Haaga-Helia
ammattikorkeakoulu Oy

Yrityksiin kohdistuvat huijaukset

Anna-Maija Rahkonen
Anne Varde

Opinnäytetyö
Johdon assistenttityön ja kielten koulutusohjelma
2019

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Anna-Maija Rahkonen, Anne Varde

Koulutusohjelma
Johdon assistenttityön ja kielten koulutusohjelma

Raportin/Opinnäytetyön nimi
Yrityksiin kohdistuvat huijaukset

Sivu- ja liitesivumäärä
75 + 0

Tämä opinnäytetyö käsittelee yrityksiin kohdistuvia huijauksia. Yrityksiin kohdistuvat huijaukset ovat suuri ongelma, josta kuitenkaan ei ole paljoa tutkimusta. Huijauksissa menetetään joka vuosi merkittäviä summia rahaa suoraan huijauksissa sekä välillisesti niiden selvittelyyn kuluvana työpanoksena. Lisäksi huijauksilla on monenlaisia psykologisia vaikutuksia.

Opinnäytetyö on tehty Kilpailu- ja kuluttajaviraston (KKV) toimeksiannosta helmi-toukokuussa 2019. Työssä esitellään kymmenen yleistä huijauskategoriaa, joiden alle mahtuu monenlaisia huijauksia. Huijaustapausten lisäksi työssä esitellään keinoja, joilla huijauksia pyritään torjumaan. Työn näkökulma on kansainvälinen, eli sekä tapauksia että torjuntakeinoja esitellään useista maista. Aiheen laajuuden ja kansainvälisen näkökulman takia työ on toteutettu parityönä, jotta saadaan katettua mahdollisimman laaja alue kielellisesti ja maantieteellisesti.

Keskeisin tutkimuksessa käytetty kirjoitettu lähde oli Helena Tuorilan selvitys *Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset* vuodelta 2017. Lisäksi lähteenä hyödynnettiin asiantuntijahaastatteluita. Koska aiheesta ei ole tehty paljoa tutkimusta, työssä käytetty tieto on kerätty pienistä paloista useista lähteistä muutaman suuremman aihetta käsittelevän julkaisun sijaan. Iso osa työn toteuttamista oli mediaseuranta monella kielellä tapauskuvausten löytämiseksi ja kansainvälisen kokonaiskuvan saamiseksi.

Tutkimuksen keskeisin havainto on, että tietoa huijauksista pitää olla lisää. Tietoa pitää olla saatavilla helposti ja heti yrityksen perustamisen alkuvaiheessa, jotta yrittäjät voivat välttyä huijauksiin lankeamiselta. Huijauksista on myös kerättävä tilastotietoa, jotta niitä voidaan torjua paremmin.

Opinnäytetyön myötä piirtyy yleiskuva yrityksiin kohdistuvien huijausten tämänhetkisestä tilanteesta. Työssä annetaan ehdotuksia, joiden pohjalta Suomessa voidaan lähteä kehittämään huijausten vastaista toimintaa. Ehdotukset perustuvat tutkimuksen aikana tehtyihin havaintoihin Suomessa vallitsevasta tilanteesta sekä erityisesti ideoihin, jotka nousivat muiden maiden toimintatavoista.

Opinnäytetyön aihe on erityisen sopiva johdon assistenttityön ja kielten koulutusohjelmaan, sillä assistentit ovat keskeisessä roolissa organisaatioissa. He voivat tietämyksellään ja toiminnallaan estää huijauksiin lankeamisen yrityksissä. Tieto yrityksiin kohdistuvista huijauksista on tärkeä osa hyvää liiketoimintaosaamista.

Asiasanat
Huijaus, petos, identiteettivarkaus, toimitusjohtajahuijaus

Sisällys

1 Johdanto

Yrityksiin kohdistuvat huijaukset ovat merkittävä ongelma, jossa yrittäjät ja myös valtio häviävät vuosittain suuria summia rahaa. Huijausten määrä on kansainvälisesti tarkasteltuna kasvanut viime vuosina suuresti. Esimerkiksi pelkästään toimitusjohtajahuijauksissa maailmanlaajuisesti menetetty summa kasvoi 136 % joulukuun 2016 ja toukokuun 2018 välisenä aikana. (FBI 2018a). Suomi pienenä kielialueena on ollut vaikkapa englannin-, ranskan- ja saksankielistä maailmaa suojatummassa asemassa, mutta myös Suomessa ja naapurimaassamme Ruotsissa huijausten määrä on noussut (YLE 2017; Nyteknik 2018).

Huijarit keksivät jatkuvasti uusia, mitä mielikuvituksellisempia tapoja saada yrityksiä lankaan. Teknologian kehitys mahdollistaa uudenlaiset huijauskeinot: konekäännökset myös suomeksi ovat nykyään jo melko hyviä ja laatu paranee jatkuvasti, kuva- ja videomanipulointi ovat arkipäivää eikä ääninauhoitteiden muokkaaminen ole mikään ongelma. Huijarit toimivat myös entistä organisoidummin ja pitkäjänteisemmin ja punovat yhä uskottavampia juonia.

Mediassa uutisoidaan toisinaan suuriin yrityksiin kohdistuneista miljoonahuijauksista, mutta tämän opinnäytetyön tarkastelun kohteena ovat erityisesti pienet ja keskisuuret yritykset. Tilastokeskuksen määritelmän mukaan PK-yritykset ovat yrityksiä, joiden liikevaihto on korkeintaan 50 miljoonaa euroa, taseen loppusumma korkeintaan 43 miljoonaa euroa ja joissa on korkeintaan 250 työntekijää (Tilastokeskus 2019). Huijauksissa menetetyt kertasummat ovat pienten ja keskisuurten yritysten kohdalla pienempiä kuin mediaan päätyvissä suurtapauksissa, mutta niiden vaikutus yrityksen kannattavuudelle ja yrittäjän henkiselle jaksamiselle on usein vähintään yhtä merkittävä. Etenkin hyvin pienet yritykset ovat huijauksille haavoittuvaisia, eikä avun saaminen huijaukseen lankeamisen jälkeen ole helppoa. Pienet yritykset ovat käytännössä resursseiltaan kuluttajan asemassa, mutta yrityksinä eivät kuitenkaan voi saada samanlaista apua julkisilta tahoilta kuin kuluttajat. (Tuorila 2017, 35.)

Opinnäytetyö on kirjoitettu Kilpailu- ja kuluttajaviraston (KKV) toimeksiannosta ja yhteyshenkilönä toimi erikoistutkija Helena Tuorila. Työssä perehdytään erilaisiin yrityshuijaustyyppeihin sekä Suomessa että ulkomailla, sillä ulkomaisista huijaustavoista suuri osa päätyy jossain vaiheessa myös Suomeen, vaikkakin Suomen oloihin sopeutettuina. Opinnäytetyössä kartoitetaan myös keinoja, joilla muissa maissa pyritään torjumaan yrityksiin kohdistuvia huijauksia, ja jotka voisivat olla hyödyllisiä myös Suomessa. Toisaalta työssä myös tarkastellaan yrityksiin kohdistuvia huijauksia yhteiskunnallisena ja yksilöä koskettavana ilmiönä niin talouden kuin psykologiankin näkökulmista.

Työ on toteutettu parityönä, jotta saadaan katettua kielellisesti ja maantieteellisesti mahdollisimman laaja alue. Työssä onkin hyödynnetty kirjoittajien ranskan, saksan, englannin, ruotsin, espanjan, italian, portugalin, hollannin, slovakin, tšekin ja puolan taitoa. Aihe on myös laaja ja haastava: tieto on pitänyt koostaa pienistä palasista lukuisista lähteistä eri kielillä. Suomessa yrityksiin kohdistuvista huijauksista ei ole tehty tutkimusta juuri lainkaan, ja muistakin maista saatava tieto on vähäistä, sillä huijauksia käsitellään yleensä kuluttajanäkökulmasta. Kirjoittajat olivat vuonna 2018 osa työryhmää, joka koosti Kilpailu- ja kuluttajaviraston toimeksiannosta kuluttajahuijauksiin keskittyvän katsauksen kansainvälisestä näkökulmasta, joten työssä on voitu hyödyntää myös kirjoittajien tietämystä kuluttajahuijauksista.

Yksi harvoja yrityksiin kohdistuvia huijauksia Suomessa käsitteleviä tietolähteitä on Helena Tuorilan vuonna 2017 laatima Kilpailu- ja kuluttajaviraston selvitys *Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset*. Muita merkittäviä opinnäytetyössä käytettyjä lähteitä ovat asiantuntijahaastattelut sekä sähköpostitiedustelut. Työtä varten haastateltiin erikoistutkija Helena Tuorilaa ja kilpailuasiainneuvos Kalle Määttää Kilpailu- ja kuluttajavirastosta sekä lainsäädäntöasioiden päällikkö Tiina Toivosta ja asiantuntija Atte Rytköstä Suomen Yrittäjiltä. Koska kyseessä ei ole haastattelututkimus, päätettiin haastattelut toteuttaa vapaamuotoisesti keskustelunomaisina. Tällöin oli mahdollista saada tietoa asioista hieman laajemmin myös kysymysten ulkopuolelta. Sähköpostitse on saatu vastauksia Helsingin uusyrityskeskus NewCo Helsingin palvelupäällikkö Toivo Utsolta sekä ruotsalaisen yrittäjäjärjestön Svensk Handelin turvallisuusasiantuntija Nina Jelveriltä.

Toimeksiantajan erityisenä toiveena on ollut saada tietoa erilaisista huijaustyypeistä eri maissa. Tämän vuoksi opinnäytetyön tiedonhausta merkittävä osa on ollut internetissä tehtyä mediaseurantaa monella kielellä sekä tutustumista eri maiden huijauksia ehkäisevien viranomais- ja järjestötahojen ohjeistuksiin. Työssä on hyödynnetty tietoa ja tapauskuvauksia Iso-Britanniasta, Yhdysvalloista, Australiasta, Kanadasta, Ranskasta, Belgiasta, Alankomaista, Luxemburgista, Espanjasta, Italiasta, Portugalista, Sveitsistä, Saksasta, Itävallasta, Puolasta, Tšekistä, Slovakiasta, Ruotsista ja Suomesta.

Opinnäytetyön aihe on siis yhteiskunnallisesti merkittävä sekä ajankohtainen. Aihe on erityisen tärkeä johdon assistenttityön ja kielten koulutusohjelman opiskelijoille, sillä sieltä valmistuvat joutuvat varmasti työssään tekemisiin yrityshuijausten kanssa. Ymmärrys huijauksista ja kyky tunnistaa niitä kuuluvat hyvään liiketoimintaosaamiseen. Monet opiskelijat myös tekevät yrityksissä kesäsijaisuuksia, ja kesälomakausi on huijauslaskujen kulta-

aikaa (Viestintävirasto 2018a) joten on tärkeää, että myös opiskelijat saavat tietoa huijauksista. Koska opinnäytetyön on tarkoitus valmistua toukokuussa, aika on otollinen muistutukselle ja ohjeistukselle, sillä kesätyöntekijät on aina hyvä perehdyttää huijauksiin.

Työn rakenne

Opinnäytetyö koostuu seitsemästä luvusta ja lähdeluettelosta. Luku yksi on johdanto ja luvussa seitsemän vedetään yhteen, mitä kaikkea opinnäytetyöprosessi on tekijöille opettanut sekä pohditaan työn merkityksellisyyttä. Näiden väliin jäävissä luvuissa käsitellään yrityksiin kohdistuvia huijauksia monesta näkökulmasta.

Luku kaksi esittelee, minkä takia yrityksiin kohdistuvat huijaukset ovat merkittävä yhteiskunnallinen ongelma. Siinä katsotaan asiaa yhteiskuntaa euromääräisesti rasittavana ilmiönä, mutta keskitytään myös tarkastelemaan psykologisia syitä, jotka johtavat huijauksen uhriksi joutumiseen sekä niiden seurauksia. Luvussa kaksi käsitellään myös lainsäädäntöä, joka koskee yrityksiin kohdistuvia huijauksia.

Luvussa kolme tutustutaan kymmeneen erilaiseen huijaustyyppiin, jotka ovat yleisiä. Jokaisesta tyypistä on lyhyt esittely ja useimmista lisäksi mielenkiintoinen tapauskuvaus Suomesta tai ulkomailta. Luvuissa neljä ja viisi käsitellään sitä, millaisin keinoin yrityksiin kohdistuvia huijauksia vastaan taistellaan eri maissa.

Luku kuusi sisältää kirjoittajien pohdintaa siitä, millaisia keinoja tai muutoksia Suomessa voitaisiin ottaa käyttöön, jotta yrityksiin kohdistuvista huijauksista johtuviin ongelmiin pystyttäisiin tarttumaan tehokkaammin. Samassa luvussa on myös tiivis ohjeistus huijausten ehkäisemisestä yrittäjille ja yrityksille.

2 Yrityksiin kohdistuvat huijaukset ilmiönä

Yrityksiin kohdistuvat huijaukset ovat merkittävä yhteiskunnallinen ongelma, jolla on monenlaisia seurauksia. Tässä luvussa käsitellään huijauksia ja niiden seurauksia yleisellä tasolla sekä juridisena ongelmana Suomen lainsäädännön edessä. Huijaus ei ole juridinen käsite, vaan kuuluu ainoastaan yleiskieleen. Huijaukselle ei siis ole mitään tarkkaa määritelmää. (Tuorila, Määttä & Peltonen 2016, 11.)

Huijarit tuntuvat olevan jatkuvasti ainakin yhden askelen edellä ja keksivät koko ajan uusia, mitä mielikuvituksellisempia huijauskeinoja sitä mukaa, kun yrittäjät ja viranomaiset oppivat tunnistamaan ja torjumaan vanhoja. Teknologian edistyessä keinoista tulee myös yhä monipuolisempia, ja etenkin kyberrikollisuuden kasvu näkyy tulevaisuudessa varmasti myös yrityksiin kohdistuvissa huijauksissa. (Tuorila 1.4.2019; Rikoksentorjunta 2019a.) Uusien teknologioiden lisäksi huijarit hyödyntävät lakimuutoksia, kuten EU:n uutta tietoturva-asetusta tai Brexitin aiheuttamaa epätietoisuutta. Erilaisista huijaustyypeistä ja niiden erityispiirteistä kerrotaan luvussa kolme.

Yrityksiin kohdistuvista huijauksista aiheutuvat ongelmat ovat moninaisia, mikä ilmenee erityisen hyvin Helena Tuorilan laatimassa julkaisussa *Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset* (2017). Huijauksissa menetetään vuosittain suuria määriä rahaa niin suoraan huijatun summan muodossa kuin myös välillisesti huijauksen selvittelyssä menetettyinä työtunteina. Joskus helpointa ja halvinta yrittäjän itsensä kannalta on vain maksaa postilaatikkoon tullut lasku, vaikka sen tunnistaakin huijaukseksi, sillä selvittelytyöhön ja reklamointiin uppoava aika, raha ja työpanos voivat olla merkittäviä. Sitä kautta laskusta aiheutuva tulonmenetys voi muodostua suuremmaksi kuin huijauslaskun summa. Laskun maksaminen kuitenkin vain kannustaa huijareita jatkamaan toimintaansa ja ylläpitää kulttuuria, joka on tällaiselle rikollisuudelle suopea. (Tuorila 2017, 9–10, 38.)

Tuorilan selvityksessä (2017, 20–24) otetaan myös esiin huijauksista aiheutuvat sosiaaliset kustannukset. Niiden vaikutukset voivat olla pien- tai yksinyrittäjälle erittäin merkittäviä siitäkin huolimatta, ettei huijauksissa aina ole kyse todella suurista summista. Tapauksen selvittelyyn kuluu tunteja, jotka ovat pois joko työ- tai vapaa-ajasta. Pahimmillaan huijauksen uhriksi joutuneen yrittäjän terveydentila heikkenee esimerkiksi murehtimisen tai selvittelytyön takia menetettyjen yöunien vuoksi. Se voi johtaa yrittäjän uusiin tulonmenetyksiin sekä tuoda yhteiskunnalle lisäkustannuksia. Huijauksen uhriksi joutuminen myös heikentää yrittäjän luottamusta muihin yrityksiin ja toimijoihin.

Yrityksiin kohdistuvat huijaukset ovat ongelmallisia myös yrityskulttuurin kannalta kokonaisuutena. Huijaukset vääristävät kilpailua ja tekevät asiallisesti toimivien ja lakeja noudattavien yritysten toiminnasta vaikeaa. Jos esimerkiksi puhelinmyynti alana koetaan lähtökohtaisesti huijaustoiminnaksi, on rehellisesti toimivan puhelinmyyntiyrityksen toiminta vaikeaa. (Rytkönen & Toivonen 6.3.2019.)

Helena Tuorilan (2017, 14) mukaan vain pieni osa huijauksista tai niiden yrityksistä päätyy poliisin tietoon. Yrityksiin kohdistuvista huijauksista tehdyistä rikosilmoituksista ei ole olemassa erillistä tilastoa, joten huijausten määristä tai määrien muutoksista ei ole kattavaa tietoa. Vuoden 2017 rikoksentorjuntakatsauksessa (Tanttari & Alanko 2017) käsitellään petosrikollisuutta ja sen torjuntaa. Katsauksessa kerrotaan petosrikollisuuden kasvaneen merkittävästi viime vuosina: vuonna 2010 poliisin tietoon tuli 20 380 tapausta, mutta vuonna 2016 määrä oli noussut 40 416 tapaukseen (Tanttari & Alanko 2017, 9). Luvut koskevat yksityishenkilöön kohdistuneita petosrikoksia, mutta on oletettavaa, että myös yrityksiin kohdistuva petosrikollisuus on kasvanut. Samasta katsauksesta löytyy myös tilasto, jonka mukaan petoksen uhriksi joutuneista tai sitä epäilleistä yksityishenkilöistä vain 42 % prosenttia teki rikosilmoituksen. 23 % jätti selvityksen mukaan rikosilmoituksen tekemättä, koska eivät uskoneet sen johtavan mihinkään. Luvut ovat peräisin eri kaupunkien turvallisuuskyselyyn sisällytetyistä petosrikollisuutta koskevista vastauksista. (Tanttari & Alanko 2017, 17.) Rikosilmoituksen tehneiden luku on siis alle puolet kaikista niistä, jotka ovat havainneet joutuneensa huijauksen uhriksi. Kalle Määtän mukaan luku vaikuttaa aivan liian korkealta (11.4.2019) ja todellisuudessa ilmoituksen tehneiden määrä olisi huomattavasti pienempi. Ei ole olemassa tutkimustietoa siitä, kuinka yksityishenkilöihin kohdistuvista huijauksista tehtyjen rikosilmoitusten määrä poikkeaa yrityksiin kohdistuvista huijauksista tehtyjen ilmoitusten määrään. Luku tuskin kuitenkaan on ainakaan merkittävästi suurempi.

Suomen Yrittäjien lainsäädäntöasioiden päällikkö Tiina Toivonen kertoi haastattelussa (Rytkönen & Toivonen 6.3.2019), että Suomen Yrittäjät saavat toisinaan yhteydenottoja, joissa yrittäjät kertovat poliisin suhtautuvan rikosilmoitukseen huijauksesta tai huijausyrityksestä ainoastaan sopimusriitana. Helena Tuorila mainitsi haastattelussa (1.4.2019) törmänneensä omaa selvitystä tehdessään myös asenteeseen, että huijauksen uhriksi joutuneen yrittäjän on vain maksettava oppirahat, jotta ei myöhemmin enää lankea samanlaiseen huijaukseen.

Vaikka yrittäjä tekisikin rikosilmoituksen, poliisi ei välttämättä aloita tutkintaa tilanteesta, jonka yrittäjä kokee ilmiselväksi huijaukseksi, koska kyse voi olla vain pienestä summasta tai poliisin näkökulmasta epäselvästä tilanteesta. Usein esimerkiksi hakemistohuijauksissa

laskut ovat korkeintaan muutamia satoja euroja, jolloin onnistuessaan huijauksen rikosnimikkeenä olisi lievä petos ja rangaistuksena sakko. Mikäli yrittäjä ei lankea huijaukseen, kyseessä on ainoastaan lievän petoksen yritys, joka ei Suomen rikoslain mukaan ole rangaistava teko. (Harmaan talouden selvitysyksikkö 2014, 2.)

Tieto siitä, ettei rikosilmoituksen tekeminen johda mihinkään konkreettisiin toimiin, voi osaltaan heikentää yrittäjien intoa tehdä rikosilmoitus etenkin silloin, jos kyse on pienestä summasta. Se puolestaan kasvattaa edelleen ongelmallista, huijauksille suopeaa kulttuuria ja saa huijarit vain jatkamaan toimintaansa. Syyttäjä voi jättää syyttämättä jopa tapauksissa, joissa yksittäisiä huijausyrityksiä on kertynyt lähes kaksisataa (Suomen Yrittäjät 2018a). Ei siis ihme, että yrittäjän voi olla vaikea uskoa saavansa apua ja oikeutta, jos joutuu huijauksen uhriksi. Toisaalta taas huijariyrityksen jääminen vaille rangaistusta voi kasvattaa huijausten määriä pitkällä aikavälillä.

Etenkin pien- tai yksinyrittäjän asema on huijauksen uhriksi joutuessa vaikea. Sopijapuolena pienet yritykset ovat aina altavastaajia ja etenkin huijauksen uhriksi joutuessaan ne ovat resursseiltaan käytännössä kuluttajaan rinnastettavassa asemassa. Kuitenkaan pienyrittäjillä ei ole samoja oikeuksia ja pääsyä saman avun äärelle kuin kuluttajalla. Kuluttajansuojalaki, kuten nimikin jo kertoo, on säädetty turvaamaan kuluttajien oikeuksia. Kuluttajansuojalakia sovelletaan kuluttajankauppaan, jossa myyjänä on elinkeinonharjoittaja ja ostajana kuluttaja. Pienyritys on lainsäädännöllisesti oikeushenkilö eikä siis nauti kuluttajansuojaa. Tämän vuoksi pienyrittäjä ei myöskään yritykseensä kohdistuvassa huijaustapauksessa voi saada apua kuluttajille suunnatuista palveluista, kuten Kilpailu- ja kuluttajavirastosta. (Tuorila 2017, 35.)

2.1 Huijausten psykologia

Huijatuksi tulemiseen liittyy vahva stigma. Kun lukee vaikkapa valelaskuja tai toimitusjohtajahuijauksia käsitteleviä uutisartikkeleita, voi jutun alla olevasta lukijoiden kommenttikentästä joskus löytää hyvinkin tylyjä mielipiteitä, joissa uhria ja hänen kärsimystään vähätellään. Kommenteissa saatetaan naureskella sille, kuinka typerä huijaukseen langenneen ihmisen pitääkään olla ja todeta, että huijauksen uhriksi joutuminen on uhrin omaa syytä. Tällaisessa ilmapiirissä kynnys kertoa tulleensa huijatuksi kasvaa hyvin korkeaksi. Kuten edellä kirjoitettiin, saattaa jopa poliisikin suhtautua huijauksen uhriksi joutuneen yrittäjän ilmoitukseen varsin kevyesti. Tämä johtaa siihen, että rikosilmoitusta ei tehdä eikä asia välttämättä nouse ikinä edes muuhun keskusteluun, vaan tapaus jää tilastoimattomaksi piilorikollisuudeksi. Eihän kukaan halua päätyä yleisesti naurun aiheeksi myöntämällä, että tuli huijatuksi!

Yksityishenkilöihin kohdistuvista huijauksista ja niiden uhreista on tehty tutkimusta. Yrityksiin kohdistuvat huijaukset ovat osaltaan erilaisia kuin kuluttaja- ja yksityishenkilöihin kohdistuvat huijaukset. Kuitenkin yrityshuijauksissakin lähes aina heikoimpana lenkkinä on yrityksen työntekijä, eli viime kädessä yksityishenkilö. Sen vuoksi tutkimustulokset huijauksen uhriksi joutumiselle altistavien tekijöiden osalta ovat sovellettavissa myös yrityksiin kohdistuvissa huijauksissa.

Huijauksen uhreista on mahdotonta piirtää yhtenäistä kuvaa, sillä syyt uhriksi joutumiselle ovat moninaisia ja joskus jopa maalaisjärjenvastaisia. Joitakin mahdollisesti altistavia tekijöitä on tutkimuksissa kuitenkin löydetty. Riku Salmivuoren kirjassa *Miljoonaperintö tarjolla* (2016) mainitaan, että yksi altistavista tekijöistä voisi olla ikä. Huijauksille ovat erityisen alttiita nuoremmat ikäluokat, etenkin opiskelijat ja nuoret aikuiset, joilla on vähemmän elämänkokemusta. Mutta vastaavasti myös vanhukset ovat heikomman teknologisen osaamisensa takia alttiita verkkohuijauksille. Toisaalta Salmivuori (2016, 171) myös kirjoittaa Detarin, Colen ja Rogersin australialaistutkimuksesta vuodelta 2015, jonka mukaan ikä vaikuttaa ainoastaan siihen, minkälaiseen petokseen uhri todennäköisimmin lankeaa. Yleisesti huijauksen tunnistamiseen huijaukseksi ikä ei australialaistutkimuksen mukaan vaikuta.

Yleinen mielipide Suomessakin vaikuttaisi esimerkiksi sanomalehtiartikkelien kommentointipalstojen perusteella olevan, että huijauksiin lankeavat vain typerykset. Kyllähän edes ihan normaalilla älyllä siunatut ihmiset ymmärtäisivät, että kyse on huijauksesta eivätkä joutuisi sen uhriksi. Riku Salmivuoren mukaan juuri tämä harhaluulo on yksi altistava tekijä uhriksi joutumisessa. *Miljoonaperintö tarjolla* -kirjassa kerrotaan, että ihmiset ajattelevat usein olevansa keskivertoa parempia tunnistamaan petokset ja siten huijausten yläpuolella. Tällainen ylpeys johtaa helposti hutilointiin ja siihen, ettei huijausta lopulta huomatakaan. (Salmivuori 2016, 174.) Älykkyyden tai koulutustason vaikutus huijauksen uhriksi joutumiseen on yleisten mielikuvien vastainen. Korkea koulutus ei erityisemmin suojaa huijauksen uhriksi joutumiselta, vaan voi jopa edesauttaa huijaukseen haksahtamista. (Fischer, Lea & Evans 2013; Freiermuth 2011.)

Mark Freiermuthin artikkelissa *Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting* (2011) tarkastellaan erityisesti niin sanottuja nigerialaiskirjeitä ja niiden uhreja. Nigerialaiskirjeiksi kutsutaan etumaksupetoksia, joissa sähköpostitse luvataan osuutta suuresta perinnöstä käsittelykulumaksua vastaan. Artikkelissa kyseiseen huijaukseen viitataan termillä 419-huijaus. Nimi tulee Nigerian lainsäädännön

asetuksen numerosta, jolla huijaussähköpostien lähettäminen tehtiin rangaistavaksi. Freiermuthin artikkelin mukaan älykäs ihminen voi kuitenkin olla huijarille otollisin kohde, vaikka yleinen mielikuva on, että huijauksen uhriksi joutuvat ovat nimenomaan vähemmän älykkäitä. Tutkimuksissa on todettu, että älykkäät ihmiset osaavat täydentää huijareiden tarinoissa olevat aukkokohdat mielekkäästi, mikä tekee tarinaan uskomisesta helpompaa ja huijaus jää helposti huomaamatta. Onhan huijarin tarina tällöin osin uhrin itsensä luoma. (Freiermuth 2011, 123, 140–141.)

Salmivuoren kirjassa esitellään muita syitä sille, miksi älykkyys oikeastaan onkin merkittävä huijauksen uhriksi joutumiselle altistava tekijä. Eräs suurimmista syistä on se, että älykäs ihminen uskoo omaan ihmistuntemukseensa ja siihen, että pystyy kyllä tunnistamaan huijausyritykset. Kun huijauksen uhri luottaa vahvasti omiin kykyihinsä ja päätöksiinsä, voi huijauksesta irtautuminen olla vaikeaa, vaikka joitain epäilyksiä alkaisikin herätä tai muut ihmiset ympärillä varoittaisivat toiminnan luonteesta. Eihän älykäs ihminen luottaisi huijariin, vaan erinomaisella ihmistuntemuksellaan kyllä huomaisi, milloin on kyse hämärämiehestä. Lisäksi korkeasti koulutetuilla ja älykkäillä ihmisillä on korkea kilpailuvietti ja kokemus omasta erinomaisuudestaan, joita huijari voi helposti hyödyntää. (Salmivuori 2016, 174–178.)

Myös huono itsetunto altistaa ihmisen lankeamaan huijaukseen (Salmivuori 2016, 175). Yrityksiin kohdistuvissa huijaustapauksissa huijari voi pönkittää uhrin itsetuntoa esimerkiksi vetoamalla hänen ammattitaitoonsa tai asemaansa. Kukapa meistä ei tahtoisi kuulla, että on monista vaihtoehdoista juuri se paras tai luotettavin ja tullut sen takia valituksi toimimaan vaikkapa oikeana kätenä toimitusjohtajan salaisessa projektissa tai jopa auttamaan pelastamaan panttivankeja terroristien kynsistä? Kyseessä on tällöin sosiaalinen manipulointi, joka on lähtökohtana monenlaisissa huijauksissa, kuten tietojenkalastelussa.

Sosiaalinen manipulointi, englanniksi ”social engineering”, voidaan määritellä monella tavalla riippuen kontekstista. Tietoturvan näkökulmasta sillä tarkoitetaan niitä menetelmiä, joita käytetään tietojärjestelmien käyttäjien saamiseksi toimimaan sosiaalisen manipuloijan toivomalla tavalla. Mouton, Leenen & Venter (2016, 187) määrittelevät sosiaalisen manipuloinnin taidoksi vaikuttaa ihmisiin tavalla, joka saa heidät paljastamaan arkaluontoisia tietoja. Bhakta & Harrisin (2015) mukaan sosiaalinen manipulointi on puolestaan ihmisten psykologista manipulointia, jonka tavoitteena on hyökkääjän pääsy järjestelmään, johon hänellä ei ole oikeuksia. Voidaan siis sanoa, että sosiaalinen manipulointi on tietoturvan ihmiselementti.

Organisaatioiden tietoturvaan ja sen kehittämiseen kiinnitetään paljon huomiota. Pelkkä huipputeknologia ei kuitenkaan riitä suojaamaan organisaatioiden ja yritysten arkaluonteisia tietoja, sillä yritysten tietoturvan heikko lenkki ovat sen työntekijät. Sosiaalinen manipulointi kohdistuu nimenomaan tähän haavoittuvuuteen ja käyttää hyväkseen ihmisluonnon taipumuksia. Työntekijät voidaan saada sosiaalisen manipuloinnin keinoin luovuttamaan arkaluonteisia tietoja ja näin avaamaan hyökkääjälle ovi suojattuihin järjestelmiin. Esimerkiksi pelkästään se, että kommunikoimme ystävällisen ja pidettävän henkilön kanssa, lisää halukkuuttamme myöntyä epätavalliseen pyyntöön. Sosiaalinen manipulointi toimii, koska ihmisten käyttäytymismallit ovat pitkälti ennalta-arvattavia. (Mouton ym. 2016.)

Heikko itsetunto ja matalampi koulutustaso voivat Salmivuoren mukaan myös suojata tietynlaisilta huijausyrityksiltä. Siinä missä älykkäät ja korkeasti koulutetut ovat kykeneviä ja jopa halukkaita paikkailemaan mielikuvituksellaan aukkoja huijarin tarinassa, heikolla itsetunnolla varustettu ihminen ei välttämättä siihen pysty. Silloin ihminen kenties huomaa huijarin tarinan valheellisuuden helpommin. Ihmiset, joilla on matalampi koulutustaso ja huono itsetunto, eivät myöskään usko yhtä auliisti omaan erityislaatuisuuteensa, jolloin joissain tapauksissa sosiaalisen manipuloinnin onnistuminen voi olla vaikeampaa. (Salmivuori 2016, 175–177).

Huijauksen psykologiset seuraukset

Huijauksen uhriksi joutumisella on monenlaisia seurauksia. Yrityksiin kohdistuvissa huijauksissa konkreettiset, helpoimmin mitattavat seuraukset ovat rahanmenetys ja pahimmissa tapauksissa jopa konkurssi. Hieman vaikeammin mitattavissa on huijauksesta aiheutunut tehokkaan työajan menetys. Aikaa kuluu kenties ensin huijaukseen osallistumiseen ja myöhemmin huijauksen selvittelyyn, reklamointiin, rikosilmoitukseen ja ehkä oikeusprosessiinkin. Huijaukseen lankeamisella on kuitenkin myös psykologisia seurauksia.

Riku Salmivuoren (2016, 178–180) mukaan huijauksen uhrin päällimmäinen tunne on häpeä. Häpeä siitä, että on ollut niin typerä ja sinisilmäinen ja että on langennut huijaukseen. Mediassa huijauksen uhreja syyllistetään niin otsikoissa kuin lehtiartikkeleiden kommenttikentissä. Huijaukseen lankeamisen siirtäminen uhrin syyksi tuntuu olevan sosiaalisesti täysin hyväksyttyä, vaikka nykyisin esimerkiksi raiskauksien kohdalla suurin osa ihmisistä ymmärtää, ettei uhria voi tilanteesta syyllistää. Salmivuori (2016, 178) kirjoittaa myös siitä, että monet huijauksen uhrit ovat ainakin harkinneet itsemurhaa. Helena Tuorilan (2017, 26) tekemässä selvityksessä mainitaan, että yrityksiin kohdistuvissa huijauksissa uhri on tullut huijauksen jälkimainingeissa tarttuneeksi ”perjantaipulloon”. Psykologiset seuraukset huijaukseen lankeamisesta voivat siis olla todella tuntuvia.

Erityisen kiinnostavaa on pohtia sitä, miten uhri määritellään yrityksiin kohdistuvissa huijauksissa. Yritys ja sen omistaja ovat tietenkin uhreja ja kokevat rahalliset menetykset. Mutta entä työntekijä, jonka kautta huijari on päässyt toteuttamaan huijauksensa? Kuinka hän selviää tilanteesta ja onko hän uhri? Tieto siitä, että on aiheuttanut toiminnallaan työnantajalleen kenties mittaviakin taloudellisia menetyksiä tai jopa konkurssin, on varmasti lamauttava ja sillä on monenlaisia psykologisia seurauksia. Huijaukseen langenneen toiminta on voinut myös vaarantaa hänen työtovereidensa toimeentulon. Koska huijauksia on tutkimuskirjallisuudessa tarkasteltu lähinnä yksityishenkilöön kohdistuvien huijausten kautta, ei tähän kysymykseen löydy kirjallisuudesta suoraa vastausta. Voi kuitenkin arvella, että työntekijän syyllisyys ja kokemus uhriksi joutumisesta ovat valtavia. Ympäröivä yhteiskunta ei kuitenkaan välttämättä tällaisissa tilanteissa koe työntekijän olevan yksi uhreista, vaan pikemminkin ainakin osasyyllinen ja kenties huijarin työtoveri.

Kilpailuasiainneuvos ja professori Kalle Määttä kertoi haastattelussa, että häpeä on myös yksi merkittävimmistä syistä, minkä takia rikosilmoitus jätetään tekemättä. Kun huijaukset jäävät piilorikollisuudeksi, on vaikea toimia niitä vastaan ja tietää, millaisin resurssein asiaan pitäisi tarttua. (Määttä 11.4.2019.) Uhrit ovat kuitenkin huijausten parhaita asiantuntijoita, joiden kokemuksista voisi oppia paljon niin huijauksista kuin keinoista niiden torjumiseksi, joten uhrien tarinoita olisi tärkeä kuulla (Salmivuori, 180).

2.2 Lainsäädäntö yrityksiin kohdistuvissa huijauksissa

Suomen ja Euroopan unionin lainsäädäntö määrittelevät, miten huijauksiin voi tarttua juridisesti, vaikka termiä huijaus ei suomalaisesta lainsäädännöstä löydy. Huijaukselle ei ole yhtä hyväksyttyä määritelmää. Kuluttajien näkemys huijauksesta poikkeaa viranomaisten näkemyksestä, jotka määrittelevät huijaukset toimivaltuuksiensa näkökulmasta. Käsitys huijauksista on siis varsin kirjava. Tätä on pohdittu mm. KKV:n julkaisussa *Kuluttajahuijaukset* (Tuorila ym. 2016, 11). Sen mukaan huijaus on yleiskieleen kuuluva käsite. Rikoslainsäädännössä käytetty termi on petos. Muita yrityshuijaustapauksissa esiin tulevia rikosnimikkeitä ovat esimerkiksi identiteettivarkaus, kiristys, tietomurto sekä markkinointirikos. Yksi huijaustapaus voi sisältää useita rikosnimikkeitä. Esimerkiksi tästä käy yritystietopalveluja tarjonneen Directan tapaus, jossa rikosnimikkeinä olivat törkeä petos ja markkinointirikos (YLE 2012).

Petos

Rikoslain (19.12.1889/39) 36 luvun 1 pykälässä petoksesta säädetään seuraavasti:

> Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava *petoksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Myös dataa käsittelemällä sekä tietojärjestelmään puuttumalla syyllistyy petokseen, mikäli toimet johtavat tietojenkäsittelyn lopputuloksen vääristymiseen. Petoksen yritys on rangaistava. (Rikoslaki 36 luku 1 §.)

Lievässä petoksessa tavoiteltu hyöty ja aiheutettu vahinko ovat kokonaisuutena arvosteltuna vähäisiä. Siitä tuomitaan sakkorangaistus. Lievän petoksen yritystä ei ole rikoslaissa säädetty rangaistavaksi. (Rikoslaki 36 luku 3 §.) Törkeän petoksen tunnusmerkistöön kuuluvat huomattavan hyödyn tavoittelu, huomattavan vahingon aiheuttaminen ja oman vastuullisen aseman tai rikoksen uhrin heikon aseman hyödyntäminen rikosta tehdessä. Törkeän petoksen yritys on rangaistava. (Rikoslaki 36 luku 2 §.)

Törkeän petoksen kohdalla huomattavana hyötynä on pidetty tuhansien eurojen varallisuusetua. Tarkkoja summia sille, milloin törkeän petoksen raja ylittyy, ei ole määritelty. Yleensä summa on vaihdellut 7 000 ja 14 000 euron välillä. (Nuutila & Majanen 2009, 990.) Kihlakunnansyyttäjä Eija Velitskin mukaan alle 500 euron rikoshyöty on niin pieni, ettei siitä muodostu syytä antaa vankeusrangaistusta (TS 2017). Vaikka lainsäädännössä myöskään lievälle petokselle ei ole määritelty tarkkoja euromääräisiä rajoja, summa vaikuttaa asettuneen tuohon 500 euroon.

Suuri osa yrityksiin kohdistuvista huijauksista on siis jonkinasteisia petoksia tai niiden yrityksiä. Esimerkiksi valelaskujen ja hakemistohuijauksien kohdalla kyse on yleensä lievästä petoksesta, koska huijattavat summat ovat melko pieniä, lähinnä muutamia satoja euroja, ja rikos siten vähäinen. Lievän petoksen yritys ei ole rangaistava teko, joten niissä tapauksissa poliisilla tai syyttäjällä ei ole mahdollisuutta tarttua ongelmaan.

Identiteettivarkaus

Identiteettivarkaus kriminalisoitiin vuonna 2015, kun Suomen rikoslain lukuun tieto- ja viestintärikoksista lisättiin säädös identiteettivarkaudesta. Rikoslain 38 luvun 9 b §:ssä säädetään seuraavasti:

> Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.

Identiteettivarkaudessa ei siis varasteta mitään aineellista, vaan esiinnytään oikeudettomasti toisena henkilönä tarkoituksena erehdyttää kolmatta osapuolta. Rikoksentekijä voi käyttää tarkoitukseensa toisen henkilötietoja, tunnistautumistietoja tai muita yksilöiviä tietoja.

Identiteettivarkaus on rangaistava, jos siitä aiheutuu uhrille taloudellista vahinkoa tai vähäistä suurempaa haittaa. Esimerkiksi se, että uhri joutuu selvittelemään tilannetta voi aiheuttaa hänelle taloudellista vahinkoa. Haittaa voi aiheutua myös tilanteissa, joissa uhri ei ole kärsinyt taloudellista vahinkoa. (Åberg 2017, 114.)

Identiteettivarkaudesta voidaan tuomita vain sakkoihin, joten sitä ei yksinään luokitella kovinkaan vakavaksi rikokseksi. Usein identiteettivarkautta käytetään jonkin muun rikoksen valmisteluun ja se tulee ilmi vasta kun toisen henkilön nimissä on tehty muita rikoksia. Toisen identiteetin käyttäminen voi olla rangaistavaa myös jonkin muun rikosnimikkeen perusteella. Kyseessä voi tällöin olla esimerkiksi petos tai väärennös. (Åberg 2017, 114.)

Kiristys

Kiristyksestä säädetään Rikoslain 31 luvun 3 §:ssä. Kiristyksessä uhri pakotetaan uhkauksella ”luopumaan taloudellisesta edusta, johon rikoksentekijällä tai sillä, jonka puolesta hän toimii, ei ole laillista oikeutta”. Uhkaus ei kiristystapauksessa ole välittömällä väkivallalla uhkaamista, sillä siinä tapauksessa rikosnimike olisi ryöstö, kuten rikoslain 31 luvun 1 §:ssä säädetään. Törkeä kiristys on kyseessä silloin, kun on uhattu erityisen vakavalla rikoksella, taloudellinen menetys on ollut huomattava joko euromääräisesti tai uhrin toimeentulo huomioiden tai on käytetty hyväksi uhrin heikkoutta. (Rikoslaki 31 luku 4 §). Sekä kiristyksen että törkeän kiristyksen yritykset ovat rangaistavia.

Teko, jolla uhria uhataan, ei välttämättä ole oikeudenvastainen. Kiristystä on esimerkiksi uhkaus paljastaa jotain haitallista tietoa työnantajalle, mikäli kiristyksen uhri ei suostu kiristäjän vaateisiin. (Lappi-Seppälä 2009, 867.)

Tietomurto

Tietomurto on säädetty rangaistavaksi Rikoslain tieto- ja viestintärikoksia käsittelevässä luvussa 38, 8 §:ssä. Sen ensimmäinen momentti kuuluu:

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Rikoslain mukaan tietomurto on rangaistavaa myös silloin, kun henkilö ottaa oikeudettomasti selon tietojärjestelmässä olevasta tiedosta tai datasta. Tietomurron yrityskin on rikos. Tietomurto on törkeä, jos se tehdään osana järjestäytyneen rikollisryhmän toimintaa tai erityisen suunnitelmallisesti ja siitä voidaan tuomita enintään kolmeksi vuodeksi vankeuteen.

Markkinointirikos

Rikoslain 30 luku käsittelee elinkeinorikoksia ja sen 1 §:ssä säädetään seuraavasti:

> Joka tavaroiden, palveluksien, kiinteistöjen, yksityisen osakeyhtiön arvopapereiden tai muiden hyödykkeiden ammattimaisessa markkinoinnissa antaa markkinoinnin kohderyhmän kannalta merkityksellisiä totuudenvastaisia tai harhaanjohtavia tietoja, on tuomittava *markkinointirikoksesta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Koivumäki & Häkkäsen (2018, 457) mukaan on käytännössä erittäin harvinaista, että markkinoijaa kohtaan nostetaan syyte markkinointirikoksesta, joten Suomessa ei ole juurikaan oikeuskäytäntöä asiasta.

Harvoihin Suomessa markkinointirikoksesta tuomion saaneisiin lukeutuu pienyrittäjille mainosnäkyvyyttä internetissä vuosina 2008–2009 kaupannut yritys Directa. Asiakasyritykset kokivat tulleensa harhaanjohdetuksi, sillä näkyvyys verkossa ei vastannut luvattua. Directan tapausta puitiin pitkään eri oikeusasteissa. Lopulta yhtiön entinen toimitusjohtaja sai viiden kuukauden ehdollisen vankeustuomion markkinointirikoksesta ja yritys tuomittiin maksamaan 1,5 miljoonaa euroa vahingonkorvauksia. (Yle 2016a.)

Perintälaki

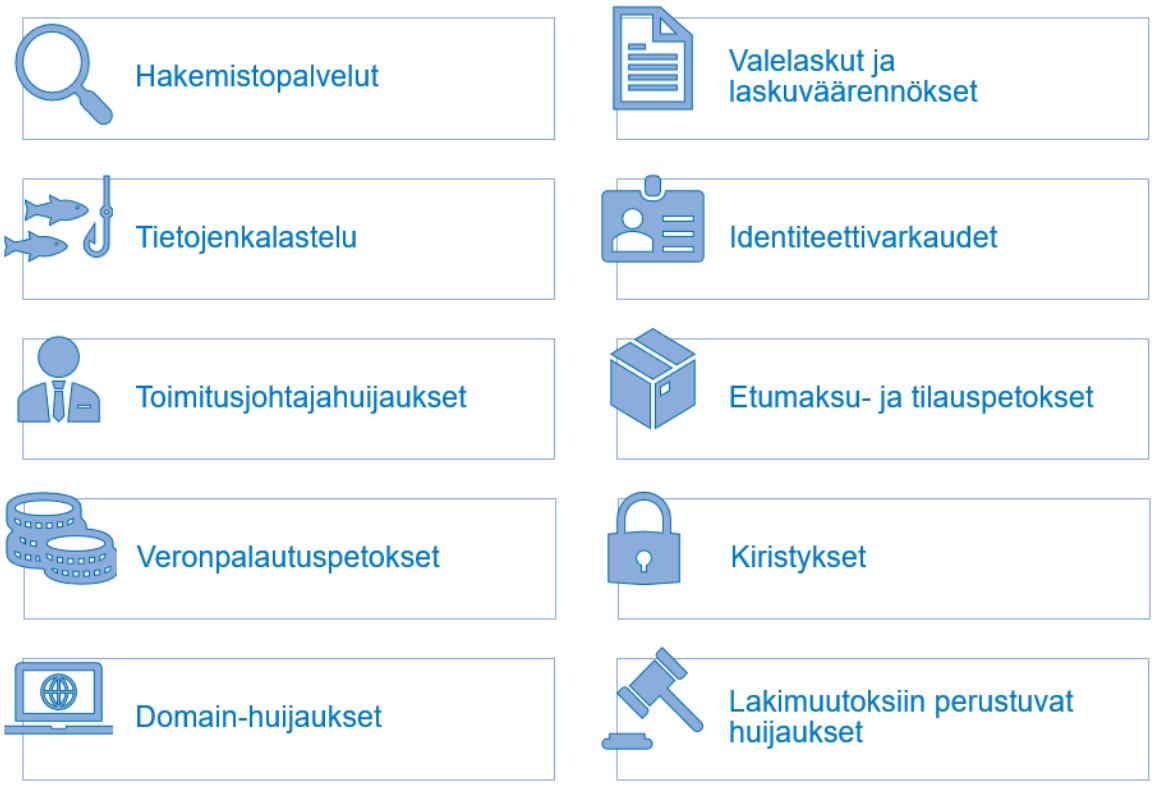
Laki saatavien perinnästä (22.4.1999/513) eli perintälaki uudistui vuonna 2013. Tuolloin lakiin kirjattiin, että perintää ei voi jatkaa, mikäli velallinen kiistää maksuvelvollisuutensa (4 b §).

Suomen Yrittäjien Tiina Toivosen mukaan (Rytkönen & Toivonen 6.3.2019) lakimuutos oli hyvin tervetullut ja on selventänyt paljon yrittäjien oikeuksia valelaskutapauksissa. Aiemmin yrittäjät saattoivat maksaa aiheettomia laskuja hyvinkin helposti luottotietojen menettämisen pelossa. Nykyisin yrittäjät tuntevat oikeutensa paremmin, ja muutos perintälaissa onkin ollut merkittävä apukeino taistelussa huijauslaskuja vastaan. Lisätiedottamista asiasta kuitenkin selvästi tarvitaan, sillä huijauslaskuja maksetaan edelleen turhaan siinä pelossa, että yrittäjä saa luottotietoihinsa merkinnän.

3 Huijaustyypit ja tyyppitapaukset

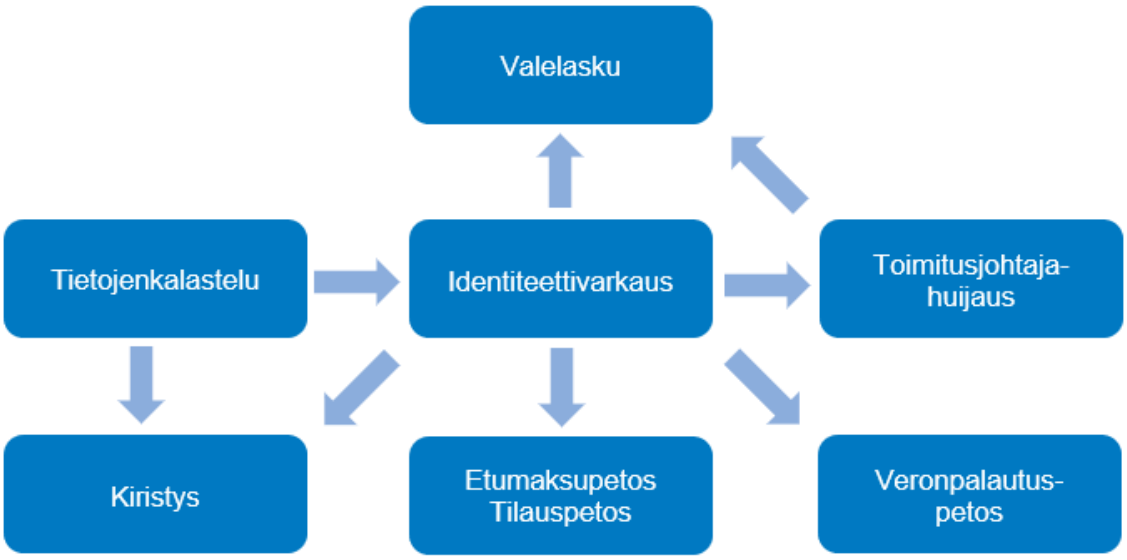
Huijausten kirjo on varsin laaja eikä huijareiden kekseliäisyydellä tunnu olevan rajaa. Huijaukset muuttavat jatkuvasti muotoaan, kehittyvät ja käyttävät tehokkaasti hyväkseen teknologian tarjoamia mahdollisuuksia. Toisaalta jotkin huijaustavat ovat osoittautuneet niin toimiviksi ja tuottaviksi, että ne jatkavat lähes saman kaavan mukaan vuodesta toiseen. Myös tietotekniikkarikollisuus eli kyberrikollisuus on yhä suuremmassa roolissa yrityksiin kohdistuvissa huijauksissa.

Tässä luvussa kuvataan yleisimpiä yrityksiin kohdistuvia huijauksia, niiden variaatioita ja esimerkkitapauksia. Huijaustyypit jaetaan opinnäytetyössä seuraaviin kymmeneen ryhmään: 1) hakemistopalvelut, 2) valelaskut ja laskuväärennökset, 3) tietojenkalastelu, 4) identiteettivarkaudet, 5) toimitusjohtajahuijaukset, 6) etumaksu- ja tilauspetokset, 7) veronpalautushuijaukset, 8) kiristykset, 9) domain-huijaukset ja 10) lakimuutoksiin perustuvat huijaukset. Viimeinen kategoria käsittää huijaukset, jotka hyödyntävät ihmisten epävarmuutta ja hämmennystä liittyen esimerkiksi lainsäädännöllisiin tai yhteiskunnallisiin muutoksiin. Nämä huijaukset voidaan toteuttaa monilla eri tavoilla.



Kuva 1. Yrityksiin kohdistuvat huijaustyypit

Huijaustapojen tarkka luokittelu on vaikeaa. Yllämainituilla huijaustyypeillä on paljon yhtymäkohtia ja päällekkäisyyksiä. Huijaus voi sisältää useamman ryhmän piirteitä. Päällekkäisyyksien ja yhtymäkohtien takia rikosnimikkeen määrittely huijaukselle voi olla hankalaa. Esimerkiksi identiteettivarkaudella on keskeinen asema monissa huijauksissa. Tietojenkalastelu voi mahdollistaa identiteettivarkauden, joka voi puolestaan johtaa esimerkiksi toimitusjohtajahuijaukseen tai veronpalautuspetokseen (kuvio 1).



Kuvio 1. Esimerkki huijaustyyppien yhtymäkohdista

3.1 Hakemistopalveluhuijaukset

Erilaisia rekisteri- ja hakemistopalveluja tarjoavat yritykset tuottavat suomalaisille yrityksille paljon vaivaa. Niiden harjoittama harhaanjohtava markkinointi on yksi yleisimmistä pk-yrityksiin kohdistuvista ongelmista. (Tuorila 2017, 15.) Hakemistopalveluhuijausten mekanismi on varsin tunnettu, ja nykyisin ainakin Helsingin uusyrityskeskus NewCo:ssa pyritään varoittamaan tämäntyyppisistä huijauksista. Ongelma koetaan suureksi, ja NewCo:ssa ollaan ymmällään siitä, että huijaukset ovat voineet jatkua jo toistakymmentä vuotta. Ongelmaan olisi jo pitänyt pystyä puuttumaan. (Utso 26.3.2019.)

Tyypillisessä tapauksessa yritykseen otetaan yhteyttä puhelimitse ja tarkistetaan yrityksen yhteystietoja. Yrittäjä saa pian puhelun jälkeen laskun hakemistopalveluyritykseltä, vaikkei ole ymmärtänyt solmineensa minkäänlaista sopimusta. Hakemistopalveluyritysten toiminta perustuukin usein harhaanjohtamiseen ja perusteettomien laskujen lähettämiseen palveluista, joita ei ole tilattu. Kaiken kukkuraksi useimmat myydyistä hakemistopalveluista ovat

kuluttajille tuntemattomia, ja näin ollen yrityksille täysin hyödyttömiä. Vasta perustetut yritykset ovat erityisesti hakemistopalveluita myyvien yritysten kohteena. (Tuorila 2017, 15.)

Laskun riitauttaminen tai sopimuksen irtisanominen voi osoittautua vaikeaksi. Hakemistoyritykseen voi olla vaikea saada yhteyttä. Jos yrittäjä kokee saaneensa perusteettoman laskun, hän voi pyytää puhelinkeskustelun tallenteen. Puhelutallenteesta voidaan todentaa sopimuksen syntyminen. Joskus nauhoituksen saaminen voi olla kuitenkin hankalaa. (Tuorila 2017, 15.)

Jotta hankaluuksilta voisi välttyä, on tärkeää olla tarkkana kaikkien puhelimitse tehtyjen markkinointiyhteydenottojen suhteen. Suomen Yrittäjät (2018b) neuvookin olemaan sitoutumatta mihinkään tilauksiin puhelimessa, vaatimaan tilauksista aina kirjallinen tarjous ja sopimusehdot sekä tutustumaan niihin huolellisesti. Epäselvästä laskusta kehotetaan tekemään reklamaatio välittömästi ja pyytämään kirjallisesti nauhoite puhelinkeskustelusta. Jos nauhoitetta ei anneta, voi ottaa yhteyttä tietosuojavaltuutettuun. Kirjeenvaihto on tärkeä dokumentoida. Mahdollisen perintäkirjeen voi riitauttaa tekemällä kirjallisen ilmoituksen pätemättömästä sopimuksesta perintätoimistolle. Siihen on syytä liittää kaikki asiaan liittyvät dokumentit.

Puhelinmarkkinoinnin lisäksi rekisteripalveluita tarjotaan kirjeitse ja sähköpostitse. Varsinkin ulkomaiset toimijat massapostittavat harhaanjohtavia kirjeitä ja sähköpostiviestejä suomalaisiin yrityksiin. Niissä saatetaan antaa vaikutelma pelkästä tietojen päivittämisestä, mutta niiden todellinen luonne selviää usein pienestä ja vaikeaselkoisesta printistä. Suomalaiset yritykset ovat saaneet tällaisia tarjouksia muun muassa World Business List, International Fairs Directory ja European Business Number -nimisiltä tahoilta. (Suomen Yrittäjät 2017a; 2018c, 2018d).

Case European Business Number

European Business Number (EBN) on harjoittanut yrityksiin kohdistuvaa harhaanjohtavaa markkinointia eri puolilla Eurooppaa jo useiden vuosien ajan. Suomen Yrittäjät varoittivat Suomeen rantautuneista EBN:n huijauskirjeistä ensimmäisen kerran vuoden 2015 joulukuussa. Sen mukaan huijauksesta oli tehty havaintoja jo aikaisemmin eri puolilla Eurooppaa. Huijauskirjeessä annetaan vaikutelma virallisen tahon ylläpitämästä yritysrekisteristä, jonka päivittäminen on ilmaista. Kuitenkin allekirjoittaessaan ja palauttaessaan paperit yrittäjä sitoutuu kolmen vuoden sopimukseen, joka maksaa satoja euroja vuodessa. (Suomen Yrittäjät 2015.)

Suomen Yrittäjät kiinnitti huomiota EBN:n huijauskirjeisiin uudelleen vuoden 2017 helmikuussa sekä vuotta myöhemmin helmikuussa 2018, kun suomalaiset yrittäjät olivat jälleen joutuneet uusien huijausaaltojen kohteeksi (Suomen Yrittäjät 2017b; Suomen Yrittäjät 2018c). Uusin EBN:ää koskeva Suomen Yrittäjien uutinen helmikuulta 2019 kertoo havainnosta, jonka mukaan ulkopuolinen sovittelija tarjoaa palvelua, jossa yhden vuoden maksua vastaan EBN luopuu kolmen vuoden maksuvaatimuksistaan (Suomen Yrittäjät 2019a).

EBN:n internet-sivuilla (www.e-b-n.eu) on mahdollisuus tehdä hakuja ja niiden kautta löytyy tietoja eurooppalaisista yrityksistä. Esimerkiksi hakusanalla ”Finland” löytyy noin 70 Suomessa toimivan yrityksen tiedot. Sivustolla selitetään European Business Numberin tarkoitusta varsin ympäripyörein sanakääntein seuraavasti:

> The European Business Number for professional participants with homepage is not just another global search engine. On the contrary - the European Business Number is refreshing in that it places reassuring limits on the endlessness of the World Wide Web. Only European non-private Internet subscribers are listed in the European Business Number so you will search precisely in the galaxy of the orbit in which you are at home. The European Business Number will help you search in the expanses of the World Wide Web and find new business partners, customers or suppliers specifically within Europe. (EBN 2019.)

EBN lähettää kirjeitään todennäköisesti tuhansittain monissa Euroopan maissa toimiviin yrityksiin. Vuoden 2018 aikana sen toiminnasta on varoiteltu esimerkiksi Ruotsissa, Alankomaissa, Irlannissa, Espanjassa, Portugalissa ja Maltalla (Förenade Bolag 2018; Fraud Help Desk 2018; JFW 2018; El Mundo Financiero 2018, Visão 2018; GRTU 2018).

EBN-huijauksen takana on olemassa oleva hampurilainen yritys nimeltä DAD Deutscher Adressdienst GmbH (Förenade Bolag 2018). Yritys on nähtävästi harjoittanut kyseenalaista liiketoimintaansa jo varsin pitkään, sillä sen nimellä löytyy internet-haulla varoituksia jopa vuodelta 2004. Tuolloin DAD Deutscher Adressdienst markkinoi palvelua saksalaisille yrityksille nimellä ”Deutsches Internet Register” (Preidel 4.12.2004). Vuonna 2005 italiankielisessä blogissa kerrottiin yrityksen harhaanjohtavasta kirjeestä, jonka otsikkona oli ”Registro Italiano in Internet” (Tentativi 7.6.2005). Näissäkin huijauksissa oli jo kyse samankaltaisesta satojen eurojen hintaisesta sitovasta tilausansasta.

Saman yrityksen käsialaa on myös tavaramerkki EuroMedi, European Medical Directory, jota markkinoidaan lähes identtisellä, yhtä harhaanjohtavalla tavalla terveydenhuollon ammattilaisille. Osittain esitäytetyn lomakkeen palauttamalla yritys sitoutuu kolmen vuoden sitovaan tilaukseen, jonka vuosimaksu hipoo tuhatta euroa. (LoschelderLeisenberg 2018.)

DAD Deutscher Adressdienst GmbH ei ole rajannut toimintaansa Euroopan rajojen sisäpuolelle. Saman yrityksen nimissä on internet-sivusto ”Commercial Register – Australian Business Number” (www.au-abn.com). Termien käyttö on erityisen harhaanjohtavaa, sillä Australian Business Number on virallinen australialaisten yrityksen yksilöllinen tunniste (Australian Government 2019). Sivusto on tehty samalla kaavalla kuin EBN:n sivusto ja myös sillä voi tehdä hakuja, joilla löytyy tietoja australialaisista yrityksistä.

3.2 Valelaskut ja laskuvääränn ökset

Vale- tai huijauslaskulla laskutetaan palvelusta, jota yritys ei ole tilannut. Valelaskut näyttävät usein oikeilta laskuilta ja niissä saatetaan jäljitellä tunnettuja yrityksiä tai brändejä. Valelaskuja lähetetään usein massapostituksina sillä oletuksella, että osa niistä maksetaan epähuomiossa. Maksamiseen saatetaan painostaa myös lyhyellä maksuajalla. Kesä on valelaskujen sesonkiaikaa, sillä kesälomansijaiset lankeavat helpommin valelaskuihin. (Tuorila 2017, 16.) Valelaskuiksi voi mieltää myös harhaanjohtavasti laskun muotoon laaditut tarjoukset.

Laskuvääränn öksissä laskun aihe on oikea, mutta laskuttajan tilinumero on vaihdettu huijarin tilinumeroksi. Alkuperäiset laskut on voitu varastaa murtautumalla postin kirjelaatikoihin. Sen jälkeen ne on väärennetty ja lähetetty eteenpäin vastaanottajalle. Lasku näyttää siis kaikin puolin aidolta, mutta rahat menevät väärään osoitteeseen. (Tuorila 2017, 16.) Myös sähköisesti lähetetty lasku voidaan väärentää. Jos huijarit onnistuvat murtautumaan yrityksen tietojärjestelmään, voivat he siepata taloushallinnon työntekijän sähköpostista laskuja, muuttaa saajan tilinumeron ja ohjata näin maksut omille tileilleen.

Aiheettomat laskut ovat yleisiä IPR-alalla (Intellectual Property Rights). Immateriaalioikeuksien ja lakipalvelujen asiantuntijayritys Kolster kertoo sivustollaan, että aiheettomat laskut ja rekisteröintipalvelujen harhaanjohtava markkinointi ovat kasvava suuntaus alalla. Uusin trendi huijauksissa on käyttää laskuissa tunnuksia, jotka sekoittuvat helposti virastojen nimien ja logojen kanssa ja pyrkiä näin harhauttamaan vastaanottaja. (Kolster 2018.)

Huijauslaskuja on saatu tyypillisesti pian sen jälkeen, kun patenttihakemus tai tavaramerkin tai mallioikeuden rekisteröintihakemus on tullut julkiseksi virallisissa kansainvälisissä

tietokannoissa (EPO, EUIPO ja WIPO). Huijarit saavat oikeat perustiedot hakijasta, hakemuksesta ja rekisteröinnistä näistä julkisista tietokannoista ja käyttävät niitä lähettämissään laskuissa saadakseen ne näyttämään virallisilta. Käytännössä kyse on harhaanjohtavasta markkinoinnista ja laskut ovat tarjouskirjeitä, joissa tarjotaan esimerkiksi rekisteröinti- tai uudistamispalveluita yleensä täysin hyödyttömissä rekistereissä. (Kolster 2018.) Esimerkki laskua jäljittelevästä tarjouskirjeestä on kuvassa 2. Myös Patentti- ja rekisterihallitus on varoittanut tavaramerkkiasiakkaitaan harhaanjohtavista laskuiksi naamioiduista tarjouskirjeistä (PRH 2017).

WPTR
World Patent and Trademark Register

REGISTRATION OF THE EUROPEAN PATENT
RENEWAL

Contract Number: [redacted]

Sent Date: [redacted]

[redacted]

Applicant

WPTR s.r.o.
Prikop 843/4
602 00 Brno
Czech Republic

Tax number: 06466036

Provider

REGISTRATION DETAILS

Title: [redacted]

Classification: [redacted]

Publication Type: [redacted]

Publication Number: [redacted]
Application Number: [redacted]
Int. Publication Number:
Week of publication [redacted]
Filing Date [redacted]

Sign the document within 14 days and send it back by e-mail to **office@wptr.biz** or by mail to:
WPTR s.r.o., Prikop 843/4, 602 00 Brno, Czech republic.

Registration Fee	Amount	
Renewal Fee for 7184400079	1 929,00	EUR
Processing Fee	25,00	EUR
Total Registration Fee	**1 954,00**	**EUR**

Registration of the European Patent:

The patent application has been published in the European patent reports, which are edited by European Patent Office. This publishing forms the basis of our offer. Please note, registration is not affiliated with the publication of the official International Patent Application registration and is not a registration by a government entity. By signing this Agreement, the Applicant signs a binding "WPTR Registration" service provided by the provider specified in the GTB article 3 paragraph 1 and undertakes to pay the provider the price stated on this form. Given that this form is exclusively an offer for the conclusion of a contract, the contractual relationship created by this contract arises at the moment of the delivery of this contract to the provider. Effective delivery is deemed to be the delivery of the contract to the address of the provider and the delivery of the contract to the email address of the provider. By signing this contract, the Contracting Authority agrees that the contractual relationship is governed by the General Business Terms and Conditions of the Provider, which are listed on the other side of this Form and are governed by the Act No. 89/2012 Coll. Civil Code. The Applicant declares that he has read and read these General Business Terms and the scope of the service provided, and he further declares that they agree with their wording.

Applicant

Date

Full name

Signature

Provider

WPTR s.r.o.
Prikop 843/4, 602 00 Brno
Czech Republic
IČ: 06466036

WPTR s.r.o., Prikop 843/4, 602 00 Brno, Czech Republic, Tax number: 06466036, www.wptr.biz, info@wptr.biz

1AC393ECF

Kuva 2. Esimerkki huijauslaskusta patentin uusimiseksi (EPO 2019)

3.3 Tietojenkalastelu

Tietojen kalastelu eli phishing on rikollista toimintaa, jolla pyritään hankkimaan luottamuksellisia tietoja, kuten henkilön sähköinen identiteetti tai rahaliikenteen tunnukset. Toiminta on hyvin yleistä: Euroopan unionin tietojen mukaan unionin kansalaisille lähetetään vuosittain noin 36 miljardia kalasteluviestiä (Euroopan unionin neuvosto 2019). Tietojen urkinta tapahtuu useimmiten oikeiden yritysten ja virastojen nimissä lähetettyjen sähköpostien välityksellä. Sähköpostien tarkoituksena on johdattaa vastaanottaja väärennetyille sivustoille ja huijata hänet luovuttamaan käyttäjätunnuksia, salasanoja tai muita henkilökohtaisia tietoja. Tietoja voidaan myös varastaa sähköpostin mukana tulevien haittaohjelmien avulla. Tietojen kalastelussa käytetään hyväksi sekä sosiaalisen manipuloinnin keinoja että teknologian tarjoamia mahdollisuuksia. (APWG 2019, 2.)

Phishing-hyökkäykset ovat todellinen uhka yrityksille. Tietoturvayhtiö Sophosin teettämässä kyselyssä 54 % 906:sta länsieurooppalaisesta IT-johtajasta vastasi, että heidän yrityksessään oli tunnistettu tapauksia, joissa työntekijät vastasivat ei-toivottuihin sähköposteihin tai avasivat niissä olevia linkkejä. Tutkimuksesta ilmeni, että suuret yritykset lankeavat todennäköisemmin phishing-ansoihin kuin pienemmät yritykset, vaikka niissä henkilökunta saa todennäköisemmin myös koulutusta tietoturvauhkiin liittyen. Tämä voi johtua siitä, että hakkerit keskittyvät laajempiin organisaatioihin suurempien voittojen toivossa. (Computer Weekly 2019; Information Age 2019.)


Subject: Due Invoice 949494

Luottamuksellinen / Konfidentiellt / Confidential

Aihe / Ämne / Subject : Due Invoice 949494

Avaa viesti tästä / Öppna meddelandet / Open message

Olet saanut luottamuksellisen viestin. Viesti avataan ja siihen voidaan vastata yläpuolella olevasta linkistä. Yhteys on suojattu TLS-salauksella. Turvallisuussyistä viestin lukemista on rajoitettu ja se voidaan lukea korkeintaan 10 päivän ajan.

Du har fått ett konfidentiellt meddelande. Meddelandet kan öppnas och svaras på från länken ovanför. Förbindelsen är skyddad med TLS-kryptering. Av säkerhetsskäl är läsningen begränsad och meddelandet kan läsas i högst 10 dagar.

You have received a confidential message. The message can be opened and replied to from the link above. The connection is protected with TLS encryption. Due to security reasons reading of the message is limited and can be read for 10 days at most.

CLICK THE FOLLOWING LINK TO OPEN THE INVOICE

Kuva 3. Turvapostiviestiä jäljittelevä tietojenkalastelu (Traficom 2018a)

Phishing-huijauksilta suojautumisessa on erityisen tärkeää suhtautua epäilevästi kaikkiin odottamattomiin yhteydenottoihin. Jotkin huijausyritykset tunnistaa helposti niiden tökeröstä kielestä tai toteutuksesta, mutta yhä useampi niistä on varsin uskottavasti rakennettu. Jos huijauksesta on pienikin epäilys, kannattaa linkki tai tiedosto jättää avaamatta. Sähköpostin lähettäjä sekä verkkosivuston osoite kannattaa tarkistaa huolellisesti. Joskus sähköpostiosoite tai verkkosivut on rekisteröity tunnusten alle, jotka muistuttavat läheisesti aitoja sivuja. Salatun yhteyden osoite alkaa https:// -tekstillä ja esimerkiksi kaikki verkkopankit käyttävät salattua selainliikennettä. Pelkkä http:// osoiterivin alussa tulisi viimeistään saada hälytyskellot soimaan. (Traficom 2017.)

Yksi yleisimmistä phishing-huijauksista pyrkii kalastelemaan Microsoftin Office 365 -ympäristön käyttäjätietoja. Huijausten määrä on kasvanut Suomessa roimasti, ja Kyberturvallisuuskeskus varoittaa niistä toistuvasti. Kevättalvella ja keväällä 2019 on ollut liikkeillä paljon O365-ympäristössä tapahtuvia tietojenkalasteluyrityksiä. Niistä moni on todella hyvin suunniteltu ja vaikea huomata huijaukseksi. (Kyberturvallisuuskeskus 2019a.)

Kalasteluviesti tulee usein sellaisen samaan organisaatioon kuuluvan ihmisen nimissä, joka on aiemmin jäänyt rikollisten haaviin. Kalasteluviesti ohjaa uhrin sivulle, joka näyttää kieliversiota myöten täysin oikealta kirjautumissivulta. Ainoastaan osoiteriviä vilkaisemalla voi huomata, että linkki on ohjannut tietojenkalastelusivulle aidon kirjautumissivun sijaan. Kyberturvallisuuskeskus suosittaa ottamaan käyttöön kaksivaiheisen kirjautumisen, jossa tavallisen salasanan lisäksi kirjautuminen pitää vahvistaa myös jollakin toisella keinolla, esimerkiksi toiseen päätelaitteeseen tulevan kertakäyttökoodin avulla. (Kyberturvallisuuskeskus 2019a, Viestintävirasto 2017a.)

Phishing on laajalle joukolle suunnattua automatisoitua tietojen kalastelua, kun taas spear phishing tai kohdennettu verkkourkinta, on tarkasti kohdennettu hyökkäys, jonka tavoitteena on hankkia luottamuksellista tietoa tietyltä henkilöltä tai organisaatiolta. Taktiikka edellyttää edistyneempää tekniikkaa ja tarkkaa tutkimusta kohteesta. Sähköpostiviesti näyttää tulevan tutulta henkilöltä tai organisaatiolta ja se on yleensä personoitu käyttäen hyväksi tietoa, joka vastaanottajasta on löydettävissä. Hyökkääjä etsii usein kohteestaan yksityiskohtaista tietoa julkisista lähteistä tai sosiaalisista verkostoista. Viestissä voidaan esimerkiksi viitata vastaanottajan mielenkiinnon kohteisiin tai sosiaalisiin kontakteihin. Näin viesti voidaan saada näyttämään aidolta ja huijauksen onnistumisen mahdollisuus kasvaa. (Knowbe4 2019.)

Spear phishing -hyökkäyksestä voi olla monenlaisia seurauksia. Se on usein ensiaskel toimitusjohtajahuijaukseen. Vastaanottaja voi myös saada sähköpostin liitetiedostosta haittaohjelman, jonka kautta hyökkääjä saa tartunnan saaneen koneen valvontaansa omistajan huomaamatta. Myös kiristysohjelmat lunnasvaatimuksineen leviävät sähköpostien liitetiedostojen välityksellä. (Knowbe4 2019.)

Tietoturvayhtiö KnowBe4:n (2019) mukaan spear phishing -hyökkäyksiä vastaan suojautumisessa auttaa muun muassa se, ettei yritysten internet-sivuilta löydy kattavaa listaa työntekijöiden sähköpostiosoitteista. Arkaluonteisia henkilökohtaisia tietoja ei tulisi koskaan lähettää sähköpostitse ja tällaisia tietoja pyytäviin viesteihin tulisi aina suhtautua suurella varovaisuudella. Myös sosiaalisessa mediassa jaetun tiedon aiheuttamista riskeistä on kaikkien organisaation jäsenten hyvä olla tietoinen, sillä mitä enemmän tietoa on saatavilla, sitä helpompaa kohdennetusta verkkourkinnasta tulee.

Vishing (voice phishing) on puhelimitse tapahtuvaa tietojenkalastelua. Huijari puhelimen päässä voi väittää olevansa esimerkiksi pankin, teknisen tuen tai viranomaisen edustaja. Useimmiten hän yrittää kalastella salasanoja, pankkitunnuksia tai luottokorttitietoja päästäkseen käsiksi uhrin rahoihin. Asiaan liittyy usein kiire eikä puhelimessa ole aikaa jäädä pohtimaan kuulemaansa. Motivaationa saattaa olla myös vakoilu tai pääsy yrityksen tietojärjestelmiin. Joskus huijarit voivat onkia puhelimitse tietoja esimerkiksi organisaation rakenteesta tai johtajien matka-aikatauluista taustatyönä myöhemmälle huijaukselle. (Proofpoint 2018.)

3.4 Identiteettivarkaudet

Identiteettivarkaudella tarkoitetaan tilannetta, jossa esiinnytään oikeudettomasti toisen henkilöllisyydellä. Rikoksentekijän tarkoituksena on erehdyttää kolmatta osapuolta käyttämällä jonkun toisen henkilön henkilötietoja, tunnistautumistietoja tai muuta vastaavaa yksilöivää tietoa. (Åberg 2017, 114.) Identiteettivarkauden tekomuotoja on monia. Yksityishenkilöiden lisäksi rikolliset voivat hyödyntää myös yritysten tai muiden oikeushenkilöiden identiteettiä. Identiteettivarkaus liittyy läheisesti moniin huijauksiin. Rikolliset saavat yritysten ja niiden avainhenkilöiden yksilöiviä tietoja virallisista yritysrekistereistä, yritysten internetsivuilta tai vaikkapa LinkedIn:stä. Tiedonkeruuseen saatetaan käyttää myös haittaohjelmia.

Keskuskauppakamarin (2017, 23) julkaisemasta *Yritysten rikosturvallisuus 2017* -selvityksestä ilmenee, että yrityksiin kohdistuvat identiteettivarkaudet ovat kasvava ilmiö. Sen mukaan 8 % kaikista kyselyyn osallistuneista yrityksistä toimialasta riippumatta ilmoitti, että

yrityksen identiteetti oli kaapattu tai yritetty kaapata viimeisen kolmen vuoden aikana. Vuonna 2012 tehdyssä kyselyssä vastaava luku oli 3 %. Suuret yritykset näyttävät valikoituvan useammin rikoksen kohteeksi, sillä niistä jopa 28 % ilmoitti joutuneensa identiteettikaappauksen tai sen yrityksen uhriksi.

Myös turva- ja vakuutuspalveluyritys mySafety (2018) raportoi identiteettivarkauksien yleistymisestä yritysten keskuudessa. Yrityksen Ruotsissa teettämän tutkimuksen mukaan 15 prosenttia pienistä ja keskisuurista yrityksistä on kokenut identiteettivarkauden. Näistä 74 prosenttia ilmoitti joutuneensa identiteettivarkauden uhriksi viimeisen vuoden aikana. MySafety tarjoaa identiteettivakuutuksia yrittäjille ja yrityksille.

Yrityksen identiteetti voidaan anastaa esimerkiksi muuttamalla tai väärentämällä yrityksen tietoja. Rikolliset voivat tehdä kaupparekisteriin väärennetyn muutosilmoituksen yrityksen yhteystiedoista, henkilökunnasta tai hallituksen jäsenistä. Muutosilmoituksen voi tehdä Patentti- ja rekisterihallitukseen (PRH) sähköisesti tai paperisena. Paperisen muutosilmoituksen voi tehdä helposti kuka tahansa vaikkapa postitse. Kaappauksen jälkeen ovi on avoin monenlaisille väärinkäytöksille. Varkaat voivat tilata tavaraa tai ottaa lainaa yrityksen nimissä, tyhjentää pankkitilit tai myydä yrityksen omaisuutta. (Suomen Yrittäjät 2018e.)

PRH:lla on palveluja, joilla yrittäjät voivat suojautua identiteettivarkauksia vastaan. Vuonna 2017 otettiin käyttöön palvelu, jossa yritys saa sähköpostitse automaattisen ilmoituksen kaupparekisteriin ilmoitetuista muutoksista. Tällä tavoin yrittäjä saa tiedon meneillään olevista muutoksista. Tämä edellyttää, että yrityksen sähköpostiosoite on kaupparekisterissä. Muussa tapauksessa yritys voi tehdä asiasta erillisen sopimuksen PRH:n kanssa. Yrittäjä voi myös valita sähköisen ilmoituksen ainoaksi ilmoituksentekotavaksi ja estää näin riskialttiiden paperisten ilmoitusten tekemisen. (PRH 2019.)

Ranskalainen ministerihuijaus

Ranskassa rikolliset ovat onnistuneet huijaamaan yli 80 miljoonaa euroa eri tahoilta esiintyen puolustusministeri Jean-Yves Drian’in identiteetillä. (Franceinfo 2019a). Tapaus on eräänlainen ääriesimerkki identiteettivarkaudesta. Se on kuin karikatyyri huijareiden kekseliäisyydestä, röyhkeydestä ja suurista ammattimaisista keinoista.

Huijausyritykset saivat alkunsa vuoden 2015 kesällä, kun huijarit alkoivat ottaa yhteyttä kymmeniin ulkomaisiin valtionjohtoihin sähköpostitse ja puhelimitse esiintyen Ranskan silloisena puolustusministerinä. Huijausta yritettiin muun muassa lähettämällä ministerin allekirjoituksella varustettuja valelaskuja ranskalaisista helikoptereista. (Franceinfo 2019a.)

Huijarit muuttivat pian taktiikkaansa ja alkoivat ottaa yhteyttä ranskalaisiin merkkihenkilöihin, liikemiehiin, yritysjohtajiin ja muihin varakkaisiin henkilöihin arkaluontoisen asian tiimoilta. Huijarit kertoivat valtion salaisesta operaatiosta, jonka tarkoituksena oli vapauttaa jihadistien kaappaamia ranskalaisia toimittajia. Huijarit selittivät, että Ranskan hallitus ei maksa lunnaita panttivangeista, joten maksun tulisi tapahtua muuta kautta. Henkilöiden isänmaallisuuteen vedoten ”puolustusministeri” pyysi heiltä lainaa, joka oli määrä maksaa nopeasti takaisin. (Franceinfo 2019a.)

Huijarit hioivat edelleen taktiikkaansa ja yrittivät vakuuttaa jotkut uhreistaan videopuhelun avulla. Valeministeri esiintyi videopuhelulla käyttäen oikean ministerin kasvoja jäljittelevää ammattimaista silikoninaamaria. Myös kulissit oli tarkkaan mietitty, sillä huijari esiintyi tilassa, joka jäljitteli ministerin työhuonetta. Jotkut lankesivat ansaan ja siirsivät suuria summia huijareiden tileille Kiinaan. (Franceinfo 2019a.)

Puolalainen pankkihuijaus

Kesällä 2018 Iso-Britanniassa asuvat puolalaiset pienyrittäjät alkoivat saada puolankielisiä yhteydenottoja pankilta, joka tarjosi mm. nykyistä edullisempia lainaehtoja sekä luottokortteja ja yritti näin saada yrityksen siirtämään rahansa kyseiseen pankkiin. Suurin osa yhteydenotoista tapahtui aluksi puhelimitse, mutta myöhemmin myös sähköpostin välityksellä. Yritys esitteli itsensä nimellä PKO, joka on yksi Puolan suurimmista pankeista, ja lisäsi sillä huijauksen uskottavuutta. Huijariyrityksen koko nimi oli Publiczny Kapitał Oszczędności, minkä lisäksi se käytti myös erittäin hämäävää PKO Bank Warszawa -nimeä. PKO-pankin virallinen nimi on PKO Bank Polski, joten nimet oli melko helppo sekoittaa keskenään. (Topmejt 2018a.)

Huijaripankki esiintyi virallisena PKO-pankkina käyttämällä Iso-Britannian Financial Conduct Authorityn sivuilta löytyviä oikean PKO-pankin tietoja, kuten yritysnumeroa ja pankin virallista osoitetta Varsovassa. Kun yrittäjät suostuivat huijaripankin asiakkaiksi ja siirsivät varansa sinne, yrityksellä ei enää ollut pääsyä tileilleen. (Topmejt 2018b.)

Muutamaa kuukautta myöhemmin PKO Bank Warszawa alkoi lähettää huijaamilleen yrityksille kirjeitä Puolan finanssivalvontakomission, eli Komisja Nadzoru Finansowegon nimissä. Kirjeet oli leimattu virallisin leimoin ja allekirjoittajana oli komission johtaja, kuten finanssivalvontakomission julkaisemassa kuvassa näkyy (kuva 4). Englanninkielisissä kirjeissä kerrottiin, että yrittäjä ei ole huolehtinut verojen ja muiden maksujen suorittamisesta Puolaan oikein, minkä vuoksi tili on jäädytetty. Kun maksut on hoidettu, yrittäjä saisi oikeuden käyttää tiliään huijaripankissa. (KNF 2018; Topmejt 2018b.)


KNF
KOMISJA NADZORU FINANSOWEGO

APPROVAL #: KNF058138066000 23

NRTCC POLICY REGULATOR
PAYMENT DUE FOR MAY, 2018
FORM NO: PLWARS0518

KNF/PIT/PLN NRTCC PAYMENT NOTIFICATION

ATTN: [redacted]

CC: PKO BANK WARSZAWA
PIOTRA SKARGI 61
03-516 WARSZAWA
POLAND

OSUSTUVO

ACT OF 22 MAY 2003 ON NRTCC INSURANCE AND FUNDS SUPERVISION, AND REFERENCE TO THE REVENUE DISCOUNT WITH AN APPROVAL ORDER KNF058138066000 23 AND FORM NO: PLWARS0518 CTOP, THE NRTCC CALCULATION FROM THE FOLLOWING ACCOUNT 561020490000008502304[redacted] CURRENT ACCOUNT, WAS CONFIRMED AS A NEWLY OPERATED ACCOUNT WITHOUT THE NRTCC CLEARANCE CERTIFICATE.

THE ABOVE ACCOUNT HAS BEEN PUT ON-HOLD/TEMPORARY SUSPENDED AND HAS BEEN RESTRICTED FROM EVERY TRANSFER (IN-OUT) UNTIL THE BENEFICIARY PROVIDES THE NRTCC CLEARANCE CERTIFICATE AND PAYENT .

THE ABOVE PAYMENT SHOULD BE MADE THROUGH OUR NOMINATED KNF LEGAL REPRESENTATIVE BY THE PAYEE AGENT. .

APP CODE: KNF_CTOP:

KOMISJA NADZORU FINANSOWEGO (KNF) POLISH FINANCIAL SUPERVISION AUTHORITY(PFSA) AND ECONOMIC DEVELOPMENT, TAX PAYMENT CONTROL DIVISION, WARSZAWA, POLAND

MAREK [illegible]OWSKI
COMMISSIONER

Kuva 4. Puolan finanssivalvontakomission nimissä lähetetty huijauskirje (KNF 2018)

Näin ei tietenkään ollut, vaan kirje finanssivalvontakomissiolta oli vain lisäkeino, jolla huijarit saivat rahastettua uhrejaan lisää. Tapauksesta varoiteltiin mediassa ja etenkin Iso-Britanniassa asuvien puolalaisten yhteisöissä, mutta myös virallinen PKO-pankki, Komisja Nadzoru Finansowego ja Financial Conduct Authority julkaisivat tiedotteen huijauksesta (FCA 2018; KNF 2018; PKO 2018; Topmejt 2018b.)

3.5 Toimitusjohtajahuijaukset

Toimitusjohtajahuijaus on yksi identiteettivarkauden muoto. Perinteisessä toimitusjohtajahuijauksessa rikolliset esiintyvät esimerkiksi johtotason henkilönä, kuten toimitusjohtajana tai lakimiehenä ja lähestyvät yrityksen taloushallintoa tai muuta maksuliikenteestä vastaavaa työntekijää useimmiten sähköpostilla. Työntekijä huijataan suorittamaan maksu, joka päätyy rikollisten tilille. Usein tilanteeseen liittyy jokin painostuskeino, kuten kiire. Esimerkiksi maksun väitetään olevan myöhässä tai pyyntö tulee myöhään perjantai-iltapäivänä juuri ennen viikonloppua. (Tuorila 2017, 17; Viestintävirasto 2017b, 13,14)

Toimitusjohtajahuijaus vaatii perehtymistä kohteena olevaan organisaatioon. Sosiaalisen median päivitykset ja sähköpostin out of office -viesti saattavat paljastaa johtajan matkasuunnitelmat. Sähköpostiosoite, jota huijari käyttää, saattaa muistuttaa hyvin läheisesti johtajan oikeaa osoitetta. Esimerkiksi, jos oikea osoite on matti.meikalainen@firma.fi, saattaa rikollinen lähettää viestejä osoitteesta matti.meikalainen@firrma.fi. Nopeasti katsottuna ei pientä eroa välttämättä huomaa. Huijaussähköposti voi tulla myös oikeasta osoitteesta, jos rikolliset ovat onnistuneet murtautumaan johtajan sähköpostiin esimerkiksi heikon salasanan vuoksi tai tietokoneeseen asennetun haittaohjelman kautta. (Viestintävirasto 2017b, 13,14)

Keväällä 2018 Helsingin poliisi tiedotti maalis-huhtikuun aikana ilmi tulleista toimitusjohtajahuijaustapauksista, joista oli tehty kymmenkunta rikosilmoitusta. Yritysten tai yhdistysten talousasioista vastaaville henkilöille oli lähetetty johtajan nimissä sähköpostiviestejä, joissa vaadittiin pikaista maksua ulkomaiselle tilille. Vaikka suurin osa huijauksista jäi yritykseksi, onnistuivat rikolliset kolmessa tapauksessa huijaamaan useita kymmeniä tuhansia euroja. Viestejä on kuvailtu uskottaviksi. Ne ovat tulleet oikealta vaikuttaneista osoitteista ja joissain tapauksissa huijari on ollut hämmästyttävän hyvin perillä organisaation asioista, kuten loma-ajoista ja työntekijöiden oikeuksista tehdä maksuja. Suurin osa viesteistä on kirjoitettu suomeksi. Huijauksissa on kyse kansainvälisestä, järjestäytyneestä ja ammattimaisesta rikollisuudesta. (Poliisi 2018.)

Vuonna 2015 kaksi suomalaista pörssiyhtiötä menettivät toimitusjohtajahuijauksessa miljoonia euroja. Ohjelmistoyritys Affecton ulkomaiselta tytäryhtiöltä vietiin taitavasti rakennetulla huijauksella 960 000 euroa. Vain hieman aiemmin toinen suomalaisyritys Konecranes oli joutunut samankaltaisen petoksen kohteeksi sen ulkomaisen tytäryhtiön kautta ja menettänyt peräti 17 miljoonaa euroa. Suomalaiset yritykset ovat päässeet huijauksissa toistaiseksi vähällä suurempiin maihin verrattuna muun muassa pienemmän kielialueen

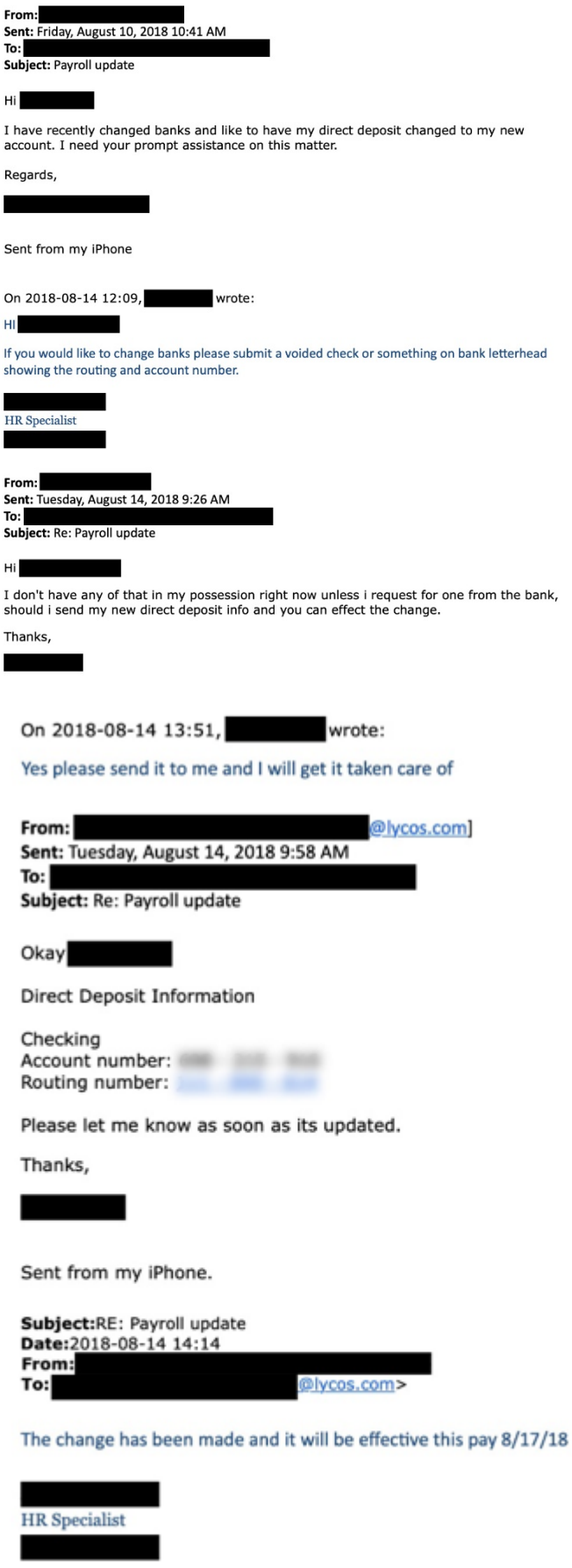
ansiosta. Huijauksissa käytetään useimmiten englantia, mutta suuremmissa maissa kuten Ranskassa ja Saksassa huijataan maan kielellä. (Kaleva 2016; YLE 2016b.)

Suurissa suomalaisissa yrityksissä organisaation kieli on yhä useammin englanti, mikä tekee niistä helpompia kohteita kansainvälisille ammattirikollisille. Affecton ja Konecranesin tapauksissa kohteena olivat nimenomaan niiden ulkomaiset tytäryhtiöt, joten voidaan olettaa, että näissä onnistuneissa huijauksissa käytettiin englantia.

Maailmanlaajuisesti toimitusjohtajahuijauksissa on kyseessä valtavat rahasummat. FBI:n raportin mukaan kohdennetut huijaussähköpostit (Business E-mail Compromise ja E-mail Account Compromise) ovat kautta maailman yli 12 miljardin dollarin bisnes. FBI:n internetrikollisuuden valvontakeskuksen (IC3) keräämien ilmoitusten mukaan kyseisissä huijauksissa oli joko menetetty tai oltu vaarassa menettää yhteensä enemmän kuin 12,5 miljardia dollaria lokakuun 2013 ja toukokuun 2018 välillä. Tämä merkitsee 136 %:n kasvua joulukuun 2016 ja toukokuun 2018 välillä. FBI:n mukaan ilmoituksia on tehty yli 78 000 150:ssä maassa. (FBI 2018a.)

Palkkahuijaus

Tietoturvayritys Agarin (2019) mukaan yritysten palkanmaksuun liittyvät huijaukset ovat kasvava trendi. Koska huijarit käyttävät paljon resursseja yritysten organisaatioon liittyvään tiedonhankintaan, halutaan näille investoinneille myös vastinetta. Huijaustavat ottavatkin mitä erilaisempia muotoja. Jos jokin huijaustaktiikka ei onnistu, kokeillaan toista. Palkkahuijaus toteutetaan toimitusjohtajahuijauksen periaatteella. Vaikka huijauksessa voi käyttää hyväkseen kenen tahansa työntekijän identiteettiä, on huijaus tuottoisin korkeapalkkaisten johtajatason henkilöiden nimissä. Huijari esiintyy työntekijänä useimmiten jäljittelemällä tämän sähköpostia (kuva 5) ja pyytää palkanmaksusta vastuussa olevaa henkilöä muuttamaan palkanmaksussa käytettäviä tilitietoja. Huijauksen onnistuessa palkka voi ohjautua huijarin tilille viikkojen tai jopa kuukausien ajan riippuen siitä, kuinka usein työntekijä tarkistaa tilitapahtumiaan.



From: [redacted]
Sent: Friday, August 10, 2018 10:41 AM
To: [redacted]
Subject: Payroll update

Hi [redacted]

I have recently changed banks and like to have my direct deposit changed to my new account. I need your prompt assistance on this matter.

Regards,

[redacted]

Sent from my iPhone

On 2018-08-14 12:09, [redacted] wrote:

HI [redacted]

If you would like to change banks please submit a voided check or something on bank letterhead showing the routing and account number.

[redacted]
HR Specialist
[redacted]

From: [redacted]
Sent: Tuesday, August 14, 2018 9:26 AM
To: [redacted]
Subject: Re: Payroll update

Hi [redacted]

I don't have any of that in my possession right now unless i request for one from the bank, should i send my new direct deposit info and you can effect the change.

Thanks,

[redacted]

On 2018-08-14 13:51, [redacted] wrote:

Yes please send it to me and I will get it taken care of

From: [redacted]@lycos.com]
Sent: Tuesday, August 14, 2018 9:58 AM
To: [redacted]
Subject: Re: Payroll update

Okay [redacted]

Direct Deposit Information

Checking
Account number: [redacted]
Routing number: [redacted]

Please let me know as soon as its updated.

Thanks,

[redacted]

Sent from my iPhone.

Subject:RE: Payroll update
Date:2018-08-14 14:14
From: [redacted]
To: [redacted]@lycos.com>

The change has been made and it will be effective this pay 8/17/18

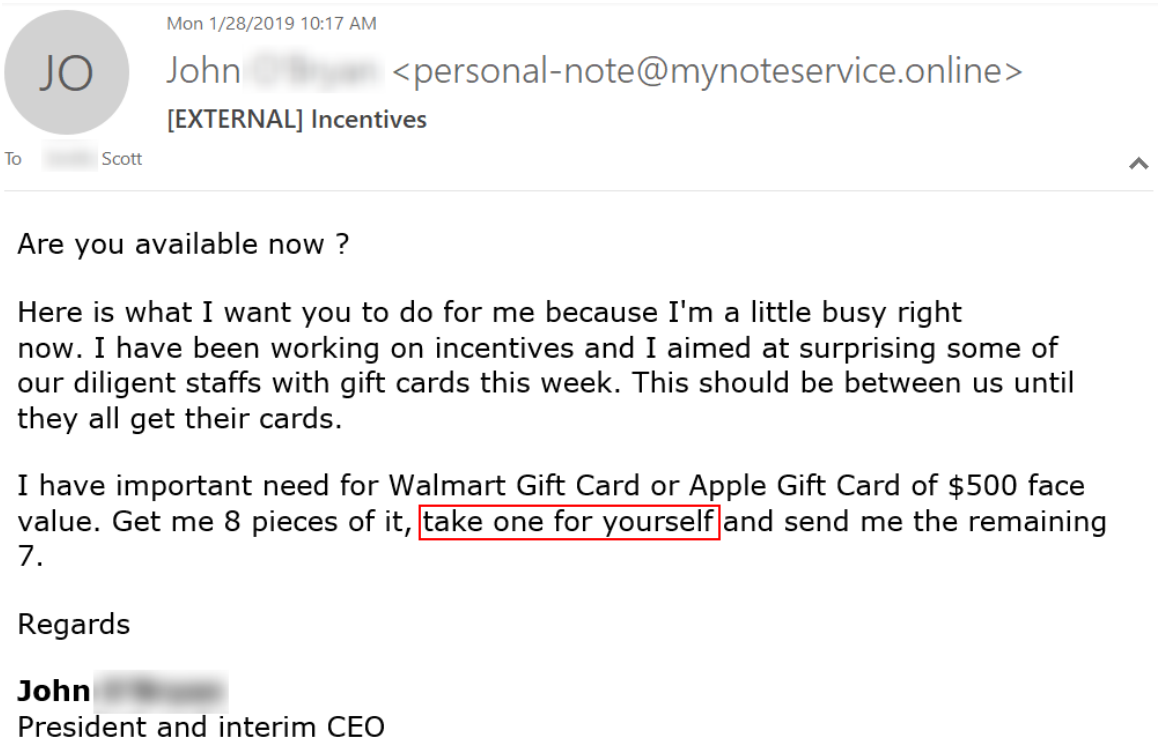
[redacted]
HR Specialist
[redacted]

Kuva 5. Sähköpostitse toteutettu palkkahuijaus (Agari 2019)

Lahjakorttihuijaus

Yhdysvalloissa FBI on kiinnittänyt huomiota yleistyneisiin yrityksiin kohdistuviin lahjakorttihuijauksiin. Loppuvuosi lahjoineen ja bonuksineen on erityisen otollista aikaa tämän tyyppisille huijauksille. Huijari esiintyy johtotason henkilönä ja antaa työntekijän tehtäväksi ostaa lahjakortteja. Työntekijää pyydetään sitten lähettämään lahjakorttien tiedot esimiehenä esiintyvälle huijarille, joka lunastaa kortit saman tien ja muuttaa ne rahaksi. (FBI 2018b.)

Tietoturvakouluttamiseen erikoistuneen KnowBe4:n perustaja ja toimitusjohtaja Stu Sjouwerman (29.1.2019) kiinnittää huomiota entistä kehittyneempiin sosiaalisen manipuloinnin taktiikoihin nopeasti yleistyneissä lahjakorttihuijauksissa. Huijaus on erinomaisesti ajoitettu. Lahjakorttien ostolle on uskottava ja perusteltu syy kuten henkilökunnalle tarkoitetut kannustimet. Lahjakorttien hankkiminen on työntekijälle uskottu luottamuksellinen tehtävä ja yllätys henkilökunnalle, joten siitä ei tule kertoa kenellekään. Lisäksi työntekijää saatetaan motivoida tarjoamalla hänelle henkilökohtaista hyötyä, esimerkiksi kehottamalla pitämään yksi lahjakortti itsellään kuten kuvassa 6.



Kuva 6. Lahjakorttihuijaus toimitusjohtajan nimissä (Sjouwerman 29.1.2019)

Tahitilaisen mehutehtaan tapaus

Tahitilaista mehutehdasta, Jus de Fruits de Mooreaa alkuvuodesta 2019 kohdannut toimitusjohtajahuijaustapaus valaisee sitä, kuinka voimakas vaikutus sosiaalisella manipuloinnilla voi olla ja kuinka vakaviin seurauksiin huijaus voi johtaa. Huomionarvoista tapauksessa on myös se, kuinka avoimesti ja yksityiskohtaisesti yrityksen toimitusjohtaja kertoi painajaiseen johtaneesta tapahtumakulusta medialle. Onhan uutisoinnilla ensiarvoisen tärkeä rooli huijauksiin liittyvän tietoisuuden levittämisessä ja monen potentiaalisen huijauksen estämisessä.

Noin 45 henkilöä työllistävä tahitilaisyritys ei ollut suinkaan tietämätön huijausten mahdollisuudesta. Huijaukset olivat olleet puheenaiheena kolmen vuoden ajan ja niihin oli varauduttu ottamalla käyttöön tiukat sisäiset menettelytavat. Näistä varotoimenpiteistä huolimatta huijarit onnistuivat murtamaan suojamuurit varsin klassisella toimintatavalla. Yrityksen kokenut kirjanpitäjä sai puhelun henkilöltä, joka esiintyi kuuluisan eurooppalaisen lakitoimiston lakimiehenä. Hetken päästä hän sai toimitusjohtajan nimissä sähköpostin, jossa annettiin ohjeita erittäin luottamuksellisesta rahoitustapahtumasta. (Tahiti Infos 2019.)

Sosiaalisen manipuloinnin keinoin huijarit saivat kirjanpitäjän mukaan juoneensa. Hänet saatiin uskomaan, että hän on osa erittäin tärkeää ja luottamuksellista tehtävää. Toiminnan uskoteltiin olevan niin salaista, ettei kirjanpitäjä saisi hiiskahtaakaan asiasta, edes itse toimitusjohtajalle. Kirjanpitäjä ohittikin huijareiden käskystä kaikki sisäisen valvonnan menettelyt. Vaikka hän tapasi toimitusjohtajaa jatkuvasti, hän ei viitannut asiaan sanallakaan. Kun toimitusjohtaja lähti lomalle viikoksi, kirjanpitäjä käsitteli yrityksen varoja ja suoritti maksuja huijareiden ohjeiden mukaisesti kiinalaisille tileille. (Tahiti Infos 2019.)

Yrityksen menettämä summa oli 150 miljoonaa CFP-frangia (noin 1,25 miljoonaa euroa). Huijaus ajoittui yrityksen epäonneksi ajankohtaan, jolloin sen rahavarat ovat joulukuun myynnistä johtuen tavallista suuremmat. Huijarit olivat luultavasti asiasta tietoisia. Huijattu summa oli suurempi kuin yrityksen rahavarat, minkä mahdollisti pankin kanssa sovittu tilinylitysmahdollisuus. Huijaus on asettanut pienen yrityksen katastrofaaliseen taloudelliseen tilanteeseen ja koko sen toiminnan sekä sitä kautta kaikkien työntekijöiden toimeentulon vaakalaudalle. (Tahiti Infos 2019.)

Toimitusjohtaja peräänkuulutti tiedotteessaan myös rahalaitosten vastuuta huijausten torjunnassa. Hän ihmetteli sitä, etteivät pienen yrityksen epätavallisen suuret ja poikkeukselliset rahasiirrot kansainvälisesti tunnettuun likaisen rahan kauttakulkumaahan saaneet

pankin hälytyskelloja lainkaan soimaan. (Tahiti Infos 2019.) Pankeilla on tärkeä rooli huijausten torjunnassa, sillä niiden tehokkaat turvajärjestelyt voivat auttaa paljastamaan petoksia ja estää niihin liittyvää rahaliikennettä.

Taloudellisten vahinkojen lisäksi tahitilaisyrityksen tapauksella on varmasti myös vakavia henkisiä seurauksia. Voi vain arvailla mitä huijaukseen langenneen työntekijän mielessä on tapahtunut huijauksen paljastuttua. Kuten luvussa 2 tuli esiin, voimakkaat häpeän tunteet sekä syyllisyys työnantajalle ja työtovereille aiheutetusta ahdingosta voivat piinata uhria. Pelko irtisanomisesta ja toimeentulon menetyksestä on varmasti myös lamauttava. Tämä voi johtaa vakavaan masennukseen eikä itsemurhan riskikään ole pois suljettu.

3.6 Etumaksupetokset ja myyjään kohdistuvat tilauspetokset

Etumaksupetoksissa yritystä pyydetään maksamaan tilauksen maksu etukäteen. Tilattua tuotetta tai palvelua ei kuitenkaan koskaan toimiteta eikä maksua palauteta. Myyjään kohdistuvissa tilauspetoksissa on kyse siitä, että yritykseltä tilataan tavaraa, jota ei ole aikomus maksaa. Ulkomainen tilaaja saattaa käyttää maksuvälineenä shekkiä, joka osoittautuu katteettomaksi. (Tuorila 2017, 18.)

Harmaa talous & talousrikollisuus -hankkeen sivustolla kerrotaan ilmiöstä, jossa yhtiömuotoisia yrityksiä käytetään työkaluina erilaisissa petoksissa. Samalla yhtiöllä saatetaan tehtailla erityyppisiä petoksia, kuten tilauspetoksia ja arvonlisäveron palautuspetoksia. Yhtiön vastuuhenkilöksi merkitään usein bulvaanihenkilöitä. (Harmaa talous & talousrikollisuus 2018.)

Yrityksiä voidaan käyttää hyväksi monella tapaa. Rikolliset saattavat perustaa uuden yrityksen pelkkään rikostarkoitukseen tai ostaa vaikeuksissa olevan yrityksen halvalla. Hyvämaineisen, rehellisen yrityksen identiteetti saatetaan kaapata tai sellaisen nimessä voidaan alkaa toimia. Rikollisten tavoitteena on tehtailla nopeasti petoksia esimerkiksi tilaamalla ja myymällä paljon ja nopeasti, ja lopulta kadota rahojen kanssa. (Harmaa talous & talousrikollisuus 2018.)

Itäisen Keski-Euroopan tilauspetokset

Slovakiassa uutisoitiin vuonna 2018 rikosaallosta, jossa onnistuttiin huijaamaan 13 yrittäjältä viidessä maassa yhteensä yli kaksi miljoonaa euroa. Huijaukset tapahtuivat Romaniassa, Slovakiassa, Tšekissä ja Unkarissa vajaan vuoden aikana. (Podnikajte 2018.) Uutisartikkelissa ei määritellä tarkemmin millä alalla huijatut yritykset toimivat.

Tapauksissa huijari esiintyi jonkin hyvämaineisen ranskalaisen, italialaisen tai isobritannialaisen yrityksen nimissä ja lähetti tilauksia yrityksille itäisen Keski-Euroopan maissa. Huijari lähestyi myyjäyritystä yleensä sähköpostitse. Sähköpostiosoite oli aina hyvin samankaltainen kuin oikeankin yrityksen osoite ja käytetyt nimet olivat yrityksen oikeita työntekijöitä, joten huijaus oli vaikea huomata. Tilauksen tavarat toimitettiin huijarille, mutta lasku puolestaan pyydettiin lähettämään sen yrityksen osoitteeseen, jonka nimissä huijari oli esiintynyt. (Podnikajte 2018.)

Eräässä tapauksessa tšekkiläistä yritystä huijattiin jopa väärentämällä paperisia dokumentteja leimoineen ja allekirjoituksineen. Ranskalaisen yrityksen nimissä lähetettiin tšekkiläiselle yritykselle suurehko tilaus. Tilaus oli tehty ranskalaisen yrityksen virallisia dokumenttipohjia käyttäen, eikä mikään niissä viitannut huijaukseen. Huijari jopa lähetti tuotteiden saavuttua vastaanottoilmoituksen edelleen yrityksen virallisia asiakirjoja käyttäen. (Podnikajte 2018.)

Koska yritykset, joiden nimissä tilaukset tehtiin, olivat hyvämaineisia ja huijaus niin hyvin suunniteltu, eivät huijatuksi tulleet yritykset osanneet epäillä mitään ennen kuin tilauksen laskua ei maksettu. Myös yritykset, joiden nimissä tilauksia on tehty, ovat tehneet asiasta ilmoituksia poliisille. (Podnikajte 2018.)

3.7 Veronpalautushuijaukset

Veronpalautuspetoksissa huijareiden tavoitteena on saada itselleen yrittäjälle kuuluvat arvonlisävero- tai muut veronpalautukset. Usein huijari hankkii yrityksen tiedot julkisista rekistereistä ja sitten ilmoittaa verohallinnolle muutoksista yrityksen tilitiedoissa. Tämän jälkeen veronpalautus pyritään saamaan uudelle tilille. (Tuorila 2017, 17.)

Vuoden 2016 syksyllä uutisoitiin mittavasta huijausaallosta, jossa suomalaisten yritysten veronpalautuksia yritettiin ohjata väärille tileille. Yksi huijauskeino, jota rikolliset pyrkivät hyödyntämään oli lähettää väärennetty paperinen muutosilmoitus yrityksen tilinumerosta. Sen jälkeen verohallintoon lähetettiin alv-palautuspyyntö, jolla yritettiin saada verottaja maksamaan veronpalautus väärälle tilille. Yhden yrityksen kohdalla huijaus onnistui ja menetetty summa oli noin 2000 euroa. Huijausyrityksistä saatiin kuitenkin vihiä ja loput niistä onnistuttiin estämään. Jos kaikki lähes kaksi sataa huijausyritystä olisivat onnistuneet, rikosvanhinkojen summa olisi noussut lähes 30 miljoonaan euroon. Rikollisten jäljet johtivat pääasiassa Viroon. (YLE 2016c.)

Tapaus paljasti tietoturva-aukon verottajan käytännöissä, sillä tilitietojen muutosta ei varmistettu yritykseltä. Huijausyritysten tultua ilmi kaikki paperiset muutosilmoitukset varmistettiin puhelimitse. (YLE 2016c.) Verottajan käytäntöä on sittemmin muutettu turvallisemmaksi niin, että yritysten tilinumero ilmoitetaan sähköisesti OmaVero-palvelussa. Paperisella lomakkeella voi tilinumeron ilmoittaa ainoastaan erityisestä syystä, kuten teknisen esteen vuoksi. (Verohallinto 2017a.)

Verohallinnon nimissä on myös lähetetty säännöllisesti huijausviestejä, joissa kerrotaan saatavasta mahdollisesti satojen eurojen veronpalautuksesta. Vastaanottajaa on houkuteltu klikkaamaan linkin kautta valesivustolle. Kyseessä on tietojenkalastelu, jonka pääasiallinen tarkoitus on varastaa käyttäjän luottokortti- tai pankkitiedot. Virheellisestä kielestä päätellen näiden urkintaviestien takana on ollut ulkomaisia huijareita. (Verohallinto 2018.)

3.8 Kiristykset

Kiristyshaittaohjelma (ransomware) on haittaohjelma, joka salakirjoittaa tietokoneen tiedostot tai lukitsee koko laitteen ja vaatii rahaa lukkojen avaamiseksi. Lunnasvaatimukset esitetään usein virtuaalivaluuttana. Haittaohjelma tarttuu yleensä sähköpostin vahingollisen liitetiedoston välityksellä. Tartunnan voi saada myös lataamalla joltakin epämääräiseltä sivustolta löytyvä ohjelma tai klikkaamalla haitallista linkkiä. Kaikki verkkoon kytketyt järjestelmät voivat saada haittaohjelmatartunnan. (Viestintävirasto 2016, 2.)

Yritykset ja organisaatiot ovat kiristyshaittaohjelmien levittäjille kiinnostava kohde. Niillä on yksityisiä enemmän rahallista arvoa ja joissain tapauksissa niiden infrastruktuuri saattaa olla kriittinen. Kiristyshaittaohjelma saattaa uhata pysäyttää jopa yrityksen koko toiminnan. Vuonna 2016 kalifornialaissairaala Hollywood Presbyterian Medical Center taipui maksamaan 17 000 dollarin lunnaat verkkorikollisille, jotka olivat onnistuneet lukitsemaan sen tietojärjestelmät ja estämään pääsyn esimerkiksi potilastietoihin. Sairaalan mukaan lunnaiden maksaminen oli nopein ja tehokkain keino saada järjestelmät taas käyttöön. Yhdysvalloissa jopa paikallisten poliisilaitosten on kerrottu joutuneen taipumaan lunnaspyyntöihin saadakseen tiedostonsa takaisin. (Los Angeles Times 2016; Daily Mail 2015.)

Suomen poliisi kehottaa kiristyshaittaohjelman saaneita olemaan maksamatta lunnaita, sillä maksaminen tukee rikollisten toimintaa, osoittaa sen olevan kannattavaa ja kannustaa heitä jatkamaan. Maksaminen ei myöskään takaa sitä, että ongelma ratkeaa. Sen sijaan kiristyksiä vastaan voi suojautua tekemällä tärkeistä tiedostoista ja järjestelmistä säännöllisesti irralliset varmuuskopiot. Myös ohjelmistot tulisi päivittää säännöllisesti. (Poliisi 2017.)

Vuonna 2016 perustettu No More Ransom -kampanja pyrkii ennalta ehkäisemään kiristyshaittaohjelmien vahinkoja ja korjaamaan niitä. Europolin vetämässä kampanjassa tehdään yhteistyötä viranomaisten ja yritysten välillä. Kampanjasivustolla www.nomoreransom.org jaetaan tietoa kiristyshaittaohjelmista ja työkaluja ohjelmien purkamiseen. Sivustolta löytyy kryptauksen purkuohjelmia, joilla lukitut tiedot voi yrittää avata. Sivusto toimii myös suomeksi. (Poliisi 2017; No More Ransom 2019.)

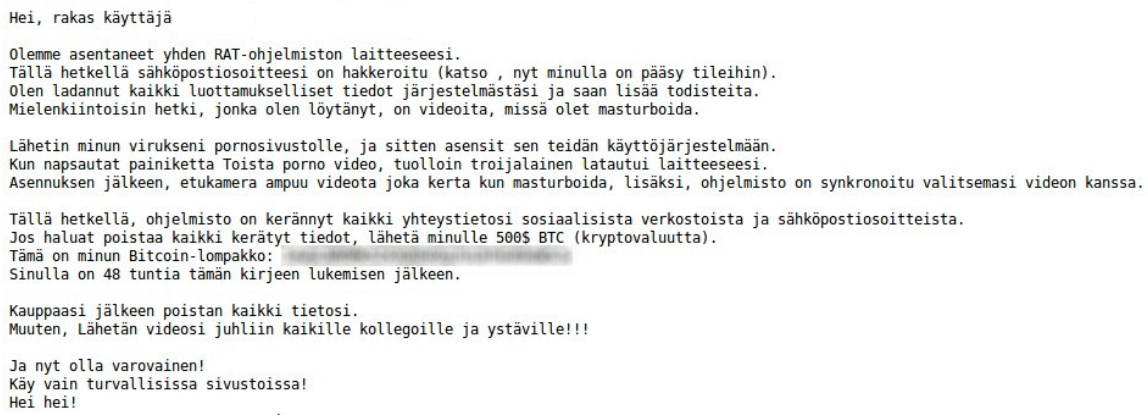
Sextortion

Vakuutusyhtiö Beazley varoitti helmikuussa 2019, että sextortion-kiristys on kasvava ilmiö yrityksissä. Kyberrikolliset yrittävät kiristää kryptovaluuttaa uhreiltaan väittämällä saaneensa kiusallista näyttöä aikuisverkkosivustojen käytöstä työtietokoneilla. (Beazley 2019.)

Tyypillisissä sextortion-tapauksissa kiristyksen uhrit ovat saaneet sähköpostia, jossa väitetään, että heidän työtietokoneidensa sisältöön on päästy käsiksi ja, että sieltä on löydetty todisteita pornografisten internetsivujen selailusta. Rikolliset väittävät kuvanneensa uhria web-kameralla, kun tämä on vieraillut näillä sivustoilla ja uhkaavat jakaa nauhoitteet uhrin sähköpostikontakteille, mikäli heidän vaatimuksiinsa ei suostuta. (Beazley 2019.)

Kiristyssähköpostit ovat usein sisältäneet linkin tai zip-tiedoston, joiden väitetään sisältävän todisteet kyseenalaisesta toiminnasta. Näitä klikkaamalla uhri saattaa kuitenkin saada koneellensa haittaohjelman, jolla voidaan varastaa tietoja tai lukita uhrin tietokone. Joissakin tapauksissa uhkauksen uskottavuutta on parannettu sisällyttämällä viestiin vanha uhrin sähköpostin salasana. Huijarit voivat ostaa näitä tietoja internetin pimeiltä sivustoilta, joilla hakkerit myyvät niitä eteenpäin. Vaikuttaisi siltä, että näissä tapauksissa kiristysten kohteet ovat olleet täysin satunnaisia. Huijarit olettavat, että tuhansista lähetetyistä kiristysviesteistä muutamat saattavat osua arkaan paikkaan ja johtaa haluttuun tulokseen. (Beazley 2019.)

Suomalaisetkin yrittäjät ovat saaneet sähköpostiviestejä, joissa yllä kuvaillun taktiikan mukaisesti yritetään kiristää kryptovaluuttaa (kuva 7). Huijausviestit on käännetty kömpelösti suomeksi ja niissä väitetään, että hakkeri on murtautunut vastaanottajan sähköpostiin ja saanut luottamuksellisia tietoja haltuunsa. Kiristäjä uhkaa lähettää arkaluontoista videomateriaalia kaikille uhrin kollegoille ja ystäville, jos tämä ei maksa pyydettyä summaa. (Suomen Yrittäjät 2018f.)



Kuva 7. Suomenkielinen sextortion-viesti (Traficom 2018b)

3.9 Domain-huijaukset

Verkkotunnus eli niin sanottu domain-nimi on yrityksen verkkoidentiteetti ja tärkeä osa sen brändiä. Verkkotunnuksia voi rekisteröidä eri ylätason verkkotunnuksien, kuten .fi, .com tai .net alle. Suomalaisia fi-päätteisiä osoitteita hallinnoiva organisaatio on Liikenne- ja viestintävirasto Traficom. Verkkotunnuksia voi rekisteröidä lähes kuka tahansa, joka täyttää operoinnista vastaavan organisaation käyttöehdot. Käytännössä rekisteröinti tapahtuu jonkin verkkotunnusvälittäjän kautta. Välittäjiä on erilaisia ja niiden hinnoittelut vaihtelevat. (Kyberturvallisuuskeskus 2019b.)

Verkkotunnusten rekisteröintiin ja uusimiseen liittyvää harhaanjohtavaa markkinointia ja huijauksia on tehty vuosien ajan. Yrityksiä on lähestytty sekä puhelimitse että sähköpostitse. Vilpillinen toimija saattaa esimerkiksi rekisteröidä tai väittää rekisteröivänsä verkkotunnuksia ja myydä niitä eteenpäin alkuperäiselle omistajalle ylihintaan tai jopa kiristää väärinkäytöksillä uhkaamalla. (Kyberturvallisuuskeskus 2019b, Tivi 2019.)

Domain-huijari saattaa väittää valheellisesti vastaanottaneensa rekisteröintipyynnön verkkotunnuksesta, joka on päätettä lukuun ottamatta identtinen yrityksen verkkotunnuksen kanssa. Esimerkiksi, jos yrityksen verkkotunnus olisi kallenkauppa.fi, voisi välittäjä väittää saaneensa rekisteröintipyynnön osoitteelle kallenkauppa.info. Huijari voi kertoa tarjoavansa etuoikeutta rekisteröimiseen ja painottaa rekisteröimättä jättämisen kauaskantoisia seurauksia. Näin yritystä painostetaan rekisteröimään osoite pikaisesti. Todellisuudessa mitään kilpailevaa rekisteröintipyyntöä ei ole tehty. Lisäksi toimijan tarjoama hinta rekisteröinnille saattaa olla moninkertainen keskimääräisiin hintoihin verrattuna. (Tivi 2019.)

Alkuvuodesta 2019 varoiteltiin sähköposteista, joilla DNS Finland -niminen taho markkinoi verkkotunnusten rekisteröintiä edellä mainitulla tavalla. Toimija pyytää rekisteröinnistä

reippaasti ylihintaa ja vaatii kerralla kymmenen vuoden rekisteröintiä varten kymmenkertaista summaa, kun rekisteröinti tavallisesti uusitaan vuosittain. Suomen kaupparekisteristä ei löydy DNS Finland -nimistä yritystä, vaikka se ilmoittaa kotisivuillaan osoitteekseen Bulevardi 21 Helsingissä. (Tivi 2019.)

DNS Finlandin toiminta näyttää olevan ulkomailta johdettua ja lukuisiin maihin ulottuvaa. Lähemmällä tarkastelulla sen internetsivustolta (www.dnsfinland.com) löytyy kieli- ja asiavirheitä. Samalla kaavalla tehtyjä eri kielisiä sivustoja löytyy myös nimillä DNS UK (www.dnsuk.org), DNS Ireland (www.dnsireland.org), DNS Benelux (www.dnsbenelux.com), DNS Spain (www.dnsspain.com) ja DNS Italy (www.dnsitaly.com). Näiden lisäksi ainakin European Trademarks & Domains (eutd.org), Internet Domain Services Austria (www.idsa.at) sekä EU Domains & Trademarks (eudt.be) vaikuttavat olevan samojen tekijöiden käsialaa. Edellä mainittujen verkkosivustojen rekisteröintitietoja tutkimalla saa selville, että kaikkien sivustojen jäljet johtavat Alankomaihin. Verkkosivuston rekisteröijäksi on merkitty joko nederlandsdomeinregister.nl tai Domeinnaam Register. Mitä todennäköisimmin kyse on yhdestä ja samasta alankomaalaistahosta.

Verkkotunnusten omistajia neuvotaan miettimään jo etukäteen mitä verkkotunnuspäätteitä heidän kannattaa hankkia. Erilaisia päätteitä on olemassa noin 1500, joten kaikkia on joka tapauksessa mahdotonta rekisteröidä. Puhelimitse tai sähköpostitse ehdotetut sopimukset kannattaa jättää huomiotta ja kääntyä sen sijaan hyvämaineisen verkkotunnusvälittäjän puoleen. Näin voi säästää pitkän pennin. (Tivi 2019.)

3.10 Lakimuutoksiin perustuvat huijaukset

Kun yhteiskunnassa tapahtuu suuria muutoksia tai lainsäädäntö muuttuu merkittävällä tavalla, on huijareilla oiva mahdollisuus käyttää yleistä epätietoutta ja tilanteen luomaa hämmennystä hyödykseen. Yrittäjät ovat tilanteessa huolestuneita oman yrityksensä jatkomahdollisuuksista ja mahdollisista seuraamuksista, jos uusia säädöksiä ei osatakaan noudattaa oikealla tavalla, joten he ovat erityisen alttiita ajautumaan huijausten uhriksi.

Mitä vieraampi tai etäisempi muutoksen alkusyy on, sitä enemmän siihen liittyy myös ennakkoluuloja ja epävarmuutta. Tämän vuoksi etenkin Euroopan unionin säädösmuutokset voivat olla erittäin hedelmällinen maaperä monenlaisille huijauksille. EU on yhä monille suomalaisille vieras. Vuonna 2016 tehdyn tutkimuksen mukaan 44 % EU-kansalaisista ei ymmärrä kuinka Euroopan unioni toimii (European Parliament 2016). Jos ei ymmärrä edes Euroopan unionin keskeisiä toimintaperiaatteita ja kokee EU-lainsäädännön jo lähtö-

kohtaisesti vaikeaselkoiseksi, on helppo uskoa monenlaisiin siihen liittyviin huijauksiin. Euroopan unionin direktiiveistä liikkuu mitä mielikuvituksellisempia tarinoita, joten voi olla vaikea hahmottaa mikä on totta ja minkä pitäisi saada hälytyskellot soimaan.

Myös erilaiset kriisi- tai katastrofitilanteet ovat hedelmällistä maaperää huijauksille. Yksityishenkilöitä sekä yrityksiä saatetaan kannustaa tekemään lahjoituksia. Tilanteet herättävät usein suuria tunteita ja avaavat ihmisten anteliaisuuden hanat. Lisäksi lahjoituksiin saattavat kannustaa hyvinkin arvovaltaiset tahot. Kaikki tämä on omiaan sumentamaan lahjoittajien harkintakykyä ja hätäisesti tehty lahjoitus saattaakin päätyä huijareiden tilille.

Kun huhtikuussa 2019 Pariisin Notre-Damea kohtasi tuhoisa tulipalo, presidentti Emmanuel Macron lupasi juhlallisesti, että katedraali rakennetaan uudelleen vain viidessä vuodessa. Lahjoituslupaukset nousivat yli 850 miljoonaan euroon vain kolmessa päivässä. Tilaisuus ansaita ei jäänyt huijareilta huomaamatta ja nopeasti mediassa varoiteltiinkin vääristä lahjoitussivustoista. (Le Monde 2019, Le Parisien 2019.) Yhdysvalloissa on tavanomaista, että työnantajat kannustavat työntekijöitä tekemään lahjoituksia katastrofitilanteissa ja lupaavat yrityksenä maksaa saman summan työntekijän valitsemalle hyväntekeväisyysjärjestölle. Tällaisissa tapauksissa myös yrityksen varoja voi päätyä hyväntekeväisyyshuijareiden käsiin. (Forbes 2015.)

GDPR-huijaukset

25.5.2018 alkaen sovellettu EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) on avannut uusia mahdollisuuksia huijauksiin. Huijarit käyttävät häikäilemättömästi hyväkseen yritysten tiedon puutetta ja epävarmuutta tietosuoja-asetukseen liittyvissä kysymyksissä sekä niiden pelkoa noudattamatta jättämisen seurauksista.

GDPR-asetus sääntelee sitä, kuinka ihmisten tunnistetietoja on säilytettävä ja käsiteltävä. Lisäksi sen mukaan yritysten on huolehdittava tietoturvansa riittävyydestä ja varauduttava mahdollisiin ongelmiin jo ennakolta. GDPR astui voimaan toukokuussa 2016, ja yrityksillä oli kahden vuoden siirtymäaika, jonka sisällä niiden piti saattaa tietojärjestelmänsä ja rekisterinsä tietosuoja-asetuksen vaatimalle tasolle. Tietosuoja-asetuksen puutteellisesta noudattamisesta voi saada pahimmillaan sakon, joka on 20 miljoonaa euroa tai 4 % yrityksen vuotuisesta liikevaihdosta. (Tivi 2018.) Näin suuren sakon uhka on omiaan lisäämään yrittäjien pelkoa ja epävarmuutta.

Suomen tietosuojavaltuutettu varoitti syksyllä 2018 Register of Commerce -nimisen organisaation nimissä lähetetyistä viesteistä, joissa pyydetään tarkistamaan tiedot EU:n tietosuoja-asetuksen mukaisesti. Viestit sisältävät lomakkeen, joka on esitäytetty vastaanottajan tiedoilla ja, joka pyydetään palauttamaan allekirjoitettuna. Kyseessä on kuitenkin huijaus, jolla allekirjoittaja saadaan lankeamaan lähes 1000 euron tilausansaan. (Tietosuojavaltuutetun toimisto 2018.)

Ranskassa monet pienyrittäjät ovat saaneet viralliselta vaikuttavia kirjeitä, joissa huomautetaan, ettei yrityksen toiminta ole EU:n tietosuoja-asetuksen mukaista ja muistutetaan rikkomuksesta määrättävästä seuraamusmaksusta. Kirjeessä kehotetaan yritystä korjaamaan asia puhelimitse. Kun asiaa tutkiva toimittaja ottaa yhteyttä kirjeen lähettäjään yrittäjän nimissä, häneltä pyydetään 793,20 euron rekisteröintimaksua. Maksulinkki lähetetään sähköpostitse ja maksu on tehtävä nopeasti, sillä linkki on voimassa vain 10 minuuttia. Henkilö puhelimen toisessa päässä väittää epämääräisesti edustavansa valtion toimistoa, joka on vastuussa GDPR:ään liittyvistä asioista. (Franceinfo 2019b.)

Brexit-huijaukset

Iso-Britannian ero EU:sta eli Brexit aiheuttaa epävarmuutta hyvin monella saralla pitkin Eurooppaa. Jatkuvasti vaihtuvat aikarajat ja eron epäselvät seuraukset ovat saaneet myös huijarit ottamaan kaiken irti suuresta muutoksesta. Brexitiin tavalla tai toisella liittyviä huijauksia on jo tässä vaiheessa ilmennyt lukuisia.

Iso-Britanniassa EU-maiden kanssa kauppaa käyviä yrityksiä on lähestytty verottajan nimissä ja pyydetty hankkimaan kaupankäyntinumero, joka oikeuttaa jatkossakin liiketoimintaan EU-alueella (Which 2019). Todellisuudessa kyse on huijauksesta, jolla pyritään kalastelemaan tietoja sekä saamaan rahaa kohteena olevilta yrityksiltä.

Brexit vaikuttaa myös rahaliikenteeseen EU:n ja Iso-Britannian välillä. Käytännössä vaikutus on luultavasti rahansiirtojen hidastuminen, mutta vaikutusten laajuutta ei voi vielä tietää tarkasti. Muutokset pankkiasioinnissa ovat huijareille erinomainen tilaisuus iskeä ja esiintyä pankin nimissä. Yrityksiä on jo ennakolta varoitettu tulevista mahdollisista huijauksista ja niitä on kehotettu olemaan erityisen valppaana tilanteissa, joissa yhteydenotto pankista tulee yllättäen ja, kun esimerkiksi puhelun aikana painostetaan tekemään nopeita päätöksiä. (Which 2019.)

Brexit-aiheisen virallisen näköisen sähköpostin välityksellä on levitetty myös troijalaista haittaohjelmaa, joka voi tallentaa arkaluonteisia tietoja, kuten käyttäjätunnuksia ja salasanoja. Sähköpostissa kehotetaan pysymään ajan tasalla Brexitin tilanteesta. Haittaohjelman on saanut koneelleen, jos on erehtynyt klikkaamaan sähköpostin Latest Brexit Update -nappia. (Latto 20.3.2019.)

Brexitiin liittyen huijataan myös Iso-Britannian ulkopuolella. Itävallassa on tavattu huijauksia, joissa esiinnytään brittiläisenä ostajana. Tuotteesta tehdään tilaus, joka pyydetään toimittamaan kiireellisesti, mutta sanotaan, että Brexitin vuoksi pankki perii lisämaksuja. Myyjä suostutellaan maksamaan lisämaksut sanomalla, että ostaja korvaa kulut korkoineen laskunmaksun yhteydessä. Mikäli myyjä lankeaa maksamaan pyydetyt lisämaksut ja lähettämään tilatun tuotteen, ei ostajaan enää saada yhteyttä. (Europakonsument 2019.)

Kun Brexit lopulta tapahtuu, aiheen ympärille syntyy luultavasti lukuisa määrä mitä mielikuvituksellisempia huijauksia, joihin ei ole vielä edes osattu varautua. Esimerkiksi Iso-Britanniassa tällä hetkellä asuvat ja yritystä pyörittävät henkilöt, joilla ei ole Iso-Britannian kansalaisuutta ovat varmasti otollinen joukko huijausten kohteeksi.

4 Huijausten vastainen toiminta Suomessa

Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset ovat yleensä kansallisia ilmiöitä, joten niiden torjumisessa on tärkeintä tiedottaminen ja viranomaisyhteistyö kansallisella tasolla (Rytkönen & Toivonen 6.3.2019). Vaikka Suomessa tehdäänkin jonkin verran viranomaisyhteistyötä, asiassa on vielä parannettavaa. Tässä luvussa tarkastellaan sitä, miten huijauksista tiedotetaan ja miten niitä pyritään torjumaan Suomessa.

Merkittävin tietolähde yrityshuijauksista Suomessa vaikuttaa olevan media. Suomen Yrittäjät tiedottavat ahkerasti huijauksista, mutta lisäksi iltapäivälehdet tarttuvat usein aiheeseen niin kuluttajapuolella kuin myös yrityksiinkin kohdistuvien huijausten osalta. Helena Tuorilan (1.4.2019) mukaan tärkeä syy tähän on se, että iltapäivälehdillä kynnys ottaa kantaa ja kertoa asiasta on matalampi kuin virallisilla tahoilla. Poliisi tai vaikkapa KKV tarvitsevat lehdistöä enemmän näyttöä huijauksesta, jotta he voivat kertoa asiasta.

On hyvä, että lehdistö tarttuu aiheeseen aktiivisesti, mutta toisaalta uutisointi voi olla toisinaan asenteellista ja shokeeraavaa, puhumattakaan netissä artikkelien alle ilmestyvistä lukijakommenteista. Tämä lisää uhrien kokemaa häpeää, mikä puolestaan vähentää uhrien halukkuutta kertoa huijauksista. Mikäli tiedottava taho olisi esimerkiksi poliisi, keskustelu voisi pysyä hieman asiallisempana.

Kuten aiemmin tuotiin esiin, poliisilla ei ole lainsäädännöllisistä syistä keinoja tarttua pienimpiin huijauksiin kovin tehokkaasti. Lievän petoksen yritys ei ole rangaistava teko, joten se ei johda rikostutkintaan. Yrittäjä ei voi tällä hetkellä lievän petoksen yrityksen kohdatessaan tehdä muuta kuin ilmoittaa asiasta esimerkiksi Suomen Yrittäjille. Lievän petoksen kohdallakaan poliisi ei välttämättä ole halukas toimimaan, koska näkee tapauksen sopimusriitana (Rytkönen & Toivonen 6.3.2019). Tällöin yrittäjälle ei jää muuta vaihtoehtoa kuin hyväksyä tulleensa huijatuksi. Tilanne on siis yrittäjille hankala, mutta suurin ongelma on kuitenkin siinä, että poliisin toimettomuus kannustaa huijareita jatkamaan toimintaansa.

4.1 Yhteistyöverkostot

Sekä Kilpailu- ja kuluttajaviraston että Suomen Yrittäjien edustajien kanssa käydyissä keskusteluissa yhdeksi merkittävimmistä työkaluista huijausten torjumisessa koettiin viranomaisten ja yksityisten tahojen välinen yhteistyö. Helena Tuorila KKV:ltä sekä Tiina Toivonen Suomen Yrittäjiltä pahoittelivat sitä, ettei Suomessa yhteistyö toimi riittävän hyvin eri tahojen välillä. Tieto ei kulje tai viimeistään yhteystyö loppuu siihen, että eri tahot haluavat jatkaa työtä omalla totutulla tavallaan sen sijaan, että yhdessä etsittäisiin toimintakeinoja,

jotka toimisivat kaikille. Valitettavaksi koettiin myös se, että muutokset eri virastojen, järjestöjen ja viranomaistahojen henkilökunnassa voivat osittain olla syynä siihen, ettei yhteistyö lähde ikinä kunnolla käyntiin. (Rytkönen & Toivonen 6.3. 2019; Tuorila 1.4.2019.)

Suomen Yrittäjät on edustettuna oikeusministeriön rikoksentorjuntaneuvostossa, jonka tehtäviin kuuluu ”suunnitella ja toteuttaa toimia rikollisuuden estämiseksi” (Rikoksentorjunta 2019b). Osana rikoksentorjuntaneuvoston toimia julkaistaan myös rikoksentorjuntakatsauksia. Vuoden 2017 rikoksentorjuntakatsauksen teemana on petosrikollisuus. Katsaus on melko laaja, mutta se keskittyy täysin kuluttajiin kohdistuviin petoksiin niin myyntipetoksien kuin identiteettivarkauksienkin kohdalla. (Tanttari & Alanko 2017.) Löydettyjen tietojen mukaan yrityksiin kohdistuvat huijaukset eivät ole olleet erityisesti esillä rikoksentorjuntaneuvostossa, vaikka muuta talousrikollisuutta siellä onkin käsitelty.

Vuonna 2013 julkaistun lehtiartikkelin mukaan (Y-lehti 2013) Suomen Yrittäjät olivat tuolloin kokoamassa verkostoa torjumaan yrityksiin kohdistuvia huijauksia. Verkoston jäseniksi mainitaan tietosuojavaltuutettu, poliisi, elinkeinoelämän järjestöjä sekä virastojen edustajia. Kun asia otettiin puheeksi haastattelussa (Rytkönen & Toivonen 6.3.2019), kävi ilmi, ettei tämäkään verkoston muodostaminen ollut edennyt alkua pidemmälle. Tämä tuntuu olevan valitettavan yleinen ongelma yrityksiin kohdistuviin huijauksiin tarttumisessa.

Monenlaisia yhteistyökuvioita on siis vireillä, mutta mikään niistä ei ole osoittautunut kovin hedelmälliseksi. Suomalainen ransomware.fi-sivu on esimerkki siitä, että julkisen ja yksityisen puolen toimijat voivat niin halutessaan tehdä myös yhteistyötä. Sivu on viestintäviraston kyberturvallisuuskeskuksen, poliisin ja F-Securen yhteistyössä laatima ja se keskittyy tiedottamaan ja antamaan neuvoja kiristyshaittaohjelmiin liittyvissä asioissa. (Ransomware.fi 2019.) Yrityksiin kohdistuvat huijaukset ovat aihe, jossa yksityisten ja julkisten toimijoiden yhteistyö olisi erityisen tärkeää, sillä huijaukset koskettavat koko yhteiskuntaa.

4.2 Suomen Yrittäjät

Suomessa merkittävin pienten ja keskisuurten yritysten avun lähde on Suomen Yrittäjät. Suomen Yrittäjät on Suomen suurin yrittäjien asioita ajava järjestö, jonka tavoitteena on tehdä Suomesta maailman paras maa yrittää. Suomen Yrittäjillä on noin 115 000 jäsenyritystä, joista 57 % on yksinyrittäjiä. Keskimäärin jäsenyrityksissä on 4–5 henkilöä. (Rytkönen & Toivonen 6.3.2019.) Suomessa on noin 285 000 yritystä (Suomen Yrittäjät 2019b), joten Suomen Yrittäjät tavoittaa niistä merkittävän osan. Lopuista yrityksistä osa kuuluu muihin yrittäjien etujärjestöihin, mutta on myös yrityksiä, jotka eivät kuulu mihinkään järjestöön.

Suomen Yrittäjät on aluejärjestöjensä kautta antanut jäsenilleen koulutusta huijausten tunnistamisessa. Lainsäädäntöasioiden päällikkö Tiina Toivonen on ollut pitämässä erilaisissa tapahtumissa alustuksia ja osallistunut huijausiltoihin asiantuntijana. Lisäksi Suomen Yrittäjät tiedottaa säännöllisesti aktiivisista huijauskampanjoista sosiaalisen median kanavissaan, uutiskirjeissään sekä omien internetsivujensa uutisosiossa. Asiantuntija Atte Rytkösen mukaan huijausaiheiset jutut ovat uutiskirjeissä kaikkein klikatuimpia, joten tästä voi päätellä aiheen kiinnostavan yrittäjiä todella paljon. Suomen Yrittäjät ei pidä kirjaa yrityksiin kohdistuvien huijausten tyypistä tai määrästä, mutta Rytkösen ja Toivosen tuntuma on, että yhä suurempi osa yrittäjiltä tulevista huijauksiin liittyvistä puheluista on ilmoituksia huijausyrityksistä avunpyyntöjen sijaan. (Rytkönen & Toivonen 6.3.2019.)

Haastattelussa 6. maaliskuuta 2019 Atte Rytkönen ja Tiina Toivonen toivat esiin painokkaasti, kuinka suuri merkitys järjestön tiedotus- ja avustustoiminnalla on ollut yrityshuijausten haittojen vähentämisessä. Hakemistohuijaukset ovat yksi yleisimmistä huijausmuodoista, mutta niiden määrä ja sen seurauksena myös niistä aiheutuneiden rahanmenetysten määrä on laskenut huippuvuosista. Aktiivisen tiedotustoiminnan ja medianäkyvyyden myötä myös aloittelevat yrittäjät ovat nykyään tietoisia hakemistohuijauksista ja lankeavat niihin harvemmin. Tämä on osoitus siitä, että huijauksista tiedottamisella on todella suuri merkitys ja vaikutus huijausten torjumisessa.

Vaikka järjestön pääasiallinen toimintatapa on vain antaa neuvoja yrityksille, Suomen Yrittäjät on myös ottanut aktiivisen roolin taistelussa huijariyrityksiä vastaan silloin, kun tapauksella on ollut erityisen suuri painoarvo. Esimerkki tällaisesta on Suomen Yrittäjien toiminta Directa-nimisen yrityksen tapauksessa.

Directa tarjosi yrityksille näkyvyyttä internetissä ja toimi Suomessa erityisen aktiivisesti vuosina 2008–2009. Yritys laskutti palvelustaan hakumäärien perusteella kiinteän summan sijaan. Yrityksen toiminnasta tehtiin yli 1400 rikosilmoitusta poliisille, mistä seurasi pitkiä, monipolvisia oikeudenkäyntejä. Lopulta Directa hävisi oikeudenkäynnit, mikä oli merkittävä voitto Suomen Yrittäjille ja suomalaisille yrityksille laajemminkin. (YLE 2016a.) Haastattelussa (Rytkönen & Toivonen 6.3.2019) tuli esiin, että Suomen Yrittäjien toiminta Directa-jutussa ja Directan saama tuomio ovat toimineet varoituksena myös muille huijariyrityksille.

4.3 Uusyrityskeskusten ja PRH:n rooli

Uusyrityskeskukset ympäri Suomen tarjoavat maksutonta yritysneuvontaa aloitteleville yrityksille. Suomen Uusyrityskeskukset ry on uusyrityskeskusten kattojärjestö, joka kannustaa yrittäjyyteen, julkaisee ilmaista perustamisopasta uusille yrittäjille sekä tiedottaa yrittäjyyteen liittyvistä uutisista ja tapahtumista. Kattojärjestön internetsivuilta löytyy paljon tietoa mm. yrityksen liikeidean keksimisestä, yritysmuodon valitsemisesta ja liiketoimintasuunnitelman laatimisesta. Missään ei kuitenkaan mainita yrityksiin kohdistuvia huijauksia, keinoja niiden välttämiseksi tai neuvoja huijauksen uhriksi joutuneelle. Myöskään perustamisoppaassa ei anneta tietoa huijauksista. (Uusyrityskeskus 2019.)

Sähköpostikeskustelu Suomen Uusyrityskeskukset ry:n verkosto- ja viestintäkoordinaattori Anna Laaksosen (22.3.2019) kanssa vahvisti havainnon, ettei kattojärjestön sivuilla tai sen julkaisemassa materiaalissa huomioida yrityksiin kohdistuvia huijauksia. Laaksonen koki puutoksen ongelmaksi ja kiitti keskustelun kautta saamastaan kehitysideasta.

Helsingin uusyrityskeskus, eli NewCo Helsinki tarjoaa konkreettista yritysneuvontaa aloitteleville yrittäjille Helsingissä. NewCo:ssa neuvotaan sekä ihmisiä, jotka vasta suunnittelevat yrityksen perustamista, että niitä, jotka ovat yrittäjyyden alkutaipaleella. Uusyrityskeskusten rooli huijausten torjumisessa on erittäin tärkeä, sillä uudet ja aloittelevat yrittäjät eivät välttämättä ole vielä esimerkiksi Suomen Yrittäjien tarjoaman avun piirissä.

Helsingin kaupungin yritysneuvonnan palvelupäällikkö Toivo Utso kertoi sähköpostitse, että yrityksiin kohdistuvat huijaukset ovat NewCo:ssa tuttu ilmiö. Aihe on esillä keskusteluissa uusien yrittäjien kanssa. NewCo ohjeistaa, ettei yrityksen puhelinnumeroa laiteta julkiseksi rekisteröinnin yhteydessä. Yrittäjiä ei koske puhelinmyynnin 14 vuorokauden perumisoikeus, joten yrittäjiä kehotetaan olemaan solmimatta minkäänlaisia sopimuksia puhelimitse ja jopa välttämään vastaamasta myöntävästi mihin tahansa kysymykseen, ellei ole täysin varma siitä, että tahtoo ostaa tarjotun palvelun (HS 2017, Utso 26.3.2019).

On olemassa myös puhelinhuijaustyyppi, jossa puhelunauhoitetta manipuloidaan jälkikäteen siten, että yrittäjä kuulostaa myöntyvän sopimukseen. Kyseisessä huijauksessa jokin yrittäjän myöntävä vastaus irrotetaan asiayhteydestään ja liitetään nauhoituksessa kohtaan, jossa yrittäjältä kysytään, tahtooko hän tilata tuotteen tai palvelun. Myöntäviä vastauksia välttämällä voi estää myös sellaiset tilanteet. (Suomen Yrittäjät 2017c.) Toivo Utson mukaan (26.3.2019) NewCo:ssa uusia yrittäjiä muistutetaan siitä, että sopimus on aina syytä pyytää nähtäväksi kirjallisena ennen kuin siihen myöntyy myös silloin, kun myynti ei tapahdu puhelimessa vaan muuten suullisesti.

NewCo:on tulee myös yhteydenottoja yrittäjiltä, jotka ovat jo joutuneet huijauksen uhriksi ja kaipaavat neuvoja. NewCo:lla ei ole resursseja auttaa yksittäisiä yrittäjiä. Yleinen ohje on, että yrittäjän pitää ottaa yhteyttä laskun lähettäneeseen tahoon ja pyrkiä selvittämään asia suoraan sen kanssa esimerkiksi kertomalla, ettei yrittäjä ole ymmärtänyt sopimuksen syntyneen. Mikäli yrittäjä kaipaa juridista apua, NewCo:sta ohjataan eteenpäin yhteistyölakimiehille, joilla ensimmäinen neuvonta on ainakin yleensä ilmainen. (Utso 26.3.2019.)

Etenkin maahanmuuttajataustaiset uudet yritykset ovat usein vaikeuksissa puhelinhuijareiden kanssa (Utso 26.3.2019). Maahanmuuttajataustaisille yrittäjille ei välttämättä ole täysin selvää, mikä on suomalainen toimintatapa ja mihin palveluihin rekisteröityminen tai niiden ostaminen on yrittäjälle Suomessa pakollista tai vähintäänkin yleistä ja suotavaa. Lisäksi moni maahanmuuttajataustainen voi olla kielitaidoltaan heikommassa asemassa, joten puhelimessa huijatuksi tulemisen riski on senkin takia korkea.

Patentti- ja rekisterihallitus, eli PRH ylläpitää kaupparekisteriä suomalaisista yrityksistä. Kun yritys perustetaan, pitää PRH:lle ilmoittaa mm. yrityksen yhteystiedot. PRH:n internetsivuilla kerrotaan ohjeena, että yritykselle pitää ilmoittaa kaupparekisteriin ainakin käynti- tai postiosoite, minkä lisäksi halutessaan voi ilmoittaa julkiseksi myös sähköpostiosoitteen, puhelinnumeron sekä verkkosivujen osoitteen. (PRH 2018.) Vaikka puhelin- ja sähköpostitiedot ovat vapaaehtoisia, moni yrittäjä varmasti lisää ne julkiseen rekisteriin ajattelematta asiaa sen tarkemmin. Yrittäjät eivät välttämättä tiedä, mihin kaikkeen tietoja voi käyttää.

Iso osa esimerkiksi hakemistohuijareista saa tietonsa uusista yrityksistä massahakuna Patentti- ja rekisterihallituksen kautta YTJ-tietopalveluista. Tietojen luovuttamisen estäminen tai rajoittaminen olisi tehokas keino torjua ja vähentää huijausten määriä, mutta se ei ole mahdollista, sillä rekisterin tiedot ovat julkisia. (HS 2017.) Käytännössä ainoa keino, jolla yrittäjä voi itse vaikuttaa tietojensa päätymiseen hakemistohuijareille, on jättää puhelinnumero- ja sähköpostitietonsa ilmoittamatta kaupparekisteriin.

Asia tuli esiin myös Suomen Yrittäjien haastattelussa. Haastattelussa (Rytkönen & Toivonen 6.3.2019) Tiina Toivonen mainitsi, että Patentti- ja rekisterihallitus saa tuloja yritysten yhteystietojen myynnistä. Tietenkään PRH ei suosittele rekisteröiviä yrityksiä jättämään laittamatta puhelinnumeroaan julkiseksi, koska tällöin yritystietojen myynnistä saadut tulot melko varmasti putoaisivat. PRH:lla voisi kuitenkin olla merkittävä rooli huijausten vähentämisessä kertomalla selvemmin, ettei puhelinnumero- ja sähköpostitietoja tarvitse tai välttämättä edes kannata lisätä rekisteriin.

5 Huijausten vastainen toiminta ulkomailla

Huijaustoiminta on usein valtioiden rajat ylittävää, joten kansainvälinen yhteistyö sen torjumiseksi on tarpeen. Tässä luvussa esitellään erilaisia kansainvälisiä yhteistyöhankkeita ja kerrotaan lisäksi joidenkin maiden erilaisista käytänteistä huijausten torjumisessa, joista Suomi voisi ottaa oppia.

Kansainvälisellä tasolla tehdään yhteistyötä yrityksiin kohdistuvien huijausten ehkäisemiseksi monella taholla, mutta on hieman epäselvää, kuinka kattavaa tai tehokasta se on, sillä tiedon löytäminen on vaikeaa. Yksittäisiä iskuja rikollisrinkien pysäyttämiseksi tehdään toisinaan, mutta tärkeää olisi jatkuva yhteistyö ruohonjuuritasolla. Ruohonjuuritason yhteistyöstä ei kuitenkaan kirjoiteta paljoakaan. Mediassa yksittäiset suuret operaatiot ovat isolle yleisölle kiinnostavampia kuin säännöllinen tietojenvaihto viranomaisten välillä, ja toisaalta yhteistyötä koordinoivat ja tekevät tahot eivät kerro yksityiskohtaisesti toiminnastaan. Huijausongelma ei ole vähentynyt vuosien varrella, vaan kuten edellä on kerrottu, kaikenlaisten huijausten määrä on lisääntynyt vuosi vuodelta. Se on nähtävissä muun muassa toimitusjohtajahuijausten rajusta kasvusta (FBI 2018a). Kasvu on osaltaan osoitus siitä, ettei yhteistyö ole ollut kovin hedelmällistä. Toimivan yhteistyön puute ei kuitenkaan ole ainoa huijausten määrän kasvua selittävä tekijä. Teknologian muutokset ja huijausten siirtyminen suurelta osin internetiin on mahdollistanut sen, että huijarit pystyvät tehtailemaan huijauksia helposti ja suurina massoina (Tuorila 1.4.2019).

Etenkin suuret ja näyttävät yrityksiin kohdistuvat huijaukset ovat maiden rajat ylittävää toimintaa. Isoimmat huijausringit ovat usein monen maan kansalaisista koostuvia, ja niihin puututaankin tehokkaammin kuin pienempiä summia huijaaviin. Vuonna 2018 FBI-johtoinen Operation Wire Wire johti 74 rikollisen pidättämiseen kuudessa eri maassa. Kyse oli toimitusjohtajahuijauksiin keskittyneistä huijareista, ja operaation yhteydessä huijareiden hallusta löydettiin lähes 2,5 miljoonaa Yhdysvaltain dollaria. Samalla saatiin estettyä yli 14 miljoonan dollarin rahasiirrot, jotka olivat parhaillaan käynnissä. (DOJ 2018.)

Myös pienempiä summia huijaavat yritykset, kuten hakemistohuijari European Business Number ja erilaiset domain-huijauksiin keskittyneet yritykset toimivat useassa maassa, mikä vaikeuttaa osaltaan niiden epärehellisen toiminnan kitkemistä. Euroopan unionin alueellakaan lainsäädäntö ei ole vielä tarpeeksi yhtenäinen huijariyritysten toiminnan estämiseksi. Esimerkiksi Itä-Euroopassa ilmapiiri on ollut huijauksille huomattavasti Länsi-Eurooppaa suopeampi ja niitä on voinut harrastaa jopa täysin laillisena bisneksenä, varsinkin jos rahan lähteenä ovat varakkaammat länsimaalaiset. Monet Suomessa esiintyvät huijaukset ovatkin peräisin Virosta, missä laki on joustavampi huijareille. (Tuorila 1.4.2019.)

5.1 Euroopan unioni

Euroopan unionilla on monia keinoja tarttua huijaustoimintaan. Erilaisten jäsenmaiden välisten yhteistyöhankkeiden ja lainsäädäntöä ohjaavien direktiivien lisäksi EU:n alaisuudessa toimii lainvalvontayhteistyövirasto Europol.

Europol ja Euroopan pankkiyhdistys EBF käynnistivät lokakuussa 2018 nettihuijauksiin keskittyvän viikon mittaisen kampanjan. Suomesta siihen osallistuivat Finanssiala ry, Suomen poliisi ja Viestintäviraston kyberturvallisuuskeskus. Kampanjan aikana pyrittiin jakamaan laajalti tietoa nettihuijauksista pääasiassa sosiaalisen median kanavissa. Sitä varten laadittiin lyhyitä ja ytimekkäitä infomateriaaleja 27:llä kielellä seitsemästä yleisimmästä nettihuijauksesta. Niissä kuvailtiin muun muassa kuinka toimivat tietojenkalasteluviestit, toimitusjohtajahuijaukset, huijaussivustot ja huijauslaskut. (Europol 2018; Viestintävirasto 2018b.) Europol on myös julkaissut eri kielillä oppaita toimitusjohtajahuijausten välttämiseksi.

Saksan keskusrikospoliisi eli Bundeskriminalamt kertoo YouTube-kanavallaan tekevänsä yhteistyötä Euroopan unionin, Europolin ja muiden kansainvälisten tahojen kanssa toimitusjohtajahuijausten torjumiseksi, mutta videolla ei tarkemmin kerrota millaista yhteistyö on ja ketkä kaikki yhteistyöverkostoon kuuluvat. Toimitusjohtajahuijaukset ja muut yrityksiin kohdistuvat huijaukset mainitaan videolla tärkeäksi yhteistyökohteeksi eri toimijoiden välillä. (BKA 2017).

Vuonna 2012 Euroopan komissio esitteli toimia, joilla ryhdyttäisiin hillitsemään etenkin hakemistohuijauksia EU-alueella seuraavan vuoden aikana (Euroopan komissio 2012). Kysyttäessä Suomen Yrittäjien Tiina Toivonen (Rytkönen & Toivonen 6.3.2019) muisti kyllä itsekin osallistuneensa Euroopan komission selvityksen tekemiseen, mutta ei ole kokenut, että asia olisi enää sen jälkeen ollut esillä.

Maaliskuussa 2019 Euroopan unionin neuvosto hyväksyi direktiivin, jolla pyritään torjumaan muihin maksuvälineisiin kuin käteisrahaan liittyviä petoksia ja väärennöksiä. Tällä direktiivillä tuodaan EU:n lainsäädäntö nykyaikaan, sillä aiemmassa lainsäädännössä esimerkiksi verkkomaksamista ja muuta digitaalisen valuutan käyttämistä koskevat säädökset ovat olleet vanhentuneita. (Maksuvälinedirektiivi (EU) 2019/713.)

Yrityksiin kohdistuvien huijausten osalta on olennaista, että direktiivissä velvoitetaan jäsenmaat jatkossa ylläpitämään palvelua, jossa huijauksen uhriksi joutuneet luonnolliset henkilöt ja oikeushenkilöt voivat tehdä ilmoituksen kokemastaan huijauksesta. Palvelussa

pitää myös olla kootusti tarjolla tietoa siitä, miten voi estyä huijauksen uhriksi joutumiselta sekä mahdollisuus saada apua. Jäsenmaiden pitää järjestää kampanjoita yleisen tietoisuuden lisäämiseksi huijauksista. Direktiivissä velvoitetaan jäsenmaat myös parantamaan yhteistyötä ja tietojenvaihtoa petosrikollisuuden vähentämiseksi. Direktiivin myötä kaikki jäsenmaat alkavat kerätä tietoa huijauksista ja niiden uhrien määrästä. (Maksuvälinedirektiivi (EU) 2019/713; Euroopan unionin neuvosto 2019.) Tietoa keräämällä saadaan tarkempi kuva siitä, millaisten ongelmien kanssa kuluttajat ja yrittäjät painivat.

Euroopan parlamentti ja Euroopan unionin neuvosto hyväksyivät direktiivin 20.3.2019 ja se julkaistiin Euroopan unionin virallisessa lehdessä 10.5.2019. Direktiivi astuu siis voimaan 30.5.2019, minkä jälkeen jäsenmailla on kaksi vuotta aikaa muokata omaa lainsäädäntöään niin, että se on yhdenmukainen direktiivissä määriteltyjen asioiden osalta ja alkaa toteuttaa sen asettamia vaatimuksia käytännössä.

5.2 Kilpailuvirastot

Suomessa kuluttajansuojalaki ei suojele yrityksiä millään tavalla, minkä vuoksi erityisesti mikro- ja yksinyrittäjien asema on kaupankäynnissä heikko. Kuten luvussa 2 kerrottiin, kuluttajansuojalaki ei suojele yrityksiä, sillä yritys ei oikeushenkilönä ole kuluttaja. Sen sijaan laki elinkeinonharjoittajien välisten sopimusehtojen sääntelystä (3.12.1993/1062), eli niin kutsuttu yrittäjänsuojalaki sääntelee kyllä sitä, minkälaisia sopimuksia yritykset voivat solmia keskenään. Sopimuksia tehdessä pitää lain mukaan ottaa huomioon myös heikomman sopijaosapuolen erityisasema. Lain ensimmäisessä pykälässä säädetään seuraavasti:

> Elinkeinonharjoittajien välisissä sopimuksissa ei saa käyttää ehtoa tai soveltaa käytäntöä, joka on sopimuksissa toisena osapuolena olevien elinkeinonharjoittajien kannalta kohtuuton ottaen huomioon toisena osapuolena olevien elinkeinonharjoittajien heikommasta asemasta johtuva suojan tarve ja muut asiaan vaikuttavat seikat.

Haastattelussa Kalle Määttä (11.4.2019) sanoi, ettei laki kuitenkaan toimi kovin hyvin.

Joissain maissa tätä erityisesti pieniä yrityksiä koskevaa ongelmaa on ratkaistu ulottamalla ainakin osa kuluttajille suunnatuista palveluista myös pienyrittäjien saataville. Käytännössä mikro- ja yksinyrittäjäthän ovat resursseiltaan kuluttajaan verrattavissa asemassa. Yksi maista, joissa pienyrittäjien asema on tietyin rajoituksin verrattavissa kuluttajaan, on Australia. Australian kilpailu ja kuluttajavirasto Australian Competition and Consumer Commission (ACCC) neuvoo kuluttajien lisäksi myös yrityksiä erilaisissa kiistatilanteissa.

5.3 Keskitetyt ilmoitussivustot

Joissain maissa on käytössä viranomaisten ylläpitämiä keskitettyjä ilmoitussivustoja tai -portaaleja, joissa sekä kuluttajat että yrittäjät voivat jättää ilmoituksia huijauksista sekä saada neuvoja siitä, miten tilanteessa tulee toimia. Sivustoilla myös ylläpidetään aktiivisia listoja käynnissä olevista huijauksista. Keskitetyt ilmoitussivustot palvelevat siis monipuolisesti sekä yksityisiä kuluttajia että yrittäjiä. Sivustojen edut eivät kuitenkaan rajoitu ainoastaan huijausten potentiaalisiin uhreihin.

Yksi erinomainen esimerkki keskitetystä ilmoitussivustosta on Iso-Britanniassa käytössä oleva Action Fraud (www.actionfraud.police.uk). Sivusto tarjoaa keskitetysti tietoa erilaisista huijauksista ja kyberrikollisuudesta sekä ohjeita siitä, kuinka välttyä niiltä. Lisäksi sivustolla julkaistaan uutisia ajankohtaisista huijauskampanjoista. Huijauksen tai kyberrikollisuuden uhri voi tehdä Action Fraudiin sähköisen ilmoituksen, josta se välitetään eteenpäin National Fraud Intelligence Bureau -poliisiyksikköön. Myös pelkästään yrityksen tasolle jääneistä kalastelusähköposteista kannustetaan ilmoittamaan. Vaikkei poliisilla olekaan resursseja tutkia jokaista ilmoitusta, auttavat ne lisäämään tietoa huijauksista, niiden tekijöistä ja uhreista, sekä antamaan tätä kautta työkaluja huijausten torjumiseen. Action Fraud tarjoaa apua myös puhelimitse.

Samalla periaatteella toimii Alankomaiden Fraud Help Desk -sivusto (www.fraudhelpdesk.nl). Myös se palvelee sekä yksityishenkilöitä että yrityksiä. Tiedottamisen, neuvonnan ja ilmoitusmahdollisuuden lisäksi Fraud Help Desk tarjoaa oikeudellista apua huokeaan hintaan yrityksille, joilla on riita-asia esimerkiksi hakemistopalveluun tai verkkotunnuksen rekisteröintiin liittyen.

Scamwatch (www.scamwatch.gov.au) on Australian kilpailu- ja kuluttajakomission (ACCC) ylläpitämä kuluttajille ja pienille yrityksille suunnattu palvelu, jonka tarkoituksena on auttaa tunnistamaan ja välttämään huijauksia. Huijauksista kannustetaan tekemään ilmoitus sivuston kautta. Tämän tarkoitus on ennen kaikkea auttaa ACCC:tä keräämään tilastotietoa huijauksista, seuraamaan suuntauksia ja ryhtymään tarvittaessa toimiin. ACCC julkaisee vuosittain raportin huijauksista. Toukokuussa 2018 julkaistun raportin mukaan vuonna 2017 Scamwatch vastaanotti yrityksiltä 5432 ilmoitusta huijauksista, joissa menetettiin noin 4,7 miljoonaa dollaria (ACCC 2018, 21).

Opinnäytetyötä tehdessä on käynyt selväksi, ettei Suomesta löydy kovinkaan tarkkaa tietoa etenkään yrityksiin kohdistuvista huijauksista. Niiden määrästä, laadusta ja niistä ai-

heutuvista rahallisista menetyksistä ja muista haitoista ei ole millään taholla kattavaa kokonaiskuvaa. Kuluttajahuijauksista löytyy hieman enemmän tietoa ja niiden vähentämiseksi ja välttämiseksi on tehty toimintasuunnitelmia, mutta vaikuttaa siltä, että yrittäjät on jätetty asian kanssa aika yksin.

Yksi keskitetyn ilmoitussivuston suurimmista eduista olisikin kerätä tietoa huijauksista. Kynnys rikosilmoituksen tekemiseen voi olla korkea etenkin, kun vaikuttaa siltä, ettei rikosilmoituksen tekeminen kovinkaan usein johda minkäänlaisiin toimiin. Sen vuoksi tiedon kerääminen huijauksista rikosilmoitusten perusteella ei vaikuta tehokkaalta keinolta. Ilmoituskynnys keskitetyllä sivustolla, jonka merkittävä tehtävä on kerätä tietoa ja varoittaa muita kuluttajia ja yrittäjiä huijauksista, on varmasti matalampi kuin virallisen rikosilmoituksen tekeminen. Näin keskitetyn sivuston avulla voisi saada paremman kokonaiskuvan yrittäjiin ja kuluttajiinkin kohdistuvien huijauksien todellisesta määrästä ja laadusta. Tietoja voisi sitten käyttää apuna esimerkiksi lainsäädäntöä ja muita toiminta- ja torjuntakeinoja suunnitellessa.

Haastattelussa (Rytkönen & Toivonen 6.3.2019) Suomen Yrittäjien Tiina Toivonen otti esiin, että rikosilmoitukset tehdään aina paikalliselle poliisilaitokselle, joita on Suomessa 11 kappaletta. Kun yhdestä huijarista tehdään ilmoituksia eri poliisilaitoksille, voi olla, että myös poliisille voi olla hankalaa hahmottaa, kuinka laajasta ilmiöstä kussakin huijaustapauksessa on kyse. Keskitetyn sivuston kautta kokonaiskuva huijauksen laajuudesta tulisi kenties paremmin selväksi.

Uudessa EU-direktiivissä (Maksuvälinedirektiivi (EU) 2019/713) on erityisen kiinnostava maininta siitä, että jäsenvaltioita olisi kannustettava perustamaan keskitetty kansallinen verkossa toimiva tiedottamisväline helpottamaan uhrien avun ja tuen saantia. Sen mukaan myös oikeushenkilöiden tulisi saada erityistä tietoa ja neuvontaa keinoista suojautua muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten kielteisiltä vaikutuksilta. Jäsenvaltioiden tulisi lisäksi ottaa käyttöön toimia petosten ja väärennysten ehkäisemiseksi tiedotus- ja valistuskampanjoiden avulla. Ehdotuksena on kehittää pysyvä verkossa toimiva väline, joka valistaisi petoskäytännöistä ajantasaisesti ja helposti ymmärrettävässä muodossa. Tämä väline voitaisiin yhdistää aikaisemmin mainittuun uhreille tarkoitettuun keskitettyyn tiedottamisvälineeseen.

5.4 Mustat listat

Esimerkiksi naapurimaassamme Ruotsissa yrittäjien etujärjestöt Förenade Bolag and Svensk Handel ylläpitävät mustaa listaa (varningslista) aktiivisista huijauksista ja yrityksistä, jotka toistuvasti huijaavat muita yrityksiä (Förenade Bolag 2019; Svensk Handel 2019a). Huijauksista kerrotaan mahdollisimman tarkat tiedot ja mukaan liitetään kuvia esimerkiksi valheellisista laskuista sekä huijariyrityksen Y-tunnus, osoite ja mahdolliset kytkökset aiempiin huijausyrityksiin. Suuri osa listalta löytyvistä huijaustiedoista koskee valheellisia laskuja, mutta myös muunlaisia huijausyrityksiä löytyy. Svensk Handel kertoo sivuillaan, että kaikenlainen hyvän markkinointitavan vastainen käyttäytyminen voi johtaa lisäämiseen listalle (Svensk Handel 2019b).

Svensk Handelin sivuilla kerrotaan kriteerit, joiden perusteella tiedot lisätään mustalle listalle. Listalle lisäämiseen riittää joissain tapauksissa yhdenkin kriteerin täyttyminen. Kriteerejä ovat esimerkiksi jäseniltä tulevien ilmoitusten suuri määrä, tarjouksen lähettäminen laskumuotoisena, perusteettomien laskujen lähettäminen, kokonaissumman puuttuminen tarjouksesta, yrityksen nimessä on suuri sekaannuksen vaara ja yrityksen osoite tai perustaja on sama kuin aiemmin mustalle listalle päätyneellä yrityksellä (Svensk Handel 2019b). Perusteita on siis todella monia, mutta suuri osa listalla olevista varoituksista koskee nimenomaan perusteettomia laskuja.

Förenade Bolag kannustaa listan yhteydessä yrittäjiä ottamaan välittömästi yhteyttä, jos he saavat esimerkiksi huijauslaskun, jotta huijauksesta saadaan tieto listalle ja sitä kautta voidaan varoittaa muita yrityksiä. Myös Svensk Handelin listan yhteydessä on lomake, jota kautta voi lähettää ilmoituksen kohtaamastaan huijauksesta. Molempien järjestöjen listat päivittyvät aktiivisesti useita kertoja kuukaudessa, ja lisäksi Svensk Handelin lista on saatavilla mobiilisovelluksena sekä Androidille että iPhonelle. Jokaisen listalla olevan tapauksen alla on mahdollisuus keskustella kyseisestä huijauksesta, ja monien tapausten alta löytyykin kommentteja, joissa kerrotaan omia kokemuksia huijauksesta. Listat ovat siis selvästi aktiivisessa käytössä ja ne koetaan myös etujärjestöjen puolella hyödyllisiksi työkaluiksi, koska tuskin siitä muuten olisi kehitetty jopa mobiilisovellusta.

Suomessa vastaaviin listoihin on kuitenkin suhtauduttu hieman vastahankaisesti eikä niitä koeta esimerkiksi Suomen Yrittäjissä erityisen hyödylliseksi ehkäisykeinoksi. Suomen Yrittäjien haastattelussa listan ylläpito miellettiin työlääksi ja juridisesti hankalaksi, sillä rehellisten yritysten päätyminen huijarilistalle aiheuttaisi yrityksille suurta haittaa. Suomen Yrit-

täjissä mustia listoja toimivammaksi keinoksi koetaan yrittäjien kouluttaminen ja kannustaminen pohtimaan, onko tarjottu tuote tai palvelu todella sellainen, mitä he kaipaavat. (Rytkönen & Toivonen 6.3.2019.)

Kilpailuasianneuvos Kalle Määtän (11.4.2019) mukaan mustat listat ovat erityisen ongelmallisia, jos niitä ylläpitää yksityinen taho. Yksityiselle taholle voi tulla houkutus lisätä listalle myös kilpailijoita tai pyrkiä muuten listan kautta vaikuttamaan kilpailutilanteeseen markkinoilla. Siksi listaa pitäisi ylläpitää viranomaisvoimin, mikäli mustat listat päätetään ottaa käyttöön. Määttä suhtautuu kuitenkin listoihin ”hyvin varauksella ja varoen” ja näkee niissä enemmän ongelmia kuin etuja. Toisaalta Kilpailu- ja kuluttajaviraston erikoistutkija Helena Tuorilan (1.4.2019) mielestä mustat listat voisivat olla hyödyllinen keino taistella huijareita vastaan ja ennen kaikkea tiedottaa yrittäjille meneillään olevista huijauskampanjoista. Suomessa ei siis edes juridiikan asiantuntijoilla ole täysin yhteneväistä linjaa mustista listoista.

Haastattelussa (Rytkönen & Toivonen 6.3.2019) Suomen Yrittäjien Atte Rytkönen toi esiin seikan, että kaikki huijaukselta näyttävä ja tuntuva ei ole huijaus, vaan ainoastaan ”bisnestä, johon ei kannata lähteä mukaan”. Esimerkiksi domain-huijaukset ovat tyyppi, jossa rajanveto on joskus vaikeaa. Niissä usein huijariyritykseksi koettu toimija ottaa kovan maksun palvelusta, jonka yrittäjä voisi tehdä itsekin joko ilmaiseksi tai vain murto-osalla kuluista. On vaikea sanoa, milloin tällaisessa tilanteessa on kyse huijauksesta ja harhaanjohtamisesta ja milloin yksinkertaisesti kalliista ostopalvelusta. Tämä on yksi esimerkki tilanteesta, jolloin mustan listan ylläpitäjä joutuu tekemään päätöksiä siitä, mikä on huijausta ja mikä ei. Jotta musta lista voisi toimia, pitäisi kenties ensin määritellä mikä tarkalleen ottaen on huijaus. Koska huijaus ei ole juridinen termi, ei lainsäädännöstä löydy kattavaa luetteloa siitä, mitä kaikkea huijaus voi olla.

Kalle Määtän (11.4.2019) mukaan verovelkarekisteri voisi olla yksi esikuva mustille listoille, mikäli Suomessa päätetään joskus alkaa ylläpitää mustia listoja vilpillisesti toimivista yrityksistä. Verovelkarekisteri on julkinen palvelu, josta voi tarkistaa yrityksen verovelat ja muut veroihin liittyvät laiminlyönnit. Mikäli yrityksellä on vähintään 10 000 euroa maksamattomia veroja, se lisätään rekisteriin. Tällöin muut yritykset voivat arvioida rekisterissä olevan yrityksen luotettavuutta kauppakumppanina. (Verohallinto 2017b.) Verovelkarekisterin kriteerit tulevat suoraan lainsäädännöstä, ja tämä olisi suotavaa myös mahdollisen mustan listan kohdalla. Lisäksi listan vaikutuksista pitäisi tehdä hyvin perusteellinen selvitys ennen sen käyttöönottoa. (Määttä 11.4.2019.)

Svensk Handelin turvallisuusasiantuntija Nina Jelverin (17.4.2019) antamien tietojen mukaan musta lista koetaan Ruotsissa erittäin hyödylliseksi ja sillä on rikoksia ehkäisevä vaikutus. Listan ylläpidosta vastaa yksi sitä varten palkattu henkilö, jonka työmäärä vaihtelee sen mukaan, kuinka paljon kulloinkin on liikkeellä esimerkiksi huijauslaskuja. Sekä Suomen Yrittäjien haastattelussa (Rytkönen & Toivonen 6.3.2019) että keskusteluissa Kalle Määtän (11.4.2019) ja Helena Tuorilan (1.4.2019) kanssa esiin nousi ongelma, että listalle joutuisi myös yrityksiä, joiden toiminta ei olisi millään tavalla vilpillistä. Jelverin mukaan myös Svensk Handel saa yhteydenottoja yrittäjiltä, jotka kokevat tulleensa lisätyksi mustalle listalle ilman syytä. Näissä tilanteissa listan ylläpitäjä kertoo syyt, jotka ovat johtaneet yrityksen lisäämiseen listalle. Yleensä silloin yrittäjä kertoo muuttavansa menettelytapojaan. Mikäli yritys todella tekee niin eikä Svensk Handel enää saa valituksia yrityksen toimintatavoista, yritys poistetaan mustalta listalta. Jelver ei sähköpostissaan kerro, että Svensk Handel olisi joutunut oikeustoimien kohteeksi listan takia.

Svensk Handelin ylläpitämälle mustalle listalle lähetetään vihjeitä vilpillisesti toimivista yrityksistä päivittäin, mutta kaikkia vihjeitä ei julkaista listalla. Listan ylläpitäjä tukeutuu julkaisupäätöstä tehdessään Svensk Handelin mustan listan yhteydessä ilmoittamiin kriteereihin. (Jelver 17.4.2019.) Koska vihjeitä kuitenkin lähetetään useita päivässä, on selvää, että myös ruotsalaiset yrittäjät kokevat palvelun hyödylliseksi ja ovat ottaneet sen aktiiviseen käyttöön.

Suomen Yrittäjillekin lähetetään ilmoituksia huijariyrityksistä, mutta määrä vaikuttaisi olevan pienempi kuin Ruotsissa. Atte Rytkösen mukaan Suomen Yrittäjien neuvontapalveluun tulee ilmoituksia keskimäärin viikoittain. Määrä vaihtelee vuoden aikana siten, että joskus aktiivisista huijauksista saattaa tulla useampi ilmoitus päivässä, mutta toisinaan taas ilmoituksia tehdään harvemmin. (Rytkönen 23.4.2019.)

5.5 Vakuutusyhtiöt

Vakuutusyhtiöillä voi olla kasvava rooli yrityksiin kohdistuvien huijausten torjunnassa. Suomessa on yrityksille toistaiseksi tarjolla melko niukasti vakuutuksia, jotka kattavat huijauksista koituvat vahingot. Vakuutustuotteita on lähinnä tietoturvauhkien ja identiteettivarkauksien varalle. Ulkomaisissa vakuutusyhtiöissä yrityksiin kohdistuvien huijausten riskit on otettu paremmin huomioon. Muun muassa Euler Hermes, joka esittelee itsensä Euroopan johtavana petosvakuutusyhtiönä, tarjoaa ainakin Ranskassa varsin kattavaa vakuutusturvaa yrityksille erilaisten huijausten varalle. (Euler Hermes 2019.)

Vakuutusyhtiöt tulevat todennäköisesti kehittelemään tulevina vuosina yhä enemmän vakuutustuotteita huijausten varalle. Sillä, että vakuutusyhtiöiden kiinnostus huijauksiin lisääntyy, on varmasti myönteinen vaikutus huijausten torjuntaan. Vakuutusyhtiöt voivat kiinnostuksellaan herätellä myös poliisia ja patistella sitä entistä aktiivisempaan ja tehokkaampaan rooliin asiassa.

Haastattelussa Helena Tuorila (1.4.2019) mainitsi, että vakuutuksilla voi olla myös kääntöpuolensa. Kun yrittäjä ottaa vakuutuksen huijauksien varalle, hän ei välttämättä enää ole arjessa yhtä varovainen, mikä voi johtaa yksinkertaisempienkin huijausten menemiseen läpi. Lisäksi Tuorilan selvityksessä *Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset* (2017, 30) tuodaan esiin, että vakuutuksen korvausmäärä voi myös rajoittaa sitä, minkälaista oikeudellista apua voi hankkia.

6 Pohdinta ja ehdotukset

Suomessa on vielä paljon tehtävää yrityksiin kohdistuvien huijausten torjumiseksi. On tullut hyvin selväksi, että tieto yrityksiin kohdistuvista huijauksista on hajallaan monien viranomaisten tai järjestöjen tietokannoissa. Koska huijaukset kuitenkin ovat merkittävä yhteiskunnallinen ongelma, olisi tärkeää saada kaikki tieto yhteen paikkaan, jotta piirtyisi selvä kuva siitä, missä yrityksiin kohdistuvien huijausten osalta mennään. Vain sillä tavalla voidaan selvittää, millaisia mahdollisia lakimuutoksia tai muita toimenpiteitä kenties tarvitaan. Tiina Toivonen kertoi haastattelussa (Rytkönen & Toivonen 6.3.2019), että Suomen Yrittäjät on järjestämässä tulevaisuudessa jäsenilleen kyselyä yrityksiin kohdistuvista huijauksista, jotta saadaan kattavampi kokonaiskuva tilanteen vakavuudesta.

Suomen lainsäädännön valossa vaikuttaa siltä, että riski vakavista seuraamuksista esimerkiksi hakemistopalveluhuijarille tai valelaskujen lähettäjälle on melko vähäinen. Koska lievän petoksen yritys ei ole rangaistava ja lievästä petoksesta tuomitaan ainoastaan sakkorangaistukseen, on huijariyritysten kannattavaa jatkaa toimintaansa.

Vuoden 2018 lopulla Tšekissä alettiin käsitellä oikeudessa hakemistopalveluhuijauksiin toistuvasti syyllistyvän yrityksen tapausta. Eräässä lehtihaastattelussa oikeusministeriön lehdistöedustaja Lucie Machálková kommentoi tapausta sanomalla, että oikeudenkäynnissä on syytä ottaa huomioon, että yritys toimii toistuvasti samalla epärehellisellä kaavalla. Vaikka yksittäiseen yrittäjään kohdistuvat summat eivät ole petoksen rajan ylittäviä, on kaikista huijauksista yhteensä muodostuva summa niin merkittävä, että asia on käsiteltävä vakavana rikoksena. (Business Info 2018.) Kenties Suomessakin voitaisiin useammin ottaa huomioon toistuvista rikoksista saatu kokonaissumma, vaikka yksittäisen huijaustapauksen suuruus jää lievän petoksen tasolle.

Uusyrityskeskuksilla ja Patentti- ja rekisterihallituksella on keskeinen rooli uusien yritysten tavoittamisessa. Aloitteleville yrittäjille tai yrityksen perustamista harkitseville on tarjolla tietopaketteja, mutta niissä ei juurikaan käsitellä yrityksiin kohdistuvia huijauksia. NewCo Helsingiltä saatujen tietojen mukaan hakemistopalveluhuijauksista kyllä varoitetaan ja opastetaan, miten välttää huijaukseen lankeaminen, mutta neuvominen tapahtuu kahdenkeskisessä tapaamisessa. Voisi olla hyödyllistä jakaa kaikille uusille yrittäjille tietoa ainakin yleisimmistä huijaustyypeistä. Tietopaketissa pitäisi löytyä tyypillisimpien tapausten kuvauksien lisäksi myös tietoa siitä, minkä tahon puoleen yrittäjä voi kääntyä apua tarvitessaan. Erityisen tärkeää olisi muistuttaa siitä, ettei laskuja ikinä pidä maksaa ihan vain varmuuden vuoksi. Samassa yhteydessä olisi myös luontevaa muistuttaa perintälaista ja siitä, ettei riitautetun laskun perintää voi jatkaa eikä sen takia voi menettää luottotietoja.

Uutta yritystä perustaessa olisi myös tärkeää löytää helposti tieto siitä, ettei kaupparekisteriin ole välttämätöntä ilmoittaa puhelinnumeroa. Jättämällä puhelinnumeron ilmoittamatta rekisteriin voi välttyä monilta hakemistopalveluhuijauksilta. Hakemistopalveluhuijaukset ovat yleisin huijaustyyppi, ja huijauksista suuri osa tapahtuu puhelimitse. Esimerkiksi uusyrityskeskukset ja muut tahot, jotka neuvovat yrityksen perustamisessa voivat ottaa tässä merkittävää roolia. Patentti- ja rekisterihallitus tuskin haluaa kertoa uusille yrittäjille, ettei puhelinnumeroa kannata ilmoittaa kaupparekisteriin. PRH voisi kuitenkin yrityksen rekisteröinnin yhteydessä kertoa selkeästi, mihin tarkoituksiin yrityksen yhteystietoja voidaan käyttää.

Viranomaisten välisen yhteistyön parantaminen tuli esiin haastatteluissa sekä Kilpailu- ja kuluttajaviraston Helena Tuorilan että Suomen Yrittäjien Tiina Toivosen ja Atte Rytkösen kanssa useamman kerran. Ainoastaan puuttumalla huijausongelmaan monella saralla yhtä aikaa voidaan saada tuntuvia muutoksia aikaan. Tulevan EU-direktiivin pitäisi tuoda tilanteeseen ainakin hieman helpotusta, sillä direktiivissä vaaditaan jäsenmaita tehostamaan viranomaisten välistä tietojenvaihtoa ja yhteistyötä. Kuitenkaan pelkkä tietojen vaihtaminen tai muu yhteistyö ei riitä, mikäli myös yhteiskunnan asenne ei muutu samalla. Huijauksiin on suhtauduttava vakavana ongelmana, mitä ne ovatkin. Niin kauan kuin yrittäjät jättävät huijaukset ilmoittamatta poliisille sen takia, että he kokevat poliisin vähättelevän ongelmaa, ei huijareita voida myöskään saada vastuuseen tekemisistään.

Naapurimaassamme Ruotsissa mustat listat, joilla varoitetaan lainvastaisesti ja harhaanjohtavasti toimivista yrityksistä, ovat ahkerassa käytössä. Yrittäjät selvästi etsivät sieltä tietoa ja saavat listojen kautta vihiä aktiivisista huijauksista jo ennen kuin ne osuvat omalle kohdalle. Listojen ylläpitäjät taas kokevat ne tärkeäksi osaksi rikoksentorjuntatyötä, kuten Nina Jelver (17.4.2019) kertoi sähköpostitse. Suomessa vastaaviin listoihin suhtaudutaan epäilyksellä. Helena Tuorilan selvityksessä (2017, 33) kyselyyn vastanneet yrittäjät toivat hyvin selväsanaisesti esiin toivovansa vastaavaa listaa myös Suomeen, mistä voi päätellä, että ainakin osa yrittäjistä kokisi listan hyödylliseksi. Kenties Suomeen voisi alkaa kehittää viranomaisen ylläpitämää mustaa listaa esimerkiksi verovelkarekisterin malliin pohjaten, kuten Kalle Määttä (11.4.2019) hyvin varovaisesti ideoi.

Lainsäädännöllisillä keinoilla voidaan vaikuttaa siihen, että huijariyritysten toiminta tehdään mahdollisimman vaikeaksi ja heitä myös rangaistaan rikollisesta toiminnastaan. Tärkeintä yrityksiin kohdistuvien huijausten torjumisessa on kuitenkin se, että yrittäjillä on paljon tietoa huijauksista. Tietoa pitää olla helposti saatavilla siitä, minkälaisia huijauksia on olemassa, kuinka ne voi tunnistaa, kuinka niihin lankeamisen voi välttää ja mitä on tehtävissä, jos on joutunut huijauksen uhriksi. Huijausten tunnistaminen on olennaista myös

siksi, että se vähentää huijareiden saamia tuloja. Tiedon levittämiseksi pitää panostaa informaatiosivustoihin, joilta löytyy kätevästi yhdestä paikasta kaikki tarvittava tieto sen sijaan, että sitä pitää lähteä etsimään monelta eri taholta. Uuden EU-direktiivin myötä tiedon löytäminen helpottuu, kun informaatiosivustot tulevat pakollisiksi kaikissa EU-maissa. Suomessa voidaan ottaa mallia Alankomaiden, Australian ja Iso-Britannian palveluista, kun suunnitellaan keskitettyä sivustoa.

Erityisesti yksin- ja mikroyrittäjät hyötyisivät suuresti siitä, että he pääsisivät esimerkiksi Kilpailu- ja kuluttajaviraston avun piiriin Australian mallin mukaan. Yksinyrittäjän asema on hyvin hauras, ja keinot sekä resurssit toimia huijaukseen langettua ovat vähäiset. Helena Tuorila kertoi haastattelussaan, että Kilpailu- ja kuluttajavirastolla olisi jo nyt tietoa ja kykyä neuvoa myös huijauksen uhriksi joutuneita yrittäjäasiakkaita. Kuluttajaneuvojat tuntevat kentän hyvin, joten heidän osaamistaan voisi hyvin hyödyntää myös yrittäjien neuvomisessa. (Tuorila 1.4.2019). Tämä ei tällä hetkellä kuitenkaan ole mahdollista, sillä KKV:n tehtävät määritellään laissa, ja lain mukaan virasto ei saa palvella kuin kuluttaja-asiakkaita. Kalle Määtän mukaan vaadittava lakimuutos ei kuitenkaan olisi suuri. Jos tahtoa löytyy, lakimuutos voitaisiin saada aikaiseksi nopeastikin, kunhan asiasta vain saadaan ensin tehtyä selvitys. (Määttä 11.4.2019.) Myös kyseisen lakimuutoksen pohjana toimivan selvityksen kannalta kaikki tieto yrityksiin kohdistuvista huijauksista on hyvin oleellista – mutta tällä hetkellä sellaista ei kootusti löydy.

Ehdotukset yrityksille

Yrityksillä itsellään on luonnollisesti keskeinen rooli huijauksilta suojautumisessa. Ensimmäinen askel tässä on työntekijöiden kouluttaminen ja tietoisuuden lisääminen. Monissa huijaustavoissa käytetään hyväksi sosiaalista manipulointia ja tietojen kalastelua. Näissä menetelmissä työntekijät ovat huijareiden ensisijaisena kohteena. Parhainkaan tietoturvajärjestelmä ei voi tukkia aukkoa, jonka työntekijä voi saada aikaan lankeamalla huijareiden virittämään ansaan. Näin ollen on tärkeää, että työntekijät tuntevat vähintäänkin yleisimmät huijaustyypit ja niihin johtavat askeleet.

On myös tärkeää tunnustaa, ettei mikään organisaatio ole immuuni huijauksille. Ei ole lainkaan liioiteltua ohjeistaa työntekijöitä suhtautumaan epäluuloisesti lähes kaikkiin sähköposteihin ja varsinkin niiden sisältämiin linkkeihin ja liitetiedostoihin. Kouluttamisessa ei tulisi unohtaa sijaisia ja kesätyöntekijöitä, joiden kokemattomuutta monissa huijauksissa pyritään käyttämään hyväksi.

Toiseksi yrityksen tulisi kiinnittää huomiota riittävään tietoturvatasoon. Kattava virustorjunta, tietoturvaohjelmisto, ohjelmistojen päivitys ja säännöllinen tietojen varmuuskopiointi ovat kaikki keskeisiä asioita yrityksen tietoturvan kannalta. Työasioita hoidetaan paljon älypuhelimella, joten niidenkin tietoturva on tärkeä varmistaa.

Yksi tietoturvan peruspilareista on hyvä salasana. Suomen yleisimmät salasanat, joita ei ainakaan tulisi käyttää, ovat SALASANA, qwerty ja 123456. Hyvä salasana on riittävän pitkä ja monimutkainen ja se sisältää myös numeroita. Hyvä vinkki on käyttää Ä- ja Ö-kirjaimia sekä erikoismerkkejä, sillä murto-ohjelmien merkkivalikoimat koostuvat yleensä vain perusaakkosista. Hyvä salasana koostuu useista peräkkäisistä sanoista, kuten TässäOnHyväSalasana. Salasana tulisi myös vaihtaa säännöllisesti. (Peltomäki & Norppa 2015, 91.)

Monimutkaisien salasanojen muistaminen voi olla vaikeaa, joten houkutus käyttää yksinkertaisia on suuri. Monet tietoturvayhtiöt tarjoavat salasanojenhallintaohjelmia, jotka tallentavat yksittäiset salasanat eri palveluihin. (SecureThoughts 2019.) Toinen tehokas keino lisätä tietoturvatasoa on ottaa käyttöön kaksivaiheinen tunnistautuminen, jossa palveluihin pitää kirjautua salasanan lisäksi myös jonkin toisen tunnisteen avulla (Viestintävirasto 2017a).

Taloushallinnon prosessit ovat myös tärkeässä asemassa huijauksilta suojautumisessa. Maksukäytännöt tulisi olla vakiintuneita ja ne tulisi rakentaa niin, että maksuja on aina hyväksymässä useampi silmäpari. Myös kaikki maksutietojen muutokset, esimerkiksi, jos tavarantoimittaja ilmoittaa tilitietojen vaihtumisesta, tulisi aina varmistaa esimerkiksi puhelimitse vaihteen kautta. Suoritetuista maksuista olisi hyvä lähettää vahvistus. Huolellisesti laaditut prosessit suojaavat huijauksilta vain, jos niitä noudatetaan kurinomaisesti, tulipa eteen kuinka kiireellinen tai erikoisluonteinen tilanne tahansa.

Avoin ja mutkaton yrityskulttuuri sekä matala hierarkia ovat tekijöitä, jotka voivat suojata yrityksiä huijauksilta. Kun yrityksessä on matala kynnys koputtaa johtotason oveen, kyseenalaistaa asioita ja kertoa epäilyksistään, on huijauksen onnistuminen paljon epätodennäköisempää. Johtotason tulisi viestiä yrityksen työntekijöille, että on jopa aivan välttämätöntä kyseenalaistaa tavanomaisesta poikkeavat pyynnöt, tulivatpa ne kuinka korkealta tasolta tahansa.

7 Lopuksi

Opinnäytetyössä on tuotu esiin syitä, miksi yrityksiin kohdistuvat huijaukset ovat merkittävä yhteiskunnallinen ongelma sekä syvästi huijauksen uhriksi joutuvaa yrittäjää koskettava tragedia. Yrityksiin kohdistuvien huijausten torjuminen ja niiden vaikutusten vähentäminen on tärkeää, mutta valitettavan vaikeaa.

On selvää, että huijauksiin puuttumiseen tarvitaan poliittisia päätöksiä ja lakimuutoksia, jos halutaan saada tehokkaita tuloksia. Tämän vuoksi aihetta kannattaisi tutkia tarkemmin niin yhteiskuntatieteellisestä, psykologisesta kuin taloustieteellisestäkin näkökulmasta. Monitieteinen lähestymistapa tuottaa aiheesta paljon tietoa, jonka pohjalta ottaa asia käsittelyyn yhteiskunnallisessa keskustelussa. Muutoksia selvästi tarvitaan, mutta tällä hetkellä muutosten tekemisen tueksi tarvittavaa tietoa on Suomessa saatavilla vain vähän.

Opinnäytteen kirjoittamisen aikana hyväksyttiin EU-direktiivi, joka velvoittaa jäsenmaat toimiin osaltaan myös yrityksiin kohdistuvien huijausten aiheuttamien ongelmien vähentämiseksi. Kun EU-direktiivin myötä Suomessakin otetaan käyttöön keskitetty palvelu, joka tarjoaa tietoa huijauksista ja mahdollisuuden ilmoittaa niistä, kertyy sitä kautta myös vihdoin tietoa huijausongelman yleisyydestä. Tuore direktiivi osoittaa hyvin, kuinka ajankohtaisesta asiasta opinnäytetyön aihepiirissä on kyse.

Opinnäytetyö valaisee myös sitä, kuinka merkittävässä roolissa yrityksen työntekijät ovat huijausten estämisessä. Tietoa pitää jakaa avoimesti ja sen pitää olla helposti löydettävissä. Assistenteilla on yrityksissä usein erityinen näköalapaikka eri osastoille ja moniin prosesseihin ja he voisivat sen myötä olla merkittävässä roolissa huijausten torjumisessa. Kirjoittajien erityisenä toiveena onkin, että tämä opinnäytetyö toimisi kimmokkeena ja inspiraationa myös johdon assistenttityön ja kielten koulutusohjelman sisältömuutoksia pohdittaessa. Jotta tulevat assistentit voivat toimia yrityksissä aktiivisesti huijausten torjumisessa, on aiheesta puhuttava jo opintojen aikana. Aihe sopii hyvin myös muiden koulutusohjelmien kursseilla käsiteltäväksi. Ovathan huijausten tunnistaminen ja välttäminen osa keskeistä liiketoimintaosaamista.

Valmis opinnäytetyö on kattava katsaus erilaisiin yrityksiin kohdistuviin huijauksiin sekä keinoihin torjua niitä. Lisäarvoa työlle tuo myös kansainvälinen näkökulma, joka kattaa suuren osan Eurooppaa, Pohjois-Amerikan ja Australian. Työn toteuttaminen parityönä oli keskeinen syy siihen, että aihetta voitiin käsitellä näin laajasti ja monipuolisesti. Toimeksi-

antajan pyyntö kansainvälisestä näkökulmasta täyttyi erinomaisesti, kun kirjoittajat pystyivät käyttämään lähteitä ja tapauskuvauksia monista maista useilla kielillä. Yksilötyönä toteutettuna opinnäytetyön sisältö olisi jäänyt huomattavasti suppeammaksi.

7.1 Opinnäytetyöprosessi

Opinnäytetyö valmistui melko ripeällä aikataululla kevään 2019 aikana. Ensimmäinen yhteydenotto Kilpailu- ja kuluttajavirastoon mahdollisen opinnäytetyöaiheen löytämiseksi oli joulukuussa 2018, mutta varsinainen tiedonhaku ja kirjoitustyö alkoivat helmikuussa 2019. Yleensä opinnäytetyö kirjoitetaan työharjoittelun aikana löydetystä aiheesta, jolloin asiaa on aikaa pohtia ja sulatella ennen varsinaisen kirjoitusprosessin alkamista. Tämän työn aihe löytyi aiemman kontaktin kautta, ja projekti saatiin käyntiin hieman nopeammin kuin yleensä.

Alusta saakka opinnäytetyön aikataulu haluttiin pitää tavoitteellisena. Ensimmäinen välitavoite oli, että puolet työstä on kirjoitettu maaliskuun puolivälissä. Toinen välitavoite oli, että ensimmäinen versio koko työstä valmistuu huhtikuun loppuun mennessä, jolloin toukokuussa jää vielä aikaa työn viimeistelyyn. Aluksi pohdittiin, pitäisikö kirjoitustyölle asettaa jonkinlaisia viikkotavoitteita tai jakaa tarkemmin sitä, mihin aiheisiin kumpikin kirjoittaja perehtyy. Lopulta sellaista ei koettu tarpeelliseksi. Itse asetettu aikataulu piti hyvin, työ eteni tasaiseen tahtiin, eikä sen valmistumisesta muodostunut missään vaiheessa ongelmaa.

Koska opinnäytetyö toteutettiin parityönä, yhteistyö olisi voinut muodostua projektissa lisähaasteeksi. Työnjako kuitenkin sujui tekijöiden välillä ilman ongelmia, sillä yhteistyöstä oli kokemusta jo aiemmista projekteista. Tärkeäksi havaittiin tiivis yhteydenpito kirjoitusprosessin aikana, jotta kumpikin olisi aina selvillä siitä, mitä toinen oli tekemässä. Avain onnistumiseen oli myös molempien sitoutuminen suunniteltuun aikatauluun.

Lisäksi aihe oli erityisen innostava ja mukaansatempaava ja se osoittautui työn edetessä jopa aina vain mielenkiintoisemmaksi. Motivoiva aihe oli merkittävä syy sille, miksi työ valmistui tiiviissä aikataulussa: kiinnostavasta aiheesta oli mukava etsiä tietoa ja kirjoittaa. Parityön etuna oli myös se, että mielenkiintoisia löydöksiä ja aiheen synnyttämiä ajatuksia pystyi aina jakamaan kirjoituskumppanin kanssa.

Kaiken kaikkiaan opinnäytetyöprojekti oli erittäin antoisa sekä tuloksellinen. Aiheen ajankohtaisuus lisäsi entisestään työn mielekkyyttä. Oli erityisen palkitsevaa huomata, kuinka paljon konkreettisia oppeja projekti antoi työelämää ajatellen. Opinnäytetyöstä on todellista ja käytännöllistä hyötyä sekä sen kirjoittajille että lukijoille.

Lähteet

ACCC 2018. Targeting scams: report of the ACCC on scam activity 2017. Luettavissa: https://www.accc.gov.au/system/files/F1240_Targeting%20scams%20report.PDF. Luettu: 18.4.2019.

Agari 2019. Email security blog. New Trend Sees BEC Gangs Focus on Executives for Payroll Diversion Scams. Luettavissa: https://www.agari.com/email-security-blog/bec-gangs-payroll-scams/. Luettu: 11.3.2019.

APWG 2019. Anti-Phishing Working Group. Phishing Activity Trends Report, Q4 2018. Luettavissa: http://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf. Luettu: 13.3.2019.

Australian Government 2019. Information and Services. Money and TaxTax. ABN Australian Business Number. Luettavissa: https://www.australia.gov.au/information-and-services/money-and-tax/tax/abn-australian-business-number. Luettu: 19.3.2019.

Beazley 2019. Beazley breach insights - February 2019. Sextortion and the dark side of the web. Luettavissa: https://www.beazley.com/news/2019/beazley_breach_insights_february_2019.html. Luettu: 4.4.2019.

BKA 2017. Bundeskriminalamt. CEO-Fraud Bekämpfung: Nationale und internationale Zusammenarbeit. Luettavissa: https://www.youtube.com/watch?v=th0AHCfPlvo. Luettu: 14.4.2019.

Bhakta, R. & Harris, I.G. 2015. Semantic analysis of dialogs to detect social engineering attacks. Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing.

Business Info 2018. Podvodníci vytahují podnikatelům z kapes miliony, za falešné registrace firem i ochranných známek. Luettavissa: https://www.businessinfo.cz/cs/clanky/podvodnici-vytahuji-podnikatelum-z-kapes-miliony-za-falesne-registrace-firem-i-ochrannych-znamek-116371.html. Luettu: 27.4.2019.

Computer Weekly 2019. Almost half UK firms hit by phishing attacks. Luettavissa: https://www.computerweekly.com/news/252459363/Almost-half-UK-firms-hit-by-phishing-attacks?asrc=EM_EDA_109542311&utm_medium=EM&utm_source=EDA&utm_campaign=20190313_Almost%20half%20UK%20firms%20hit%20by%20phishing%20attacks. Luettu: 14.3.2019.

Daily Mail 2015. News. Small Massachusetts police department forced to pay $500 Bitcoin ransom after hackers held their computer system hostage. Luettavissa: https://www.dailymail.co.uk/news/article-3028318/Massachusetts-police-department-forced-pay-hackers-500-Bitcoin-ransom.html. Luettu: 5.4.2019.

DOJ 2018. The United States Department of Justice. Press release. 74 Arrested in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes. Luettavissa: https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals. Luettu: 19.4.2019.

EBN 2019. FAQ. Luettavissa: https://www.e-b-n.eu/faq.php. Luettu: 19.3.2019.

El Mundo Financiero 2018. Empresas. Alerta ante el fraude multimillonario del "European Business Number". Luettavissa: https://www.elmundofinanciero.com/noticia/74538/empresas/alerta-ante-el-fraude-multimillonario-del-european-business-number.html. Luettu: 18.3.2019.

EPO 2019. European Patent Office. Fee payments and refunds. Warning. WPTR. Luettavissa: http://documents.epo.org/projects/babylon/eponot.nsf/0/2D51FFC7D6B77A02C12579D4004E5A3F/$File/warning_invoice_wptr_en.pdf. Luettu: 30.4.2019.

Euler Hermes 2019. Assurance fraude. Luettavissa: https://www.eulerhermes.fr/assurance-fraude.html. Luettu: 29.4.2019.

Euroopan komissio 2012. Lehdistötiedote. Euroopan komissio vahvistaa yritysten suojaa markkinointihuijauksia vastaan. Luettavissa: http://europa.eu/rapid/press-release_IP-12-1264_fi.htm. Luettu: 6.4.2019.

Euroopan unionin neuvosto 2019. Lehdistötiedote. EU tiukensi sääntöjään muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten torjumiseksi. Luettavissa: https://www.consilium.europa.eu/fi/press/press-releases/2019/04/09/eu-puts-in-place-tighter-rules-to-fight-non-cash-payment-fraud/. Luettu: 27.4.2019.
Europakonsument 2019. Brexit: Abzocke mit Kleinanzeigen. Luettavissa: http://europakonsument.at/de/news/brexit-abzocke-mit-kleinanzeigen Luettu: 6.4.2019.

European Parliament 2016. News. Teaching about the EU: "44% of Europeans don't understand how the EU works". Luettavissa: http://www.europarl.europa.eu/news/en/headlines/society/20160408STO22170/teaching-about-the-eu-44-of-europeans-don-t-understand-how-the-eu-works. Luettu: 26.4.2019.

Europol 2018. Press release. Europol and the European Banking Federation launch awareness campaign on 7 most common online financial scams. Luettavissa: https://www.europol.europa.eu/newsroom/news/click-here-and-see-how-your-money-disappears-%E2%80%93-criminal-cyberscams-of-21st-century. Luettu: 18.4.2019.

FBI 2018a. Public Service Announcement. Business E-mail Compromise, The 12 Billion Dollar Scam. Luettavissa: https://www.ic3.gov/media/2018/180712.aspx#ref2. Luettu: 28.2.2019.

FBI 2018b. Field-offices. Phoenix. Press-release. FBI Tech Tuesday: Business Email Compromise (BEC)-Gift Card Fraud. Luettavissa: https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-business-email-compromise-bec-gift-card-fraud. Luettu: 11.3.2019.

FCA 2018. Financial Conduct Agency. Warnings. Publiczny Kapital Oszczednosci. Luettavissa: https://www.fca.org.uk/news/warnings/publiczny-kapital-oszczednosci-clone-fca-authorised-firm. Luettu: 29.3.2019.

Fischer, P., Lea, S. & Evans, K 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43, 2060–2072.

Forbes 2015. Charity Scams Put The 'Disaster' In Disaster Relief. Luettavissa: https://www.forbes.com/sites/causeintegration/2015/10/05/charity-scams-put-the-disaster-in-disaster-relief/#2effd608c6fa. Luettu: 27.5.2019.

Franceinfo 2019a. Faits-divers. Vidéo. Faux ministre, vrai escroc. Luettavissa: https://www.francetvinfo.fr/faits-divers/video-faux-ministre-vrai-escroc_3185417.html. Luettu: 29.3.2019.

Franceinfo 2019b. Données personnelles : "Mise en conformité RGPD", l'arnaque qui cible les petites entreprises. Luettavissa: https://mobile.francetvinfo.fr/replay-jt/france-2/20-heures/donnees-personnelles-larnaque-qui-cible-les-petites-entreprises_3208715.html#xtref=https://www.google.com/. Luettu: 11.3.2019.

Fraud Help Desk 2018. Alerts. Fresh fake forms from European Business Number. Luettavissa: https://www.fraudhelpdesk.org/alerts/fresh-fake-forms-european-business-number/. Luettu: 18.3.2019.

Freiermuth, M. R. 2011. Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. Discourse & Communication, 5, 2, s. 123–145. Luettavissa: https://doi.org/10.1177/1750481310395448. Luettu: 14.4.2019.

Förenade Bolag 2018. Varningslistan. European Business Number. Luettavissa: http://www.forenadebolag.se/varningslistan/european-business-number/. Luettu: 18.3.2019.

Förenade Bolag 2019. Varningslistan. Luettavissa: http://www.forenadebolag.se/varningslistan/. Luettu: 17.3.2019.

GRTU 2018. Malta Chamber of SMEs. ATTENTION! European Business Number. Luettavissa: http://www.grtu.eu/index.php/3624-attention-european-business-number#. Luettu: 18.3.2019.

Harmaa talous & talousrikollisuus 2018. Ilmiöt. Ammattimainen yritysten hyväksikäyttö. Ammattimainen yritysten hyväksikäyttö on petosrikollisuutta. Luettavissa: https://www.vero.fi/harmaa-talous-rikollisuus/ilmi%C3%B6t/ammattimainen-yritysten-hyv%C3%A4ksik%C3%A4ytt%C3%B6/. Luettu: 8.4.2019.

Harmaan talouden selvitysyksikkö 2014. Hakemistopalvelut poliisille tehdyissä tutkintapyynnöissä. Verohallinto. Luettavissa: https://www.vero.fi/contentassets/a7f35eeac5a74429aa2b57ede5e0a421/hakemistopalveluyritykset-poliisille-tehdyissa-tutkintapyynnoissa.pdf. Luettu: 6.4.2019.

HS 2017. Helsingin Sanomat. Yrittäjäksi ryhtyvä saa soittovyöryn puhelinmyyjiltä – Älä sano puhelun aikana kyllä mihinkään, ellet halua tilata, neuvoo asiantuntija. Luettavissa: https://www.hs.fi/ura/art-2000005178615.html. Luettu: 5.4.2019.

Information Age 2019. Phishing attacks hook almost half of UK firms. Luettavissa: https://www.information-age.com/phishing-attacks-hook-almost-half-of-uk-firms-123480666/. Luettu: 14.3.2019.

Jelver, N.17.4.2019. Turvallisuusasiantuntija (säkerhetsexpert). Svensk Handel. Sähköposti.

JFW 2018. Beware – European Business Number (EBN). Luettavissa: https://jfw.ie/beware-european-business-number-ebn/. Luettu: 18.3.2018.

Kaleva 2016. Kotimaa. Ainakin neljääkymmentä suomalaisyritystä saatiin petettyä toimitusjohtajahuijauksella. Luettavissa: https://www.kaleva.fi/uutiset/kotimaa/ainakin-neljaakymmenta-suomalaisyritysta-saatiin-petettya-toimitusjohtajahuijauksella/735861/. Luettu: 21.3.2019.

Keskuskauppakamari 2017. Yritysten rikosturvallisuus 2017: Riskit ja niiden hallinta. Keskuskauppakamari. Helsinki. Luettavissa: https://kauppakamari.fi/wp-content/uploads/2017/10/yritysten-rikosturvallisuus-2017web.pdf. Luettu: 20.3.2019.

KNF 2018. Komisja Nadzoru Finansowego. Komunikaty. Ostrzeżenie dotyczące podmiotu „Publiczny Kapitał Oszczędności” (wykorzystującego również nazwę „PKO Bank Warszawa”). Luettavissa: https://www.knf.gov.pl/o_nas/komunikaty?articleId=62420&p_id=18. Luettu: 29.3.2019.

KnowBe4 2019. Spear Phishing. Luettavissa: https://www.knowbe4.com/spear-phishing/. Luettu: 13.3.2019.

Koivumäki, E. & Häkkänen, P. 2018. Markkinointijuridiikka. Kauppakamari. Porvoo.

Kolster 2018. Ilmiöt. Harhaanjohtava markkinointi. Varo patentti- ja tavaramerkkialan huijauslaskuttajia. Luettavissa: https://www.kolster.fi/blog/varo-patentti-ja-tavaramerkkialan-huijauslaskuttajia. Luettu: 3.4.2019.

Kyberturvallisuuskeskus 2019a. Aktiivista kalastelua ja tietomurtoja. Luettavissa: https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/aktiivista-kalastelua-ja-tietomurtoja. Luettu: 26.4.2019.

Kyberturvallisuuskeskus 2019b. Verkkotunnuspäätteitä kaupataan .fi-verkkotunnuksen haltijoille aktiivisesti. Ajankohtaista. Tietoturva nyt. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkotunnuspaatteita-kaupataan-fi-verkkotunnuksen-haltijoille-aktiivisesti. Luettu: 13.4.2019.

Laaksonen, A. 22.3.2019. Verkosto- ja viestintäkoordinaattori. Suomen Uusyrityskeskukset ry. Sähköposti.

Los Angeles Times 2016. Business. Technology. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. Luettavissa: https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html. Luettu: 5.4.2019.

Lappi-Seppälä, T. 2009. RL 31 Luku. Ryöstö ja kiristys. Teoksessa Lappi-Seppälä, T., Hakamies, K., Koskinen, P., Majanen, M., Melander, S., Nuotio, K., Nuutila, A-M., Ojala, T. & Rautio I. Rikosoikeus, s. 851–870. WSOYPro. Helsinki.

Latto, N. 20.3.2019. Watch out for these “Brexit” scams. avast blog. Luettavissa: https://blog.avast.com/brexit-scam. Luettu: 29.4.2019.

Le Monde 2019. En trois jours, Notre-Dame a reçu plus de dons que les 10 plus grandes œuvres caritatives en un an. Luettavissa: https://www.lemonde.fr/les-decodeurs/article/2019/04/19/en-trois-jours-notre-dame-a-recu-plus-de-dons-que-les-dix-plus-grandes-uvres-caritatives-en-un-an_5452697_4355770.html. Luettu: 28.5.2019.

Le Parisien 2019. Notre-Dame : enquête ouverte pour «escroquerie» après des appels aux dons frauduleux. Luettavissa: http://www.leparisien.fr/faits-divers/notre-dame-une-enquete-ouverte-pour-escroquerie-apres-des-appels-aux-dons-frauduleux-19-04-2019-8056767.php. Luettu: 28.5.2019.

LoschelderLeisenberg 2018. Warnung vor Rechnungen der EuroMedi – European Medical Directory. Luettavissa: http://www.abofalle-anwalt.de/euromedi-european-medical-directory/. Luettu: 19.3.2019.

Maksuvälinedirektiivi. Euroopan parlamentin ja neuvoston direktiivi muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta ja neuvoston puitepäätöksen 2001/413/YOS korvaamisesta. (EU) 2019/713. EUVL L 123.

Mouton, F., Leenen, L. & Venter, H. S. 2016. Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209.

mySafety 2018. Lehdistötiedotteet. Pienten ja keskisuurten yritysten identiteettivarkaudet ovat kasvussa – nämä ovat tyypillisimmät varkaudet. Luettavissa: https://www.mysafety.fi/lehdistohuone/pienten-ja-keskisuurten-yritysten-identiteettivarkaudet-ovat-kasvussa. Luettu: 10.4.2019.

Määttä, K. 11.4.2019. Kilpailuasiainneuvos. Kilpailu- ja kuluttajavirasto. Haastattelu. Helsinki.

Nyteknik 2018. Vd-bedrägerierna ökar lavinartat – och blir allt smartare. Luettavissa: https://www.nyteknik.se/sakerhet/vd-bedragerierna-okar-lavinartat-och-blir-allt-smartare-6906582. Luettu: 28.2.2019.

No More Ransom 2019. Salauksen purkaminen. Luettavissa: https://www.nomoreransom.org/fi/decryption-tools.html. Luettu: 5.4.2019.

Nuutila, A-M & Majanen, M. 2009. RL 36 Luku. Petos ja muu epärehellisyys. Teoksessa Lappi-Seppälä, T., Hakamies, K., Koskinen, P., Majanen, M., Melander, S., Nuotio, K., Nuutila, A-M., Ojala, T. & Rautio I. Rikosoikeus, s. 973–1005. WSOYPro. Helsinki.

Peltomäki, J. & Norppa, K. 2015. Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Talentum. Helsinki.

PKO 2019. PKO Bank Polski. News. Fraud warning: Publiczny Kapital Oszczednosci. Luettavissa: https://www.pkobp.pl/pkobppl-en/news/general-news/fraud-warning-publiczny-kapital-oszczednosci/. Luettu: 29.3.2019.

Podnikajte 2018. Podnikatelia, pozor na nový druh podvodu cez falošných odberateľov. Luettavissa: https://www.podnikajte.sk/zahranicny-obchod/novy-druh-podvodu-falosni-odberatelia. Luettu: 10.4.2019.

Poliisi 2017. Tiedotteet > Kiristyshaittaohjelmista on tullut maailmanlaajuinen turvallisuusuhka. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/kiristyshaittaohjelmista_on_tullut_maailmanlaajuinen_turvallisuusuhka_58230. Luettu 5.4.2019.

Poliisi 2018. Helsingin poliisilaitos. Tiedotteet. Sähköpostin välityksellä tehtäviä toimitusjohtajapetoksia yritetään edelleen – yhdistyksiltä ja yrityksiltä on huijattu jopa kymmeniä tuhansia euroja. Luettavissa: https://www.poliisi.fi/helsinki/tiedotteet/1/0/sahkopostin_valityksella_tehtavia_toimitusjohtajapetoksia_yritetaan_edelleen_yhdistyksilta_ja_yrityksilta_on_huijattu_jopa_kymmenia_tuhansia_euroja_70167. Luettu: 21.3.2019.

Preidel, M. 4.12.2004. Esse est percipi. Das Weblog eines Grafikdesigners. Abzocke II, DAD Deutscher Adressdienst Luettavissa: https://www.qxm.de/leben/20041204-204100/abzocke-ii-dad-deutscher-adressdienst. Luettu: 19.3.2019.

PRH 2017. Uutiset 2017. Varoitus harhaanjohtavista, laskunnäköisistä tavaramerkkien tarjouskirjeistä Luettavissa: https://www.prh.fi/fi/uutislistaus/2017/P_13761.html. Luettu 3.4.2019.

PRH 2018. Patentti- ja rekisterihallitus. Taustatietoa ilmoittajalle. Yrityksen osoite- ja yhteystiedot. Luettavissa: https://www.prh.fi/fi/kaupparekisteri/useinkysytyt/yhteystiedot.html. Luettu: 1.4.2019.

PRH 2019. Kaupparekisteri. Välty huijauksilta. Näin suojaudut yrityskaappauksilta ja huijausilmoituksilta. Luettavissa: https://www.prh.fi/fi/kaupparekisteri/valty_huijauksilta.html. Luettu: 15.4.2019.

Proofpoint 2018. Security Awareness Training. Vishing Attacks: Who's Really on the Line? Luettavissa: https://www.proofpoint.com/us/security-awareness/post/vishing-attacks-whos-really-line. Luettu: 25.4.2019.

Ransomware.fi 2019. Look out for ransomware. Luettavissa: https://www.ransomware.fi/. Luettu: 25.4.2019.

Rikoksentorjunta 2019a. Kyberrikokset. Luettavissa: https://rikoksentorjunta.fi/kyberrikokset. Luettu: 28.4.2019.

Rikoksentorjunta 2019b. Rikoksentorjuntaneuvosto. Luettavissa: https://rikoksentorjunta.fi/rikoksentorjuntaneuvosto. Luettu: 5.4.2019.

Rikoslaki 19.12.1889/39

Rytkönen, A. asiantuntija & Toivonen T. lainsäädäntöasioiden päällikkö. 6.3.2019. Suomen Yrittäjät. Haastattelu. Helsinki.

Rytkönen, A. 23.4.2019. Asiantuntija. Suomen Yrittäjät. Sähköposti.

Salmivuori, R. 2016. Miljoonaperintö tarjolla: kuinka verkkopetos toimii. Myllylahti Oy. Espoo.

SecureThoughts 2019. Why Your Small Business Needs a Password Manager. Luettavissa: https://securethoughts.com/small-business-needs-password-manager/. Luettu: 30.4.2019.

Sjouwerman, S. 29.1.2019. Scam Of The Week: CEO Fraud bad guys are now bribing your users. Security Awareness Training Blog. Luettavissa: https://blog.knowbe4.com/bad-guys-now-bribing-users. Luettu: 11.3.2019.

Suomen Yrittäjät 2015. Uutiset. Euroopan laajuinen yrityshuijaus myös Suomessa – varo tätä kirjettä. Luettavissa: https://www.yrittajat.fi/uutiset/492244-euroopan-laajuinen-yritys-huijaus-myos-suomessa-varo-tata-kirjetta. Luettu: 18.3.2019.

Suomen Yrittäjät 2017a. Uusi valetarjouksen lähettäjä Uruguaysta – Yrittäjien lakimiehet neuvovat tarkkuuteen Luettavissa: https://www.yrittajat.fi/uutiset/549174-uusi-valetarjouksen-lahettaja-uruguaysta-yrittajien-lakimiehet-neuvovat-tarkkuuteen. Luettu: 26.4.2019.

Suomen Yrittäjät 2017b. Uutiset. Huijauskirjeitä liikkeellä – European Business Number on vedättänyt aiemminkin. Luettavissa: https://www.yrittajat.fi/uutiset/549034-huijauskirjeita-liikkeella-european-business-number-vedattanyt-aiemminkin. Luettu: 18.3.2019.

Suomen Yrittäjät 2017c. Uutiset. ”Can you hear me” -huijauspuhelu muuntaa muotoaan, älä vastaa kyllä. Luettavissa: https://www.yrittajat.fi/uutiset/555503-can-you-hear-me-huijauspuhelu-muuntaa-muotoaan-ala-vastaa-kylla. Luettu: 5.4.2019.

Suomen Yrittäjät 2018a. Uutiset. Yrittäjä sai neljä outoa ”kuten syksyllä on sovittu” -puhelua, sitten alkoi laskutulva – poliisi: ei rikosta. Luettavissa: https://www.yrittajat.fi/uutiset/592038-yrittaja-sai-nelja-outoa-kuten-syksylla-sovittu-puhelua-sitten-alkoi-laskutulva. Luettu: 28.3.2019.

Suomen Yrittäjät 2018b. Uutiset. Tallenne kertoo kaiken oleellisen: Näin luettelofirma yrittää vedättää yrittäjää Luettavissa: https://www.yrittajat.fi/uutiset/573295-tallenne-kertoo-kaiken-oleellisen-nain-luettelofirma-yrittaa-vedattaa-yrittajaa. Luettu: 19.3.2019.

Suomen Yrittäjät 2018c. Uutiset. Varoitus! Suomeen tulee taas läjäpäin EBN:n huijauskirjeitä. Luettavissa: https://www.yrittajat.fi/uutiset/566742-varoitus-suomeen-tulee-taas-lajapain-ebnn-huijauskirjeita. Luettu: 18.3.2019.

Suomen Yrittäjät 2018d. Uutiset. Uusi huijaus – Viestiin ei kannata reagoida millään tavalla. Luettavissa: https://www.yrittajat.fi/uutiset/571612-uusi-huijaus-viestiin-ei-kannata-reagoida-millaan-tavalla. Luettu: 26.4.2019.

Suomen Yrittäjät 2018e. Uutiset. Yrittäjä kertoo: Näin rikolliset yrittivät kaapata firmani. Luettavissa: https://www.yrittajat.fi/uutiset/569664-yrittaja-kertoo-nain-rikolliset-yrittivat-kaapata-firmani. Luettu: 15.4.2019.

Suomen Yrittäjät 2018f. Yrittäjiä koetetaan kiristää pornolla – kyseessä on täysi huijaus. Luettavissa: https://www.yrittajat.fi/uutiset/596193-yrittajia-koetetaan-kiristaa-pornolla-kyseessa-taysi-huijaus. Luettu: 24.4.2019.

Suomen Yrittäjät 2019a. Uutiset. Huijauskirjeiden lähettäjä EBN tarjoaa nyt ”sovintomaksua”. Luettavissa: https://www.yrittajat.fi/uutiset/603458-huijauskirjeiden-lahettaja-ebn-tarjoaa-nyt-sovintomaksua. Luettu: 18.3.2019.

Suomen Yrittäjät 2019b. Yrittäjyys Suomessa. Luettavissa: https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363. Luettu: 16.3.2019.

Svensk Handel 2019a. Varningslistan. Luettavissa: https://www.svenskhandel.se/sakerhetscenter/varningslistan/. Luettu: 17.3.2019.

Svensk Handel 2019b. Kriterier för publicering. Luettavissa: https://www.svenskhandel.se/sakerhetscenter/varningslistan/kriterier-for-publicering/?id=22535. Luettu: 17.3.2019.

Tahiti Infos 2019. Arnaque au Président : le témoignage du directeur de Jus de fruits de Moorea. Luettavissa: https://www.tahiti-infos.com/Arnaque-au-President-le-temoignage-du-directeur-de-Jus-de-fruits-de-Moorea_a180354.html. Luettu: 10.4.2019.

Tilastokeskus 2019. Tietoa tilastoista. Käsitteet. PK-yritys. Luettavissa: https://www.stat.fi/meta/kas/pk_yritys.html. Luettu: 28.4.2019.

Tanttari, S. & Alanko, M. Petosrikollisuus ja sen ehkäisy. Rikoksentorjuntakatsaus 2017. Oikeusministeriön julkaisuja 58/2017. Oikeusministeriö. Luettavissa: http://urn.fi/URN:ISBN:978-952-259-659-8. Luettu: 5.4.2019.

Tentativi 7.6.2005. Attenzione al Registro Italiano Internet. Luettavissa: http://tentativi.blogspot.com/2005/06/attenzione-al-registro-italiano.html. Luettu: 19.3.2019.

Tietosuojavaltuutetun toimisto 2018. Tietosuoja-asetukseen liittyviä tilaaja-ansaviestejä liikkeellä. Luettavissa: https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-asetukseen-liittyvia-tilaaja-ansaviesteja-liikkeella. Luettu: 11.3.2019.

Tivi 2018. Uutiset. Gdpr on täällä kohta, rikkoja voi saada jopa 20 miljoonan sakot – näin organisaatiot valmistautuvat asetukseen. Luettavissa: https://www.tivi.fi/uutiset/gdpr-on-taalla-kohta-rikkoja-voi-saada-jopa-20-miljoonan-sakot-nain-organisaatiot-valmistautuvat-asetukseen/d5bf6003-fd86-3263-becd-57553ff1bfe4. Luettu: 26.4.2019.

Tivi 2019. Uutiset. Klassikkohuijauksella nyhdetään rahaa suomalaisyrityksiltä: vipuun menneiden kannattaa ilmoittaa poliisille. Luettavissa: https://www.tivi.fi/uutiset/klassikko-huijauksella-nyhdetaan-rahaa-suomalaisyrityksilta-vipuun-menneiden-kannattaa-ilmoittaa-poliisille/d14f4b74-529f-37bb-a1ad-f5dc0734546a. Luettu: 13.4.2019.

Topmejt 2018a. Uwaga, oszuści w Wielkiej Brytanii podszywają się pod PKO BP. Luettavissa: https://topmejt.co.uk/uwaga-oszusci-w-wielkiej-brytanii-podszywaja-sie-pod-pko-bp/ Luettu: 28.3.2019.

Topmejt 2018b. Uwaga, przekręt! Oszuści podszywają się pod bank PKO. Luettavissa: https://topmejt.co.uk/uwaga-przekret-oszusci-podszywaja-sie-pod-bank-pko/. Luettu: 28.3.2019.

Traficom 2017. Liikenne- ja viestintävirasto. Kyberturvallisuus. Taltuta kyberhuijari! Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/03/ttn201703091241.html. Luettu: 13.3.2019.

Traficom 2018a. Liikenne- ja viestintävirasto. Kyberturvallisuus. Sähköpostitunnukset vaarassa – varo uutta turvapostiviestiksi naamioitunutta huijausta! Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/10/ttn201810041403.html. Luettu: 30.4.2019.

Traficom 2018b. Liikenne- ja viestintävirasto. Kyberturvallisuus. Tietoturva nyt! Pornokiristysuhkaus on pelkkä huijaus. Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/10/ttn201810020934.html. Luettu: 30.4.2019.

Tuorila, H. 2017. Kilpailu- ja kuluttajaviraston selvityksiä 2/2017. Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset. Luettavissa: https://www.kkv.fi/globalassets/kkv-suomi/julkaisut/selvitykset/2017/kkv-selvityksia-2-2017-pk-yrityksiin-kohdistuvat-huijaukset.pdf. Luettu: 28.2.2019.

Tuorila, H. 1.4.2019. Erikoisasiantuntija. Kilpailu- ja kuluttajavirasto. Haastattelu. Helsinki.

Tuorila, H., Määttä, K. & Peltonen A. 2016. Kilpailu- ja kuluttajaviraston selvityksiä 1/2016. Kuluttajahuijaukset. Luettavissa: https://www.kkv.fi/globalassets/kkv-suomi/julkaisut/selvitykset/2016/kkv-selvityksia-1-2016-kuluttajahuijaukset.pdf. Luettu: 28.2.2019.

Utso, T. 26.3.2019. Palvelupäällikkö. Helsingin kaupungin yritysneuvonta NewCo Helsinki. Sähköposti.

Uusyrityskeskus 2019. Luettavissa: https://www.uusyrityskeskus.fi/. Luettu: 30.3.2019.

Verohallinto 2017a. Yhteystiedot ja asiointi. Lomakkeet. Yritysasiakkaan ilmoitus tilinumerosta. Luettavissa: https://www.vero.fi/tietoa-verohallinnosta/yhteystiedot-ja-asiointi/lomakkeet/kuvaus/yritysasiakkaan_ilmoitus_tilinumerosta_/. Luettu: 3.4.2019.

Verohallinto 2017b. Verovelkarekisteri. Luettavissa: https://www.vero.fi/henkiloasiakkaat/maksaminen/maksuvaikeudet/verovelkarekisteri/. Luettu: 18.4.2019.

Verohallinto 2018. Tietoa huijausviesteistä. Luettavissa: https://www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/tietoa_verofisivustost/tietoa_huijausviesteist/. Luettu: 26.4.2019.

Viestintävirasto 2016. Selviytymisopas kiristys-haittaohjelmia vastaan. Kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen. Viestintäviraston julkaisu 005/2016 J. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf. Luettu: 5.4.2019.

Viestintävirasto 2017a. Kyberturvallisuus. Tietoturva nyt! Kaksivaiheinen tunnistautuminen pelastaa paljolta - pelkkä salasana ei suojaa kaikilta uhkilta. Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/08/ttn201708301327.html. Luettu: 29.4.2019.

Viestintävirasto 2017b. Näin meitä huijataan! Verkossa yleisesti tavattuja huijausmenetelmiä. Viestintävirasto. Kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Nain_meita_huijataan.pdf. Luettu: 21.3.2019.

Viestintävirasto 2018a. Kesäloma on laskuhuijarin sesonkiaikaa. Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/06/ttn201806131421.html. Luettu: 28.2.2019.

Viestintävirasto 2018b. Kyberturvallisuus. Tietoturva nyt! Europol kampanjoi: Suojaa itsesi ja rahasi nettihuijareilta. Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/10/ttn201810161521.html. Luettu: 18.4.2019.

Visão 2018. Actualidade. Sociedade. Se receber uma carta para atualizar o European Business Number tenha cuidado, pode estar a cair num logro. Luettavissa: http://visao.sapo.pt/actualidade/sociedade/2018-07-10-Se-receber-uma-carta-para-atualizar-o-European-Business-Number-tenha-cuidado-pode-estar-a-cair-num-logro. Luettu: 18.3.2019.

Which 2019. Which? Consumer rights. Brexit Scams. Luettavissa: https://www.which.co.uk/consumer-rights/advice/brexit-scams. Luettu: 6.4.2019.

YLE 2012. Directan johdon syytteet törkeästä petoksesta hylättiin. Luettavissa: https://yle.fi/uutiset/3-6180076. Luettu: 30.4.2019.

YLE 2016a. Pitkään eri oikeusasteissa puidulle Directa-tapaukselle päätös: KKO tuomitsi ex-toimitusjohtajan liiketoimintakieltoon. Luettavissa: https://yle.fi/uutiset/3-9343495. Luettu: 24.4.2019.

YLE 2016b. Talous. Nyt iskevät valetoimitusjohtajat – KRP kertoo pörssiyhtiöiden menettäneen miljoonia. Luettavissa: https://yle.fi/uutiset/3-8625155. Luettu: 21.3.2019.

YLE 2016c. Talous. Satojen suomalaisyritysten rahat vaarassa – verottaja paljasti mittavan alv-huijauksen. Luettavissa: https://yle.fi/uutiset/3-9254054. Luettu: 3.4.2019.

YLE 2017. "Toimitusjohtajahuijaukset" yrityksissä lisääntyneet – äkilliset rahansiirtopyynnöt tavallisia. Luettavissa: https://yle.fi/uutiset/3-9721473. Luettu: 28.2.2019.

Y-lehti 2013. Kiireinen yrittäjä on helppo huijattava. Luettavissa: https://www.y-lehti.fi/arkisto/artikkeli/4851/Kiireinen+yritt%C3%A4j%C3%A4+on+helppo+huijattava. Luettu: 5.4.2019.

Åberg, L. 2017. Rikoksen uhrin käsikirja. PS-Kustannus. Jyväskylä.