Tietojenkalasteluviestien kehitys ja niiltä suojautuminen

Patrik Sulander

Haaga-Helia ammattikorkeakoulu
Tradenomi, Tietojenkäsittely
Opinnäytetyö
2022

Tiivistelmä

Tekijä(t)
Patrik Sulander

Tutkinto
Tietojenkäsittelyn Tradenomi

Raportin/Opinnäytetyön nimi
Tietojenkalasteluviestien kehitys ja niiltä suojautuminen

Sivu- ja liitesivumäärä
36 + 5

Tämän opinnäytetyön tavoitteena oli selvittää tietojenkalasteluviestien kehitystä ja niiltä suojautumista viimeisen 5 vuoden aikana sekä arvioida mahdollista kehitystä myös lähitulevaisuuden osalta. Ymmärtämällä jo tapahtuneita hyökkäyksiä edistetään myös mahdollisuuksia suojautua hyökkäyksiltä tulevaisuudessa. Erilaisia tietojenkalasteluviestejä on hyvin paljon erilaisia, joten tässä tutkimuksessa ei varsinaisesti keskitytty yksittäisten kalasteluviestien kehitykseen, vaan suuren otannan perusteella luotuun kokonaiskuvaan, sekä siihen miten ihmisten mielipiteet tietojenkalasteluviesteistä tukevat tilastoja hyökkäyksistä ja niiltä suojautumisesta.

Opinnäytetyön tavoitetta rajattiin seuraavilla tutkimuskysymyksillä:

- Minkälaisten tietojenkalasteluviestien määrä on kasvanut, mitkä ovat vähentyneet? Onko muutokselle olemassa selkeitä syitä.
- Mitkä hyökkäykset ovat toimivimpia ja miksi? Onko ihmisten käytös viestejä kohtaan muuttunut.
- Mihin suuntaan hyökkäykset tulevat todennäköisesti kehittymään seuraavien vuosien aikana? Millä tavoin pystymme ennakoimaan ja suojautumaan näiltä hyökkäyksiltä.

Tutkimuskysymyksiin rakennettiin perusteltuja vastauksia hyödyntämällä olemassa olevia tilastoja sekä vastauksia, jotka syntyivät luodun haastattelun avulla. Tutkimustulosten lisäksi tutkimus koostuu johdannosta, tietoperustasta, tutkimusosasta sekä pohdinnasta.

Tutkimuksessa todettiin, että viestien määrät sekä tappiot ihmisille ovat joka vuosi kasvamassa ja hyökkäykset ovat kehittyneet laadukkaammiksi ja henkilökohtaisemmiksi. Tärkeimmän ja heikoimman suojan eli ihmisten täytyisi muuttaa asennetta hyökkäyksiä kohtaan, jotta ne olisi mahdollista pysäyttää. Tutkimus suoritettiin päätökseen toukokuussa vuonna 2022.

Asiasanat
Tietojenkalastelu, kyberturvallisuus, viestintä, tietoturva

Sisällys

1 Johdanto 1
1.1 Tavoitteet ja rajaukset 2
2 Mitä on tietojenkalasteluviestit 4
3 Tietojenkalasteluviestien historia 5
4 Erilaisia tietojenkalastelukäsitteitä ja -tekniikoita 8
4.1 Käsitteitä (Cyber Risk Aware s.a. & Panda Security 2021) 8
4.2 Tekniikoita 10
5 Käyttäjän manipulointi (Social engineering) 12
5.1 Miten hyökkäykset toimivat käytännössä 12
5.2 Ihmisten heikkoudet (Kaspersky s.a.) 12
5.3 Erityisiä hyökkäysmenetelmiä 13
6 Suojautuminen tietojenkalastelulta 14
6.1 Toiminta viestiä avatessa 14
6.2 Teknillinen puoli ja kalasteluviestien tunnistaminen 14
6.3 Hyökkäysten estäminen 15
7 Tietojenkalasteluviestien kehitys tilastoina ja suojautuminen 18
7.1 Tutkimusmenetelmät 18
8 Tuloksien esittäminen 20
8.1 Toteutus 20
8.1.1 Tilastovertailu 20
8.1.2 Haastattelutulokset 30
8.1.3 Johtopäätökset 33
9. Pohdinta 35
Lähteet 37
Liitteet 40
Liite 1. Kysely 40

1 Johdanto

Vuonna 2020 96 % sosiaalisista hyökkäyksistä saapui sähköpostin kautta (Verizon 2020). Voidaan pohtia, johtuuko tämä määrä esimerkiksi korona-ajasta sekä sen luomasta uudesta ajanjaksosta. Sillä koronaepidemian aikana etätyöskentely on kasvanut huomattavasti työympäristöissä, vai ovatko tilastot näyttäneet samalta jo vuosia. Tietojenkalasteluviestien avulla kyberrikolliset pyrkivät saamaan viestien vastaanottajilta arkaluonteisia tietoja itselleen. Tämä hyökkäystapa on ollut jo pitkään suosittu kyberrikollisten keskuudessa sillä yksinkertaisuudessaan ne ovat halpoja ja helppoja tehdä, mutta toimivatko yksinkertaisimmat hyökkäykset enää nykypäivänä, kun tietoisuus niiden käytöstä hyökkäyksissä on kasvanut. Tämän tyyppisiin kysymyksiin pureudun tässä opinnäytetyössäni.

Tietojenkalasteluviestit eli huijausviestit ovat iso osa kyberrikollisuutta, ja ne ovat seuranneet ihmisten elämää nykyteknologian kehittymisen siivellä. Uutisissa nykypäivänä vähän väliä uutisoidaan uusista kalasteluviestihyökkäyksistä, joilta ketään digitaalisten työkalujen kuten puhelimien ja sähköpostien käyttäjä ei ole turvassa. Ne ovat osa monien ihmisten arkea nykypäivänä. Uskon myös vahvasti, että niiden uhkaavuus meidän digitaalisessa maailmassamme on vain kasvamassa, kun koko ajan enemmän ihmiset siirtyvät enemmän digitaalisten palveluiden käyttöön, jonka johdosta myös tietoturvauhkien määrät ovat lisääntyneet huomattavasti. Onneksi on myös hyvä huomata, että tietoisuus tietojenkalasteluviestien olemassaolosta ja vaaroista on myös nousussa.

Tässä tutkimuksessa tutkin siis tietojenkalasteluviestien kehitystä ja arvioin mihin suuntaan tietojenkalasteluviestit voisivat olla menossa seuraavien muutamien vuoden aikana. Päädyin kyseiseen aiheeseen, koska tällä hetkellä työskentelen uhka-analyytikkona yrityksessä, jonka tavoite on kouluttaa asiakasyritysten työntekijöille tietojenkalasteluviestien vaaroista erilaisten hyökkäyssimulaatioiden avulla, jotka myötäilevät oikeita hyökkäyksiä, joita näemme päivittäin. Lisäksi ajankohtaisesti tiedotamme sekä koulutamme uusista hyökkäyksistä, hyökkäystekniikoista ja miten niiden suojautumiseen on mahdollista varautua omilla teoilla.

Tutkimusmenetelminä käytän tässä tutkimuksessa vertaisarviointia sekä kyselyä. Käytän vertaisarviointiin hyödyksi tuloksia jo olemassa olevista tilastoista, vertailen vuosien 2016 sekä 2021 välisiä uhkatilastoja keskenään ja suurimpia eroavaisuuksia. Raportit löytyvät internetistä. Arvioitavien tilastojen välillä on siis 5 vuotta aikaa. 5 vuotta on tarpeeksi pitkä aika teknologian kehityksen kannalta ja näin pystymme myös luomaan tarkemman ja luotettavamman tutkimuksen. Näiden analysoinnin sekä nimettömän Google Forms -kyselylomakkeen (kohderyhmä 15 henkilöä) vastausten ja mielipiteiden perusteella pystytään saamaan tuloksia tietojenkalasteluviestien edellisten vuosien

kehityksestä aina nykyhetkeen. Sekä ennakoimaan miten nämä olemassa olevat muutokset todennäköisesti tulevat vaikuttamaan tulevien vuosien suuntaan ja kehitykseen. Onko jopa tietojenkalasteluviestien kulta-aika pian ohitse?

85 % tietomurroista sisälsi inhimillisen elementin vuonna 2021 (Phishingbox 2021). Kysely satunnaisilta ihmisiltä liittyen tietojenkalasteluviestien kehitykseen on äärimmäisen tärkeä tutkimuksessani, sillä melkein kaikki tietomurrot johtuvat uhrin eli viestin vastaanottajan toiminnasta. Hyökkääjät eivät loisi näitä hyökkäyksiä eivätkä ne myöskään menestyisi ilman ihmisten eli kohteiden apua. Tämän takia on mielestäni tärkeää kuulla miten ihmiset suhtautuvat hyökkäyksiin ja onko heidän osaltansa mitään muutosta tapahtunut toiminnassa vuosien varrella.

1.1 Tavoitteet ja rajaukset

Tavoitteenani on käyttää jo olemassa olevia tilastoja hyödyksi sekä ihmisten mielipiteitä liittyen kehitykseen, joiden avulla pystyn perustella tarpeeksi kattavasti kehitykseen liittyvät lopputulokset ja seuraukset. Sekä luoda ennakoiva kokonaiskuva tietojenkalasteluhyökkäysten kehityksestä suojautumisen tueksi. Tulevaisuuden ennustaminen ei ole koskaan varmaa, mutta pystymme tutkimaan tähän mennessä tapahtunutta kehitystä tarpeeksi suuren aikaeron välillä ja sen avulla luomaan mahdollisen skenaarion mihin suuntaan kyberrikolliset todennäköisesti tulevat kehittämään kalasteluhyökkäyksiä. Haluan myös tuoda tietojenkalasteluviestejä enemmän esille tutkimuksellani, koska uskon että niiden toiminta-alue tulee tulevina vuosina vain kasvamaan kyberrikoksissa. Kysymys kuuluukin millä tavoin? On tärkeä, että ymmärrämme hyökkäyksiä sekä niiden kehitystä. Tällä tavoin pystymme tulevaisuudessa suojautumaan niiltä paremmin ja estämään laajoja hyökkäyksistä johtuvia tietovuotoja niin yritysmaailmassa kuin meidän kaikkien yksityiselämässäkin.

Erilaisia tietojenkalasteluviestejä on hyvin paljon erilaisia, joten tässä tutkimuksessa en varsinaisesti keskity yksittäisten kalasteluviestien kehitykseen teknillisesti tai kaikkiin maailman tietojenkalasteluhyökkäyksiin, joita tapahtuu satoja tuhansia päivässä. Vaan pyrkimys on luoda kokonaiskuva pienemmästä otannasta olemassa olevien tilastojen avulla. Käytän tutkimuksessani hyödyksi raportteja vuosien 2016 ja 2021 väliltä (2022 ei ole vielä tarpeeksi materiaalia analysoitavaksi) sekä myös laatimani nimettömän kyselyn vastauksia. Suuntaan kyselyn ja pilkon olemassa olevien tilastoiden materiaalin vain olennaisiin asioihin, jotka auttavat saamaan vastauksia tämän opinnäytetyön tutkimuskysymyksiin. Esittelen tutkimuskysymykset tässä luvussa myöhemmin. Eli keskityn arvioimaan ja vertailemaan mitä tekniikoita ja tapoja hyökkääjät ovat alkaneet enemmän käyttämään hyödyksi tietojenkalasteluviestien hyökkäyksissä viimeisen 5 vuoden aikana ja miksi sekä

miten nämä muutokset ovat vaikuttaneet hyökkäyksiltä suojautumiseen. Ala puolella löytyvät tutkimuskysymykset, joihin tämän tutkimuksen avulla pyrin löytämään vastaukset.

Tutkimuskysymykset:

Minkälaisten tietojenkalasteluviestien määrä on kasvanut, mitkä ovat vähentyneet? Onko muutokselle olemassa selkeitä syitä.

Mitkä hyökkäykset ovat toimivimpia ja miksi? Onko ihmisten käytös viestejä kohtaan muuttunut.

Mihin suuntaan hyökkäykset tulevat todennäköisesti kehittymään seuraavien vuosien aikana? Millä tavoin pystymme ennakoimaan ja suojautumaan näiltä hyökkäyksiltä.

2 Mitä on tietojenkalasteluviestit

Tässä luvussa kerron lyhyesti mitä tietojenkalastelu itsessään on ja niiden historiasta, miten hyökkäykset ovat kehittyneet alun perin. Tämän avulla on helpompi lähteä tutkimaan viestien kehitystä lähimenneisyydessä sekä tulevaisuudessa.

”Kalasteluviestit ovat yksinkertaisin kyberhyökkäystapa ja samalla myös vaarallisin ja toimivin, koska hyökkäykset kohdistuvat kaikista hauraimpaan ja voimakkaimpaan tietokoneeseen maailmassa: ihmismieli”, kuvailee Adam Kujawa, Malwarebytes Lab:n johtaja (Malwarebytes 2022). Miksi käyttäisi tuhottomasti aikaa palomuurien ohittamiseen muilla keinoilla, kun hyvin tehdyllä kalasteluviestillä voi saada suoraan käyttäjätunnukset ja salasanat järjestelmään kirjautumiseen. Hyökkäyksissä siis käytetään hyödyksi sosiaalista manipulointia (englanniksi social engineering). Luvussa 5 kerron kattavammin mitä tämä manipulointi oikein on.

Ensimmäiseksi tässä kyberrikoksessa hyökkääjät ottavat uhreihin yhteyttä sähköpostilla, tekstiviestillä tai soittamalla (webopedia 2021). Hyökkääjä esiintyy yleensä luotettavana toimijana käyttäen hyödyksi esimerkiksi verkkotunnuksien väärentämistä huijatakseen vastaanottajaa luulemaan viestin lähettäjää joksikin muuksi kuin todellisuudessa on (Malwarebytes 2022). Lopullisena tavoitteena on saada potentiaalinen uhri toimimaan jollakin tavalla lähettämäänsä tietojenkalasteluviestiä kohtaan.

Toiminnat voivat olla muun muassa linkin avaamista johtaen haitalliselle sivustolle, viestiin liitetty tiedosto, joka sisältää haittaohjelman tai viestissä suoraan pyydetään lähettäjältä joitakin arkaluonteisia tietoja kuten salasanoja ja henkilötunnuksia (Malwarebytes 2022). Näistä haittaohjelmista ja erilaisista tekniikoista kerron vielä tarkemmin seuraavassa luvussa.

Kerron siis luvussa 5 kattavammin miten hyökkääjät sitten saavat kohteensa reagoimaan heidän haluamallaan tavalla kalasteluviesteihin. Tämä on hyökkäysten tärkein vaihe saada kohde uskomaan, että on turvallista toimia viestin mainitsemalla tavalla. Hyökkääjät käyttävät erilaisia houkuttimia ja syöttejä kiinnittääkseen kohteen huomion viestiin. Yleisesti halutaan saada vastaanottaja erilaisten tunteiden valtaan, jotta huomio saadaan (Malwarebytes 2022). Myös päätöksentekotaidot voivat uhrilla hämärtyä, kun kyseessä on jokin hyvin houkutteleva tarjous tai pyyntö. Hyökkääjät käyttävät hyödyksi esimerkiksi kiirettä (toimi nyt tai rahasi katoavat), sääliä (läheinen on sairas), onnistumiseniloa (lottovoitto) tai pelkoa nostattavia tunteita, joihin kuuluu muun muassa ilmoitusluontaiset uhkailut: ”meillä on nyt teidän järjestelmä hallinnassamme”.

3 Tietojenkalasteluviestien historia

Ensimmäistä kertaa julkisesti tietojenkalastelua käytettiin hyödyksi tammikuun 2. päivä vuonna 1996. Silloin AOL (America Online) oli yksi johtavista Internetpalveluntarjoajista (PhishProtection s.a.). Tämä suosio veti myös hakkereita puoleensa ja hakkerit suorittivat tietojenkalastusviestejä palvelunkäyttäjiä vastaan. Aluksi hyökkääjät varastivat hyökkäyksissä käyttäjätunnuksia sekä salasanoja. Myöhemmin käyttämällä hyödyksi näitä varastettuja tietoja sekä heidän kehittämäänsä algoritmia, hyökkääjät alkoivat myös luoda satunnaisia luottokorttinumeroita. Näitä luottokorttinumeroita käytettiin uusien AOL käyttäjien luomiseen, siten tietojenkalasteluviesteissä hyökkääjät väittivät onnistuneesti olevansa AOL:n työntekijöitä ja pyysivät käyttäjiä vahvistamaan käyttäjänsä antamalla laskutustietoja ja muita henkilökohtaisia tietoja (PhishProtection s.a.). Nämä olivat erittäin onnistuneita, sillä hyökkääjät olivat onnistuneesti muovanneet viestien muotoilun ja värit samoiksi kuin virallisissa AOL viesteissä. Onnistuneiden hyökkäyksien avulla hyökkääjät pääsivät käsiksi uhrien käyttäjiin ja pystyivät käyttämään näitä tilejä hyödyksi uusien hyökkäyksien teossa. Toisekseen onnistuneista hyökkäyksistä oli vaikea syyttää palvelun käyttäjiä sillä mitään tämänkaltaisia hyökkäyksiä ei ollut aikaisemmin nähty. Hyvin pian AOL edistikin omaa tietoturvaansa (muun muassa lisäämällä varoitustekstejä saapuviin sähköpostiviesteihin pyytäen, että käyttäjät eivät paljastaisi henkilökohtaisia tietojaan sähköpostin kautta) ja näin hyökkääjien täytyi vaihtaa muihin tekniikoihin. Mielenkiintoista nähdä miten yhteen palveluntarjoajaan kohdistuneet hyökkäykset kehittyivät niin nopeasti suojauksen ohella käsi kädessä.

2000 – luvulla nähtiinkin suuri tietojenkalasteluviestien murros, samalla kun internetin käyttö sekä käyttäjämäärät jatkoivat kasvua. Syntyi uudenlaisia tietojenkalasteluviestejä niistä ensimmäisenä niin sanottu ”Love Bug” (Cofense s.a.) vuonna 2000. Viestit oli otsikoitu ”ILOVEYOU”, viestit sisälsivät hyvin yksinkertaisen pyynnön tarkistaa viestin liitteenä tulleen ”LOVELETTER” kirjeen. Viestien vastaanottajat, jotka eivät voineet vastustaa kiusausta ja avasivat kirjeet päästivät tietokoneisiinsa haitallisen madon. Mato kopioi ja tuhosi paikallisessa tietokoneessa sijaitsevia tiedostoja. Mato myös lähetti saman kalasteluviestin uhrin osoitekirjassa oleviin sähköpostiosoitteisiin. Oli arvioitu, että noin 45 miljoonaa Windows tietokonetta, joutui tämän hyökkäyksen uhriksi. Nykyään tämän tyyppisistä hyökkäyksistä käytetään termiä ”catphishing”, josta kerron lisää seuraavassa luvussa.

2000 – luvun alussa internetin mukana sähköinen kaupankäynti yleistyi ja rakkauskirjeiden lisäksi verkkokaupat ja sähköiset maksujärjestelmät houkuttelivat myös hyökkääjiä. Hyökkääjät ostivat itselleen verkkotunnuksia, jotka mukailivat oikeiden maksualustojen kuten PayPal ja eBay käyttämiä verkkotunnuksia (Phishprotection s.a.). Ostettujen verkkotunnusten avulla hyökkäyksien

tunnistaminen ja erottaminen virallisista toimijoista on vaikeaa, jos uhri ei huolellisesti tarkista lähettäjän sekä verkkosivuston osoitetta. Hyökkäyksissä lähetettiin väärennettyjä sähköpostiviestejä isojen maksualustojen nimissä ja tämän avulla hyökkääjät saivat monet maksualustojen asiakkaat syöttämään luottokorttitietoja linkkien johtamille valesivustoille, joissa asiakasta pyydettiin päivittämään luotto – ja muita henkilötietoja.

2004 vuodesta lähtien tietojenkalastus levisi laajemmin pankkeihin, yrityksiin ja palveluiden asiakkaisiin. Useita uusia tekniikoita oli monipuolisesti hyökkäyksissä mukana, kuten kohdennetut hyökkäykset, puhelimitse tapahtuvia hyökkäyksiä sekä ohjelmia, jotka tallentavat näppäimistön painalluksia (engl. spear phishing, vishing, smishing, keylogging). Vuosi, jolloin tietojenkalastelu todella nousi uusiin ulottuvuuksiin. Valmiita tietojenkalastusohjelmia oli saatavilla pimeiltä markkinoilta, joita kuka vaan pystyi käyttämään helposti hyödyksi omissa hyökkäyksissä ja organisoidut hakkeriryhmät alkoivat teettämään tarkempia tietojenkalastelukampanjoita. Tämän laajemman kasvun seurauksena tappiot hyökkäyksistä suurenivat myös. Jopa 3,6 miljoonaa ihmistä menetti tietojenkalasteluhyökkäyksille 3,2 miljardia dollaria Gartnerin raportin mukaan vuosien 2006 ja 2007 välillä (Malwarebytes s.a.).

Vuoden 2013 syyskuussa kiristysohjelma ransomware levisi noin 250 000:n tietokoneeseen, hyökkäys oli ensimmäinen salaushaittaohjelmaa levittänyt tietojenkalasteluhyökkäys (phishing.org s.a.). Tämä kiristysohjelma salaa ja lukitsee vastaanottajan tietokoneen tiedostot ja vaatii vastaanottajalta lunnaita lukitsemisen avaamiseen. Hyökkäyksissä haittaohjelmaa levitettiin .zip tiedostossa sekä linkin välityksellä. Hyökkäyksiä levitettiin kahdessa erilaisessa sähköpostiviestissä, ensimmäinen oli kohdistettu yrityssähköposteihin, viestit sisälsivät väitetysti asiakasvalituksia. Toisenlainen viesti koski ongelmaa sekkien kanssa ja nämä olivat suunnattu yksityisiin sähköpostiosoitteisiin.

Sosiaalinen media on myös vaikuttanut suuresti kalasteluviesteihin. Suurin piirtein vuoden 2016 vaihteessa kyberrikolliset alkoivat käyttämään laajasti isoimpia sosiaalisen median alustoja hyödyksi hyökkäyksissä ja tiedonkeruussa. (Cyber Risk Aware s.a.) Näissä pitkälle kehitetyissä hyökkäyksissä kyberrikolliset alkoivat jäljitellä isojen brändien viestintätyylejä ja ulkoasuja omien kalasteluviestien teossa. Suosiossa oli hyökkäykset, jotka lähetettiin väärennetyiltä asiakaspalvelutileiltä ja sivustoilta. Hyökkäykset olivat todella kannattavia rikollisille, sillä ne olivat nopeita ja erittäin vaikea jäljittää pankkitileille pääsyä. Kannattavuutta edelsi myös kattava taustatietojen tiedustelu ennen hyökkäystä. Kohdennetut hyökkäykset ovat siitä lähtien ollut näkyvästi käytössä.

Saman vuoden lopussa tapahtui yksi tunnetuimmista tietojenkalasteluhyökkäyksistä, kun hakkerit pääsivät käsiksi Hilary Clintonin kampanjajohtajan John Podestan Gmail-tiliin. Hyökkäys oli toteutettu yhdellä vanhimmista taktiikoista tietojenkalastelussa, sähköpostiviestissä väitettiin hänen sähköpostinsa salasanan olevan vaarantunut (vaihda salasana). Tililtä olleita yksityisiä viestejä päätyi

lehdistölle sekä muille puolueille ja viestejä käytettiin sitten Clintonin kampanjaa vastaan (Cyber Risk Aware s.a.) Tässä on yksi merkittävimmistä esimerkeistä, kuinka suurta valtaa tietojenkalastelulla ja varastetuilla tiedoilla voi saada. Raha ei ole ainoa resurssi mitä hyökkäyksillä voi tavoitella.

Tietojenkalasteluviestit elävät muiden maailmassa tapahtuvien muutosten mukana. Siitä hyvänä esimerkkinä on vuonna 2020 levinnyt koronavirustauti (covid-19). Pandemiaan liittyvät tietojenkalasteluviestit alkoivat näkyä sähköposteissa erittäin runsaslukuisasti (phishing.org s.a.). Teemana viesteissä on nähty koronaan liittyen moninaisesti tarkastuksiin liittyen, etätyöskentelyyn kuin karanteenista poistumiseen liittyviä varoituksia. Tämän kaltaisia hyökkäyksiä, jotka vaikuttavat suurimpaan osaan ihmisistä on helppo käyttää hyväkseen sillä kohteita ei tarvitse sen enempää valikoida vaan hyökkäyksiä on voitu lähettää mihin tahansa osoitteisiin. Myös ajankohtaisella aiheella herätetään vastaanottajan mielenkiintoa avaamaan lähetetty viesti.

4 Erilaisia tietojenkalastelukäsitteitä ja -tekniikoita

Tietojenkalasteluviestejä on lukuisia erilaisia ja uusien teknologioiden, tietoturvan sekä mahdollisuuksien perässä myös hyökkäykset kehittyvät ja monipuolistuvat entisestään. Tässä luvussa käydään tutkimuksessa tarvittavia käsitteitä läpi sekä pureudutaan hieman syvemmin erilaisiin tekniikoihin, joita hyökkääjät käyttävät hyödyksi.

4.1 Käsitteitä (Cyber Risk Aware s.a. & Panda Security 2021)

Email phishing

- Tietojenkalasteluviestit, jotka ovat lähetetty massa kampanjoina mahdollisimman moneen eri sähköpostiosoitteeseen. Yksi suosituimmista tavoista lähettää kalasteluviesti.

Spear Phishing

- Keihäällä ilmaistaan sitä, että tämän tyyppisissä kalasteluviesteissä on keskitytty vain yhteen kohteeseen. Kalasteluviesti on räätälöity tarkasti vastaanottajasta saatujen tietojen mukaan. Yleisimpänä tapana viestit on muokattu näyttämään vastaanottajan yrityksen lähettämältä viestiltä.

Vishing

- Yleisesti tietojenkalastelutekniikka, joissa hyökkääjät soittavat kohteen puhelimeen. Hyökkääjä voi esittäytyä esimerkiksi ”IT-tukena” yrittäen saada vastaajan luottamuksen puolelleen ja näin saada henkilökohtaisia tietoja vastaanottajalta.

Whaling

- Myös kohdennettu hyökkäys, mutta hyökkäyksen kohteena on henkilö, joka on tärkeässä roolissa yrityksessä (esim. CEO, CFO). Korkean tason johtajilla on pääsy kaikista arkaluontoisimpiin tietoihin, joka houkuttelee hyökkääjiä.

Business Email Compromise

- Hyökkäys on lähetetty oikealta yrityssähköpostilta. Kyberrikolliset käyttävät jo kaapattua tiliä muiden hyökkäysten tekemiseen, tekee hyökkäyksen tunnistamisen erittäin vaikeaksi. Toimii parhaiten yrityksen sisällä tehdyissä hyökkäyksissä.

Smishing

- Tietojenkalasteluviestejä, joita lähetetään tekstiviestillä kohteiden puhelimiin. Yleensä samantapaisia kuin sähköpostit ja sisältävät esimerkiksi haitallisen linkin.

Catphishing

- Näissä hyökkäyksissä hyökkääjä yrittää luoda henkilökohtaista suhdetta uhrin kanssa. Hyökkääjä käyttää luottamusta hyväkseen saadakseen haluamansa. Rakkauskirjeet ja deittailusovelluksissa tapahtuvat hyökkäykset ovat näistä tunnetuimpia.

Angler phishing

- Hyökkääjä käyttää sosiaalisen median sovelluksien ilmoitus- tai suoraviestitoimintoja hyökkäyksen toteuttamiseen.

Landing Page

- Hyökkääjän pystyttämä huijaus verkkosivusto. Eli laskeutumissivu, jolle uhri ohjataan sen jälkeen, kun hän on painanut kalastusviesteissä olevia linkkejä.

Malware

- Laitteelle asentuva haittaohjelma. Haittaohjelma on ladattava dokumentti, niitä voi löytyä kalasteluviestien linkeistä tai liitetyistä tiedostoista. Vakoiluohjelmat ovat yleisiä, ohjelmat tallentavat esimerkiksi viestin avaajan näppäin painalluksia. Ohjelmat voivat olla myös aggressiivisempia ja esimerkiksi ajaa alas uhrin koko verkon.

Ransomware

- Haittaohjelma, joka uhkaa lukita tai poistavan uhrin tiedostoja tai henkilökohtaisia tietoja salauksella, jos uhri ei maksa tiettyä summaa hyökkääjälle. kiristysohjelmahyökkäykset ovat kohdistuneet yhä useammin sairaaloihin, kunnallisiin viranomaisiin ja sähkölaitoksiin, mikä on lisännyt niiden vaikutusvaltaa uhkaamalla laajalle levinneitä häiriöitä.

Session Hijacking

- Uhrin istunnon kaappaaminen. Haitallinen tiedosto voi avata hyökkääjälle pääsyn uhrin sen hetkiseen istuntoon digitaalisella laitteella.

Nigerialaiskirjeet

- Näiden hyökkäysten onnistumisprosentti on verrattavissa pieni hurjiin lähetysmääriin verrattuna, mutta kun viestejä lähetetään paljon joka päivä, niin auttamatta kalastusviestien uhreja syntyy. Todella yleisiä, yleensä viesteissä uhria pyydetään auttamaan rahansiirrossa tai uskotellaan jotain todella hyvältä kuulostavaa liiketoimintaa.

4.2 Tekniikoita

HTTPS-protokolla on jo pitkään ollut verkkosivustojen apuna turvaten käyttäjän ja verkkosivuston välisen liikenteen. Vuodesta 2017 lähtien (phishing.org s.a.), ovat myös tietojenkalastelijat alkaneet käyttää tätä protokollaa hyödykseen myös omissa verkkosivustoissaan. Tämä antaa usein sivustolla kävijöille vääränlaista turvallisuuden tunnetta, sillä vaikka sivuston ja selaimen käyttäjän välinen liikenne on turvattu se ei kuitenkaan hirveästi hyödytä käyttäjää, kun sivuston omistaa hakkeroija itse. Tämänkaltaisia turvallisuuden tunnetta nostavia pieniä tekniikoita, näkyy useasti tietojenkalasteluviesteissä. Toisena suosittuna esille nousee varoituskyltit. Moni sähköpostipalvelin lisää näitä kylttejä viestien yläpuolelle varoituksena epäluotettavasta lähettäjästä. Hyökkäyksissä kyltit useasti ilmoittavat, että viesti on tullut luotettavalta lähettäjältä, vaikka todellisuus on kaikkea muuta. Näin hyökkääjät käyttävät erilaisia turvallisuuskeinoja omaksi edukseen.

Miten hyökkäykset ohittavat sitten roskapostisuodattimia ja liitteiden skannaustyökaluja? Hyökkääjillä on olemassa useita tekniikoita näiden hämäämiseksi. Yleisin tapa on sähköpostin lähettämistietojen väärentäminen (engl. spoofing). Hyökkääjät väärentävät viestit näyttämään kuin ne lähtisivät luotettavalta lähettäjältä muokkaamalla verkkotunnusta, tämänkaltaiset identiteettivarkaudet ovat toimiva keino saamaan vastaanottajan luottamuksen. Haitallisia linkkejä hyökkääjät naamioivat kahteen osaan tai käyttävät linkin lyhennys palveluita, joita löytyy useita ilmaisia internetistä. Samantapaisia keinoja rikolliset käyttävät avainsanoja tunnistavia skannaustyökaluja vastaan, viestit voidaan olla piilotettu esimerkiksi kuvan sisälle, jolloin skannaus tunnistaa vain kuvan eikä sen sisällä olevia sanoja. Harvinaisemmin nähtynä keinona hyökkäyksissä maalataan osa tekstistä valkoiseksi, valkoisella pohjalla tekstiä ei näyttäisi olevan edes olemassa (LIFARS 2021). Haitalliset tiedostot ovat onneksi myös tarkasti skannattu läpi ja usein ne tarttuvatkin roskapostisuodattimiin. Hyökkääjillä on tekniikoita myös tähän, useasti näkyy puheposteja tai vastaajaviestejä (engl. vishing) nykyään myös sähköpostissa (phishing s.a.). Ne useasti sisältävät oikean vastaajaviestin, mutta viestien oheen on liitettynä toinen väärennetty tiedosto esimerkiksi ”voicemailmth.mp3”. Tiedosto vaikuttaa äänitiedostolta, mutta todellisuudessa kyseessä on .htm -tiedosto (verkkosivu) jonka tiedostonimi on vain käännetty oikealta vasemmalle vakuuttamaan vastaanottaja sekä roskapostisuodattimet sen turvallisuudesta (Krebs on Security 2011).

Sähköposti ja puhelinten viestintäsovellukset ovat suosituimpia tietojenkalastelualustoja, hyökkääjillä on kuitenkin muitakin keinoja uhrien tavoittelemiseen Hakukoneiden tietojenkalastelu (engl. search engine phishing) on sitä, kun hakkerit upottavat omia verkkosivujaan hakukoneiden tuloksiin. Miksi tämä toimii? Kun käyttäjä näkee sivuston Googlen hakutulossivun toisena tuloksena, luo tämä automaattisesti tunteen käyttäjälle siitä, että sivusto on luotettava. Sivustoilla voi olla erittäin

hyviä tarjouksia verkkokaupan muodossa. Hyökkääjät keräävät käyttäjältä pankki- tai henkilötietoja niiltä henkilöiltä, jotka tarttuvat houkutukseen (Panda Security 2021).

Miten hyökkääjät keräävät rahoja onnistuneista hyökkäyksistä? Tietojenkalasteluhyökkäyksissä rahansiirtovälineinä hyökkääjät käyttävät usein lahjakortteja ja kryptovaluuttoja. Hyökkääjät suosivat näitä valuutanvaihto tekniikoita sillä niitä ei voida jäljittää eikä niiden lunastaminen vaadi henkilötietojen syöttämistä. Rikolliset käyttävät paljon käteistä ja nämä maksutavat ovat kuin verkkoalustojen käteinen: nopeita, liki mahdotonta peruuttaa kauppa sekä vaikea liittää keneenkään henkilöön. (Delta Community Credit Union 2021)

Tekniikoita on paljon ja ne kehittyvät koko ajan entistä ovelimmiksi. Välillä vanhat tekniikat nousevat taas yleisempään käyttöön, kun uudempiin hyökkäystekniikoihin on varauduttu paremmin. Tämä on todellista kissa ja hiiri leikkiä tietoturvan ja hyökkäysten välillä. Onko mahdollista, että nämä kaikki hyökkäyskeinot pystytään pysäyttämään tulevaisuudessa? Näitä skenaarioita tutkimme empiirisessä osassa.

5 Käyttäjän manipulointi (Social engineering)

Useasti kuvitellaan, että hyökkäyksissä hyödynnetään vain tietoverkkojen ja teknologian heikkouksia, mutta erittäin useasti heikko kohta on ihminen ja melkein jokainen hyökkäys sisältää jollain tapaa sosiaalista manipulointia. 85 % tietomurroista sisälsi inhimillisen elementin vuonna 2021 (Phishingbox 2021). Sosiaalisella manipuloinnilla tarkoitetaan haitallisia toimintoja ja tekoja, jotka toteutetaan vuorovaikuttamalla ihmisiin. Tällä psykologisella keinolla huijataan ihmisiä antamaan arkaluonteisia tietoja tai päästään jopa käsiksi uhrin tietoverkkoon. Tämä tekniikka on siis äärimmäisen isossa roolissa suurimmassa osassa tietojenkalasteluhyökkäyksissä nykypäivänä, sillä se perustuu täysin käyttäjien tekemiin virheisiin, jonka johdosta hyökkäyksiä on myös paljon vaikeampi ennustaa.

Huijaukset perustuvat ihmisten ajatusten ja toiminnan ympärille. Hyökkääjät suunnittelevat hyökkäykset miettien kohteiden motivaatioita, miten manipuloida käyttäjä toimimaan hyökkääjän haluamalla tavalla.

5.1 Miten hyökkäykset toimivat käytännössä

Hyökkäykset tapahtuvat muutamassa eri vaiheissa. Yleensä perustuen todelliseen viestintään hyökkääjän sekä kohteen välillä. Ensimmäinen vaihe on yleensä tiedustelu, hyökkääjät keräävät tietoja kohteesta tai kohteista, jotta luottamuksen rakentaminen ja soluttautuminen on mahdollista. Toinen vaihe perustuu luottamuksen hyödyntämiseen, hyökkäys ei ole mahdollista ennen kuin kohde uskoo lähettäjään ja hänen pyytämiin toimiin. Viimeisenä vaiheena kun on saatu kohde toimimaan halutulla tavalla, on irtautuminen viestinnästä. Hyökkääjä haluaa pyyhkiä kaikki jäljet ja asiat, jotka voivat yhdistää rikolliseen. Nämä kaikki vaiheet voivat toteutua yhdessä keskustelutuokiossa tai keskustelua on voitu käydä uhrin ja hyökkääjän välillä jo useita kuukausia.

5.2 Ihmisten heikkoudet (Kaspersky s.a.)

Käyttäjien tietämättömyys on monissa hyökkäyksissä avainasemassa. Teknologian nopean kehittymisen takia monet käyttäjät eivät ole täysin perillä asioista. Hyökkääjät voivat hyödyntää tätä pyytämällä uhria lataamaan jotain tietoturvapäivityksiä, vaikka todellisuudessa ohjelma on haittaohjelma. Monet eivät myöskään ymmärrä tietojensa arvoa. Esimerkiksi jos uhri päätyy antamaan puhelinnumeronsa tietojenkalastelijalle, kasvaa häneen kohdistuva tekstiviesti- sekä puheluhyökkäyksien riski huomattavasti.

Uhrin kohonneet tunteet ovat useasti hyödynnetty näissä hyökkäyksissä. Käyttäjä on paljon riskialttiimpi toimimaan viestin haluamalla tavalla, kun tunteet nousevat järjen edelle. Hyökkäyksissä useasti halutaan nostaa tunteita kuten pelkoa, uteliaisuutta, vihaa, syyllisyyttä ja surullisuutta. Kiireellisyys on kanssa keino, jolla käyttäjä pyritään saamaan tekemään hätiköityjä ratkaisuja. Esimerkiksi tarjous on voimassa vain tämän kerran tai käyttäjällä on vain 2 päivää aikaa vaihtaa käyttäjän salasana tai muuten käyttäjä poistetaan kokonaan käytöstä.

5.3 Erityisiä hyökkäysmenetelmiä

Fyysiset tietomurtohyökkäykset omaavat yleensä erittäin suuren riskin hyökkääjälle, mutta sen myötä palkkiot ovat myös riskin arvoisia. Hyökkääjät esiintyvät henkilökohtaisesti kohteen kanssa tavoitteena pääsy luvattomille alueille tai tietoihin käsiksi. Teeskennellen luotettavaa edustajaa tai pelaten hämmentävän sosiaalisen tilanteen hyökkääjän pussiin. Esimerkiksi kohde avaa oven hyökkääjälle tai käyttää tietokoneessa hyökkääjän tarjoamaa USB-tikkua tai Cd-levyä, tämän kautta hyökkääjä saa pääsyn järjestelmään ja lukuisat eri keinot tavoitteen saavuttamiseen ovat auki. (Kaspersky s.a.)

Vaihtokauppa tai palvelus palveluksesta on myös nähty lähestymistapa. Kohde innostuu jostakin arvokkaasta, joka on saavutettavissa pienellä vastapalveluksella. Todellisuudessa kohde ei saa mitään palkkiota ja vain hyökkääjä jää voitolle vaihtokaupasta. Kohteita on myös pyydetty asentamaan oman yrityksen järjestelmiin kiristysohjelmia, josta käyttäjä saisi vaihtokauppana suuren summan rahaa itselleen.

Pelko on useasti hyökkääjien hyödyntämä tunnetila. Tästä tunnetaan niin sanotut ”scareware” hyökkäykset. Scareware on haittaohjelma, jota käytetään uhrin pelotteluun ja pakottamalla toimimaan (Imperva s.a.). Hyökkäyksissä ilmoitetaan kohteelle väärennetyistä haittaohjelmatartunnoista tai väitetään käyttäjän tilin olevan vaarantunut. Pelko voi saada kohteen toimimaan harkitsemattomasti, toivoen että tilanne saataisiin mahdollisimman nopeasti rauhoitettua.

Monissa sosiaalista manipulointia hyödyntävissä hyökkäyksissä on jokin ennalta lavastettu tilanne tai viestin lisänä vanha kaapattu viestiketju kohteen kanssa. Hyökkääjä toimii tämänkaltaisissa lavastetuissa hyökkäyksissä (engl. pretexting) jo ennalta tunnettuna toisena osapuolena. Kun kohde huomaa vanhan viestiketjun välitettynä viestissä tai aikaisemmin aiheena olleen tilanteen niin hyvin harvoin epäilykset viestin tai toisen osapuolen luotettavuudesta nousevat esille. Esimerkiksi IT-tukihenkilöksi tekeytynyt hyökkääjä voi pyytää käyttäjiltä tunnuksia ja salasanoja. Monesti käyttäjät luovuttavat tietoja, kun pyyntö tulee turvallisen oloiselta taholta (Imperva s.a.).

6 Suojautuminen tietojenkalastelulta

Tietojenkalasteluviestejä on monenlaisia ja käyttäjille voi olla todella vaikeaa tunnistaa mikä viesti on turvallista avata sekä mikä ei. Suurin osa kalastusviesteistä menee suoraan roskapostiin sähköpostien kehittyneiden suodattimien ansiosta, mutta eivät valitettavasti kaikki. Valitettavasti myös tietojenkalasteluviestit eivät tule loppumaan, joka päivä useiden ihmisten sähköpostitilit ovat kohteina hyökkäyksille. Ainakaan vielä ei ole keksitty täysin varmaa suojaa hyökkäyksiltä, kuitenkin viesteissä on tiettyjä piirteitä, jotka auttavat käyttäjiä tunnistamaan sekä suojautumaan tietojenkalasteluviesteiltä

6.1 Toiminta viestiä avatessa

Välillä viestit pääsevät roskapostisuodattimien läpi suoraan saapuneet-kansioon ja silloin todennäköisyydet, että vastaanottaja avaa lähetetyn viestin kasvavat huomattavasti. Ensimmäiseksi viestiä tarkasteltaessa on hyvä käydä läpi viestin otsikko, kun otsikko ei anna viitteitä mistään tutusta tai odotetusta viestistä on jo hyvä pohtia, onko viestin avaaminen välttämätöntä. Alustalla mistä viesti lähetetään ei ole kovinkaan suurta vaikutusta viestiin reagoinnissa, sillä hyökkääjät käyttävät samoja tekniikoita alustasta riippumatta. Kyberrikollisten tavoite tietojenkalasteluviesteillä on saada vastaanottaja avaamaan linkin tai liitteen, mutta myös viestiin vastaaminen antaa jo hyökkääjille paljon mahdollisuuksia. Yleisesti tärkeimpänä asiana on pysyä rauhallisena, hyökkääjät pyrkivät herättämään vastaanottajassa tunteita sosiaalisella manipuloinnilla, jotta uhri toimisi harkitsemattomasti eli toimisi viestiä kohtaan ennen kuin uhri edes ajattelee mahdollisia riskejä. Tärkeintä on siis miettiä mahdollisia riskejä rauhassa, ennen vuorovaikutusta viestien kanssa (Kaspersky s.a.). Näitä epäilyksiä voi nousta jo miettiessä mitä tunteita viesti itsessään herättää, onko viestin luoma tilanne millään tapaa edes realistinen. Nämä tunteet voivat nousta pintaan, kun lähettäjä tarjoaa uhrille jotain, mikä on liian hyvää ollakseen totta tai viestistä tulee selvästi hyvin kiireisen tapauksen tuntuinen, silloin on hyvä kysyä neuvoja esimerkiksi IT-tuesta tai muulta apuhenkilöltä kasvotusten tai toisessa viestintä sovelluksessa. Varsinkin jos viestissä pyydetään antamaan henkilökohtaisia tietoja, on tärkeä varmistaa viestin turvallisuus ennen kuin toimii.

6.2 Teknillinen puoli ja kalasteluviestien tunnistaminen

Jotta kalasteluviestejä pystyttäisiin tunnistamaan, on hyvä tietää tarkemmin teknillisiä puolia sekä näkökulmia viestejä kohtaan, jotka auttavat paljastamaan haitalliset viestit. Tärkeä tunnistamisen keino on ensimmäiseksi tutkia viestin yleiskuvaa ja miettiä piirteitä kuten sisältääkö viesti sisällössään paljon kirjoitusvirheitä, onko viestin rakenne ja kuva ammattimaisia sillä varsinkin yrityksistä lähtevät oikeat viestit ovat yleisesti erittäin tarkasti ja laadukkaasti tehtyjä. Jos lähettäjä tervehtii viestissä vain yleisesti eli ei käytä vastaanottajan nimeä, vaikka lähettäjän pitäisi nimi tietää on

suuri mahdollisuus, että sama viesti on lähetetty useille vastaanottajille. Vastaanottajan tulisi pysyä erittäin varovaisena avattaessa viestiä sellaisessa tilanteessa, jossa lähettäjän osoite on hänelle tuntematon, eikä hän ole odottanut saavansa kyseistä viestiä. Valitettavasti nämäkään asiat eivät yksinomaan paljasta sitä onko viesti haitallinen. Kohdistetut hyökkäykset voivat olla muotoiltu niin tarkasti, että viesti näyttää aidolta ja siltä, että se on tullut tutulta lähettäjältä ja tarkoitettu nimenomaan vastaanottajalle. Edellä mainittujen piirteiden tarkastelu viesteistä nostaa kuitenkin huomattavasti turvallisuutta ja suojaa yleisiltä hyökkäysviesteiltä. Hyökkäyksissä hyökkääjät käyttävät myös hyödyksi verkkotunnuksia, jotka ovat lähes samannäköisiä yritysten käyttämien oikeiden verkkotunnuksien kanssa sisältäen kuitenkin pieniä kirjoitusmerkkejä esimerkiksi ”micros0ft” (Microsoft s.a.). Jos vastaanottaja vilkaisee vain nopeasti verkkotunnusta, on todella vaikea huomata pieniä muutoksia lähettäjän osoitteessa. Yleisin tapa miten hyökkääjät jakavat haittaohjelmia on linkit. Tärkeä tekniikka linkkien tarkastelemiseen on hiiren pitäminen linkkien päällä ennen linkin klikkaamista ja tarkastella osoitetta ja sen määränpäätä ennen kuin suuntaa kyseiselle sivustolle, jos linkin osoite ei yhdisty millään tavalla lähettäjään on erittäin mahdollista, että kyseessä on haitallinen linkki. Nämä haitalliset linkit vievät hyökkääjien luomille kalastussivustoille, jotka ovat yleensä pystytetty varsin nopealla aikataululla ja siten hyvin vaatimattoman näköisiä. Ne voidaan tunnistaa URL-osoitteesta erityisesti, jos linkki on lyhennetty tai muuten ei näytä yhdistyvän lähettäjään suurella todennäköisyydellä osoite johtaa haitalliselle sivustolle (Microsoft 2021). Haitallisten sivustojen ero virallisiin verkkosivuihin on suoraviivaisuus, sillä tietojenkalastelusivustot useasti kysyvät heti sivustolle saapuessa jo arkaluonteisia tietoja käyttäjästä. Rauhallisuus on hyvä ominaisuus myös haitallisten sivustojen tunnistamiseen aina kun saapuu verkkosivustolle, jossa ei ole aikaisemmin käynyt.

6.3 Hyökkäysten estäminen

Maalaisjärjellä sekä omalla kiinnostuksella torjua kyberuhkia saadaan jo hyvä pohja hyökkäysten estämiseksi, mutta mitä tämä käytännössä tarkoittaa? Torjuakseen tietojenkalasteluviestejä on hyvä pysyä ajan tasalla sen hetkisistä trendeistä myös hyökkäyksissä, tämä ei kuitenkaan vaadi sitä, että tarvitsisi lukea päivittäin uusimmat uutisartikkelit lävitse. Hyökkäyksissä useasti käytetään hyödyksi tärkeänä virastona esiintymistä. Useimmat yrityksistä kuten pankit, vakuutusyhtiöt ja muut virastot eivät pyydä henkilökohtaisia tietoja sähköpostitse, mutta se on kuitenkin mahdollista. Tämänlaisissa tilanteissa saadessa viralliselta taholta viestin, ei tarvitse viestiä avata sähköpostista, vaan voit siirtyä lähettäjän virallisten verkkosivujen kautta tarkastamaan omat tapahtumat tai suoraan soittaa viralliselle taholle varmistaakseen viestin aitouden (Kaspersky s.a.). Tämä lähestymistapa toimii myös yksittäisiltä henkilöiltä saaduissa viesteissä. Se on jo iso suoja, kun vastaanottaja ei toimi välittömästi vaan ottaa oman aikansa vastaanotetun viestin kanssa.

Oman yksityisen sähköpostitilin käyttäminen tilitietoina työn ulkopuolisissa sovelluksissa ja palveluissa vähentää ja pienentää huomattavasti riskiä vaarantaa koko työympäristö. Sähköpostia on huomattavasti vaikeampi kohdentaa myös hyökkäyksissä, jos sähköpostitilejä ei ole jaettu julkiseen tietoon esimerkiksi erilaisissa sosiaalisen median palveluissa. Jos tuntemattomat lähettäjät löytävät yksityisen tilin eli kun käyttäjä on vastannut roskapostiin, on silloin hyvä vaihtaa sähköpostitilin nimeä nopeasti. Näin on mahdollista välttyä suurelta määrältä roskaposteja sekä hyökkäyksiltä, sillä useasti lähettäjät vahvistavat ja kirjaavat ylös vastaanottajat, jotka vastaavat ja tekevät heistä näin tärkeämmän prioriteetin (Kaspersky s.a.)

Tärkeitä ulkopuolisia työkaluja on paljon, mutta niistä ei ole mitään hyötyä, jos ohjelmistoja ei pidetä ajan tasalla. Hyökkääjät löytävät uusia tietoturva-aukkoja verkkoselaimista ja ohjelmista jatkuvasti, varsinkin Windowsin tuotteet ovat yleisesti kohteita tietojenkalasteluviesteissä, joten on tärkeä pitää ohjelmat turvallisina ja päivitettyinä. Tärkeimmät työkalut, jotka nostavat turvallisuuden tasoa huomattavasti ovat roskapostisuodatin, virustorjuntaohjelma, palomuuri ja VPN-yhteys. Palomuurit sekä virustorjuntaohjelmat skannaavat jokaisen tiedoston, jotka liikkuvat internetistä käyttäjän laitteelle ja näin toimivat viimeisenä lukkona estäen haitallisten tiedostojen leviämisen (Phishing, s.a.). VPN-yhteydellä on mahdollista salata oma verkkoliikenne ja näin estää hyökkääjien yritykset siepata liikennettä tai jäljittää liikennettä käyttäjään. Sähköpostipalveluntarjoajat ovat ja kehittävät jatkuvasti omia alustojaan hyökkääjiä vastaan. Palveluiden suodattimet nykypäivänä pystyvät jo todentamaan yleisesti tunnettuja haitallisia URL-osoitteita sekä liitteinä lähetettyjä tiedostoja ja näin laskemaan huomattavasti saapuvan haitallisen materiaalin määrää. Microsoft kertoo raportissaan vuodelta 2020 estäneensä vuonna 2019 yli 13 miljardia haitallista ja epäilyttävää sähköpostiviestiä (Microsoft 2020). Sähköpostipalvelut voivat myös sisältää raportointipainikkeen, sen avulla sähköpostipalvelimilla käyttäjät voivat lähettää sähköpostiviestejä tarkistettavaksi eteenpäin, jos epäilee viestin turvallisuutta. Monet ulkopuoliset palvelut nykypäivänä tuottavat myös simulaatioita eli harjoitusviestejä, jotka vaikuttavat todentuntuisilta kalastusviesteiltä. Näiden avulla vastaanottajat voivat harjoitella tunnistamaan haitallisia viestejä, harjoitukset voivat yleisesti myös nostaa käyttäjien mielenkiintoa kyberturvallisuutta kohtaa. Googlella on ilmainen ohjelmisto: ”Phishing Quiz”, jonka avulla voi testata omaa osaamistaan.

Jos hyökkääjät saavat käyttäjän salasanan, todennäköisesti hyökkääjä yrittää päästä samalla salasanalla eri palveluihin ja tileihin käsiksi. Siksi on tärkeätä käyttää monimutkikkaita ja eri salasanoja eri palveluissa useiden hyökkäysten estämiseksi. Tässä apukeinoina toimivat salasananhallintaohjelmat, jotka hyödyttävät paljon laatiessa useita salasanoja monille eri palveluille. Niiden avulla salasanat pysyvät aina muistissa. Lisä suojaustasona voidaan pitää kaksivaiheista tunnistautumista, joka torjuu hyökkääjät, joilla on pääsy salasanaan varmistamalla henkilöllisyyden kirjautuessa myös toisella tavalla kuten sormenjälkitunnistuksella (Kaspersky s.a.). Sillä pystytään viimeisenä

suojana estämään hyökkääjien tunkeutumiset käyttäjien tileille, tämä palvelu on mahdollista ottaa käyttöön useissa palveluissa nykypäivänä.

Nykyään hyökkääjät käyttävät usein hyödyksi haitallisia kiristysohjelmia (engl. ransomware), joissa hyökkääjät panttaavat uhrien tärkeitä tiedostoja siihen saakka, kunnes lunnaat on maksettu. Näiden tehoa hyökkäyksissä on mahdollista vähentää huomattavasti varmuuskopioimalla tiedostoja säännöllisesti (SecurityScorecard 2021).

Mitä tehdä, jos on joutunut onnistuneen hyökkäyksen uhriksi? Tärkeintä on toimia mahdollisimman nopeasti ja ottaa mahdollisimman paljon tietoja ylös viestin lähettäjästä, osoitteesta sekä toiminnasta mikä johti hyökkäykseen. Tämän jälkeen salasanojen vaihto kaikissa palveluissa, joissa sama salasana on ollut käytössä, sillä useasti rikolliset yrittävät päästä tileille sisään monissa eri palveluissa kuten aikaisemmin mainittiin. Ilmoitus eteenpäin hyökkäyksestä IT-tukihenkilölle, jos tili on yhteydessä organisaatioon välttääkseen isommat konfliktit ja turvaten muiden organisaation sisäiset käyttäjätilit. Jos uhri on menettänyt rahaa tai joutunut identiteettivarkauden uhriksi on syytä ilmoittaa hyökkäyksestä lainvalvontaviranomaisille (Microsoft s.a.).

7 Tietojenkalasteluviestien kehitys tilastoina ja suojautuminen

7.1 Tutkimusmenetelmät

Tutkimusmenetelmänä käytän tässä opinnäytetyössä kvantitatiivista tutkimusta (määrällinen) sekä kvalitatiivista tutkimusta (laadullinen). Pidän näitä molempia menetelmiä hyödyllisenä arvioidessani tietojenkalasteluviestien kehitystä. Tilastot kattavat faktat lähetetyistä kalasteluviesteistä ja niiden määristä, mutta nämä tilastot ovat jo olemassa. Ovatko ihmiset yleisesti huomanneet tätä kehitystä? Haastattelulla pystymme todentamaan tilastot sekä muutokset satunnaisten ihmisten kokemuksilla sekä muuttuvilla asenteilla. Tutkimuksessa siis haluan selvittää tarkemmin syitä miksi jotkut hyökkäystekniikat ovat toimivampia kuin toiset eli tietojenkalasteluviestien kehitystä, mikä on vaikuttanut hyökkääjien ajattelutavan muutoksiin, johtuuko kehitys esimerkiksi paremmin suojautuvista kohteista?

Tämän saavuttamiseksi on mielestäni tärkeää vertailla erilaisia olemassa olevia tilastoja, keräämällä faktoja sekä lukuja ylös on mahdollista luoda kokonaiskuva viestien kehityksestä. Nämä tilastot toimivat strukturoidun kyselyn tukena, jotta pystyn tekemään tärkeitä johtopäätöksiä tässä opinnäytetyössä. Onneksi on jo olemassa lähteitä tarvittaville tilastoille, sillä tiedonkeruu perustuen vain minun keräämien tietojenkalasteluviestien perusteella ei antaisi tarpeeksi tarkkaa kuvaa kehityksestä. Siksi käytän vertailutuloksiin lähteinä jo olemassa olevia tilastoja APWG:n (Anti-Phishing Working Group) kalasteluviestien hyökkäystrendejä koskevia raportteja sekä FBI:n Internet Complaint Centerin (IC3) tarjoamia julkisia raportteja. APWG on kansainvälinen liittouma, joka luo globaalin vastauksen tietoverkkorikollisuuteen teollisuuden, hallituksen sekä lainvalvontasektorin välillä (APWG, s. a.). IC3 taas tarjoaa pääasiassa amerikkalaisille suoran kanavan ilmoittaa kansalaisiin kohdistuneista kyberrikoksista (IC3, 2021). Nämä julkiset raportit ovat erittäin arvokkaita tutkimuksessa ja yleisesti tämänkaltaiset raportit auttavat estämään rikoksia sekä jakamaan näkemyksiä kehittyvistä uhista. Raportoinnit keskittyvät yritysmaailmassa tapahtuneisiin tietojenkalastelu-hyökkäyksiin sekä myös tavallisten kansalaisten ilmoittamien uhkien ympärille. Vuosittaisten tilastotietojen avulla pystyn arvioimaan mihin suuntaan kehitys on menossa tietojenkalasteluviestien osalta. Näissä raporteissa on analysoitu dataa 200 000–900 000 yksittäisen raportoidun uhkatapahtuman laajuudelta riippuen raportista. Varsinkin vanhemmissa raporteissa oli selvästi vähemmän dataa, johtuen heikommasta tiedonkeruusta sekä matalammista uhkien ilmoitus määristä. Näin suurella otannalla pystymme luomaan realistisen kuvan yleisestä tietojenkalasteluviestien kehityksestä. Saavuttaakseni tiedot hyökkäysten muutoksista viimeisten viiden vuoden aikana tutkin siis vain vuosien 2016 sekä 2021 välisiä raportteja.

Lisäksi tarvitsen syvemmän katselmuksen ihmisten mielipiteitä, asenteesta tietojenkalasteluviesti-hyökkäyksiin ja kokemuksia. Tilastoja ja ihmisten kokemuksia vertaillen voidaan luoda laajempi yhteenveto tietojenkalasteluviestien kehityksestä. Onko heidän mielestään näkynyt huomattavia muutoksia kalasteluviestien edistymisessä viimeisen 5 vuoden aikana ja miten he uskovat hyökkäyksien muuttuvan tulevaisuudessa. Apuna käytän mielipiteiden keräämiseen strukturoitua haastattelua, Google Forms -lomaketta, jonka lähetän 15 ihmiselle, joilla on eri tasoisia lähtöpisteitä kyselyyn. Muutamilla henkilöillä, joille lomake lähetetään on jo tietoturvaan liittyvää kokemusta sekä taustaa ja taas osalla ei ole syvempää tietoturvaan liittyvää osaamista. Tämän avulla saadaan kohderyhmä kohdennettua erilaisten ihmisten näkökulmiksi. Tietojenkalasteluviestejä lähetetään myös satunnaisesti päivittäin kaikille ihmisille ja kuka vaan meistä voi joutua tietojenkalasteluviestien kohteeksi. Kyselyyn vastataan nimettömänä ja sen tekemiseen menee noin 3–5 minuuttia. Huomioiden vastaajien tietopohjia kysymyksien ohelle on annettu selkeitä esimerkkejä kysymyksiin vastaamisen avuksi.

Alla on esiteltynä haastattelulomakkeen rakenne:

1. Oletko huomannut jotain tiettyjä muutoksia saamissasi tietojenkalasteluviesteissä viimeisen 5 vuoden aikana? Esimerkkejä muutoksista: Olen vastaanottanut enemmän kalasteluviestejä, kalasteluviestit ovat siirtyneet eri alustalle (tekstiviestit, sähköposti, sosiaalinen media), kalasteluviestit ovat luovempia/paremmin tehtyjä.
   Kuvaile huomaamiasi muutoksia vastauskenttään.

2. Oletko ollut lähellä joutua/joutunut tietojenkalasteluviestin uhriksi? Minkälainen viesti oli ja miksi se oli vakuuttava?
   Kirjoita avoin vastaus vastauskenttään.

3. Oletko muuttanut omaa asennettasi/suojautumistasi tietojenkalasteluviesteihin liittyen viimeisen 5 vuoden aikana? Jos olet niin millä tavoin?
   Kirjoita avoin vastaus vastauskenttään.

4. Tulevatko tietojenkalasteluviestit olemaan mielestäsi vaarallisempia tulevaisuudessa? Arvioi numeroin 1–5
   (1 = Paljon vaarattomampia 3 = Ei muutosta 5 = Paljon vaarallisempia)

5. Edelliseen kysymykseen viitaten syitä omalle arviolle – Avoin vastaus.

8 Tuloksien esittäminen

8.1 Toteutus

Kappaleessa käsittelen jo olemassa olevia tilastoja sekä haastattelutuloksia, jotta on mahdollista saada mahdollisimman luotettava ja monipuolinen kuva tietojenkalasteluviestien kehityksestä sekä suojautumisesta. Tilastovertailun kohdistin tilastoihin, jotka ovat hyödyllisiä tutkimuksemme arvion kannalta, ja joiden vertailuun löytyy tarpeeksi tietoa vuosien 2016 sekä 2021 väliltä. Tietojenkalasteluviestejä lähetetään miljoonia päivittäin ja tilastoja löytyy erittäin paljon, mutta pidin tärkeänä keskittymisen siihen dataan mikä on olennaista tutkimuksen kannalta ja rajata tilastoja arvokkaisiin tuloksiin. Kaikkia raporttien olemassa olevia tilastoja ei ole siis tuotu tutkimuksessa esille, eikä se olisi tuonut tutkimukselle lisäarvoa. Kappaleen lopussa käsittelen yhteenvetona kaikkia saatuja tuloksia sekä arvioin niiden vaikutusta tietojenkalasteluviestien kehitykseen ja suojautumiseen havaintomatriisin avulla.

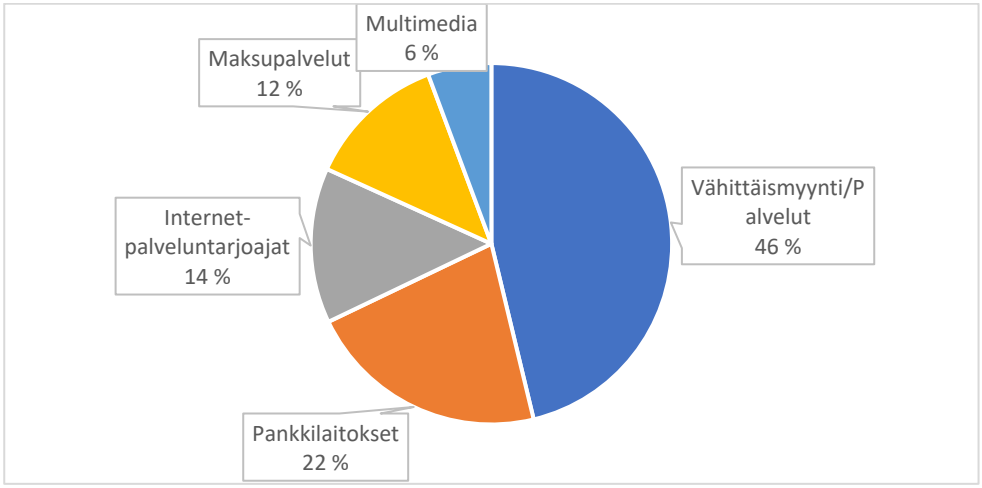
8.1.1 Tilastovertailu

APWG on kansainvälinen liittouma, joka luo globaalin vastauksen tietoverkkorikollisuuteen teollisuuden, hallituksen sekä lainvalvontasektorin välillä (APWG, s. a.). Alla olevat tilastot ovat kerätty APWG:n vuosien 2016–2021 Q4 raporteista. Tilastoiden lähteenä toimivat APWG:n jäsenyritysten jäsenten raportoimat viestit sekä julkisen yleisön ilmoittamat tietojenkalasteluviestit yritysmaailmassa. Tilastoissa vaihtelevat tilastoidut vuodet riippuen saatavilla olevasta aineistosta sekä niiden merkityksellisyydestä tilastojen vertailussa.

Kuva 1. Havaittujen yksittäisten tietojenkalastelusivustojen määrä vuosilta 2016–2021 (mukaillen APWG, 2016, 2017, 2018, 2019, 2020, 2021)

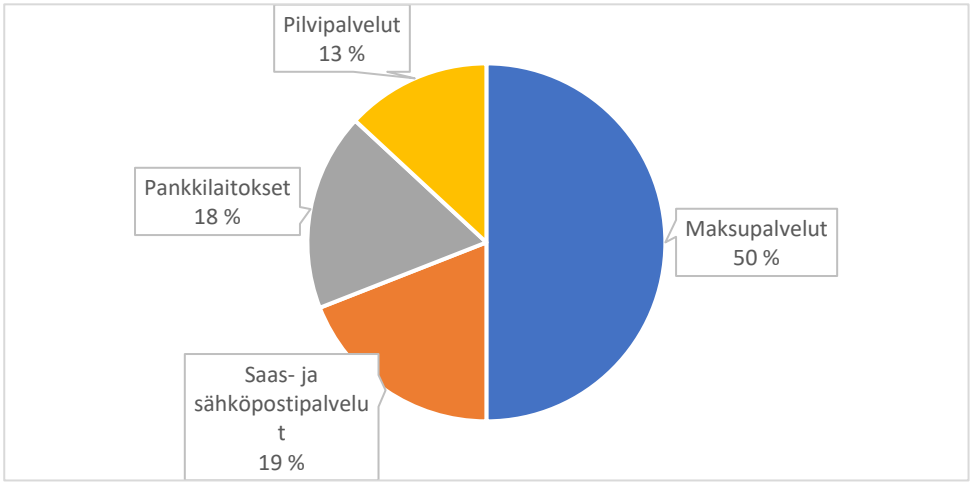
APWG:n näkemät 316,747 huijaussivustoa vuoden 2021 viimeisellä vuosineljänneksellä oli korkein kokonaismäärä heidän historiassaan (kuva 1). Tietojenkalastelusivustojen määrä on yli kolminkertaistunut vuoden 2020 alusta (APWG, 2021). Tilastoihin voi myös vaikuttaa tekniikan kehittyminen sekä ihmisten ahkerampi ilmoittaminen eteenpäin tapahtuvista hyökkäyksistä, eikä nousua voida suoraan verrata maailmassa tapahtuvien hyökkäysten määrään. Silti havaittujen tietojenkalastelusivustojen määrän huimalla nousulla vuoden 2019 jälkeen voidaan todeta, että tietojenkalastelu-hyökkäykset ovat myös määrältään edelleen noususuhdanteessa, eivätkä hiipumassa oleva hyökkäystekniikka.

Seuraavaksi lähdin tutkimaan vuosien 2016–2021 välisiä eroja hyökkäysten kohteissa ja ympäristöjä mitkä ovat hyökkääjien suosiossa. Kohdistetuimmat toimialat hyökkäyksissä 2016–2021 eli teollisuuden sektorit, jotka ovat olleet eniten tietojenkalasteluviestihyökkäyksien kohteena tai hyökkäyksissä apuna käytettävinä ympäristöinä. Tilastot ovat siis tulkittavissa monella tapaa, mutta tärkeimpänä tietona tutkimuksemme tueksi halusin selvittää, miten kohdistetut toimialat ovat kehittyneet sekä muuttuneet hyökkäyksissä viimeisen 5 vuoden aikana. Kaikki alle 5 prosenttiin koko tilastoista kuuluvat toimialat jätin merkitsemättä meidän verrattaviin tilastoihin eri vuosilta, koska suurin osa lopuista tuloksista oli luokittelemattomia ja ne eivät olisi tuoneet lisäarvoa keräämäämme dataan. Näin tulokset ovat prosentuaalisesti tiivistetty suurimpien kohdistettujen toimialojen välillä.



Kuva 2. Hyökkäysten kohdistamat toimialat 2016 (mukaillen APWG, 2016)

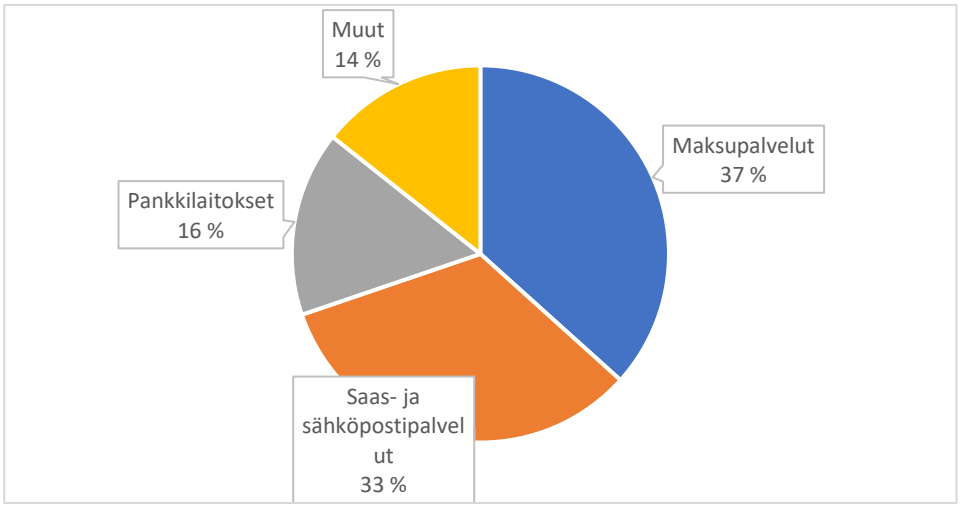
Vuonna 2016 vähittäiskaupat sekä pankkilaitokset olivat selkeät kärki kohteet tietojenkalastelu-hyökkäyksissä (kuva 2). Pankkilaitoksien toimialalle kuuluvat myös muut organisaatiot, jotka hallinnoivat rahaa kuten vakuutus- ja pankkikorttiyhtiöt. Vähittäismyyntipalveluihin kuuluvat kaikki suoraan asiakkaiden kanssa vuorovaikutuksessa olevat toimialat. Jo seuraavan vuoden tilastoissa palvelut ovat lajiteltu omiin kategorioihin, joten otanta tulee selvästi pienemään.



Kuva 3. Hyökkäysten kohdistamat toimialat 2017 (mukaillen APWG, 2017)

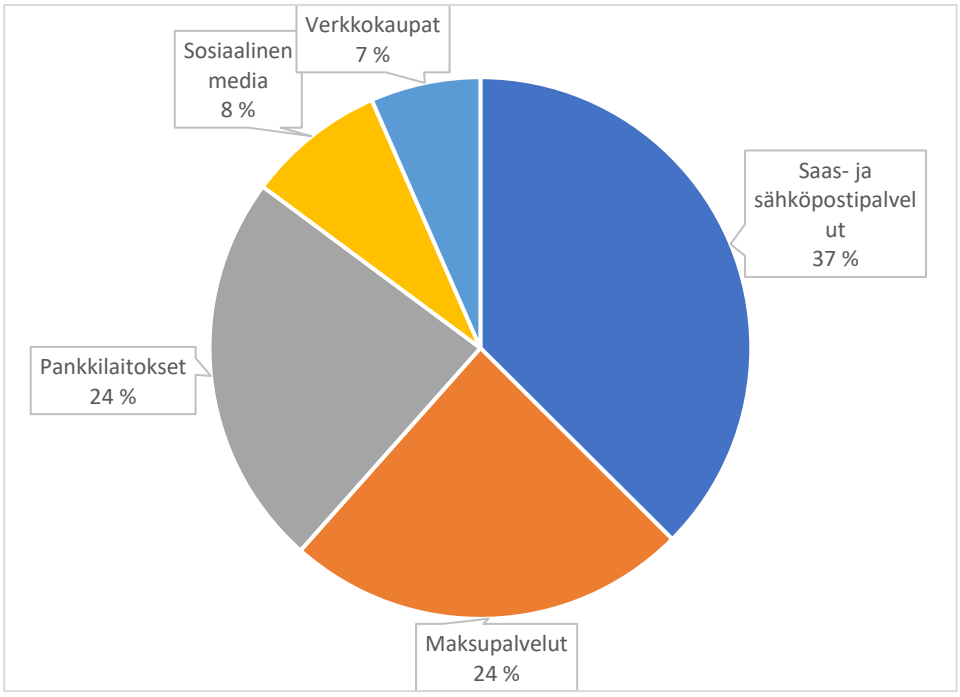
Vuoteen 2017 mennessä (kuva 3) maksupalvelujen osuus hyökkäyksissä kohdennetuista toimialoista kasvoi 12 prosentista 50 prosenttiin ja oli näin merkittävin muutos edeltävään vuoteen verrattuna. Maksupalveluihin kohdistettuihin hyökkäyksiin kuuluvat kaikki verkkomaksutapahtumat ja palvelut kuten PayPal, eBay ja Visa. Myös selkeä ero edeltävään vuoteen näkyi siinä, että tietojenkalasteluviestit kohdistuivat enemmän sovelluspohjaisiin palveluihin, kuten sähköpostipalveluiden

tarjoajiin ja tiedostojenjakopalveluihin. Hyökkääjän pystyivät käyttämään näitä palveluja hyödyksi muun muassa haitallisten ohjelmien jaossa uhreille. Ylipäätään vuonna 2017 palvelualustat kuten pilvipalvelut nousivat selvästi esille.



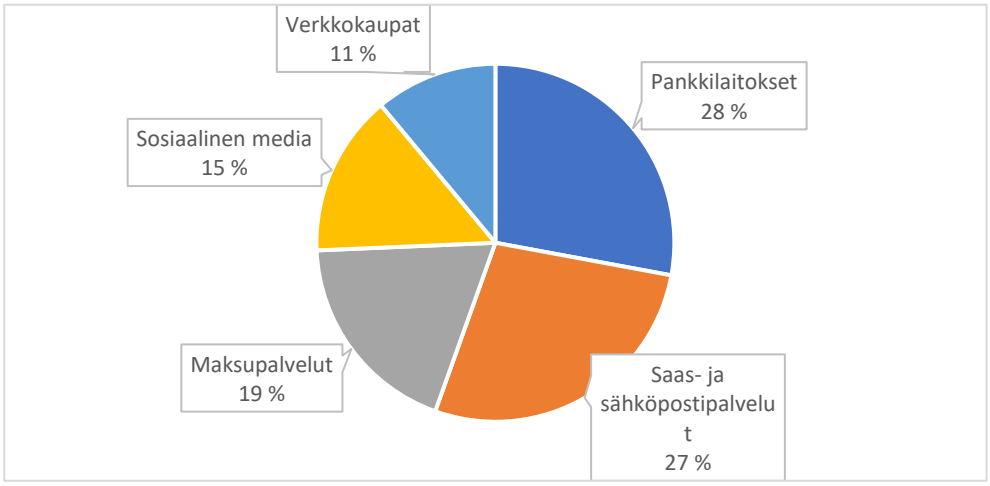
Kuva 4. Hyökkäysten kohdistamat toimialat 2018 (mukaillen APWG, 2018)

Sama teema ja kehitys näkyy kuvassa 4, joka kuvaa vuoden 2018 tietojenkalasteluviestien kohdistamia toimialoja. Saas- ja sähköpostipalvelut ovat jo kolmasosa kaikista suurimpiin toimialoihin kohdennetuista hyökkäyksistä. Maksupalvelut ja pankkilaitokset täydentävät nämä 3 selvästi suurinta toimialaa, joihin hyökkäykset kohdistuvat.



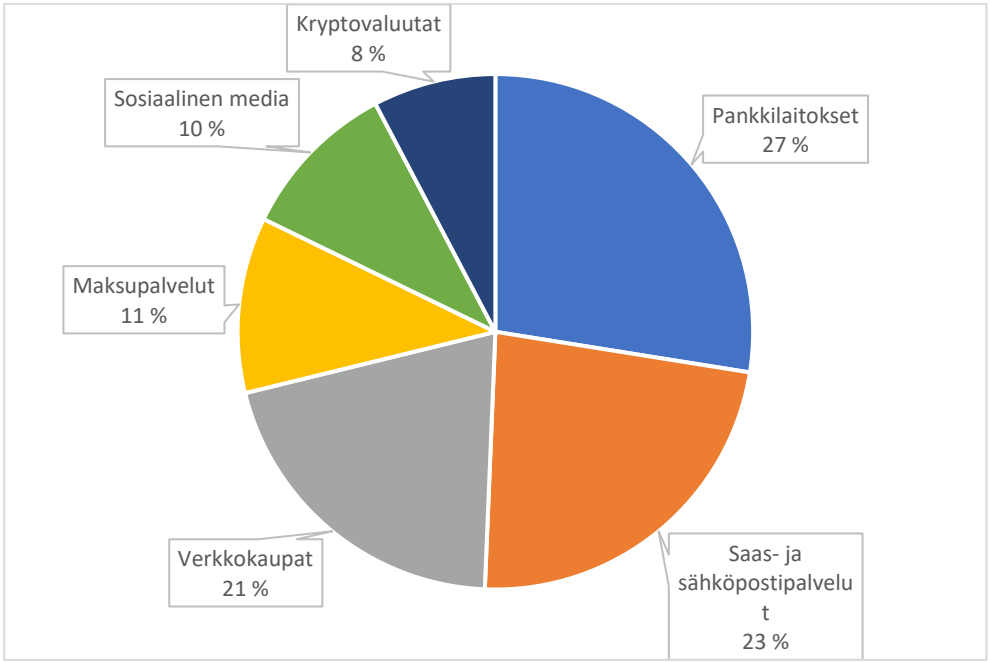
Kuva 5. Hyökkäysten kohdistamat toimialat 2019 (mukaillen APWG, 2019)

Vuonna 2019 merkittävin muutos oli sosiaalisen median sekä verkkokauppojen toimialojen kasvu yli 5 prosenttiin kaikista kohdistetuista toimialoista (kuva 5). Sosiaalista mediaa hyökkääjät käyttävät hyödyksi lähettämällä uhreille suoraan yksityisviestejä tai jakamalla haitallisia linkkejä palveluiden sisällä. Verkkokauppojen asiakkaille kohdennetuissa tietojenkalasteluviesteissä hyökkääjät useasti esittävät yrityksiä väittäen viestien vastaanottajille esimerkiksi puuttuvista maksuista tai tarjoavat ilmaisia tuotteita. Verkkokaupat ovat olleet jo vuosia merkittävä bisnes ja ilmiönä trendaava samalla tavalla kuin sosiaalinen mediakin. Ihmisten elämä pyörii enemmän digitaalisessa maailmassa. Saas- ja pilvipalvelut säilyivät tietojenkalastelun yhtenä yleisimpänä kohteena. Hyökkääjät keräävät uhreilta käyttäjätunnuksia sekä salasanoja näihin palveluihin ja näin hyödyntäen kaapattuja yrityssähköpostitilejä (BEC) hyökkääjät pystyvät tunkeutumaan suoraan yritysten sisälle sekä jakamaan ”luotettavasti” omia tiedostojaan muille työntekijöille.



Kuva 6. Hyökkäysten kohdistamat toimialat 2020 (mukaillen APWG, 2020)

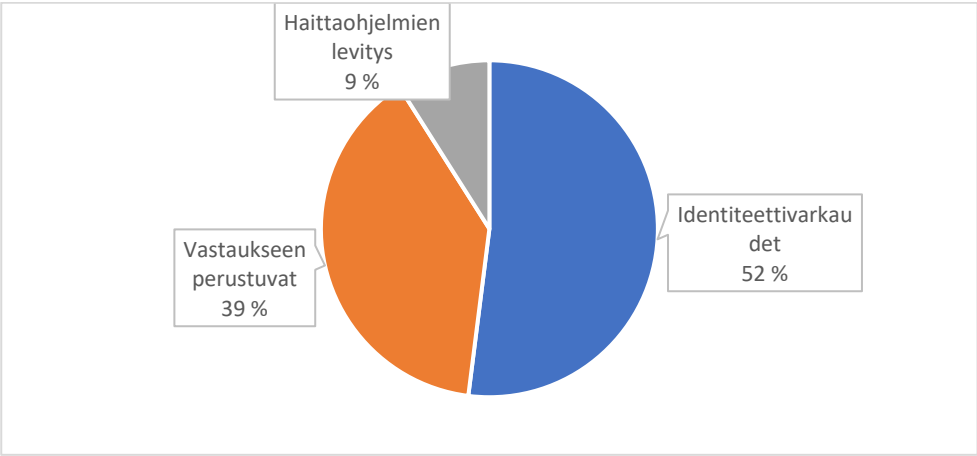
Vuonna 2020 suurimpia muutoksia toimialoissa olivat verkkokauppojen ja sosiaalisen median alustojen nousu ja Saas- ja sähköpostipalveluiden lievä lasku verrattaessa edeltävään vuoteen. Yksi syy verkkokauppoihin ja sosiaalisiin medioihin kohdistuvien hyökkäyksien kasvussa voi olla alkanut koronaviruspandemia, joka pakotti enemmän ihmisiä pysymään kotona ja näin keskustelut sekä kaupankäynti siirtyivät enemmän kybermaailmaan. Kuvasta 6 huomataan myös, että pankkilaitokset ja maksupalveluiden toimialat ovat säilyneet vahvoina kohteina hyökkäyksille ja siellähän se raha liikkuu. Hyökkäyksien viestien teemoina ovat yleensä ennakkomaksut (houkuttelu), veroilmoitukset ja pankkien lähettämät viestit, joissa pyydetään vastaanottajaa avaamaan linkki ja muuttamaan olemassa olevia asiakastietoja. Nämä kalasteluviestit ovat olleet pankkien murheina jo pitkään, kuten näistä tilastoista vuodesta 2016 lähtien pystytään sanomaan.



Kuva 7. Hyökkäysten kohdistamat toimialat 2021 (mukaillen APWG, 2021)

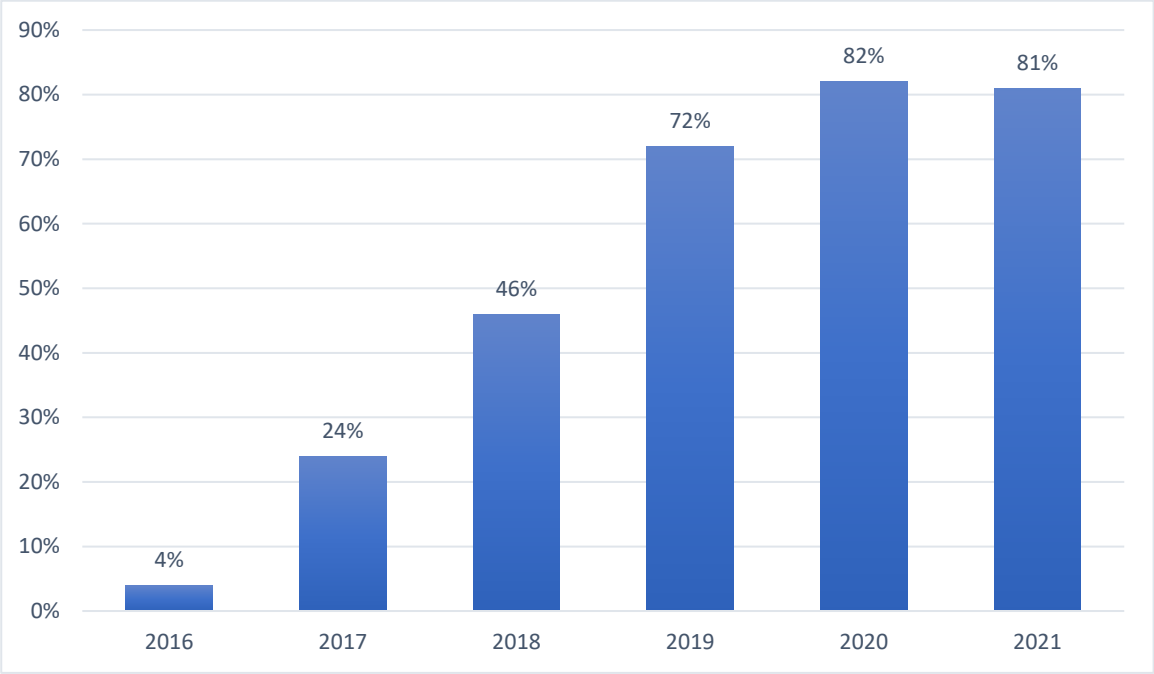
Kuvassa 7 nähdään vuoden 2021 hyökkäysten kohdistetuimmat toimialat. Merkittävin nousu tietojenkalasteluviestien kohteena on kryptovaluutat, kohteeseen lukeutuvat erilaiset kryptovaluuttojen vaihtopalvelut sekä elektroniset lompakot, joissa valuuttoja säilytetään. Sosiaalisen manipuloinnin avulla hyökkääjät hyödyntävät tätä toimialaa siten, että viestissä vastaanottajalle luvataan ilmaisia kryptovaluuttoja tai niitä luvataan palkkioksi pienestä vastapalveluksesta.

Suurimpina muutoksina vuosien 2016 sekä 2021 välillä on tapahtunut muutos teknologian käytössä. Käyttäjien määrä digitaalisen maailman palveluissa on kasvanut ja varsinkin uudemmat palvelut ja ilmiöt kuten verkkokaupat, kryptovaluutat sekä sosiaalinen media ovat selvästi nousseet enemmän hyökkäysten kohteiksi ja alustoiksi mitä hyökkääjät hyödyntävät kalasteluviesteissään. Myös pankit ja muut talouteen keskittyvät toimialat ovat säilyneet erittäin merkittävänä osana hyökkäyksiä.



Kuva 8. Löytyneet uhkat tietojenkalasteluviesteissä 2021 (mukaillen APWG, 2021)

Kuvissa 1–7 käytiin lävitse suosituimpia toimialoja, joihin rikolliset kohdistavat omia tietojenkalasteluviestejä, mutta mitä uhkia nämä hyökkäykset sitten sisältävät. Kuvassa 8 on tilastoitu vuoden 2021 APWG:n tilasto löytyneistä uhkista tietojenkalasteluviesteissä. 52 % viesteistä tavoittelee identiteettivarkautta eli hyökkääjän tavoite on saada uhri antamaan henkilökohtaisia tietojaan hyökkääjälle (esimerkiksi käyttäjätunnukset, salasanat ja pankkitiedot). 39 % Hyökkäyksistä tavoittelee vastausta vastaanottajalta. Hyökkäyksiä on paljon erilaisia, vastauksilla hyökkääjä pystyy esimerkiksi varmistamaan, että vastaanottajan tili on aktiivinen näin kohdistamaan kyseisen tilin tulevissa hyökkäyksissä. Viesteissä myös annetaan uskomattomia tarjouksia, mistä vastaanottaja ei pysty kieltäytymään tai saamalla vastaukseksi vastaanottajan puhelinnumeron hyökkääjä pystyy jatkamaan hyökkäystä puhelimen kautta. Vain 9 % löytyneistä uhkista oli haittaohjelmien levitystä, mikä oli hieman yllättävää. Tämä voi johtua suoraan siitä, että sähköpostipalveluiden suodattimet sekä virustorjuntaohjelmat ovat niin kehittyneitä, että ne torjuvat suurimman osan haittaohjelmista. Hyökkääjät käyttävät siis uhkissa todella paljon hyödyksi sosiaalista manipulointia ja tavoittelevat enemmän vuorovaikutuksella uhrien arkaluonteisia tietoja ja tilejä kuin suoraan haittaohjelmien jakoa kohteille.



Kuva 9. HTTPS:llä isännöidyt tietojenkalasteluhyökkäykset prosentuaalisesti kaikista hyökkäyksistä 2021 (mukaillen APWG, 2021)

Yleisesti HTTPS:n käyttö on yleistynyt kaikilla verkkosivuilla, parantaen verkkosivustojen yleistä turvallisuutta. Kuten kappaleessa 4.2 todettiin, ovat myös tietojenkalastelijat alkaneet käyttää tätä protokollaa hyödykseen myös omissa verkkosivustoissaan sivustolla kävijöille vääränlaista turvallisuuden tunnetta. Nykyään siis jopa 80 % kaikista hyökkäyssivustoista käyttävät tätä protokollaa, tämä on yksi todiste siitä, että hyökkäykset ovat kehittyneet teknillisesti ja näin ovat vaikeampia tunnistaa turvallisista viesteistä kuin ennen.

Internet Complaint Center (IC3)

Tutkimuksessa keräsin vertailudataa myös FBI:n Internet Crime Complaint Center (IC3) vuosien 2016 sekä 2021 julkisista raporteista. IC3 tarjoaa amerikkalaisille suoran kanavan ilmoittaa kyberrikoksista ja heidän raporteissaan on analysoitu ja tutkittu verkkorikollisten uhkia. Hyödyntämällä myös FBI:n raportteja pystyn esittämään vielä monipuolisemmin dataa tietojenkalasteluviestien kehityksestä.

Taulukko 1. Vuoden 2016 kyberrikosten tyyppejä (mukaillen IC3 2016, 17)

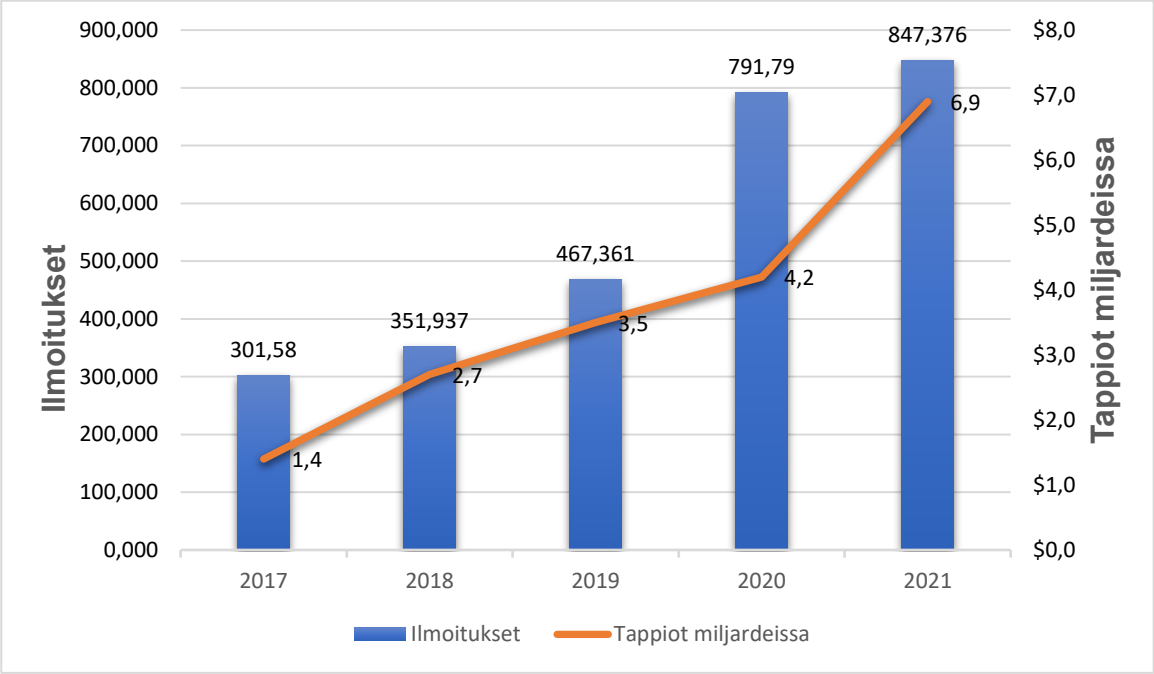
Kyberrikostyyppi	**Uhrien lukumäärä**
Maksamatta jättäminen/toimittamatta jättäminen	81,029
Henkilökohtaiset tietovuodot	27,573
419	25,716
Verkkourkinta/huijauspuhelut/huijaustekstiviestit	19,465
Kiristys	17,146
Identiteettivarkaudet	16,878
Luottokorttipetokset	15,895
Lisämaksu	15,075
Luottamuspetos (engl. catphishing)	14,546
Viranomaisena esiintyminen	12,344
Kaapattu sähköpostitili	12,005

Taulukossa 1 nähdään siis yleisimpiä rikostyyppejä ja niihin langenneiden uhrien lukumääriä. Alkuperäisestä taulukosta poimin ylös suurimmat rikostyypit. Uhrien lukumäärää pystytään suoraan vertailemaan siihen, mitkä hyökkäykset ovat eniten onnistuneet. Silti on tärkeä muistaa, että esimerkiksi 419-hyökkäyksistä hyvänä esimerkkinä on nigerialaiskirjeet, joita lähetetään yleensä todella isoissa määrissä eri vastaanottajille, joten suoraan onnistumisprosenttiin ei tilastot ole verrattavissa. Mielestäni 419 voisi laittaa samaan kategoriaan aiheen ”maksamatta jättäminen” rikoksiin, sillä molemmissa tapauksissa hyökkääjä tavoittelee vastaanottajalta maksua ennen kuin katkaisee yhteyden uhriin. Tilastojen eri rikostyypeissä on todella paljon samoja piirteitä ja tyypin verkkourkinta/huijauspuhelut/huijaustekstiviestit rikokset ovat varmasti monien muidenkin näiden rikosten alkuperäinen lähde. Silti tilastoista on helppo nostaa ylös hyökkäystyypit, jotka ovat selvästi onnistuneet uhrien lukumäärään vertaillessa. Sosiaalinen manipulointi on erittäin suuressa roolissa melkein jokaisessa hyökkäystyypissä, kuten kiristyksissä, identiteettivarkauksissa, luottokorttipetoksissa, luottamuspetoksissa (rakkauskirjeet), viranomaisena esiintymisissä sekä kaapatuissa sähköpostitileissä. Kaikissa näissä eri rikostyypeissä on hyökkääjä saanut uhrin käyttäytymään haluamallansa tavalla saavuttaakseen tavoitellun palkinnon.

Taulukko 2. Vuoden 2021 kyberrikosten tyyppejä (mukaillen IC3 2021, 22)

Kyberrikostyyppi	**Uhrien lukumäärä**
Verkkourkinta/huijauspuhelut/huijaustekstiviestit	323,973
Maksamatta jättäminen/toimittamatta jättäminen	82,478
Henkilökohtaiset tietovuodot	51,829
Identiteettivarkaudet	51,629
Kiristys	39,360
Kryptovaluutat	36,202
Sosiaalinen media	36,034
Luottamuspetos (engl. catphishing)	24,299
Tekninen tuki	23,903
Sijoittaminen	20,561
Kaapattu sähköpostitili	19,954
Peukalointi (engl. spoofing)	18,522

Taulukossa 2 suurimmat muutokset mitä on tapahtunut 5 vuodessa (taulukko 1) verrattuna vuoteen 2016 ovat verkkourkinnan/huijauspuheluiden/huijaustekstiviestien uhrien määrän nousu melkein 16 kertaiseksi, sekä ylipäätään uhrien nousu melkein jokaisella rikostyypillä. Edelleen manipulointia hyväksikäyttävät rikokset ovat suuressa roolissa melkein kaikissa rikoksissa. Taulukosta on tippunut 419 eli suurimmaksi osaksi juuri nigerialaiskirjeet ja hyökkäykset, joita suoritetaan massakampanjoina. Uusina yleisinä rikosten aiheina ovat nousseet sijoittaminen, tekninen tuki, sosiaalinen media, kryptovaluutat sekä peukalointi. Sijoittaminen, sosiaalinen media sekä kryptovaluutat ovat kaikki trendikkäitä ilmiöitä tänä päivänä ja kasvavia ympäristöjä, mikä voi selvästi näkyä syynä onnistuneihin hyökkäyksiin aiheen tiimoilta. Alkuperäisessä taulukossa mainitaan erikseen, että sosiaalinen media sekä kryptovaluutta rikostyypit tarkoittavat tässä taulukossa työkaluja, joita rikolliset käyttävät ponnahduslautana rikosten helpottamiseksi. Peukaloinnilla tarkoitetaan rikoksia, joissa hyökkääjät ovat muuttaneet tietojaan ja näin esittäytyvät esimerkiksi vastaanottajan läheisenä tuttuna omassa hyökkäyksessään. Ylipäätään uhrien lukumäärät ovat selvästi nousseet näissä IC3:lle ilmoitetuissa kyberrikoksissa 5 vuoden aikana.



Kuva 10. Ilmoitukset ja tappiot 2017–2021 välillä (mukaillen IC3 2021, 7)

Miettiessä syitä miksi tietojenkalasteluviestejä tehdään tai syitä miksi hyökkäyksiä tultaisiin tekemään myös tulevaisuudessa, isoin tekijä on palkkiot, jotka tekevät hyökkääjille rikoksista kannattavia. Hyökkääjien tavoitteet itse hyökkäyksissä vaihtelevat suuresti, mutta yleisimpänä tavoitteena on raha. Kuvassa 10 voidaan nähdä, että hyökkäykset ovat tuottaneet vuonna 2021 5,5 miljardia enemmän kuin vuonna 2017. Myös ilmoitukset tapahtuneista kyberrikoksista ovat kasvaneet huomattavasti vuosien välillä. Tämän perusteella voidaan todeta, että yhä enemmän rikoksia tapahtuu ja sen myötä tappiot hyökkäysten takia ovat jyrkässä noususuhdanteessa. On muun muassa arvioitu, että ransomware hyökkäysten tappiot tulevat nousemaan 265 miljardiin dollariin vuoteen 2031 mennessä (Cloudwards 2022).

8.1.2 Haastattelutulokset

Haastatteluiden pohjana tutkimuksessa käytettiin strukturoitua kyselylomaketta. Haastattelu sisälsi 5 kysymystä, joista 4 oli avoimia ja yksi kysymys sisälsi lineaarisen asteikon sisältäen vastaus asteikonnumeroiden 1–5 väliltä. Kyselylomakkeeseen vastasi 15 henkilöä nimettömästi, joista jokainen vastasi kaikkiin 5 kysymykseen. Alun perin lomake lähetettiin 25 valitulle henkilölle, joista halusin muodostaa mahdollisimman satunnaisen otannan. 20 henkilöä lomakkeen vastaanottajista ei omannut minkäänlaista koulutusta liittyen tietotekniikkaan tai tietoturvaan. Alla on vielä kertaus kysymyksistä ja perustelut jokaiselle kysymykselle, miksi se on osa kyselyä.

1. Oletko huomannut jotain tiettyjä muutoksia saamissasi tietojenkalasteluviesteissä viimeisen 5 vuoden aikana? Esimerkkejä muutoksista: Olen vastaanottanut enemmän kalasteluviestejä,

kalasteluviestit ovat siirtyneet eri alustalle (tekstiviestit, sähköposti, sosiaalinen media), kalasteluviestit ovat luovempia/paremmin tehtyjä. Kuvaile huomaamiasi muutoksia vastauskenttään.

- Kysymyksen avulla oli tarkoitus selvittää näkevätkö vastaajat mitään merkittäviä muutoksia tietojenkalasteluviestien kehityksessä viimeisen 5 vuoden aikana.

2. Oletko ollut lähellä joutua/joutunut tietojenkalasteluviestin uhriksi? Minkälainen viesti oli ja miksi se oli vakuuttava? Kirjoita avoin vastaus vastauskenttään.

- Tämän kysymyksen avulla tarkoitus oli selvittää minkälaiset hyökkäykset ovat vaarallisimpia vastaajien mielestä ja miksi.

3. Oletko muuttanut omaa asennettasi/suojautumistasi tietojenkalasteluviesteihin liittyen viimeisen 5 vuoden aikana? Jos olet niin millä tavoin? Kirjoita avoin vastaus vastauskenttään.

- Tämän avulla pystytään todentamaan yleisiä suojautumiskeinoja, joita ihmiset käyttävät omassa elämässään hyökkäyksiä vastaan sekä muutoksia asenteissa ja tavoissa suojautumista kohtaan viimeisen 5 vuoden aikana.

4. Tulevatko tietojenkalasteluviestit olemaan mielestäsi vaarallisempia tulevaisuudessa? Arvioi numeroin 1 – 5 (1 = Paljon vaarattomampia 3 = Ei muutosta 5 = Paljon vaarallisempia)

- Yleinen otanta, jolla saadaan kuva ihmisten suhtautumisesta tietojenkalasteluviestien kehitykseen.

5. Edelliseen kysymykseen viitaten syitä omalle arviolle – Avoin vastaus

- Tavoite kerätä tarkempia mielipiteitä siitä, miksi tietojenkalasteluviestit voisivat olla kehittymässä tiettyyn suuntaan.

Vastaukset

Alla on luetelma vastauksista 5 eri kysymykseen, joita keräsin strukturoidun haastattelun avulla. Haastattelusta on kerätty ydinasiat sekä mielipiteet, joihin nojautui useampi henkilö.

Vastaukset kysymykseen 1:

- 8 vastaajan mielestä tietojenkalasteluviestien määrä on lisääntynyt.
- 8 vastaajista myös mainitsi viestien olevan laadukkaampia, vastaajat nostivat ylös esimerkkeinä paremman kieliasun ja viestien olevan paljon henkilökohtaisempia eli kohdennettuja.

- 3 vastaajista painotti viestien siirtyneen useille alustoille kuten sosiaaliseen mediaan sekä tekstiviesteihin. Yksi vastaajista eritoten painotti, että Instagramissa tulee paljon yksityisviestejä automatisoiduilta bottitileiltä.
- 1 vastaajista ei ollut huomannut mitään eroa tietojenkalasteluviesteissä viimeisen 5 vuoden aikana.

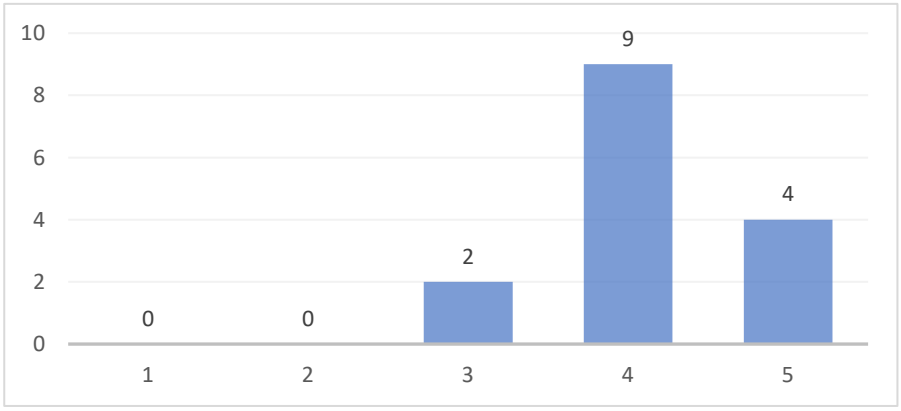
Vastaukset kysymykseen 2:

- 11 vastaajista kertoi, ettei heillä ole ollut lähellä piti tilanteita tietojenkalasteluviestien kanssa.
- 3 vastaajista kertoi melkein joutuneensa hyökkäyksen uhriksi, kaksi viesteistä koski pankkitunnuksia ja yhdessä viestissä väitetysti Facebook ilmoitti kaverin merkinneen vastaanottajan uuteen kuvaansa.
- Yksi vastaajista kertoi kaverinsa joutuneen tietojenkalasteluviestin uhriksi, hyökkääjät väittivät puhelussa olevansa tietoturva miehiä.

Vastaukset kysymykseen 3:

- 8 vastaajista kertoi olevansa varovaisempia ja tarkempia epäilyttävien viestien kanssa kuin ennen.
- 5 vastaajista kertoi, etteivät ole muuttaneet omaa suojautumista tai asennetta tietojenkalasteluviestejä kohtaan millään tavoin.
- Yksi vastaajista painotti oman tietotaidon ja osaamisen tietoturvasta kasvaneen huomattavasti viimeisten vuosien aikana.

Vastaukset kysymykseen 4:



Kuva 11. Tulevatko tietojenkalasteluviestit olemaan vaarallisempia tulevaisuudessa arvio 1–5

Haastattelussa kysyttiin tilastodiagrammin avulla vastaajien arvioita siihen, kuinka vaarallisia tietojenkalasteluviestit tulee olemaan tulevaisuudessa. Arvoasteikolla numero 1 tarkoittaa paljon

vaarattomampia ja numero 5 paljon vaarallisempia. Vastaajista 13 (86,7 %) uskoi tietojenkalasteluviestien olevan tulevaisuudessa vaarallisempia. Kaksi vastaajista (13,3 %) arvioi numeron 3 eli ei suurempaa muutosta suuntaan tai toiseen viestien vaarallisuuden suhteen.

Vastaukset kysymykseen 5:

- Jopa 11 vastaajan mielestä hyökkäykset tulevat olemaan vaarallisempia tulevaisuudessa, koska teknologia kehittyy ja yksi heistä viittasi lisäksi kokemukseen: ”Hyökkääjät tietävät koko ajan paremmin mikä toimii mitä enemmän tietotekniikka tulee elämään ja näin saavat mahdollisuuksia eri ideoiden toteuttamiseen”.
- 1 vastaajista uskoi hyökkäysten olevan vaarallisempia, koska kaikki henkilökohtaiset tiedot siirtyvät enemmän verkkoon sekä totesi uskovansa myös identiteettivarkauksien yleistyvän.
- Kaksi vastaajista ei osannut arvioida tarkemmin syitä omalle arviolle.

8.1.3 Johtopäätökset

Tässä kappaleessa käsitellään kaikkia saatuja tuloksia kootusti niin olemassa olevista tilastoista kuin strukturoidusta kyselystä havaintomatriisin avulla. Tuloksia arvioimalla luon johtopäätöksiä, joiden perusteella luon lopullisen yhteenvedon pohdinta osuudessa tietojenkalasteluviestien kehityksestä ja suojautumisesta nyt ja lähitulevaisuudessa.

Taulukko 3. Havaintomatriisi tutkimustuloksista

Aihe	**Tilastot (kuva ja taulukko)**	**Kyselylomakkeen vastaukset (kysymys)**
1. Tietojenkalasteluviestien määrä	Kuvat 1–7, 10 ja taulukot 1,2	1
2. Hyökkäystekniikat ja niiden toimivuus	Kuvat 8–10 ja taulukot 1,2	1,2
3. Ihmisten käyttäytyminen	10	3
4. Hyökkäysten tulevaisuus	Kuvat 8–11	4,5
5. Suojautuminen	Kuvat 8,10 ja taulukot 1,2	2,3

Kuvien 1 ja 10 avulla voidaan havaita, että tietojenkalasteluviestien, tappioiden, uhrien sekä ilmoitusten määrä ovat kaikki kasvamassa. Mitään viitteitä ei ole siitä, että tietojenkalasteluviestit olisivat vähentymässä tai eivät olisi enää tuottoisia rikollisille. Taulukoista 1 ja 2 huomataan myös, että tappiot yrityksille ja uhreille kasvavat vuosi vuodelta samoin kuin kyberrikosten uhrien määrät. Käyttäjien lisääntyvän määrän myötä verkossa varsinkin tuoreemmat toimialat kuten

verkkopalveluympäristöt, kryptovaluutat sekä sosiaalinen media ovat nousseet rikollisten suosioon hyökkäyksien alustoina (kuva 7).

Haastatteluiden 1 ja 2 kysymysten vastausten perusteella voidaan todeta, että viimeisen 5 vuoden aikana tietojenkalasteluviesteistä on tullut laadukkaampia sekä henkilökohtaisempia, esimerkiksi kielioppi on parempaa viestien sisällössä. Hyökkääjät ovat alkaneet hyödyntämään enemmän suojaustekniikoita omissa hyökkäyksissään luoden valheellisen turvallisuudentunteen uhreille (kuva 9). Kuvan 8 sekä taulukon 2 avulla voidaan todeta sosiaalisen manipuloinnin olevan isossa roolissa suurimmassa osassa onnistuneista hyökkäyksistä. Rikolliset tavoittelevat vuorovaikutuksella ja luottamuksella uhreilta arkaluonteisia tietoja enemmän kuin suoraan haittaohjelmilla. Vakuuttavilla tarinoilla (engl. pretexting), kuten työkaverina esiintymisellä esimerkiksi tavoitellaan uhrin luottamusta ja sitä kautta pääsyä arkaluonteisiin tietoihin tai palveluihin käsiksi.

Kuvan 10 avulla voidaan sanoa, että ihmiset myöskin ilmoittavat enemmän eteenpäin havaituista kalasteluviesteistä. Haastattelun vastausten perusteella kysymykseen 3 voidaan havaita, että Ihmiset ovat varovaisempia digitaalisten laitteiden kanssa ja ovat nostaneet varovaisuutta saapuvien viestien suhteen. Tällä ei voida suoraan sanoa olevan yhteyttä siihen, että ihmisten osaaminen tietoturvan suhteen olisikaan yleisesti parantunut.

Kuvan 11 tilastodiagrammin perusteella, ihmiset uskovat tietojenkalasteluviestien olevan vaarallisempia tulevaisuudessa, suurimpana syynä ihmiset pitivät teknologian jatkuvaa kehitystä tälle arviolle. Hyökkäykset tuottavat rikollisille vuosi vuodelta enemmän rahaa ja yritykset kärsivät suurempia tappioita (kuva 10). Tietojenkalasteluviestit ovat kehittyneet luovemmiksi ja henkilökohtaisemmiksi ja nämä asiat tekevät hyökkäyksistä tulevaisuudessakin entistä vaarallisempia.

Tietoturva kehittyy, kuten myös sähköpostienpalveluiden suodattimet ja virustorjuntaohjelmat. Myös tietojenkalasteluviestit ovat kehittyneet ja hyökkääjät ovat löytäneet tapoja, miten ohittaa näitä tietoturvan eri tasoja. Suora vuorovaikutus uhriin esimerkiksi sosiaalisen median kautta on todella vaikea estää automaattisilla ohjelmilla, viimeisenä lukkona toimii vastaanottaja eli ihminen. Vastausten perusteella kysymykseen 3 ei voida kuitenkaan todeta, että ihmiset olisivat hirveästi muuttaneet omaa suojautumista hyökkäyksiä kohtaan.

9. Pohdinta

Tutkimuksen tavoitteena oli luoda kokonaiskuva ja perusteluja tietojenkalasteluviestien kehityksestä ja suojautumisesta viimeisen 5 vuoden aikana sekä ennakoida mahdollista kehityksen suuntaa myös tulevaisuudessa. Olemassa olevia tilastoja sekä luotua Google Forms -kyselyä hyödyntämällä oli tarkoitus löytää vastauksia erityisesti seuraaviin tutkimuskysymyksiin:

- Minkälaisten tietojenkalasteluviestien määrä on kasvanut, mitkä ovat vähentyneet? Onko muutokselle olemassa selkeitä syitä.
- Mitkä hyökkäykset ovat toimivimpia ja miksi? Onko ihmisten käytös viestejä kohtaan muuttunut.
- Mihin suuntaan hyökkäykset tulevat todennäköisesti kehittymään seuraavien vuosien aikana? Millä tavoin pystymme ennakoimaan ja suojautumaan näiltä hyökkäyksiltä.

Kybermaailmasta on tullut iso osa ihmisten arkea ja tutkimustulosten avulla voidaan todeta, että myös tietojenkalasteluviestit ovat kehittyneet muuttuvan maailman mukana. Hyökkäykset keskittyvät yhä enemmän ajankohtaisiin ilmiöihin kehittäen näin mahdollisimman suuren onnistumisprosentin hyökkäyksistä. Varsinkin verkkokaupat, kryptovaluutat sekä sosiaalinen media ovat koko ajan enemmän kohdennettu huijausviesteissä myös pankit ovat edelleen suuresti esillä, koska ihmiset käyttävät näitä palveluja säännöllisesti.

Tutkimustuloksissa havaittiin myös, että tietojenkalasteluviestien määrä ja tappiot hyökkäysten johdosta ovat molemmat koko ajan kasvamassa. Hyökkääjät ovat alkaneet keskittymään enemmän arkaluonteisiin tietoihin ja uhreihin, mutta varmasti tuottoisat hyökkäykset myös rahallisesti ovat osa syy siihen, miksi tietojenkalasteluviestien määrä ei ole laantunut vaan päinvastoin niitä huomataan vuosi vuodelta enemmän.

Tutkimuksessa todettiin myös, että hyökkäykset toimivat koska niistä on tullut entistä kohdennettuja ja vuorovaikutteisempia viestien vastaanottajien kanssa. Sosiaalinen manipulointi ja taidokkaammat viestit olivat myös asioita, jotka nousivat esiin kyselyn vastauksista. Ihmisten varovaisuus on kasvanut viestejä availlessa ja joka vuosi ilmoitustenmäärä kalasteluviesteistä on kasvanut. Tutkimuksen perusteella ei voida kuitenkaan todeta, että ihmisten asenteet tai osaaminen tietoturvaa ja uhkia kohtaan olisivat hirveästi muuttuneet viimeisen 5 vuoden aikana.

Kyselyn ja tilastojen perusteella tietojenkalasteluviestit tulevat olemaan vaarallisempia tulevaisuudessa. Hyökkäykset ovat kehittyneet viimeisen 5 vuoden aikana teknologian mukana ja jatkuvan kehityksen mukana myös hyökkäyksistä tulee ennalta arvaamattomampia. Sähköpostien

suodattimet pystyvät koko ajan tarkemmin torjumaan haitallisia viestejä yhdessä palomuurien ja virustorjuntaohjelmien kanssa. Hyökkääjät käyttävät kuitenkin kasvavissa määrin sosiaalista manipulointia hyödyksi huijatakseen sekä tietoturvaohjelmistoja että ihmisiä. Ohjelmat eivät voi torjua kaikkia saapuvia viestejä ja nokkelilta hyökkäyksiltä, kuten ”pretexting” viestejä torjuttaessa tarvitsee vastaanottavan ihmisen toimia viimeisenä turvatoimena. 5 kappaleessa mainittiin, että vuonna 2021 85 % tietovuodoista johtui ihmisten tekemistä päätöksistä. Ihmisten täytyy olla varovaisempia ja valppaampia jokaista saapunutta viestiä kohtaan ja miettiä tarkkaan onko syytä toimia viestin lähettäjän haluamalla tavalla. Tämä on tärkein keino, millä hyökkäyksiä pystytään torjumaan. Tähän pystytään vaikuttamaan esimerkiksi simuloiduilla hyökkäyksillä, jotka ylläpitävät ihmisten kykyä torjua oikeita hyökkäyksiä. Valitettavasti kyselyn perusteella ei suurimman osan suojautumiskeinot ole muuttuneet viimeisen 5 vuoden aikana, eikä simulaatioiden kaltaiset suojauskeinot ole hirveän yleisiä tällä hetkellä. Ilman suuria muutoksia ihmisten asenteissa tai suojautumisessa, uskon tietojenkalasteluviestien aiheuttamien tappioiden kasvavan moninkertaisiksi tulevien vuosien aikana.

Mielestäni tässä opinnäytetyössä saavutettiin tavoite. Havaittiin ja tutkittiin suurimpia muutoksia tietojenkalasteluviestien kehityksessä viimeisen 5 vuoden aikana sekä arvioitiin miten suojautuminen voisi olla mahdollista hyökkäyksiltä. Tulosten luotettavuutta on aina vaikea arvioida, kun aineistona on satoja tuhansia ilmoitettuja viestejä, eivätkä suuret kokonaisuudetkaan silti ole lähellekään sitä tasoa missä määrin tietojenkalasteluviestejä lähetetään joka päivä ympäri maailmaa. Aineisto oli kuitenkin niin laaja kuin oli työn olosuhteiden kannalta järkevä ottaa mukaan otantaan. Tulevaisuutta on mahdoton ennustaa, mutta käytettyjen tilastoiden ja kyselyn mielipiteiden avulla pystyttiin toteamaan, että ihmisten suojautumisessa täytyy tapahtua muutoksia. Yhä vaarallisemmat tietojenkalasteluviestit tulevat muutoin rikastuttamaan rikollisia moninkertaisina lähitulevaisuudessa. Esimerkiksi tämän tutkimuksen avulla olisi mahdollista tuoda ihmisille tietojenkalasteluviestien vaaroja esille ja sitä myöten vaikuttaa positiivisesti asenteisiin tietoturvaa kohtaan.

Jatkokehittämisideoina syventäisin tutkimusta suurempien ihmismäärien haastatteluun luoden näin laajempia päätelmiä ja käsityksiä ihmisten mielipiteistä. Myös kysymysten syvempi otanta ihmisten tietoturvalliseen osaamiseen toisi uusia näkökulmia siihen, miten ihmisten valmius tietojenkalasteluviesteihin on kehittynyt ja miten ihmisille olisi mieluisinta tuoda esille ja kouluttaa tietoturvaa.

Lähteet

APWG s. a. About us. Luettavissa: https://apwg.org/about-us/ Luettu: 05.04.2022.

APWG 2016. Phishing Activity Trends Report, 4th Quarter 2016. Luettavissa: https://docs.apwg.org//reports/apwg_trends_report_q4_2016.pdf Luettu: 06.04.2022.

APWG 2017. Phishing Activity Trends Report, 4th Quarter 2017. Luettavissa: https://docs.apwg.org//reports/apwg_trends_report_q4_2017.pdf Luettu: 08.05.2022.

APWG 2018. Phishing Activity Trends Report, 4th Quarter 2018. Luettavissa: https://docs.apwg.org//reports/apwg_trends_report_q4_2018.pdf Luettu: 05.05.2022.

APWG 2019. Phishing Activity Trends Report, 4th Quarter 2019. Luettavissa: https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf Luettu: 02.05.2022.

APWG 2020. Phishing Activity Trends Report, 4th Quarter 2020. Luettavissa: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf Luettu: 04.05.2022.

APWG 2021. Phishing Activity Trends Report, 2th Quarter 2021. Luettavissa: https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf Luettu: 06.05.2022.

APWG 2021. Phishing Activity Trends Report, 4th Quarter 2021. Luettavissa: https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf Luettu: 06.04.2022.

Cloudwards 2022. Ransomware Statistics, Trends and Facts for 2022 and Beyond. Luettavissa: https://www.cloudwards.net/ransomware-statistics/#Sources Luettu: 12.05.2022.

Cofense s.a. History of phishing. Luettavissa: https://cofense.com/knowledge-center/history-of-phishing/ Luettu: 08.04.2022.

Cyber Risk Aware s.a. The Background and Evolution of Phishing. Luettavissa: https://www.cyber-riskaware.com/the-background-and-evolution-of-phishing/ Luettu: 09.04.2022.

Delta Community Credit Union 2021. Only Scammers Get Paid with Gift Cards or Cryptocurrency. Luettavissa: https://www.deltacommunitycu.com/us/en/knowledge-center/blog/september-2021/only-scammers-get-paid-with-gift-cards-or-cryptocu.html Luettu: 10.04.2022.

Imperva s.a. Social Engineering. Luettavissa: https://www.imperva.com/learn/application-security/social-engineering-attack/ Luettu: 23.03.2022.

Internet Crime Complaint Center 2016. 2016 Internet Crime Report. Luettavissa https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf Luettu: 10.05.2022.

Internet Crime Complaint Center 2021. 2021 Internet Crime Report. Luettavissa: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf Luettu: 10.05.2022.

Kaspersky s.a. All about phishing Scams & Prevention: What You Need to Know. Luettavissa: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips Luettu: 02.03.2022.

Kaspersky s.a. What is Social Engineering? Luettavissa: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering Luettu: 23.03.2022.

Krebs on Security 2011. Right-to-left override Aids Email Attacks. Luettavissa: https://krebsonsecurity.com/2011/09/right-to-left-override-aids-email-attacks/ Luettu: 02.04.2022.

LIFARS 2021. Filter evasion phishing. Luettavissa: https://lifars.com/2021/01/filter-evasion-phishing/ Luettu: 11.04.2022.

Malwarebytes 2022. Phishing. Luettavissa: https://www.malwarebytes.com/phishing Luettu: 06.04.2022.

Microsoft 2020. Microsoft Digital Defense Report. Luettavissa: https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/ Luettu: 16.04.2022.

Microsoft s.a. Protect yourself from phishing. Luettavissa: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44 Luettu: 20.04.2022.

Panda Security 2021. 11 Types of Phishing. Luettavissa: https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/ Luettu: 27.03.2022.

Phishing s.a. History of phishing. Luettavissa: https://www.phishing.org/history-of-phishing Luettu: 09.04.2022.

PhishingBox 2020. Data Breach Investigations Report - 2020. Luettavissa: https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-dbir-2020 Luettu: 01.04.2022.

PhishingBox 2021. Data Breach Investigations Report – 2021. Luettavissa: https://www.phishing-box.com/news/phishing-news/verizon-data-breach-investigations-report-dbir-2021 Luettu: 01.04.2022.

PhishProtection s.a. History of phishing. Luettavissa: https://www.phishprotection.com/resources/history-of-phishing/ Luettu: 28.03.2022.

SecurityScorecard 2021. 12 Types of Phishing Attacks and How to Identify Them. Luettavissa: https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them Luettu: 10.04.2022.

Webopedia 2021. Phishing. Luettavissa: https://www.webopedia.com/definitions/phishing-meaning/. Luettu: 07.04.2022.

Liitteet

Liite 1. Kysely

Tietojenkalasteluviestien kehitys

Opparikysely

Vastaamiseen menee noin 3 - 5 minuuttia ja kysely suoritetaan nimettömänä.

1. Oletko huomannut jotain tiettyjä muutoksia saamissasi tietojenkalasteluviesteissä viimeisen 5 vuoden aikana? Kuvaile huomaamiasi muutoksia vastauskenttään.

Esimerkkejä muutoksista: Olen vastaanottanut enemmän kalasteluviestejä, kalasteluviestit ovat siirtyneet eri alustalle (tekstiviestit, sähköposti, sosiaalinen media), kalasteluviestit ovat luovempia/paremmin tehtyjä.

Oma vastauksesi

2. Oletko ollut lähellä joutua/joutunut tietojenkalasteluviestin uhriksi? Minkälainen viesti oli ja miksi se oli vakuuttava? Kirjoita avoin vastaus vastauskenttään.

Oma vastauksesi

3. Oletko muuttanut omaa asennettasi/suojautumistasi tietojenkalasteluviesteihin liittyen viimeisen 5 vuoden aikana? Jos olet niin millä tavoin? Kirjoita avoin vastaus vastauskenttään.

Oma vastauksesi

4. Tulevatko tietojenkalasteluviestit olemaan mielestäsi vaarallisempia tulevaisuudessa? Arvioi numeroin 1 – 5

	1	2	3	4	5	
Paljon vaarattomampia	○	○	○	○	○	Paljon vaarallisempia

5. Edelliseen kysymykseen viitaten syitä omalle arviolle

Oma vastauksesi

Lähetä

Tyhjennä lomake