jamk

Verkkorikollisuus

Tietojenkalastelu organisaatioissa

Sebastian Laaksonen

Opinnäytetyö
Toukokuu 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK) tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Laaksonen Sebastian

Verkkorikollisuus, tietojenkalastelu organisaatioissa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2022, 49 sivua.

Tietojenkäsittely ja tietoliikenne, tieto- ja viestintätekniikan tutkinto-ohjelma, Opinnäytetyö AMK

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Tietojenkalastelu on osa jokapäiväistä elämäämme. Internetin globaalin käytön kasvun myötä tietojenkalastelulle altistuu yhä useampi henkilö. Sen päätarkoituksena on rikollinen käyttö eli tietojen varastaminen tai varastetun tiedon hyödyntäminen lopullisessa hyökkäyksessä. Törmäämme kyseiseen ilmiöön toisinaan myös huomaamattamme. Kalasteluun voi törmätä käytännössä missä tahansa esimerkiksi työpaikalla.

Opinnäytetyön tarkoituksena oli selvittää mitä tietojenkalastelu tarkoittaa terminä, miten tietojenkalastelua toteutetaan ja miten sitä vastaan voidaan puolustautua. Työssä käytiin läpi yleisimpiä tietojenkalastelumenetelmiä esimerkiksi sähköpostihuijauksia. Työn tärkeimpänä tavoitteena oli tunnistaa miltä ne näyttävät ja miten niitä vastaan voidaan puolustautua. Tutkimus toteutettiin haastatteluita ja omia työympäristön havainnointeja hyödyntäen. Aineistoa kerättiin myös verkosta löytyvien tutkimusten, raporttien ja artikkeleiden pohjalta. Työssä käytiin läpi myös esimerkkien avulla miltä tietojenkalasteluhyökkäykset näyttävät ja miten maailmantilanteita voidaan käyttää hyödyksi hyökkäyksiä tehdessä esimerkiksi COVID-19 pandemian aikana.

Tutkittujen tietojen ja haastatteluiden pohjalta ilmeni, että tietojenkalastelua ei välttämättä kouluteta organisaatoissa, vaikka nykypäivänä tietojenkalastelu on yksi suurimmista tietoturvauhista. Koulutuksen tarpeellisuutta kuvaa se, että suurin osa tietojenkalastelun onnistumista johtuu käyttäjän tekemisestä. Tutkimuksen johtopäätöksenä voitiin todeta, että tietojenkalastelu on suuri uhka organisaatioille kyberhyökkäyksien osalta. Tietojenkalastelua vastaan voidaan suojautua organisaatioissa teknillisillä hallintakeinoilla, sekä käyttäjän tietoisuuden avulla. Käyttäjän rooli kalastelun onnistumisessa on suuri. Suurin osa kalasteluista onnistuu käyttäjän tekemän toimenpiteen vuoksi.

Avainsanat (asiasanat)

Verkkorikollisuus, tietojenkalastelu, organisaatio, verkkourkinta

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Laaksonen Sebastian

Cybercrime, phishing in organizations

Jyväskylä: JAMK University of Applied Sciences, May 2022, 49 pages

School of Technology. Degree Programme in Information and communication technology. Bachelor's thesis

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Phishing is a part of our daily lives. As the global use of the Internet grows, more and more people are being exposed to phishing scams. Its main purpose is criminal use, i.e. the theft of data or the exploitation of stolen data in a final attack. We sometimes encounter this phenomenon unnoticed. You can come across fishing practically anywhere, for example at a workplace.

The purpose of the study was to find out what the term phishing means, how phishing is carried out and how it can be defended against it. The most common phishing methods, such as e-mail scams, were reviewed. The main goal of the study was to identify what they look like and how to protect against them. The research was carried out using interviews and own observations of the work environment. The material was also collected based on research, reports, and articles available online. The work also looked at examples of what phishing attacks look like and how global situations can be exploited in attacks such as the COVID-19 pandemic.

Based on the data and interviews researched, it emerged that phishing is not necessarily trained in organizations, although phishing is one of the biggest security threats today. The need for training is illustrated by the fact that most of the success of phishing is due to what the user does. The study concluded that phishing is a major threat to organizations in terms of cyber-attacks. Phishing can be protected in organizations with technical management measures and user awareness. The role of the user in the success of fishing is great. Most fishing is successful because of the action taken by the user.

Keywords/tags (subjects)

Cybercrime, phishing, organization

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

Taulukot

Lyhenteet ja termit

APWG eli Anti-Phishing Workin Group on vuonna 2013 perustettu voittoa tavoittelematon järjestö, jonka tavoitteena on identiteettivarkauksien ja petosten tuhoaminen, jotka johtuvat tietojenkalastelusta, haittaohjelmista ja sähköpostin spooffauksesta (Phishing Activity Trends Report – Q4 2021 2021).

SOC englanniksi Security Operations Center tarkoittaa tietoturvapalvelua, jolla tuotetaan asiakkaalle teknistä tilannekuvaa mahdollisten tietoturvauhkien ja tietoturvapoikkeamien varalta (What Is a Security Operations Center (SOC)? n.d.).

Phishing suomeksi tietojenkalastelu termillä tarkoitetaan tapoja, joissa käyttäjältä yritetään saada henkilökohtaisia tai erityisen arkoja henkilötietoja huijaamalla käyttäjää sähköpostihuijauksilla, valheellisilla verkkosivustoilla, tai haittaohjelmilla. Tietojenkalastelun yksi toteutumismuodoista on psykologinen manipulointi, jota voidaan hyödyntää varsinaisen hyökkäyksen toteuttamisessa. Tietojenkalastelu on yksi suurimmista tietoturvauhista (Hadnagy, Fincher & Dreeke 2015).

OV-Sertifikaatti eli organisaation validointi tehtävänä on varmistaa hakevan organisaation henkilöllisyyden. Näitä voivat olla esimerkiksi organisaatio, järjestö tai yritys (SSL n.d.).

EV-Serfikaatti eli laajennettu validointi toimii samalla periaatteella kuin OV-sertifikaatti, mutta se edustaa korkeampaa luottamustasoa kuin aikaisemmin mainittu OV-sertifikaatti. EV vaatii tiukempia validointiratkaisuita, joilla pyritään täyttämään selainfoorumin / varmentajan laajennuksen vaatimukset (SSL n.d.).

DV-Sertifikaatti eli domain-validointi on näistä kolmesta sertifikaatista validointitasoltaan alhaisin. DV-sertifikaatin tehtävä on ainoastaan varmistaa, että varmenteen pyytävä hallinoi suojattavaa verkkotunnusta (SSL n.d.).

2FA eli kaksivaiheinen tunnistautuminen on ylimääräinen suojaustaso, jolla varmistetaan, että verkkotiliin pääsyä yrittävät ihmiset ovat sitä, mitä he sanovat olevansa. Ensin käyttäjä syöttää käyttäjätunnuksensa ja salasanansa. Sen sijaan, että hyökkääjä pääsisi kirjautumaan tilille suoraan, heidän on annettava toinen tieto esimerkiksi pin-koodi, tekstiviestivarmennus (What is Two-Facton Authentication. (2FA) n.d.)

DNS eli nimipalvelu tarjoaa tietokannan, jota käytetään käännöksissä ihmisen luettavista isäntänimistä, kuten www.opensource.com, IP-osoitteisiin, kuten 54.204.39.132, jotta Internetiin kytketyt tietokoneet ja muut laitteet voivat käyttää niitä (Both 2017)

SPF eli Sender Policy Framework on menetelmä, joka todentaa onko sähköposti lähetetty oikealta sähköpostipalvelimelta käyttäen lähettäjän tietoja sähköpostin toimituksesta. Sallitut sähköpostipalvelimet tai palvelimet määritel-lään verkkotunnuksen omistajan toimesta (Görling 2007).

DKIM eli DomainKeys Identified Mail on menetelmä, joka on suunniteltu tunnistamaan huijaussähköpostit tarjoamalla mekanismin, jonka avulla sähköpostin vastaanottava taho voi tarkistaa sähköpostin saapuneen hyväksytystä verkko-tunnuksesta (Dedhia 2016).

DMARC eli ja Domain-based Message Authentication, Reporting and Conformance on sähköpostin vahvistusjärjestelmä, joka on suunniteltu tunnistamaan ja estämään sähköpostin hui-jaus. Se tarjoaa mekanismin, jonka avulla vastaanottava organisaatio voi tarkistaa, että verkkotun-nuksen järjestelmänvalvojat ovat valtuuttaneet verkkotunnuksesta saapuvan postin ja ettei sähkö-postia (mukaan lukien liitteitä) ole muutettu kuljetuksen aikana (Dedhia 2016).

IP eli Internet Protocol on uniikki osoite jonka avulla voidaan todentaa esimerkiksi yksittäinen laite internetissä tai sisäverkossa. IP-osoitetta käytetään tiedon välittämiseen laitteen ja internetin välityksessä (What is an IP Address – Definition and Explanation n.d.)

1 Johdanto

Tietojärjestelmä on integroitu joukko komponentteja tiedon keräämiseen, tallentamiseen ja käsittelyyn, sekä informaation, tiedon ja digitaalisen tuotteiden tarjoamiseen. Joukolla komponentteja tarkoitetaan, että tietojärjestelmä sisältää seuraavat komponentit: ohjelmisto, tietoliikenne, tietokannat ja tietovarastot, henkilöresurssit, proseduurit sekä tietokonelaitteiston. Organisaatiot käyttävät tietojärjestelmiä esimerkiksi henkilöstönhallintaan. Suurimpia tietojärjestelmiä maailmalla ovat esimerkiksi eBay ja Amazon, jotka perustavat koko toimintansa tietojärjestelmien ympärille. (Vladimir 2020.). Kun puhutaan tietojärjestelmistä. Yksi suurista toimijoista, jotka käyttävät tietojärjestelmiä on terveydenhuolto. Terveydenhuollossa näitä käytetään parantamaan palvelua, sekä vähentämään lääketieteellisiä virheitä. (LeRouge, Mantzana & Wilson 2017.)

Tietojenkalastelu eli englanniksi phishing on rikos, jossa käytetään sosiaalista manipulointia tai teknisiä tapoja käyttäjien tai organisaatioiden tietojen varastamiseen. Kohteena voivat olla esimerkiksi käyttäjän henkilötiedot, käyttäjätunnukset tai esimerkiksi luottokortin tiedot. Sosiaalisen manipuloinnin tarkoituksena on saada käyttäjä luottamaan hyökkääjään. Hyökkääjän tarkoituksena on saada käyttäjä tuntemaan, että käyttäjä on tekemisissä luotettavan tahon kanssa, esimerkiksi organisaation IT-tuen kanssa. Luotettavuutta pyritään herättämään esimerkiksi luotettavilla sähköpostiosoitteilla ja sähköpostiviesteillä. Sähköpostiviestit johtavat käyttäjän yleensä väärennetylle verkkosivustolle. Teknisillä tavoilla tarkoitetaan esimerkiksi haittaohjelman asentamista käyttäjän työasemalle, jonka avulla pyritään varastamaan esimerkiksi käyttäjän käyttäjätunnukset. (Phishing Activity Trends Report – Q4 2021 2021, 2.)

Internettiä käyttää Statistan tekemän raportin mukaan 4,9 biljoonaa ihmistä (Number of internet users worldwide from 2005 to 2021 n.d.). Internetin käytön merkittävän kasvun myötä ihmiset jakavat yhä enemmän henkilökohtaisia tietojaan verkossa. Tämän seurauksena valtava määrä henkilökohtaisia tietoja ja rahoitustapahtumia tulee alttiiksi verkkorikollisille. Tällä hetkellä tietojenkalastelua pidetään yhtenä yleisimmistä esimerkeistä Internetin petoksista.
Tietojenkalasteluhyökkäykset voivat aiheuttaa uhreille vakavia menetyksiä, mukaan lukien arkaluontoiset tiedot, identiteettivarkaudet, yritykset ja hallituksen salaisuudet. (Alkhalil, Hewage, Nawaf & Khan 2021.)

Anti-Phishing Working Groupin (APWG) mukaan organisaatioissa tietojenkalastelu on merkittävä tietoturvauhka. Organisaatiotasolla haittaohjelmien uhriksi joutui vuoden 2021 viimeisellä neljänneksellä 36 % enemmän organisaatioista verrattuna vuoden 2021 kolmannelle neljännekselle. Talousala oli vuoden 2021 viimeisen neljänneksen useimmiten hyökätty sektori. Talousalalle kohdistui näistä hyökkäyksiä 23,2 % verran. (Phishing Activity Trends Report – Q4 2021 2021, 2.)

Työn toimeksiantajana oli Jyväskylän ammattikorkeakoulun IT-instituutti. IT-instituutissa on mahdollista opiskella ohjelmointia, kyberturvallisuutta, tietojärjestelmien kehittämistä ja ylläpitoa, sekä hallintaa. IT-instituutista voi valmistua joko insinööriksi (AMK) tai tradenomiksi. (ICT-ala n.d.). Opinnäytetyö tehtiin CYBERDI-projektille, jonka tarkoituksena on vahvistaa Jyväskylän ammattikorkeakoulun ja Poliisikorkeakoulun osaamista kyberrikollisuuden havaitsemisessa ja tutkinnassa sekä profiloitua päteviksi kyberrikollisuuden tutkimuksen asiantuntijoiksi ainakin Euroopan tasolla. Projektin rahoituksesta vastaa opetus- ja kulttuuriministeriö. CYBERDI-projektin kokonaisuus on jaoteltu kolmeen osioon: Kyberrikollisuuden torjuminen, tietoisuuden kasvattaminen sekä yhteistyön vahvistamiseen. (CYBERDI n.d.)

Jyväskylän ammattikorkeakoulussa opiskelee yli 8500 opiskelijaa. Ammattikorkeakoulu tarjoaa yli 40 tutkintoa seitsemältä eri alalta. Opiskelijoita on nykypäivänä jopa yli 70 eri maasta. Vahvuusaloja on määritelty strategiaan kuusi. Näitä ovat matkailu, robotiikka, automaatio, sovellettu kyberturvallisuus, monialainen koulutus sekä biotalous. Arvoiksi ammattikorkeakoulu on määritellyt luovuuden, luottamuksen sekä vastuiden. Projektin tarkoituksena kehittää osaamista kilpailukykyiseksi ja olla kansainvälisesti kilpailukyvyn kehittäjä sekä oppimisen uudistaja. Yksiköitä ammattikorkeakoulussa on neljä, sekä hallintoyksikkö. (Jamk n.d.)

Tämän opinnäytetyön tarkoituksena on tuoda esille tietojenkalastelun eri näkökulmat ja selvittää miten nykypäivänä tietojenkalastelua hyödynnetään. Tavoitteena on, että opinnäytetyön tulosta voidaan hyödyntää selittämään tietojenkalastelua käsitteenä, sekä avata tietojenkalastelun eri toimintatapoja. Opinnäytetyö sisältää myös käytännön esimerkkejä hyökkäyksistä, joita on toteutettu vuosien aikana. Näiden tarkoituksena on avata miltä esimerkiksi tyypillinen tekstiviestihuijaus näyttää. Aiheen tutkiminen korreloi suoraan omaan työnkuvaan. Aihe on nykyaikana yksi merkittävimpiä tietoturvauhkia, joka koskettaa käytännössä kaikkia henkilöitä siirryttäessä koko ajan enemmän globaalisti digitaaliseen maailmaan.

2 Tutkimusmenetelmät

2.1 Tutkimuskysymys

Tämä opinnäytetyö pyrkii löytämään vastauksen seuraavaan tutkimuskysymykseen:

- Mitä termi tietojenkalastelu tarkoittaa ja miten sitä vastaan voidaan suojautua?

Tämä on pääsykysymys, joka pitää sisällään tietojenkalastelun terminä sekä puolustautumisen näkökulman. Koska opinnäytetyön pääkysymys on laaja niin se on jaoteltu muutamaan alikysymykseen. Alakysymysten tarkoituksena on antaa suuntaa siihen mistä näkökulmasta pääkysymystä on tätä opinnäytetyötä tehdessä käsitelty. Näitä ovat esimerkiksi:

- Miltä tietojenkalastelu näyttää käyttäjän näkökulmasta?
- Mitä ovat tietojenkalastelumenetelmät?

2.2 Tutkimusmetodologia

Opinnäytetyön tutkimusmenetelmäksi valittiin kvalitatiivinen menetelmä. Kvalitatiivinen menetelmä tarkoittaa, että prosesseja ei tutkita tai mitata kokeellisesti määrän, intensiteetin tai taajuuden mukaan. Kvalitatiivinen menetelmä on suunniteltu viittaamaan todellisten tilanteiden ja tapausten tutkimiseen, jotka sisältävät runsaasti tietoa, kun taas määrällisessä menetelmässä käytetään mittauksia ja staattista tietoa ja analysoidaan tiedot matemaattisesti tai numeerisesti. Kvalitatiivinen menetelmä voi heijastaa kirjoittajan omaa näkökulman, kunhan se on aitoa ja luotettavaa. (Labaree n.d.)

Haastattelut ovat tuotettu tutkimuksessa teemahaastatteluna. Haastatteluissa on pyritty selvittämään henkilöiden tietämystä tietojenkalastelusta käsitteenä, sekä mahdollisesti aiheen ympärillä toimimisesta. Haastattelut suoritettiin osaltaan kasvotusten ja osaltaan puhelimitse. Haastatteluihin on valittu kollegoita sekä ystäviä.

2.3 Aineiston kerääminen

Työ toteutettiin tutustumalla aiheeseen liittyviin artikkeleihin ja tutkimuksiin, sekä tietoa kerättiin myös haastatteluiden ja tutkijan työkokemuksen kautta. Työ aloitettiin tutkimalla tietojenkalastelua käsitteenä, tietojenkalastelun eri menetelmiä ja niiden hyötyjä. Tarkastelun kohteena oli myös, miten tietojenkalastelua vastaan voidaan suojautua. Lisäksi tutkimuksen tarkoituksena on havainnollistaa tietojenkalastelun toimintatavat. Tämän työn tuloksia voivat hyödyntää ne henkilöt, jotka haluavat laajentaa käsitystään tietojenkalastelusta.

Haastatteluihin valikoitiin viisi eri henkilöä eri organisaatioista. Henkilöiden valitseminen perustui henkilöiden työtehtäviin, jotka työskentelevät eri organisaatioissa. Haastattelut toteutettiin nimettömänä. Tässä työssä haastateltavista käytetään titteliä. Osa haastateltavista henkilöistä työskentelee tietoturvan parissa, jonka avulla haastatteluihin saatiin teknistä näkökulmaa. Kyseiset henkilöt työskentelevät kaikki eri aloilla, jonka vuoksi haastatteluiden tuloksiin saatiin eriäviä vastauksia.

Taulukko 1 Haastateltavat

Titteli	Työkokemus
Tietoturva-asiantuntija	3-vuotta
Opettaja	1-vuotta
Kuljetussuunnittelija	2-vuotta
Tietoturva-asiantuntija	4-vuotta
O365-asiantuntija	8-vuotta

2.4 Tutkimuseettinen tarkastelu

Tutkimusetiikan tehtävä on antaa ohjeita siihen, miten luotettava tutkimus tehdään, joka ei riko minkäänlaisia tekijänoikeuksia. Eettisen opinnäytetyön tehdäkseen tuloksen tulee olla rehellinen, kun analysoidaan olemassa olevaa tietoa. Tärkeintä on säilyttää objektivisuus eikä antaa henkilökohtaisten tunteiden vaikuttaa tekemiseen, sekä säilyttää varovaisuus tutkiessaan tietoa. Tutkittaessa tulee kunnioittaa rehellisyyttä, huolellisuutta ja tarkkuutta. Eettisten periaatteiden mukaan toisen asiantuntijan tai tutkijan työtä ja sen saavutukset tulee ottaa asiallisella tavalla huomioon niin, että heidän tekemää työtä kunnioitetaan. Tähän sisältyy esimerkiksi tekstissä viittaaminen. (JAMKin eettiset periaatteet 2018.) Tämä opinnäytetyö on toteutettu ohjeistuksen mukaisesti ja niitä tullaan seuraamaan tämän työn teossa.

2.5 Rajaukset

Opinnäytetyö rajataan tietojenkalastelun menetelmiin, tavoitteisiin ja siihen miten niitä vastaan voidaan puolustautua. Työssä tullaan käymään läpi pinta puolisesti edellä mainitut kohdat ja avataan niiden tärkeimmät hyödyt ja käyttötarkoitukset. Työssä ei ole tarkoitus käydä läpi eri hyökkäyksiin liittyviä teknillisiä osa-alueita eikä niihin käytettyjä ohjelmointimenetelmiä.

3 Tietojenkalastelu

3.1 Tietojenkalastelu terminä

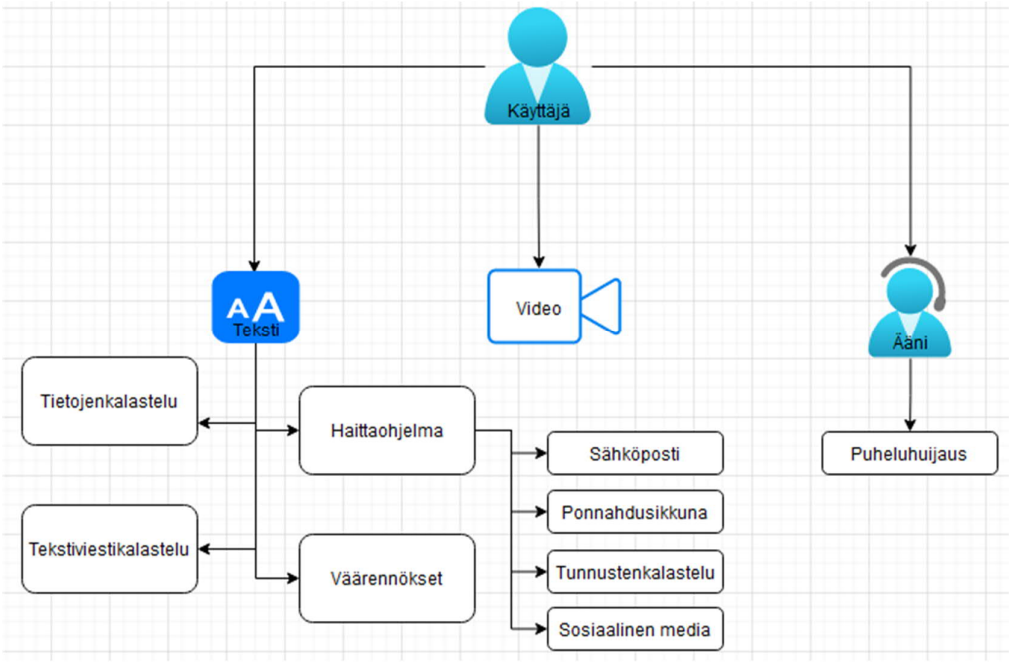
Tietojenkalastelu termillä tarkoitetaan tapoja, joissa käyttäjälle lähetetään esimerkiksi sähköpostiviestejä, jotka näyttävät olevan luotettavasta lähteestä. Tavoitteena on saada käyttäjän henkilökohtaisia tietoja. Tietojenkalastelu perustuu manipulointiin ja teknisiin keinoihin. (Hadnagy, Fincher & Dreeke 2015.)

Sähköpostiviesti voi sisältää esimerkiksi haitallisen liitetiedoston, joka lataa haittaohjelman käyttäjän tietokoneelle. Se voi myös sisältää linkin haitalliselle verkkosivustolle. Nämä verkkosivut voivat pyrkiä saamaan käyttäjän lataamaan haittaohjelman tai luovuttamaan henkilökohtaista tietoa verkkosivun kautta. Hyökkääjät käyttävät aikaa tiedon keruuseen käyttäjistä. Tällä tavalla hyökkääjät voivat luoda sähköposteja, jotka ovat käyttäjän näkökulmasta personoituja ja relevantteja. (Hadnagy, Fincher & Dreeke 2015.)

Tietojenkalastelua voidaan toteuttaa myös muilla tavoin kuin sähköpostilla. Nykypäivänä tietojenkalastelua toteutetaan myös esimerkiksi tekstiviestitse ja puhelimitse. Tekstiviestien avulla voidaan nykypäivänä toimia kutakuinkin identtisesti sähköpostiin verrattuna. (Hadnagy, Fincher & Dreeke 2015.). Kuten opettaja alla oleva totesi ei tietojenkalastelun toteutustavat ole tuttuja. Toisaalta termi tietojenkalastelu on tuttu.

> *”Tietojenkalastelu terminä on tuttu, mutta sen kaikkia toteutustapoja en osaa kuvata. Termi nousee ajoittain esille median kertoessa isoista tietomurto tapauksista. Esimerkiksi COVID 19 -tietojenkalastelu pisti omaan silmään ja herätti olemaan tarkempi tarkastelemaan mitä tietopyyntöjä Omakannasta tulee kuten koronarokotustodistuksen osalta.” (Opettaja)*

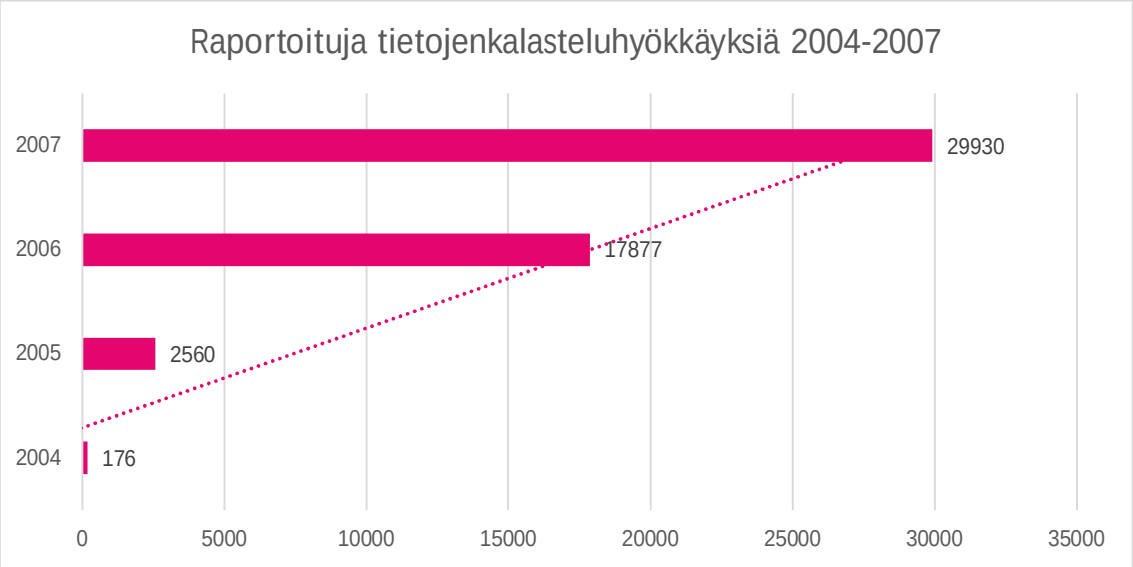
Alla olevassa kuviossa (Kuvio 1) on havainnollistettu minkä tyyppisiä kalasteluita hyödynnetään eri formaattien kautta. Kuviosta voidaan havaita, että suurin osa tietojenkalastelusta tapahtuu käyttäen tekstipohjaista formaattia hyökkäyksien toteuttamiseen. Nykypäivänä tulee kuitenkin huomioida, että kalastelua tehdään, myös videon ja äänen välityksellä (Rastenis, Ramanauskaité, Janulevičius, Čenys, Slotkiené & Pakrijauskas 2020).



Kuvio 1 Eri formaatit (Rastenis, Ramanauskaité, Janulevičius, Čenys, Slotkiené & Pakrijauskas 2020)

3.2 Tietojenkalastelun historia

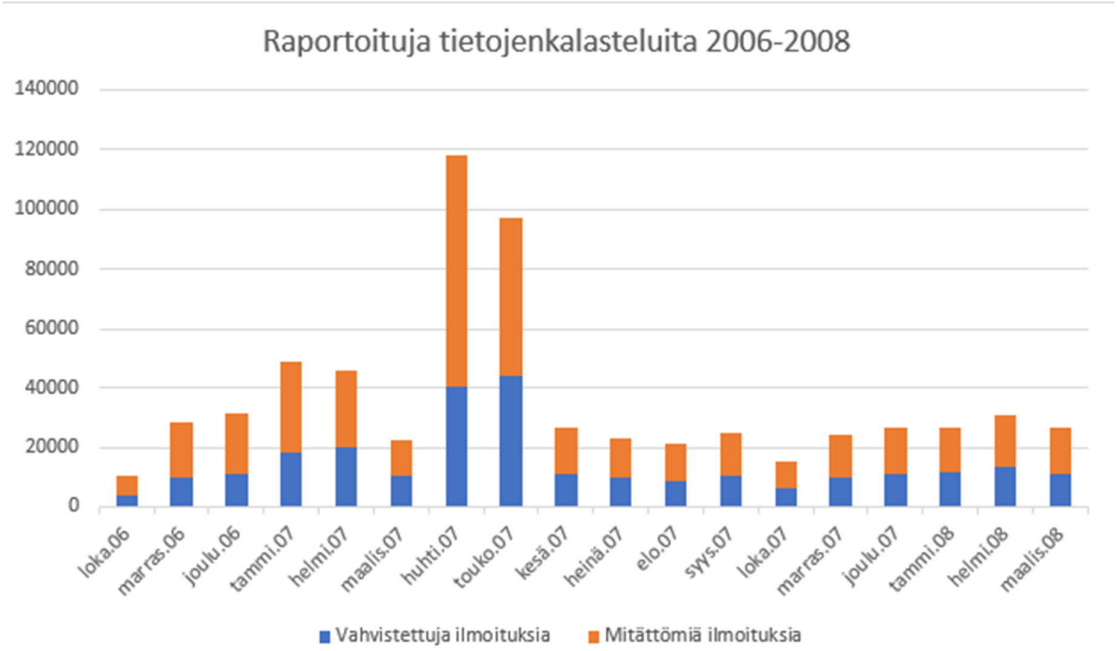
Sana ”phishing” suomeksi tietojenkalastelu sai alkunsa vuonna 1996. Termi keksittiin analogian perusteella, että huijarit käyttivät sähköpostia koukkuna käyttäjien käyttäjätunnusten, salasanojen ja muiden arkaluontoisten tietojen varastamiseen. Kirjainten ”ph” käytön uskotaan olevan peräisin sanasta ”phreaking”, joka tarkoittaa matkapuhelinverkon signaalien manipulointia ilmaisten puheluiden suorittamiseen. Tietojenkalastelu sanana ilmestyi ensimmäisen kerran, kun hyökkääjät varastivat tietoa amerikkalaisessa palvelussa nimeltään American Online. Hyökkäyksen tarkoituksena oli varastaa käyttäjien salasanoja. (Martino & Perramon 2010.). Alla havainnollistettu (Kuvio 2) APWG:n raportissa (2007) esille nostetut lukumäärät 2000 luvun alkupuolelta raportoituja tietojenkalasteluhyökkäyksiä. Trendistä voidaan huomata, että vuoteen 2007 mennessä tietojenkalasteluhyökkäyksien määrä oli kovassa kasvussa.



Kuvio 2 Tietojenkalasteluhyökkäyksiä 2004-2007 (Phishing Activity Trends Report – January 2004 2004; Phishing Activity Trends Report – January 2005 2005; Phishing Activity Trends Report – January 2006 2006; Phishing Activity Trends Report – January 2007 2007)

Helmikuussa 2007, 2008 ja 2009 suosituimmat palvelut tietojenkalastelussa olivat PayPal, sekä Ebay. PayPaliin kohdistui hyökkäyksiä kyseisellä aikavälillä 14 501 kappaletta (Martino & Perramon 2010). Vuonna 2016 PhisMe julkaisi tutkimuksen, jonka mukaan arviolta ~90 % kyberhyökkäyksistä ja sen aiheuttamista tietomurroista sai alkunsa tietojenkalasteluhyökkäyksestä (Enterprise Phishing Susceptibility Reporte n.d.). Vuonna 2018 96 % sosiaalisen manipuloinnin hyökkäyksistä tehtiin sähköpostin avulla (Data breach investigation report 2018 n.d.).

Martinon ja Perramon (2010) raportissa on kuvattu vuosien 2006–2008 aikana raportoituja tietojenkalasteluita PhishTank verkkosivustolle. Verkkosivuston tarkoituksena on kerätä käyttäjien tekemiä ilmoituksia mahdollisista tietojenkalastelu yrityksistä. Alla on kuvattu kuvion 3 avulla PhishTankin tekemän raportin mukaisesti ilmoitettuja tietojenkalasteluhyökkäyksiä. PhishTankin tekemän tarkistuksen mukaan ilmoitukset luokitellaan vahvistetuiksi tai mitättömäksi (Martino & Perramon 2010). Kuviosta 3 voidaan päätellä, että huhtikuussa 2007 ja toukokuussa 2007 ilmoitusten määrissä on ollut suuri nousu verrattuna muihin kuukausiin



Kuvio 3 Raportoituja tietojenkalasteluita 2006-2008 (Martino & Perramon 2010)

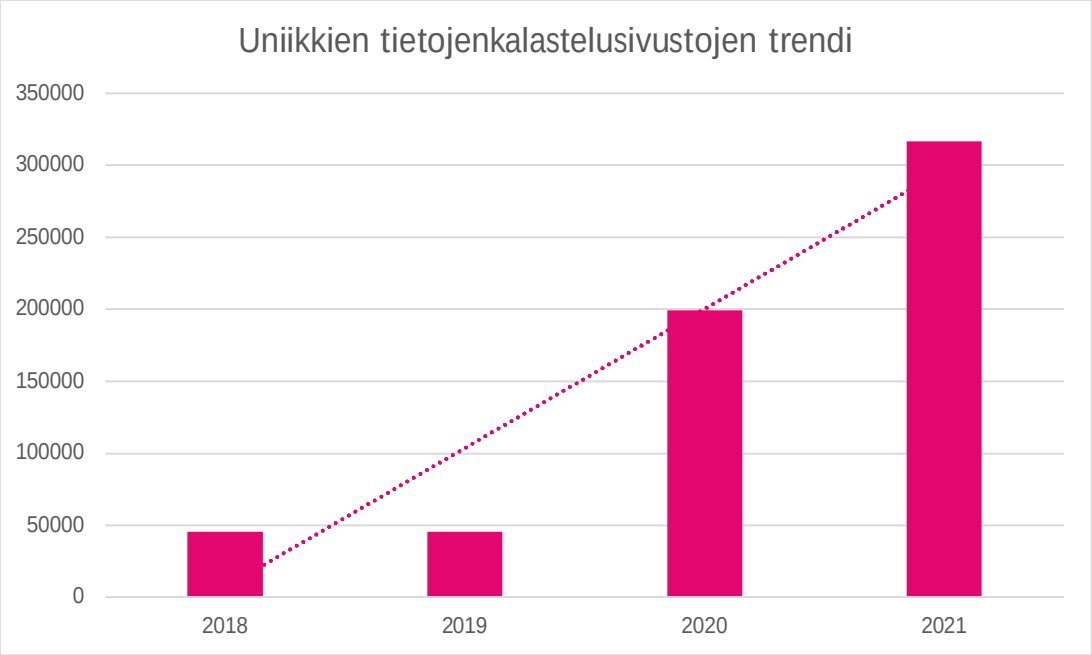
3.3 Tietojenkalastelun tavoite

Tietojenkalastelun tavoitteena on saada henkilöltä esimerkiksi hänen luottokorttinsa tiedot, salasanat, verkkopankin tunnukset, käyttäjän asiakasnumero johonkin palveluun tai asentaa haittaohjelma käyttäjän koneelle (Phishing attacks n.d.). Kilpailu ja kuluttajavirasto nostaa omassa artikkelissaan myös tavoitteeksi saada käyttäjän henkilötietoja. Näitä voivat olla esimerkiksi käyttäjän sosiaaliturvatunnus (Tietojenkalastelu n.d.). Tietojen avulla hyökkääjä pääsee käsiksi henkilön arkaluontoisiin tietoihin, joiden avulla hyökkääjä voi kiristää henkilöä. Mahdollisesti saatujen luottokorttinumeron tai verkkopankkitunnuksien avulla hyökkääjä voi hyötyä rahallisesti käyttämällä väärin näitä tietoja (Phishing attacks n.d.)

3.4 Tietojenkalastelun nykytilanne

Nykypäivänä tietojenkalastelu on nouseva trendi. APWG tarjoaa raportteja vuoden neljänneksien mukaan. Raportista voidaan tarkastella uniikkien tietojenkalastelusivustojen määriä. Vuoden 2018 viimeisellä neljänneksellä esimerkiksi joulukuussa uniikkeja sivustoja on havaittu 45 974 kappaletta (Phishing Activity Trends Report – Q4 2018 2018), kun taas esimerkiksi vuoden 2021 viimeisellä neljänneksellä joulukuussa sivustoja on havaittu 316 747 kappaletta. Kyseinen määrä on suurin

koskaan havaittu määrä APWG:n raportointihistorian aikana. Raporttien perusteella voidaan havaita trendin kasvavuus. Alla on kuvattu (Kuvio 4) uniikkien tietojenkalastelusivustojen määrät joulukuussa vuosien 2018 ja 2021 välissä. (Phishing Activity Trends Report – Q4 2021 2021.) Kuvion avulla voidaan havaita, että vuoden 2018 ja vuoden 2021 välinen kasvu on ollut noin kuusinkertainen.

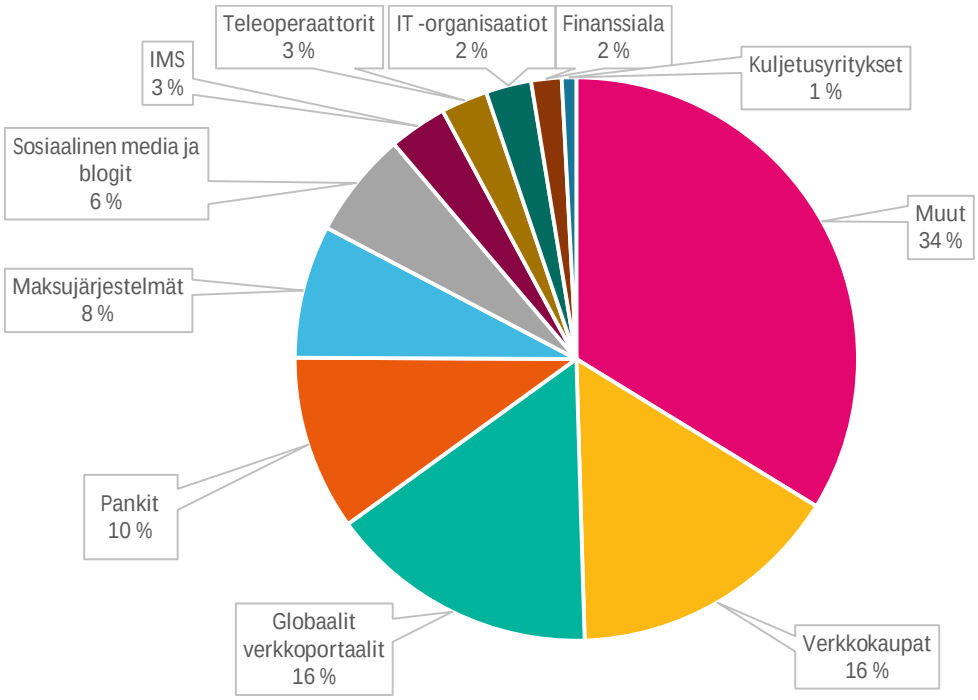


Kuvio 4 Uniikkien tietojenkalastelusivustojen trendi (Phishing Activity Trends Report – Q4 2017 2017; Phishing Activity Trends Report – Q4 2021 2021)

APWG raportin mukaan organisaatiotasolla vuoden 2021 viimeisellä neljänneksellä tietojenkalasteluhyökkäyksiä kohdennettiin eniten finanssialaan (sisältäen pankit). Finanssialaan APWG raportin mukaan kohdistui 23,2 % kalasteluhyökkäyksistä. Hyökkäykset webmail ja SaaS -palveluita tuottavia organisaatioita kohtaan pysyivät korkeana. Prosentuaalisesti näihin kohdistuneita kalasteluhyökkäyksiä kohdennettiin 19,5 % kaikista hyökkäyksistä. Hyökkäykset kyseisiä (webmail ja SaaS) organisaatioita kohtaan pienenivät kuitenkin kolmannelta neljännekseltä 29,1 % -> 19,5 %. (Phishing Activity Trends Report – Q4 2021 2021.)

IBM:n teettämässä raportissa arvioitiin kuinka paljon tietojenkalastelut ovat maksaneet. Tietojenkalastelu on ollut vuoden 2021 toiseksi kallein hyökkäysvektori. Ainoastaan yrityssähköpostien

murrot nousivat vuoden 2021 aikana kalleimmaksi hyökkäysvektoriksi. Yrityssähköpostien murtojen arvioitiin maksavan organisaatioille keskimäärin 5,1 miljoona dollaria. Tietojenkalastelun arvioitiin maksavan arviolta 4,65 miljoonaa dollaria. (Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year 2022.) Statistan teettämässä tutkimuksessa vuoden 2021 ensimmäisellä neljänneksellä tietojenkalasteluhyökkäyksiä eri organisaatiotasoilla on kuvattu alla olevassa kuviossa 5 (Johnson 2021). Kuviosta voidaan havaita, että suurimpia organisaatiotasoja, joihin kohdistettu kalastelua on globaalit verkkopankit, sekä verkkokaupat. Kuljetusyrityksiin kohdistuneita hyökkäyksiä oli vuoden 2021 ensimmäisellä neljänneksellä vain yksi prosentti kaikista organisaatiotasoista.



Kuvio 5 Hyökkäykset toimialottain (Johnson 2021)

Tietojenkalasteluhyökkäyksissä usein rikollisen tarkoituksena on saada käyttäjä asentamaan haluamansa ohjelmiston työasemalle tai matkapuhelimelle. Kuten Kyberturvallisuuskeskus (2020) mainitsee: ”Huijari yrittää suostutella uhria asentamaan maksuttoman etähallintaohjelman, kuten Anydesk, TeamViewer, SupRemo, Alpemix, Zoho Assist, tai muu vastaava. Windowsin lisäksi näitä

ohjelmia saa myös MacOS:lle ja Linuxille, jos soittaja vain saa suostuteltua uhrin asentamaan ohjelman. Huijari voi myös pyytää ostamaan Google Play tai iTunes -lahjakortteja tai virtuaalivaluuttaa ja haluaa niiden koodit. Pyyntöihin ei pidä suostua."

Jonesin (2022) tekemässä artikkelissa on kuvattu vuoden 2020 kolmannella neljänneksellä yleisimpien haitallisten liitetiedostojen tyypit, jotka on lähetetty sähköpostin välityksellä. Listalla ensimmäisenä on Windowsin suoritettavat tiedostot, joiden osuus on 74 %. Kyseinen liitetiedostotyyppi on huomattavasti suositumpi kuin listalla toisena oleva komentotiedostot, joiden osuus oli 11 %. Kolmantena listalla on mainittu Office-tiedostot, joiden osuus 5 %. Listalle mahtui myös esimerkiksi PDF-tiedostot, pakatut tiedostot, java-tiedostot sekä pikakuvakkeet.

Jones (2022) mainitsee myös artikkelissaan, joka on nähtävillä kuviossa 6 mihin toimialaan hyökkäykset kohdistuvat. Listauksen perustana on käytetty organisaation kokoa, jonka perusteella on arvioitu eri toimialojen osuuksia tietojenkalasteluissa. Listauksessa nousee esille, että huomioimatta toimialan kokoa niin lääkintä ja terveydenhuolto nousee jokaisessa organisaation koossa.

Pieni (1-249)	**Keskikokoinen (250-999)**	**Suuri (1000+)**
44,7% Lääkintä ja terveydenhuolto	49,2% Lääkintä ja terveydenhuolto	49,3 Lääkintä ja terveydenhuolto
41,1% Koulutusala	49,7% Rakennusala	46,8% Rakennusala
40,9% Teollisuusala	43,5% Liikepalvelut	55,9% Teknologiala

Kuvio 6 Kalasteluiden määrä eri alojen organisaatioissa (Jones 2022)

3.5 Yleisimmät tietojenkalastelussa käytetyt teemat 2021

Vuoden 2021 yleisimmät kalastelumenetelmät on listattu Verizonin (Irwin 2022) teettämässä raportissa. COVID-19 on ollut viimeisimmät kaksi vuotta hyökkääjien lähteenä tietojenkalasteluhyökkäyksien teemana. Suurin osa näistä hyökkäyksistä sisälsivät haitallisen liitetiedoston, joka asentaa haittaohjelman työasemalle. COVID-19 mahdollistamana tehtiin ”Spider-Man” huijaus. Spider-Man oli vuoden 2021 katsotuin elokuva. Rajoitusten takia elokuvateattereiden ollessa kiinni hyökkääjät rakensivat internettiin haitallisia streamaus-sivustoja. Sivustojen tarkoituksena oli mahdollistaa käyttäjälle elokuvan katsominen tai lataaminen ilmaiseksi. Sivustolla kuitenkin pyydettiin käyttäjää syöttämään pankkikortin tiedot vahvistamista varten. (Irwin 2022.)

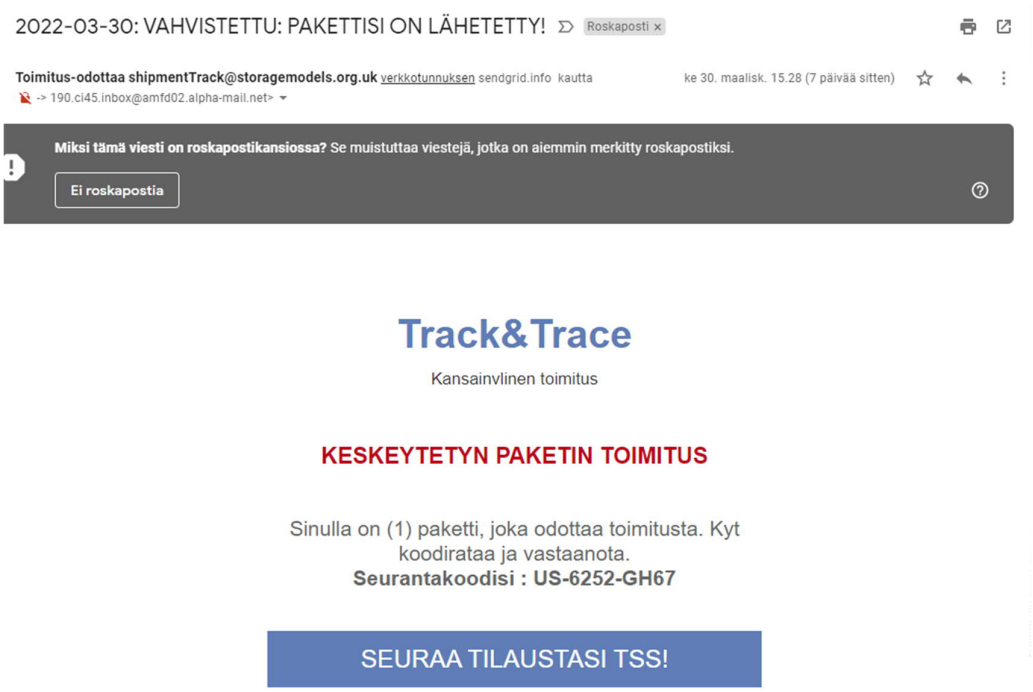
Microsoft Office 365 on yksi käytetyimmistä sovelluksista maailmanlaajuisesti. Joten yhtenä suurimmista tietojenkalastelu teemoista käytettiin Office 365 -palvelua. Yksi suurimmista kalasteluhyökkäyksistä toteutettiin esittämällä, että käyttäjälle on jätetty ääniviesti. Viesti sisälsi haitallisen liitteen, joka peitettiin näyttämään käyttäjälle jätettynä ääniviestinä. Kun käyttäjä avasi haitallisen liitetiedoston käyttäjää pyydetiin vahvistamaan väärennetty reCAPTCHA-koodi, jonka jälkeen käyttäjä siirrettiin väärennetylle Microsoft O365 -kirjautumissivustolle. Sivusto käytti Microsoftin O365 -kirjautumissivustoa, sekä organisaatioiden logoja sivuston luotettavuuden lisäämiseksi. Sivustolla pyydettiin käyttäjien käyttäjätunnusta sekä salasanaa. Henkilöt, jotka syöttivät käyttäjätunnuksen ja salasanan, saivat vahvistuksen, että validointi onnistui. Todellisuudessa käyttäjän tunnus ja salasana vuodettiin hyökkääjille. (Irwin 2022.)

Huhtikuussa 2021 hyödynnettiin väärennettyä PlayStation 5-arvontaa kalasteluhyökkäyksissä. Sähköposti sisälsi väärennetyn arvontalinkin. Käyttäjää pyydettiin syöttämään arvontasivustolle sähköpostiosoitteensa. Hyökkäyksen onnistumiseksi sähköpostin luotettavuutta pyrittiin lisäämään käyttämällä esimerkiksi Playstation 5 -konsolin kuvaa. (Irwin 2022.)

4 Tietojenkalastelun toteutustapoja

4.1 Sähköpostihuijaukset

Sähköpostin avulla hyökkääjä lähettää tuhansia sähköposteja eri henkilöille. Näistä lähetetyistä viesteistä hyökkääjä toivoo, että edes prosentuaalisesti muutama ihminen lankeaa huijaukseen. Huijauksessa tyypillisin toimintapa on luoda sähköposti, joka pyytää käyttäjää tekemään jotain. Esimerkiksi vahvistamaan käyttäjätilin tai uhata käyttäjätilin umpeutumisesta. (Phishing attacks n.d.). Sähköpostihuijauksissa sähköpostin lähetysosoite ja linkit pyritään saamaan näyttämään mahdollisimman aidon palvelun kaltaisilta. Jos käyttäjä klikkaa sähköpostissa olevaa linkkiä niin tässä kohtaa siirrytään hyökkääjän tekemällä sivustolle. Sivustolla yleensä pyydetään täyttämään omat tiedot ja vahvistamaan nämä. Mahdollisesti myös sivustolta pyydetään lataamaan jotain, jonka avulla hyökkääjä asentaa haittaohjelman käyttäjän koneelle. (Muhammet 2018.)



Kuvio 7 Esimerkki sähköpostihuijauksesta (Opiskelijan saama sähköposti)

Yllä olevassa kuviossa 7 on esimerkki opiskelijan saamasta sähköpostihuijauksesta. Kuviosta voidaan havaita, että kyseessä on kalastelu seuraavien merkkien osalta. Suomennos on virheellinen, josta puuttuu kokonaan ääkköset. Viestissä oleva ”seuraa tilaustasi tss!” linkki vie epäilyttävälle

sivustolle. Normaalissa tilanteessa linkistä tulisi jo pystyä havainnoimaan onko kyseessä aito sivusto. Lähettäjäosoite ei viittaa logistiikkayrityksen osoitteeseen.

4.1.1 Linkit sähköpostihuijauksissa

Sähköpostihuijauksessa käytetään usein linkkejä. Linkkien ulkomuoto pyritään saamaan näyttämään mahdollisimman aidolta. Niin, että käyttäjä ei erota onko kyseessä aito sivusto. Väärin kirjoitetut osoitteet ovat yksi yleisimmistä tavoista saada käyttäjä avaamaan kyseisen sivuston. Huijauksissa käytetään linkkejä, jotka näyttävät aidolta, mutta tosiasiassa vievät käyttäjän huijaussivustolle. Tämä on mahdollista HTML-koodin avulla. Tarkoituksena on, että käyttäjä kuvittelee menevänsä aidolle sivustolle eikä välttämättä huomaa, että kyseessä on huijaussivusto. (Hadnagy, Fincher & Dreeke 2015.)

Kuten aiemmassa kappaleessa mainittiin, on hyökkääjien tavoitteena saada näyttämään osoitteet mahdollisimman aidoilta. Tämän havainnollistamiseksi käydään läpi yksi esimerkki, miten käyttäjiä huijataan. Sähköpostitse saapuu esimerkiksi huijaussähköposti otsikolla ”Salasanasi on vanhenemassa” (Kuvio 8). Viesti sisältää linkin, joka on muotoa minunorganisaatio.salasananuusiminen.com. Jos kyseessä olisi aito viesti niin linkin tulisi olla esimerkiksi muotoa minunorganisaatio.fi/salasananuusiminen. Tässä esimerkissä aikaisemmin mainitun osoitteen voi omistaa kuka tahansa eli tässä tapauksessa huijari. Tällä tavoin käyttäjää yritetään saada uskomaan, että viestissä oleva linkki todellisuudessa olisi organisaation omistuksessa oleva osoite. Tavallisessa huijaussähköpostissa linkki sisältää joko virheellisesti kirjoitetun osoitteen tai alitoimialueen kuten esimerkissä on kuvattu. (Phishing attacks. n.d.)

Kuvio 8 Haitallisen linkin esimerkkikuva (Opiskelijan kuva)

4.2 Käyttäjän manipulointi

Käyttäjän manipuloinnilla (englanniksi Social engineering) tarkoitetaan hyökkäystekniikkaa, jota käytetään laajasti kyberhyökkäyksissä. Manipulointi kohdistuu kyberhyökkäyksen heikoimpaan lenkkiin eli käyttäjään.

4.2.1 Mitä käyttäjän manipulointi tarkoittaa?

Toisinkuin järjestelmiä ja verkkoa, käyttäjää ei voida suojata manipuloinnilta erilaisten työkalujen esimerkiksi palomuurien tai virustorjunnan avulla. Käyttäjien manipuloinnilla on huomattavasti korkeampi taloudellinen hyöty verrattuna siihen, jos hyökkääjä käyttäisi esimerkiksi 100 tuntia yrittäessään hyökätä suojattua järjestelmää vastaan. (Ozkaya 2018.) Myös Barbosa, Breda ja Morais (2017) ovat sitä mieltä, että käyttäjä on kyberhyökkäyksen heikoin lenkki ja käyttäjän avulla hyökkäys voidaan toteuttaa koskematta tietoturvallisesti suojattuja järjestelmiä vastaan.

4.2.2 Missä käyttäjän manipulointia ilmenee?

Nykypäivänä käyttäjät paljastavat itsensä helposti manipuloinnilla tehtäviä hyökkäyksiä varten. Elämme ajassa, jossa käyttäjät elävät elämäänsä sosiaalisissa medioissa. Käyttäjät paljastavat tietoja jokapäiväisestä elämästä esimerkiksi perheestä ja työpaikasta. Nykyään internetissä Facebookissa, Twitterissä, Instagramissa ja Snapchatissa on hyökkääjän mahdollista kerätä tietoa käyttäjän persoonallisuudesta (Ozkaya 2018). Kuitenkin Christopher ja Paul (2021) viittaavat omassa kirjassaan siihen, että käyttäjän manipulointi ei aina ole pahaan tarkoitukseen. Käyttäjän manipulointia kuten mitä tahansa työkalua voidaan käyttää joko pahaan tai hyvään tarkoitukseen.

4.2.3 Käyttäjän manipuloinnin eri menetelmät

Hyökkäykset voidaan jakaa kahteen eri kategoriaan. Metsästykseen, englanniksi hunting, tai tiedon keräämiseen, englanniksi farming. Metsästys-lähestymistapa pyrkii toteuttamaan sosiaalisen manipuloinnin hyökkäyksen minimaalisella vuorovaikutuksella kohteen kanssa. Kun määritetty tavoite on saavutettu ja tietoturvaloukkaus todettu, viestintä todennäköisesti lopetetaan. Tämä on yleisimmin käytetty menetelmä kyberhyökkäysten tukemiseen, ja toimintatapa sisältää pääsääntöisesti yhden kohtaamisen. Tiedon keräämistä ei usein harjoiteta, mutta tätä tekniikkaa voidaan

kuitenkin käyttää tilannetarkoituksiin. Hyökkääjä pyrkii solmimaan suhteen uhriin saadakseen tietoa pidemmäksi ajaksi. Koko prosessin aikana vuorovaikutus voi muuttua, kohde voi oppia totuuden ja hyökkääjä voi yrittää lahjoa tai kiristää kohdetta turvautuen näin perinteiseen rikolliseen käyttäytymiseen. (Barbosa, Breda & Morais 2017, 2.)

4.3 Puheluhuijaukset (soitto)

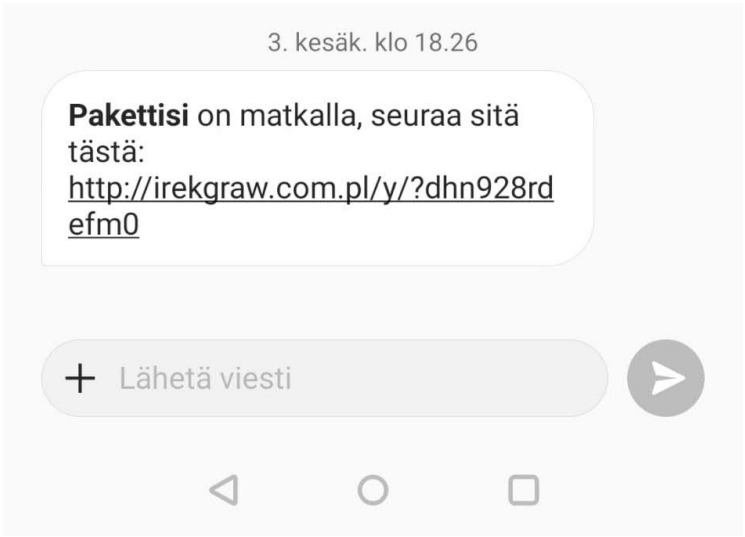
Puheluhuijauksien periaatteet ovat samat kuin esimerkiksi tekstiviestihuijauksissa, mutta huijaukset tapahtuvat joko ääniviesteillä tai puheluilla (Bahar 2022). Rikollisten puhelinnumerot on muutettu näyttämään esimerkiksi suomalaisesta puhelinnumerosta tulevasta puhelusta. Saapuva puhelu voi tulla todellisuudessa eri numerosta kuin puhelimessa näkyvä numero on. Kyberturvallisuuskeskus (2020) toteaa: ”Kyberturvallisuuskeskukselle on raportoitu satoja puhelinnumeroita, joista huijaussoittoja on tullut. Useimmiten huijaussoitot tulevat esimerkiksi numeroista +35840..., +35845..., 09-alkuisista numeroista, tai muiden kotimaisten telealueiden suuntanumeroista. Myös yritysnumeroita ja samoja numeroita ilman ulkomaan suuntanumeroa näkyy paljon.”

4.4 Tekstiviestihuijaukset

Tekstiviestihuijaukset ovat käytännössä identtisiä sähköpostihuijauksien kanssa, mutta hyökkäyksessä käytetään apuna tekstiviestejä. Tekstiviestihuijauksista käytetään englannin kielistä sanaa smishing, joka tulee sanojen phishing ja sms:n yhdistelmästä. Kyseiset huijaukset kategorisoidaan käyttäjän manipuloinniksi, jossa yritetään saada käyttäjän luottamus tekstiviestissä olevan haitallisen linkin tai tiedoston avaamiseksi. Koska käyttäjät käyttävät nykyään omia matkapuhelimia työssä, on tekstiviestitse saapuvat tietojenkalasteluviestit myös uhka organisaatioille. (What is Smishing and How to Defend Against it n.d.) Monet käyttäjät ovat nykyaikana kyenneet tunnistamaan sähköpostihuijaukset. Tekstiviestitse saapuvat huijaukset mahdollistavat uuden tavan hyökkääjälle pyrkiä käyttäjää avaamaan esimerkiksi haitallisen linkin (Kyberturvallisuuskeskus 2021).

Esimerkki Flubot-haittaohjelmakampanjasta tekstiviestitse alla. Kuviossa 9 on esitetty tekstiviestitse leviävä haitake, jonka tarkoituksena on saada käyttäjä avaamaan haitallinen linkki ja toimimaan linkin pyynnön mukaan. Linkistä on mahdollista havaita, että normaali kuriiripalvelu lähettäisi oman organisaation nimissä olevan linkin tai linkki sisältäisi organisaation omistuksessa

olevan verkkotunnuksen. Linkki itsessään harvoin on haitallinen, mutta linkistä aukeava verkkosivusto on. Kyseistä haittaohjelmakampanjaa on kuvattu tarkemmin kappaleessa 7.4.



Kuvio 9 Esimerkki tekstiviestihuijauksesta (Opiskelijan kuva)

5 Tietojenkalastelulta puolustautuminen

5.1 Puolustautuminen

Tietojenkalastelua vastaan pystytään suojautumaan usealla eri keinoilla. Tässä tutkimuksessa on tuotu aikaisemmin esille, että käyttäjä on heikoin lenkki tietojenkalastelun onnistumisessa. Kalastelua vastaan on myös mahdollista puolustautua teknisillä hallintakeinoilla. Eli kuten tietoturva-asiantuntija haastattelussaan toteaa, on puolustautumiseen käytössä eri keinoja.

> *”SOC arkipäivystäjänä tietojenkalastelun havainnointiin käytetään 3. osapuolen lokienhallintajärjestelmää, jonka avulla pystytään havainnoimaan, onko esimerkiksi käyttäjä vieraillut haitallisella sivustolla. Lokienhallintajärjestelmän avulla pystytään myös havainnoimaan, onko käyttäjän tunnuksilla kirjauduttu tuntemattomasta IP-osoitteesta. Tuntematon IP-osoite viittaa yleensä siihen, että käyttäjän tunnus on vuotanut” (Tietoturva-asiantuntija)*

Jonesin (2020) artikkelissa nostetaan esille mistä taloudelliset menetykset koostuvat, mikäli tietojenkalasteluhyökkäys onnistuu. Listalle nousee esimerkiksi seuraavia asioita: käyttäjätiliä ei voi käyttää, korjausaika, maineelle aiheutuva vahinko, henkisen omaisuuden menetys ja suorat rahalliset tappiot. Tulee kuitenkin huomioida, että taloudelliset hyödyt eivät ole ainoa asia, joita tietojenkalasteluhyökkäyksessä voidaan menettää. Näitä voivat olla esimerkiksi seuraavat: menetetyt tiedot, vaarantuneet tilit ja tunnistetiedot, mainevauriot, sekä haittaohjelmatartunnat mukaan lukien kiristysohjelmat.

5.1.1 Puolustautuminen käyttäjän tietoisuuden avulla

Puolustautumisessa hyökkäyksiä vastaan on käyttäjillä suurin vastuu niiden onnistumisesta sekä epäonnistumisesta. Käyttäjän vastuulla on pyrkiä tunnistamaan, onko kyseessä aito viesti palveluntarjoajalta vai onko kyseessä tietojenkalastelu. Yleisesti ottaen palveluntarjoajat eivät koskaan pyydä käyttäjän sosiaaliturvatunnusta eikä pankkitietoja sähköpostin tai muun viestimen avulla. (Viljanen 2017.). Kuten kuljetussuunnittelija alla toteaa ei organisaatioissa välttämättä kouluteta tietojenkalastelua terminä tai miten sitä tulisi havainnoida.

> *”Organisaatiossamme ei minun aikanani ole koulutettu tai kerrottu tietojenkalastelusta yhtään, vaikka sitä tapahtuu kuitenkin yllättävän usein. Pääsääntöisesti omalla kohdalla kalastelua on tapahtunut tekstiviestien kautta. Sähköpostin avulla kalastelua on saapunut harvemmin ja se on suodattunut suoraan roskapostiksi (Kuljetussuunnittelija)*

Alla on listattu muutamia esimerkkejä, joita käyttäjän tulisi huomata mahdollisesta tietojenkalastelusta (Viljanen 2017).

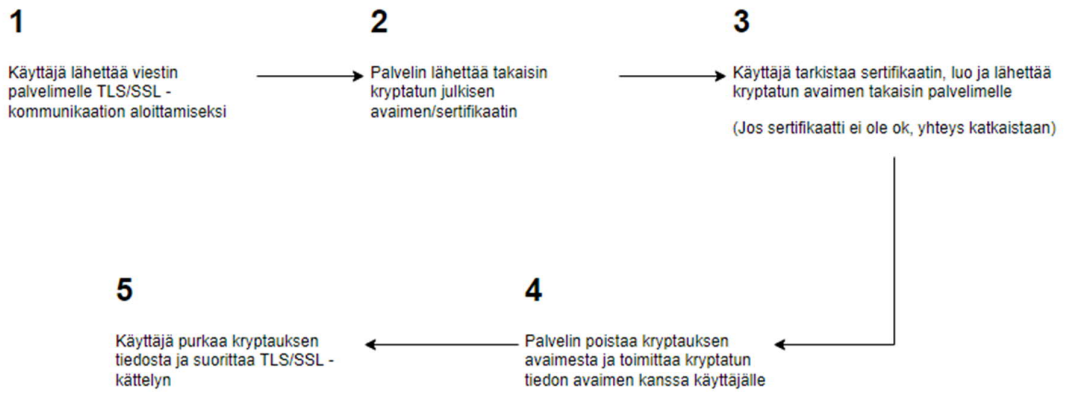
- Tarkista sähköpostiviestin kirjoitusasu
    - Oikeinkirjoitus, sekä mahdollisesti käytetyt logot
- Viestissä kehotetaan toimimaan nopeasti. Eli tällä avulla saadaan käyttäjälle vähemmän aikaa miettiä viestin oikeellisuutta.
- Pankkitietojen, sosiaaliturvatunnusten tai luottokorttitietojen pyyntö
- Viestissä olevat liitteet. Viestin liite voi viitata mihin tahansa sivustoon

5.2 Puolustautuminen teknisillä hallintakeinoilla

Tässä kappaleessa kuvataan tekniset hallintakeinot. Teknisinä hallintakeinoina toimivat sähköpostinsuodatus, kaksivaiheinen tunnistautuminen, virustorjunta sekä sähköpostin todennus. Hallintakeinojen tarkoituksena on toimia ehkäisevinä tapoina puolustautumiseen.

5.2.1 Puolustautuminen varmenteiden avulla

Varmenteella tarkoitetaan digitaalista sertifikaattia verkkosivustolla, jolla taataan suojattu ja turvallinen yhteys käyttäjän ja verkkosivuston välillä. Tämä tarkoittaa käytännössä sitä, että liikenne käyttäjän ja palvelimen välillä on salattua (SSL n.d.). Salatun liikenteen avulla suojellaan käyttäjän henkilökohtaisia tietoja kuten käyttäjätunnus ja salasana, luottokortin tiedot, käyttäjän henkilökohtaiset tiedot esimerkiksi henkilötunnus (What is an SSL certificate – Definition and Explanation n.d.). Varmenteen avulla estetään hakkereita tai tahoja, joiden tavoitteena on varastaa tietoa tai mahdollisesti vakoilla tietoa. Varmenteita on olemassa kolmea eri lajia: EV-sertifikaatti, OV-sertifikaatti ja DV-sertifikaatti. Alla on havainnollistettu kuvion (Kuvio 10) avulla, miten varmenne toimii (SSL n.d.).



Kuvio 10 Varmenteen toiminta (SSL n.d.)

Toisinaan hyökkääjät luovat verkkosivustoja, jotka näyttävät näennäisesti aidolta verkkosivustolta ja tämän avulla pyrkivät siihen, että käyttäjä ostaa tai syöttää tietonsa kalastelusivustolle. On mahdollista, että kalastelusivusto sisältää varmenteen, joka on kuvattu aiemmassa kappaleessa. Eli varmenteen avulla suojautumiseen ei voi luottaa jokaisessa tilanteessa. (What is an SSL certificate – Definition and Explanation n.d.)

5.2.2 Sähköpostinsuodatus

Sähköpostinsuodatin on suunniteltu tunnistamaan hyökkääjiltä tai markkinoijilta saapuvat vaaralliset sähköpostit. Hyökkääjät käyttävät usein sähköposteja, jotka väittävät tarjoavansa hyödyllistä palvelua tai suojelevan sinua välittömältä vaaralta. Ne ovat itse asiassa vain hämäystä, jonka tarkoituksena on saada sinut napsauttamaan linkkiä, joka lataa haittaohjelmia tietokoneellesi tai lähettää sinut vaaralliselle sivustolle. (Spam Filtering n.d.)

Sisältösuodattimet analysoivat sähköpostin sisällä olevan tekstin ja käyttävät näitä tietoja päättääkseen, merkitäänkö se roskapostiksi vai ei. Roskapostiviestien sisältö on usein ennakoitavissa, varsinkin, koska niillä on yleensä samat perustavoitteet: tarjota tarjouksia, mainostaa selkeää materiaalia tai muuten koskettaa ihmisten tunteita ja toiveita, kuten ahneutta tai pelkoa. Sisältösuodattimet voivat etsiä rahaan liittyviä sanoja, kuten "alennus", "rajoitettu aika" tai "tarjous". Suodattimen käynnistämiseksi kohdesanalla on yleensä oltava useita käyttötarkoituksia. Sisältösuodattimet voivat myös tutkia sähköpostissa sopimatonta seksuaalista kielenkäyttöä, joka voi

viitata avoimeen sisältöön. Joissakin kampanjoissa hyökkääjä voi käyttää seksuaalisesti avoimen sisällön sähköposteja houkutellakseen käyttäjiä avaamaan sähköpostin ja sitten napsauttamaan haitallisia linkkejä. (Spam Filtering n.d.)

Mustan listan sähköpostin roskapostisuodattimet estävät sähköpostit lähettäjiltä, jotka on lisätty roskapostittajien luetteloon. Mustalistan suodattimet päivitetään säännöllisesti, koska roskapostittajat voivat vaihtaa sähköpostiosoitteitaan suhteellisen helposti. Jos roskapostittaja vaihtaa sähköpostin verkkotunnuksesta toiseen, sähköposti saattaa silti päästä läpi suodattimen, kunnes se päivitetään ja lähettäjän sähköpostit merkitään jälleen roskapostiksi. Organisaation on myös mahdollista käyttää omaa mustan listan roskapostisuodatusta, jonka avulla voidaan määritellä organisaation haluamansa sähköpostiosoitteet estetyksi. (Spam Filtering n.d.)

Kuviossa 11 on esimerkki mustan listan suodatuksesta, jonka avulla saapunut sähköposti on siirretty karanteeniin. Riippuen sähköpostisuodattimen toiminnasta, osoitteiden lisääminen mustalle listalle saattaa tapahtua myös manuaalisesti riippuen suodattimen valmistajasta sekä konfiguraatiosta.

Kuvio 11 Roskapostisuodattimen karanteeniraportti (Opiskelijan saama sähköposti)

Otsikkosuodattimet tutkivat sähköpostin otsikon nähdäkseen, voiko se olla peräisin laittomasta lähteestä. Tämä voi sisältää IP-osoitteita, joita roskapostittajat yleensä käyttävät. Se voi myös sisältää tietoja, jotka osoittavat, että sähköposti on vain yksi kopio useista sähköpostiviesteistä,

jotka on lähetetty samanaikaisesti ennalta organisoiduille vastaanottajaryhmille. (Spam Filtering n.d.)

Suodattimen avulla voidaan määrittää erityisiä sääntöjä, joita voidaan soveltaa kaikkiin tuleviin sähköposteihin. Jos sähköpostin sisältö tai alkuperä vastaa jotakin säännöistä, se voidaan lähettää automaattisesti roskapostikansioon. Otsikkosuodattimen avulla voidaan esimerkiksi asettaa suodattimen etsimään tiettyjä sanoja tai lauseita sähköpostin tekstiosasta. Jos nämä sanat ovat olemassa, viesti lähetetään roskapostikansioon. Sääntöihin perustuva roskapostisuodatus on hyödyllinen myös tiettyihin lähettäjiin kohdistamisessa. Suodatin voidaan määrittää etsimään tietoja verkkotunnuksesta, josta sähköposti tulee, tai sen lähettäjän nimestä. (Spam Filtering n.d.)

Suodattimien avulla on myös mahdollistaa suodattaa tyypilliset liitetiedostojen tyypit. Suodatuksen avulla voidaan esimerkiksi estää .exe eli suoritettavien tiedostojen lähettäminen sähköpostin välityksellä. Liitetiedostotyyppien estämisellä voidaan ehkäistä hyökkääjien mahdollisuutta lähettää haitallisia tiedostoja sähköpostin välityksellä. (Anti-malware protection FAQ n.d.)

5.2.3 Kaksivaiheinen tunnistautuminen (2FA)

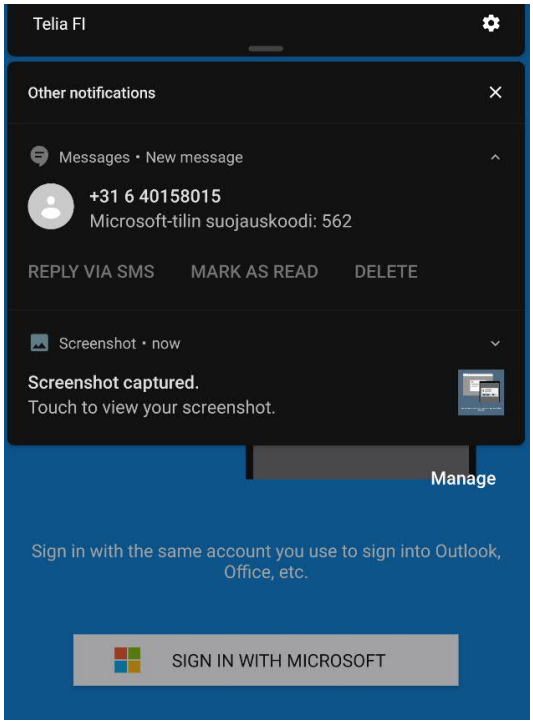
Kaksivaiheinen tunnistautuminen (2FA) on ylimääräinen suojaustaso, jolla varmistetaan, että verkkotiliin pääsyä yrittävät ihmiset ovat sitä, mitä he sanovat olevansa. Ensin käyttäjä syöttää käyttäjätunnuksensa ja salasanansa. Sen sijaan, että hyökkääjä pääsisi kirjautumaan tilille suoraan, heidän on annettava toinen tieto. Tämä toinen tekijä voi tulla jostakin seuraavista luokista. (What is Two-Facton Authentication (2FA) n.d.):

- Jotain mitä tiedät: Tämä voi olla henkilökohtainen tunnusnumero (PIN), salasana, vastaukset "salaisiin kysymyksiin" tai tietty näppäinpainalluskuvio
- Jotain mitä sinulla on: Yleensä käyttäjällä on hallussaan jotain, kuten luottokortti, älypuhelin tai pieni laitteistotunnus
- Jotain, mitä olet: Tämä luokka on hieman edistyneempi, ja se voi sisältää sormenjäljen, iirisskannauksen tai äänijäljen biometrisen kuvion

Mikäli käyttäjän tunnus on vuodettu eli hyökkääjällä on hallussaan käyttäjän tunnus ja salasana, 2FA:n avulla käyttäjän tilille ei ole mahdollista kirjautua. Joten vaikka salasanasi varastettaisiin tai

puhelimesi katoaisi, on erittäin epätodennäköistä, että rikollinen pääsisi kirjautumaan tilille. Tarkasteltaessa asiaa toisesta näkökulmasta, jos kuluttaja käyttää 2FA:ta oikein, verkkosivustot ja sovellukset voivat luottaa käyttäjän henkilöllisyyteen ja avata tilin lukituksen. (What is Two-Facton Authentication (2FA) n.d.)

Alla olevassa kuviossa 12 on havainnollistettu kaksivaiheisen tunnistautumisen toiminta. Kyseessä on esimerkki yhdestä tavasta käyttää 2FA:ta, mutta vaihtoehtoisia tapoja on olemassa, kuten yllä on kuvattu. Tässä kohtaa käyttäjä on syöttänyt jo tunnuksen ja salasanan verkkosivustolle. Koska 2FA on käytössä, niin käyttäjän tulee syöttää vielä Microsofilta saatu suojauskoodi ennen verkkosivustolle kirjautumista.



Kuvio 12 Esimerkki kaksivaiheisesta tunnistaumisesta (Opiskelijan kuva)

5.2.4 Virustorjunta

Virustorjunnalla tarkoitetaan erityistä ohjelmistoa, jonka tavoitteena on tarjota parempaa suojausta kuin mitä käyttöjärjestelmät tarjoavat (esimerkiksi Windows tai Mac OS X). Virustorjunnan päätarkoituksena on toimia ehkäisevänä ratkaisuna. Toisinaan virustorjunnan ehkäisevä ratkaisu ei

onnistu estämään haitallisen ohjelman pääsyä työasemalla, joten virustorjunnan tehtävänä on myös puhdistaa työasemalta saastuneet ohjelmat tai poistaa kokonaan saastunut ohjelma työasemalta. Kyseiset ohjelmistot käyttävät useita eri menetelmiä saastuneen ohjelmiston havaitsemiseen. Mainittuja menetelmiä ovat heuristiikkaan perustuva havainnointi ja allekirjoitukseen perustuva havainnointi. (Koret & Bachaalany 2015, 3.)

Allekirjoitukseen perustuva havainnointi on yleisin käytetty menetelmä. Jokaisella virustorjunta ohjelmistolla on sanasto, joka sisältää näytteitä haitallisesta koodista, joita kutsutaan allekirjoituksiksi. Kun tiedosto avataan, virustorjunta vertailee avattua tiedostoa aikaisemmin kuvattuun sanastoon. Jos virustorjunta havaitsee, että sanastosta löytyy vastaava tiedosto, niin se laukaisee ennalta määriteltyjä toimintoja estääkseen viruksen leviämisen. Koska uusia viruksia ja haittaohjelmia julkaistaan joka päivä, ei allekirjoitukseen perustuva havainnointi kykene estämään kaikkia viruksia ja haittaohjelmia. (Anand 2012.)

Heuristiikkaan perustuva havainnointi perustuu epäilyttävän toiminnan havaitsemiseen. Kyseinen menetelmä eroaa allekirjoitukseen perustuvasta havainnoinnista siten, että se pyrkii havainnoimaan kaikkien ohjelmistojen toimintaa. Heuristiikkaan perustua havainnointi ei kykene havaitsemaan uusia viruksia tai haittaohjelmia. Esimerkiksi jos tiedosto yrittää kirjoittaa tietoa suoritettavaan tiedostoon se laukaisee käyttäjälle hälytyksen mahdollisesti epäilyttävästä toiminnasta. (Anand 2012.)

5.2.5 Sähköpostin todennus

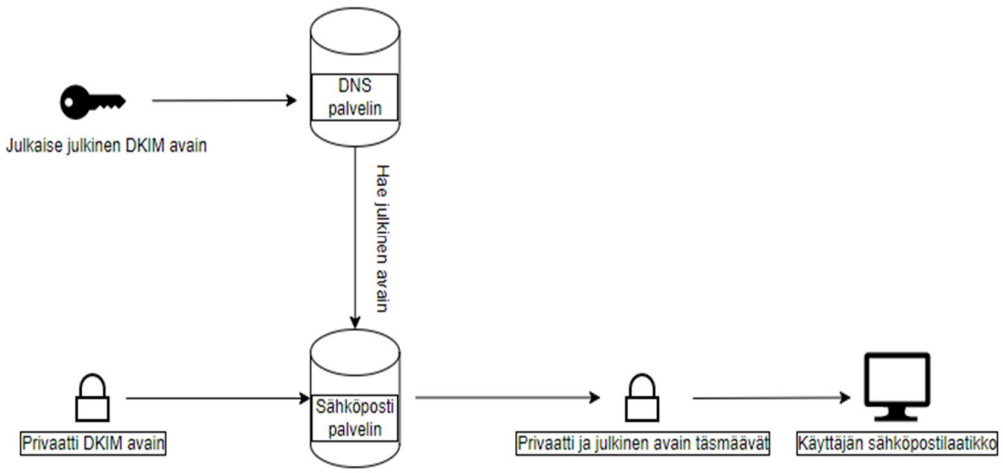
Sähköpostin todentamisella tarkoitetaan kolmea eri menetelmää: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) ja Domain-based Message Authentication, Reporting and Conformance (DMARC). Nämä ovat menetelmiä ja protokollia sähköpostin huijauksen estämiseksi ja sähköpostipalvelimen aitouden tarkistamiseksi. SPF ja DKIM voidaan ottaa käyttöön itsenäisesti, kun taas DMARC käyttää SPF:n ja DKIM:n yhdistelmää verkkotunnuksen suojaamiseen. (SPF, DKIM & DMARC overview n.d.)

SPF on menetelmä, joka todentaa onko sähköposti lähetetty oikealta sähköpostipalvelimelta käyttäen lähettäjän tietoja sähköpostin toimituksesta. Sallitut sähköpostipalvelimet tai palvelimet

määritellään verkkotunnuksen omistajan toimesta. SPF käyttää lähettäjän verkkotunnusta selvittääkseen Domain Name System (DNS)-palvelusta onko lähettäjällä oikeus lähettää sähköpostia. Esimerkiksi, kun paypal.com-sivustolta tuleva sähköposti pyytää käyttäjien tilin ja salasanan vahvistamista, SPF voi tarkistaa, onko se todellakin lähetetty verkkotunnuksesta paypal.com vai onko se osa huijausta. (Görling 2007.)

DKIM on menetelmä, joka on suunniteltu tunnistamaan huijaussähköpostit tarjoamalla mekanismin, jonka avulla sähköpostin vastaanottava taho voi tarkistaa sähköpostin saapuneen hyväksytystä verkkotunnuksesta (Dedhia 2016). DKIM:n toiminta perustuu julkiseen ja privaattiin avaimeen. Avaimia verrataan keskenään, ja mikäli avaimet vastaavat toisiaan, sähköposti saapuu hyväksytystä verkkotunnuksesta. Julkinen avain sijaitsee lähetetyn sähköpostin otsikkotiedoissa. Julkinen avain sisältää tarvittavat tiedot allekirjoituksen todentamiseen. (What is DKIM? n.d.)

DKIM:n toiminta on kuvattu alla olevassa kuviossa 13. Julkinen avain on sijoitettuna DNS-palvelimelle, jota verrataan privaatin avaimen kanssa. Privaatti avain sijaitsee sähköpostipalvelimessa. Jos privaattiavain vastaa julkisen avaimen tietoa, niin voidaan todeta, että DKIM allekirjoitus on onnistunut ja viesti päätyy käyttäjän sähköpostilaatikkoon. Mikäli avaimet eivät vastaa toisiansa niin vastaanottava sähköpostipalvelin määrittelee mitä viestille tapahtuu. (What is DKIM? n.d.)



Kuvio 13 DKIM avaimen toiminta (What is DKIM? n.d.)

DMARC on sähköpostin vahvistusjärjestelmä, joka on suunniteltu tunnistamaan ja estämään sähköpostin huijaus. Se tarjoaa mekanismin, jonka avulla vastaanottava organisaatio voi tarkistaa, että verkkotunnuksen järjestelmänvalvojat ovat valtuuttaneet verkkotunnuksesta saapuvan postin ja ettei sähköpostia (mukaan lukien liitteitä) ole muutettu kuljetuksen aikana. Sen tarkoituksena on siis torjua tiettyjä tekniikoita, joita usein käytetään tietojenkalastelussa ja sähköpostiroskapostissa. Näitä ovat esimerkiksi sähköpostit, joissa on väärennetyt lähettäjän osoitteet ja jotka näyttävät olevan peräisin laillisilta organisaatioilta. (Dedhia 2016.)

DMARC on rakennettu kahden aiemmin kuvatun mekanismin päälle: SPF:n ja DKIM:n. Sen avulla sähköpostin lähettäjä voi julkaista käytännön siitä, mitä mekanismia (DKIM, SPF tai molempia) käytetään sähköpostin lähettämisessä ja kuinka vastaanottajan tulee käsitellä epäonnistumisia. Lisäksi se tarjoaa raportointimekanismin näiden käytäntöjen mukaisesti suoritetuista toimista. Se siis koordinoi DKIM:n ja SPF:n tuloksia ja määrittelee, missä olosuhteissa loppukäyttäjien usein näkyvää Lähettäjä: -otsikkokenttää tulisi pitää laillisena. DMARC-asetukset antavat mahdollisuuden valvoa, asettaa karanteeniin ja hylätä sähköpostit, jotka on havaittu huijauksiksi tai roskapostiksi. (Dedhia 2016.)

6 Organisaation osoitusvelvollisuus ja vastuut tietojenkalastelussa

Organisaation on usein vaikea todistaa, mitä henkilökohtaisia tietoja hyökkääjä on saanut. Koska hyökkääjällä on esimerkiksi samat oikeudet Office 365 -tiliin kuin tilin haltijalla, hänellä on pääsy kaikkiin tilin omistajan tietoihin. Käytännössä tämä tarkoittaa käyttäjän postilaatikoiden sisältöä, organisaation koko osoitekirjaa ja OneDriven sisältöä. Lisäksi hyökkääjä voi kirjautua muihin organisaation tietojärjestelmiin, joita voidaan käyttää Office 365:n tai Internetin kautta, kuten Sharepoint-palveluihin. (Tietojen kalasteluun perustuvat tietoturvaloukkaukset n.d.)

Organisaation tulee siis pystyä näyttämään, mitä tietoa hyökkääjä on saanut, ja sulkea pois tiedot, jotka eivät olisi voineet joutua vääriin käsiin hyökkäyksessä. Usein unohdetaan, että hyökkääjä on rikollinen, joka kerää tietoa ja pyrkii muuttamaan kerätyt tiedot rahaksi. On hyvin todennäköistä, että kaikki hyökkääjän käyttämät tiedot kerätään mahdollista myöhempää käyttöä varten. Lisäksi saatujen tietojen tarkoituksena voi olla muuta vahinkoa, kuten yksilöiden kiristämistä tai petosyritystä. (Tietojen kalasteluun perustuvat tietoturvaloukkaukset n.d.)

Siksi organisaation tulee kehittää pilvipalveluihin kirjautumista, näiden palvelujen valvomista ja kirjausominaisuuksien hyödyntämistä. Lisäksi tulee harkita, välitetäänkö ja säilytetäänkö sähköpostissa henkilötietoja sisältävät asiakirjat, kuten ansioluettelot, sairauslomatodistukset, työsopimukset, passikopiot tai yksityiskohtaiset asiakastiedot. (Tietojen kalasteluun perustuvat tietoturvaloukkaukset n.d.)

> *” EU:n tietosuoja-asetuksen 5 artikla toteaa rekisterinpitäjän osoitusvelvollisuudesta muun muassa seuraavaa: ”henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”)” (Tietojen kalasteluun perustuvat tietoturvaloukkaukset. n.d.)*

7 Käytännön esimerkkejä

7.1 Käyttäjän manipulointi

Yksi suurimmista hyökkäyksistä koskien käyttäjän manipulointia suoritettiin vuonna 2014 organisaatioon nimeltään Yahoo!. Hyökkäyksen avulla hyökkääjät saivat käsiinsä yli 500 miljoona käyttäjä tietoa. FBI on vahvistanut, että hyökkäyksessä käytettiin sosiaalista manipulointia saadakseen hyökkääjät ohittamaan tällaisten tietojen suojaamiseen käytettyjen tietoturvatyökalujen ja -järjestelmien kerrokset. Hyökkäyksessä käytettiin apuna sähköpostia. Käyttäjille lähetettiin tietojenkalastelusähköposti, joka mahdollisti hyökkäyksen toteuttamisen. (Ozkaya 2018.)

Toisena esimerkkinä verkkolaitteita valmistava yritys Ubiquiti Networks, joka joutui manipuloinnin kohteeksi vuonna 2015. Hyökkääjät pystyivät keräämään tietoja toimitusjohtajasta ja omaksuivat tehokkaasti hänen personallisuuteensa. He käyttivät tätä tietoa hyväkseen ja esiintyivät toimitusjohtajana talousosastolle. Hyökkääjät väittivät talousosastolle, että organisaatio, joka toimii ulkomailla, on vaihtanut maksutapaansa. Talousosastolla työskennellyt käyttäjä ei epäillyt kyseistä pyyntöä vaan siirsi rahat väärennetyn organisaation tilille. Käyttäjä havaitsi vasta myöhemmin, että pyyntö ei tullut oikealta toimitusjohtajalta. Myöhemmin tutkimuksissa havaittiin, että tietoturvan järjestelmät olivat edelleen käytössä eikä niihin ollut tehty muutoksia. Tutkimuksessa todettiin, että hyökkäys oli toteutettu puhtaasti käyttäjän manipuloinnin avulla. (Ozkaya 2018.)

7.2 Tietojenkalastelu sähköpostit

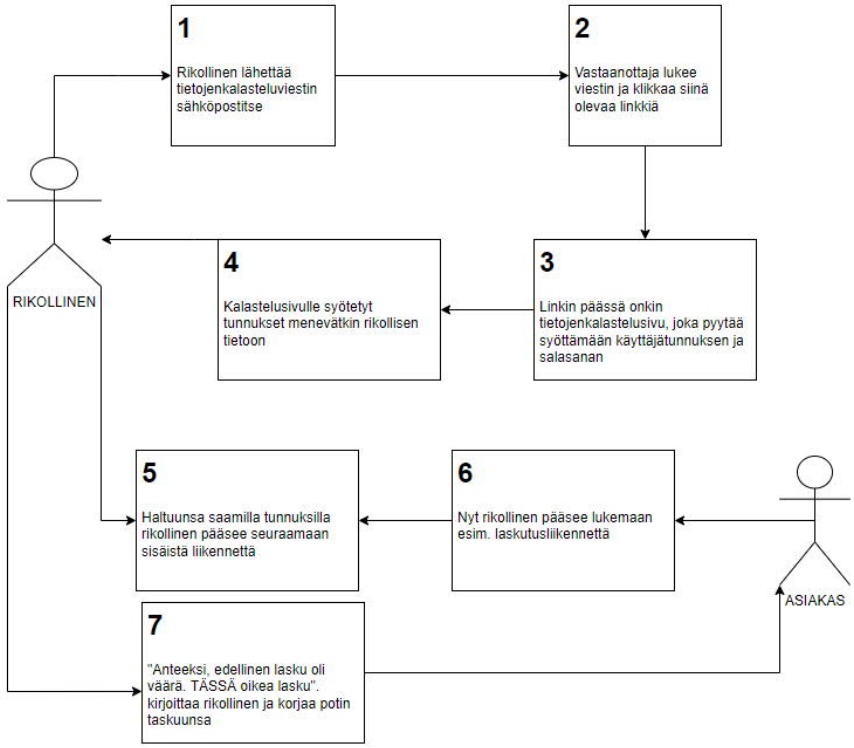
Hilary Clintonin kampanjan aikaan hänen puheenjohtajansa John Podestan sähköposti kaapattiin. Kaappaus tapahtui hyökkääjän esittäydyttyä Googlen työntekijänä. Sitten he kertoivat hänelle, että hänen salasanansa oli vaarantunut, ja antoivat väärän linkin salasanan vaihtopaikkaan. John lopulta syötti tunnuksensa sivustolle ja antoi täten kirjautumistietonsa hyökkääjille. (Gilbert 2016.)

Hyökkäyksen onnistuttua hyökkääjät paljastivat 50 000 sähköpostia. Myöhemmin WikiLeaks-sivusto paljasti näistä sähköposteista tuhansia. Jotkut näistä sähköposteista ovat johtaneet epämukavuuteen demokraattisessa puolueessa 8. marraskuun vaaleja edeltävänä viimeisenä kuukautena. Paljastaen Clintonin viime vuoden presidentinvaalikampanjan sisäisen toiminnan, epävarmuuden ja kaiken. (Gilbert 2016.)

7.3 Office 365 -huijaus

Sähköpostihuijauksen käytännön esimerkkinä on kyberturvallisuuskeskuksen vuosikatsauksessa esiin tuotu Office 365 -huijaus. Hyökkäys kasvatti kyberturvallisuuskeskuksen Office 365 tikettien määrän yli 30:een kesäkuusta 2018 eteenpäin, kun esimerkiksi helmikuussa 2018 tikettien määrä oli vain neljä. (Tietoturvan vuosi 2018.)

Kyseinen kampanja eli hyökkäys oli lähinnä kohdennettu vain yritysten johdolle sekä IT-ylläpidolle. Yksi osa, jota hyökkäyksessä tehtiin, oli sähköpostien edelleen ohjaus Office 365 Exchange Online palvelussa. Tämän havaitseminen tavallisesti käytössä olevien ylläpitotyökalujen kanssa on hankalaa. (Tietoturvan vuosi 2018).



Kuvio 14 Office 365 -huijauksen vaiheet (Tietoturvan vuosi 2018)

Yllä olevassa kuviossa 14 on havainnollistettu hyökkäyksen vaiheet. Hyökkäyksessä käytettiin normaaliin tapaan sähköpostia hyökkäyksen toteuttamiseen. Kun käyttäjä oli mennyt syöttämään tun-

nukset haitalliselle verkkosivustolle, niin voidaan havaita, että näiden avulla hyökkääjä pääsee lukemaan sähköpostiliikennettä. Tämän tiedon avulla rikollinen kykenee väärentämään laskupohjan, jota käyttäjä oli aikaisemmin käsitellyt sähköpostissa. Tämän tiedon avulla rikollinen pystyi lähettämään väärennetyn laskun, jonka käyttäjä maksoi. Tässä kohtaa rahat siirtyivät rikollisen tilille.

7.4 Flubot-haittaohjelmakampanja

Flubot -haittaohjelmakampanjaa on nähty Suomessa viimeksi kesällä 2021. Haittaohjelmakampanjan tavoitteena oli saada käyttäjät avaamaan tekstiviestitse lähettyä haitallista linkkiä, jonka tavoitteena oli asentaa käyttäjän matkapuhelimeen haitallisen sovelluksen. Pelkästään linkin avaaminen ei asentanut haittaohjelmaa vaan sivusto pyysi suostumusta asentamiseen. Poikkeuksena kampanjassa oli se, että se kohdistui vain Android -käyttöjärjestelmiin. Muiden käyttöjärjestelmien osalta haitallisilla sivustoilla pyrittiin keräämään käyttäjiltä esimerkiksi luottokorttien tietoja. (Kyberturvallisuuskeskus 2021.)

Tekstiviestejä lähetettiin vuorokauden sisällä jopa 70 000 kappaletta. Tekstiviesteistä oli käytössä monia eri variaatioita. Yhtenä yhtenäistävänä tekijänä viestit eivät sisältäneet ä- ja ö-kirjaimia, joka osaltaan kuvastaa jo sitä, että viesti ei ole aito (Kyberturvallisuuskeskus 2021). Esimerkki haitallisesta tekstiviestistä on esitetty kuviossa 9.

8 Tutkimuksen toteutus

Tutkimus toteutettiin tutustumalla aiheeseen liittyviin artikkeleihin, raportteihin ja kirjallisuuteen. Työssä käytettiin pohdinnassa myös opiskelijan omaa työnkuvaa apuna. Työn tarkoituksena oli tutustua tietojenkalasteluun terminä ja sitä vastaan puolustautumiseen. Tutkimusmenetelmänä työssä käytettiin kvalitatiivista menetelmää, koska tutkimuksen tarkoituksena oli avata teoreettisesti ja havainnollistamisen pohjalta tietojenkalastelua.

Työn tarkoituksena oli ymmärtää teorian avulla tutkittavaa asiaa, sekä kokonaisvaltaisen ja syvemmän käsityksen saamista tutkittavasta asiasta. Tutkimuksessa käytiin myös läpi yleisimpiä tapoja puolustautua tietojenkalastelua vastaan. Työstä rajattiin pois tekniset toteutukset ja teknologioiden läpikäynti. Puolustautumisen osalta työssä käsiteltiin termistöä ylätasolla.

Aiempia tutkimuksia osittain tähän opinnäytetyöhön liittyen on olemassa. Aiheesta on tehty opinnäytetöitä sekä kirjallisuutta. Aiemmista tutkimuksista on kerätty aineistoa myös tähän työhön ja niihin on viitattu lähteissä. Aineistoa kerättiin laadullisen tutkimuksen avulla monista eri lähteistä. Koska kyseessä on teoriaan pohjautuva työ, ei tieto muutu, joten tiedon pysyvyys on huomioitu toteutuksessa. Haastatteluiden osalta aineisto on kerätty alla kuvatulla menetelmällä.

Haastatteluita opinnäytetyössä toteutettiin viisi kappaletta eri aloilla työskentelevien henkilöiden kanssa. Haastatteluiden pääpainopiste oli selvittää miten henkilöt tunnistavat tietojenkalastelun. Haastattelut toteutettiin teemahaastatteluina, joita käytettiin työn lainauksissa. Haastatteluiden tarkoituksena ei ollut kerätä tutkimukseen määrällistä tietoa vaan tarkoituksena oli tuoda kokemuksiin pohjautuvaa tietoa tietojenkalastelun ymmärtämisestä ja onko tietojenkalastelua perehdytetty / koulutettu organisaatioissa.

9 Tutkimuksen tulokset

Tutkimuksen lähtökohtana oli vastata tutkimuskysymykseen, joka muodostui kahdesta eri osa-alueesta. Työn lopullisena tavoitteena oli avata tietojenkalastelu terminä niin, että kuka vain luettuaan ymmärtää mitä se tarkoittaa. Tämän opinnäytetyön tulokset jakautuvat karkeasti kolmeen osaan: Tietojenkalastelu terminä, puolustautuminen sekä organisaatioiden vastuu tietojenkalastelun estämisessä.

Työssä haastateltiin viittä henkilöä liitteen 1 mukaisesti. Jokaisessa haastattelussa nousi esille, että organisaatioissa ei ole perehdytetty / koulutettu henkilöstöä sillä aikavälillä, kun henkilöt ovat kyseisessä organisaatiossa toimineet. Kun huomioidaan todellisuus, että tietojenkalastelu on yksi suurimmista tietoturvauhista, niin organisaatioiden tulisi kouluttaa paremmin henkilöstöä. Koska haastatteluita toteutettiin vain viiden henkilön osalta, on mahdollista, että organisaatioissa perehdytetään / koulutetaan henkilöstöä vaikkakin kyseiset henkilöt eivät koulutusta olleet saanut.

Kun tarkastellaan tietojenkalastelusivustojen kasvua vuosittain aikaisemmin esitettyyn kuvioon 4, voitiin havaita, että uniikkien tietojenkalastelusivustojen määrä on kasvanut räjähdysmäisesti vuosien 2018–2021 välillä. Tämä osoittaa sen, että koulutus ja perehdyttäminen on tärkeä osa organisaation toimintaa, ottaen huomioon sen, että käyttäjä on heikoin lenkki tietojenkalastelun onnistumisessa. Tarkastellessa historiaa voidaan havaita, että tietojenkalastelu terminä on ollut jo esillä vuodesta 1996. Tutkimuksessa nousi esille myös se, että se on toiseksi kallein hyökkäysvektori vuonna 2021, joka osaltaan kuvastaa sitä, että tietojenkalastelun tietoturvauhka on suuri ja sen taloudelliset menetykset ovat toiseksi suurimmat vuonna 2021.

Tutkimuksessa käytetyn pääsykysymyksen tuloksena voitiin todeta, että tietojenkalastelu on yksi suurimmista tietoturvauhista nykypäivänä. Voitiin siis todeta, että jokaisen internettiä käyttävän henkilön tulisi jollakin tasolla ymmärtää mitä tietojenkalastelu tarkoittaa ja miten sitä vastaan voidaan puolustautua. Kun pohditaan pääkysymyksen tulosta, niin sen onnistumista voidaan arvioida vasta sen mukaan, avaako tämä työ lukijalle pääkysymyksessä esitetyt osa-alueet. Mikäli lukija ymmärtää tietojenkalastelun terminä tämän opinnäytetyön lukemisen jälkeen voidaan todeta, että työn tulos on saavutettu.

Yhtenä alikysymyksenä työssä oli mitä ovat tietojenkalastelumenetelmät. Tietojenkalastelumenetelmiä tutkittaessa voitiin todeta, että COVID-19 on yksi käytetyimmistä menetelmistä sen aiheuttaman pelon vuoksi. Yleisesti menetelminä käytetään tunnettuja asioita kuten elokuvia, konsolivalmistajia sekä Microsoftin tuottamaa O365 -palvelua. Tämä palvelu on maailmanlaajuisesti käytössä ja siksi se koskettaa laajasti organisaatioita.

Tutkimuksessa nousi esiin teknisten hallintakeinojen tärkeys tietojenkalastelun puolustautumisessa. Mitä suurempi määrä tietojenkalasteluhyökkäyksiä pystytään estämään ennen kuin ne päätyvät loppukäyttäjälle, sitä enemmän vähennetään mahdollisten hyökkäyksien onnistumisia. Tätä tulosta voidaan pohjustaa sillä, että tutkimuksen aikana esiin nousi se, että käyttäjä on tietojenkalastelun heikoin lenkki. Teknisiä vaihtoehtoja on useita eli organisaatioilla on mahdollisuus ottaa käyttöön esimerkiksi vain osa hallintakeinoista, jotka auttavat tietojenkalastelua vastaan puolustautuessa.

Työssä selvitettiin myös vuoden 2020 kolmannella neljänneksellä yleisimmät käytetyt liitetiedostotyypit tietojenkalasteluhyökkäyksissä. Yleisin liitetiedostotyyppi oli suoritettavat tiedostot 74 % osuudella. Tämän vuoksi sähköpostinsuodatus on ensiarvioisen tärkeä kalasteluiden torjunnassa kaiken kokoisissa organisaatioissa toimialasta riippumatta. Sähköpostinsuodatuksen yksi oleellisimmista tehtävistä on estää juuri yleisimpien liitetiedostotyyppien läpi pääseminen loppukäyttäjälle.

Tutkimalla organisaatioita niiden koon mukaan, voidaan todeta myös se, että lääkintä ja terveydenhuoltoon kohdistuu eniten tietojenkalasteluhyökkäyksiä. Se on yksi suurimmista toimialoista. Riippumatta organisaation koosta lääkintä ja terveydenhuollon osuus hyökkäyksissä on seuraava: pienissä organisaatioissa 44,7 %, keskikokoisissa 49,2 % ja suurissa 49,3 %.

10 Yhteenveto

Tutkimuksen tarkoituksena oli tuoda esille tietojenkalastelun eri näkökulmat ja selvittää miten nykypäivänä tietojenkalastelua hyödynnetään. Työn tuloksena oli selittää tietojenkalastelu käsitteenä, sekä avata tietojenkalastelun eri toimintatapoja. Tutkimuskysymyksenä työssä oli: Mitä termi tietojenkalastelu tarkoittaa ja miten sitä vastaan voidaan suojautua?

Termiä tietojenkalastelu tutkimuksessa käsiteltiin neljästä eri näkökulmasta: Historia, tavoite, nykytilanne sekä käytännön esimerkit. Näiden tarkoituksena oli avata lukijalle tietojenkalastelu terminä ja tuoda esille kuinka laajasta käsitteestä on kyse. Koska kyseessä on nykypäivänä yksi suurimmista tietoturvauhista, on tärkeää tutkimuskysymyksen kannalta tuoda lukijalle perusteet selkeästi esille. Lopputuloksena tämän aihealueen tutkiminen vastaa tutkimuskysymyksen ensimmäiseen osaan.

Tutkimuskysymyksen toisena aihealueena oli tuoda esille, miten tietojenkalastelua vastaan voidaan suojautua. Tutkimuksessa käsiteltiin aihetta kolmesta eri näkökulmasta: organisaation vastuu puolustautumisessa, käyttäjän vastuu puolustautumisessa sekä tekninen puolustautuminen. Aihealueiden tutkimisessa päätarkoituksena oli havainnollistaa, että käyttäjällä on suurin vastuu tietojenkalastelun onnistumisessa. On myös tärkeä huomioida, että organisaatioilla on vastuu kouluttaa käyttäjiä tietojenkalastelua vastaan. Teknisestä näkökulmasta puolustautumista käsiteltiin viidellä eri menetelmällä. Voidaan siis todeta, että teknisiä hallintakeinoja on olemassa, mutta niiden käyttöönottoa organisaatioissa tulisi huomioida. Hallintakeinojen ylläpitoa ja ajantasaisuutta tulisi organisaatioiden pystyä valvomaan, jolloin hallintakeinot eivät pääse vanhenemaan. Tämän aihealueen tutkiminen vastaa tutkimuskysymyksen toiseen osaan.

Tutkimusmetodologiaksi valitsin tutkimuksessani kvalitatiivisen menetelmän. Tutkimuksessa tutkimusmenetelmän valinta onnistui mielestäni hyvin. Kyseinen menetelmä valittiin siitä syystä, että opinnäytetyön lopputuloksena oli avata lukijalle tietojenkalastelu siten, että kuka vain opinnäytetyön lukenut henkilö ymmärtää mitä se tarkoittaa ja miten sitä vastaan voidaan pyrkiä suojautumaan. Todellisten tapausten tutkiminen auttaa hahmottamaan miltä tietojenkalastelu todellisuudessa näyttää. Jos tutkimusmenetelmäksi olisi valittu esimerkiksi määrällinen menetelmä niin aihetta olisi pitänyt käsitellä matemaattisesta näkökulmasta, joka ei vastaa taas tutkimuskysymykseen.

Opinnäytetyön tekohetkellä aiheesta löytyi paljon tietoa verkkojulkaisuiden sekä raporttien muodossa. Tässä vaiheessa jälkikäteen pohdittuna aiheeseen liittyen oli vaikea löytää kirjallisuudesta lähteitä, sekä niin sanotusti luotettavia lähteitä, joita olisi arvioitu toisten tutkijoiden toimesta. Tämä nousee opinnäytetyössä esille siinä, että lähteinä on käytetty usein verkkojulkaisuita, joiden kirjottajasta ei välttämättä ole mainintaa. Lähteiden aitoutta pyrin vahvistamaan sillä, että etsin aiheeseen liittyen toisen lähteen ja vertasin, onko kirjoitettu teksti vastaavaa kuin käyttämässäni lähteessä.

Tutkimus opetti itselleni sen, että tietojenkalastelu on nykypäivänä yksi suurimmista tietoturvauhista. Tekemäni haastatteluiden pohjalta voitiin todeta, että organisaatioissa ei välttämättä kouluteta henkilöstöä tietojenkalastelun uhkiin. Haastatteluissa kävi ilmi, että tietojenkalastelu terminä ei välttämättä ole tuttu. Tämä altistaa sille, että henkilö ei välttämättä tunnista mahdollista hyökkäystä.

Jatkokehityskohteena olisi mielenkiintoista tutkia tietojenkalastelua teknillisestä näkökulmasta eli siitä, miten tietojenkalasteluhyökkäyksiä todellisuudessa toteutetaan. Tutkimalla tätä aihetta olisi mahdollista saada syvempi tietämys tietojenkalastelusta kokonaisuutena. Tämä mahdollistaisi kokonaisvaltaisemman käsityksen saamisen aiheesta. Koska kyseessä on tietoturvauhka, jonka toteutustavat teknisesti tulee muuttumaan, niin aiheen tutkiminen säännöllisesti olisi jatkokehityksen kannalta oleellista. Tutkimalla tietojenkalastelua teknisestä näkökulmasta mahdollistettaisiin laajempien esimerkkien käyttäminen esimerkiksi koulutusmateriaalissa.

Toisena jatkokehityskohteena olisi tutkia miten eri toimialoihin verrattuna tietojenkalastelukampanjat eroavat toisistaan. Tarkoituksena olisi saada syvempi ymmärrys vaikuttaako toimiala kampanjan tyyppiin. Onko esimerkiksi julkishallinnolliseen organisaatioon kohdennettu kampanja sama kuin mitä finanssialalle? Tämä auttaisi ymmärtämään miten tietojenkalastelua tulisi kouluttaa eri toimialoissa.

Kolmantena jatkokehityskohteena olisi miten organisaatioiden tulisi kouluttaa henkilöstöä tietojenkalastelun tunnistamisessa ja kuinka suuri rahallinen hyöty saataisiin verrattuna mahdollisiin haittoihin verrattuna. Kuten aikaisemmin mainittiin, tietojenkalastelu on yksi kalleimmista hyök-

käysvektoreista eli taloudelliset menetykset voivat olla huomattavia. Koulutuksella voitaisiin mahdollisesti estää tietojenkalastelun onnistuminen. Tutkimuksen päätarkoituksena oli vastata aikaisemmin mainittuun tutkimuskysymykseen. Tähän tutkimuskysymykseen vastaamalla toimeksiantaja voi käyttää tätä tutkimusta esimerkiksi henkilöstön kouluttamiseen. Tutkimus antaa hyvän pohjan toimeksiantajalle ymmärtää mitä tietojenkalastelu on ja sitä myöten mahdollisesti luoda oman koulutuspohjan henkilöstölle.

Jatkokehityskohteena opinnäytetyön tekoprosessissa tulisi kirjata pohdintaa aina työn tekemisen hetkellä. Tällöin työssä nousseet asiat pystyttäisiin tuomaan selkeämmin pohdintaan. Tämä auttaisi tutkijaa myös ajattelemaan jo tekovaiheessa mitä tutkittavassa osa-alueessa on sellaista, joka vastaa esimerkiksi suoraan tutkimuskysymykseen. Toisena jatkokehityskohteena tulisi perehtyä huomattavasti aikaisemmin olemassa olevaan tutkimusmateriaaliin, jopa jo ennen työn aloittamista. Tätä voidaan perustella sillä, että pystytään jo ennen työn aloittamista varmistamaan, että aiheesta löytyy materiaalia ja lähteitä työn tekoa varten.

Opinnäytetyön teko onnistu mielestäni kokonaisuudessaan hyvin. Alkuperäiseen tutkimuskysymykseen pohjautuen työ antaa mielestäni vastauksen ja mahdollistaa lukijalle ymmärryksen tietojenkalastelun terminä. Työn lukemisen jälkeen lukijalla on mielestäni hyvä ymmärrys siitä mihin tutkimuskysymyksessä haluttiin vastata, jolloin sisällöltään kokonaisuus on hyvä. Huomioiden kuitenkin aiemassa kappaleessa esitettyjen jatkokehityskohteiden avulla kokonaisuudesta olisi voinut tulla vielä selkeämpi.

Lähteet

Anand, A. 2012. How Antivirus Sofware Works. Verkkosivusto. Viitattu 20.4.2022. https://bypasst-hesecurity.blogspot.com/2012/11/how-antivirus-software-works.html.

Alkhalil, Z. Hewage, C, Nawaf, L, Khan, I. 2021. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Mielipidekirjoitus. Viitattu 7.3.2022. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full .

Anti-malware protection FAQ. N.d. Verkkojulkaisu. Viitattu 18.4.2022. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-faq-eop?view=o365-worldwide.

Bahar, F. 2022. Everything you need to know about phishing, smishing and vishing. Artikkeli. Viitattu 1.5.2022. https://www-proquest-com.ezproxy.jamk.fi:2443/docview/2622295218?pq-origsite=primo.

Barbosa, H., Breda, F., Morais, T. 2017. Social Engineering and Cyber Security. PDF-tiedosto. Viitattu 2.4.2022. https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY.

Both, D. 2017. Introduction to the Domain Name System (DNS). Verkkojulkaisu. Viitattu 16.4.2022. https://opensource.com/article/17/4/introduction-domain-name-system-dns.

Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year. 2022. Verkkojulkaisu. Viitattu 10.3.2022. https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/.

CYBERDI. N.d. Verkkojulkaisu. Viitattu 21.4.2022. https://jyvsectec.fi/2018/10/cyberdi/.

Data breach investigation report 2018. Verkkojulkaisu. Viitattu 20.1.2022. http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.

Dedhia, C. 2016. How to protect yourselves against email spoofing?. Artikkeli. Viitattu 22.4.2022. https://janet.finna.fi/PrimoRecord/pci.cdi_proquest_reports_1775200007.

Enterprise Phishing Susceptibility Report. N.d. PDF-tiedosto. Viitattu 18.1.2022. https://cofense.com/whitepaper/enterprise-phishing-susceptibility-report/.

Financial Cryptography. 2005. Verkkojulkaisu. Viitattu 12.2.2022. https://financialcryptography.com/mt/archives/000609.html.

Gilbert, B. 2016. Hillary Clinton's campaign got hacked by falling for the oldest trick in the book. Verkkojulkaisu. Viitattu 9.2.2022. https://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10?r=US&IR=T.

Görling, S. 2007. An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism. Artikkeli. Viitattu 22.4.2022. https://janet.finna.fi/PrimoRecord/pci.cdi_emerald_primary_10_1108_10662240710737022.

Hadnagy, C., Fincher, M., Dreeke, R. 2015. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. E-kirja. Viitattu 2.4.2022.

Hadnagy, C., Wilson, P. 2010. Social Engineering: The Art of Human Hacking. E-kirja. Viitattu 1.4.2022. https://ebookcentral-proquest-com.ezproxy.jamk.fi:2443/lib/jypoly-ebooks/reader.action?docID=706746.

ICT-ala. N.d. Verkkojulkaisu. Jyväskylän ammattikorkeakoulun verkkosivut. Viitattu 20.4.2022. https://www.jamk.fi/fi/hae-opiskelemaan/ict-ala.

Irwin, L. 2022. 2021 Review of phishing scams. Verkkojulkaisu. Viitattu 10.2.2022. https://www.itgovernance.eu/blog/en/2021-review-of-phishing-scams.

JAMKin eettiset periaatteet. 2018. PDF-tiedosto. Jyväskylän ammattikorkeakoulun verkkosivut. Viitattu 13.3.2022. https://www.jamk.fi/fi/file/eettiset-periaatteet.

Jamk. N.d. Verkkojulkaisu. Jyväskylän ammattikorkeakoulun verkkosivut.Viitattu 10.2.2022. https://www.jamk.fi/fi/jamk.

Johnson, J. 2021. Organizations most targeted by phishing attacks in 1st quarter 2021, by category. Viitattu 10.3.2022. Verkkojulkaisu. https://www.statista.com/statistics/420442/organizations-most-affected-by-phishing/.

Jones, C. 2022. 50 Phishing Stats You Should Know In 2022. Verkkojulkaisu. Viitattu 2.5.2022. https://expertinsights.com/insights/50-phishing-stats-you-should-know/.

Kyberturvallisuuskeskus. 2020. Väärennettyjä puheluita teknisen tuen nimissä. Verkkojulkaisu. Päivitetty 4.3.2021. Viitattu 2.5.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa.

Kyberturvallisuuskeskus. 2021. Julkaisimme vakavan varoituksen tekstiviestitse levitettävästä haittaohjelmasta. Verkkojulkaisu. Viitattu 8.1.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/julkaisimme-vakavan-varoituksen-tekstiviestitse-levitettavasta-haittaohjelmasta.

Koret, J., Bachaalany, E. 2015. E-kirja. The Antivirus Hacker's Handbook. Wiley: Indianapolis. Viitattu 10.4.2022.

Labaree, R. V. N.d. Research Guides: Organizing Your Social Sciences Research Paper: Qualitative Methods. Research Guide. Viitattu 10.3.2022. https://libguides.usc.edu/writingguide/qualitative.

LeRouge, C., Mantzana, V., Wilson E. 2017. Healthcare information systems research, revelations, and visions. Verkkojulkaisu. Viitattu 2.4.2022. https://www.tandfonline.com/doi/full/10.1057/palgrave.ejis.3000712.

Martino, A,the Perramon, X. 2010. PDF-tiedosto. Viitattu 2.4.2022. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.624.6627&rep=rep1&type=pdf.

Muhammet, B., Zahit, G. 2018. Detection of phishing attacks. PDF-tiedosto. Viitattu 20.1.2022. https://ieeexplore.ieee.org/document/8355389.

Number of internet users worldwide from 2005 to 2021. N.d. Statistan julkaisema raportti. Verkkosivusto. Viitattu 13.3.2022. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

Ozkaya, E. 2018. Introduction to Social Engineering. E-kirja. Viitattu 2.4.2022. https://ebookcentral-proquest-com.ezproxy.jamk.fi:2443/lib/jypoly-ebooks/reader.action?docID=5379705&query=.

Phishing Activity Trends Report – January 2004. 2004. Verkkojulkaisu. Anti-Phishing Working Groupin raportti. Viitattu 8.3.2022. https://docs.apwg.org/reports/APWG.Phishing.Attack.Report.Jan2004.pdf.

Phishing Activity Trends Report – January 2005. 2005. Verkkojulkaisu. Anti-Phishing Working Groupin raportti. Viitattu 8.3.2022. https://docs.apwg.org/reports/APWG_Phishing_Activity_Report-January2005.pdf.

Phishing Activity Trends Report – January 2006. 2006. Verkkojulkaisu. Anti-Phishing Working Groupin raportti. Viitattu 8.3.2022. https://docs.apwg.org/reports/apwg_report_jan_2006.pdf.

Phishing Activity Trends Report – January 2007. 2007. Verkkojulkaisu. Anti-Phishing Working Groupin raportti. Viitattu 8.3.2022. https://docs.apwg.org/reports/apwg_report_january_2007.pdf.

Phishing Activity Trends Report – Q4 2017. 2017. Verkkojulkaisu. Anti-Phishing Working Groupin raportti. Viitattu 7.3.2022. https://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf.

Phishing Activity Trends Report – Q4 2021. 2021. Verkkojulkaisu. Anti-Phishing Working Groupin raportti. Viitattu 7.3.2022. https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf.

Phishing attacks. N.d. What is a phishing attack. Verkkojulkaisu. Impervan verkkojulkaisu. Viitattu 21.1.2022. https://www.imperva.com/learn/application-security/phishing-attack-scam/.

Rastenis, J., Ramanauskaité, S., Janulevičius, J., Čenys A., Slotkiené A., Pakrijauskas K. 2020. Verkkojulkaisu. Viitattu 20.4.2022. https://www.mdpi.com/2076-3417/10/7/2363/htm.

SPF, DKIM & DMARC overview. N.d. Verkkojulkaisu. Viitattu 20.4.2022. https://docs.titanhq.com/en/12726-spf,-dkim---dmarc-overview.html.

Spam Filtering. N.d. Verkkojulkaisu. Viitattu 19.4.2022. https://www.fortinet.com/resources/cyberglossary/spam-filters.

Tietojenkalastelu. N.d. Päivitetty 27.1.2022. Verkkojulkaisu. Kilpailu ja kuluttajaviraston verkkosivut. Viitattu 2.5.2022. https://www.kkv.fi/kuluttaja-asiat/huijaukset/tietojenkalastelu/.

Tietojenkalasteluun perustuvat tietoturvaloukkaukset. N.d. Verkkojulkaisu. Tietosuojavaltuutetun toimisto. Viitattu 10.3.2022. https://tietosuoja.fi/tietojenkalastelu.

Tietoturvan vuosi. 2018. PDF-tiedosto. Kyberturvallisuuskeskuksen raportti. Viitattu 08.02.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf.

Vladimir Z. 2020. Information system. Verkkojulkaisu. Viitattu 2.4.2022. https://www.britannica.com/topic/information-system.

What is an IP Address – Definition and Explanation. N.d. Verkkojulkaisu. Viitattu 20.3.2022. https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address.

What is an SSL certificate – Definition and Explanation. N.d. Verkkojulkaisu. Viitattu 7.4.2022. https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate.

What is Two-Facton Authentication (2FA). N.d. Viitattu 8.4.2022. https://authy.com/what-is-2fa/.

Viljanen V. 2017. Verkkourkinta. Verkkojulkaisu. Viitattu 10.3.2022. https://www.yksityisyydensuoja.fi/verkkourkinta.

What is DKIM?. N.d. Verkkojulkaisu. Viitattu 20.4.2022. https://dmarcian.com/what-is-dkim/.

What is Smishing and How to Defend Against it. N.d. Verkkojulkaisu. Viitattu 10.4.2022. https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it.

What Is a Security Operations Center (SOC)?. N.d. Verkkojulkaisu. McAfeeViitattu 10.3.2022. https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html.

Liitteet

Liite 1. Haastattelurunko

Kysymykset

- Mikä on työnkuvasi?
- Vastuu / toiminta-alueesi?
- Tiedostatko mitä termi tietojenkalastelu tarkoittaa?
- Kuinka usein kohtaat työarjessa tietojenkalastelua?
- Mikä on yleisin heräte tietojenkalastelusta tai mahdollisesta tietojenkalastelusta?
- Onko sinulle koskaan aiheutunut vahinkoa tietojenkalastelusta? Esimerkiksi tunnusten vuotaminen?
- Onko työpaikallasi perehdytetty henkilöstöä mahdollisista tietojenkalastelusta ja eri menetelmistä? Esimerkiksi tietoturvakoulutus työn alkaessa?
    - Mikäli ei niin toivoisitko koulutusta tietojenkalastelusta?
- Minkälaisia työkaluja organisaatiossanne on käytössä tietojenkalastelun havaitsemiseen ja ennaltaehkäisemiseen?