Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2022

Riku Ihalin

# Tietojenkalastelu teknisenä ilmiönä

– menetelmät, seuraukset ja lieventäminen

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2022 | 34 sivua

Riku Ihalin

# Tietojenkalastelu teknisenä ilmiönä

## – menetelmät, seuraukset ja lieventäminen

Tietojenkalastelu koskettaa monipuolisesti yksityishenkilöitä sekä yrityksiä, ja sen seuraukset voivat olla erittäin haitallisia. Työn tarkoituksena on luoda yleiskuva tietojenkalastelun tilanteesta 2020-luvun alussa. Tietojenkalastelu ilmiönä on kokenut räjähdysmäistä kasvua, ja sen vaikutukset ovat olleet merkittävämpiä kuin koskaan ennen. Työ toteutettiin tutkimalla raportteja tietojenkalastelusta, internetissä julkaistuja tutkimustöitä sekä omia kokemuksia aiheesta.

Tutkittujen lähteiden mukaan tietojenkalastelun määrä on noussut huomattavasti 2020-luvun alussa. Seurauksien listaamisen jälkeen esitetyt merkittävät tapahtumat tietojenkalastelusta näyttävät, kuinka suuri onnistuneen hyökkäyksen vaikutus voi olla. Työssä tutkitaan myös COVID-19-pandemian vaikutusta tietojenkalastelun kasvuun. Lieventämiskeinoissa huomataan, kuinka suuressa roolissa harjoittelu ja ihmisten kouluttaminen on tietojenkalastelun torjumiseen. Lieventämismenetelmät ovat suunnattu pienyrityksille ja yksityishenkilöille.

Asiasanat:

tietoturva, tietomurto, tietojenkalastelu, internet

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Bachelor of Engineering, Information Technology

2022 | 34 pages

Riku Ihalin

# Phishing as a technological phenomenon

## – methods, consequences, and mitigation

Phishing impacts businesses and people in their personal lives in multiple different ways and can be very damaging. The aim of this thesis is to create a clear picture of the current situation of phishing at the start of the 2020s. Phishing, as a phenomenon, has seen explosive growth and its effects have been more notable than ever before.

The thesis was conducted by examining reports about phishing, studies published on the internet as well as personal experiences on the subject. The structure of the thesis covers base information on phishing, the consequences of a successful phishing attack, notable examples of phishing, a more detailed look at phishing from the start of 2020 to Q2 of 2022, the effect of the COVID-19 pandemic on the phenomenon and at the end some mitigation techniques for small businesses and people in their personal lives.

Keywords:

hacking, phishing, cybersecurity, internet

# Sisältö

**Käytetyt lyhenteet** **6**

**1 Johdanto** **7**

**2 Taustaa tietojenkalastelusta** **8**
2.1 Tietojenkalastelun määritelmä 8
2.2 Tietojenkalastelun syitä 9
2.3 Tietojenkalastelun menetelmiä 10

**3 Syvempi perehtyminen tietojenkalastelun menetelmiin** **11**
3.1 Puhelinpohjainen tietojenkalastelu 11
3.2 Sähköpostipohjainen tietojenkalastelu 13

**4 Tietojenkalastelun seuraukset** **15**
4.1 Luvaton pääsy tietoihin 15
4.2 Haittaohjelmien leviäminen 16
4.3 Luvaton pääsy järjestelmiin 17

**5 Merkittäviä esimerkkejä tietojenkalastelusta – yksittäistapauksia ja kampanjoita** **18**
5.1 Hyökkäys Ukrainan sähköverkkoon (2015) 18
5.2 Colonial Pipeline -hyökkäys (2021) 19
5.3 Facebookin & Googlen huijaus (2013–2015) 19
5.4 FACCn ja Crelan Pankin CEO-huijaukset (2016) 19
5.5 Sony Pictures -tietovuoto (2014) 20
5.6 Koronaviruksen vaikutus tietojenkalastelukampanjoihin 20

**6 Tietojenkalastelun nykytilanne** **22**
6.1 Uniikit tietojenkalastelusivustot ja sähköpostit 22
6.2 Suurimmat toimialat tietojenkalastelun kohteena 24
6.2.1 Toimialat tietojenkalastelun kohteena 2020 24
6.2.2 Toimialat tietojenkalastelun kohteena 2021 26
6.2.3 Toimialat tietojenkalastelun kohteena 2022 1. ja 2. neljänneksellä 27

**7 Tietojenkalastelun ja sen vaikutusten lieventäminen** **28**
7.1 Automaattiset päivitykset 28
7.2 Automaattiset varmuuskopiot 29
7.3 Monivaiheinen tunnistautuminen 30
7.4 Ihmisten kouluttaminen ja harjoittelu 30

**8 Yhteenveto** **31**

**Lähteet** **32**

# Kuviot

Kuvio 1. Uniikit tietojenkalastelukampanjoissa käytetyt sivustot ja sähköpostit (APWG 2020; APWG 2021; APWG 2022). 23
Kuvio 2. Toimialojen keskiarvo tietojenkalastelun kohteena 2020 (APWG, 2020). 25
Kuvio 3. Toimialojen keskiarvo tietojenkalastelun kohteena 2021 (APWG, 2021). 26
Kuvio 4. Toimialojen keskiarvo tietojenkalastelun kohteena 2022 (APWG, 2022). 27

# Käytetyt lyhenteet

| | |
|---|---|
| APWG | Anti Phishing Work Group, järjestö joka seuraa ja raportoi tietojenkalastelua maailmanlaajuisesti. Järjestön tarkoituksena on tuoda esille ja kouluttaa tietojenkalastelun tilanteesta ja vaaroista. |
| SaaS | Software as a Service on ohjelmiston jakelumalli, jossa palvelu tarjotaan ylläpitämällä ohjelmistoa palvelimille internetin välityksellä. Esimerkkejä ovat yrityssovellukset kuten sähköpostipalvelut, CRM-palvelut ja laskutus- ja palkanmaksupalvelut. (Wikipedia, 2022) |
| MFA | Multi-factor authentication, eli monivaiheinen tunnistautuminen on turvallisuustoimenpide, joka vaatii kahden tai useamman todennuksen käyttämisen järjestelmään kirjautumista varten. Esimerkiksi salasanan ja mobiililaitteelle/sähköpostiin lähetetyn koodin yhdistelmä. (Kyberturvallisuuskeskus, 2020) |
| EoL | End-of-life, tarkoittaa laitteen tai ohjelmiston tulleen elinkaarensa loppuun eikä valmistaja enää takaa tai valmista päivityksiä. (Kyberturvallisuuskeskus, 2020) |

# 1 Johdanto

Työn tarkoitus on tuoda esille nykytilannetta tietojenkalastelusta. Ilmiö vaikuttaa laajasti yksityishenkilöihin sekä yrityksiin ja sen kasvu on ollut räjähdysmäinen viime vuosina. Opinnäytetyö keskittyy pääasiassa tietojenkalasteluun yritysympäristöissä, mutta myös yksityiselämän tilannetta käsitellään. Motivaatio työn aiheeseen syntyi omista kokemuksistani huijausviestien kanssa viime vuosina eri yhteyksissä, kuten ns. tullihuijausten kanssa sekä uutisten seuraamisesta tietoturvasektorilla. Tietojenkalastelun vastaisen työryhmän (engl. Anti Phishing Work Group, APWG) mukaan vuonna 2022 on huhti-kesäkuussa havainnoitu n. 1,1 miljoonaa tietojenkalasteluhyökkäystä monilla erilaisilla vaikutuksilla, mikä on ollut suurin määrä havaintoja järjestön olemassaolon aikana 2003–2022. (APWG, 2022b)

Tietojenkalastelu perustuu sosiaaliseen manipulaatioon, jossa hyödynnetään ihmistä yrityksen heikkona kohteena. Tietojenkalastelussa ei niinkään käytetä teknisiä menetelmiä, muuten kuin esim. huijaussivustojen toteuttamiseen tai huijaussähköpostien automatisointiin. Tietojenkalastelun seuraukset voivat olla hyvinkin monipuolisia ja tutkin opinnäytetyössäni näitä erilaisia seurauksia sekä niiden lieventämistä. Tietojenkalastelun kohteena on aina organisaation suurin tietoturvahaavoittuvuus eli ihminen.

Tietojenkalastelun huomaa myös yksityiselämässä ajankohtaisten tietojenkalastelukampanjoiden aikana. Hyvänä esimerkkinä toimii 2020–2021 koronarokotuksien varjolla haitallisten linkkien lähettely; hyvin mahdollisesti 2022 energiakriisiä käytetään vastaavalla tavalla hyödyksi. Opinnäytetyössä tutkitaan merkittävimpiä kampanjoita sekä yksittäistapauksia, joita tietojenkalastelussa on käytetty hyödyksi, sekä näiden tuottamia seurauksia.

# 2 Taustaa tietojenkalastelusta

Ensimmäisessä osassa työtä määritellään avainkysymyksiä mitä, miksi ja miten tietojenkalastelusta. Näiden avulla kartoitetaan tietojenkalastelua ilmiönä, sekä sen monipuolisia vaikutuksia. Kysymysten tarkoitus on myös luoda pohjaymmärrys ilmiöstä, jotta pystyn selkeämmin avaamaan ilmiön nykytilannetta ja merkittäviä seurauksia.

Tässä työssä ei käsitellä tietojenkalastelun historiaa ja alkuvaiheita. Antti Virtanen (2011) on tehnyt Turun ammattikorkeakoulussa opinnäytetyön, jossa hän käy kattavasti läpi tietojenkalastelun historiaa sen alkuvaiheista asti.

## 2.1 Tietojenkalastelun määritelmä

Tietojenkalastelu on yksinkertaisimmillaan haitallisten tekijöiden tapa saada käsiinsä tietoa, jota ei olisi tarkoitus saada. Tämä voi olla rahaa, tietoa kohteesta tai pääsy vastaanottajan järjestelmään (Kyberturvallisuuskeskus, 2020). Tämä tieto vaihtelee tapauskohtaisesti ja niin vaihtelevat seurauksetkin. Tietojenkalastelun skaalana voi olla jonkin toisen työntekijän nimi tai puhelinnumero tai jopa salasana, joka mahdollistaa pääsyn kohteen järjestelmään. Myös yksityiselämässä esiintyy usein tietojenkalastelua haitallisten sähköpostien ja tekstiviestien muodossa, jotka lähes aina tähtäävät saamaan kohteelta jotakin nopeaa taloudellista hyötyä kuten luottokortin tietoja tai maksutoimitusta. Tämä tekee tietojenkalastelusta erittäin laajan alan ja tarkoittaa, että sen vaikutukset ja tarkoitukset eivät toistu aina samanlaisina. Lähes aina tietojenkalastelussa on kyseessä jonkinnäköinen sosiaalinen manipulointi. Hyökkääjän näkökulmasta on myös tärkeää harkita kohdekohtaisesti mitä yrittää saada selville. Esimerkiksi helpdeskin työntekijältä on varmastikin turha yrittää udella hyödyllisiä salasanoja, mutta helpdeskin kautta voi hyvin löytää tavan päästä jatkamaan manipulaatiota syvemmälle organisaation sisälle vaikka yhteystietojen avulla.

Tietojenkalastelu voidaan jakaa yleiseen tietojenkalasteluun ja kohdistettuun tietojenkalasteluun (Kyberturvallisuuskeskus, 2020). Yleinen tietojenkalastelu saattaa olla kokonaiselle organisaatiolle tai käyttäjäryhmälle lähetetty sähköposti, joka sisältää haitallisen linkin tai liitteen. Tässä tarkoituksena olisi saada mahdollisimman monta ihmistä painamaan tätä linkkiä. Yleisestä tietojenkalastelusta eriteltynä menetelmänä on kohdistettu tietojenkalastelu, jossa muotoillaan yhteydenotto vastaanottajan mukaan. Siinä käytetään hyväksi ennalta selvitettyjä tietoja henkilöstä, jotta saadaan yhteydenotto näyttämään mahdollisimman aidolta. Tämäntyyppinen kohdistettu tietojenkalastelu tähdätään mitä useimmin henkilöihin, joilla on päätösvaltaa ja näin ollen myös pääsy arkaluontoisiin sekä tärkeisiin tietoihin ja palveluihin. Daniel E. O'Learyn (2019) tekemässä tutkimuksessa kävi ilmi kohdistetun tietojenkalastelun koskettavan eniten organisaatioiden johtajia sekä niitä, jotka työskentelevät taloudellisella sektorilla.

## 2.2 Tietojenkalastelun syitä

Tietojenkalastelua toteutetaan monista syistä ja monilla tarkoituksilla. Yksinkertaisin selitys tietojenkalastelulle on jokin taloudellinen hyöty hyökkääjälle. Rahalliset huijaukset ovat varsinkin yksityishenkilöille selvin uhka. Olemme varmasti kaikki saaneet tekstiviestejä tai sähköposteja, joiden tarkoitus on vain urkkia yksityistietoja tai maksutietoja. Yrityselämässä esiintyy myös tietojenkalastelun taloudellista käyttöä, mikä tosin tapahtuu hieman eri tavalla. Yrityksiltä ei suoraan oteta rahaa joidenkin tunnusten avulla, vaan useammin tarkoituksena on päästä näillä tunnuksilla käsiksi arkaluontoisiin järjestelmiin. Tämän pääsyn jälkeen saatetaan levittää järjestelmään kiristysohjelma, joka on varsin näkyvä ja painostava tapa saada rahaa yritykseltä. Näkymätön ja myös vakava seuraus onnistuneesta tietojenkalastelusta on yrityssalaisuuksien tai tietojen siitä, miten kohteen järjestelmään päästään, levittäminen ja myynti. Käyttäjätunnuksia on mahdollista käyttää oikeuksien korottamiseen (engl. privilege escalation) järjestelmässä ja tämän kautta käyttää alkuperäisiä

tunnuksia ponnahduslautana laajempiin ja/tai vakavampiin hyökkäyksiin. (Wright, Aaron & Bates 2016).

## 2.3 Tietojenkalastelun menetelmiä

Tietojenkalastelussa käytetään monia eri käytäntöjä ja jotkut niistä ovat selkeästi yleisempiä eri käyttötarkoituksiin. Monista niistä käytetään englanninkielisestä tietojenkalastelua merkitsevästä sanasta phishing muokattua sanaa, kuten vishing ja smishing. Vishing on lyhenne voice phishing -termistä, jolla tarkoitetaan VoIP-palveluiden käyttämistä tietojenkalastelun välineenä. Smishing taas on lyhenne sms phishingistä, jolla viitataan tekstiviestien välillä toteutettuun tietojenkalasteluun.

Yleisin vektori, jota tietojenkalastelussa käytetään, on sähköposti. Sähköposti tarjoaa helpon tavan levittää laajasti haitallisia viestejä, jotka saattavat pyytää vastauksia kysymyksiin, sisältää haitallisia linkkejä, joiden painamista kannustetaan esittämällä asia hyvin kiireisenä, tai haitallisia liitetiedostoja, joiden lataaminen koneelle voi johtaa moneen haitalliseen seuraukseen.

Vielä erikseen mainittavana on sähköpostien kanssa käsikädessä menevä ilmiö, eli huijaussivustot. Niitä on omassa näkemyksessäni kahta erilaista tyyppiä, vaikka niiden käyttötarkoitus on sama: verkkosivu, joka on erikseen tehty näyttämään luotettavalta ja oikealta sivustolta (esim. Office365-kirjautumissivun näköiseksi tehty) tai aivan oikea sivusto, joka on kaapattu hyökkääjän toimesta. Niiden ero on se, että ensimmäisen voi tarkalla silmällä ja fiksulla nettikäytöksellä välttää, kun taas jälkimmäiselle ei voi paljon itse tehdä. Yleensä nämä ovat tavallisia sivuja, joille on saatu pääsy ja asetettu haitallista koodia ajamaan. Tämän seurauksena saatetaan ottaa talteen kirjautumistietoja tai ajaa koodia käyttäjän tietokoneella ilman käyttäjän tietoa.

# 3 Syvempi perehtyminen tietojenkalastelun menetelmiin

Tietojenkalastelua toteutetaan suurella määrällä menetelmiä. Aihetta käsiteltiin luvussa 2.3, mutta tämän kappaleen tarkoitus on tutkia vielä syvemmin näitä erilaisia menetelmiä sekä toimia yhteytenä avaamaan tietojenkalastelun monia seurauksia. Monesti ajatellaan, että huijausviestit saattavat esiintyä vain sähköpostissa mutta tämä ei pidä paikkaansa. Maailma on jatkuvasti kasvavassa määrin lähestymässä tilannetta, jossa aina suurempi määrä laitteita on yhdistettynä internettiin; yritysten laajentaminen verkkosivuiltaan sosiaaliseen mediaan on aiheuttanut räjähdysmäisen hyökkäysvektorien kasvun.

On tärkeää huomioida myös tietojenkalastelun avainkohteet. Erään tutkimuksen aikana taloudellinen sektori oli suurin kohderyhmä tietojenkalastelulle (Wright, Aaron & Bates, 2016). Tämä ei ole kuuden vuoden aikana muuttunut juuri mitenkään, sillä uusimman AWPG-raportin mukaan taloudelliseen sektoriin kohdistuu 27,6 % tietojenkalastelusta (APWG, 2022b). Yksityisihmisille taas sosiaalinen media ja sinne itsestään asioiden jakaminen on tehnyt tietojenkalastelusta monella tavalla helpompaa. Ihmisten yhteystiedot ovat helpommin saatavissa ja on helpompaa kohdistaa tietojenkalastelua, joka osuu kohteen kiinnostuksiin, mikä puolestaan nostaa vastauksen saamisen todennäköisyyttä.

## 3.1 Puhelinpohjainen tietojenkalastelu

Puhelimitse tapahtuvaan tietojenkalasteluun sisältyy puhelimitse sekä tekstiviesteillä toteutettu tietojenkalastelu. Tekstiviestitse tapahtuva tietojenkalastelu vaikuttaa varsinkin yksityisihmisiin, sillä useassa tietojenkalastelukampanjassa levitetään laajalti tekstiviestiä, joissa kehotetaan avaamaan linkki ja seuraamaan ohjeita. Tästä hyvä esimerkki on ainakin Suomessa suosittu “tullihuijaus”, jossa ilmoitetaan tullimaksusta, jota ei oikeasti

ole olemassa. Usein tekstiviestihuijaukset tulevat numeroista, jotka pystytään helposti erottamaan oikeasta lähteestä. Viime vuosina on ilmaantunut myös huijausviestejä, jotka näkyvät samassa ketjussa oikean lähettäjän viestien kanssa. Tarkoituksena voi olla suoran maksutoimituksen hakeminen linkin avulla mahdollisesti yritys urkkia viestin kautta henkilötietoja, kuten luottokortin tietoja, pankkitilin tunnuksia tai salasanoja; huijausviestit voivat sisältää linkkien lisäksi myös kehotuksia ottamaan numeroon yhteyttä tai annettuun sähköpostiosoitteeseen, jotta kohdetta pystyttäisiin manipuloimaan lisää. (Mishra & Soni, 2019)

Puhelinsoitoilla tapahtuvassa tietojenkalastelussa ei tavallisesti tavoitella välitöntä voittoa, ellei kyseessä ole jokin monivaiheinen huijaus. Puhelimitse pyritään luomaan kontakti kohteen kanssa, jotta tietojenkalastelua saataisiin jatkettua. Harvoin siis yhden puhelun aikana tähdätään siihen, että kohteelta saataisiin huijattua vaikkapa rahaa. Tällaisesta monivaiheisesta huijauksesta esimerkkinä olisi vaikka it-tukihuijaukset, jossa puhelimitse esitetään auttavan jonkin tietoteknisen ongelman kanssa kohteen tietokoneella. Oikeana tavoitteena huijauksessa on saada uhrilta rahaa, joko suoraan tilisiirrolla tai usein jollakin laajasti käytössä olevalla lahjakortilla.

Nämä esimerkit tosin ovat paremminkin esimerkkejä huijauksista, eivätkä niinkään tietojenkalastelusta. Yksityishenkilöiltä harvoin etsitään mitään tiettyä tietoa, vaan suoraa ja nopeaa rahallista hyötyä. Yritysten tapauksessa taas puhelimitse tapahtuvassa tietojenkalastelussa tarkoituksena on saada selville tietoa, jota ei ole julkisesti tarkoitus saada. Tähän kuuluu esimerkiksi yritykseen soittaminen, jossa puhelun aikana tarkoitus on selvittää yhteystietoja, joita ei löydy muuten.

Tekstiviestitse tietojenkalastelua yrityksissä voidaan toteuttaa hyvin samanlaisella tavalla kuin sähköpostitsekin. Esimerkkinä toimii viesti, jossa muistutetaan vanhentuvasta käyttäjätunnuksesta tai salasanasta, joka täytyy muuttaa viestin sisältämän linkin kautta.

Tuoreimmassa APWG:n raportissa on todettu jyrkkä 70 % kasvu puhelimitse tapahtuvan tietojenkalastelun sekä huijausten kannalta. Puhelimitse huijauksia toteutetaan myös viestipalveluiden, kuten WhatsAppin ja Facebook Messengerin kautta. Kuitenkin tutkimuksessa todettiin tekstiviestien olevan suuressa roolissa edelleen. (APWG, 2022b)

### 3.2 Sähköpostipohjainen tietojenkalastelu

Sähköpostitse tapahtuva tietojenkalastelu kohdistuu sekä yksityishenkilöihin että yrityksiin. Sähköpostin vahvuudet tietojenkalastelun kannalta ovat mahdollisuus sisällyttää helposti haitallisia ohjelmia linkkeihin tai liitteisiin, ja mahdollisuus lähettää massana viestejä. Nämä mahdollisuudet johtavat korkeaan vastaustodennäköisyyteen, joka puolestaan mahdollistaa haitalliset jatkotoimet.

Rahallista haittaa sähköpostihuijauksilla voidaan myös hakea välittömästi. Yksityishenkilöille tämä saattaa esiintyä arvontavoitoilla, joihin ei muista edes liittyneensä, tai tuntemattomien sukulaisten jättämiin perintöihin. Yleensä huijaukset olisivat helposti tunnistettavissa, mutta huonolla ymmärryksellä aiheesta ja viestien luomasta kiireen tunteesta johtuen monet silti jäävät näihin huijauksiin. Yrityksille sähköposteja käytetään yksityishenkilöihin verrattuna monipuolisemmin. Tarkoituksena voi olla käyttäjätunnusten ja salasanojen selvittäminen, korkeamman aseman omaavan työntekijän yhteystietojen selvittäminen, haittaohjelmien, kuten kiritysohjelmien tai keyloggereiden asentaminen sekä suorat rahalliset huijaukset. Rahallisista huijauksista tuon esille kaksi esimerkkiä: toimitusjohtajahuijaus sekä BEC (Business E-mail Compromise).

Toimitusjohtajahuijauksessa tarkoitus on lähettää jollekin tärkeässä roolissa, mutta ei kuitenkaan seniorina toimivalle henkilölle sähköposti, jossa esitetään olevan tämän henkilön yläpuolella toimiva henkilö. Usein kohteina ovatkin henkilöt, jotka ovat yritysten talousasioista vastuussa. Tarkoitus huijauksessa on saada kohde siirtämään rahaa yritykseltä jollekin ulkomailla sijaitsevalle

pankkitilille. Tässä ideana on vedota siihen, että työntekijä uskoo pyynnön tulevan oikeasti ihmiseltä, joka on tätä korkeampana, kuten toimitusjohtajalta tai osastonpäälliköltä. Toimitusjohtajahuijauksissa painostetaan työntekijää tekemään siirron nopeasti ja korkealla prioriteetilla, sekä kierretään mahdollisuus keskustella asiasta puhelimitse. (Junger, Wang & Schlömer, 2020)

BEC-hyökkäykset toimivat siltä kannalta erilaisesti kuin toimitusjohtajahuijaus, että niissä ei niinkään käytetä mahdollisesti toimitusjohtajan tai päällikön väärennettyä sähköpostia, vaan käytetään ilmaisen sähköpostipalvelun kautta tehtyjä osoitteita. Näillä pyritään samaan kuin toimitusjohtajahuijauksessa, eli tarkoituksena on esittää työntekijää yrityksessä ja saada rahallista hyötyä. Yleensä tämä tapahtuu joko suoraan tilisiirrolla, lahjakortilla tai esittämällä työntekijää, jonka pankkitilin numero vaihtui. (APWG, 2022b)

Sähköpostien avulla levitetään myös kohdeverkkoihin erilaisia haittaohjelmia. Näiden käyttötarkoituksia ja vaikutuksia avaan tarkemmin vielä työn seuraavassa osassa. Kuitenkin listatakseni ainakin muutamia esimerkkejä: kiristysohjelmat, joilla kohteen tiedostoja salataan ja vaaditaan rahaa salauksen purkamiseksi ja keyloggerit, joiden tarkoitus on passiivisesti toimia kohteen laitteella ja kerätä napinpainalluksia ja näin kalastella esimerkiksi käyttäjätunnuksia ja salasanoja. Äärimmäisessä tapauksessa haittaohjelma voi toimia takaovena haitalliselle tekijälle, joka antaa pääsyn laitteelle ja tätä kautta yrityksen verkkoympäristöön.

# 4 Tietojenkalastelun seuraukset

Onnistuneesta tietojenkalastelusta voi seurata useita haitallisia seurauksia, joiden vaikutukset voivat olla laajoja. Usein tietojenkalastelun tarkoituksena on rahallinen hyöty hyökkääjälle, mutta tietojenkalastelulla voi myös olla käyttötarkoituksia muussa haitallisessa toiminnassa tai jopa poliittisia seurauksia. Tuon esille muutamia esimerkkejä tunnetuista tai muuten merkittävistä tietojenkalasteluhyökkäyksistä sekä kampanjoista, jotta saan tuotua esille konkreettisia esimerkkejä tietojenkalastelun vaikutuksesta oikeassa elämässä.

## 4.1 Luvaton pääsy tietoihin

Tietojenkalastelun nimestä tämä on ehkä ensimmäinen seuraus, joka tulee ihmisille mieleen. Luvaton pääsy tietoihin on seuraus siitä, kun erilaisia menetelmiä käyttäen on haitallinen tekijä saanut tietoonsa jotakin, jota ei olisi tarkoitus olla ulkopuolisen tiedossa. Tämä on sinänsä laaja seuraus, sillä yrityksestä, sen koosta ja tiedon herkkyydestä riippuen voi olla vaikea sanoa, mitä seuraukset voivat eri tilanteissa olla. Luvattomiin tietoihin voidaan lukea esim. käyttäjätunnuksia, salasanoja, yrityssalaisuuksia, taloudellisia tietoja, yhteystietoja tai jopa ihmisten aikatauluja ja kalentereja.

Luvaton pääsy tietoihin tapahtuu yleensä sosiaalisen manipulaation kautta. Sähköpostiviestillä tai puhelimitse haitallinen tekijä lähtee urkkimaan tietoa yrityksestä tai henkilöltä. Usein tämä toteutetaan esittämällä jotakin tahoa, jolla olisi auktoriteetti ja lupa näihin tietoihin. Tässä on tärkeä muistaa, että tahot, joilla olisi lupa näitä tietoja kysellä eivät melkeinpä ikinä näitä tietoja kysele. Kaikki ovat varmasti tavanneet jonkinlaisen muunnoksen lauseesta “ylläpito ei ikinä kysele käyttäjätunnuksiasi tai salasanojasi”.

Tämä luvaton tieto ei myöskään aina pysy pelkästään haitallisella tekijällä. Pimeässä verkossa toimii huutokauppoja sekä avoimia kauppasivustoja, joissa käydään kauppaa selvitetyistä käyttäjätunnuksista, salasanoista sekä yritysten

salatuista tiedoista. Tämän takia tietojenkalastelun vaikutukset eivät aina ole myöskään välittömiä; selvitetty tieto saatetaan myydä eteenpäin ja haittoja ilmenee vasta kaukana tulevaisuudessa. Myös yrityksen sisällä pyörivien yhteystietojen selvittäminen ja jakaminen voi olla todella haitallista, sillä tämä mahdollistaa tietojenkalastelun kohdistamista joihinkin tiettyihin henkilöihin. Joko tämä antaa mahdollisuuden lähteä yrittämään tietojenkalastelua näihin selvitettyihin yhteystietoihin, tai näiden avulla voidaan toteuttaa muita huijauksia. Esimerkiksi taloudesta vastaavan osastopäällikön sähköpostin avulla voidaan tehdä melkein identtinen kopio, josta lähettää pyyntöjä lähettää maksuja ulkomaan tileille, kuten toimitusjohtajahuijauksissa tuli todettua.

## 4.2 Haittaohjelmien leviäminen

Vaikka APWG:n mukaan yritykset ovat lähiaikoina parantaneet tietoturvaa siihen malliin, että haittaohjelmat pidetään tehokkaasti pois työntekijöiden sähköposteista, ei niitä kuitenkaan ole täysin kitketty pois. Erilaisilla huijausmetodeilla saadaan kuin saadaankin ihmisiä asentamaan itse haittaohjelmia laitteilleen, minkä vaikutukset voivat olla tuhoisia. Vakavimpia haittaohjelmia ovat kiristysohjelmat, joiden toiminta perustuu haitallisten tekijöiden ohjelmaan, jonka päätoimintatapa on salata kohteen kriittiset tiedostot. Tämän salauksen jälkeen tekijät vaativat suuria summia rahaa salausten purkamista vastaan. Tässä voidaan myös käyttää hyväksi luvatonta pääsyä tietoon, jossa kohdeyritystä uhataan yrityssalaisuuksien levittämisellä, jos maksua ei toteuteta. Mainittakoon silti, että varsinkin yritystietoturva alkaa olemaan niin tehokasta, että haitalliset tekijät harvoin saavat haittaohjelmia työntekijöiden sähköpostilaatikoihin asti. APWG:n mukaan huimat 95 % haitallisista sähköposteista nimenomaan olivat tarkoitusperältään etsimässä tietoa tai hakemassa vastausta, kuten BEC-huijauksessa. (APWG, 2022b)

Kiristäminen ja haittaohjelmat koskettavat myös yksityishenkilöitä. Internetistä voi lukea satoja kokemuksia kiristetyiksi tulleilta ihmisiltä. Usein tämä manipulaatio kohdistuu ihmisiin, joita huijataan lähettämään jotain arkaluontoista tietoa tai kuvia itsestään haitalliselle tekijälle. Tämän jälkeen

uhria aletaan painostaa lähettämään rahaa tekijälle, tai uhrin jakamat arkaluontoiset asiat jaetaan tämän perheelle ja ystäville. Myös haitallisten sähköpostiviestien kautta ihmisten tietokoneille ja mobiililaitteille saatetaan levittää haittaohjelmia, kuten yritysmaailmassakin. Yksityiselämässä näkyy samanlaisia kiristysohjelmia ja vakoiluohjelmia, joiden tarkoitus on saada selville esimerkiksi pankkitunnuksia tai muuta yksityistä tietoa.

### 4.3 Luvaton pääsy järjestelmiin

APWG:n tutkimuksen mukaan haittaohjelmia ei usein saada toimitettua onnistuneesti yritysten sähköposteihin. Tämän takia suositumpi menetelmä sähköpostin käyttöön tietojenkalastelussa on käyttäjätunnusten urkkiminen. Jos haitallinen tekijä onnistuu tietojenkalastelulla saamaan käyttäjätunnuksia ja salasanoja haltuunsa, voi näillä tiedoilla lähteä rakentamaan ja etsimään uusia hyökkäysvektoreita kohteen järjestelmässä. Tämä mahdollistaa myös haittaohjelmien asentamisen kohteen laitteelle, josta niitä pystyy levittämään eteenpäin verkkoon. Täten haittaohjelmat eivät ole ainoastaan uhka suorana latauksena sähköpostista, vaan ovat myös seuraus käyttäjätunnusten vuodosta.

Luvaton pääsy ja käyttäjätunnusten etsiminen ei kosketa vain yrityksiä, vaan myös yksityishenkilöitä. Erityisenä kohteena yksityiselämässä ovat erilaiset suoratoistopalveluiden käyttäjätunnukset, joita myydään eteenpäin itsellä pitämisen sijasta. (Broadcom, 2016)

# 5 Merkittäviä esimerkkejä tietojenkalastelusta – yksittäistapauksia ja kampanjoita

Tässä luvussa käsitellään merkittävimpiä esimerkkejä tietojenkalastelusta ja sen vaikutuksista oikeassa elämässä. Esimerkkien vaikutukset vaihtelevat rahallisesta menetyksestä sotilaalliseen/poliittiseen vaikutukseen. Esimerkit eivät ole mitenkään järjestyksessä vaikutusten suuruuden tai vakavuuden kannalta, vaan ne ovat listattu vain merkittävinä tapahtumina. Valitsin nämä esimerkit, sillä niissä esiintyy monipuolisesti tietojenkalastelun menetelmiä sekä niiden vaikutuksia. Jotkut ovat olleet myös merkittäviä skaalaltaan; sillä esimerkiksi Amy Myers Jaffe kuvailee Colonial Pipelineen kohdistunutta hyökkäystä “tärkeimpänä onnistuneena hyökkäyksenä Yhdistysvaltojen energiainfrastruktuuriin” (Gonzalez, Lefebvre & Geller, 2021).

## 5.1 Hyökkäys Ukrainan sähköverkkoon (2015)

Vuonna 2015 tapahtuneessa hyökkäyksessä Ukrainen sähköverkkoon hyödynnettiin kohdistettua tietojenkalastelua. Tällä menetelmällä saatiin ensimmäinen pääsy järjestelmiin, jonka jälkeen hyökkääjät käyttivät BlackEnergy 3 -haittaohjelmaa katkaisemaan etäyhteydellä n. 230 000 ihmiseltä sähköt 1–6 tunnin ajaksi. Vaikka vaikutus on prosentuaalisesti pieni ihmisiin, jotka Ukrainassa sähköä käyttävät, oli tämä silti 2015 ensimmäinen onnistunut kyberhyökkäys energiantuotantoon. 2019 tutkimuksessaan Overland mainitsee, että on tärkeää panna merkille Ukrainan olevan erikoistapaus, sillä osa sen infrastruktuurista on huonokuntoista ja suuri osa sähköverkosta on rakennettu aikana, jolloin Ukraina kuului vielä Neuvostoliittoon. Sähköverkkoa on myös korjattu ja paikattu venäläisillä osilla ja tietokoneohjelmistot ovat myös tuttuja venäläisille. Lisäksi Venäjän ja Ukrainan välinen sotatilanne ja korkea mahdollisuus venäläiseen soluttautumiseen vaikuttaa tilanteen poikkeuksellisuuteen. (Overland, 2019).

### 5.2 Colonial Pipeline -hyökkäys (2021)

Colonial Pipelinen hyökkäyksessä on epävarmaa, mitä tietojenkalastelumenetelmää käytettiin. Tutkinnan mukaan on hyvin todennäköistä, että murretut käyttäjätunnukset ostettiin pimeästä verkosta. Näillä käyttäjätunnuksilla järjestelmään levitettiin kiristysohjelma, jolla vaadittiin maksuksi 75 bitcoinia tai 4,4 miljoonaa dollaria. Summa maksettiin ja vaikka osa maksusta saatiin myöhemmin takaisin, oli tällä hyökkäyksellä laajoja seurauksia tietoturvalle Yhdysvalloissa. Toukokuun 12. päivä 2021 Yhdysvaltojen presidentti Joe Biden allekirjoitti asetuksen 14028, jonka tarkoitus on nostaa tietokoneohjelmien tietoturvastandardeja hallituksen käyttöön, kiristää valvontaa ja tietoturvaa olemassa olevissa järjestelmissä, parantaa tiedonjakoa ja kouluttamista, perustaa kyberturvan arviointitoimikunta sekä parantaa kriisivalmiutta. (Executive Order 14028, 2021).

### 5.3 Facebookin & Googlen huijaukset (2013–2015)

Facebookin ja Googlen huijauksissa käytössä oli menetelmä, jota ei tässä työssä vielä aikaisemmin listattu. Kyseessä on yrityksiin kohdistuva rahallinen huijaus, jossa yritykselle lähetetään laskuja jonkun yhteistyökumppanin nimissä. Näissä laskuissa on kuitenkin huijarin tilinumero maksukohteena. Huijaus perustuu summien kohtuullisuuteen, jota ei tarkisteta kunnolla, sillä se vaikuttaa tavalliselta kyseiselle yhteistyökumppanille. Huijauksessa kahden vuoden aikana liettualainen mies huijasi vähän yli 100 miljoonaa euroa, kunnes jäi kiinni ja joutui vankilaan. (Huddlestone Jr., 2019).

### 5.4 FACCn ja Crelan Pankin toimitusjohtajahuijaukset (2016)

FACCn ja Crelan Pankin huijauksissa nähtiin onnistunut toimitusjohtajahuijaus. Siinä seurattiin kaavaa, jossa hyökkääjä oli onnistunut jäljittelemään toimitusjohtajan sähköpostiosoitetta ja lähetti työntekijälle viestin, jossa pyysi kiirrellisesti siirtämään suuren summan rahaa tilille osana tärkeää hankintaa.

Raportoinnissa on jäänyt epäselväksi esimerkiksi FACC:n kohdalla, mitä oli mennyt väärin tietoturvallisesti, että huijaus onnistui. Kuitenkin toimitusjohtaja Walter Stephanin todettiin olevan ainakin joiltain osin epäonnistunut toimissaan. Sisäisen tutkinnan jälkeen toimitusjohtaja sekä talousosaston päällikkö erotettiin yrityksestä. FACC:n tapauksessa siirrettiin 42 miljoonaa euroa, kun taas Crelan pankin tarkkaa määrää ei tiedetä. Pankki kertoi jälkeenpäin koko tilanteen maksaneen 75,6 miljoonaa euroa, mutta on vaikea sanoa, kuuluiko tähän oikaisumaksuja. (Cohen, 2022; Zorz, 2018).

### 5.5 Sony Pictures -tietovuoto (2014)

Sony Pictures -elokuvastudioon kohdistunut tietovuoto tapahtui monessa vaiheessa. Alkuperäinen pääsy saatiin lähettämällä osoitteesta, joka näytti pintapuolisesti Applen sähköpostilta, viestiä johtajille studiossa. Näissä viesteissä oli linkki huijaussivustoon, joka pyysi käyttäjätunnuksia ja salasanoja. Näiden käyttäjätunnusten avulla hyökkääjät pääsivät käsiksi kaikkeen dataan, jota Sony Picturesta oli. Internettiin vuodettiin työntekijöiden henkilötietoja ja palkkatietoja. Lisäksi vasta suunniteltuja tai tuotannossa olevia elokuvia vuodettiin internettiin. Hyökkäykseen oli myös yhdistetty poliittista viestintää, sillä tekijät vaativat studion peruvan The Interview -komediaelokuvan julkaisun. Elokuvassa tehdään pilaa Pohjois-Korean johtajan kustannuksella, ja myöhemmin Yhdysvallat ovat syyttäneet Pohjois-Korean tukeneen hyökkäystä. Pohjois-Korea on kuitenkin kieltänyt kaiken syyllisyyden hyökkäykseen. (Gabi & Siman-Tov, 2014)

### 5.6 Koronaviruksen vaikutus tietojenkalastelukampanjoihin

COVID-19-pandemian aikana todettiin myös epidemia huijauksissa ja tietojenkalastelussa. Rokotuksia ja ihmisten paniikkia käytettiin hyväksi kalastelemaan ihmisten henkilötietoja haitallisilla viesteillä ja linkeillä, joissa esitettiin kyselyitä tai tarjottiin mahdollisuutta hakea rokotteita. Myös rahallista hyötyä haettiin, sillä huijarit myös esittivät tarjoavansa maksullisia rokotuksia.

Huijaukset kohdistuivat jopa sellaisiin henkilöihin, jotka syystä tai toisesta eivät rokotuksia halunneet. Huijarit tarjosivat netissä mahdollisuuksia ostaa negatiivisia testejä tai rokotustodistuksia, mutta on epävarmaa, saiko luvattuja tuotteita ikinä. (Federal Communications Commission, 2022)

Pandemia aiheutti myös maailmanlaajuisen muutoksen korotettuun määrään etätyöskentelyä, jonka vaikutukset näkyvät edelleen maailmassamme. Monet työntekijät joutuivat sopeutumaan hätäisesti digitaalisiin viestintä- ja työskentely-ympäristöihin. Usein työntekijät eivät saaneet kunnollista koulutusta tai orientaatiota etätyöskentelyyn ja sen tietoturvaan. Tämä laajensi tietoturvahaavoittuvuuksia erittäin jyrkästi eikä tietojenkalastelu ollut tämän suhteen poikkeus. Asioita, joita pystyttiin ennen jakamaan turvallisesti toimistossa, kirjoitettiin suojaamattomiin viestintäpalveluihin, joista tieto vuosi herkästi ulospäin. (Al-Qahtani & Cresci, 2022)

# 6 Tietojenkalastelun nykytilanne

Tietojenkalastelun nykytilanteen tutkimista varten valitsin tarkasteltavaksi vuosien 2020–2022 välisen ajanjakson. Koin tämän aikavälin antavan riittävän hyvän kuvan alkavan vuosikymmenen tietojenkalastelun tilanteesta ja sen erilaisista vaikutuksista. Lähteenä tilanteen katsastamiseen käytin APWG:n neljännesten raportteja, joita on 2020 ja 2021 tehty 4 ja 2022 vasta 2.

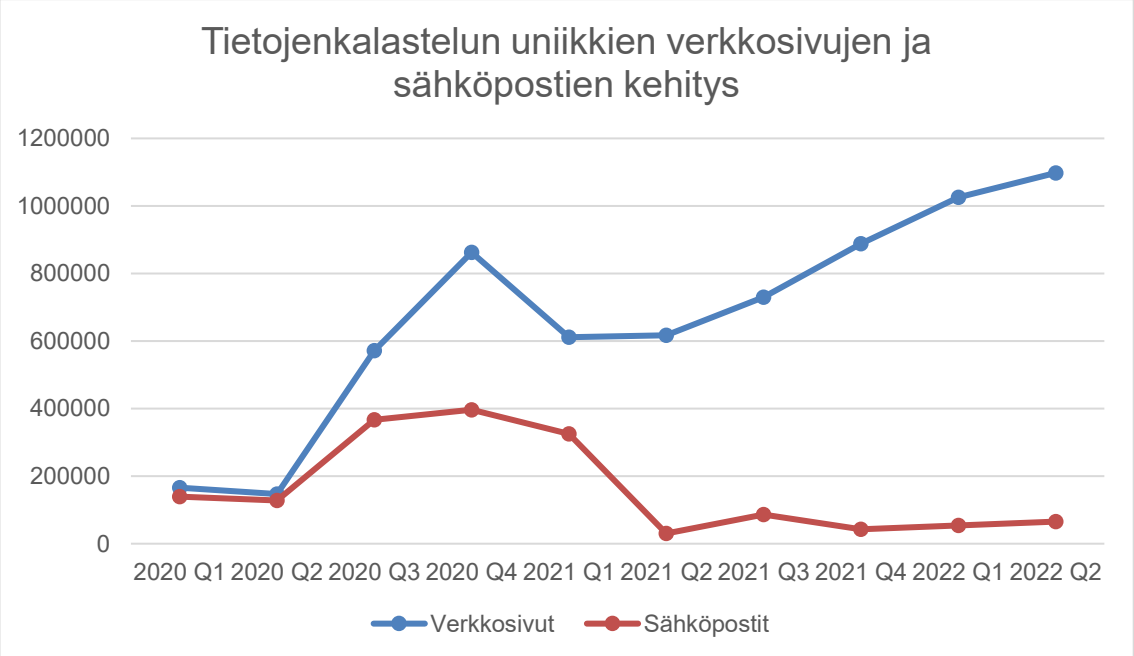
Tutkimuksen rajaamiseksi paremmin työssä jaetaan omiin osioihin tärkeimmät käsiteltävät aiheet, eli uniikit verkkosivut ja sähköpostit sekä toimialat. Näin luodaan kuva jokaisen tilanteen muutoksista viimeisten vuosien aikana, sillä jopa 2,5 vuoden aikana on tapahtunut suurta kasvua sektorilla. APWG:n raporttien mukaan itsessään vuoden 2020 aikana tietojenkalastelun määrä tuplaantui ja 2022 puolessavälissä tietojenkalastelun määrä on nelinkertaistunut 2020 alkuun verrattuna. (APWG, 2022b)

## 6.1 Uniikit tietojenkalastelusivustot ja sähköpostit

Avainmenetelmät, joita APWG seuraa aktiivisesti raporteissaan tietojenkalastelun ja huijausten tilanteen selventämiseksi ovat uniikit sivustot ja sähköpostit. Niiden avulla pystytään luomaan selkeämpi kuva siitä, kuinka paljon uhkia kullakin neljänneksellä on ollut. Kaavion selventämänä näkee helposti, kuinka suuri vaikutus COVID-19-pandemialla oli tietojenkalastelun nousuun. Pandemian alkaessa 2020 alkupuolella tietojenkalastelu lähti räjähdysmäiseen kasvuun eikä ole toistaiseksi tullut alaspäin, vaan päinvastoin 2022 on nähty ennätysmäisiä määriä tietojenkalastelua. Kiinnostavaksi datapisteeksi jää uniikkien tietojenkalastelusähköpostien laantuminen samaan aikaan, kun huijaussivustot jatkavat nousuaan. Tämä johtuu todennäköisesti yritysten lisäpanostuksesta tietoturvaan uhan noustessa esille etätyöskentelyn aikana, minkä seurauksena yritysten tietoturva on tiukentanut sähköpostiin kohdistuvia rajoituksia. Huijaussivustoja tosin on vaikeampi välttää, sillä niiden

levittämiseen käytetään usein paljon luotettavamman näköisiä viestejä verrattuna suoriin huijausviesteihin. (APWG, 2022b)

APWG kertoo saavansa datansa tutkimukseen kahdesta lähteestä: heille ilmoitetuista tietojenkalastelukampanjoista joko jäseniltä tai järjestön ulkopuolelta tulevista ilmoituksista, sekä jäsenten tietojenkalasteluverkkosivujen lisäämisestä APWG:n eCrime eXchange -palveluun. Näiden kahden datapisteen erona on se, että verkkosivustoja voidaan levittää tuhansilla erinäköisillä osotteilla, jotka ohjaavat uhrin samalle sivustolle. Tästä syystä uniikkien verkkosivujen seuraaminen antaa tarkemman tilanteen siitä, kuinka paljon tietojenkalastelua tapahtuu. Sähköpostikampanjoissa taas saatetaan käyttää samoja otsikoita, mutta johtaa eri huijaussivustoille. Tällä tilastolla pystytään karkeasti arvioimaan tietojenkalastelun monipuolisuutta ja se voi toimia korvikkeena tietojenkalastelun määrän mittaamiselle. Kuitenkin uniikit verkkosivut ovat tähän parempia. (Kuvio 1.)




Kuvio 1. Uniikit tietojenkalastelukampanjoissa käytetyt sivustot ja sähköpostit (APWG 2020; APWG 2021; APWG 2022).

## 6.2 Suurimmat toimialat tietojenkalastelun kohteena

APWG tuo esille raporteissaan toimialat ja toimialojen osuudet tietojenkalastelusta käsitellyllä neljänneksellä. Tässä työssä tarkasteltiin vuosia kokonaisuuksina ottamalla keskiarvo toimialojen osuuksista jokaisesta neljänneksen raportista. Ratkaisua vaikeutti jonkun verran “muu” osion muuttuminen ja irtaantuminen omiksi osioikseen, jos ne kasvoivat tarpeeksi suuriksi. Työssä mainitaan vuosikohtaisesti nämä tärkeät muutokset, jos ja kun niitä tulee vastaan.

### 6.2.1 Toimialat tietojenkalastelun kohteena 2020

Vuoden 2020 alussa koko maailmaan vaikutti COVID-19-pandemia. Tästä aiheutuneen etätyöskentelyn ja muun verkkotoiminnan käytön suurentuminen johti suureen nousuun kyberrikollisuudessa, eikä tietojenkalastelu ollut poikkeus. APWG:n ensimmäisen neljänneksen raportissa on omistettu oma osuutensa koronaviruksen vaikutuksista huijauksiin. (APWG, 2020a)

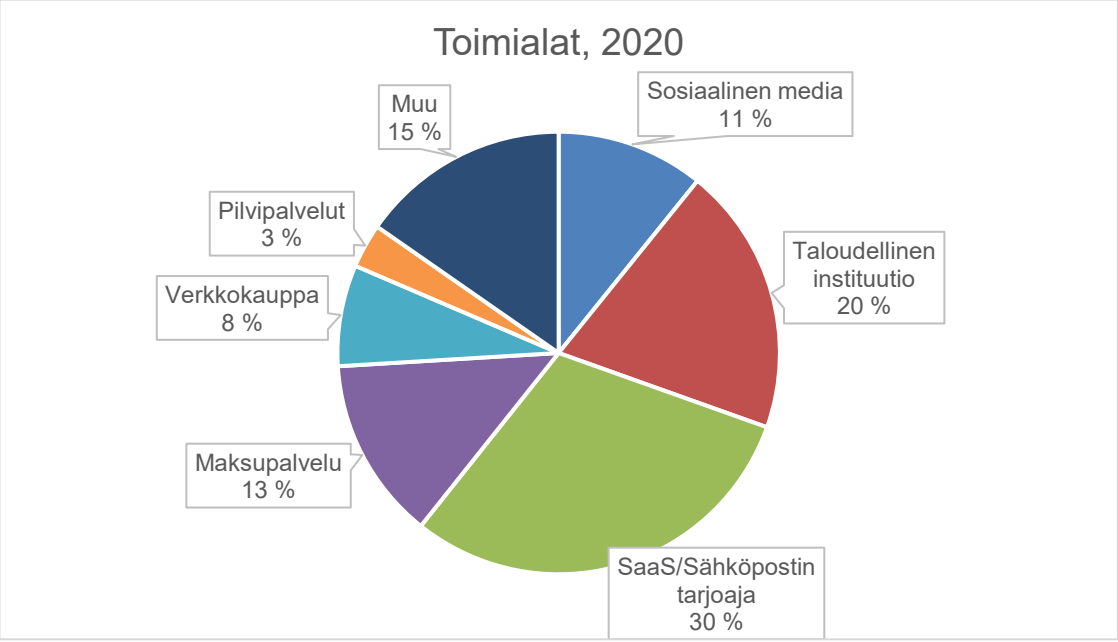
Työ ei kuitenkaan käsittele jokaista neljännestä erikseen, vaan keskittyy erityisesti “muu”-osion sisältöön. 2020 ensimmäisen neljänneksen kaavioissa esiintyi vielä 2 eri lohkoa otsikolla “other”, mutta neljännesten edetessä nämä alkoivat pirstaloitua omiin osioihinsa. Raporteista jää epäselväksi se, että kasvoivatko osiot tarpeeksi suuriksi oikeuttaakseen omat lohkonsa vai selvennetiinkö tilastoja vain, jotta saataisiin parempi kuva tilanteesta. (APWG, 2020a; 2020b; 2020c; 2020d)

Jo toisessa neljänneksessä 2020 näkyy ensimmäinen erotus “other”-osiosta, missä mainitaan logistiikkaan ja kuljetuspalveluihin kohdistuvat hyökkäykset. Tämän sektorin erottelu kuitenkin kääntyy vuoden aikana järkeväksi, sillä tähän toimialaan kohdistuvat hyökkäykset kasvoivat 2. neljänneksestä melkein kaksinkertaisesti 4. neljännekseen mennessä. Vaikka 2. neljänneksellä logistiikkaan kohdistui vain 3,5 % tietojenkalasteluhyökkäyksistä, 4.

neljänneksellä logistiikkapalvelut vastasivat jo 6,4 % raportoiduista hyökkäyksistä. (Kuvio 2.)

Toinen sektori, joka raporteissa irtaantui “muu”-osiosta omaksi lohkokseen, oli teleoperaattorit. Tämä jako tuli vasta 3. neljänneksellä, jolloin teleoperaattorit vastasivat 3,2 % tietojenkalasteluhyökkäyksistä. Viimeisellä neljänneksellä oli kuitenkin tämä laskenut 2,5 %:iin. (Kuvio 2.)

Vielä merkittävä maininta tulee vuoden viimeisestä raportista, jossa kerrotaan koko 2020 jakson ajalta kymmeneen eniten kohdennettuun organisaatioon kohdistuvan n. 60 % kaikista tietojenkalasteluhyökkäyksistä. Raportissa mainitaan lisäksi pienen määrän hyökkäyksistä kohdistuvan kryptovaluutan vaihtosivuihin; voimme nähdä näiden hyökkäysten määrän kasvaneen vuosien 2021-2022 raporttien välillä kryptovaluutan saapuessa valtavirran suosioon. (APWG, 2020d)

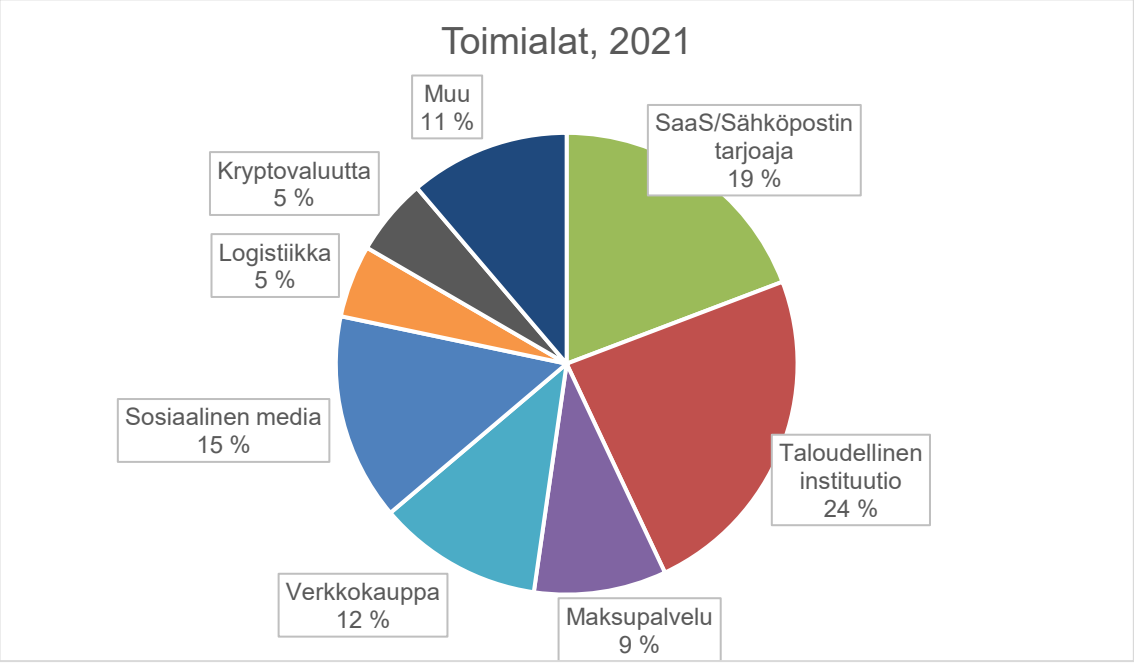



Kuvio 2. Toimialojen keskiarvo tietojenkalastelun kohteena 2020 (APWG, 2020a; 2020b; 2020c; 2020d).

### 6.2.2 Toimialat tietojenkalastelun kohteena 2021

Vuoden 2021 aikana näemme pieniä eroavaisuuksia edellisen vuoden tuloksiin. Taloudellisiin instituutioihin kohdistuvat hyökkäykset ovat pysyneet muutaman prosenttiyksikön päässä edellisestä vuodesta, mutta esim. verkkosovelluspalvelun (engl. Software as a Service, SaaS) sekä sähköpostin tarjoajiin kohdistuvat hyökkäykset ovat laskeneet jyrkästi. Tämän vuoden aikana todettiin myös kryptovaluuttoihin kohdistuneiden hyökkäysten kasvaneen niin suureksi toimialaksi, että se lisättiin seurantaan omaksi sektorikseen. Kryptovaluutan osuus tietojenkalasteluhyökkäyksistä oli alhaisimmillaan 2021 aikana aluksi 2,0 % ja nousi 3. neljänneksellä 7,5 %:iin, kunnes laski vuoden lopussa 6,5 %:iin. (APWG, 2021a; 2021b; 2021c; 2021d)

Vielä vuoden keskivaiheessa teleoperaattorit mainittiin pienenä sektorina, jolloin toimiala vastasi 2,4 % tietojenkalasteluhyökkäyksistä 2. neljänneksellä ja 3,5 % 3. neljänneksellä (Kuvio 3.). Sektoria ei kuitenkaan mainita muissa raporteissa enää erikseen, joten se on tätä kuvausta varten pienen osuuden ja osittaisen puuttumisen takia 1. ja 4. neljänneksellä sisällytetty “muu”-osioon.

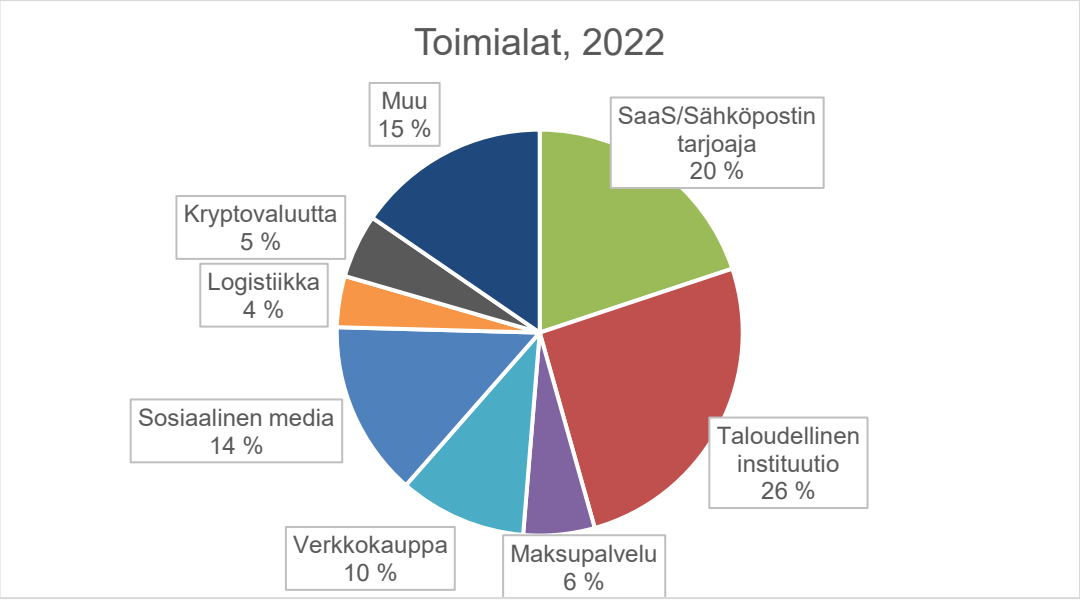



Kuvio 3. Toimialojen keskiarvo tietojenkalastelun kohteena 2021 (APWG, 2021a; 2021b; 2021c; 2021d).

### 6.2.3 Toimialat tietojenkalastelun kohteena 2022 1. ja 2. neljänneksellä

Vuotta 2022 koskevat tilastot käsittelevät vain kahta ensimmäistä neljännestä, sillä opinnäytetyö kirjoitushetkellä muita APWG:n raportteja ei valitettavasti ollut vielä julkaistu. Tästä johtuen meille jää epävarmaksi se, millaista kehitystä sektoreilla tulee tapahtumaan vuoden 2022 edetessä. Tilastoilla saa kuitenkin luotua kuvaa siitä, millaiselta tilanne on alkuvuodesta näyttänyt. Kuten muinakin vuosina, taloudelliset instituutiot ja SaaS/sähköpostin tarjoajat ovat suurimmat kohteet tietojenkalasteluhyökkäyksille. Kryptovaluutta on myös onnistunut ainakin toistaiseksi vakiinnuttamaan itsensä rikollisten kohteeksi. (Kuvio 4.)

Vuoden 2022 2. neljänneksellä erityismainittavaa oli puhelimen välityksellä tapahtuvien huijausten kasvaneen melkein 70 % verrattuna vuoden 1. neljännekseen (APWG, 2022b). Myös kryptovaluutasta puhutaan erikseen, sillä sen vakiintumisen jälkeen 2. neljänneksellä kryptovaluuttaan kohdistuva tietojenkalastelu oli aktiivisempaa kuin verkkopeleihin, hallitusten verkkosivuihin ja teleoperaattoreihin yhteensä (APWG, 2022b).




Kuvio 4. Toimialojen keskiarvo tietojenkalastelun kohteena 2022 (APWG, 2022a; 2022b).

# 7 Tietojenkalastelun ja sen vaikutusten lieventäminen

Tietojenkalastelun lieventämiseen on olemassa monia lieventämismenetelmiä, mutta tärkeimpiä näistä ovat ihmisten kouluttaminen ja hyvien tietoturvakäytäntöjen asettaminen sekä noudattaminen. Tietojenkalastelua voidaan lieventää joillakin teknisillä keinoilla, joita työssä käsitellään. Kyberturvallisuuskeskuksen “Pienyritysten kyberturvallisuusopas” listaa suojautumiskeinoiksi automaattiset päivitykset, automaattiset kopiot ja monivaiheisen tunnistautumisen (Kyberturvallisuuskeskus, 2020). Näiden teknisten menetelmien lisäksi käyn läpi merkittäviä asioita, joita harjoittamalla työntekijät ja yksityishenkilöt pystyvät tunnistamaan ja välttämään tietojenkalasteluhyökkäyksiä.

Alla olevat lieventämismenetelmät koskettavat pääsääntöisesti pienyrityksiä sekä yksityishenkilöitä. Suuremmilla yrityksillä on enemmän resursseja, joita käyttää tietojenkalastelun ja muiden kyberuhkien torjuntaan. Isommille yrityksille on tärkeää esim. panostaa enemmän yrityksen reagointikykyyn sekä valvontaan tietojenkalastelun kannalta, eikä suoranaisesti vaikutusten lieventämiseen.

## 7.1 Automaattiset päivitykset

Ohjelmien sekä käyttöjärjestelmien automaattisten päivitysten päällä pitäminen takaa sen, että käytössä ovat aina uusimmat versiot. Tämä ei takaa ainoastaan sitä, että järjestelmät toimivat useimmiten paremmin tai tehokkaammin, vaan päivityksissä yleisesti korjataan tiedossa olevia tietoturvahaavoittuvuuksia. Näin ollen automaattisten päivitysten avulla tai manuaalisten päivitysten tekemisellä välittömästi, kun ne ovat saatavilla, vähennetään huomattavasti tietoturvauhkien määriä järjestelmissä. (Kyberturvallisuuskeskus, 2020)

Sivuhuomiona automaattisiin päivityksiin on mainittava ohjelmistojen tai laitteiden mahdollisuus tulla EOL-tilaan. EOL eli end-of-life tarkoittaa, että kyseinen ohjelmisto tai järjestelmä on tullut elinkaarensa loppuun. Nämä ohjelmistot on erittäin tärkeää vaihtaa versioon, jota päivitetään edelleen tai

täysin uuteen ohjelmistoon, joka ajaa saman asian ja saa edelleen päivityksiä. EOL-esimerkkejä voivat olla esimerkiksi käyttöjärjestelmät, kuten vaikka Windows XP, jonka tukeminen päättyi 2014. (Kyberturvallisuuskeskus, 2020)

Järjestelmien päivitettynä pitäminen on siis erittäin tärkeää, sillä näin vähennetään haitallisten tekijöiden hyökkäyspinta-alaa. Vanhentuneilla versioilla vaikkapa sähköposti- ja PDF-lukuohjelmissa voi olla haavoittuvuuksia, joita ei enää uusista versioista löydy. Nämä haavoittuvuudet päästävät läpi tietojenkalasteluhyökkäyksiä, jotka päivitetyillä versioilla saataisiin suljettua pois. Myöskin tärkeässä roolissa ovat haittaohjelmien torjuntaohjelmistot ja niiden päivitettynä pitäminen; tämä on kuitenkin lieventämismenetelmä, eikä niinkään torjuntamenetelmä. Kun onnistuneen tietojenkalasteluhyökkäyksen jälkeen haitallinen tekijä yrittäisi levittää järjestelmään haittaohjelmia, voi torjuntaohjelmisto toimia vielä turvaverkkona ennen kuin suurempaa vahinkoa voi syntyä.

## 7.2 Automaattiset varmuuskopiot

Varmuuskopioiden luominen keskeisistä ja herkistä tiedoista on lieventämismenetelmä nimenomaan kiristysohjelmia vastaan. Kun yrityksen tärkeimmät tiedot on varmuuskopioitu ja tallennettu erilliselle fyysiselle laitteelle, voidaan huomattavasti lieventää vahinkoa, jota syntyy kiristysohjelmien seurauksena. Suurin osa kiristysohjelmista toimii salaamalla kohteen tietoja, mutta jos varmuuskopiot ovat ajantasaisia, ei kyseinen hyökkäys aiheuta yhtä paljon paniikkia ja tuhoa. Varmuuskopioiden kannalta on myös äärimmäisen tärkeää testata säännöllisesti, että niiden palauttaminen on mahdollista ja toimii moitteettomasti. Kun testaus tehdään säännöllisesti, ei oikeassa haittatilanteessa synny epävarmuutta tai tule ilmi, ettei kopioiden palauttaminen onnistukaan. (Kyberturvallisuuskeskus, 2020)

### 7.3 Monivaiheinen tunnistautuminen

Monivaiheisella tunnistautumisella tarkoitetaan useammalla eri menetelmällä tehtävää henkilöllisyyden tunnistautumista. Tässä voidaan yhdistää esim. salasana sekä matkapuhelimeen lähetettävä muuttuva koodi, kuten mobiilivarmenne (Kyberturvallisuuskeskus, 2020). Monivaiheinen tunnistautuminen antaa voimakkaan turvaverkon tietojenkalastelua vastaan, sillä jos käy vaikka niin, että käyttäjän tunnukset vuotavat, ei niitä päästä hyödyntämään ilman pääsyä myös muille tunnistautumiskeinoille. Tällä tavalla monivaiheinen tunnistautuminen minimoi huomattavasti riskiä niin pienyrityksille kuin yksityishenkilöillekin, ja omasta mielestäni se on tärkein menetelmä ottaa käyttöön aina kun mahdollista.

### 7.4 Ihmisten kouluttaminen ja harjoittelu

Tietojenkalastelun kohdistuessa ihmiselementtiin organisaatiossa on tärkeää muistaa, että työntekijöiden jatkuvalla kouluttamisella ja testaamisella saadaan luotua ymmärrystä uhasta. Kun yrityksen sisällä toteutetaan tietojenkalasteluun pohjautuvia harjoitustilanteita, niin opitaan toimimaan oikeissa tilanteissa. Näiden harjoitusten ja koulutusten kautta olisi hyvä saada selvennettyä, miten tunnistaa tietojenkalastelussa käytettyjä menetelmiä. Tärkeää olisi opettaa tunnistamaan huijausviestin tuntomerkit, kuten mahdollisesti heikompi kielen osaaminen, kiireellisen tunteen luominen viestinnällä, menneisiin tapaamisiin tai keskusteluihin (joita ei välttämättä tapahtunut) viittaaminen sekä epäilyttävät pyynnöt tunnuksista tai linkkien painamisesta.

# 8 Yhteenveto

Tietojenkalastelun nykytilanne näyttää pahalta, mutta olen varma, että yritykset ja yksityishenkilöt pystyvät mukautumaan uusiin tietoturvan haasteisiin ja kehityksiin. Pandemian aiheuttama räjähdysmäinen tietojenkalastelun kasvu saattaa aiheuttaa yrityksille suuremman motivaation kouluttaa työntekijöitään, sekä kehittää tietoturvaa vähentääkseen tietojenkalastelun tehokkuutta. Yksityiselämässä varovaisuudella sekä terveellä skeptisyydellä pystyy suojautumaan monilta mahdollisilta tietojenkalasteluhyökkäyksiltä. Etätyöskentely on myös edelleen monelle uusi työskentelytapa, ja vaikka moni yritys haluaa työntekijät takaisin toimistolle, en usko, että pääsemme tilanteeseen, jossa kaikki ovat takaisin toimistolla. Tämän takia yhä edelleen suurin vastuu tietojenkalastelun estämisestä jää jokaiselle itselleen.

Tietojenkalastelu on ilmiö, jonka en usko voivan ikinä kitkeytyä pois. Se on tekijöilleen hyvin tehokas keino saada pieniäkin etuja nopeasti kehittyvässä tietoturvaympäristössä. Koska sen kohteena on yrityksen heikoin kohta eli sen työntekijät, on mahdotonta poistaa tätä ilmiötä olemasta. Kuitenkin opinnäytetyössä kuvatuilla lieventämis- ja suojautumismenetelmillä pystytään jo vaikeuttamaan tietojenkalastelun onnistumista sekä lieventämään onnistuneiden hyökkäysten vaikutusta järjestelmiin – ja ihmisiin.

On vaikea arvioida tietojenkalastelun tulevaisuutta. Edelleen maailma etenee jatkuvasti suuntaan, jossa tietoja annetaan sekä myydään eteenpäin suuremmissa määrin. Vaikka monet IoT-ratkaisut saattavat ensin helpottaa käyttäjän elämää, on tärkeä ajatella myös tietoturvan kannalta mihin kaikkeen omia henkilötietojaan liittää. Mitä enemmän laitteita kytketään verkkoon, sitä enemmän hyökkäyspinta-alaa haitallisilla tekijöillä on, mistä saada tietoa. Tämän lisäksi myös huijausviestit ja haitalliset yhteydenotot etenevät huolestuttavan uskottavaan suuntaan. Kuitenkin toivoisin, että ihmisten herääminen tietojenkalastelun tuomaan haittaan saa koulutuksen ja oman tietoturvan harjoittamisen enemmän esille ja vaikutuksia pystyttäisiin näin minimoimaan tulevaisuudessa.

# Lähteet

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET information security*, *16*(5), 324–345. https://doi.org/10.1049/ise2.12073

APWG 2020a. Phishing Attack Trends Report – 1Q 2020. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

APWG 2020b. Phishing Attack Trends Report – 2Q 2020. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

APWG 2020c. Phishing Attack Trends Report – 3Q 2020. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf

APWG 2020d. Phishing Attack Trends Report – 4Q 2020. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

APWG 2021a. Phishing Attack Trends Report – 1Q 2021. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

APWG 2021b. Phishing Attack Trends Report – 2Q 2021. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf

APWG 2021c. Phishing Attack Trends Report – 3Q 2021. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf

APWG 2021d. Phishing Attack Trends Report – 4Q 2021. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf

APWG 2022a. Phishing Attack Trends Report – 1Q 2022. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

APWG 2022b. Phishing Attack Trends Report – 2Q 2022. Viitattu 21.11.2022. https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf

Broadcom. (2016). *Netflix malware and phishing campaigns help build emerging black* market. Viitattu 7.11.2022. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=20612677-97ad-48e1-

9f1f-b35117ea4967&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Cohen, G. (2022). *Throwback attack: How a single whaling email cost $61 million*. Industrial Cybersecurity Pulse. Viitattu 12.11.2022. https://www.industrialcybersecuritypulse.com/strategies/throwback-attack-how-a-single-phishing-email-cost-61-million/

Executive Order 14028, “Improving the Nation’s Cybersecurity,” Washington, D.C.: Federal Register, Vol. 86, No. 93, May 12, 2021, pp. 26633–26647. Viitattu 12.11. 2022. https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

Federal Communications Commission *Covid-19 vaccines scams*. (2022). Viitattu 8.1. 2022. https://www.fcc.gov/covid-19-vaccines-scams

Gonzalez, G., Lefebvre, B., & Geller, E. (2021). *'jugular' of the U.S. fuel pipeline system shuts down after cyberattack*. POLITICO. Viitattu 7.11.2022. https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984

Huddlestone Jr., T. (2019). *How this scammer used phishing emails to steal over $100 million from Google and facebook*. CNBC. Viitattu 12.11.2022. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(1). https://doi.org/10.1186/s40163-020-00119-4

Kyberturvallisuuskeskus. (2020). *Pienyritysten Kyberturvallisuusopas.* Viitattu 23.11.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Mishra, S., & Soni, D. (2019). SMS phishing and mitigation approaches. *2019 Twelfth International Conference on Contemporary Computing (IC3)*. https://doi.org/10.1109/ic3.2019.8844920

O'Leary, D. E. (2019). What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analyzes. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3427436

Overland, I. (2019). The geopolitics of renewable energy: Debunking four emerging myths. *Energy Research & Social Science*, *49*, 36–40. https://doi.org/10.1016/j.erss.2018.10.018

Siboni, G., & Siman-Tov, D. (2014). *Cyberspace Extortion: North Korea vs. United States*. Inss.org.il. Viitattu 8.11.2022. https://www.inss.org.il/publication/cyberspace-extortion-north-korea-versus-the-united-states/

Virtanen, A. (2011) Tietojenkalastelu 2011 – Menetelmät, määrä ja suojautuminen. https://www.theseus.fi/bitstream/handle/10024/37568/Antti_Virtanen.pdf?sequence=1&isAllowed=y

Wikipedia (2022). Software as a Service. Viitattu 23.11.2022. https://en.wikipedia.org/wiki/Software_as_a_service

Wright, A., Aaron, S., & Bates, D. W. (2016). The Big Phish: Cyberattacks Against U.S. Healthcare Systems. Journal of general internal medicine, 31(10), 1115–1118. https://doi.org/10.1007/s11606-016-3741-z

Zorz, Z. (2018). *Belgian bank Crelan loses €70 million to Bec Scammers*. Help Net Security. Viitattu 12.11.2022. https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/