Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Jaakko Kemppainen

Ohje tietojenkalastelua vastaan pienissä ja keskisuurissa yrityk-sissä

Toiminnallinen opinnäytetyö

Metropolia Ammattikorkeakoulu

Liiketalouden tutkinto-ohjelma

Opinnäytetyö

Huhtikuu 2023

Tekijä(t) Otsikko	Jaakko Kemppainen Ohje tietojenkalastelua vastaan pienissä ja keskisuurissa yrityksissä
Sivumäärä Aika	32 sivua + 1 liite Huhtikuu 2023
Tutkinto	Tradenomi
Tutkinto-ohjelma	Liiketalous
Suuntautumisvaihtoehto	Esimiestyö ja työyhteisön kehittäminen
Ohjaaja	Lehtori Tiina Mikkola

Tietojenkalastelu on toimintaa, missä tietojenkalastelija vakuuttaa uhrinsa luovuttamaan salassa pidettävää tai muuten arvokasta tietoa käyttämällä psykologisia keinoja. Opinnäytetyön toiminnallisena tuotoksena tehtiin ohje tietojenkalastelua vastaan, ja ohjeen kohderyhmäksi valikoituivat pienten ja keskisuurten yritysten työntekijät Suomessa. Opinnäytetyön tuotoksena syntyneen ohjeen tarkoitus on valistaa tietojenkalastelusta, ja tarjota suojautumis- ja ennaltaehkäisykeinoja sitä vastaan henkilön koulutustasosta riippumatta.

Työ toteutettiin ilman toimeksiantajaa tehtynä avoimien Internet- ja kirjallisuuslähteiden kirjallisuuskatsauksena, jonka lopputuloksena luotiin ohje tietojenkalastelua vastaan. Työtä käsiteltiin psykologisesta näkökulmasta. Työssäni käytetty aineisto oli pääosin kansainvälisten tutkijoiden kuten Hadnagyn, Stajanon ja Brownin keräämää, ja näitä aineistoja tuettiin kotimaisten viranomaisten ja tutkijoiden aineistoilla ja havainnoilla.

Työssä käytetty aineisto osoitti, että yritykset ja niiden henkilöstöt ovat haavoittuvaisia tietojenkalastelun kautta tehdyille tietomurroille, koska yritysten nykyiset koulutukset ja koulutusmateriaalit aiheesta eivät ota tarpeeksi huomioon hyökkääjien käyttämiä kognitiivisia harhoja sekä psykologisia keinoja. Koulutukset kärsivät usein monimutkaisesta kielestä, teknisten termien paljoudesta sekä käyttäjäystävällisyyden puutteesta. Aineisto osoitti myös sen, että yritysten toimintaohjeet eivät ota tarpeeksi huomioon psykologisia keinoja ja manipulointia, joita hyökkääjät käyttävät säännöllisesti.

Työn toiminnallisena osana tuotettu ohje tarjoaa lyhyet selitteet tietojenkalastelun variaatioille, niissä käytetyille psykologisille keinoille, yleisiä turvallisen verkon käytön periaatteita, sekä toimintaohjeet näitä vastaan. Ohjetta lyhennettiin käytännöllisyyden vuoksi. Ohjeen tehokkuus riippuu käyttäjän valppaudesta ja kyvystä tunnistaa epäilyttävää viestintää, ja ohjetta pitää kehittää vastaamaan monimutkaisempien kalasteluhyökkäysten luomaan uhkaan.

Avainsanat
Tietojenkalastelu, psykologia, manipulointi

Author(s) Title	Jaakko Kemppainen Guide against phishing in small and medium-sized companies
Number of Pages Date	32 pages + 1 appendix April 2023
Degree	Bachelor of Business Administration
Degree Programme	Economics and Business Administration
Specialisation option	Leadership and Organizational Development
Instructor	Tiina Mikkola, Senior Lecturer

Phishing is an activity where the phisher convinces his victim to hand over confidential or otherwise valuable information using psychological means. As an output of the thesis work, an instruction against phishing was made, and the target group of the instruction was selected to be employees of small and medium-sized companies in Finland. The purpose of the guidelines created as a result of the thesis is to educate about phishing, and to offer protection and prevention measures against it, regardless of the person's level of education.

The study was carried out as a literature review of open Internet and literary sources without a client, the end result of which was the creation of an instruction against phishing. The study was handled from a psychological point of view. The material for the study was mainly collected by international researchers such as Hadnagy, Stajano and Brown, and these materials were supported by the materials and observations of domestic authorities and researchers.

The material used in the work showed that companies and their personnel are vulnerable to data breaches carried out through phishing, because the companies' current trainings and training materials on the subject do not sufficiently take into account the cognitive biases and psychological methods used by the attackers. The training often suffers from complicated language, a lot of technical terms and a lack of user-friendliness. The data also showed that the operating instructions of the companies do not sufficiently take into account the psychological methods and manipulation that attackers regularly use.

The instruction produced as the outcome of the study offers short explanations for the variations of phishing, the psychological methods used in them, general principles of safe network use, and action instructions against them. The instructions were shortened for practicality. The effectiveness of the instruction depends on the user's vigilance and ability to recognize suspicious communication, and the instruction must be developed to respond to the threat posed by more complex phishing attacks.

Keywords
Phishing, psychology, manipulation

Sisällys

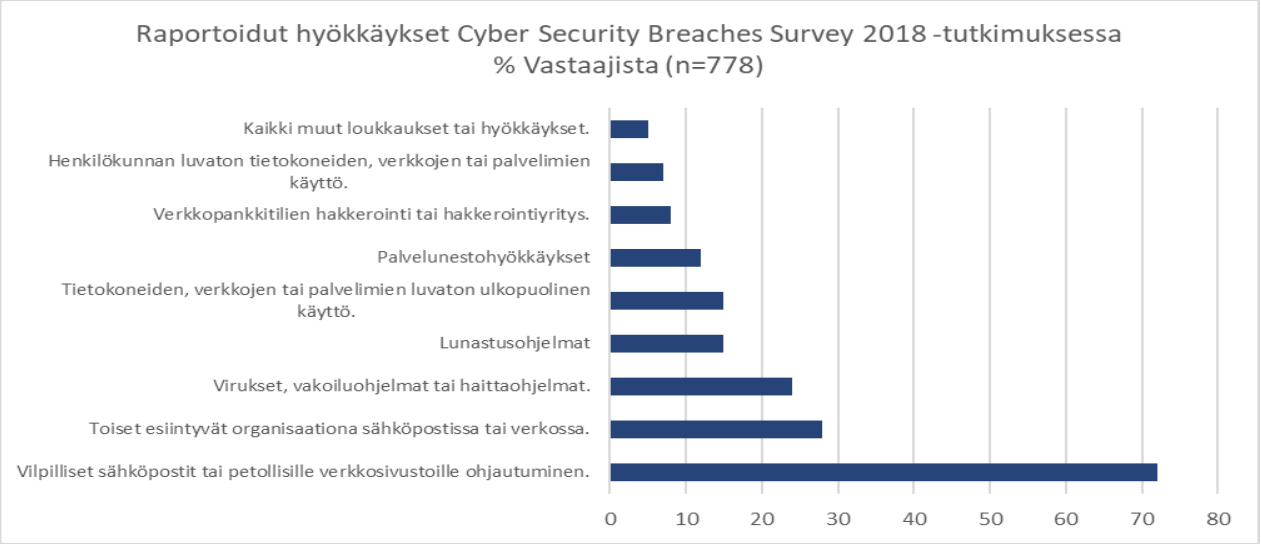
1 Johdanto

1.1 Työn tausta ja lähtökohdat

Lokakuussa 2020 psykoterapiakeskus Vastaamo tiedotti, että yritys on tullut tietomurron kohteeksi (MTV Uutiset 2020). Arviolta tuhansien ihmisten mielenterveyttä sekä muita arkaluontoisia tietoja sisältävät asiakirjat päätyivät rikollisten toiminnan ansiosta Internettiin, mikä näkyi uhrien arjessa kiristyssähköposteina, joissa vaadittiin lunnaita vastineeksi tietojen salaamisesta (MTV Uutiset 2020). Julkisuuteen vuoti myöhemmin tietoja, jotka viittasivat tietomurron olleen yrityksen johdon tiedossa (Kantomaa 2021).

Tietojenkalastelu on tietomurroissa käytetyistä menetelmistä tutkijoiden mukaan yleisin, sillä pelkästään vuonna 2018 sosiaalisen manipuloinnin hyökkäyksistä 93 % hyödynsi tietojenkalastelua (Moinescu & Răcuciu & Glăvan & Antonie & Eftimie 2019, 163–164). Tietojenkalastelu-hyökkäykset hyödyntävät monia metodeja, kuten linkkien manipulointia, linkkien väärentämistä (spoofing), URL-lyhennyspalveluita, IP-osoitteen käyttöä linkin sijasta sekä epämääräisten liitetiedostojen käyttöä (Moinescu ym. 2019, 163). Viranomaiset kuten Europol ja yksityiset toimijat kuten Anti-Phishing Working Group (APWG) ovat huomanneet tietojenkalastelun määrän kasvaneen vuosien 2020 ja 2021 välillä (Anti Phishing Working Group 2021, 6–7).

Tutkijat Furnell ja Dowling käsittelevät artikkelissaan laajasti tietoturvamurtojen, rikollisuuden ja väärinkäytösten mittaamisen nykyisiä ongelmia, mutta työni kannalta on oleellista nähdä, kuinka paljon tietomurrot ovat lisääntyneet viimeisen neljän vuoden aikana. Vuonna 2018 tehdyssä tutkimuksessa selvitettiin, millaisen kyberrikollisuuden kohteeksi vastaajat olivat joutuneet edeltävän vuoden aikana. Kuvion 1 tuloksista näkyy, että harhaanjohtavat sähköpostit ja sivustot olivat selkeästi yleisimmät hyökkäystyypit. Juuri näitä hyökkäystyyppejä käytetään tyypillisesti tietojenkalastelussa. (Furnell & Dowling 2019, 19–20.)



Kuvio 1. Kyberturvallisuusrikkomustutkimuksessa 2018 raportoidut hyökkäykset (Furnell & Dowling 2019, 19).

Tietoturvallisuuden parantaminen ja tietojenkalastelulta suojautuminen vaativat huolellista suunnittelua, sillä nykyisen tiedon valossa tietojenkalastelu tulee entistä enemmän osaksi meidän kaikkien arkea. On myös mahdollista, että tulevaisuudessa organisaatiot saattavat joutua kehittämään ohjelistoja työntekijöiden Internet-toiminnalle työajan ulkopuolella, koska valtava määrä tietoa on hyökkääjän kerättävissä pelkästään sosiaalisen median alustoja käyttämällä. Samalla on aivan yhtä todennäköistä, että rikollisten luoma paine ajaa yksityisen ja julkisen sektorin toimijat kehittämään teknisiä ratkaisuja näihin haasteisiin.

Suomessa ihmisten joutuminen tietojenkalastelun uhriksi on kasvamassa. Tutkijat Kolttola ja Näsi havainnoivat katsauksessaan Suomalaiset väkivallan ja omaisuusrikosten kohteina 2021, että vuonna 2018 vastaajista 0,7 prosenttia oli luovuttanut henkilötietojaan tietojenkalastelun takia, kun taas vuonna 2021 sama luku oli kasvanut 1,2 prosenttiin (Kolttola & Näsi 2022, 32–33). Tietojenkalastelu on myös kyberturvallisuuskeskuksen mukaan yleistymässä osana suomalaisten verkon käyttöä, sillä pelkästään pankkitunnusten kalastelusta aiheutui vuonna 2021 yli kahdeksan miljoonan euron menetykset, kun rikolliset saivat tietojenkalastelulla haltuunsa kuluttajien pankkitunnuksia ja niiden avulla tyhjensivät pankkitilejä (Kyberturvallisuuskeskus 2022, 23).

Näiden tietojen avulla voidaan tehdä alustavia olettamuksia. Tilastot, asiantuntijoiden lausunnot ja heidän laatimansa raportit viittaavat siihen, että tietojenkalastelu on kasvava uhka yrityksille ja yksilöille. Tietojenkalastelun kasvavasta määrästä voidaan myös tehdä

olettamus, että hyökkääjät käyttävät myös muita kuin teknisiä (palomuurien murtamiset ja hakkerointi) keinoja osana murtojaan, ja tämän työn olettamuksena on, että nämä keinot ovat psykologisia tietoteknisen sijasta.

1.2 Tavoite ja toimintasuunnitelma

Opinnäytetyö aloitettiin vuonna 2021 tavoitteena luoda organisaatioille ohjeistus sosiaalista manipulaatiota hyödyntävää tietojenkalastelua vastaan. Työn aihe valittiin puhtaasti mielenkiinnosta tietoturvaa kohtaan, koska pandemian aikana yleistynyt etätyökulttuuri lisäsi yritysten haavoittuvuuksia työskentelyn siirtyessä entistä enemmän Internettiin. Aihe on ajankohtainen, koska tietojenkalastelu on yksi nopeimmin kasvavista tietomurtojen keinoista, ja tilanne on pahentunut entisestään pandemian aikana.

Tavoitteenani on tuottaa ohje, jota on mahdollista käyttää nopeasti ja tehokkaasti viestinnän tarkistamiseen, joten ohje ei voi olla kooltaan liian suuri. Ohjeen pitää sisältää teoriaa aiheen monimutkaisuuden takia, mutta sen pitää samalla olla helposti omaksuttavissa sen päivittäistä käyttöä silmällä pitäen. Tavoitteena on ohjeistus, jonka rakenne sisältää ilmiön (tietojenkalastelu) kuvauksen, tietoa erilaisista metodeista, tyypilliset varoitusmerkit sekä varotoimenpiteet niitä vastaan.

Kohderyhmä valikoitiin harkitsemalla työn kirjoittajan omaa osaamista tietotekniikan saralla sekä todennäköisintä hyötyä ajatellen, koska kirjoittajan oma osaaminen tietotekniikasta ei riitä syvemmän ohjeistuksen kirjoittamiseen. Aiheen monimutkaisuuden ja resurssitarpeen takia voidaan myös olettaa, että tietojenkalastelu on isompi uhka pienille ja keskisuurille yrityksille, koska isoilla yrityksillä ja organisaatioilla on enemmän valmiutta ja osaamista torjua tietojenkalastelua. ”Rivityöntekijöiden” alttius tietojenkalastelulle on myös yksi syy sille, miksi tämä ryhmä valikoitui työni kohderyhmäksi.

Aiheeseen perehtyminen aloitettiin rajaamalla tietolähteet. Tietoa lähdettiin etsimään hakutermeillä ”tietojenkalastelu”, ”phishing”, ”suojautuminen” sekä ”tietojenkalastelijat”. Tietoa haettiin myös hakulauseilla, kuten ”mitä keinoja tietojenkalastelijat käyttävät”, ” kuinka suojautua tietojenkalastelulta” sekä ”tietojenkalastelu ja pienet- ja keskisuuret yritykset”.

Näiden termien käytöllä pyrittiin etsimään vastauksia kysymyksiin tietojenkalastelusta ilmiönä, sen keinoista sekä alalla vallitsevista suojautumiskeinoista ja kokemuksista tie-

toturvan koulutuksen kannalta. Aineiston keruun tavoitteena oli siis vastata, ketkä tekevät tietomurtoja (kyberrikolliset), miten he toteuttavat sitä (psykologiset keinot ja hyökkäysvariaatiot) ja miten tietojenkalastelulta on mahdollista suojautua (ennaltaehkäisy). Teoreettisen tiedonkeruun jälkeen aloitettiin ohjeen kokoaminen.

Ohje koottiin tiedonkeruun aikana kerätyn teorian pohjalta. Ohjeen kirjoituksen jälkeen opinnäytetyön raportti viimeisteltiin työskentelyn reflektion kirjoittamisella ja toiminnallisen osuuden (ohje) arvioinnilla. Lopuksi kirjoitettiin aiheen tulevaisuutta ja ohjetta käsittelevä yhteenveto.

Opinnäytetyöraportin rakenne käsittelee tietojenkalastelua/sosiaalista manipulaatiota ketkä, miten ja miksi (kirjoittajan reflektio) rakenteella. Ensimmäiseksi käsiteltiin kyberrikollisia ja tietomurtoja ”ketkä” kysymyksen vastaamiseksi, minkä jälkeen avattiin manipulointia, kognitiivisia harhoja sekä tapoja, miten edellä mainitut rikolliset hyödyntävät näitä. Näiden osioiden jälkeen kirjoitettiin ennaltaehkäisystä ja eri keinoista suojautua tietojenkalastelulta, ja raportti päätettiin työskentelyn reflektoinnilla.

1.3 Lähteiden valinta

Työhön tarvittava aineisto kerättiin Internetin avoimia lähteitä käyttäen. Aineistot olivat kansainvälisiä ja kotimaisia, mutta lähteistä suurin osa on kansainvälisten tutkijoiden keräämää tutkimustietoa. Lähteet olivat avoimia kirjallisuus- ja Internet-lähteitä, koska kolmea vuotta tuoreemmat kirjallisuuslähteet aiheesta ovat harmillisen harvassa.

Työn lähteitä arvioitiin käyttämällä muun muassa Pohjois-Michiganin yliopiston kirjaston suosittelemaa kuuden kriteerin menetelmää. Näitä kriteereitä ovat auktoriteetti, tarkkuus, objektiivisuus, ajankohtaisuus, kattavuus ja ulkoasu (Northern Michigan University 2018). Näiden kriteereiden avulla pyrittiin parantamaan työn lähdekriittisyyttä.

Lähdekriittisyyden varmistamiseksi kaikkia lähteitä tarkasteltiin niiden auktoriteetin, tarkkuuden, objektiivisuuden, ajankohtaisuuden, kattavuuden ja ulkoasun kannalta. Lähteen auktoriteettia arvioidessa kiinnitettiin huomiota lähteen läpinäkyvyyteen kysymällä, kuka on vastuussa sisällöstä ja onko kirjoittajalla kokemusta puhua koko aiheesta? Auktoriteettia tarkastelemalla on myös mahdollista havaita mahdolliset kolmannet osapuolet tai toimeksiantajat, jotka pyrkivät johdattelemaan lukijaa jollain tavalla.

Tarkkuudella viitataan lähteen keräämien/kokoamien tietojen luotettavuuteen. Ovatko lähteen käyttämät tiedot ja kirjoittajan lähteet helppoa löytää ja varmistaa itse? Työni kannalta oli erityisen tärkeää, että lähteiden keräämä tieto oli kerätty läpinäkyvällä ja varmennettavalla tavalla.

Lähdekriittisyyden tärkeimpiä osa-alueita on objektiivisuus. Opinnäytetyötä tehdessäni olen huomannut miten paljon ihmisten ennakkoasenteet ja oma asema työelämässä/yritysmaailmassa vaikuttavat siihen, mitä he sanovat ja jättävät sanomatta. Tietoturvallisuuden ongelmia ratkovat yritykset pyrkivät kaikki tarjoamaan omia tuotteitaan ja ratkaisujaan kuluttajille, joten tietynlainen skeptisyys on tarpeen näiden lähteiden raportteja ja julkaisuja luettaessa.

Objektiivisuutta käsitellessä on tärkeää tarkistaa, sisältääkö lähde mainoksia tai muuta johdattelua. Mikäli lähde sisältää mainontaa, onko se eroteltu selkeästi lähteen tiedotussisällöstä? Objektiivinen lähde ei sisällä puolueellisia väitteitä, joita on perusteltu perusteettomilla olettamuksilla.

Ajankohtaisuus on työn lopputuotoksena syntyvän ohjeistuksen kannalta tärkeä osa-alue. Tietotekniikkaa käsitellessä muutaman vuoden väli voi tehdä valtavan muutoksen tiedon tuoreuteen, joten työhön valittiin lähteitä, jotka sisälsivät julkaisun päivämäärän ja päivämäärät mahdollisille päivityksille. Näin pyrittiin varmistamaan se, että työssä käytetyt lähteet eivät olisi viittä vuotta vanhempia.

Kattavuus määrittelee, kuinka laadukkaaksi lähde luetaan. Kattava lähde käsittelee esitellyt aiheet ja väittämät riittävällä argumentoinnilla ja tuella oikealle kohderyhmälle. Kattava lähde päivittää myös käytettyjä lähteitä lisäämällä uutta tietoa aikaisempiin aineistoihin niissä käytettyjä faktoja hyödyntämällä.

Ulkoasu voi viestiä lähteen auktoriteetista, luotettavuudesta sekä ajankohtaisuudesta. Mikäli verkkolähteen ulkoasu on sekava ja linkit ja tiedostot eivät aukea, voidaan olettaa, että muutkaan tiedot eivät ole välttämättä kunnossa tai koottu asianmukaisesti. Lähteitä valittaessa kriteereiksi valittiin alustavasti materiaalia ainoastaan vuosilta 2018–2022, jotta työ olisi ajankohtainen.

Työskentelyn aikana tuli selväksi, että aikaväli 2018–2022 ei tuottanut tarpeeksi työni kannalta oleellista tietoa, joten laajensin työni aikaväliä vuosille 2000–2022. Aiheen kan-

nalta tämä herättää aiheellisia huolia, koska tietoturvaa käsitellessä neljä vuotta on erittäin pitkä aika, puhumattakaan kahdestakymmenestä vuodesta. Toisaalta työni tarkoitus ei ollut kehittää metodeja hakkerien käyttämiä teknisiä menetelmiä vastaan, vaan sen sijaan panostaa ihmisten ajattelumalleista ja hyökkääjien menetelmistä valistamiseen.

Verkkolähteitä löytyi paljon, mutta esimerkiksi tietoturvallisuuteen keskittyvät tutkimusraportit käsittelivät hyvin harvoin pelkästään tietojenkalastelua. Tietojenkalastelu on saanut osansa tutkijoista 2000-luvun alussa, mutta usein lähinnä osana tutkimuksia, jotka käsittelivät huijauksia ja niitä tekeviä rikollisia. Tietojenkalastelusta löytyy paljon blogeja, raportteja ja artikkeleita, mutta usein nämä olivat kaupallisen toimijan kuten tietoturvaa konsultoivien yritysten lähteitä ja näin ollen lähteen puolueettomuudesta ei voitu olla varmoja.

Tuorein aineisto työtä varten tuli pääosin avoimien tietolähteiden kuten Emerald Insightin ja Research Gate:n kautta. Näiden lähteiden arvioinnissa käytin samoja periaatteita kuin Internet-lähteiden kanssa, koska halusin välttää samoja löydöksiä listaavien tutkimusten toistoa työssäni. Tutkimusartikkeleita käsitellessä kiinnitin huomiota kattavuuteen, ja erityisesti muiden tutkijoiden töiden täydentämiseen.

Kirjallisuuslähteisiin ei luonnollisesti sisällytetty kaikkia Internet-lähteiden kriteereistä, mutta näiden arvioinnissa kiinnitin huomiota enemmän ajankohtaisuuteen ja kirjoittajan osaamiseen eli auktoriteettiin aiheesta. Osa verkkolähteistä ei puolestaan sovi aikaisempaan mainintaani kaupallisista lähteistä, koska esimerkiksi Mozilla ja Microsoft ovat isoja brändejä tietotekniikan ja tietokoneiden saralla. Markkinoita hallitsevien yritysten tietolähteitä pitää käsitellä terveellä skeptisyydellä.

MDN Web Docs on Mozilla säätiön (Mozilla Foundation) ylläpitämä avoimen lähdekoodin yhteistyöprojekti, joka tarjoaa muun muassa oppimisresursseja kehittäjille ja opiskelijoille (Mozilla Foundation 2023). Avoimen lähdekoodin lähteiden luotettavuus on kyseenalaista, mutta tietojenkalastelun nopean kehityksen takia aiheelle omistautuneiden harrastelijoiden ja ammattilaisten ylläpitämää tietokantaa voidaan kuitenkin pitää ajankohtaisempana kuin muita tietolähteitä koska niitä päivitetään useammin. Näillä alustoilla julkaisevat henkilöt sitoutuvat myös menettelyohjeeseen, ja Mozilla ja Microsoft tarkistavat näiden julkaisujen todenmukaisuuden.

Viranomaisten raporteissa keskityttiin aiheelle keskeisiin toimijoihin. Näiksi toimijoiksi laskettiin lainvalvojat, kuten Keskusrikospoliisi, Europol sekä Anti-Phishing Working Group (APWG). Kaikki edellä mainitut organisaatiot keräävät, tutkivat ja ennaltaehkäisevät tietojenkalastelua, joten näiden ryhmien aineisto on oleellista työlleni.

2 Kyberrikollisuus

Kyberrikollisuus sisältää erilaisia tasoja, ihmistyyppejä sekä motivaatioita. Kyberrikoksiin syyllistyvät henkilöt voidaan jakaa erilaisiin kategorioihin, jotka eroavat toisistaan tietomurtajan osaamisen, perimmäisen motivaation sekä olosuhteiden luomien mahdollisuuksien osalta. On myös tärkeää muistaa, että kyberrikolliset sopivat hyvin harvoin samaan ”muottiin” osaamisensa ja motivaationsa suhteen.

Kyberrikollisia motivoi ensisijaisesti raha, mutta kyberrikollisten joukkoon mahtuu myös puhtaasta uteliaisuudesta, ideologisista tai muista syistä tietomurtoja tekeviä ihmisiä. Tutkijat Edwards, Williams, Peersman ja Rashid Bristolin yliopistosta kävivät läpi kyberrikollisia ja heidän motivaatioitansa tutkineita tutkimuksia ja tieteellisiä julkaisuja vuosien 2000–2015 välillä. Tutkijat vertailivat vuosien aikana kerättyä tutkimustietoa tarkoituksenaan ymmärtää paremmin modernien kyberrikollisten motivaatioita.

Datasta kävi ilmi, että kyberrikokseen syyllistyvät olivat usein miehiä (60–90 % vastaajista), jotka työskentelivät ja viettivät aikaansa paljon Internetissä, olivat korkeasti koulutettuja sekä olivat varhaisessa iässä vuorovaikutuksessa tietotekniikan kanssa. Dataa vertailemalla tutkijat havaitsivat, että vastaajien todennäköisyys syyllistyä rikokseen verkossa kasvoi yhdessä Internetin käytön lisääntyessä (Edwards ym. 2022, 29–30). Tutkijat havaitsivat myös, että kyberrikokseen syyllistyneet henkilöt kärsivät usein huonosta itsehillinnästä (Edwards ym. 2022, 29).

Kyberrikollisten lokerointi eri ryhmiin ei ole yksiselitteistä. Tutkijat pyrkivät kompensoimaan tätä katsauksessaan nojaamalla Marcus K. Rogersin vuonna 2006 julkaistuun tutkimukseen A two-dimensional circumplex approach to the development of a hacker taxonomy, jossa hän pyrki luomaan ja kehittämään luokittelumetodeja kyberrikollisille. Rogers luokitteli erilaiset kyberrikolliset eri luokkiin, jotka ovat noviisit, kyberpunkit, sisäiset, pikkuvarkaat, vanha kaarti, ammattirikolliset, informaatiosoturit, poliittiset aktivistit sekä virusten kirjoittajat/”skriptaajat” (Kuvio 2)

Rikollinen	Osaaminen ja työkalut	Motivaatio
Noviisit	Valmiit työkalut	Jännitys ja ego
Kyber-Punkit	Rajallista ohjelmointikykyä	Huomio ja rahallinen palkkio
Sisäiset	Ex-työntekijä	Katkeruus ja kostonhimo
Pikkuvarkaat	Vaihtelevaa	Raha
Vanha Kaarti	Monipuolista osaamista	Älyllinen haaste
Ammattirikolliset	Vaihtelevaa	Raha
Informaatiosoturit	Vaihtelevaa	Raha ja valtion tuki
Poliittiset aktivistit	Vaihtelevaa	Ideologia
Virusten skriptaajat	Monipuolista osaamista	Vaihtelevaa

Kuvio 2. Kyberrikollisten taksonomia, Rogers, 2006.

Rogers määritteli noviisit valmiita Internetistä ladattavia ohjelmia ja työkaluja käyttäviksi amatööreiksi, jotka tekevät tietomurtoja pitkälti jännityksen ja egon takia. Harrastelijoiksi voidaan myös laskea kyberpunkit, joilla on monipuolisempaa osaamista kuin noviiseilla. (Rogers 2006, 97–102, teoksessa Edwards ym. 2022, 25–26.)

Sisäiset viittaa organisaation sisäisiin henkilöihin eli nykyisiin tai entisiin työntekijöihin, jotka syystä tai toisesta päättävät kostaa tai aiheuttaa harmia työnantajalleen. Sisäisiä ei ole asetettu taksonomiassa korkealle osaamisen kannalta, mutta näillä henkilöillä on usein yksityiskohtaista tietoa yrityksestä ja sen haavoittuvaisuuksista, mikä tekee heistä vaarallisempia. (Rogers 2006, 97–102, teoksessa Edwards ym. 2022, 25–26.) Näillä henkilöillä on usein myös IT-osaamista, jota he käyttävät tyypillisesti kostaakseen työnantajalleen jonkin koetun tai aidon vääryyden.

Puhtaasti rahallisista syistä tietomurtoja tekeviksi ryhmiksi voidaan laskea pikkuvarkaat ja ammattirikolliset sekä virusten kirjoittajat. Näiden ryhmien osaamista on paikoin vaikea määritellä, koska osaaminen näiden ryhmien edustajien kesken voi vaihdella laajasti, ja koska Rogers ei kokenut nykyisen tutkimustiedon antavan tarpeeksi selkeitä vastauksia näistä ryhmistä. (Rogers 2006, 97–102, teoksessa Edwards ym. 2022, 26–27.) Nämä ryhmät ovat usein osa laajempia rikollisryhmiä, joilla on motivaatiota ja resursseja jatkuvasti kehittää uusia huijauksia ja hyökkäysmetodeja.

Muista kuin rahallisista syistä murtoja tekeviksi ryhmiksi lasketaan Vanha Kaarti, informaatiosoturi sekä poliittiset aktivistit. Rogers määritteli Vanhan kaartin vanhemman sukupolven hakkereiksi, jotka tekevät tietomurtoja älyllisen haasteen ja uteliaisuuden takia. (Rogers 2006, 97–102, teoksessa Edwards ym. 2022, 19–20.) Informaatiosoturit ovat

korkeasti koulutettuja ja kokeneita, joten he ovat usein valtioiden tai valtiollisten toimijoiden rekrytoimia ja patriotismista motivoituneita yksilöitä. Rogers huomauttaa, että informaatiosoturit ja ammattirikolliset ovat näistä ryhmistä vähiten ymmärrettyjä, ja alleviivasi että tämän ryhmän koko kasvoi Itäblokin maiden tiedustelupalveluiden lakkautusten jälkeen, mikä voi selittää näiden yksilöiden korkean osaamistason. (Rogers 2006, 97–102, teoksessa Edwards ym. 2022, 25.)

Poliittiset aktivistit tekevät tietomurtoja ideologisista tavoitteista. Rogers lisäsi tämän kategorian tasapainottamaan muita kategorioita datassa sekä lisäämään taksonomian syvyyttä. Poliittiset aktivistit ovat esimerkki alaluokasta, jollaisia Rogers spekuloi tulevien tutkimusten tarvitsevan lisää hakkerien ymmärtämiseksi.

Uhkia ja hyökkääjiä käsitellessä on tärkeää muistaa, että suurin uhka yritykselle tulee usein sisältä. Nämä murrot voivat olla vahingossa tapahtuneita, huolimattomuudesta johtuvia tai tahallisia. Tahalliset sisäpiiriläisten aiheuttamat tietomurrot voivat johtua useista eri syistä. Ne ovat silti vähemmistössä tarkastellessa tietomurtoja, joista suurin osa johtui puhtaasta virheestä ilman pahaa tahtoa työnantajaa kohtaan (Antonucci 2017, 98–99).

Tutkijat painottavat katsauksessa useasti, että tiedonkeruuseen käytetyt metodit saattavat vinouttaa dataa, ja luoda näin harhaluuloja kyberrikollisista tai heidän motivaatioistaan. Aiheen tutkimista haittaa toistaiseksi tutkijoiden mukaan huono pääsy rikollisyhteisöihin, vaihtelevat ja löyhät käsitteet sekä nykyisten tutkimusten aikana tehdyt oletamukset kyberrikollisuudesta ja sen todellisesta tilasta. (Rogers 2006, 97–102, teoksessa Edwards ym. 2022, 24.)

3 Tietojenkalastelu

3.1 Mitä tietojenkalastelu on

Sosiaalinen manipulointi on kirjallisuuden ja tutkimusdatan valossa erittäin yleistä toimintaa, jossa hyökkääjä pyrkii manipuloimaan kohdetta käyttämällä psykologisia keinoja, kuten kognitiivisia harhoja sekä suostutteluperiaatteita. Tietojenkalastelu on yksi yleisimmistä työkaluista tietomurroissa, ja se on oleellinen osa monimutkaisemmissakin hyökkäyksissä. Tietojenkalastelua on mahdotonta torjua täysin, mutta jatkuva koulutus ja aiheen käsittely interaktiivisten pelien kautta on osoittanut positiivisia lopputuloksia oppimisen kannalta. (Chaudhary 2016, 69.)

Tietojenkalastelu tai ”phishing” englanniksi tarkoittaa tilannetta/toimintaa, jossa hyökkääjä huijaa käyttäjän avaamaan haitallisen linkin tai sähköpostiliitteen naamioimalla ne kiinnostavaksi sisällöksi (F-Secure 2023). Tietojenkalastelu on kasvava uhka kaikille yrityksille ja yksilöille (Toikkanen 2020, 5-6). Tietojenkalastelu hyödyntää psykologisia malleja sekä yleisiä kognitiivisia harhoja.

3.2 Tietojenkalastelun psykologia

3.2.1 Suostuttelu

Tämän työn kannalta on oleellista ymmärtää suostuttelun (eng. Persuasion) ja kognition kannalta oleelliset tekijät, jotta voidaan selittää, miten ihmisten valppaus herpaantuu sosiaalisen manipuloinnin hyökkäyksissä. Ensyklopedia Britannica määrittelee suostuttelun prosessiksi, jossa muiden ihmisten viestintä vaikuttaa henkilön asenteisiin tai käyttäytymiseen ilman pakko (Encyclopaedia Britannica 2021). Sosiaalista manipulointia hyödyntävät hyökkääjät hyödyntävät suostuttelua, mutta he usein lisäävät tilanteisiin keinotekoisen kiireen ja paineen, mikä helpottaa hyökkääjää uhrin toiminnan ohjaamisessa. Tutkijat Jones, Armstrong, Tornblad ja Namin listasivat useita uhrin vakuuttamisen periaatteita, kun he tutkivat hyökkääjien käyttämiä suostuttelun periaatteita (eng. persuasion principles) huijauksissa (Jones & Armstrong & Tornblad & Namin 2020, 315–316).

Tutkiessaan puhelimen välityksellä tapahtuvaa tietojenkalastelua, tai ”vishingiä” Jones ym. pohjasivat tutkimustaan esimerkiksi Graggin, Cialdinin ja Stajanon töihin, joita tutkijat tekivät itsenäisesti. Kaikki kolme tutkijaa tutkivat tietojenkalastelua ja sen taustalla olevia psykologisia keinoja, ja viimeisin näistä tutkimuksista määritteli seitsemän psykologista periaatetta näille huijauksille. Stajano ja Wilson määrittelivät näiksi periaatteiksi häiriön, auktoriteetin, lauma-ajattelun, epärehellisyyden, ystävällisyys, tarve ja ahneus, ja aika (Stajano & Wilson 2011, 71–73).

Häiriön (eng. Distraction) tarkoitus on ohjata kohteen huomio muualle, ja käytännössä tämä tarkoittaa, että ihmiset keskittyvät vain siihen, mikä heitä itseään milläkin hetkellä kiinnostaa (Stajano & Wilson 2011, 71–72). Auktoriteettiin vetoaminen on keino, jota huijarit käyttävät, kun he haluavat pakottaa uhrin toimimaan tietyllä tavalla esiintymällä esimerkiksi poliisina tai yrityksen esihenkilönä (Stajano & Wilson 2011, 72). Lauma-ajattelun tutkijat määrittelivät ihmisten tavaksi seurata muiden ihmisten esimerkkiä, vaikka seuraamukset voivat olla negatiivisia.

Epärehellisyysperiaatteen ideana on saada uhri osaksi rikosta ja näin varmistaa, että heidän kynnyksensä ilmoittaa murrosta tai puhua tilanteesta viranomaisille on korkea. Ystävällisyys on ymmärrettävästi yksi periaatteista, koska ihmisillä on luonnollinen taipumus miellyttää muita, ja hyökkääjät vastaavat tähän olemalla mahdollisimman ystävällisiä kohteelleen tai esiintymällä henkilönä, joka tarvitsee apua (Jones ym. 2020, 314–315). Tarvetta ja ahneutta hyödyntävät rikolliset pyrkivät kiinnittämään uhrin huomion tarjoamalla heille mahdollisuutta jonkin tietyn tarpeen tai tavoitteen saavuttamiseen (Jones ym. 2020, 315).

Viimeinen Stajanon ja Wilsonin listaama huijauksen periaate on aika (Jones ym. 2020, 315). Kiireen ja tunteen hyödyntäminen kohteen manipuloinnissa tuli esiin useasti tämän työn lähteissä, ja se perustuu keinotekoiseen kiireeseen, missä kohteelle painotetaan, että heillä on hyvin rajallisesti aikaa tarttua huijarin tarjoamaan ”mahtavaan tilaisuuteen”. Ajan käyttäminen osana huijausta on tuttu näky tietojenkalastelussa, jossa kiirettä käytetään perustelemaan esimerkiksi yrityksen sisäisten sääntöjen rikkomista huijauksen kohteelle.

Suostutteluperiaatteet ovat yleisiä ja arkisessa käytössä muidenkin kuin tietojenkalastelijoiden toimesta. Markkinoijat ja myyntityötä tekevät ihmiset käyttävät häiriöitä ja aikaa osana työtään miltei päivittäin, ja poliisit ja muut viranomaiset vetoavat auktoriteettiinsa osana työtään. Suostutteluperiaatteiden tiedostaminen on erityisen tärkeää tietojenkalastelua käsitellessä, koska ne voivat auttaa työntekijää havaitsemaan manipulaation mahdollisimman aikaisin.

3.2.2 Manipulointi ja opittu avuttomuus

Amerikkalainen Psykologinen Yhdistys (APA) määrittelee termistössään manipuloinnin käyttäytymiseksi, joka on suunniteltu hyväksikäyttämään, hallitsemaan tai muutoin vaikuttamaan toisiin oman edun nimissä (Manipulation 2022). Tietojenkalastelijat pyrkivät manipuloimaan uhrejansa ja hyötymään uhrille haitallisen toimenpiteen tekemisestä, ja onnistuakseen he yrittävät vaikuttaa uhriin erilaisten psykologisten/kognitiivisten harhojen avulla. Avaan seuraavaksi tietojenkalastelussa esiintyvää psykologiaa ja termistöä.

Tietojenkalastelun kannalta on oleellista ymmärtää termi kognitio sekä tarkastella niiden suhdetta suostutteluun. Kognitiolla tarkoitetaan kaikkia tietämisen ja tiedostamisen muo-

toja, kuten havaitseminen, käsitys, muistaminen, päättely, tuomitseminen, kuvitteleminen ja ongelmanratkaisu (Cognition 2022). Tavat miten omaksumme tietoa ja miten reagoimme siihen, on oleellista tietojenkalastelua käsitellessä.

Eero Vuoksimaa Lääkäriseura Duodecimista kirjoitti, että kognitiiviset toiminnot heikkenevät ajan myötä, ja käytännössä tämä tarkoittaa, että yksilön kyky omaksua uutta tietoa heikkenee ajan myötä (Vuoksimaa 2019, 1076–1078). Rikolliset usein hyödyntävät tätä tietoisuuden luonnollista rappeutumista kohdentaen hyökkäyksensä vanhoihin ja muistisairaisiin ihmisiin (Niemi 2018). Voidaan siis olettaa, että tietojenkalastelijat hyödyntävät uhrin mahdollista kognition heikkenemistä tietojenkalastelua suunnitellessaan.

Teoksessaan Successful Cybersecurity Professionals : How to Change Your Behavior to Protect Your Organization Steven Brown mainitsee relevanteiksi psykologian tieteenaloiksi muun muassa behaviorismin, sosiaalipsykologian, kognitiivisen psykologian sekä niiden alalajit, kuten ehdollisen refleksin (eng. Conditioned response), humanismin sekä yhdenmukaisuuspsykologian/teorian (conformism) (Brown 2020, 2–3). Brown kirjoittaa, että kognitiivisen psykologian tutkijat ovat tiedostaneet opitun avuttomuuden (eng. Learned Helplessness) merkityksen ihmisten käytöksessä, kun kohtaamme stressaavia tilanteita arjessamme. APA määrittelee opitun avuttomuuden ilmiöksi, ”jossa yksilöiden sanotaan oppivan, että heiltä puuttuu hallinta ympäristöönsä ja sen tapahtumiin, mikä puolestaan heikentää motivaatiota tehdä muutoksia tai yrittää muuttaa tilanteita” (Learned helplessness 2022).

Opittu avuttomuus on usein huonojen tai tekemättä jääneiden päätösten takana. Opittu avuttomuus voi vakavimmissa tapauksissa olla merkki mielenterveyden ongelmista (Learned helplessness 2022), mutta kaikki ihmiset kokevat jonkinasteista avuttomuutta tai jähmettymistä elämänsä aikana. Opittu avuttomuus on läsnä omassa arjessamme, kun kohtaamme tilanteita, joissa vakuutamme itsellemme, että emme voi vaikuttaa tilanteeseen mitenkään.

Tietoturvallisuuden kannalta opittu avuttomuus voi olla erityisen tuhoisaa, koska mahdollisen tietomurron esto riippuu siitä, kuinka aikaisin tietomurto tai laitteen saastuminen saadaan vastuuhenkilöiden ja yritysjohdon tietoon. Työntekijän on suotavaa ilmoittaa epäilyttävästä toiminnasta myös siksi, että hän voi ennakoivalla toiminnallaan suojella itseään mahdolliselta rikosoikeudelliselta vastuulta. ”Jähmettynyt” henkilö on myös todennäköisesti helpommin manipuloitavissa hyökkääjän kannalta, koska stressaantunut henkilö ottaa hyökkääjän ”avun” vastaan todennäköisemmin kuin rauhallinen henkilö.

3.2.3 Kognitiiviset harhat

Kognitiiviset harhat (eng. cognitive bias) ovat tapoja, joilla tietty henkilö ymmärtää tapahtumia, tosiasioita ja muita ihmisiä, ja ne perustuvat hänen omiin uskomuksiinsa ja kokemuksiinsa, jotka eivät välttämättä ole järkeviä tai tarkkoja (Cognitive Bias 2022). Kognitiiviset harhat näkyvät elämässämme väärinä uskomuksina ja asenteina, ja tyypillinen esimerkki tästä on rasismi, joka usein juontaa juurensa negatiivisiin kokemuksiin tai ympäristöstä opittuihin asenteisiin. Kognitiiviset harhat eivät tee henkilöstä hyvää tai pahaa, koska kaikilla ihmisillä on jonkinasteista taipumusta katsoa maailmaa oman elämänkokemuksensa kautta.

Tietojenkalastelijalle kognitiiviset harhat ovat työkalu, jolla voidaan luoda tiettyjä mielikuvia ja saattaa kohde kiihtyneeseen mielentilaan, jossa kohteen arvostelukyky on heikentynyt (Gragg 2002, 6–8). Hadnagy ja Fincher nostivat työssään esiin kognitiivisia harhoja, mitkä vaikuttavat päätöksentekokykyymme. Näitä harhoja ovat kehystäminen (eng. framing effect), miellettävyysheuristiikka (eng. availability heuristic) sekä vahvistumisharha (eng. confirmation bias) (Hadnagy & Fincher & Dreeke 2015, 68–70).

Hadnagy ym. määrittelivät kehystämisen tilanteeksi, jossa päätöksemme/toimintamme riippuu siitä, miten päätös nähdään muitten näkökulmasta (Hadnagy ym. 2015, 70). Kehystäminen on erittäin arkinen kognitiivinen harha, ja kaikki ihmiset ovat vähintään kerran elämässään tehneet päätöksen sen perusteella, miten päätös nähdään läheisten tai ystävien näkökulmasta omien kiinnostusten tai halujen sijasta. Kyberrikolliset hyödyntävät kehystämistä usein esimerkiksi pornohuijauksen kautta, missä uhria uhkaillaan heidän sivuhistoriansa/tietokoneen kameran sisällön julkaisemisella, ja luodaan näin pelkoa seuraamuksista ja mainehaitasta uhrille.

Huono maine ja sen seuraamukset ovat yksi vaihtoehto tietojenkalastelijalle, mutta toinen merkittävä vaihtoehto on miellyttävyysheuristiikka. Miellyttävyysheuristiikkaa viittaa tapaamme valikoida ja suodattaa informaatiota oman lähimuistimme perusteella (Hadnagy ym. 2015, 70–71). Tyypillinen esimerkki tästä on pankkitunnuksia/henkilötietoja kalasteleva viesti, jossa mainitaan viimeisin uutisissa ollut kryptovaluutta, jotta uhrin alitajunta yhdistäisi muistissa tuoreena olleen tiedon tästä kryptovaluutasta tilaisuuteen saada osa voitoista.

Vahvistusharha tarkoittaa ihmisten taipumusta käsitellä tietoa etsimällä tai tulkitsemalla tietoa, joka on yhdenmukainen olemassa olevien uskomusten kanssa (Brown 2020, 84).

Vahvistusharha näkyy arjessa virheellisen tiedon sisäistämisenä puhtaasti siksi, että virheellinen tieto sopii paremmin henkilön omaan maailmankuvaan (Brown 2020, 84–85). Tietojenkalastelijat hyödyntävät vahvistusharhaa kohteen ohjaamisessa, koska on helpompaa ohjata uhria, joka uskoo sähköpostissa oleviin väittämiin.

Vahvistusharhat ovat yleisiä kognitiivisia harhoja, joita on mahdollista havaita esimerkiksi ihmisten äänestyskäyttäytymistä havainnoidessa. Ihmiset asettavat usein suhteettoman paljon huomiota oman ehdokkaansa positiivisiin puoliin, ja vastaavasti jättävät huomiotta ehdokkaan negatiiviset puolet. Samanlainen ajattelu on läsnä enemmistön elämässä, koska monia ihmissuhteitamme voi ohjata harhainen tai ”siloteltu” käsitys toisesta henkilöstä.

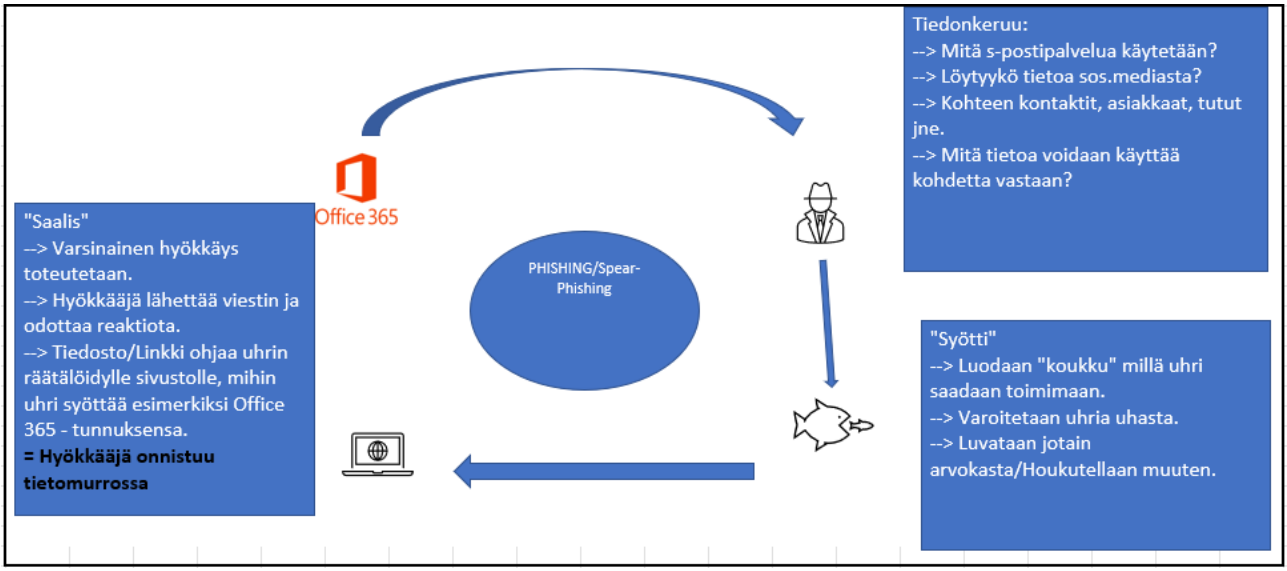
Hadnagy ym. toivat esiin myös fysiologisen olotilan (kehon terveys ja vastaavat) vaikutuksen päätöksiin, joita teemme. Vaikka kehomme kunnolla ja ulkoisilla ärsykkeillä (lämpötila, äänet, valoisuus jne.) on merkitystä päätöksentekoomme, en käsittele ohjeessa ulkoisia ärsykkeitä/ympäristövaikuttimia tarkemmin, koska työn kannalta oleellisempaa on kuitenkin ymmärtää ihmisten alitajunnasta kumpuavaa tarvetta sopeutua muihin ihmisryhmiin, ja sovittaa käytöstään muiden ihmisten kaltaiseksi (Hadnagy ym. 2015, 72–74).

3.3 Tietojenkalastelun variaatiot

Tietojenkalastelu sisältää karkeasti kolme vaihetta, ja ne ovat tiedonkeruu, syötti ja saalis (Kuvio 3). Tiedonkeruun aikana hyökkääjä perehtyy kohteeseensa ja käytössä oleviin viestintäkanaviin, ja laatii näiden perusteella varsinaisen tietojenkalasteluviestin. Tiedonkeruuta on mahdollista tehdä avoimien lähteiden kuten uutismedian, sosiaalisen median, yritysten julkaisujen avulla tai sisäisten lähteiden kautta, joiksi lasketaan Intranet-viestit, sähköpostit, kuitit ja muut fyysiset dokumentit.

Tiedonkeruun avulla hyökkääjä yrittää etsiä tietoa, jota voidaan käyttää kohdetta vastaan. Heikkouden paikannettuaan tietojenkalastelija luo syötin, joka on psykologisia keinoja käyttävä huijausviesti. Tyypillisesti nämä viestit pyrkivät herättämään hämmennystä ja paniikkia kohteessaan painottamalla tilanteen kiireellisyyttä tai painottamalla mahdollisia negatiivisia seurauksia kohteelle, mikäli he eivät toimi hyökkääjän haluamalla tavalla.

Viimeisessä vaiheessa hyökkääjä toteuttaa itse hyökkäyksen. Tietojenkalasteluviestit ovat massatuotantoa ja niitä lähetetään tuhansittain päivittäin. Viestit tyypillisesti ohjaavat uhrin väärennetylle verkkosivulle. Väärennetyllä sivulla uhri luovuttaa tunnuksen, joita hyökkääjät käyttävät esimerkiksi verkkopankkiin kirjautumiseen.



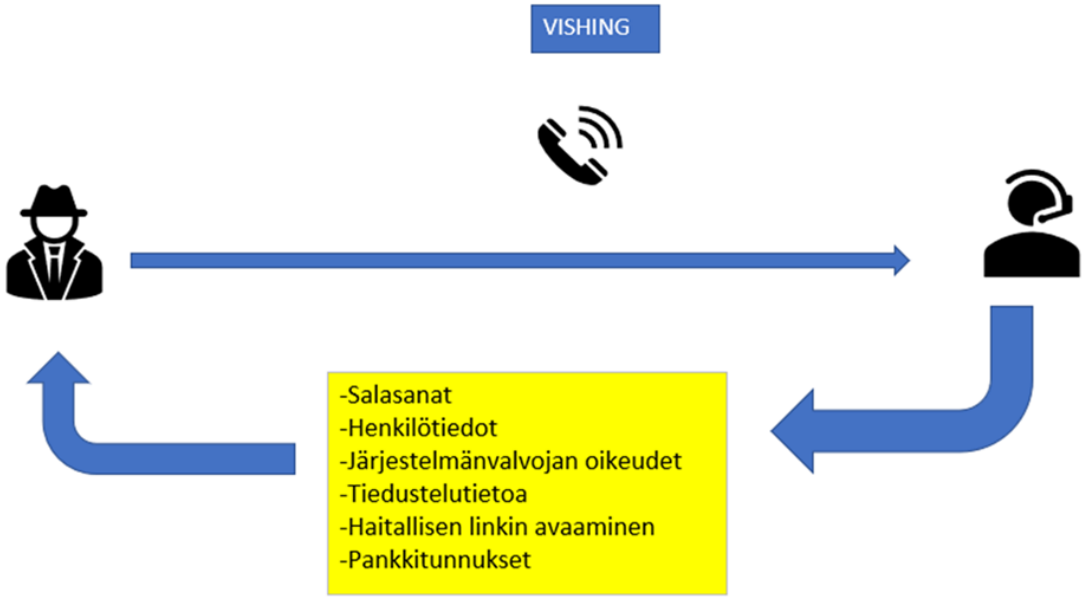
Kuvio 3. Tietojenkalastelun kehä (Moinescu ym. 2019, 163–164).

Tietojenkalasteluhyökkäykset ovat arkipäivää. Jokainen meistä on saanut vähintään yhden huonolla kieliopilla kirjoitetun viestin, jonka osoitetiedot eivät johda minnekään, ja sen sävy kannustaa aggressiivisesti klikkaamaan epämääräistä linkkiä tai postin mukana tullutta liitetiedostoa (Kuvio 4). Tyypillisesti nämä yksinkertaisia virheitä sisältävät viestit eivät ole huolellisesti suunniteltuja ja kohdennettuja viestejä, mutta ne tarjoavat hyödyllisiä esimerkkejä tietojenkalasteluviestien perusteista.

Kuvio 4.Tyypillinen tietojenkalastelusähköposti. Kirjoittajan oma sähköposti, 2022.

Omaan sähköpostiini saapunut viesti (Kuva 4) on hyvä esimerkki tyypillisestä tietojenkalastelusähköpostista. Viesti sisältää kirjoitusvirheitä, epämääräisiä linkkejä ja aikamääreen 30.09.2019, jolla pyritään luomaan kiireen tunnetta, ja näin lisätään todennäköisyyttä, että klikkaan linkkiä. Viesti on esimerkki tietojenkalasteluviestistä, jota lähetetään isoja määriä, joten jo muutaman henkilön huijaus sadasta ihmisestä voi olla rahallisesti kannattavaa.

Työntekijälle nämä yksinkertaiset viestit eivät ole suurin uhka, mutta niitä ei pidä aliarvioida. Tietomurtajat kehittävät jatkuvasti uusia metodeja näitten viestien parantelemiseksi, ja kohdennettu tietojenkalastelu on harvoin yhtä yksinkertainen kuin aiemmin tarjoamassani esimerkissä (Europol 2021, 30–31). Europol arvioi vuoden 2021 katsauksessaan internetrikollisuuteen, että pandemian aikana rikolliset ovat kehittäneet tietojenkalastelumenetelmiä yhdistelemällä tietoa aiemmista tietomurroista, jotta he pystyvät luomaan mahdollisimman kohdennettuja viestikampanjoita korkean profiilin kohteita varten (Europol 2021, 31–32).

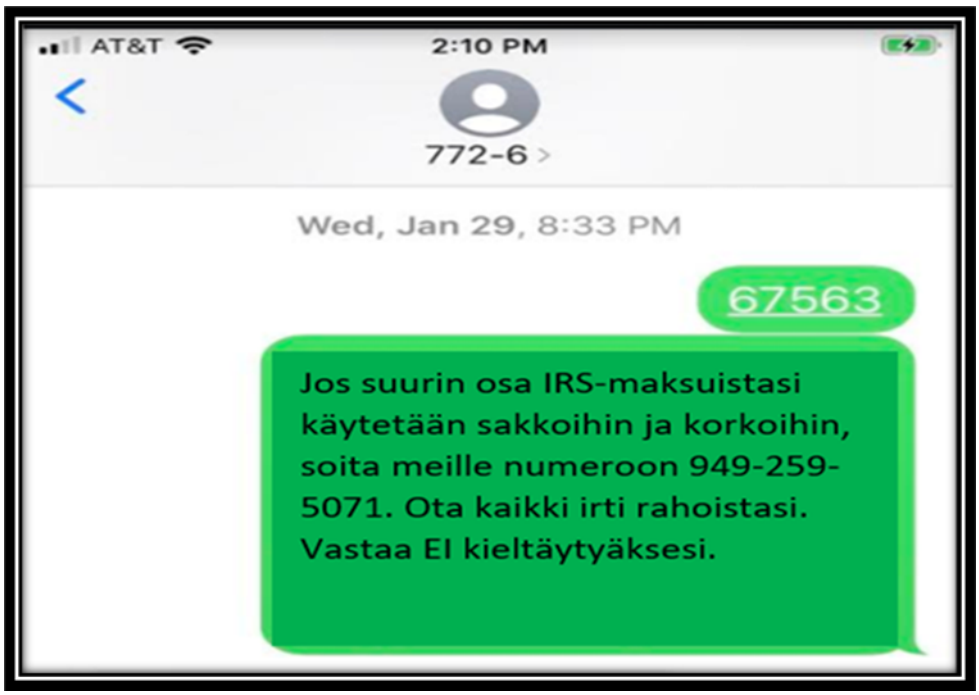


Kuvio 5. Opas puhelinhuijauksiin (Ollman 2007, 3).

Puhelinurkinta tai Vishing on manipuloinnin menetelmä, jolla uhri vakuutetaan luovuttamaan henkilökohtaista, taloudellista tai muuta tietoa (Ollman 2007, 3). Tämän menetelmän nimi on yhdistelmä englannin kielen sanoja ”voice” (ääni), ja aiemmin mainittu phishing (tietojenkalastelu) (Ollman 2007, 3). Puhelinurkinnassa uhrin toimintaa pyritään ohjaamaan niin, että hän soittaa hyökkääjälle, jotta uhri saadaan luovuttamaan tietoja puhelimitse (Kuvio 5) sekä avaamaan hyökkääjän lähettämien tekstiviestien sisältämiä linkkejä tai tiedostoja.

Puhelinurkinta ei eroa sähköpostin välityksellä tehdystä tietojenkalastelusta paljon, mutta puhelinurkinta vaatii enemmän vuorovaikutustaitoja hyökkääjältä, koska hänen pitää kyetä vakuuttamaan uhri puhelinkeskustelussa sähköpostien sijasta. Puhelinurkinta noudattaa yleensä käsikirjoitusta, jonka mukaan uhrin laite on hyökkäyksen kohteena ja korjatakseen tilanteen teknikkona esiintyvä hyökkääjä pyytää uhria luovuttamaan kirjautumistietoja tai suorittamaan etähallintaohjelman, jolla hyökkääjä voi suoraan ottaa laitteen haltuun. Uhrilta saatuja kirjautumistietoja käytetään tämän jälkeen joko tilien tyhjentämiseen, ostosten tekoon, sähköpostien sisältämien tietojen keruuseen tai tulevien hyökkäysten tukemiseen. Puhelinurkinta voi olla myös työkalu laajemman tietomurron valmistelussa.

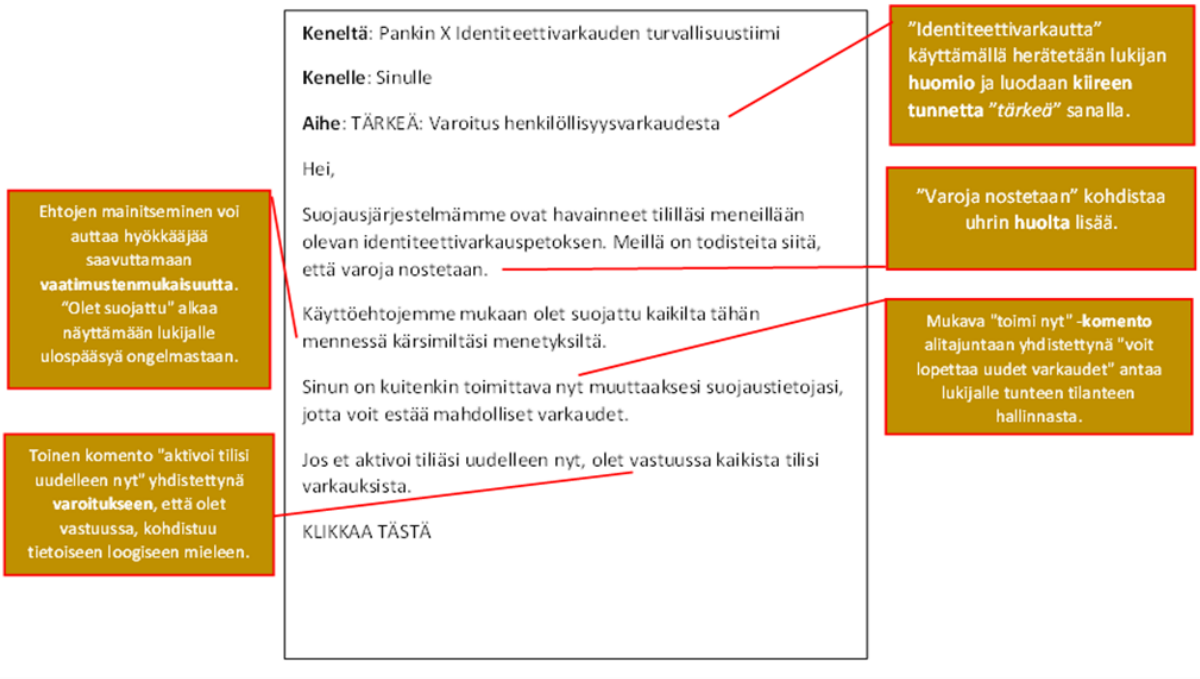
Tietojenkalastelussa voidaan käyttää myös tekstiviestejä. Näiden erittäin yleisten viestien teksti on yleensä laadittu huonolla suomen kielellä, ja viestien sävy painostaa uhria tekemään jonkin toiminnon, kuten haitallisen linkin avaamisen, millä kalastetaan uhrin tietoja (Kuva 6). Suomessa näitä usein Kelan tai pankkien viestejä jäljitteleviä viestejä on käytetty ja käytetään edelleen henkilötietojen kalasteluun (Kemppi 2022).



Kuvio 6. Huijaustekstiviesti. Kirjoittajan oma puhelin.

Tekstiviestien välityksellä tehty tietojenkalastelu vaatii tietämystä ihmisten päätöksenteosta, ja hyökkääjät hyödyntävät kognitiivisia harhojamme viestejä laatiessaan. Viestin sisältö on tyypillisesti tunteisiin vetoavaa, ja sen tarkoitus on saattaa uhri kiihtyneeseen tilaan, jossa hän ei kiinnitä yhtä paljon huomiota mahdollisiin ristiriitaisuuksiin (Hadnagy ja Fincher 2015, 77). Tekstiviestihuijausten havaitseminen on varsin helppoa, mutta muun muassa Kyberturvallisuuskeskus varoittaa huijarien käyttävän kopioituja logoja sekä allekirjoituksia, jotta viesti olisi mahdollisimman vakuuttava (Kyberturvallisuuskeskus 2022).

Käyn nyt läpi lyhyesti tyypillisen tietojenkalasteluun luodun sähköpostin. Ian Mann käsitteli kirjassaan Hacking the Human : Social Engineering Techniques and Security Countermeasures tyypillisen huijausviestin rakenteen kappale kappaleelta. Mann avaa kirjassaan myös, mitä tunteita kohteessa yritetään herätellä (Kuvio 7).



Kuvio 7. Tyypillinen tietojenkalastelusähköposti (Mann 2008, 135).

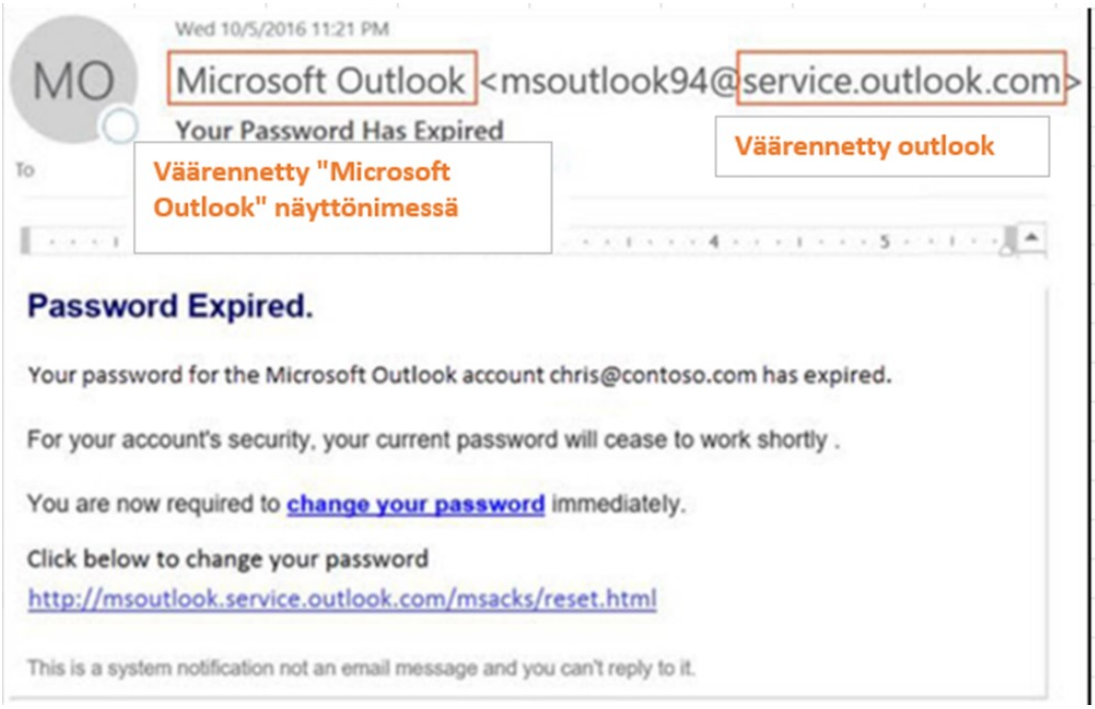
Sähköpostin ensimmäinen näkyvä osa on viestin aihe, joten luonnollisesti tietojenkalastelijat pyrkivät luomaan otsikon, joka takaa viestin avaamisen. Yllä olevassa esimerkissä otsikkoa käytetään huomion herättämiseksi ja kiireen tunteen luomiseksi käyttämällä sanoja kuten 'tärkeä' (Mann 2008, 134–135). Vastaavasti puheet "suojajärjestelmästä" antavat uhrille ulospääsytien tilanteesta, jolloin uhri klikkaa linkkejä korkeammalla todennäköisyydellä.

Hyökkääjät ovat luonnollisesti kehittäneet vastakeinoja yritysten tietoturvan käytäntöjä vastaan. Työntekijät eivät voi luottaa ainoastaan teknisiin ratkaisuihin tietojenkalastelulta suojautumisessa, sillä tietojenkalastelijat kehittävät jatkuvasti erilaisia keinoja ohittaa organisaatioiden suojausmenetelmiä (virustentorjunta ja roskapostisuodattimet). Chaudhary listasi näiksi keinoiksi muun muassa haitallisia ohjelmia ja linkkejä sisältävät verkkojulisteet tai verkkomainokset (Kuva 8), sosiaalisen median ja foorumien julkaisut sekä "pahan kaksosen" käyttäminen (Chaudhary 2016, 22–23).

Kuvio 8. Esimerkki pahantahtoisesta verkkojulisteesta osana tietojenkalastelua. Kirjoittajan sähköposti.

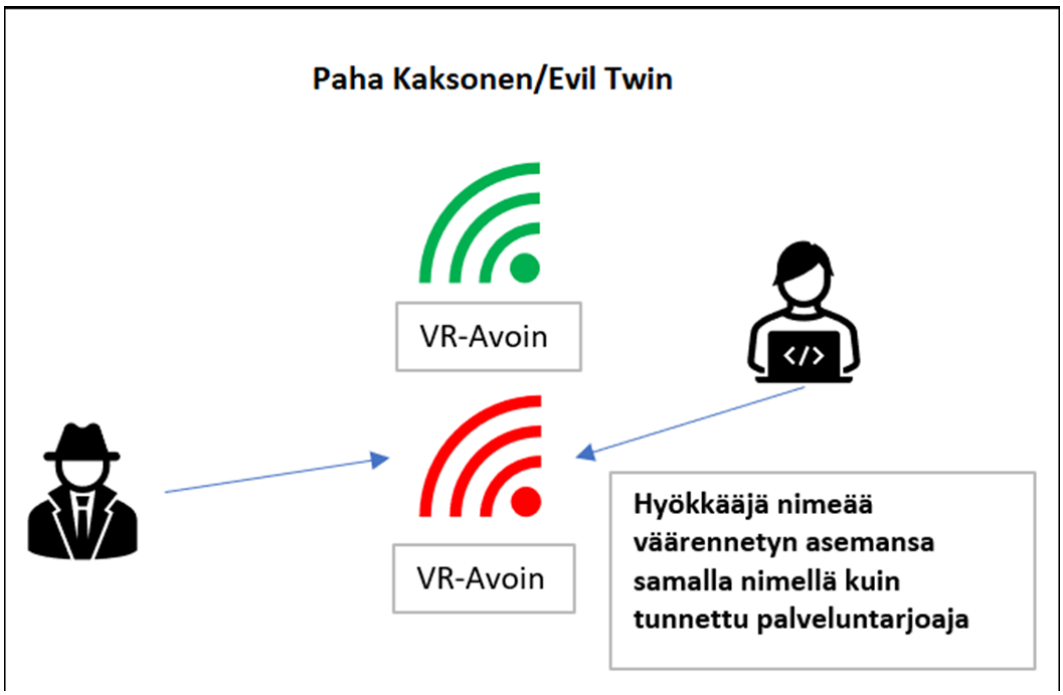
Digitaalisessa mainonnassa verkkobannerit, jotka tunnetaan myös nimellä näyttöbannerimainokset tai näyttömainokset, ovat klikattavia digitaalisia mainoksia, jotka on upotettu verkkosivustoille ohjaamaan liikennettä mainostajan verkkosivustolle (Adobe 2022). Tietojenkalastelijat sisällyttävät näihin näyttömainoksiin haittaohjelmia ja linkkejä väärennetylle verkkosivulle, joka on räätälöity muistuttamaan esimerkiksi lähettipalvelun sisäänkirjautumissivuja (Kuva 8). Tietojenkalastelijat ovat aktiivisia myös sosiaalisen median alustoilla ja Discordin kaltaisilla suoratoistopalveluiden keskustelupalstoilla, missä he hyödyntävät tyypillisiä suostutteluperiaatteita uhrin toiminnan ohjaamiseksi (Abdul 2022).

”Spooffaus” tai suoraan käännettynä huijaus on menetelmä, jossa hyökkääjä väärentää sähköpostin verkkotunnuksen, ja luo näin vaikutelman täysin turvallisesta sivusta, mikä on tehty näyttämään mahdollisimman paljon autenttiselta verkkosivulta. Hyökkääjä voi muun muassa väärentää Lähettäjä-otsikkokentän (from) saadakseen sen näyttämään aidolta. Tällä viestillä yritettiin huijata vastaanottaja napsauttamaan salasanan vaihto -linkkiä ja luopumaan valtuustiedoistaan (Microsoft 2022).



Kuvio 9. Väärennetty sähköposti, Microsoft, 2022.

”Paha kaksonen” (eng. Evil Twin) -hyökkäyksessä (Kuvio 10) hyökkääjä naamio verkkoasemansa tunnuksen muistuttamaan esimerkiksi julkisen WiFi-verkon tunnusta (Chaudhary 2016, 22). Harva ihminen tarkistaa julkiseen WiFi-verkkoon kirjautuessaan, että verkko on autenttinen, joten tietojenkalastelijoille ”pahaan kaksoseen” kirjautuvat uhrit tarjoavat tiedustelumateriaalia ja arvokasta dataa, jota tietojenkalastelijat käyttävät joko tietojenkalastelussa tai kohdennetuissa hyökkäyksissä tulevaisuudessa. Paha kaksonen on hyvä esimerkki hyökkäysmetodista, mikä ottaa huomioon ihmisten taipuvuuden luottaa (lauma-ajattelu) ja omaksua itselle mukavaa tietoa (miellyttävyysheuristiikka).



Kuvio 10. Paha kaksonen tietojenkalastelussa (Chaudhary, 19).

Tietojenkalastelua käsitellessä on tärkeää muistaa, että tietojenkalastelu ei tapahdu ainoastaan verkossa. Tietomurtoja tekevät henkilöt hyödyntävät myös työkaluja kuten muistitikkuja kohteen laitteiden saastuttamisessa, ja keinon teho perustuu ihmisten luontaiseen uteliaisuuteen (Chaudhary 2016, 23). Fyysinen tietojenkalastelu vaatii enemmän osaamista ja vuorovaikutustaitoja, mutta mikäli kohdeyrityksellä ei ole esimerkiksi kulunvalvontaa yrityksen tiloissa, tietojenkalastelija voi melko huoletta kävellä työasemille ja vaihtaa käyttäjän muistitikun haitta- ja vakoiluohjelmia sisältävään muistitikkuun.

3.4 Suojautuminen ja ennaltaehkäisy

Tietojenkalastelun ennaltaehkäisy on äärimmäisen vaikeaa, koska Internet mahdollistaa erittäin laajan taustatutkimuksen tekemisen kohteesta, ja sosiaalisen median ansiosta jaamme enemmän tietoa elämästämme kuin koskaan. Tilannetta ei auta tietoteknisen osaamisen puute, mikä koskee suurta osaa henkilöstöstä pienissä ja keskisuurissa yrityksissä (Pham ym. 2019, 11–12), mikä vuorostaan altistaa organisaatioita tietomurroille.

Yksittäisten ihmisten olisi hyvä harkita tarkkaan kaikkea tietoa, mitä he itsestään verkkoon jakavat sekä välttää tarpeetonta tiedostojen lataamista ja kiinnittää erityistä huomiota sähköposteihin, jotka sisältävät nopeaan toimimiseen kannustavia lauseita

(Investigation 2021). David Gragg suosittelee ohjeessaan organisaatiota aloittamaan tietoturvansa toteutuksen paikantamalla tietoja, kommunikaatioväyliä sekä muita asioita, jotka ovat ehdottomasti tarkoitettu ainoastaan organisaation henkilöstölle (Gragg 2003, 11). Mikään ei kuitenkaan osoita, että tällainen kanavien tarkastelu olisi mahdotonta toteuttaa yksilön tasolla, ja monet meistä pystyvät varmasti tunnistamaan, mitä laitteita pitkin emme ole tai emme halua olla tavoitettavissa työasioiden merkeissä.

Tutkijat Alghenaim, Bakar ja Rahim arvostelivat artikkelissaan Anti-Phishing Tools: State of the Art and Detection Efficiencies erilaisia ohjelmia, jotka on suunniteltu tai ovat sovellettavissa tietojenkalastelua vastaan. Tutkijoiden lopullinen johtopäätös oli, että mitä tarkempia torjuntatyökalut ovat, sitä enemmän ne auttavat parantamaan käyttäjien kykyä tunnistaa tietojenkalastelulähteet ja reagoida nopeasti mahdollisiin hyökkäyksiin (Alghenaim & Bakr & Rahim 2022, 3–4). Tutkijat tulivat samaan lopputulokseen kuin Toikkanen, joka huomasi jatkuvan koulutuksen suuren vaikutuksen henkilön kykyyn tunnistaa haitallisia tietojenkalasteluviestejä (Toikkanen 2020, 48–50).

Alghenaim, Bakar ja Rahim listasivat maksullisia työkaluja, joiden tavoitteena on auttaa yksittäistä työntekijää tunnistamaan haitalliset verkkosivut ja sähköpostit. SpoofGuard ja VIPRE Safesend ovat työkaluja, jotka eivät vaadi työnantajan osallistumista, ja ovat näin ollen sopivia tämän työn tarkoitukseen, mutta näiden käyttöön pitää luonnollisesti hakea suostumus työnantajalta tai yrityksen tietoturvavastaavalta selainlaajennusten tai muiden ohjelmien asentamiseen. Työntekijän on hyvä myös tiedostaa näiden välineiden rajoitukset ja heikkoudet, joita kyberrikolliset käyttävät tulevaisuudessa näiden ohjelmien ohittamiseen.

SpoofGuard on selainlaajennus, joka varoittaa käyttäjää, mikäli hän on väärennetyllä sivustolla. Väärennetyt sivustot ovat nimensä mukaisesti haitallisia verkkosivuja, joita tietojenkalastelijat käyttävät kirjautumistietojen keräämiseen esimerkiksi verkkopankin käyttäjiltä. Kalastelijat käyttävät näitä tietoja oikealle sivustolle siirtymiseen ilman, että palveluntarjoajat huomaavat mitään epäilyttävää (Stanford Security Lab 2023).

VIPRE Safesend on maksullinen sähköpostiin liitettävä ohjelma, joka tarkistaa viestin lähettäjän autenttisuuden. Safesend torjuu näin yhtä tietojenkalastelun yleisimmistä keinoista (kollegaksi tekeytyminen) ja analysoi samalla viestissä olevia liitetiedostoja. Safesendin käyttäjä voi myös kustomoida ohjelmaa tunnistamaan ja varoittamaan käyttäjää salassa pidettävän tiedon vahingossa lähettämisestä (Vipre 2023).

Valveutuneet tai muuten tietoturvansa parantamisesta kiinnostuneet työntekijät voivat myös itse hakea tietoa tietojenkalastelusta. Internet on lähteenä paikoin epäluotettava, ja tietoa ei ole aina saatavilla suomeksi. Kotimaiset viranomaiset ja ministeriöiden alaisena toimivat tutkimuslaitokset julkaiset koulutusmateriaaleja tietoturvasta yksilöille ja organisaatioille.

Kuluttajaliitto ja Kyberturvallisuuskeskus jakavat säännöllisesti tutkimus- ja koulutusmateriaalia tietoturvallisuudesta suomalaisille. Kuluttajaliiton vuonna 2021 laatima koulutuspaketti *”Näin tunnistat digihuijauksen”* sisältää esimerkkejä ja suojautumistapoja erilaisilta huijauksilta (Kuluttajaliitto 2021). Huijausviesteiltä suojautumiseksi Kuluttajaliitto suosittelee hyödyllisiksi havaittuja sääntöjä:

1. Muista, että organisaatiot kuten pankit eivät koskaan kysy sinulta tunnuslukuja tai salasanoja.

2. Tarkista viestin lähettäneen henkilön sähköpostiosoite. Mikäli osoite on tuntematon, vältä linkkien/tiedostojen avaamista ennen kuin varmistut alkuperästä.

3. Sisältääkö viesti painostamista tai muuta ohjailua?

4. Kysy itseltäsi, miksi juuri sinuun on otettu yhteyttä. Kuulostaako viestin sisältö liian hyvältä ollakseen totta?

Seuraamalla näitä ohjeita työntekijä voi tehdä valtavan muutoksen työpaikkansa tietoturvaan. Tietojenkalastelijat pyrkivät tyypillisesti käyttämään suostutteluperiaatteita ja kognitiivisia harhoja, jotta kalastelun uhri ei tiedostaisi epäilyttäviä pyyntöjä tai käskyjä. Tietojenkalastelun torjuminen vaatii yrityksen henkilöstöltä ennaltaehkäisevää toimintaa sosiaalisen median kanavilla, mutta myös harjoittelun ja teknisten työkalujen yhteensovittamista.

3.5 Tulevaisuudennäkymiä

Työn aikana vuosien 2000–2022 ajalta kerätty tutkimustieto osoittaa, että tietojenkalastelua ei ymmärretä niin hyvin kuin pitäisi. Tietojenkalastelua ei ole tutkittu yhtä paljon kuin hakkerointia ja muita tietomurtoja, ja tämä näkyy edelleen paikoittaisena tietojenka-

lastelun aliarviointina. Tulevaisuudessa työnantajien voidaan olettaa panostavan enemmän viestinnän ja vuorovaikutuksen koulutukseen, koska nykyiset koulutusmetodit eivät vaikuta tehokkailta tietojenkalastelulta suojautumisessa.

Kyberturvallisuuskeskus arvioi katsauksessaan myös vuoden 2022 aikana tapahtuvaa kehitystä tietoturvallisuuden kannalta. Keskuksen tutkijat arvioivat, että vuoden 2022 aikana lainsäätäjät Euroopan Unionissa tulevat ulottamaan lisää sääntelyä digitaalisten palveluiden pelisääntöihin ja tekoälyyn tarkoituksenaan tehdä älylaitteista ja datan hallinnasta turvallisempaa (Kyberturvallisuuskeskus 2022, 26). Tietojenkalastelun kannalta tämä tarkoittaa, että työntekijöiden tietoturvaohjeistuksia joudutaan todennäköisesti päivittämään miltei kaikissa organisaatioissa, jotta EU:n lakisääteiset vaatimukset täyttyisivät.

Kyberturvallisuuskeskuksen katsaus tuo myös esiin teknisten välineiden kehityksen ja niiden vaikutuksen tietomurroilta suojautumiseen. Tekoälyn hyödyntäminen tietojenkalastelussa ja tietomurroissa yleisesti tulee todennäköisesti kasvamaan, koska tekoälyn avulla kyberrikolliset pystyvät vakuuttavasti automatisoimaan toimintaansa tehokkaammaksi ja vakuuttavammaksi (Kyberturvallisuuskeskus 2022, 27). Kyberturvallisuuskeskus päätyy myös samaan johtopäätökseen kuin tietoturvan asiantuntijat, jotka ovat jo pitkään puhuneet tietoturva-ammattilaisten osaajapulasta Suomessa, joten tulevaisuudessa näitä ammattilaisia tarvitaan lisää.

Tietojenkalastelun torjumiseen ja tutkimiseen pitää panostaa merkittävästi lisää. Vuosi 2022 oli täynnä pieniä ja suuria tietomurtoja, ja organisaatioiden nykyiset työkalut tietojenkalastelua vastaan eivät toimi tarpeeksi tehokkaasti. Jatkuvalla koulutuksella on positiivinen vaikutus tietojenkalastelua vastaan, mutta tietojenkalastelun torjuminen vaatii myös henkilöstön valistamista ja aktiivista kehitystyötä (Toikkanen 2020, 62–63).

4 Ohjeen laatiminen

Ohjeen laatiminen aloitettiin kirjallisuuteen ja tietoon perehtymällä. Teoreettisen tiedonkeruun jälkeen aloitettiin tarpeettomien tai työn tarpeiden kannalta epäoleellisten lähteiden karsiminen. Lopuksi tehtiin ohjaajan palautteen mukaiset korjaukset ja tarkennukset ohjeeseen ja opinnäytetyön raporttiosuuteen.

Aineiston keruun aikana kävi selväksi, että työntekijöiden tietämys tietojenkalastelusta ja sen riskeistä ei ole ajantasaista. Chaudhary reflektoi työssään aikaisempaa tutkimusmateriaalia ja kirjallisuutta tietojenkalastelun vastakeinoista ja huomasi, että koulutettujenkin työntekijöiden tietämys tietojenkalastelusta oli hälyttävän alhaista (Chaudhary 2016, 63–64). Tilanne voi kehittyä parempaan suuntaan, mutta organisaatioiden ja oppilaitosten haluttomuus tarjota koulutusta aiheesta on kasvava ongelma (Chaudhary 2016, 65).

Ohjeen laatimisessa käytetty teoreettinen aineisto osoitti, että tietojenkalastelijat hyödyntävät tiettyjä psykologisia keinoja uhrien hämäämiseksi. Tutkijat Ferreira, Coventry ja Lenzini kokivat, että yleisten suostutteluperiaatteiden kategorisointi ja listaaminen olisivat hyödyllinen lisäys tulevia tutkimuksia silmällä pitäen (Ferreira & Coventry & Lenzini 2015, 44–45). Päätin koota listan suostutteluperiaatteista ohjetta varten, koska koin, että näiden keinojen listaaminen hyödyttäisi myös yksittäistä työntekijää, ja tarjoaisi samalla konkretiaa, jota tietotekniikkaa vähemmän tuntevat henkilöt kaipaavat.

Listojen lisäämisen on myös tarkoitus palvella työntekijää tietoisuuden lisäämisen kannalta. Siponen määritteli jo vuonna 2000 tietoisuuden lisäämisen tavoitteeksi käyttäjälähtöisten vikojen minimoimisen (Siponen 2000, 31). Hoppe, Gatzert ja Gruner havainnoivat saman todetessaan, että nykyisin pienten ja keskisuurten yritysten ongelmat tietoturvallisuuden kannalta liittyivät pitkälti organisaatioiden turvallisuuskulttuurien puutteisiin riskitietoisuuden, tietoisuuden ja asenteen kannalta (Hoppe & Gatzert & Gruner 2021, 253). Esittelemällä suostutteluperiaatteet pyrin lisäämään työntekijän tietoisuutta tietojenkalastelusta ilmiönä ja keinoista, joita siinä käytetään.

Tietoisuuden lisäämiseksi sisällytin ohjeeseen myös kuvalliset selitykset kolmelle yleisimmälle tietojenkalastelumetodille. Lisäsin ohjeeseen esimerkin ”Pahan Kaksosen” käytöstä lähinnä työntekijän valistamiseksi, koska etätyökulttuurin takia monet meistä tekevät töitä etänä 2–3 päivää viikossa. Kahvilassa tai kirjastossa työskentelevät ihmiset eivät välttämättä tiedä tästä julkisten verkkojen sisältämästä riskistä, joten koin sen hyödylliseksi lisäksi ohjeeseen.

Tietoturvallisuuden ja koulutuksen kannalta oli myös tärkeää pitää ohje mahdollisimman selkeänä ja yksinkertaisena. Niina Kinnunen toteaa väitöskirjassaan, että yritysten ja julkisten toimijoiden tarjoamat ohjeistukset sisältävät usein vaikeaselkoista ja teknisillä termeillä täytettyä tekstiä (Kinnunen 2015, 169). Ohjeen piti myös olla käyttäjäystävällinen, koska yritysten työntekijät käsittelevät satoja sähköposteja päivittäin, joten edellä mainittu tarkistuslista piti tiivistää yhteen tai kahteen sivuun (Toikkanen 2020, 60–61).

5 Tietojenkalastelu ja siltä suojautuminen -ohje

Ohjeen rakenne on jaettu käsitteisiin, hyökkäysvariaatioihin ja suojautumiskeinoihin. Ohjeen tavoitteena on vastata kysymyksiin mitä ja miten sekä lopuksi tarjota keinoja tietojenkalastelua vastaan. Ohjeen rakenne määrittyi helppokäyttöisyyden ja ohjaajalta saadun palautteen perusteella.

Ohje alkaa tietojenkalastelun ja keskeisten psykologisten keinojen määrittelemisellä, jotta lukija saa alustavan käsityksen tietojenkalastelusta ja sen metodeista. Esimerkki tietojenkalasteluviestistä on sijoitettu psykologisten keinojen alle, jotta lukijalle jäisi mahdollisimman tuore muistikuva näistä keinoista ennen tietojenkalasteluvariaatioiden esittelyä. Näin pyrin luomaan asiayhteyksiä ohjeen lukijan muistiin.

Ohje keskittyy tietojenkalastelusähköposteihin (phishing), tekstiviesteihin (smishing) ja puhelimen välityksellä tehtyyn tietojenkalasteluun. Ohje sisältää myös maininnan ”pahan kaksosen” käyttämisestä, koska julkisten verkkojen vaarallisuus ei ole välttämättä yhtä tunnettua kuin edellä mainitut kalastelukeinot. Ohjeeni keskittyy näihin hyökkäysvariaatioihin niiden yleisyyden takia.

Alun perin ohje sisälsi enemmän teoriaa aiheesta, mutta tämä rakenne ei palvellut ohjeen käytettävyyttä, joten jätin ohjeeseen ainoastaan työntekijälle oleellisen tiedon. Ohjeen viimeinen sivu sisältää kehotuksen lukea tämä opinnäytetyö, mikäli lukija on kiinnostunut aiheesta tarkemmin. Näin työlle oleellinen tieto välittyy lukijalle ja ohje itse pysyy mahdollisimman tiiviinä ja käyttäjäystävällisinä.

Ohjeen viimeinen osa sisältää tarkistuslistan viestinnän tarkentamista varten. Listat ovat ohjeen pääasiallinen ”työkalu” tietojenkalastelua vastaan, ja niitä on tarkoitus käyttää työntekijän päivittäisessä työskentelyssä. Tarkistuslistojen on myös tarkoitus harjaannuttaa työntekijää yleisimpien psykologisten keinojen havaitsemiseen toiston kautta.

Ohje sisältää myös ohjeita sosiaalista mediaa varten. Epäilyttävän viestinnän sijasta tämä osio keskittyy ainoastaan yksityisyysasetuksien muokkaamiseen, koska useat tutkijat mainitsivat sosiaalisen median käytön osana kalastelijoiden tekemää tiedustelua. Kalastelijoiden toimintaa on mahdollista vaikeuttaa varmistamalla, että työntekijän seuraajat/kaverit sosiaalisessa mediassa ovat ainoastaan tuttuja tai muuten turvallisia henkilöitä.

Alkuperäisessä ohjeessa viestinnän tarkistuslistoja oli useampia, mutta ohjaajalta saadun palautteen jälkeen päädyin yhdistämään viestien ja puhelujen tarkistuslistat, koska toimintaohjeet mainittuihin tilanteisiin olivat pitkälti samat. Listat on laadittu aineistossa esiintyvien psykologisten keinojen perusteella, ja ne keskittyvät suostutteluperiaatteisiin ja kognitiivisiin harhoihin.

Ohjeen kohderyhmäksi valikoituivat pienten ja keskisuurten yritysten työntekijät, joiden tietoteknisen osaamisen oletetaan olevan matalaa mahdollisen matalan koulutustason takia. Ohjeen aikaisempien versioiden kriittisen tarkastelun jälkeen päädyin muokkaamaan ohjeen tekstiä käyttäjäystävällisemmäksi. Ongelma ratkaistiin tekstin virkamiesmäisyyden poistamisella tai tiivistämisellä sekä lukijan suoran puhuttelun avulla.

Ohjeesta poistettiin myös aiemmissa versioissa olleet linkit viranomaisten raportointisivuille, koska ne voivat olla ristiriidassa yritysten omien tietoturvaohjeistuksien kanssa. Linkit poistettiin ohjeesta myös siksi, että ohjeen on tarkoitus keskittyä tietojenkalastelun ennaltaehkäisyyn mahdollisen tietovuodon raportoinnin sijasta. Ohjeeseen jätettiin linkit verkkotunnuksien ja sähköpostien varmentamista varten, mutta samalla ohjeessa muistetaan mainita, että nämä työkalut eivät itsessään riitä lähettäjän tai verkkosivun turvallisuuden varmistamiseen.

6 Yhteenveto

6.1 Työn tavoitteiden toteutuminen

Työn laajuutta kavennettiin työskentelyn aikana, jotta työn toiminnallinen osuus (ohje) onnistuisi työntekijöiden valistamisessa tietojenkalastelusta. Lopullinen tuotos soveltuu työntekijän päivittäisen viestinnän tarkistamiseen työssä olevien listojen avulla, mutta toimeksiantajan puuttumisen takia ohjeen tehokkuus käytännössä on epäselvää. Ohje sisältää aineistonkeruun aikana havaitut tärkeimmät psykologiset periaatteet (suostutteluperiaatteet) sekä selitykset näille periaatteille.

Työn alkuperäinen tarkoitus muuttui työskentelyn aikana paljon. Alun perin työn piti käsitellä tietojenkalastelua ja siltä suojautumista myös organisaation näkökulmasta, mutta ohjaajalta saatu palaute osoitti, että työn pitäisi keskittyä vain yksittäisen työntekijän nä-

kökulmaan. Nykyinen työ soveltuu pienten ja keskisuurten yritysten työntekijöitten päivittäiseen työskentelyyn, ja sitä voidaan käyttää perustana monipuolisemman ohjeistuksen tekemiseen.

6.2 Oman toiminnan arviointi

Opinnäytetyöprosessi aloitettiin vuoden 2021 alussa tavoitteena luoda ohje tietoturvauhkia vastaan pääkaupunkiseudun yrityksille. Ohjaajan kanssa käytyjen keskustelujen jälkeen päädyin rajaamaan työn aiheen tietojenkalasteluun pienissä ja keskisuurissa yrityksissä. Päätös kaventaa aihetta tehtiin, koska tietojenkalastelua haastavampien tietomurtojen käsittely vaatii monipuolista tietoteknistä osaamista.

Työ alkoi opinnäytetyöprosessille ominaisella suunnitteluvaiheella, missä työn aihetta ja tutkittavia asioita rajattiin käsiteltäviin kokonaisuuksiin. Työn suunnitteluvaiheessa työ oli alun perin tarkoitettu yrityksen työntekijöille ja yrityksen johdolle, mutta työn palautusvaiheessa kävi viimeistään selväksi, että palautettu työ ei palvele työntekijän tai työnantajan koulutusta ja valistusta tietojenkalastelusta. Joulukuun 2021 jälkeen työ oli jo myöhästynyt varsinaisesta palautuksestaan, mutta päätin silti korjata olemassa olevaa työtä, jotta lopullinen tuotos palvelisi työyhteisön tietoturvan kehittämistä.

Työ kärsi alusta loppuun suunnitelmallisuuden ja rakenteen puutteesta. Työn alkuvaiheessa tehty tiedonhaku tehtiin ilman kunnollista dokumentointia ja lähdekritiikkiä, ja tämä näkyi työssä katkeilevana ja asiayhteyksistä irrallisina argumentteina ja perusteluina. Työn merkittävimpiä haasteita oli löytää kotimaisia lähteitä työn tueksi, koska monet kotimaiset tutkijat ovat kirjoittaneet tietoturvallisuuden toteutuksesta yritystasolla yksittäisten työntekijöiden sijasta.

Isoin virhe työn teossa oli kuitenkin tiukkojen aikataulujen huomioimatta jättäminen. Työskentely tapahtui paikoin niin isojen aikavälien saattamana, että aikaisemmin kirjoitetut muistiinpanot olivat joko täysin hajanaisia, ja taustalla olleet ideat oppaan rakenteesta ja suunnasta saattoivat olla kokonaan unohdettu. Tämän takia työ valmistui vasta vuoden 2022 aikana, ja edelleen merkittävien puutteiden höystämänä.

Työn puutteiden korjaamiseksi priorisoin työn korjattavat osiot vuoden 2022 syksynä. Aloitin korjaamalla lähdekritiikkiä suodattamalla kritiikin läpäisemättömät lähteet pois työstä. Internet-lähteiden arvioinnissa käytin kuuden kohdan menetelmää, missä arvioin

lähteen auktoriteettia, tarkkuutta, objektiivisuutta, ajankohtaisuutta, kattavuutta ja ulkoasua.

Työn seurattavuuden parantamiseksi ja viimeistelyä varten aloitin päiväkirjan käyttämisen. Päiväkirja sisälsi päivämäärän, työskentelyn aloituksen kellonajan, tehtävät kyseisellä päivällä, lopetusajan sekä yhteenlasketun käytetyn ajan. Päiväkirja auttoi työskentelyn suunnittelussa ja tehtävien priorisoinnissa. Työhön lisättiin myös kotimaisia lähteitä, ja tietomurtojen ennaltaehkäisyä varten oppaaseen lisättiin konkreettisia keinoja parantaa henkilökohtaista suojausta tietojenkalastelua vastaan.

Työn lopulliset korjaukset tehtiin kevään 2023 aikana. Aikaisemmista korjauksista riippumatta työ kärsi edelleen puutteista lähdeviitteissä, lähdeluettelossa sekä tekstin sujuvuudessa. Korjauksia tehtiin edellä mainittuihin lähteisiin ja kappaleiden rakenteisiin.

7 Johtopäätökset ja kehittämiskohteet

Tekniset ratkaisut (virustentorjuntaohjelmat, sähköpostifiltterit ym.) eivät ole tarpeeksi tehokkaita ratkaisuja tietojenkalastelua vastaan. Tietojenkalastelun vahvuudet ovat olleet tiedossa jo vuosikymmeniä, mutta ihmisten kyky vastata niihin ei ole nähnyt merkittävää kehitystä. Toiminnallisen opinnäytetyöprosessin aikana olen lukenut tutkimuksia ja väitöskirjoja, jotka käsittelevät tietojenkalastelua niin hyökkääjän kuin kohteen näkökulmasta.

Merkittävää kehitystä tietojenkalastelua vastaan ei ole nähty, koska ongelman juurisyitä ei ole käsitelty asiaankuuluvalla tavalla. Monet yritykset panostavat paljon pääomaa, osaamista ja aikaa erilaisten turvallisuustoimien, ohjeiden ja ohjelmien kehittämiseen, mutta harva jos kukaan vaikuttaa panostavan psykologisten haavoittuvaisuuksien kouluttamiseen. Ihmiset tiedostavat yksinkertaisimmat hyökkäystavat, kuten tökerön ”afrikkalainen prinssi” huijauksen, mutta he samalla tuntuvat olettavan, että kehittyneemmät hyökkäysmetodit ja viestit on varattu vain valtiollisille toimijoille ja isoimpien organisaatioiden edustajille.

Valtavaa osaa ihmisten käytöksestä tietoverkoissa tuntuu ohjaavan lähinnä lauma-ajattelu, missä ihmiset tottuvat helposti huonoihin ratkaisuihin, ja näin sinetöivät huonoja ratkaisuja osaksi organisaation toimintakulttuuria. Tietämättömyyttä tietojenkalastelusta voi paikoin pahentaa myös ihmisten taipumus kohdella työpaikan työvälineitä ja laitteita

eri tavalla kuin kodin vastaavia. Ihmisillä on usein myös harhainen käsitys omasta merkityksestään tai sen puutteesta tietoturvan suhteen.

Yritysten ja laajemman yhteiskunnan on kaikkien panostettava tulevaisuudessa psykologian ja tietoturvan koulutukseen paljon. Nykyisellään koulutuksen ongelmia ovat aihealueiden ja termien vaikeus sekä koulutusmateriaalit, jotka eivät tue oppimista tarpeeksi hyvin. Organisaatioiden ja opintolaitosten olisi suotavaa lisätä yhteistyötään näillä aihealuilla, jotta voidaan luoda koulutusta ja osaamista, mikä ottaa huomioon tietoturvan inhimilliset elementit samalla luoden perustan tietotekniikan osaamiselle. Nykyinen osaajapula tietotekniikan kannalta ei ole toimiva pitkällä aikavälillä.

Ohje tarvitsee lisää syvyyttä ajankohtaisuuden ja tehokkuuden ylläpitämiseksi. Ohjeen hyöty perustuu tällä hetkellä käyttäjän omaan valppauteen, koska ohjeen varoituslistoista on hyötyä vain tilanteissa, joissa käyttäjän epäilykset heräävät jo yhteydenoton aikana. Ohjeen pitäisi näin ollen sisältää jonkinlaista ”asennevalmennusta” yksinkertaisten tarkistuslistojen sijasta, koska tietojenkalastelijat kehittävät jatkuvasti keinoja ohittaa alitajuntamme käyttämällä tässä opinnäytetyössä kohdattuja psykologisia menetelmiä. Ohjetta voisi kehittää erottelemalla tietotekniikan ja psykologian erillisiksi osioiksi samalla kumpaakin osa-aluetta täydentäen. Näin tekemällä ohjeen lukijaa koulutettaisiin enemmän ajattelutapaan mekaanisen suorituksen (tarkistukset) sijasta samalla täydentäen heidän tietoteknistä osaamistaan. Ohjeen myöhempi versio palvelisi näin myös kokeneempia ja tietoteknisesti taidokkaampia työyhteisöjä, mutta tämä lähestymistapa loisi uusia ongelmia tiedon omaksumisen kannalta.

Useat tutkijat havainnoivat, että nykyiset tietoturvakoulutusmateriaalit kärsivät juuri vaikeasti omaksuttavan ja paisuneen teorian määrästä, joten kehitetyn ohjeen pitäisi sisältää enemmän tietoa samalla pysyen verrattain lyhyenä. Pelkästään tekstiin perustuvan tiedoston sijasta ohje voisi olla vaikkapa virtuaalitodellisuuteen siirretty ohjelma, missä työntekijä harjoittelee joko yksin tai työtovereidensa kanssa tietojenkalastelun tunnistamista. Tällä tavalla ohje voisi onnistua paremmin työyhteisön ja yksittäisen käyttäjän tietoturvallisuuden parantamisessa.

Tietojenkalastelu on usein kohdennettu haavoittuvaisimpiin ihmisiin, joten luonnollisesti muistisairaiden ja mielenterveysongelmien kanssa kärsivien ihmisten kanssa työskentelevät lähihoitajat voisivat hyötyä ohjeistuksesta. Tällaisessa tilanteessa ohjeistuksen pitäisi olla entistä rajatumpaa, ja keskittyä ainoastaan turvalliseen netin käyttöön ja esimerkiksi asiakkaan (eläkeläisen) valistamiseen aiheesta. Muistisairauden luonteen takia

ohjeen tueksi olisi suotavaa laatia myös fyysisiä varoituskortteja, joita muistisairas henkilö voisi käyttää sähköposteja ja tekstiviestejä lukiessaan.

Yleisesti ottaen suuri osa ammattikunnista hyötyisi paljon tietojenkalastelun vastaisesta ohjeistuksesta, koska tietojenkalastelua tehdään monella eri toimialalla. Erityisesti henkilötietoja ja pankkitunnuksia käsittelevät työntekijät (sosiaalityöntekijät, pankkivirkailijat, omais- ja lähihoitajat jne.) tulevat tarvitsemaan työkaluja tietojenkalastelun tunnistamiseen, koska tekniset keinot huijausten toteuttamiseen kasvavat kiihtyvällä tahdilla. Yhtenäistä koulutusta, mikä toimisi kaikille näille ammattikunnille, ei kuitenkaan todennäköisesti ole mahdollista luoda.

Lähteet

Abdul, Shan 2022. What Is the Discord Name and Shame Scam? How to Avoid It. Make Use Of 16.10.2022. https://www.makeuseof.com/discord-name-and-shame-scam/. Luettu 24.11.2022.

Adobe. Web banner design ideas and inspiration. 2022. https://www.adobe.com/express/learn/blog/web-banner-design-ideas-and-inspiration. Luettu 10.2.2023.

Alghenaim, Mohammed & Bakar, Nur & Rahim, Fiza 2022. Anti-Phishing Tools: State of the Art and Detection Efficiencies. Applied Mathematics & Information Sciences 16(6), 929–934.

American Psychological Association. Cognition. 2022. https://dictionary.apa.org/cognition Luettu 19.4.2022

American Psychological Association. Learned helplessness. 2022. https://dictionary.apa.org/learned-helplessness Luettu 7.4.2022

American Psychological Association. Manipulation. 2022. https://dictionary.apa.org/culture Luettu 12.4.2022.

American Psychological Association. Motivation. 2020. https://dictionary.apa.org/motivation. Luettu 24.5.2021.

Anti-Phishing Working Group. 2021. Anti-Phishing Working Group. Päivitetty 8.6.2021. https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf Luettu 23.11.2022.

Antonucci, Domenic 2017. The Cyber Risk Handbook : Creating and Measuring Effective Cybersecurity Capabilities, John Wiley & Sons, Incorporated, New Jersey.

Brown, Steven 2020. Successful Cybersecurity Professionals. How to Change Your Behavior to Protect Your Organization. Business Expert Press, New York.

Cambridge Dictionary. Cognitive bias. 2022. https://dictionary.cambridge.org/dictionary/english/cognitive-bias Luettu 25.11.2022

Chaudhary, Sunil 2016. The Use of Usable Security and Security Education to Fight Phishing Attacks. Tampereen yliopisto, Tampere.

Edwards, Matthew & Williams, Emma & Peersman, Claudia & Awais, Rashid 2022. Characterising Cybercriminals: A Review. https://arxiv.org/pdf/2202.07419.pdf. Luettu 21.3.2022

Encyclopaedia Britannica. Persuasion. 2021. https://www.britannica.com/science/persuasion-psychology Luettu 19.5.2021.

Europol. Internet Organized Crime Threat Assessment. 2021. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf. Luettu 28.11.2021

Federal Bureau of Investigation. Business Email Compromise. 2021. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise. Luettu 10.5.2021.

Ferreira, Ana & Coventry, Lynne & Lenzini, Gabriele 2015. Principles of Persuasion in Social Engineering and Their Use in Phishing. 17th International Conference on Human Computer Interaction 9190, 36–47.

F-Secure. Mitä on tietojenkalastelu?. 2023. https://www.f-secure.com/fi/articles/what-is-phishing. Luettu 20.11.2022.

Furnell, Steven & Dowling, Samantha 2019. Cyber crime: a portrait of the landscape. Journal of criminological research, policy and practice 5, 13–26.

Hadnagy, Christopher & Fincher, Michele & Dreeke, Robin 2015. Phishing Dark Waters. The Offensive and Defensive Sides of Malicious Emails. John Wiley & Sons Incorporated, Indianapolis.

Hoppe, Felicitas & Gatzert, Nadine & Gruner, Petra 2021. Cyber risk Management in SMEs: insights from industry surveys. The Journal of Risk Finance 22, 240–260.

Jones, Keith & Armstrong, Miriam & Tornblad, McKenna & Namin, Akbar 2020. How social engineers use persuasion principles during vishing attacks. Information and Computer Security 29, 314–331.

Kantomaa, Raija 2021. Oikeuden paperit paljastavat: Näin Vastaamon tietomurto tapahtui – salainen kauppasumma paljastui. MTV Uutiset 08.02.2021. https://www.mtvuutiset.fi/artikkeli/oikeuden-paperit-paljastavat-nain-vastaamon-tietomurto-tapahtui-salainen-kauppasumma-paljastui/8055050. Luettu 25.5.2021.

Kemppi, Janiko. Tilisi yritetään tyhjentää – näin rikolliset lähestyvät nyt suomalaisia. Iltalehti 11.1.2021. https://www.iltalehti.fi/tietoturva/a/94f3d4d7-b0e1-49d8-af2d-5a010ced710b. Luettu 22.2.2022.

Kinnunen, Niina 2015. Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen. Vaasan Yliopisto, Vaasa.

Kolttola, Ilari & Näsi, Matti 2022. Suomalaiset väkivallan ja omaisuusrikosten kohteena 2021: Kansallisen rikosuhritutkimuksen tuloksia. Katsauksia 51, Helsingin Yli-opisto, Helsinki.

Kuluttajaliitto. Tunnista digihuijaus – koulutuspaketti itseopiskeluun. 2021. https://www.kuluttajaliitto.fi/materiaalit/tunnista-digihuijaus-koulutuspaketti-itseopiskeluun/. Luettu 18.11.2022.

Kyberturvallisuuskeskus. Kyberturvallisuus elää kasvun aikaa – torjumme häiriöitä ennakolta. 3.2022. Traficom Julkaisu. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2021.pdf. Luettu 11.4.2022.

Mann, Ian 2008. Hacking the Human : Social Engineering Techniques and Security Countermeasures. Taylor & Francis Group, Hampshire.

MDN Web Docs. Your blueprint for a better internet. 2023. Mozilla Foundation. https://developer.mozilla.org/en-US/about. Luettu 30.4.2022.

Microsoft. Anti-spoofing protection in EOP. 25.3.2022. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-spoofing-about?view=o365-worldwide. Luettu 28.3.2022.

Moinescu, Radu & Răcuciu, Ciprian & Glăvan, Dragos & Antonie, Narcis-Florentin & Eftimie, Sergiu 2019. Aspects of human weaknesses in cyber security. Scientific Bulletin of Naval Academy 22, 163–170.

MTV Uutiset. Aikajana Vastaamo-kohusta: Tietomurto vei "psykoterapiapalveluiden Onnibussilta" kymmenientuhansien ihmisten tiedot – tämä tapauksesta toistaiseksi tiedetään. 2020. https://www.mtvuutiset.fi/artikkeli/tietomurto-vei-psykoterapiapalveluiden-onnibussilta-kymmenientuhansien-ihmisten-tiedot-tama-tapahtumien-kulusta-toistaiseksi-tiedetaan/7966596. Luettu 25.5.2021.

Northern Michigan University. Evaluating Internet Sources. 2018. Lydia M. Olson Library. https://lib.nmu.edu/help/resource-guides/subject-guide/evaluating-internet-sources. Luettu 20.11.2022.

Ollman, Gunter 2007. The Vishing guide. https://nsi.org/ReferenceLibrary/599.pdf. Luettu 11.12.2021

Pham, Hiep Cong & Brennan, Linda & Parker, Lukas & Phan-Le, Nhat Tram & Ulhaq, Irfan & Nkhoma, Mathews Zanda & Nhat Nguyen, Minh 2020. Enhancing cyber security behavior: an internal social marketing approach. Information & Computer Security 28, 133–159.

Rogers, Marcus 2006. A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation 3, 97–102.

Safesend. Vipre. 2023. https://vipre.com/products/email-security/safe-send-software-outlook/. Luettu 25.3.2023.

SANS Institute. A Multi-Level Defense Against Social Engineering. 2002. https://sansorg.egnyte.com/dl/AbCFV3mA3o. Luettu 3.6.2021.

Scams and Safety. Business Email Compromise. 2021. Federal Bureau of Investigation. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise. Luettu 18.5.2021.

Siponen, Mikko 2000. A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8, 31–41.
Spoofguard. Stanford Security Lab. 2023. https://crypto.stanford.edu/SpoofGuard/. Luet-tu 14.2.2023

Stajano, Frank & Wilson Paul 2011. Understanding scam victims: seven principles for systems security. Communications of the ACM 54 (3), 70–75.

Toikkanen, Perttu 2020. Tietojenkalastelusimulaationa järjestetyn koulutuksen vaikutus työntekijöiden kykyyn tunnistaa sähköpostin kautta tulevia tietojenkalasteluviestejä. Pro Gradu -tutkielma. Vaasan Yliopisto. https://osuva.uwasa.fi/bitstream/handle/10024/11244/Perttu%20Toikkanen%20Pro%20Gradu%20PDF.pdf?sequence=2&isAllowed=y. Luettu 11.11.2022

Vuoksimaa, Eero 2019. Kognitiivisten toimintojen muutokset - mikä on ikääntymistä, mikä sairautta? Lääketieteellinen aikakauskirja Duodecim 135 (11), 1075–1084.

Liite 1 Ohje

Tietojenkalastelu ja siltä suojautuminen

Jaakko Kemppainen, Liiketalouden tutkinto-ohjelma

Mitä tietojenkalastelu on?

Tietojenkalastelu tarkoittaa toimintaa, jossa hyökkääjä huijaa käyttäjän avaamaan haitallisen linkin tai sähköpostiliitteen naamioimalla ne kiinnostavaksi sisällöksi. Tietojenkalastelu hyödyntää **psykologisia malleja** sekä yleisiä **kognitiivisia harhoja**. Tietojenkalastelu on uhka meille kaikille ja tämän ohjeistuksen tarkoituksena on valistaa sinua tietojenkalastelusta, sen eri variaatioista, ja torjumisesta.

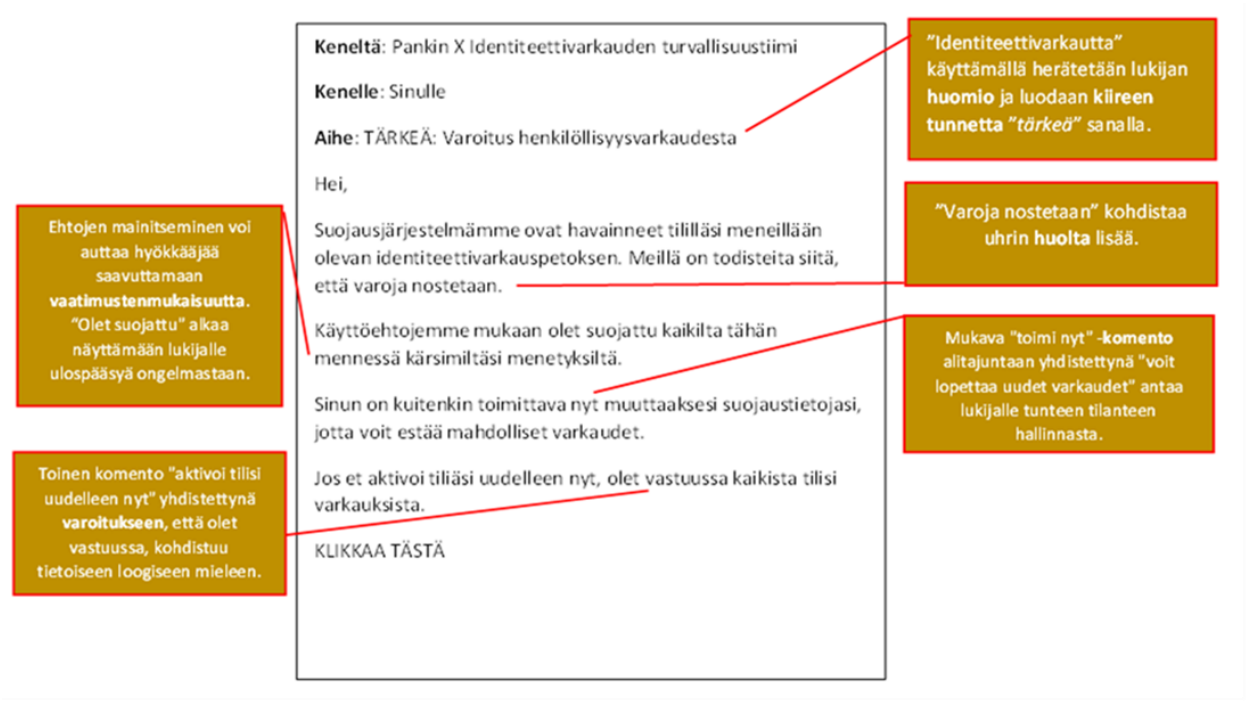
Kuvassa on tyypillinen roskapostiin joutunut **tietojenkalasteluviesti**. Tietojenkalastelua tekevät pääosin kyberrikolliset, mutta myös organisaation sisällä olevat pahantahtoiset työntekijät voivat syyllistyä siihen.

Miten sitä tehdään?

Onnistuakseen kalastelijat kääntävät mielenmaisemasi ja ajattelutapasi sinua vastaan. Suuri osa meistä reagoi tietyllä tavalla samoihin tilanteisiin, ja kalastelijat käyttävät tätä tietoa vaikuttaessaan valppauteesi ja keskittymiskykyysi. Alla muutama esimerkki näistä keinoista:

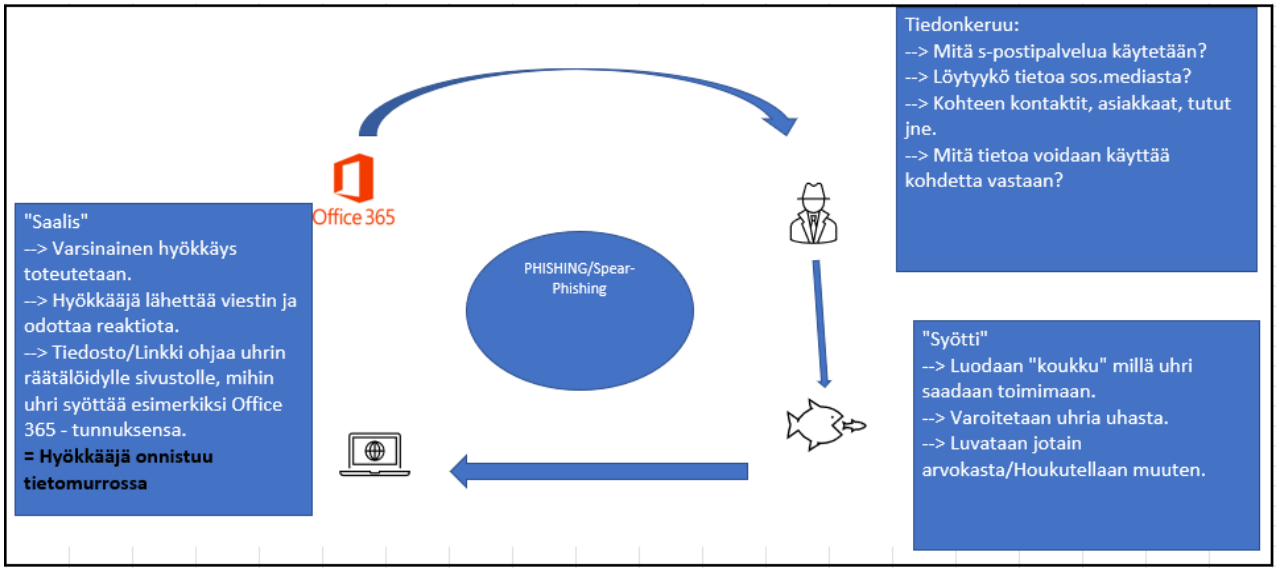
Häiriö
➔ Huomiosi kiinnitetään johonkin epäoleelliseen, jotta hyökkääjä onnistuu tietomurrossa
Auktoriteetti
➔ Hyökkääjä esiintyy auktoriteetin omaavana henkilönä, kuten vuoropäällikkönä tai jossakin muussa sinua korkeammassa asemassa kohdeorganisaatiossa.
Lauma-ajattelu
➔ Sinua houkutellaan toimimaan samalla tavoin kuin muutkin.
Epärehellisyysperiaate
➔ Sinua huijataan osaksi rikollista toimintaa, jolloin kynnys murrosta ilmoittamiseen nousee.
Ystävällisyys
➔ Hyökkääjä esiintyy apua tarvitsevana henkilönä ja saa käytöksellään sinut laskemaan varauksesi häntä kohtaan.
Tarve ja Ahneus
➔ Hyökkääjä hyödyntää sinun halujasi ja tarpeitasi, ja pyrkii ahneuden avulla saamaan sinut unohtamaan maalaisjärkesi
Aika
➔ Hyökkääjä uskottelee sinulle, että nyt on kiire korjata jokin ongelma tai että sinulla on rajallinen tilaisuus valtaviin rahasummiin tai rakkauden löytämiseen.

Alla on esimerkki tyypillisestä sähköpostista, jota käytetään tietojenkalasteluun. Viestistä on nostettu esiin sanamuotoja, joita tyypillisesti käytetään tietojenkalastelussa.



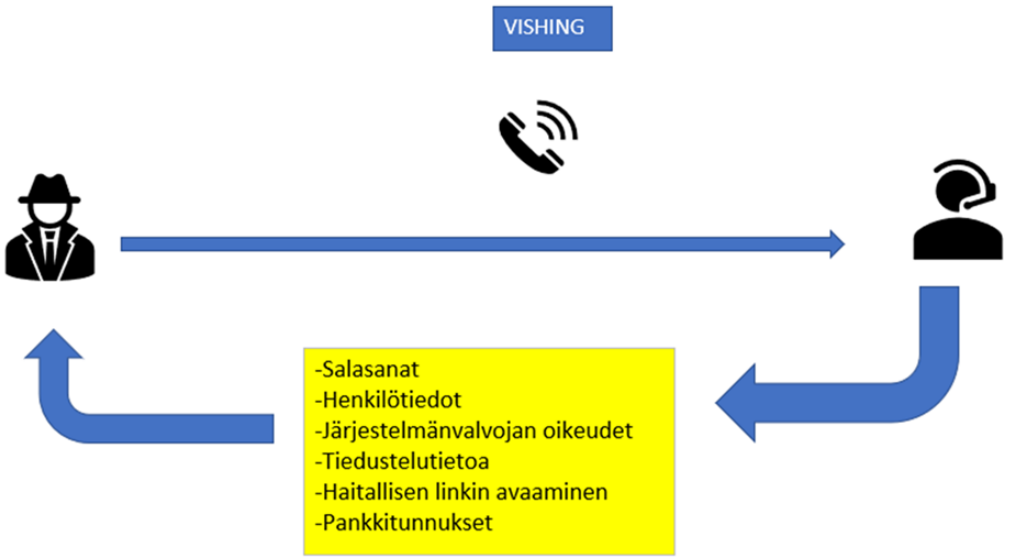
Tietojenkalastelua voidaan tehdä sähköpostien, puhelinten, tekstiviestien ja verkkoasemien avulla. Alla muutama esimerkki:

1. Phishing/Tietojenkalastelusähköposti



Tämä on yleisin ja petollisin tietojenkalastelukeino. Ohjeen alussa esitelty viesti oli esimerkki Phishingistä. Tietojenkalastelu noudattaa kuvassa esitettyjä kolmea vaihetta: tiedonkeruu, koukku, ja koppi. Menetelmää käytetään usein **käyttäjätietojen** varastamiseen, mukaan lukien **kirjautumis-tiedot** ja **luottokorttinumerot**.

2. Vishing/Puhelinkalastelu



Vishing tai **puhelinkalastelu** on kuten sen nimi viittaa puhelimella tehtyä **tietojenkalastelua**. Tietojenkalastelija soittaa sinulle, ja sanoo olevansa Martti Bärgström ylemmästä johtoportaasta. Martti vaatii sinua luovuttamaan palkanlaskun käyttämän Excel-tiedoston salasanan, ja hän ei syystä tai toisesta pääse itse käsiksi tähän tiedostoon, vaikka tiedät kaikkien pamppujen saavan nämä tunnukset käyttöönsä koeajan jälkeen.

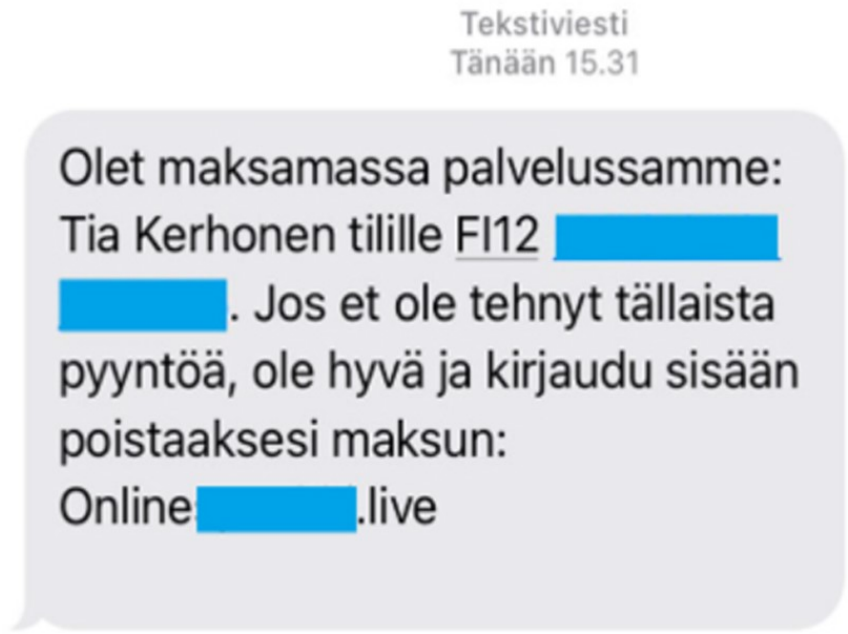
Luovutat salasanan, koska Martti on palkollinen yrityksessäsi, ja hänhän kuulostaa niin itsevarmalta (ja kärsimättömältä) puhelimessa, ettet voi sanoa ei. Samassa yhteydessä Martti kysyy sinulta lisää esihenkilöittesi työajoista, mihin vastaat luonnollisesti kertomalla kaiken. Yleinen variaatio tästä hyökkäyksestä on ”työkaverin” soitto, jonka aikana he väittävät arkisesti unohtaneensa käyttäjätunnuksensa, ja he pyytävät lupaa ”lainata” tunnuksiasi vain ”tämän kerran” sisäänkirjautumista varten.

Yhteistyökyky on työyhteisön terveyden kannalta elintärkeää, mutta muista että ohjeet tunnuksien jakamisesta ja siihen liittyvistä kielloista ovat olemassa hyvästä syystä!

On myös mahdollista, että saat puhelun yrityksen ”IT-tuelta” / ”Microsoftilta”, missä epäilyttävän intialaiselta kuulostava herrasmies kertoo saastuneesta koneestasi, jonka korjaaminen vaatii käyttäjäoikeuksien luovuttamista etähallintaohjelman muodossa. Koneen saastumisesta säikähtäneenä käynnistät pyydetyn etähallintaohjelman.

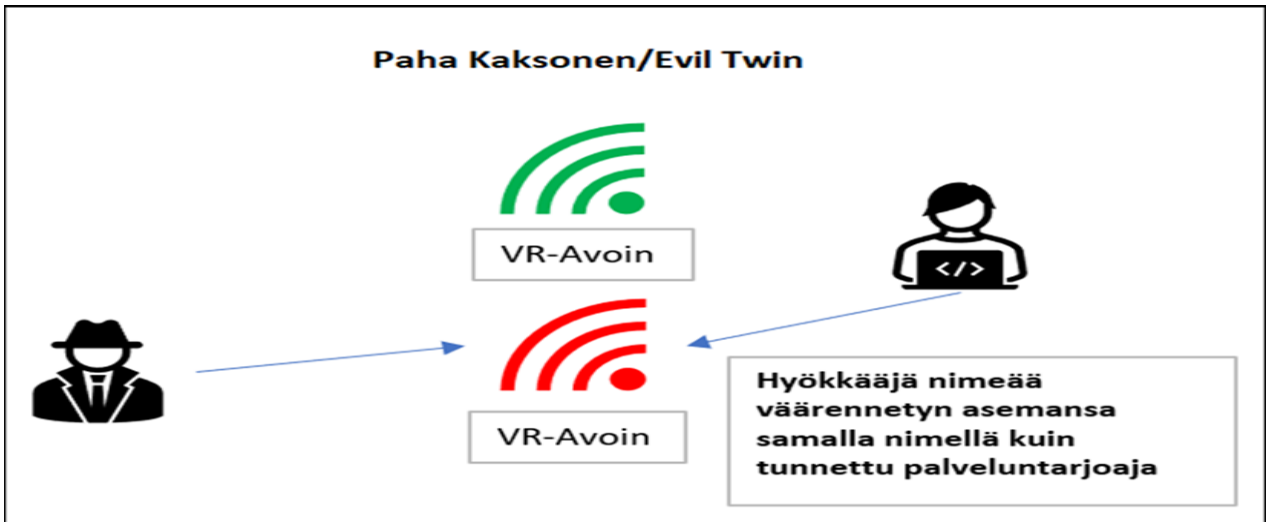
Määrittelemättömän ajan jälkeen saat sitten tietää, että yrityksen tärkeät tiedostot on lukittu kiristysohjelman taakse.

3. Smishing/Tekstiviestihuijaukset



Tietojenkalastelussa voidaan käyttää myös tekstiviestejä. Näiden viestien teksti on yleensä laadittu huonolla suomen kielellä, ja viestien sävy painostaa uhria tekemään jonkin toiminnon, kuten haitallisen linkin avaamisen, millä kalastetaan uhrin tietoja. **Usein ”Kelan” lähettämä tekstiviesti**. Näidenkin viestien laatu on kuitenkin kohonnut, eikä oikeakielisyys enää ole varma tae viestin asiallisuudesta.

4. Valheellinen WiFi/”Paha kaksonen”



Julkisen WiFi:n käyttö ei muutenkaan ole hyvä idea, mutta työasioiden tekeminen sillä on erittäin vastuutonta, koska verkkoaseman tunnuksen **väärentäminen** ei ole vaikeaa. **Älä tee työasioita julkisia verkkoja käyttäen!**

Mistä tunnistat tietojenkalastelun?

Muista, että pankit, viranomaiset, organisaation IT-tuki yms. eivät koskaan pyydä käyttäjätunnuksia, salasanoja, luottokorttitietoja tai vastaavia sähköpostilla, tekstiviestillä tai puhelimessa.

Alla ohjeet epäilyttävien viestien ja puheluiden varalle:

Tarkista viestin lähettäneen henkilön sähköpostiosoite. Mikäli osoite on **tuntematon**, vältä linkkien/tiedostojen avaamista ennen kuin varmistut alkuperästä. Muista myös, että kollegan sähköpostiosoite voi olla kaapattu, joten tutultakin lähettäjältä saapunut viesti voi olla tietojenkalastelua.

Kysy itseltäsi, **miksi** juuri sinuun on otettu yhteyttä. Kuulostaako viestin sisältö liian hyvältä ollakseen totta?

Tarkista sisältääkö viesti/sähköposti/puhelu…

Käskyjä/kehotuksia/painostusta?

Epäloogisia ehdotuksia/komentoja?

Kiireen ja/tai seurausten painottamista?

Normista poikkeavia verkkotunnuksia/linkkejä?

Yrityksen normaalien toimenpiteiden ohittamista?

Epäselkeitä tai epäilyttäviä yhteystietoja?

Älä tee toimenpidettä ja ilmoita tietosuojavastaavalle ja/tai esihenkilöllesi.

Ja puhelimessa asiakkaan/muun kanssa kysy itseltäsi…

Varmistiko soittaja henkilöllisyytensä?

Vastasiko asiakas/soittaja varmennuskysymyksiin oikein?

Välttääkö soittaja vastaamasta yksinkertaisiin kysymyksiin?

Yrittääkö soittaja uhkailla/suostutella sinua?

Yrittääkö soittaja ohjata sinua käyttämään muita laitteita/ohjelmia?

Painottaako soittaja kiirettä ja hitauden mahdollisia seurauksia?

Kyseleekö henkilö muitten työntekijöiden tietoja ja/tai asemaa organisaatiossa?

Pyydä anteeksi, sulje puhelu ja ilmoita tietosuojavastaavalle ja/tai esihenkilöllesi.

HUOM! TYÖYHTEISÖN TIETOTURVALLISUUTTA ON MAHDOLLISTA PARANTAA PARHAITEN OLEMALLA HUOLELLINEN, MERKKAAMALLA EPÄILYTTÄVÄ VIESTINTÄ YLÖS SEKÄ LOPUKSI VARMISTAMALLA, ETTÄ TIETO NÄISTÄ VIESTEISTÄ/PUHELUISTA MENEE ETEENPÄIN ESIHENKILÖLLESI JA YRITYSJOHDOLLE!

Miten voit tarkistaa verkkotunnuksen oikeellisuuden?

Mikäli epäilet verkkotunnuksen rehellisyyttä, käytä alla olevaa alustaa **tarkistukseen**:

URL-Tarkistin: https://transparencyreport.google.com/safe-browsing/search

Kopioi epäilyttävät URL-tunnus asettamalla kursori osoitteen kohdalle, ja kopioi URL hiiren oikeaa näppäintä klikkaamalla ja valitse ”Kopioi/Copy” → Siirry ohjeen linkin kautta sivulle. → Klikkaa hakupalkkia hiiren oikealla näppäimellä ja valitse ”Liitä/Paste” → Klikkaa Search/Hae

HUOM! Yllä oleva sivu ei ole 100 % keino tarkistaa verkkotunnuksen rehellisyyttä. Muista että verkkotunnus/URL on mahdollista väärentää. (ja kollegan sähköposti voi olla kaapattu)!! Tuplatarkista aina, jos sisältö epäilyttää!!!!

Miten voit varjella omia ja organisaatiosi tietoja sosiaalisessa mediassa?

Voit myös tehdä kalastelijoiden elämästä **vaikeampaa vähentämällä omaa näkyvyyttäsi Internetissä.** Tämä onnistuu helpoiten sosiaalisen median yksityisyysasetuksien muokkaamisella. Alla ohjeet näiden asetuksien muuttamiseksi **Facebookille**, **Instagramille** ja **Snapchatille**.

Yksityisyysasetukset Facebookissa: https://www.facebook.com/

Siirry Facebookiin → Valitse käyttäjäprofiilisi oikeasta yläkulmasta, ja valitse ”Asetukset ja yksityisyys” → Valitse ”Asetukset” → Valitse ”Yksityisyys” → Muokkaa asetuksia valitsemalla ”Muokkaa” → Valitse valikosta joko vaihtoehdot ”Kaverit” tai ”Vain minä” oman harkintasi mukaan. → Tee muokkaukset asetuksiin niin, että ainoastaan lisäämäsi henkilöt voivat nähdä julkaisusi ja toimintasi alustalla.

Yksityisyysasetukset Instagramissa: https://www.instagram.com/

Siirry Instagramiin → Siirry profiilisi oikeasta alakulmasta (tunnistaa omasta profiilikuvastaan) → Klikkaa kolmea horisontaalista palkkia ja klikkaa seuraavaksi ”Asetukset/Settings” → Valitse ”Yksityisyys” → Klikkaa harmaata palkkia kohdan ”Yksityinen tili” vierestä ja varmista että se muuttuu siniseksi.

Yksityisyysasetukset SnapChatissa: https://www.snapchat.com/fi-FI

Siirry Snapchattiin. → Klikkaa hammaspyöräsymbolia avataksesi tilisi asetukset. → Rullaa vaihtoehtoja alas, kunnes löydät ”Yksityisyyden hallinta” vaihtoehdon. → Tee muutokset profiilisi näkyvyyteen ja kontakteihin ja klikkaa ”Takaisin” vaihtoehtoa asetusten tallentamiseksi.

Sosiaalista mediaa käyttäessä olisi myös tärkeää ymmärtää, että kaikkea ei kannata sanoa/jakaa. Työnantaja harvoin arvostaa sitä, että jaat työasioitasi edes ystävillesi. Jos jaat niitä tuntemattomille tai puolitutuille ihmisille, riski tietojen väärinkäyttöön tietojenkalastelijoiden toimesta kasvaa merkittäväksi. Ennen kuin julkaiset yllä mainituilla alustoilla mitään, kysy itseltäsi, sisältääkö julkaisusi asioita/tietoja työnantajastasi ja/tai työnkuvastasi. Mieti myös, onko sinulla ylipäätään lupaa julkaista asiasta mitään. Mikäli vastaus toiseenkin näistä kysymyksistä on ei, **ÄLÄ JULKAISE**. Ennen julkaisua kannattaa aina myös miettiä, keillä on mahdollisuus nähdä julkaisu. Mitä suurempi mahdollinen yleisö on, sitä enemmän varovaisuutta tarvitaan.

Lopuksi

Tämän oppaan tarkoituksena on valistaa sinua tietojenkalastelusta sekä tarjota työkaluja tietojenkalastelua ja manipulointia vastaan oman ja työyhteisösi tietoturvallisuuden parantamiseksi. Mikäli tämä ohjeistus herätti mielenkiintosi aihetta kohtaan, suosittelen, että luet aiheesta tekemäni opinnäytetyön ***Ohje tietojenkalastelua vastaan pienissä ja keskisuurissa yrityksissä,*** missä käsittelen tietojenkalastelua tarkemmin.