Lari Ruutiniemi

HOXHUNT-TIETOJENKALASTELUKOULUTUS VAIKUTTAA POSITIIVISESTI MUIHINKIN TURVALLISUUDEN OSA-ALUEISIIN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Ruutinimi, Lari
Hoxhunt-tietojenkalastelukoulutus vaikuttaa positiivisesti muihinkin turvallisuuden osa-alueisiin
Jyväskylä: Jyväskylän yliopisto, 2024, 68 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tietojenkalastelu on merkittävä tietoturvariski organisaatioille, ja sen torjumiseksi tarvitaan teknisten ratkaisujen lisäksi työntekijöiden kouluttamista. Hoxhunt on pelillistetty tietojenkalastelukoulutus, joka lähettää tietojenkalasteluviestien kaltaisia sähköposteja työntekijöiden työsähköposteihin. Tässä tutkielmassa tarkastellaan Hoxhunt-tietojenkalastelukoulutuksen vaikutuksia Verohallinnon työntekijöihin, sekä sitä vaikuttaako Hoxhunt tietojenkalastelulta suojautumisen lisäksi myös rakentavasti muihin turvallisuuden osa-alueisiin. Tutkimuskysymykset ovat: ovatko Verohallinnon työntekijät kokeneet Hoxhunt tietojenkalastelukoulutuksen vaikuttaneen heidän käyttäytymiseensä, miten Hoxhunt on vaikuttanut Verohallinnon työntekijöiden käyttäytymiseen ja onko Hoxhuntilla positiivisia vaikutuksia myös muiden turvallisuuden osa-alueiden osalta? Tutkimusmetodina käytettiin monimenetelmällistä tutkimusta. Määrällinen kyselytutkimus suoritettiin Verohallinnon työntekijöille ja lisäksi suoritettiin laadullinen Verohallinnon virkamiehen haastattelu. Analyysimenetelminä käytettiin ristiintaulukointia, teemoittelua ja sisältöanalyysia. Tulokset osoittavat, että Hoxhunt on parantanut tietojenkalastelun tunnistuskykyä ja raportointia. Hoxhunt on lisännyt kykyä arvioida sähköpostin lähettäjän luotettavuutta, sekä sähköpostin linkkien ja liitteiden turvallisuutta. Lisäksi koulutus on lisännyt huomiota myös muissa turvallisuuden osa-alueissa, kuten turvallisuushäiriöistä ilmoittamisessa ja hallinnollisessa turvallisuudessa, sekä henkilöstö- ja toimitilaturvallisuudessa. Koulutuksen myötä yleinen varovaisuus on kasvanut ja kiinnostus tietoturvallisuuta kohtaan on noussut myös vapaa-ajalla. Tuloksissa korostuu erityisesti se, että koulutuksella on ollut suurimmat myönteiset vaikutukset yli 50-vuotiaisiin ja naisiin. Johtopäätöksenä myös on, että kouluttamalla yhtä turvallisuuden osa-aluetta voidaan vaikuttaa myös muiden turvallisuuden osa-alueiden kehittämiseen ja turvallisuuskulttuuriin.

Asiasanat: tietojenkalastelu, sosiaalinen manipulointi, tietoturvallisuus, tietoturvakoulutus

ABSTRACT

Ruutiniemi, Lari
Hoxhunt phishing training affects positively also in other areas of security
Jyväskylä: University of Jyväskylä, 2024, 68pp.
Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

Phishing is a significant cybersecurity risk for organizations, and combating it requires not only technical solutions but also employee training. Hoxhunt is a gamified phishing training program that sends phishing-like emails to employees' work email accounts. This thesis examines the effects of Hoxhunt phishing training on the employees of the Finnish Tax Administration and explores whether Hoxhunt, in addition to improving protection against phishing, also contributes positively to other areas of security. The research questions are: Have employees of the Finnish Tax Administration perceived that the Hoxhunt phishing training has influenced their behavior? How has Hoxhunt affected their behavior? And does Hoxhunt have positive effects on other areas of security as well? A mixed-methods approach was used as the research methodology. A quantitative survey was conducted among the employees of the Finnish Tax Administration, complemented by a qualitative interview with an official from the organization. Data analysis methods included cross-tabulation, thematic analysis, and content analysis. The results show that Hoxhunt has improved the ability to recognize and report phishing attempts. Additionally, the training has had positive effects on other areas of security, such as physical security and personnel security. Hoxhunt has enhanced employees' ability to assess the reliability of email senders, links, and attachments. General caution has increased, and interest in cybersecurity has grown. Notably, the effects of the training were most significant among employees over the age of 50 and women. The findings also suggest that training in one area of security can positively impact the development of other areas of security and strengthen the overall security culture. The results show that Hoxhunt has increased employee attention to phishing and reporting security incidents. Hoxhunt has increased the ability to assess the reliability of the email sender address, as well as the security of email links and attachments. In addition, the training has also increased attention to other areas of security, such as reporting security incidents and administrative security, as well as personnel and premises security. As a result of the training, general caution has increased and interest in information security has also increased in free time. The results particularly emphasize that the training has had the greatest positive effects on people over 50 years of age and women. The conclusion is also that by training one area of security, the development of other areas of security and the security culture can also be influenced.

Keywords: phishing, social engineering, information security, cybersecurity training

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Verohallinnossa otettiin tietoturvallisuuden parantamiseksi käyttöön vuonna 2021 Hoxhunt-tietojenkalastelukoulutus, joka harjaannuttaa koulutettavan tunnistamaan tietojenkalastelusähköposteja. Hoxhunt lähettää koulutettavan työsähköpostiin virallisen organisaatioviestinnän kaltaisia huijausviestejä, jotka koulutettavien tulisi tunnistaa ja raportoida sähköpostin liiteohjelmalla. Onnistuneen raportoinnin jälkeen koulutettavalla on mahdollisuus suorittaa mikrokoulutus vaihtuvasta tietojenkalasteluun liittyvästä aiheesta.

Tällä tutkimuksella pyritään selvittämään, minkälainen vaikutus Hoxhuntilla eli pelinkaltaisella tietojenkalastelukoulutuksella on Verohallinnon työntekijöihin. Parantaako koulutus tietoturvallisuutta koulutettavien itsensä mielestä ja jos parantaa, voiko se vaikuttaa positiivisesti myös muihin turvallisuuden osaalueisiin? Tutkimusmenetelmä on monimenetelmällinen ja siinä suoritettiin Verohallinnon Hoxhunt-palveluomistajan haastattelu ja tehtiin kyselytutkimus Verohallinnon työntekijöille.

Tietojenkalastelu aiheuttaa yrityksille mittavia taloudellisia vahinkoja ja se on yksi suurimmista riskeistä. IBM Securityn vuoden 2023 raportin mukaan, tietojenkalastelu oli suurin yksittäinen tietoturvaloukkauksissa käytetty hyökkäysvektori. Noin joka kuudes tietoturvaloukkaus (16 %) oli aiheutunut ensisijaisesti tietojenkalastelusta ja sen taloudelliset vaikutukset olivat tarkastelujakson toiseksi suurimmat (4,8 milj. $) ja ainoastaan sisäpiirin aiheuttamat vahingot olivat tätäkin suuremmat (4,9 milj. $). Raportissa tarkasteltiin 553 organisaatioon kohdistuneita tietoturvaloukkauksia maaliskuun 2022 ja maaliskuun 2023 välisenä aikana. (IBM Security, 2023).

Tarve vastata ihmisen aiheuttamaan riskiin on olemassa. Tietojärjestelmiä rakennettaessa keskitytään parantamaan turvallisuutta teknisillä ratkaisuilla, ja ihmisten valintojen rooli jää usein vähemmälle huomiolle. Teknisillä ratkaisuilla ei kuitenkaan voida riittävästi vaikuttaa ihmisen itsensä aiheuttamaan riskiin. Järjestelmä voi esimerkiksi vaatia salasanan olevan tietyn mittainen merkkijono, ja näin ihminen pystytään "pakottamaan" tietoturvallisempaan ratkaisuun. Kuitenkaan pakolla ei voida juurikaan vaikuttaa käyttäjän huolellisuuteen salasanansa säilyttämisen tai luovuttamisen suhteen. Tietoturvan kokonaisuuteen

tarvitaan siis yhdistelmä teknistä tietoturvallisuutta ja käyttäjän turvallisuustietoisuutta. Tässä tutkielmassa keskitytään näistä jälkimmäiseen.

Kiinnostukseni ihmisten käyttäytymistä kohtaan kumpuaa voimakkaasti omasta taustastani. Olen kouluttanut ihmisiä noin 15 vuoden ajan erilaisiin aihepiireihin liittyen. Kokemukseni mukaan jakamalla tietoa ja osallistamalla voidaan vaikuttaa ihmisten asenteisiin ja parantaa turvallisuuskulttuuria. Mitä enemmän ihmisellä on tietoa ja erityisesti henkilökohtaista tunnetta vaikuttamisen mahdollisuudesta, sitä enemmän hän kokee olevansa aktiivinen toimija ja todellisuudessa osallistuu enemmän. Parhaat tulokset saavutin silloin, kun osallistuja koki, että hänen omilla mielipiteillään ja tekemisellään oli merkitystä. Kokemukseni mukaan osallistamalla ihmisiä voidaan vaikuttaa kokonaisvaltaisesti heidän käyttäytymiseensä jopa koulutettavan aiheen ulkopuolella, jos ihmisen itsensä vaikutusmahdollisuuksia korostettiin koulutuksessa. Vaikka Hoxhunt ei lupaa saavansa aikaan vaikutuksia tietojenkalastelulta suojautumisen ulkopuolella, vaikuttaa se osallistavan käyttäjiään tavalla, joka saattaa vaikuttaa myös tietojenkalastelukoulutusta laajemmalle. Tällä tutkimuksella haluan selvittää, saanko akateemista vahvistusta omalle näkemykselleni ihmisten osallistamisen tehokkuudesta vai en.

Tutkielma muodostuu seuraavista luvuista. 1. Johdanto, 2. kirjallisuuskatsaus, 3. tutkimusmenetelmät, 4. tutkimuksen tulokset, 5. johtopäätökset ja 6. pohdinta. Johdannon lopussa käydään läpi keskeiset käsitteet, sekä kuvataan Verohallinto ja Hoxhunt yleisellä tasolla. Kirjallisuuskatsauksessa perehdytään tietoturvallisuuden määritelmän lähtökohtiin ja siihen, että ihminen on merkityksellisessä roolissa tietoteknisten ratkaisujen rinnalla. Lisäksi määritellään tietojenkalastelu ja siinä käytetyt toimintatavat, sekä esimerkkitapausten kautta kuvataan tietojenkalastelua käytännössä. Luvun lopussa kuvataan sosiaalisen manipuloinnin merkitys tietojenkalastelussa ja käydään läpi keinoja tietojenkalastelun torjumiseksi. Tutkimusmenetelmät-luvussa kuvataan käytetty tutkimusmenetelmä, tutkimuskysymykset, hypoteesit, aineiston kerääminen ja analysointi, sekä pohditaan tutkimuksen luotettavuutta ja eettisyyttä. Tutkimuksen tulokset -luvussa käydään läpi saavutetut tulokset ja verrataan esimerkiksi iän ja sukupuolen vaikutusta tuloksiin. Johtopäätökset-luvussa esitetään tulokset vastaamalla tutkimuskysymyksiin ja suhteutetaan ne taustakirjallisuuteen, arvioidaan tulosten käytettävyyttä ja rajoitteita. Lopuksi Pohdinta-luvussa arvioin tutkimuksen käytännöllistä ja tieteellistä merkitystä ja esitän jatkotutkimusaiheita.

1.1 Keskeiset käsitteet

Haittaohjelma (engl. Malicious Software tai Malware). Haittaohjelma on ohjelma, joka tarkoituksellisesti aiheuttaa tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat esimerkiksi virukset, madot ja troijalaiset sekä näiden yhdistelmät. (Sanastokeskus, 2018, s. 31).

Sosiaalinen manipulointi (engl. Social Engineering). Sosiaalisella manipuloinnilla tarkoitetaan kohteena olevan henkilön kannalta positiivista tai negatiivista toimintaa. Sosiaalinen manipulointi voidaan määritellä aktiivisena toimintana, missä sosiaalisen vuorovaikutuksen keinoin tarkoituksena on saada ihminen tai organisaatio tekemään jonkin merkityksellisen teon (Hadnagy & Wilson, 2020, luku 3 09.13; Niettaanmäki ym., 2021, s. 141). Sillä toisaalta voidaan myös tarkoittaa kohteen kannalta pelkästään negatiivista toimintaa. Tietoturvallisuuden asiayhteydessä sosiaalisessa manipuloinnissa, hyökkääjä pyrkii käyttämään hyödykseen jokaisen tietojärjestelmän heikkoutta eli ihmisen psykologiaa. Eri kanavien, kuten puhelinsoittojen ja sosiaalisen median avulla hyökkääjä pyrkii saamaan ihmisen luovuttamaan itse arkaluonteisia tietoja (Bossomaier ym., 2019, s. 87).

Tietojenkalastelu (engl. Phishing). Tietojenkalastelu on yritys anastaa kohteen henkilökohtaisia tietoja käyttämällä tekaistua sähköpostiviestiä. Tarkoitus on esiintyä kohteen näkökulmasta laillisena ja luotettavana toimijana ja huijata hänet paljastamaan yksityisiä tietoja kuten pankkikortin numero ja salasana, joita voidaan hyväksikäyttää rahanhankkimistarkoituksessa. Tietojenkalastelusähköposti saattaa sisältää linkin aidonkaltaiselle tekaistulle verkkosivulle, johon kyseiset tiedot tulisi syöttää. (James, 2005, s. 2, 10). Whitty & Young (2016, luku 12.1) mukaan tietojenkalastelussa on kyse sosiaalisen manipuloinnin ja teknisen harhauttamisen yhdistelmästä, jossa usein käytetään tunnettuja pankki- tai muiden organisaatioiden tietoja luottamuksen rakentamiseksi. Sähköpostin lisäksi tietojenkalasteluviestejä voi esiintyä myös sosiaalisessa mediassa. Lisäksi tietojenkalasteluviesti voi yrittää saada kohde klikkaamaan linkkiä tai siirtymään sivustolle, mihin on upotettu jokin haittaohjelma.

Tietoturvaloukkaus (engl. Security Breach). Tietoturvaloukkauksella tarkoitetaan oikeudetonta puuttumista tietoon tai tietojärjestelmään. (Sanastokeskus, 2018, s. 17).

1.2 Verohallinto

Verohallinnosta annetun lain (503/2010) 1§ mukaan: ”Verotusta varten on valtiovarainministeriön alainen Verohallinto, jonka virka-alueena on koko maa”. Verohallinto itse kuvaa internetsivuillaan toimintaansa seuraavasti: Verohallinnon tehtävänä on toteuttaa verotus oikean määräisenä ja oikeaan aikaan, ja siten varmistaa yhteiskunnan toimintojen rahoitus. Verot välitetään kuukausittain eteenpäin yhteiskunnan palveluja ylläpitäville tahoille: valtiolle, kunnille, Kansaneläkelaitokselle, seurakunnille ja metsänhoitoyhdistyksille. Tärkein Verohallinnon sähköinen palvelukanava on OmaVero-palvelu. (Verohallinto 2023a). OmaVero on Verohallinnon sähköinen asiointipalvelu, missä käyttäjät voivat ilmoittaa verotukseen liittyviä asioista ja saada tiedoksi esimerkiksi verotuspäätöksiä. (Verohallinto 2023b). OmaVeroa on käytetty tietojenkalastelun kulissina (Verohallinto, 2023c; luku 2.2.3). Vuoden 2022 lopussa Verohallinnolla oli toimipaikkoja 55 paikkakunnalla eri puolella Suomea.

1.3 Hoxhunt

Hoxhunt Oy on suomalainen vuonna 2016 perustettu tietoturvayritys, joka tarkoituksena on pienentää ihmisten aiheuttamaa tietoturvariskiä. Hoxhunt tarjoaa yrityksille tietojenkalastelukoulutusta, jossa työntekijöiden sähköposteihin lähetetään oikeankaltaisia tietojenkalasteluviestejä. Yrityksen työntekijöiden tehtävänä on tunnistaa tietojenkalastelu ja raportoida se sähköpostin raportointipainikkeesta. Raportoinnin jälkeen työntekijälle ilmoitetaan, oliko kyse Hoxhuntin lähettämästä viestistä, ja jos oli, hänelle tarjotaan vaihtuva mikrokoulutus tietojenkalastelun jostakin osa-alueista. Koulutus on rakennettu pelin kaltaiseksi ja koulutettava voi kerätä pisteitä ja saavuttaa edistymistä kuvaavia tasoja tunnistaessaan viestejä ja suorittaessaan mikrokoulutuksia. Omaa edistymistään koulutettava voi seurata henkilökohtaisesta näkymästä, jossa on nähtävissä suoritettujen koulutusten määrä ja niistä kerätyt pisteet. Hoxhuntin raportointipainikkeen avulla on myös mahdollista raportoida oikeita tietojenkalastelu tai huijausviestejä käyttäjäorganisaation turvallisuustoiminnon käsiteltäväksi (Hoxhunt, 2023). Yrityksen Hoxhunt Oy liikevaihto oli 7,1 miljoonaa euroa vuonna 2022 ja se työllisti 86 henkilöä (Suomen Asiakastieto, 2023).

2 KIRJALLISUUSKATSAUS

Kirjallisuuskatsauksessa perehdytään tutkittavan ongelman taustoihin, määritellään oleelliset käsitteet, kuten tietoturvallisuus ja tietojenkalastelu, sekä osoitetaan, miten ihminen on kirjallisuuden perusteella oleellinen osa tietojärjestelmien turvallisuutta. Kirjallisuuden perusteella käyttäjien kouluttaminen on olennaista tietojenkalastelulta suojautumisessa. Tietojenkalastelun määrittelyssä esitellään kyberhyökkäys- ja tietojenkalastelumalleja ja esimerkkitapausten kautta kuvataan tietojenkalastelun merkittävyyttä. Tietojenkalastelusta ei ole tehty tutkimuksia oman tutkimukseni näkökulmasta. Ei ole aiemmin tutkittu sitä, miten tietojenkalastelu vaikuttaa muihin turvallisuuden osa-alueisiin. Kuvaan suppeasti aiempia tutkimuksia, joissa näkökulmana on ollut erityisesti huomion määrä tietojenkalastelulta suojautumisessa. Tämä näkökulma on oleellinen huomioida kyselytutkimuksessa, jossa selvitetään Hoxhuntin vaikutuksia huomion määrään eri turvallisuuden osa-alueissa.

2.1 Tietoturvallisuus

Tunnetuin tietoturvallisuuden malli kirjallisuudessa on CIA-malli (engl. CIA Triad). Mallissa tietoturvallisuus koostuu kolmesta osa-alueesta, jotka ovat tiedon luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability). Kaikkien osa-alueiden tulisi olla hallinnassa, jotta tietoturvallisuus toteutuu. Luottamuksellisuus pyrkii estämään tiedon luvattoman käytön eli tieto ei saa vahingossa joutua tai sitä ei saa tahallisesti luovuttaa taholle, jolla ei ole oikeutta sen hallintaan. Eheys pyrkii estämään tiedon tahatonta tai luvatonta muuttamista. Saatavuus puolestaan pyrkii takaamaan, että tieto on kaikkien tarkoitettujen tahojen käytettävissä. (Raggad, 2010, s. 20; ISO27001, 2017, luku 5, Hakala ym., 2006, s. 4).

Raggad (2010, s. 21) kritisoi CIA-mallia siitä, että se ei riittävästi ota huomioon liiketoiminnan tarpeita kokonaisuutena, vaan sen keskittyy liikaa turvallisuuden tavoitteiden kuvaamiseen. Kritiikki kulminoituu siihen, että vaikka turvallisuuden tarpeet saavutettaisiin, voisivat silti liiketoiminnan tarpeet jäädä

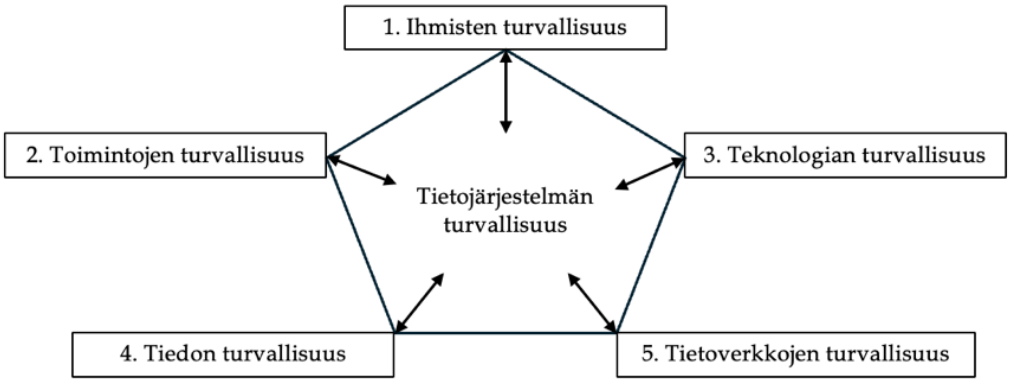
saavuttamatta. CIA-mallin kolme turvallisuuden tavoitetta eivät riittävästi kuvaa liiketoiminnan turvaamisen kokonaisuutta ja malliin tulisi lisätä neljäs tavoite, tietoturvallisuuden johtaminen. CIA-mallia tulisi laajentaa ottamalla mukaan lisää turvallisuuden tavoitetiloja, huomioida liiketoiminnan tavoitteet, sekä tunnistetut riskit ja uhat.

Raggad (2010, s. 22–23) ehdottaa kahden uuden tavoitteen, pääsynvalvonnan (Authentication) ja kiistämättömyyden (Non-Repudiation) mukaan ottamista riskienhallinnan kokonaisuuteen. Pääsynvalvonnalla tarkoitetaan käyttäjien tunnistamista ennen kuin pääsyoikeus järjestelmään tai sen osaa myönnetään. Yleisesti tämä tarkoittaa käyttäjätunnukseen ja salasanaan perustuvaa tunnistautumista. Toisena lisäyksenä on kiistämättömyys, jonka tarkoituksena on digitaalisesti varmistaa, että tiedonsiirron molemmat osapuolet ovat tunnistettuja ja luotettavia. Riskillä tarkoitetaan, että jokin epätoivottu tapahtuma, kuten tietovuoto tai korruptoituminen tapahtuu aiheuttaen taloudellisia tappioita. Riskinhallinnalla tarkoitetaan liiketoiminnan kannalta oleellisten riskien tunnistamista, arvioimista ja käsittelyä. Jos jonkin toiminnon riski on hyväksyttävää riskiä suurempi, tulisi siihen kohdistaa lisää toimenpiteitä riskin pienentämiseksi. Riskinhallinnan tulisi olla liiketoiminnan eri osa-alueiden tuntevien ihmisten suorittama ja siihen kuuluu uhkien ja haavoittuvuuksien tunnistaminen, sekä käytössä olevien suojaamistoimien kartoitus. Raggadin paranneltu malli, Security Star, on esitetty kuviossa 1.

KUVIO 1 Security Star -malli (Raggad, 2010, s. 22-23).

Raggadin (2010, s. 10–11) jatkaa tietoturvallisuuden mallintamista ottamalla huomioon kokonaisuuden, jossa ihminen on merkitsevässä roolissa. Raggadin mukaan tietojärjestelmän turvallisuus koostuu viidestä toisiinsa sidoksissa olevasta turvallisuuden osa-alueesta: ihmisistä (engl. People Security), toiminnoista (engl. Security of Information System Activities), tiedosta (Data Security), teknologiasta (Technology Security) ja tietoverkoista (Network Security). Sen lisäksi, että samassa digitaalisessa toimintaympäristössä olevat osat ovat yhteydessä toisiinsa, ne ovat vuorovaikutussuhteissa itsensä kanssa. Tietoturvallinen digitaalinen

toimintaympäristö muodostuu näiden osien kokonaisuudesta ja yhdessä nämä osa-alueet muodostavat tietototurvallisen järjestelmän. Seuraavaksi kuvataan tarkemmin Raggadin tietoturvallisuuden mallin osia. Raggadin tietoturvallisuuden mallin on kuvattu kuviossa 2.



KUVIO 2 Raggadin (2010, s. 10–11) tietoturvallisuuden malli.

Ihmiset ovat osa tietojärjestelmää. Ihmiset ovat vuorovaikutuksessa keskenään ja he luottavat toisiin ihmisiin ja muihin järjestelmän osiin omien tehtäviensä suorittamiseksi. Ihmisten tuotteliaisuus on lopulta tulosta muiden osa-alueiden turvallisuuden toteutumisesta. Jos jokin osa-alueen luottamuksellisuus, eheys tai saatavuus vaarantuu, se voi vaarantaa alkuperäisen tehtävän suorittamisen ja johtaa tehokkuuden laskuun. Turvallisuuskulttuurilla tarkoitetaan ajan kanssa muodostuvaa inhimillistä toimintaa heidän oman toimintansa suojaamiseksi. Ihmiset pyrkivät suojaamaan oman toimintansa ja löytämään turvallisia toimintatapoja. Vahva turvallisuuskulttuuri voi pelastaa tilanteessa, jossa varsinaista koulutusta ei ole tietyn turvallisuushäiriön hoitamiseksi. Esimerkiksi vahva kulttuuri voi auttaa vaarallisen toiminnan tunnistamisessa ja eteenpäin ilmoittamisessa. Toisaalta heikon turvallisuuskulttuurin tilanteessa ihmiset saattavat tiedostamattaan toimia turvallisuusperiaatteiden vastaisesti, esimerkiksi luovuttaa tietoa vahingossa väärälle henkilölle. Turvallisuusperiaatteiden vahvistamisen tulisi lähteä liikkeelle kouluttamisesta. Jos turvallisuusperiaatteiden taustoja ei riittävästi kouluteta, periaatteet voivat jäädä pinnallisiksi. Kouluttamisen kautta tulisi luoda pohja turvallisuusperiaatteiden omaksumiseksi. (Raggad, 2010, s. 12–13).

Toiminnot (engl. System Activities) tarkoittavat organisaation turvallisuusperiaatteita, prosesseja, standardeja ja ohjeita. Organisaation turvallisuusperiaatteissa määritellään, miten tietojärjestelmän osat turvataan. Sen tulisi määritellä kaikkia osallistujia koskevat turvallisuuden tavoitteet aina käyttäjästä tietojärjestelmän omistajaan saakka. Kaikkien osallistujien tulisi aktiivisesti osallistua turvallisuusperiaatteiden määrittämiseen, tunnistaa oma roolinsa tietojärjestelmän suojaajana ja samalla valvoa periaatteiden noudattamista. Hyvästä tietoturvaperiaatteesta on helppo viestiä ja sitä on helppo päivittää ja valvoa. (Raggad, 2010, s. 13).

Datalla (engl. Data Resources) tarkoitetaan kaikkea tietojärjestelmän ihmisten tai ohjelmien välittämää tietoa, josta tuotetaan informaatiota järjestelmän päätöksenteon tueksi. Nämä tiedot voivat olla vain käsitteellisiä ja niillä ei ole todellista muotoa, mutta niillä on arvoa tietojärjestelmän kannalta. Teknologialla (engl. Technology) tarkoitetaan työkaluja, koneita, sähkölaitteita ja tietämystä, joka liittyy laitteiden käyttämiseen. Tietoverkoilla (engl. Network) tarkoitetaan kaikkia fyysisiä resursseja, jotka liittyvät tietoverkkojen infrastruktuuriin, rakennuksiin ja välineistöön. (Raggad, 2010, s. 14–16).

2.2 Tietojenkalastelu

> ”Kun muut reiät on pikkuhiljaa tukittu, hyökkääjät ovat siirtyneet tekniikkaan, joka toimii aina: käyttäjien huijaamiseen” - Mikko Hyppönen (2021, s. 73).

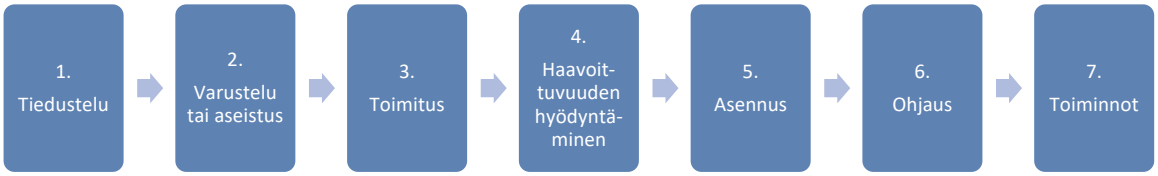
Tietojenkalastelu on internethuijaus, jossa tarkoituksena on käyttäjän tunnistetietojen saaminen hyökkääjän haltuun. Tietojenkalasteluviestit ovat yleensä ilmoituksia pankeilta, maksupalveluilta ja muilta palveluntoimittajilta tai organisaatioilta. Ilmoitus yrittää rohkaista käyttäjän kiireellisesti syöttämään tai päivittämään henkilökohtaiset tietonsa hyökkääjän järjestelmään. Kiireellisyyden tunnetta pyritään luomaan esimerkiksi kertomalla valheellinen tarina käyttäjän tietojen katoamisesta tai palvelun poistumisesta. (Kaspersky, 2023a). Hyökkääjä voi tekeytyä yrityksen johtajaksi, työkaveriksi tai kiinteistön välittäjäksi (SocialEngineer, 2023). Toimintatapana on kiireellisyyden tunteen luominen esimerkiksi seuraavalla tavalla: ”*Jos et toimita henkilökohtaisia tietojasi tämän viikon aikana, tilisi suljetaan*”. Ironisesti tekniikkana voi myös olla vetoaminen tietojenkalastelun vastaiseen toimintaan: ”*Jos haluat suojautua tietojenkalastelua vastaan, klikkaa linkkiä ja syötä käyttäjätunnuksesi ja salasanasi*”. (Kaspersky, 2023a).

Kasperskyn (2023a) mukaan keskimääräinen tietojenkalastelusivuston elinaika on viisi päivää. Tämä johtuu siitä, että nykyaikaiset tietojenkalastelufiltterit, jotka vertaavat huijausviestissä olevaa URL-linkkiä tiedossa olevien tietojenkalastelusivustojen osoitteisiin eli musta listoihin (engl. Black List), saavat nopeasti tiedot uusimmista huijaussivuistoista ja pystyvät estämään sivustoille siirtymisen. Tämän takia huijarit joutuvat jatkuvasti rekisteröimään uusia sivustoja.

2.2.1 Kyberhyökkäys- ja tietojenkalastelumallit

Tietojenkalastelu voi olla osa kyberhyökkäystä, minkä vaiheita on mallinnettu useilla eri tavoilla. Tässä luvussa kuvataan yleisimmät kyberhyökkäyksen etenemiseen liittyvät Cyber Kill Chain ja MITRE ATT&CK viitekehykset. Esimerkkinä käytetään Suomen tietosuojavaltuutetun kuvausta tietojenkalastelun prosessista, jota peilataan Cyber Kill Chainin vaiheisiin. Cyber Kill Chainin vaiheita kuvataan tässä tutkielmassa tarkemmin ja MITRE ATT&CK viitekehystä yleisemmällä tasolla.

Lockheed Martin julkaisi vuonna 2011 kyberhyökkäyksen etenemistä kuvaavan ylätason viitekehyksen nimeltä Cyber Kill Chain, jossa hyökkäyksen eteneminen on kuvattu seitsemän perättäisen toisiaan seuraavan vaiheen kautta. (BlackBerry, 2023). Vaiheet ovat tiedustelu, varustelu tai aseistaminen, toimitus, haavoittuvuuden hyödyntäminen, asennus, ohjaus ja toiminnot (Lockheed Martin, 2023). Cyber Kill Chain -malli on kuvattu kuviossa 3.



KUVIO 3 Cyber Kill Chain -malli (Lockheed Martin, 2023).

Cyber Kill Chain mallin kyberhyökkäys alkaa tiedusteluvaiheesta (1), missä hyökkääjä etsii hyökkäyksen toteuttamisen kannalta arvokasta tietoa kohteesta useita lähteitä käyttäen. Tiedustelun kohteena voi olla esimerkiksi sähköpostiosoitteiden hankkiminen tietojenkalastelua varten. Varustelu- tai aseistusvaiheessa (2) tiedusteluun perustuen valitaan ja valmistellaan hyökkäykseen sopivat työkalut, esimerkiksi haittaohjelmat, joilla haluttu vaikutus voidaan toteuttaa. Toimitusvaiheessa (3) hyökkääjä toimittaa valmistellun haitallisen sisällön sähköpostin, internetsivun tai USB-laitteen kautta kohteeseen. Tämän jälkeen haavoittuvuutta hyödynnetään (4) tavoitteena päästä ajamaan hyökkääjän koodia kohteen tietojärjestelmässä. Haittaohjelma asennetaan (5) tietojärjestelmään, jotta se saadaan hyökkääjän lopulta hyökkääjän hallintaan (6) etäkäytön mahdollistamiseksi. Viimeinen vaihe on hyökkäyksen alkuperäisten tavoitteiden toteuttaminen suorittamalla halutut toiminnot (7). Lockheed Martin lähtee siitä, että hyökkäys voidaan pysäyttää rikkomalla hyökkäysketju periaatteessa missä kohtaa ketjua tahansa ja estämällä hyökkääjän eteneminen seuraavaan vaiheeseen. (Lockheed Martin, 2023).

Vuonna 2018 MITRE julkaisi oman ilmaisen ja vapaan tietokannan viitekehyksensä nimeltä MITRE ATT&CK (lyh. engl. Adversarial Tactics, Techniques, and Common Knowledge). Tietokantaa päivitetään kahdesti vuodessa perustuen julkiseen uhkatietoon ja tapahtumaraportteihin. Mallissa eri hyökkäystaktiikoita on neljätoista ja jokainen niistä sisältää useita tekniikoita ja niiden alaluokkia. Tekniikoita vuoden 2023 lopussa yli 240 kappaletta. Tietojenkalastelua voidaan hyödyntää, sekä tiedustelu- ja toimitustaktiikkojen yhteydessä. Tietojenkalastelulla on neljä alaluokkaa ja se voidaan toteuttaa käyttämällä: liitetiedostoja, linkkejä, palveluita tai puhelinta. (MITRE, 2023).

Cyber Kill Chain ja MITRE-viitekehykset eroavat siinä, että MITRE ATT&CK menee syvemmälle tarkoituksena tarkemmin kuvata hyökkäyksissä käytettäviä taktiikoita, tekniikoita ja proseduureja. Tavoitteena on tarjota konkreetista kyberuhkatietoa organisaatiolle kyberturvallisuuden kehittämiseksi. Toinen ero on periaatteellinen. Cyber Kill Chain väittää, että hyökkäyksen torjumiseksi ketju on katkaistava ja estettävä seuraavaan vaiheeseen siirtyminen. Ketjun voidaan periaatteessa katkaista missä vaiheessa hyökkäystä tahansa. MITRE

ATT&CK viitekehys ei vastaavaa väitä ja on sen sijaan muutakin kuin pelkkä hyökkäystaktiikoiden vaiheistus. (BlackBerry, 2023).

Tietosuojavaltuutetun toimiston (2023) internetsivut kuvaavat tietojenkalastelun etenemistä Office 365 -huijausesimerkin avulla. Kyseessä ei ole malli vaan enemmänkin tyypillisen tietojenkalastelun etenemisen kuvaus. Esimerkistä voidaan tunnistaa Cyber Kill Chain -mallin vaiheet. Alla kuviossa 4 on yhdistetty Cyber Kill Chain ja esimerkin vaiheet ja tekstissä ne on merkitty sulkuihin. Esimerkissä onnistunut hyökkäys voi johtaa uusien kohteiden etsimiseen ja uuden hyökkäyksen käynnistämiseen. Esimerkissä Office 365 hyökkäys ei ala vaiheesta 1 vaan vaiheesta 2. Myöhemmin hyökkäyksen edetessä palataan vaiheeseen yksi ja saadaan lisää tietoa seuraavien hyökkäysten kohdentamiseksi, minkä jälkeen hyökkäystä voidaan edelleen jatkaa.

KUVIO 4 Office 365 huijaus kuvattuna Cyber Kill Chain -mallin avulla.

Tyypillistä on, että tunnuksia kalastellaan sähköpostilla ja erilaisilla kalastelusivustoilla, joita on luotu lähes kaikille pilvialustoille kuten Office 365, Dropbox, Google, Facebook ja Instagram (2. varustelu tai aseistus). Kalastelu alkaa niin, että henkilön postilaatikkoon tulee aidonnäköinen viesti luotettavalta taholta, esimerkiksi oman organisaation sisältä (3. toimitus). Viesti sisältää tyypillisesti turvapostilinkin tai tiedostonjakolinkin. Linkin ohjautuu esimerkiksi oikeaan OneDrive/Sharepoint-tiedostoon, jossa pyydetään avaamaan asiakirja. Kun asiakirja avataan, aukeaa aidolta näyttävä Office 365 -kirjautumissivusto. Hyökkääjän tavoitteena on saada vastaanottaja syöttämään tunnuksensa tälle sivustolle, jolloin ne välittyvät hyökkääjän käyttöön (4. haavoittuvuuden hyödyntäminen). (Tietosuojavaltuutetun toimisto, 2023).

Kun hyökkääjä on saanut tunnukset haltuunsa, hän kirjautuu kyseiseen tiliin ja avaa sähköpostilaatikon (5. asennus). Hyökkääjä luo sääntöjä kuten saapuvien viestien eteenpäin ohjaus hänen omaan sähköpostiinsa (6. ohjaus). Hyökkääjä lataa yrityksen yhteystietoluettelon (1. tiedustelu). Hän linkittää OneDriven niin, että sinne tallennetut tiedostot päätyvät myös hänen haltuunsa (7. toiminnot). Tunnukset saatetaan myös myydä eteenpäin. Hyökkääjä aloittaa postituskampanjan yrityksestä saamillaan tiedolla tarkoituksena kalastella lisää uusia tunnuksia (aloitus uudelleen vaiheesta 3. toimitus). Hyökkäys ja menetetty

tunnus havaitaan usein vasta siinä vaiheessa, kun yritys saa varoituksen roskapostista sen yhteystietoihin kuuluvalta toiselta yritykseltä. (Tietosuojavaltuutetun toimisto, 2023).

2.2.2 Hyökkäysvektorit

Tietojenkalastelu (engl. Phishing) tarkoittaa uskottavaksi tekeytyvien sähköpostien lähettämistä tarkoituksena vaikuttaa henkilöön tai kerätä tältä henkilökohtaista tietoa (Social-Engineer, 2023). MITRE ATT&CK viitekehyksen (2023) mukaan tietojenkalastelu voidaan toteuttaa liitetiedostojen, linkkien, palveluiden, kuten sosiaalisen median palveluiden tai puhelun avulla. Tavoitteena on saada vastaanottaja avaamaan liitetiedosto, klikkaamaan linkkiä tai luovuttamaan tietoa hyökkääjälle. Tietojenkalastelu voi olla ei-kohdennettua, jolloin kalastelukampanjassa lähetetään samanlainen sähköposti useille vastaanottajille tai se voidaan kohdistaa tietylle organisaatiolle tai yksilölle. Tietojenkalastelussa voidaan hyödyntää sosiaalisen manipuloinnin tekniikoita.

Spearfishing eli vapaasti käännettynä keihäskalastelu on kohdennettua tietojenkalastelua. Termillä keihäskalastus (vrt. valaiden kalastaminen keihäällä) kuvataan sitä, että kohde on yksittäinen, eikä kyseessä ole ei-kohdennettu tietojenkalastelu. Hyökkääjä valitsee yksittäisen kohteen, organisaation tai yksilön, jolle tietojenkalasteluviesti lähetetään. Oleellista on, että hyökkääjä on tiedustelemalla tai sosiaalisen manipulaation keinoin saanut selville viestin luotettavuutta lisääviä seikkoja, joita viestissä hyödynnetään. (MITRE, 2023).

Huijauspuhelu (engl. Vishing). Huijauspuhelu tarkoittaa puhelimen välityksellä tapahtuvaa tietojenkalastelua. Tarkoituksena on saada kohde luovuttamaan puhelimitse henkilökohtaisia tietoja, joita voidaan hyväksikäyttää samoin kuin tietojenkalastelussa. Uhria voidaan pyytää myös siirtymään huijaussivustolle syöttämään vastaavat tiedot tai siirtämään itse rahaa huijarin hallinnoimalle pankkitilille. (Whitty & Young, 2016, luku 12.2). Huijauspuhelu saattaa sisältää puhelinnumeron väärentämisen eli spooffaamisen (engl. Phone Spoofing), jossa puhelu vaikuttaa tulevan oikeasta numerosta, joka kuitenkin on hyökkääjän hallussa (MITRE, 2023).

Huijaustekstiviesti (engl. SMiShing) on tietojenkalastelua puhelimen ja tekstiviestien välityksellä. Tekniikat ovat tietojenkalastelun kaltaisia, mutta alustana toimii tekstiviesti. Huijaustekstiviestit voivat sisältää linkkejä kalastelusivustoille, ja peitetarinana voidaan käyttää pankkien, tunnettujen brändien tai virastojen nimiä. (Social-Engineer, 2023).

URL-osoitteen manipulaatio (engl. Typosquatting) on sosiaalisen manipulaation muoto, jossa hyökkääjä rekisteröi itselleen verkkosivuston, joka on hyvin samankaltainen kuin tunnettu sivusto (kuten Office 365 -esimerkin huijaussivustossa luvussa 2.2.1). Tarkoituksena on erehdyttämättä saada käyttäjä siirtymään sivustolle, jonka nimessä on alkuperäiseen sivuun nähden tahallinen kirjoitusvirhe. Erehdyttämisessä on kaksi tapaa. Joko hyökkääjä luottaa käyttäjän itse oma-aloitteisesti tekemään kirjoitusvirheeseen tämän yrittäessä siirtyä oikealle sivustolle. Esimerkiksi käyttäjä kirjoittaa selaimeen gooogle.com (ylimääräinen o-kirjain) google.com sijasta. Toisena tapana on virheellisen linkin liittäminen tietojenkalastelusähköpostin yhteyteen. Kirjoitusasun muokkaaminen voi tapahtua lisäämällä tai poistamalla

merkkejä alkuperäiseen osoitteiseen nähden tai niissä voi olla kokonaan erilainen loppu, esimerkiksi .org, kun alkuperäinen loppu olisi .com. (Kaspersky (2023b).

Kaspersky (2023b) listaa useita huijaussivustojen tarkoituksia:

1. Alkuperäisen sivun imitointi tunnusten kalastamiseen.
2. Väärennetty verkkokauppa. Alkuperäisen sivuston verkkokauppa on väärennetty. Maksu otetaan vastaan mutta tuotetta ei toimiteta tilaajalle.
3. Kilpailijoiden rahastus. Liikenne ohjataan oikean sivuston kilpailijoille maksua vastaan.
4. Mainostulojen keruu. Valesivusto kerää mainostuloja sivuston kävijämäärien perusteella.
5. Identiteettivarkaus kyselyiden verukkeella. Huijaussivusto esittää keräävänsä asiakaspalautetta, todellisena tarkoituksena kuitenkin on identiteettivarkaus.
6. Kumppanuusmarkkinointi. Huijaussivusto ohjaa liikenteen oikealle sivustolle ja näin se pääsee nauttimaan alkuperäisen sivuston todellisesta kumppanuusmarkkinoinnista saaden osuuden sen verkkokaupan myynnistä.
7. Haittaohjelman asentaminen sivustolle siirryttäessä.
8. Huumori- tai pilasivustot, joiden tarkoitus voi olla kosto.

Toimitusjohtajahuijaus tai BEC-huijaus, joka tulee sanoista Business E-mail Compromise, tarkoittaa huijausta, jossa ulkopuolinen pääsee seuraamaan yrityksen sisäistä sähköpostiliikennettä ja huijaa työntekijöitä sitä kautta. Tarkoitus on saada uhri uskomaan, että yrityksen täytyy kiireellisesti maksaa lasku ulkopuoliselle taholle. Tätä varten hyökkääjä pyrkii löytämään yrityksestä ne henkilöt, jotka pystyvät liikuttamaan yrityksen rahoja. Tämä voi tapahtua esimerkiksi yrityksen puhelinvaihteeseen soittamalla. Nykyisin myös LinkedIn ja verkkorekrytointi antavat mahdollisuuden organisaation rakenteen, avainhenkilöiden, sekä käytössä olevien teknologioiden selvittämiseen. Kohteiden tunnistamisen jälkeen hyökkääjä esiintyy tyypillisesti yrityksen toimitusjohtajana, talousjohtajana tai hallituksen jäsenenä. Yhteydenotto voi tapahtua sähköpostilla tai puhelimitse. Viestinnän tapa voi olla joko aggressiivinen tai suostutteleva. (Hyppönen, 2021, s.110–111).

Imitointi (engl. Impersonation) tarkoittaa peitetarinan käyttämistä ja tekeytymistä toiseksi henkilöksi. Tarkoituksena on hankkia tietoa, hyväksikäyttää henkilöä tai hankkia pääsyoikeus yritykseen tai tietojärjestelmään. Imitointi voidaan toteuttaa digitaalisesti, kuten sähköpostilla tai puhelimella. Se voidaan toteuttaa myös fyysisesti, tapaamalla henkilöitä kasvotusten. Peitetarinana voi olla esiintyminen teknisen tuen henkilönä tai tavaran toimittajana. Hyökkääjän tarkoituksena voi olla esimerkiksi saastuttaa yrityksen tietokoneita syöttämällä haitallinen USB-tikku työasemaan. (Social-Engineer, 2023).

2.2.3 Esimerkkitapauksia

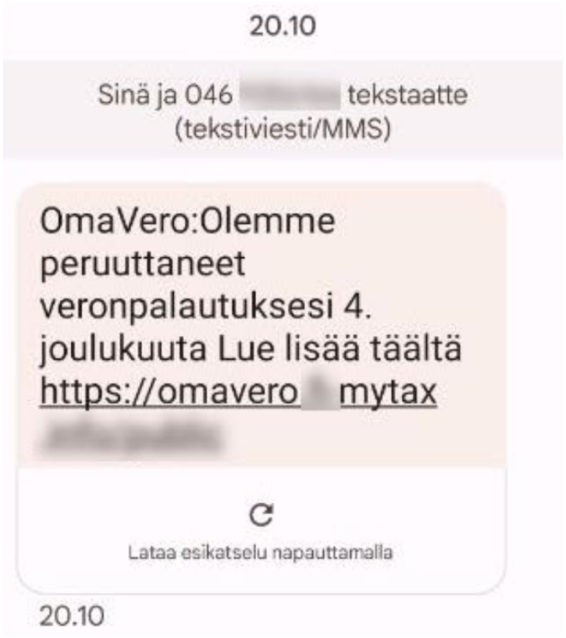
Social-Engineering -verkkosivuston (2023) mukaan tietojenkalastelussa hyökkääjät käyttävät seuraavia peitetarinoita: ajankohtaiset tapahtumat, hyväntekeväisyyshuijaukset, taloudelliset toimijat ja valtion virastot. Korona-virus oli ja on edelleen merkittävä globaali tapahtuma. Yhdysvaltojen kauppakomissio pitää tilastoa Korona-viruksen käyttämisestä huijauksissa. Tammikuun 2020 ja kesäkuun 2023 välisenä aikana raportoitiin yhteensä yli 417 000 Koronaan liittyvää petostapausta, joiden yhteenlaskettu rikosvahinko oli 1.1 biljoonaan dollaria (Yhdysvaltojen kauppakomissio, 2023).

Hyväntekeväisyyshuijauksesta oli kyse marraskuun 2018 Kalifornian metsäpalojen jälkimainingeissa. Lukemattomat perheet jäivät kodittomiksi ja heidän ahdinkoaan käytettiin hyväksi. Huijarit käyttivät tilaisuutta hyväkseen ja kohdeyrityksen toimitusjohtajan nimissä lähettivät sähköpostilla yrityksen työntekijöille vetoomuksia lahjakorttien ostamiseksi metsäpalon uhrien auttamiseksi. Todellisuudessa kerätyt varat menivät huijareille. (Agari, 2018).

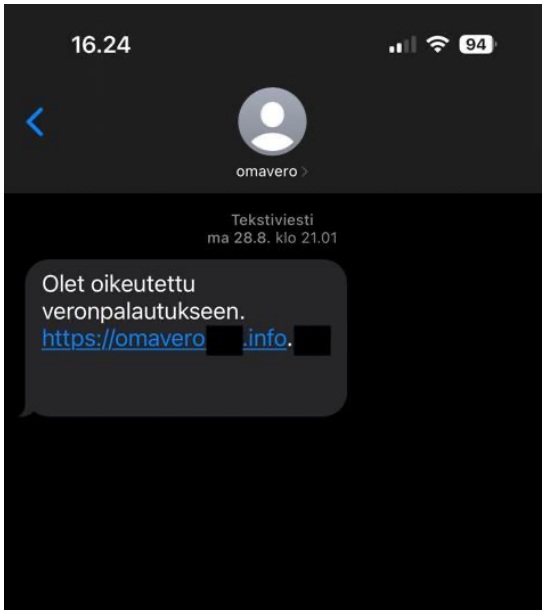
Huijarit tekeytyvät pankeiksi. Yksi tavallinen hyökkäysvektori on lähettää kalastelusähköposti tekeytyen pankin edustajaksi. Tavoitteena on saada vastaanottaja klikkaamaan linkkiä tai avaamaan liitetiedosto. Tammikuussa 2020 Daily Mailin (2020) mukaan amerikkalainen Citibank joutui huijauksen peitteeksi. Sen nimissä lähetettiin sähköposti, joka sisälsi linkin sivustolle update-citi.com, joka näytti pankin aidolta kirjautumissivustolta. Sivustolla pyydettiin pankkitunnuksia ja henkilötietoja. Artikkelin mukaan hyökkäyksessä vaarantuneita henkilötietoja saatettiin käyttää pian tämän jälkeen jakelupalvelu FedExiin liittyneessä huijauksessa. Jakelupalvelu FedExin nimissä lähetettiin huijaustekstiviesti, joka sisälsi tekaistun linkin todellisuudessa olemattoman lähetyksen toimitustietoihin.

Tietojenkalastelussa voidaan käyttää hyväksi tunnettujen organisaatioiden tai viranomaisten tietoja (Whitty & Young,2016, luku 12.1). Verohallinto on julkaissut sivuillaan tietoa huijauksista, joissa on käytetty hyväksi Verohallinnon nimeä ja/tai visuaalista ilmettä. Verohallinnon nimissä on soitettu huijauspuheluita ja lähetetty huijausviestejä sekä sähköposteina, että tekstiviesteinä (Verohallinto, 2023c). Seuraavassa on esimerkkejä siitä, miltä huijausviestit voivat näyttää.

OmaVero-huijaus tekstiviestinä. Verohallinnon nimissä on lähetetty tekstiviestejä, joissa kerrotaan joko saadusta tai peruutetusta veronpalautuksesta. Kuviossa 5 on Verohallinnon sivulla (2023c) julkaistu kuva ja kuviossa 6 on omaan yksityiseen liittymääni 28.8.2023 saapunut OmaVero-huijaus. Vaikka kuvien linkit tuskin ovat enää käyttökelpoisia, kuvista on poistettu tietoja yksityiskohtaisten linkkien salaamiseksi.

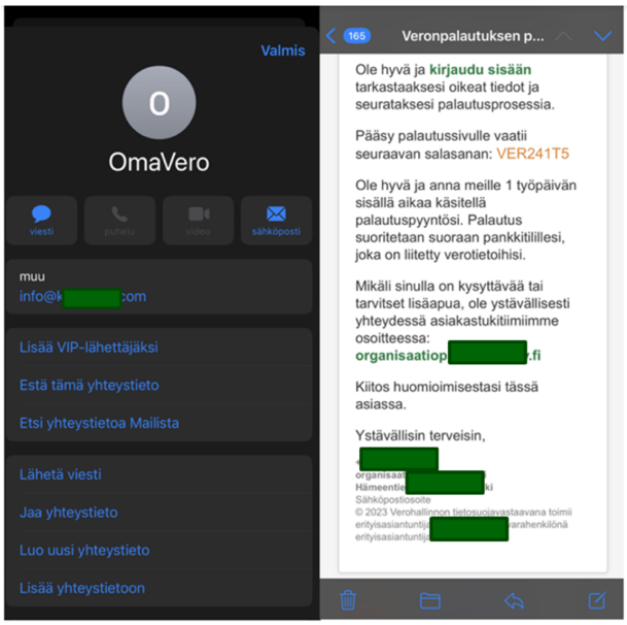


KUVIO 5 Verohallinnon julkaisema OmaVero-huijaus tekstiviestillä.

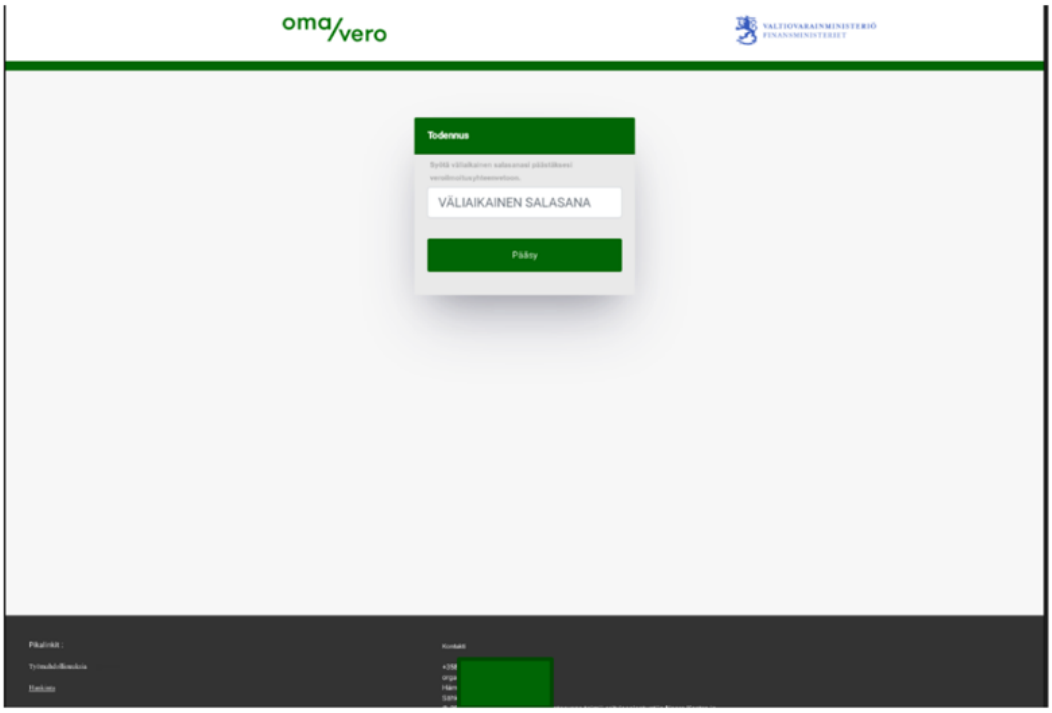


KUVIO 6 Itselleni lähetetty OmaVero-huijaus tekstiviestillä 28.8.2023.

OmaVero-huijaus sähköpostilla. Verohallinnon nimissä on lähetetty myös sähköposteja, joista Verohallinto on julkaissut (2023c) sivuillaan kuvan (kuvio 7), jossa ote saapuneesta tekstiviestistä. Kuviossa 8 on esimerkki tekaistusta, OmaVeroa muistuttavasti huijaussivustosta.



KUVIO 7 OmaVero-huijauksesta sähköpostilla.



KUVIO 8 Omavero.fi -osoitetta muistuttava hujaussivusto.

Tapaus Prykarpattyaoblenegro. Vuoden 2015 jouluaaton aattona Ukrainan sähköverkkoon tehtiin kyberhyökkäys. Yritys nimeltään Prykarpattyaoblenegro, joka vastasi osittain Ukrainan kaukosähköverkosta joutui Venäjältä toimineiden hyökkääjien kohteeksi. Hyökkääjät murtautuivat sähköverkon ylläpitäjien koneisiin ja ottivat ne hallintaansa niin etteivät nämä pystyneet käyttämään koneiden näppäimistöjä ja hiiriä. Hyökkääjät kytkivät sähköverkon osia yksitellen pois

päältä, sillä seurauksella, että lopulta 230 000 ukrainalaista jäi viettämään jouluaaton aattoa pimeyteen. Tilanne saatiin kuitenkin hallintaan muutamassa tunnissa ja sähköt palautettua. Muuntamoasemille oli mentävä manuaalisesti kääntämään kytkimiä, sillä hyökkääjä oli ylikirjoittanut etäohjaukseen käytettävien sovittimien Firmware-koodin. Hyökkäys oli toteutettu lähettämällä työntekijöiden sähköposteihin normaalinoloisia Word-tiedostoja, jotka olivat sisältäneet haitallista koodia. Koodi mahdollisti takaportin luomisen ja työntekijöiden koneiden seuraamisen salaa. (Hyppönen, 2021, s.247).

Google ja Facebook toimitusjohtajahuijauksen kohteena. Vuonna 2019 liettualainen Evaldas Rimašauskas tuomittiin Yhdysvalloissa viiden vuoden vankeuteen BEC-huijauksesta (Business E-mail Compromise, ks. luku 2.2.2.). Rimašauskas oli vuosien 2013–2015 aikana perustanut Googlen ja Facebookin yhteistyöyrityksiä muistuttavia, täsmälleen samannimisiä valeyrityksiä. Googlen ja Facebookin työntekijöille lähetettiin huijaussähköposteja, joilla onnistuttiin erehdyttämään heidät maksamaan oikeiden yhteistyöyritysten sijaan maksuja valeyritysten tileille Latviaan. Huijaussähköpostit oli lähetetty käyttäen yhteistyötyritysten sähköpostiosoitteiden kaltaisia osoitteita. Lisäksi uskottavuuden rakentamisessa oli käytetty tekaistuja laskutietoja, sopimuksia ja kirjeitä, jotka sisälsivät Googlen ja Facebookin johtajien tekaistuja allekirjoituksia. Näiden avulla pankkeja oli erehdytetty luulemaan, että kyse oli laillisista rahansiirroista. Tällä tavalla Google ja Facebook erehdytettiin siirtämään yli 120 miljoonaa dollaria väärin perustein. Vuonna 2017 Liettua otti Rimašauskasin kiinni ja luovutti Yhdysvaltoihin, jossa hänet tuomittiin vankeuden lisäksi luovuttamaan 49 miljoonaa dollaria takaisin ja maksamaan yli 26 miljoonan dollarin sakot. (United States Attorney's Office, 2019). Rikoksen jäljelle päästiin, koska Rimašauskas oli käyttänyt henkilökohtaista sähköpostiosoitettaan erään valeyrityksen perustamisen yhteydessä. Vaikka sähköpostiosoite oli vaihdettu heti perustamisen jälkeen, se oli nähtävissä historiatiedoista. (Hyppönen, 2021, s.112).

2.2.4 Aikaisempia tutkimuksia

Tässä luvussa perehdytään tietojenkalastelusähköposteista tehtyihin aiempiin tutkimuksiin. Vaikuttaa siltä, että omasta tutkimusaiheestani ei ole olemassa aiempaa tutkimusta, jossa olisi tutkittu vastaavia kysymyksiä. Niinpä esittelen tässä tietojenkalasteluun liittyviä tutkimuksia ja joita peilaan myöhemmin Hoxhuntin käyttämään koulutukseen. Erityisesti Parsons ym. (2015) tutkimus on oleellinen oman tutkimukseni kannalta. Sen perusteella voidaan päätellä, että jos tietojenkalastelua osataan odottaa, tunnistuskyky sitä kohtaan paranee ja viesteihin kohdistetaan enemmän huomiota.

Tutkimukset voidaan jakaa kahteen ryhmään: niihin, joissa tutkimukseen osallistujille on etukäteen kerrottu, että kyse on tietojenkalasteluun liittyvästä tutkimuksesta ja niihin, joissa osallistujaa ei ole varoitettu etukäteen. Parsons ym. (2015) ovat tutkimuksessaan kritisoineet sitä, että mikäli osallistujille kerrotaan testaamisesta etukäteen, tilanne ei vastaa todellisuutta. He neuvovat suhtautumaan kriittisesti tällaisiin tutkimuksiin.

Parsons ym. (2015) tutkivat osallistujien kykyä erottaa tietojenkalastelusähköposti oikeasti sähköpostista ja ylipäätään tietojenkalastelututkimusten

luotettavuutta. Puolelle 117 Adelaiden yliopiston tutkimukseen osallistuneista opiskelijoista yksiselitteisesti tiedotettiin, että tutkimuksessa on kyse tietojenkalastelun tunnistamisesta. Tulokset osoittivat, että tiedon saaneet osallistujat olivat selvästi parempia erottamaan viestit toisistaan ja he käyttivät myös enemmän aikaa viestien tutkimiseen. Tästä voitiin päätellä, että tietojenkalastelututkimukset, joissa osallistujia on etukäteen varoitettu, eivät välttämättä tuota luotettavaa tutkimustulosta. Todellisessa elämässä harvoin muistutetaan ihmisiä tietojenkalastelusta. Tutkijat muistuttivat, että vastaavissa tutkimuksissa tulisi kiinnittää tarkkaa huomiota tutkimuksen järjestelyihin ja osallistujille annettaviin ohjeisiin.

Jagatic ym. (2007) tutkivat tietojenkalastelua Indianan yliopiston opiskelijoilla. Tutkimuksessa 921 oppilaalle lähetettiin sähköposti, joka vaikutti saapuvan joko tuntemattomasta yliopiston sähköpostiosoitteesta tai vastaanottajan ystävältä. Tutkimukseen osallistuneille ei etukäteen kerrottu, että kyse on tutkimuksesta. Tutkimuksessa selvisi, että sosiaalisella yhteydellä tai sen kokemuksella oli suuri merkitys viestin vastaanottajiin. Ystävältä saapuvaksi tekeytyvällä viestillä oli paljon suurempi todennäköisyys saada vastaanottaja klikkaamaan sähköpostissa olevaa linkkiä. Kun sähköposti saapui tuntemattomalta lähettäjältä, linkkiä, klikkasi 16 % vastaanottajista, mutta kun viesti tuli ystävältä, 72 % vastaanottajista klikkasi linkkiä ja toimitti sen jälkeen henkilökohtaisia tietojaan linkin kautta.

2.3 Sosiaalinen manipulointi

Sosiaalista manipulointia käytetään tietojenkalastelun yhteydessä. Sosiaalinen manipulointi voidaan määritellä sen kohteen kannalta pelkästään negatiiviseksi, haitalliseksi toiminnaksi (Bossomaier ym., 2019, s. 87). Toisaalta se voidaan määritellä myös niin, että se pitää sisällään myös kohteen kannalta positiivista toimintaa (Hadnagy & Wilson, 2020, luku 3 09.13).

Hadnagy & Wilson (2020) määrittelevät sosiaalinen manipuloinnin tieteenalaksi, jossa vaikutetaan yksilöihin saaden heidät tekemään jonkin elämäänsä liittyvän toimenpiteen. Tämä toimenpide voi joko olla yksilön etujen mukaista tai niiden vastaista. Tämä sisältää esimerkiksi tiedonhankinnan, pääsyoikeuden saamisen tai kohteen oman toiminnan aikaansaamisen. Määritelmä kattaa siis yksilöön kohdistuvat positiiviset ja negatiiviset vaikutukset. Esimerkiksi lääkäri, psykologi tai terapeutti saattavat manipuloida potilaan tekemään jonkin positiivisen elämänmuutoksen. Toisaalta huijari saattaa käyttää sosiaalista manipulaatiota, jonka tarkoitus on saada kohde tekemään jotakin kohteen itsensä kannalta haitallista. Määritelmä laajentaa sosiaalisen manipuloinnin kattamaan myös jokapäiväisiä elämän vuorovaikutustilanteita. Esimerkiksi tilanteet, joissa lapsi vaikuttaa vanhempiinsa saadakseen tahtonsa läpi tai opettaja vaikuttaa oppilaisiin, jotta nämä oppisivat enemmän tai lääkäri tiedustelee tietoa asiakkaaltaan hoidon mahdollistamiseksi. Sitä käytetään myös poliisitoiminnassa ja seurustelusuhteissa.

Kun kyseessä on petostarkoitus, sosiaalinen manipulointi voidaan jakaa kolmeen osaan. Hadnagy & Wilson (2020, luku 3: 1:06.30) mukaan sosiaalinen

manipulaatio koostuu kolmesta osasta: peitetarinasta, manipulaatiosta ja sen täytyy liittyä tekijän ahneuteen. Kohde on sosiaalisen manipuloinnin kohteena, jos nämä kolme osatekijää ovat olemassa.

Verizonin (2023, s. 32) julkaiseman Data Breach Investigation Report 2023 mukaan sosiaalinen manipulointi on lisääntynyt vuoteen 2022 verrattuna, johtuen BEC-huijauksien yleistymisestä. Sosiaalisessa manipuloinnissa voidaan käyttää peitetarinoita ja tiedonhankintaa kohteeseen. Keksitty tarina voi vaikkapa liittyen siihen, että kohteelle uskotellaan hänen läheisensä olevan vaarassa ja tarvitsevansa apua pikaisesti. Raportissa todetaan, että vaikka peitetarinoiden käyttö on lisääntynyt vuodesta 2018, massakalastelu on kuitenkin toteutuneiden tietomurtojen yleisin syy. Läheltä piti -tapauksia, joissa sosiaalista manipulointia on käytetty, raportoidaan enemmän kuin, mitä raportoidaan toteutuneita tietomurtoja. Kaikista sosiaalisen manipuloinnin tapauksista peitetarinoita oli käytetty yli 50 % tapauksissa ja massatietojenkalastelua 44 % tapauksista.

2.4 Tietojenkalastelulta ja sosiaaliselta manipuloinnilta suojautuminen

> ”Koulutus on ainut varmin tapa suojautua sosiaaliselta manipuloinnilta. Oleellista on, että käyttäjiä koulutetaan tunnistamaan tietojenkalastelu, sen käyttämät tekniikat ja toimintatavat.” (Hadnagy & Wilson, 2020, luku 3 09.13).

Tässä luvussa esitellään tietojenkalastelulta suojautumisen keinoja yleisellä tasolla. Keinoina ovat teknologiset keinot ja käyttäjälähtöiset keinot. Kirjallisuuden perusteella molempia keinoja tarvitaan, vaikka käyttäjälähtöisten keinojen merkitys tietojenkalastelulta suojautumisessa näyttäisi olevan suurempi kuin teknologisten suojauskeinojen. Tekniset keinot auttavat tietojenkalasteluun mutta sen sisältämään sosiaaliseen manipulointiin auttaa vain käyttäjien koulutus (Hadnagy & Wilson, 2020, luku 3). Seuraavat keinot tietojenkalastelua vastaan ottavat huomioon myös sosiaalisen manipuloinnin osuuden.

Suojautuminen tietojenkalastelua vastaan edellyttää monikerroksista lähestymistapaa, joka yhdistää tekniset ratkaisut ja käyttäjien tietoisuuden (Hong, 2012, s. 78–81; Parmar, 2012, s. 8–11; Almomani ym., 2013, s. 13–14). Tietojenkalastelulta voidaan suojautua teknologisin keinoin, käyttäjälähtöisin keinoin ja hallinnollisin keinoin, kuten organisaatioiden turvallisuuspolitiikkojen avulla. Oleellista on useiden keinojen samanaikainen käyttäminen turvallisuuden parantamiseksi. Tekniset keinot eivät yksin riitä, koska monet niistä ovat alttiita kiertämiselle tai edellyttävät nopeaa reagointia uusissa hyökkäyksissä (Hong, 2012, s. 78–81). Teknologian ja käyttäjien tietoisuuden yhdistelmä luo vahvimman suojan tietojenkalastelua vastaan. Esimerkiksi monikerroksiset järjestelmät, joissa yhdistetään tekniset algoritmit, kuten tekstianalyysi ja koneoppiminen, sekä käyttäjälähtöiset varoitusjärjestelmät, voivat tarjota reaaliaikaista suojaa ja kasvattaa verkkoyhteisön valmiuksia reagoida uhkiin. Näiden menetelmien yhdistelmä mahdollistaa sekä proaktiivisen hyökkäysten torjunnan että reaktiivisen suojan uusien uhkien sattuessa (Almomani ym., 2013, s. 13–14).

Tekniset suojautumiskeinot keskittyvät hyökkäysten torjumiseen ennen kuin ne tavoittavat käyttäjän. Teknisiin keinoihin lukeutuvat sähköpostisuodattimet, mustiin listoihin (engl. Black List) perustuvat tietojenkalastelufiltterit, koneoppimisen hyödyntäminen haitallisten viestien ja sivustojen tunnistamisessa ja monivaiheinen tunnistautuminen. Musta listalla tarkoitetaan tunnistettujen haitallisten sähköpostien URL-linkkien listausta, joita voidaan käyttää tietojenkalastelun tunnistamiseen. Sähköpostisuodattimia voidaan käyttää estämään epäilyttävästä sähköpostiosoitteesta saapuvia viestejä. Koneoppimiseen perustuvat algoritmit tunnistavat haitallisia verkkosivustoja ja voivat asettaa niitä estettyjen sivustojen listalle. Lisäksi monivaiheinen tunnistautuminen tekee tilien kaappaamisesta vaikeampaa, koska pelkkä tilin ja salasanan vuotaminen ei vielä riitä tilin kaappaamiseksi. Teknisiin keinoihin lukeutuvat myös tietojenkalastelusivustojen alas ajaminen ja käyttäjille tulevat selainvaroitukset. (Hong, 2012, s. 78–79). Parmar (2012, s. 8–11) lisää teknisiin suojautumiskeinoihin järjestelmien palautustyökalut, joiden avulla järjestelmä voidaan palauttaa takaisin alkuperäisiin asetuksiin ja poistaa mahdolliset haittaohjelma.

Kyberturvallisuuskeskus (2024) on kuvannut monivaiheista tunnistautumista näin. Monivaiheisella tunnistautumisella tarkoitetaan sitä, että käyttäjän henkilöllisyys varmistetaan kahta tai useampaa eri tunnistautumistapaa käyttämällä. Monivaiheinen tunnistautuminen perustuu kolmelle periaatteelle, josta kahden on toteuduttava, jotta tunnistus on riittävä: 1. asia, jotka ovat käyttäjän tiedossa, kuten salasana, 2. asia, jonka käyttäjä omistaa, kuten matkapuhelimeen lähettävä koodi ja 3. asia, joka käyttäjällä on, kuten sormenjälki. Monivaiheisella tunnistautumisella voidaan hankaloittaa tietojenkalastelua. Rikolliset voivat saada haltuunsa palvelun salasanan mutta eivät pääse kirjautumaan sisään, koska heillä ei ole todentamiseen tarvittavaa tietoa kätössään.

Käyttäjälähtöinen koulutus on välttämätöntä tietojenkalastelun torjumiseksi (Parmar, 2012, s. 8–11). Useat lähteet painottavat käyttäjälähtöisiä keinoja ja koulutuksen merkitystä tietojenkalastelulta ja sosiaaliselta manipuloinnilta suojautumisessa. Käyttäjälähtöiset keinot keskittyvät tietoisuuden lisäämiseen ja käyttäjien kouluttamiseen. Keinoina voidaan hyödyntää simuloituja tietojenkalasteluharjoituksia ja mikropelejä, jotka lisäävät käyttäjien kykyä tunnistaa tietojenkalasteluhyökkäyksiä. Käyttäjälähtöisiin keinoihin voidaan lukea myös yksityisyyden suojaaminen erityisesti sosiaalisessa mediassa, mikä voi vähentää riskejä kohdennetuilta hyökkäyksiltä, kuten spearphishingiltä. (Hong, 2012, s. 79–81). Muita koulutusmenetelmiä voivat olla verkkopohjaiset koulutukset, simuloidut tietojenkalasteluharjoitukset, päivittäiseen työympäristöön sidotut koulutukset ja perinteiset luokkahuonekoulutukset. Näiden menetelmien yhdistäminen luo tehokkaan koulutusstrategian, joka parantaa käyttäjien kykyä tunnistaa ja torjua tietojenkalasteluyrityksiä ja sosiaalista manipulointia, vähentäen samalla inhimillisten virheiden riskiä. (Kumaraguru ym., 2010, s. 8–11).

3 TUTKIMUSMENETELMÄ

Tässä luvussa käsitellään tarkemmin tutkielman tutkimusmenetelmät, tutkimusongelmat, tutkimuskysymykset ja tutkimuksen lähtökohdat. Aineiston keruu toteutettiin kahdessa osassa hyödyntäen monimenetelmällistä tutkimusmenetelmää. Ensimmäisessä vaiheessa suoritettiin taustoittava haastattelu Verohallinnon Hoxhunt -palvelusta vastaavalle virkamiehelle (myöhemmin Hoxhunt-palveluomistaja). Aineiston keräämisessä oli haasteita ja niitä käsitellään otoksen edustavuutta ja luotettavuutta käsittelevissä luvuissa. Tavoitteena oli selvittää Hoxhuntin käyttöperiaatteet Verohallinnossa. Toisessa vaiheessa toteutettiin Verohallinnon työntekijöille kyselytutkimus, jonka perusteella pääosin vastataan tutkimuskysymyksiin.

Monimenetelmällisessä tutkimusmenetelmässä on kyse laadullisten ja määrällisten aineistojen yhdistämisestä, tavoitteena rakentaa tutkittavasta ilmiöstä kokonaisvaltaisempi kuva (Åkerbland, 2024). Tässä tutkielmassa päädyttiin monimenetelmälliseen tutkimusmetodiin, koska tutkittavasta ilmiöstä ei olisi saatu riittävää kuvaa vain toisella tutkimusmetodilla. Ensisijaisena tavoitteena oli määrällinen tutkimus ja sen laadukkaan kyselytutkimuksen suorittaminen. Heti tutkimuksen alkuvaiheessa kävi ilmi, että tämä ei olisi mahdollista ilman ilmiön tarkempaa tuntemusta. Hoxhunt-palveluomistajan haastattelu loi mahdollisuuden taustoittaa ilmiötä ja rakentaa laadukkaampi kyselytutkimus. Lisäksi kyselytutkimuksen avoimet vastaukset loivat syvyyttä tutkittavaan ilmiöön ja paljastivat näkökulmia, jotka muutoin olisivat jääneet löytämättä. Tutkimuksen laadullinen osuus rajoittuu vain yhteen haastatteluun, sekä kyselyn avoimiin vastauksiin.

Taustojen selvittämisessä perehdytään Verohallinnon käyttämän Hoxhunt palvelun toimintaan ja käyttötapauksiin. Miten käyttäminen tapahtuu ja minkälaiset ovat koulutuksen erityispiirteet? Kuinka usein koulutuksia suoritetaan ja mitkä ovat niistä saadut tulokset? Verohallinnon Hoxhuntin palveluomistajan haastattelussa varmistutaan siitä, että kyselytutkimus laaditaan oikeansuuntaisesti.

Kyselytutkimus oli tarkoitus lähettää Verohallinnon kaikille työntekijöille. Pyrkimys oli suorittaa yksinkertainen satunnaisotanta perusjoukosta. Verohallinnon turvallisuusyksikön johto kuitenkin eväsi koko organisaation jakelun, vaikka sen toteuttamista oli sovittu etukäteen Verohallinnon edustajan kanssa

joulukuussa 2023. Arvioin tämän vaikutusta tulosten luotettavuuteen tuonnempana.

Parsons ym. (2015) mukaan tietojenkalastelun tunnistuskyky paranee, jos tiedossa on, että viesti saattaa olla tietojenkalasteluviesti. Tällöin myös aikaa käytetään enemmän viestien tunnistamiseen. Tässä tutkimuksessa tehtiin olettama, että nimenomaisesti käytetty aika tai huomion määrä on oleellinen tekijä tietojenkalastelun tunnistamisessa. Tätä mitattiin kysymällä vastaajilta sitä, kuinka paljon he kiinnittävät huomiota eri asioihin, kuten sähköpostin lähettäjän sähköpostiosoitteeseen Hoxhuntin käytön seurauksena.

Tutkimus ei ota kantaa Hoxhunt-simulaatioiden sisältöön tai laatuun. Nyt tutkittiin erityisesti huomion määrää vaikuttavana tekijänä tietojenkalastelussa. Huomioitava on, että vaikka henkilö kiinnittää huomiota enemmän, se ei automaattisesti tarkoita parantunutta kykyä tunnistaa viestejä. Vaaditaan siis sekä huomiota, että kykyä tunnistaa viestit. Tämä tutkimus ei ota kantaa kykyyn, vaan ainoastaan huomion määrään.

3.1 Tutkimuskysymykset

Tutkimuskysymys on jaettu tutkimuskysymykseen ja kahteen apututkimuskysymykseen. Tutkimuskysymys pyrkii selvittämään vaikuttaako Hoxhunt Verohallinnon työntekijöiden käyttäytymiseen. Apututkimuskysymykset pyrkivät selvittämään, minkälaisia vaikutukset ovat olleet erityisesti turvallisuuden muissa osa-alueissa.

Tutkimuskysymys

1. Ovatko Verohallinnon työntekijät kokeneet Hoxhunt-tietojenkalastelukoulutuksen vaikuttaneen heidän käyttäytymiseensä?

Apututkimuskysymykset

2. Miten Hoxhunt on vaikuttanut Verohallinnon työntekijöiden käyttäytymiseen?
3. Onko Hoxhuntilla positiivisia vaikutuksia myös muiden turvallisuuden osa-alueiden osalta?

3.2 Hypoteesit

Hypoteesi on tavallisesti teoriasta johdettu olettamus ilmiön toimintamekanismista, jota testataan empiirisellä aineistolla (Tilastokeskus, 2024). Tässä tutkimuksessa hypoteesille ei ole olemassa tieteellistä taustaa, koska aiempaa tutkimusta ei ole löytynyt. Hypoteesit on muodostettu perustuen omaan kokemukseeni tutkittavasta aiheesta.

Hypoteesit

1. Kyllä, Hoxhunt on vaikuttanut työntekijöiden käyttäytymiseen.
2. Hoxhunt on parantanut Verohallinnon työntekijöiden tietojenkalastelun tunnistuskykyä.
3. Kyllä, Hoxhunt on vaikuttanut positiivisesti myös muissa turvallisuuden osa-alueissa lisääntyneenä huomion määränä.

3.3 Aineiston kerääminen ja otoksen edustavuus

Tässä luvussa käsitellään aineiston kerääminen ja arvioidaan otoksen edustavuutta perusjoukosta. Hoxhunt-palveluomistajan haastattelu suoritettiin etäyhteydellä 12.2.2024. Kysymykset on esitetty liitteessä 1. Määrällinen aineisto kerättiin kyselytutkimuksena anonyymina kyselytutkimuksena Webropol-järjestelmän kautta. Kysely julkaistiin Verohallinnon sisäisessä viestintäkanavassa ja se oli auki noin kolme viikkoa 16.2.-8.3.2024 välisenä aikana. Kyselyn kysymykset ovat kokonaisuudessaan nähtävissä liitteestä 2. Kysely toteutettiin vain suomen kielellä. Haastattelun ja kyselyn vastaukset on esitetty oleellisilta osin tutkimuksen tuloksissa.

Kyselyyn vastasi yhteensä 224 henkilöä (n=224). Vastausprosentti oli noin 4 % jos verrataan vuoden 2023 lopun Verohallinnossa työskentelevien määrään 5313 henkilöä (Verohallinto, 2024). Vastaajista miehiä oli 36, naisia 180, muunsukupuolisia 3 ja 5 ei halunnut kertoa sukupuoltaan. Sukupuolen osalta vertailu suoritettiin vain miesten ja naisten välillä. Vastaajista kuudesosa oli miehiä (17 %). Verohallinnossa vuoden 2023 lopussa oli miehiä 28 % ja naisia 72 % (Verohallinto, 2024). Näin ollen otannassa oli miehiä noin 40 % vähemmän kuin Verohallinnossa. Sukupuolen osalta arvioin, että otos vastaa kohtuullisesti perusjoukkoa.

Vastausten ikäjakauma asettui välille alle 25-vuotiaat ja enintään 69-vuotiaat. Verrataan vastauksia Verohallinnon tilastoihin. Kyselyn vastaajista alle 25-vuotiaita oli 3 %, 25–29-vuotiaita 12 %, 30–39-vuotiaita 25, 40–49-vuotiaita 28 %, 50–59-vuotiaita 24 %, 60–69-vuotiaita 8 % ja yli 69-vuotiaita ei ollut yhtään vastaajista. Vuoden 2023 lopussa Verohallinnossa oli töissä 5313 henkilöä. Työntekijöiden keski-ikä oli 45,6 vuotta. Verohallinnon ikäjakaumassa oli alle 25-vuotiaita 4 %, 25–34-vuotiaita 22 %, 35–44-vuotiaita 21 %, 45–54-vuotiaita 22 % ja yli 54-vuotiaita 31 %. (Verohallinto, 2024). Kyselyn alle 25-vuotiaiden määrä 3 % on lähellä Verohallinnon määrää 4 %. Yli 50-vuotiaita vastaajia kyselyssä oli yhteensä 32 % ja Verohallinnossa yli 54-vuotiaita oli 31 %. Lisäksi kyselyssä suurin ikäluokka oli 40–49-vuotiaat, kun Verohallinnon keski-ikä oli 45,6 vuotta vuoden lopussa. Arvioin otoksen vastaavan hyvin perusjoukkoa iän perusteella. Taulukossa 1 on esitetty kyselyn vastaajien ikäjakauma ja Verohallinnon työntekijöiden ikäjakauma.

TAULUKKO 1 Kyselyn ja perusjoukon ikäjakauma

Kyselyn ikäjakauma	n	%	Verohallinnon ikäjakauma	n	%
alle 25	7	3 %	alle 25	208	4 %
25–29	27	12 %	25–34	1176	22 %
30–39	57	25 %	35–44	1142	21 %
40–49	63	28 %	45–54	1155	22 %
50–59	53	24 %	yli 54	1631	31 %
60–69	17	8 %			

3.4 Aineiston analysointi

Määrällisen aineiston analyysissä käytettiin ristiintaulukointia, jolla tutkitaan muuttujien jakautumista ja niiden välisiä riippuvuuksia. Riippuvuus- tai riippumattomuustarkastelussa tutkitaan, onko tarkastelun kohteena olevan selitettävän muuttujan jakauma erilainen selittävän muuttujan eri luokissa. (Tietoarkisto, 2024). Vastaajien sukupuolta, ikää, sekä pidemmälle pelaamista ja haastavampaa peliversiota eli ns. Spicy modea käytettiin taustamuuttujina ja niitä tarkasteltiin suhteessa keskeisiin teemoihin. Analysointi toteutettiin vastausten suhteellisten prosenttiosuuksien laskemisella sekä vastausten jakautumisen tarkastelulla. Laadullisen aineiston analyysissä käytettiin teemoittelua ja sisältöanalyysia, jolloin saatiin syvällisempi ymmärrys vastaajien kokemuksista ja näkemyksistä. Vastausten käsittelyssä hyödynnettiin esimerkkilainauksia.

Aineiston analysoinnin tavoitteena on vastata tutkimuskysymyksiin, muodostaa yleiskäsitys Hoxhuntin vaikuttavuudesta, sekä arvioida hypoteesien toteutumista. Yleiskäsitys muodostetaan analysoimalla kyselytutkimuksen tulokset aihealueittain erikseen ja kokonaisuutena. Tutkimuskysymyksiin pyritään vastaamaan muodostamalla seuraavat prosenttiosuudet vastausten perusteella. Mikä osuus vastaajista (%-osuus) kokee Hoxhuntin vaikuttaneen huomiota lisäävästi tai vähentävästi? Entä mikä osuus vastaajista kokee Hoxhuntin vaikuttaneen huomiota lisäävästi tai vähentävästi henkilöstö- tai tilaturvallisuuden osalta?

Ristiintaulukoinnin osalta käytettiin riippumattomuustestiä, jossa tutkitaan, onko tarkastelun kohteena olevan selitettävän muuttujan jakauma erilainen selittävän muuttujan eri luokissa. Testinä käytettiin ns. Pearsonin χ^2-testiä (Khiin neliö -testi), joka perustuu havaittujen ja odotettujen frekvenssien vertailuun. Kun χ^2-luku on suuri, eroavat nämä frekvenssit paljon toisistaan ja kun se on pieni, ovat erot havaittujen ja odotettujen frekvenssien välillä pienet. Ristiintaulukoiden yhteydessä käytetään χ^2-arvoa, vapausasteiden määrää ((rivien määrä-1) * (sarakkeiden määrä-1)) ja p-arvoa. P-arvo kuvaa todennäköisyyden, jolla havaittua vastaava tai vahvempi yhteys löydettäisiin siinä tapauksessa, että nollahypoteesi on tosi. P-arvon tulkinnassa on perinteisesti käytetty merkitsevyystasoja 5 % (p=0,05), 1 % (p=0,01) tai 0,1 % (p=0,001), ja esimerkiksi p-arvon ollessa alle 0,05 on voitu todeta, että erot ovat tilastollisesti melkein merkitseviä. Esimerkiksi jos riippumattomuustestin p-arvo on 0,069. On siis n. 7 %:n todennäköisyys saada vähintään otoksessa havaittu arvo, kun oletetaan, että

nollahypoteesi on tosi. Toisin sanoen, todennäköisyys tehdä väärä päätelmä tulosten merkitsevyydestä on korkeampi kuin usein käytetty 5 %:n riskitaso. Mitä suurempi otoskoko, sitä todennäköisempää saada merkitseviä tuloksia. Tilastollisen merkitsevyyden lisäksi täytyy aina pohtia myös erovaisuuksien suuruuden sisällöllistä merkitystä ja välttää merkitsevyystasojen orjallista tulkintaa (Tietoarkisto, 2024).

3.5 Tutkimuksen luotettavuus ja eettisyys

Tutkimuksen luotettavuuteen vaikutti merkittävästi se, että kysely tavoitti vain osan Verohallinnon henkilöstöstä. Alun perin sain Verohallinnolta tutkimusluvan ja julkaisuoikeuden kyselyyn koko Verohallinnon henkilöstölle. Kuitenkin julkaisuhetken tullessa ajankohtaiseksi kävi ilmi, että kyselyä ei aiota julkaista koko Verohallinnon laajuudessa. Tämä on osaltaan vaikuttanut tulosten merkitsevyyteen. Eli tuloksista ei pystytty tekemään niin selviä johtopäätöksiä kuin isommasta otannasta olisi pystytty tekemään. Lopputuloksena Verohallinnon 4500 henkilön mahdollisesta joukosta kyselyn sai vain noin 2500 henkilöä. Kysely julkaistiin vain turvallisuusyksikön viestintäkanavassa, jossa seuraajia kyselyn julkaisuajankohtajana oli noin 2500 henkilöä. Kanavan seuraaminen perustuu vapaaehtoisuuteen. Tässä tutkimuksessa ei pystytä arvioimaan sitä, millä perusteella turvallisuusyksikön viestintäkanavaa seurataan. Toisin sanoen kanavan seuraamisen vapaaehtoisuus ja henkilöiden erilaiset seuraamisen motiivit voivat aiheuttaa sen, että kanavaa mahdollisesti seuraavat useammin ne henkilöt, jotka ovat jollakin tapaa keskimääräistä kiinnostuneempia turvallisuudesta.

Eettisyys on kaikkea tieteellistä tutkimusta koskeva vaade, joka koskee tutkimuksen laatua ja on tutkimuksen toinen puoli. Monimenetelmällisyyden voidaan ajatella vahvistavan tutkimuksen eettisyyttä. Jo tutkimustehtävän asettaminen ja määrittely ovat eettisiä kysymyksiä. (Åkerbland & Seppänen-Järvelä, 2024, luku 3.3). Kyselyn luotettavuutta arvioitaessa tulee käsitellä myös sitä, että olen itse töissä Verohallinnon turvallisuusyksikössä. Olen ottanut tutkimuksen osaksi Hoxhunt-palveluomistajan haastattelun vahvistamaan tutkimuksen luotettavuutta ja eettisyyttä. Toisaalta oma läheinen yhteyteni aiheeseen on tarkoittanut tutkittavan aiheen taustojen syvällisempää tuntemista. Tämä mahdollisti kyselytutkimuksen laatimisen siten, että siinä voitiin käyttää Verohallinnon turvallisuuteen liittyviä vertailukysymyksiä, jotka ovat oleellisia ja konkreettisia vastaajien näkökulmasta. En käytä tutkimuksessa itseäni viitteenä. Verohallintoon ja Hoxhuntiin liittyvät seikat käydään läpi Hoxhunt-palveluomistajan haastattelun kautta. Arvioin, että näillä toimilla olen onnistunut säilyttämään objektiivisuuden tutkimuksen aikana ja pystynyt esittämään tulokset ja analyysin puolueettomasti, eettisiä periaatteita noudattaen.

Tulosten luotettavuutta tulee arvioida myös siten, että tarkastellaan, onko tutkimuksen kysymykset asetettu niin, että vastaajat ymmärtävät ne ja pystyvät vastaamaan niihin. Kyselyssä tehtiin ratkaisu kysyä vastaajilta heidän arviotaan Hoxhuntin vaikutuksista heidän huomionsa määrään liittyen turvallisuuden eri osa-alueisiin. Tällöin on kyse heidän kokemuksestaan ja kyvystään arvioida

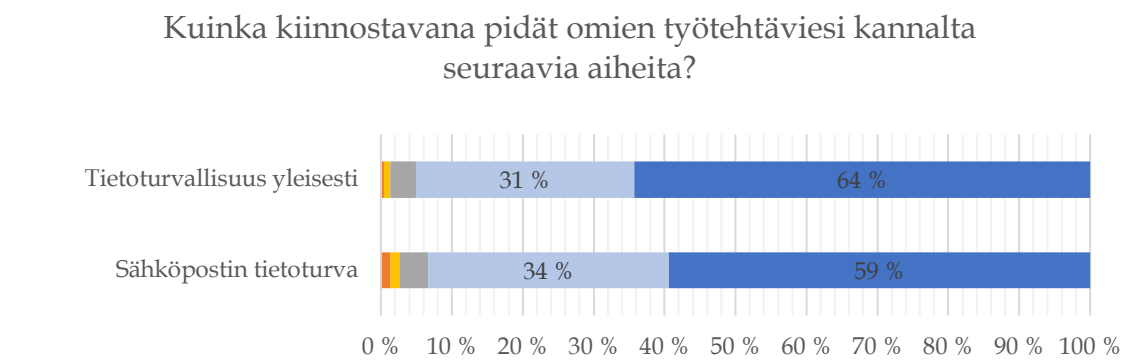
asioita. Olennaista ei ole vain se, kiinnittävätkö he enemmän huomiota, vaan se, ovatko he Hoxhuntin seurauksena alkaneet kiinnittää enemmän huomiota tiettyihin osa-alueisiin, kuten sähköpostin sisältöön. Tällöin vastaaja joutuu arvioimaan Hoxhuntin vaikutusta huomionsa määrään, eikä pelkästään huomion tasoa. Tämä aiheuttaa haasteen vastausten luotettavuudelle. Toisaalta vastauksissa nähdään merkittäviä eroja eri turvallisuuden osa-alueissa. Jossakin osa-alueissa vaikutuksia koetaan olevan ja joissakin niitä ei ole. Nämä erot vähentävät tulosten luotettavuuteen kohdistuvia paineita.

4 TUTKIMUKSEN TULOKSET

Tässä luvussa käsitellään tutkimuksen tulokset. Hoxhunt-palveluomistajan haastattelun tulosten kautta selvitettiin Hoxhuntin käyttötapaukset Verohallinnossa ja henkilöstölle osoitetussa kyselyn tulosten kautta selvitettiin sen vaikutuksia henkilöstöön. Tutkimuksen tulokset osoittavat, että Hoxhuntilla on ollut vaikutusta, sekä palveluomistajan, että kyselyn vastaajien mielestä. Hoxhunt vaikuttaa tietoturvallisuuden lisäksi positiivisesti myös muihin turvallisuuden osa-alueisiin kuin pelkästään tietoturvallisuuteen. Hoxhuntin ansiosta huomiota kiinnitetään tietoturvallisuuden lisäksi myös muihin turvallisuuden osa-alueisiin, kuten henkilöstö-, toimitilaturvallisuus ja turvallisuusperiaatteisiin. Tämän lisäksi analyysi osoitti eroja miesten ja naisten välillä. Naiset kokevat turvallisuuden muita osa-alueita koskevan huomionsa lisääntyneen miehiä enemmän turvallisuuden muihin osa-alueisiin. Tulokset myös osoittavat, että jatkamalla Hoxhuntin pelaamista pidemmälle, sen teho kasvaa lisääntyneenä huomion määränä erityisesti muissa turvallisuuden osa-alueissa.

Tutkimuksen kysymykset oli muotoiltu niin, että voitiin selvittää Hoxhuntin vaikutuksia käyttäjiinsä huomion määrässä mitattuna. Vastaajat saivat arvioida, kiinnittävätkö he vähemmän tai enemmän huomiota eri turvallisuuden osa-alueisiin. Vastaajat saivat vastata myös, että Hoxhuntilla ei ollut vaikutusta tai, että he eivät pystyneet arvioimaan sitä.

Vastaajat osoittivat korkeaa kiinnostusta tietoturvallisuutta kohtaan. Kyselyssä selvitettiin lähtökohtaista suhtautumista tietoturvallisuuteen. *K5: Kuinka kiinnostavana pidät omien työtehtäviesi kannalta seuraavia aiheita (asteikolla 1–5)*: *Tietoturvallisuus yleisesti ja sähköpostin tietoturva.* Kyselyn vastaajista yhteensä 95 % piti tietoturvallisuutta työtehtävien kannalta jonkin verran (31 %) tai erittäin kiinnostavana (64 %). Vastaavasti 93 % vastaajista piti sähköpostin tietoturvaa työtehtävien kannalta kiinnostavana (34 %) tai erittäin kiinnostavana (59 %). Vastausten keskiarvot asteikolla 1–5 olivat tietoturvallisuudessa yleisesti 4,6/5 ja sähköpostin tietoturvan osalta 4,5/5. Kuviossa 9 on esitetty tietoturvan ja sähköpostin kiinnostavuus työtehtävien kannalta.

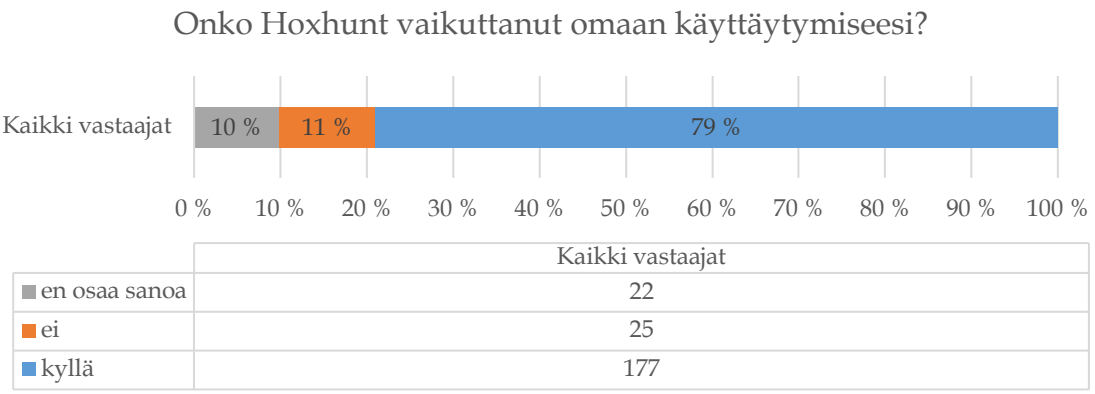


	Sähköpostin tietoturva	Tietoturvallisuus yleisesti
1 = en pidä lainkaan kiinnostavana	3	1
2 = jonkin verran kiinnostavana	3	2
3 = neutraali suhtautuminen	9	8
4 = jonkin verran kiinnostavana	76	69
5 = erittäin kiinnostavana	133	144

KUVIO 9 Tietoturvan kiinnostavuus työtehtävien kannalta.

4.1 Hoxhuntilla on vaikutusta käyttäytymiseen

Tutkimuksen tulokset osoittivat, että Hoxhuntilla on vastaajien mielestä ollut vaikutusta heidän käyttäytymiseensä. Noin kahdeksan kymmenestä (79 %) on sitä mieltä, että Hoxhunt on vaikuttanut heidän käyttäytymiseensä. Noin yksi kymmenestä (11 %) arvioi, että vaikutusta ei ole ollut ja joka kymmenes (10 %) ei osannut sanoa (kuvio 10). Hoxhunt-palveluomistaja (2024) arvioi, että Hoxhuntilla on ollut vaikutusta Verohallintolaisten käyttäytymiseen valppaustason ja yleisen varuillaan olon kohoamisena. Tämä on vaikuttanut myös Verohallinnon turvallisuuteen: ”Eli yleinen varovaisuus kun kasvaa, niin totta kai silloin vaikutuksia sitten myös koko Veron turvaan, että henkilöstö on siellä jo niin sanottuna kilpenä”. Osalla Hoxhuntin käyttäjistä on ollut myös negatiivisia kokemuksia. Seuraavissa luvuissa arvioidaan sitä, millaisia nämä positiiviset ja negatiiviset vaikutukset ovat tarkemmin olleet. Lisäksi arvioidaan sitä, miten käyttäjien sukupuoli ja ikä vaikuttavat sekä sitä, vaikuttaako pidemmälle pelaaminen.



KUVIO 10 Hoxhuntin vaikutus käyttäytymiseen.

4.2 Hoxhunt on käytössä laajasti Verohallinnossa

Hoxhuntin käyttöä Verohallinnossa selvitettiin haastattelemalla Verohallinnon Hoxhuntista vastaavaa virkamiestä, josta tässä tutkimuksessa käytetään nimitystä Hoxhunt-palveluomistaja. Hoxhunt-palveluomistaja (2024) kertoi haastattelussa, että Verohallinto otti Hoxhuntin käyttöön vuonna 2021 tai 2022 koekäytöllä. Tämän jälkeen käyttöä laajennettiin koskemaan kaikkia suoraan Verohallinnon palveluksessa olevia. Vuonna 2023 otettiin mukaan myös palveluntoimittajat. Vuonna 2024 helmikuussa se oli käytössä noin 4900 henkilöllä. Hoxhuntin käyttö perustuu vapaaehtoisuuteen. Verohallinnossa oli tuohon aikanaan töissä yhteensä noin 6300 henkilöä, jos lasketaan mukaan kaikki omat työntekijät ja palveluntoimittajat. Näin ollen käyttöaste koko Verohallinnossa oli noin 78 %.

Hoxhunt-palveluomistaja (2024) kertoi, että ”Hoxhunt on pelillistetty tietojenkalastelukoulutusohjelma, joka on integroitu käyttäjän työsähköpostilaatikkoon”. Käyttäjä ei siis lähtökohtaisesti tiedä, mitkä viesteistä ovat Hoxhunt-järjestelmän lähettämiä ja mitkä tulevat muista lähteestä: ”Noin viikon tai kahden välein, keskimäärin 10 päivän välein, sähköpostilaatikkoon tulee Hoxhuntista simulaatioviesti, joka tulisi tunnistaa ja raportoida.” (Hoxhunt-palveluomistaja, 2024).

Hoxhunt-simulaatiot voivat olla erilaisia tunteisiin – esimerkiksi kiireen tunteeseen tai uteliaisuuteen – vetoavia viestejä. Hoxhunt-palveluomistaja (2024) kertoi esimerkin simulaatiosta. Sähköpostiin tulee kollegan nimissä viesti, jossa kerrotaan, että vastaanottajan autoa on naarmutettu parkkipaikalla. Viestissä vedotaan kiireeseen ja uteliaisuuteen, tarkoituksena saada kohde reagoimaan nopeasti sen enempää miettimättä. Verohallinnossa kaikki epäilyttävät viestit voidaan raportoida tietoturva-asiantuntijoiden arvioitaviksi käyttäen sähköpostiin asennettua raportointipainiketta. Jos raportoitu viesti on osa Hoxhunt-koulutusta, käyttäjälle avautuu selaimeen näkymä koulutusportaaliin. Jos taas kyseessä ei ole Hoxhunt-viesti, käyttäjä saa ilmoituksen ja voi halutessaan raportoida sen asiantuntijoiden arvioitavaksi.

Hoxhuntissa on kyse myös pelaamisesta. Käyttäjä kerää pisteitä eli tähtiä onnistuneista simulaatioviestien tunnistuksista ja tietojenkalasteluaiheisista mikrokoulutuksista. Etenemällä pidemmälle simulaatiot muuttuvat haastavimmiksi (Hoxhunt, 2023). Tekemällä onnistuneita tunnistuksia käyttäjä saa tähtiä, pääsee pelaamaan eteenpäin, etenee ylöspäin portaita ja tulee lopulta vastustuskykyisemmäksi tietojenkalastelulle. Yhdestä onnistuneesta, riittävän nopeasta Hoxhunt-viestin raportoinnista saa kaksi pistettä eli tähteä. Tämän jälkeen on mahdollisuus ansaita kolmas tähti suorittamalla mikrokoulutus Hoxhunt-portaalissa. Keräämällä tähtiä voi saavuttaa tasoja ja seurata edistymistään. Kun Hoxhuntissa etenee pidemmälle, simulaatioiden vaikeustaso kasvaa automaattisesti. Lisäksi käyttäjä voi valita vielä haastavammat simulaatiot – eli ns. Spicy moden – käyttöönsä, kun on onnistunut keräämään 50 tähteä. Tällöin simulaatioiden vaikeustaso on normaalia suurempi. 50 tähden kerääminen tarkoittaa noin 17 onnistunutta riittävän nopeasti tunnistettua ja raportoitua simulaatiota ja niihin kuuluvien mikrokoulutusten suorittamista. (Hoxhunt-palveluomistaja, 2024).

4.3 Tietojenkalastelun tunnistuskyky ja raportointi on parantunut

Hoxhunt (2023) itse väittää nettisivuillaan ohjelman suojaavan organisaatiota tietojenkalastelua vastaan. Tämän tutkimuksen tulokset osoittavat, että näin on myös Verohallinnon työntekijöiden mielestä, sekä kyselytutkimuksen numeraalisten että avointen vastausten perusteella. Myös Hoxhunt-palveluomistajan haastattelun tulokset tukevat tätä käsitystä. Aloitetaan ensin kyselyn numeraalisista vastauksista, minkä jälkeen käydään läpi avointen vastausten tulokset. Tämän luvun viimeisessä osiossa tarkastellaan Hoxhunt-palveluomistajan näkemyksiä.

Tietojenkalastelun tunnistuskykyä selvitettiin kolmen osa-alueen kautta: sähköpostin lähettäjän sähköpostiosoite, sähköpostin sisältö ja sähköpostin sisältämien linkkien URL-osoitteiden kirjoitusasu. Lisäksi vaikutuksia raportointiin selvitettiin turvallisuushäiriöistä ilmoittaminen osa-alueen kautta. Arviota pyydettiin kuusiportaisella asteikolla seuraavalla tavalla:

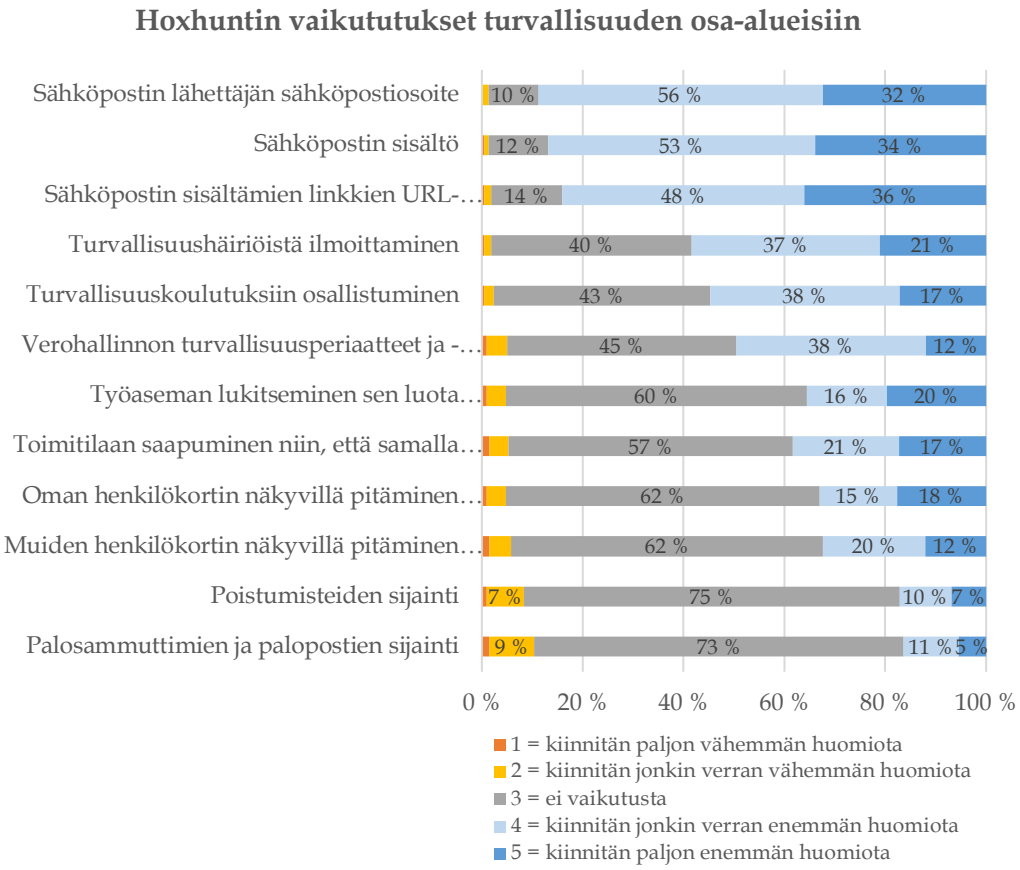
> *K6: Onko Hoxhunt vaikuttanut käyttäytymiseesi työhön liittyen? Arvioi osa-alueita seuraavalla asteikolla 1–5, missä…*
>
> *0 = en osaa arvioida vaikutusta*
> *1 = kiinnitän paljon vähemmän huomiota*
> *2 = kiinnitän jonkin verran vähemmän huomiota*
> *3 = ei vaikutusta*
> *4 = kiinnitän jonkin verran enemmän huomiota*
> *5 = kiinnitän paljon enemmän huomiota*

Kyselyn vastaajat kokivat, että heidän huomionsa määrä on lisääntynyt erityisesti tietojenkalastelun osalta. Suurin vaikutus Hoxhuntilla koettiin olevan

sähköpostin lähettäjän sähköpostiosoitteeseen, toiseksi suurin sähköpostin sisältöön ja kolmanneksi sähköpostin sisältämiin linkkeihin. Neljänneksi eniten vaikutusta oli turvallisuushäiriöistä ilmoittamiseen. Vastaukset on alempana esitetty kootusti kuvioissa 11 ja taulukossa 2 vaikuttavuusjärjestyksessä. Vaikuttavin osa-alue on se, jonka vastausten keskiarvo on suurin. Tuloksissa otettiin huomioon kaikki sellaiset vastaukset, joissa vastaaja oli kokenut voivansa antaa arvion kysymyksestä. Eli "en osaa arvioida" -vastaukset jätettiin vertailun ulkopuolelle.

Noin 88 % vastaajista koki, että Hoxhunt on vaikuttanut huomion määrään koskien sähköpostin lähettäjän sähköpostiosoitetta jonkin verran tai paljon enemmän. Vastaavasti 87 % vastaajista koki huomion lisääntyneen sähköpostin sisällön osalta. Sähköpostien linkkeihin kiinnitti enemmän huomiota 84 % vastaajista ja turvallisuushäiriöistä ilmoittamiseen 58 %.

Osa vastaajista (10–14 %) koki, että Hoxhuntilla ei ollut vaikutusta huomion määrään. Sähköpostin lähettäjän sähköpostiosoitteen osalta 10 %, sähköpostin sisällön osalta 12 % ja linkkien osalta 14 % vastaajista eivät kokeneet Hoxhuntin vaikuttaneen lainkaan. Turvallisuushäiriöiden osalta havaittiin merkittävä ero ei-vaikutusta vastanneiden osuudessa. Turvallisuushäiriöiden osalta 40 % vastaajista koki, että vaikutusta ei ollut.



KUVIO 11 Hoxhuntin vaikuttavuus turvallisuuden osa-alueissa.

Tarkasteltaessa vastausten keskiarvoja asteikolla 1–5, lähes samalle tasolla asettuvat kolmen kärki: sähköpostiosoite (4,20), sähköpostin sisältö (4,19) ja linkit (4,18). Jokaisessa näissä keskiarvo on yli neljä. Turvallisuushäiriöistä ilmoittamisen keskiarvo oli selvästi matalampi arvolla 3,77. Taulukossa 2 on esitetty kaikkien osa-alueiden tarkemmat tulokset ja osa-alueiden keskiarvot kaikkien vastaajien kesken. Taulukosta on jätetty pois ne, jotka eivät osanneet arvioida vaikutuksia jonkin osa-alueen osalta. Vaikutuksia turvallisuuden muihin osa-alueisiin käsitellään seuraavassa luvussa 4.4.

TAULUKKO 2 Hoxhuntin vaikutukset turvallisuuden osa-alueisiin.

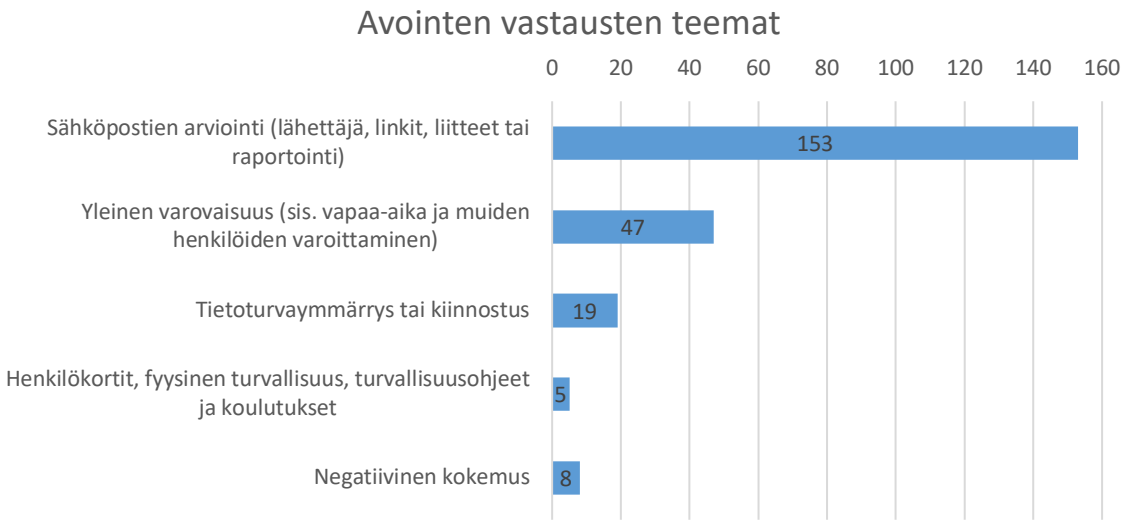
	1 n %-osuus	2 n %-osuus	3 n %-osuus	4 n %-osuus	5 n %-osuus	Yhteensä	Keskiarvo (1–5)
Sähköpostin lähettäjän sähköpostiosoite	0 0,0 %	3 1,4 %	22 9,9 %	125 56,3 %	72 32,4 %	222 100 %	4,20
Sähköpostin sisältö	1 0,5 %	2 0,9 %	26 11,8 %	117 52,9 %	75 33,9 %	221 100 %	4,19
Sähköpostin sisältämien linkkien URL-osoitteiden kirjoitusasu	1 0,5 %	3 1,4 %	31 14,2 %	105 47,9 %	79 36,1 %	219 100 %	4,18
Turvallisuushäiriöistä ilmoittaminen	1 0,5 %	3 1,4 %	85 39,7 %	80 37,4 %	45 21,0 %	214 100 %	3,77
Turvallisuuskoulutuksiin osallistuminen	1 0,5 %	4 1,9 %	90 42,9 %	79 37,6 %	36 17,1 %	210 100 %	3,69
Verohallinnon turvallisuusperiaatteet ja -ohjeet	2 0,9 %	9 4,1 %	99 45,4 %	82 37,6 %	26 11,9 %	218 100 %	3,56
Työaseman lukitseminen sen luota poistuttaessa	2 1,0 %	8 3,8 %	124 59,6 %	33 15,9 %	41 19,7 %	208 100 %	3,50
Toimitilaan saapuminen niin, että samalla ovenavauksella ei pääse sisään luvattomia	3 1,4 %	8 3,8 %	118 56,5 %	44 21,1 %	36 17,2 %	209 100 %	3,49
Oman henkilökortin näkyvillä pitäminen Verohallinnon tiloissa	2 1,0 %	8 3,8 %	130 62,2 %	32 15,3 %	37 17,7 %	209 100 %	3,45
Muiden henkilökortin näkyvillä pitäminen Verohallinnon tiloissa	3 1,4 %	9 4,3 %	128 61,8 %	42 20,3 %	25 12,1 %	207 100 %	3,37
Poistumisteiden sijainti	2 1,0 %	15 7,4 %	152 74,5 %	21 10,3 %	14 6,9 %	204 100 %	3,15
Palosammuttimien ja palopostien sijainti	3 1,5 %	18 8,9 %	148 73,3 %	22 10,9 %	11 5,4 %	202 100 %	3,10
Keskiarvo	0,8 %	3,6 %	46,0 %	30,3 %	19,3 %		

Tarkastellaan seuraavaksi kyselyn avoimia vastauksia. 224 kyselyyn vastaajasta 177 kertoi Hoxhuntin vaikuttaneet omaan käyttäytymiseensä. He kaikki jättivät myös avoimen vastauksen. Kyselyn vastaajat kertoivat avoimissa vastauksissa Hoxhuntin vaikuttaneet seuraavilla tavoilla. Tarkkuus sähköpostien arvioinnissa on lisääntynyt, yleinen varovaisuus ja epäluuloisuus on kasvanut ja tietoturvaymmärrys on syventynyt. Huomiota kiinnitetään aiempaa enemmän sähköpostin lähettäjän sähköpostiosoitteeseen, sähköpostin sisältämien linkkien kirjoitusasuun, sähköpostin sisältöön ja turvallisuushäiriöiden raportoimiseen.

Avointen vastausten analysoinnissa käytettiin teemoittelua. Kyselyn avoimien vastausten kirjoitusasuissa oli muotoja, joista oli vaikea selvittää vastaajien

tarkoitusperää yksiselitteisesti. Esimerkiksi useat vastaukset sisälsivät mainin-nan sähköpostista, kuten vaikkapa ”olen tarkempi sähköpostien kanssa töissä sekä kotona”. Vastauksesta ei varsinaisesti voi päätellä, mitä “tarkkuus” tarkoit-taa, mutta siitä voi päätellä vastauksen liittyvän sähköposteihin ja vaikutusten ulottuvan myös työpaikan ulkopuolelle. Teemoittelussa tehtiin seuraavat ratkai-sut teemojen välillä ja tarkasteltiin kutakin vastausta sen perusteelle, sisältääkö se teeman mukaista sisältöä. Yksi vastaus saattoi kuulua useaan teemaan. Tee-moja tunnistettiin yhteensä viisi, jotka on luetteloitu seuraavaksi ja kuvattu ku-viossa 12. Teemoista kolme ensimmäistä käsitellään tässä luvussa ja kaksi myö-hemmissä luvuissa.

1. Sähköpostin arviointi (lähettäjä, linkit, liitteet ja raportointi)
2. Yleinen varovaisuus (sis. vapaa-aika ja muiden henkilöiden varoit-taminen)
3. Tietoturvaymmärrys tai -kiinnostus
4. Henkilökortit, fyysinen turvallisuus, turvallisuusohjeet ja -koulu-tukset
5. Negatiivinen kokemus



KUVIO 12 Hoxhuntin vaikutukset avoimissa vastauksissa teemojen mukaan.

Sähköposteihin liittyvät vastaukset yhdistettiin yhdeksi teemaksi: *Sähköpostin ar-viointi (lähettäjä, linkit, liitteet ja raportointi)*. Tähän teemaan sisältyivät kaikki vas-taukset, jotka sisälsivät maininnan sähköpostista, sen lähettäjästä tai sen luotet-tavuudesta, linkeistä, sähköpostin liitteistä tai niiden luotettavuuden arvioin-nista, sekä vastaukset, joissa viitattiin sähköpostin raportointiin. Vastaajista 153 henkilöä eli 86 % kertoi Hoxhuntin vaikuttaneet sähköpostien arviointiin. Tulos vastaa numeraalisten kysymysten vastauksia. Edellä, luvussa 4.3 kerrottiin, että 84–88 % vastaajista kertoi huomion lisääntyneen sähköpostien arvioinnissa. Vas-taajat kertoivat kiinnittävänsä aiempaa enemmän huomiota sähköpostiviesteihin ja niiden sisältöihin. Tarkkuus kohdistui erityisesti viestin lähettäjään, linkkeihin

ja liitteisiin. Monet vastaajat kertoivat, että he eivät enää automaattisesti klikkaa linkkejä tai avaa liitteitä ilman, että ovat tarkistaneet niiden alkuperän. Avoimia vastauksia esitellään jatkossa sitaateissa kuvaamaan tyypillistä vastausta kyseisestä teemasta.

> "Tarkistan sähköpostin lähettäjän, liitteet ja linkit nykyisin paljon aiempaa tarkemmin ennen viestin avaamista."

> ”Kaikki yhtään epämääräinen s-posti tulee raportoiduttua heti. Ehkä sen vuoksi saapunutta sähköpostia tavallaan "skannaa" eri silmillä, vaikka tuskin normaalistikaan tulisin avanneeksi odottamattomilta lähettäjiltä tulleita linkkejä.”

Toisena teemana tunnistettiin *Yleinen varovaisuus (sis. vapaa-aika ja muiden henkilöiden varoittaminen).* Tähän teemaan liittyivät kaikki maininnat kohonneesta varovaisuudesta liittyen tietoturvallisuuteen tai huijauksiin, sekä maininnat vaikutuksista vapaa-aikaan. Vastaajista 47 henkilöä eli 27 % kertoi vaikutuksia olleen yleiseen varovaisuuteen tai vapaa-aikaan. Monet vastaajat kertoivat suhtautuvansa sähköposteihin ja viestintään yleisesti ottaen aiempaa kriittisemmin. Tämä näkyi sekä työelämässä, että vapaa-ajalla, mikä viittaa siihen, että Hoxhuntin vaikutus ulottuu myös henkilökohtaisiin toimintatapoihin.

> "Olen varovaisempi sekä töissä että vapaa-ajalla sähköpostin, sosiaalisen median, verkkopankin yms. kanssa. Jaan tietoa myös läheisilleni (puoliso ja lapset) tietoturvasta, riskeistä ja mahdollisista väärinkäytöksistä."

> ”Hoxhuntin ansiosta kiinnitän enemmän huomiota kaikkeen mahdollisesti epäilyttävään eli mielestäni minusta on tullut terveellisen epäluuloinen kaikkea kohtaan…”

Kolmantena teemana oli *Tietoturvaymmärrys tai -kiinnostus.* Tähän teemaan kuuluivat kaikki vastaukset, joissa mainittiin parantunut ymmärrys tai kiinnostus tietoturvallisuudesta, huijaustekniikoista tai yleisesti tietojenkalastelusta. Lisäksi luokkaan sisällytettiin vastaukset, joissa mainittiin Hoxhuntin pelillisyys. Jotta vastauksen osa luokiteltiin tähän ryhmään, tuli sen sisältää jokin muu ajatus kuin pelkästään sähköpostiin liittyvä tietojenkalastelu. Vastaajista 19 henkilöä eli 11 % kertoi, että Hoxhunt on vaikuttanut heidän tietoturvaymmärrykseensä. Osa vastaajista koki, että heidän ymmärryksensä tietoturvasta on syventynyt. Hoxhuntin pelillinen lähestymistapa sai kiitosta vastaajilta, ja monet kokivat, että koulutus auttoi ymmärtämään paremmin tietojenkalasteluun liittyviä riskejä.

> "Hoxhunt on lisännyt ymmärrystä asioista, joihin sähköposteissa on kiinnitettävä huomiota."

> ”Epäilen lähetettyä sähköpostia phishingiksi hyvin matalalla kynnyksellä. Pelillistäminen tekee sen, että haluan mahdollisimman nopeasti raportoida epäilyttävät postit. Tuplatarkistan silti aina ennen raportointia, että kyseessä on todella Hoxhunt-posti, koska oppiminen ja oikea toimintatapa on mielestäni tärkeämpi kuin peli…”

Hoxhuntin vaikutuksista kertoo myös Hoxhunt-palveluomistaja (2024). Hän kertoo, että Hoxhunt on vaikuttanut Verohallinnon työntekijöihin kolmella tapaa: valppaustason nousuna, viestien tarkempana tutkimisena ja tietoturvallisuuden yleisenä huomioimisena. Työntekijöiden valppaustaso on noussut, mikä näkyy käyttäjien kommenteissa ja raporteissa. Toiseksi käyttäjät tukivat viestejä tarkemmin kuin aikaisemmin, eivätkä niin herkästi klikkaile tuntemattomia viestejä. Kolmanneksi tietoturvallisuuden yleinen huomioiminen on noussut, mikä näkyy

Vaikutuksista kertoo myös se, että Verohallinto vaikuttaa pärjäävän kansainvälisessä vertailussa muihin organisaatioihin verrattuna hyvin. Verrattaessa Hoxhunt-viestien klikkauslukuja, eli siis sitä, kuinka usein Hoxhunt-simulaation linkkiä klikataan, taso on Verohallinnossa kansainvälistä vertailulukua parempi. Verohallinnon keskimääräinen klikkausprosentti on Hoxhunt-palveluomistajan (2024) mukaan noin 2 %, kun se vastaavilla organisaatioilla Hoxhuntin oman ilmoituksen mukaan on noin 5 %. Tässä tutkimuksessa ei ole selvitetty sitä, mikä oli klikkausprosentti ennen Hoxhuntin käyttöönottoa.

4.4 Positiivisia vaikutuksia myös muihin turvallisuuden osa-alueisiin

Tulosten perusteella Hoxhunt on vaikuttanut positiivisesti tietojenkalastelulta suojautumisen lisäksi myös muihin turvallisuuden osa-alueisiin. Aiemmin kuviossa 11 ja taulukossa 2 (s. 36 ja 37) on esitetty Hoxhuntin vaikutukset turvallisuuden eri osa-alueissa. Kokonaisuutena voidaan havaita, että vastaukset jakautuvat vastausvaihtoehtojen osalta eri kysymysten ja turvallisuuden osa-alueiden välillä. Tulokset käydään läpi vaikuttavuusjärjestyksessä niin, että vaikuttavin on se turvallisuuden osa-alue, joka on saanut suurimman keskiarvon vastausten tuloksissa. Tämä on lähes sama järjestys, yhtä poikkeusta lukuun ottamatta, kuin jos verrattaisiin Hoxhuntin seurauksena lisääntynyttä huomion määrää, eli vastausten neljä ja viisi yhdistettyä osuutta. Turvallisuuden osa-alueet ryhmitellään vaikuttavuuden perusteella. Tämän jälkeen käsitellään kyselyn avoimet vastaukset ja Hoxhunt-palveluomistajan näkemykset.

Turvallisuushäiriöistä ilmoittaminen käsiteltiin jo aiemmin. Mainittavaa kuitenkin, että se liittyy sekä tietojenkalastelulta suojautumiseen että muihin turvallisuuden osa-alueisiin. Verohallinnossa työntekijät voivat raportoida epäilyttäviä sähköpostiviestejä suoraan sähköpostilaatikosta. Tämän lisäksi esimerkiksi fyysisen turvallisuuden turvallisuushäiriöistä voi raportoida muuta kautta. (Hoxhunt-palveluomistaja, 2024). Turvallisuushäiriöistä ilmoittaminen koskettaa siis kaikista häiriöistä ilmoittamista, ei pelkästään tietojenkalastelusta ilmoittamista. Huomion määrä on lisääntynyt turvallisuushäiriöistä ilmoittamisen osalta. Turvallisuushäiriöistä ilmoittaminen (58 %) sijoittui vastaajien mielestä seuraavan kahden osa-alueen, turvallisuuskoulutusten ja turvallisuusohjeiden, kanssa samalle tasolle. 58–50 % vastaajista koki huomion lisääntyneen näissä osa-alueissa.

Turvallisuuskouluksiin osallistuminen on seuraavana tietojenkalastelun jälkeen lisääntyneen huomion määrässä mitattuna. 55 % vastaajista koki, että Hoxhunt on vaikuttanut huomion määrään lisäävästi jonkin verran tai paljon enemmän koskien turvallisuuskoulutuksiin osallistumista. 43 % vastaajista koki, että Hoxhuntilla ei ollut vaikutusta. 2 % vastaajista koki, että Hoxhunt oli vaikuttanut vähentävästi jonkin verran tai paljon vähemmän huomion määrään.

Verohallinnon turvallisuusperiaatteet ja ohjeet ovat tuloksissa hyvin lähellä turvallisuuskouluksiin osallistumista. 50 % vastaajista koki, että Hoxhunt on vaikuttanut huomion määrään lisäävästi jonkin verran tai paljon enemmän koskien turvallisuusohjeita. 45 % vastaajista koki, että Hoxhuntilla ei ollut vaikutusta. 5 % vastaajista koki, että Hoxhunt oli vaikuttanut vähentävästi jonkin verran tai paljon vähemmän huomion määrään.

Tuloksista voidaan huomata seuraava neljän osa-alueen ryhmä, jota vastaajat ovat arvioineet samankaltaisesti: työaseman lukitseminen sen luota poistuttaessa, toimitilaan saapuminen, niin, että samalla ovenavauksella ei pääse sisään muita, oman henkilökortin näkyvillä pitäminen ja muiden henkilökortin näkyvillä pitäminen Verohallinnon tiloissa. 38–32 % vastaajista koki huomion lisääntyneen näissä osa-alueissa.

Työaseman lukitsemisella tarkoitetaan työasemalta, esimerkiksi kannettavan tietokoneelta, uloskirjautumista niin, että sitä ei voi käyttää syöttämättä salasanaa. Työaseman lukitseminen sen luota poistuttaessa eroaa vaikuttavuudeltaan edellisistä osa-alueista. Enää 36 % vastaajista koki, että Hoxhunt on vaikuttanut huomion määrään lisäävästi jonkin verran tai paljon enemmän. 60 % vastaajista koki, että Hoxhuntilla ei ollut vaikutusta. Noin 5 % vastaajista koki, että Hoxhunt oli vaikuttanut vähentävästi jonkin verran tai paljon vähemmän huomion määrään.

Toimitilaan saapuminen asettuu lähes samalle tasolle työaseman lukitsemisen kanssa. 38 % vastaajista koki, että Hoxhunt on vaikuttanut huomion määrään lisäävästi jonkin verran tai paljon enemmän. 56 % vastaajista koki, että Hoxhuntilla ei ollut vaikutusta. 5 % vastaajista koki, että Hoxhunt oli vaikuttanut vähentävästi jonkin verran tai paljon vähemmän huomion määrään. Tässä osa-alueessa vastausten keskiarvo asettui vähän työaseman lukitsemisen alapuolelle, vaikka vastaajista suurempi osa koko lisääntynyttä huomiota.

Oman henkilökortin näkyvillä pitäminen ja muiden henkilökorttien näkyvillä pitämiseen kiinnitti Hoxhuntin takia enemmän huomiota lähes saman verran vastaajista. 33 % vastaajista koki, että Hoxhunt on vaikuttanut huomion määrään lisäävästi jonkin verran tai paljon enemmän oman henkilökortin näkyvillä pitämiseen Verohallinnon tiloissa. Vastaava luku muiden henkilökorttien osalta oli 32 %. Molemmissa osa-alueissa 60 % vastaajista koki, että vaikutusta ei ollut. Myös molemmissa osa-alueissa noin 5 % vastaajista koki, että Hoxhunt oli vaikuttanut jonkin verran vähemmän tai paljon vähemmän huomion määrään.

Vaikuttavuudeltaan viimeisen ryhmän muodostavat poistumisteiden sijainti, sekä palosammuttimien ja palopostien sijainti. Tässä ryhmässä vaikuttavuus oli heikoin. Poistumisteiden sijainnin osalta 17 % vastaajista koki, että Hoxhunt on lisännyt huomion määrää jonkin verran tai paljon. Kolme neljästä vastaajasta (75 %) koki, että vaikutusta ei ollut. 8 % vastaajista koki, että Hoxhunt vaikutti huomion määrää jonkin verran vähemmän tai paljon vähemmän.

Palosammuttimien ja palopostien sijainnin osalta 16 % vastaajista koki, että Hoxhunt on lisännyt huomion määrää jonkin verran tai paljon. Vähän alle kolme neljästä (73 %) koki, että vaikutusta ei ollut. Noin 11 % vastaajista koki, että Hoxhunt vaikutti huomion määrää jonkin verran vähemmän tai paljon vähemmän.

Turvallisuuden eri osa-alueissa vaikuttavuudeltaan selvän kärjen muodosti tietojenkalastelulta suojautuminen. Tarkasteltaessa kaikkia vastauksia voidaan tietojenkalastelulta suojautumisen lisäksi tunnistaa kolme ryhmää, joissa vaikuttavuus on ollut samankaltaisella tasolla. Seuraavaksi taulukossa 3 on kuvattu turvallisuuden eri osa-alueet ryhmittäin. Otsikoksi on valittu jokin ryhmää kuvaava ominaisuus tai joitakin ryhmää kuvaavia ominaisuuksia, ja ryhmän perässä on kuvattu vaikuttavuuden vaihteluväli prosenttina, jotka on kuvattu jo aiemmin. Tietojenkalastelulta suojautuminen -ryhmään sijoitettiin sähköpostin lähettäjän sähköpostiosoite, sähköpostin sisältö ja sähköpostin linkkien kirjoitusasu. Häiriöilmoitukset ja hallinnollinen turvallisuus -ryhmään sijoitettiin turvallisuushäiriöistä ilmoittaminen, turvallisuuskoulutuksiin osallistuminen ja turvallisuusperiaatteet ja -ohjeet. Toimitila- ja henkilöstöturvallisuuteen sijoitettiin työaseman lukitseminen sen luota poistuttaessa, toimitilaan saapuminen niin, että samalla oven avauksella ei pääse luvattomia henkilöitä, oman henkilökortin näkyvillä pitäminen ja muiden henkilökorttien näkyvillä pitäminen Verohallinnon tiloissa. Huomioitavaa on, että työaseman lukitseminen on osa tietoturvallisuutta, vaikka tässä yhteydessä määriteltiin kuuluvan toimitilaturvallisuuteen.

TAULUKKO 3 Hoxhuntin vaikuttavuus ryhmittelyn perusteella.

		%
1. Tietojenkalastelulta suojautuminen		84–88
	Sähköpostin lähettäjän sähköpostiosoite	88
	Sähköpostin sisältö	87
	Sähköpostin linkkien kirjoitusasu	84
2. Häiriöilmoitukset ja hallinnollinen turvallisuus		50–58
	Turvallisuushäiriöstä ilmoittaminen	58
	Turvallisuuskoulutuksiin osallistuminen	55
	Turvallisuusperiaatteet ja -ohjeet	50
3. Toimitila- ja henkilöstöturvallisuus		32–38
	Työaseman lukitseminen sen luota poistuttaessa	36
	Toimitilaan saapuminen niin, että samalla oven avauksella ei pääse luvattomia henkilöitä	38
	Oman henkilökortin näkyvillä pitäminen Verohallinnon tiloissa	33
	Muiden henkilökorttien näkyvillä pitäminen Verohallinnon tiloissa	32
4. Pelastusturvallisuus		16–17
	Poistumisteiden sijainti	17
	Palosammuttimien ja palopostien sijainti	16

Vastaajien avoimista vastauksista voimme saada lisää tietoa Hoxhuntin vaikutuksista turvallisuuden muihin osa-alueisiin. Avoimia vastauksia käsiteltiin aiemmin luvussa 4.3 ja kuviossa 12. Avointen vastausten neljäntenä teemana oli *Henkilökortit, fyysinen turvallisuus, turvallisuusohjeet ja -koulutukset*. Samaan

teemaan oli yhdistetty kaikki vastaukset vaikutuksista turvallisuuden muihin osa-alueisiin. Vastaajista 4 henkilöä koki, että Hoxhunt on vaikuttanut myös muihin turvallisuuden osa-alueisiin. Henkilöt mainitsivat yhteensä neljä eri asiaa: henkilökorttien käyttämisen, vieraiden henkilöiden saapumisen estämisen, turvallisuusohjeisiin perehtymisen, turvallisuuskouluksiin osallistumisen ja tarkemman huolehtimisen muistiinpanovälineistä. Seuraavassa on sitaatteja avoimista vastauksista.

> ”… Olen tarkempi saapuneiden sähköpostien ja linkkien avaamisen kanssa. Käytän aina henkilökorttia ja katson aina ettei ovesta pääse sisään "vieraita" henkilöitä.”

> ”Olen Hoxhuntin myötä perehtynyt entistä tarkemmin annettuihin turvallisuusohjeisiin ja innostunut osallistumaan myös Turvan [turvallisuusyksikön] järjestämiin erilaisiin koulutuksiin.”

> ”… Tiedostan riskejä ihan konkreettisella tasolla. Entistä useammin siirrän esim. muistiinpanovihkonikin päivän päätteeksi kaappiin enkä jätä esille.”

Hoxhuntin vaikutuksista muihin turvallisuuden osa-alueisiin kertoo Hoxhunt-palveluomistaja (2024). Hän kertoo seuraavansa sisäisen viestintäkanavan ja erillisten henkilöstökyselyn kautta henkilöstön palautteita ja kommentteja. Näiden perusteella hän arvioi, että Hoxhunt vaikuttaa valppauteen kaikkien viestien suhteen, sekä työpaikalla mutta myös vapaa-ajalle. Tämän Hoxhunt saattaa lisätä kiinnostusta muuhunkin turvallisuuteen: ”…joissakin palautteissa on myös se, että on saanut sitten kipinän kiinnostuksen siihen muuhunkin turvallisuuteen… niin sitten sitä tietoisuutta on saanut kasvatettua vähän muihinkin osa alueisiin, kuin pelkästään sitten siihen kalasteluun.”.

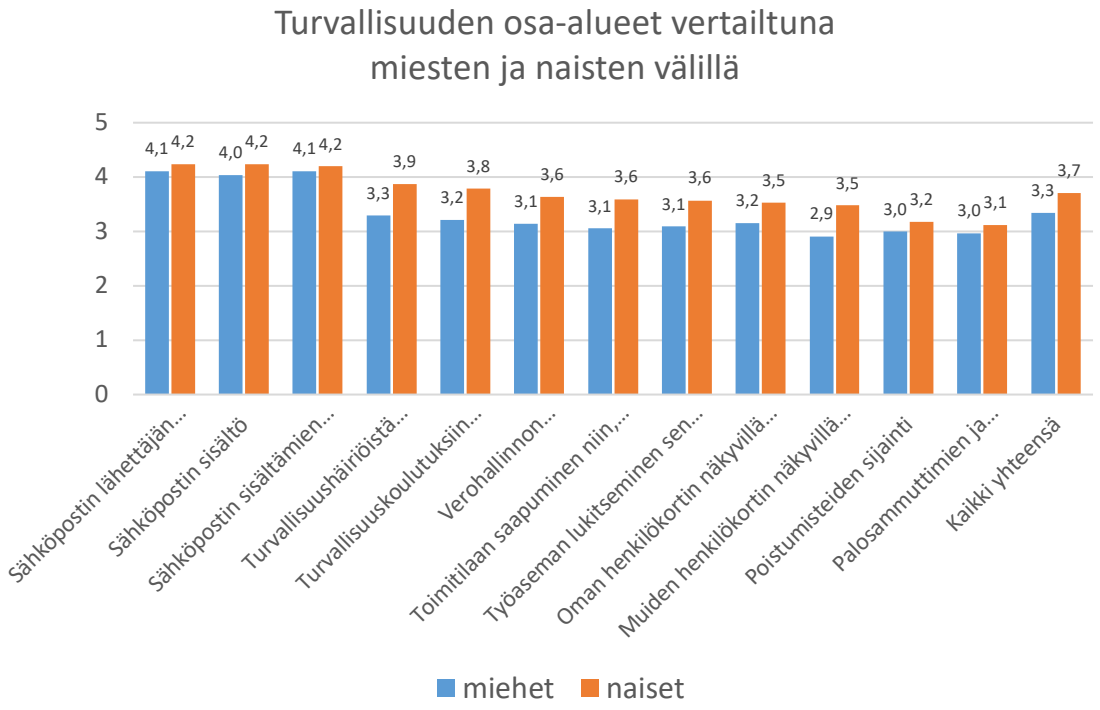
4.5 Naiset kokivat vaikutukset suuremmiksi kuin miehet

Naiset kokevat Hoxhuntin vaikuttavan enemmän kuin miehet. Tarkastellaan aluksi tuloksia miesten ja naisten turvallisuuden osa-aluekohtaisten vastausten keskiarvojen kautta ja sen jälkeen osa-aluekohtaisesti. Molemmat näkökulmat ovat tarpeen, sillä niistä voidaan havaita eroja miesten ja naisten välillä. Keskiarvot luovat näkymän kokonaisuuteen ja osa-aluekohtainen läpikäynti paljastaa eroja miesten ja naisten suhtautumisessa Hoxhuntin vaikuttamaan huomion määrään. Kyselyyn vastasi 36 miestä ja 180 naista. Miesten osuus on otannassa suhteellisen pieni, vain kuudesosa (17 %). Tuloksissa otettiin huomioon ne, jotka ilmoittivat sukupuolekseen mies tai nainen. Muunsukupuoliset ja ne, jotka eivät halunneet kertoa sukupuoltaan jätettiin tarkastelun ulkopuolelle.

Aiemmin on kerrottu, että kaikista kyselyyn vastaajista 79 % kertoi Hoxhuntin vaikuttaneen omaan käyttäytymiseensä. Kun tarkastellaan miesten osuutta vastaajista huomateen, että hieman suurempi osa miehistä kertoi Hoxhuntin vaikuttaneen heidän käyttäytymiseensä. Miesten osalta ”*en osaa sanoa*” vastausten osuus oli naisia pienempi. Miehistä 83 % (n=30) kertoo Hoxhuntin vaikuttaneen omaan käyttäytymiseensä, 11 % (n=4) kertoo, että se ei vaikuttanut

ja 6 % (n=2) ei osannut sanoa. Naisista 79 % (n=143) kertoo Hoxhuntin vaikuttaneen omaan käyttäytymiseensä, 11 % (n=19) kertoo, että se ei vaikuttanut ja 10 % (n=18) ei osannut sanoa (n=). Ristiintaulukoinnin riippumattomuustesti (χ^2= 0,85; vapausasteita=2 ja p=0,65) kuitenkin osoittaa, että näistä tuloksista ei voida todeta sukupuolten välillä olevan eroa. Koska p-arvo (0,65) on selvästi yli yleisesti käytetyn merkitsevyyden rajan (p=0,05), miesten ja naisten vastausten eroilla ei ole tilastollisesti merkitsevää riippuvuutta. Tämä ei kuitenkaan tarkoita, etteikö eroa voisi todellisuudessa olla miesten ja naisten välillä, vaikka merkitsevää riippuvuutta ei todettu.

Kyselyssä selvitettiin Hoxhuntin vaikutuksia turvallisuuden eri osa-alueisiin seuraavan kysymyksen kautta. *K6: Onko Hoxhunt vaikuttanut käyttäytymiseesi työhön liittyen? Arvioi osa-alueita seuraavalla asteikolla 1–5.* Kysymys vastausvaihtoehtoineen on käsitelty aiemmin luvussa 4.3. Kuviossa 13 on esitetty turvallisuuden osa-alueiden vertailu miesten ja naisten välillä.



KUVIO 13 Turvallisuuden osa-alueiden keskiarvot miesten ja naisten välillä.

Miesten ja naisten suhtautumisessa Hoxhuntin vaikuttavuuteen havaitaan tulosten perusteella eroa. Kun verrataan miesten ja naisten keskimääräistä suhtautumista Hoxhuntin vaikuttavuuteen, naiset kokevat sen järjestäen suuremmaksi jokaisella osa-alueella. Kun verrataan kaikkia turvallisuuden osa-alueita yhteensä, miehet kokevat vaikutukset keskimäärin tasolle 3,3 ja naiset tasolle 3,7 (asteikolla 1–5). Naiset kokivat Hoxhuntin vaikutukset noin 11 % suuremmiksi kuin miehet. Vertailun helpottamiseksi käytetään samaa turvallisuuden osa-alueiden ryhmittelyä kuin aiemmin on luvussa 4.4 esitetty. Lähimpänä miesten ja naisten näkemykset ovat tietojenkalastelulta suojautumista ja poistumisturvallisuutta

koskevissa kysymyksissä. Erot näissä ryhmissä ovat keskimäärin 0,1–0,2 yksikköä. Eniten miesten ja naisten näkemykset eroavat toisistaan ryhmässä häiriöilmoitukset ja hallinnollinen turvallisuus, jonka osalta ero on keskimäärin 0,5–0,6 yksikköä eli naisiin vaikutukset olivat 16–18 % suuremmat miehiin verrattuna. Toiseksi eniten näkemykset eroavat toisistaan toimitila- ja henkilöstöturvallisuuden ryhmässä. Naiset kertoivat 12–20 % suuremmista vaikutuksista.

Miesten vastaukset eroavat naisten vastauksista muullakin tapaa kuin pelkän keskiarvon perusteella. Miestä huomattavasti pienempi osuus kiinnitti paljon enemmän huomiota turvallisuuden osa-alueisiin. Tietojenkalastelulta suojautumisen osalta miesten ja naisten tulosten keskiarvot ovat lähes samat. Jos verrataan vastaajia, jotka kokivat Hoxhuntin lisänneen huomiota paljon enemmän, huomataan merkittävä ero. Miehet antoivat suhteellisesi noin puolet vähemmän näitä vastauksia: sähköpostin lähettäjän osoite: naiset 37 % ja miehet 19 %, sähköpostin sisältö: naiset 38 % ja miehet 19 % ja sähköpostin sisältämät linkit: naiset 40 % ja miehet 19 %. Taulukossa 4 on esitetty miesten ja naisten vastaukset turvallisuuden osa-aluekohtaisesti.

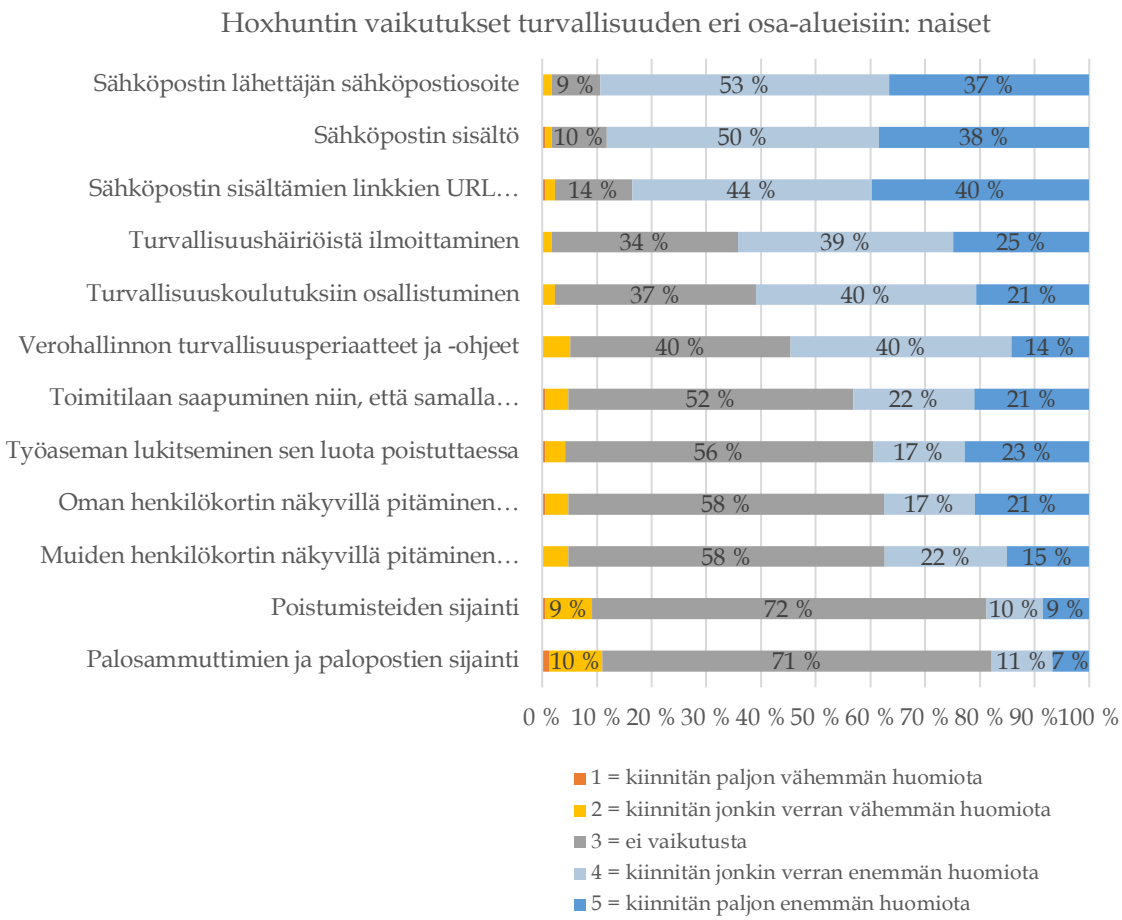
TAULUKKO 4 Turvallisuuden osa-alueet vertailu miesten ja naisten välillä.

		1		2		3		4		5		n Yht.	Keskiarvo (1–5)	
		n	%-osuus	n	%-osuus	n	%-osuus	n	%-osuus	n	%-osuus			
Sähköpostin lähettäjän sähköpostiosoite	miehet	0	0 %	0	0 %	3	8 %	26	72 %	7	19 %	36	4,11	x^2=5,22; vap=4; p=0,026
	naiset	0	0 %	3	2 %	16	9 %	94	53 %	65	37 %	178	4,24	
Sähköpostin sisältö	miehet	0	0 %	0	0 %	5	14 %	25	69 %	6	17 %	36	4,03	x^2=7,26; vap=4; p=0,122
	naiset	1	1 %	2	1 %	18	10 %	88	50 %	68	38 %	177	4,24	
Sähköpostin sisältämien linkkien URL…	miehet	0	0 %	0	0 %	3	8 %	26	72 %	7	19 %	36	4,11	x^2=9,99; vap=4; p=0,041
	naiset	1	1 %	3	2 %	25	14 %	77	44 %	70	40 %	176	4,20	
Turvallisuushäiriöistä ilmoittaminen	miehet	1	3 %	0	0 %	23	68 %	8	24 %	2	6 %	34	3,29	x^2=20,38; vap=4; p<0,001
	naiset	0	0 %	3	2 %	59	34 %	68	39 %	43	25 %	173	3,87	
Turvallisuuskoulutuksiin osallistuminen	miehet	1	3 %	0	0 %	25	74 %	7	21 %	1	3 %	34	3,21	x^2=22,74; vap=4; p<0,001
	naiset	0	0 %	4	2 %	62	37 %	68	40 %	35	21 %	169	3,79	
Verohallinnon turvallisuusperiaatteet ja -ohjeet	miehet	2	6 %	0	0 %	25	71 %	7	20 %	1	3 %	35	3,14	x^2=24,37; vap=4; p<0,001
	naiset	0	0 %	9	5 %	71	40 %	71	40 %	25	14 %	176	3,64	
Työaseman lukitseminen sen luota poistuttaessa	miehet	1	3 %	2	6 %	26	76 %	3	9 %	2	6 %	34	3,09	x^2=9,05; vap=4; p=0,059
	naiset	1	1 %	6	4 %	94	56 %	28	17 %	38	23 %	167	3,57	
Toimitilaan saapuminen niin, että samalla…	miehet	2	6 %	1	3 %	26	74 %	5	14 %	1	3 %	35	3,06	x^2=11,37; vap=4; p=0,023
	naiset	1	1 %	7	4 %	87	55 %	37	24 %	25	16 %	157	3,59	
Oman henkilökortin näkyvillä pitäminen…	miehet	1	3 %	1	3 %	26	76 %	4	12 %	2	6 %	34	3,15	x^2=7,19; vap=4; p=0,126
	naiset	1	1 %	7	4 %	97	58 %	28	17 %	35	21 %	168	3,53	
Muiden henkilökortin näkyvillä pitäminen…	miehet	3	9 %	1	3 %	26	76 %	4	12 %	0	0 %	34	3,91	x^2=23,12; vap=4; p<0,001
	naiset	0	0 %	8	5 %	96	58 %	37	22 %	25	15 %	166	3,48	
Poistumisteiden sijainti	miehet	1	3 %	1	3 %	27	84 %	3	9 %	0	0 %	32	3,00	x^2=5,97; vap=4; p=0,202
	naiset	1	1 %	14	8 %	119	72 %	17	10 %	14	8 %	165	3,18	
Palosammuttimien ja palopostien sijainti	miehet	1	3 %	2	6 %	26	81 %	3	9 %	0	0 %	32	2,97	x^2=3,59; vap=4; p=0,463
	naiset	2	1 %	16	10 %	116	71 %	18	11 %	11	7 %	163	3,12	

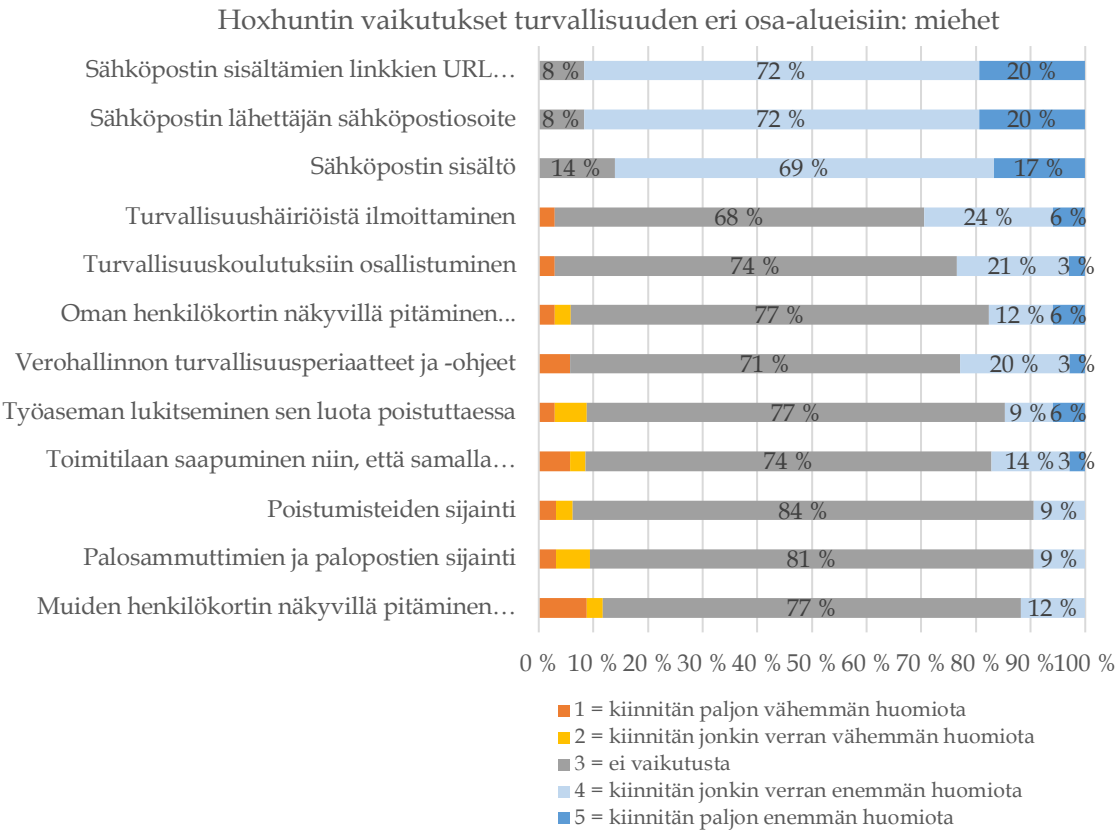
Miesten osalta Hoxhunt ei ole vaikuttanut huomion määrään kaikissa turvallisuuden osa-alueissa. Häiriöilmoitukset ja hallinnollinen turvallisuus -ryhmässä keskiarvot ovat tietojenkalastelulta suojautumisen jälkeen seuraavaksi korkeimmat (ka. 3,1–3,3). Tässä ryhmässä havaitaan myös eroa naisten kokemuksiin. Naisiin verrattuna huomattavasti pienempi osuus miehistä kiinnittää paljon huomiota Hoxhuntin seurauksena eri turvallisuuden osa-alueisiin. Miesten tason 5 vastausten määrät ovat suhteellisesti noin neljäs tai seitsemäsosa naisten vastauksiin verrattuna: turvallisuushäiriöistä ilmoittaminen: naiset 25 % ja miehet 6 %, turvallisuuskoulutuksiin osallistuminen: naiset 21 % ja miehet 3 % ja turvallisuusohjeet: naiset 14 % ja miehet 3 %.

Häiriöilmoitukset ja hallinnollinen turvallisuus ja pelastusturvallisuuden ryhmissä tuloksissa on myös merkittävää eroa. Miesten huomio ei ollut lisääntynyt niin paljon kuin naisten. *Huomio on lisääntynyt paljon* -vastauksia oli paljon vähemmän: työaseman lukitseminen: naiset 23 % ja miehet 6 %, toimitilaan saapuminen: naiset 16 % ja miehet 3 % ja oman henkilökortin näkyvillä pitäminen: naiset 21 % ja miehet 6 %. Kahdessa osa-alueessa, muiden henkilökorttien näkyvillä pitämisessä (2,91) ja palosammuttimien ja palopostien sijainnissa (2,97) keskiarvo on alle 3. Tämä tarkoittaa, että suurempi osuus vastaajista on kokenut Hoxhuntin vaikuttaneet huomioon vähentävästi. Myös poistumisteiden sijainnin osalta miehet eivät kokeneet vaikutusta huomioinnin määrään (ka. 3,0). Lisäksi näissä kolmessa osa-alueissa miehet eivät antaneet lainkaan tason 5 vastauksia.

Miesten ja naisten vastausten erot näkyvät myös *ei vaikutusta* -vastausten jakautumisessa muiden kuin tietojenkalastelun suojautuminen ryhmän osalta. Tietojenkalastelulta suojautuminen -ryhmässä miehistä 8–14 % kokee, että Hoxhuntilla ei ollut vaikutusta huomion määrään. Muissa kuin tietojenkalastelulta suojautuminen ryhmässä, miehistä 68–84 % kokee, että Hoxhuntilla ei ollut vaikutusta huomion määrään. Ryhmässä häiriöilmoitukset ja hallinnollinen turvallisuus, miehistä näin kokee 68–74 %. Toimitila ja henkilöstöturvallisuuden ryhmässä luvut ovat 74–76 % ja pelastusturvallisuuden ryhmässä 81–84 %. Naisten osalta vastaavaa selvää eroa tietojenkalastelulta suojautumisen ja muiden ryhmien välillä ei ole. Naisista 9–14 % kokee, että Hoxhunt ei ole vaikuttanut tietojenkalastelulta suojautumisen ryhmässä. Muissa ryhmissä naisista 34–72 % kokee, että Hoxhuntilla ei ollut vaikutusta. Ryhmässä häiriöilmoitukset ja hallinnollinen turvallisuus, naisista näin kokee 34–40 %. Tässä ryhmässä ero noin kaksikertainen miehiin verrattuna. Miehistä suhteellisesti noin kaksinkertainen määrä kokee, että Hoxhuntilla ei ole vaikutusta huomion määrään häiriöilmoitukset, turvallisuuskoulutukset ja -ohjeet ryhmän osalta. Toimitila ja henkilöstöturvallisuuden ryhmässä naisten luvut ovat 55–58 % ja pelastusturvallisuuden ryhmässä 71–72 %. Kuvioissa 14 on esitetty miesten vastaukset pinottuna pylväskaaviona ja kuviossa 15 vastaava kaavio naisten osalta. Kuvioista on helpommin hahmotettavissa miesten ja naisten vastausten jakautumisen erot kuten edellä sanallisesti on kuvattu.



KUVIO 14 Hoxhuntin vaikutus naisiin turvallisuuden osa-alueissa.



KUVIO 15 Hoxhuntin vaikutus miehiin turvallisuuden osa-alueissa.

Ristiintaulukoinnin merkitsevyyttä testattiin χ^2-testillä. Osassa vertailuista miesten ja naisten välillä tulokset eivät olleet tilastollisesti merkitseviä ($p>0,05$) seuraavissa osa-alueissa: sähköpostin sisältö ($p=0,122$), työaseman lukitseminen sen luota poistuttaessa ($p=0,059$), oman henkilökortin näkyvillä pitäminen ($p=0,126$), poistumisteiden sijainti ($p=0,202$) ja palosammuttimien ja palopostien sijainti. ($p=0,463$). Kokonaisuutena voidaan todeta, että kaikissa osa-alueissa naisten keskiarvot olivat miehiä suuremmat ja seitsemässä osa-alueessa havaittiin tilastollista merkitsevyyttä. Erityisesti häiriöilmoitukset ja hallinnollinen turvallisuus ryhmässä havaittiin erittäin merkittävä tilastollinen merkitsevyys ($p<0,001$) ja selvä ero keskiarvojen osalta. Tämä tarkoittaa, että Hoxhunt on vaikuttanut naisiin erityisesti tässä ryhmässä.

4.6 Yli 50-vuotiaiden osalta vaikutukset ovat suurimmat

Kyselytutkimuksessa selvitettiin iän vaikutusta tuloksiin. Yli 50-vuotiaiden osalta Hoxhunt vaikuttaa enemmän kuin alle 50-vuotiaiden osalta. Ikäryhmien vertailuissa havaittiin, että Hoxhunt lisäsi vähiten huomiota turvallisuuden osa-alueisiin 30–39-vuotiaiden ryhmässä, kun taas 60–69-vuotiailla vaikutukset olivat suurimmat. Tuloksia tarkasteltiin myös vertaamalla sukupuolen ja iän välistä suhdetta, mutta valitettavasti miesten osalta vastauksissa ikäryhmät kapenivat

liian pieniksi uskottavan vertailun suorittamiseksi. Miesten osalta eri ikäryhmissä oli vastaajia 0–9 kappaletta. Naisten osalta vastaajia eri ikäryhmissä oli enemmän, johtuen siitä, että vastaajista suurin osa oli naisia. Näin ollen tarkastelu tehtiin pelkästään ikäjakauman perusteella. Ikäryhmiä yhdistettiin niin, että alle 25-vuotiaiden vastaukset yhdistettiin 25–29 vuotiaisiin ja muodostettiin enintään 29-vuotta täyttäneiden ryhmä. Taulukossa 5 on esitetty kaikkien ikäryhmien vastausten keskiarvot turvallisuuden eri osa-alueiden osalta asteikolla 1–5. Taulukossa on käytetty ehdollista muotoilua havainnollistamaan yhden osa-alueen vastausten jakautumista ikäryhmittäin. Vertailu on suoritettu vastaavasti jokaisessa osa-alueessa.

TAULUKKO 5 Ikäryhmien vertailu turvallisuuden osa-alueissa.

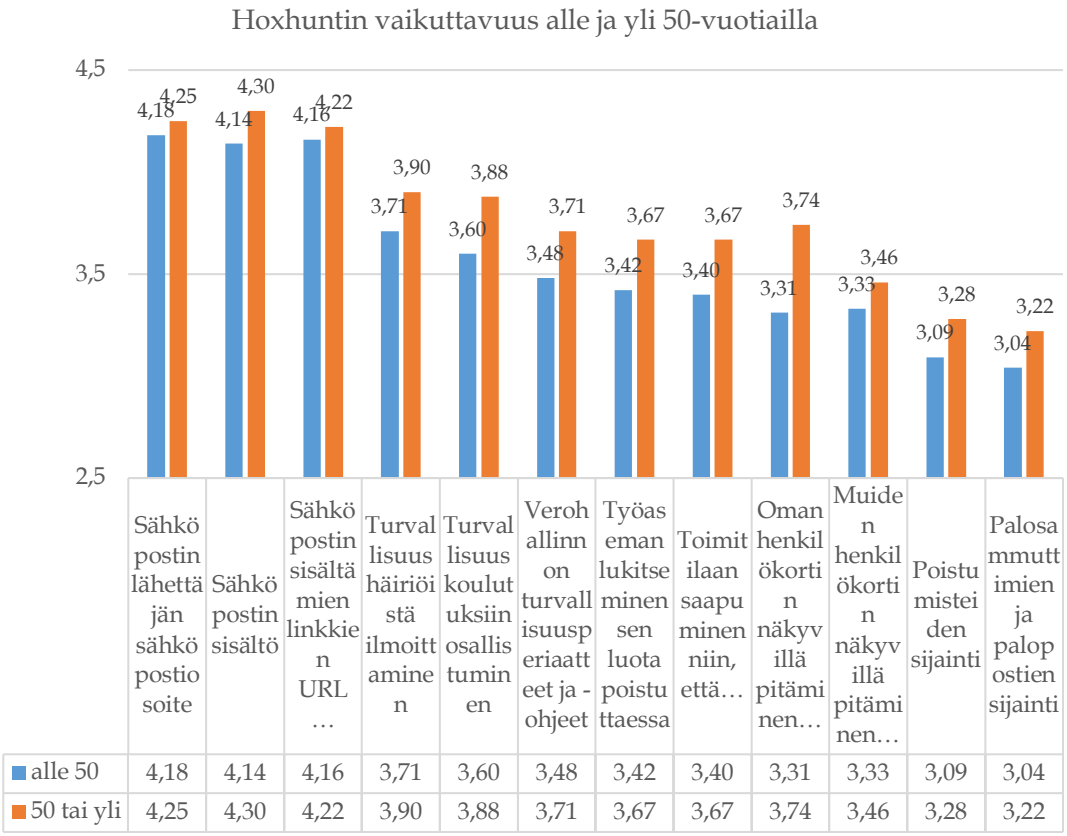
	Ikäryhmien keskiarvot asteikolla 1–5					
Turvallisuuden osa-alue	29 tai alle	30–39	40–49	50–59	60–69	kaikki
Sähköpostin lähettäjän sähköpostiosoite	4,26	4,07	4,22	4,23	4,29	4,20
Sähköpostin sisältö	4,09	4,15	4,16	4,29	4,35	4,19
Sähköpostin sisältämien linkkien URL-osoitteiden…	4,27	4,16	4,10	4,21	4,24	4,18
Turvallisuushäiriöistä ilmoittaminen	3,78	3,73	3,66	3,84	4,06	3,77
Turvallisuuskoulutuksiin osallistuminen	3,61	3,58	3,61	3,90	3,82	3,69
Verohallinnon turvallisuusperiaatteet ja -ohjeet	3,52	3,46	3,48	3,71	3,71	3,56
Työaseman lukitseminen sen luota poistuttaessa	3,52	3,36	3,42	3,62	3,81	3,50
Toimitilaan saapuminen niin, että samalla…	3,57	3,29	3,43	3,65	3,75	3,49
Oman henkilökortin näkyvillä pitäminen…	3,40	3,21	3,37	3,70	3,88	3,45
Muiden henkilökortin näkyvillä pitäminen…	3,30	3,21	3,46	3,40	3,67	3,37
Poistumisteiden sijainti	3,03	3,00	3,20	3,24	3,40	3,15
Palosammuttimien ja palopostien sijainti	2,93	2,94	3,20	3,20	3,27	3,10
Osa-alueen alhaisimipien tulosten lukumäärä	1	9	2	0	0	
Osa-alueen korkeimpien tulosten lukumäärä	1	0	0	2	10	

Vertailun perusteella kaksi ikäryhmää erottuu muista: 30–39-vuotiaat ja 60–69-vuotiaat. 30–39-vuotiaiden ryhmän osalta Hoxhuntin vaikutukset huomion määrään ovat keskimäärin kaikkein alhaisimmat. Yhdeksän osa-alueen osalta 12:sta keskiarvo on kaikkein alhaisin kaikista ikäryhmistä. Lisäksi kolmessa muussa osa-alueessa keskiarvo on alle kaikkien vastaajien keskiarvon. 60–69-vuotiaat kertoivat päinvastoin Hoxhuntin vaikuttavan lisäävästi kaikkein eniten huomion määrään. 10 osa-alueen osalta 60–69-vuotiaiden vastausten keskiarvo oli kaikkein suurin verrattuna muihin ikäryhmiin. Kahden osa-alueen osalta vastaukset olivat yli kaikkien vastaajien keskiarvon.

Vastauksista voidaan myös havaita osittaista toistuvuutta verrattaessa ikäryhmien vastauksista. Kuudessa turvallisuuden 12 osa-alueesta vastausten keskiarvot jakautuvat niin, että 29-vuotiaat tai alle ryhmään verrattuna vastausten keskiarvo laskee 30–39-vuotiaiden ryhmän osalta, minkä jälkeen se lähtee nousemaan jokaisen seuraavan ikäryhmän osalta. Toisaalta kuuden osa-alueen osalta näin ei käy.

Trendinä on Hoxhuntin vaikuttavuuden nousu 50-vuotiailla tai sitä vanhemmilla. Kuviossa 16 on esitetty pylväskaaviona koottujen ikäryhmien alle 50-

vuotiaat ja 50-vuotiaat tai yli vastausten keskiarvot. Kuviosta voidaan havaita, että jokaisessa turvallisuuden osa-alueessa yli 50-vuotiaat kertoivat Hoxhuntin vaikuttaneen enemmän huomion määrään lisäävästi. Tarkastellaan tuloksia turvallisuuden osa-alueiden ryhmittelyn kautta. Tietojenkalastelulta suojautuminen ryhmässä ero on vähäistä, vain 0,1–0,2 yksikköä. Häiriöilmoitukset ja hallinnollinen turvallisuus -ryhmässä ero on 0,2–0,3 yksikköä. Toimitila- ja henkilöstöturvallisuus -ryhmässä ero on 0,1–0,4 yksikköä ja pelastusturvallisessa molemmissa osa-alueissa 0,2 yksikköä. Suurin ero ikäryhmien välillä on oman henkilökortin mukana pitämisellä Verohallinnon tiloissa: 0,4 yksikköä.



	Sähköpostin lähettäjän sähköpostiosoite	Sähköpostin sisältö	Sähköpostin sisältämien linkkien URL …	Turvallisuushäiriöistä ilmoittaminen	Turvallisuuskoulutuksiin osallistuminen	Verohallinnon turvallisuusperiaatteet ja -ohjeet	Työaseman lukitseminen luotaessa	Toimitilaan saapuminen niin, että…	Oman henkilökortin näkyvillä pitäminen…	Muiden henkilökorttien näkyvillä pitäminen…	Poistumisteiden sijainti	Palosammutinten ja palopostien sijainti
alle 50	4,18	4,14	4,16	3,71	3,60	3,48	3,42	3,40	3,31	3,33	3,09	3,04
50 tai yli	4,25	4,30	4,22	3,90	3,88	3,71	3,67	3,67	3,74	3,46	3,28	3,22

KUVIO 16 Hoxhuntin vaikutukset alle ja yli 50-vuotiaisiin.

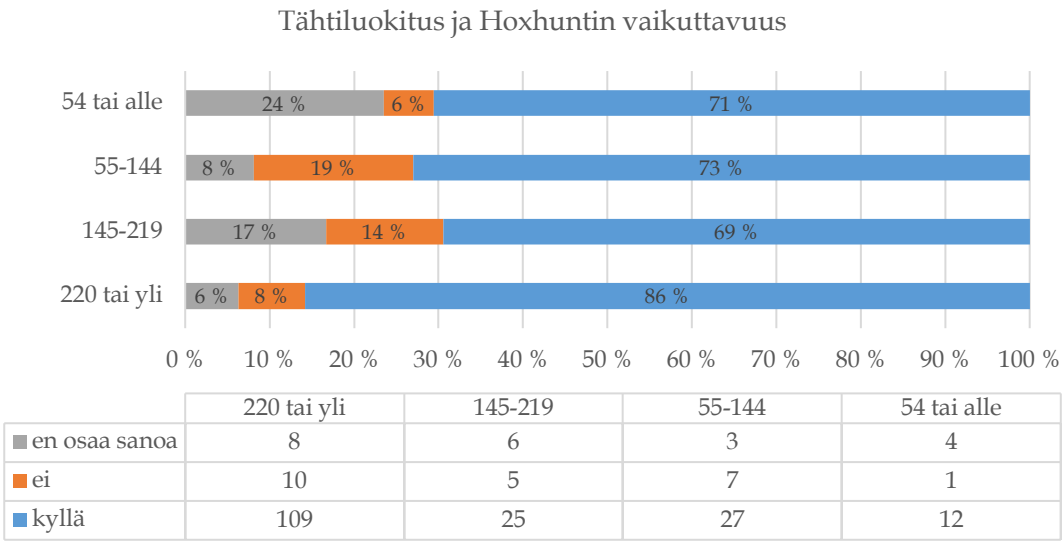
Ristiintaulukoinnin merkitsevyyttä testattiin χ^2-testillä. Taulukossa 6 on esitetty yhdistettyjen ikäryhmien alle ja yli 50-vuotiaiden vastaukset. Ristiin taulukoinnin merkittävyyden testauksessa kävi ilmi, että tulokset eivät olleet tilastollisesti merkitseviä ($p>0,05$) useassa osa-alueessa. Vain Verohallinnon turvallisuusperiaatteet ja -ohjeet ($p=0,019$), toimitilaan saapuminen niin, että sisään ei pääse muita ($p=0,029$) ja oman henkilökortin näkyvillä pitäminen ($p=0,002$) osa-alueissa tulokset ovat tilastollisesti merkittäviä. Kokonaisuutena voidaan kuitenkin arvioida, että kaikissa osa-alueissa yli 50-vuotiaiden keskiarvot ovat suuremmat ja kolmessa niistä tulokset ovat tilastollisesti merkittäviä.

TAULUKKO 6 Tarkemmat vastaukset alle ja yli 50-vuotiaiden ryhmissä.

	Ikä	1 n	2 n	3 n	4 n	5 n	n yht.	Keski-arvo (1–5)	
Sähköpostin lähettäjän sähköpostiosoite	alle 50	0	2	16	88	47	153	4,18	x^2=0,73; vap=4; p=0,950
	50 tai yli	0	1	6	37	25	69	4,25	
Sähköpostin sisältö	alle 50	1	1	21	82	47	152	4,14	x^2=3,92; vap=4; p=0,417
	50 tai yli	0	1	5	35	28	69	4,30	
Sähköpostin sisältämien linkkien URL…	alle 50	1	0	24	74	51	150	4,16	x^2=8,89; vap=4; p=0,064
	50 tai yli	0	3	7	31	28	69	4,22	
Turvallisuushäiriöistä ilmoittaminen	alle 50	1	3	58	59	25	146	3,71	x^2=6,32; vap=4; p=0,176
	50 tai yli	0	0	27	21	20	68	3,9	
Turvallisuuskoulutuksiin osallistuminen	alle 50	1	4	65	54	19	143	3,60	x^2=6,93; vap=4; p=0,139
	50 tai yli	0	0	25	25	17	67	3,88	
Verohallinnon turvallisuusperiaatteet ja -ohjeet	alle 50	1	7	72	57	12	149	3,48	x^2=11,78; vap=4; p=0,019
	50 tai yli	1	2	27	25	14	69	3,71	
Työaseman lukitseminen sen luota poistuttaessa	alle 50	2	4	93	19	24	142	3,42	x^2=8,29; vap=4; p=0,081
	50 tai yli	0	4	31	14	17	66	3,67	
Toimitilaan saapuminen niin, että samalla…	alle 50	2	4	88	31	17	142	3,40	x^2=10,79; vap=4; p=0,029
	50 tai yli	1	4	30	13	19	67	3,67	
Oman henkilökortin näkyvillä pitäminen…	alle 50	2	5	97	24	15	143	3,31	x^2=17,31; vap=4; p=0,002
	50 tai yli	0	3	33	8	22	66	3,74	
Muiden henkilökortin näkyvillä pitäminen…	alle 50	1	5	94	30	12	142	3,33	x^2=8,91; vap=4; p=0,063
	50 tai yli	2	4	34	12	13	65	3,46	
Poistumisteiden sijainti	alle 50	2	10	108	12	7	139	3,09	x^2=4,84; vap=4; p=0,304
	50 tai yli	0	5	44	9	7	65	3,28	
Palosammuttimien ja palopostien sijainti	alle 50	3	11	107	11	6	138	3,04	x^2=7,28; vap=4; p=0,121
	50 tai yli	0	7	41	11	5	64	3,22	

4.7 Pelaamalla pitkälle vahvistuu käsitys vaikuttavuudesta

Mitä pidemmälle Hoxhuntia pelaa, sitä vahvemmaksi koetaan sen vaikutukset. Kyselyssä selvitettiin sitä, kuinka pitkälle vastaajat olivat Hoxhuntia pelanneet kysymällä *K3*: *Mikä on Hoxhunt-koulutuksesta keräämäsi tähtien määrä kyselyn aikana?* Yhdestä Hoxhunt-simulaatiosta voi enimmillään kolme tähteä, jos simulaation on raportoinut riittävän nopeasti ja suorittanut sen jälkeisen mikrokoulutuksen (Hoxhunt-palveluomistaja, 2024). Tulosten perusteella iällä tai sukupuolella ei ollut merkitystä pidemmälle pelaamisen kanssa. Kuviossa 17 on esitetty Hoxhuntin tähtien määrä suhteessa siihen arvioiko vastaaja Hoxhuntin vaikuttaneen hänen käyttäytymiseensä. *K7: Onko Hoxhunt vaikuttanut mielestäsi omaa käyttäytymiseesi?*



	220 tai yli	145-219	55-144	54 tai alle
en osaa sanoa	8	6	3	4
ei	10	5	7	1
kyllä	109	25	27	12

KUVIO 17 Tähtien määrän vaikutus Hoxhuntin vaikuttavuuteen.

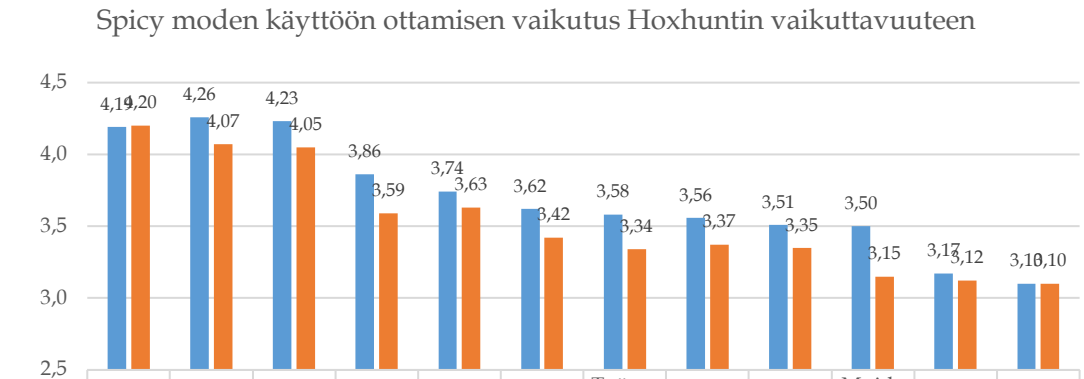
Kyselyllä tähtiluokitukset muodostettiin Hoxhunt-järjestelmästä määräytyvien omien tasojen perusteella. Tämä ei kuitenkaan osoittautunut toimivaksi ratkaisuksi, koska kaikkiin tasoihin ei tullut lainkaan vastauksia. Tähtiluokitukset yhdistettiin neljään luokkaan: 54 tai alle, 55–144, 145–219 ja 220 tai yli. Alimman luokan raja valittiin mahdollisimman lähelle 50 koska se on alin taso, jossa Spicy mode voidaan ottaa käyttöön. Tätä ei kysymyksiä laatiessa osattu ottaa huomioon.

Aiemmin on kerrottu, että 79 % kaikista vastaajista arvioi Hoxhuntin vaikuttaneen omaan käyttäytymiseensä. Tarkasteltaessa tuloksia huomataan, että vastaajista, joille tähtiä oli kertynyt alle 220, 69–73 % kertoi Hoxhuntin vaikuttaneen käyttäytymiseensä. Vasta ylitettäessä 220 tähden raja raportoitu osuus on yli keskiarvon, 86 %. Tarkasteltaessa ei-vastauksia, niiden suhteellinen osuus on suurin (19 %) 55–144 tähteä raportoinen osalta. Seitsemän vastaajaa kertoo, ettei Hoxhunt ole vaikuttanut heidän käyttäytymiseensä. Tämän jälkeen osuus lähteen laskuun. Huomattavaa myös on, että ”*en osaa sanoa*” -vastausten suhteellinen osuus on suurin aloittelijoiden ryhmässä (tähtiä 54 tai alle). Trendi on laskeva, jos tarkastellaan neljää ryhmää kokonaisuutena. Mitä enemmän tähtiä on kerätty, sitä vähemmän on epävarmuutta. Tilastollisen merkitsevyyden osalta voidaan todeta, että tulokset ovat melkein tilastollisesti merkittäviä (x^2=12,27, vapausasteet=6, p=0,056). Kokonaisuutena voidaan todeta, että mitä pidemmälle pelaa, sitä pienempi on epävarmuus Hoxhuntin vaikuttavuudesta.

4.8 Spicy modella pelaavat kokivat vaikutukset suuremmiksi

Hoxhuntin vaikutukset koetaan suuremmiksi, jos haastavammat simulaatiot eli Spicy mode on otettu käyttöön. Spicy mode tarkoittaa sitä, että Hoxhunt-simulaatioiden vaikeustaso on normaalia suurempi eli pelin vaikeuskerroin kasvaa.

(Hoxhunt-palveluomistaja, 2024). Kyselyn vastaajilta kysyttiin *K4: Oletko ottanut käyttöön Hoxhunt-koulutuksesta haastavamman version eli "Spicy moden" (kyllä / ei)?* Vastaajista 145 eli noin kaksi kolmesta (66 %) kertoi ottaneensa Spicy moden käyttöön ja vastaajista 76 eli noin kolmannes (34 %) kertoi, ettei ole ottanut. Huomion arvoista on, että myös pidemmälle pelanneiden keskuudesta löytyi henkilöitä, jotka eivät ole ottaneet haastavampi simulaatioita käyttöön. Näin ollen Spicy moden käyttöönotto ei ollut täysin riippuvainen pelkästään pidemmälle pelaamisesta. Kuviossa 18 on esitetty vertailu niiden, jotka ovat ottanee Spicy moden käyttöön ja niiden välillä, jotka eivät ole ottaneet.



KUVIO 18 Spicy moden käyttämisen vaikuttavuus.

Tuloksista voidaan nähdä, että Spicy modella pelaavat arvioivat Hoxhuntin vaikutukset suuremmiksi. Jokaisessa turvallisuuden osa-alueessa, paitsi sähköpostin lähettäjän sähköpostiosoitteessa, Spicy modella pelaavat arvoivat Hoxhuntin vaikuttavan enemmän lisäävästi huomion määrään. Sähköpostin lähettäjän sähköpostiosoitteenkin osalta molemmat ryhmät arvioivat Hoxhuntin vaikuttavan huomion määrään samalla tavalla. Suurin ero turvallisuuden osa-alueissa oli muiden henkilökorttien näkyvillä pitäminen, jossa ero *kyllä* (3,51) ja *ei* (3,15) vastauksien välillä oli 0,35 yksikköä. Toiseksi suurin ero oli turvallisuushäiriöistä ilmoittamisessa, jossa ero *kyllä* (3,86) ja *ei* (3,59) vastauksien välillä oli 0,27 yksikköä. Kolmanneksi suurin ero oli työaseman lukitseminen sen luota poistuttaessa, jossa ero *kyllä* (3,58) ja *ei* (3,34) vastauksissa oli 0,24 yksikköä. Pienimmät erot olivat jo edellä mainitun lähettäjän sähköpostiosoitteen lisäksi pelastusturvallisuudessa. Poistumisteiden sijainnin osalta *kyllä* (3,17) ja *ei* (3,12) vastausten välillä eroa oli vain 0,05 yksikköä ja palosammuttimien ja palopostien sijainnin osalta sitä ei ollut ollenkaan. Molemmissa ryhmissä keskiarvo oli 3,10.

Ristiintaulukoinnin merkitsevyyden testauksessa huomattiin, että useasta osa-alueesta ei saatu tilastollisesti merkitsevää tulosta. Taulukossa 7 on esitetty tarkemmat vastaukset osa-alueittain Spicy modella pelaavien ja ei-pelaavien välillä. Tulokset olivat merkittäviä ($p<0,05$) sähköpostin sisällön ($p=0,045$), turvallisuushäiriöstä ilmoittamisen ($p=0,038$), työaseman lukitseminen sen luota poistuttaessa ($p=0,004$), oman henkilökortin näkyvillä pitäminen ($p=0,039$) ja muiden henkilökortin näkyvillä pitämisen (0,042) osalta. Muissa osa-alueissa tulokset eivät olleet tilastollisesti merkittäviä. Kokonaisuutena voidaan todeta, että kaikissa osa-alueissa Spicy modella pelaavien keskiarvot olivat, joko yhtä suuret tai suuremmat kuin ei-pelaajien keskiarvot. Lisäksi viidessä osa-alueessa havaittiin tilastollisesti merkitsevä eroa.

TAULUKKO 7 Tarkemmat vastaukset Spicy moden pelaamisen osalta.

		1	2	3	4	5	n yht.	Keski- arvo (1–5)	
		n	n	n	n	n			
Sähköpostin lähettäjän sähköpostiosoite	kyllä	0	2	13	84	45	144	4,19	x2=0,97; vap=4; p=0,915
	ei	0	1	9	39	26	75	4,20	
Sähköpostin sisältö	kyllä	0	2	16	68	57	143	4,26	x2=9,77; vap=4; p=0,045
	ei	1	0	9	48	17	75	4,07	
Sähköpostin sisältämien linkkien URL…	kyllä	0	2	15	74	52	143	4,23	x2=7,56; vap=4; p=0,109
	ei	1	1	16	30	25	73	4,05	
Turvallisuushäiriöistä ilmoittaminen	kyllä	1	0	50	54	33	138	3,86	x2=10,12; vap=4; p=0,038
	ei	0	3	35	24	11	73	3,59	
Turvallisuuskoulutuksiin osallistuminen	kyllä	1	1	55	53	25	135	3,74	x2=3,94; vap=4; p=0,413
	ei	0	3	32	26	11	72	3,63	
Verohallinnon turvallisuusperiaatteet ja -ohjeet	kyllä	1	4	63	53	20	141	3,62	x2=4,37; vap=4; p=0,358
	ei	1	5	35	28	5	74	3,42	
Työaseman lukitseminen sen luota poistuttaessa	kyllä	1	1	82	17	31	132	3,58	x2=15,38; vap=4; p=0,004
	ei	1	7	40	16	9	73	3,34	
Toimitilaan saapuminen niin, että samalla…	kyllä	2	3	73	29	26	133	3,56	x2=8,85; vap=4; p=0,065
	ei	1	5	43	14	10	73	3,37	
Oman henkilökortin näkyvillä pitäminen…	kyllä	1	2	86	17	28	134	3,51	x2=10,08; vap=4; p=0,039
	ei	1	6	41	15	9	72	3,35	
Muiden henkilökortin näkyvillä pitäminen…	kyllä	1	3	78	29	21	132	3,50	x2=9,86; vap=4; p=0,042
	ei	2	6	47	13	4	72	3,15	
Poistumisteiden sijainti	kyllä	2	7	101	13	10	133	3,17	x2=4,09; vap=4; p=0,394
	ei	0	8	48	8	4	68	3,12	
Palosammuttimien ja palopostien sijainti	kyllä	3	9	99	12	8	131	3,10	x2=5,43; vap=4; p=0,246
	ei	0	9	46	10	3	68	3,10	

4.9 Hoxhuntin negatiiviset vaikutukset ja ”en osaa arvioida”

Tutkimuksen tuloksia on esitelty aiemmin pääasiassa huomion muuttumisen kautta, esimerkiksi minkä verran Hoxhunt vaikuttaa lisäävästi huomion määrään eri turvallisuuden osa-alueissa. Tässä luvussa tarkastellaan Hoxhuntin negatiivisia vaikutuksia, sekä sitä, miten vastaajien *”en osaa arvioida”* -vastaukset ovat kytköksissä Hoxhuntin vaikuttavuuteen. Luvussa tarkastellaan myös avointen vastausten näkökulmia, sekä Hoxhunt-palveluomistajan ajatuksia aiheesta.

Tutkimuksen tulokset eivät itsessään ole positiivisia tai negatiivisia, vaan ne ovat tuloksia, havaintoja tietystä kysymyksestä. Tämän tutkielma keskittyy tarkastelemaan Hoxhuntin vaikutuksia erityisesti huomion määrän lisääntymisenä tai vähentymisenä. Tässä luvussa negatiivisuus on määritelty avoimesti käsittämään kaikki käytökseen heikentävästi vaikuttavat seikat. Oleellista on, että vastaaja esittää muuttuneen käytöksensä negatiivisessa valossa. Esimerkiksi negatiiviset tunteet tai vastaajan näkökulmasta heikentynyt oma käytös ovat negatiivisia vaikutuksia. Kaikista vastuksista ei voi suoraan tulkita tarkoittaako vastaaja, että Hoxhuntin vaikutus on hänen mielestään negatiivinen vai esimerkiksi neutraali muutos käyttäytymiseen.

Avointen vastausten viidentenä teemana oli *Negatiivinen kokemus*, johon sisällytettiin kaikki kielteiset ajatukset Hoxhuntin vaikutuksista. Vastaajista pieni osuus kahdeksan henkilöä eli noin 4 % kertoi suoranaisista negatiivisista kokemuksista. Negatiiviset kokemukset liittyivät yleiseen luottamuspulaan, liian nopeaan raportointiin, Hoxhunt-järjestelmän ongelmiin ja epäluuloisuuteen. Pahiten ja lyhyimmällä vastauksella Hoxhuntin vaikutuksia kertoo eräs vastaajista, joka kertoo Hoxhuntin vaikuttaneen yleiseen luottamukseen.

> ”En luota enää mihinkään”

Eräs vastaajista kertoo negatiivisesta vaikutuksesta, koska Hoxhunt-järjestelmä kannustaa reagoimaan nopeasti mahdollisiin huijausviesteihin. Hänen mukaansa nopeasti reagoiminen ei ole toivottua. Peli palkitsee, jos Hoxhunt-simulaation raportoi riittävän nopeasti (Hoxhunt-palveluomistaja, 2024).

> ”Alussa Hoxhuntilla oli melko negatiivinen vaikutus, sillä pelin tulostilastoilla katsotaan kuka on nopein vastaamaan tai reagoimaan viestiin. Sähköposteihin nopeasti reagoiminen oli siis haluttu käyttäytymismalli… Pidän tulostilastojen seuraamista aika negatiivisen käyttäytymismallin ruokkivana tukena organisaatiolle…”

Yksi vastaajista kertoi Hoxhunt järjestelmän teknisten ongelmien aiheuttavan tuskastumista, koska Hoxhuntin lomallelähtöilmoitus tai muu ominaisuus ei toimi oikein.

> ”…hoxhunt -peli itsessään tuskastuttaa usein, kun sen toiminnot eivät toimi oikein (esim. lomalle asettamisen jälkeen viestejä tulee silti läpi, tai peli sekoilee muutenvaan itsekseen, josta käyttäjä joutuu itse kärsimään pelitilastoissaan.”

Neljä muuta vastaajaa kertoivat epäluuloisuuden tai kyynisyyden kasvaneen viestejä kohtaan. Vastauksista huokuu negatiivinen sävy vaikkakin juuri viestien aitouden epäileminen on avainasemassa tietojenkalastelun tunnistamisessa (Parsons, 2015). Kaksi vastaajista kertoo epäluuloisuuden heijastavan myös puheluihin ja sosiaalisen median käyttöön.

> ”Minusta on tullut epäluuloinen Somessa. En myöskään herkästi vastaa vieraisiin puhelinnumeroihin. …”

> ”Ei uskalla avata outoja henkilökohtaisia viestejä tai vastata kaikkiin puheluihin, siis omassa puhelimessa. En ota enää osaa mihinkään kilpailuihin somessa. Oikeastaan hermostuttaa jo koko some ja sähköinen asiointi.”

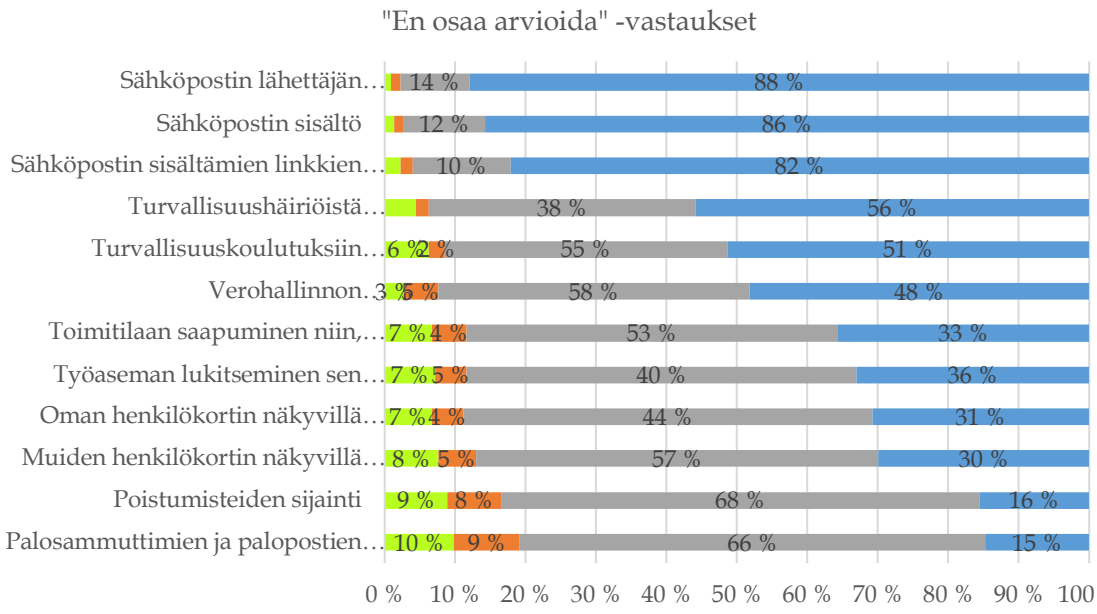
Eräs vastaajista kertoo epäilevyyden ja kyynisyyden nousseen sähköposteja kohtaan.

> ”Epäileväisyys ja kyynisyys sähköposteja kohtaan on kasvanut. Jos joku erikoinen sähköposti ei kuulu Hoxhuntiin, niin raportoin sen.”

Hoxhunt-palveluomistaja (2024) kertoi haastattelussa, että ylimääräisiksi koettujen Hoxhunt-viestien saapuminen häiritsee joitain työntekijöitä: ”Osa kokee, että se häiritsee työn tekemistä, kun sieltä tulee ylimääräisiä viestejä. Kun viestejä tulee niin paljon muutenkin niin, että he haluaisivat sitten sen takia olla mukana. Tai sitten kokee, että ne ovat niin helppoja, että ärsyttää ettei halua olla siinä mukana.”.

Viimeisenä käsitellään Hoxhuntin vaikutuksista *en osaa arvioida* -vastausten osuus. Aiemmissa luvuissa on käsitelty vastaukset, joissa vastaaja on ollut jotakin mieltä. Kuviossa 19 on esitetty ”*en osaa sanoa*” -vastaukset sekä yhdistetysti vastaukset, joissa huomio on vähentynyt (vastaukset 1 ja 2) ja vastaukset, joissa huomion määrä on lisääntynyt (vastaukset 4 ja 5). Huomioitavaa on, että esitetyt suhteelliset osuuden poikkeavat aikaisemmin kuvatuista, koska nyt huomioidaan myös tämä osuus vastaajista.

Tulokset osoittavat, että *en osaa sanoa* -vastaukset ja huomion väheneminen, vastaukset (1 ja 2), käyttäytyvät keskimäärin kääntäen verrannollisesti huomion lisääntymiseen (vastaukset 4 ja 5). Turvallisuuden osa-alueissa, joissa huomion lisääntyminen oli suurinta, oli vähiten *en osaa sanoa* -vastauksia ja myös vähiten vastauksia, joissa huomio oli vähentynyt. Esimerkiksi sähköpostin lähettäjän sähköpostin osalta huomiota enemmän kiinnitti 197 vastaajaa, vähemmän 3 ja 2 vastaajaa ei osannut arvioida vaikutusta. Vastaavasti turvallisuuden osa-alueissa, joissa huomion lisääntyminen oli vähäisintä, oli eniten ”*en osaa arvioida*” -vastauksia ja vastauksia, joissa huomio oli vähentynyt. Esimerkiksi palosammuttimien ja palopostien sijainnin osalta huomiota kiinnitti enemmän 33 vastaajaa, vähemmän 21 vastaajaa ja 22 vastaajaa ei osannut arvioida vaikusta. Tämä ei täysin toteudu kaikkien turvallisuuden osa-alueiden osalta. Jossain turvallisuuden osa-alueissa, kuten Verohallinnon turvallisuusperiaatteet ja ohjeet, havaitaan keskimääräisestä linjasta vähäisempi määrä ”*en osaa arvioida*” -vastauksia.



	Palosammuttimien ja palopostien sijainti	Poistumisteiden sijainti	Muiden henkilökortin näkyvillä pitämisen…	Oman henkilökortin näkyvillä pitämisen…	Työaseman lukitseminen sen luota poistuttaessa	Toimitilaan saapuminen niin, että…	Verohallinnon turvallisuusperiaatteet ja -ohjeet	Turvallisuuskoulutuksiin osallistuminen	Turvallisuushäiriöistä ilmoittaminen	Sähköpostin sisältämien linkkien URL…	Sähköpostin sisältö	Sähköpostin lähettäjän sähköpostiosoite
0 = En osaa arvioida vaikutusta	22	20	17	15	16	15	6	14	10	5	3	2
1 +2 = kiinnitän jonkin verran tai paljon vähemmän huomiota	21	17	12	10	10	11	11	5	4	4	3	3
3 = ei vaikutusta	148	152	128	130	124	118	99	90	85	31	26	22
4 + 5 = kiinnitän jonkin verran tai paljon enemmän huomiota	33	35	67	69	74	80	108	115	125	184	192	197

KUVIO 19 En osaa arvioida -vastauksien osuus kaikista vastauksista.

5 JOHTOPÄÄTÖKSET

Hoxhunt vaikuttaa positiivisesti huomion määrään kaikissa tutkituissa turvallisuuden osa-alueissa. Suurinta vaikutus oli tietojenkalastelun osalta. Hoxhunt vaikuttaa enemmän naisiin kuin miehiin ja jonkin verran enemmän yli 50-vuotiaisiin kuin tätä nuorempiin. Lisäksi mitä pidemmälle tai haastavampia Hoxhunt-simulaatioita pelaa, sitä enemmän positiivisia vaikutuksia ilmenee. Hoxhunt vaikuttaa negatiivisesti vain hyvin pieneen osaan vastaajista ja positiiviset vaikutukset ylittävät selvästi negatiiviset vaikutukset. Hoxhunt on lisännyt sitä pelanneiden kykyä arvioida sähköpostin lähettäjän luotettavuutta, sähköpostin linkkejä ja liitteitä. Yleinen varovaisuus on kasvanut, sekä kiinnostus tietoturvallisuuta kohtaan on noussut. Johtopäätöksenä myös on, että kouluttamalla yhtä turvallisuuden osa-aluetta voidaan vaikuttaa myös muiden turvallisuuden osa-alueiden kehittämiseen ja turvallisuuskulttuuriin. Näin ollen ei välttämättä tarvita yhtä suuria panostuksia kaikissa turvallisuuden osa-alueissa, jos yhdellä osa-alueella onnistutaan vaikuttamaan kohderyhmiin riittävästi.

Tässä luvussa esitetään tutkimuksen tulokset vastaamalla tutkimusongelmiin. Tuloksia tarkastellaan suhteessa taustakirjallisuuteen, sekä arvioidaan tulosten merkitystä luotettavuutta ja käytettävyyttä sekä esitetään jatkotutkimusaiheita. Tämän tutkimuksen tavoitteena oli arvioida Hoxhunt-tietojenkalastelukoulutuksen vaikutuksia Verohallinnon työntekijöihin seuraavien tutkimuskysymysten avulla.

Tutkimuskysymys:

1. Ovatko Verohallinnon työntekijät kokeneet Hoxhunt-tietojenkalastelukoulutuksen vaikuttaneen heidän käyttäytymiseensä?

Apututkimuskysymykset:

2. Miten Hoxhunt on vaikuttanut Verohallinnon työntekijöiden käyttäytymiseen?
3. Onko Hoxhuntilla positiivisia vaikutuksia myös muiden turvallisuuden osa-alueiden osalta?

Tutkimuksen tulokset osoittavat, että 79 % Verohallinnon työntekijöistä kokee Hoxhunt-tietojenkalastelukoulutuksen vaikuttaneen heidän käyttäytymiseensä. Vastaus tutkimuskysymykseen on siis kyllä: Verohallinnon työntekijät ovat kokeneet Hoxhuntin vaikuttaneen heidän käyttäytymiseensä. Lähes kahdeksan kymmenestä on sitä mieltä, että vaikutuksia on ollut. Tutkimuksessa selvitettiin myös miesten ja naisten vastausten eroja tähän kysymykseen. Vaikka miehet vaikuttaisivat pitävän Hoxhuntia vähemmän tehokkaana lisääntyneen huomion määrässä mitattuna, tulokset eivät osoittaneet tilastollisesti merkittävää riippuvuutta sukupuolen osalta. Tulokset tukivat hypoteesia, joka oli, että Hoxhunt on vaikuttanut työntekijöiden käyttäytymiseen.

Ensimmäisessä apututkimuskysymyksissä pohdittiin sitä, miten Hoxhunt on vaikuttanut Verohallinnon työntekijöiden käyttäytymiseen. Tähän kysymykseen saatiin myös vastauksia. Hoxhunt-koulutus on merkittävästi vaikuttanut työntekijöiden käyttäytymiseen, erityisesti heidän valppauteensa ja turvallisuuskäytäntöihinsä. Tulokset osoittavat, että koulutuksella on ollut laajaa vaikutusta sähköpostiviestinnän tarkkuuteen, yleiseen tietoturvatietoisuuteen ja raportointikäytäntöihin. Avoimissa vastauksissa vastaajista 86 % kertoi arvioivansa sähköposteja aiempaa tarkemmin. Lisäksi vaikutukset ovat ulottuneet työelämän ulkopuolelle, mikä vahvistaa koulutuksen kokonaisvaltaista merkitystä. 27 % vastaajista kertoi vaikutuksia olleen yleiseen varovaisuuteen tai vapaa-aikaan. Vaikka Hoxhuntin vaikutukset ovat pääosin myönteisiä, osa vastaajista kertoi negatiivisesta epäluuloisuuden kokemuksesta. Tulokset tukivat hypoteesia, joka oli, että Hoxhunt on parantanut työntekijöiden tietojenkalastelun tunnistuskykyä.

Toisessa apututkimuskysymyksessä pohdittiin, onko Hoxhuntilla positiivista vaikutusta myös muiden turvallisuuden osa-alueiden osalta. Huomion määrä on oleellinen tekijä turvallisuudessa, kuten tietojenkalastelun tunnistamisessa (Parsons ym., 2015). Kyselytutkimuksessa kävi ilmi, että Verohallinnon työntekijöiden huomion määrä on lisääntynyt useilla turvallisuuden osa-alueilla. Merkittävin vaikutus huomion määrään oli tietotojenkalastelun tunnistuskyvyn osalta (84–88 %). Tähän ryhmään lukeutuivat sähköpostin lähettäjän sähköpostiosoite, sähköpostin sisältö ja sähköpostin linkit. Toisiksi eniten vaikusta oli turvallisuushäiriöiden raportoinnin ja hallinnollisen turvallisuuden osalta (50–58 %). Tähän ryhmään kuuluivat turvallisuushäiriöistä ilmoittaminen, turvallisuuskoulutuksiin osallistuminen ja Verohallinnon turvallisuusperiaatteet ja ohjeet. Kolmanneksi eniten vaikutusta oli henkilöstö- ja toimitilaturvallisuuden osalta (32–38 %). Tähän ryhmään kuuluivat toimitilaan saapuminen niin, että samalla ovenavauksella ei pääse sisään luvattomia henkilöitä, työaseman lukitseminen sen luota poistuttaessa, oman henkilökortin näkyvillä pitäminen ja huomion kiinnittäminen muiden henkilökortin käyttöön Verohallinnon tiloissa. Vähäisin vaikutus oli pelastusturvallisuudessa (16–17 %). Tähän ryhmään kuuluivat poistumisteiden sijainti ja palosammuttimien ja palopostien sijainti. Huomioitavaa kuitenkin on, että osa raportoi, että Hoxhuntilla ei ollut vaikutusta ja jopa, että se vähensi huomion määrää turvallisuuden osa-alueissa. Vastaus toiseen apututkimuskysymykseen on kyllä: Hoxhuntilla on ollut vaikutusta muiden turvallisuuden osa-alueiden osalta lisääntyneenä huomion määränä. Näin ollen Hoxhunt on vaikuttanut turvallisuuteen parantavasti myös muissa osa-alueissa kuin

tietoturvallisuudessa. Tulokset tukivat hypoteesia, joka oli, että Hoxhunt on vaikuttanut positiivisesti myös muilla turvallisuuden osa-alueilla lisääntyneenä huomion määränä.

Miesten ja naisten välillä havaittiin merkittäviä eroja. Naiset arvioivat kaikilla osa-alueilla Hoxhuntin vaikutukset keskimäärin 11 % suuremmiksi kuin miehet. Suurin ero oli turvallisuushäiriöistä ilmoittamisen ja hallinnollisen turvallisuuden osalta, jossa naiset kertoivat Hoxhuntin vaikuttavan 15–17 % enemmän kuin miehet. Myös henkilöstö- ja toimitilaturvallisuuden osalta naiset kertoivat Hoxhuntin vaikuttaneen 12–20 % enemmän miehiin verrattuna. Miehet eivät keskimäärin kokeneet Hoxhuntilla olevan huomiota lisäävää vaikutusta poistumisteiden, sekä palosammuttimien ja palopostien osalta.

Tutkimus osoitti, että yli 50-vuotiaat kokevat Hoxhuntin vaikutukset suuremmiksi kuin alle 50-vuotiaat. Myös 30–39-vuotiaat erottuivat muista ikäryhmistä. Tässä ryhmässä Hoxhuntin vaikutukset olivat keskimäärin kaikkein pienimmät. Tulokset eivät olleet tilastollisesti merkitseviä kaikkien turvallisuuden osa-alueiden osalta. Vain Verohallinnon turvallisuusperiaatteet ja -ohjeet ($p=0,019$), toimitilaan saapuminen niin, että sisään ei pääse muita ($p=0,029$) ja oman henkilökortin näkyvillä pitäminen ($p=0,002$) osa-alueissa tulokset ovat tilastollisesti merkittäviä. Kokonaisuutena voidaan kuitenkin sanoa, että kaikissa osa-alueissa yli 50-vuotiaiden keskiarvot ovat suuremmat ja kolmessa niistä tulokset ovat tilastollisesti merkittäviä. Näin ollen johtopäätöksenä voidaan todeta, että yli 50-vuotiaiden osalta Hoxhunt vaikuttaa enemmän kuin alle 50-vuotiaiden osalta.

Suojautuminen tietojenkalastelua vastaan edellyttää monikerroksista lähestymistapaa, joka yhdistää tekniset ratkaisut ja käyttäjien tietoisuuden (Hong, 2012, s. 78–81; Parmar, 2012, 8–11; Almomani ym., 2013, 13–14). Keinona ovat teknologiset keinot ja käyttäjälähtöiset keinot, joita voivat olla simuloidut tietojenkalasteluharjoitukset ja mikropelit, jotka lisäävät käyttäjien kykyä tunnistaa tietojenkalasteluhyökkäyksiä (Hong, 2012, s. 79–81). Hoxhunt lukeutuu pääosin käyttäjälähtöisiin keinoihin sen koulutusnäkökulmien kautta mutta osittain myös teknologisiin keinoihin, koska tietojenkalasteluviestien raportointi on mahdollista yhdistää organisaation häiriönhallintaprosessiin Hoxhunt-järjestelmän kautta (Hoxhunt-palveluomistaja, 2024). Tutkimuksen tulokset osoittavat, että Hoxhuntilla on vaikutusta käyttäytymiseen ja tietojenkalastelulta suojautumiseen. Johtopäätöksenä voidaan todeta, että kirjallisuuden ja tulosten näkökulmasta Hoxhunt toimii tietojenkalastelua vastaan ja vaikuttaa merkittävästi tietojenkalastelulta suojautumiseen.

Raggad (2010, s. 12–13) kuvaa turvallisuuskulttuuria inhimilliseksi toiminnaksi, jonka rakentamisessa kouluttamisen tulisi luoda pohja turvallisuusperiaatteiden omaksumiselle. Tutkimus on osoittanut, että Hoxhunt vaikuttaa työntekijöiden turvallisuuskäyttäytymiseen töissä ja jopa vapaa-ajalla. Tämän voidaan ajatella olevan turvallisuuskulttuurin muodostumisesta kertovaa toimintaa. Jos henkilö itse omaksuu turvallisia toimintatapoja, joita hän toteuttaa vapaa-ajallaan, jossa työnantajalla ei ole mahdollisuutta valvoa toimintaa, voidaan ajatella samojen toimintatapojen toteutuvan myös töissä. Näin ollen Hoxhunt vaikuttaisi kehittävän turvallisuuskulttuuria kokonaisuutena pelkän tietojenkalastelukoulutuksen ohella.

Tuloksien merkitystä arvioitaessa on otettava huomioon tietoturvallisuuden lähtökohtaisen kiinnostavuuden merkitys, vaikka tutkimuksen tulos ei anna siihen selvää vastausta. Vastaajista 95 % piti tietoturvallisuutta yleisesti ja 93 % sähköpostin tietoturvaa työtehtävien kannalta kiinnostavana. Tästä lähtökohdasta ajateltuna, Hoxhunt on siis vaikuttanut merkittävästi kohderyhmään, joka on kiinnostunut tietoturvallisuudesta. Voidaan ajatella, että vaikutukset olisivat saattaneet olla vieläkin suuremmat sellaiseen kohderyhmään, jota tietoturvallisuus ei lähtökohtaisesti kiinnosta. Tähän päätelmään on kuitenkin suhtauduttava kriittisesti sillä, kiinnostavuuden alkutilannetta ei ole mitattu ja kyseessä voi olla kehäpäätelmä siltä osin, että Hoxhunt on saattanut vaikuttaa positiivisesti tähän kiinnostavuuteen. Toisaalta kiinnostavuus voi johtua muistakin tietoturvaviestinnän ja -koulutusten toimenpiteistä ja muista seikoista.

6 POHDINTA

Tutkimuksella ja sen tuloksilla on ollut merkitystä. Se osoittanut, että Hoxhunt vaikuttaa merkittävästi myös muihin turvallisuuden osa-alueisiin. Voitaisiin ajatella, että kouluttamalla yhtä turvallisuuden osa-aluetta, vaikutetaan itseasiassa turvallisuuskulttuurin kehittymiseen kokonaisuutena. Vastauksena johdannossa esittämääni kysymykseen, koen, että olen saanut akateemisen vastauksen omille ennakkoajatuksilleni siitä, että kouluttamalla tiettyä turvallisuuden osa-aluetta voidaan kehittää turvallisuustietoista ajattelua kokonaisuutena.

Tutkimuksen toteutuksessa oli puutteita, eikä se onnistunut alkuperäisen suunnitelman mukaisesti. Tutkimusta ei julkaistu siinä laajuudessa kuin oli tarkoitus. Tämän seurauksena tutkimukseni tavoitti vain osan verohallintolaisista ja otoskoko jäi tästä syystä tavoitetta pienemmäksi. Myös tästä syystä tutkimuksen otanta ei ollut riittävän laaja, jotta ristiintaulukoinnista olisi tilastotieteellisesti saatu merkitseviä tuloksia kaikissa vertailuissa. Se, että tilastollista merkitsevyyttä ei pystytty osoittamaan kaikissa tilanteissa ei kuitenkaan tarkoita, etteikö ilmiötä olisi olemassa. Nämäkin tulokset saattavat antaa suuntaa jatkotutkimuksen tekemiselle. Toisena heikkoutena oli kyselyn ikäjakauman rakentaminen. Olisi ollut helposti ennen kyselyn julkaisua selvitettävissä, miten Verohallinto itse kerää tietoa työntekijöistään. Tätä tietoa olisi voitu käyttää kyselyn lähtökohtana. Nyt kysely toteutettiin eri ikähaarukoilla, joten otoksen edustavuus ei ollut paras mahdollinen. Kolmantena, tutkimus selvitti ainoastaan vastaajien näkemyksiä Hoxhuntin vaikutuksista huomion määrään. Ei siis selvitetty sitä, millä tasolla huomio oli ennen Hoxhuntia. On siis esimerkiksi mahdollista, että huomion määrä on ollut jo ennen Hoxhuntin käyttöä korkea, joten henkilö voi arvioida, että se ei ole näin ollen lisääntynyt. On myös mahdollista, että se on jopa laskenut, jos Hoxhunt koetaan liian itsestäänselväksi, yksinkertaiseksi tai ärsyttäväksi. Neljäntenä tutkimuksessa ei myöskään tutkittu oman osallistumisen määrän merkitystä. Toisin sanoen, vaikka koulutettava saa Hoxhunt-viestejä, voi olla, että hän ei yksinkertaisesti reagoi niihin ollenkaan. Tämä vaikuttaa suoraan koulutuksen määrään mikrokoulutusten poisjääntinä ja vaikuttavuuteen kokonaisuutena. Hoxhuntissa koulutettava kannustetaan ottamaan osaa ja jatkuvasti arvioimaan viestien oikeellisuutta. Hänen omalle harkinnalleen tämän jälkeen jää, raportoiko hän viestejä vai ei. Hän altistuu siis turvallisuusajattelulla jossain

määrin jatkuvasti, mutta hänen oma osallistumisensa vaikuttaa Hoxhuntin kokonaisvaikuttavuuden määrään.

Jatkotutkimusaiheiksi ehdotan perehtymistä turvallisuuskulttuurin rakentumiseen osakokonaisuuksista. Mielenkiintoista olisi selvittää, miten yksittäiset turvallisuuskoulutukset tai ohjelmat vaikuttavat turvallisuuskulttuuriin. Ja tarkemmin, mitkä yksittäiset teot, toimet tai koulutuksen osat ovat vaikuttavimpia turvallisuuskulttuurin rakentamisessa. Onko juuri osallistaminen ja jatkuva osallistuminen avainasemassa turvallisuuskulttuurin kehittämisessä? Oma kokemukseni on, että vastaus tähän kysymykseen on kyllä, osallistumisella on merkitystä, mutta olisi mielenkiintoista saada lisää tutkimustietoa aiheesta turvallisuuskulttuurin kehittymisen kannalta.

Toisena jatkotutkimusajatuksena ehdotan vertailevaa tapaustutkimusta organisaatioon, joka on ottamassa Hoxhuntia käyttöön. Tiedonkeruu, esimerkiksi kyselytutkimus, voitaisiin suorittaa ennen Hoxhuntin käyttöönottoa ja uudestaan toisen kerran tietyn ajan kuluessa käyttöönoton jälkeen. Tällä voitaisiin vertailla lähtötilannetta ja Hoxhuntin aiheuttamaa muutosta kohderyhmässä. Samalla vertailu voitaisiin suorittaa myös verrokkiryhmän kesken, joka ei käytä Hoxhuntia. Näin ollen voitaisiin selvittää osallistavan turvallisuuskoulutuksen vaikutuksen laaja-alaisemmin organisaatioiden turvallisuuskulttuurin kehittämisen hyväksi.

LÄHTEET

Agari. (2018). Agari Email Security yrityksen internetsivut. *Hostile Landscape of Email Threats Leverages California Wildfire Tragedy.* Haettu osoitteesta 11.12.2023 https://www.agari.com/blog/hostile-landscape-of-email-threats-leverages-california-wildfire-tragedy

Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A. & Almomani, E. (2013). *A survey of phishing email filtering techniques*. IEEE Communications Surveys & Tutorials, 15(4), 2070-2090. Haettu osoitteesta https://www.researchgate.net/publication/236250451_A_Survey_of_Phishing_Email_Filtering_Techniques

BlackBerry. (2023). *MITRE ATT&CK vs Cyber Kill Chain : What's the Difference?*. Haettu osoitteesta 12.12.2023 https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/mitre-attack-vs-cyber-kill-chain

Bossomaier, T., D'Alessandro, S. & Bradbury, R. (2019). *Human dimensions of cybersecurity*. NewYork : Auerbach Publications s. 87.

Daily Mail. (2020). *Cybercriminals were using a fake Citibank website to steal debit card and social security numbers in ordet to access bank accounts.* Haettu osoitteesta 11.12.2023 https://www.dailymail.co.uk/sciencetech/article-7922171/Cybercriminals-using-fake-Citibank-website-access-bank-account.html

Hakala, M., Vainio, M. & Vuorinen, O. (2006). *Tietoturvallisuuden käsikirja*. Jyväskylä : Docendo Finland Oy. s. 4-5.

Hong, J. (2012). *The state of phishing attacks.* Communications of the ACM, 55(1), s. 74–81. Haettu osoitteesta 20.10.2024 https://dl.acm.org/doi/pdf/10.1145/2063176.2063197

Hoxhunt. (2023). *Hoxhunt internetsivut*. Haettu osoitteesta 24.11.2023 https://www.Hoxhunt.com

Hoxhunt-palveluomistaja. (2024). Hoxhunt-palveluomistajan haastattelu. Haastattelun kysymykset on nähtävissä liitteesä 1.

Hyppönen, M, (2021). *Internet.* Helsinki: WSOY. s. 73, 110-111, 247.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. Ladattu verkosta 24.11.2023 https://www.ibm.com/reports/data-breach

ISO27001. (2017). *SFS-EN ISO/IEC 27001:2017. Informaatioteknologia.* Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. s. 5.

Jagatic, T., Johnson, N., Jakobsson, M. & Mencher Filippo. (2007). *Social Phishing.* Haettu verkosta 14.12.2023 https://dl.acm.org/action/downloadSupplement?doi=10.1145%2F1290958.1290968&file=10-p94-jagatic.jp.pdf

James, L. (2005). *Phishing Exposed*. Rockland: Syngress Publishing, Inc. 2, s. 10-11. Haettu verkosta 29.11.2024 https://www.academia.edu/25034390/Syngress_Publishing_Phishing_Exposed?uc-sb-sw=304565

Kaspersky. (2023a). *Encyclopedia by Kaspersky: What is phishing?* Haettu verkosta 30.11.2023 https://encyclopedia.kaspersky.com/knowledge/what-is-phishing/

Kaspersky. (2023b). *What is Typosquatting?* Ladattu verkosta 11.12.2023 https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). *Teaching johnny not to fall for phish.* ACM Transactions on Internet Technology (TOIT), 10(2), 8–11. Haettu verkosta https://www.researchgate.net/publication/220169843_Teaching_Johnny_not_to_fall_for_phish

Laki Verohallinnosta. (2010). Verohallinnosta annettu laki (2010/503). Haettu verkosta 10.8.2024 https://www.finlex.fi/fi/laki/ajantasa/2010/20100503

Lockheed Martin. (2023). *The Kyber Kill Chain.* Haettu verkosta 12.11.2023 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE. (2023). *MITRE ATT&AK*. Haettu verkosta 12.12.2023 https://attack.mitre.org

Niettaanmäki, P., Lehto, M., Savonen, M. (2021). *Yhteiskunnan digimurros*. Jyvästäkylän yliopiston IT-tiedekunta. Haettu verkosta 23.11.2023 http://urn.fi/URN:ISBN:978-951-39-8647-6. s. 141.

Parmar, B. (2012). *Protecting against spear-phishing.* Computer Fraud & Security, 2012(1), s. 8–11. Haettu verkosta 29.11.2024 https://www.faronics.com/assets/Spearphishing_BP_EMEA.pdf

Raggad, B. (2010). *Information Security Management. Consepts and Practice.* London: Taylor & Francis Group. s. 10-16, 20.

Hadnagy, C. & Wilson, P. (2020). *Social Engineering: The Art of Human Hacking.* Ascent audio. Audiokirja. Luku 3, kohta 09.13 ja 1:06.30.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. & Jerram, C. (2015). *The design of phishing studies: Challenges for researchers.* The University on Adelaide. Haettu verkosta 14.12.2023 https://www-sciencedirect-com.ezproxy.jyu.fi/science/article/pii/S0167404815000231

Social-Engineer. (2023). *Social Engineering Framework.* Social Engineer, LLC. Haettu verkosta 11.12.2023 https://www.social-engineer.org

Suomen asiakastieto. (2023). *Hoxhunt Oy yritystiedot*. Ladattu verkosta 24.11.2023 https://www.asiakastieto.fi/yritykset/fi/hoxhunt-oy/27587227/yleiskuva

Sanastokeskus. (2018). *Kyberturvallisuuden sanasto*. TSK 52. Turvallisuuskomitea. Haettu verkosta 22.11.2023 https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. s. 17, 31.

Tietoarkisto. (2024). Tampereen yliopiston tietoarkisto. *Ristiintaulukointi.* Haettu verkosta 24.11.2024 https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/ristiintaulukointi/ristiintaulukointi/

Tietosuojavaltuutetun toimisto. (2023). *Tietojenkalasteluun perustuvat tietoturvaloukkaukset.* Haettu verkosta 6.12.2023 https://tietosuoja.fi/tietojenkalastelu

Tilastokeskus. (2024). *Tietoa tilastoista. Hypoteesi.* Haettu verkosta 30.11.2024 https://stat.fi/meta/kas/hypoteesi.html?utm_source=chatgpt.com

United States Attorney's Office. (2019). *South District of New York.* Viimeksi päivitetty 19.12.2019. Haettu verkosta 7.12.2023 https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business

Verizon. (2023). *Data Breach Investigations Report 2023.* s. 32. Haettu verkosta 14.12.2023 https://www.verizon.com/business/resources/T625/reports/2023-data-breach-investigations-report-dbir.pdf

Verohallinto. (2023a). *Verohallinto lyhyesti.* Verohallinto. Haettu verkosta 5.12.2023 https://www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/verohallinnon-vuosi/verohallinto-lyhyesti/

Verohallinto. (2023b). *Tietoa Omaverosta ja apua asiointiin*. Verohallinto. Viimeksi päivitetty 19.11.2023. Haettu verkosta 5.12.2023 https://www.vero.fi/tietoa-verohallinnosta/yhteystiedot-ja-asiointi/asioi-verkossa/tietoa-omaverosta/

Verohallinto. (2023c). *Tietoja huijauksista*. Verohallinto. Haettu verkosta 5.12.2023. https://www.vero.fi/tietoa-verohallinnosta/yhteystiedot-ja-asiointi/asioi-verkossa/tietoa-sähköisestä-asioinnista/tietoa-huijauksista/

Verohallinto. (2024). *Verohallinnon henkilöstökertomus 2023.* Verohallinnon tilastot.

Whitty, M. & Young, G. (2017). *Cyberpsychology : The Study of Individuals, Society and Digital Technologies*. Chichester: John Wiley & Sons, Incorporated. Luvut 1, 12.1-2.

Yhdysvaltojen kauppakomissio. (2023). *Federal Trade Comission*. FTC COVID-19 and Simulus Reports. Haettu verkosta 11.12.2023 https://public.tableau.com/app/profile/federal.trade.commission/viz/COVID-19andStimulusReports/Map

Åkerbland, L. & Seppänen-Järvelä, R. (2024). Monimenetelmällinen tutkimus. Opas suunnitteluun ja toteutukseen. Gaudeamus. Luku 1.1, 3.3.

LIITE 1 HAASTATTELUN KYSYMYKSET

Tässä liitteessä on kuvattu Verohallinnon Hoxhunt-palveluomistajalle esitetyt haastattelukysymykset.

1. Mikä on Hoxhunt?
2. Mihin Hoxhuntia käytetään Verohallinnossa?
3. Kuinka kauan Hoxhunt on ollut käytössä Verohallinnossa?
4. Kuinka monta käyttäjää Hoxhuntilla on Verohallinnossa?
5. Onko Hoxhuntilla ollut vaikutuksia Verohallinnon työntekijöihin?
6. Onko Hoxhuntin vaikutuksia työntekijöihin tutkittu? Jos on tutkittu, millaisia tulokset ovat olleet?
7. Onko Hoxhuntilla ollut vaikutuksia Verohallinnon turvallisuuteen? Jo on, niin millaisia vaikutuksia?
8. Mitä tietoja Hoxhunt tarjoaa Verohallinnon Hoxhuntin käytöstä?
9. Kuinka monta käyttäjää Hoxhuntissa on Verohallinnossa?
10. Onko Hoxhunt-järjestelmästä saatavissa tilastoja? Jos on, niin millaisia?
11. Kuinka monta Hoxhunt-harjoitusta Verohallinnon työntekijät ovat suorittaneet yhteensä? Entä keskimäärin työntekijää kohden?
12. Mikä on epäonnistumisprosentti keskimäärin?
13. Mitä muuta haluaisit kertoa Hoxhuntista tai sen käyttötavoista, tarkoituksesta tai muusta yksityiskohdasta, jota nyt ei ole vielä käsitelty?
14. Mikä on Spicy mode?
15. Kuinka kauan olet toiminut Hoxhunt-palveluomistajana?
16. Voitko antaa jonkin esimerkin Hoxhunt-viestistä?

LIITE 2 KYSELYN KYSYMYKSET

Tässä liitteessä on kuvattu Verohallinnon henkilöstölle lähetetyn kyselyn kysymykset. Kysymykset koostuvat taustakysymyksistä ja varsinaisista kysymyksistä. Vastausvaihtoehdot on esitetty taulukon soluissa tai erillisillä riveillä.

Taustakysymykset:

1. Ikä

alle 25	25–29	30–39	40–49	50–59	60–69	70 tai yli

2. Sukupuoli

mies	nainen	jokin muu	en halua kertoa

3. Mikä on Hoxhunt-koulutuksesta keräämäsi tähtiesi määrä kyselyyn vastaamisen aikana?

alle 9	9–14	15–21	22–30	31–41
42–54	55–69	70–89	90–114	145–179
180–219	220–264	265 tai yli		

4. Oletko ottanut käyttöön Hoxhunt-koulutuksesta haastavamman version eli "Spicy moden"

kyllä	en

5. Kuinka kiinnostavana pidät omien työtehtäviesi kannalta seuraavia aiheita…

   a) tietoturvallisuus yleisesti
   b) sähköpostin tietoturva

   Arvioi väittämiä seuraavalla asteikolla 1–5, missä…

   1 = en pidä lainkaan kiinnostavana
   2 = jonkin verran kiinnostavana
   3 = neutraali suhtautuminen
   4 = jonkin verran kiinnostavana
   5 = erittäin kiinnostavana

Varsinaiset kysymykset:

6. Onko Hoxhunt vaikuttanut käyttäytymiseesi työhön liittyen?

   Arvioi osa-alueita seuraavalla asteikolla 1–5, missä…

   0 = en osaa arvioida vaikutusta
   1 = kiinnitän paljon vähemmän huomiota
   2 = kiinnitän jonkin verran vähemmän huomiota
   3 = ei vaikutusta
   4 = kiinnitän jonkin verran enemmän huomiota
   5 = kiinnitän paljon enemmän huomiota

Arvio, kuinka paljon kiinnität sen seurauksena huomiota seuraaviin osa-alueisiin:

a) Sähköpostin lähettäjän sähköpostiosoite
b) Sähköpostin sisältämien linkkien URL-osoitteiden kirjoitusasu (eli verkko-osoitteet, jotka alkavat: ”https://”)
c) Sähköpostin sisältö
d) Työaseman lukitseminen sen luota poistuttaessa
e) Oman henkilökortin näkyvillä pitäminen Verohallinnon tiloissa
f) Muiden henkilökortin näkyvillä pitäminen Verohallinnon tiloissa
g) Toimitilaan saapuminen niin, että samalla ovenavauksella ei pääse sisään luvattomia henkilöitä
h) Poistumisteiden sijainti
i) Palosammuttimien ja palopostien sijainti
j) Verohallinnon turvallisuusperiaatteet ja -ohjeet
k) Turvallisuushäiriöistä ilmoittaminen

7. Onko Hoxhunt vaikuttanut mielestäsi omaa käyttäytymiseesi?

kyllä	ei	en osaa sanoa

8. Jos vaikutusta on ollut eli vastasit kysymykseen nro 7 ”kyllä” kuvaile tarkemmin, miten?

   [avoin vastaus]