Joonas Hellsten

VERKKOHUIJAUSTEN TYYPIT SOSIAALISESSA MEDIASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Hellsten, Joonas
Verkkohuijausten tyypit sosiaalisessa mediassa
Jyväskylä: Jyväskylän yliopisto, 2017, 24 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Luoma, Eetu

Tutkielmassa tutkitaan verkkohuijausten tyyppejä sosiaalisessa mediassa määritellen ensin verkkohuijaukset ja sitten soveltaen periaatteita sosiaalisen median kontekstiin. Tutkielma on toteutettu kirjallisuuskatsauksena. Siinä havaitaan, että sosiaalisessa mediassa esiintyy saman tyyppisiä huijauksia, kuin sen ulkopuolellakin. Tällaisia huijauksia ovat muun muassa tietojenkalasteluhuijaukset, sosiaalisen suostuttelun avulla levitettäviin haittaohjelmiin liittyvät huijaukset, sekä 419 -huijaukset. Muutamia huijaustyyppejä ei havaittu esiintyvän sosiaalisen median kontekstin ulkopuolella, sillä ne vaativat sosiaalisen verkostoitumissivun alustakseen. Nämä huijaustyypit liittyvät julkisuuden henkilönä tai huijauksen uhrin ystävänä esiintymiseen valeprofiilien avulla, palveluihin, jotka tarjoavat seuraajia käyttäjän profiilille, sekä sosiaalisten verkostoitumissivujen haitallisiin liitännäissovelluksiin.

Asiasanat: verkkohuijaus, sosiaalinen media, sosiaalinen verkostoitumissivu, tietojenkalastelu, haittaohjelma

ABSTRACT

Hellsten, Joonas
Types of online scams in social media
Jyväskylä: University of Jyväskylä, 2017, 24 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Luoma, Eetu

In this thesis, types of online scams in social media are examined first by defining online scams and then applying the principles of them to social media setting. The thesis is a literature review in which it was found that in social media there are similar types of scams than outside of it. These types of scams were phishing scams, scams related to social engineering malware attacks and 419 -scams. There were a couple of scam scenarios that were not detected outside of social media context due to social networking site required as a platform for the scams. These were scams involving impersonation of celebrities or friends, services offering followers for the user's profile and malicious applications and widgets inside social networking sites.

Keywords: online scam, social media, social networking site, phishing, malware

KUVIOT

KUVIO 1 Esimerkki tietojenkalasteluviestistä..... 10

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT

1 JOHDANTO ... 6

2 VERKKOHUIJAUKSET ... 9
2.1 Roskaposti ja haitalliset huijauskeinot ... 9
2.2 Verkkohuijausten toteutukset ... 11
2.3 Länsi-Afrikan huijaukset ... 12
2.4 Yhteenveto ... 13

3 SOSIAALINEN MEDIA JA VERKKOHUIJAUKSET ... 15
3.1 Sosiaalisen median määritelmät ... 15
3.2 Verkkohuijaukset sosiaalisilla verkostoitumissivuilla ... 17
3.2.1 Roskaposti ja haitalliset huijauskeinot ... 17
3.2.2 Klikkausten kaappaus ... 18
3.2.3 419 –huijaukset ... 19
3.2.4 Toisena käyttäjänä esiintyminen ja tiedon väärinkäyttö ... 19
3.3 Yhteenveto ... 19

4 YHTEENVETO ... 21

LÄHTEET ... 23

1 JOHDANTO

Internet on lyhyessä ajassa kasvanut vahvaksi ihmisten väliseksi kommunikointikanavaksi ja sen nopeus, halpuus ja käyttäjien nimettömyys ovat mahdollistaneet, että huijaustoimintaa on helppo harjoittaa verkossa (Baker, 1999). Tambe Ebotin ja Siposen (2014) mukaan verkkohuijaamisella (engl. internet fraud, online scam) tarkoitetaan toimintaa, jolla pyritään huijaamaan internetin käyttäjiä tietokoneiden mahdollistamia kanavia, kuten esimerkiksi sähköpostia, chat -huoneita ja sosiaalista mediaa käyttämällä.

Monia huijauksia on toteutettu myös ennen internetin -aikakauden alkua muun muassa kirjeiden (Baker, 1999; Whitty & Buchanan 2012), sekä puhelinsoittojen välityksellä (Baker, 1999). Esimerkiksi rahahuijaukset, joissa uhreilta huijataan rahaa käyttämällä romanttisia suhteita apuvälineenä, perustuvat samanlaisiin kirjeiden välityksillä tehtäviin huijauksiin (Whitty & Buchanan, 2012). Myös esimerkiksi kyseenalaisiin sijoitus- ja liiketoimintamahdollisuuksiin liittyviä huijauksia ja pyramidihuijauksia on toteutettu jo ennen internetin aikakautta (Baker, 1999; Grazioli & Järvenpää, 2000).

Internet on kuitenkin mahdollistanut sellaisten uusien huijaustapojen syntymistä, joita on ollut aikaisemmin käytännössä mahdotonta toteuttaa. Esimerkiksi verkkosivun kaappaustekniikkassa (engl. page jacking) internet -käyttäjä uudelleenohjataan huijaussivustolle, joka näyttää erehdyttävästi sivustolta, jolla käyttäjän oli alun perin tarkoitus vierailla. Verkkosivun kaappauksen myötä käyttäjä saattaa tulla syöttäneeksi esimerkiksi verkkopankkitilinsä tiedot oikeaa verkkopankin kirjautumissivua muistuttavalle huijaussivustolle, eikä välttämättä edes tiedä tulleensa huijatuksi. (Grazioli & Järvenpää, 2000).

Verkkohuijauksia käsiteltiin tässä kirjallisuuskatsauksessa sosiaalisen median (engl. social media) näkökulmasta. Kaplanin ja Haenleinin (2010) mukaan sosiaalisella medialla tarkoitetaan Web 2.0 -pohjaisia verkkosovelluksia, joiden avulla välitetään käyttäjien luomaa sisältöä (engl. user-generated content). Web 2.0 -käsitteellä Kaplan ja Haenlein (2010) tarkoittavat uutta verkon käyttötapaa, jossa verkon käyttäjät eivät enää luo yksilöinä web -sisältöä, vaan ovat sen sijaan osallisina sisällön jatkuvassa kehityksessä yhteistyössä kaikkien muiden verkon käyttäjien kanssa.

Kaplanin ja Haenleinin (2010) mukaan Vickery ja Wunsch-Vincent (2007) tarkoittavat käyttäjien luomalla sisällöllä sellaista sisältöä, joka täyttää kolme kriteeriä: Sisällössä tulee näkyä luovia piirteitä, esimerkiksi kommentointi-, tai muokkausmahdollisuuksia ja sisällön ei tule kuulua ammatillisessa tarkoituksessa suoritettaviin toimintoihin, kuten esimerkiksi markkinointiin kaupallisessa mielessä. Sisällön tulee myös olla saatavilla kaikille ihmisille julkisella verkkosivulla, tai tietylle ihmisryhmälle sosiaalisella verkostoitumissivulla (engl. social networking site). Sosiaalisella verkostoitumissivulla tarkoitetaan web -sovellusta, johon voi tehdä profiilin, luoda yhteyksiä muihin käyttäjiin, sekä tutkia omia ja muiden käyttäjien yhteyksiä (Ellison, 2007). Yhteydet muihin käyttäjiin voivat olla esimerkiksi verkon ulkopuolisesta ystävyydestä johtuvia tai vain verkkotuttavuuksien välisiä yhteyksiä. Käyttäjät kommunikoivat sosiaalisilla verkostoitumissivuilla muun muassa tilapäivitysten, viestien, kommenttien ja median jakamisen avulla. (Gundecha & Liu, 2012).

Verkkohuijausten tyyppejä sosiaalisessa mediassa on tärkeä tutkia: Internet on kasvamassa osaksi arkipäivää (Vickery & Wunsch-Vincent, 2007) ja kasvu on aiheuttanut myös verkossa tapahtuvien petollisten toimintatapojen lisääntymistä (Baker, 1999). Sosiaalinen media on tullut osaksi ihmisten jokapäiväistä elämää ja tarjoaa uusia hyökkäysmahdollisuuksia rikollisille. Sosiaalisilla verkostoitumissivuilla jaetaan paljon henkilökohtaisia tietoja, joita voidaan käyttää huijausten kohdentamiseen (Jagatic ym., 2007; Wüest, 2010). Tietoa ja esimerkkejä huijauksien tyypeistä tarvitsevat erityisesti vanhemmat verkon käyttäjät, sillä Chakrabortyn ja muiden (2013) mukaan seniorit ovat omaksumassa sosiaalista mediaa käyttöönsä nopeasti ja ovat suojattomin ikäryhmä tietoturvan ja yksityisyyden kannalta.

Verkkohuijauksia ja sen tyyppejä käsittelevää kirjallisuutta on olemassa, mutta kirjallisuus, joka kokoaisi verkkohuijausten tyypit sosiaalista mediaa näkökulmana näyttäen, on vähäistä. Verkkohuijausten tyyppejä tutkimalla voitaisiin avata uusia tutkimusmahdollisuuksia liittyen muun muassa huijausten tiedostamiseen ja ehkäisyyn. Tietoisuuden lisäämisen tärkeyden lisäksi on mielenkiintoista tutkia, onko sosiaalisessa mediassa tapahtuvissa huijausten tyypeissä eroa verrattuna sosiaalisen median ulkopuolisiin verkkohuijauksiin. Tutkielmassa halutaankin vastata seuraavaan tutkimuskysymykseen: Minkä tyyppisiä verkkohuijauksia sosiaalisessa mediassa tapahtuu ja ovatko huijaukset erityyppisiä sosiaalisessa mediassa, kuin sen ulkopuolella?

Tutkielma toteutettiin kirjallisuuskatsauksena, jossa sovellettiin Okolin ja Schabramin (2010) systemaattisen tietojärjestelmätieteen kirjallisuuskatsauksen ohjetta. Kun kirjallisuuskatsauksen tarkoitus oli mietitty, alettiin kerätä artikkeleita verkkohuijauksiin ja sosiaaliseen mediaan liittyen. Artikkeleita haettiin digitaalisten kirjastojen ja julkaisuarkistojen julkaisuja tutkimalla muun muassa AIS Electronic Library (AISEL), Google Scholar ja ACM Digital Library -palveluista. Hakutermeinä käytettiin muun muassa seuraavia: ”social media”, ”internet/online scam/fraud”, sekä ”social media scam”. Haettuihin artikkeleihin tehdyn pienen perehtymisen jälkeen karsittiin pois ne, jotka eivät liity tämän kirjallisuuskatsauksen aihepiiriin, muun muassa yksinomaan yritysten näkökulmasta

sosiaalista mediaa käsittelevät artikkelit. Karsinnan jälkeen kirjallisuuskatsaukseen valittiin mukaan esimerkiksi verkkohuijaukset ja sosiaalisen median määritteleviä tieteellisiä julkaisuja, sekä julkaisuja, joissa nämä käsitteet esiintyvät eri näkökulmista. Mukaan otettiin myös muita verkosta löytyviä artikkeleita. Mukaan otettiin esimerkiksi uutisia, joita on käytetty muun muassa havainnollistamisessa, sekä otettiin lähteinä esiintyviä artikkeleita.

Verkkohuijaukset määriteltiin tarkoittamaan mitä tahansa internetin mahdollistamaa toimintaa, jonka tarkoituksena on verkkokäyttäjien huijaaminen (Tambe Ebot & Siponen, 2014). Täten kirjallisuuskatsauksessa voidaan paneutua monimuotoisesti erityyppisiin huijauksiin, kuten esimerkiksi haittaohjelmien levittämiseen sosiaalisen suostuttelun avulla, tietojenkalasteluhuijauksiin, sekä 419 -huijauksiin. Tarkastelussa keskityttiin erityisesti huijausten tyyppeihin ja niiden esittelyyn, eikä esimerkiksi huijaamiselta suojautumiseen. Sosiaalisen median näkökulmasta tarkastelu rajattiin koskemaan pääosin sosiaalisia verkostoitumissivuja, kuten esimerkiksi Facebookia ja Twitteriä.

Ensimmäisessä varsinaisessa sisältöluvussa käsitellään verkkohuijauksia yleisellä tasolla ja tarkastellaan, minkä tyyppisiä huijauksia verkossa on. Toisessa luvussa käsitellään sosiaalista mediaa ja erityisesti sosiaalisia verkostoitumissivuja yleisesti, sovelletaan verkkohuijausten tyyppejä sosiaaliseen mediaan ja tutkitaan sosiaalista mediaa verkkohuijauksien alustana. Lisäksi luvussa vertaillaan sosiaaliseen mediaan kuuluvia verkkohuijaustyyppejä sosiaalisen median ulkopuolisiin, kuten esimerkiksi sähköpostin välityksellä, tapahtuviin huijaustyyppeihin. Lopuksi esitellään johtopäätökset -osio, jossa käydään läpi kirjallisuuskatsauksen menetelmät, tavoitteet, havainnot ja johtopäätökset, kerrataan vastaus tutkimuskysymykseen, sekä esitetään tulevaisuuden näkökulmat aiheen tutkimiselle.

2 VERKKOHUIJAUKSET

Jotta verkkohuijauksia voidaan tarkastella sosiaalisen median näkökulmasta, tulee ensiksi tutkia, mitä verkkohuijauksista on yleisesti kirjoitettu informaatioteknologian alan kirjallisuudessa. Tässä luvussa määritellään käsitteitä, joita liitetään läheisesti verkkohuijauksiin, sekä esitellään kirjallisuuden avulla verkkohuijausten trendejä tutustuen muun muassa verkkohuijauksiin liittyviin teknologioihin. Lisäksi tutustutaan jonkin verran siihen, mitä aiheita verkkohuijaukset yleensä koskevat ja erikoistapauksena tutustutaan Länsi-Afrikan huijaustyyppeihin.

2.1 Roskaposti ja haitalliset huijauskeinot

Ensimmäinen tärkeä käsitepari verkkohuijauksiin liittyen on roskaposti ja sen lähettäminen (engl. spam). Tällä tarkoitetaan suurille ihmisjoukoille pyytämättä lähetettyjä viestejä, joiden tarkoitus on usein houkutella vastaanottajiaan osallistumaan kaupalliseen toimintaan, muun muassa lääkkeiden tai teknologisten hyödykkeiden, esimerkiksi ohjelmistojen, tilaamiseen. Myös haitallisia huijauskeinoja, esimerkiksi tietojenkalastelua ja haittaohjelmien levitystä toteutetaan roskapostiviestien välityksellä. (Anderson ym., 2007).

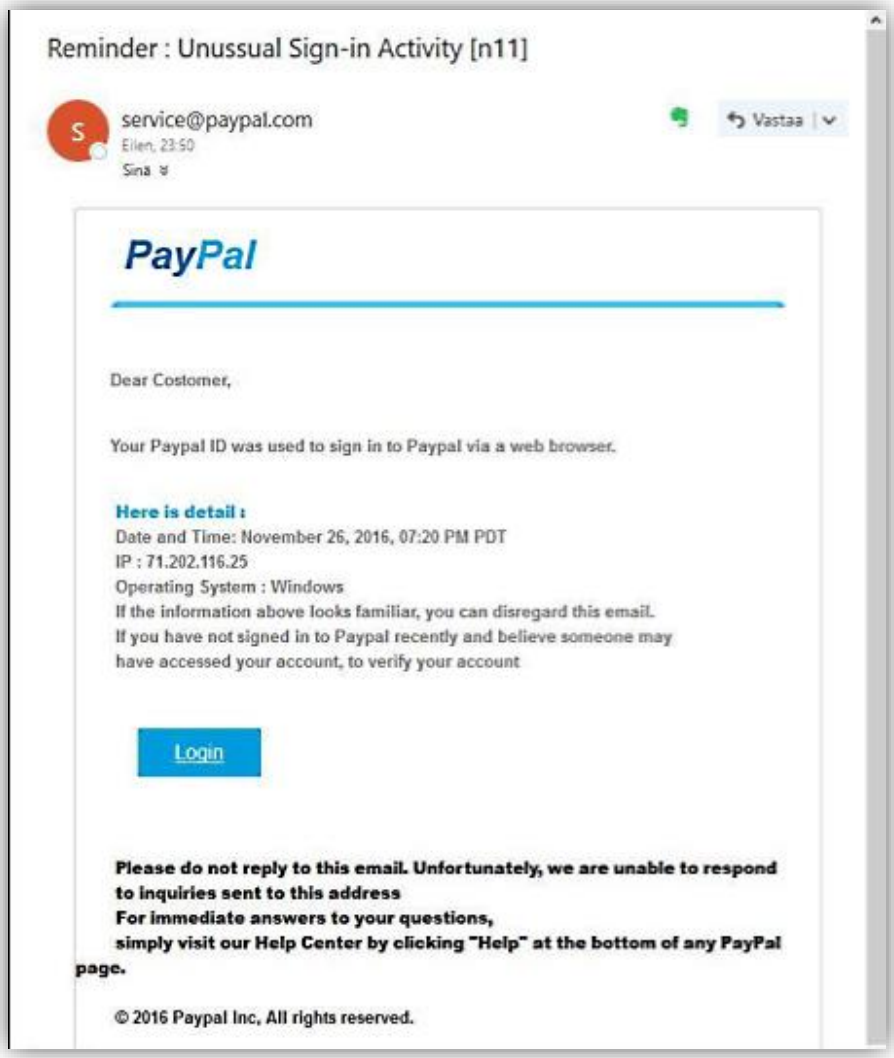
Jagaticin ja muiden (2007) mukaan tietojenkalastelulla (engl. phishing) tarkoitetaan huijaustyyppiä, jossa huijarit esiintyvät valheellisesti jonain luotettavana toimijana ja pyrkivät siten keräämään arkaluontoista tietoa huijauksen uhreilta. Huijarit voivat esiintyä muun muassa pankkialan toimijoina: esimerkiksi Osuuspankki on julkaissut tiedotteissaan esimerkkejä tietojenkalastelusivuista ja huijaussähköposteista, joilla pyritään urkkimaan pankin asiakkaiden henkilö- ja pankkitunnuksia[1]. Huijari voi myös esiintyä henkilönä, jonka tietojenkalasteluviestin vastaanottaja tuntee: tällöin on jopa nelinkertaisesti todennäköisempää, että vastaanottajan huijaaminen onnistuu. Huijarit voivat esimerkiksi selvittää uhrin tuttavapiiristä julkisesti saatavilla olevaa tietoa muun muassa sosiaalisten verkostoitumissivujen avulla. (Jagatic ym., 2007).

Andersonin ja muiden (2007) mukaan toinen esimerkki haitallisista huijauskeinoista tietojenkalastelun lisäksi on haittaohjelmien (engl. malware) levittäminen sosiaalisen suostuttelun avulla (engl. social engineering). Abrahamin ja Chengalur-Smithin mukaan Erbschloe (2004) on todennut, että sosiaalisella suostuttelulla tarkoitetaan sitä, että huijarit pyrkivät manipuloimaan uhriaan psykologisia keinoja, muun muassa uhrin tunteita, hyväksikäyttämällä. Pyrkimyksenä on saada uhri avustamaan huijareita järjestelmiin ja verkkoihin tunkeutumisessa

1 https://www.op.fi/op/henkiloasiakkaat/tietoturva/opn-asiakkaiden-tietojenkalastelu-aktiivista---huijarit-kayttavat-myos-puhelinta?cid=151881773&srcpl=3

ja väärinkäytössä. Organisaatioiden suurin tietoturvahaavoittuvuus piilee tietokoneita käyttävissä työntekijöissä (Erbschloe, 2004; Abraham & Chengalur-Smith, 2010).

Abrahamin ja Chengalur-Smithin (2010) mukaan sosiaalisessa suostuttelussa uhrissa voidaan esimerkiksi pyrkiä herättämään kiinnostusta, jännitystä, empatiaa, pelkoa, tai ahneutta. Esimerkiksi pelon tunne voidaan saavuttaa esittämällä käyttäjälle tekaistuja varoitusviestejä tietoturvasta ja uskotellaan käyttäjä asentamaan tietoturvapäivitys, joka onkin oikeasti haittaohjelma. Kiinnostuksen tunteeseen vetoaminen taas käy ilmi alla olevasta huijausviestistä, jossa väitetään käyttäjän Paypal –verkkomaksutilille tulleen kirjautumisia tuntemattomasta osoitteesta ja kehotetaan käyttäjää varmentamaan tilinsä linkkiä klikkaamalla (kuvio 1). Linkin klikkaaminen vie käyttäjän huijaussivustolle, joka muistuttaa oikeaa Paypal –sivuston kirjautumissivua. Käyttäjien ahneutta voidaan Abrahamin ja Chengalur-Smithin (2010) mukaan hyväksikäyttää tarjoamalla käyttäjille ilmaista tavaraa, muun muassa alennuskuponkeja. Tällöin linkkien klikkaaminen tai sähköpostiliitteiden avaaminen johtaa kuitenkin haittaohjelmien asentumiseen tai henkilökohtaisten tietojen vaarantumiseen.



KUVIO 1 Esimerkki tietojenkalasteluviestistä

Sosiaaliseen suostuttelun liittyviä hyökkäyksiä voidaan myös kohdentaa koskemaan esimerkiksi opiskelijoita keräämällä heidän sähköpostiosoitteitaan sosiaalisilta verkostoitumissivuilta tai chat -huoneista, tai arvaamalla osoitteet, mikäli ne perustuvat etu -ja sukunimiin. Tällä tavoin viestit voidaan saada näyttämään, että ne tulevat luotettavista lähteistä (Abraham & Chengalur-Smith, 2010; Jagatic ym., 2007) ja kuten edellä mainittiin, tällöin huijaus onnistuu todennäköisemmin (Jagatic ym., 2007).

Sosiaalisen suostuttelun avulla levitettävien haittaohjelmien tulee huijata käyttäjä suorittamaan haittaohjelma avaamalla haitallinen web -linkki tai sähköpostin liitetiedosto, jonka lisäksi haittaohjelman tulee läpäistä tekniset suojauskeinot, kuten esimerkiksi virustorjuntaohjelmat, aktivoituakseen. Haittaohjelmat voivat asentumisen onnistuessa muun muassa muokata laitteiden tietoturva-asetuksia, varastaa laitteeseen tallennettuja salasanoja, vakoilla verkkopankkitapahtumia, asentaa laitteeseen etähallintamahdollisuuksia hyökkääjille, sekä esimerkiksi asentaa laitteen verkkoselaimen uudelleenohjaamaan käyttäjänsä haitallisille verkkosivuille. Jälkimmäisestä esimerkkinä on edellä mainittu verkkosivun kaappaustekniikka (Grazioli & Järvenpää, 2000). Lisäksi haittaohjelmat yleensä leviävät muun muassa kopioimalla itseään laitteen verkkolevyille ja USB -muistitikuille, sekä sähköpostitse haittaohjelman suorittaneen käyttäjän sähköpostikontakteille. (Abraham & Chengalur-Smith, 2010).

Vaikka haittaohjelmat voivat asentua myös ilman käyttäjän minkäänlaisia toimenpiteitä hyväksikäyttämällä haavoittuvuuksia (engl. exploits), sosiaalinen suostuttelu on silti yksi suurimpia välineitä, joilla haittaohjelmia toimitetaan. Lisäksi monesti haavoittuvuuksien avulla tarttuvienkin haittaohjelmien mahdolliset uhrit tulee sosiaalisen suostuttelun keinoin saada ensin siirtymään verkkosivuille, joissa näitä haavoittuvuuksia on hyväksikäytetty (Raman, 2008).

2.2 Verkkohuijausten toteutukset

Verkkohuijaukset erottuvat tavallisista huijauksista siten, että ne ovat internetin kanavien mahdollistamia (Tambe Ebot & Siponen, 2014): verkkohuijausten toteutukseen käytetään esimerkiksi jo edellä mainittua roskapostia ja online –ilmoitustauluja (Tambe Ebot & Siponen, 2014; Baker, 1999). Lisäksi huijauksien kanavina käytetään myös sosiaalista mediaa (Tambe Ebot & Siponen, 2014), sekä verkossa sijaitsevia sijoituslehtiä (Baker, 1999). Huijauksien infrastruktuuria on tutkittu Andersonin ja muiden (2007) tekemässä tutkimuksessa roskapostiviesteistä kerätyillä tiedoilla, joilla pystyttiin mittaamaan muun muassa huijauskampanjoiden kestoja ja huijausta isännöivien, sekä huijausviestejä välittävien palvelinten sijainteja maapallolla. Lisäksi web -huijaussivujen, joita tutkittiin roskapostiviestien linkkejä seuraamalla, kuvankaappauksia keräämällä ja vertailemalla voitiin arvioida huijausten yhtäläisyyttä.

Andersonin ja muut (2007) analysoivat tutkimuksensa tuloksia aluksi luokittelemalla roskapostiviestien takana olevat huijaukset (noin 2300 uniikkia kappaletta) kategorioihin. Huijausten luokittelu oli heidän mukaansa vaikeaa, sillä luokitteluvaiheessa moniin huijaussivustojen osoitteisiin ei saanut enää yhteyttä ja toisaalta moni huijaus sisälsi dynaamista sisältöä, eikä siten sisältynyt mihinkään kategoriaan. Suurin osa Andersonin ja muiden (2007) tutkimuksessa tutkituista huijauksista, noin 29,6 %, olikin ei-kategorioituvia. Seuraavaksi suurin huijauskategoria tutkimuksessa (noin 16,7 % huijauksista) olivat informaatioteknologiaan liittyvät huijaukset, joihin kuuluvat muun muassa tarjoukset ilmaisista tai alennettuun hintaan myytävistä hyödykkeistä, esimerkiksi ohjelmistoista. Muita tutkimuksessa havaittuja huijauksia olivat muun muassa huijaukset liittyen kelloihin ja lääkkeisiin.

Anderson ja muut (2007) tutkivat myös huijausten isäntäpalvelimien sijainteja maapallolla ja tuloksena saatiin, että yli puolet isäntäpalvelimista sijaitsi Yhdysvalloissa. Muita suuria maita huijauksien isännöinnin kannalta olivat muun muassa Länsi-Euroopan maat, Kanada sekä Kiina. Samankaltaisia tuloksia esittää Tambe Ebotin ja Siposen (2014) mukaan Ultrascan (2010)[2], jonka mukaan muun muassa juuri Yhdysvalloissa, Kiinassa ja Kanadassa voidaan nähdä huijaustoiminnan määrän kasvua. Yhdysvaltojen huijauspalvelimien suuren määrän pohdittiin Anderson ja muiden (2007) tutkimuksessa johtuvan siitä, että huijauksen infrastruktuurilla täytyy olla korkea saatavuustaso (engl. availability), jotta huijarit voivat saada huijauksestaan voittoa. Lisäksi Anderson ja muut (2007) esittivät, että huijausten verkkoyhteyksien tulee olla stabiileja, joten heidän mukaansa on mahdollista, että monet huijausten isäntäpalvelimet sijoitetaan Yhdysvaltoihin juuri palvelinten korkean saatavuustason ja stabiilien verkkojen vuoksi.

Roskapostien välittäjät olivat tutkimuksessa enemmän jakautuneet ympäri maailmaa, kuin palvelimet: Anderson ja muut (2007) perustelevat tätä sillä, että roskapostien välittäjät tarvitsevat vain lyhyen aikavälin toteuttaakseen tehtävänsä. Roskapostien välittäjien tehtävä on vain lähettää roskapostia maailmalle, eivätkä ne vaadi kanssakäymistä roskapostien vastaanottajien kanssa toisin kuin isäntäpalvelimet, joiden tulee palvella ja olla saatavilla mahdollisimman pitkään kerätäkseen mahdollisia uhreja.

2.3 Länsi-Afrikan huijaukset

Andersonin ja muiden (2007) tutkimuksen lisäksi kirjallisuudessa on havaittavissa eräs konkreettinen huijaustyyppi, jonka operoimiseen roskapostiviestejä käytetään. Tambe Ebotin ja Siposen (2014) mukaan Burrell (2008) on todennut, että tässä huijaustyypissä huijarit toimivat pääosin Länsi-Afrikassa kehitellen viesteihin tarinoita, joilla pyritään huijaamaan ja harhaanjohtamaan internetin käyttäjiä rahallisen voiton saavuttamiseksi. Tambe Ebotin ja Siposen (2014) mu-

2 http://www.ultrascan-agi.com/

kaan tarinat saattavat koskea muun muassa saatavilla olevia perintöjä, lemmikkieläimiä tai kultaa. Tarinoihin liitetään Burrellin (2008) mukaan muun muassa väkivaltaa, köyhyyttä tai henkilökohtaisia tragedioita. Tambe Ebotin ja Siposen (2014) mukaan Herley (2012) on todennut, että huijausviesteillä pyritään huijaamaan viestien vastaanottajia maksamaan kaupan olevista hyödykkeistä maksuja etukäteen. Salifu (2008) on Tambe Ebotin ja Siposen (2014) mukaan todennut, että maksut ovat pääasiassa logistiikkaan liittyviä, muun muassa rahti-, vakuutus- ja karanteenimaksuja, jotka huijauksen uhrin tulee maksaa ennen kuin tulli voi hyväksyä tavaran toimitettavaksi. Burrellin (2008) mukaan edellä kuvatun tyylisiä huijauksia kutsutaan usein 419 -huijauksiksi (engl. 419 scams), jossa 419:llä viitataan Nigerian poliisin käyttämään koodiin petoksille. Toisena nimityksenä 419 -huijauksista käytetään etukäteismaksupetosta (engl. advance fee fraud).

Tambe Ebotin ja Siposen (2014) tutkimuksessa tutkittiin kamerunilaisille ammatti-verkkohuijareille tehtyjä haastatteluita ja selvitettiin muun muassa, minkälaisia rationaalisia päätösprosesseja he tekevät, kun he suunnittelevat huijauksia ja miten heistä ylipäätään tuli verkkohuijareita. Tutkijoiden mukaan verkkohuijariksi tulemiseen ajoivat pidempään verkkohuijauksia tehneillä muun muassa kostonhimo johtuen huijareiden kokemasta kaltoinkohtelusta liittyen kyvyttömyyteen hankkia laillista työtä johtuen paikallisesta korruptiosta ja ostajien hyväksikäytöstä. Kostosta huijarit haluavat palkaksi taloudellista hyötyä. Nuorempi sukupolvi noin 20 -vuotiaita huijareita kokee Tambe Ebotin ja Siposen (2014) mukaan, että verkkohuijaaminen on kustannustehokas keino saavuttaa vanhempien huijareiden rikas elintaso. Myös Burrellin (2008) haastattelemat nuoremmat huijarit kertoivat alkaneensa huijata johtuen vertaistensa, esimerkiksi huijariystäviensä, vaikutuksesta, sekä uskomuksista liittyen varakkaaseen elämään.

Huijariksi tulemisen syiden lisäksi Tambe Ebot ja Siponen (2014) tutkivat, miten haastatellut verkkohuijarit suunnittelevat ja toteuttavat huijauksensa. Alustavan tutkimusdatan mukaan he aluksi valitsevat tarkasti muun muassa taktiikan, jolla huijaus toteutetaan, esimerkiksi roskapostien välityksellä tai sosiaalisessa mediassa. Sitten huijausstrategioita mietitään uudelleen, mikäli tarve tulee, esimerkiksi jos huijauksen kohde ei ole menossa huijaukseen mukaan, voidaan laskea myytävien (vale)hyödykkeiden hintoja. Huijausten suunnittelustrategioiden hiomisen lisäksi huijareiden täytyy Tambe Ebotin ja Siposen (2014) mukaan kehittää strategioita huijauksen toteutukseen. Näihin kuuluu muun muassa huijausten kohteiden suostuttelu maksamaan hyödykkeistä etukäteen muun muassa aiemmin mainittuja logistiikkamaksuja luomalla valedokumentteja, joilla maksuja perustellaan.

2.4 Yhteenveto

Ensimmäisessä sisältöluvussa tutkittiin, mitä verkkohuijauksista on kirjoitettu tutkimuskirjallisuudessa. Havaittiin muun muassa, että verkkohuijauksissa ros-

kapostiviestit ovat oleellisessa asemassa: niiden avulla toteutetaan monia huijauksia liittyen muun muassa hyödykekauppaan. Roskapostiviesteillä voidaan huijata rahaa esimerkiksi markkinoimalla olemattomia lääkkeitä tai ohjelmistoja halvalla tai yrittämällä saada uhri mukaan etukäteismaksupetokseen, jossa hänelle luvataan esimerkiksi perintöjä, lemmikkieläimiä, kultaa tai hyödykkeitä etukäteen maksettavia logistiikkamaksuja vastaan. Lisäksi roskapostiviestit voivat olla haitallisia, jolloin niillä voidaan yrittää saada uhri asentamaan järjestelmäänsä haittaohjelmia tai luovuttamaan arkaluontoisia tietojaan verkkohuijareille. Verkkohuijausten toteutukseen käytetään roskapostiviestien lisäksi apuna myös sosiaalista mediaa muun muassa huijausviestien välitykseen ja tietojen keräämiseen huijauksen mahdollisista uhreista. Havaittiin, että huijauksissa on useimmiten motiivina rahallinen hyöty ja Länsi-Afrikan 419 -huijausten tapauksessa myös kostonhimo johtuen paikallisesta köyhyydestä ja korruptiosta, sekä tunne kyvyttömyydestä tehdä laillista työtä. Verkkohuijausten määrän todettiin olevan suurta myös muun muassa Yhdysvalloissa, Kanadassa ja Kiinassa. Seuraavassa luvussa käsitellään sosiaalista mediaa yleisesti alustana ja näkökulmana tälle kirjallisuuskatsaukselle, sekä tutkitaan verkkohuijauksia sosiaalisilla verkostoitumissivuilla.

3 SOSIAALINEN MEDIA JA VERKKOHUIJAUKSET

Tässä luvussa käsitellään sosiaalista mediaa näkökulmana tälle kirjallisuuskatsaukselle. Aluksi luvussa käsitellään sosiaalisen median määritelmiä ja pyritään yhdistelemään niitä. Sosiaalisen median määrittelyjen jälkeen tutkitaan verkkohuijausten tyyppejä sosiaalisten verkostoitumissivujen kontekstissa. Lopuksi esitetään yhteenveto tässä luvussa käsitellyistä määritelmistä, sekä vastataan tutkielman tutkimuskysymyksiin, jotka kuuluvat: Minkä tyyppisiä verkkohuijauksia sosiaalisessa mediassa tapahtuu ja ovatko huijaukset erityyppisiä sosiaalisessa mediassa, kuin sen ulkopuolella?

3.1 Sosiaalisen median määritelmät

Aiemmin tutkittiin Kaplanin ja Haenleinin (2010) määritelmää sosiaalisesta mediasta. Määritelmän mukaan sosiaalinen media on joukko web 2.0 -perustaisia web -sovelluksia, joissa tuotetaan käyttäjien luomaa sisältöä. Kaplanin ja Haenleinin (2010) määritelmän lisäksi tutkitaan Kietzmannin ja muiden (2011) sosiaalisen median viitekehystä. Tämän viitekehyksen mukaan sosiaalinen media koostuu toiminnallisista osasista, joita ovat läsnäolo, suhteet, identiteetti, maine, ryhmät, keskustelut ja jakaminen. Kietzmannin ja muiden (2011) mukaan tulee kuitenkin huomata, että jokin toiminta sosiaalisessa mediassa voi kuulua useampaan edellä mainituista osasista samanaikaisesti ja kaikkien osasten periaatteiden ei tarvitse täyttyä, jotta toiminnan voidaan laskea kuuluvan sosiaaliseen mediaan. Kietzmannin ja muiden (2011) mukaan Smith toteaa artikkelissaan[3], että jotkut osaset painottuvat viitekehyksessä enemmän riippuen sosiaalisen median palvelusta, sillä esimerkiksi YouTube -videopalvelussa jakaminen on tärkeimmässä osassa ja suhteet ovat pienemmässä roolissa. Facebookissa taas suhteet ovat tärkeämmässä roolissa, kuin jakaminen. Seuraavaksi käydään lyhyesti läpi toiminnalliset osaset, joista Kiezmannin ja muiden (2011) sosiaalisen median viitekehys muodostuu.

Läsnäololla (engl. presence) tarkoitetaan Kietzmannin ja muiden (2011) mukaan toisten ihmisten saavutettavuuden tasoa, sekä ihmisten sijaintia oikeassa ja/tai virtuaalisessa maailmassa. Läsnäolon määrään vaikuttavat Kaplanin ja Haenleinin (2010), sekä Kietzmannin ja muiden (2011) mukaan intiimiys ja välittömyys. Kaplanin ja Haenleinin (2010) mukaan intiimiys kuvaa sitä, onko viestintä välitettyä vai tapahtuuko se esimerkiksi kasvotusten ja välittömyys sitä, tapahtuuko viestintä samanaikaisesti vai eriaikaisesti. Välitetyssä viestinnässä, esimerkiksi puhelinkeskustelussa, on matalampi läsnäolon määrä, kuin kasvotusten tapahtuvassa viestinnässä. Samoin eriaikaisessa viestinnässä, esimerkiksi sähköpostikeskustelussa, on matalampi läsnäolon määrä, kuin samanaikaisessa viestinnässä, esimerkiksi chat -keskustelussa. (Kaplan & Haenlein, 2010). Läsnäolon

3 http://nform.com/ideas/social-software-building-blocks/

määrä osapuolten välisessä kommunikaatiossa on yhteydessä siihen, miten paljon kommunikaatio vaikuttaa osapuolten käyttäytymisiin. Jos kommunikaatiossa on suuri läsnäolon määrä, se vaikuttaa vuorovaikutuksessa oleviin osapuoliin enemmän. (Kaplan & Haenlein, 2010; Kietzmann ym., 2011).

Suhteilla (engl. relationships) tarkoitetaan tapoja, joilla käyttäjät ovat joillakin tavoilla sidoksissa toisiinsa. Suhteet voivat johtaa esimerkiksi keskusteluihin tai tapaamisiin osapuolten välillä, mutta suhteelle syy voi olla myös vain kaveriksi lisääminen itsessään. (Kietzmann ym., 2011). Suhteiden vahvuudet voivat vaihdella: Kietzmannin ja muiden (2011) mukaan Krackhardt (1992) on todennut, että vahvat suhteet ovat pitkäkestoisia ja osapuoliaan vaikuttavia. Hansen (1999) taas on Kietzmannin ja muiden (2011) mukaan todennut, että heikot suhteet ovat etäisiä ja niissä kanssakäyminen on harvinaista.

Identiteetillä (engl. identity) tarkoitetaan ihmisen itsestään luoman identiteetin tasoa sosiaalisessa mediassa sisältäen esimerkiksi sen, mitä tietoa ihmiset haluavat itsestään kertoa (Kietzmannin ym., 2011). Kietzmannin ja muiden (2011) mukaan käyttäjän tietoja voivat olla esimerkiksi sukupuoli ja nimi, oli nimi sitten käyttäjän oikea nimi tai nimimerkki. Lisäksi Kietzmannin ja muiden (2011) mukaan Kaplan ja Haenlein (2010) ovat todenneet, että käyttäjä voi rakentaa identiteettiään muun muassa tiedostetusti tai tiedostamattaan kertomalla tietoja aatteistaan, tykkäyksen kohteistaan tai tunteistaan.

Keskusteluilla (engl. conversations) Kietzmann ja muut (2011) tarkoittavat sitä, miten sosiaalisen median käyttäjät ovat vuorovaikutuksessa keskenään. Keskustelut voivat tapahtua monesta syystä, esimerkiksi käyttäjät voivat haluta vaihtaa ajatuksiaan toistensa kanssa, tai löytää samankaltaisia ihmisiä ja uusia näkökulmia. Lisäksi keskusteluiden välineet ja tasot voivat olla erilaisia. Esimerkiksi Twitter -sivuston maksimissaan 140 -merkkiä pitkien julkaisujen kautta käytävä keskustelu on monesti nopeampaa ja lyhyempikestoista, kuin esimerkiksi blogien syvällisemmät ja pidemmät keskustelut. (Kietzmann ym., 2011).

Maineella (engl. reputation) Kietzmann ja muut (2011) kuvaavat tapaa, jolla sosiaalisen median käyttäjät voivat arvioida itsensä ja muiden asemaa sosiaalisessa mediassa. Käyttäjän maine viittaa myös hänen julkaisemansa sisällön laatuun. Maine voi muodostua muun muassa sisällöstä tykkäysten ja ei-tykkäysten kautta, sivustojen tekemien automaattisten luotettavuusarviointien johdosta, tai esimerkiksi LinkedIn -sivustolla muiden käyttäjien osoittaman kannatuksen kautta. (Kietzmann ym., 2011).

Ryhmillä (engl. groups) Kietzmann ja muut (2011) tarkoittavat sitä, millä tavalla käyttäjät voivat ryhmäytyä toistensa kanssa. Ryhmät voivat olla käyttäjän itse luomia, esimerkiksi kaverilistojen jäsenten lajittelu ryhmiin. Ryhmät voivat myös toimia kuten ryhmät verkon ulkopuolella, esimerkiksi avoimet ryhmät, ryhmät joihin voi hakea jäseneksi ja sellaiset ryhmät, joihin voi liittyä vain, kun niihin kutsutaan. (Kietzmann ym., 2011).

Jakaminen (engl. sharing) kuvaa Kietzmannin ja muiden (2011) viitekehyksessä käyttäjien sisällön vaihtamista ja vastaanottamista muiden käyttäjien kesken, sekä sisällön levittämistä muille käyttäjille. Jaettava sisältö voi olla esimer-

kiksi ääntä, videota, tekstiä, kuvia tai sijainteja. Jakaminen on sosiaalisessa mediassa yksi kanssakäymisen muoto ja sosiaalinen media koostuukin käyttäjistä, joilla on yhteys esimerkiksi edellä mainitun tyyppisiin jaettuihin sisältöihin. (Kietzmann ym., 2011).

Kietzmannin ja muiden (2011), sekä Kaplanin ja Haenleinin (2010) määritelmiä hyväksikäyttäen voidaan todeta, että sosiaalinen media on web -teknologioita ja uusia verkon käyttöperiaatteita alustanaan käyttävä kommunikaatiokanava. Kommunikaatio muiden käyttäjien kanssa käy muun muassa käyttäjien luoman sisällön jakamisen, ryhmien, sekä keskusteluiden avulla ja siihen vaikuttavat muun muassa suhteet ja läsnäolo. Muiden käyttäjien kanssa kommunikoimalla käyttäjä voi luoda yhteyksiä ja luoda yhteyksiä muihin saman henkisiin ihmisiin. Lisäksi käyttäjä voi luoda itselleen identiteetin muun muassa kertomalla itsestään ja kiinnostusten kohteistaan, sekä ansaita maineen muun muassa julkaisemansa sisällön kautta. Vaikka sosiaalisen median alustoja on erityyppisiä, tässä kirjallisuuskatsauksessa tarkastellaan verkkohuijauksien tyyppejä erityisesti sosiaalisten verkostoitumissivujen kannalta.

3.2 Verkkohuijaukset sosiaalisilla verkostoitumissivuilla

Aiemmin tutkielmassa määriteltiin sosiaaliset verkostoitumissivut web -sovelluksiksi, joihin voi luoda profiilin, luoda yhteyksiä muihin käyttäjiin, sekä tutkia käyttäjien yhteyksiä toisiinsa. Tällaisilla sovelluksilla on miljoonia käyttäjiä ja niiden käytöstä on tullut osa jokapäiväistä elämää. (Ellison, 2007). Sosiaaliset verkostoitumissivut tarjoavat kuitenkin myös uusia hyökkäysmahdollisuuksia, jotka perustuvat sen luottamuksen hyväksikäyttöön, joka ihmisillä on verkostojaan kohtaan (Wüest, 2010). Seuraavaksi tutkitaan näitä hyökkäysmahdollisuuksia.

3.2.1 Roskaposti ja haitalliset huijauskeinot

On tärkeä huomata, että roskapostiviestien lähetystä ja julkaisua tapahtuu myös sosiaalisilla verkostoitumissivuilla muun muassa pikaviestien, tilapäivitysten, kommenttikenttien, sekä valheellisten tapahtumakutsujen avulla. Wüest (2010) on todennut, että roskapostiviestien lähettäjille sosiaaliset verkostoitumissivut ovat olennainen tapa lähettää roskapostia sivujen suurien käyttäjämäärien, sekä useimmiten viestien ilmaisuuden vuoksi. Usein kuitenkin roskapostiviestien lähettämiseksi vaaditaan, että molemmat käyttäjät ovat yhteydessä toisiinsa, joten huijarit luovat tekaistuja valetilejä ja yrittävät lähettää ystäväpyyntöjä käyttäjille. Jos käyttäjät hyväksyvät näitä yhteyspyyntöjä, pyynnön hyväksyneille käyttäjille voidaan alkaa lähettää roskapostiviestejä. Roskapostiviestin voi sisällyttää myös itse yhteyspyyntöviestiin, jolloin käyttäjien välillä ei tarvitse vielä olla yhteyttä roskapostiviestin perille saamiseksi. Wüest (2010).

Roskapostiviestien lähettämiseen käytetään myös tietojenkalastelulla kaapattuja tilejä, jolloin roskapostiviesti kaapatun tilin yhteyksille näyttää tulevan tunnetulta käyttäjältä. (Wüest, 2010). Kuten aiemmin mainittiin, tällöin viesti on uskottavampi ja saattaa onnistua tarkoituksessaan todennäköisemmin (Jagatic ym., 2007; Wüest, 2010). Wüestin (2010) mukaan tietojenkalastelu sosiaalisilla verkostoitumissivuilla tapahtuu siten, että sivustoista tehdään kopioita, jotka näyttävät alkuperäisiltä sivustoilta, mutta ovat oikeasti huijaussivustoja. Käyttäjät pyritään saamaan syöttämään alkuperäisen sivuston kirjautumistietonsa näille huijaussivustoille, jolloin hyökkääjät saavat kirjautumistiedot haltuunsa.

Myös sosiaalisen suostuttelun haittaohjelmia voidaan välittää sosiaalisen median avulla. Wüestin (2010) mukaan käyttäjät voivat saada haitallisia linkkejä esimerkiksi verkostoitumissivujen roskapostien välityksellä, esimerkiksi kuvatiedostoksi naamioitua Nemucod -haittaohjelmaa on jaettu Facebookin yksityisviestien välityksellä[4]. Haittaohjelmia voidaan levittää myös sosiaalisten verkostoitumissivujen haitallisten liitännäisten kautta. Esimerkiksi Facebookin liitännäissovellukset voivat olla haitallisia monella tapaa: ne voivat salaa päästä käsiksi käyttäjien tietoihin ja levitä julkaisemalla haitallista linkkiä tartunnan saaneen käyttäjän nimissä. Linkit voidaan myös naamioida käyttämällä URL -lyhennepalveluita (engl. URL shortening services), esimerkiksi “bit.ly” -alkuisia linkkejä naamioimaan alkuperäinen linkki. Tällöin käyttäjän on vaikea erottaa, onko alkuperäinen linkki luotettava. Linkkien klikkaamisen lisäksi käyttäjä voidaan myös huijata itse suorittamaan hyökkääjän antama haitallinen koodi, esimerkiksi JavaScript –koodinpätkä, selaimessaan. Wüest (2010).

Wüestin (2010) mukaan esimerkkinä haitallisista liitännäissovelluksista ovat esimerkiksi haitalliset kyselysovellukset, sillä ne saattavat ennen kyselyn tulosten julkaisua vaatia käyttäjää lähettämään kyselylinkki ystävilleen, jolloin kyselyn tekijä saa käyttäjän sovellukselle antamien oikeuksien avulla haltuunsa tietoja käyttäjistä ja saa kyselylinkin leviämään muille käyttäjille. Eräs toinen esimerkki haitallisesta huijaamisesta sosiaalisilla verkostoitumissivuilla ovat Wüestin (2010) mukaan seuraajahuijaukset (engl. follower scams). Huijaukset perustuvat paineeseen kerätä paljon seuraajia verkostoitumissivuilla, joten huijarit tarjoavat palveluita, joissa käyttäjätunnuksen ja salasanan luovuttamista vastaan tarjotaan käyttäjän seuraajamäärän kasvua. Tällöin käyttäjät menettävät kirjautumistietonsa huijareille ja muutenkin salasanan jakaminen on usein myös verkostoitumissivujen sääntöjen vastaista. Seuraajahuijauksissa tarjottavat palvelut voivat olla myös maksullisia (Wüest, 2010).

3.2.2 Klikkausten kaappaus

Klikkausten kaappaus (engl. clickjacking) tarkoittaa Wüestin (2010) mukaan sitä, että käyttäjä huijataan klikkaamaan jotain, jonka olemassaolosta hän ei tiennyt.

4 https://www.bleepingcomputer.com/news/security/facebook-spam-campaign-spreading-nemucod-downloader-and-locky-ransomware/

Käyttäjän hiiren osoittimen kohdalle voidaan piilottaa kohde, jota käyttäjän halutaan klikkaavan ja naamioida näkymä esimerkiksi peliksi, jossa kehotetaan käyttäjää klikkaamaan jotakin kohtaa ruudulla. Tällöin käyttäjä tiedostamattaan tulee klikanneeksi esimerkiksi näkymätöntä "tykkää" -painiketta tai vaihtaneeksi profiilinsa asetuksia. (Wüest, 2010).

3.2.3 419 –huijaukset

Myös 419 -huijauksia, eli etukäteismaksupetoksia tapahtuu sosiaalisessa mediassa. Tambe Ebotin ja Siposen (2014) mukaan huijarit voivat sähköpostin sijaan myös julkaista verkon käyttäjiä harhaanjohtavat tarinansa sosiaaliseen mediaan ja yrittää saada käyttäjiä mukaan huijauksiin. Wüestin (2010) mukaan sosiaalisten verkostoitumissivujen avulla huijarin on helppo löytää monia huijattavia ja sama huijaus on toistettavissa useita kertoja. Lisäksi sivustoilta saatavien tietojen avulla tällaisia huijauksia voidaan kohdentaa paremmin.

3.2.4 Toisena käyttäjänä esiintyminen ja tiedon väärinkäyttö

Sosiaalisilla verkostoitumissivuilla on helppoa tehdä jonkun käyttäjän ystävää tai julkisuuden henkilöä imitoiva valeprofiili samalla nimellä ja hankkia julkisesti saatavilla olevia kuvia imitoitavista henkilöistä profiilikuviksi. Valeprofiileilla voi lähettää roskapostia ja levittää väärää tietoa, tai juoruja. Lisäksi julkisuuden henkilöiden valeprofiileilla voidaan yrittää kerätä yhteyksiä, joille voidaan myöhemmin huhujen ja väärän tiedon levittämisen jälkeen lähettää roskapostia. (Wüest, 2010).

Sosiaalisilta verkostoitumissivuilta löytyvien tietojen väärinkäytöstä kerrottiin jo aiemmin, kun todettiin, että tietoja voidaan käyttää esimerkiksi kohdennettujen tietojenkalasteluhuijausten toteutukseen (Abraham & Chengalur-Smith, 2010; Jagatic ym., 2007). Wüestin (2010) mukaan eräs tapa kerätä tietoja väärinkäyttöä varten onkin se, että esimerkiksi organisaatioiden arkaluontoisia tietoja pyritään huijaamaan tekemällä valeprofiili sosiaaliselle verkostoitumissivulle ja luomalla yhteyksiä organisaation jäseniin peitetarinan avulla. Kun hyökkääjä on tavallisten keskustelujen kautta luonut luottamuksen uhriin, muun muassa sosiaalisen suostuttelun keinoja käyttämällä hyökkääjä voi yrittää saada organisaation jäsenen paljastamaan organisaation tietoja tai asentamaan haittaohjelman tietokoneelleen (Wüest, 2010).

3.3 Yhteenveto

Tässä luvussa käsiteltiin sosiaalista mediaa näkökulmana tälle kirjallisuuskatsaukselle. Sosiaalisen median havaittiin olevan uudenlainen verkon viestintäkanava, jossa käyttäjät muun muassa luovat suhteita toisiinsa, verkostoituvat ja ja-

kavat sisältöjä. Lisäksi tutkittiin verkkohuijauksia erityisesti sosiaalisten verkostoitumissivujen näkökulmasta. Havaittiin, että verkkohuijauksen tyyppejä, joita esiteltiin aiemmin ilman sosiaalisen median kontekstia, esiintyy myös sosiaalisilla verkostoitumissivuilla. Roskapostiviestejä esiintyy sähköpostipalveluiden lisäksi myös sosiaalisilla verkostoitumissivuilla, kuten myös haitallisen huijaamisen muotoja: tietojenkalastelua ja haittaohjelmien levitystä sosiaalisen suostuttelun avulla. Jopa 419 -huijauksia julkaistaan sosiaalisilla verkostoitumissivuilla. Lisäksi sosiaalisilla verkostoitumissivuilla havaittiin esiintyvän huijauksia, joita ei havaittu esiintyvän ilman sosiaalisen median kontekstia: Tällaisia huijauksia olivat haitallisiin huijaustyyppeihin kuuluvat seuraajahuijaukset, sekä haitalliset, verkostoitumissivujen profiilitietoja käyttävät liitännäissovellukset. Lisäksi havaittiin huijaustyyppi liittyen julkisuuden henkilön tai ystävien imitointiin sosiaalisten verkostoitumissivujen valeprofiilien avulla. Mielenkiintoista oli myös se, että sosiaalisia verkostoitumissivuja voidaan käyttää myös apuna huijausten räätälöintiin hakemalla uhreista saatavilla olevia tietoja. Seuraavassa luvussa esitellään tutkielman yhteenveto sisältäen muun muassa johtopäätökset ja jatkotutkimusaiheet.

4 YHTEENVETO

Tässä kandidaatin tutkielmassa tutkittiin verkkohuijausten tyyppejä sosiaalisessa mediassa rajaamalla tarkastelu koskemaan erityisesti sosiaalisia verkostoitumissivuja. Tutkielma toteutettiin kirjallisuuskatsauksena, johon kerättiin tieteellisiä artikkeleita, joista karsittiin mukaan tutkimusongelman kannalta olennaisimmat artikkelit. Kirjallisuudesta löytyi artikkeleita liittyen verkkohuijauksiin ja sen keinoihin ja tyyppeihin, mutta kirjallisuus, jossa kootaan huijaustyypit sosiaalisen median näkökulmasta, on vähäistä. Kirjallisuuskatsaus tehtiin tarkoituksena lisätä lukijan tietoisuutta verkkohuijauksen muodoista sosiaaliseen mediaan soveltaen, sekä edistää verkkohuijausten tutkimusta luomalla näkökulmia verkkohuijausten tutkimuksen tulevaisuudelle.

Kirjallisuuskatsauksen artikkeleiden pohjalta voitiin todeta, että verkkohuijaaminen on lisääntyvä ongelma internetin ja sosiaalisen median käytön lisääntyessä. Sosiaaliset verkostoitumissivut ovat osana ihmisten jokapäiväistä elämää, tarjoten myös uusia huijausmahdollisuuksia verkon käyttäjiä kohtaan. Sosiaalisten verkostoitumissivujen avulla voidaan päästä käsiksi käyttäjien henkilökohtaisiin tietoihin ja toteuttaa heitä kohtaan yhä kohdennetumpia ja siten uskottavampia huijauksia. Tästä voidaan päätellä, että sosiaalisen median käyttäjät eivät ole turvassa edes luottamuksellisten verkostoidensa sisällä: kuka tahansa voi joutua huijausyritysten kohteeksi. Sosiaalisessa mediassa huijaukset näyttävät olevan erityisen vaarallisia, sillä huijarien uhristaan saaman hyödyn lisäksi uhrin identiteetti verkostossa voi vaurioutua ja hänen tietonsa voidaan arkistoida huijareiden käsiin ikiajoiksi.

Tutkielman tutkimuskysymys kuului: Minkä tyyppisiä verkkohuijauksia sosiaalisessa mediassa tapahtuu ja ovatko huijaukset erityyppisiä sosiaalisessa mediassa, kuin sen ulkopuolella? Tutkimuskysymykseen vastauksena saatiin tämän kirjallisuuskatsauksen perusteella, että sosiaalisella medialla voidaan toteuttaa saman tyyppisiä verkkohuijauksia, kuin sosiaalisen median ulkopuolisilla verkon viestintäkanavilla, esimerkiksi sähköpostilla. Sosiaalisilla verkostoitumissivuilla julkaisuissa ja yksityisviesteissä esiintyy niin ikään roskapostia ja sillä toteutettavia haitallisia huijausmenetelmiä: haittaohjelmien levitystä sosiaalisen suostuttelun avulla, sekä tietojenkalastelua. Lisäksi 419 –huijauksia, eli etukäteismaksupetoksia toteutetaan verkostoitumissivuilla julkaisuja tekemällä.

Ovatko huijaukset sitten erityyppisiä sosiaalisessa mediassa, kuin sen ulkopuolella? Voivat olla, sillä sosiaaliset verkostoitumissivut tarjoavat sellaisia huijausmahdollisuuksia, joita ei ole mahdollista toteuttaa ilman sosiaalista verkostoitumissivua alustana. Nämä huijaukset liittyvät muun muassa toisena käyttäjänä esiintymiseen valeprofiilien avulla käyttäen apuna esimerkiksi aitojen käyttäjien julkisesti saatavilla olevia kuvia ja tietoja. Lisäksi havaittiin myös huijaukset liittyen verkostoitumissivuille ominaisiin, haitallisiin liitännäissovelluksiin, jotka voivat väärin käyttää käyttäjän tietoa ja tehdä muita haittaohjelmille ominaisia toimenpiteitä käyttäjien tileille. Edellisten lisäksi verkostoitumissivuilla

käyttäjien himoitsemaan suureen seuraajamäärän vedoten toteutetaan myös haitallista huijaamista, jossa luvataan käyttäjän seuraajamäärän nousua.

Tulevaisuudessa olisi mielenkiintoista tutkia, minkälaisia automaattisia keinoja voitaisiin kehittää opastamaan käyttäjiä turvalliseen sosiaalisen median käyttöön. Automaattiset keinot voisivat olla muun muassa selainlisäosia ja sosiaalisten verkostoitumissivujen liitännäissovelluksia, jotka estävät käyttäjiään tulemasta huijatuiksi. Näiden keinojen tuomien hyötyjen tutkimus voisi edistää haavoittuvien sosiaalisen median käyttäjien tietoisuutta ja estää heitä tulemasta huijatuiksi, kun huijaamismenetelmät kehittyvät verkon mukana yhä monimuotoisimmiksi.

LÄHTEET

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183-196.

Anderson, D. S., Fleizach, C., Savage, S., & Voelker, G. M. (2007). *Spamscatter: Characterizing internet scam hosting infrastructure* (Doctoral dissertation, University of California, San Diego).

Baker, C. R. (1999). An analysis of fraud on the Internet. *Internet Research*, *9*(5), 348-360.

Burrell, J. (2008). Problematic empowerment: West African Internet scams as strategic misrepresentation. *Information Technologies & International Development*, *4*(4), 15.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948-956.

Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer- Mediated Communication*, *13*(1), 210-230.

Erbschloe, M. (2004). *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Burlington, MA: Elsevier Butterworth-Heinemann.

Grazioli, S., & Järvenpää, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *30*(4), 395-410.

Gundecha, P., & Liu, H. (2012). Mining social media: a brief introduction. *New Directions in Informatics, Optimization, Logistics, and Production*. Informs, 1-17

Hansen, M. T. (1999). The search-transfer problem: The role of weak ties in sharing knowledge across organization subunits. *Administrative science quarterly*, *44*(1), 82-111.

Herley, C. (2012). Why do nigerian scammers say they are from nigeria? *WEIS*.

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

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), 59-68.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business horizons*, *54*(3), 241-251.

Krackhardt, D. (1992). The strength of strong ties: The importance of philos in organizations. *Networks and organizations: Structure, form, and action, Harvard Business School Press, Boston*, 216-239.

Okoli, C., Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems, 10*(26).

Raman, K. (2008). Ask and you will receive. '*Mcafee security journal'Debuts*, 9.

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime*, *15*(4), 432-443.

Tambe Ebot, A. C., & Siponen, M. (2014). Toward a Rational Choice Process Theory of Internet Scamming: The Offender's Perspective. *Proceedings of International Conference on Information Systems, 6*, 4603-4612.

Vickery, G., & Wunsch-Vincent, S. (2007). *Participative web and user-created content: Web 2.0 wikis and social networking*. Paris, France: OECD.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cyber-crime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.