Ida Koskinen

TIETOJENKALASTELUN TAVAT JA SUOJAUTUMIS-KEINOT

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Koskinen, Ida
Tietojenkalastelun tavat ja suojautumiskeinot
Jyväskylä: Jyväskylän yliopisto, 2016, 26 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Seppänen, Ville

Tässä kandidaatin tutkielmassa käsitellään tietojenkalastelun tapoja ja erilaisia suojautumiskeinoja kirjallisuuskatsauksen keinoin. Tietojenkalastelu on jatkuvasti kasvava ilmiö, mikä ei rajoitu enää pelkästään sähköpostiin. Nykyään tietojenkalastelua esiintyy esimerkiksi tekstiviesteissä, pikaviesteissä ja yhteisöpalveluissa. Tietojenkalastelu voi aiheuttaa merkittäviä henkilökohtaisia ja taloudellisia vahinkoja sekä yrityksille että yksityishenkilöille. Tästä huolimatta käyttäjät eivät useinkaan ole tarpeeksi tietoisia tietojenkalastelun riskeistä ja käyttäjät nähdäänkin usein heikoimpana lenkkinä tietoturvassa. Tietojenkalastelun tavat kehittyvät koko ajan, eikä yhtä luodinkestävää ratkaisukeinoa ole olemassa. Usein parhaan suojan saa yhdistelemällä useita suojautumiskeinoja. Käyttäjien kouluttaminen on myös tärkeää, sillä tekniset suojautumiskeinot eivät torju kaikkia hyökkäyksiä.

Asiasanat: tietojenkalastelu, hyökkäys, suojautuminen, käyttäjän manipulointi, tietoturva

ABSTRACT

Koskinen, Ida
Phishing methods and defenses
Jyväskylä: University of Jyväskylä, 2016, 26 p.
Information Systems, Bachelor's Thesis
Supervisor: Seppänen, Ville

The goal of this bachelor's thesis is to examine phishing methods and different defenses with a literature review. Phishing is continuously growing phenomenon which is no longer limited only to email. Today phishing occurs for example in text messages, instant messages and social networking sites. Phishing can cause significant personal and financial damage to both businesses and individuals. Despite this, users are often not aware enough of the risks of phishing and users are often seen as the weakest link in the information security. Phishing methods are developing all the time and no single silver-bullet solution exists. Often the best protection may be a combination of several protection methods. Training of users is also important because technical defenses don't prevent all the attacks.

Keywords: phishing, attack, defense, social engineering, information security

SISÄLLYS

1 JOHDANTO

Internet on tämän päivän suurin kommunikointikanava ja se on osa jokapäiväistä elämää. Käytämme internetiä niin työskentelyyn kuin vapaa-ajan viettoon, ja internetin avulla hoidamme nykyään myös esimerkiksi laskujen maksamisen. Lisäksi internet koskettaa koko ajan yhä suurempaa yleisöä, kun lapset siirtyvät yhä nuorempina käyttämään internetiä. Vaikka internet on mullistanut elämän täysin ja mahdollistanut paljon asioita, joita ilman internetiä ei olisi voitu toteuttaa, liittyy siihen myös uhkia.

Käyttäjän manipulointi (*engl. social engineering*) on keino saada käyttäjät vaarantamaan tietojärjestelmien turvallisuus. Sen sijaan, että tietojärjestelmiä vastaan hyökättäisiin teknisesti, valitaan käyttäjät hyökkäyksen kohteeksi ja pyritään saamaan heidät luovuttamaan pääsy haluttuun tietoon. Tämä voi tapahtua esimerkiksi manipuloimalla käyttäjiä paljastamaan arkaluontoista tietoa tai jopa suorittaa hyökkäys käyttämällä vaikutusvaltaa ja suostuttelua. (Krombholz, Hobel, Huber & Weippl, 2015.)

Käyttäjän manipuloinnin perimmäisenä tavoitteena on saada suora pääsy yrityksen tietoihin tai tietojärjestelmään. Saatuaan pääsyn haluttuihin tietoihin, hyökkäyksen toteuttaja voi kerätä, muuttaa tai tuhota tietoja samoin kuin häiritä palveluita. Käyttäjän manipuloinnin hyökkäykset voidaan luokitella esimerkiksi fyysisiin, sosiaalisiin, teknisiin ja sosioteknisiin. (Thornburgh, 2004.)

Yksi sosioteknisen käyttäjän manipuloinnin muoto on tietojenkalastelu. Tietojenkalastelu toteutetaan yleensä sähköpostin tai suoraviestinnän avulla ja se on suunnattu suurelle käyttäjäryhmälle, samoin kuin roskaposti. Käyttäjän manipulointi on puolestaan suunnattu joko yksilöihin tai pieniin ihmisryhmiin. (Krombholz ym., 2015.)

Termi tietojenkalastelu (*engl. phishing*) keksittiin vuonna 1996 kuvaamaan America On-line:n (AOL) käyttäjätilien kohtaamia käyttäjän manipuloinnin hyökkäyksiä. Tietojenkalastelun määritelmä ei kuitenkaan ole johdonmukainen kirjallisuudessa. Tämän aiheuttaa se, että tietojenkalastelu on laaja ongelma ja se sisältää vaihtelevia toimintaperiaatteita. (Khonji, Iraqi & Jones, 2013.)

Nirmal, Janet ja Kumar (2015) määrittelevät tietojenkalastelun olevan verkossa tapahtuva turvallisuuteen kohdistuva hyökkäys, missä hakkerin tavoit-

teena on kerätä käyttäjien arkaluontoisia tietoja, kuten salasanoja tai luottokorttitietoja. Hyökkäys toteutetaan uskottelemalla käyttäjille, että kaikki mitä he näkevät, on totta (Nirmal ym., 2015).

Hongin (2012) mukaan tietojenkalastelulla tarkoitetaan puolestaan eräänlaista käyttäjän manipuloinnin tapaa, jossa rikolliset käyttävät huijaussähköpostiviestejä saadakseen ihmiset jakamaan arkaluontoisia tietoja tai asentamaan haittaohjelman tietokoneelleen. Uhrit kuvittelevat viestien tulevan luotettavalta taholta, vaikka todellisuudessa ne tulevat huijarilta. Sen sijaan, että tietojenkalastelu kohdistuisi järjestelmiin joita ihmiset käyttävät, se kohdistuu ihmisiin, jotka käyttävät kyseisiä järjestelmiä. (Hong, 2012.)

Chaudhry, Chaudry ja Rittenhouse (2016) kuvailevat tietojenkalastelun olevan keino huijata käyttäjiä antamaan henkilökohtaisia ja taloudellisia tietoja tai lähettämään varoja suoraan hyökkääjille. Yleisimmät kalasteluhyökkäykset käyttävät elektronista viestintää, kuten sähköpostia, levittääkseen linkkiä haitalliselle sivustolle joka näyttää luotettavalta. Tietojenkalastelu on sekamuotoinen hyökkäys, joka yhdistää sekä käyttäjänmanipulointia että teknistä puolta. Näin ollen tietojenkalastelun torjunta vaatii molempien puolien huomioimista. (Chaudhry ym., 2016.)

Tietojenkalastelu koskettaa suurta määrää ihmisiä. Vuonna 2007 arviolta 3,6 miljoonaa ihmistä Yhdysvalloissa joutui tietojenkalastelun uhriksi. Uhrit menettivät yhteensä 3,2 miljardia dollaria hyökkäyksissä. (Bergholz ym., 2010.) Tämän lisäksi tietojenkalastelu on jatkuvasti kehittyvä uhka. Vishwanath, Harrison ja Ng (2016) kuvailevat tietojenkalastelun olevan yksi suurimmista uhkista kyberturvallisuudelle. Vuodesta 2007 kyberrikollisuus on kasvanut 782 % ja tietojenkalastelu kattaa tästä yli kolmanneksen (Vishwanath ym., 2016.)

Tietojenkalastelu on yhä enemmän kaikkialle leviävä ja kehittyvä ilmiö, joka on levinnyt sähköpostiviesteistä jo IP-puheluihin, tekstiviesteihin, pikaviesteihin, yhteisöpalveluihin sekä moninpeleihin (Hong, 2012). Näin ollen tietojenkalastelu on ajankohtainen ilmiö ja erityisesti jatkuvasti kehittyvät tietojenkalastelun tavat kaipaavat lisää tutkimusta. Lisäksi erilaisten suojautumiskeinojen esittely on tärkeää, jotta käyttäjät pystyvät suojautumaan entistä tehokkaammin tietojenkalastelulta.

Tämän kandidaatin tutkielman tarkoituksena on tutkia tietojenkalastelua ja erityisesti erilaisia kalastelutapoja sekä suojautumiskeinoja. Tutkimus toteutetaan kirjallisuuskatsauksena ja tutkimuskysymyksinä tässä tutkielmassa toimivat seuraavat:

- Millaisia tietojenkalastelutapoja yksityishenkilöt ja yritykset voivat kohdata?
- Miten tietojenkalastelulta voi suojautua?

Tutkielman toisen luvun alussa kerrotaan yleisesti tietojenkalasteluhyökkäysten toteuttamisesta ja tietojenkalastelun kohdistamisesta. Tämän jälkeen luvussa siirrytään käsittelemään erilaisia tietojenkalastelutapoja, joita yksityishenkilöt ja yritykset voivat kohdata. Tietojenkalastelutavat kuitenkin kehittyvät koko ajan ja uusia menetelmiä tulee jatkuvasti lisää, joten tässä tutkielmassa on esitelty

joitain yleisimpiä tietojenkalastelutapoja. Lisäksi tietojenkalasteluhyökkäykset ovat usein hyvinkin monimuotoisia ja saattavat sisältää piirteitä useammastakin kalastelutekniikasta, jolloin niiden määrittely vain yhden tekniikan edustajaksi on vaikeaa.

Kolmannessa luvussa käydään läpi erilaisia suojautumiskeinoja, joiden avulla tietojenkalastelulta voidaan suojautua. Suurin osa suojautumiskeinoista on teknisiä, mutta näiden lisäksi myös käyttäjien kouluttamisella on suuri rooli tietojenkalastelun torjunnassa.

Neljännessä luvussa eli yhteenvedossa kerrataan saadut tulokset ja kootaan tutkielmassa käsitellyt asiat yhteen. Lisäksi yhteenvedossa esitellään mahdollisia jatkotutkimusaiheita myöhempiä tutkimuksia varten.

2 TIETOJENKALASTELUN TAVAT

Tässä luvussa esitellään erilaisia tietojenkalastelun tapoja. Ensiksi tarkastellaan, miten tietojenkalasteluhyökkäys yleensä toteutetaan ja millaisia vaiheita hyökkäyksessä voidaan nähdä. Seuraavaksi käsitellään tietojenkalastelun kohdistamista. Tämän jälkeen siirrytään tutkimaan erilaisia tietojenkalastelutapoja.

2.1 Tietojenkalasteluhyökkäyksen toteuttaminen

Khonji, Iraqi ja Jones (2013) toteavat tietojenkalasteluhyökkäysten kohdistuvan haavoittuvuuksiin, jotka löytyvät järjestelmistä inhimillisten tekijöiden vuoksi. Useat kyberhyökkäykset leviävät käyttäjien heikkouksia hyödyntävien mekanismien avulla, mikä tekee käyttäjistä heikoimman elementin turvallisuusketjussa (Khonji ym., 2013).

Tietojenkalastelu toteutetaan yleensä sarjana vaiheita, jotka johtavat uhrin antamaan henkilökohtaisia tai taloudellisia tietojaan jollekin, ketä uhri pitää vilpittömänä henkilönä. Tietojenkalastelussa hyökkääjä käyttää sosiaalisia taitojaan saadakseen tietoja henkilöstä, organisaatiosta tai sen tietokonejärjestelmistä. (Nirmal ym., 2015.)

Tietojenkalasteluhyökkäyksen nähdään muodostuvan kolmesta osasta: syötistä, koukusta ja sieppauksesta. Syötti on yleisimmin luotettavalta näyttävä sähköpostiviesti, joka sisältää linkin koukkuun. Koukku on usein piilotettu monimutkaistamalla URL:ää. Koukkuna toimii sivusto, joka matkii luotettavaa sivustoa jolle uhri on valmis antamaan luottamuksellisia tietoja. Sieppaukseen kuuluu kerättyjen tietojen hyödyntäminen hyökkääjän toimesta. (Chaudhry ym., 2016.)

Normaalisti tietojenkalasteluhyökkäys alkaa siten, että hyökkääjä isännöi huijaussivustoa. Seuraavaksi käyttäjä vastaanottaa vakuuttavan sähköpostin, joka sisältää huijaussivustolle johtavan linkin. Kolmanneksi käyttäjä painaa linkkiä ja luotettavan sivuston näköinen huijaussivusto aukeaa. Viimeiseksi käyttäjä antaa luottamuksellisia tietojaan huijaussivustolle ja hyökkääjä käyttää

keräämiään tietoja omien henkilökohtaisten hyötyjen saavuttamiseksi. (Nirmal ym., 2015.)

2.2 Tietojenkalastelun kohdistaminen

Normaalia tietojenkalastelua ei kohdisteta tiettyihin yksilöihin tai ryhmiin, vaan tarkoituksena on saada mahdollisimman moni menemään lankaan (Krombholz ym., 2015). Viime vuosina on kuitenkin alkanut esiintyä myös erittäin tarkkaan kohdistettua ja suurta vahinkoa yrityksille aiheuttavaa tietojenkalastelua (Zhao, An & Kiekintveld, 2016). Tiettyyn henkilöön tai ryhmään kohdistuvaa tietojenkalastelua kutsutaan termillä spear phishing ja sen muoto, jossa uhriksi valitaan korkean luokan henkilö, on nimetty whalingiksi.

Spear phishing eli keihäsmäinen tietojenkalastelu tarkoittaa tietojenkalastelun kohdistamista tiettyyn henkilöön tai ryhmään sen sijaan, että pyrittäisiin kalastelemaan sattumanvaraisten käyttäjien tietoja. Ennen keihäsmäisen tietojenkalastelun toteuttamista, hyökkääjä yleensä etsii potentiaalisia uhreja ja tietoja heistä, jonka jälkeen hyökkääjä voi lähettää viestin, joka vaikuttaa tulevan luotettavalta lähteeltä. (Chaudhry ym., 2016.) Viesti saattaa vaikuttaa tulevan esimerkiksi ystävän sähköpostiosoitteesta ja se voi sisältää kuvan tai muuta sisältöä, jota uhriksi joutunut on tottunut saamaan ystävältään (Heartfield & Loukas, 2016).

Whaling on yksi keihäsmäisen tietojenkalastelun muoto. Siinä uhreiksi valitaan korkean luokan henkilöitä, kuten yritysjohtajia tai virkamiehiä. (Chaudhry ym., 2016.) Esimerkiksi vuonna 2008 Yhdysvalloissa toteutettiin whaling -hyökkäys, jossa useille toimitusjohtajille lähetettiin valheellinen haaste. Haasteen mukana tuli liite, joka sisälsi haittaohjelman. (Hong, 2012.)

Keihäsmäinen tietojenkalastelu aiheuttaa erityisesti yrityksille uudenlaisia ongelmia. Yrityksen työntekijät voidaan valita uhreiksi, jolloin hyökkääjä pyrkii saamaan työntekijät luovuttamaan yrityksen tärkeitä tiedostoja tai myöntämään hyökkääjälle pääsyn yrityksen tärkeisiin tietoihin. Hyökkääjä voi väittää esimerkiksi olevansa suuren yrityksen toisen toimipisteen työntekijä, joka tarvitsee jostain syystä pääsyn sellaisiin tietoihin, mihin hänellä ei ole oikeuksia. Yhdenkin työntekijän lankeaminen huijaukseen voi aiheuttaa yritykselle suuriakin tappioita. (Hong, 2012.)

2.3 Erilaiset tietojenkalastelutavat

2.3.1 **Linkkien manipulointi**

Ehkä yleisin tapa toteuttaa tietojenkalasteluhyökkäys on lähettää suurelle määrälle käyttäjiä sähköpostiviesti, joka sisältää linkin huijaussivustolle. Sähköpostiviestin tulee muistuttaa mahdollisimman paljon luotettavaa viestiä, jotta käyt-

täjät luulevat sitä aidoksi ja siinä pitää olla mukana sopiva viesti. Käytettyjä viestejä ovat esimerkiksi ilmoitus tilin lopettamisesta tai uudesta tilitapahtumasta, jonka käyttäjä tunnistaa vääräksi ja täten hänen täytyy käydä perumassa se. (Moore & Clayton, 2007a.)

Käyttäjä joutuu huijaussivustolle klikattuaan sähköpostissa ollutta linkkiä. Käyttäjän selain saattaa päästä suoraan kalastelusivustolle tai tulla uudelleen ohjatuksi alkuperäiseltä sivustolta. Uudelleenohjaus voi tapahtua esimerkiksi hyödyntämällä laillista uudelleenohjausohjelmistoa Googlelta tai Ebayltä. Aukeneva sivusto on täydellinen kopio sivusta, jolle käyttäjä luulee menevänsä ja sisältää usein varoituksia huijauksista, mikä vakuuttaa käyttäjän antamaan tietonsa sivustolle. (Moore & Clayton, 2007a.)

Clone phishing eli kloonattu tietojenkalastelu tarkoittaa sitä, että aiemmin vastaanotettu luotettava sähköpostiviesti kloonataan, jolloin siitä saadaan tehtyä huijausviesti. Huijausviesti sisältää yleensä linkin hyökkääjän internet sivustolle. Linkit on usein tehty näyttämään luotettavilta linkeiltä esimerkiksi korvaamalla O-kirjaimet numerolla 0. (Chaudry ym., 2016.)

2.3.2 **Verkkosivustojen väärentäminen**

Useimmat kalasteluyritykset yrittävät saada käyttäjät menemään väärennetyille sivustoille ja antamaan henkilökohtaisia tietojaan. Isännöidäkseen huijaussivustoa, kalastelijat käyttävät ilmaisia webhotelleita ja vaarantunutta konetta tai rekisteröivät uuden verkkotunnuksen. (Hong, 2012.)

Rekisteröitäessä uutta verkkotunnusta, kalastelijat etsivät nimiä, jotka muistuttavat sivustoja, joita he haluavat imitoida. Esimerkiksi kalastelija, joka haluaa imitoida Ebayn sivuja, saattaa rekisteröidä tunnuksen ebay-login.com. Toinen yleisesti käytetty tapa on vaihtaa oikean osoitteen kirjaimia siten, ettei eroa juurikaan huomaa. Tästä esimerkkinä toimivat w:n korvaaminen kahdella v-kirjaimella tai O:n korvaaminen numerolla 0. (Hong, 2012.)

Yksi muoto verkkosivustojen väärentämisestä on kuva-kuvassa -hyökkäys (*engl. picture-in-picture attack*). Kuva-kuvassa -hyökkäyksessä kalastelusivusto näyttää väärennetyn ponnahdusikkunan, joka jäljittelee oikeaa sivustoa näyttävää selainta (Herzberg & Jbara, 2008). Väärennettyjä ponnahdusikkunoita ei voi raahata ulos niiden pääikkunoista eikä niitä voi maksimoida. Näin ollen yksi tapa testata, onko ponnahdusikkuna aito vai väärennös, on raahata ponnahdusikkuna ulos pääikkunasta ja kokeilla maksimoida sitä. (Jackson, Simon, Tan & Barth, 2007.)

Hakukonekalastelussa (*engl. Search Engine Phishing*) kalastelijat luovat väärennettyjä verkkosivustoja ja saavat hakukoneet näyttämään ne. Kalastelijat manipuloivat hakukoneita siten, että ne näyttävät väärennetyt sivustot parhaimpina tuloksina. Tällöin käyttäjät erehtyvät helposti luulemaan väärennettyjä sivuja aidoiksi. Hakukoneella tehty haku johdattaa uhrit näille väärennetyille sivustoille, joissa käyttäjät voivat päätyä antamaan henkilökohtaisia tietoja luullessaan olevansa luotettavalla sivustolla. (Chaudhry ym., 2016; Heartfield & Loukas, 2016.)

2.3.3 **Clickjacking**

Clickjacking, eli vapaasti suomennettuna klikkauksien kaappaus, on nouseva ilmiö internetissä. Klikkauksien kaappauksille voivat altistua sovellukset ja sivustot, jotka sisältävät graafista sisältöä. Clickjacking pyrkii saamaan käyttäjän olemaan vuorovaikutuksessa, eli esimerkiksi klikkaamaan, käyttöliittymäelementtejä. (Huang, Moshchuk, Wang, Schecter & Jackson, 2012.) Clickjacking tapahtuu siten, että hyökkääjä lisää luotettavan nettisivuston päälle läpinäkyvän sivuston, joka on haitallinen. Käyttäjä luulee olevansa luotettavalla sivustolla ja painavansa luotettavia painikkeita, vaikka todellisuudessa hän on kalastelusivustolla. (Shahriar & Haddad, 2015.)

Likejacking, eli vapaasti suomennettuna tykkäyksien kaappaus, on yksi clickjackingin muoto. Siinä hyökkääjän sivusto huijaa käyttäjät klikkaamaan Facebookin ”tykkää” -painiketta sijoittamalla näkymättömän painikkeen harmittoman käyttöliittymäelementin, kuten ”lunasta ilmainen iPad” -painikkeen päälle. Kun käyttäjä pyrkii lunastamaan ilmaisen iPadin, ilmestyy hänen Facebook -ystäviensä uutisvirtaan ilmoitus, jonka mukaan käyttäjä on tykännyt hyökkääjän sivustosta. (Huang ym., 2012; Rehman, Khan, Saqib & Kaleem, 2013.)

Toinen clickjackingin muoto on cursorjacking eli vapaasti suomennettuna kursorin kaappaus. Cursorjacking hyödyntää tekniikkaa, joka muuttaa kursorin sijaintia. Käyttäjä siis näkee kursorin olevan tietyssä kohdassa, vaikka todellisuudessa kursori onkin jossain muualla. Hyökkääjä korvaa oikean kursorin valekursorilla, ja saa näin ollen käyttäjän painamaan haluttua kohtaa. (Rehman ym., 2013.)

2.3.4 **Haittaohjelmapohjainen kalastelu**

Malware-Based phishing eli vapaasti suomennettuna haittaohjelmapohjainen tietojenkalastelu tarkoittaa hyökkäyksiä, jotka johtavat haittaohjelmien asentamiseen ja niiden käyttämiseen uhrien tietokoneilla. Yleensä haittaohjelma on esitetty sähköpostin liitteenä, joka on ladattavissa. Kalasteluhyökkäyksissä asennetut haittaohjelmat sisältävät usein keyloggereita ja näytön kaappaajia, eli vakoiluohjelmia, jotka kaappaavat näppäimistön syöttöä tai näytön kuvaruutua ja lähettävät tiedot tietojenkalastelijalle. Joissain tapauksissa myös uhrien tietokoneiden kontrolloiminen voi olla hyökkäyksen tavoite. Tietokonetta voi tällöin käyttää myöhempiin kalasteluhyökkäyksiin erityisesti uhrien tuttavia vastaan, jolloin heille pystytään lähettämään roskapostia tai heitä vastaan voidaan tehdä palvelunestohyökkäys. (Chaudhry ym., 2016.)

Haittaohjelmaa voidaan käyttää myös istunnon kaappaamiseen, jossa käyttäjän verkkotoimintoja tarkkaillaan kunnes todennettu istunto tietyn tilin kanssa on vakiintunut. Kun yhteys on vakiintunut, haittaohjelma ottaa vallan ja voi suorittaa luvattomia toimenpiteitä, kuten rahan siirtämistä, käyttäjän huomaamatta. (Chaudhry ym., 2016.)

2.3.5 **Paha kaksonen -hyökkäys**

Evil twin eli paha kaksonen -hyökkäys tarkoittaa sitä, että WiFi -verkkoon pystytetään tukiasema, joka toimii tietojenkalasteluvälineenä. Kalastelijan pystyttämä tukiasema näyttää luotettavalle, mutta todellisuudessa se tarjoaa kalastelijalle mahdollisuuden tarkkailla yhteyden käyttöä. Paha kaksonen -hyökkäys on helppo toteuttaa. Hyökkääjä pystyy konfiguroimaan kannettavan tietokoneen helposti saatavilla olevien ohjelmistojen avulla toimimaan tukiasemana langattomassa verkossa. Seuraavaksi hyökkääjä pystyy selvittämään oikean tukiaseman käyttämän SSID:n eli langattoman lähiverkon verkkotunnuksen ja radiotaajuuden. Tämän jälkeen hyökkääjä voi ottaa käyttöön oman tukiasemansa, joka käyttää samaa SSID:tä kuin oikea tukiasemakin. (Song, Yang & Gu, 2010.)

Paha kaksonen -hyökkäys on usein onnistunut, sillä hyökkääjä sijoittaa oman tukiasemansa lähemmäksi käyttäjiä, jolloin sillä on voimakkaampi signaali käyttäjien laitteisiin kuin oikealla tukiasemalla. Käyttäjien tietokoneet valitsevat kalastelijan tukiaseman automaattisesti, jos valittavissa on useita tukiasemia samalla SSID:llä. Myös ne käyttäjät, jotka valitsevat tukiaseman manuaalisesti, päätyvät yleensä pahaan kaksoseen, koska sen signaali on vahvin. (Song ym., 2010.)

Paha kaksonen -hyökkäykset ovat suosittuja, koska niitä on helppo tehdä ja vaikea jäljittää. Tukiasemia voidaan pystyttää ja sammuttaa yhtäkkiä ja satunnaisesti, minkä lisäksi hyökkäykset ovat hyvin lyhytaikaisia hyökkääjän lopettaessa hyökkäyksen heti, kun hän on saavuttanut tavoitteensa. Paha kaksonen -hyökkäyksiä esiintyy eniten lentokenttien, kahvioiden, hotellien ja kirjastojen läheisyydessä. (Song ym., 2010.)

Hyökkäyksen avulla hyökkääjä pystyy sieppaamaan arkaluonteisia tietoja, kuten salasanoja ja luottokorttitietoja, vakoilemalla tietoliikenneyhteyksiä tai aloittamalla man-in-the-middle -hyökkäyksen. Hyökkääjä voi myös manipuloida DNS -palvelimia tai DNS -viestintää, ohjata reititystä ja aloittaa uusia kalasteluhyökkäyksiä. (Song ym., 2010.) Paha kaksonen -hyökkäys ei ole suunnattu kehenkään tiettyyn henkilöön, vaan potentiaalisia uhreja ovat kaikki toimintasäteellä sijaitsevat käyttäjät (Heartfield & Loukas, 2016).

2.3.6 **Mies välissä -hyökkäys**

Mies välissä -hyökkäys (*engl. Man-in-the-Middle Attack*) hyödyntää tietoa siitä, että HTTPS -palvelin lähettää todistuksen julkisen avaimen kanssa selaimelle. Jos tämä todistus ei ole luotettava, koko viestintäyhteys on altis haavoittuvuuksille. Mies välissä -hyökkäys korvaa alkuperäisen todistuksen todentamalla oikeaksi HTTPS -palvelimen, jolla on muokattu todistus. Hyökkäys on onnistunut silloin, jos käyttäjä laiminlyö todistuksen tarkistamisen, kun selain lähettää varoituksen. (Callegati, Cerroni & Ramilli, 2009.)

Mies välissä -hyökkäys toimii siten, että hyökkääjä toimii yhdyskäytävänä käyttäjän ja palvelimen välissä. Näin ollen hyökkääjä pystyy sieppaamaan käyttäjän ja palvelimen välillä liikkuvan liikenteen ja muokkaamaan halutessaan

kulkevia viestejä tai lisäämään sekaan uusia viestejä ilman, että kumpikaan osapuoli huomaa sitä. Mies välissä -hyökkäyksen vuoksi sekä käyttäjä että palvelin näkevät turvalliselta näyttävän yhteyden toistensa välissä. (Callegati ym., 2009.)

Mies välissä -hyökkäyksestä on olemassa myös erilaisia variaatioita, kuten lähiverkossa (LAN) tapahtuva hyökkäys. Siinä hyökkääjä on saman verkon sisällä kuin käyttäjä tai palvelin. LAN -verkossa tapahtuva hyökkäys voi johtua joko siitä, että LAN on täysin avoin, jolloin hyökkääjä voi vapaasti yhdistyä siihen, tai koska LAN -verkon palvelin on rikottu ja luvattomat käyttäjät voivat kirjautua sisään. (Callegati ym., 2009.) Myös GSM- ja UMTS -verkoissa voi tapahtua mies välissä -hyökkäyksiä (Meyer & Wetzel, 2004).

2.3.7 **Tekniset kalasteluhyökkäykset**

Jotkut kalasteluhyökkäykset on suunnattu käyttäjien tietokoneisiin tai internet yhteyksiin ennemmin kuin käyttäjiin. Tällaisia hyökkäyksiä ovat esimerkiksi järjestelmän uudelleenkonfigurointi hyökkäys ja pharming. Nämä ovat puhtaasti teknisiä hyökkäyksiä, eivätkä sisällä käyttäjän manipulointia. Näin ollen tulisi myös miettiä, voidaanko näitä kutsua tietojenkalasteluhyökkäyksiksi. (Chaudhry ym., 2016.)

System reconfiguration attacks eli vapaasti suomennettuna järjestelmän uudelleenkonfigurointi hyökkäykset muuttavat käyttäjien tietokoneiden asetuksia haitallisia tarkoituksia varten. Esimerkkinä tästä toimii tilanne, jossa kirjanmerkkeihin tallennettu pankin verkkosivujen URL on muutettu väärään muotoon, jolloin se johtaa käyttäjän väärälle sivustolle. (Chaudhry ym., 2016.)

Pharming on tietojenkalastelun muoto, joka muokkaa isäntätiedostoja, joita käytetään DNS:än horjuttamiseen. Tässä tapauksessa isäntätiedostot uhrin koneella tai hakuihin käytetty DNS on peukaloitu. Tämän seurauksena URL pyynnöt tai nimipalvelu palauttaa väärennetyn osoitteen ja myöhempi kommunikointi on ohjattu valesivustolle. Näin ollen käyttäjät saattavat antaa luottamuksellisia tietoja valesivustolle. (Chaudhry ym., 2016.)

2.3.8 **Uudenlaiset kalasteluhyökkäykset**

Myös älypuhelimet altistuvat tietojenkalastelulle. He, Chan ja Guizani (2015) luettelevat neljä keskeistä syytä sille, miksi hakkerit valitsevat älypuhelimet tietojenkalasteluun. Ensimmäisenä syynä on se, että on helppoa naamioida infektoituneet sovellukset luotettaviksi sovelluksiksi ja jakaa niitä sovelluskaupoissa. Toiseksi älypuhelimissa on yleensä pienet näytöt, jolloin on helpompi naamioida merkkejä luotettavuudesta, joihin käyttäjät luottavat päättäessään onko sivusto luotettava. Tällaisia merkkejä ovat esimerkiksi merkit siitä, että sivusto on suojattu tietoverkkosalausprotokollalla. Kolmanneksi älypuhelimissa on useita kanavia, kuten pikaviestit ja tekstiviestit, joiden kautta hakkerit voivat käyttää tietojenkalastelua. Neljänneksi käyttäjät eivät yleensä ole tietoisia siitä, että tietojenkalastelu on myös älypuhelimia koskeva uhka. Lisäksi monet

käyttäjät luottavat älypuhelimiinsa enemmän kuin tietokoneisiinsa. (He ym., 2015.)

Älypuhelimien lisäksi myös muut internetiin kytketyt laitteet voivat altistua erilaisille haittaohjelmille ja tietojenkalastelulle. Tämä on kasvava ongelma erityisesti siitä syystä, että yhä useampi kodinkone on kytketty internetiin. Tätä kutsutaan termillä esineiden internet (*engl. internet ot things*). Turvallisuus ja yksityisyys ovat suurimmat ongelmat esineiden internetissä (Suo, Wan, Zou & Liu, 2012). Tämä johtuu siitä, ettei perinteisiä turvallisuustoimenpiteitä voi lisätä suoraan esineiden internet -teknologioihin niiden erilaisuuden vuoksi. Näin ollen esineiden internetiin kuuluviin kodinkoneisiin tulee kehittää uudenlaisia suojamekanismeja tietoturvahyökkäyksiä vastaan. (Sicari, Rizzardi, Grieco & Coen-Porisini, 2015.)

3 SUOJAUTUMISKEINOT

Tietojenkalastelu on laaja ongelma, eikä yhtä luodinkestävää ratkaisua löydy vähentämään kaikkia haavoittuvuuksia tehokkaasti. Näin ollen useita menetelmiä käytetään samanaikaisesti, jotta tiettyjä hyökkäyksiä pystytään vähentämään. (Khonji ym., 2013.)

Tietojenkalastelun nähdään olevan sosiotekninen hyökkäys, jossa kalastelijat hyödyntävät uteliaisuutta, pelkoa ja empatiaa sekä perinteisiä kalastelutekniikoita huijatakseen käyttäjät uhreiksi. Näin ollen tietojenkalastelun tehokas torjunta vaatii molempien puolien huomioimista, mikä asettaa haasteita tehokkaiden suojautumiskeinojen luomiseen. (Chaudhry ym., 2016.) Vaikka pystyttäisiin kehittämään kalasteluhyökkäykset täydellisesti torjuva ohjelma, on riskinä aina se, että käyttäjä lankeaa hyökkäykseen jolloin toimiva järjestelmä ei yksin riitä torjumaan kaikkia hyökkäyksiä. Näin ollein yksi tärkeimmistä suojautumiskeinoista tietojenkalastelua vastaan onkin käyttäjien kouluttaminen ja tietoisuuden lisääminen.

Tässä luvussa esitellään erilaisia tapoja suojautua tietojenkalastelua vastaan. Suurin osa tavoista on teknisiä, mutta myös käyttäjien kouluttaminen on tärkeää ja siksi sekin on esitelty tässä luvussa.

3.1 Varoitukset

Ensimmäisiä nimenomaan tietojenkalastelua varten kehitettyjä suojautumiskeinoja olivat selaimissa olevat työkalurivit (Fette ym., 2007). Yleinen ongelma varoitusten kanssa on se, että käyttäjät sulkevat ne välittömästi niiden ilmaantuessa. Monet varoitukset ovat myös niin monimutkaisia, etteivät käyttäjät ymmärrä, mikä on ongelmana tai mitä heidän pitäisi tehdä. Jotkut varoitukset puolestaan häiritsevät käyttäjiä ärsyttävästi. Joskus varoitukset ovat myös niin huomaamattomia, etteivät käyttäjät näe niitä. (Hong, 2012.)

Egelmanin, Cranorin ja Hongin mukaan (2008) varoituksia on olemassa sekä passiivisia että aktiivisia. Passiiviset varoitukset ilmoittavat mahdollisista

vaaroista esimerkiksi vaihtamalla väriä tai näyttämällä tekstimuodossa olevaa tietoa häiritsemättä käyttäjää. Egelman ym. (2008) kuitenkin huomasivat tutkimuksessaan passiivisten varoitusten olevan hyödyttömiä, sillä ne jäävät usein huomaamatta tai käyttäjät eivät luottaneet niihin.

Microsoft Internet Explorer 7:stä löytyy passiivinen varoitus, joka on toteutettu ponnahdusikkunalla. Varoitus näytetään käyttäjälle, kun selain uskoo sivuston olevan epäilyttävä, mutta sen ei ole varmennettu olevan kalastelusivusto eli sitä ei löydy esimerkiksi mustalta listalta. Kyseinen varoitus ei anna käyttäjälle mitään vaihtoehtoja eikä se suosittele tekemään mitään. (Egelman ym., 2008.)

Aktiiviset varoitukset puolestaan pakottavat käyttäjän huomaamaan varoitukset häiritsemällä heitä. Esimerkkinä aktiivisesta varoituksesta on Microsoftin Internet Explorer 7:stä löytyvä varoitus, joka antaa käyttäjälle mahdollisuuden joko sulkea ikkunan (suositeltavaa) tai näyttää sivuston (ei suositeltavaa). Kyseinen varoitus on koko näytön laajuinen ja se muuttaa osoitekentän punaiseksi. (Egelman ym., 2008.)

3.2 Tietojenkalasteluviestien suodattaminen

Tietojenkalasteluviestien suodattaminen on ensisijainen suojautumiskeino roskapostia ja keihäsmäistä tietojenkalastelua vastaan (Zhao ym., 2016). Hongin (2012) mukaan ensimmäisen tietojenkalasteluviestien suodattimen kehittivät Fette, Sadeh ja Tomasic (2007). PILFERiksi nimetty suodatin hyödyntää koneoppimista sähköpostiviestien suodattamisessa. Suodatin tunnistaa, jos sähköposteissa käyty keskustelu on petollista eli uhriksi valittu luulee keskustelevansa luotettavan lähteen kanssa, vaikka todellisuudessa keskusteleekin hyökkääjän kanssa. Suodatin tunnistaa useita piirteitä, jotka merkitsevät hyvin usein tietojenkalastelua. Suodattimen havaitessa näitä piirteitä sähköpostiviesteissä, se merkitsee viestit tietojenkalasteluviesteiksi. Tällaisia piirteitä ovat esimerkiksi IP-pohjaiset URL:ät, yhteensopimattomat URL:ät sekä verkkotunnusten lukumäärä. (Fette ym., 2007.)

Ensimmäisen suodattimen kehittämisen jälkeen tutkijat ja kehittäjät ovat etsineet täydentäviä piirteitä ja kehittäneet koneoppimisen tekniikoita eteenpäin (Hong, 2012). Nykyään suodattimet hyödyntävät yleensä sekä mustia että valkoisia listoja ja koneoppimisen tekniikoita (Zhao ym, 2016).

3.3 Kalastelusivustojen esto

Kalastelusivustojen tunnistamiseen on olemassa kaksi yleistä tapaa: heuristiikat, jotka tutkivat URL:n, HTML:n ja palvelimen ominaisuuksia luokitellakseen sivustoja, sekä manuaalisesti varmennetut mustat listat (Hong, 2012).

3.3.1 **Heuristiikat**

Ensimmäisen puolustautumiskeinon tietojenkalastelua vastaan pitäisi olla Alsharnoubyn, Alacan ja Chiassonin (2015) mielestä automatisoitu tietojenkalastelun havaitseminen. Jos käyttäjät eivät koskaan näe hyökkäyksiä, eivät he voi niihin myöskään langeta. Automaattiset sähköpostin luokitteluun tarkoitetut työkalut käyttävät usein koneoppimisen tekniikoita, tilastollisia luokittelijoita ja roskapostisuodatin tekniikoita identifioidakseen potentiaalisia kalasteluviestejä. Kalastelusivustojen huomaamiseen tarkoitetut tekniikat puolestaan sisältävät mustat listat, koneoppimisen, URL ominaisuuksien luokittelun ja verkkotunnusten analysoinnin, visuaalisen samanlaisuuden arvioinnin, kontekstuaalisen analyysin ja käyttäjien käyttäytymisen ennustamisen sekä tiedon keräämisen. (Alsharnouby ym., 2015.)

Selaimiin on saatavilla useita erilaisia kaupallisia lisäosia, jotka on kehitetty estämään kalastelusivustoille pääsy tai varoittamaan mahdollisista kalastelusivustoista. Tutkimusten mukaan lisäosia kuitenkin käytetään lähinnä varoittamaan käyttäjiä kalastelusivustoista, eivätkä ne niinkään estä haitallisille sivustoille pääsyä. (Hong, 2012).

Heuristiikkojen käyttämisessä on sekä hyvät että huonot puolet. Heuristiikat voivat havaita hyökkäykset heti niiden ilmaantuessa toisin kuin mustia listoja käytettäessä, jolloin pitää odottaa listan päivittymistä. Huonona puolena on kuitenkin se, että hyökkääjät voivat suunnitella hyökkäykset siten, etteivät heuristiikat huomaa niitä. Lisäksi heuristiikat voivat tuottaa vääriä positiivisia, eli ne voivat virheellisesti merkitä laillisen sivuston kalastelusivustoksi. (Sheng ym., 2009.)

3.3.2 **Mustat listat**

Mustat listat voivat olla joko automaattisia, eli esimerkiksi koneoppimisen avulla toteutettuja, tai manuaalisesti ylläpidettyjä. Mustien listojen avulla kalastelusivustoille pääsy joko estetään tai käyttäjälle näytetään varoitus, mikäli hän yrittää mennä tiedetylle kalastelusivustolle. (Alsharnouby ym., 2015.) Mustat listat toimivat siten, että URL:iä verrataan mustalla listalla oleviin tunnettuihin kalastelusivustoihin. Mustat listat ovat olleet yksiä vallitsevista roskapostin suodatin tekniikoista. (Sheng ym., 2009.)

Tunnetuimmat mustat listat ovat Googlen, Microsoftin ja PhishTankin, joissa kaikissa URL:ät tarkistetaan manuaalisesti. Googlen musta lista on integroitu Firefoxin ja Chromen selaimiin, joten käyttäjiltä ei vaadita mitään erillisiä toimenpiteitä itsensä suojaamiseksi. (Hong, 2012.) Google on ilmoittanut, että 9500 sivustoa siirretään mustalle listalle päivittäin (Arachchilage & Love, 2014). Microsoftin musta lista on puolestaan integroitu Internet Explorerin selaimeen. PhishTankin musta lista hyödyntää internetin käyttäjien tietämystä kalastelusivustojen tunnistamiseen. PhishTankissa käyttäjät saavat ehdottaa mahdollisia kalastelusivustoja ja kun riittävän moni käyttäjä on käynyt äänestämässä kyseistä sivustoa kalastelusivustoksi, se siirretään mustalle listalle. (Hong, 2012.)

Sheng ym. (2009) selvittivät mustien listojen tehokkuutta käyttämällä 191 uutta kalastelusivustoa tutkiakseen kahdeksaa tietojenkalastelun estämiseen tarkoitettua työkalua. Tutkimuksen tuloksista käy ilmi, että mustat listat ovat alussa tehottomia, sillä suurin osa niistä tunnisti alle 20 % kalastelusivuista ensimmäisen tunnin aikana. Lisäksi mustia listoja päivitetään eri tahtiin ja 12 tunnin kuluttua 47–83 % kalastelusivustoista oli ilmestynyt mustille listoille. Tutkimuksessa huomattiin, että kaksi työkalua, jotka käyttivät heuristiikkoja täydentääkseen mustia listoja, tunnistivat merkittävästi enemmän kalastelusivustoja alussa kuin muut työkalut, jotka käyttivät vain mustia listoja. Heuristiikkojen tunnistamilla kalastelusivustoilla kesti kuitenkin kauan ilmestyä mustille listoille. (Sheng ym., 2009.)

Koska mustien listojen päivittäminen vie aikaa ja useat kalastelusivustot ovat pystyssä vain muutamista tunneista muutamaan päivään, on ehdotettu valkoisten listojen käyttöönottoa. Valkoiset listat sisältävät tiedot hyvistä URL:istä, joita verrataan esimerkiksi sähköpostiviestin sisältämään linkkiin. Valkoiset listat ovat vaikuttaneet lupaavilta, mutta ne tuottavat jonkin verran vääriä positiivisia tuloksia eli ne saattavat estää luotettaviakin sivustoja, kun taas mustat listat aiheuttavat ainoastaan vääriä negatiivisia. (Bergholz ym., 2010.)

3.4 Kalastelusivustojen alasajo

Useat organisaatiot tunnistavat ja ajavat alas kalastelusivustoja. Jos internetin käyttäjä yrittää mennä alasajetulle kalastelusivustolle, hänelle näytetään yleensä virheilmoitus ”page not found” (*suom. ”sivua ei löytynyt”*). APWG ja Carnegie Mellon yliopisto ovat kehittäneet tähän liittyen innovaation, jonka mukaan kalastelusivustojen alasajajat korvaavat kalastelusivuston opetusviestillä, joka kouluttaa käyttäjiä tietojenkalastelusta. Vuosien 2010 ja 2012 välisenä aikana opetusviesti oli laitettu 1285 alasajettuun kalastelusivustoon ja sitä oli katsottu lähes 200 000 kertaa. (Hong, 2012.)

Kalastelusivustoja ei kuitenkaan saada vielä tarpeeksi nopeasti ajettua alas. Moore ja Clayton (2007b) huomasivat tutkimuksessaan, että jotkut palveluntarjoajat ovat nopeampia poistamaan kalastelusivustoja kuin toiset. Tästäkin huolimatta sivustot poistetaan liian hitaasti ja niillä ehtii vierailla liikaa käyttäjiä. Riittävän nopealla kalastelusivustojen alasajolla saataisiin vähennettyä tietojenkalastelua merkittävästi. (Moore & Clayton, 2007b.)

3.5 Verkkosivustojen asianmukainen tunnistaminen ja todennus

Erilaisia menetelmiä on kehitetty auttamaan käyttäjiä tunnistamaan sivustot joilla he ovat. On kuitenkin epävarmaa, kuinka paljon näistä on apua käytännössä. Extended Validation (EV) on sertifikaatti yritysten varmentamiseen.

Mentäessä sivustolle, joka on sertifioitu EV:llä, selaimen osoitekenttä muuttuu automaattisesti siten, että siinä näkyy sivuston tuotenimi. (Hong, 2012.)

Jackson, Simon, Tan ja Barth (2007) kuitenkin toteavat tutkimuksessaan EV sertifikaattien olevan tehottomia suojelemaan käyttäjiä tietojenkalastelu-hyökkäyksiltä. He silti uskovat EV:n tulevan tehokkaammaksi ajan saatossa, kun useammat finanssialan sivustot ottavat sen käyttöönsä ja tietoisuus EV:stä lisääntyy (Jackson ym., 2007).

Salainen kuva on useiden finanssialan sivustojen käyttämä tekniikka, jossa käyttäjä valitsee kuvan, joka näytetään hänelle aina sisäänkirjautumisen yhteydessä. Kuvan avulla käyttäjä tietää olevansa oikealla sivustolla. (Hong, 2012.) Salaisesta kuvasta on olemassa useita erilaisia versioita, esimerkiksi Bank of America käyttää SiteKeytä ja Yahoolla on Sign-in Seal (Alsharnouby ym., 2015).

Schechter, Dhamija, Ozment ja Fischer (2007) kuitenkin toteavat tutkimuksessaan, ettei salainen kuva ole kovin tehokas suojautumiskeino. Käyttäjät eivät välttämättä huomaa salaisen kuvan puuttumista kirjautumissivulta. Lisäksi Schechter, Dhamija, Ozment ja Fischer (2007) toteavat, ettei salainen kuva aina takaa turvattua sivustoa. Mies välissä -hyökkäyksissä hyökkääjä on saattanut kaapata salaisen kuvan ja näyttää sen uhrille kirjautumissivulla. Tämän vuoksi käyttäjän on erittäin tärkeää varmistaa, että sivuston osoite on oikea ja HTTPS on aktivoitu. (Schechter ym., 2007.)

3.6 Käyttäjien kouluttaminen

Tietoturvassa käyttäjä nähdään usein heikoimpana lenkkinä, sillä vahvinkin tekninen turvausjärjestelmä voidaan kiertää, jos hyökkääjä manipuloi onnistuneesti käyttäjän antamaan salasanansa, avaamaan epäilyttävän sähköpostin liitteen tai vierailemaan vaarantuneella sivustolla (Heartfield & Loukas, 2016; Khonji ym., 2013). Dhamijan, Tygarin ja Hearstin (2006) tekemän tutkimuksen mukaan 90 % osallistujista luuli hyvin tehtyä kalastelusivustoa luotettavaksi sivustoksi. Tämän lisäksi ongelmana on se, että käyttäjille itselleen turvallisuus on usein vain toissijainen asia. Käyttäjät keskittyvät varsinaisen tehtävän suorittamiseen, kuten ostosten tekemiseen, eivätkä he näin ollen huomaa turvallisuusindikaattoreita. (Alsharnouby ym., 2015.)

Tästä huolimatta käyttäjien kouluttaminen nähdään yhtenä vähiten suosittuna suojautumiskeinona, sillä käyttäjiä voi olla haastavaa motivoida kiinnostumaan tietoturvasta ja lisäksi käyttäjien kouluttaminen ei takaa täysin varmaa suojaa tietojenkalastelulta. Tänä päivänä mikään suojautumiskeino ei kuitenkaan takaa täysin pitävää suojautumiskeinoa. (Hong, 2012.) Tämän vuoksi käyttäjien kouluttaminen olisi ensisijaisen tärkeää.

Yhtenä tapana kouluttaa käyttäjiä ovat erilaiset mikropelit, jotka on suunniteltu opettamaan käyttäjiä tietojenkalastelusta. Sheng ym. (2007) ovat kehittäneet pelin nimeltä Anti-Phishing Phil, joka opettaa selaimen osoiteriveistä, verkkotunnuksista ja kalastelusivustoista. Tämän jälkeen peli testaa, mitä käyttäjät ovat oppineet. Tutkimuksessaan Sheng ym. (2007) huomasivat, että käyttä-

jät, jotka olivat pelanneet peliä, tunnistivat paremmin petolliset sivustot kuin henkilöt, jotka eivät olleet pelanneet peliä. Näin ollen pelejä voidaan pitää tehokkaana tapana kouluttaa käyttäjiä tietojenkalastelusta ja tietoturvasta. (Sheng ym., 2007.)

Toinen tapa kouluttaa käyttäjiä on sulautettu kouluttaminen, jossa opetusmateriaalit on integroitu ensisijaisiin tehtäviin, joita käyttäjät toteuttavat jokapäiväisessä elämässään. Tietojenkalastelu on yleisimmin toteutettu joko sähköpostin tai verkkosivustojen avulla, jolloin sulautettu kouluttaminen voidaan toteuttaa jompaakumpaa näistä hyödyntämällä. Kumaraguru, Sheng, Acquisti, Cranor ja Hong (2010) ovat kehittäneet sulautettua kouluttamista hyödyntävän PhishGurun, joka kouluttaa käyttäjiä tietojenkalastelusta samalla, kun he käyttävät normaalisti sähköpostiaan. PhishGuru toimii siten, että se lähettää käyttäjille määräajoin sähköpostiviestejä, jotka muistuttavat kalasteluviestejä. Jos käyttäjä menee lankaan ja klikkaa sähköpostissa olevaa linkkiä, hänelle näytetään viesti, joka kertoo hänen olevan vaarassa joutua kalasteluhyökkäyksen uhriksi. Tämän lisäksi viesti sisältää vinkkejä, joilla voi turvata itsensä tietojenkalastelulta. (Kumaraguru ym., 2010.)

Suurin osa tämän tutkielman esittelemistä suojautumiskeinoista eivät ole täysin varmoja, vaan käyttäjä voi itse mahdollistaa tietojenkalasteluhyökkäyksen, vaikka käytössä olisin erilaisia teknisiä suojautumiskeinoja. Tämän vuoksi on äärimmäisen tärkeää, että käyttäjät itse pystyvät aktiivisesti tarkkailemaan mahdollisia merkkejä tietojenkalastelusta, eivätkä vain luota teknisiin suojautumiskeinoihin. Tässä asiassa käyttäjien kouluttaminen nousee tärkeimmäksi tekijäksi. Käyttäjien kouluttamisella ja tietoisuuden lisäämisellä saadaan ihmiset suojattua paremmin kalasteluhyökkäyksiltä, kuin pelkillä teknisillä suojautumiskeinoilla.

Tämän lisäksi kalasteluhyökkäysten jatkuva kehittyminen aiheuttaa sen, ettei teknisiä suojautumiskeinoja ehditä kehittämään tarpeeksi nopeaksi (Sheng ym., 2009; Bergholz ym., 2010). Erityisesti uudenlaisia hyökkäyksiä vastaan ei ole teknisiä suojautumiskeinoja, jolloin ainoa suojautumiskeino on käyttäjän oma toiminta. Näin ollen käyttäjien kouluttaminen on ensisijaisen tärkeää tietojenkalastelun torjunnassa.

4 YHTEENVETO

Tutkielman tavoitteena oli selvittää erilaisia tietojenkalastelutapoja sekä mahdollisia suojautumiskeinoja niitä vastaan. Uusia tietojenkalastelutapoja kehitetään kuitenkin koko ajan lisää, minkä lisäksi monet tietojenkalasteluhyökkäykset voivat sisältää elementtejä eri kalastelutavoista. Näin ollen tietojenkalasteluhyökkäyksiä voi olla vaikeaa määritellä tietynlaiseksi kalasteluhyökkäykseksi. Kun erilaisia hyökkäyksiä tulee koko ajan lisää, kehitetään myös uusia suojautumiskeinoja niitä vastaan. Tässä tutkielmassa on pyritty esittelemään yleisimpiä kalasteluhyökkäyksiä ja erilaisia suojautumiskeinoja mahdollisimman monipuolisesti.

Tietojenkalasteluhyökkäykset ovat usein sosioteknisiä hyökkäyksiä, jotka sisältävät sekä käyttäjän manipulointia että teknisiä kalastelutapoja. Näiden lisäksi on olemassa myös täysin teknisiä kalasteluhyökkäyksiä, jotka eivät sisällä käyttäjän manipulointia. Kun normaalissa tietojenkalasteluhyökkäyksessä käyttäjä yritetään huijata esimerkiksi houkuttelun tai vakuuttelun avulla luovuttamaan henkilökohtaisia tietojaan tai asentamaan haittaohjelma koneelleen, keskittyvät tekniset kalasteluhyökkäykset esimerkiksi käyttäjien tietokoneisiin tai internetyhteyksiin.

Erilaisia tietojenkalastelun tapoja ovat esimerkiksi linkkien manipulointi, paha kaksonen -hyökkäys ja mies välissä -hyökkäys. Tietojenkalastelun tarkoituksena on saada käyttäjät luovuttamaan henkilökohtaisia tietoja, kuten luottokorttitietoja, tai saada heidät asentamaan haittaohjelma koneelleen. Yleensä hakkereiden tarkoituksena on levittää hyökkäystä mahdollisimman laajalle ja saada paljon uhreja.

Tämän lisäksi on olemassa myös tiettyyn henkilöön tai ryhmään kohdistuvaa tietojenkalastelua, jota kutsutaan nimellä keihäsmäinen tietojenkalastelu. Siinä uhrista haetaan ennakkoon mahdollisimman paljon tietoa esimerkiksi sosiaalisen median avulla, jonka jälkeen luodaan mahdollisimman luotettavan näköinen sähköpostiviesti. Keihäsmäisen tietojenkalastelun yksi muoto on whaling, jossa uhreiksi valitaan korkean luokan henkilöitä, kuten yritysjohtajia. Keihäsmäinen tietojenkalastelu ja whaling altistavat erityisesti yritykset suurille tappioille.

Tietojenkalastelun sosioteknisen luonteen vuoksi tehokas suojautuminen vaatii sekä sosiaalisen että teknisen puolen huomioimista. Yhtä luodinkestävää suojautumiskeinoa ei ole vielä onnistuttu keksimään, minkä vuoksi useita suojautumiskeinoja käytetään usein yhtä aikaa. Esimerkkejä erilaisista suojautumiskeinoista ovat varoitukset, kalasteluviestien suodattaminen ja verkkosivustojen asianmukainen tunnistaminen ja todennus. Tekniset suojautumiskeinot pyrkivät joko estämään käyttäjän pääsyn kalastelusivustolle tai ne varoittavat käyttäjää kalastelusivustosta.

Erityisen ongelman tehokkaan suojautumiskeinon kehittämiselle asettaa käyttäjä, joka nähdään usein heikoimpana lenkkinä tietoturvan kannalta. Vahvinkin tekninen suojausmenetelmä voidaan kiertää, jos hyökkääjä onnistuu manipuloimaan käyttäjän antamaan haluttuja tietoja. Näin ollen yhtenä tärkeimpänä suojautumiskeinona tietojenkalastelua vastaan nähdään käyttäjien kouluttaminen. Käyttäjien kouluttaminen on siitäkin syystä erityisen tärkeää, etteivät tekniset suojauskeinot ole täysin varmoja. Liika luottaminen teknisten suojautumiskeinojen toimintaan saattaa altistaa kalasteluhyökkäykselle.

Tällä hetkellä käyttäjiä ei kuitenkaan kouluteta vielä tarpeeksi varomaan tietojenkalastelua. Tulevaisuudessa olisikin syytä keskittyä lisäämään käyttäjien tietoutta erilaisten kalastelutapojen tunnistamisesta ja niiltä suojautumisesta. Erityisesti organisaatiot ja yritykset ovat vaarassa menettää kilpailuasemansa ja kohdata suuria tappioita, jos työntekijät suostuvat antamaan salaista tietoa yrityksestä hakkerille. Yritysten olisikin syytä harkita työntekijöiden kouluttamista tietojenkalastelusta.

Käyttäjien kouluttamista varten on kehitetty erilaisia pelejä, jotka kertovat tietojenkalastelusta ja opettavat tunnistamaan kalasteluhyökkäyksiä. Yhtenä esimerkkinä toimivat mikropelit kuten Anti-Phishing Phil. Toisena tapana on sulautettu kouluttaminen, missä opettaminen tapahtuu esimerkiksi sähköpostia käytettäessä.

Tietojenkalastelu on jatkuvasti kasvava ongelma, mitä osaltaan pahentaa yhä useampien laitteiden siirtyminen internetiin. Esineiden internetin myötä myös normaalit kodinkoneet ovat alttiita erilaisille tietoturvahyökkäyksille. Yksi esimerkki esineiden internetin aiheuttamasta tietoturvauhkasta on internetiin liitettyjen kameroiden katselu salaa samoin kuin mikrofonien salakuuntelu. Ongelmaa pahentaa entisestään se, ettei monissa kodinkoneissa ole juuri minkäänlaista tietoturvaa, minkä lisäksi käyttäjät eivät ole tarpeeksi tietoisia mahdollisista uhkista. Yksi yleinen virhe minkä käyttäjät tekevät, on saman salasanan käyttö useissa internetiin kytketyissä laitteissa, jolloin hakkerin on helppo päästä käsiksi kaikkiin kodin laitteisiin.

Myös tietojenkalastelu voi levitä esineiden internetiin tulevaisuudessa. Hakkerit kehittävät kokoajan uusia keinoja varastaa ihmisten henkilökohtaisia tietoja, joten on vain ajan kysymys, milloin ensimmäiset tietojenkalasteluhyökkäykset tapahtuvat esineiden internetiä hyödyntäen.

Erilaisia tietojenkalastelutapoja on todella paljon, eikä tässä tutkielmassa ole käsitelty kaikkia. Tämän lisäksi myös erilaisia suojautumiskeinoja kehitetään kokoajan lisää. Näin ollen aiheesta löytyisi vielä paljon lisää tutkittavaa.

Jatkotutkimuksissa voisi tutkia sitä, miksi käyttäjät lankeavat tietojenkalasteluun ja millaisilla toimilla tämä voitaisiin estää. Lisäksi mielenkiintoinen tutkimusaihe olisi esineiden internetin avulla tapahtuva tietojenkalastelu. Kaiken kaikkiaan tietojenkalastelu on hyvin laaja ilmiö, mikä ei ole häviämässä minnekään. Näin ollen tutkittavaa löytyy varmasti vielä paljon.

LÄHTEET

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Bergholz, A., De Beer, J., Glahn, S., Moens, M. F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of computer security*, *18*(1), 7-35.

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy*, *7*(1), 78-81.

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.

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

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. Teoksessa *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (s. 1065-1074). ACM.

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

He, D., Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. *IEEE Wireless Communications*, *22*(1), 138–144.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, *48*(3), 37.

Herzberg, A., & Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology (TOIT)*, *8*(4), 16.

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

Huang, L. S., Moshchuk, A., Wang, H. J., Schecter, S., & Jackson, C. (2012). Clickjacking: attacks and defenses. Teoksessa *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)* (s. 413-428).

Jackson, C., Simon, D. R., Tan, D. S., & Barth, A. (2007). An evaluation of extended validation and picture-in-picture phishing attacks. Teoksessa *International Conference on Financial Cryptography and Data Security* (s. 281-293). Springer Berlin Heidelberg.

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *Communications Surveys & Tutorials, IEEE*, *15*(4), 2091–2121.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113–122.

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.

Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. Teoksessa *Proceedings of the 3rd ACM workshop on Wireless security* (s. 90-97). ACM.

Moore, T., & Clayton, R. (2007a). An Empirical Analysis of the Current State of Phishing Attack and Defence. Teoksessa *WEIS*.

Moore, T., & Clayton, R. (2007b). Examining the impact of website take-down on phishing. Teoksessa *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (s. 1-13). ACM.

Nirmal, K., Janet, B., & Kumar, R. (2015, February). Phishing-the threat that still exists. Teoksessa *Computing and Communications Technologies (ICCCT), 2015 International Conference on* (s. 139–143). IEEE.

Rehman, U. U., Khan, W. A., Saqib, N. A., & Kaleem, M. (2013). On detection and prevention of clickjacking attack for osns. Teoksessa *Frontiers of Information Technology (FIT), 2013 11th International Conference on* (s. 160-165). IEEE.

Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). The emperor's new security indicators. Teoksessa *2007 IEEE Symposium on Security and Privacy (SP'07)* (s. 51-65). IEEE.

Shahriar, H., & Haddad, H. (2015). Security assessment of clickjacking risks in web applications: metrics based approach. Teoksessa *Proceedings of the 30th Annual ACM Symposium on Applied Computing* (s. 791-797). 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* (s. 88-99). ACM.

Sheng, S., Wardman, B., Warner, G., Cranor, L. F., Hong, J., & Zhang, C. (2009). An empirical analysis of phishing blacklists. Teoksessa *Proceedings of Sixth Conference on Email and Anti-Spam (CEAS)*.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164.

Song, Y., Yang, C., & Gu, G. (2010). Who is peeping at your passwords at Starbucks?-To catch an evil twin access point. Teoksessa *DSN* (Vol. 10, s. 323-332).

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. Teoksessa *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 3, s. 648-651). IEEE.

Thornburgh, T. (2004). Social engineering: the dark art. Teoksessa *Proceedings of the 1st annual conference on Information security curriculum development* (s. 133-135). ACM.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*.

Zhao, M., An, B., & Kiekintveld, C. (2016). Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks. Teoksessa *Proceedings of the 30th AAAI Conference on Artificial Intelligence (AAAI)*.