Digitaaliset uhat työpaikalla: Kyselytutkimus työntekijöiden kokemuksista tietojenkalastelusta

Mathias Helminen

Haaga-Helia ammattikorkeakoulu
Tietojenkäsittelyn tradenomi
Opinnäytetyö
2024

Tiivistelmä

Tekijä(t)
Mathias Helminen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Digitaaliset uhat työpaikalla: Kyselytutkimus työntekijöiden kokemuksista tietojenkalastelusta

Sivu- ja liitesivumäärä
25 + 4

Tässä tutkimukseen perustuvassa opinnäytetyössä kartoitettiin työntekijöiden kokemuksia tietojenkalastelusta. Tietojenkalastelu on yksi osa kyberrikollisuutta ja sillä on yhä suurempi vaikutus organisaatioihin ympäri maailman. Tutkimus toteutettiin määrällisellä eli kvantitatiivisella kyselyllä. Opinnäytetyöllä pyrittiin selvittämään, kuinka hyvin täysi-ikäiset suomalaisessa organisaatiossa työskentelevät henkilöt tuntevat tietojenkalastelu-termin, millaista tietojenkalastelua he ovat kohdanneet työelämässä, kohdistuuko tietojenkalastelu tietyllä alalla toimiviin yrityksiin enemmän kuin muihin ja millaisia keinoja yritykset käyttävät ennaltaehkäistäkseen tietojenkalasteluyrityksiä.

Opinnäytetyön tietoperustassa käydään läpi, mitä tietojenkalastelulla tarkoitetaan terminä, millaisia tapoja rikolliset käyttävät toteuttaakseen tietojenkalastelua ja mihin tietojenkalastelu perustuu psykologisesti. Tietoperustassa käydään myös läpi erilaisia tapoja, joilla voidaan suojautua tietojenkalasteluyrityksiltä. Kaikki muu tietojenkalasteluun liittyvä on rajattu pois opinnäytetyön tietoperustasta.

Opinnäytetyön tutkimuskysely sisälsi kymmenen kysymystä, joiden perusteella vastattiin tutkimuskysymyksiin. Kyselyyn vastasi 32 henkilöä ja se toteutettiin kevään 2024 aikana. Kysely tehtiin Microsoft Forms -alustalla.

Kyselytutkimuksesta saatujen tulosten perusteella voidaan todeta, että yleinen tuntemus tietojenkalastelusta oli hyvä vastaajien keskuudessa. Sähköpostilla tapahtuvaa tietojenkalastelua on kokenut yli 50 prosenttia kyselyyn vastanneista ja se oli suosituin tietojenkalastelun muoto. Kyselyn perusteella ei voida tehdä luotettavia päätelmiä siitä, millä alalla tietojenkalastelua tapahtuu eniten, sillä vastaajia ei ollut tarpeeksi. Kyselyn perusteella organisaatioiden menetelmät torjua tietojenkalastelua ovat monipuoliset ja hyvät. Menetelmiä ovat muun muassa tietoturvakoulutus työntekijöille ja vahvat salasana- ja tunnistautumisvaatimukset. Tutkimuksesta saatujen tietojen mukaan organisaatioiden kyky suojautua tietojenkalastelua vastaan on hyvällä mallilla.

Opinnäytetyöstä saatujen tulosten perusteella näyttää siltä, että ihmisten tietoisuus tietojenkalastelusta on hyvä ja organisaatiot tiedostavat siitä aiheutuvat riskit.

Asiasanat
Tietojenkalastelu, tietoturva, kyberrikollisuus, verkkourkinta, tietomurto

Sisällys

1 Johdanto

Opinnäytetyöni aihe liittyy työssä käyvien ihmisten kokemuksiin tietojenkalasteluyrityksistä yritysmaailmassa. Valitsin tämän aiheen, koska tietojenkalastelu on merkittävä ja jatkuvasti kasvava digitaalinen uhka nykyaikaisissa työympäristöissä ympäri maailman. Se muodostaa vakavan haasteen organisaatioille ja työntekijöille, sillä se voi johtaa arkaluonteisen tiedon vuotamiseen, taloudellisiin menetyksiin ja mahdollisesti koko yrityksen konkurssiin. Opinnäytetyön tavoitteena on syventyä tähän ilmiöön ja selvittää, millaisia kokemuksia työntekijöillä on tietojenkalastelusta omalla työpaikallaan.

Tietoturvaan liittyvät asiat ovat olleet esillä muutaman viime vuoden aikana yhä enemmän ja media on alkanut uutisoimaan aiheesta ahkerasti. Yleensä uutisointi on kohdistunut tietomurtoihin ja niistä aiheutuneisiin vahinkoihin. Yhä useammin tietomurroilla on vakavia yhteiskunnallisia seurauksia kuten Vastaamon tapauksessa Suomessa, jossa hakkeri varasti ja julkisti tietokannan, joka sisälsi ihmisten henkilökohtaisia tietoja. (Yle 2020.) Tietojenkalastelu on siis usein keskeisessä roolissa, kun tapahtuu tietomurto, sillä sen avulla hyökkääjä pyrkii pääsemään käsiksi yksilön tai organisaation yksityisiin tietoihin.

Tämä opinnäytetyö pitää sisällään kvantitatiivisen tutkimuksen, joka toteutettiin kyselytutkimuksella. Kysely sisälsi valmiiksi annettuja vastausvaihtoehtoja erilaisiin kysymyksiin, joten vastausten tilastoiminen ja esittäminen oli yksinkertaista. Kohtaan tietojenkalastelua työssäni päivittäin ja siksi halusin tutkia aihetta lisää. Uskon, että tutkimuksesta saatavilla vastauksilla on hyötyä työssäni.

Tämä opinnäytetyö on rajattu tietojenkalasteluun yritysmaailmassa ja kyselytutkimus on suunnattu täysi-ikäisille henkilöille, jotka ovat töissä Suomessa toimivassa yrityksessä. Kyselytutkimuksesta on rajattu pois yksityiselämässä tapahtuneet tietojenkalasteluyritykset.

Opinnäytetyön tietoperusta on rajattu niin, että siinä käydään läpi vain, mitä tietojenkalastelu on, miten sitä tapahtuu ja mihin se perustuu. Jos haluaa ymmärtää tietojenkalastelusta enemmän niin silloin pitää tutustua psykologisiin tekniikoihin, joita hyökkäyksissä käytetään. Näitä psykologisia menetelmiä käydään myös läpi opinnäytetyön tietoperustassa.

Tällä opinnäytetyöllä haetaan vastauksia seuraaviin tutkimuskysymyksiin:

- Tietävätkö työelämässä olevat henkilöt mitä tietojenkalastelu on?
- Millaista tietojenkalastelua työssä käyvät ihmiset ovat kohdanneet työelämässä?
- Kohdistuuko tietojenkalastelu tietyllä alalla toimiviin yrityksiin enemmän kuin muihin?
- Millaisia keinoja yritykset käyttävät ennaltaehkäistäkseen tietojenkalasteluyrityksiä?

1.1 Keskeiset käsitteet

Tietojenkalastelu on termi, jolla yleensä tarkoitetaan yhtä verkkorikollisuuden osa-aluetta, jossa uhria lähestytään aidolta näyttävällä sähköpostilla, tekstiviestillä tai puhelulla, aikomuksena saada huijattua uhrilta joko henkilökohtaisia tietoja tai salasanoja. Tietojenkalastelu on yksi ensimmäisistä vaiheista verkon kautta tehtävissä kyberhyökkäyksissä. (Phishing.org s.a.)

Phishing on englanninkielinen sana ja tarkoittaa tietojenkalastelua. Termiä käytetään yleisesti, kun puhutaan sähköpostilla tapahtuvasta tietojenkalastelusta. Tavallisesti kun puhutaan phishing-sanasta, sillä tarkoitetaan huijausviestejä, jotka on lähetetty massana satunnaisille vastaanottajille. (IBM s.a.)

Spear phishing on englanninkielinen sana ja tarkoittaa kohdennettua tietojenkalastelua. Erona tavalliseen tietojenkalasteluun on se, että kohdennettu tietojenkalastelu on kohdistettu ennalta valittuihin henkilöihin. (Kaspersky s.a. b.)

Smishing on englanninkielinen sana ja tarkoittaa tekstiviestillä tai pikaviestipalvelun kautta toteutettavaa tietojenkalastelua. (Kaspersky s.a. a.)

Vishing on englanninkielinen sana ja tarkoittaa puhelimitse toteutettavaa tietojenkalastelua. (F-Secure s.a.)

Monivaiheinen tunnistautuminen (engl. Multi-Factor Authentication, MFA) on autentikointimenetelmä, jossa käyttäjän tulee vahvistaa kirjautuminen palveluun tai laitteelle vähintään kahdella eri tavalla. Monivaiheisen tunnistautumisen käyttäminen ennaltaehkäisee tietojenkalastelua. (AWS s.a.)

Sosiaalinen manipulointi on tapa vaikuttaa toisen ihmisen käyttäytymiseen hyödyntämällä psykologisia keinoja. Yleensä sosiaalisella manipuloinnilla yritetään vaikuttaa kohteeseen niin, että kohde tekee asioita, jotka ovat itselleen haitallisia. (Colorado Department of Education 2020.)

2 Tietojenkalastelu

2.1 Mitä tietojenkalastelu on?

Tietojenkalastelulla tarkoitetaan yhtä kyberrikollisuuden osa-aluetta, jossa uhria lähestytään aidolta näyttävällä sähköpostilla, tekstiviestillä tai puhelulla, aikomuksena saada huijattua uhrilta joko henkilökohtaisia tietoja tai salasanoja. Hyökkääjän tarkoitus on esiintyä jonain toisena henkilönä, yleensä luotettuna sellaisena, kuten esimerkiksi poliisina tai työkaverina. Tämän jälkeen hyökkääjä yrittää käyttää kalasteltuja tietoja omien tavoitteidensa saavuttamiseen, kuten rahojen varastamiseen uhrin tililtä tai henkilökohtaisten tiedostojen lataamiseen uhrin tietokoneelta. (Phishing.org s.a.)

Tietojenkalastelu perustuu sosiaaliseen manipulointiin, jota hyökkääjä käyttää hyväkseen lähettäessään huijausviestiä. Tällaisia psykologisia keinoja on esimerkiksi kiireen tunteen lisääminen viestiin tai auktoriteetin käyttäminen esiintymällä uhrin esihenkilönä. (Colorado Department of Education 2020.) Uhrin on tällöin tehtävä vaikea päätös, uskoako viestin lähettäjää vai ei. Usein käy niin, että uhri uskoo hyökkääjää ja tekee juuri niin kuin hyökkääjä haluaa.

2.2 Tietojenkalastelun historia

Tietojenkalastelua kuvailtiin ensimmäisen kerran vuonna 1987 HP Users Group:n julkaisussa Intertext, mutta tiettävästi ensimmäiset hyökkäykset tehtiin vasta noin kymmenen vuotta myöhemmin vuonna 1996. (Graphus 2023.)

Vaikka tietojenkalastelu alkoi 1990-luvulla, niin se yleistyi 2000-luvun puolessa välissä. Ensimmäiset tunnetut ja isommat tietojenkalastelua hyödyntävät hyökkäykset kohdistuivat verkkokauppoihin kuten eBayhin ja PayPaliin. Tällöin hyökkääjät esittivät olevansa edellä mainittujen yritysten henkilökuntaa ja pyysivät asiakkaita lähettämään luottokorttiensa tiedot heille. (Graphus 2023.)

2010-luvulla kyberrikollisuus alkoi muuttamaan muotoa entistä ammattimaisempaan suuntaan. Tietojenkalastelusta tuli silloin hakkerien käytetyimpiä menetelmiä päästä sisään järjestelmiin. Vuonna 2017, 91 % kaikista kyberhyökkäyksistä alkoi tietojenkalastelulla. (Fortra 2017.) Kuusi vuotta myöhemmin vuonna 2023, luku on pysynyt miltei samana Cloudflaren tekemän tutkimuksen mukaan. (Cash J. Dzuba E. 16.8.2023.)

2.3 Mitä tietojenkalastelulla halutaan saavuttaa?

Kyberrikollisten isoin motivaatio tehdä rikoksia on ansaita rahaa laittomasti, eikä tietojenkalastelu poikkea tästä. Nykyään melkein kaikki laitteet, joita kannamme mukana ovat yhteydessä internetiin. Maksamme niillä laskumme ja säilytämme niillä henkilökohtaisia asioita, kuten kuvia ja

salasanoja. Tämä tarjoaa rikollisille laajan hyökkäysvektorin, jonka avulla he voivat rikoksia tekemällä tienata rahaa. (Grimes R. 22.1.2023.)

Rahan jälkeen seuraavaksi suurin motivaation lähde on tiedon varastaminen. Tiedot voi tietysti myydä, mutta kyberrikolliset voivat myös varastaa tietoa muista syistä. Tällaisia syitä on esimerkiksi teollisuusvakoilu, jossa motivaationa on saada tärkeää tietoa kilpailevan yrityksen toiminnasta ja sitä kautta hyötyä tilanteesta. (Grimes R. 22.1.2023.)

Kolmas syy kyberhyökkäyksille on yksinkertaisesti halu häiritä tai aiheuttaa harmia. Hyvä esimerkki on Ukrainassa käynnissä oleva sota, johon on oleellisesti kuulunut erilaiset kyberoperaatiot. Tietojenkalastelua on voitu käyttää välineenä päästä sisään vihollisarmeijan tietojärjestelmiin ja sitä kautta häiritä heidän toimintaansa. Näissä operaatioissa ei motiivina ole ollut raha tai tiedon varastaminen vaan mahdollisimman suuren tuhon aiheuttaminen elektronisesti.

2.4 Sosiaalinen manipulointi tietojenkalastelussa

Tietojenkalasteluun liittyy paljon psykologisia tekijöitä, joiden avulla uhri yritetään saada tekemään itselleen haitallisia asioita, kuten luovuttamaan salasanansa tai tärkeät henkilökohtaiset tiedot. Ihmisten manipulointia on tutkittu jo vuosikymmeniä ja samat menetelmät pätevät myös tietojenkalasteluun, joten siitä syystä on hyvä käydä läpi mitä nämä menetelmät pitävät sisällään.

Ihmisen aivot luovat automaattisesti tapoja ja rutiineja, jotta energiaa kuluisi mahdollisimman vähän elintoimintojen ylläpitämiseen. Tästä syntyy malleja, joita toistamme usein, esimerkiksi hampaiden pesu heti herättyämme, tai sosiaalisen median selaaminen puhelimella ennen nukkumaanmenoa. Olisi hyvin raskasta ja aikaa vievää, jos joutuisimme ajattelemaan kaikista pienempiäkin päivän aikana tapahtuvia valintoja liian pitkään. Onneksi ihmisen mieli on kuitenkin tehty niin, että tällaiset ajatukset ja valinnat tehdään yleensä tiedostamatta. (World of Work Project 2019.)

Psykologi Robert Cialdini loi perusteet psykologiselle suostuttelulle kirjassaan ”Influence: The Psychology of Persuasion” ja kirja julkaistiin vuonna 1984. Kirjassa hän tutkii, mitkä asiat vaikuttavat päätöksen tekemiseen osta- ja myyntitilanteissa. Hän päätyi kuuteen ydinperiaatteeseen, jotka vaikuttavat osto- ja myyntikäyttäytymiseen. Näillä kuudella menetelmällä voidaan manipuloida ihmisiä tekemään asioita heidän tiedostamattaan. Cialdinin löytämät kuusi periaatetta ovat: vastavuoroisuus, niukkuus, auktoriteetti, johdonmukaisuus, pidettävyys ja sosiaalinen yhteisymmärrys. (World of Work Project 2019.)

2.4.1 Vastavuoroisuus

Tietojenkalastelussa vastavuoroisuudella tarkoitetaan ihmisten halua antaa vastapalveluksia toisilleen. Sosiaalisen manipuloinnin avulla hyökkääjä voi esimerkiksi kehua uhria hyvin tehdystä työstä. Tämä voi kuulostaa pieneltä ja mitättömältä eleeltä, mutta ihminen lähtökohtaisesti haluaa tuntea olonsa hyväksytyksi. Tällä tavalla manipuloija kasvattaa luottamusta uhriinsa ja odottaa saavansa vastapalveluksen tulevaisuudessa. Tällainen vuorovaikutus on tavallista ihmisten välillä, mutta vilpillisellä mielellä oleva henkilö voi hyötyä tästä paljonkin. (Cialdini 2006, 13–16.)

2.4.2 Niukkuus

Tietojenkalastelussa niukkuus voi tarkoittaa esimerkiksi rajallisesti saatavia tuotteita tai ainutlaatuisia mahdollisuuksia. Esimerkiksi alennusmyyneistä voi löytyä tarjouksessa olevia tuotteita, joita ei muuten ostaisi, mutta koska tuote on tarjouksessa niin henkilö päättää tehdä ostopäätöksen. Tässä tapauksessa rajallinen aika ja edullinen hinta luo ihmiselle paineen ostaa kyseisen alennustuotteen. (Cialdini 2006, 178–183.)

2.4.3 Auktoriteetti

Ihmiset on luotu kuuntelemaan auktoriteetin omaavaa ihmistä jo aikojen alusta asti. Se todennäköisesti johtuu siitä, että meidät on kasvatettu pienestä pitäen kuuntelemaan ihmisiä, joilla on meitä enemmän valtaa. Pieninä lapsina kuuntelimme vanhempiamme, koulussa kuuntelimme opettajiamme ja nykyään työelämässä kuuntelemme esihenkilöitämme. Auktoriteettiin liittyy yleensä myös palkinnot ja rangaistukset, eli hyvästä teosta voidaan palkita, kun taas pahasta teosta voidaan rangaista. Sosiaalisessa manipuloinnissa vilpillinen henkilö voi esiintyä esimerkiksi lääkärinä ja tällä tavalla vaikuttaa uhrin käyttäytymiseen. Lääkäriä pidetään yleensä auktoriteettina, jonka takia uhri saadaan tekemään asioita, joita hän ei muuten tekisi. (Cialdini 2006, 157–164.)

2.4.4 Johdonmukaisuus ja sitoutuneisuus

Johdonmukaisuudella ja sitoutuneisuudella viitataan usein ihmisten haluun pysyä sovituissa asioissa tai tehdyissä lupauksissa. Usein sosiaalisessa manipuloinnissa rikollinen aloittaa keskustelun uhrin kanssa, jossa hänen motiivinaan on saada uhrin luottamus. Keskustelun aloitus ja aihe eivät välttämättä liity millään tavalla siihen, mitä rikollinen haluaa uhrista. Kun uhrin luottamus on saatu, rikollinen alkaa kyselemään hellävaraisesti häntä kiinnostavia kysymyksiä, joihin rikollinen toivoo uhrin vastaavan. Eli johdattelemalla keskustelua, rikollinen yrittää saada vastauksia häntä hyödyttäviin kysymyksiin. (Cialdini 2006, 43–47.)

2.4.5 Pidettävyys

Ihmiset lähtökohtaisesti tykkäävät toisista ihmisistä, jotka ovat heille mukavia. Tämä perustuu ihmisen luontaiseen käyttäytymiseen. Joten olemalla mukava ja oikeasti kiinnostunut toisesta ihmisestä, ansaitset yleensä hänen luottamuksensa. Tätä myös rikolliset osaavat hyödyntää, eikä ole yhtään poikkeavaa, että sosiaalinen manipulointiyritys perustuu sille, että hyökkääjä esittää mukavaa ja helposti lähestyttävää henkilöä. (Cialdini 2006, 126–129.)

2.4.6 Sosiaalinen yhteisymmärrys

Sosiaalisella yhteisymmärryksellä tarkoitetaan tässä kontekstissa mielipiteiden ja käytöstapojen kopiointia ja matkimista toisilta ihmisiltä. Ihmiset saattavat esimerkiksi tehdä ostopäätöksiä ystävien mielipiteiden perusteella, sillä ihmisille on luonnollista kuunnella ystävien mielipiteitä. On myös paljon todennäköisempää, että ihminen tekee myönteisen ostopäätöksen sen perusteella, mitä hänen suosikki julkisuuden henkilö mainostaa. Ihmisille on luontaista kopioida tiettyjä käyttäytymismalleja muilta, varsinkin jos he eivät ole aivan varmoja, miten pitäisi toimia. (Cialdini 2006, 87–91.)

3 Tietojenkalastelun eri toteuttamistapoja

3.1 Phishing

Phishing on englanninkielinen sana ja tarkoittaa suomeksi tietojenkalastelua. Tietojenkalastelu-hyökkäyksessä hyökkääjä yrittää saada uhrin jakamaan yksityisiä tietoja tai dataa, johon hyökkääjällä ei muuten olisi pääsyä. Hyökkääjä esittää melkein aina olevansa joku toinen henkilö kuin oikeasti on, tarkoituksenaan saada uhri uskomaan, että viesti on tullut aidolta ja oikealta lähettäjältä. Tämä tapahtuu usein sähköpostiviestien välityksellä, jolloin hyökkääjä lähettää haittaohjelman tai haittaohjelmaan ohjaavan linkin sähköpostilla mahdollisimman monelle henkilölle, toivoen että uhrit avaisivat kyseisen sähköpostiviestin sisältämän tiedoston tai linkin. Haittaohjelma voi olla esimerkiksi väärennetty, mutta aidon näköinen Word- tai Excel-tiedosto. Kun uhri avaa haitallisen tiedoston, hänen laitteensa suorittaa haittaohjelman ja ”saastuu”. Tämän seurauksena hyökkääjä on onnistuneesti saanut varastettua halutut tiedot. (IBM s.a.)

Tietojenkalastelun toimivuus perustuu massoittain lähetettyihin kalasteluviesteihin. Usein hyökkääjä on saanut jollain tavalla haltuunsa runsaan määrän sähköpostiosoitteita, joihin hän lähettää kalasteluviestin ja toivoo, että mahdollisimman moni avaa sen. Jos uhri avaa sähköpostissa olevan linkin ja syöttää tietonsa tai salasanansa siellä kysyttyihin kysymyksiin tai pyyntöihin, hyökkääjä saa kaikki tiedot omalle tietokoneelleen. (Imperva s.a.)

Tietojenkalastelu ei rajoitu pelkästään sähköpostilla tehtäviin huijausyrityksiin, vaan sitä tehdään myös internet-puheluilla (engl. vishing) tai perinteisillä tekstiviesteillä (engl. smishing.) Molemmat näistä toimivat samalla tavalla kuin sähköpostilla tehtävä tietojenkalastelu, eli hyökkääjä yrittää saada uhrin tekemään halutun asian, joka on vahingollinen uhrille. (Malwarebytes s.a.)

Kuva 1. Tyypillinen tietojenkalastelusähköposti

Omaan sähköpostiini tullut viesti (Kuva 1) on tyypillinen esimerkki tietojenkalastelusähköpostista. Viesti sisältää oudon linkin ja otsikossa lukee ”winning confirmation”. En ole osallistunut mihinkään

kilpailuun, lähettäjä ei ole entuudestaan tuttu ja viestissä oleva linkki vie nettisivulle, joka on selkeää tietojenkalastelua. Tällaisia samanlaisia viestejä lähetetään usein mahdollisimman monelle henkilölle ja toivotaan, että uhri avaa linkin.

3.2 Spear phishing

Kohdennettu tietojenkalastelu (engl. spear phishing) eroaa tavallisesta tietojenkalastelusta sillä, että se kohdistuu ennalta valittuun kohteeseen, ja tarkoituksena on, että laatu korvaa määrän. Kohdennetussa tietojenkalastelussa kohde voi esimerkiksi olla kohteena olevan yrityksen johtohenkilö. Eli hyökkääjä kohdistaa tietojenkalastelun ennalta määrättyyn henkilöön. Tällä tavalla hyökkääjä pyrkii saamaan tarvittavat salasanat tai tiedot uhrilta, päästäkseen sisään hyökättävään kohteeseen ja heidän tietojärjestelmiinsä. Kohdennettu tietojenkalasteluyritys on myös vaikeampi toteuttaa verrattuna tavalliseen kalasteluyritykseen, sillä se vaatii paljon enemmän taustatyötä ja valmisteluja hyökkääjältä. (Kaspersky s.a. b.)

Kohdennettua tietojenkalastelua voi myös tehdä soittamalla tai tekstiviestitse, tällöin puhutaan kohdennetusta smishingistä ja vishingistä.

3.3 Smishing

Smishing tulee englannin kielen sanojen SMS (short message services) ja phishing yhdistelmästä. Kyseessä on siis tekstiviestillä tapahtuva tietojenkalastelu, jossa hyökkääjä lähettää haitallisen linkin tai tiedoston sisältävän tekstiviestin uhrin puhelimeen. Tällainen linkki yleensä vie käyttäjän oikean näköiselle nettisivulle, jolloin uhri luovuttaa esimerkiksi salasanansa suoraan hyökkääjälle. Toinen hyökkääjän tapa hyödyntää linkkiä on ohjata uhri lataamaan haitallinen ohjelma puhelimeensa. Tällöin hyökkääjä voi esimerkiksi päästä suoraan käsiksi uhrin puhelimen koko sisältöön. (Kaspersky s.a. a.)

Smishingiin pätee samat lainalaisuudet kuin tavalliseenkin sähköpostilla tehtävään tietojenkalasteluun. Hyökkääjä pyrkii saamaan uhrin luottamuksen esittämällä luotettavaa henkilöä esimerkiksi esiintymällä poliisina tai verkkokauppana. Myös psykologiset keinot pätevät smishingiin, tunteiden avulla hyökkääjä pyrkii saamaan uhrin tekemään itselleen haitallisia asioita. Hyvänä esimerkkinä hyökkääjä yleensä lisää kiireen tuntua viestin sisältöön, laittaen painetta uhrille päätöksentekoon. (Kaspersky s.a. a.)

Paras tapa suojautua tekstiviestillä tapahtuvaa tietojenkalastelua vastaan on olla avaamatta epämääräisiä ja odottamattomia tekstiviestejä. Yleensä pitkälle pääsee jo pelkällä maalaisjärjellä. On myös hyvä pitää mielessä, että mitään arkaluontoisia tietoja ei kysytä tekstiviestillä, joten niitä ei myöskään pitäisi antaa kysyttäessä. Jos esimerkiksi pankki lähettää sinulle tekstiviestin, niin he

yleensä ohjaavat sinut menemään heidän nettisivuillensa suoraan ilman minkään linkin avaamista. Tällaisessa tilanteessa, jos alat epäröimään tilannetta niin voit aina soittaa pankkiin ja kysyä, että ovatko he lähettäneet kyseisen tekstiviestin. (Kaspersky s.a. a.)

3.4 Vishing

Vishing tulee englannin kielen sanojen voice ja phishing yhdistelmästä. Kyberrikolliset ovat jo pitkään käyttäneet tätä metodia huijatessaan ihmisiä. Vishingissä hyökkääjä soittaa uhrille ja esittää olevansa joku muu kuin oikeasti on, eli tietojenkalastelu tapahtuu puhelimitse. Tämän tarkoitus on huijata uhri luulemaan, että hyökkääjä on se henkilö, joka hän sanoo olevansa, eli esimerkiksi poliisi tai muu luotettavalta kuulostava henkilö. (F-Secure s.a.)

Nykyaikaisella tekniikalla vishing-huijausta ei ole aina niin helppoa tunnistaa. Yksi isoimmista syistä tähän on niin sanottu ”deepfake” -tekniikka, jonka avulla kuka tahansa voi esiintyä toisena henkilönä. Tämä on avannut rikollisille oivan tavan huijata ihmisiä. Deepfake perustuu tekoälyyn ja sen perimmäinen tarkoitus oli helpottaa ihmisten arkea. Deepfake-huijauksella tehtyjä huijauksia on raportoitu tapahtuneen paljon viimeisten vuosien aikana. Yksi tällainen esimerkki löytyy muutaman vuoden takaa, jolloin kyberrikolliset onnistuivat huijaamaan Iso-Britannialaiselta yritykseltä noin 243 000 dollaria. Hyökkääjät esiintyivät emoyrityksen toimitusjohtajana käyttäen deepfakella tehtyä aidon kuuloista ääntä. Huijaus meni täydestä ja uhriyritys maksoi väärennetyn laskun uskoen, että puhelu tuli oikealta toimitusjohtajalta. (Trend Micro 2019.)

4 Kuinka tietojenkalastelulta voi puolustautua?

Tietojenkalasteluhyökkäykset ovat tänä päivänä entistä paremmin suunniteltuja ja toteutettuja ja siitä syystä jokaisen kannattaisi miettiä, miten niiltä voisi välttyä parhaiten. Ensimmäinen askel tähän on tiedostaminen, mitä tietojenkalastelu on ja millä tavalla sitä ilmenee. Tietämättömyys on yksi suurimmista syistä, miksi ihmiset joutuvat huijauksen uhreiksi. Yritysmaailmassa työntekijöille pidetään usein koulutus liittyen tietojenkalasteluun, kun he aloittavat työn uudessa yrityksessä. Tämä on tietenkin erinomainen asia, jos tällaisia koulutuksia pidetään, mutta aina niin ei kuitenkaan tapahdu. Tässä tapauksessa puhutaan ennaltaehkäisevän koulutuksen tärkeydestä. Mielestäni ensisijainen vastuu tietojenkalastelun perusperiaatteista kuuluu yksilölle itselleen, varsinkin kun elämme digitaalisten laitteiden aikakautta. (Simister A. 23.4.2024.)

Ennaltaehkäisevän koulutuksen lisäksi tehokas tapa suojautua tietojenkalastelulta on käyttää teknisiä järjestelmiä kuten päätelaitteen suojausta tai virustorjuntaa. Nykyään tällaiset järjestelmät tulevat automaattisesti uusien laitteiden mukana, mutta niiden pitäminen ajan tasalla on tärkeää. Tässä luvussa käyn lyhyesti läpi tärkeimmät tekniset suojautumistavat sekä ennaltaehkäisevän koulutuksen tärkeyden yritysmaailmassa. (Simister A. 23.4.2024.)

4.1 Ennaltaehkäisevä koulutus yrityksessä

Kuten jo yllä mainitsin, ennaltaehkäisevä koulutus ja tietämys tietojenkalastelusta on avainasemassa, kun halutaan suojautua tietojenkalasteluhyökkäyksiltä. Isoimmassa vaarassa ovat yleensä pienet tai keskisuuret yritykset, joilla ei ole omaa tietoturvayksikköä. Heidän tapauksessaan olisi erittäin tärkeä panostaa ennaltaehkäisevään koulutukseen, sillä riittävällä tietämyksellä pystytään usein välttämään tietojenkalastelun aiheuttamat vaarat. (America’s Cyber Defense Agency s.a.)

Ennaltaehkäisevästä koulutuksesta puhuttaessa tärkein asia olisi tehdä ohjeet tietojenkalastelun tunnistamiseen. Siinä tulisi käydä läpi tietojenkalastelun eri muodot ja esimerkkien avulla näyttää, miltä oikeat hyökkäykset näyttävät. Hyvin tehdyn oppaan avulla työntekijät tulisivat tietoisiksi tietojenkalastelun eri menetelmistä, ja he osaisivat tunnistaa esimerkiksi sähköpostilla tulevan tietojenkalasteluhyökkäyksen. Oppaita ei myöskään tarvitse tehdä itse, jos tarvittavaa osaamista ei löydy yrityksestä. Esimerkiksi Suomen Kyberturvallisuuskeskuksella on ilmaisia oppaita, joita yritykset voivat hyödyntää toiminnassaan. (Kyberturvallisuuskeskus s.a.)

Ennaltaehkäisevässä koulutuksessa olisi tärkeä panostaa koulutuksen uusittavuuteen, tarkoittaen sitä, että koulutuksia olisi hyvä järjestää useamman kerran vuodessa. Tällä tavalla työntekijät pääsisivät harjoittelemaan useamman kerran vuodessa, ja tietojenkalastelu aiheena pysyisi mielessä

paremmin. Tällä tavalla myös tietoturva saataisiin pysymään työntekijöiden ajatuksissa läpi vuoden.

4.2 Monivaiheinen tunnistautuminen (MFA)

Yksi tärkeimmistä teknisistä tavoista suojata käyttäjiä tietojenkalastelulta on ottaa käyttöön monivaiheinen tunnistautuminen. Nimi tulee englannin kielen sanoista multi-factor authentication (MFA). Nykyään melkein aina palveluihin kirjaudutaan salasanalla ja rikolliset ovat erityisen kiinnostuneita niistä. Monivaiheisen tunnistautumisen tärkein idea on lisätä yksi turvakerros lisää kirjautumista tehdessä. Melkein kaikkiin nykyaikaisiin järjestelmiin saadaan liitettyä jokin monivaiheisen tunnistautumisen metodi. Ajatus siinä on, että hyökkääjän saadessa salasanan haltuunsa hän ei pysty pelkästään sillä kirjautumaan kohdejärjestelmään, vaan hän joutuu antamaan myös jonkin muun varmenteen. Tällaisia varmenteita voi olla esimerkiksi sähköpostiin lähetettävä koodi, jonka syöttämällä käyttäjä pääsee kirjautumaan järjestelmään, olettaen, että myös salasana on oikein. Varmenteeksi sopii myös esimerkiksi sormenjälki. (AWS s.a.)

Monivaiheinen tunnistautuminen kannattaisi ottaa käyttöön kaikkiin mahdollisiin järjestelmiin ja sovelluksiin työpaikalla sekä yksityiselämässä. Tällä menetelmällä saadaan usein estettyä tietojenkalasteluhyökkäykset, sillä hyökkääjä pääsee harvoin käsiksi uhrin monivaiheisen tunnistautumisen metodeihin. Eli vaikka salasana päätyisi rikollisille, he eivät hyötyisi siitä juurikaan.

4.3 Päätelaitteiden suojaus

Teknologia mahdollistaa nykyään todella kattavan ja hyvän suojan työasemien ja puhelimien suojaamiseen kyberrikollisilta. Tässä yhteydessä päätelaitteilla tarkoitan juuri tietokoneita ja puhelimia. Nykyään melkein jokainen yritys on jollain tavalla riippuvainen tietokoneista; niillä tehdään töitä, niillä säilytetään tärkeää dataa ja niiden avulla pyöritetään tärkeitä järjestelmiä. On siis erittäin tärkeää, että myös päätelaitteiden suojaus on ajan tasalla. Tämä kaikki korostuu nykyaikaisessa työympäristössä, jossa työntekijät tekevät töitä muualta kuin fyysiseltä toimistolta käsin. Työntekoon tarkoitettuja yritykseltä saatuja tietokoneita saatetaan käyttää omien henkilökohtaisten asioiden hoitoon vapaa-ajalla ja tästä seuraa väistämättä riskejä, joita koitetaan minimoida päätelaitteiden suojauksella.

Päätelaitteiden suojaamiseen on monia eri tekniikoita, mutta yleisin tapa on käyttää virustorjuntaohjelmaa, jonka tehtävä on havaita erilaisia haitallisia indikaattoreita käyttäjän päätelaitteelta. Tällaisia indikaattoreita voi olla esimerkiksi epäilyttävät nettisivut tai haitallisten tiedostojen tiivisteet. Kyseiset uhat liittyvät yleensä kuitenkin haittaohjelmiin. Tällä tavalla pyritään siis havaitsemaan ja tunnistamaan uhkia päätelaitetasolla, kun hyökkääjä ei ole vielä päässyt sisään uhrin järjestelmiin. (Check Point s.a.)

Toinen hyvä tapa suojata päätelaitteita on käyttää EDR-järjestelmää. EDR tulee englannin kielen sanoista Endpoint Detection and Response. Sen tarkoitus on havaita uhkia laajemmin kuin virustorjuntaohjelman. EDR-järjestelmiä käytetään yleensä isommissa yrityksissä, joissa on omat resurssit omalle tietoturvayksikölle. (Check Point s.a.)

4.4 Salasanojen hallintasovellus

Salasana ei saisi koskaan olla sama useassa sovelluksessa tai järjestelmässä, sillä salasanan päätyessä hyökkääjälle hän voisi yrittää käyttää salasanaa muihin uhrin järjestelmiin tai sovelluksiin. Salasana ei myöskään saisi olla liian heikko, eli sen pitäisi olla tarpeeksi pitkä ja sisältää kirjaimia, numeroita ja erikoismerkkejä. Ihmisen on vaikea muistaa useita satunnaisia ja pitkiä salasanoja ja siitä syystä olisi hyvä käyttää salasanojen hallintasovellusta, sillä siellä on helppo luoda monimutkaisia uniikkeja salasanoja.

Salasanojen hallintasovelluksen idea on siinä, että sovelluksen sisään voi tallentaa monimutkaisia ja satunnaisesti generoituja salasanoja jokaiselle eri sovellukselle ja järjestelmälle erikseen. Tällöin vältytään samojen helppojen salasanojen käyttämiseltä uudestaan eri sovelluksissa. Riittää, että muistaa yhden ainoan salasanan, jolla kirjaudutaan salasanojen hallintasovellukseen. Tämä on erittäin tehokas tapa välttää samojen salasanojen käyttö eri sovelluksissa. Hyökkääjän saadessa käsiinsä yhden käyttämäsi salasanan, et joudu vaihtamaan kaikkia salasanojasi vaan riittää, että vaihdat ainoastaan kyseisen salasanan. Erilaisia salasananhallintaohjelmia on useita ja niiden käyttö on helppoa, vaikka ei olisikaan suurta tietoteknistä osaamista. (Kyberturvallisuuskeskus 2020.)

5 Kyselytutkimus työntekijöiden kokemuksista tietojenkalastelusta

5.1 Kyselytutkimus

Kyselytutkimus toteutettiin, jotta saataisiin vastauksia opinnäytetyön alussa esitettyihin tutkimuskysymyksiin. Tutkimuskysymykset olivat seuraavanlaisia: Millaista tietojenkalastelua työssä käyvät ihmiset ovat kohdanneet työelämässä? Tietävätkö työelämässä olevat henkilöt mitä tietojenkalastelu on? Kohdistuuko tietojenkalastelu tietyllä alalla toimiviin yrityksiin enemmän kuin muihin? Millaisia keinoja yritykset käyttävät ennaltaehkäistäkseen tietojenkalasteluyrityksiä?

Kyselyä testattiin kahdella eri testikäyttäjälle ennen sen julkaisua. Kysely ehti olemaan auki vain kaksi päivää, sillä muuten aika opinnäytetyön tekemiseen olisi loppunut kesken. Kyselytutkimuksessa oli kymmenen kysymystä liittyen tutkittavaan aiheeseen eli tietojenkalasteluun ja lopussa oli vapaamuotoinen tekstikenttä palautteelle. Kyselytutkimukseen vastasi 32 henkilöä. Itse kysely tehtiin Microsoft Forms -alustalla. Yritin parhaani mukaan levittää tutkimuskyselyä eri alalla työskenteleville henkilöille, jotta vältyttäisiin siltä, että pelkät työkaverini tietoturva-alalta vastaisivat kyselyyn. Tästä syystä annoin kyselyn täytettäväksi vain kahdelle työkaverilleni. Vähäisen vastaajamäärän takia kyselyn tuloksia ei voi pitää luotettavana, mutta kysely kuitenkin antaa suuntaa ihmisten tietoisuudesta tietojenkalastelusta.

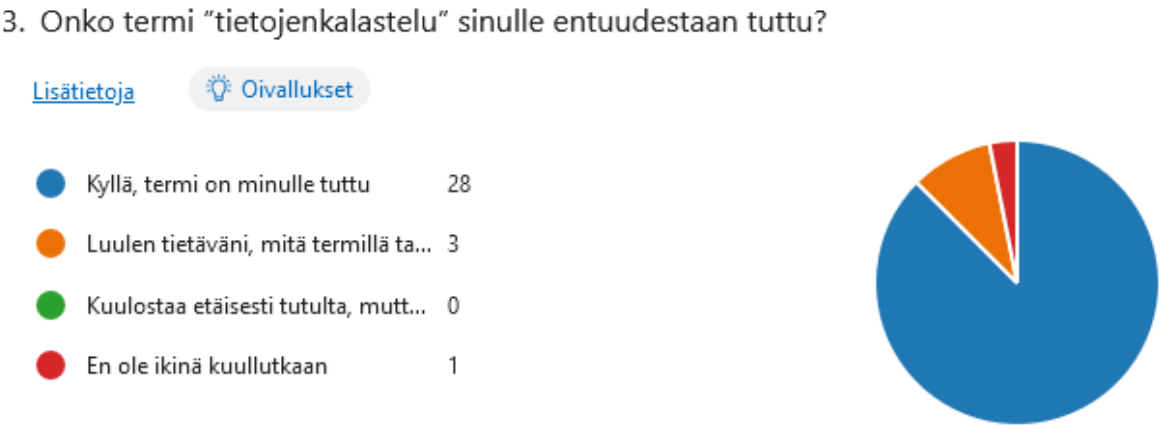
5.2 Kysymysten ja vastausten läpikäynti

Tutkimuskyselyn ensimmäisellä kysymyksellä (kuva 2) oli tarkoitus selvittää vastaajan ikä. Tällä haluttiin kartoittaa vastaajien ikähaarukkaa, jotta saataisiin tarkka tieto, minkä ikäiset ihmiset kyselyyn vastasivat. Vastausvaihtoehdot olivat 18-vuotiaasta aina yli 50-vuotiaaseen. Ikähaarukka oli jaettu neljään eri vaihtoehtoon. 59 prosenttia vastaajista oli 30–39-vuotiaita ja edusti suosituinta ikäluokkaa kyselyssä. Hyvänä kakkosena suosituissa vastausikäluokissa oli 18–29-vuotiaat henkilöt 34 prosentilla.

Kuva 2. Ikäjakauma

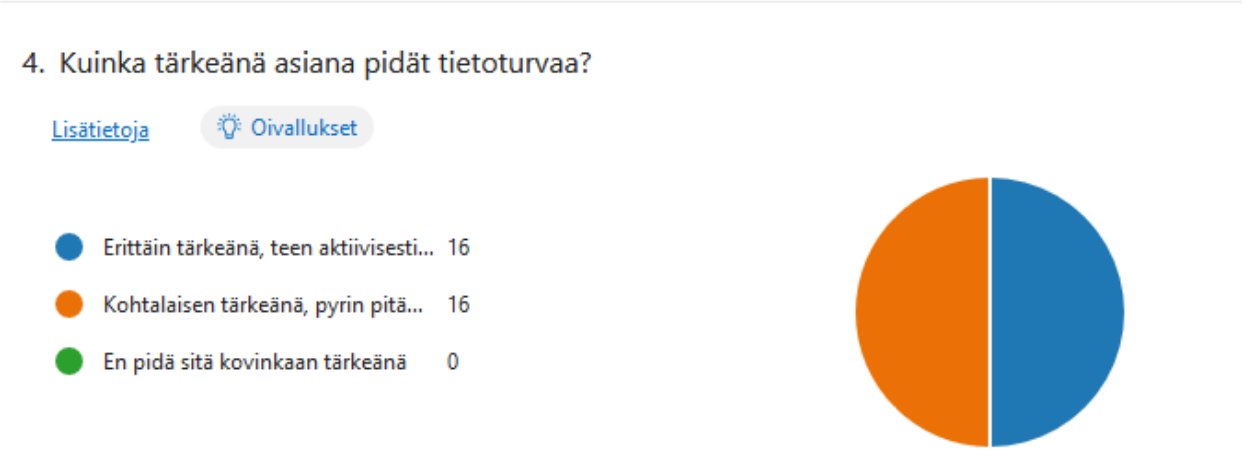
Toinen tutkimuskyselyn kysymys liittyi siihen, millä alalla kyselyyn vastaajat olivat töissä. Tässä kysymyksessä oli vastausvaihtoehtona pelkästään avoin tekstikenttä. 36 prosenttia vastaajista oli IT-alalla töissä ja näin ollen se oli kyselyn suosituin ala. Muita suosittuja aloja oli muun muassa myynti, sosiaali- ja terveysala sekä kiinteistöala. IT-alalla olevien henkilöiden jälkeen vastaukset jakautuivat tasaisesti edellä mainituille muille aloille.

Kyselyn kolmannessa kysymyksessä (kuva 3) kysyttiin termin ”tietojenkalastelu” tuntemusta. Tällä kysymyksellä haluttiin selvittää henkilöiden tietämystä tietojenkalastelusta termin tasolla. Ei tullut yllätyksenä, että melkein kaikki vastaajat olivat tietoisia kyseisestä termistä. Ainoastaan neljälle henkilölle termi ei ollut entuudestaan tuttu ja selkeä. Hyvä merkki on, että niin moni vastaaja oli tietoisia tietojenkalastelusta sanana.



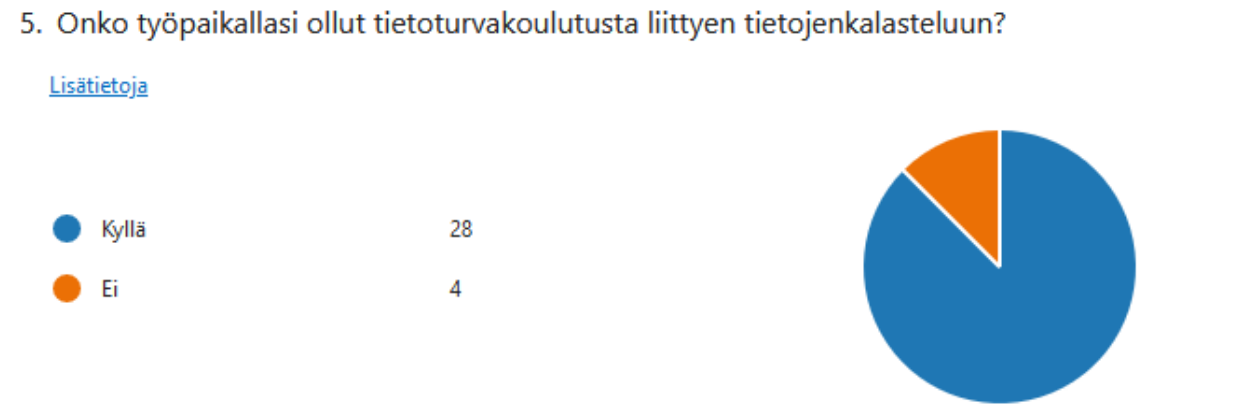
Kuva 3. Tietojenkalastelu-termin tuntemus

Seuraava, eli neljäs kysymys (kuva 4), liittyi siihen, kuinka tärkeänä vastaajat pitivät tietoturvaa. Tämä kysymys on mielestäni tärkeä, koska henkilökohtainen käyttäytyminen yleensä liittyy vahvasti myös käyttäytymiseen töissä. Oli hienoa huomata, että kaikki kyselyyn vastanneet henkilöt pitivät tietoturvaa itselleen erittäin tärkeänä tai kohtalaisen tärkeänä asiana.



Kuva 4. Tietoturvan tärkeys

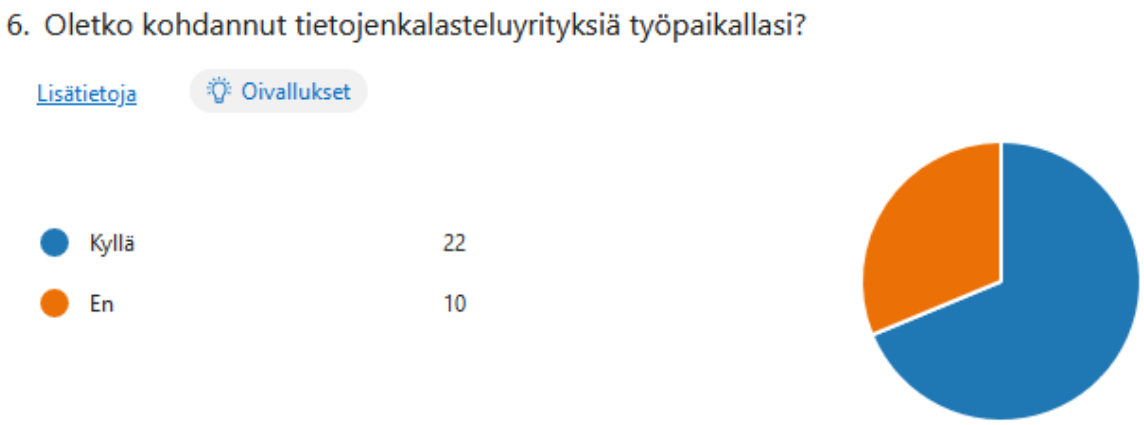
Viides kysymys kyselyssä (kuva 5) liittyi siihen, onko vastaajilla ollut tietoturvakoulutusta tietojenkalastelusta työpaikallaan. Vastanneista 88 prosenttia sanoi, että heillä on ollut tietoturvakoulutusta aiheesta. Mielestäni prosentti on todella suuri ja kertoo hyvää siitä, että yritykset panostavat entistä enemmän tietoturvakoulutukseen. Tällä on suuri merkitys, kun halutaan torjua mahdollisia tietojenkalasteluyrityksiä, sillä tietämys on yleensä paras puolustus.



Kuva 5. Tietojenkalasteluun liittyvät tietoturvakoulutukset

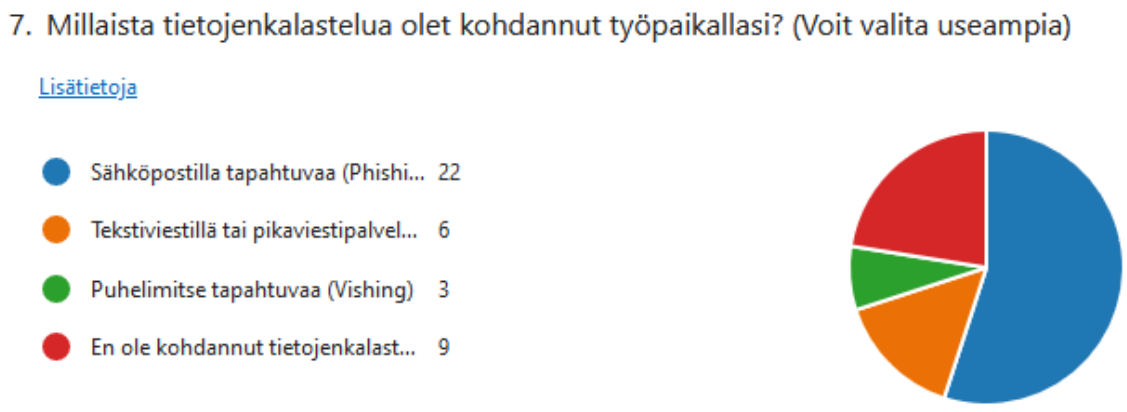
Kuudes kysymys (kuva 6) liittyi tietojenkalasteluyrityksiin vastaajien työpaikoilla. Kysymyksellä haettiin siis henkilöiden omakohtaisia kokemuksia tietojenkalasteluyrityksistä. Yllättävää itselleni oli

se, että tietojenkalastelua oli kohdannut työpaikallaan 69 prosenttia vastaajista. Luku on mielestäni todella suuri, vaikka samalla tiedän, että tietojenkalastelua tapahtuu paljon.



Kuva 6. Tietojenkalasteluyritykset työpaikalla

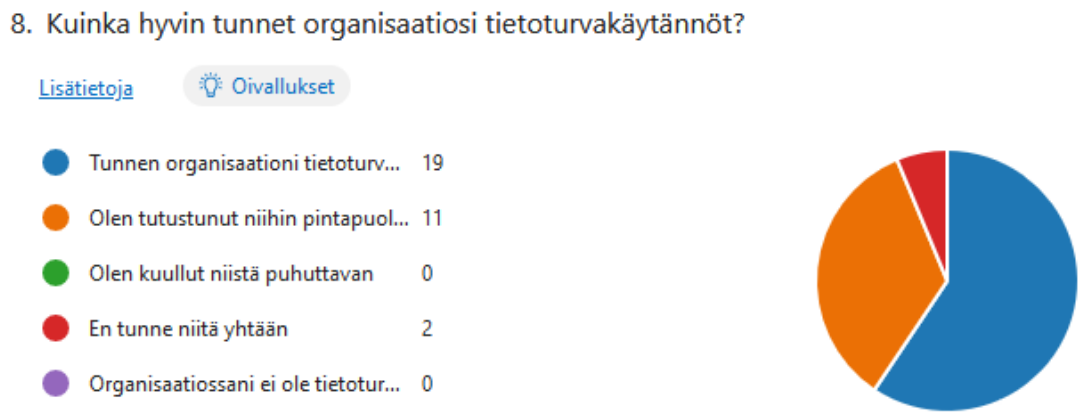
Seitsemäs kysymys (kuva 7) oli jatkoa edelliselle kysymyksellä ja sillä haluttiin selvittää, että millaista tietojenkalastelua henkilöt olivat mahdollisesti kokeneet työpaikoillaan. Vastausvaihtoehtoina oli sähköpostilla, tekstiviestillä ja puhelulla tapahtuvat tietojenkalasteluyritykset sekä vaihtoehto, että ei ole kohdannut tietojenkalastelua ollenkaan. Tässä kysymyksessä sai valita useampia vastausvaihtoehtoja, jos halusi. 69 prosenttia vastanneista oli kohdannut sähköpostilla tulleita tietojenkalasteluyrityksiä, tekstiviestillä tai pikaviestipalvelun kautta tulleita yrityksiä koki 19 prosenttia vastanneista. Puhelimitse tapahtuvia tietojenkalasteluyrityksiä oli kokenut 9 prosenttia vastanneista.



Kuva 7. Erilaiset tietojenkalasteluyritykset työpaikalla

Kahdeksas kysymys (kuva 8) liittyi siihen, kuinka hyvin vastaajat tunsivat organisaationsa tietoturvakäytännöt. Valitsin kysymyksen, sillä halusin tietää, onko vastaajilla tiedossa organisaation tietoturvakäytännöt. Yleinen oletus oli se, että jos tiedetään yrityksen tietoturvakäytännöt, niin silloin

myös ollaan tietoisia tietojenkalastelun vaikutuksista organisaatioon. Tässä kysymyksessä vastausvaihtoehtoina oli viisi eri vaihtoehtoa: ”tunnen organisaation tietoturvakäytännöt”, ”olen tutustunut niihin pintapuoleisesti”, ”olen kuullut niistä puhuttavan”, ”en tunne niitä yhtään” ja ”organisaatiossani ei ole tietoturvakäytäntöjä”. 59 prosenttia vastanneista tunsi organisaationsa tietoturvakäytännöt, 34 prosenttia oli tutustunut niihin pintapuoleisesti ja kuusi prosenttia ei tuntenut niitä yhtään. Vastauksista on nähtävissä, että suurin osa vastanneista on ainakin jollain tasolla tietoisia organisaationsa tietoturvakäytännöistä.

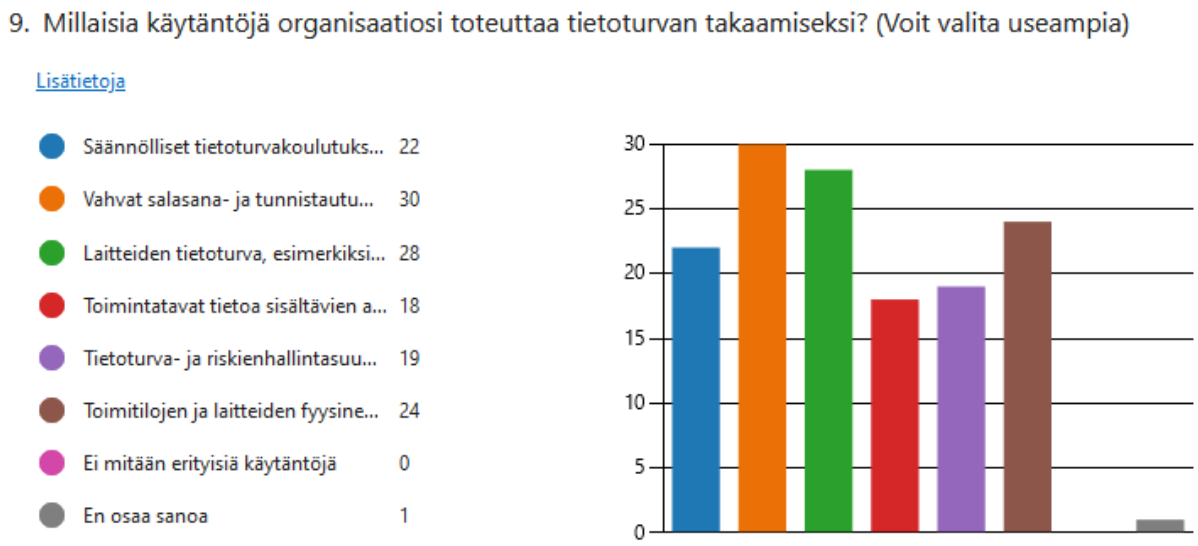


Kuva 8. Organisaation tietoturvakäytäntöjen tunteminen

Yhdeksäs kysymys (kuva 9) liittyi vastaajan organisaation käytäntöihin toteuttaa tietoturvaa. Tässä kysymyksessä sai valita useampia vastausvaihtoehtoja. Kysymyksellä oli tarkoitus kartoittaa organisaation kykyä ennaltaehkäistä tietojenkalastelua, mutta sillä saatiin myös tietoa siitä, millaisia yleisiä tietoturvaan liittyviä käytäntöjä on käytössä. Vastausvaihtoehtoja oli tässä kysymyksessä kahdeksan ja tietojenkalasteluun liittyi seuraavat vastausvaihtoehdot: ”säännölliset tietoturvakoulutukset henkilöstölle”, ”vahvat salasana- ja tunnistautumisvaatimukset”, ja ”laitteiden tietoturva, esimerkiksi puhelimien ja tietokoneiden päivitykset”.

Vastanneista jopa 94 prosenttia sanoi, että heillä on organisaatiossaan käytössä vahvat salasana- ja tunnistautumisvaatimukset. Näillä metodeilla voidaan lähtökohtaisesti suojautua hyvin tietojenkalasteluyrityksiä vastaan. 69 prosentilla on organisaatiossaan säännöllisiä tietoturvakoulutuksia henkilöstölle. Myös laitteiden tietoturvasta oli huolehdittu organisaatiotasolla hyvin, sillä 88 prosenttia vastaajista sanoi, että organisaatiolla on niihin liittyviä käytäntöjä. Laitteiden tietoturvasta huolehtiminen on myös erittäin tärkeää, kun halutaan minimoida tietojenkalasteluyritysten vaikutukset.

Muista vastauksista voidaan nostaa esiin toimitilojen ja laitteiden fyysinen suojaus, johon vastaajien organisaatioissa oli käytännöt 75 prosentilla. Yksikään vastaaja ei valinnut vastausvaihtoehtoa, että organisaatiossa ei olisi mitään erityisiä käytäntöjä tietoturvaan liittyen.

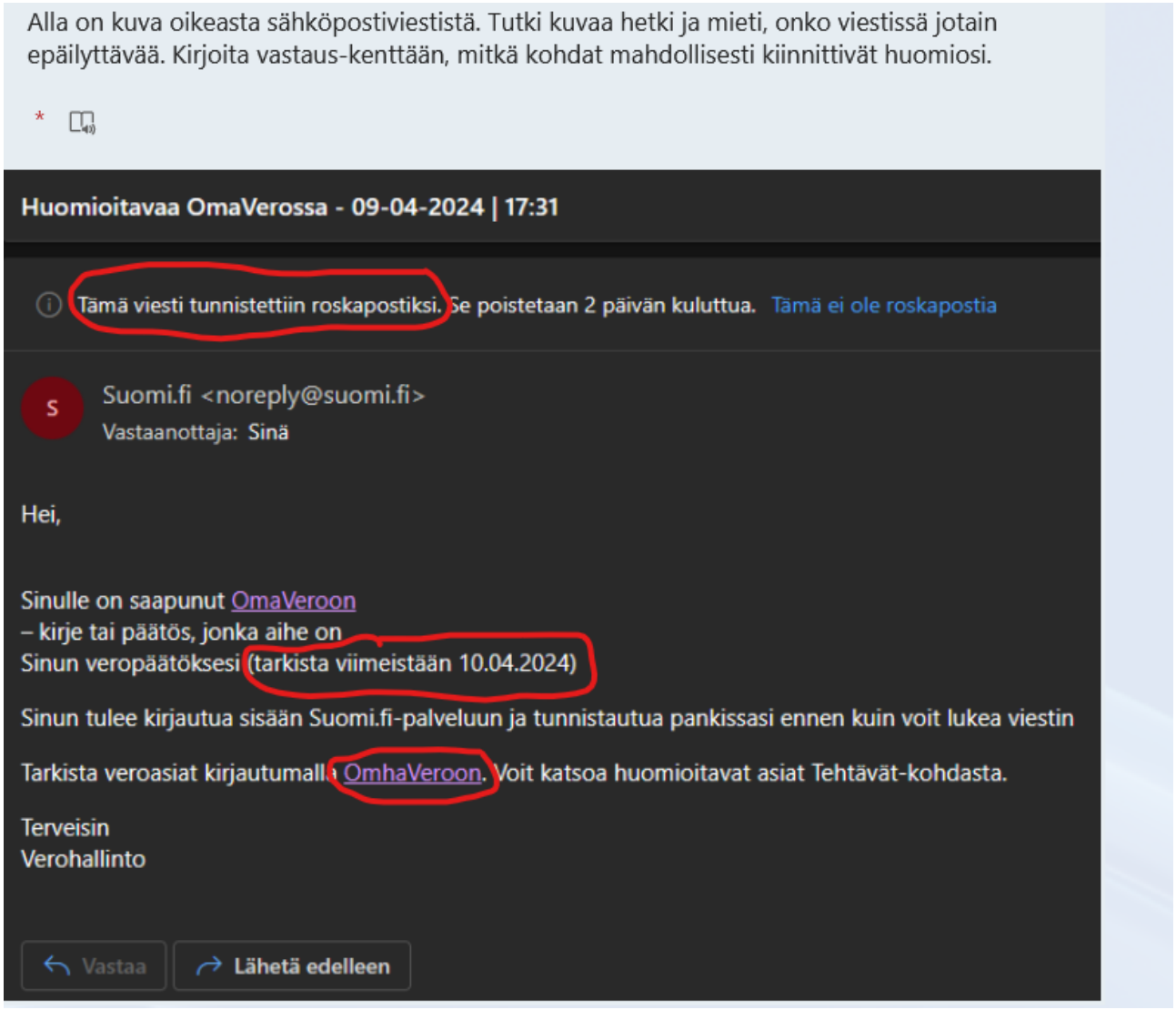


Kuva 9. Organisaation käytännöt tietoturvan takaamiseksi

Kyselyn viimeinen, eli kymmenes kysymys (kuva 10), sisälsi kuvan oikeasta tietojenkalasteluviestistä ja sillä haluttiin kartoittaa, huomaako vastaaja epäjohdonmukaisuuksia viestistä. Vastaajan piti siis etsiä merkkejä, jotka viittaisivat tietojenkalasteluviestiin. Tämä kysymys sisälsi vapaan tekstikentän, mihin vastaajan piti kirjoittaa havaintonsa. En halunnut suoraan mainita, että kyseessä on kalasteluviesti, vaan jätin sen vastaajan pohdittavaksi. Sähköpostiviestissä oli selkeitä merkkejä, joiden avulla voidaan tunnistaa geneerinen sähköpostihuijausviesti. Tällaisia piirteitä oli muun muassa selkeä kirjoitusvirhe, tekstiin upotettu hyperlinkki, merkintä tunnistetusta roskapostista ja kiireen tunteen luominen vastaanottajalle.

Vastauksia läpikäydessä ensimmäinen huomaamani asia oli, että kaikki vastaajat olivat löytäneet vähintään yhden epäjohdonmukaisuuden viestistä. Yleisin huomio liittyi kirjoitusvirheeseen tekstissä olevassa upotetussa linkissä (kuva 10), jonka huomasi 82 prosenttia vastanneista. Toiseksi yleisin huomio oli, että sähköpostiviesti oli tunnistettu automaattisesti roskapostiksi. Tämän huomasi vastanneista 47 prosenttia. Seuraavaksi eniten kommentteja tuli kiireen tunteen luontiin, jonka mainitsi vastauksissaan 44 prosenttia vastaajista. Kirjoitusvirheistä ja huonosta suomen kielestä mainitsi vastauksissaan 34 prosenttia vastaajista. Muutamat vastaajat kommentoivat sähköpostin yleistä epäjohdonmukaisuutta esimerkiksi, että Suomi.fi ja Omavero menivät viestissä sekaisin.

Tästä kysymyksestä voi vetää selkeän johtopäätöksen, että vastaajat olivat hyvin tietoisia, millaisista elementeistä tietojenkalasteluviesti koostuu. Mikään epäjohdonmukaisuus ei jäänyt vastaajilta huomaamatta vaan kaikki virheet oli löydetty ainakin kertaalleen.



Kuva 10. Tietojenkalasteluviesti ja epäjohdonmukaisuudet ympyröitynä punaisella

Kyselyn viimeinen kohta oli vapaaehtoinen palautteen anto liittyen kyselyyn. Tämä kohta oli vapaaehtoinen ja vastaajista palautetta antoi kahdeksan henkilöä. Palautteiden sävy oli todella positiivinen. Yksi vastaajista olisi toivonut 7. kysymykseen avoimen vastausvaihtoehdon, sillä hänen organisaatiossaan tulee säännöllisesti myös Facebookin kautta kalasteluyrityksiä. Avoin vastausvaihtoehto oli hyvä idea, jonka olisin voinut sisällyttää kysymysvaihtoehtoihin.

5.3 Kyselytulosten analysointi

Asetin opinnäytetyön alussa tutkimuskysymykset, joihin halusin saada vastauksia kyselytutkimuksen avulla. Ensimmäinen tutkimuskysymys liittyi henkilöiden tuntemukseen tietojenkalastelusta. Kyselyn avulla selvitin ensin, onko tietojenkalastelu terminä entuudestaan tuttu. Ainoastaan yksi vastaaja ei tiennyt, mitä termillä tarkoitetaan, mutta muille vastaajille termi oli tuttu entuudestaan. Tietojenkalastelu vaikutti olevan siis hyvin tiedossa melkein kaikilla vastanneilla. Tähän yksi syy

saattaa olla kyselyyn vastanneiden henkilöiden ikä, sillä yleensä voidaan olettaa, että nuoremmat ihmiset ovat tietoisempia tietokoneiden ja puhelimien tietoturvasta kuin vanhemmat ihmiset. Ainoastaan kaksi vastaajaa kaikista vastaajista oli iältään yli 40-vuotiaita. Uskon, että jos useampi vastaaja olisi ollut vanhempaa ikäluokkaa niin tietämys tietojenkalastelusta olisi ollut erilainen. Kyselyn muiden kysymysten tulosten perusteella voidaan myös tehdä johtopäätös, että tietojenkalastelu oli tuttu aihe vastaajille, sillä vastauksista kävi selkeästi ilmi tietoisuus asiasta.

Toinen tutkimuskysymys liittyi siihen, millaista tietojenkalastelua työelämässä olevat henkilöt ovat kokeneet organisaatioissaan. Kyselyyn peilaten voidaan todeta, että vastaajat olivat kokeneet kaikkia tietojenkalasteluyrityksiä, joita tässä opinnäytetyössä käsittelin. Ylivoimaisesti kuitenkin yleisin tietojenkalastelutapa oli sähköpostilla tapahtuva toiminta. 55 prosenttia vastaajista oli saanut tietojenkalasteluviestin sähköpostin välityksellä työpaikallaan. 19 prosenttia vastaajista oli saanut tekstiviestillä tai pikaviestipalvelun kautta tulleen kalasteluviestin. Puhelimitse tapahtuvaa tietojenkalastelua oli kokenut kolme vastaajaa, eli yhdeksän prosenttia vastaajista. 28 prosenttia vastaajista ei ollut kokenut tietojenkalasteluyrityksiä organisaatiossaan.

Kyselyn perusteella voidaan todeta, että suosituin tietojenkalastelutapa oli sähköpostilla tapahtuva toiminta. Tämä johtuu varmasti siitä, että suurin osa tietojenkalastelusta tapahtuu nykyään sähköpostien välityksellä. Sähköpostilla tapahtuva tietojenkalastelu on myös hyökkääjille edullinen tapa toteuttaa tietojenkalastelua, sillä viestien lähetys ei maksa mitään. Sähköpostilla voidaan myös lähettää suuri määrä huijausviestejä nopeasti ja tehokkaasti, joten siitäkin syystä se on erityisen suosittu menetelmä rikollisten parissa.

Kolmas tutkimuskysymys liittyi siihen, millä alalla ihmiset ovat kohdanneet eniten tietojenkalasteluyrityksiä. Tähän kysymykseen vastaaminen vaati tarkempaa analysointia kyselyllä saaduista vastauksista. 36 prosenttia vastanneista oli töissä IT-alalla, muuten vastaajien työpaikat jakaantuivat tasaisesti eri aloille. Kyselystä saaduilla vastauksilla voidaan vetää pieni johtopäätös siitä, että IT-alalla työskentelevät saavat muita aloja enemmän tietojenkalasteluviestejä. Tämä johtuu varmasti siitä, että he työskentelevät joka päivä tietokoneilla ja ovat siksi otollisemmassa asemassa verkkorikollisille. Tosin tässä kyselyssä vastaajia ei ollut tarpeeksi, jotta asiasta voisi vetää isompia johtopäätöksiä.

Neljäs ja viimeinen tutkimuskysymys liittyi organisaatioiden tapoihin ennaltaehkäistä tietojenkalasteluyrityksiä. Kyselyn yhdeksännellä kysymyksellä hain vastauksia tähän tutkimuskysymykseen. Tutkitusti tehokkaimpia tapoja suojautua tietojenkalastelulta on säännölliset tietoturvakoulutukset, joissa opetetaan, mitä tietojenkalastelu on ja miten niitä voi tunnistaa. Vastanneista 69 prosenttia sanoi, että heidän organisaationsa järjestää säännöllisiä tietoturvakoulutuksia. Itse yllätyin suuresti isosta prosentuaalisesta määrästä, joiden organisaatio järjestää tietoturvakoulutuksia. Tämä on

merkki siitä, että tietojenkalastelu otetaan nykyään vakavasti ja tiedostetaan riskit, jotka johtuvat tietojenkalastelusta.

Kyselyn perusteella organisaatioissa on käytössä myös hyviä teknisiä menetelmiä tietojenkalastelua vastaan. 94 prosenttia kyselyyn vastanneista sanoi, että heillä on käytössään organisaatiossa vahvat salasana- ja tunnistautumisvaatimukset. 88 prosenttia vastaajista kertoi, että heidän laitteidensa tietoturvasta pidetään huolta. Molemmat edellä mainitut prosenttiluvut ovat todella suuria ja se on mielestäni jälleen yksi merkki siitä, että organisaatiot tiedostavat tietojenkalastelun uhat. Vahvoilla salasanoilla ja monivaiheisella tunnistautumisella päästään jo pitkälle, kun halutaan suojautua tietojenkalasteluyrityksiltä.

Kaiken kaikkiaan kyselystä saatujen vastausten perusteella voidaan todeta, että organisaatiot käyttävät monipuolisesti erilaisia keinoja suojautua tietojenkalastelulta. 75 prosenttia vastaajista sanoi, että heidän organisaatioillaan on käytössä käytännöt toimitilojen ja laitteiden fyysiseen suojaamiseen. Tietoturva- ja riskienhallintasuunnitelmat olivat käytössä 59 prosentilla vastaajista ja heidän organisaatioissansa. 56 prosenttia vastaajista kertoi, että heidän organisaatiossaan on käytössä toimintatavat tietoa sisältävien aineistojen siirtoon ja käsittelyyn.

Tutkimuskyselystä saadut vastaukset helpottivat tutkimuskysymyksiin vastaamista todella paljon ja niiden perusteella sain tehtyä loogiset ja hyvät päätelmät esitettyihin tutkimuskysymyksiin. Tietojenkalastelu on hyvin yleistä Suomessa toimivissa yrityksissä ja myös työntekijät ovat hyvin perillä tästä. Organisaatiot kohtaavat kaiken tyylistä tietojenkalastelua, mutta eniten törmätään sähköpostilla tulleisiin huijausyrityksiin. IT-ala näyttää olevan kaikista yleisin ala, johon kohdistuu tietojenkalastelua, ainakin tämän tutkimuksen perusteella. Yrityksillä on käytössään paljon erilaisia keinoja, joilla he suojautuvat tietojenkalastelua vastaan, niin kuin aikaisemmin jo mainitsin. Se on merkki siitä, että uhat tiedostetaan ja ennaltaehkäiseviä keinoja toteutetaan.

6 Pohdinta

6.1 Johtopäätökset

Opinnäytetyötä aloittaessani minua mietitytti, millainen yleinen tietämys ihmisillä on tietojenkalastelusta ja tapahtuuko sitä paljon eri organisaatioissa. Minulla oli omakohtaista kokemusta oman työni kautta tietojenkalastelusta, mutta en tiennyt, missä määrin sitä tapahtuu muilla aloilla. Tämä tutkimuskysely vastasi hyvin minua mietityttäneisiin tutkimuskysymyksiin, joita mietin ennen kuin aloin tekemään opinnäytetyötä. Kaikilla aloilla, joissa ollaan tekemisissä tietokoneiden ja puhelimien kanssa esiintyy tietojenkalastelua, mutta tietojenkalastelun muodot saattavat olla erilaiset.

Tutkimuskyselyn perusteella voidaan sanoa, että organisaatiot ovat hyvin tietoisia tietojenkalastelusta ja tietoturvasta yleisesti. Olin positiivisesti yllättynyt, että tietojenkalastelu oli tuttua melkein kaikille kyselyyn vastanneille. Tosin olen itse sitä mieltä, että tietoturvaan pitääkin keskittyä entistä enemmän nyt ja tulevaisuudessa. Yritykset kansainvälistyvät ja ovat koko ajan enemmän riippuvaisia tietokoneista ja järjestelmistä. Loppujen lopuksi tietoturvan tehtävä on suojata organisaation eri toimintoja ja mahdollistaa datan turvallinen käsittely niin, että data ei joudu vääriin käsiin. Tässä olemme mielestäni menossa oikeaan suuntaan ja juuri nyt näyttää siltä, että tietoturva otetaan yrityksissä tosissaan.

6.2 Pohdintaa omasta oppimisesta

Tämä opinnäytetyö on ollut mahtava kokemus itselleni, koska olen päässyt syventämään osaamistani ja tutkimaan pintaa syvemmälle. Opinnäytetyön tekeminen oli pitkä prosessi ja alkuun se tuntui ylitsepääsemättömältä esteeltä, mutta kun aloin tutkimaan aihetta enemmän, niin asiat selkeytyivät mielessäni. Niin kuin olen jo aiemmin maininnut, työskentelen tietoturva-alalla ja olen tietojenkalastelun kanssa tekemisissä päivittäin. Siitä huolimatta opinnäytetyötä tehdessäni vastaan on tullut paljon uusia ja mielenkiintoisia asioita, joista en ole aikaisemmin ollut tietoinen. En ole myöskään aiemmin pitänyt itseäni kovana kirjoittajana, mutta opinnäytetyön myötä olen oppinut, että pystyn tuottamaan paljonkin tekstiä lyhyessä ajassa.

Olen kerran aikaisemmin toteuttanut samantyylisen kyselyn kuin tässä opinnäytetyössä, mutta se ei liittynyt tietoturvaan mitenkään. Koin kyselyn tekemisen opettavaiseksi ja hauskaksi kokemukseksi, josta on varmasti hyötyä myös tulevaisuudessa. Lisäksi huomasin, että kysymysten

asettelu oli ennakoitua vaikeampaa, kuin olin kuvitellut. Kysymysten mietintään meni yllättävän paljon aikaa, mutta se kannatti, sillä olin tyytyväinen kysymyksiin, jotka kyselyyn lopulta valitsin.

Tietoperustan kirjoittaminen oli myös ennakoitua työläämpää, koska lähteitä ja erilaisia nettisivuja oli paljon aiheesta kuin aiheesta. Lähteiden runsaudesta tuli positiivinen ongelma – mitä lähteitä haluan käyttää ja ovatko ne luotettavia? Sain kuitenkin parsittua kasaan luotettavat lähteet, joita halusin käyttää ja huomasin, että niistä on paljon hyötyä myös nykyisessä työssäni nyt ja tulevaisuudessa.

Lähteet

America’s Cyber Defense Agency s.a. Teach Employees to Avoid Phishing. Luettavissa: https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing. Luettu: 26.3.2023

AWS s.a. What is Multi-Factor Authentication (MFA)? Luettavissa: https://aws.amazon.com/what-is/mfa/. Luettu: 26.3.2023

Cash J. Dzuba E. 16.8.2023. Introducing Cloudflare's 2023 phishing threats report. Cloudflare blogi. Luettavissa: https://blog.cloudflare.com/2023-phishing-report. Luettu: 27.3.2023

Check Point s.a. EDR vs Antivirus. Luettavissa: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/endpoint-detection-and-response-edr-benefits/edr-vs-antivirus/. Luettu: 29.3.2023

Colorado Department of Education 2020. Social Engineering Education. Luettavissa: https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation. Luettu: 26.3.2023

Fortra 2017. 91% of Cyber Attacks Start with a Phishing Email: Here's How to Protect against Phishing. Luettavissa: https://www.digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing. Luettu: 26.3.2023

F-Secure s.a. Mitä on tietojenkalastelu? Luettavissa: https://www.f-secure.com/fi/articles/what-is-phishing. Luettu: 24.3.2023

Graphus 2023. The History of Phishing. Luettavissa: https://www.graphus.ai/blog/history-of-phishing/. Luettu: 23.3.2023

Grimes R. 22.1.2023. Motivations of Phishing Criminals. KnowBe4 blogi. Luettavissa: https://blog.knowbe4.com/motivations-of-phishing-criminals. Luettu: 28.3.2023

IBM s.a. What is phishing? Luettavissa: https://www.ibm.com/topics/phishing. Luettu: 26.3.2023

Imperva s.a. Phishing attacks. Luettavissa: https://www.imperva.com/learn/application-security/phishing-attack-scam/. Luettu: 25.3.2023

Kaspersky s.a. a. What is Smishing and How to Defend Against it. Luettavissa: https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it. Luettu: 29.3.2023

Kaspersky s.a. b. What is spear phishing? Definition and risks. Luettavissa: https://usa.kaspersky.com/resource-center/definitions/spear-phishing. Luettu: 28.3.2023

Kyberturvallisuuskeskus 2020. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon. Luettu: 28.3.2023

Kyberturvallisuuskeskus s.a. Ohjeet ja oppaat yksityishenkilöille. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille. Luettu: 28.3.2023

Malwarebytes s.a. What is social engineering? Luettavissa: https://www.malwarebytes.com/social-engineering. Luettu: 27.3.2023

Phishing.org s.a. What is phishing? Luettavissa: https://www.phishing.org/what-is-phishing. Luettu: 22.3.2023

Robert B. Cialdini PH.D. 2006. Influence: The Psychology of Persuasion, Revised Edition. Harper Business. New York. Luettu: 30.3.2024

Simister A. 23.4.2024. 10 Ways to Prevent Phishing Attacks. Lepide blogi. Luettavissa: https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/. Luettu: 24.4.2024

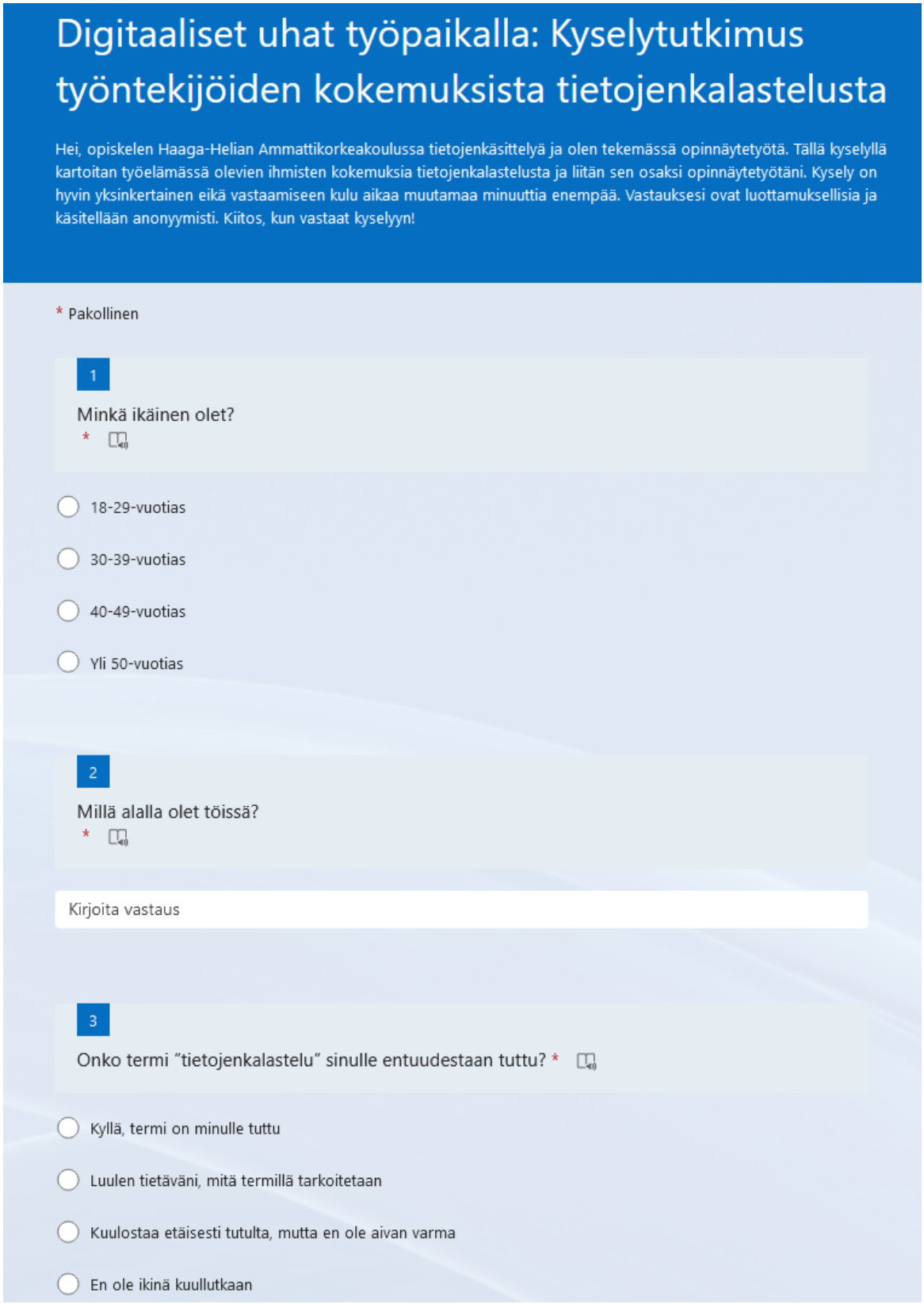
Trend Micro 2019. Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company. Luettavissa: https://www.trendmicro.com/vinfo/mx/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company. Luettu: 27.3.2023

World of Work Project 2019. Cialdini’s 6 Principles of Persuasion: A Simple Summary. Luettavissa: https://worldofwork.io/2019/07/cialdinis-6-principles-of-persuasion/. Luettu: 29.3.2023

YLE 2020. Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa. Luettavissa: https://yle.fi/a/3-11612399. Luettu: 23.3.2023

Liitteet

Liite 1. Kyselytutkimus



Digitaaliset uhat työpaikalla: Kyselytutkimus työntekijöiden kokemuksista tietojenkalastelusta

Hei, opiskelen Haaga-Helian Ammattikorkeakoulussa tietojenkäsittelyä ja olen tekemässä opinnäytetyötä. Tällä kyselyllä kartoitan työelämässä olevien ihmisten kokemuksia tietojenkalastelusta ja liitän sen osaksi opinnäytetyötäni. Kysely on hyvin yksinkertainen eikä vastaamiseen kulu aikaa muutamaa minuuttia enempää. Vastauksesi ovat luottamuksellisia ja käsitellään anonyymisti. Kiitos, kun vastaat kyselyyn!

* Pakollinen

1

Minkä ikäinen olet? *

- 18-29-vuotias
- 30-39-vuotias
- 40-49-vuotias
- Yli 50-vuotias

2

Millä alalla olet töissä? *

Kirjoita vastaus

3

Onko termi "tietojenkalastelu" sinulle entuudestaan tuttu? *

- Kyllä, termi on minulle tuttu
- Luulen tietäväni, mitä termillä tarkoitetaan
- Kuulostaa etäisesti tutulta, mutta en ole aivan varma
- En ole ikinä kuullutkaan

4

Kuinka tärkeänä asiana pidät tietoturvaa?
*

- ○ Erittäin tärkeänä, teen aktiivisesti toimenpiteitä saavuttaakseni maksimaalisen tietoturvan
- ○ Kohtalaisen tärkeänä, pyrin pitämään puhelimen ja tietokoneen päivitykset ajan tasalla
- ○ En pidä sitä kovinkaan tärkeänä

5

Onko työpaikallasi ollut tietoturvakoulutusta liittyen tietojenkalasteluun?
*

- ○ Kyllä
- ○ Ei

6

Oletko kohdannut tietojenkalasteluyrityksiä työpaikallasi?
*

- ○ Kyllä
- ○ En

7

Millaista tietojenkalastelua olet kohdannut työpaikallasi? (Voit valita useampia)
*

- ☐ Sähköpostilla tapahtuvaa (Phishing)
- ☐ Tekstiviestillä tai pikaviestipalvelun (esim. WhatsApp) kautta tapahtuvaa (Smishing)
- ☐ Puhelimitse tapahtuvaa (Vishing)
- ☐ En ole kohdannut tietojenkalastelua työpaikallani

8

Kuinka hyvin tunnet organisaatiosi tietoturvakäytännöt?
*

- ○ Tunnen organisaationi tietoturvakäytännöt
- ○ Olen tutustunut niihin pintapuoleisesti
- ○ Olen kuullut niistä puhuttavan
- ○ En tunne niitä yhtään
- ○ Organisaatiossani ei ole tietoturvakäytäntöjä

9

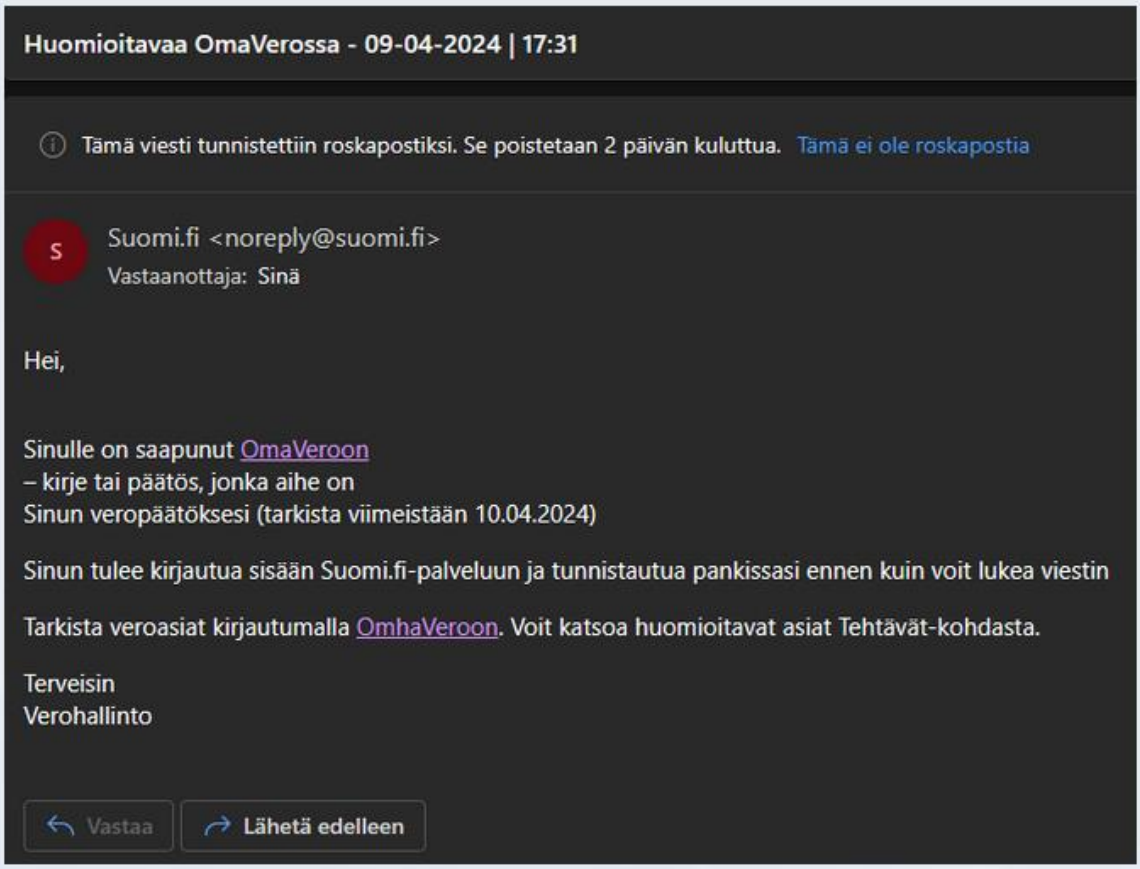
Millaisia käytäntöjä organisaatiosi toteuttaa tietoturvan takaamiseksi? (Voit valita useampia)
*

- ☐ Säännölliset tietoturvakoulutukset henkilöstölle
- ☐ Vahvat salasana- ja tunnistautumisvaatimukset
- ☐ Laitteiden tietoturva, esimerkiksi tietokoneiden ja puhelimien ohjelmistopäivitykset
- ☐ Toimintatavat tietoa sisältävien aineistojen siirtoon ja käsittelyyn
- ☐ Tietoturva- ja riskienhallintasuunnitelma
- ☐ Toimitilojen ja laitteiden fyysinen suojaaminen
- ☐ Ei mitään erityisiä käytäntöjä
- ☐ En osaa sanoa

10

Alla on kuva oikeasta sähköpostiviestistä. Tutki kuvaa hetki ja mieti, onko viestissä jotain epäilyttävää. Kirjoita vastaus-kenttään, mitkä kohdat mahdollisesti kiinnittivät huomiosi.

*



Kirjoita vastaus

11

Kiitos kyselyyn vastaamisesta! Alle voit vielä kirjoittaa vapaaehtoisen palautteen kyselystä.

Kirjoita vastaus

Lähetä