoihin
- ◯ Other: _____

Olen havainnut tietoturvan laiminlyöntiä työympäristössäni käytettävien laitteiden/ohjelmistojen ylläpidon tai yleisesti käytettävien työtapojen osalta *

- [ ] Laitteiden tai ohjelmistojen osalta
- [ ] Käytettyjen työtapojen osalta
- [ ] Molempien osalta
- [ ] En ole havainnut
- [ ] Other:

Jos vastasit edelliseen kysymykseen myönteisesti, niin milloin havaitsit laiminlyöntiä?

- [ ] Viimeisen kuukauden sisällä
- [ ] Viimeisen vuoden sisällä
- [ ] 1-3 vuotta sitten
- [ ] Yli kolme vuotta sitten

Huomaan, että toimistollamme on minulle täysin vieras henkilö, jolla ei ole myöskään saattajaa. Mitä teen asian suhteen? *

- [ ] Tiedustelen häneltä käynnin tarkoituksen ja varmistan kulkuluvan
- [ ] En mitään
- [ ] Kysyn mahdollisesti asiasta tietävältä taholta (esim. aulahenkilöltä), että onko kyseisellä henkilöllä lupa olla tiloissa
- [ ] Kysyn häneltä, että millä asialla hän on
- [ ] En tiedä

Käytän työkoneellani VPN-yhteyttä, jos käytän verkkoyhteyttä *

- ◯ Kyllä
- ◯ Ei
- ◯ Vain etätöissä

Jos huomaan tietoturvallisuuteen tai tietosuojaan liittyvän epäkohdan tai ongelman, niin miten minun tulisi toimia? *

- ◯ Asia ei ole minun vastuullani, joten en tee mitään asian suhteen
- ◯ Ilmoitan välittömästi tietosuojavastaavalle tai esimiehelleni
- ◯ Kerron asiasta kollegalleni
- ◯ Ilmoitan asiasta ulkoiselle IT-kumppanillemme
- ◯ En tiedä

Säilytän oheislaitteitani tai muita laitteitani (kun ne eivät ole aktiivisessa käytössä) *

- ◯ Lukitsemattomassa tilassa
- ◯ Lukitussa tilassa
- ◯ Kannan laitteitani aina mukana ja pidän niitä jatkuvasti valvottuna
- ◯ Säilytän laitteitani tai oheislaitteita monessa eri paikassa
- ◯ Other: _____

IT-kumppanimme tai ICT-osastomme työntekijä vaatii laitteeni tai käyttämäni järjestelmän salasanaa, miten toimin? *

- ◯ Kerron heille salasanani, jos he kertovat tarvitsevansa sitä
- ◯ En kerro heille salasanaani
- ◯ Kerron heille salasanani ja vaihdan sen toimenpiteen jälkeen
- ◯ En tiedä
- ◯ Other: _____

Säilytän henkilötietoja tai muita arkaluonteisia tietoja sisältäviä fyysisiä dokumentteja *

- ◯ Lukitsemattomassa tilassa
- ◯ Lukitussa tilassa
- ◯ En säilytä tai käsittele kyseisiä tietoja fyysisessä muodossa

Säilytän henkilötietoja tai muita arkaluonteisia tietoja digitaalisessa muodossa *

- ☐ Pääosin tietokoneellani työpöydällä
- ☐ Työpaikkani hallitsemassa suojatussa dokumenttivarastossa
- ☐ En säilytä kyseisiä tietoja
- ☐ En käsittele kyseisiä tietoja
- ☐ Pilvitallennustilassa
- ☐ Other: _____

Jos työpaikalta saamani laite häviää *

- [ ] Ilmoitan siitä välittömästi ICT-osastolle
- [ ] Yritän ensin itse etsiä laitteen miettimällä, että missä olen käyttänyt sitä viimeksi
- [ ] Yritän omatoimisesti löytää laitteeni käyttämällä Apple ID- tai Google-tilin tarjoamaa paikannuspalvelua
- [ ] Yritän saada puhelimeen yhteyden soittamalla
- [ ] Laitan sosiaaliseen mediaan tai muualle katoamisilmoituksen, jotta puhelin löytyisi
- [ ] Yritän itse etsiä puhelimen edellä mainituilla yhdellä tai useammalla tavalla, ilmoittamatta siitä ICT-osastolle
- [ ] Other: _____

Mitä voin pahimmassa tapauksessa menettää, jos laiminlyön tietoturvaani? *

- [ ] Rahaa
- [ ] Arkaluontoista tietoa
- [ ] Nettiyhteyden
- [ ] Maineen
- [ ] Henkilöllisyyden
- [ ] Kaikki edellä mainitut
- [ ] En mitään

Iso kiitos vastauksistasi! Niitä hyödynnetään tietoturvan kehittämiseen organisaatiossamme.

Submit Clear form