Heikki Hakala

TYÖNTEKIJÖIDEN TIETOTURVATIETOISUUS PUOLUSTUSKEINONA SÄHKÖPOSTIKALASTELUUN PK-YRITYKSISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Hakala, Heikki
Työntekijöiden tietoturvatietoisuus puolustuskeinona sähköpostikalasteluun pk-yrityksissä
Jyväskylä: Jyväskylän yliopisto, 2024, 32 s.
Tietojärjestelmätiede, kandidaatintyö
Ohjaaja: Ari Kuusio

Inhimillisten tekijöiden, kuten huolimattomuuden ja virheiden merkitys tietomurroissa on merkittävä. Esimerkiksi Verizonin Data Breach Investigations Raportin DBIR (2023) sekä Gartnerin (2023a) tietoturvaohjeen mukaan vuonna 2022 tapahtuneissa tietomurroissa ja -vuodoissa 82 % piti sisällään inhimillisen tekijän. Tässä tutkielmassa tarkastellaan työntekijöiden tietoturvatietoisuutta puolustuskeinona sähköpostikalastelua vastaan. Ratkaisua tutkimusongelmaan haetaan kahden tutkimuskysymyksen kautta. Aluksi tarkastellaan, miten sähköpostikalastelijat pyrkivät huijaamaan kohteitaan. Ensin selvitetään sähköpostikalasteluhyökkäyksien onnistumiseen johtavia tekijöitä. Sen lisäksi arvioidaan niiden merkitystä kyberturvan kentällä. Sähköpostikalastelijoiden havaittiin huijaavan kohteitaan tekeytymällä kohteelle entuudestaan tutuksi lähettäjäksi. Toisella tutkimuskysymyksellä selvitetään tietoturvatietoisuuden rooli yrityksen tietoturvassa. Kirjallisuuskatsauksesta käy ilmi tietoturvatietoisuuden olevan perusedellytys organisaation tietoturvakulttuurin luomisessa. Sen lisäksi avataan tietoturvan, kyberturvan ja tietoturvatietoisuuden käsitteitä seikkaperäisemmin. Ihmiskeskeisen kyberturvan kautta pohditaan tietoturvatietoisuuden merkityksestä pienien ja keskisuurien yritysten eli pk-yritysten tietoturvan rakentamisessa sekä esitellään sen arvioimiseen käytettäviä mittareita. Luvussa esitellään myös työntekijän tietoturvatietoisuuteen vaikuttavia psykologisia, fysiologisia, sosiaalisia sekä organisatorisia tekijöitä. Viimeiseksi tarkastellaan työntekijöiden tietoturvatietoisuuden ja sähköpostikalastelun suhdetta ja merkitystä toisiinsa pk-yritysten näkökulmasta. Tietoturvatietoisuuden voidaan ajatella mahdollistavan yritykselle oikeanlasten sähköpostikalastelua ennaltaehkäisevien toimenpiteiden tekemisen.

Asiasanat: kyberturva, tietoturvatietoisuus, työntekijät, käyttäjät, sosiaalinen manipulointi, sähköpostikalastelu, pk-yritykset

ABSTRACT

Hakala, Heikki
Employee information security awareness as a defense against email phishing in SMEs
Jyväskylä: University of Jyväskylä, 2024, 32 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Ari Kuusio

Human factors such as negligence and errors play a significant role in data breaches. For example, according to Verizon's Data Breach Investigations Report DBIR (2023) and Gartner's (2023a) security advisory, 82% of data breaches and leaks in 2022 involved a human factor. This thesis examines employee information security awareness as a defense against email phishing. The solution to the research problem is sought through two research questions. First, the factors that lead to the success of an email phishing attack will be explored. It then assesses their relevance in the modern cyber security arena. Email phishers were found to deceive their targets by posing as a sender the recipient already knew. The second research question examines the role of security awareness in todays' cyber security of the enterprise. The literature review shows that security awareness is a basic prerequisite for creating a security culture in an organisation. In addition, the concepts of information security, cyber security and information security awareness are explained in more detail. Through a human-centred cybersecurity approach, the importance of security awareness in building information security in small and medium-sized enterprises (SMEs) will be discussed and the indicators used to assess it will be presented. The chapter also presents the psychological, physiological, social, and organisational factors that influence employee security awareness. The final chapter presents the findings of the literature review and examines the relationship and importance of the relationship between employee security awareness and email phishing from the perspective of SMEs. Security awareness can be thought to enable a company to take the right preventive measures against email phishing.

Keywords: cybersecurity, information security awareness, employees, users, social engineering, phishing, SMEs

TAULUKOT

SISÄLLYS

1 JOHDANTO

Inhimillisten tekijöiden, kuten huolimattomuuden ja virheiden merkitys tietomurroissa on merkittävä. Esimerkiksi Verizonin Data Breach Investigations Raportin DBIR (2022) sekä Gartnerin (2023a) tietoturvaohjeen mukaan vuonna 2022 tapahtuneissa tietomurroissa ja -vuodoissa 82 % piti sisällään inhimillisen tekijän. Verizonin vuoden 2023 raportissa työsähköposteihin kohdistuvien kalastelujen määrä oli yli kaksinkertaistunut edellisvuoteen verrattuna (Verizon, 2023). Arvioiden mukaan yli 80 prosenttia organisaatioista on kokenut sähköpostikalasteluhyökkäyksiä, joista seuraa miljardien dollarien tappiot vuosittain (Thomas, 2018). Useissa lähteissä, kuten Archibald & Renaud, 2019; Hadnagy & Wilson, 2010; Hadnagy & Fincher, 2015; Rohan ym., 2023; Thomas, 2018 sekä Wang ym., 2020 todetaan ihmisen olevan tietoturvan heikoin lenkki. Vuoden 2019 koronapandemia on lisännyt etätyötä sekä -opiskelua huomattavasti, mikä on pakottanut tietojärjestelmien osaamattomatkin käyttäjät työskentelemään yksin päätelaitteillaan (Hoheisel ym., 2023). Edellä mainittu on pahentanut osaamattomuudesta aiheutuvia uhkia entisestään (An ym., 2023; Hoheisel ym., 2023). Datan arvon noustessa globaalissa taloudessa organisaatioilla ei ole varaa olla suojaamatta tietovarantojaan varkaudelta tai tahattomalta vuodolta (Rawindaran ym., 2022). Burda ym. (2023, s. 1) nostavat huolenaiheeksi myös yritysten väliset riippuvuussuhteet, missä pieni tai keskisuuri (pk-yritys) yritys toimii alihankkijana suurelle yritykselle. Tällöin pk-yrityksen tietoturvan vaarantuminen altistaa myös muut toimitusketjun osat vaaraan. Yksi merkittävimmistä haasteista organisaatioiden tietoturvassa on Badan ym. (2019) mukaan uhkien tiedostamisen muuttamisessa toiminnaksi eli käyttäytymiseksi.

Tässä tutkielmassa tarkastellaan työntekijöiden tietoturvatietoisuuden vaikutusta pk-yritysten kykyyn puolustautua sähköpostikalastelua vastaan. Tutkimusongelmalla selvitetään, miten pienien ja keskisuurien yritysten työntekijöiden tietoturvatietoisuuden taso vaikuttaa heidän taipumuksiinsa avata kalastelusähköposteja ja toimia hyökkääjän haluamalla tavalla. Pieniksi ja keskisuuriksi yrityksiksi luokitellaan sellaiset yritykset, joiden palveluksessa on alle 250 työntekijää ja vuosiliikevaihto on alle 50 miljoonaa euroa (Tilastokeskus, 2023). Tutkielman lähdeaineistossa on pääasiassa Suomen ulkopuolella toteutettuja

tutkimuksia, kuten Alharbi ym., 2021; Archibald & Renaud, 2019; Rawindaran ym., 2022; Wilson ym., 2023 koskien pk-yritysten tietoturvatietoisuutta. Kuitenkin pienen ja keskisuuren yrityksen määritelmä näissä tutkimuksissa henkilöstömäärän mukaan on kuitenkin sama kuin suomalaisissa. Täten tutkielma painottuu, muttei rajoitu ulkomaisiin pk-yrityksiin.

Esitettyyn tutkimusongelmaan haetaan ratkaisua seuraavilla tutkimuskysymyksillä:

- Millä keinoilla sähköpostikalastelijat pyrkivät huijaamaan yritysten työntekijöitä?
- Millainen rooli työntekijöiden tietoturvatietoisuudella on pk-yrityksen tietoturvan rakentamisessa?

Tämä tutkielma on toteutettu kuvailevana kirjallisuuskatsauksena. Salmisen (2011, s. 6) mukaan ”sitä (kuvailevaa kirjallisuuskatsausta) voi luonnehtia yleiskatsaukseksi ilman tiukkoja ja tarkkoja sääntöjä”. Lähdemateriaali on kerätty pääasiassa JYKDOK:n sekä Google Scholar -tietokannoista. Tutkielman edetessä lähteiden hakuun hyödynnettiin myös Scopus -tietokantaa. Tuloksista valittiin lopulliseen aineistoon pääosin julkaisufoorumi JUFO 1-3 luokituksen saaneita julkaisuja. Tietoturvallisuuteen ja tietomurtoihin liittyviä tilastoraportteja on haettu Google -hakukoneella. Viitteiden hallinnassa on käytetty Zoteron selainlisäosaa, työpöytäsovellusta ja Microsoft Word -lisäosaa.

Aineiston haussa käytettiin aluksi seuraavia termejä: henkilöstön tietoturvatietoisuus, työntekijöiden tietoturvatietoisuus, työntekijät, tietoturvatietoisuus, sähköpostikalastelu sekä näiden yhdistelmiä. Myöhemmin lähteitä arvioitaessa kävi ilmi, että tutkimuksen kohdetta täytyy rajata, jotta laajuus pysyy kandidaatin tutkielman puitteissa. Kohde päätettiin rajata koskemaan vain pieniä ja keskisuuria yrityksiä. Näin kohdennetun tutkimuksen tarvetta lisää se, että pienet yritykset ovat useiden lähteiden mukaan erityisen haavoittuvaisia tietomurroille (Archibald & Renaud, 2019; Bada & Nurse, 2019; Rawindaran ym., 2022; Wilson ym., 2023). Archibaldin ja Reanudin (2019 s. 1) mukaan jopa 60 % pienistä yrityksistä, jotka kokevat vakavan tietomurron, ovat kykenemättömiä palautumaan murron aiheuttamista vahingoista ja siten joutuvat lopettamaan liiketoimintansa kokonaan. Hadnagy & Fincher (2015 s. 75) rinnastavat pk-yritysten tietoturvan tason joissain tapauksissa yksityishenkilöihin, joiden valmiudet puolustautua tietoturvahyökkäyksiä vastaan ovat paljon pienemmät verrattuna suuriin yrityksiin, joilla on käytössä omat turvallisuusosastot kriisien varalle. Archibald & Renaud (2019) sekä Wilson ym. (2023) nostavat yrityksen sisäisen IT-turvallisuushenkilöstön puuttumisen yhdeksi merkittävimmistä haavoittuvuuksien (eng. vulnerability) aiheuttajista.

Ensimmäisessä sisältöluvussa, luvussa 2. selvitetään, millä keinoilla sähköpostikalastelijat pyrkivät huijaamaan yritysten työntekijöitä. Sähköpostikalastelun (eng. phishing) perusidea on pyrkiä vakuuttaman kohteensa klikkaamaan haitallista linkkiä tai liitetiedostoa (Archibald & Renaud, 2019; Burda ym., 2023; Hadnagy & Fincher, 2015; Thomas, 2018). Useimmissa tapauksissa linkki itsessään pyrkii lataamaan kohteen järjestelmään haittaohjelman tai viemään

verkkosivuille, joilla huijataan käyttäjien salasanoja tai arkaluonteisia tietoja (Gehl & Lawson, 2022). Sähköpostikalastelu on nykyaikainen tapa suorittaa sosiaalista manipulointia, joka on ikiaikainen vaikuttamisen tekniikka (Archibald & Renaud, 2019). Hadnagy & Wilson (2010, s. 1) määrittelevät sosiaalisen manipuloinnin (eng. social engineering) olevan vaikuttamisen työkalu siinä kuin mikä tahansa muukin, ja jolla on monia eri merkityksiä eri konteksteissa. Tämän tutkielman kontekstiin sopii Hadnagyn & Wilsonin (2010, s. 1) määritelmä, jonka mukaan sosiaalinen manipulaatio on rikollisen toimijan pyrkimystä huijata toista ihmistä toimenpiteisiin, jotka tekevät hänet tai hänen edustamansa organisaation haavoittuvaiseksi rikokselle, kuten tietojen varastamiselle tai vuotamiselle.

Tutkielman kolmannessa luvussa vastataan toiseen tutkimuskysymykseen tarkastelemalla, millainen rooli henkilöstön tietoturvatietoisuudella on yrityksen tietoturvan rakentamisessa. Siposen (2000, s. 1) mukaan tietoturvatietoisuudella (eng. Information Security Awareness, ISA) tarkoitetaan tilaa, jossa organisaation käyttäjät ovat tietoisia sekä sitoutuneita tietoturvatehtäväänsä, joka ohjeistetaan yleensä loppukäyttäjien tietoturvaohjeessa. Takemura & Komatsu (2013) toteavat artikkelissaan tietoturvatietoisuuden toimivan yrityksen tietoturvan tason mittarina. Termit tietoturva ja kyberturva ovat merkityksiltään hyvin samankaltaisia ja niitä käytetäänkin usein ristiin monissa lähteissä. Suomen valtionvarainministeriön Henkilöstön tietoturvaohjeen (2013**,** s. 17) mukaan tietoturva on "tietojen, tietojärjestelmien ja tietoverkkojen suojaamista tahalliselta tai tahattomalta häviämiseltä, luovuttamiselta, luvattomalta käytöltä, häirinnältä tai vahingoittamiselta". Tietoturva on siten keskeinen osa organisaatioiden toimintaa ja sen avulla pyritään säilyttämään organisaation tietovarantojen eheys, luottamuksellisuus ja saatavuus niille henkilöille, joilla on niihin käyttöoikeus (SFS-standardi 27000, 2020 s. 14; Valtionvarainministeriö, 2013 s. 17). Kyberturvallisuuteen liittyy edellä mainittujen lisäksi myös tietojärjestelmien fyysisiä osia kuten päätelaitteita ja reitittimiä (Valtionvarainministeriö, 2013, s. 20). Tässä tutkielmassa käytetään pääosin termiä tietoturva, koska sen katsotaan soveltuvan paremmin tutkielman kontekstiin.

Yhteenvetoluvussa kiteytetään tulokset ja esitetään jatkotutkimusaiheita. Keskeisinä tuloksina voidaan nähdä sähköpostikalastelijoiden hyökkäävän kohteidensa päätöksentekokykyyn vaikuttaviin tekijöihin kuten luottamukseen ja tunteisiin. Tietoturvatietoisuuden merkitys todetaan monissa lähteissä olevan organisaation tietoturvan kannalta perustavan laatuinen tekijä. Sähköpostikalastelun torjumisessa tietoturvatietoisuus mahdollistaa oikeanlaisen suhtautumisen kalastelusähköposteihin sekä ennakoiviin toimenpiteisiin ryhtymisen.

2 SÄHKÖPOSTIKALASTELU

Tässä luvussa käsitellään sähköpostikalastelua hyökkäysvektorina (eng. attack vector). Kalastelu on Varshneyn ym. (2024) mukaan jo vanha metodi, minkä ensimmäinen esiintyminen tapahtui vuonna 1995, kun hyökkääjät tekeytyivät American Onlinen työntekijöiksi ja huijasivat palvelun käyttäjiltä käyttäjätunnuksia ja salasanoja. Hyökkäysvektoreilla tarkoitetaan toimenpiteitä, joilla verkkoihin pyritään murtautumaan (Hadnagy & Fincher, 2015 s. 22; Verizon, 2023). Sähköpostikalastelun teknisten aspektien käsittelyn yhteydessä esitellään esimerkkinä OWASP-säätiön (eng. Open Worldwide Application Security Project) vakavaksi luokittelemaa haavoittuvuutta hyödyntävä sähköpostikalastelukampanja. Lisäksi pureudutaan sähköpostikalastelun merkitykseen tämän hetken kyberturvallisuuden kentällä sekä sivutaan sen vaikutuksia Suomessa Kyberturvallisuuskeskuksen raporttien ja julkaisujen pohjalta. Luvun lopussa tuodaan esiin kirjallisuudessa esiintyneitä sosiaalisessa manipulaatiossa ja sähköpostikalastelussa havaittuja kehityssuuntia.

2.1 Sähköpostikalastelu hyökkäysvektorina

Sähköpostikalastelun aiheeseen pureuduttaessa on ymmärrettävä sosiaalisen manipulaation (eng. social engineering) perusajatus (Hadnagy & Fincher, 2015). Laaja-alaisen katsauksen aiheeseen saa Hadnagyn ja Wilsonin (2010) kirjasta sosiaalisesta manipuloinnista ihmisten hakkeroimisen taiteenlajina. Kirjassa tarkastellaan erilaisia keinoja, joilla pyritään huijaamaan uhreja sekä tapoja ehkäistä huijatuksi tulemista (Hadnagy & Wilson, 2010). Hadnagy & Fincher (2015 s. 54) tuovat sähköpostikalastelua käsittelevässä kirjassaan esiin sosiaalisen manipuloinnin pitävän sisällään myös hyväntahtoista sosiaalista vaikuttamista, mikä tekee termin tulkinnasta ongelmallista joissain tilanteissa. Heidän kirjansa kuvailee sähköpostikalastelua puolustajien sekä hyökkääjien näkökulmasta. Sosiaalisen manipuloinnin termin monitulkintaisuuden ongelman ratkaisemiseksi Wang ym., (2020) tutkimuksessa tehtiin perusteellinen kirjallisuustutkimus, jossa

jäljitettiin sosiaalisen manipulaation alkuperäinen merkitys kyberturvallisuudessa, analysoitiin järjestelmällisesti termin käsitteellistä ja teknistä kehitystä sekä keskusteltiin käsitteellisistä ongelmista. Edellä mainitun työn perusteella artikkelissa esitetään yhteensopivampaa ja täsmällisempää määritelmää sosiaaliselle manipulaatiolle kyberturvallisuuden kontekstissa (Social Engineering in Cyber Security, SEiCS). Wang ym. (2020 s. 12) mukaan sosiaalinen manipulointi tarkoittaa kyberturvan kontekstissa ”hyökkäystyyppiä, jossa yksi tai useampi hyökkääjä hyödyntää ihmisten haavoittuvuuksia sosiaalisen vuorovaikutuksen avulla rikkoakseen tietoturvaa teknisten keinojen sekä haavoittuvuuksien avulla tai ilman niitä”. Wangin ym. (2020) määritelmä ei tullut vastaan sellaisenaan lähdeaineistoa hakiessa, joten termi ei ole vielä ainakaan laajasti vakiintunut.

Sähköpostikalastelu on menetelmä, jossa naamioidaan pahantahtoinen vaikuttamiseen tai tietojen hankkimiseen tarkoitettu sähköposti näyttämään olevan peräisin legitiimiltä taholta (Hadnagy & Fincher, 2015; Verizon, 2023). Tavoitteena on saada kohde toimimaan ajattelemattomasti (Hadnagy & Fincher, 2015). Cooper ym. (2021) tutkivat ilmoitusten ja varoitusten vaikutusta mobiilikäyttäjien alttiuteen joutua tietojen kalastelun uhriksi. Cooper ym. (2021 s. 3) luettelevat artikkelissaan yleisimmiksi kalastelusähköpostiviestien tunnuspiirteiksi:

- kiireellisyyden vaikutelman,
- toiminnan vaatimisen,
- rahallisen hyödyn tarjoamisen,
- kirjoitus- ja kielioppivirheet,
- tervehdysvirheet,
- allekirjoitusvirheet,
- virheelliset URL-osoitteet,
- linkkien napsauttamista koskevat pyynnöt,
- tietopyynnöt,
- väärennetty lähettäjä,
- väärennetty lähettäjä tai sisältö,
- pyytämättömät tai odottamattomat liitetiedostot,
- osoitteiden yhteensopimattomuus,
- uhkaava kielenkäyttö ja
- korostetun yksilöity viestisisältö.

Edellä mainituista erityisesti väärennetty lähettäjä, väärennetty- tai korostetun yksilöity viestisisältö sekä pyytämättömät tai odottamattomat liitetiedostot ovat tämän tutkielman kontekstin kannalta mielenkiintoisia sekä mainitaan Verizonin vuoden 2023 DBIR-julkaisussa useaan otteeseen (Verizon, 2023). Sähköpostikalastelun perusidea on pyrkiä vakuuttaman kohteensa klikkaamaan haitallista linkkiä tai liitetiedostoa (Archibald & Renaud, 2019; Burda ym., 2023; Hadnagy & Fincher, 2015; Thomas, 2018). Useimmissa tapauksissa linkki itsessään pyrkii lataamaan kohteen järjestelmään haittaohjelman tai viemään verkkosivuille, joilla huijataan käyttäjien salasanoja tai muita arkaluonteisia tietoja (Cooper ym.,

2021; Gehl & Lawson, 2022; Verizon, 2023). Näiden lisäksi hyökkääjien tavoitteena voi olla identiteettivarkaus, datan hävittäminen tai vääristäminen tai arkaluonteisten tietojen haaliminen (Thomas, 2018).

Hadnagyn & Fincherin (2015, s. 41) mukaan, ehkä hieman humoristisestikin toteavat, että ”kalastelusähköposteja lähettävät ihmiset eivät välttämättä ole psykologianopiskelijoita, mutta hyvät kalastelijat ymmärtävät päätöksenteon perusprosessit”. Päätöksenteon perusprosessien ymmärtäminen antaa mahdollisuudet heikentää uhrin loogista ajattelua, jos kalastelijat pystyvät herättämään uhrissa voimakkaita tunteita (Hadnagy & Fincher, 2015; Hoheisel ym., 2023; Wang ym., 2020). Tunteita herättävän viestin on myös toimiakseen saavutettava haluttu vaikutus etäältä (Archibald & Renaud, 2019; Hadnagy & Fincher, 2015). Hadnagy & Fincher (2015) samoin kuin Varshney ym. (2024) mainitsevat sähköpostikalastelijan kannalta otollisiksi, kohteessa herätettäviksi, tunteiksi ahneuden, pelon, surun, uteliasuuden sekä halun, mitä uhrissa pyritään herättämään. Kaikkein vakuuttavimmat kalastelijat voivat niin sanotusti päästä uhrinsa pään sisään ja vakuuttaa tälle, että joku hänelle tärkeä henkilö on vaarassa (Verizon, 2023). Tällöin kyseessä on harvinaisempi ja vaikeammin toteutettavissa oleva räätälöity hyökkäys (Varshney ym., 2024; Verizon, 2023). WithSecuren (2023) tietopaketissa todetaan toisaalta räätälöityihin hyökkäyksiin suunniteltujen työkalujen olevan nykyaikana helposti saatavilla avoimista lähteistä. Näistä työkaluista esimerkkinä mainitaan Social Engineering Toolkit (SET) (WihtSecure, 2023). Jos taustalla vaikuttaa muita tekijöitä kuten myöhemmin luvussa kolme mainittavia kognitiivisia vinoumia, vaikutus on sitä suurempi, koska silloin kohteen päätöksenteko on tunnepitoisuuden lisäksi impulsiivista tai perustuu kokonaan virheelliseen tietoon tai arvioon todellisesta tilanteesta (Hadnagy & Fincher, 2015).

Cooperin (2021 s. 3) mukaan sähköpostikalastelun toteuttamiseen kuuluu yleensä kolme vaihetta. Ensimmäisessä vaiheessa uhri vastaanottaa kalastelusähköpostin, joka sisältää ainakin yhden tai useamman aiemmin mainituista kalastelusähköpostin tunnuspiirteistä. Seuraavassa vaiheessa sosiaalisen manipulaation onnistuessa vaikuttamaan uhrin kognitioon ja sitä kautta käyttäytymiseen, uhri ryhtyy sähköpostissa esitettyihin toimiin. Viimeisessä vaiheessa varastetut tiedot monetisoidaan, vuodetaan, muokataan tai tuhotaan. (Cooper, 2021 s. 3).

Seuraavassa esimerkissä esitellään OWASP-säätiön (2022) vakavaksi luokittelemaa Follina -haavoittuvuutta hyödyntävää sähköpostikalasteluhyökkäystä. Vakavan haavoittuvuudesta tekee sen toimintaperiaate, joka mahdollistaa haavoittuvuuden laukaisun ilman että kohde itse välttämättä edes avaa sähköpostin liitteenä olevaa tiedostoa omassa järjestelmässään. Kriittinen ongelma liittyy Microsoft Support Diagnostic Tool (MSDT) -protokollan manipulointiin, joka mahdollistaa hyökkääjän koodin suorittamisen uhrin järjestelmässä jopa tiedostojen esikatselutilassa. (OWASP-Foundation, 2022; BlackBerry, 2023). Tämän esimerkin tapauksessa kyse oli työsähköpostihuijauksesta (eng. Business E-mail Compromise, BEC), jossa hyökkääjä kaappasi yrityksen sähköpostiliikenteestä aidon sähköpostikeskustelun ja tekeytyi sen toiseksi osapuoleksi (The DFIR report, 2023). Hyökkäyksen tavoitteena oli päästä käsiksi kohteen palvelimilla sijaitseviin arkaluontoisiin tiedostoihin. Verizonin (2023 s. 26) DBIR raportissa sekä

WithSecuren (2023) tietopaketissa todetaan suurimman osan haittaohjelmista levittyvän sähköposteilla ja kulkevan Microsoft Office tiedostojen muodossa. Se on hyökkääjien kannalta edullista, koska suurin osa näistä tiedostoista kykenee koodin suoritukseen asiakkaan järjestelmässä (Verizon, 2023 s. 26).

2.2 Sähköpostikalastelun kehitys ja nykytila

Kybersää -julkaisu on Kyberturvallisuuskeskuksen kuukausittainen koonti Suomen kyberturvan kentän ilmiöistä ja uhkatilanteista, missä sateinen sää tarkoittaa huolestuttavaa ja myrskyisä vakavaa uhkatasoa (Kyberturvallisuuskeskus, 2023a; Kyberturvallisuuskeskus, 2023b). Toukokuussa 2023 Kyberturvallisuuskeskuksen (2023a) Kybersäässä todettiin sähköpostikalastelujen ja huijauspuheluiden tuoneen kybersäähän epävakautta. Sateisen kybersään taustalla ovat esimerkiksi yrityssähköpostitileihin kohdistuvat tietojenkalastelut (BEC) sekä niitä seuranneet tietomurrot (Kyberturvallisuuskeskus, 2023a). Lokakuussa 2023 Kyberturvallisuuskeskus julkaisi vakavan varoituksen Microsoft 365 -tilien salasanojen kalasteluaallosta (Kyberturvallisuuskeskus, 2023b), mikä tukee Hadnagyn & Fincherin (2015 s. 179), Thomasin (2018), Cooperin (2021, s. 1) sekä Hoheiselin (2023, s. 1) havaintoa sähköpostikalasteluhyökkäysten yleistyvyydestä.

Noin yksi kolmesta kalastelusähköpostista avataan kohteen toimesta yhden minuutin ja neljänkymmenen sekunnin sisällä ja heistä 12 prosenttia klikkaa linkkiä tai liitetiedostoa alle neljän minuutin sisällä (Thomas, 2018). Sähköpostikalastelu oli nostettu 2022 DBIR -raportissa neljän avainpolun joukkoon, mitä pitkin järjestelmiin tunkeudutaan (Verizon, 2022). Vuotta myöhemmässä raportissa se oli jo yleisimpien kolmen avainpolun joukossa sijalla kaksi (Verizon, 2023). Kalastelusähköpostin linkkien ja liitetietiedostojen nopeaa avaamista voidaan selittää sosiaalisen manipuloinnin vaikutuksella uhriin.

Hyviä kohteita sähköpostikalastelulle ovat avuliaat, empaattiset, luottavaiset ja auktoriteetteja, kuten virnaomaisia, kunnioittavat henkilöt (Archibald & Renaud, 2019; Verizon, 2023; Wang ym., 2020). Hyökkääjä käyttää hyväkseen edellä mainittuja ominaisuuksia ja taipumuksia sekä mahdollisuuksien mukaan kohteensa huonoa tilannetietoisuutta ja huolimattomuutta (Archibald & Renaud, 2019; Valtionvarainministeriö, 2013; Varshney ym., 2024). Pienien ja keskisuurien yrityksien henkilöstö onkin erittäin otollinen kohde sähköpostikalastelijoille heidän ydinliiketoimintaan keskittymisensä sekä rajallisten resurssiensa ansiosta (Bada & Nurse, 2019; Rawindaran ym., 2022; Wilson ym., 2023). Edellä mainittujen ajankäytön ja resurssien ongelmien lisäksi tapaustutkimuksissa, kuten Wilson ym. (2023) sekä Burda ym. (2023), nostettiin esiin myös pk-yritysten vääristyneitä arvioita riskeistä eli uhkien toteutumisen todennäköisyydestä sekä yritysten suojausten tasosta (Burda ym., 2023; Wilson ym., 2023). Wilson ym. (2023) tutkivat Yhdistyneissä Kuningaskunnissa pk-yrityksen uhka- ja selviytymisarvioita yleisimmistä verkkouhista, joista yksi on sähköpostikalastelu. Burdan ym. (2023) tutkimus oli empiirinen tapaustutkimus hollantilaiseen pk-yritykseen, missä toteutettiin räätälöity sähköpostikalastelukampanja.

Sosiaalinen manipulointi ja sähköpostikalastelu kehittyvät tekniikan kehityksen mukana (Aldawood & Skinner, 2019; Hadnagy & Fincher, 2015; Thomas, 2018). Yksi tästä kehityksestä syntynyt paradigma on kehittyneet jatkuvat uhat (eng. Advanced Persistent Threats, APT) (Thomas, 2018). APT:t ovat alati kehittyneempiä hyökkäysmenetelmiä, joilla rikolliset organisaatiot sekä valtiolliset toimijat Thomasin (2018) sekä Wangin ym. (2020) mukaan pyrkivät pääsemään käsiksi arkaluonteisiin tietoihin, säilyttämään jalansijan organisaatiossa mahdollisia tulevia hyökkäyksiä varten ja muokkaamaan tietoja kohteen toiminnan häiritsemiseksi (Thomas, 2018). Esimerkkinä APT -hyökkäyksestä voidaan käyttää vuoden 2016 Yhdysvaltojen presidentinvaaleihin kohdistunutta Venäjän informaatiohyökkäystä, jolla Gehln & Lawsonin (2022) sekä Thomasin (2018) mukaan onnistuttiin vaikuttamaan vaalitulokseen. Tästä voidaan päätellä, että sähköpostikalastelua käytetään rahallisen hyödyn lisäksi myös poliittiseen vaikuttamiseen.

Gehl & Lawson (2022) käsittelevät kirjassaan manipuloivan kommunikaation kehitystä 2000-luvun alun propagandasta nykypäivän verkoissa tapahtuviin huijauksiin ja petoksiin sosiaalisen manipulaation näkökulmasta. Venäjän 2016 informaatio-operaation lisäksi aiemmin käsitelty APT TA570 -ryhmän toteuttama kalastelukampanja, joka hyödynsi Follina-haavoittuvuutta erään haittaohjelmiston levittämiseksi, on määritelty APT-hyökkäykseksi (OWASP Foundation, 2022; Blackberry, 2023). Järjestäytyneen rikollisuuden ja valtiollisten toimijoiden lisäksi myös pienemmän mittakaavan verkkorikolliset kehittävät omaa toimintaansa olosuhteiden mukaan (Hoheisel ym., 2023). Tähän liittyen Hoheisel ym. (2023) tutkivat Covid-19 pandemian vaikutuksia sähköpostikalastelun trendeihin ja havaitsivat sähköpostikalastelujen aiheiden keskittyvän pandemian aikana Covid-19 aihepiirin ympärille, tavoitteenaan herättää pelon tunteita.

Varshneyn ym. (2024 s. 8) mukaan ihmisten tietoturvatietoisuus perinteisiä sähköpostikalasteluhyökkäyksiä kohtaan on parantunut. Samassa yhteydessä he mainitsevat suurimman osan organisaatioista olevan suojattu perinteiseltä sähköpostivälitteiseltä kalastelulta palomuurien, suojattujen sähköpostiporttien, päätelaitteiden suojauksien sekä edellä mainitun tietoisuuden parantumisen takia. Kuitenkin Varshney ym. (2024) painottavat sähköpostikalastelun torjunnan kattavan tutkimisen tärkeyttä kyberturvallisuuden kokonaisuuden kannalta. He tukevat väitettään tilastolla, jonka mukaan kaikista kyberturvallisuuteen kohdistuvaista hyökkäyksistä 90 % alkaa räätälöidyllä kalasteluhyökkäyksellä (spear phising) (Varshney ym., 2024 s. 1).

3 TIETOTURVATIETOISUUDEN ROOLI TIETOTURVASSA

Tässä luvussa käsitellään aluksi tietoturvatietoisuutta yleisellä tasolla. Luvussa tuodaan esiin yksilön tietoturvatietoisuuteen vaikuttavia tekijöitä, esitellään pintapuolisesti ihmiskeskeisen kyberturvan konteksti sekä tietoturvatietoisuuden arvioimiseen käytettäviä mittareita. Sen jälkeen arvioidaan pk-yritysten tietoturvatietoisuuden tasoa tilastoraporttien ja lähteiden tapaustutkimusten perusteella.

3.1 Tietoturvatietoisuus

Tietoturvatietoisuutta on tarkasteltu erilaisissa tutkimuksissa ja julkaisuissa jo pidemmän aikaa. Yhdysvaltain kansallisen standardien ja teknologian instituutin NIST (1998) luomassa viitekehyksessä tietoturvatietoisuus mainitaan ennakkoedellytykseksi kaikelle tietoturvakoulutukselle ja opetukselle. Siponen (2000) esittää, että kaikkien käyttäjien käyttäytymiseen vaikuttavien lähestymistapojen, kuten tietoisuuden lisääminen, on täytettävä keskeisten käyttäytymisteorioiden vaatimukset ja tarjottava loppukäyttäjille vastauksia, joissa selitetään, miksi heidän olisi noudatettava turvallisuusohjeita.

Groblerin ym. (2021, s. 3) tutkimuksessa määritellään tietoisuuden olevan yksi tietoturvakulttuurin indikaattoreista sekä ihmiskeskeisen kyberturvan osatekijä. Artikkelissa todetaan tietoisuuden olevan tiedonhankinnan ja tulkinnan yhdistelmä, joka sisältää neljä vaihetta, joista ensimmäinen on käytettävissä olevien tietojen hankkiminen (perception, acquiring available facts). Seuraavaksi on tosiasioiden ymmärtäminen suhteessa tietämykseen kyseisistä tilanteista. Kolmanneksi projektio (eng. projection) eli sen hahmottaminen, miten tilanne todennäköisesti kehittyy. Viimeiseksi mainitaan ennustaminen (eng. prediction), jolla arvioidaan, miten ulkopuoliset voimat voivat vaikuttaa tilanteeseen ja sitä kautta projektioihin. Esimerkiksi ennustamisvaiheesta Grobler ym. (2021) nostavat kalastelusähköpostiviestissä pyydettyjen toimenpiteiden noudattamisesta

seuraavan tilanteen pohtimista. (Grobler ym., 2021). Takemura & Komatsu (2013, s. 99) määrittävät tietoturvatietoisuuden mittariksi yksilön tietoturvaan liittyvästä tietämyksestä ja arviointikyvystä. Täten tietoturvatietoisuutta voidaan käyttää työkalun ominaisuudessa, kun arvioidaan tietoturvan tasoa organisaatiossa.

Grobler ym. (2021) jakavat käyttäjän näkökulmasta ihmiskeskeisen kyberturvallisuuden neljään kategoriaan, jotka ovat demografia ja kulttuuri, tilannetietoisuus, psykologia ja käyttäytyminen sekä viimeisenä kognitiiviset tekijät. Näistä tilannetietoisuus sekä psykologia ja käyttäytyminen ovat erityisen tarkastelun alaisina Groblerin ym. (2021) tutkimuksessa sekä tämän tutkielman kontekstissa kiinnostavia. Archibald ja Renaud (2019) käyttävät termiä ihmisten muodostama palomuuri (eng. human firewall) kuvaamaan organisaation henkilöstön roolia tietoturvassa. Heidän mukaansa ihmisten tietoturvatietoisuus ja -käyttäytyminen ovat kriittisiä tekijöitä yrityksen tietoturvan kannalta. Valtionvarainministeriön ohjeessa (2013, s. 18) todetaan ”suurimpien tietoturvallisuuden ongelmien liittyvän kiireeseen, huolimattomuuteen, osaamattomuuteen sekä tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin”. Huolimattomuudesta ja osaamattomuudesta Parsons ym. (2014, s. 167) käyttävät termiä neutraali riskikäyttäytyminen.

Cooper ym. (2021) mainitsevat artikkelissaan yksilön tietoisuuden luokittelusta kahteen eri ajattelun tilaan. Tässä jaossa tietoisuus jaetaan S1- ja S2- ajattelutiloihin (Cooper ym., 2021). S1 -ajattelutila tarkoittaa Cooperin ym. (2021) mukaan tilaa, jossa yksilön päätökset ovat rutiininomaisempia ja vähemmän harkittuja. S2 -tilassa yksilöt tekevät päätöksiä harkitummin ja täten päätöksien katsotaan olevan tietoisempia (Cooper ym., 2021). Tämän kuvailun perusteella voidaan ajatella sähköpostikalastelijoiden kohdentavan viestinsä S1- ajattelutilassa työskenteleville henkilöille. Näistä ajattelutiloista ei löytynyt muista lähteistä mainintoja, joten niiden syvällisempää analysointia ja pohdintaa ei voitu muihin lähteisiin verrattuna tehdä.

Yksilön tietoturvatietoisuuteen päätöksenteon taustalla vaikuttavia tekijöitä on useita. Hadnagy & Fincher (2015, s. 35–36) mainitsevat yksilön tulkintaan vaikuttavista kognitiivisista vinoumista, jotka ovat taipumuksia ajatella tietyllä tavalla aiempien kokemuksien perusteella. Niitä ovat kehystämisvaikutus (eng. framing effect), jossa yksilön reaktiot riippuvat tavasta, jolla tilanne tai asia esitetään. Saatavuusvinouma (eng. availability heuristic), jossa yksilö tekee nopean päätöksen ensimmäisenä muistamansa asian perusteella. Viimeisenä mainittiin vahvistusvinouma (eng. confirmation bias) eli taipumus tulkita vastaanotettua tietoa näkökulmasta, joka on yhtenevä yksilön omien uskomusten kanssa. (Hadnagy & Fincher 2015, s 35–36). Näiden vinoumien vaikutusta lisää merkittävästi psyykkeeseen vaikuttavat fyysiset olotilat kuten unen puute, nälkä ja vessahätä. Nämä olotilat tekevät päätöksenteosta impulsiivisempaa. (Hadnagy & Fincher, 2023, s. 37–38). Wilson ym. (2023) vastaavasti kuvailevat artikkelissaan vahvistusvinouman kanssa yhtenevän kognitiivisen vinouman. He kuvailevat sitä taipumuksena etsiä tai kiinnittää huomiota sellaiseen tietoon, joka tukee

henkilön omaa näkökulmaa tai asemaa. Esimerkkinä he mainitsevat tämän vinouman esiintymisen pk-yrityksissä mahdollisesti uutisoinnin seurauksena, koska mediassa usein esitetään vain isoihin kansallisiin ja monikansallisiin organisaatioihin tehtyjä iskuja (Wilson ym., 2023).

Tietoturvatietoisuuden tason arvioimisessa voidaan hyödyntää erilaisia mittareita. Monissa tutkimuksissa tähän on käytetty käyttäytymistieteissä syntyneitä käyttäytymismalleja ja -teorioita (Alahmari ym., 2023; Grobler ym., 2021; Siponen, 2000). Taulukkoon 1 on poimittu lähteissä eniten esiin nousseet tietoturvatietoisuuden ilmenemistä selittävät sekä sen parantamisessa hyödynnettävät käyttäytymismallit ja -teoriat. Taulukon ensimmäisessä sarakkeessa kerrotaan mallin tai teorian suomenkielinen nimi, alkuperäinen englanninkielinen nimi ja käytetty lyhennys. Keskimmäisessä sarakkeessa on mallin tai teorian selitys. Viimeisessä sarakkeessa luetellaan lähteet, joissa kyseinen teoria tai malli on esiintynyt.

Parsons ym. (2014) tutkimuksessa tuotettiin empiirisesti validoitu mittari arvioimaan, missä määrin organisaatioiden tietojärjestelmät ovat alttiita työntekijöiden riskikäyttäytymisen aiheuttamille uhkille. Heidän tutkimuksestaan syntyi tietoturvan inhimillisten aspektien kyselylomake (eng. Human Aspects of Information Security Questionnaire, HAIS-Q). Tämän tutkielman kontekstissa riskikäyttäytymisellä tarkoitetaan esimerkiksi kalastelusähköpostien linkkien ja liitetiedostojen avaamista. An ym. (2022) sekä Parsons ym. (2014) tuovat esiin sosiaalisten osatekijöiden huomioon ottamisen tärkeyden HAIS-Q kyselyä käytettäessä tietoturvatietoisuuden tason arvioimiseen. An ym. (2022) esittävät sosiaalisen koulutustason (eng. Social Education Level, SEL) mallin hyödyntämistä sosiaalisten osatekijöiden kattamiseksi. Sosiaalisen koulutustason mittarina An ym. (2023) tutkimuksessa käytettiin henkilön työvuosia.

Grobler ym. (2021) toteavat käyttäytymistieteiden teorioiden avustavan tietoturvassa tarjoamalla arvokasta tietoa kognitiivisesta kuormituksesta ja -vinoumista. Kuten Taulukosta 1 on havaittavissa, monissa tutkimuksissa on hyödynnetty erityisesti suojelumotivaatioteoriaa (PMT) sekä suunnitellun käyttäytymisen teoriaa (TPB) selittämään käyttäjien toimintaa ja sen taustalla vaikuttavia psykologisia prosesseja. Huomion arvoista on, että tuoreissakin tutkimuksissa, kuten Varshneyn ym. (2024 s. 2) systemaattisessa kirjallisuuskatsauksessa, todetaan sähköpostikalastelun puolustusmekanismeja tutkivien julkaisujen lähestyvän ongelmaa vain harvoissa tapauksissa sosiaalisesta tai kognitiivisesta näkökulmasta.

TAULUKKO 1 Käyttäytymistieteiden malleja

MALLI TAI TEORIA	LYHYT KUVAUS	VIITATTU
Tietoturvan inhimilliset aspektit, The human aspects of information security (HAIS). Parsons ym., 2014	• Kattava asteikko internetin turvallisuuden tietämyksen, -asenteiden ja käyttäytymisen mittaamiseen • Perustuu tietämys-asenne-käyttäytymismalliin ja sosiaaliseen koulutustasoon	(Aldawood & Skinner, 2019; An ym., 2023; Parsons ym., 2014; Rohan ym., 2023; Wang ym., 2020)
Tietämys-asenne-käyttäytymismalli, knowledge-attitude-behavior, (KAB). Parsons ym., 2014	• Tietämys-Asenne-Käyttäytymismalli • Kun tietokoneen käyttäjien tietämys tietoturvapolitiikasta ja -menettelyistä lisääntyy, heidän asenteensa tietoturvapolitiikkaa ja -menettelyjä kohtaan paranee, minkä pitäisi johtaa riskejä karttavampaan tietoturvakäyttäytymiseen	An ym., (2023); Parsons ym., (2014)
Suojelumotivaatioteoria, protection motivation theory, (PMT). Herath & Rao, 2009	• Tietoturvatietoisuuden lisäämisen kannalta suojelumotivaation painopiste on pelkoon eli uhan aiheuttaman riskin kokemukseen vetoamisessa. • Kolme tekijää: 1. Uhan koettu vakavuus 2. Uhan esiintymisen koettu todennäköisyys 3. Vasteen, eli ennaltaehkäisevän käyttäytymisen koettu tehokkuus	Wilson ym. (2023); An ym. (2023); Thomas (2018); Alahmari ym. (2023); Bada ym. (2019); Grobler ym. (2021); Herath & Rao (2009); Parsons ym. (2014)
Suunnitellun käyttäytymisen teoria, theory of planned behavior, (TPB). Ajzen & Madden, 1986	• Muodostuu: o Käyttäjän asenteesta toivottua käyttäytymistä kohtaan o Subjektiivisista normeista o Koetusta käyttäytymisen hallinnasta • Pitää sisällään perustellun toiminnan teorian (eng. Theory of Reasoned Action, TRA) (Ajzen & Madden, 1986) o uskomukset, asenteet, aikomukset ja käyttäytyminen muodostavat kausaalisen ketjun siten, että uskomukset johtavat asenteisiin, asenteet johtavat aikomuksiin ja edelleen käyttäytymiseen.	Parsons ym., (2014); An ym. (2023); Thomas (2018); Ajzen & Madden (1986); Alahmari ym. (2023); Bada ym. (2019); Herath & Rao (2009); Siponen (2000): Takemura & Komatsu (2013)

3.2 Tietoturvatietoisuus pk-yritysten näkökulmasta

Organisaation henkilöstön tietoturvatietoisuus on keskeinen tekijä yrityksen tietoturvan rakentamisessa sekä uhkien ehkäisyssä (Alahmari ym., 2023; Albrechtsen & Hovden, 2010; Bada & Nurse, 2019; Rohan ym., 2023; Siponen, 2000). Tietoturvatietoisuuden parantamisella ja ylläpidolla voidaan ehkäistä tahattomasta, mutta riskialttiista tietoturvakäyttäytymisestä johtuvia tietomurtoja (Parsons ym., 2014). Tietoturvatietoisuus on monien lähteiden, kuten Siposen (2000) ja Badan ym. (2019), mukaan perusedellytys yrityksen tietoturvan kokonaisuuden rakentamisessa. Pk-yritysten näkökulmasta tietoturvatietoisuuden ylläpitämisen merkitys on monissa tapauksissa suurempi verrattuna suuriin yrityksiin, koska pk-yrityksien kyky palautua tietomurroista on heikompi (Archibald & Renaud, 2019). Suurienkin yritysten näkökulmasta pk-yritysten tietoturvatietoisuuden tason on oltava riittävä, koska toimitusketjuhyökkäyksen sattuessa kaikki saman ketjun osat voivat olla murron uhreja (Burda ym., 2023; Verizon, 2022).

Bada & Nurse (2019) tutkivat kirjallisuuskatsauksena ja tapaustutkimuksena lontoolaisten pk-yritysten kyberturvallisuusstrategioita. Tutkimuksen tavoitteena oli ehdottaa koulutusohjelmaa, jonka painopisteenä olisivat teknisten aspektien sijaan työntekijät. He toteavat eritysesti pk-yritysten olevan verkkorikollisten kohteena kyberrikollisuuden kasvaessa kaikilla toimialoilla. Heidän tapaustutkimuksessaan tuotiin esiin pk-yritysten saavutettavuuden ongelma, jonka hypoteesina ennustettiin johtuvan siitä, että yritysten työntekijät ovat liian sidottuja päivittäisten liiketoimintojen hoitamiseen. (Bada & Nurse, 2019). Walesilaisessa tutkimuksessa Rawindaran ym. (2022) selvittivät, miten walesilaiset pk-yritykset käsittelevät verkkorikollisuutta ja hallinnoivat päivittäistä verkkotoimintaansa pitääkseen tietonsa ja järjestelmänsä turvassa. Tutkimuksen tuloksista he nostivat esiin, että pk-yrityksien tietoturvatietoisuuden matalampi taso jarruttaa siirtymistä kohti tuoreempaa ja turvallisempaa teknologiaa kuten koneoppivia uhkien tunnistustyökaluja. Pk-yritykset priorisoivat liiketoimintaansa oikean, tietojen suojaamiseen vaadittavan, teknologian käytön yli (Bada & Nurse, 2019; Rawindaran ym., 2022; Wilson ym., 2023).

Acquisti ym. (2018) tarkastelivat kirjallisuuskatsauksessaan yksityisyyden suojaa ja turvallisuutta koskevaa päätöksentekoa tarkoituksenaan löytää keinoja, jotka ohjaavat käyttäjiä parempaan päätöksentekoon. He esittivät tähän tarkoitukseen työntekijöiden pehmeää holhousta. Pehmeällä holhouksella (eng. paternalism) tarkoitetaan esimerkiksi tekaistujen kalastelusähköpostien lähettämistä työntekijöille, minkä tarkoitus on seurata heidän käyttäytymistään vastaanottaessa kalastelusähköposteja. Tutkimuksessaan he esittävät, että pehmeän holhouksen tavoitteena on käyttäytymisen taustalla olevien psykologisten prosessien synnyttämien kokemuksien mahdollinen hyödyntäminen. Tällaisten toimien perimmäisenä tavoitteena on lisätä yksilön tai organisaation hyvinvointia joko lieventämällä tai hyödyntämällä ihmisten käyttäytymisvinoumia tavalla, joka saa ihmiset tekemään tietoisempia ja toivottavampia itsenäisiä valintoja (Acquisti ym., 2018). Archibaldin & Renaudin (2019) tutkimuksessa samasta

toimenpiteestä käytetään termiä ihmisten läpäisytestaus (eng. human penetration testing). Esimerkkinä tällaisesta voidaan pitää Burdan ym. (2023) tapaustutkimusta eurooppalaiseen pk-yritykseen, jonka tavoitteena oli saada ymmärrystä kalastelun kohteeksi joutuvien työntekijöiden kognitiivisista prosesseista.

Pk-yritysten heikompaan tietoturvan tasoon mainitaan monissa lähteissä kuten Bada & Nurse, 2019; Wilson ym., 2023 ja Verizon, 2023 samoja toistuvia syitä, tietoturvatietoisuuden matalampi taso, ammattitaidon puute sekä resurssien riittämättömyys (Bada & Nurse, 2019; Wilson ym., 2023; Verizon, 2023). Koolen ym. (2024 s. 7) toteavat, ettei ole realistista olettaa pk-yritysten kykenevän saman tason turvallisuustoimenpiteisiin kuin suuret yritykset. Wilson ym. (2023) nostavat esiin organisaatioiden asenteet ja ymmärryksen puutteen tehottomien tietoturvatoimenpiteiden syiksi. He mainitsevat yhdysvaltalaisesta tutkimuksesta, missä 370 pientä yritystä vastasi kyselytutkimuksessa käyttävänsä antivirusohjelmistoja, mutta alle puolet vastanneista ylläpitivät ohjelmistopäivityksiä sitä mukaa kun niitä ilmestyi (Wilson ym., 2023). Artikkelissa mainittiin myös australialaisesta tutkimuksesta, jossa 40 % vastanneista pienyrityksistä kertoi käyttävänsä tehottomia puolustusmekanismeja (Wilson ym., 2023).

Rawindaranin (2022 s. 13) tutkimuksessa käsiteltiin organisatorisia tekijöitä yksilön toiminnan taustalla. Elementeillä kuten päätöksiä tekevällä roolilla, tietyllä roolilla, iällä tai sukupuolella ei havaittu olevan vaikutusta tietoturvatietoisuuden tasoon. Suurimmat kaksi vaikuttavaa tekijää heidän artikkelinsa mukaan olivat organisaation koko ja henkilöstön koulutuksen taso. Korkeasti koulutettu henkilöstö yhdistettynä pienikokoiseen organisaatioon osoittautuivat tietoturvatietoisuuden tason kannalta edullisimmiksi tekijöiksi (Rawindaran ym., 2022 s. 15). Korkean koulutuksen tärkeyttä tukee myös Burdan ym. (2023) tutkimuksen havainto, jossa eurooppalaisen pk-yrityksen henkilöstö havaitsi odotettua nopeammin kalasteluhyökkäyksen ja tieto hyökkäyksestä jaettiin nopeasti kaikille yrityksen työntekijöille.

Bada & Nurse (2019) esittävät pk-yrityksien voivan parantaa kokonaisturvallisuuttaan luomalla organisaatioon tietoturva-asetelman, jossa työntekijät suojelevat intuitiivisesti yrityksen tietovarantoja. Toisin sanoen tietoturvatietoisuuden tavoitetilana on mahdollistaa organisaatiokulttuuri, joka ilmenee työntekijöiden tiedostamattomana, tietoturvan kokonaisuuden kannalta edullisena sähköpostikäyttäytymisenä. Badan & Nursen (2019) mukaan pk-yritysten tietoturvatietoisuuden parantamiseen pyrkivien lähestymistapojen on oltava holistisia. Tällä tarkoitetaan ydinliiketoiminnan sisällyttämistä sekä rajallisten resurssien huomioimista tietoturvatietoisuuden parantamiseen pyrkivissä toimenpiteissä (Bada & Nurse, 2019; Koolen ym., 2024). Tietoturvatietoisuuden avulla mahdollistetaan organisaation toimijoiden tietoturvan tason nosto hyödyntämällä muun muassa organisaation ulkopuolisia toimijoita koulutuksissa ja harjoituksissa (Takemura & Komatsu, 2013). Tietoturvatietoisuuden tason nostoon tarkoitetussa koulutuksessa voidaan hyödyntää virtuaalisia laboratorioita, simulaatioita, pelejä ja moderneja sovelluksia (Mashtalyar ym., 2021). Edellä mainittuja metodeja voidaan tarjota työpajoilla, luennoilla tai muilla virtuaalisilla opetusmuodoilla (Mashtalyar ym., 2021; Verizon, 2023). Gartnerin (2023b) ohjeessa

suositellaan teoreettisen opetuksen sijaan työntekijän roolia vastaavaa sekä oikean maailman tilannetta simuloivaa tilannekoulutusta. Alati kehittyvien uhkien takia tietoturvatietoisuutta lisäävien koulutusten ja kampanjoiden tulee olla jatkuvia (Adams & Sasse, 1999; Alsulami ym., 2021; ISO/IEC 27001:2023; Smadi ym., 2018). Toisin sanoen yritysten täytyy tiedostaa, että toimivia kertaluonteisia koulutuksia ei ole olemassa.

Alahmari ym. (2023) sekä Bada & Nurse (2019) myöntävät tietoisuuskampanjoiden ja koulutusten olevan välttämättömiä, mutta toteavat niiden olevan riittämättömiä yrityksen tietoturvan ylläpitämisessä. Alahmari ym. (2023) esittävät tutkimuksessaan turvallisuustietämyksen jakamisen (eng. security knowledge sharing, SKS) mahdollisuutena parantaa organisaation tietoturvaa tehokkaammin kuin koulutukset ja kampanjat yksinään. Tätä väitettä tukee Burdan ym. (2023) havainto, jossa pk-yrityksen pieni koko mahdollisti nopean tiedon kulun läpi organisaation tapausyrityksessä tehdystä kalasteluhyökkäyksestä. Tietoturvatietämyksen jakamiseksi on siis luotava tai mahdollistettava organisaatiokulttuuri, jossa tähän kyetään (Ashenden, 2008; Bada & Nurse, 2019; Koolen ym., 2024).

Koolen ym. (2024) esittävät tietoturvan ylläpitämiseksi pienien ja keskisuurien yritysten näkökulmasta kohtuullisten turvallisuustoimenpiteiden kartoittamista. He määrittävät toimen-piteet kohtuullisiksi, kun ne ovat oikeassa suhteessa turvallisuusriskeihin ja implementointikustannuksiin (Koolen ym., 2024). Resurssien puitteissa on suositeltavaa investoida koneoppiviin tai automaatiota hyödyntäviin kalastelun tunnistus- ja torjuntatyökaluihin vastaamaan modernien kalasteluhyökkäysten uhkiin (Koolen ym., 2024; Rawindaran ym., 2022; Varshney ym., 2024). Sähköpostikalastelun nopeasti kehittyvän luonteen takia Opara ym. (2024 s. 3) sekä Smadi ym. (2018 s. 3) suosittelevat konkreettiseksi työkaluksi dynaamisesti oppivaa neuroverkkoa hyödyntävää kalastelusähköpostien ja -verkkosivujen tunnistustyökalua.

4 POHDINTA

Tässä osuudessa kootaan tutkielman keskeiset tulokset ja käydään niihin liittyvää pohdintaa. Toisessa alaluvussa arvioidaan tämän tutkielman menetelmää, prosessia sekä kerättyä aineistoa laadun ja kattavuuden näkökulmista. Sen lisäksi tuodaan esiin tutkielman rajoitteita.

4.1 Tulokset

Varshneyn ym. (2024 s. 8) mukaan ihmisten tietoturvatietoisuus perinteisiä sähköpostikalasteluhyökkäyksiä kohtaan on parantunut. Samassa yhteydessä he mainitsevat suurimman osan organisaatioista olevan suojattu perinteiseltä sähköpostivälitteiseltä kalastelulta palomuurien, suojattujen sähköpostiporttien, päätelaitteiden suojauksien sekä edellä mainitun tietoisuuden parantumisen takia. Toisaalta Wilsonin ym. (2023) tuloksissa tuodaan esiin, että erityisesti pk-yritysten käsitys organisaation ja henkilökunnan kyvykkyyksistä sähköpostikalastelun torjunnassa on usein yltiöpositiivinen.

Yksi keskeisimmistä tietoturvatietoisuuden sähköpostikalastelua torjuvista ominaisuuksista on oikeanlainen varauksellinen suhtautuminen sähköpostiviesteihin (Hadnagy & Fincher, 2015; Thomas, 2018; Varshney ym., 2024; Wilson ym., 2023). Thomasin (2018 s. 6) mukaan yksilöt, joilla on aiempaa tietoa, kuten henkilökohtaista tai toisen käden kokemusta kalasteluhyökkäyksestä, suhtautuvat sähköposteihin varautuneemmin. Sen lisäksi yksilön epäileväinen luonne mainitaan vahvana indikaattorina kyvystä olla lankeamatta kalastelun uhriksi (Thomas, 2018). Korkeampi tekninen osaaminen, kuten tietämys evästeiden kaltaisista seurantatiedoista, vakoiluohjelmista, verkkoturvallisuudesta ja virusten leviämisestä, johtaa myös alhaisempaan alttiuteen tulla huijatuksi (Thomas, 2018).

Riittävään tietoturvatietoisuuden tasoon voidaan katsoa sisältyvän oikeanlaisten ennakoivien toimenpiteiden toteuttaminen (Naqvi ym., 2023). Tällaisia toimenpiteitä ovat turvallisuus ja tietoisuuskampanjat sekä -koulutukset (Alahmari ym., 2023; Bada & Nurse, 2019). Näiden lisäksi on mahdollistettava

tietoturvatietojen jakaminen organisaation sisällä (SKS) (Alahmari ym., 2023; Bada & Nurse, 2019). Erityisesti pk-yritysten näkökulmasta uhkatilanteista tiedottaminen läpi organisaation on toivottavaa, koska organisaation pienemmän koon havaittiin Burdan ym. (2023 s. 5) tutkimuksessa nopeuttavan hyökkäyksen torjunnassa. Riskikartoitusten eli potentiaalisimpien uhkien kartoitusten tulokset tulee tiedottaa yrityksen työntekijöille (Rohan ym., 2023). Kirjallisuuskatsauksen havainnoista on myös tulkittavissa, että riittävän tietoturvatietoisuuden ilmentymäksi voidaan lukea järjestelmien ajantasaisuudesta huolehtiminen (Hadnagy & Fincher, 2015; Koolen ym., 2024; Varshney ym., 2024; WithSecure, 2023). Samoin kuin käyttöjärjestelmien, ohjelmien ja sovellusten päivityksistä huolen pitäminen, tietoturvatietoisuuteen liittyy ymmärrys turvallisuustilanteen ja uhkatekijöiden kehittyvästä luonteesta (Hadnagy & Fincher, 2015).

Hyökkääjien tavoitteena kaikissa kalastelun muodoissa on saada uhri toimimaan hyökkääjän määrittelemällä tavalla. Tässä onnistuakseen hyökkääjän tulee estää kohdettaan ajattelemasta kriittisesti (Hadnagy & Fincher, 2015). Kuten luvussa kaksi todettiin, tunteiden herättäminen kohteessa saa tämän useissa tapauksissa toimimaan ajattelemattomasti. Erityisesti kiireellisyyden tunteen herättäminen heikentää uhrin päätöksenteon tarkkuutta (Cooper ym., 2021; Hadnagy & Wilson, 2010; Hadnagy & Fincher, 2015; Thomas, 2018; Varshney ym., 2024). Vaikka, kuten ylempänä Varshney ym. (2024 s. 2) toteavat, tietoisuuden sähköpostikalastelusta parantuneen, onnistunut sosiaalinen manipulointi on uhkatekijänä lähes mahdoton kitkeä kokonaan vaarattomaksi (Hadnagy & Fincher, 2015). Kalasteluviestien muuttuessa jatkuvasti vaikeammin tunnistettaviksi, erityisesti räätälöidyt kalasteluhyökkäykset (spear phisihing) muodostavat vakavan uhan modernin kyberturvan kentällä (Verizon, 2023).

Alati kehittyvien uhkien takia tietoturvatietoisuutta lisäävien koulutusten ja kampanjoiden tulee olla jatkuvia (Adams & Sasse, 1999; Alsulami ym., 2021; ISO/IEC 27001:2023; Smadi ym., 2018). Toisin sanoen yritysten täytyy tiedostaa, että toimivia kertaluonteisia koulutuksia ei ole olemassa. Täten työntekijöiden tietoturvatietoisuuden tasoa tulee myös seurata jatkuvasti, jotta mahdolliset heikkoudet ja vahvuusalueet tietoturvassa voidaan tunnistaa (Adams & Sasse, 1999; Rohan ym., 2023). Tähän liittyen Thomas (2018) suosittelee yritysten johtohenkilöille työntekijöiden segmentoimista eri käyttäjätyyppeihin, jotta riskikäyttäytyjät voidaan tunnistaa ja heidän toimiaan ennakoida. Tietoturvakäyttäytymisen mittaamiseen havaittiin useissa lähteissä käytettävän suojelumotivaatioteoriaa (PMT) sekä suunnitellun käyttäytymisen teoriaa (TPB) (Thomas, 2018). Koulutukset ja kampanjat tulee mahdollisuuksien mukaan räätälöidä vastaamaan työntekijöiden omia työnkuvia sekä organisaation näkökulmasta yrityksen liiketoiminnan kontekstia (Bada & Nurse, 2019). Sähköpostikalastelun nopeasti kehittyvän luonteen takia Opara ym. (2024 s. 3) sekä Smadi ym. (2018 s. 3) suosittelevat konkreettiseksi työkaluksi dynaamisesti oppivaa neuroverkkoa hyödyntävää kalastelusähköpostien ja -verkkosivujen tunnistustyökalua.

Koolen ym. (2024) esittävät pienien ja keskisuurien yritysten näkökulmasta kohtuullisten turvallisuustoimenpiteiden kartoittamista. He määrittävät toimenpiteet kohtuullisiksi, kun ne ovat oikeassa suhteessa turvallisuusriskeihin ja

implementointikustannuksiin (Koolen ym., 2024). Resurssien puitteissa on suositeltavaa investoida koneoppiviin tai automaatiota hyödyntäviin kalastelun tunnistus- ja torjuntatyökaluihin vastaamaan modernien kalasteluhyökkäysten uhkiin (Koolen ym., 2024; Rawindaran ym., 2022; Varshney ym., 2024). Cooperin ym. (2021) tapaustutkimuksessa tutkittiin erilaisten varoitusten ja merkkiäänien tehokkuutta kohderyhmän vastaanottamien kalasteluviestien tunnistamisessa. Tutkimuksessa havaittiin hälytysten ja varoitusten auttavan kalastelusähköpostien tunnistamisessa nopeammin kuin ilman varoituksia (Cooper ym., 2021). Varoituksilla ja hälytyksillä voitiin siis siirtää kohdehenkilön ajattelu vähemmän tarkkaavaisesta S1 -ajattelutilasta harkitumpaan ja tietoisempaan S2 -ajattelutilaan, mikä ehkäisee sosiaalisen manipuloinnin onnistumista.

Tutkielmaan valittujen lähteiden näkökulmissa havaittiin jonkin verran eroja. Rawindaran ym. (2022 s. 15) toteavat oikean koulutustason ja sopivan henkilöstömäärän olleen riittäviä tekijöitä pk-yrityksen datan suojaamiseen ja liiketoiminnan jatkamiseen. He toteavat jopa havainneensa, että mitä pienemmästä ja koulutetummasta pk-yrityksestä oli kyse, sitä parempi sen tietoturvan taso oli. Samaan sävyyn Burda ym. (2023) havaitsivat matalan organisaatiohierarkian nopeuttaneen odottamattoman paljon hyökkäyksestä tiedottamista ja sitä kautta sen torjumista pienikokoisessa eurooppalaisessa yrityksessä. Toisaalta monissa lähteissä havaittiin, että suuri osa pienistä ja keskisuurista yrityksistä luulee olevansa paremmassa turvassa kyberhyökkäyksiltä kuin todellisuudessa ovat (Aldawood & Skinner, 2019; Alharbi ym., 2021; Wilson ym., 2023). Syyksi tähän mainittiin lähes poikkeuksetta pienempien yritysten rajallisemmat resurssit ja erillisten tietoturvallisuuteen erikoistuneiden osastojen puuttuminen (Bada & Nurse, 2019; Hadnagy & Fincher, 2015; Wilson ym., 2023; Verizon, 2023).

4.2 Tutkielman prosessin analyysi

Tämä tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena. Kuvailevasta kirjallisuuskatsauksesta Salminen (2011 s. 6) toteaa, että ”sitä voi luonnehtia yleiskatsaukseksi ilman tiukkoja ja tarkkoja sääntöjä”. Kuvaileva kirjallisuuskatsaus on luonteeltaan asioita ja ilmiöitä selittävä, ja se sisältää narratiivisia piirteitä, mikä soveltuu hyvin kuvaamaan tietoturvatietoisuuden kaltaista psykologista ominaisuutta ja sähköpostikalastelua ilmiönä. Tarvittaessa tutkittavan ilmiön ominaisuuksia pystytään myös luokittelemaan kuvailevaa kirjallisuuskatsausta käytettäessä ja tutkimuskysymykset voivat olla väljempiä kuin meta-analyysissä tai systemaattisessa kirjallisuuskatsauksessa (Salminen, 2011).

Aineistonhakuun hyödynnetyt tietokannat JYKDOK, Google Scholar ja Scopus ovat laajasti hyödynnettyjä ja hyväksi havaittuja. Aineiston hakutermit ja valintakriteerit on niin ikään tarkasti määritetty. Empiirisen osan puuttuessa tutkielman käytännön läheisyyttä pyrittiin lisäämään sisällyttämällä lähteisiin tunnettujen yritysten kuten Gartnerin ja Verizonin tilastoraportteja. Tutkielman

prosessin johdonmukaisuutta heikentää alkuperäisen tutkimussuunnitelman aikataulussa pysymättömyys ja haasteet aihealueen rajauksessa.

Lähteiden valintakriteereinä käytettiin Julkaisufoorumin 0–3 JUFO-luokitusta. Valintoja tehdessä pyrittiin suosimaan vähintään luokituksen yksi saaneita julkaisukanavia ja konferenssijulkaisuja. Tietoturvatietoisuuden ja sähköpostikalastelun aihepiireihin pureutuneita julkaisuja löytyi hakutuloksista hyvin ja vähintään JUFO-luokituksen kaksi saaneita valikoitui 10 kpl eli 20 % koko aineistosta. Britanniassa sekä Pohjois-Amerikassa kokonaan tai osittain tehtyjä vertaisarvioituja julkaisuja valikoitui suhteellisen paljon, yhteensä 23 kpl, lopullisen viidenkymmenen lähteen joukkoon. Ison-Britannian ja Pohjois-Amerikan alueilla tehtyjä tutkimuksia on siis tämän tutkielman lähteistä melkein puolet (48 %). Voidaan hypoteesin omaisesti alustavasti todeta näillä alueilla panostettavan paljon tietoturvatietoisuuden ja sähköpostikalastelun tutkimukseen.

5 YHTEENVETO

Tässä tutkielmassa tarkasteltiin työntekijöiden tietoturvatietoisuuden vaikutusta yrityksen kykyyn puolustautua sähköpostikalastelua vastaan painottuen pienien ja keskisuurien yritysten kontekstiin. Tutkimusongelmaan haettiin ratkaisua kahden tutkimuskysymyksen kautta. Tutkimuskysymykset ja niiden vastaukset on kiteytetty taulukkoon 2, missä kysymykset ovat vasemmassa sarakkeessa ja vastaukset oikeassa.

Sähköpostikalastelijoiden havaittiin huijaavan kohteitaan tekeytymällä heille entuudestaan tutuiksi lähettäjiksi tai auktoriteetiksi kuten viranomaiseksi (Archibald & Renaud, 2019; Hadnagy & Fincher, 2015; Varshney ym., 2024; Verizon, 2023; Wang ym., 2020). Tämän tarkoituksena on saavuttaa kohteen luottamus. Toisena merkittävänä vaikutuskeinona on tunteiden herättäminen, minkä pääasiallinen tarkoitus on vaikuttaa kohteen päätöksentekokykyyn (Hadnagy & Fincher, 2015; Hoheisel ym., 2023; Varshney ym., 2024; Wang ym., 2020).

Tietoturvatietoisuuden katsottiin olevan perustavanlaatuinen tekijä yrityksen tietoturvan rakentamisessa ja ylläpidossa (Alahmari ym., 2023; Bada ym., 2019; Bada & Nurse, 2019; Siponen, 2000). Riittävään tietoturvatietoisuuden tasoon katsotaan sisältyvän henkilöstön realistinen arvio henkilökohtaisista sekä yrityksen kyvykkyyksistä puolustautua todennäköisimpiä uhkia vastaan (Wilson ym., 2023). Tietoturvatietoisuutta ylläpitävien toimenpiteiden tulee olla jatkuvia eli osa yrityksen organisaation kulttuuria (Ashenden, 2008; Bada & Nurse, 2019; ISO/IEC 27001:2023; Koolen ym., 2024).

Sähköpostikalastelun torjumisessa tietoturvatietoisuuden ominaisuuksista nousi esiin kolme keskeistä tekijää. Riittävä tietoturvatietoisuuden taso mahdollistaa oikeanlaisen suhtautumisen odottamattomiin tai muulla tavalla epäilyttäviin sähköpostiviesteihin (Hadnagy & Fincher, 2015; Thomas, 2018; Varshney ym., 2024; Wilson ym., 2023). Edellä mainitun toteutuessa yrityksellä on edellytykset toteuttaa oikeanlaisia ennakoivia toimenpiteitä sähköpostikalastelun torjumiseksi, kuten tietoturvakoulutuksia, -työpajoja ja harjoituksia (Koolen ym., 2024; Mashtalyar ym., 2021; Naqvi ym., 2023). Ennakoiviin toimenpiteisiin kuuluu myös keskeisesti käytössä olevien järjestelmien päivityksien ajantasaisuuden varmistaminen sekä mahdollisuuksien mukaan sähköpostikalastelun

torjuntaohjelmien ja työkalujen käyttö (Naqvi ym., 2023). Varshney ym. (2024 s. 8) toteavat ihmisten perinteistä sähköpostikalastelua koskevan tietoisuuden parantuneen viime vuosina.

TAULUKKO 2 Tutkimuskysymykset ja vastaukset

TUTKIMUSKYSYMYS	VASTAUKSET
Millä keinoilla sähköpostikalastelijat pyrkivät huijaamaan yritysten työntekijöitä?	• Vetoamalla tunteisiin (Hadnagy & Fincher, 2015; Hoheisel ym., 2023; Wang ym., 2020) • Herättämällä kohteessaan luottamusta (Archibald & Renaud, 2019; Verizon, 2023; Wang ym., 2020) • Tekeytymällä kohteelle entuudestaan tutuksi tai läheiseksi lähettäjäksi (Hadnagy & Fincher, 2015; Verizon, 2023)
Millainen rooli työntekijöiden tietoturvatietoisuudella on pk-yrityksen tietoturvan rakentamisessa?	• Työntekijöiden tietoturvatietoisuus luo perustan koko yrityksen tietoturvalle (Alahmari ym., 2023; Bada ym., 2019; Bada & Nurse, 2019; Siponen, 2000) • Hyvä tietoturvatietoisuuden taso pitää sisällään myös henkilöstön realistisen arvion omista ja organisaation kyvyistä uhkien torjumisessa (Koolen ym., 2024; Verizon, 2023; Wilson ym., 2023)

Vertaisarvioituja, vähintään JUFO -luokituksen kaksi lähteitä löytyi melko hyvin (10 kpl). Erityisesti Britanniassa tehtyjä tutkimuksia esiintyi hakutuloksissa paljon. Varshneyn ym. (2024) mukaan sähköpostikalastelun psykologisia aspekteja ei vielä ole tutkittu laajemmin aiemmissa tutkimuksissa. Tutkielmaan valikoidussa lähdemateriaalissa on muutamien vertaisarvioimattomien lähteiden (esim. Gartnerin ja Verizonin raporttien) lisäksi JUFO -luokituksen nolla tai yksi saaneita julkaisuja. Vertaisarvioimattomien lähteiden kuten kirjojen ja raporttien tapauksissa valittiin lähteitä, joita oli laajasti siteerattu tai ovat tutkimuskentällä muuten yleisesti tunnettuja. Gartnerin ja Verizonin materiaalien sisällyttämisellä pyrittiin lisäämään tutkielman käytännönläheisyyttä. Lähdemateriaalin valintakriteerien lisäksi tutkielman luotettavuutta pyrittiin lisäämään kuvaamalla tutkimusprosessia tarkasti sekä käyttämällä tunnettua hyväksi havaittua tutkimusmenetelmää eli kuvailevaa kirjallisuuskatsausta.

Tutkimuskysymysten vastauksista voidaan alustavasti vetää johtopäätös, että pk-yritysten on aktiivisesti pyrittävä parantamaan henkilöstönsä tietoturvatietoisuutta torjuakseen nykyaikaisia sähköpostikalasteluhyökkäyksiä. Pk-yritysten rajallisten resurssien takia turvallisuuskoulutukset on suunniteltava

vastaamaan työntekijöiden omia työnkuvia. Sen lisäksi yrityksen johdon tulisi kartoittaa, mitkä uhkatyypit ovat todennäköisimpiä kohdistumaan omaan yritykseen, jotta varautumiseen tehtäviä toimenpiteitä voidaan rajata vastaamaan organisaation käytössä olevia resursseja.

Esitettyjen tulosten perustuessa puhtaasti kirjallisuuskatsaukseen olisi mielenkiintoista tarkastella aihetta syvemmin esimerkiksi kyselyn tai tapaustutkimuksen keinoin. Niillä voitaisiin saavuttaaa konkreettisempia ja tuoreempia tuloksia suomalaisten pk-yritysten tietoturvatietoisuuden tasosta, empiirisen näkökulman tukiessa teoreettista tietopohjaa. Olisi myös kiinnostavaa tutkia työntekijöiden asenteiden vaikutusta organisaation tehokkuuteen sähköpostikalastelun torjumisessa. Olisi myös hyödyllistä tutkia tietoturvatietoisuuden tason kehitystä pitkittäistutkimuksena yksittäisen yrityksen sisällä, mikäli mahdollista, yrityksen perustamisvaiheesta alkaen. Pitkittäistutkimuksia voisi sisällyttää esimerkiksi tietoturvariskien minimoimiseen tarkoitettujen prosessien kuten riskienkartoituksien ja hankintaprosessien yhteyteen.

LÄHTEET

2022 Data Breach Investigations Report. (2022). Verizon Business. Noudettu 17. maaliskuuta 2023, osoitteesta https://www.verizon.com/business/en-sg/resources/reports/dbir/

2023 Data Breach Investigations Report. (2023). Verizon Business. Noudettu 3. joulukuuta 2023, osoitteesta https://www.verizon.com/business/resources/reports/dbir/

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, *22*(5), 453–474. https://doi.org/10.1016/0022-1031(86)90045-4

Alahmari, S., Renaud, K., & Omoronyia, I. (2023). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and E-Business Management*, *21*(1), 123–158. https://doi.org/10.1007/s10257-022-00575-2

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432–445. https://doi.org/10.1016/j.cose.2009.12.005

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. *Sensors*, *21*(20), Article 20. https://doi.org/10.3390/s21206901

An, Q., Hong, W. C. H., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2023). How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, *22*(2), 305–317. https://doi.org/10.1007/s10207-022-00637-z

Archibald, J. M., & Renaud, K. (2019). Refining the PoinTER "human firewall" pentesting framework. *Information & Computer Security*, *27*(4), 575–600. https://doi.org/10.1108/ICS-01-2019-0019

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *09.01.2019*. https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

Blackberry (2023). *Follina Vulnerability*. Noudettu 2. joulukuuta 2023, osoitteesta https://www.blackberry.com/us/en/solutions/endpoint-security/security-vulnerabilities/follina-vulnerability

Boehm, F., Hey, T., & Ortner, R. (2016). How to measure IT security awareness of employees: A comparison to e-mail surveillance at the workplace. *European Journal of Law and Technology*, *7*(1). https://ejlt.org/index.php/ejlt/article/view/500

Burda, P., Altawekji, A. M., Allodi, L., & Zannone, N. (2023). The Peculiar Case of Tailored Phishing against SMEs: Detection and Collective DefenseMechanisms at a Small IT Company. *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 232–243. https://doi.org/10.1109/EuroSPW59978.2023.00031

Cooper, M., Levy, Y., Wang, L., & Dringus, L. (2021). Heads-up! An alert and warning system for phishing emails. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 47–68. https://doi.org/10.1108/OCJ-03-2021-0006

Gartner (2023b). *Definition of Security – Gartner Information Technology Glossary*. (2023). Gartner. Noudettu 3. joulukuuta 2023, osoitteesta https://www.gartner.com/en/information-technology/glossary/security

Gartner (2023a). Driving Secure Employee Behaviors. https://emt.gartnerweb.com/ngw/globalassets/en/publications/documents/driving_secure_employee_behaviors.pdf

Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*. https://www.frontiersin.org/articles/10.3389/fdata.2021.583723

Hadnagy, C., & Wilson, P. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, Incorporated.

http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=706746

Hadnagy, C., Fincher, M., & Dreeke, R. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=1895166

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers and Security*, *128*. Scopus. https://doi.org/10.1016/j.cose.2023.103158

Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review*, *52*, 105914. https://doi.org/10.1016/j.clsr.2023.105914

Kyberturvallisuuskeskus (2023a). *Sähköpostikalastelut ja huijauspuhelut toivat huhtikuun kybersäähän epävakautta*. (2023, toukokuuta 11). Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa_04/2023

Kyberturvallisuuskeskus (2023b). Kybersää lokakuu https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%20lokakuu%202023.pdf

Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021). Social Engineering Attacks: Recent Advances and Challenges. Teoksessa A. Moallem (Toim.), *HCI for Cybersecurity, Privacy and Trust* (ss. 417–431). Springer International Publishing. https://doi.org/10.1007/978-3-030-77392-2_27

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, *132*, 103387. https://doi.org/10.1016/j.cose.2023.103387

Opara, C., Chen, Y., & Wei, B. (2024). Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics. *Expert Systems with Applications*, *236*, 121183. https://doi.org/10.1016/j.eswa.2023.121183

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of

Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. *Computers*, *11*(12), Article 12. https://doi.org/10.3390/computers11120174

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, *9*(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234

Salminen, A. (2011). Mikä Kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. https://urn.fi/URN:ISBN:978-952-476-349-3

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

SFS-EN ISO/IEC 27001:2023 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset

Smadi, S., Aslam, N., & Zhang, L. (2018). Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. *Decision Support Systems*, *107*, 88–102. https://doi.org/10.1016/j.dss.2018.01.001

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Takemura, T., & Komatsu, A. (2013). An Empirical Study on Information Security Behaviors and Awareness. Teoksessa R. Böhme (Toim.), *The Economics of Information Security and Privacy* (ss. 95–114). Springer. https://doi.org/10.1007/978-3-642-39498-0_5

The DFIR Report (2022, lokakuuta 31). Follina Exploit Leads to Domain Compromise. https://thedfirreport.com/2022/10/31/follina-exploit-leads-to-domain-compromise/

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management*, *13*(6), 1. https://doi.org/10.5539/ijbm.v13n6p1

Tilastokeskus. (2023). Noudettu 2. lokakuuta 2023, osoitteesta https://www.stat.fi/meta/kas/pk_yritys.html

OWASP-säätiö. (2022) *The Follina Vulnerability – A Critical Threat to Microsoft Office | OWASP Foundation*. (2022). Noudettu 7. lokakuuta 2023, osoitteesta https://owasp.org/www-community/vulnerabilities/follina

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*, *238*. Scopus. https://doi.org/10.1016/j.eswa.2023.122199

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

Wilson, M., De Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Information technology security training requirements: A role- and performance-based model* (NIST SP 800-16; 0 p., s. NIST SP 800-16). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-16

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. *Journal of Computer Information Systems*, *63*(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791

WithSecure. (2023) Unveiling the Arsenal. https://www.withsecure.com/content/dam/with-secure/en/resources/WS_Unveiling_the_Arsenal_EN.pdf