Juho Koistinen

SÄHKÖPOSTIN VÄLITYKSELLÄ TEHTÄVÄ TIETO-JENKALASTELU

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Koistinen, Juho
Sähköpostin välityksellä tehtävä tietojenkalastelu
Jyväskylä: Jyväskylän yliopisto, 2017, 29 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja(t): Kollanus, Sami

Tämä kirjallisuuskatsauksena tehty kandidaatintutkielma tarkastelee tietojenkalastelua esittelemällä sähköpostin välityksellä tapahtuvan tietojenkalastelun keinoja, suojautumistapoja ja syitä sille miksi se onnistuu. Tietojenkalastelua tapahtuu koko ajan maailmanlaajuisesti ja sen uhriksi voi joutua lähes kuka tahansa. Tietojenkalastelu aiheuttaa vuosittain mittavia taloudellisia vahinkoja sekä yksityisille ihmisille, että organisaatioille. Sähköposti on ollut yleisesti eniten käytetty alusta, jolla lähetetään tietojenkalasteluviestejä, ja vaikka teknologian kehittyessä tulee koko ajan uusia tapoja ja mahdollisuuksia lähettää tietojenkalasteluviestejä, niin sähköpostin välityksellä niitä lähetetään yhä edelleen valtavia määrä. Tutkielmassa esitellään neljä yleistä keinoa, joiden avulla tietojenkalastelua toteutetaan sähköpostin välityksellä: kohdennettu tietojenkalastelu, nigerialaiskirjeet, kloonaustietojenkalastelu ja haittaohjelmiin perustuva tietojenkalastelu. Nämä kaikki tietojenkalastelutavat ovat tehokkaita oikein toteutettuna ja siksi on tärkeää osata suojautua niiltä. Kaksi tärkeintä tapaa suojautua sähköpostin välityksellä tehtävältä tietojenkalastelulta ovat teknologiset ratkaisut ja koulutus. Teknologisia ratkaisuja on olemassa monia erilaisia ja yhdistämällä nämä teknologiset ratkaisut tietojenkalastelun vastaisen koulutuksen kanssa saadaan paras mahdollinen suoja tietojenkalastelua vastaan. Täydellistä suojaa tietojenkalastelua kohtaan on kuitenkin lähes mahdotonta saavuttaa. Tietojenkalastelijat pyrkivät ymmärtämään ihmisiä ja vaikuttamaan heidän ajattelu- ja toimintatapoihinsa, saadakseen ihmiset luottamaan itseensä ja luovuttamaan tietojaan ajattelematta asiaa loppuun asti. Myös ihmisten henkilökohtaiset tekijät kuten ikä, sukupuoli, kulttuuri ja aikaisemmat kokemukset voivat vaikuttaa tietojenkalastelun onnistumiseen.

Asiasanat: tietojenkalastelu, sähköposti, kohdennettu tietojenkalastelu, haittaohjelma, tietoturva

ABSTRACT

Koistinen, Juho
Phishing in email services
Jyväskylä: University of Jyväskylä, 2017, 29 p.
Information Systems Science, Bachelor's thesis
Supervisor(s): Kollanus, Sami

This bachelor's thesis, done as a literary review examines phishing by introducing execution and protection ways for email phishing and reasons why it is successful so often. Phishing is happening all the time worldwide and almost anyone can be a victim of it. Phishing causes every year massive economic damages to normal people and organizations. Email has been commonly the most used phishing platform for phishing and even technology evolves all the time and new ways for phishing come up, massive amounts of phishing messages are sent via email. This bachelors thesis introduces four common execution ways for phishing: spear phishing, nigerian letters, clone phishing and malware based phishing. These are effective ways for phishing and that is why it is important to know how to be protected against them. Two most important ways to be protected against phishing are technological solutions and education. There are many kinds of technological solutions and combining these solutions with education is the most effective way to be protected against phishing. However, it is almost impossible to be fully covered against phishing. Phishers try to understand people and try to affect to their way of thinking, to be able to gain their trust and get them to give information without thinking. People personal aspects as age, gender, culture and earlier experiences may also affect to the effectiveness of phishing.

Keywords: phishing, email, spear phishing, malware, information security

KUVIOT

SISÄLLYS

1 JOHDANTO

Tietojenkalastelu on ollut jo pitkään suuri ongelma ja se on yleistymisensä takia kasvamassa koko ajan yhä merkittävämmäksi ongelmaksi. Teknologian kehittyminen ja sen tuleminen yhä enemmän osaksi ihmisten jokapäiväistä elämää avaa koko ajan uusia mahdollisuuksia tietojenkalastelun toteuttamiselle. Käytännössä kuka tahansa, joka omistaa sähköpostiosoitteen, sosiaalisen median käyttäjätilin tai ylipäätään käyttää mitä tahansa palvelua internetissä, jonka kautta voi olla jotenkin yhteydessä muihin käyttäjiin on potentiaalinen tietojenkalastelun uhri. Erittäin suuri osa maailman ihmisistä voi siis joutua tietojenkalastelun uhriksi ja tilastojen mukaan tietojenkalasteluyritykset onnistuvatkin usein. (Hadnagy & Fincher, 2015.).

Tietojenkalastelua ei kohdisteta ainoastaan yksityisiä ihmisiä kohtaan, vaan yritykset ja organisaatiot joutuvat myös todella usein tietojenkalastelun kohteiksi. Kalastellessa tietoja yrityksiltä ja organisaatioilta, tietojenkalastelijat voivat päästä käsiksi todella merkittäviin ja arvokkaisiin tietoihin ja tästä johtuen tietojenkalastelusta aiheutuvat maailmanlaajuiset vuosittaiset haitat ovat rahallisesti merkittäviä, sillä maailmanlaajuisesti puhutaan miljardeista Yhdysvaltain dollareista. (Tambe Ebot, 2017.). Tietojenkalastelun tutkiminen on siis ollut jo pitkään todella ajankohtainen aihe ja tulee olemaan todella tärkeä tutkimuskohde myös tulevaisuudessa. Aiheen tutkiminen on tärkeää, jotta tietojenkalastelun onnistumista voidaan ehkäistä ja ymmärretään paremmin, että miten ja miksi tietojenkalastelu onnistuu niin usein. Tietojenkalastelu olisi usein helposti havaittavissa, mutta silti monesti se havaitaan vasta liian myöhään, kun vahinko on jo tapahtunut. Aiheen tutkiminen on tarpeellista ja välttämätöntä, jotta tietojenkalastelusta aiheutuvia vahinkoja saataisiin pienennettyä. Tutkimalla aihetta ja viemällä tietoa eteenpäin, pystytään ehkäisemään tietojenkalastelun onnistumista merkittävästi. (Hong, 2012.).

Suuri osa maailman ihmisistä käyttää päivittäin sähköpostia sekä vapaa-ajallaan, että työpaikallaan ja siksi tässä tutkielmassa on keskitytty juuri sähköpostin välityksellä tehtävään tietojenkalasteluun. Tietojenkalastelua voidaan toteuttaa monien muidenkin alustojen avulla, mutta sähköposti on ollut jo pitkään yksi yleisimmistä ja tehokkaimmista tietojenkalastelualustoista. (Hong,

2012). Tutkielmassa annetaan monipuolinen kuvaus sähköpostin välityksellä tehtävästä tietojenkalastelusta ja aihetta lähestytään useasta eri näkökulmasta. Tutkielmassa annetaan yleinen kuvaus aiheesta tietojenkalastelu sekä kerrotaan sen maailmanlaajuisista vaikutuksista. Tarkastellaan erilaisia keinoja, joiden avulla tietoja voidaan kalastella sähköpostin välityksellä, sekä suojautumistapoja näille tietojenkalastelukeinoille. Tutkielmassa pohditaan myös sitä miksi tietojenkalastelu onnistuu ja millaiset asiat voivat vaikuttaa sen onnistumiseen. Tutkimuskysymyksiä tutkielmassa on kolme:

- Millaisin eri keinoin tietoja pystytään kalastelemaan sähköpostin välityksellä?
- Miten tietojenkalastelulta voidaan suojautua?
- Miksi tietojenkalastelu onnistuu niin usein ja millaiset tekijät vaikuttavat sen onnistumiseen?

Tutkielma on toteutettu kirjallisuuskatsauksena Okolin ja Schabramin (2010) IT-alan tutkimukseen suunnatun kirjallisuuskatsauksen ohjeistuksen mukaisesti. Tutkielman lähdeaineisto on hankittu suurimmalta osin Google Scholar- ja Finna-palveluiden avulla, käyttämällä hakusanoina keskeisiä tutkielmaan liittyviä käsitteitä (phishing, email, spear phishing, malware, information security), sekä näiden käsitteiden yhdistelmiä ja variaatioita. Käytetty lähdeaineisto on ollut pääasiassa englanninkielistä, aiheesta olevan suomenkielisen tutkimuksen vähäisyyden takia.

2 TIETOJENKALASTELU

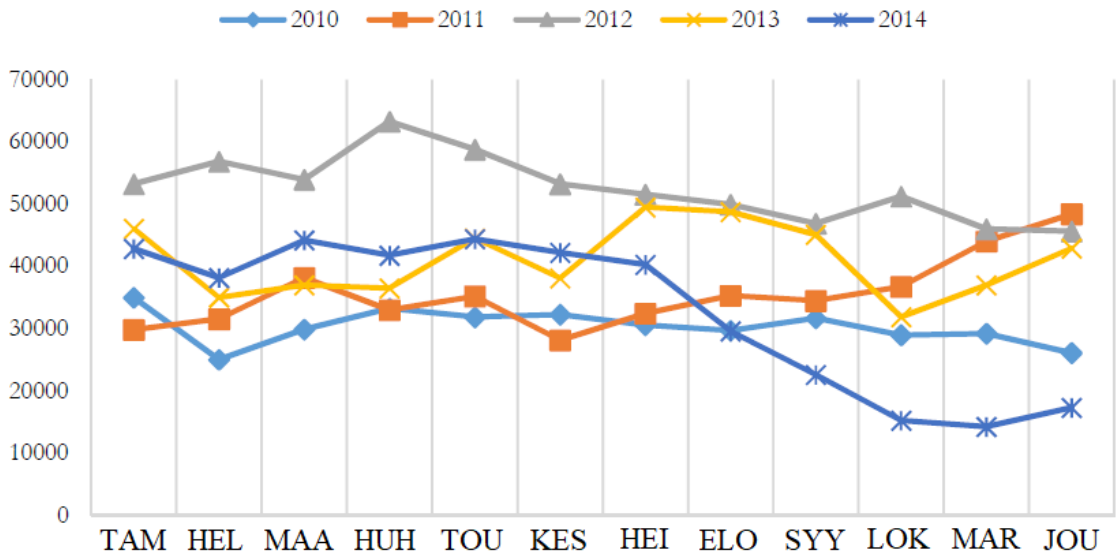
Tietojenkalastelu (*engl. phishing*) on rikollista toimintaa, jonka avulla yritetään esimerkiksi sähköpostin välityksellä saada ihmisiltä henkilökohtaisia tai arkaluonteisia tietoja kuten salasanoja ja luottokortin tietoja. (Banu & Banu, 2013.) Sen avulla pyritään siis saamaan ihmisiltä tai organisaatioilta tietoa, jolla on jotain hyödynnettävää arvoa. Tämä tietojenkalastelun avulla saatava tieto on useimmiten rahallisesti arvokasta, mutta sillä voi olla myös muunlaista arvoa, josta tietojenkalastelijat voivat hyötyä. Tietojenkalastelussa hyödynnetään yleensä vahvasti sosiaalista manipulointia (*engl. social engineering)* sekä teknologista tietämystä. (Chaudhary, 2016.) Yhdistämällä nämä molemmat taidot tietojenkalastelijat pystyvät hankkimaan uhriensa luottamuksen, sekä luottamuksen saatuaan, onnistuvat hankkimaan luottamuksellisia tietoja uhreiltaan (Hadnagy & Fincher, 2015).

Tietojenkalastelu sai alkunsa 1990-luvun alussa ja termiä tietojenkalastelu käytettiin ensimmäisen kerran vuonna 1996, ja siitä lähtien tietojenkalastelun määrä on lisääntynyt valtavasti ja siitä on tullut todella suuri ongelma maailmanlaajuisesti (Chaudhry, Chaudhry & Rittenhouse, 2016). Viime vuosien aikana kalastelu huijaukset ovat muuttuneet kokonaisvaltaisemmiksi ja kehittyneet hienostuneemmiksi. Tietojenkalastelua kohdistetaan nykyään paljon enemmän tietyille kohderyhmille sen sijaan, että sitä tehtäisiin sattumanvaraisesti. (Hong, 2012.) Tutkimusten mukaan hyvin toteutettu tietojenkalasteluun käytettävä verkkosivusto pystyy huijaamaan jopa 90 prosenttia sivulle päätyvistä ihmisistä. Tietojenkalastelu on hyvin toteutettuna todella tehokasta, koska iästä, koulutuksesta, sukupuolesta, aikaisemmasta kokemuksesta ja tietokoneen käyttötunneista huolimatta, kuka tahansa voi joutua tietojenkalastelun uhriksi. Tutkimusten mukaan näillä kaikilla tekijöillä on kuitenkin vaikutusta tietojenkalastelun onnistumisen todennäköisyyteen, mutta mikään niistä ei sulje pois mahdollisuutta tietojenkalastelun onnistumiselle. Vaikka ihminen on siinä tilanteessa, että hän odottaa tietojenkalastelun olevan mahdollista, niin hän ei silti välttämättä pysty tunnistamaan hyvin tehtyä väärennettyä tietojenkalastelu -verkkosivua aidosta verkkosivusta. (Dhamija, Tygar & Hearst, 2006.)

2.1 Vaikutukset

Usein ajatellaan, että tietojenkalastelijat ovat pääasiassa amatöörejä, jotka pyrkivät vain tekemään kiusaa ihmisille. Tämä ei kuitenkaan läheskään aina pidä paikkaansa, vaan kun on kyse hienostuneemmista ja vaarallisemmista tietojenkalasteluhyökkäyksistä, on niiden taustalla yleensä ammattimaisesti toimivia rikollisia. Verkossa käsitellään koko ajan yhä enemmän yksityisten ihmisten ja organisaatioiden arkaluonteisia ja rahallisesti arvokkaita tietoja ja tämän takia tietojenkalastelusta saatavat tuotot ovat koko ajan kasvussa. (Jakobsson & Myers, 2007.) Vuonna 2004 arvioitiin että edellisen vuoden aikana 57 miljoonaa aikuista Yhdysvaltain kansalaista oli vastaanottanut tietojenkalastelu -sähköpostiviestin. Näistä 57 miljoonasta 11 miljoonaa eli 19 prosenttia oli klikannut sähköpostiviestin sisältämää linkkiä. Ja näistä 11 miljoonasta 1,78 miljoonaa eli 3 prosenttia muisti antaneensa arkaluonteisia tietojaan verkkosivulle, jolle linkki oli johtanut. (Litan, 2004.) On arvioitu, että vuonna 2013 tietojenkalastelun takia menetetyn rahan arvo oli yhteensä noin 5.9 miljardia Yhdysvaltain dollaria (RSA EMC2, 2014).

Tietojenkalastelu on siis nykypäivänä maailmanlaajuisesti merkittävä ongelma, sen ympärillä liikkuu valtavia määriä rahaa ja se voi koskettaa ketä tahansa. Kaikki tietojenkalasteluun liittyvät tilastot ja luvut ovat vain arvioita, koska todellisia määriä on mahdotonta tietää, sillä suuri osa tapahtuvasta tietojenkalastelusta jää joko kokonaan huomaamatta tai se ei muuten vain päädy virallisiin tilastoihin. Tästä johtuen todelliset tietojenkalasteluun liittyvät luvut ovat todennäköisesti paljon suurempia. (Chaudhry, Chaudhry & Rittenhouse, 2016.) Kuukausittain avataan tuhansia uusia tietojenkalasteluverkkosivustoja ja kuvio 1 kuvaa vuosien 2010-2014 aikana kuukausittain avattuja ja raportoituja uusia tietojenkalasteluun käytettyjä verkkosivuja. Kuviosta voi nähdä kuinka määrissä on jonkin verran heittelyitä, mutta tilastot pysyvät melko tasaisina koko kuvatun ajanjakson aikana. Tämänkin kuvion luvut ovat vain arvioita ja todellisuudessa määrät ovat todennäköisesti huomattavasti suurempia. (Chaudhary, 2016.)



KUVIO 1 Vuosien 2010-2014 välillä avattujen ja raportoitujen tietojenkalastelu-verkkosivujen määrä. (Chaudhary, 2016)

Tietojenkalastelua tapahtuu maailmanlaajuisesti ja lähes kukaan modernissa yhteiskunnassa elävä ei voi täysin välttyä siltä nykypäivänä, sillä siitä on tullut niin jokapäiväinen ja yleinen ilmiö. Tilastollisesti voidaan kuitenkin huomata, että Yhdysvalloissa on olemassa eräänlainen tietojenkalastelun keskittymä, sillä tietojenkalasteluun käytettävistä verkkosivuista suurinta osaa pidetään yllä Yhdysvalloista käsin ja ero seuraaviin maihin on suuri. (Chaudhary, 2016.)

2.2 Tietojenkalastelun toteutus

Jotta voidaan ymmärtää, että kuinka tietojenkalastelulta voidaan suojautua, täytyy ensin ymmärtää, että miten tietojenkalastelu toimii ja millaisin eri keinoin tietojenkalastelua toteutetaan. Tietojenkalasteluhyökkäys voidaan toteuttaa esimerkiksi niin, että sähköpostilla lähetetään väärennetty viesti, joka usein lähetetään jonkin tunnetun brändin nimissä. Tällä tavoin tietojenkalastelun tekijä pyrkii saamaan huijauksen kohteen luottamuksen heräämään. (Hong, 2012.). Sähköpostiviestit voivat esimerkiksi sisältää linkin, joka vie jonkin luetettavan brändin väärennetylle verkkosivulle. Tämän verkkosivun avulla pyritään keräämään henkilökohtaisia tietoja. (Banu & Banu, 2013.). Tietojenkalastelu sisältää usein kolme päävaihetta. Ensimmäisessä vaiheessa tietojenkalastelun uhri vastaanottaa ”syötin” eli tekaistun sähköpostiviestin. Toisessa vaiheessa kalastelun uhri toimii sähköpostiviestin pyytämällä tavalla ja päätyy esimerkiksi väärennetylle verkkosivulle. Tällä verkkosivulla uhrin käyttämälle laitteelle saattaa asentua haittaohjelmia, tai hänet saadaan luovuttamaan henkilökohtai-

sia tietojaan. Kolmannessa vaiheessa tietojen kalastelijat hankkivat rahaa, hyödyntämällä tietojenkalastelun avulla saamiaan tietoja. (Hong, 2012.)

Tietojenkalastelua ei yleensä kohdisteta suoraan järjestelmiin vaan järjestelmiä käyttäviin ihmisiin. Tämän takia palomuureista, salausohjelmistoista tai muista suojauskeinoista ei ole käytännössä hyötyä, jos tietokonetta käyttävä ihminen lankeaa huijaukseen. (Hong, 2012.) ”Ihmiset voivat olla tietoturvan heikoimpia lenkkejä. Amatöörit hyökkäävät järjestelmiä vastaan ja ammattilaiset hyökkäävät ihmisiä vastaan” (Streeter, 2015). Tämän takia suurin osa tietojenkalastelu -sähköpostiviesteistä keskittyy käyttämään sosiaalisia tekniikoita, teknisten toteutusten sijaan. Tällä tavoin on paljon suurempi todennäköisyys onnistua tietojenkalastelussa ja se on helpompi toteuttaa. Ihmisille saatetaan esimerkiksi lähettää tekaistu sähköpostiviesti, jossa kerrotaan, että heidän käyttäjätililleen on yritetty murtautua ja heidän tulee todentaa käyttäjätilinsä uudelleen antamalla käyttäjätietonsa. (Hong, 2012.)

Alun perin tietojenkalastelua tehtiin enimmäkseen sähköpostin välityksellä, mutta nykyään on kuitenkin olemassa paljon muitakin alustoja, joiden avulla tietojenkalasteluhuijauksia voidaan tehdä. Tekstiviestit, erilaiset viestisovellukset kuten WhatsApp, sosiaalinen media ja verkossa pelattavat moninpelit ovat nykyään myös suosittuja alustoja toteuttaa tietojenkalastelua. (Hong, 2012.) Sähköposti on kuitenkin yhä nykyään eniten käytetty ja suosituin alusta toteuttaa tietojenkalastelua. Seuraavissa kappaleissa esitellään yleisimpiä tapoja toteuttaa tietojenkalastelua sähköpostipalveluiden välityksellä.

2.2.1 Kohdennettu tietojenkalastelu

Kohdennettu tietojenkalastelu (*engl. spear-phishing*) tarkoittaa tietojenkalastelua, jossa otetaan kohteeksi jokin tietty joukko ihmisiä. Sen sijaan, että lähetetään esimerkiksi suuria määriä sähköpostiviestejä sattumanvaraisesti ihmisille, otetaan kohteeksi jokin tietty pienempi joukko ihmisiä, joilla on jotain yhteistä. Kohteeksi otetaan usein jokin tietty yritys tai organisaatio. (Banu & Banu, 2013.) Kohdennetussa tietojenkalastelussa lähetettävät sähköpostiviestit ovat hyvin suunniteltuja ja personalisoitua. Ne tehdään tarkasti kohteen mukaan ja ne pyritään saamaan mahdollisimman aidon näköisiksi. Sähköpostiviestit sisältävät usein joko linkin väärennetylle verkkosivulle tai kannustavat lataamaan jotain, minkä mukana uhri saa haittaohjelman käyttämälleen laitteelle. Tarkasti kohteen mukaan tehty tietojenkalastelu on viime vuosien aikana lisääntynyt merkittävästi ja lähetetyt sähköpostiviestit ovat kehittyneet ja muuttuneet paljon uskottavammiksi kuin aikaisemmin. Hyökkäyksien tekijät ovat siis alkaneet käyttää paljon enemmän vaivaa siihen, että saavat huijauksensa onnistumaan. (Parmar, 2012.)

Tilastojen mukaan noin 19 prosenttia kohdennetusta tietojenkalastelusta onnistuu, kun taas tavallisista tietojenkalasteluhyökkäyksistä vain noin 5 prosenttia onnistuu. Kohdennetut tietojenkalasteluhyökkäykset ovat yleensä paljon kalliimpia toteuttaa kuin tavalliset tietojenkalasteluhyökkäykset. Kohdennetut tietojenkalasteluhyökkäykset voivat olla tekijälleen jopa viisi kertaa kalliimpia,

mutta niiden avulla voidaan saada jopa kymmenen kertainen tuotto tavalliseen tietojenkalasteluun verrattuna. (Parmar, 2012.) Tietojenkalastelu aiheuttaa suuria taloudellisia vahinkoja. Erityisesti kohdennetut tietojenkalasteluhyökkäykset voivat aiheuttaa yrityksille ja organisaatioille suuria taloudellisia menetyksiä (Wang, Herath, Chen, Vishwanath & Rao, 2012).

Kohdennetut tietojenkalasteluhyökkäykset pyrkivät usein vaikuttamaan ihmisiin psykologisesti. Väärennetyissä sähköpostiviesteissä huijarit esiintyvät esimerkiksi jonain hyvin tunnettuna pankkina ja sitä kautta saavat uhrin luottamuksen puolelleen. Esimerkiksi vuonna 2011 kohdennetun tietojenkalastelumenetelmän avulla onnistuttiin huijaamaan 44 päivän aikana kahdeksan miljoonaa dollaria Condé Nast Publications -nimiseltä yhdysvaltalaiselta aikakauslehtien kustantajayhtiöltä. Hyökkäyksen tekijä esiintyi aidon oloisessa sähköpostiviestissä yrityksenä, joka toimittaa Condé Nast Publications:lle painotarvikkeita. Sähköpostiviestissä vain yksinkertaisesti pyydettiin maksamaan kaikki yritysten väliset maksut uudelle tilille. (Parmar, 2012.) Kohdennettu tietojenkalastelu on myös tehokas tapa murtautua esimerkiksi jonkin yrityksen tai organisaation järjestelmiin. Vuonna 2011 RSA Security nimisen tietoturvayhtiön työntekijöille lähetettiin tekaistuja sähköpostiviestejä. Yksi yhtiön työntekijöistä erehtyi klikkaamaan sähköpostissa ollutta linkkiä ja hyökkäyksen tekijät onnistuivat pääsemään RSA Securityn järjestelmiin niin sanotun nollapäivähaavoittuvuuden avulla. (Caldwell, 2013.)

Ihmiset jakavat nykyään todella paljon tietoa itsestään sosiaalisessa mediassa. Jaetut tiedot ovat usein myös todella yksityiskohtaisia ja henkilökohtaisia. Tietojenkalastelussa näitä tietoja joita ihmiset jakavat itsestään sosiaalisessa mediassa on helppo käyttää hyödyksi. (Parmar, 2012.) Kohdennettu tietojenkalastelu perustuu siihen, että kerätään ennalta tietoa hyökkäyksen kohteesta ja sitten tietoja hyödyntämällä kehitetään mahdollisimman aidon oloinen väärennetty sähköpostiviesti. Tietojenkalastelua on siis nykyään paljon helpompi valmistella ja rakentaa juuri oikeanlainen sähköpostiviesti tietylle kohteelle. (Caldwell, 2013.) Edellä mainitussa RSA Securityn esimerkissä hyödynnettiin juuri sosiaalista mediaa. Hyökkäyksen tekijät olivat hyödyntäneet LinkedIn-palvelua. He olivat etsineet LinkedInistä tietoa yrityksen työntekijöistä ja valinneet näiden tietojen avulla valinneet tietyt henkilöt yrityksen sisältä. He olivat tehneet tekaistun rekrytointisuunnitelman ja lähettäneet sen henkilöille. (Parmar, 2012.)

Jos kohdennettua tietojenkalastelua käytetään korkeatasoisia kohteita kohtaan, käytetään siitä nimitystä ”whaling” eli valaanpyynti. Nimitys viittaa siihen, että kyseessä on tavallista korkeatasoisempi, merkittävämpi ja suurempi kohde. Esimerkiksi vuonna 2008, useat yhdysvaltalaiset suurten yritysten toimitusjohtajat saivat sähköpostin kautta valheellisia haasteita oikeuteen ja haasteet sisälsivät haittaohjelmia, jotka levisivät toimitusjohtajien käyttämiin järjestelmiin heidän lukiessaan viestejä. (Hong, 2012.)

2.2.2 Nigerialaiskirjeet

Yksi maailmanlaajuisesti suosittu tietojenkalastelutapa on nigerialaiskirjeet, eli niin sanottu ”419-huijaus”. Numero 419 huijauksen nimessä tulee Nigerian rikoslain luvusta, joka käsittelee tätä huijausta. Sille on joissain tapauksissa tyypillistä, että uhrista hankitaan ennakkoon tietoja, joiden avulla huijauksesta saadaan tehtyä uskottavampi ja helpommin onnistuva ja siksi se voidaan laskea tietyissä tapauksissa kohdennetuksi tietojenkalasteluksi. Nigerialaiskirjeet perustuvat siihen, että uhrille uskotellaan, että jos hän maksaa jonkin summan rahaa niin hän saa tulevaisuudessa suuremman summan rahaa. (Isacenkova, Thonnard, Costin, Francillon & Balzarotti, 2014.) Eli uhrille lähetetään esimerkiksi sähköpostiviesti, jossa viestin lähettäjä esiintyy jonain arvovaltaisena tai rikkaana henkilönä, jolla on huomattava omaisuus. Viestin lähettäjä kuitenkin tarvitsisi jonkin tietyn summan rahaa, jotta voi siirtää omaisuutensa esimerkiksi Eurooppaan. Uhrille luvataan, että jos hän nyt auttaa lähettämällä rahaa, niin hän saa sen moninkertaisena takaisin jossain vaiheessa. (Dyrud, 2005.)

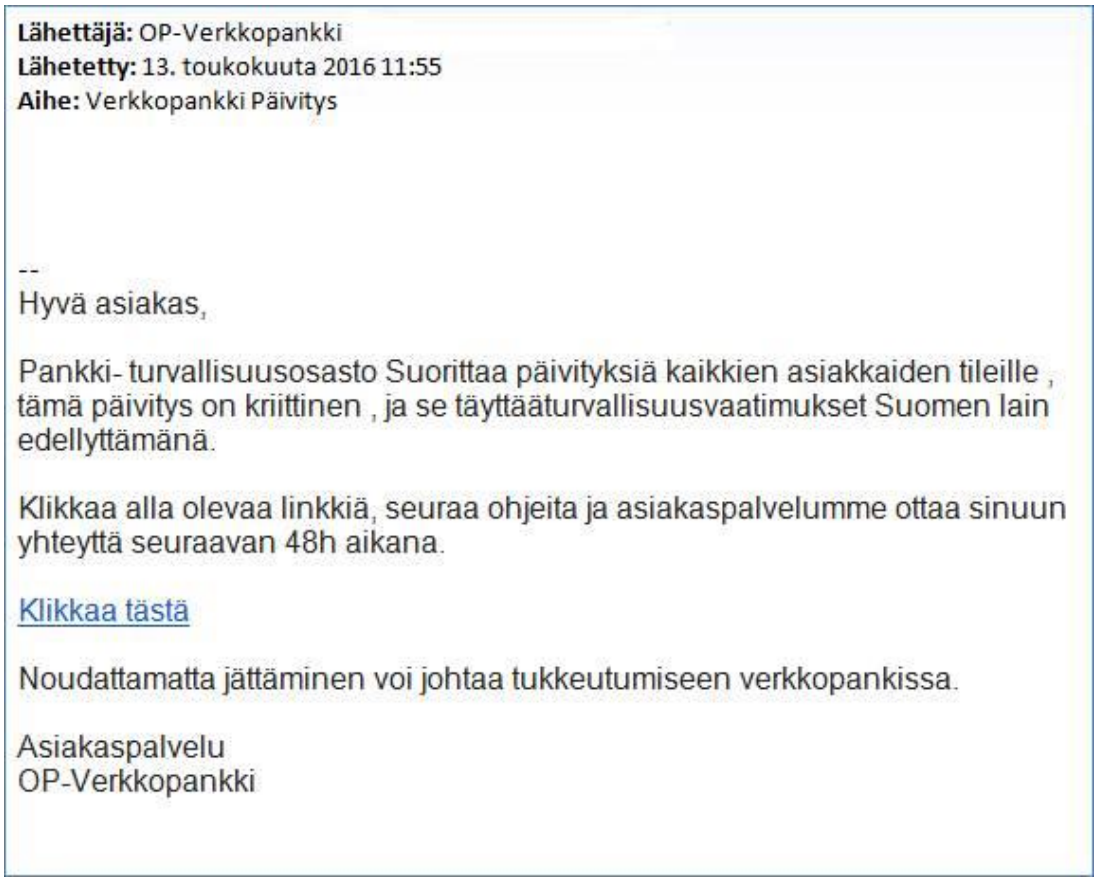
Nigerialaiskirjeet saivat alkunsa 1980-luvulla Nigeriassa. Alun perin huijaus toteutettiin tavallisen postin välityksellä, mutta tekniikan kehityttyä alettiin käyttää sähköpostia. Tämä helpotti huijauksen tekemistä huomattavasti, koska sähköpostin välityksellä huijausviestejä pystytään lähettämään vaivattomasti suuria määriä eri puolille maailmaa. Huijaus on levinnyt maailmanlaajuiseksi, mutta nimitys nigerialaiskirjeet on säilynyt. (Cukier, Nesselroth & Cody, 2007.) Nigerialaiskirjeiden tyyppisistä huijauksista ei ole olemassa kovin tarkkoja tilastoja, koska kyse on laittomasta toiminnasta ja kaikkia huijauksia ei saada mitenkään tilastoitua. Tilastoja on kuitenkin olemassa. Tilastojen mukaan huijausten määrä on koko ajan kasvussa ja niiden avulla tienataan koko ajan suurempia summia. Tilastojen arvioiden mukaan vuonna 2013 huijaukset tuottivat maailmanlaajuisesti yhteensä yli 12,7 miljardia dollaria. Suomessa huijaukset tuottivat arvioiden mukaan ainakin noin 5,55 miljoonaa dollaria vuoden 2013 aikana. (Ultrascan AGI, 2014.)

Suomessa sai paljon julkisuutta vuonna 2014 tapaus, jossa Sunny Car Center -nimisen autokauppahankkeen toimitusjohtaja Markku Ritaluoma joutui tyypillisen 419-huijauksen uhriksi. Häneen otti yhteyttä henkilö, joka esiintyi Sambian entisen presidentin lesken Regina Chiluban asianhoitajana. Ritaluomalle luvattiin yli 30 miljoonan euron sijoitusta autokauppahankkeeseen. Ritaluomaa pyydettiin kuitenkin maksamaan etukäteen yli 300 000 euroa oikeus- ja asianhoitokuluja. Ritaluoma maksoi rahat siitä huolimatta, että keskusrikospoliisi ensin jäädytti varat ja varoitti Ritaluomaa mahdollisesta huijauksesta. (Yle uutiset, 21.8.2014.)

2.2.3 Kloonaustietojenkalastelu

Kloonaustietojenkalastelu (*engl. clone phishing*) tarkoittaa tietojenkalastelua, jossa jonkin legitiimin sähköpostiviestin sisältöä on muokattu niin, että esimerkiksi sen sisältämä liite tai linkki on korvattu valheellisella liitteellä tai linkillä.

Muuten viestin sisältö kloonataan täysin samanlaiseksi kuin alkuperäisen viestin sisältö. Kloonatun sähköpostiviestin sisältämät liitteet sisältävät usein haittaohjelmia ja linkit ohjaavat hyökkäyksen uhrin tekaistulle verkkosivulle, jonka avulla pyritään keräämään uhrilta henkilökohtaisia tietoja. (Khan, 2013.) Kloonattu sähköpostiviesti saattaa myös ohjata hyökkäyksen uhrin verkkosivulle, joka on kloonattu versio jostain uhrin usein käyttämästä verkkosivusta. Tällä tavoin hyökkäyksen tekijät pyrkivät usein saamaan uhrin kirjautumistiedot johonkin verkkopalveluun. (Banu & Banu, 2013.) Taidokkaimmissa huijauksissa valheellinen verkkosivu tehdään vastaamaan täydellisesti vastaavaa aitoa verkkosivua ja se on lähes mahdotonta erottaa aidosta verkkosivusta. Kuvio 2 näkyy Osuuspankin nimissä lähetetty tietojenkalastelusähköpostiviesti. Sähköpostiviesti on pyritty saamaan näyttämään siltä, että se voisi oikeasti olla Osuuspankin lähettämä. Sähköpostiviestin tarkoituksena on saada tietojenkalastelun kohde klikkaamaan sähköpostiviestissä olevaan linkkiä, joka johtaa valheelliselle väärennetylle verkkosivulle, jossa tietojenkalastelun kohde yritetään saada luovuttamaan henkilökohtaisia tietojaan. Sähköpostiviestissä kohteen päätöksentekokykyyn pyritään vaikuttamaan, kertomalla kyseessä olevan kriittinen ja kiireellinen asia, ja näin ollen kohde pyritään saamaan tekemään nopeita päätöksiä ajattelematta asiaa tarpeeksi.



Lähettäjä: OP-Verkkopankki
Lähetetty: 13. toukokuuta 2016 11:55
Aihe: Verkkopankki Päivitys

--
Hyvä asiakas,

Pankki- turvallisuusosasto Suorittaa päivityksiä kaikkien asiakkaiden tileille , tämä päivitys on kriittinen , ja se täyttääturvallisuusvaatimukset Suomen lain edellyttämänä.

Klikkaa alla olevaa linkkiä, seuraa ohjeita ja asiakaspalvelumme ottaa sinuun yhteyttä seuraavan 48h aikana.

Klikkaa tästä

Noudattamatta jättäminen voi johtaa tukkeutumiseen verkkopankissa.

Asiakaspalvelu
OP-Verkkopankki

KUVIO 2 Osuuspankin nimissä lähetetty tietojenkalastelusähköpostiviesti. (Osuuspankki)

2.2.4 Haittaohjelmiin perustuva tietojenkalastelu

Haittaohjelmiin perustuvaa tietojenkalastelua on käytännössä kaikki tietojenkalastelu, jossa tietojenkalastelun kohteen tietokoneella tai muulla laitteella ajetaan jotain haittaohjelmaa tietojenkalastelutarkoituksessa (Jakobsson & Myers, 2007). Tietojenkalastelusähköpostiviestin avulla pyritään asentamaan haittaohjelmia tietojenkalastelun kohteen käyttämälle laitteelle. Haittaohjelmia piilotetaan tietojenkalasteluviestin liitteisiin tai tietojenkalasteluviesti voi ohjata uhrin verkkosivulle, josta haittaohjelma asentuu uhrin huomaamatta. Haittaohjelmia käytetään usein hankkimaan ihmisten kirjautumistietoja verkkopankkeihin ja näiden kerättyjen tietojen avulla väärennetään tilisiirtoja, mutta haittaohjelmia voidaan käyttää myös muiden verkkopalveluiden kirjautumistietojen hankintaan, sekä ihmisten henkilötietojen hankkimiseen. Tavallinen tietojenkalastelu tehdään usein pelkästään käyttäjää vastaan, mutta haittaohjelmiin perustuvaa tietojenkalastelu on kehittyneempää tietojenkalastelua ja sitä tehtäessä, tarvitaan myös paljon teknistä osaamista, ihmisten käyttäytymisen ymmärtämisen lisäksi (Birk, Gajek, Grobert & Sadeghi, 2007.).

Haittaohjelmiin perustuvan tietojenkalastelun alkuvaiheessa tarvitaan sosiaalisen manipuloinnin taitoja, jotta uhri saadaan avaamaan sähköpostiviesti ja klikkaamaan tietojenkalasteluviestin osaa, josta haittaohjelma asentuu hänen käyttämälleen laitteelle. Tämän jälkeen astuu esiin tietojenkalastelijan tekninen osaaminen. Teknisesti taitava tietojenkalastelija pystyy hankkimaan käytännössä mitä tahansa tietoja uhrin käyttämältä laitteelta, tämän edes huomaamatta sitä (Jakobsson & Myers, 2007.).

Haittaohjelmiin perustuva tietojenkalastelu on paljon työläämpää ja vaativampaa, kuin tavallinen sähköpostin välityksellä tehtävä tietojenkalastelu, jossa pyritään keräämään tietoja pelkän sähköpostiviestin avulla. Haittaohjelmiin perustuvan tietojenkalastelun avulla voidaan kuitenkin saada tavallista arvokkaampia tietoja ja se on onnistuessaan todella tehokas tietojenkalastelun muoto (Gajek, Sadeghi, Stuble & Winandy, 2007.).

3 TIETOJENKALASTELULTA SUOJAUTUMINEN

Tämä luku käsittelee suojautumista tietojenkalastelulta. On olemassa erilaisia keinoja, joiden avulla pystytään ennalta ehkäisemään sitä, että ihmiset joutuvat tietojenkalastelun uhriksi. Aluksi luvussa käsitellään erilaisia teknologisia ratkaisuja, joiden avulla pystytään suojautumaan tietojenkalastelulta. On olemassa monia erilaisia teknologisia ratkaisuja. Teknologiset ratkaisut kehittyvät koko ajan ja niitä tulee koko ajan lisää. Tästä syystä olisi mahdotonta käydä läpi kaikki mahdolliset teknologiset ratkaisut ja siksi tässä tutkielmassa käsitellään tärkeimpiä ja tehokkaimpia teknologisia ratkaisuja, joita tällä hetkellä on olemassa. Teknologisten ratkaisuiden lisäksi tässä luvussa käsitellään koulutuksen merkittävyyttä tietojenkalastelulta suojautumisessa. Koulutusta voidaan toteuttaa erilaisin tavoin ja tässä luvussa kerrotaan muutamia hyviä keinoja kouluttaa ihmisiä suojautumaan tietojenkalastelulta.

3.1 Teknologiset ratkaisut

Teknologiset ratkaisut pyrkivät usein tekemään tietojenkalastelun näkymättömäksi loppukäyttäjälle. Se tarkoittaa käytännössä sitä, että pyritään estämään tietojenkalastelun päätyminen loppukäyttäjälle. Eli jos tietojenkalastelun yritys ei ikinä edes päädy loppukäyttäjälle asti, niin silloin loppukäyttäjä ei voi joutua huijatuksi. Eri keinoja toteuttaa tämä ovat esimerkiksi tietojenkalastelu -sähköpostiviestien suodattaminen ja väärennettyjen verkkosivujen estäminen ja poistaminen. (Hong, 2012.)

Tietojenkalastelua varten on kehitetty omia suodattimia sähköpostipalveluihin. Nämä suodattimet pyrkivät tunnistamaan tavallisten sähköpostiviestien joukosta tietojenkalasteluun käytettäviä sähköpostiviestejä. Suodattimet etsivät sähköpostiviestistä asioita jotka voivat viitata siihen, että sähköpostiviestiä käytetään tietojenkalasteluun. Tietojenkalastelu -viesteissä saattaa esimerkiksi esiintyä URL-osoitteita jotka sisältävät eroavia verkkotunnuksia. (Hong, 2012.) Sähköpostisuodattimet voivat myös luokitella sähköpostiviestejä etsimällä nii-

den sisällöstä ja lähetysosoitteesta avainsanoja, jotka voivat viitata tietojenkalastelun (Almomani, Gupta, Atawneh, Meulenberg & Almomani, 2013). Täydellisen suodattimen tekeminen on kuitenkin lähes mahdotonta, koska tietojenkalastelu -viestit eroavat paljon toisistaan ja ne saattavat olla niin taidokkaasti tehtyjä, että niitä ei voi suodattimen avulla tunnistaa. Tietojenkalastelu -viestejä on mahdollista estää myös todennus- ja vahvistuspalveluiden teknologioiden avulla. Tällaisia ovat esimerkiksi: SPF (Sender Policy Framework) ja DKIM (DomainKeys Identified Mail). SPF hyödyntää SMTP-protokollaa (Simple Mail Transfer Protocol), jonka avulla se tunnistaa väärennettyjä sähköpostiosoitteita. DKIM puolestaan tarkistaa viestin lähettäjän verkkotunnuksen ja viestin yhtenäisyyden. Nämäkään teknologiat eivät kuitenkaan toimi täydellisesti vaan nekin on mahdollista kiertää. Ja ne eivät toimi kovin hyvin laajemmassa mittakaavassa. (Hong, 2012.) Tavalliset roskapostisuodattimet voivat myös tunnistaa tietojenkalastelu -sähköpostiviestejä. Roskapostisuodattimet eivät kuitenkaan välttämättä tunnista tietojenkalasteluun käytettäviä sähköpostiviestejä, jos tietojenkalastelu -viesti on tehty hyvin. Usein tietojenkalastelu -sähköpostiviestien onnistuminen perustuu siihen, että ne lähetetään suurelle joukolle ihmisiä kerralla, eikä viestin sisältöön välttämättä panosteta kovinkaan paljoa. Kaikista huolellisimmin tehdyt tietojenkalastelu -viestit ovat kuitenkin niin hyvin toteutettuja, että tavalliset roskapostisuodattimet eivät tunnista niitä haitallisiksi, eivätkä siis osaa suodattaa niitä. (Fette, Sadeh & Tomasic, 2007.)

Tietojenkalasteluun käytettävien verkkosivujen estäminen on mahdollista. Sivujen estäminen ehkäisee sähköpostiviestien välityksellä huijaamiseksi joutumista siten, että kun henkilö klikkaa tietojenkalastelu -viestissä olevaa linkkiä niin hän saa joko varoituksen sivustosta jolle hän on siirtymässä tai siirtyminen sivustolle estetään kokonaan. Estäminen voidaan toteuttaa esimerkiksi tutkimalla URL:ää tai manuaalisesti tehdyillä mustilla listoilla. Monilla yrityksillä on omia mustia listoja tietojenkalastelua vastaan. Esimerkiksi Microsoft ja Google ylläpitävät omia mustia listojaan ja ne ovat integroineet listansa omiin verkkoselaimiinsa. Eli kun käyttäjä käyttää Microsoftin Internet Explorer- tai Edgeä-verkkoselainta, tai Googlen Chrome-verkkoselainta, niin hänet on automaattisesti suojattu mustalla listalla olevilta tietojenkalastelu -verkkosivustoilta. Suojaus toimii niin, että se joko estää kokonaan pääsyn haitalliselle verkkosivulle tai sitten se antaa varoituksen siirryttäessä verkkosivulle, joka on mahdollisesti haitallinen. (Hong, 2012.) Varoitusjärjestelmät eivät kuitenkaan ole kovin tehokkaita, koska ihmiset jättävät usein näytölle ilmestyvät varoituspalkit huomioimatta ja siirtyvät haitalliselle verkkosivulle niistä huolimatta (Dhamija, Tygar & Hearst, 2006). Verkkoselaimiin on myös saatavilla lisäosia, jotka suojaavat tietojenkalastelulta (Jansson & von Solms, 2013).

PhisTank-niminen verkkosivusto pitää myös yllä omaa mustaa listaansa. PhisTank:in musta lista perustuu siihen, että tavalliset käyttäjät saavat ilmiantaa sinne tietojenkalastelu -verkkosivustoja. Ja kun tarpeeksi moni eri käyttäjä äänestää samaa verkkosivustoa, niin se joutuu mustalle listalle. (Hong, 2012.) PhisTank julkaistiin vuonna 2006 ja siitä lähtien sivustolla on annettu ääniä lähes 16 miljoonaa ja vahvistettuja tietojenkalastelu -verkkosivustoja on listalla yli

kaksi miljoonaa (PhisTank, 2017). Mustat listat eivät kuitenkaan ole kovin tehokkaita, koska ne suojaavat vain jo listalle päätyneiltä verkkosivuilta. Koko ajan ilmestyy uusia tietojenkalastelu -verkkosivuja, ja siihen kuluu aina aikaa, että ne päätyvät mustalle listalle. Ja kaikki tietojenkalasteluun käytettävät verkkosivut eivät päädy välttämättä ikinä yhdellekään mustalle listalle. (Hong, 2012.)

Myös viruksentorjuntaohjelmat suojaavat tietojenkalastelulta. Jos tietojenkalastelu -sähköpostiviestiin on piilotettu jokin yleisesti tunnettu haittaohjelma ja huijauksen kohde erehtyy aktivoimaan sen, niin viruksentorjuntaohjelma todennäköisesti onnistuu estämään haittaohjelman asentumisen uhrin käyttämälle laitteelle. Haittaohjelmia kuitenkin tulee koko ajan uusia ja ne kehittyvät nopeasti. Siksi viruksentorjuntaohjelmien on mahdoton tunnistaa kaikkia uusia haittaohjelmia. Tämän takia viruksentorjuntaohjelmatkaan eivät voi taata täydellistä suojaa. (Parmar, 2012.)

Tietojenkalasteluun käytettäviä verkkosivuja voidaan myös kokonaan sulkea. Muutamat tietojenkalasteluun keskittyvät organisaatiot tunnistavat tietojenkalasteluun käytettäviä verkkosivuja ja sulkevat niitä. Tämän jälkeen käyttäjät eivät voi enää päätyä kyseisille verkkosivuille, koska niitä ei enää ole olemassa. Myös käyttöliittymiä voidaan kehittää paremmiksi. Yksi tapa on sisällyttää käyttöliittymiin tietoturvavaroituksia. Tietoturvavaroitusten ongelma on siinä, että käyttäjät sulkevat usein varoitukset lukematta niitä. Varoitukset usein keskeyttävät sen mitä käyttäjä on juuri sillä hetkellä tekemässä ja ne koetaan sen takia ärsyttäviksi. (Hong, 2012.)

Erilaiset teknologiset ratkaisut ovat hyviä ennalta ehkäisemään tietojenkalastelua, mutta mitkään teknologiset ratkaisut eivät kuitenkaan ole täysin varmoja keinoja, vaikka käytettäisiin montaa eri teknologista ratkaisua samaan aikaan. Teknologian toimivuuteen ei siksi saa luottaa liikaa. (Kumaraguru, Sheng, Acquisti, Cranor & Hong, 2010.). Seuraava luku kertoo tarkemmin ihmisten kouluttamista tietojenkalastelua vastaan, joka on teknologisten ratkaisuiden ohella todella tärkeää.

3.2 Koulutus

Yksi tapa välttää tietojenkalastelua on ihmisten kouluttaminen. Erityisesti yritysten tulisi jatkuvasti käyttää resurssejaan työntekijöidensä ja myös asiakkaidensa kouluttamiseen tietojenkalastelua vastaan. (Parmar, 2012.) Tietojenkalastelua vastaan koulutuksesta ja harjoittelusta on tutkitusti hyötyä (Mayhorn & Nyeste, 2012). Useimmiten koulutus ja niin sanottu ”maalaisjärki” ovat riittäviä estämään lähes kaikki tietojenkalastelu -yritykset. (Parmar, 2012.) Ihmisten kouluttamisessa on usein se ongelma, että ihmiset ajattelevat osaavansa jo valmiiksi tunnistaa mahdollisen tietojenkalastelun, ja siten olevansa jo valmiiksi kykeneviä suojelemaan itseään siltä (Hong, 2012).

Kouluttamisessa tietojenkalastelua vastaan on olemassa useita eri lähestymistapoja. Yksi lähestymistapa koulutukselle on opettaa ihmisille keinoja

tunnistaa tietojenkalasteluun käytettäviä sähköpostiviestejä. (Almomani, Gupta, Atawneh, Meulenberg & Almomani, 2013.) Tietojenkalasteluun käytettävät sähköpostiviestit sisältävät usein samanlaisia piirteitä ja asioita, ja oppimalla tunnistamaan niitä on mahdollista oppia välttämään huijatuksi tuleminen (Robila & Ragucci, 2006). Internetissä on tarjolla paljon ilmaista materiaalia, jonka avulla voi oppia tunnistamaan tietojenkalasteluun käytettäviä sähköpostiviestejä. Esimerkiksi maiden hallitukset ja monet voittoa tavoittelemattomat organisaatiot julkaisevat koko ajan ajankohtaista materiaalia liittyen tietojenkalastelun riskeihin ja siihen, kuinka oppia tunnistamaan se. Monet tietoturvayritykset tarjoavat myös koulutuspalveluita, joiden avulla esimerkiksi toiset yritykset voivat kouluttaa henkilökuntaansa tietojenkalastelun riskeihin liittyen. (Almomani, Gupta, Atawneh, Meulenberg & Almomani, 2013.)

Toinen lähestymistapa on käyttää koulutuksessa apuna tilanteita, joissa simuloidaan aitoja tietojenkalastelu -yrityksiä. Aitojen tilanteiden simuloiminen on todettu tehokkaaksi ja toimivaksi tavaksi kouluttaa ihmisiä. Tilanteiden simuloiminen tapahtuu käytännössä siten, että ihmisille lähetetään testimielessä tietojenkalastelu -viesti ja siten testataan, että kuinka moni tajuaa huijauksen. Ihmisille lähetetään jälkeen päin tiedot siitä, että he ovat olleet osallisena testissä ja heille annetaan palautetta heidän toiminnastaan. (Jansson & von Solms, 2013.) Aitoja tietojenkalastelu -sähköpostiviestejä simuloiden toimii esimerkiksi PhishGuru niminen harjoitusjärjestelmä, joka opettaa käyttäjiään välttämään tietojenkalastelulla huijatuksi tulemista. PhisGuru-järjestelmä lähettää käyttäjille harjoitusviestin, ja jos käyttäjä klikkaa simuloidussa tietojenkalastelu -sähköpostiviestissä olevaa linkkiä, niin hän saa siitä ilmoituksen ja hän saa eteensä materiaalia, jossa kerrotaan kuinka kyseisen tietojenkalastelu -viestin olisi voinut tunnistaa. (Kumaraguru, Cranshaw, Acquisti, Cranor, Hong, Blair & Pham, 2009.) Tutkimuksen mukaan PhisGuru-järjestelmän avulla onnistuttiin vähentämään 45 prosenttia tietojenkalastelun onnistumista koehenkilöiden keskuudessa kuukauden aikana. Tutkimukseen osallistui yli 500 koehenkilöä. (Hong, 2012.) Monet organisaatiot ovat kehittäneet omia harjoituksiaan tietojenkalastelua vastaan. Esimerkiksi Yhdysvaltojen asevoimien sotilasakatemia USMA (United States Military Academy) on kehittänyt oman Carronade-nimisen harjoituksen sähköpostilla tehtävää tietojenkalastelua vastaan. (Dodge, Carver & Ferguson, 2007.)

Kouluttamisessa voidaan käyttää hyväksi erilaisia aiheen kouluttamista varten tehtyjä sovelluksia ja pelejä. Hyvä esimerkki koulutuksessa käytettävästä pelistä on Anti-Phishing Phil -niminen peli, joka on kehitetty käytettäväksi koulutuksessa tietojenkalastelua vastaan. Tutkimusten mukaan Anti-Phishing Phil -pelin avulla saatiin aikaan parempia tuloksia kuin, pelkästään lukemalla tietojenkalasteluun liittyvää materiaalia. (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge 2007.) Anti-Phishing Phil -pelin ideana on opettaa ihmiset tunnistamaan tietojenkalastelu -sähköpostiviestien ominaisuuksia samalla kun he pelaavat peliä. Pelissä pääsee eteenpäin, kun onnistuu tunnistamaan oikein tietojenkalasteluun käytettäviä verkkosivuja, verkkotunnuksia ja muita tietojenkalasteluun liittyviä ominaisuuksia. (Hong, 2012.)

Parhaan tuloksen koulutuksessa tietojenkalastelua vastaan saa yhdistelemällä eri keinoja. Eli käyttämällä hyväksi sovelluksia ja pelejä, sekä opiskelemalla erilaisia materiaaleja liittyen tietojenkalasteluun. Tällä tavalla on mahdollista oppia teoriassa tietoja siitä, että millaisia asioita tietojenkalastelu -sähköpostiviestit voivat sisältää, sekä oppia käytännössä sen, että miltä tietojenkalastelu -viestit usein näyttävät. Kun yhdistetään teoria ja käytäntö koulutuksessa, saadaan parhaita tuloksia. (Almomani, Gupta, Atawneh, Meulenberg & Almomani, 2013.) Koulutuksen avulla ei kuitenkaan ole mahdollista saavuttaa täydellisiä tuloksia. Tietojenkalasteluun käytettävät sähköpostiviestit kehittyvät koko ajan ja koko ajan tulee uudenlaisia tapoja kalastella tietoja ihmisiltä. Siksi koulutus on tärkeää, jotta ihmiset pysyvät ajan tasalla siitä, että millaisia asioita he voivat odottaa mahdollisilta tietojenkalastelu -sähköpostiviesteiltä. Ihmisten koulutuksen voidaan katsoa olevan sekä vahvin että heikoin lenkki suojautumisessa tietojenkalastelua vastaan. Hyvällä koulutuksella on mahdollista päästä hyviin tuloksiin tietojenkalastelulta suojautumisessa, mutta pitää kuitenkin muistaa, että tietojenkalastelu kohdistetaan yleensä juuri ihmisiä eikä järjestelmiä kohtaan. Ihmisen tekemä virhe on koulutuksesta huolimatta todennäköisempi kuin järjestelmän tekemä virhe. (Chaudhry, Chaudhry & Rittenhouse, 2016.)

Kaikista tehokkain suoja tietojenkalastelua vastaan saadaan yhdistämällä teknologiset ratkaisut ja kouluttamalla ihmisiä tunnistamaan tietojenkalasteluun käytettäviä sähköpostiviestejä. Yhdistämällä nämä molemmat suojautumiskeinot lasketaan tietojenkalastelun onnistumisen riskiä huomattavasti. Tämä yhdistelmäkään ei ole täysin varma ratkaisu, mutta nämä kaksi keinoa toimivat kuitenkin yhdessä paljon tehokkaammin kuin yksittäin. Tietojenkalasteluun käytettävät sähköpostiviestit kehittyvät koko ajan ja siksi mikään teknologinen ratkaisu tai koulutus ei ole välttämättä riittävän tehokasta (Kumaraguru, Sheng, Acquisti, Cranor & Hong, 2010).

4 MIKSI IHMISET LUOVUTTAVAT TIETOJAAN NIIN HELPOSTI?

Tämä luku käsittelee tietojenkalastelun vaikutusta ihmisiin ja sitä, että miksi tietojenkalastelu onnistuu niin helposti. Tietojenkalastelu olisi yleensä helposti havaittavissa ja estettävissä, mutta silti tietojenkalastelu toimii usein ja ihmiset eivät edes välttämättä tajua joutuneensa tietojenkalastelun uhriksi. Tietojenkalastelussa hyökkääjä pyrkii yleensä herättämään uhrin luottamuksen esiintymällä jonain tahona, jonka uhri kokee luotettavaksi. Tietojenkalastelun tekijä on voinut selvittää etukäteen uhrista erinäisiä tietoja. Hyökkääjä voi esimerkiksi tietää tietojenkalastelun kohteen koko nimen, sähköpostiosoitteen ja muita pieniä henkilökohtaisia tietoja. Tietojenkalastelun toteuttaja voi hyödyntää näitä tietoja ja tehdä kohteelle personoidun viestin, joka vaikuttaa luotettavalta, koska siinä on kohteen henkilökohtaisia tietoja ja se vaikuttaa tulleen luotettavasta ja tutusta lähteestä. Tällöin tietojenkalastelun kohde toimii herkemmin ajattelematta sen pidemmälle ja toimii juuri niin kuin tietojenkalastelun tekijä haluaa. (Speed, Nykamp, Heiser, Anderson & Nampalli, 2013.)

4.1 Päätöksentekoprosessin ymmärtäminen ja siihen vaikuttaminen

Tietojenkalastelu perustuu usein ihmisten päätöksentekoprosessin ymmärtämiseen. Ihmiset eivät aina ajattele rationaalisesti tai loogisesti tehdessään päätöksiä, vaan monet pienet asiat kuten esimerkiksi havainnot ja tuntemukset vaikuttavat päätösten tekemiseen. Tietojen kalastelijat pyrkivät ymmärtämään, kuinka ihmiset tekevät päätöksiä ja yrittävät manipuloida päätöksenteon olosuhteita niin, että ihmiset päätyvät tekemään huonon päätöksen. Päätöksenteko ei aina välttämättä liity ihmisten tyytyväisyyteen päätöksen suhteen. Ihmiset tekevät joskus huonoja päätöksiä, mutta ovat silti jollain määrin tyytyväisiä päätökseensä. Lähes kaikki ihmiset tekevät päivittäin pieniä ja suuria päätöksiä, ilman kaikkea olennaista tietoa, jota saattaisi tarvita päätöksenteossa. Välillä päätöksiä

tehtäessä, ei päätöksen aiheuttamaa lopputulosta ajatella ollenkaan, ennen kuin on jo liian myöhäistä. Tietojen kalastelijat ymmärtävät, että heillä on hyvä mahdollisuus vaikuttaa ihmisten päätöksentekoon vaikuttamalla ihmisten tunteisiin. Tietojenkalastelu-viesteillä voidaan pyrkiä esimerkiksi vaikuttamaan ihmisten ahneuteen, pelkoon, sympatiaan, uteliaisuuteen tai himoon. Tietojenkalasteluviesteillä yritetään saada ihmisissä heräämään jokin tunnereaktio ja jos tunnereaktio on tarpeeksi vahva, se voi vaikuttaa kriittisesti päätöksentekoprosessiin ja mahdollistaa näin tietojenkalastelun onnistumisen (Hadnagy & Fincher, 2015.). Tietojenkalastelusähköpostiviestille on usein tyypillistä, että sen avulla luodaan kohteelle sellainen kuva, että kyse on jostain tärkeästä asiasta kuten hänen pankkitilinsä väärinkäytöstä ja hänen on toimittava nopeasti korjatakseen jokin asia. Tällöin tietojenkalastelun kohde ei välttämättä kerkeä ajatella asiaa kunnolla ja tuntiessaan tilanteen kiireelliseksi, toimii tietojenkalastelijoiden haluamalla tavalla ja luovuttaa henkilökohtaisia tietojaan (Hong, 2012.).

Päätöksiä tehdessä tulisi aina olla varma, että ymmärtää kunnolla asian josta on päättämässä ja asiasta on tarjolla tietoa niin paljon kuin tarpeellista. Lisäksi tulisi miettiä, että onko olemassa muita vaihtoehtoja ja mikä on päätöksen mahdollinen lopputulos. Myös aikaisemmista virheistä voi aina oppia ja toimia niiden perusteella paremmin seuraavalla kerralla. (Hadnagy & Fincher, 2015.)

4.2 Iän, sukupuolen, kulttuurin ja kokemuksen vaikutus

Tutkimusten mukaan sukupuolella, iällä, kulttuurilla ja aikaisemmalla kokemuksella on vaikutusta tietojenkalastelun prosentuaalista onnistumista tarkasteltaessa. Ikä, sukupuoli, kulttuuri tai aikaisempi kokemus eivät aina ole merkittäviä tekijöitä tietojenkalastelun onnistumisessa, sillä käytännössä kuka tahansa voi joutua tietojenkalastelun uhriksi, mutta on huomattu, että ne vaikuttavat jossain määrin tietojenkalastelun prosentuaaliseen onnistumiseen (Chaudhary, 2016.). Tutkimusten mukaan naiset ovat alttiimpia tietojenkalastelulle kuin miehet ja tietojenkalastelun onnistumisprosentti on suurempi, jos tietojenkalastelun uhri on vastakkaista sukupuolta. Myös ikä ja ihmisten teknologinen kokemus vaikuttavat tietojenkalastelun onnistumisen todennäköisyyteen. Tilastojen mukaan nuoret ihmiset ovat alttiimpia tietojenkalastelulle kuin muut ikäluokat, kun taas ihmiset joilla on paljon teknologista kokemusta ovat tietojenkalastelulle vähemmän alttiita. (Jagatic, Johnson, Jakobsson & Menczer, 2007.)

Jos henkilö on saanut koulutusta, jonka tarkoituksena on oppia tunnistamaan tietojenkalasteluviestejä, niin silloinkin todennäköisyys tietojenkalastelun onnistumiselle on pienempi (Downs, Holbrook & Cranor, 2007). Tutkimusten mukaan, ihmiset tunnistavat tietojenkalasteluviestejä paremmin, jos heille on muistutettu niiden olemassa olosta ja heitä on kehotettu olemaan valppaana niiden varalta. Tietojenkalastelun onnistuminen on siis epätodennäköisempää, jos henkilö on ollut lähiaikoina tekemisissä aiheen kanssa (Pattinson, Jerram, Parsons, McCormac & Butavicius, 2012.). Kaikista eniten tietojenkalastelulle on

altis 18-25 vuotias nainen, jolla ei ole paljoa teknologista kokemusta tai koulutusta tietojenkalastelusta (Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010).

Myös ihmisten tausta ja se minkälaisessa kulttuurissa on kasvanut vaikuttavat tietojenkalastelun onnistumisen todennäköisyyteen. Kulttuuri ja tausta voivat vaikuttaa esimerkiksi siihen, kuinka ihmiset ajattelevat ja toimivat erilaisia järjestelmiä, kuten esimerkiksi juuri sähköpostia käyttäessään. Tietynlaiset kulttuurit ja taustat voivat saada ihmiset toimimaan varovaisemmin käyttäessään sähköpostia, kun taas toisenlaisista kulttuureista ja taustoista peräisin olevat ihmiset voivat toimia paljon huolettomammin ja ovat näin ollen on todennäköisempää, että tietojenkalastelu onnistuu heihin kohdistettuna (Chaudhary, 2016.). Ihmisillä on erilaisia uskomuksia ja mielipiteitä liittyen eri asioihin ja näihin uskomuksiin ja mielipiteisiin vaikuttavat monet asiat kuten aikaisemmat kokemukset. Aikaisemmat kokemukset tekevät ihmisistä tietoisempia tietojenkalastelun suhteen ja voivat muuttaa heidän mielipiteitään siitä. Jos aikaisempaa kokemusta ei ole niin tietojenkalasteluun suhtaudutaan todennäköisesti paljon huolettomammin (Vishwanath, Herath, Chen, Wang & Rao, 2011.).

5 YHTEENVETO

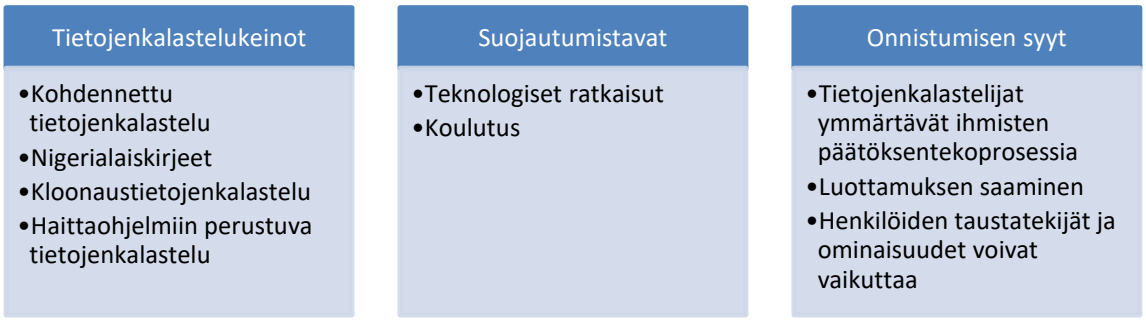
Tietojenkalastelu alkoi yleistymään jo kauan sitten, mutta tällä hetkellä se on ajankohtaisempi aihe kuin koskaan ennen ja on ajankohtainen aihe varmasti myös tulevaisuudessa, sillä tällä hetkellä vuosittain tietojenkalastelun aiheuttamat taloudelliset vahingot ovat miljardeissa Yhdysvaltain dollareissa. Sähköposti on ollut aina perinteisin alusta toteuttaa tietojenkalastelua ja se on yksi yleisimmistä alustoista tänäkin päivänä, sillä sähköpostiviestejä lähetetään tietojenkalastelutarkoituksessa maailmanlaajuisesti joka päivä miljardeja kappaleita.

Tutkielman ensimmäinen tutkimuskysymys käsitteli erilaisia keinoja, joiden avulla tietojenkalastelua voidaan toteuttaa sähköpostipalveluissa. Tutkielmaa varten haettuun lähdemateriaaliin perustuen voi todeta, että sähköpostin välityksellä tehtäviä tietojenkalastelutapoja on olemassa todella paljon ja niistä nousi selkeästi esille neljä merkittävää ja yleistä tapaa. Kohdennettu tietojenkalastelu, nigerialaiskirjeet, kloonaustietojenkalastelu ja haittaohjelmiin perustuva tietojenkalastelu. Kaikkia näitä tapoja pystytään hyödyntämään tehokkaasti oikein toteutettuna ja niissä olevien samankaltaisuuksien ansiosta näitä tapoja on mahdollista myös yhdistellä keskenään.

Toisessa tutkimuskysymyksessä haettiin vastausta tietojenkalastelulta suojautumiseen. Tietojenkalastelua vastaan suojautuessa on olemassa kaksi päätapaa: teknologiset ratkaisu ja koulutus. Teknologisiksi ratkaisuiksi tietojenkalastelusähköpostiviestejä vastaan on kehitetty esimerkiksi erilaisia suodattimia eri sähköpostipalveluihin, todennus- ja vahvistuspalveluita, viruksentorjuntaohjelmiin on sisällytetty tietojenkalastelun ehkäisy ja teknologiayritykset ovat lisänneet tuotteisiinsa mustia listoja tietojenkalasteluverkkosivuista ja tunnetuista tietojenkalastelun tekijöistä. Teknologisten ratkaisuiden avulla tietojenkalastelua voidaan ehkäistä, mutta mikään teknologinen ratkaisu ei ole täysin varma tietojenkalastelua vastaan, sillä tietojenkalastelua ei yleensä kohdisteta järjestelmää kohtaan, vaan se kohdistetaan käyttäjään, sillä ihminen eli käyttäjä on aina tietoturvan heikoin lenkki. Siksi ihmisten koulutus tietojenkalastelua vastaan on tärkeää. Ihmisten kouluttamista varten on kehitetty erilaisia palveluita ja ohjelmia, joiden avulla ihmiset voivat kouluttautua tunnistamaan tie-

tojenkalastelua. Koulutuksenkaan avulla ei silti voida ehkäistä tietojenkalastelua kokonaan, vaan myös henkilö joka on saanut koulutusta tietojenkalatelua vastaan, voi joutua sen uhriksi. Kaikista paras lopputulos saadaan yhdistämällä sekä teknologiset ratkaisut, että ihmisten koulutus. Tällöin päästään lopputulokseen, jossa tietojenkalastelun havaitseminen tarpeeksi ajoissa on todennäköisintä.

Tutkielman viimeinen tutkimuskysymys käsitteli sitä, että miksi tietojenkalastelu onnistuu. Tietojenkalastelun onnistumisen kannalta on usein tärkeää ymmärtää ihmisten päätöksentekoprosessia ja sitä, kuinka sen avulla voi saada tietojenkalastelun onnistumaan. Tietojenkalastelijat pyrkivät usein vaikuttamaan ihmisten tunteisiin ja siten he saavat ihmiset tekemään päätöksiä joita he eivät ajattele loppuun asti, ennen kuin on jo liian myöhäistä. Tietojenkalastelu-viesteillä pyritään usein myös ihmiset uskomaan, että heillä on kiire toimia ja siten ihmiset eivät kerkeä ajatella niin selkeästi ennen päätöksentekoaan. Tietojenkalastelijat pyrkivät myös hankkimaan kohteensa luottamuksen, esiintymällä jonain luotettavana tahona. Tietojenkalastelu voi onnistua käytännössä kenelle tahansa, mutta tutkimusten mukaan tietyt tekijät henkilöissä altistavat ihmisiä enemmän tietojenkalastelun onnistumiselle. Tutkimusten mukaan kaikista alttiimpia tietojenkalastelulle ovat 18-25 vuotiaat naiset, joilla ei ole teknologista kokemusta ja koulutusta liittyen tietojenkalasteluun. Kuvio 3 kuvaa edellä läpikäytyjä tutkielman keskeisimpiä tutkimustuloksia.



KUVIO 3 Tutkielman keskeiset tulokset

Tämä tutkielma tehtiin käytännössä kokonaan tietojenkalastelusta sähköpostin välityksellä, vaikka on olemassa paljon muitakin alustoja, joiden avulla voidaan toteuttaa tietojenkalastelua. Joitain tutkielmassa esitettyjä asioita voidaan kuitenkin myös hyödyntää tarkasteltaessa tietojenkalastelua muissakin kuin sähköpostipalveluissa. Monet tutkielmassa esitetyt tietojenkalastelutavat ja suojautumiskeinot toimivat myös muualla kuin sähköpostissa. Tietojenkalastelun onnistumiseen vaikuttavia tekijöitä voidaan myös soveltaa muissakin alustoissa kuin pelkästään sähköpostissa. Tietojenkalastelukeinoja ja suojautumistapoja on myös olemassa paljon enemmän kuin tutkielmassa esitellyt keinot ja suojautumistavat. Tutkielmassa kuitenkin pyrittiin käsittelemään yleisimpiä ja tärkeimpiä keinoja ja suojautumistapoja.

Teknologia kehittyy koko ajan ja siksi koko ajan tulee uusia keinoja ja alustoja tietojenkalastelulle. Tietojenkalastelussa riittää siis myös tulevaisuudessa paljon tutkittavaa. Tulevaisuuden tutkimuskohteita voisivat olla esimerkiksi juuri uusiin teknologioihin liittyvä tietojenkalastelu ja tietojenkalastelijoiden profiloiminen ja heidän motiiviensa kartoittaminen. Varsinaisista tietojenkalastelijoista henkilöinä ei ole tehty kovin paljoa tutkimusta. Tietojenkalastelun onnistumisen taustalla olevia psykologisia syitä voisi myös kartoittaa vielä enemmän tulevaisuudessa.

LÄHTEET

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A. & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE Communications Surveys & Tutorials, 15*(4), 2070-2090.

Banu, M. N. & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies, 4*(6), 783-786.

Birk, D., Gajek, S., Grobert, F., & Sadeghi, A. R. (2007). Phishing phishers-observing and tracing organized cybercrime. Teoksessa *Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on* (3). IEEE.

Caldwell, T. (2013). Spear-phishing: How to spot and mitigate the menace. *Computer Fraud & Security, 2013*(1), 11-16.

Chaudhry, J. A., Chaudhry, S. A. & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and its Applications, 10*(1), 247-256.

Chaudhary, S. (2016). *The use of usable security and security education to fight phishing attacks* (Väitöskirja). Tampere: Tampere University Press. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-03-0292-4

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, narrative and the" Nigerian Letter" in electronic mail. Teoksessa *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (70). IEEE.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. Teoksessa *Proceedings of the SIGCHI conference on Human Factors in computing systems* (581-590). ACM.

Dodge, R. C., Carver, C. & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. Teoksessa *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (37-44). ACM..

Dyrud, M. A. (2005). I brought you a good news: An analysis of Nigerian 419 letters. Teoksessa *Proceedings of the 2005 Association for Business Communication Annual Convention* (20-25).

Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. Teoksessa *Proceedings of the 16th international conference on World Wide Web* (649-656). ACM.

Gajek, S., Sadeghi, A. R., Stuble, C., & Winandy, M. (2007). Compartmented security for browsers-or how to thwart a phisher with trusted computing. Teoksessa *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on* (120-127). IEEE.

Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. John Wiley & Sons.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

Isacenkova, J., Thonnard, O., Costin, A., Francillon, A. & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security, 2014*(1), 1-18.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Jakobsson, M. & Myers, S. (toim.). (2007). *Phishing and countermeasures : Understanding the increasing problem of electronic identity theft*. Hoboken, N.J.: Wiley-Interscience.

Jansson, K. & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584-593.

Khan, A. A. (2013). Preventing phishing attacks using one time password and user machine identification. *arXiv Preprint arXiv:1305.2704*

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. Teoksessa *Proceedings of the 5th Symposium on Usable Privacy and Security* (3). ACM.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT), 10*(2), 7.

Litan, A. (2004). Phishing attack victims likely targets for identity theft. *Gartner Group research, 2004.*

Mayhorn, C. B. & Nyeste, P. G. (2012). Training users to counteract phishing. *Work, 41*(Supplement 1), 3549-3552.

Okoli, C. & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Working Papers on Information Systems*, 10 (26).

Osuuspankki tietojenkalasteluohjeistus (1.6.2016). Haettu 15.11.2017 osoitteesta: https://www.op.fi/op/henkiloasiakkaat/tietoturva/opn-asiakkaiden-tietojenkalastelu-aktiivista---huijarit-kayttavat-myos-puhelinta?cid=151881773&srcpl=3

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security, 2012*(1), 8-11.

PhisTank (2017). *PhisTank Stats, 2017*. Haettu 20.10.2017 osoitteesta https://www.phishtank.com/stats.php

Pattinson, M., Jerram, C., Parsons, K., McCormac, A. & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28.

Robila, S. A., & Ragucci, J. W. (2006). Don't be a phish: steps in user education. Teoksessa *ACM SIGCSE Bulletin* (Vol. 38, No. 3, 237-241). ACM.

RSA EMC2 ” 2013 A Year in Review” (2014), Haettu 4.11.2017 osoitteesta http://www.emc.com/collateral/fraudreport/rsa-online-fraud-report-012014.pdf

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility

and effectiveness of interventions. Teoksessa *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (373-382). ACM.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. Teoksessa *Proceedings of the 3rd symposium on Usable privacy and security* (88-99). ACM.

Speed, T., Nykamp, D., Heiser, M., Anderson, J. & Nampalli, J. (2013). *Mobile security : How to secure, privatize and recover your devices*. Birmingham: Packt Publishing.

Streeter, D. C. (2015). The effect of human error on modern security breaches. *Strategic Informer: Student Publication of the Strategic Intelligence Society, 1*(3), 2.

Tambe Ebot, A. C. (2017). *Explaining two forms of internet crime from two perspectives: Toward stage theories for phishing and internet scamming* (Väitöskirja). Jyväskylä Studies in Computing 172. Jyväskylän yliopisto. Haettu osoitteesta http://urn.fi/URN:ISBN:978-951-39-6954-7

Ultrascan Advanced Global Investigations (23.7.2014): *419 Advance Fee Fraud Statistics 2013*. Haettu 15.11.2017 osoitteesta http://www.ultrascan-agi.com/public_html/html/pdf_files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H. R. (2011). Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576-586.

Wang, J., Herath, T., Chen, R., Vishwanath, A. & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication, 55*(4), 345-362.

Yle Uutiset: ”Siirto eteläafrikkalaiselle tilille käynnisti poliisitutkinnan: Sunny Car Centerin maksu jäädytettiin” (21.8.2014). Haettu 20.11.2017 osoitteesta https://yle.fi/uutiset/3-7423771