LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Digitalisaation vaikutukset verkkorikollisuuteen
Case: Tilausansat

Hietanen, Vesa

2017 Leppävaara

Digitalisaation vaikutukset verkkorikollisuuteen
Case: Tilausansat

Vesa Hietanen
Tulevaisuuden innovatiiviset
digitaaliset palvelut (YAMK)
Opinnäytetyö
Maaliskuu, 2018

Laurea-Ammattikorkeakoulu
Tulevaisuuden innovatiiviset digitaaliset palvelut
Tradenomi (YAMK)

Vesa Hietanen

Tiivistelmä

Digitalisaation vaikutukset verkkorikollisuuteen. Case: Tilausansat

Vuosi 2018 Sivumäärä 112

Opinnäytetyön tarkoituksena oli selvittää, kuinka digitalisaatio vaikuttaa verkkorikollisuuteen ja luo sinne mahdollisuuksia rikoksen tekemiselle, esimerkkinä tilausansat. Opinnäytetyön tarkoituksena oli tuottaa tietoa finanssialan yrityksille ja Keskusrikospoliisin rikostorjuntaan sekä dataa Poliisihallitukselle, jota he voivat käyttää sisäisessä tiedotuksessa. Opinnäytetyön tavoitteena oli luoda katsaus tilausansoihin ilmiönä ja antaa tietoa, kuinka kehittää omia järjestelmiä ja prosesseja tilausansoja vastaan.

Tietoperusta rakennettiin digitalisaatiosta, maksamisesta ja maksuvälineistä, lainsäädännöstä sekä rikollisuuden muuttumisesta digitalisaation aikana. Työn näkökulma perustui tapaustutkimus lähestymistapaan, jossa käytettiin kvalitatiivisia ja kvantitatiivisia menetelmiä. Opinnäytetyössä tehtiin suunnattu kyselytutkimus alan ammattilaisille, joilla oli kokemusta tilausansoista ja verkkorikollisuudesta. Tärkeimpänä kysymyksenä oli, mikä aiheuttaa tämän tilausansa ilmiön ja kuinka sitä vastaan tulisi taistella. Tutkimuksessa käytettiin aineistoa suoraan poliisin rikostilastoista, oikeusjärjestelmän rangaistustilastoja eri maksuvälinepetoksien kategorioissa sekä maksamiseen ja digitalisaatioon liittyviä tilastoja. Vastaajien ryhmä käsitti yhteensä 73 ihmistä, jotka koostuivat mm. lakimiehistä, syyttäjistä, poliiseista, riskiasiantuntijoista, korttiasiantuntijoista, luottopäälliköistä sekä tuoteasiantuntijoista.

Keskeisistä tuloksista kävi selkeästi ilmi, miksi tämä rikosilmiö oli kasvanut räjähdysmäisesti. Rikostorjunnan kehittämisessä poliisille halutaan paremmat työkalut esitutkintaan ja syyllisille rikossyytteet asiakasmanipuloinnista ja harhaanjohtamisesta. Tukea, tiedotusta ja valistusta tulee keskittää ihmisille, joiden digitalisaation taidot eivät ole valtaväestön tasolla.

Johtopäätöksinä esitettiin, että lainsäädäntöön tulisi saada muutoksia. Lainsäädäntöön pitäisi saada selkeä oikeuskäytäntöön perustuva rangaistavuus, jonka jälkeen tilausansoja tarjoavien yrityksien toiminta voitaisiin lopettaa. Viranomais-ja yksityissektorin tulisi miettiä yhteistyömuotoja tehostaakseen rikostorjuntaa. Suurelle osalle viranomaisista ja finanssialan edustajistakin oli epäselvää, minkälaisista rikoksista on kysymys.

Asiasanat: verkkorikollisuus, tilausansa, digitalisaatio, maksaminen, lainsäädäntö

Laurea University of Applied Sciences
Degree Programme in Innovative Digital Services of the Future
Master's Thesis

Vesa Hietanen

Abstract

The effects of digitalization on cybercrime. Case: Subscription traps

Year 2018 Pages 112

The purpose of the thesis was to find out how digitalization affects cybercrime and creates opportunities for crime, for example, subscription traps. The aim of the thesis was to provide information to financial companies, to the Finnish National Bureau of Investigation and to the Finnish National Police Board which they can use in internal information. The thesis aimed at creating an overview of subscription traps as a phenomenon, and to providing information on how to develop systems and processes against such traps.

The theoretical framework of this thesis was built on digitalization, payment and payment methods, legislation and changes in crime during digitalization. This thesis was based on a case study approach to qualitative and quantitative methods. In the thesis a survey was conducted to professionals who had experience in subscription traps and cybercrime. The most important questions were what creates subscription traps and how do we fight them. The study used material directly from police criminal records, statistics on the penalties of the judicial system in various categories of payment fraud, and statistics on payment and digitization. The group of respondents comprised of 73 people who were made up of lawyers, prosecutors, police officers, risk specialists, payment card specialists, credit managers and product specialists.

The key findings in this thesis showed clearly why the phenomenon of subscription traps has exploded exponentially. In the prevention of such traps, the police should have better tools and methods for pre-trial investigations and criminals should be charged or customer manipulation and misrepresentation. Support, awareness, and education should be focused on the individuals whose digitalization skills are not on a par with the majority.

In conclusion, the study suggested that legislative changes should be made. Legislation should have clear penalties based on legal practices through which the activities of the responsible parties behind these subscription traps can be shut down. The authorities and the private sector should consider forms of cooperation in order to enhance the prevention of such crime. Additionally, it was found out in the study that for a large number of authorities and financial representatives, it remained unclear what kind of crime subscription traps are.

Keywords: cybercrime, subscription traps, digitalization, phishing, payments, legislation

Sisällys

Lyhenteet

Cardaus	Anastetuilla maksukorttitiedoilla tehtäviä verkko-ostoja
TOR	The Onion Router
EU	Euroopan unioni
RIKITRIP	Poliisin tietokanta
Chargeback	Maksun palautus
Issuer	Maksukortteja myöntävät pankit ja rahoituslaitokset
Acquirer	Maksutapahtumien vastaanottaja ja tilittäjä
3D-secure	Standardi turvamekanismi maksukortti ostoksiin
CEMEA	Central Europe, Middle East and Africa
PSD2	Payment Service Directive 2
PSP	Maksupalveluntarjoajat
FinTech	Financial technology
Debit-kortti	Osto tai käteisnosto veloitetaan pankkitililtä
Credit-kortti	Osto tai käteisnosto veloitetaan korttiluotolta
URL-osoite	Uniform Resource Locator
ETL	Esitutkintalaki (22.7.2011/805)
RL	Rikoslaki (24.8.1990/769)
HetiL	Henkilötietolaki (22.4.1999/523)
PL	Perustuslaki (11.6.1999/731)
VPN	Virtual Private Network
PCI DSS-standardi	Payment Card Industry Data Security Standard
EMV-standardi	Europay – Mastercard - Visa
Bottiverkko	Maantieteellisesti hajanainen, osa saastuneiden koneiden verkostoa joka koostuu uhrikoneista
Skimmaus	Maksukortin kopioimista rikolliseen tarkoitukseen

1. Johdanto

Turvallinen toimintaympäristö on edellytys kaikelle yhteistyölle, tarkoitetaan sillä sitten yhteiskuntaa, perhettä tai tässä tapauksessa sähköistä maailmaa (Peltomäki & Norppa 2015, 10). Meistä jokainen toimii yhteiskunnassa eri tavalla ajatellen omaa turvallisuuttaan. Itse olen nähnyt vuosien varrella paljon erilaisia nettiin liittyviä petoksia ja huijauksia ja huomannut, kuinka me ihmiset olemme yhteiskunnassa eriarvoisessa asemassa, kun puhumme turvallisuudesta. Tämä korostuu erityisesti sähköisessä maailmassa.

Yrityselämä tuottaa kuluttajille uusia digitalisaation välineitä helpottamaan arkea ja esimerkiksi maksamista ja näin ollen tuottaa palveluilleen lisäarvoa. Verkossa asioiminen halutaan tehdä helpoksi, nopeaksi ja vaivattomaksi, mutta kuinka tärkeänä näissä palveluissa nähdään turvallisuus? Rikolliset oppivat myös hyvin nopeasti uuden teknologian ja yleensä sen, missä ovat rikollisuuden mentävät aukot ja mitä pystyy hyödyntämään rikosta tehdessä. Netti on yhä useammin rikoksessa käytetty apuväline, jota käytetään rikoksen suunnitteluun, tekoon tai rikoksella saadun hyödyn kätkemiseen. Monesti viranomaiset ja alan asiantuntijat tulevat ennalta ehkäisyssä muutaman askeleen jäljessä rikollisia ja pyrkivät selvittämään uusia rikoksen muotoja, kun niitä ilmestyy julkisuuteen.

Tilausansat ovat omien tutkimusteni mukaan alkaneet Suomessa vuonna 2011–2012 ja todennäköisesti samoihin aikoihin myös muualla Euroopassa. Caroline Theorellin (2017) tutkimuksen mukaan tilausansat ovat vuosien varrella aiheuttaneet paljon ongelmia kuluttajissa, finanssilaitoksissa sekä viranomaisissa. Tilausansat ovat tyypillisesti kokonaan nettimaailmassa tapahtuvaa rikollisuutta, joka on ns. rajat ylittävää rikollisuutta, jota pääsääntöisesti johdetaan Suomen rajojen ulkopuolelta. Tilausansa tarkoittaa sitä, että kuluttaja saa laskuja tuotteesta tai palvelusta, jota ei ole omasta mielestään tilannut. Tämä taas johtaa siihen, että kuluttajaa on tahallisesti erehdytetty, sillä kuluttaja ei saa mainoksesta tai viestistä todenmukaista kuvaa asiasta. Tässä rikollisuuden lajissa on myös harhaanjohtavaa markkinointia, jossa pääsääntöisesti mainostetaan ja markkinoidaan tuotetta tai palvelua, jota kuluttaja

kuitenkaan erittäin harvoin saa maksusta huolimatta. Sähköisessä maailmassa medialukutaito tarkoittaa sitä, kuinka vastaanottaja pystyy suodattamaan tietoa, arvioimaan tiedon laatua sekä sitä, millaisilla keinoilla kuluttajaan pyritään vaikuttamaan. Medialukutaitoa on myös taito ymmärtää, millaisia valintoja tietosisällössä on tehty, kuka tiedon on tuottanut ja mitä mahdollisesti jätetään kertomatta. (Kilpailu- ja Kuluttajavirasto 2016.)

Seuraavissa osioissa käydään läpi aihetta, tavoitetta ja käytettyjä tutkimusmenetelmiä. Tämän opinnäytetyön kannalta tärkeimmät valinnat tehtiin tutkimusmenetelmiin liittyvissä ratkaisuissa. Aiheesta ei ole aikaisemmin tehty suomenkielistä tukimusta, joten materiaalin olisi tarkoitus olla mahdollisimman kattava osoitus tilausansoihin liittyvästä rikollisuudesta. Tilausansoja on tutkinut kuluttajatutkimuksina muun muassa Caroline Theorell (2017) kuudessa eri Euroopan maassa, mutta tämän tutkimuksen tarkoituksena on selvittää alan ammattilaisten näkökulmasta, kuinka ilmiötä voisi rajoittaa tai saada lopetetuksi kokonaan.

2. Aiheen valinta ja tavoitteet

Tämän opinnäytetyön aiheeksi tuli tekijää erittäin suuresti kiinnostava digitalisaatio ja siinä erityisesti rikokset, jotka muuntautuvat nykyaikana sähköisessä maailmassa. Aihetta tarkastellaan erityisesti tilausansojen näkökulmasta ja niin, kuinka ne vaikuttavat kuluttajiin, rahoituslaitoksiin sekä viranomaisiin. Valintaan vaikutti suuresti oma kokemus, koska olen vuodesta 2011 alkaen toiminut kyseisten rikosten parissa, sekä kiinnostus selvittää rikoksien laajamittaista suunnitelmallisuutta sekä ammattimaisuutta.

Opinnäytetyön tarkoituksena on kartoittaa digitaalisessa maailmassa tapahtuvaa rikollisuutta ja erityisesti pureutua tilausansa-nimellä kulkeviin rikoksiin. Tavoitteena on luoda Poliisihallitukselle, Europolille sekä finanssialan toimijoille uutta tietoa rikoksen torjuntaan, kehitykseen sekä ennalta ehkäisyyn kyseisiä rikoksia vastaan. Kananen (2014, 52) kertoo, että tieteellisessä työssä pitää aina olla ongelma, jotta

tieteellinen tutkimus voidaan tehdä. Tutkimusaihe tulee fokusoida ja rajata, jotta tutkittavan ilmiön tiedonsaanti olisi mahdollista ja tutkimusaihe hallinnassa. Tutkimukseni tarkoitus oli saada käsitys niistä tekijöistä, jotka selittävät tilausansojen suuren määrän nettirikollisuudessa, ja siitä, miksi ihmiset niihin lankeavat. Asetin tutkimukselle seuraavat tutkimuskysymykset:

1. Mikä on suurin syy tilausansoihin liittyvän rikollisuuden suureen määrään?
2. Miten tilausansoihin liittyvää rikollisuutta voisi parhaiten ennaltaehkäistä?
3. Miten poliisi/pankki/maksupalveluiden tarjoaja voisi paremmin ennaltaehkäistä kyseisenlaista rikollisuutta?
4. Minkälaista yhteistyötä poliisin/pankin ja maksupalveluiden tarjoajan pitäisi tehdä tilausansoihin liittyen?

Opinnäytetyön tarkoitus on olla kokonaisuudessaan julkinen ja mahdollisesti olla käytettävissä kaikille, jotka ovat tekemisissä rikoksentorjunnan kanssa tai selvittämässä mainittuja petoksia ja rikoksia.

2.1 Rajaukset

Tässä työssä keskitytään maksuvälinepetoksien näkökulmasta rikoksen muotoihin, joita etenkin Suomessa pankit ovat tilastoineet jo useamman vuoden ajan. Työssä ei anneta suoraa ohjeistusta, kuinka ennalta ehkäisevä toiminta tulisi rakentaa, tähän palataan ainoastaan pohdintojen muodossa. Opinnäytetyö antaa työntekijän omasta kokemuksesta ja työn pohjalta nousseiden havaintojen perusteella lisää tietoa kyseisenlaisesta rikollisuuden muodosta. Alan ammattilaisten vastausten perusteella pyritään löytämään tilausansojen tyypillisimmät toimintaperiaatteet ja ominaispiirteet.

Digitalisaatiota on hyvä käsitellä sen verran, jotta ymmärretään, mitä kehittynyt teknologia tarjoaa niin hyvässä kuin pahassakin. Digitalisaatiossa käydään läpi myös sähköistä asiointia ja siihen liittyvää tunnistautumista, joka on taas turvallisuuden ja erityisesti maksamiseen liittyvän turvallisuuden kannalta erityisen tärkeää. Tämä

osio antaa siten kattavamman kuvan siitä, kuinka tärkeätä on suojella kuluttajia rikollisten kalasteluyrityksiltä. Lainsäädäntö otetaan tarkasteluun erityisesti petoksien ja maksuvälinepetoksien osalta. On tärkeää ymmärtää myös, kuinka hankalaa nettiin liittyvien rikoksien tutkinta on ja kuinka moniin tilausansoihin liittyvien rikosten tutkinta on lähes mahdotonta.

Vaikka opinnäytetyössä viitataan myös kyberturvallisuuteen, tarkoituksena ei ole kuitenkaan käsitellä aihetta erityisen tarkasti, sillä aihe itsessään on todella laaja ja käsittää monia eri kokonaisuuksia. Kyberturvallisuutta on kuitenkin hyvä sen verran ymmärtää tässä opinnäytetyössä, koska tietojenkalastelu kuuluu osana kyberturvallisuuteen ja on siten osa tätä kokonaisuutta. Tietojenkalastelut aiheuttavat monessa eri muodossaan nykypäivänä valtavia taloudellisia vahinkoja niin kuluttajille kuin pankeille.

2.2 Opinnäytetyön eteneminen ja rakenne

Opinnäytetyön luvut 3–4 sisältävät tutkimuksen kannalta tärkeän teoriaosuuden. Teoriaosuus käsittelee keskeisimmät käsitteet digitaalisuuden ympäristöstä, digitaalisuuden turvallisuusuhista, maksamisesta, rikollisuudesta sekä lainsäädännöstä. Luvussa 4.4 tutustutaan tarkemmin tilausansaan sekä kerrotaan, minkälaisesta nettirikollisuudesta on kysymys digitaalisuuden maailmassa. Luvussa viisi esitetään tutkimuksen toteutusta. Tämä pureutuu menetelmän kuvaukseen, aineiston keruun toteutusta, aineiston analyysia sekä mietitään tilausansojen haasteita ja rikostorjuntaa tarkemmin. Viimeisessä, kuudennessa luvussa esitetään tutkimuksen eettisyys, luotettavuus sekä analysoidaan tarkemmin työtä ja esitetään kehittämisehdotukset.

Työn lopputuloksena on tuottaa lisää informaatiota ennalta ehkäisevään toimintaan tilausansarikollisuutta vastaan. Työ ei anna suoraan ohjeita viranomaisille ja alan ammattilaisille, kuinka yrityksen rikoksen ehkäisy tulisi suorittaa. Työ antaa informaatiota siitä, kuinka järjestelmällistä, suunnattua ja tehokasta rikollisuuttaa tilausansat ovat Suomessa ja muualla Euroopassa.

2.3 Keskeiset käsitteet

Tilausansalla tarkoitetaan yritystä tai tahoa, joka saa kuluttajan tilaamaan mainoksen, viestin tai muunlaiseen tekstiin piilotetun viestinnän perusteella jotakin sellaista, mitä kuluttaja ei ole ymmärtänyt tai tarkoituksella tilannut. Harhauttaminen voi tässä tapauksessa olla sekä tahallista että tahatonta. Olennaista tilausansoissa on kuitenkin se, että tarjouksen tai mainoksen vastaanottaja ei saa viestin sisällöstä realistista tietoa ja tämä vaikuttaa hänen lopulliseen ostopäätökseen. Hyvänä esimerkkinä on älypuhelimen osto, jossa käyttäjä harhautetaan tekemään sopimus huomaamatta suoratoistopalveluun kalliilla kuukausimaksulla. Yleensä näistä suoratoistopalvelusopimuksista on erittäin vaikea päästä irti, ja irtisanomisprosessi on tehty asiakkaalle hyvin hankalaksi. Tilausansan houkuttimina olevia älypuhelimia ei koskaan lähetetä, vaan puhelin saatetaan arpoa yhdelle asiakkaalle tai korvata jollain toisella huomattavasti arvottomammalla tuotteella. (Viestintävirasto 2017.)

Tietojenkalastelu (phishing ja social engineering) on yleensä aidolta näyttävä sähköposti, tilausansa tai muu huijaussivusto, jolla yritetään huijata ihmisiä paljastamaan luottamuksellisia tietoja. Sosiaalinen manipulointi pyrkii hyödyntämään ihmiselle luontaista taipumusta olla luottavainen yhdistettynä teknisiin tarkoituksiin tietojen varastamiseksi. (Peltomäki & Norppa 2015, 171.)

Maksuvälinepetos käsitellään Suomen rikoslain 8§:ssä (24.8.1990/769), ja se määritellään Suomen rikoslain 37 luvussa maksuvälinerikoksista. Maksuvälinepetos määritellään, kun henkilö/henkilöt hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä,

1. käyttää maksuvälinettä ilman sen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen tai muuten ilman laillista oikeutta tai
2. luovuttaa maksuvälineen tai maksuvälinelomakkeen toiselle saattaakseen sen ilman laillista oikeutta käytettäväksi, on tuomittava maksuvälinepetoksista sakkoon tai vankeuteen enintään kahdeksi vuodeksi (Rikoslain 37 luku 8§ 24.8.1990/769).

Lievässä maksuvälinepetoksessa huomioidaan tavoitellun hyödyn tai aiheutetun vahingon määrä. Mikäli kokonaisuus on vähäinen, on rikoksentekijä tuomittava sakkoon. (Rikoslain 37 luku 10§ 24.8.1990/769.)

Törkeässä maksuvälinepetoksessa määritellään,

1. mikäli aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa tai
2. rikoksentekijä on rikoksen tekemistä varten tehnyt tai teettänyt maksuvälinelomakkeita, joista rikoksessa käytetty maksuväline on valmistettu, taikka rikos muuten tehdään erityisen suunnitelmallisesti ja maksuvälinepetos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä maksuvälinepetoksesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi. (Rikoslain 37 luku 9§ 24.8.1990/769.)

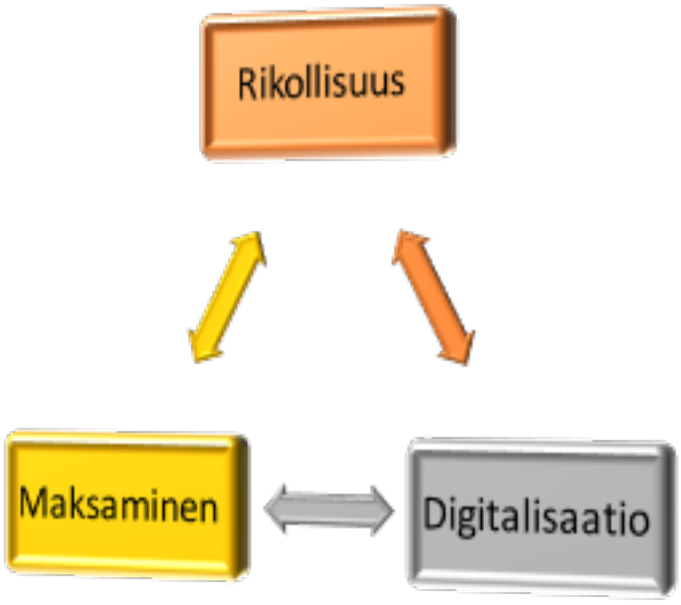
Nettirikollisuudessa kuvataan, kuinka rikoksen uhriksi voi joutua yksilö, yritys, järjestö kuin valtiokin. Limnellin, Majewskin ja Salmisen (2014) mukaan nettirikollisuus on moniulotteista eikä rajanveto perinteisempään rikollisuuteen ole aina kovin selkeätä. Nettirikollisuuden määrittämisessä voidaan tarkastella toiminnan kohdetta (tieto) ja luonnetta (oikeudeton pääsy tietoon tai omaisuuteen ja sen manipuloimiseen) yleisesti tai ottaa tarkasteluun rikolliset toimintaperiaatteet. Nettirikollisuus voi käyttää useita eri keinoja ja instrumentteja, sen kohteena on yleensä useita eri kohteita ja motiivit ovat erilaisia (rahan ansaitseminen tai varastaminen). Vaikuttavuus ja vahingollisuus riippuvat pitkälti rikollisten tietoteknisestä osaamisesta. Rikosten tutkinta ja todistaminen jälkikäteen ovat haasteellisia. Ratkaisevassa osassa on kuitenkin se, minkälaisia digitaalisia jälkiä rikolliset jättävät jälkeensä netissä. Kiteytetysti voi sanoa, että rikollisuus ja rikolliset ovat siellä missä rahakin.

3. Tutkimuksen metodologia

Tutkimus syntyy yleensä inhimillisestä käytännöstä. Historian saatossa ihmiskunnalla on aina ollut ongelmia, joiden ratkaisemiseen on pyritty mahdollisimman tehokkain

metodein. Tutkimukseen ryhdytään myös sen takia, koska ongelmien ratkaiseminen ei aina suju jokapäiväisen ajattelutavan mukaan. Tarvitaan uutta tietoa, joka auttaa ymmärtämään ratkaistavien ongelmien olemusta ja löytämään keinoja ongelmista selviämiseen. Siihen tietoon, joka saa alkunsa jokapäiväisestä kokemuksesta ja arkielämän toiminnasta, on monin tavoin kietoutunut myös tutkimuksen avulla kehitetty tieto. Tieteellinen tieto on monin osin sulautunut yhteiskunnan yhteiseen, kollektiiviseen tietovarantoon, josta kansalaiset eivät enää oivalla tällaisen tiedon olemassaoloa. Monia asioita pidetäänkin itsestään selvinä. (Hirsjärvi, Remes & Sajavaara 2005, 20–21.)

Lähdeaineistona toimivat sekä viranomaisille ja maksupalveluiden parissa toimiville ammattilaisille suunnatut teoriat, artikkelit, katsaukset sekä muut työkalut. Kuviossa 1 esitellään opinnäytetyön viitekehys. Tässä opinnäytetyössä kietoutuu yhteen toimintaympäristönä toimiva digitalisoitunut maailma (netti), siellä toimiva rikollisuus sekä maksaminen, joka yhä enemmissä määrin siirtyy sähköiseen muotoon. Kaikki osa-alueet vaikuttavat opinnäytetyöhön ja sen seurauksena syntyvään lopputulokseen, ilmiöön ja ominaisuuksiin yhdestä nettirikollisuuden kasvavasta ongelmasta eli tilausansoista.



Kuvio 1: Opinnäytetyön viitekehys

3.1 Tapaustutkimus

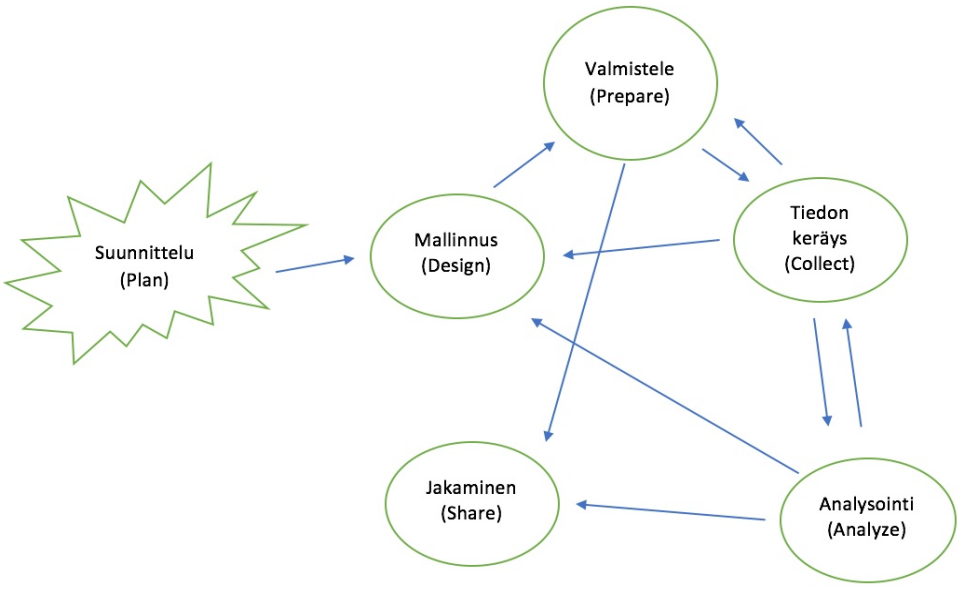
Tässä opinnäytetyössä käytettiin tutkimusmenetelmänä tapaustutkimusta. Tutkimusmenetelmänä tapaustutkimus on yleinen tutkimusmenetelmä, ja tästä johtuen tehtyjä tutkimuksia on laajalti saatavissa. Tapaustutkimuksen avulla voidaan koota tietoa ympäristöstä ja tämän tiedon perusteella edistää uusia teorioita. Tapaustutkimus voidaan määritellä empiiriseksi tutkimukseksi, joka monimuotoisia ja erilaisilla tavoilla saavutettuja tietoja käyttäen, tutkii nykyistä tapahtumaa tai ihmisiä tietyssä ympäristössä. (Metsämuuronen 2001, 16.) Tapaustutkimus perustuu tutkittavaan aiheeseen sekä kuinka- ja miksi-kysymyksiin, joiden avulla kerätään tietoa tutkimukseen ja tutkittavaan aiheeseen.

Tapaustutkimuksella tuotetaan tietoa nykymaailmassa tapahtuvasta ilmiöstä sen todellisessa tilanteessa ja toimintaympäristössä. Tapaustutkimuksen raportointi on mahdollista tehdä selkeästi ymmärrettäväksi, ja siinä on mahdollista väistää tutkimukselle tyypillistä tiedeslangia. Tapaustutkimusraportti hyväksyy lukijan tehdä omia johtopäätöksiä tutkimuksen tuloksista. (Metsämuuronen 2001, 17.)

Tapaustutkimuksessa tutkimusaineiston kokoaminen tapahtuu monin eri keinoin. Tutkimusaineisto voidaan kerätä havainnoimalla, haastattelemalla, arkistomateriaaleista tai erilaisista dokumenteista (Yin 2009, 83). Kehittämistyössä tapaustutkimuksen tarkoituksena on tuottaa uutta tietoa kehittämisen tueksi.

3.1.1 Aineiston keruu ja analysointi

Aineistonkeruu- ja analysointiprosessissa on käytetty Yinin teoriamallia. Kuvio 2 tuo esiin Yinin suosittelemaa lineaarista ja iteratiivista prosessia aineiston kasaamiseen ja analysoinnin vaiheista. Ensimmäisenä on suunnitteluvaihe (Plan). Siitä edetään tutkimuksen suunnitteluun (Design), valmisteluun (Prepare), tiedon keräämiseen (Collect), analysointiin (Analyze) ja tutkimustulosten jakamiseen (Share). Tutkimuksen edetessä mallinnus-, valmistelu, tiedonkeruu-sekä jakamisvaiheisiin voidaan aina palata uudestaan ja viimeistellä niitä tutkimuksen edetessä. (Yin 2009, 2–10.)



Kuvio 2: Yin malli: Tapaustutkimuksen vaiheet (Yin 2009)

3.1.2 Tutkimuksen suunnittelu

Tutkimusstrategian suunnittelussa on hyvä suunnitella tutkimuksen suorittaminen kysymysten kautta. Ensimmäinen kysymys on, mikä on tutkimusongelman rakenne. Onko päämääränä kuvata tapahtumaa vai sitä, yrittääkö ongelma selostaa jotakin sosiaalista ilmiötä. Toiseksi, vaatiiko tutkimus käyttäytymisen tai toimintojen hallintaa vai pyrkiikö se kuvaamaan luonnostaan tapahtuvia ilmiöitä. Viimeisenä, onko tutkimuksen kohteena oleva ilmiö olemukseltaan nykyaikaan asettunut vai menneisyyteen liittyvä. Näiden kysymysten avulla voidaan vahvistaa, onko tutkimus kuvaileva, ennustava, vai kartoittava. (Yin 2009, 7–11.)

Tapaustutkimuksen teorian mukaan hyvin valmistellut tutkimuskysymykset ja ymmärrettävä tutkimusyksikkö suuntaavat oikean tutkimusmetodin valitsemista. Tämä vaikuttaa myös selkeästi analyysin luomiseen, johtopäätösten muotoiluun, aineiston keruuseen, sekä tutkimusraportin ja tulosten kirjoittamiseen. Näiden osatekijöiden avulla asioihin tulee kiinnittää huomiota ja valita oikea tutkimusmenetelmä.

Yinin mukaan tutkimuksen suunnittelussa tärkeimmät neljä osa-aluetta ovat

1. tutkimushypoteesi
2. tutkimuksen analysointiyksikkö
3. tutkimuskysymykset
4. tutkimustulosten looginen yhteys tutkimushypoteesiin.

Oman tutkimukseni tavoitteina oli perehtyä tutkimusmetodologiaan, siihen liittyvään kirjallisuuteen ja artikkeleihin sekä suunnitella tutkimuksen aihe. Kokonaisuuden kannalta oli myös hyvä määritellä alussa analysointiyksikkö, tutkimuskysymykset sekä käytettävät metodit. Tutkimuskysymysten avulla pystyin rajaamaan käytettävän teorian, joka auttoi taas aiheiden sekä tutkimuskysymysten tarkemmassa asettelussa.

Liitteessä 1 on esitetty tutkimuksen attribuutit, jotka on koottu oman näkemykseni mukaisesti mukaillen lähdeaineistoa. Tapaustutkimus kohdistui nettirikollisuuteen, ja siinä tarkasteltiin muuttujana digitaalista maailmaa. Analysointiyksikkönä on nettirikollisuus, joka liittyy digitaalisuuteen sekä maksamiseen. Nettirikollisuus on hyvin laaja käsite, ja sitä voidaan tutkia sekä tarkastella monesta eri näkökulmasta. Tässä tutkimuksessa tarkasteltiin suureen laajuuteen levinnyttä rikollisuuden osaa, jossa käytetään hyväksi nykypäivän teknologiaa ja digitaalisuuden tuomaa anonymiteettiä.

3.1.3 Valmistelu

Valmisteluvaiheessa kehitetään tutkimusprotokolla. Sen kautta tutkija pystyy ylläpitämään tavoitteet ja ennustamaan tulevat haasteet ja kaudet. Tutkimusprotokolla on perusteellinen hanke tutkimusprojektista. (Yin 2009, 78–82.)

Valmisteluvaiheeseen kuuluu tutkimusaineiston kokoaminen. Yin määrittelee viisi taitoa, joita edellytetään tutkimuksen aikana, jotta tutkijalla on mahdollisuus tulkita haastatteluvastauksia. Ensimmäiseksi mainitaan kyky esittää hyviä kysymyksiä ja tulkita niiden vastauksia. Toiseksi mainitaan kyky olla hyvä kuuntelija. Tässä on

tärkeä mainita se seikka, että tutkija osaa myös ajatella asioita omien ideologioiden ulkopuolelta. Kolmanneksi mainitaan joustavuus ja mukautuvuus, jotta uudet tilanteet nähdään mahdollisuuksina eikä uhkina. Neljäntenä on kyky tarttua tutkittaviin asioihin ja viimeisenä kyky käsitellä ennalta sovittuja teorioita puolueettomasti.

Tutkimukseni valmisteluun kuului haastateltavien kartoittaminen ja yhteydenpito. Haastateltavat valittiin tarkoituksella mahdollisimman monelta eri sektorilta, yksityiseltä ja julkiselta sektorilta. Ainoana vaatimuksena oli, että henkilö oli ollut ammatillisessa mielessä tekemisissä tilausansojen kanssa. Vastaajat Suomessa ja muualla Euroopassa toimivat muun muassa seuraavilla titteleillä: kihlakunnansyyttäjä, luottopäällikkö, tuoteasiantuntija, riskiasiantuntija, rikosylikonstaapeli, criminal police inspector, riskienhallintapäällikkö, korttiasiantuntija, detective inspector, detective sergeant sekä lakimies.

3.1.4 Aineiston keräys

Aineiston kokoamisessa tulee noudattaa kolmea eri käytäntöä. Ensimmäisenä on käytettävä tutkimustietokanta, jonne aineistot kerätään johdonmukaisesti. Toisena periaatteena on käytettävien aineistojen moninaisuus ja niiden laaja-alainen käyttäminen tutkimuksessa. Viimeisenä sääntönä on säilyttää kerätyn materiaalin ja tutkimustulosten uskottavuusketju. Tämä tarkoittaa sitä, että aineiston kysymyksistä voidaan tuottaa kytkös käytettäviin menetelmiin, aineistoon sekä tutkimustuloksista saatuihin ratkaisuihin. (Yin 2009, 112–126.)

Aineistoa kerätään käyttäen erilaisia metodeja ja eri tavoilla. On tärkeää muistaa, että jokaisen lähteen vahvuudet ja heikkoudet tulee ottaa huomioon. Aineiston keräämiseen voi käyttää haastatteluja, arkistomateriaaleja, havainnointia, tai muita aiheeseen liittyviä dokumentteja. Aineiston kokoamisessa tavoitteena on käyttää aineistoa kattavasti ja asianmukaisesti. (Yin 2009, 99–113.)

Tutkimusstrategiana oli kvalitatiivinen puolistrukturoitu haastattelumenetelmä. Ennen haastattelun alkua haastateltaville kerrottiin, mikä oli kyselyn tarkoitus ja mitä

varten tietoa kerättiin (liite 11). Tässä vaiheessa kerrottiin myös, että kysymyksiä oli yhteensä 9 kappaletta. Kysymykset olivat asiakysymyksiä, joiden tarkoituksena oli saada vastaajilta mahdollisimman laaja kuvaus ilmiöstä. Näillä kysymyksillä yritettiin saada lisäselvitystä, uusia näkökulmia sekä mahdollisia vastaajaryhmien asenteita.

3.1.5 Aineiston analyysi

Aineistoa tarkasteltiin monipuolisesti ja yksityiskohtaisesti korostaen esiin merkityksellisiä teemoja. Analyysissä käytettiin induktiivista päättelyä, joka oli seurausta aineistosta nousevien merkittävien yksityiskohtien takia. Analysointivaiheessa aineistoa yleensä tiivistetään, eritellään ja luokitellaan, jotta pystytään luomaan onnistuneita tulkintoja. (Yin 2009, 128–130.)

Yin (2009, 130–135) määrittelee neljä yleisintä strategiaa datan analysointiin, jolla pyritään aineiston oikeudenmukaisuuteen ja aineistosta tehtyyn luotettavaan analyyttiseen johtopäätökseen sekä sulkemaan vaihtoehtoisia tulkintoja. Nämä strategiat on kuvattu seuraavassa taulukossa.

Strategia	Strategian kuvaus
Analyysi pohjautuu olemassa olevaan teoriaan	Tämä on yleisin käytetty strategia. Olemassa oleva teoria vaikutta tutkimuskysymyksiin ja mahdollistaa uusien hypoteesien ja ehdotuksien luomisen aineistosta.
Tutkittavan tapauksen kuvauksen kehittäminen	Tätä strategiaa käytetään, mikäli tutkijalla on käytettävissään paljon aineistoa kerättynä. Tämä strategia korostuu, mikäli tutkimuksen alussa ei ole määritelty

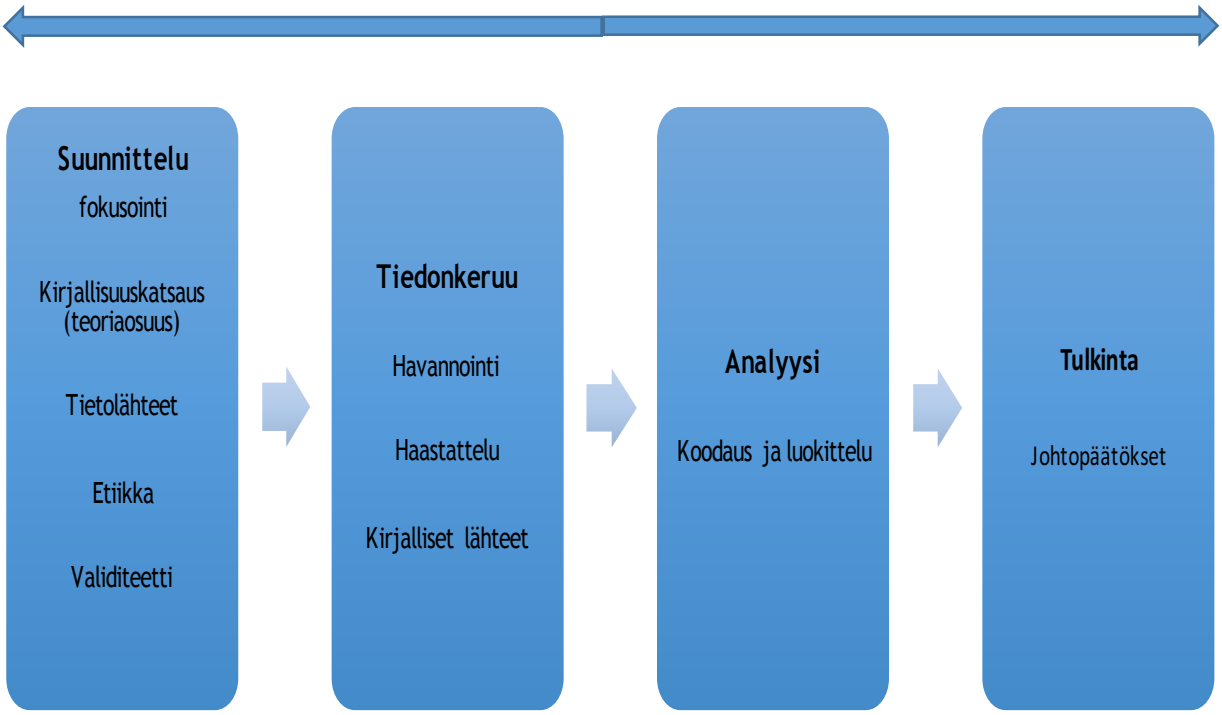
	tarkasti tutkimuskysymyksiä ja/tai tutkimushypoteesia.
Määrällisen ja laadullisen datan käyttö	Kokeneemmat tutkijat käyttävät kyseistä strategiaa laadullisen ja määrällisen datan analysointityökaluna tukemaan tutkimusta laaja-alaisemmin
Tutkitaan kilpailevaa hypoteesia / teoriaa	Tutkitaan ja testataan olemassa olevaa hypoteesia/teoriaa. Strategiassa hyödynnetään olemassa olevia strategioita ja lähestymistapoja datan analysoinnissa

Taulukko 1: Datan analysoinnin neljä strategiaa (Yin 2009, 130-131)

Opinnäytetyön aineisto kerättiin kyselylomakkeiden avulla ja jokainen vastaus purettiin omaksi kokonaisuudeksi myöhempää purkua varten. Analyysin toisessa vaiheessa aineiston purun ja puhtaaksikirjoituksen sekä analysointiprosessin suoritin kolmivaiheisena prosessina. Ensimmäisessä vaiheessa kokosin kaikki vastaukset Excel-lomakkeelle. Analyysin toisessa vaiheessa käytin Yinin analyysiteorian ensimmäistä vaihtoehtoa (Taulukko 1), jossa listasin eri sarakkeisiin kaikki samankaltaiset vastaukset ja toisistaan selkeästi eroavat vastaukset. Kolmannessa vaiheessa tein tiivistetystä aineistosta johtopäätökset.

3.2 Kvalitatiivinen menetelmä

Yhtenä menetelmänä opinnäytetyössä käytetään laadullista eli kvalitatiivista menetelmää, jossa pyritään selvittämään ja ymmärtämään tutkittavaa ilmiötä.



Kuvio 3: Laadullisen tutkimuksen prosessikaavio (Kananen 2010)

Kulmakivenä on se, että mitä vähemmän ilmiöstä on informaatiota, sitä todennäköisempää on käyttää kvalitatiivista tutkimusta. Kvalitatiivinen tutkimus soveltuukin parhaiten, kun halutaan selville vastauksia seuraaviin tilanteisiin (Kananen 2010, 40–41):

1. Ilmiöstä ei ole teoriaa, tietoa tai tutkimusta.
2. Halutaan saada syvällisempi ja tarkempi näkemys ilmiöön.
3. Käytetään triangulaatiota eli mixed-tutkimusstrategiaa.
4. Kehitetään ja luodaan ja uusia teorioita.
5. Halutaan ilmiöstä kattava kuvaus.

Kaikista tapauksista ja malleista ei löydy teorioita ja valmiita kuvauksia. Tutkija yrittää mukauttaa jotakin olemassa olevaa teoriaa uuteen ilmiöön ja pyrkiä tällä levittämään teorian yleistävyyttä (Kananen 2010, 40–41). Tutkimusongelmaa pyritään rat-

kaisemaan hyödyntämällä viranomaisohjeita, lainsäädäntöä, artikkeleita, alan kirjallisuutta sekä työelämässä kartutettua tietoa. Luotettavuuden arvioinnista on hyvä muistaa laadullisessa tutkimuksessa, että mitään selkeitä ohjeita ei ole olemassa. Tutkimusta tarkastellaan aina kokonaisuutena, jolloin sen sisäinen johdonmukaisuus korostuu. Vaikka tutkimusraportissa seuraavan listan kohdat olisivat erillisinä täytettynä, niiden pitää olla myös suhteessa toisiinsa. (Tuomi & Sarajärvi 2012,140–141.)

1. *Tutkimuksen kohde ja tarkoitus:* Mitä olen tutkimassa, miksi ja miten?
2. *Omat sitoumuksesi tutkijana tässä tutkimuksessa:* Miksi tämä tutkimus on ollut itselleni tärkeä? Mitä olen olettanut, kun aloitin tutkimuksen tekemisen, onko ajatukseni ja mielikuvani muuttuneet matkan varrella?
3. *Aineiston keruu:* Miten aineiston keruu on tapahtunut menetelmänä ja tekniikkana? Miten aineiston keruuseen liittyneet erityispiirteet sekä mahdolliset ongelmat ja tutkijan mielestä muut merkitykselliset seikat näkyvät tutkimuksessa?
4. *Tutkimuksen tiedonantajat:* Millä perusteella tutkimuksen tiedonantajat valittiin, miten heihin otettiin yhteyttä, montako henkilöä kaikkiaan tutkimuksessa oli? Tutkimuksen tekijän pitää tässä kohtaa pitää myös huolta, että tiedonantajien henkilöllisyys ei paljastu esimerkiksi asuinpaikkakunnan perusteella.
5. *Tutkija-tiedonantaja-suhde:* Arvio, miten suhde toimi. Lukivatko tiedonantajat tutkimuksen tulokset ennen niiden julkaisua, muuttivatko heidän kommenttinsa tuloksia?
6. *Tutkimuksen kesto:* Minkälainen aikataulu tutkimuksella oli? Saivatko vastaajat riittävästi aikaa vastauksilleen?
7. *Aineiston analyysi:* Miten aineisto analysoitiin, miten tuloksiin ja johtopäätöksiin päädyttiin ja minkä takia?
8. *Tutkimuksen luotettavuus:* On arvioitava, miksi tutkimus on eettisesti korkeatasoinen, miksi tutkimusraportti on luotettava?
9. *Tutkimuksen raportointi:* Miten tutkimusaineisto on koottu ja analysoitu. (Tuomi & Sarajärvi 2012,140–141.)

3.3 Kvantitatiivinen menetelmä

Kvantitatiivinen eli määrällinen tutkimus tarkoittaa tapausta, jossa käytetään laskennallisia menetelmiä. Usein määrällinen tutkimus tehdään kyselylomakkeilla tai haastatteluilla. Kvantitatiivisen tutkimuksen avulla selvitetään lukumäärin ja prosenttiosuuksiin liittyviä kysymyksiä. Kvantitatiivinen tutkimus edellyttää tarpeeksi suurta ja edustavaa otosta. Asioita kuvataan numeeristen suureiden avulla ja usein selvitetään myös eri asioiden välisiä riippuvuuksia tai tutkittavassa ilmiössä tapahtuneita muutoksia. Kvantitatiivisen tutkimuksen avulla saadaan yleensä selvitettyä olemassa oleva tilanne, mutta ei pystytä riittävästi selvittämään asioiden syitä. (Heikkilä 2014.)

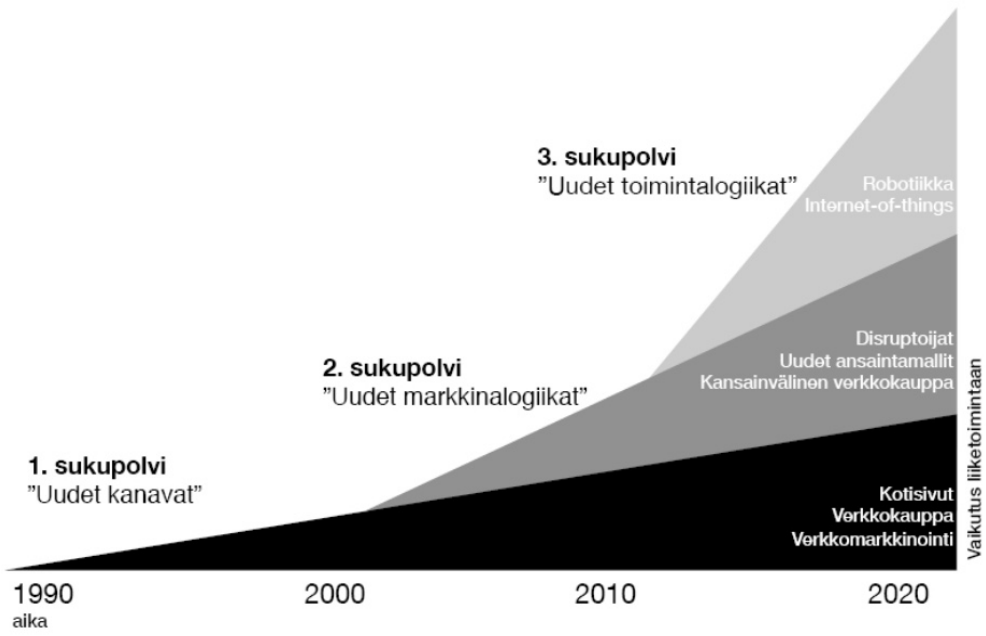
Tässä opinnäytetyössä kvantitatiivista menetelmää käytettiin kyselylomakkeiden sekä haastattelujen avulla. Yksityiskohtaisessa ja yksiselitteisessä kyselyssä (liite 11-20) oli ainoastaan avoimia kysymyksiä, sillä tällä tavoin kyselystä saataisiin parhaiten esiin ongelmakohdat sekä kehitysehdotukset. Nämä edellä mainitut menetelmät osoittautuivat erittäin tärkeäksi osaksi koko tutkimusta. Kyselylomakkeita testattiin neljällä koehenkilöllä. Koetäyttämisen jälkeen lomakkeisiin tehtiin palautteiden perusteella tarvittavat muutokset, ennen kuin ne jaettiin kaikille. Tutkimuksessa kysyttiin tilausansojen osalta seuraavat aihealuekokonaisuudet:

- Kuinka kauan vastaaja on ollut tekemisissä kyseisen rikollisuuden kanssa?
- Osaako arvioida, mistä tilausansarikollisuus tulee?
- Kuinka paljon nämä rikokset työllistävät itseään/organisaatiota?
- Miksi tilausansarikollisuutta on nykyään niin paljon?
- Kuinka tämänkaltaista rikollisuutta voisi torjua?
- Kuinka yhteistyötä voisi parantaa eri toimijoiden kesken?

4. Tutkimuksen tietoperusta

4.1 Digitalisaatio

Netissä näkyy ilmaisten tuotteiden ja halvan hinnan mielikuva. Halpa hinta houkuttaa, mutta sillä on myös toinen vaikutus: ilmainen tai lähes ilmainen tuo viehätystä ja mielihyvää. Ilmaista tai lähes ilmaista tuotetta ei voi epäillä huijaukseksi (Järvinen 2010, 218). Digitalisaatio-sanan käyttö on yleistynyt viime vuosina räjähdysmäisesti, mutta sille ei löydy varsinaisesti kunnon määrittelyä. Digitalisaatiota kuvaillaan usein esimerkkien tai tapauksien kautta, mutta ei kuitenkaan määritellä, mitä se varsinaisesti on. Tämän päivän yhteiskunnassa digitalisaation taustalla on digitalisoituminen. Digitalisaatiosta puhutaan, kun digitalisoituminen muuttaa markkinoiden dynamiikkaa, ihmisen käyttäytymistä ja yritysten ydintoimintaa. Digitalisaatio saa muutosvoimansa digitalisoitumisesta. Teknologia ja markkinat eivät itsessään luo digitalisaatiota vaan sen mahdollistamat tavat operoida. (Ilmarinen & Koskela 2015, 22–24.)



Kuvio 4: Digitalisaation kehityskulku (Ilmarinen & Koskela 2015)

Digitalisaatiota voi analysoida yksittäisen yrityksen, markkinoiden ja toimialojen tasolla sekä laajemmin yhteiskunnan tasolla. Digitalisaation lohkominen mikro- ja makrotasoihin auttaa käsittämään sen valtavaa dynamiikkaa. Makrotaso tarkoittaa yhteiskunnan, talouden, rakenteiden ja markkinoiden dynamiikan ja ihmisten käyttäytymismallien muuttumista ja muuntautumista ja sen selittämistä digitalisoitumisen avulla. Mikrotasolla ilmiötä tarkastellaan yksittäisen toimijan, kuten yritysten kannalta. Tässä yhteydessä suunnitellaan, kuinka digitaalisuus muuttaa mekanismeja, strategioita, palveluita, tuotteita, ansainnan malleja, toimintamalleja sekä osaamista. (Ilmarinen & Koskela 2015, 24–26.)

Yhteiskuntaa koskevaa digitalisaatiota voidaan luonnehtia verkkoon kytkettyjen älykkäiden tuotteiden ja palveluiden avulla. Teollinen internet eli IoT on suomalaisten yritysten yleisnäkymä digitalisaation kenttään. Muita näkökulmia ovat yhteiskunnan rooli digitaalisten tuotteiden ja palveluiden tuottajana, kehittäjänä ja hyödyntäjänä, joista vastineeksi yritysten kilpailukyvyn vaatimukset Suomessa vahvistuvat ja siten luovat pohjaa digitalisaation kasvulle Suomessa. Kuluttajapuolen digitalisaation kehityksen myötä on todettu, kuinka sekä markkina- että innovaatiopotentiaali kasvavat avoimuuden lisääntyessä. Vakiintuneesti teollisuudessa on toimittu suljetuissa ympäristöissä oman kuplan sisällä. Kuluttajapuolen ekosysteemeistä tunnetuimpia menestyjiä ovat muun muassa Apple ja Googlen Android, jotka tarjoavat kehittäjille yhtenäisen alustan ja markkinat. (ETLA-raportit 2015.)

4.1.1 Tietoyhteiskunnan kehitys

Länsimainen tapa ratkaista ongelmia on asettaa lakeja ja valvoa niiden noudattamista. Tietoyhteiskunnassa ja digitalisaation maailmassa lakien kiertäminen on suhteessa helpompaa. Tieto ja data liikkuvat valon nopeudella sinne, missä sen käsittelyä valvotaan ja säädellään vähiten. Eri tavalla kuin materiaalivirtojen, datavirtojen tarkkailu sekä rajoittaminen ovat käytännössä mahdotonta nykyisellä teknologialla. Tietoyhteiskunta on globaali eikä istu lainkaan perinteiseen malliin, joka perustuu itsenäisten valtioiden harjoittamaan paikalliseen sääntelyyn. (Järvinen 2010, 22.)

Samalla kun nettiin liitetyt laitteet lisääntyvät räjähdysmäisesti, lisääntyvät myös niitä uhkaavat virukset ja muut uhat. F-Securen tutkimusjohtaja Mikko Hyppönen on tutkinut uhkia jo yli 25 vuoden ajan, ja ensimmäiset 15 vuotta olivat hänen mukaansa harrastelijoiden puuhastelua. Viruksia koodattiin huvin ja jännityksen vuoksi, ei ensisijaisesti taloudellista hyötyä etsien. 2000-luvun alussa tilanne muuttui toiseen suuntaan, ja silloin ilmestyivät ensimmäiset rahaa tekevät haittaohjelmat. Pelikenttä on viime vuosina muuttunut oleellisesti ja tule varmasti myös muuttumaan lisää. Nykyään suojattavia laitteita on useita, ja jokainen niistä toimii eri logiikalla, käyttöjärjestelmällä ja suojauksella. Jokaisella laitteella on erilaiset alustat, tietoa on pilvessä, hallittavia tilejä on paljon ja niille annetaan usein samat helposti muistettavat salasanat. (Peltomäki & Norppa 2015, 17.)

Tablettitietokoneiden ja älypuhelinten määrän räjähdysmäinen kasvu nosti internetiin liitettyjen laitteiden määrän 12,5 miljardiin vuonna 2010 samalla, kun maailman väkiluku kasvoi 6,8 miljardiin. Tämä tarkoittaa, että laitteita on ensi kertaa maailmassa henkilöä kohden yli kaksi kappaletta. Kun internetiin kytkettyjen laitteiden määrän suhteuttaa käyttäjäkuntaan, laitteiden määrä henkilöä kohden nousee 6,25:een. (Limnéll, Majewski & Salminen 2014, 216.)

Kansalaisen näkökulmasta yksi suuri kasvava riski on laitteiden nopea vanhentuminen. Verkkoa hyödyntävien päätelaitteiden käyttöikä on lyhyt, koska sinänsä käyttökelpoisille laitteille ei tehdä enää päivityksiä ja laitteista tulee ns. verkonpainoja. Verkkoon kytketty vanha, suojaamaton ja päivittämätön laite tarjoaa rikolliselle uuden käyttöalueen esimerkiksi palvelunestohyökkäyksen osana. (Peltomäki & Norppa 2015, 117.) Euroopan unioni on julkistanut digitaalistrategian, jossa hahmotellaan seitsemän tärkeintä toimenpidealaa. Näihin kuuluvat nykyistä nopeammat internetliittymät, digitaalisen osallisuuden edistäminen sekä tieto- ja viestintäteknologioiden hyödyntäminen ratkaistaessa väestön ikääntymiseen liittyviä yhteiskunnallisia haasteita. Kyseinen digitaalistrategia on ensimmäinen Eurooppa 2020 -strategian seitsemästä lippulaivahankkeesta, joilla pyritään älykkääseen, kestävään ja osallistavaan kasvuun. (Liikenne- ja viestintäministeriö 2011, 13.)

4.1.2 Digitaalinen ympäristö

Internet koskettaa ja liittää yhä suuremman osan suomalaisen elämää, moni asia ja palvelu löytyvät kuluttajille netistä ja tulevaisuudessa ainoastaan netistä. Tilastokeskuksen mukaan 16–74-vuotiaista suomalaisista noin 90 prosenttia käyttää nettiä ja noin 70 prosenttia käyttää nettiä useita kertoja päivässä. Vaikka netin käyttö on keskimäärin vähäisempää vanhemmalla sukupolvella, silti 65–74-vuotiaistakin jo noin 30 prosenttia eli yli 200 000 käyttää nettiä useita kertoja päivässä. Suomessa vuosi 2014 oli varsinaisesti mobiilin läpimurtovuosi. Lähes 70 prosentilla suomalaisista on käytössään älypuhelin, ja 35 prosentilla on käytössään tabletti. Näillä alustoilla suoritetaan myös rikollisia kiinnostavia pankki- ja maksutapahtumia sekä sähköiseen tunnistautumiseen liittyviä tapahtumia yhä enemmän. Esimerkkinä alustojen muutoksesta Yhdysvalloissa vuonna 1980–2000 syntyneistä kuluttajista joka viides ei käytä internetiä enää lainkaan tietokoneella. (Ilmarinen & Koskela 2015, 36–40.)

Sosiaalisen median palvelujen käytön osuus kasvaa koko ajan. Uusia palveluja tulee markkinoille lisää, ja tässä yhteydessä sosiaalisen media käyttö noudattelee paljolti mobiilin käyttöä. Yhteisöpalvelujen käyttäjistä lähes 95 prosenttia käyttää Facebookia. Twitterin, LinkedInin sekä Instagramin osuus on noin 10–20 prosenttia. Näissä yhteisöpalveluissa on selkeästi nähtävissä suuri ikäjakauma. Instagram on tällä hetkellä suosittu erityisesti nuorten keskuudessa, kun taas LinkedIn on suunnattu työikäisille. (Ilmarinen & Koskela 2015, 36–40.)

Tulevaisuuden sosiaalisessa mediassa, nettiyhteisöissä ja sosiaalisissa verkostoissa käyttäjille tarjotaan sellaista vuorovaikutusta, joka ei ole sidoksissa päätelaitteeseen, sen enempää kuin aikaan tai paikkaankaan. Erilaisissa aktiivitiloissa käyttäjä voi esimerkiksi puheohjattujen sensorien avulla kommunikoida yhteisöjen kanssa ilman, että kantaisi teknologiaa mukanaan. Maailma on kovaa vauhtia menossa siihen suuntaan, jossa supertietokoneet voivat käsitellä valtavia määriä erilaista dataa: tietoa, kuvia, merkityksiä, symboleja, sisältöjä ja tulkintoja. (Heinonen 2009, 16.)

4.1.3 Digitaalisuuden turvallisuusuhat

Turvallisuus on olennainen asia, kun puhutaan digitalisaatiosta. Turvallisuus on merkittävin yksittäinen uhkatekijä, joka vaikuttaa jokaiseen palveluntarjoajaan ja kuluttajaan. Sekä digitaalisessa että fyysisessä maailmassa on uhkia, joiden likvidointi on harvoin mahdollista tai riskitöntä. Vaikka turvallisuusasiat ovat tärkeitä organisaatioille, uhkien laatu sekä liiketoiminnan luonne ja merkitys liiketoiminnan kannalta vaikuttavat varautumiseen. Esimerkiksi asiakas- ja henkilötietojen hallintaan liittyvä sääntely sekä korttimaksamisen PCI DSS asettavat ehtoja sille, miten turvallisuusasioita tulee organisaatioissa käsitellä. (Ilmarinen & Koskela 2015, 224–225.)

Kyberturvallisuus on hyvä esimerkki siitä, kuinka turvallisuuteen muodostuu uusia alueita ja miten joudumme ottamaan turvallisuusajattelussamme uusia yksityiskohtia tarkasteluun. Nykyajan turvallisuusajattelumme eroaa parin vuosikymmenen takaisesta kylmän sodan ajan näkymästä. Turvallisuus on saanut uusiksi määritelmiksi muun muassa energian, ympäristön, talouden sekä inhimillisyyden. Tällä edellä mainitulla muutoksella puhutaan laajentuneesta turvallisuudesta. Kaiken kattavaa turvallisuutta ei ole, eikä sellaisen saavuttaminen ole mahdollista. Uhkat, epävarmuus ja muutos ovat koko ajan läsnä nykyajan yhteiskunnassa. Kaikkea ei voi yrittää turvata, vaan turvattavat arvot on laitettava järjestykseen ja niihin on kohdistettava tärkeysjärjestyksen mukaisia turvatoimia. (Limnéll, Majewski & Salminen 2014, 27–28.)

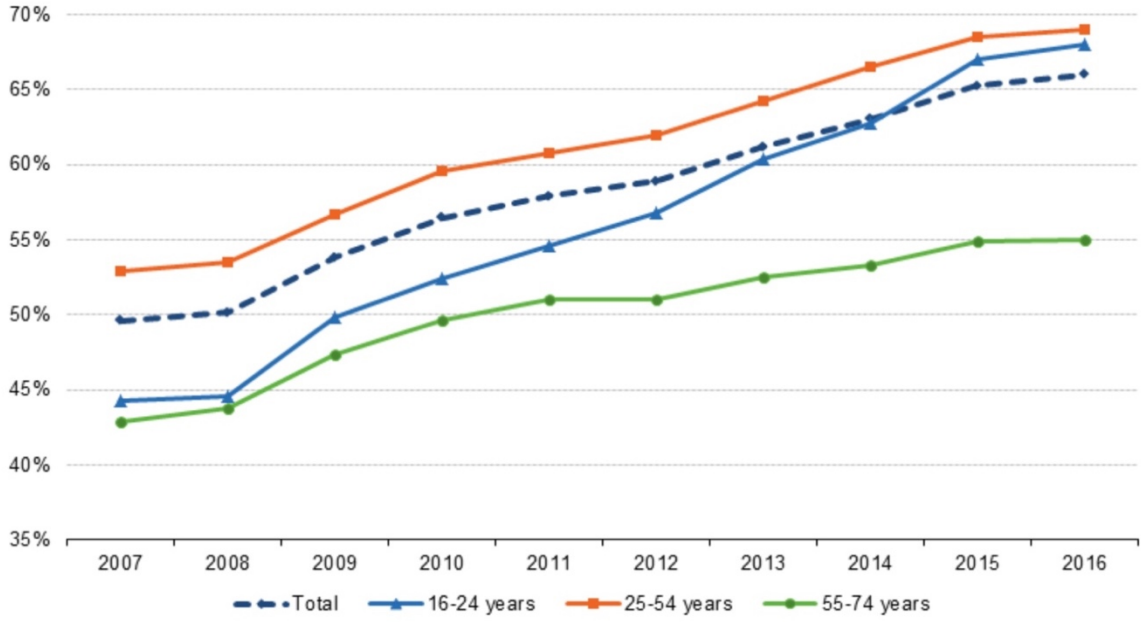
Digitalisaation tuloksena on syntynyt uusia uhkakuvia sekä yhteiskunnan että palvelujen käyttäjien perspektiivistä. Digitaaliset palvelut pohjautuvat avoimuuteen, kun palvelut ja rajapinnat ovat käsillä avoimen netin kautta. Tietoverkoissa kulkee suuret volyymit informaatiota, osin arkaluonteista informaatiota digitaalisessa muodossa samanaikaisesti. Maksaminen rahaliikenne ja tunnistautuminen ovat pitkälle jo digitalisoitunutta. Verkottuneessa yhteiskunnassa turvallisuus syntyy alihankkijoiden, toimittajien, kumppanien ja palveluntarjoajien ekosysteemin yhteistoiminnan tuloksena. Ketjuun lisätään yleensä myös asiakkaat ja käyttäjät, jotka ovat usein ”ketjun heikoin lenkki”. (Ilmarinen & Koskela 2015, 224–225.)

Tietoyhteiskunnassa laajasti ottaen on paljon potentiaalia sekä riskejä ja uhkia – todellisia ja koettuja. Nämä uhat eivät ole internetin tai tekniikan vaan toimijoiden itsensä luomia. Riskejä ja ongelmia ilmenee lisäksi siitä, että internetissä vaikutuksen laajuus, nopeus ja vahingollisen tiedon saatavuuden helppous tekevät yhteisöstä vaikeasti hallittavia. Sääntöjen ja rajoitusten sijaan pitäisi lisätä sosiaalisen median kriittistä lukutaitoa ja käydä yhteisöjen sisällä rohkeasti arvokeskustelua. Internet, kuten mikä tahansa teknologia, on itsessään arvoneutraalia. (Heinonen 2009, 11.) Tietoyhteiskunnan muokkautuessa uudeksi yhteiskunnaksi, jossa nerokas teknologia on läsnä joka paikassa, manipuloinnin, kontrolloin ja väärinkäytösten mahdollisuus lisääntyy samassa yhteydessä uusien mahdollisuuksien avautumisen myötä ihmisten väliseen vuorovaikutukseen virtuaaliyhteisöissä (Heinonen 2009, 16).

Näiden tilastojen valossa ei aiheuta suurta ihmetystä se seikka, että monet tilausansayritykset mainostavat ja markkinoivat sosiaalisessa mediassa. Tilausansojen kohdalla sosiaalisen median ykköseksi nousee Facebook, jossa kyseiset yritykset hyödyntävät kohdennettua markkinointia. Facebook ja siellä markkinointi on tilausansayrityksille alusta, josta yritetään houkuttelevilla tarjouksilla ohjata kuluttajat omille sivuille luovuttamaan maksutietonsa. Kaikki kohteet, joissa verkossa voidaan tarjota asiakkaille kohdennettua markkinointia, ovat myös otollisia paikkoja tilausansoille ja samankaltaiselle rikollisuudelle. Tilausansamainoksia ja -bannereita on tosin havaittu myös tunnettujen iltapäivälehtien nettisivuilta Suomessa, joten mikä tahansa kaupallinen sivusto saattaa olla mahdollinen tilausansabannerin levittäjä, joka tarjoaa mainostajille markkinapaikkoja.

4.2 Maksaminen ja maksuvälineet

Digitaalinen kaupankäynti on lisääntynyt viime vuosina huomattavalla tavalla, ja tämän ohella myös kuluttajille tarjottavat maksutavat ovat lisääntyneet ja laajentuneet (Kilpailu- ja kuluttajavirasto 2017).



Kuvio 5: Kuluttajat jotka ostivat tavaroita tai palveluja netin kautta (Eurostat 2017)

Ylipäätään kaupat ja pankit haluaisivat eroon käteisestä, koska rahan käsittely maksaa. Kauppojen kustannukset kohoavat, kun ne joutuvat investoimaan turvalliseen setelien kuljetukseen ja säilytykseen. Kuluttajina näemme rahaliikenteen tileillämme virtuaalisena, ja ostopäätösten tekeminen on helppoa. Käteisellä maksava kiinnittää lähtökohtaisesti enemmän huomiota hintoihin ja harkitsee tarkemmin kulutustottumuksiaan. Kuluttaminen viehättää, koska tavarat ja palvelut voi hankkia verkossa huomattavasti helpommin. Lainaa saa helposti tekstiviestillä eikä vakuuksia tarvita. Lainaraha on sekin virtuaalista – numeroita, joiden edessä on miinusmerkki. (Järvinen 2010, 100–101.)

Verkkokauppias päättää itse verkkosivustonsa toteuttamisesta ja on vastuussa siitä, että se täyttää lain edellytykset. Tiedonantovelvoitteet on laissa merkitty selkeästi elinkeinonharjoittajalle, joten tietojen saamista ei voi jättää kuluttajan aktiivisuuden varaan. Verkkokaupan maksutapahtumaa koskevien sopimusehtojen on myös oltava kokonaisuudessaan verkkosivuilla vaivatta saatavilla (Kilpailu-ja kuluttajavirasto 2017).

Asiakkaiden velvollisuus maksuvälineistä on määritelty korttiehdoissa ja verkkopalveluja koskevissa ehdoissa. Asiakkaan vastuu kortin tai pankkitunnusten käytöstä lakkaa siltä osin, kun pankkitunnuksia tai korttia on käytetty sen jälkeen, kun pankki tai pankin ilmoittama taho (esim. sulkupalvelu) on vastaanottanut ilmoituksen katoamisesta tai kortin tai pankkitunnusten oikeudettomasta käytöstä. Asiakkaalle saattaa syntyä vastuu maksuvälineen varastamisesta, katoamisesta tai väärinkäyttötilanteesta, jos asiakas on toiminut huolimattomasti. Lievä huolimattomuus saattaa johtaa vastuuseen, mutta vastuu rajoittuu pääsääntöisesti 50 euroon. Vastuuraja ei koske tapauksia, joissa asiakkaan katsotaan toimineen tahallisesti tai törkeän huolimattomasti. Törkeänä huolimattomuutena pidetään esim. tapauksia, joissa maksukorttia ja tunnuslukua säilytetään samassa lompakossa. (Danske Bank.) Moni kuluttaja unohtaa, että älypuhelinkin toimii nykyään monessa paikassa maksuvälineenä. Kuluttajariitalautakunta rinnastaa ostamiseen käytetyn puhelimen maksukorttiin. Mikäli maksuvälineen katoamisesta ei heti huomattuaan tee ilmoitusta, puhelimella tehdyt ostokset jäävät kokonaan kuluttajan maksettavaksi.

Maksupalvelulakiin liittyen kauppiaan on säilytettävä korttitositteet 18 kuukautta aiemman 9 kuukauden sijaan. Taustalla on maksupalvelulain säännös maksajan oikeudesta vaatia palautusta virheellisesti veloitetusta, oikeudettomasta tai toteutumatta jääneestä maksutapahtumasta viimeistään 13 kuukauden kuluessa veloituspäivästä. Kauppiaan vastuulla on myös varmistaa, että kortinhaltijalla on oikeus käyttää korttia. Jos näin ei tehdä, kauppias vastaa kortin oikeudettomasta käytöstä. (Danske Bank.)

World Payments Report vuodelta 2017 kertoo, että suomalaiset kuuluvat korttimaksamisen kärkeen maailmassa. Suomalaisten innokkuus maksukorttien käyttöön johtuu innovatiivisista maksujärjestelmistä, vahvasta taloudesta sekä vahvasta yksityisestä kulutuksesta. Raportin mukaan maksukorttien lisääntymistä pidetään maailmanlaajuisena ilmiönä, ja kaikkiaan maksukorttitapahtumissa oli kasvua maailmanlaajuisesti 11,2 prosenttia vuodesta 2014 vuoteen 2015. Korttitapahtumia rekisteröitiin maailmassa vuonna 2015 yhteensä 433 miljardia. Kaksi aluetta maailmassa jatkoi kasvuaan, kehittyvä Aasia, jossa kasvua oli 43,4 prosenttia, ja Keski-Eurooppa, Lähi-

itä ja Afrikka (CEMEA), jossa kasvua oli 16,4 prosenttia. Debit-kortit ja tilisiirrot olivat johtavat digitaaliset välineet vuonna 2015, kun taas sekkien käyttö laski edelleen maailmanlaajuisesti. (Finanssiala & World payments Report 2017.)

4.2.1 Maksamisen turvallisuus

Maksamisen turvallisuudesta puhuttaessa suomalaisten maksukortteja turvataan ja valvotaan erilaisilla turvatoiminnoilla, joissa on mukana muun muassa verkkomaksamisen kieltäminen kokonaan, säädettäviä nosto- ja maksurajoja tai maantieteellisen rajauksen käyttö maksukorteissa. Nosto- ja maksurajoja säätämällä voi jokainen maksukortinhaltija määritellä, kuinka paljon kortilla voi nostaa tai ostaa vuorokauden aikana. Verkkomaksuominaisuutta suositellaan aktivoitavaksi silloin, kun tekee ostoksia netissä, ja muulloin suljettavaksi, jotta mahdollisessa väärinkäyttötilanteessa rikolliset eivät pysty käyttämään kortin verkkomaksuominaisuutta. (Korttiturvallisuus.fi. 2012)

Kansainvälisesti verkkokauppoihin on lisätty turvallisuutta muun muassa Verified by Visa- ja Mastercard SecureCode –palvelujen avulla, joilla pyritään todentamaan kortin ja asiakkaan asioiminen luotettavasti. Ne eivät jätä kauppiaan palvelimelle korttitietoja. Suomessa palvelu perustuu siihen, että asiakas hyväksyy maksun tavallisin verkkopankkitunnuksin ja ostaa tuotteita turvallisemmin. Todentamispalvelut suojaavat sekä kauppiasta että kuluttajaa. Maksukortilla maksaessaan kuluttajalla on mahdollisuus saada rahat takaisin kortin myöntäjältä. Kortin myöntäjä luottaa kuluttajaan, kun myöntää kortin, ja kuluttaja voi luottaa, että kuluttajansuoja toimii, kun noudattaa ehtoja. Oman turvallisuuden vuoksi myös yrityksistä kannattaa ottaa selvää. Jos jokin asia tuntuu siltä, että kaikki ei täsmää, silloin todennäköisesti kaikki ei ole kunnossa. Muutamia nyrkkisääntöjä on aina hyvä pitää mielessä: kannattaa esimerkiksi tehdä ostoksia ennestään tutuissa tai yleisesti hyvämaineisissa ja luotettavissa verkkokaupoissa ja lukea toimitus- ja palautusehdot ennen kuin valitsee maksa-kuvakkeen. Yleensä verkkokauppiaat lähettävät asiakkaalle tilausvahvistuksen sähköpostilla. Mikäli kuluttajan tarkoituksena ei ole ostaa mitään, ei kannata antaa kortin tietoja mielipidekyselyihin tai vastaaviin tiedusteluihin.

Maksutapahtumien vertailussa on hyvä muistaa se tosiasia, että luottokortilla maksaessa voi vaatia maksunpalautusta kuluttajansuojalain 7 luvun 39§:n nojalla luottokorttiyhtiöiltä, mikäli tavaraa ei toimiteta tai se on virheellinen. Debit- ominaisuudella maksaessa ostosten osalta kuluttaja voi vaatia hyvitystä korttiyhtiöltä, jos yhtiö on korttiehdoissaan tai muutoin tähän sitoutunut. Viime vuosina maksunvälityspalvelut ovat saaneet enemmän jalansijaa markkinoilla. Maksunvälityspalveluiden käyttö saattaa olla kannattavaa silloin, jos ei halua antaa myyjälle korttitietoja tai jos ei omista luottokorttia. Kaikkia maksunvälityspalveluita ei ole kuitenkaan suunniteltu toimimaan verkkokaupassa. Rahojen vastaanottajan henkilöllisyyttä ei välttämättä tarkasteta eivätkä kaikki maksunpalveluyritykset hyväksy palauttamaan varoja, jos tuote jää saapumatta. Postiennakko toimii rajat ylittävässä kaupassa vain joillakin suurimmilla verkkokaupoilla. Tässä tapauksessa kuluttajalla ei ole mahdollisuutta tarkastaa tuotetta ennen sen maksamista. Viimeisenä on pankkisiirto, jossa tuotteet maksetaan etukäteen tilisiirrolla. Pankkisiirrossa olisi hyvä selvittää erityisen huolella yrityksen taustatiedot ja perehtyä verkosta löytyvään materiaaliin myyjästä. Rahoja on lähes mahdotonta saada takaisin, mikäli myyjä osoittautuu epäluotettavaksi tai ajautuu konkurssiin. (Euroopan kuluttajakeskus Suomessa 2014.)

Tulevaisuudessa uuteen avoimeen arkkitehtuuriin pohjautuva biometristen ja mobiilien varmenteiden verkosto luo pääsyn valtiohallinnon tietokantoihin luoden pohjan laajamittaiselle valtiotason tunnistamiselle. Lähiaikoina biometriikan teknologian demokratisoituminen muuttaa käyttäytymistä siten, että kuluttajien yleisimmin käyttämissään ostopaikoissa maksutunnisteena toimivat kasvot tai muu biometrinen tunnistusmenetelmä ilman mitään erillistä mukana kannettavaa fyysistä tunnistetta. (Suomen Pankki 2016, 17.)

4.2.2 Maksamisen tulevaisuus

Maksutekniikan tärkeimpiä palveluja koskee uudistettu maksupalveludirektiivi (PSD2), joka tuli voimaan vuoden 2018 alussa. Sen avulla Eurooppa ottaa tärkeän askeleen kohti täysin yhteen toimivia digitaalimarkkinoita. PSD2-direktiivin odotetaan antavan kauaskantoisia vaikutuksia pankkien, maksupalveluntarjoajien (PSP),

FinTechin ja muiden yritysten kesken. Se myös innostaa muita maapallon maksualueita kehittämään samankaltaisia aloitteita maksujen digitalisoimiseksi. (World payments Report 2017.)

Viime vuosina puhutuimpia aiheita maksamisessa ovat olleet nopeat maksut ja näkymätön maksaminen. Viimeisimmätkin maksukortit häviävät kuvasta ja maksaminen Suomessa, verkossa ja ulkomailla hoituu uusilla innovaatioilla. Meidän sukupolvemme saattaa olla viimeinen sukupolvi, joka käyttää muovikortteja maksamiseen. Perinteisillä finanssiyrityksillä on merkittävä riski menettää hallintaa ja merkityksellisyyttään kuluttajan jokapäiväisessä elämässä. Tätä muuttuvaa tilannetta korostaa ketterämpi FinTech-yritysten mahdollisuus kiertää sääntelyä ja toimia etulinjan kuluttajarajapinnassa, samalla kun pankkeja ja muita finanssiyrityksiä sitovat lukuisat ohjeistukset ja raportointivelvollisuudet viranomaisten suuntaan. Ketteryys on nykyhetken ja tulevaisuuden avainsana: mitä nopeammin pystyy reagoimaan muuttuvaan toimintaympäristöön, sitä paremmin palvelee älylaiteaddiktoitunutta kuluttajaa. (Suomen Pankki 2016, 7.)

Uudet diginatiivit muuttavat maksamiseen liittyvän tulevaisuudenkuvan. He haluavat maksamisen ja maksupalvelujen mukautuvan elämäntyyliinsä ja valitsevat ne ratkaisut, jotka vahvistavat heitä parhaalla mahdollisella tavalla. Asiakasuskollisuus tietyille brändeille ei ole heille olennaista. Tämä johtaa siihen, että perinteiset toimijat joutuvat uudistamaan ratkaisujaan valmistautuessaan palvelemaan uutta sukupolvea ja reagoimaan nopeasti heidän toiveisiinsa ja odotuksiinsa. Digitaalisten tekniikoiden yleistyminen ja kehittyminen antavat kuluttajille ennennäkemätöntä vaikutusvaltaa markkinoilla. (Suomen Pankki 2016, 10.)

Nykyhetkeä sekä tulevaisuutta on jo maksutapavalikoima mobiilin ohjaamana verkossa. Vaihtoehtoja on seuraavasti:

1. Maksukorttitietojen tallennus kauppa- tai palvelukohtaisesti ja tallennetuilla tiedoilla tehdyt veloitukset käyttö- tai aikaperusteisesti.

2. Maksujen ja veloitussopimuksien hyväksyminen luotetussa mobiilipalvelussa, johon maksukorttitiedot on tallennettu.
3. Uusi pankkitilimaksaminen. Astuu voimaan aiemmin mainitun PSD2-maksupalveludirektiivin myötä.
4. Apple Pay ja vastaavat uudet EMV-standardin mukaiset korttimaksupohjaiset mobiilit maksupalvelut. (Suomen Pankki 2016, 20.)

4.2.3 Kuluttajansuoja verkkokaupassa

Etämyynnillä tarkoitetaan myyntiä, josta tehdään myynti- tai palveluntarjontajärjestelmässä kulutushyödykesopimus ja joka tapahtuu ilman, että osapuolet ovat yhtä aikaa paikalla ja jonka tekemiseen käytetään yleensä useampaa etäviestintä. Tässä yhteydessä etäviestimellä tarkoitetaan postia, tietoverkkoa, puhelinta, televisiota tai muuta välinettä, jota voidaan käyttää sopimuksen tekemiseen ilman, että asianosaiset ovat yhtä aikaa läsnä. (KSL 6 luku 7§.)

Etämyynnissä ennen sopimuksen muodostumista kuluttajalle on annettava selkeästi määritetyt ennakkotiedot. Ennakkotietojen antamistapa säilyy ennallaan, eli tiedot esitetään selkeästi verkossa. Aiemmin vaadittuja kohtia oli 8, nyt niitä on yhteensä 21. Suurin osa 21 kohdasta löytyy vastuullisesti toimivista verkkokaupoista. Sivuilta tulee ilmetä kattavat hintatiedot, yhteystiedot, tuotekuvaukset koko tilaukselle kaikkine kuluineen sekä kattavasti kuvatut toimitusehdot. Suurimmat muutokset kuluttajansuojalaissa on tehty palautuskuluihin, palauttamiseen sekä kaupan peruuttamiseen. Kuluttajien sekä pankkien keskuudessa keskustelua on aiheuttanut vakiomuotoinen eli standardin mukainen peruutuslomake. KSL:n 6 luvun 9§:llä viitataan peruuttamislomakkeeseen. Kyseessä on kuitenkin vain lista asioista, joita tarvitaan peruutusten tekemiseen. Palautuksien sekä peruutusten tekeminen on ollut suurimpia ongelman aiheuttajia tilausansoissa, sillä kuluttajille ei ole yleensä annettu minkäänlaista kanavaa tai välinettä tehdä peruutusta ehtojen mukaisesti. (KSL 6 luku 9§.)

KSL:n 6 luvun 10§ määritellään, kuinka kaupankäyntiä suorittavien verkkosivustojen tulee tiedottaa selkeästi tilaushetkellä toimintarajoituksista ja se, miten maksut hyväksytään. Koska verkkokaupoissa tilaamiseen yhdistyy tavallisesti maksuvelvollisuus, tulee kuluttajalle ymmärrettävällä tavalla ennen tilauksen tekemistä osoittaa tuotteiden hintatiedot, toimituskulut, pääominaisuudet sekä mahdollinen sopimuksen kesto ja sopimusvelvoitteiden minimikesto. (KSL 6 luku 10§.) Nämä verkkokauppoja koskevat muutokset on selostettu EU-direktiivissä, ja ne ovat tulleet voimaan 13.6.2014 alkaen. Näiden muutoksien tarkoituksena on sovittaa yhteen säännöt EU:n alueella ja tehdä toiminta selväpiirteiseksi kauppiaille ja asiakkaille. Tilausansoja tulee Suomen markkinoille myöskin EU:n ulkopuolelta, jolloin kyseiset säännöt eivät lähtökohtaisesti toimi samojen määräysten mukaan. EU:n ulkopuolisissa maissa kuluttajan oikeudet vaihtelevat suuresti ja voivat erota paljon EU:n yhteisistä ohjeista. Erilaisten sääntöjen takia kuluttajan tulisi aina yksityiskohtaisesti selvittää, voiko tuotetta palauttaa ja mitkä ovat palautusoikeudet. Näiden lisäksi EU:n ulkopuolisista maista tilatuista tuotteista pitäisi saada selville, täyttävätkö ne EU:n ja Suomen tuoteturvallisuusmääräykset. (Tulli 2016.)

Aikaisemmin oli voimassa kuluttajan lakisääteinen palautusoikeus maksutta, mutta se ei ole enää voimassa. Tähän liittyen vaatimuksena kuitenkin on, että verkkokaupan ennakkotiedoissa palautuskulut tulee laittaa esille ymmärrettävästi kuluttajille. Tilauksen tai tuotteiden palauttaminen tulee kuitenkin tehdä 14 päivän kuluessa peruutusilmoituksen lähettämisestä. Moni kuluttaja on myös luullut, että tavaran noutamatta jättäminen ei aiheuta mitään velvoitetta ja se olisi sama asia kuin peruutuksen tekeminen. Kauppias voi hyödyntää lakia, joka liittyy palautuksiin. Toimituksista voidaan periä todennäköinen maksu, mikäli peruutusilmoitus on tekemättä ja tuote jätetty noutamatta. Tapauksia tapahtui paljon erityisesti tilausansoissa, joissa oli tilattu erilaisia kauneuteen ja hyvinvointiin liittyviä tuotteita Yhdysvalloista. (Kilpailu- ja kuluttajavirasto 2016.)

4.2.4 Asiakkaan tunnistaminen ja tietosuoja

Maksuihin liittyvien väärinkäytösten ehkäisemiseksi verkkokaupoille maksamisratkaisuja tarjoavilla yrityksillä on velvollisuus noudattaa maksajan tunnistamiselle asetettuja edellytyksiä. Verkkokaupan asiakkaiden ja kuluttajien omien tietojen päätyminen sivullisille tulee estää riittävin tietosuojajärjestelyin. (Kilpailu- ja kuluttajavirasto 2017.)

Asiakkaan vahva tunnistaminen tarkoittaa toimintaa, joka perustuu kahden tai useamman seuraavan osatekijän käyttöön – tekijät ryhmitellään hallussapidoksi, tiedoksi ja henkilökohtaiseksi omaisuudeksi:

1. jokin, jonka ainoastaan käyttäjä tietää, esim. kiinteä salasana, tunnus, henkilökohtainen tunnusluku
2. jokin, joka on ainoastaan käyttäjän hallussa, esim. tunniste, toimikortti, matkapuhelin
3. jokin, jota käyttäjä on ominaisuuksiltaan, esim. sormenjälki tai muu biometrinen tunniste.

Näiden valittujen tekijöiden on oltava lisäksi toisistaan riippumattomia, eli yhden tekijän paljastuminen ei vaaranna toista tekijää tai toisia tekijöitä. Vähintään yhden tekijöistä tulisi olla sellainen, ettei sitä voida käyttää uudelleen eikä jäljentää eikä henkilön tietämättä varastaa netin välityksellä. Kuluttajan vahvan tunnistamisen menettely pitäisi suunnitella niin, että se ei vaaranna tunnistamistietojen luottamuksellisuutta. (European Banking Authority 2014.)

Tietosuoja on käsitteenä jonkin verran harhaanjohtava. Tietosuoja-käsitteellä tarkoitetaan yksityisyyden suojaamista, ei tietojen suojaamista. Tietosuojaa valvova viranomainen, tietosuojavaltuutettu, spesifioi tietosuojan piiriin yksityiselämän suojan ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. (Tietosuojavaltuutettu.) Lakitekstien perusteella tietosuoja kuuluu perustuslakiin, jossa yksityiselä-

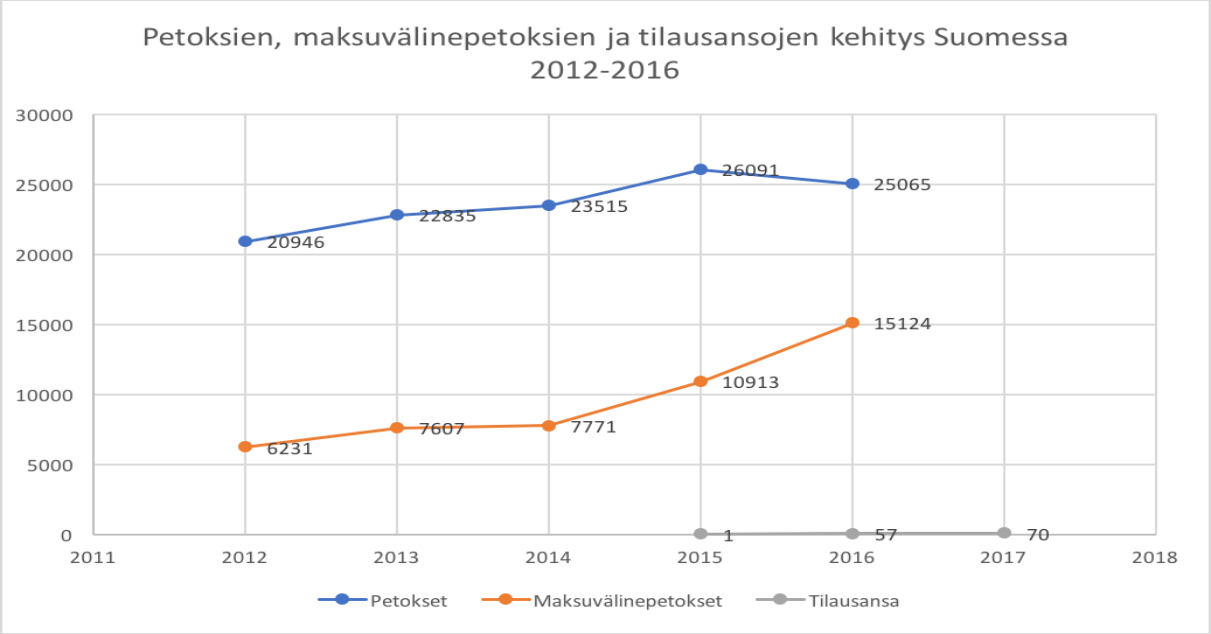
män suoja on määritelty perusoikeudeksi (PL 10§). Tietosuojalla tarkoitetaan henkilötietojen hallintaa tavalla, joka antaa suojaa henkilön yksityiselämään. Henkilötietolaki määrittää henkilötiedot ”kaikenlaisilla luonnollisilla henkilöillä tai heidän ominaisuuksiaan tai elinolosuhteita kuvaavia merkintöjä, jotka voidaan tunnistaa henkilöä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi” (HetiL 3§). Verkkokaupoissa tietosuoja ja sitä määrittelevä lainsäädäntö pitää ottaa huomioon henkilötietojen keräämisessä ja säilyttämiseen liittyvissä käytänteissä. Tietosuojalainsäädäntö säätelee kerätyn tiedon hyödyntämistä esimerkiksi markkinointitarkoitukseen.

Tietosuoja-asetuksen tietoyhteiskunnan palveluihin liittyen, lapselle suoraan palveluja tarjottaessa lapsen henkilötietojen tarkastelu on lainmukaista, jos lapsi on vähintään 16 vuotta. Alle 16-vuotiaille henkilötietojen käsittelyyn edellytetään huoltajan valtuutus tai suostumus. Tietosuoja-asetuksen 8 artiklan tarkoituksena on parantaa lasten henkilötietojen käsittelyn suojaa. Tämän on toivottava, sillä lapset eivät välttämättä tiedä kovin hyvin omien henkilötietojen käsittelyyn koskevista riskeistä, seurauksista sekä oikeuksistaan. Poikkeuksellista suojaa tarvitaan erityisesti lasten henkilötietojen käyttämiseen markkinointitarkoituksiin sekä käyttäjäprofiilien luomiseen. Sosiaalisen median palveluille ja mobiilipeleille on kuvaavaa henkilötietojen käsittelyyn koskevat käyttöehdot, jotka ovat yleensä vaikeaselkoisia ja hyvin pitkiä. Suostumalla näihin ehtoihin, annetaan yrityksille mahdollisuudet käyttää kuluttajan palveluun tuottamaa sisältöä hyväksi ja toisaalta rajoitetaan merkittävästi kuluttajan oikeuksia. (Kilpailu-ja kuluttajavirasto 2016.)

4.3 Rikokset ja rikosilmoitukset

Suomessa poliisi ei kategorisoi tilausansoja erikseen järjestelmäänsä. Tilausansa on ollut hakukelpoinen sana poliisin RIKITRIP-järjestelmässä, ja vuonna 2017 elokuuhun mennessä yhteensä tilausansa-hakusanalla löytyi rikosilmoitus 70 kertaa, vuonna 2016 yhteensä 57 kertaa ja vuonna 2015 ainoastaan kerran. Kirjaustapa vaikuttaa siihen, kuinka nopeasti nämä tiedot poistuvat poliisin rikosilmoitusjärjestelmästä.

Poliisilaitoksilla on ollut useita kirjauskäytäntöjä, kun puhutaan tilausansarikollisuudesta. Yleisesti ottaen tapahtumapaikaksi näille kirjataan usein ulkomaat. (Poliisihallitus 2017.)



Kuvio 6: Poliisille, tullille ja rajavartiolaitoksille tietoon tulleet rikokset (Tilastokeskus & Poliisihallitus)

Ulkomailla tapahtunut Suomen kansalaista, Suomessa pysyvästi asuvaa henkilöä tai näihin rinnastettavaa henkilöä taikka suomalaista oikeushenkilöä koskeva rikosasia kirjataan pääsääntöisesti sekalais-eli S-ilmoituksena. Ilmoitus kirjataan henkilön Suomessa olevan asuin- tai kotipaikan poliisin yksikköön. Lähtökohtaisesti kyseisen asian tutkinta kuuluu tapahtumapaikan maan esitutkintaviranomaiselle. (Poliisihallitus 2017.)

Verkkorikosten määrän kasvun lisäksi tapaukset ovat tulleet aikaisempaa vakavammiksi ja kansainvälisemmiksi. Määrän nopeaan lisääntymiseen on vaikuttanut todellisten rikosten määrän kasvu, mutta ilmeisesti myös rikosten saattaminen yleisemmin poliisin tietoon. Useissa tapauksissa kysymys on laajemmasta kansainvälisestä tutkimuskokonaisuudesta, josta vain osa on tapahtunut Suomessa. Verkkoon liittyvät uhat

ovat yleensä suunnitteilla tai meneillään olevia rikoksia, jolloin poliisi on toimivaltainen viranomainen. (Lardot & Kaartinen 2014.)
Maksukorttirikollisuus muuttaa rakennettaan uusien tietoturvastandardien uudistamisen myötä. Verkkorikollisuuden kasvussa on nähtävissä erityisesti etämyyntiin liittyvien petoksien kasvu. Maksuvälinetappiot kasvavat verkkokaupassa, mutta ne ovat vähentyneet kivijalkapaikoissa. Etämyyntipetosten maailmanlaajuiset organisoidut toteutukset kasvattavat tappioita ja vaikeuttavat petosten selvittämistä. Verkkokaupat ulkoistavat maksuliikennepalvelunsa usein toiseen maahan, ja pankkisalaisuuden piirissä olevien transaktiotietojen hankkiminen edellyttää pitkää ja hidasta prosessia oikeusapupyynnön myötä. Suomessa sekä muualla Euroopassa on yleistynyt tekomuoto, jossa rikolliset pyrkivät välttämään kiinni jäämistä hankkimalla suuren kokonaisrikoshyödyn valtavalla määrällä suorituksia, joissa yksittäisen teon aiheuttama vahinko on kohtuullisen pieni. Tällä tavalla toimimalla rikolliset pilkkovat toimensa niin pieniksi, etteivät ne täytä viranomaisen priorisointikriteerejä. (Keskusrikospoliisi 2013.)

4.3.1 Rikollisuuden muuttuminen digitalisaation aikana

Digitaalisuuden johdosta myös rikollisuus muuttuu ja muuntautuu. Nettipetosten ja kyberrikollisuuden volyymiksi arvioidaan vuositasolla jo satoja miljardeja dollareita maailmanlaajuisesti. Ammattimainen rikollisuus tähtää aina taloudelliseen hyötyyn, ja toiminta on usein kansainvälistä ja organisoitua. Verkossa käyttäjillä on identiteetti tai itse asiassa useita eri identiteettejä, joilla heidät tunnetaan ja tunnistetaan eri palveluissa. Identiteettivarkauksia on ollut olemassa aikaisemminkin, mutta digitaaliset identiteetit lisäävät mahdollisuuksia ja tilaisuuksia uudenlaiseen rikolliseen aktiviteettiin. Esineiden internetin ja teollisen internetin myötä myös jokaisella laitteella, sensorilla ja anturilla on oma identiteettinsä, mikä entisestään lisää välttämättömyyttä identiteetin suojaamiselle. (Ilmarinen & Koskela 2015, 225–226.)

Sosiaaliseen mediaan ja internetiin liittyvät rikokset ovat monitahoisia. Varsinaiset verkkorikolliset käyttävät sosiaalista mediaa viestintään omien sosiaalisten verkostojen kanssa. He käyttävät paljon sosiaalista mediaa toimintansa mainostamiseen ja

palveluiden myymiseen. Rikoksentekijä pyrkii hankkimaan myytäväksi kelpaavaa tietoa sieltä, mistä sitä helpoiten on saatavilla. (Lardot & Kaartinen 2014.) Onnistunut verkkorikos koostuu erilaisista joukoista osatekoja, joissa kaapataan tietoa, jalostetaan sekä muutetaan tieto tai palvelu rahaksi ja lopulta siirretään rahavarat rikoksen tilaajille (Kajantie 2010).

Tilastokeskuksen mukaan petosten määrä on ollut kasvussa koko 2000-luvun, ja etenkin viime vuosina kasvu on vain noussut. Erilaisia petoksia ilmoitettiin poliisille vuonna 2008 noin 16 000, kun vuonna 2013 luku oli jo melkein 23 000. Vuonna 2011 petosten määrästä noin 40 prosenttia oli netissä tehtyjä, mutta vuonna 2012 luku oli jo 50 prosenttia Facebookissa, jossa tilausansat tavoittavat suuria määriä kuluttajia ja huijaukset leviävät palvelun eri ominaisuuksien kautta. Facebookin sponsoroitu mainos voi ilmestyä tilaamatta uutisvirtaan tai henkilön tietynlaiseen profiiliin, ja sitä klikkaamalla käyttäjä ohjataan tilausansasivulle. (Forss 2014, 105.)

Kilpailu-ja kuluttajavirasto kertoo sivuillaan saaneensa vuonna 2017 yhteensä 1453 yhteydenottoa huijauksista ja tilausansoista. Lisääntyneitä huijauksia varten, on Kilpailu-ja kuluttajavirasto käynnistänyt Varo huijareita verkossa –kampanjan, jolla on tarkoitus kannustaa kuluttajia tarkkaivaisuuteen verkossa asioidessa. Kampanjalla on myös tarkoitus tarjota kuluttajille tietoa huijauksista ja vinkkejä välttää huijaukset ja opastaa kuluttajat ottamaan yhteyttä viranomaisiin huijauksen tapahtuessa. (Kilpailu-ja kuluttajavirasto 2018.)

Etupäässä järjestäytynyt rikollisuus on tehnyt uusia aluevaltauksia nettirikollisuuteen, jossa rikosseuraamukset ovat huumerikoksia pienemmät. Tietoverkossa riski on huomattavasti pienempi, sillä kiinnijäämisen todennäköisyys on marginaalinen. Pitkälle viety automatisointi tekee verkkorikosten toteuttamisesta myös kustannustehokasta, jolloin suurempi osa tuotosta jää rikollisille rikoshyötynä. Reaalimaailmassa sekä tietomassan prosessointi, kerääminen että riskien hallinta olisi kalliimpaa, sillä ne edellyttäisivät kalliin ja hankalan ihmistyövoiman käyttämistä. (Kajantie 2010.)

Itä-Uudenmaan poliisilaitoksen ja Tietoyhteiskunnan kehittämiskeskuksen tekemässä tietotekniikkarikoskyselyssä kysyttiin 1201 vastaajalta omakohtaisia kokemuksia rikoksista. Olennaisia poimintoja kyselyssä oli muun muassa se, että vastaajista 4,2 prosenttia ilmoitti, että nettipalveluun syöttämiä luottokorttitietoja oli jokin taho käyttänyt väärin. Sosiaalisen median palveluun liittyvää käyttäjätiliä oli käytetty luvatta 17,7 prosentin kohdalla. Vastaajista 95,4 prosenttia ilmoitti, että ei ollut kohdannut taloudellisia vahinkoja, kun vastaavasti 0,8 prosenttia ilmoitti menettäneensä yli 2000 euroa. Vastaajista 93,3 prosenttia ilmoitti, että ei ollut tehnyt rikosilmoitusta häneen kohdistuneesta rikoksesta. Yleisesti tätä selitettiin sillä, että ei uskottu poliisin kykyyn selvittää näitä rikoksia, ei haluttu joutua mahdollisen tutkinnan ja oikeusprosessin osapuoleksi, ei koettu joutumista rikoksen uhriksi ja rikos tai siitä aiheutunut vahinko oli kuluttajien mielestä liian vähäinen. (TIEKE 2012.)

Alla mainitut uhat ja trendit on määritelty useiden ammattilaisten toimesta, johon rikollisuuden trendit ja uhat suuntautuvat. Ensinnäkin rikollisten määrä kasvaa ja kyberrikoksen tekemisen kynnys madaltuu. Kyberrikospalveluiden kysyntä kasvaa, mikä johtaa haittaohjelmien testaukseen, kehittämiseen ja jakelun voimakkaaseen kasvuun, bottiverkkojen rakentamiseen, maksukorttien tietojen varkauksiin ja niiden kauppaamiseen sekä rahanpesupalveluihin. Asiantuntemus tietoverkoissa lisääntyy, ja sen myötä kehitetään entisestään monimutkaisempia ja aggressiivisempia haittaohjelmia. Kyberrikollisuus globalisoituu entisestään internetin laajentumisen ja nopeuksien kasvamisen myötä. Kasvu tulee lisääntymään erityisesti Kaakkois-Aasiassa, Etelä-Amerikassa ja Afrikassa. Mobiililaitteiden määrän kasvaessa haittaohjelmistojen kehittämisen painopiste siirtyy mobiililaitteisiin, ja tämän avulla rikokset tulevat myös lisääntymään pilvipalveluihin kohdistuvissa rikoksissa. Rikolliset pyrkivät useammin murtautumaan pilvipalveluihin vakoillakseen ja saadakseen maksukorttitietoja. Rikoksen avulla hankitun rahan pesuntarve lisääntyy myös. Pienien summien peseminen pk-yritysten ja useiden ihmisten kautta tulee lisääntymään. Myös sähköisten valuuttojen ja nimettömien maksujärjestelmien kysyntä rikollispiireissä kasvaa. (Peltomäki & Norppa 2015, 118–119.)

4.3.2 Tietojenkalastelu

Tietojenkalastelu tarkoittaa henkilötietojen tai muun sensitiivisen tiedon saamista toiselta henkilöltä rikolliseen tai muuhun väärinkäytön tarkoitukseen. Tyypillinen huijaus sisältää yleensä sähköpostiviestin, joka vaikuttaa tulleen yleensä finanssilaitokselta tai muulta tunnetulta yritykseltä, jossa kysytään tilinumeroita, korttitietoja tai muita tietoja, joita rikollinen voi hyväksikäyttää rikoksen tekemiseen. (Schmalleger & Pittaro 2008, 191–192.)

Kalastelusivun URL-osoite on usein pyritty luomaan alkuperäistä vastaavaksi. Viestit näyttävät usein asiakaspalvelun tai muualta yrityksestä saapuneilta, koska ne on luotu näyttämään erehdyttävästi oikeilta nettisivustoilta, osin rakentamaan luottamusta lähettäjästä (liite 1) ja (liite 2) kuluttajan suuntaan. (Forss 2014, 108.)

Oikealta näyttävien kalastelusivujen tekeminen on suhteellisen helppoa. Kuluttaja on myös luonteeltaan usein hyväuskoinen ja siten hyvä kohde rikokselle. Tämä yhdistelmä on rikolliselle äärimmäisen houkutteleva ja helppo työkalu, jolla erilaisia huijauksia, petoksia tai suurempia rikoskokonaisuuksia voidaan suorittaa. Tietojenkalastelu on usein ensimmäinen vaihe onnistuneen hyökkäyksen suorittamisessa. Valtaosa tietojenkalastelusivustoille johtavista linkeistä levitetään sähköpostin avulla. Myös sosiaalisessa mediassa, kaupallisilla sivustoilla sekä piraattisivustoilla olevia bannereita on käytetty tietojenkalastelun tarkoituksessa. Huijarit voivat saada nämä edellä mainitut paikat näyttämään hyvin aidoilta, joten niitä voi olla hyvin vaikea havaita rikollisessa mielessä tehdyiksi. Tietojenkalastelun avulla kerätään tarvittavia tietoja, käyttäjätunnuksia, pankkitunnuksia sekä maksukorttitietoja. (Viestintävirasto 2017.)

Tietojenkalastelu on hyvin yleistä ja kasvaa entisestään tulevaisuudessa, koska se toimii hyvänä väylänä. Ihmiset antavat hyväuskoisesti tietojaan huijareille kyseenalaistamatta viestin alkuperää ja tarkoitusta. Kaikkia digitaalisuuden muotoja huijauksissa on olemassa, sillä tietoja kalastellaan myös tekstiviestein ja suoraan puhelimitse ja huijarit esiintyvät sosiaalisen manipuloinnin keinoin viranomaisina tai

minkä tahansa yrityksen edustajina. (Hietanen 2015.) Huijaukset ovat kautta aikojen perustuneet ihmisten hyväuskoisuuteen. Yksinäisyys, empatia ja halu tehdä helppoa rahaa ovat asioita, joihin rikolliset vetoavat tehdessään huijauksiaan. Moni huijari hyödyntää myös ajattelemattomuutta: pienellä printattu tai sivuun sijoitettu teksti jätetään usein huomioimatta, ja uhri sitoutuu sen enempää asiaa miettimättä tietyn palvelun kestotilaajaksi. Osa uhreista ilmoittaa verkkohuijauksista poliisille, mutta osa kärsii tappion nahoissaan, koska ei yksinkertaisesti kehtaa myöntää tulleensa huijatuksi. Huijatuksi tuleminen koetaan edelleenkin usein häpeäksi. (Haasio 2013, 46.)

4.3.3 Maksuvälinepetokset

Maksuvälinepetos on rikos, jossa tekijä käyttää toisen maksuvälinettä ilman lupaa tai oikeutusta. Tuomitsemisen edellytyksenä on lisäksi, että tekijän tarkoituksena on hankkia taloudellista hyötyä. Hyödyn ei tarvitse tulla välttämättä tekijälle itselleen, vaan rikoksella voidaan myös hyödyttää toista. Rikokseen syyllistyy myös luottorajan ylittävä laillinen käyttäjä, mikäli hän aiheuttaa ylityksellä vahinkoa. Tällöin rankaisemisen edellytyksenä on, ettei hänen ole ollut tarkoitusta korjata vahinkoa. Maksuvälinepetoksesta on säädetty myös törkeän ja lievän muoto. Rikoksen rangaistusasteikko on joko sakkoa tai vankeutta. Vankeuden ajanjakso voi vaihdella 14 päivän ja 2 vuoden välillä. (Minilex.)

Jos maksuvälinepetoksissa maksukorttien oikeudettomaan käyttöön liittyvä törkeä maksuvälinepetos ja törkeä kätkentä tulee ilmi, poliisilla on mahdollisuus tuomioistuimen määräyksestä suunnata epäillyn käyttämiin verkko-osoitteisiin televalvontaa. Yleensä tässä vaiheessa poliisilla ei ole enää tietoteknistä jälkeä käytettävissä, joten sitä voisi rinnastaa siihen, että valvontakamera laitettaisiin päälle vasta pahoinpitelyn jälkeen. (Kajantie 2010.)

Poliisille ilmoitetut rikokset koko maassa

Ilmoitettu Kpl	2011	2012	2013	2014	2015	2016	2017 01-07
LIEVÄ MAKSUVÄLINEPETOS	458	548	788	946	1 581	2 754	636
MAKSUVÄLINEPETOKSEN VALMISTELU	13	19	19	22	26	24	16
MAKSUVÄLINEPETOS	5 053	5 546	6 690	6 699	9 199	12 195	3 036
TÖRKEÄ MAKSUVÄLINEPETOS	147	126	122	123	194	161	123
Yhteensä	**5 671**	**6 239**	**7 619**	**7 790**	**11 000**	**15 134**	**3 811**

Taulukko 2: Poliisille ilmoitetut rikokset koko maassa

Maksuvälinepetoksiin kuuluu muitakin tekotapoja kuin korttirikoksia, esimerkiksi sekkien väärentäminen. Tämä rikollisuuden laji on kuitenkin sen verran vähäistä, että tilastosta voidaan päätellä nimenomaan maksukorttirikosten kehitystä. Tilastonousuihin vaikuttaa niin rikollisten, poliisien kuin kansalaistenkin aktiivisuus. (Poliisi.) Poliisin luetteloissa näkyvä selkeä piikki vuodesta 2015 alkaen selittyy osin sillä, että pankit ohjeistivat asiakkaittaan tekemään tilausansoihin liittyvistä reklamaatioista myös rikosilmoituksen poliisille.

Maksuvälinepetokset tekopaikan mukaan

Tekopaikka	2015	2016	2017 01-08
Kiinteistö	26,91%	20,06%	37,75%
Ulkoalue	2,44%	2,51%	4,73%
Kulkuväline tekopaikkana	0,40%	0,51%	1,22%
Internet	70,25%	76,91%	56,30%
Tekopaikka	**100,00%**	**100,00%**	**100,00%**

Taulukko 3: Maksuvälinepetokset tekopaikan mukaan

Internetissä tapahtuvien maksuvälinepetoksien osalta selvittämisen kannalta tärkeätä on IP-osoite. IP-osoite tarkoittaa sellaista numerosarjaa, joka yksilöi jokaisen internetiin kytketyn päätelaitteen. Toisaalta erilaiset VPN-yhteydet ja TOR-verkko tarjoavat internetin käyttäjille anonymiteettiä, jolloin myös rikollisilla on aiempaa parempi ominaisuus häivyttää omat jälkensä verkossa. (Helopuro, Perttula & Ristola 2009, 290–293.)

Järjestäytyneen maksukorttirikollisuuden analysoimisessa, torjunnassa ja ymmärtämisessä on tärkeätä ottaa huomioon ilmiön kansainvälinen, rajat ylittävä luonne. Useimmat maksu- ja luottokortit ovat kansainvälisiä maksuvälineitä, jotka on tuotu markkinoille sitä varten, että kuluttajat voivat hyödyntää niitä globaalisti. Maksukorttidata kiertää maapallon muutamassa sekunnissa, mutta jälkikäteen ilmi tulleen maksukorttirikoksen kansallisessa tutkinnassa tarvittavat tiedot ovat usein pankkisalaisuuden piirissä, ja niiden saaminen toisesta maasta edellyttää usein oikeusapupyyntöä. Laillisen yritystoiminnan piiristä opitut riskien hajauttamiset toimivat nykypäivänä myös rikollisessa maailmassa. Maksukorttirikollisuudessa on kyse suurimittaisesta rikollisesta toiminnasta, jonka muun muassa Europol arvioi vuonna 2010 aiheuttaneen pelkästään Euroopan unionin alueella noin 1,5 miljardin euron vuosittaiset tappiot. (Poliisi.)

4.3.4 Petoksen luonne

Usein on helpompi nähdä tärkeitä hahmoja, kun todisteita kerätään laaja-alaisesti. Mitä opimme petoksesta, kun tarkastelemme sitä evolutiivisessa viitekehyksessä. Petosta tutkitaan evolutiivisesti siten, että sen kaikkia muotoja tarkastellaan ja etsitään samanaikaisesti yleisiä periaatteita. Tähän mennessä petoksen muotoja on löydetty erittäin paljon ja periaatteita erittäin vähän. Uudet keinot leviävät nopeasti, koska määritelmän mukaan niiden vastaisia puolustuksia ei ole. Tästä alkaa petkuttajan ja petkutettavan niin sanottu koevolutiivinen kamppailu, joka käydään evolutiivisessa ajassa. (Trivers 2011, 44.)

Psykologia on opettanut meitä yli vuosisadan Sigmund Freudin ja Daniel Kahnemanin tyyliin ja sisältöön liittyvillä asioilla, että ihmiset tekevät usein päätöksiä, jotka eivät ole heidän edun mukaisia. Ihmiset eivät tee sitä, mikä on heille oman edun mukaista, eivätkä he valitse, mitä todella haluavat. Tällaiset huonot päätökset antavat heille mahdollisuuden tulla huijatuksi. Tämä totuus on niin perustavanlaatuista, että sitä voi verrata Raamatun ensimmäiseen tarinaan, jossa käärme laittoi viattoman Eevan tekemään päätöksen hetkessä, jota hän lopulta katui koko loppuelämänsä. (Akerlof & Shiller 2015, 1–2.)

Petoksen havaitseminen menestyy hyvin, kun petos on yleistä, mutta ei silloin, kun se on harvinaista. Tämä tarkoittaa sitä, että petkuttaja ja petkutettava ovat juuttuneet kehämäiseen suhteeseen siinä mielessä, että kumpikaan ei voi ajaa toista sukupuuttoon. Ajan mittaan petkuttajan ja petkutettavan suhteelliset frekvenssit heilahtelevat, mutta tämä tapahtuu sellaisen rajojen sisällä, että kumpikaan ei katoa. Vastaavalla tavalla itsemme kaltainen verbaalinen laji varoittaa muita uusista tempuista sitä useammin, mitä yleisemmiksi temput tulevat. Parantuneet älylliset kyvyt valikoivat syvällisempiä pettämisen keinoja, jotka vuorostaan valikoivat parempia petoksen havaitsemiskykyjä. Toisin sanoen petos valikoi jatkuvasti petettävän mentaalista kykyä. Koska ymmärrettävä lähde liikkuu eli kehittyy kauemmaksi petettävän kyvystä havaita se, alati uudenlaiset erottelukeinot lisääntyvät. Kyky paljastaa petos edellyttää erityisiä taitoja, jotka eivät ole välttämättömiä sellaisen kohteen erottelussa, joilla ei ole kykyä piiloutua. Niinpä petos on luultavasti ollut merkittävä tekijä älykkyyden kehityksessä, ainakin erittäin sosiaalisilla lajeilla. (Trivers 2011, 51–52.)

4.4 Tilausansat

Liian hyvältä kuulostava tarjous on useimmiten huijaus. Tilausansoiksi kutsutuissa huijauksissa pyydetään yleensä yhden euron maksu, jotta kuluttajaa voidaan pyytää syöttämään korttitiedot. Oleellista ei ole siis ilmoitettu tuotteen hinta, vaan ainoa päämäärä on saada kuluttajan korttitiedot ja päästä veloittamaan korttia. Kun asiakas syöttää korttitiedot, kuluttaja sitoutuu ja hyväksyy myös ehdot, joissa sitoutuu johonkin kestotilaukseen. Esimerkkinä voisi käyttää treffipalveluita, kosmetiikkaa

sekä pilvipalveluita, joissa käyttäjä sitoutetaan huomaamatta suoratoistopalvelun asiakkaaksi kalliilla kuukausimaksulla. Yleensä näistä suoratoistopalvelusopimuksista on erittäin vaikea päästä irti, ja irtisanomisen prosessi on tehty asiakkaalle hyvin vaikeaksi. Näissä tilausansan houkuttimena olevaa tuotetta ei koskaan lähetetä, vaan se saatetaan arpoa yhdelle asiakkaalle tai korvata jollain toisella huomattavasti arvottomammalla tuotteella

Kuvio 7: Tuotteita mitä tilausansoissa on markkinoitu kuluttajille (Enforcement and European Consumer Centres 2016)

4.4.1 Historiaa

Vuodesta 2012 lähtien tilausansoja on tullut joka vuosi lisää. Jotkin veloittajat saattoivat vaihtaa yrityksen nimeä, mutta toimintatapa säilyi koko ajan samanlaisena. Tilausansat alkoivat vaikuttaa suomalaisiin kuluttajiin ensiksi Yhdysvaltojen suunnalta, josta tuli paljon kosmetiikkaan ja erityisesti laihduttamiseen liittyviä tilausansahuijauksia. Nopeasti tämän jälkeen ilmiö kasvoi kuukausi kuukaudelta, ja Tanskaan liittyvät huijaukset lisääntyivät nopeasti. Ilmiössä huomattiin myös tuotteiden vaihtuminen fyysisistä tuotteista digitaalisiin palveluihin. Tämä osittain sen takia, että

yritykset halusivat tehdä prosessinsa mahdollisimman joustavaksi sekä välttää chargeback-toimeksiantoja. Erityisesti Facebookissa tilausansat saivat aluksi toimia vapaasti ja niiden tutkinta oli suhteellisen vaikeata. Tutkinnoissa huomattiin, että kohdennetut mainokset ilmestyivät vain tiettyihin profiileihin, erityisesti vanhempiin ikäluokkiin.

Veloittaja	Ehdot/nettisivut	Yhteystiedot	Lisätietoa
Jobform	http://www.jobform.com/fi/home/terms		
Radioplanets	http://radioplanets.com/terms	Info.fi@RadioPlanets.com	
Quizonaut	http://fi.quizonaut.com/terms.asp		
Forburgerpost	http://www.forbrugerpost.dk/terms.asp		
Help24care.com	http://www.help24care.com/	help@hurraflix.com	(laskuttajasivusto)
Jbmember.com	http://jbmember.com/		veloittajana Jukebux
cscfee.com	http://cscfee.com/terms/		maksunvälittäjä
HQbill	www.hqbill.net	support-suomi@hqbill.net	veloittaa seuraavien palvelumaksuja: www.badults.fi, www.datebeach.fi
mr.cal365.com	https://fi.campaign.mrcal365.com/terms.aspx?campaign=6		online kalenteri
Transfer safe	https://transfersafe.net/#/		tiedostojen siirto palvelu
Pointworld	http://pointworld.com		

Taulukko 4: Yleisimmin toistuvat tilausansat

4.4.2 Toimintatapa

Huijarisivustojen kautta luvataan kaikkea mahdollista. Uhreja näillä sivustoilla on jo tuhansia. Facebookissa suomalaisia tuotetestaajia käyttävillä sivustoilla on ollut monia erilaisia tarjouksia. Useimmat näistä yrityksistä ilmoittavat postiosoitteeksi Tanskan, mutta itse tutkiessani tapauksia sain selville, että esimerkiksi Jobform.com on rekisteröity Yhdistyneisiin arabiemiraatteihin, Jobform.comin IP-osoite oli rekisteröity Thaimaahan ja kuluttajariidat käsiteltiin niiden omien ehtojen mukaisesti Hongkongissa.

Jatkuvassa veloituksessa on kyseessä internetistä tehty tilaus, joka uusitaan määräajoin. Palvelu voi olla esimerkiksi jatkuva pääsy jollekin sivustolle tai osallistuminen kilpailuun tai kyselyyn. Yleensä asiakas on tilausta tehdessä huomaamatta sitoutunut jatkuvasti tapahtuvaan veloitukseen. Jatkuva veloitus toimii niin, että liike veloittaa ilmoitetulta kortilta maksun kuukausittain, joskus myös vuosittain. Veloituksen aikataulu määräytyy tilatun palvelun mukaisesti. Joissakin tapauksissa jonkin sivuston käytön ensimmäiset päivät ovat maksuttomia. Jos tilausta ei tämän määräajan sisällä peruuta, tulee sivustolta kuukausittain veloitus. Toimintamalli on kaikissa tapauksissa lähes samanlainen. Internetissä, sähköpostissa tai Facebookissa on ollut mainos, jossa on tarjottu esimerkiksi Niken lenkkitossuja tai laihdutuspillereitä kahden euron toimitusmaksun hinnalla. Tervetuliaislahjan saadakseen on pitänyt vastata kyselyyn, joka on ollut yleensä vähintään viiden sivun mittainen. Ennen vastaamista on hyväksyttävä pienellä painetut ehdot, joiden mukaan asiakas sitoutuu kahden euron lahjan tilaamalla 40–80 euroa kuukaudessa maksavaan jäsenyyteen. Asiakkaat eivät ole saaneet luvattuja tuotteita, mutta luottokortilta on mennyt ensin kahden euron ja myöhemmin 40–80 euron veloituksia.

Toistuvasti veloittajia on useita, mutta ongelmana on ollut erityisesti Jobform.com, WeKeepItSafe, Pointworld sekä Jukebux. Erityisesti Jobform.comin kohdalla volyymit ovat olleet todella suuria. Tutkiessani Jobform.comin huijauksia huomio kiinnittyi erityisesti osallistumissivun (liite 4) asetteluun. Tavallisella pöytätietokoneella tai kannettavalla sivun harmaa osuus, jossa kerrotaan maksuehdoista, on näkyvissä.

Jos sivun ottaa esiin tabletilla tai mobiililla, harmaa osa ei tule esille, mikäli ei ymmärrä vierittää sivua alaspäin. Tämän sivun jälkeen tulee esille sivu, johon syötetään korttitiedot (liite 5). Tässä sivussa selvästi annetaan ymmärtää, että maksu on vain 2 euroa eikä muita maksuja veloiteta puhumattakaan kuukausiveloituksista. Maksukorttien turvallisuusasiantuntijana huomio kiinnittyy myös muualle sivun turvallisuuteen. Sivusto on https://, mutta kuinka turvallisesti korttitietoja käsitellään, siitä ei ole varmuutta. Sivustoilla ei ole 3D-secure-toimintoa, jotta asiakas voisi varmistua turvallisesta korttitietojen käsittelystä. Tutkinnan alla on ollut myös se, päätyykö sivustoilta korttitietoja TOR-verkon cardaus-sivustoille, mutta tähän ei ole saatu täydellistä varmistusta.

Jatkuvaveloituksissa asiakas on usein tietämättään sitoutunut siihen, että veloittaja veloittaa kuukausittain saman summan ns. jäsenmaksuna. Jobform.com ilmoittaa, ensimmäinen jäsenmaksu 40 euroa menee viisi päivää siitä, kun asiakas on liittynyt palveluun ja antanut korttitietonsa. WeKeepItSafe ilmoittaa ehdoissaan, että hyväksymällä veloituksen asiakas saa seitsemän päivän ajan kokeilujäsenyyden 1,00 euron hintaan. Lisäksi asiakas hyväksyy, että jäsenyys uusiutuu automaattisesti. Jäsenyys ei maksa 1,00 euroa enempää ensimmäisten seitsemän päivän ajan, jota pidetään koeaikana. Jos asiakas ei halua jatkaa jäsenyyttä koeajan jälkeen, jäsenyys täytyy peruuttaa ennen seuraavaa maksupäivää. Koeajan loppumisen jälkeen jäsenyys maksaa 1,30 euroa päivässä, ja se veloitetaan kerran kuukaudessa (30 päivää 39,00 eurolla), kunnes asiakas peruuttaa jäsenyyden. Eräs tutkimani tapaus on hyvä esimerkki siitä, kuinka yrityksillä ei ole tarkoitustakaan lähettää asiakkaille minkäänlaisia yhden euron tuotteita. Tässä yrityksessä jäsenyyslahjana oli Android-tabletti ja palveluun liityttiin 5.5.2014. Linkki lahjan lunastamiseen oli erillisessä palvelussa (giftcable.com), ja se ilmoitettiin sähköpostiin tulleella viestillä. Tilausansayrityksillä on myös tarkoituksena naamioida sähköposti roskapostiksi, jotta se mahdollisesti ohjautuisi kuluttajan roskapostikansioon. Näin tehdään sen vuoksi, että kuluttajan olisi se vielä hankalampi havaita ja vastata sähköpostiin määrätyssä ajassa.

8.5 asiakirjat hyväksytty giftcable.com palvelussa. Syntymäaika piti vahvistaa erikseen passi tai henkilökortin kopiolla. Eli piti skannata heille materiaalit
9.5. jäsenyys irtisanottu
12.5 ehdotettu lahjan vaihtamista yrityksen puolelta (kieltäydytty)
15.5 yritys kysynyt vahvistusta kotiosoitteesta. Piti lähettää sähkö tai puhelinlasku
18.5. yritys tarjonnut Amazonin 20€ lahjakorttia (kieltäydytty)
20.5 tilaus kuulemma käsitelty ja lahja lähetetään muutamassa päivässä
26.5. kyselty missä lahja menee
28.5. yritys vastannut, että lahja tulee mahdollisimman pian
16.6 viimeisin kysely. Vastasivat 19.6 etteivät voi antaa tarkkaa aikataulua mutta lahja tulee mahdollisimman pian

Taulukko 5: Tilatun tuotteen seuranta

Tilausansoista on nähty myös kehittyneempiä versioita, huijauksia joissa on kaapattu henkilöiden identiteettejä sekä tunnettujen yritysten brändejä. Pointworldin nimissä oli tehty kuvitteellinen Ilta-Sanomien artikkeli (liite 7), joka todellisuudessa oli huijaussivusto. Huijausartikkelissa kerrottiin, kuinka Apple teki yhteistyötä Pointworldin kanssa jakaessaan yhdellä eurolla iPhone-puhelimia. Artikkelin tarkoitus oli henkilöhaastatteluin ja käyttökokemuksien avulla (liite 8) luoda lukijalle luottamus palveluun ja siihen, että sijoittamalla yhden euron saa puhelimen itselleen. Artikkeli oli hyvin ammattimaisesti tehty ja sitä tutkiessa ilmeni, kuinka lukijoiden kommentteja myöden (liite 10) yksityiskohdat oli mietitty tarkasti. Normaalisti tietojenkalastelu-viestit ovat ainakin osittain olleet huonolla suomen kielellä kirjoitettuja, mutta tässä huijauksessa suomen kieli oli lähestulkoon täydellistä. Pointworld on myös ison S-Ryhmän nimissä kiertävän tilausansa huijauksen takana, jota levitetään mm. sivun http://prisma500.org kautta.

Erityisesti tilausansojen alkuvaiheessa moni yritys tarjosi markkinoinnissa fyysisiä tuotteita. Tämä kuitenkin johti monen yrityksen kohdalla ns. chargeback-käsittelyyn issuer-pankkien toimesta, koska ne eivät lähettäneet markkinoituja tuotteita kuluttajille. Välttääkseen korttijärjestöjen VISAn sekä Mastercardin chargeback-prosessit

yritykset siirtyivät palveluihin tai digitaalisiin sisältöihin. Näiden ansiosta pystyttiin kiertämään chargeback-prosessiin joutuminen ja toiminnan jatkumista pystyttiin jatkamaan pidempään.

Muutamia tilausansayrityksiä lopetti toimintansa tietyn ajan kuluttua, ja tutkimuksien mukaan tämä johtui osittain kasvaneista chargeback-tapauksista. Tilausansayritykset vaihtoivat tämän takia yleensä acquirer-pankkia ja yrityksen nimeä. Toiminta jatkui pienen hiljaiselon jälkeen kuitenkin lähes identtisillä nettisivuilla ja tuotteilla. Yritys saa tällä tavalla aloittaa puhtaalta pöydältä, sillä korttijärjestöt eivät valvo acquirer-pankin vaihtoa.

4.4.3 Kuinka varautua tilausansaan

Tilausehdot tulisi lukea huolella, myös pienellä kirjoitettu teksti. On mahdollista, että kuluttaja tilausta tehdessään saattaa sitoutua jatkuvasti tapahtuvaan veloitukseen. Kuluttajan pitää saada itselleen kirjallinen todiste palvelun peruutuksesta. Kuluttaja voi tehdä sen esimerkiksi tulostamalla tai tallentamalla lähettämänsä peruutuksen ja/tai ilmoituksen hyväksytystä peruutuksesta. **P**eruutus on tehtävä ennen veloituspäivää tai ennen kokeiluajan umpeutumista. Ehtoja hyväksymättä tilauksessa ei voi yleensä edetä. Mikäli minkään tuotteen tilauksen yhteydessä ei ole luettavissa ehtoja, joissa selkeästi kerrotaan kuluista, maksuista, tilauksen peruuttamisesta ja siitä aiheutuvista kuluista, ei tuotetta tulisi tilata. Kuluttajan pitäisi myös ottaa selvää jo ennen tilausta, minne voi olla yhteydessä, mikäli haluaa reklamoida tuotteen tai irtisanoa jäsenyyden. Jokainen rehellinen kauppias ilmoittaa edellä mainitut asiat selkeästi. Mikäli ei ymmärrä ehtoja, ei tuotetta tulisi tilata. Mikäli kuluttaja on jo tehnyt tilauksen, josta veloitetaan jatkuva maksu, ja haluaa sen peruuttaa, kuluttajan velvollisuus on ilmoittaa asiasta veloittajalle. Tuotteen tilauksesta yleensä lähetetään sähköpostiin vahvistus. Mikäli kuluttajalla ei ole muita yhteystietoja, kuluttajan tulisi vastata vahvistukseen ja ilmoittaa, että haluaa peruuttaa jäsenyyden välittömästi. Kuluttajan pitää säilyttää kopio lähettämästään sähköpostista. Mikäli veloitukset jatkuvat irtisanomisen jälkeen, voi kuluttaja olla yhteydessä kortinmyöntäjään. Kuluttajan velvollisuus on tarkastaa lasku ja tiliote

huolellisesti joka kuukausi. Mikäli havaitsee siellä epäselvyyksiä, pitää ottaa yhteyttä kortinmyöntäjään välittömästi, vaikka kyseessä olisi pienikin tapahtuma. (Korttiturvallisuus.fi.2012)

Korttipalveluita tarjoava Nets Group tarjoaa Norjassa, Tanskassa, Suomessa ja Ruotsissa pankeille palvelua, jolla pyritään estämään tilausansayritysten veloitukset. Palvelu perustuu siihen, että järjestelmä analysoi dataa jatkuvasti ja veloittajia, summia ja toistuvia kaavoja, jotka ovat tyypillisiä tilausansayritykselle. Mainittu kaava voi olla esimerkiksi ensi pieni muutaman euron veloitus, jota seuraa yleensä saman veloittajan useiden kymmenien eurojen veloitus muutamien päivien päästä. (Nets Group 2017.)

Netsin arvion mukaan jopa 25% kaikista Pohjoismaiden reklamaatiotapauksista voi johtua tilausansoista. Tarkkaa lukua on kuitenkin vaikea arvioida, koska suuri osa kuluttajista ei raportoi tapahtumista pankille tai poliisille. Erityisesti Norjassa Nets on saanut palvelusta rohkaisevia lukuja. Vuonna 2016 aloitettu palvelu on estänyt noin 100 asiakkaalta yli 31 000 veloitustapahtumaa yhteisarvoltaan yli 1,8 miljoonaa euroa, ja kaikki tämä noin neljässä kuukaudessa. Korttireklamaatioiden ilmoitukset vähenivät samassa ajassa noin 20 prosenttia. Koska tilausansayritykset muuttavat koko ajan nimiään, korttipalveluita tarjoavia pankkejaan sekä muita tunnisteita, on datan jatkuva analyysi tilausansojen ennalta ehkäisemiseksi välttämätöntä. (Nets Group 2017.)

Nets Groupin tarjoama palvelu pankeille ja muille kortinmyöntäjille asettaa kuluttajat eriarvoiseen asemaan, sillä asiakas ei voi tietää, käyttääkö oma kortinmyöntäjä Netsin palveluita vai ei. Tietojeni mukaan suomalaisilla pankeilla ja kortin myöntäjillä on hyvin vaihtelevia toimintatapoja korttitransaktioiden seurantaan ja ennalta ehkäisyyn. Osalla toimijoista monitorointi on laajamittaista, tehokasta ja suunnitelmallista. On kuluttajan itsensä vastuulla selvittää, minkälaisia turvapalveluja oma kortinmyöntäjä tarjoaa ja suosittelee erilaisiin tilanteisiin. Kuluttajia valistetaan myös turvallisesta kortin käyttämisestä viranomaisten, issuer- ja acquirer-pankkien toimesta yhteisellä www.korttiturvallisuus.fi-sivustolla.

EU:ssa on myös mietitty, kuinka torjua kyseisenlaista rikollisuutta. Euroopan komissio julkaisi 17.3.2017 lehdistötiedotteen, jossa se toi esille sosiaalisen median vastuuta rikostorjunnassa petoksia vastaan. EU oli huolissaan siitä, että toimijat eivät noudattaisi EU:n sääntöjä, joilla suojellaan kuluttajia epäoikeudenmukaisilta käytännöiltä. EU ei myöskään hyväksy sitä, että kuluttajat EU:n alueella joutuisivat turvautumaan Yhdysvaltojen tuomioistuimiin ratkaisemaan riita-asioita. Sosiaalisen median yritysten on otettava enemmän vastuuta huijauksista ja petoksista, jotka tapahtuvat heidän alustoillaan. Sosiaalisen median yritysten on poistettava verkkosivustoiltaan petokset ja huijaukset, jotka voivat johtaa kuluttajia harhaan, kun he ovat tietoisia tällaisista käytänteistä. Tässä yhteydessä kansallisilla kuluttajansuojaviranomaisilla pitäisi olla suora ja standardoitu viestintäkanava, joka ilmoittaa tällaisista väärinkäytöksistä sosiaalisen median operaattoreille. Seuraavassa on lueteltu petoksien ja huijauksien tyyppejä, joihin EU vaatii sosiaalisen median yrityksiltä toimia:

- Huijaukset, joihin liittyy maksuja kuluttajilta
- Tilausansoja, joissa kuluttajille tarjotaan rekisteröitymistä ilmaiseen kokeiluun, mutta niille ei anneta selkeää ja riittävää tietoa.
- Väärennettyjen tuotteiden markkinointi.
- Väärennetyt kampanjat, joihin on kytketty euron tuote, mutta todellisuudessa on piilotettu pitkäaikainen jäsenyys, jossa on mahdollisuus menettää useita satoja euroja. (Euroopan komissio 2017.)

4.4.4 Tilausansojen piirteet Suomessa sekä Euroopassa

Ruotsin kuluttajavirasto ja Euroopan kuluttajavirasto tekivät 27.2.–7.3.2017 kvantitatiivisen tutkimuksen, joka koski kuluttajien kokemuksia tilausansoista kuudessa eri EU-maassa (Ruotsi, Suomi, Hollanti, Belgia, Itävalta ja Norja). Tutkimuksissa pyrittiin löytämään tapauksien taustalla oleva ilmiö ja kartoittamaan sen laajuus. Tutkimuksen tarkoituksena oli saada selvyys, kuinka laajasta rikollisuuden lajista on kysymys. (Theorell 2017, 2.)

Tutkimuksessa haastateltiin yhteensä 6112 kuluttajaa, joiden ikäjakauma oli 18–75 vuotta. Tutkimuksen myötä kävi selväksi, kuinka erityisesti Ruotsissa ja Suomessa kuluttajat törmäsivät joka viikko ns. ”liian hyvä ollakseen totta” -tarjouksiin netissä ja sosiaalisessa mediassa. Tutkituista kuluttajista hollantilaiset ja belgialaiset tilasivat eniten ”liian hyvä ollakseen totta” tuotetta/palvelua, joka myös johti ei-toivottuihin sopimuksiin heidän osaltaan. Ikäjakauman kannalta tällaisiin tarjouksiin sortuu nuoria aikuisia (18–29-vuotiaat) eniten Hollannissa ja Belgiassa. 60–75-vuotiaat olivat taas riskialtteimpia tilausansoille Ruotsissa. Kaikista vastaajista, suurin osa sanoi ottaneensa veloittajaan jollakin tavalla yhteyttä. Näissä ilmoituksissa kuluttajat ilmoittivat veloittajalle, että he eivät olleet liittyneet mihinkään tilaukseen, tai olivat suoraan yrittäneet perua tilausta. Monet kuitenkin lopulta tyytyivät maksamaan veloitetun summan tilausansayritykselle. Kaikista vastaajista noin 10 prosenttia ilmoitti ottaneensa yhteyttä pankkiin tai luottolaitokseen tekemällä reklamaation kiistetyistä veloituksista. Keskimäärin kuluttajat sanoivat menettäneensä 115,70 euroa tilausansayrityksille viimeisen kolmen vuoden aikana. (Theorell 2017, 6–8.)

Tutkimuksen mukaan eroja näkyy siinä, minkälaisiin houkutteleviin tarjouksiin ihmiset tarttuvat. Miehet huomaavat paremmin tilausansoja, joissa mainostetaan tabletteja, matkapuhelimia tai virustorjuntaohjelmia. Naiset taas huomaavat paremmin mainokset, jotka liittyvät ruokavalioon, laihduttamiseen tai kauneudenhoitoon. Rahallisesti naisten ja miesten tilausansat eroavat merkittävästi. Miehet menettävät keskimäärin 147 euroa, kun taas naisten keskimääräinen tappio oli 74 euroa. Tämä ero voi johtua siitä, että miehille kohdennetut tuotteet ovat lähtökohtaiset kalliimpia kuin naisten tuotteet ja miehiä halutaan lähestyä tekniikalla ja it-tuotteilla. (Theorell 2017, 29.)

Nuorilla (18–25-vuotiailla) on enemmän kokemusta tilausansoista kuin vanhemmilla kuluttajilla (26–75-vuotiaat). 18–25-vuotiaiden ikäryhmässä tilausansoista oli kokemusta 15 prosentilla, kun taas ikäryhmässä 26–75-vuotiaat tilausansoista oli kokemusta 11 prosentilla vastaajista. 26–75-vuotiaista, joilla oli kokemusta tilausansoista, 12 prosenttia sanoi olleensa yhteydessä pankkiin/luottolaitokseen ja reklamoineensa

kiistetyt tapahtumat. Vastaavasti ainoastaan 2 prosenttia 18–25-vuotiaista oli tehnyt reklamaation pankille tai luottolaitokselleen. (Theorell 2017, 30.)

4.5 Lainsäädäntö

On hyvä käsittää myös lainsäädäntöä ja etenkin sen joustamattomuutta, kun keskustellaan nettimaailmassa tapahtuvista rikoksista. Esimerkiksi kuluttajansuojalain 2 luvun 6§:n mukaan markkinoinnissa tai asiakassuhteessa ei saa antaa valheellisia tai harhaanjohtavia tietoja, jos tiedot ovat omiaan johtamaan siihen, että kuluttaja tekee ostopäätöksensä tai muun kulutushyödykkeeseen liittyvän päätöksen, jota hän ei ilman annettuja tietoja olisi tehnyt. Valheelliset tai harhaanjohtavat tiedot koskevat hintaa. Kiellettyä on myös antaa kuluttajalle mielikuva, että kysymys on yksittäisestä ostosta, vaikka todellisuudessa kysymys on pitkäaikaisesta sopimuksesta. (HE 32/2008 vp., 24–25.)

Suomen rikosoikeuden soveltamisalasta määritellään 1§:ssä (16.8.1996/626) Suomessa tehdyt rikokset seuraavasti. Suomalaiseen kohdistunut rikos 5§:n (16.8.1996/626) mukaan Suomen ulkopuolella tehtyyn rikokseen, joka on kohdistunut Suomen kansalaiseen, säätiöön, suomalaiseen yhteisöön, muuhun oikeushenkilöön tai Suomessa pysyvästi asuvaan ulkomaalaiseen, sovelletaan Suomen lakia, jos teosta Suomen lain mukaan saattaa seurata yli kuuden kuukauden vankeusrangaistus. Kansainvälinen rikos 7§:n (16.8.1996/626) mukaan Suomen ulkopuolella tehtyyn rikokseen, jonka rankaiseminen tekopaikan laista riippumatta perustuu Suomea velvoittavaan kansainväliseen sopimukseen tai muuhun Suomea kansainvälisesti velvoittavaan säädökseen tai määräykseen, sovelletaan Suomen lakia. Rikoksen tekopaikka 10§:n (16.8.1996/626) mukaan rikos katsotaan tehdyksi siellä, missä rikollinen teko suoritettiin, että siellä, missä rikoksen tunnusmerkistön mukainen seuraus ilmeni. Jos rikos jäi yritykseksi, rikos katsotaan tehdyksi sielläkin, missä rikoksen täyttyessä sen tunnusmerkistön mukainen seuraus joko todennäköisesti tai tekijän käsityksen mukaan olisi ilmennyt. Rikosprosessi muodostaa eri toimijoiden prosessitoimista koostuvan ketjun, jonka etenemisessä voidaan erottaa neljä peräkkäistä päävaihetta:

1. esitutkinta
2. syyteharkinta ja syyttäjän muu päätöksenteko
3. oikeudenkäynti tuomioistuimessa
4. rangaistuksen täytäntöönpano.

Rikoksen vuoksi voi rikosoikeudellisten vaatimusten lisäksi syntyä myös yksityisoikeudellisia, siviililaissa määriteltyjä vaateita, joista selvästi yleisin on vahingonkorvausvaatimus. Tämän kaltaisia asioita ei ole kuitenkaan välttämätöntä käsitellä rikosprosessuaalisessa järjestyksessä. Mikäli rikoksen asianomistaja haluaa esittää yksinomaan rikokseen perustuvan vahingonkorvausvaatimuksen, kysymyksessä ei ole rikosasia vaan riita-asia, koska lain mukaan sellaisen asian käsittelyssä noudatetaan, mitä oikeudenkäynnistä riita-asioissa säädetään 11.7.1997/689, 3:1:n 2. virkkeessä. Riita-asian oikeudenkäynnistä käytetään nimitystä siviiliprosessi. Rajanvetoa siviiliprosessin ja rikosasian tai rikos- ja siviiliprosessin välillä ei siten ratkaise vaatimuksen peruste vaan sen laatu. (Virolainen & Pölönen 2003, 5.)

4.5.1 Rikoksien esitutkinta ja realiteetteja

Esitutkinnalla tarkoitetaan selvityksen saamista epäillystä rikoksesta mahdollisen syyteharkinnan suorittamista ja rikosoikeuden käynnin valmistelua varten. Rikoksella tarkoitetaan tässä yhteydessä rangaistavaksi säädettyä tekoa. Rikosprosessiin laajassa mielessä kuuluvat esitutkinnan jälkeen seuraava mahdollinen syyttäjän tekemä syyteharkinta, oikeudenkäynti tuomioistuimessa ja rangaistuksen täytäntöönpano. (Tolvanen & Kukkonen 2011, 1–3.)

Rikos voi nykyaikana tulla poliisin tietoon monella eri tavalla. Rikoksen uhri eli asianomistaja tekee tavallisesti ilmoituksen teosta, jota hän epäilee rikokseksi. Suuri osa rikoksista tulee toisaalta esitutkintaan poliisin oman havainnoin tai esitutkintaa edeltävän tarkoituksellisen valvonnan tai rikostiedustelun kautta. Rikosilmoituksen kirjaamisen kynnys viranomaisella on matala. Ilmoitukseen riittää, kun ilmoittaja pystyy yksilöimään tosiseikat, joiden hän epäilee täyttävän rikoksen tunnusmerkit.

Ilmoittajan pitää pystyä kertomaan tapahtuman kulku, joka on liitettävissä kohtuullisella tarkkuudella tiettyyn paikkaan ja aikaan. Esitutkintaviranomainen voi tutkia ulkomailla tehdyksi epäillyn rikoksen, mikäli rikokseen RL 1 luvun säännösten nojalla voidaan soveltaa Suomen lakia ja jos esitutkinnan toimittaminen Suomessa on tutkinnallisista syistä ja rikosvastuun toteuttamisen kannalta asianmukainen. (ETL 3:8:1.) Lain esitöiden mukaan huomioon voidaan ottaa esimerkiksi se, missä valtiossa rikoksesta epäilty oleilee ja missä valtiossa asiaa koskeva selvitys on parasta kerätä yhteen. Myös mahdollisella ulkomailla aloitetulla rikostutkinnalla ja sen vaiheella on merkitystä. Kun rikos on tehty ulkomailla, esitutkintaviranomaisen tulisi olla yhteydessä tekopaikan viranomaisiin sen selvittämiseksi, missä tutkinta- ja syytetoimet olisi käytännöllistä tehdä. Viranomaisen kansalliset toimivaltuudet eivät suojaa rikosuhrin oikeusturvaa verkossa tarvittavalla tavalla. (Tolvanen & Kukkonen 2011, 51–57.)

Verkko on globaali, viranomainen ei. Verkko on nopea, mutta viranomaisten tietojenvaihtokanavat ovat hitaat. Kysymys ei ole aina viranomaisen hitaudesta tai osaamattomuudesta, kyseessä on reunaehtojen muuttuminen ja se, että lainsäädäntö ei pysy mukana globaalin tietoyhteiskunnan kehityksessä. Rikospaikalle ei jää tekijästä DNA:ta kuten fyysisissä rikoksissa, eikä silminnäkijähavaintoja ole. Viestinnän suoja nauttii verkossa suurta turvaa verrattuna esimerkiksi kotirauhaan tai muuhun yksityisyyteen. Epäillyn luo voidaan tehdä kotietsintä, kun se on välttämätöntä tutkittaessa rikosta, josta säädetty ankarin rangaistus on vähintään kuusi kuukautta vankeutta. Tähän verrattuna viestinnän tunnistamistietoja ei voida hankkia eikä vahinkoa voida estää ennalta, jos 200 000 suomalaiselta keräillään sopivalla toteutustavalla maksukorttitietoja ja muita henkilötietoja, koska se rikkoisi yksityistä viestintää. (Kajantie 2010.)

4.5.2 Tuomiot eri oikeusasteissa

Näistä taulukoista on hyvin vaikea sanoa, kuinka moni on liittynyt tilausansoihin, mutta pääsääntöisesti seuraavassa taulukossa esitetyt lukemat koostuvat skimmauk-

sista ja korttivarkauksista, joissa tekijöinä oli pääasiassa ulkomaisten järjestäytyneiden rikollisryhmien jäseniä. Rikosten luonne muuttui vuodesta 2012 lähtien, jolloin nettipetoksia ja lompakkovarkauksia ilmoitettiin aiempaa enemmän. (Poliisi.)

	Oikeudessa tuomitut (lkm)
Kaikki Suomen alueet yhteensä	
37:8§ Maksuvälinepetos	
2012	432
2013	341
2014	293
2015	326
2016	285
37:9§ Törkeä maksuvälinepetos	
2012	55
2013	75
2014	59
2015	48
2016	68
37:10§ Lievä maksuvälinepetos	
2012	34
2013	31
2014	25
2015	24
2016	14
37:11§ Maksuvälinepetoksen valmistelu	
2012	4
2013	2
2014	3
2015	7
2016	3

Taulukko 6: Rangaistukset eri maksuvälinepetoksien kategorioissa (Tilastokeskus)

Tilausansoihin liittyviä tapauksia on käsitelty tuomioistuinkäsittelyssä. Vuonna 2015 kuluttaja-asiamies avusti käräjäoikeudessa yli 30 kuluttajaa tilausansasaatavien perintään liittyvissä tapauksissa. Kaikissa kyseisissä tapauksissa käräjäoikeus asettui kuluttaja-asiamiehen kannalle ja perintätoimistoja vastaan. Myös hovioikeus on ollut samalla kannalla käräjäoikeuden kanssa kaikista niistä tapauksista, jotka olivat edenneet sinne asti. Tuomioissa on kiinnitetty huomiota erityisesti asiakaspalveluun, jonka puuttumista pidetään sopimusrikkomuksena. (Kauppalehti 2016.)

4.5.3 Oikeusjärjestelmän haasteet nettirikollisuudessa

Sosiaalisessa mediassa toteutettua rikosta ei voi selvittää käsittelemättä viestinnän tunnistamistietoja, joiden käsittelystä esitutkinnassa päättää tuomioistuin joko pakkokeinolain tai sananvapauslain perusteella. Tietoverkon palveluiden kaltaisessa uudessa ympäristössä toimintavaltasäätelyä joudutaan kuitenkin mukauttaa, sillä lainsäätäjä ei aiemmassa sääntelyssä ole voinut ottaa verkkoa toimintaympäristönä huomioon. Lainsäädännön kehitystyö vaatii suunnittelua ja valmistelua sekä vie prosessina oman aikansa, muutokset tietoverkkojen maailmassa ovat sen sijaan vaikuttavia ja erityisen nopeita. Erityinen haaste viranomaisille on sosiaalisen median kansainvälinen luonne ja sen laajuus. Poliisilla ja muilla Suomen viranomaisilla on operatiivinen toimivalta vain Suomessa, muussa ympäristössä oleva tieto on hankittava hitaalla oikeusapumenettelyllä. (Lardot & Kaartinen 2014.)

Tavallisesti lainsäädännössä pyritään teknologianeutraliteettiin erityisesti keskeisten kysymysten, kuten perusoikeuksien suojan osalta. Verkossa toimivaltuudet ovat epätasapainossa vastaavien reaalimaailman toimivaltuuksien kanssa. Rikoksesta epäillyn lähettämän tai vastaanottaman kirjeen tai muun esineen voi pysäyttää ja takavarikoida epäiltäessä rikosta, josta säädetty ankarin rangaistus on vuosi vankeutta. Lainsäätäjän käsissä on, tuleeko tietoverkossa rikosvahingot hallita ensisijaisesti siviilioikeudellisin menettelyin, jolloin tietysti nykytilanne vastaa hyvin lainsäätäjän tahtoa. Tämä johtaa siihen, että yhteiskunta kantaa kasvavat kustannukset kollektiivisesti. Rikoshyötyä ei saada pois, jos rikosta ei pysty, voida tai saa tutkia tai rikosta ei edes ole tapahtunut. (Kajantie 2010.)

Digitalinen maailma on globaali, mutta lainsäädäntö on paikallista, vaikka EU-alueella yhdenmukaisuutta on jo viety pitkälle. Lainsäädännön erot voivat luoda ongelmia, kun aina ei ole selkeää, minkä maan lainsäädännön mukaan pitäisi toimia. Tämä on erikoinen ongelma erityisesti Euroopan alueella, jossa maita on paljon. Tämän johdosta Euroopan unioni on kehitellyt digitaalisia sisämarkkinoita, joiden tavoitteena on purkaa esteitä maiden rajat ylittävältä digitaaliselta toiminnalta. (Ilmarinen & Koskela 2015, 69.)

Rikosoikeuden käytön tehokkuutta voidaan analysoida rangaistusjärjestelmän tehokkuutena ja kyvykkyytenä torjua rikoksia. Rikosoikeuden hyvinvointivaltiollistuminen on merkinnyt rikosoikeuden yhä lisääntyvää sitoutumista tavoiteorientoituneeseen ajatteluun pitkälti rikosoikeudelle asetettujen uusien yhteiskuntapoliittisten ohjailutehtävien takia. Rikosoikeuden käytön tehokkuutta hyötynäkökulmasta tarkastellaan yleensä lähinnä yleis- ja erityisestävyyden käsitteiden avulla. Rikosoikeuden hyötynä tulee olla kompetenssi torjua rikollisuutta ja sillä aiheutettua haittoja. Hyötytavoitteena pidetään myös yksilön oikeusturvan takaamista. (Mäkelä 2001, 106.)

5. Tutkimuksen toteutus

Viidennessä luvussa esitellään kyselyn ja aineisto analysoinnin tutkimustulokset. Luvussa käydään myös läpi menetelmän kuvausta ja aineiston keruun toteutusta. Luvun lopussa käydään läpi tilausansojen haasteita, ennaltaehkäisyä ja rikostorjunnan kehittämistä. Luku päätetään tulosten yhteenvetoon.

Tutkimukseen liittyvän kyselyn kysymykset koostuivat yhdeksästä avoimesta kysymyksestä, jotka jaoteltiin kolmeen eri teemaan. Ensimmäisessä teemassa tutkittiin, kuinka laajasta ongelmasta on kysymys meidän yhteiskunnassamme. Toisessa osiossa tutkittiin, miksi ilmiö on saanut jatkua pitkään ja minkälaisia toimenpiteitä pitäisi olla ennalta ehkäisemässä tilausansoja. Kolmannessa ja viimeisessä teemassa tutkittiin, kuinka toimijoiden tulisi parantaa yhteistyötä tilausansojen rikostorjunnassa. Liitteissä 13-20 on koottuna haastattelukysymykset, samankaltaiset vastaukset sekä huomiot ja eriävät vastaukset. Tuloksia havainnollistetaan taulukoilla sekä kuvioilla, ja tarkoituksena osoittaa, että löydetyt tutkimustulokset ovat validit.

5.1 Menetelmän kuvaus ja perustelu

Laadullisen aineiston (haastattelut, media-aineistot sekä tilastot) ohella on tässä tutkimuksessa käytetty myös määrällisiä aineistoja (tilastot sekä survey-aineistoja). Tutkimuksen suunnittelu aloitettiin Poliisihallituksen ja Europolin edustajan kanssa keväällä 2017. Aiheen laajuutta ja soveltuvuutta suunniteltiin aluksi tehtäväksi ainoastaan Suomen sisällä, mutta tilausansojen laajuuden takia, tutkimus päätettiin laajentaa kattamaan koko Eurooppa. Tutkimuksen suunnittelussa kaikki kysymykset haluttiin esittää avoimina kysymyksinä, jotta vastaajilta saataisiin mahdollisimman laaja-alaisesti vastauksia sekä mielipiteitä ilmiöstä.

Kävin avoimia keskusteluja poliisien ja finanssialan kollegoiden kanssa tilausansoista kevään ja kesän 2017 aikana, jotta tuli selvyyttä siitä, mihin suuntaan tilausansat ovat kehittyneet muutaman viime vuoden aikana. Etsin tilausansoja internetistä ja osallistuin jatkuvaveloituksiin täyttämällä osallistumislomakkeita 1.5.2017-31.8.2017 välisenä aikana. Taustatietoja tilausansa yrityksistä etsittiin mm. https://www.scamner.com sivuston kautta koko tutkimuksen ajan. Tällä tavalla pyrin saamaan selville kaikki olennaiset ja muuttuneet tiedot tilausansa yrityksistä Suomessa ja muualla Euroopassa.

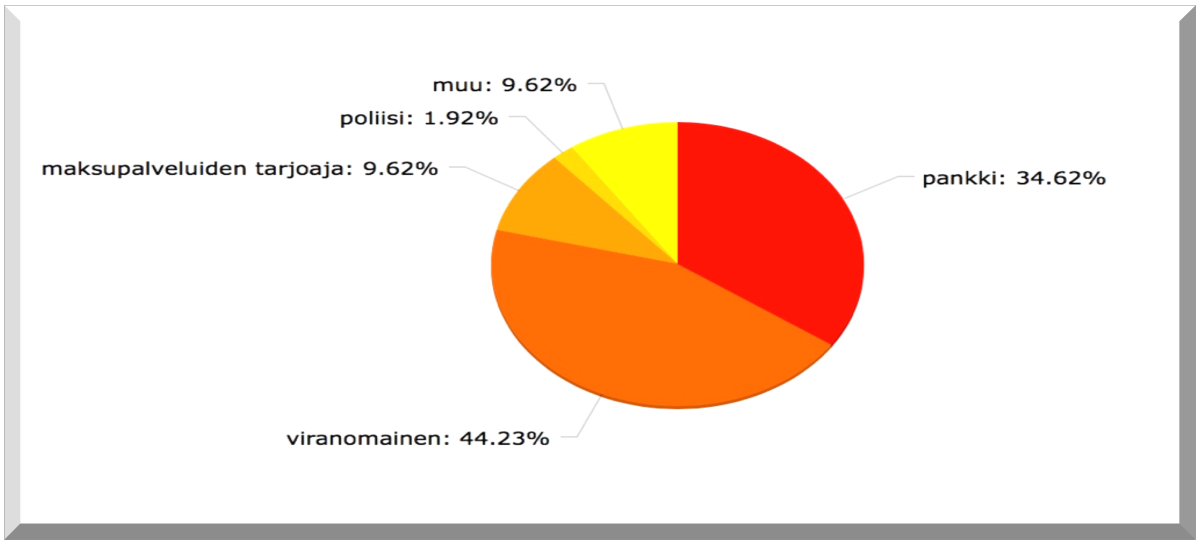
Tutkimuksessa nousi kysymyksiä esiin, kuten; miksi tilausansa yritykset voivat tehdä petoksiaan suhteellisen vapaasti joutumatta vastuuseen? Miksi viranomaiset ovat haluttomia puuttumaan ongelmaan? Tavoitteena oli tuottaa syvällisempää tietoa aiheesta ja havaita asioita, jotka vaikuttavat petosten suureen määrään.

5.2 Aineiston keruun toteutus

Kysely suunnattiin sidosryhmilleni, ammatilliselle kontaktiverkostolle, joilla oli kokemusta tilausansojen rikostorjunnasta. Vastaajia oli mm. International Association of Financial Crimes Investigators-yhdistyksestä, European Cyber Crime and Fraud Investigators-yhdistyksestä, Suomen Maksukorttien Riskienhallinnan työryhmästä sekä

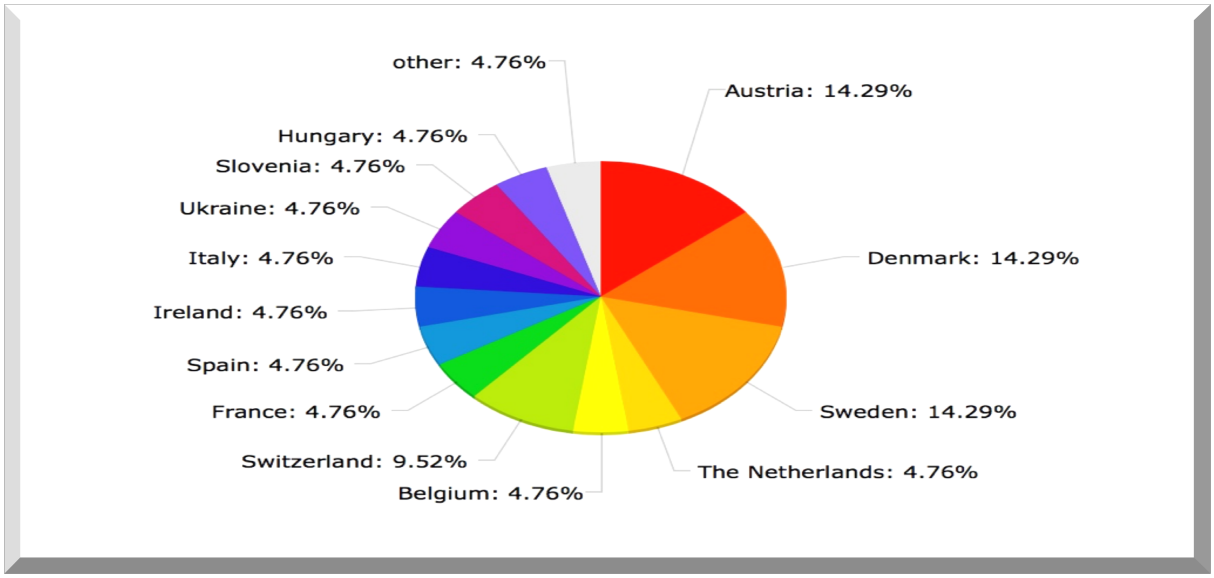
Keskusrikospoliisista, Helsingin poliisista, syyttäjänvirastosta sekä Europolista. Vastaajat valittiin International Association of Financial Crimes Investigators Euroopan jaoston jäsenrekisteristä, European Cyber Crime and Fraud Investigators yhdistyksen jäsenrekisteristä, omasta LinkedIn verkostostani sekä Europolin ja Keskusrikospoliisin kontaktien kollegoista, joilla on tutkinnallista kokemusta tilausansoista. Kysely järjestettiin 13.8.–13.9.2017 välisenä ajanjaksona.
Kuluttajille suunnattuja samanlaisia kyselyitä on tehty muualla Euroopassa, mutta tämä kysely oli ensimmäinen, joka suunnattiin rikostorjunnan ammattilaisille Euroopassa. Tutkimusaineisto kerättiin elektronista kyselylomaketta käyttäen sivulta https://www.kyselynetti.com, jonne tehtiin yksi suomenkielinen ja yksi englanninkielinen kyselylomake. Kyselyssä pyrittiin selvittämään tilausansaa ilmiönä (Liite 11) sekä ilmiön taustaa. Uusintapyyntö lähetetiin kahden viikon kuluttua ensimmäisestä viestistä. Valmisteluvaiheessa sovittiin myös valikoitujen testihenkilöiden kanssa haastattelulomakkeen läpikäymisestä. Valikoidut testihenkilöt valittiin omasta ammatillisesta kontaktiverkostosta. Ennen varsinaista kyselyä, kävin neljän testihenkilön kanssa läpi kyselylomaketta, ja muutoksia tehtiin lopulliseen versioon testihenkilöiden palautteiden perusteella. Kyselylomaketta muutettiin kaksi kertaa testihenkilöiden palautteen perusteella. Kysely lähetettiin sähköpostilla ja LinkedIn verkoston kautta yhteensä 94 asiantuntijalle. Lopulliseksi vastaajamääräksi muodostui 73 asiantuntijaa. Vastausprosentiksi tuli 78%.

Kaikille kyselyyn osallistujille oli esillä samat 9 avointa kysymystä tilasansoista (Liite 13-20). Tutkimusta syvennettiin haastatteluilla kahden eri poliisin edustajan kanssa. Tilausansojen ilmiötä poliisin näkökulmasta selvitettiin Keskusrikospoliisin, Europolin, Poliisihallituksen, sekä Poliisiammattikorkeakoulun edustajan kanssa.



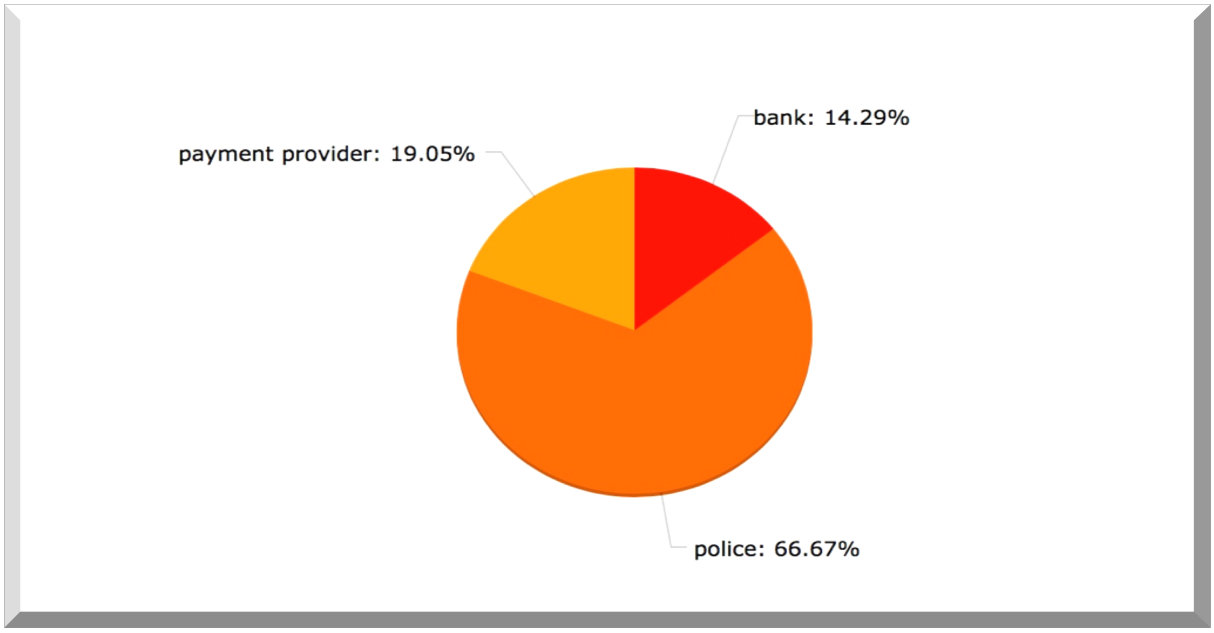
Kuvio 8: Suomesta kyselyyn osallistujien organisaatioiden edustus

Samanlaisella rakenteella ja samoilla kysymyksillä tehtiin kysely myös Euroopan viranomaisille ja rikostorjunnan parissa työskenteleville. Vastausaika oli sama kuin Suomeen suunnatulla kyselyllä. Euroopasta pyrittiin saamaan tasapuolisesti vastaajiksi viranomaisia sekä finanssialan edustajia.



Kuvio 9: Kyselyyn osallistujien Euroopan edustajien maat

Vastauksissa oli paljon samankaltaisuuksia Suomen vastausten kanssa, vaikka vastaajarakenne poikkesi paljon Suomesta. Euroopasta tulleissa vastauksissa enemmistö oli poliisien edustajia, kun Suomessa poliisien osuus oli vain muutaman prosentin luokkaa.



Kuvio 10: Euroopasta kyselyyn osallistujien organisaatioiden edustus

5.3 Aineiston analyysi

Tutkimuksen aineisto tallentui suoraan ilman välivaiheita Excel-tiedostoksi, jollaisena sitä saatettiin heti keräämisen jälkeen käsitellä ja analysoida tilastollisin menetelmin. Aluksi aineisto käytiin läpi tarkastelemalla muuttujia kuvaavia tunnuslukuja, jakaumia, keskilukuja sekä hajontalukuja. Näin saatiin yleiskuva aineistosta. Huomiota kiinnitettiin myös mm. puuttuviin arvoihin, joita kuitenkin aineistossa oli vähän. Aineiston käsittelyssä hyödynsin monia tilastollisia menetelmiä aineiston hallitsemiseksi, tiivistämiseksi ja analysoimiseksi. Näistä olen koonnut tiivistelmän seuraavaan taulukkoon sen mukaan, mihin tutkimuskysymyksiin hain niillä vastausta.

TUTKIMUSKYSYMYS	MENETELMÄ
1. Milloin ensimmäisen kerran olit tekemisissä tilausansoihin liittyvän rikollisuuden kanssa?	Frekvenssit ja prosenttijakaumat
2. Kuinka paljon tilausansoihin liittyvistä oman organisaatiosi reklamaatioista, asiakkaat EIVÄT ole tehneet rikosilmoitusta poliisille? (% arvio)	Frekvenssit ja keskiarvo
3. Osaatteko omien tutkimuksien perusteella sanoa, mistä kyseinen rikollisuus tulee? (maa, kaupunki)	Frekvenssit ja prosenttijakaumat
4. Kuinka paljon tilausansoihin liittyvät reklamaatiot työllistävät itseäsi/osastoasi?	Frekvenssit, prosenttijakaumat ja keskiarvo
5. Mikä on mielestäsi suurin syy tilausansoihin liittyvän rikollisuuden suureen määrään?	Frekvenssit ja prosenttijakaumat
6. Miten mielestäsi tilausansoihin liittyvää rikollisuutta voisi parhaiten ennaltaehkäistä?	Frekvenssit ja prosenttijakaumat
7. Miten toivot, että poliisi/pankki/maksupalveluiden tarjoaja voisi paremmin ennaltaehkäistä kyseisenlaista rikollisuutta?	Frekvenssit ja prosenttijakaumat
8. Minkälaista yhteistyötä toivoisit poliisin/pankin/maksupalveluiden tarjoajan kanssa tilausansoihin liittyen?	Frekvenssit ja prosenttijakaumat
9. Onko jotain mitä haluaisit lisätä kyselyyn tai kommentoida?	Frekvenssit ja ryhmittelyanalyysi

Taulukko 7: Tutkimuskysymykset ja tutkimuksessa käytetyt tilastolliset menetelmät, joilla kysymyksiin haettiin vastausta

Suomesta kyselyyn vastasi 52 henkilöä. Vastaajat toimivat muun muassa kihlakunnansyyttäjinä, luottopäällikköinä, tuoteasiantuntijoina, riskiasiantuntijoina, riskienhallintapäällikköinä, korttiasiantuntijoina sekä lakimiehinä. Yhteistä kaikille vastaajille oli se, että he ovat työssään olleet jollakin tavalla tekemisissä tilausansoihin liittyvän rikollisuuden kanssa ja osaavat arvioida Suomen tilannetta tilausansarikollisuuden näkökulmasta. Euroopasta tuli vastauksia yhteensä 21 kappaletta, 14 eri maasta. Myös Euroopan vastaajien keskuudesta valittiin ihmisiä, jotka ovat olleet tekemisissä tilausansarikollisuuden kanssa ja osaavat antaa kokonaisuuteen liittyviä vastauksia tämän hetkisestä tilanteesta eri puolilla Eurooppaa ja mahdollisia kehitysideoita.

Sektori	Suomi		Muu Eurooppa		Kaikki	
	f	%	f	%	f	%
Viranomaiset	25	47	13	65	38	52
Yksityinen	23	43,5	7	35	30	41
Muu	5	9,5	0	0	5	7
Yhteensä	53	100	20	100	73	100

Taulukko 8: Kyselyyn vastanneet asiantuntijat maantieteellisen sijainnin ja edustetun sektorin mukaan (N=73)

Kvalitatiivista sisällönanalyysiä hyödynnettiin avoimien kysymysten vastausten käsittelyssä. Lähestymistapa oli induktiivinen, aineistolähtöinen. Avovastausten analyysi eteni seuraavien vaiheiden kautta:

- Aineistoon perehtyminen: asiantuntijoiden vastaukset luettiin huolellisesti
- Mitä asioita tai teemoja vastauksista nousi esiin
- Mitkä tekijät yhdistävät esille nousseita asioita tai teemoja
- Aineisto luokiteltiin muodostettujen kategorioitten mukaisiin luokkiin
- Laskettiin luokkien jakaumat

Kyselyn tuloksista korostui kolme tärkeintä yksityiskohtaa tilausansoista. Nämä kolme yksityiskohtaa ovat:

1. Tilausansasivusto on helppo sekä nopea perustaa ja kiinnijäämisriski on pieni
2. Viranomaisten puutteelliset työkalut torjua tilausansa rikoksia.
3. Kuluttajien herkkäuskoisuus harhaanjohtaviin mainoksiin liittyen

Empiirisen aineiston määrällinen kuvaus näyttää, että monet vastaajat olivat törmänneet tilausansoihin useita vuosia sitten. Pankit ja muut finanssilaitokset kertoivat, että ongelma alkoi näkyä vuonna 2013, kun taas poliisit ilmoittivat, että ongelma ilmeni heillä vuonna 2014. Monet ilmoittivat, että tilausansat työllistävät vielä nykyäänkin useita tunteja viikossa, vaikka pankit ja finanssilaitokset ovat ottaneet suoremman lähestymistavan tilausansojen kitkemiseksi ja asiakkaiden varojen säästämiseksi. Suurin osa finanssialan vastaajista totesi, että monipuoliset huijauskeinot ja

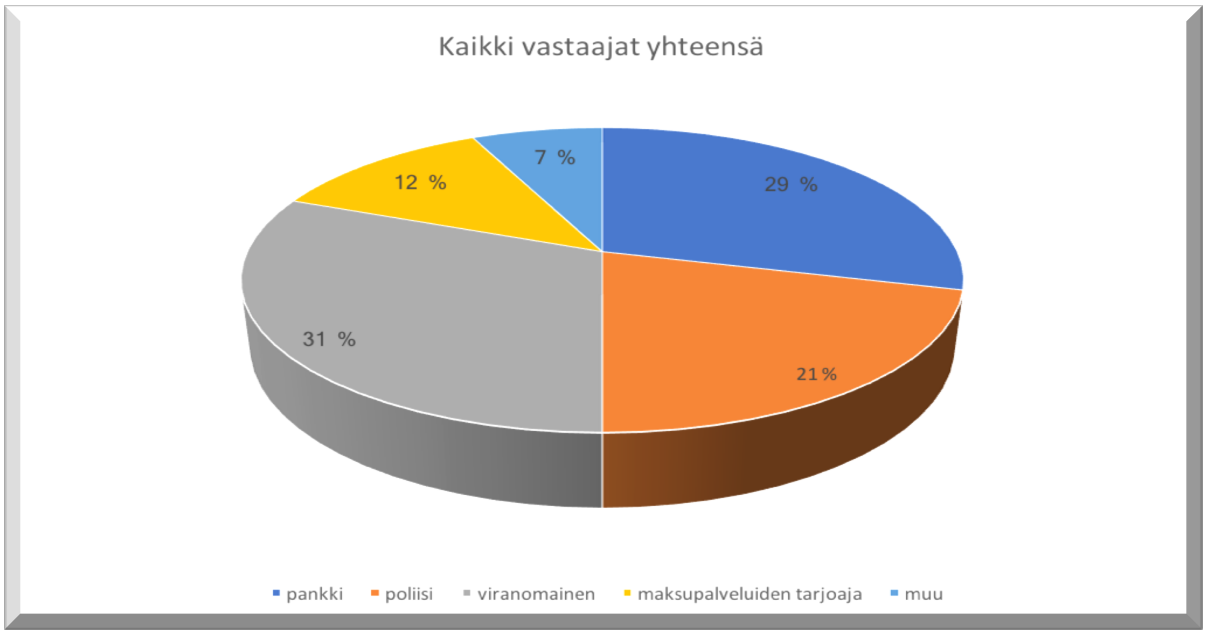
harhaanjohtavat mainokset-yhtälö on haasteellinen selittää monille kuluttajille. Moni pankin ja finanssilaitoksen edustaja sanoi kyseessä olevan vuodesta 2014 lähtien suurin yksittäinen aihe, josta he saavat reklamaatioiden osalta valituksia. Vastaajat arvioivat, että kaikista käsittelyyn otetuista reklamaatioista kolmasosa liittyy tilausansoihin.

Enforcement and European Consumer Centres Misleading ”free” trials and subscription traps tutkimuksessa (2016) tilausansoista, löytyy samanlaisia tuloksia tähän tutkimuksen liittyen. Merkittävät yhteiset huomiot ovat:

1. Lisäämällä tietoisuutta riskeistä kuluttajille, lisäämällä informaatiokanavia ja tietoja siitä miten vältetään tilausansoja
2. Sosiaalisen median toimijoille tiedon lisäämistä ongelmasta ja yhteisvastuullisuutta rikostorjunnassa tilausansoja vastaan
3. Viranomaisille paremmat työkalut rikostorjunnassa tilausansoja vastaan. Rikostorjunnassa tarvitaan myös kansainvälistä rajat ylittävää yhteistyötä

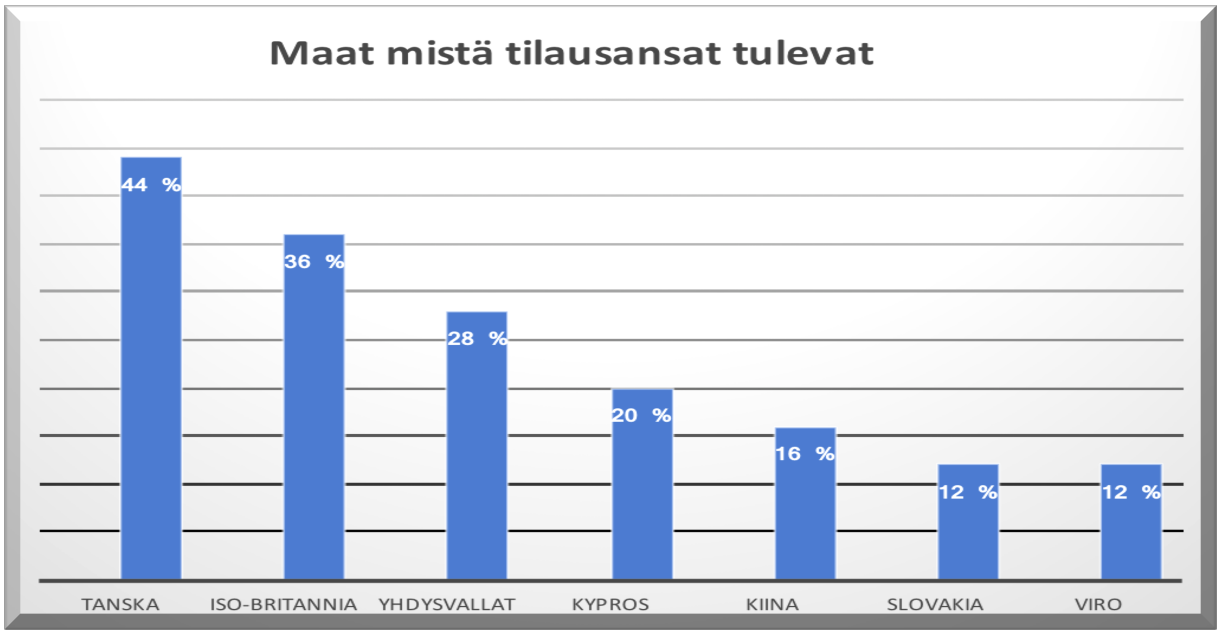
Aineiston käsittelyssä hyödynnettiin sekä kvantitatiivista että kvalitatiivisia menetelmiä. Tilastollisia menetelmiä käytettiin aineiston hallitsemisiksi, keskittämiseksi ja analysoimiseksi. Metodit tukivat hyvin toisiaan: avovastausten tuottama laadullisempi ja yksityiskohtaisempi kuva tilausansa rikollisuudesta syvensi petosrikollisuudesta syntyvää kuvaa, ja antoi syvällisempää ymmärrystä maksuvälinerikollisuudesta.

Aineiston merkittävin huomio liittyy ajankohtaan. Suurin osa ulkomaalaisista vastaajista sanoi olleensa ensimmäisen kerran tekemisissä tilausansa rikollisuuden kanssa vuosina 2007-2009, viidesosa vastaajista. Tässä oli merkittävä ero suomalaisiin vastaajiin. Enemmistö suomalaisista oli nähnyt tilausansa rikollisuutta ensimmäisen kerran vuosina 2013-2015, noin puolet vastaajista.



Kuvio 11: Kaikki kyselyyn vastaajat yhteensä

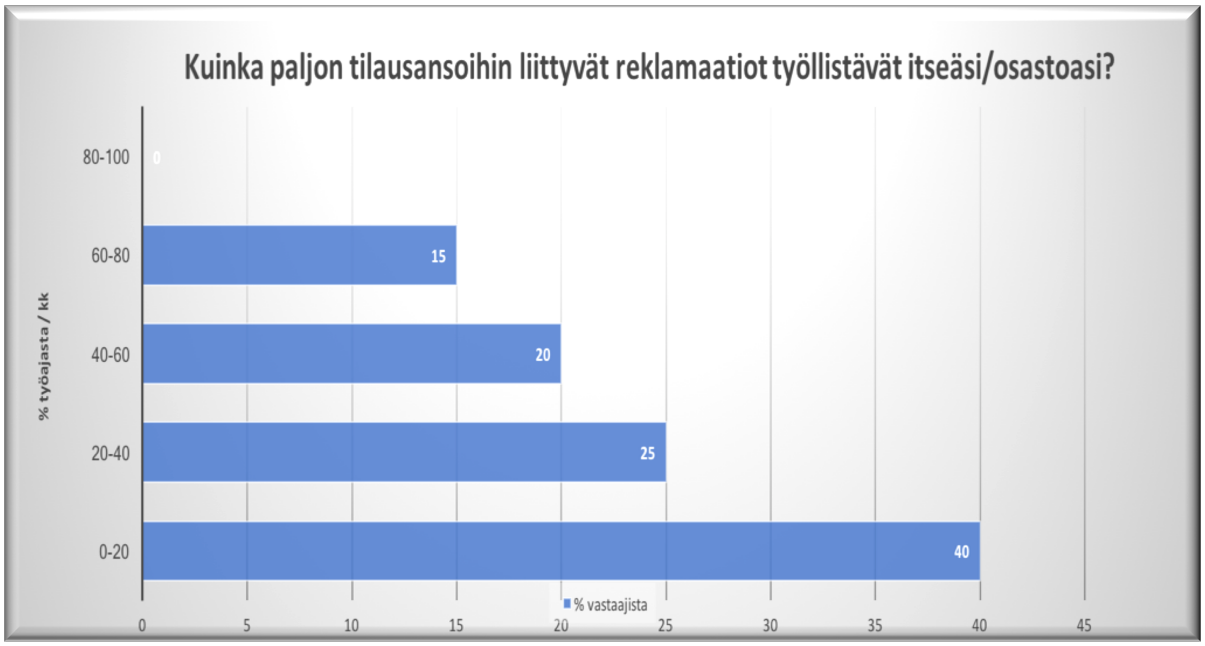
Haastatteluaineiston analysoinnin tulokset osoittavat Tanskan merkityksellistä asemaa tilausansarikollisuudessa. Kaikista vastaajista, noin puolet nimesi Tanskasta tulevan tilausansarikollisuuden ongelmaksi yritysten liiketoiminnalle ja asiakkaille. Tätä Tanskan osuutta korostaa osittain (taulukko 4) aikaisemmin mainitut tilausansayritykset, joista neljällä löytyy Tanskasta yhteystiedot. Ongelma on myös siinä, että tilausansayritykset käyttävät ja vaihtavat usein acquirer-pankkeja ympäri maailmaa, aina Islannista Mauritiukselle asti. Kyselyssä kävi ilmi, että yleensä tilausansarikollisuus on lähtöisin alueilta, joissa lainsäädäntö, tietotekniikkaosaaminen sekä alhainen kiinnijäämisriksi suosivat tämän kaltaista rikollisuutta.



Taulukko 9: Kyselyyn vastanneet asiantuntijat, jotka tietoihinsa perustuen määrittelivät, mistä tilausansa rikollisuus tulee (N=73)

Kyselyn vastaajat ilmoittivat, että tilausansoihin liittyvistä reklamaatioista keskimäärin neljä viidesosasta ei tehdä rikosilmoitusta poliisille. Nämä lukemat tukevat sitä tilastoa mitä poliisit ovat tilastoineet (kuvio 6) tilausansoista aikaisemmin. Poliisille ilmoitetut tilausansa rikokset ajalla 1.1.2015 – 21.8.2017 lukumäärä on ollut vain 128 kappaletta. Näiden lukujen lisäksi on myös kuluttajia, jotka eivät ilmoita poliisille eivätkä tee reklamaatiota pankilleen. Näiden kuluttajien määrää voi vain arvailla.

Moni finanssialan toimija sanoi, että tilausansat työllistävät vielä nykyäänkin useita tunteja viikossa, vaikka finanssialalla on otettu suorempi lähestymistapa tilausansojen kitkemiseksi ja asiakkaiden varojen säästämiseksi. Viranomaisissa ja erityisesti poliisille ilmoitetut jutut rajoitetaan esim. näyttö tai kustannusperusteella syyttäjän toimesta. Keskimääräiseesti vastaajat ilmoittivat, että kuukausittaisesta työajasta kolmasosa kuluu tilausansojen selvittelyssä. Tämä tukee sitä tulosta minkä Netsin Group arvioi tutkimuksessaan, jonka mukaan jopa 25% kaikista Pohjoismaiden reklamaatiotapauksista voi johtua tilausansoista. (Nets Group 2017.)



Taulukko 10: Kyselyyn vastanneet asiantuntijat kertoivat kuinka paljon tilausansoihin liittyvät reklamaatiot työllistävät itseään tai osastoaan (N=73)

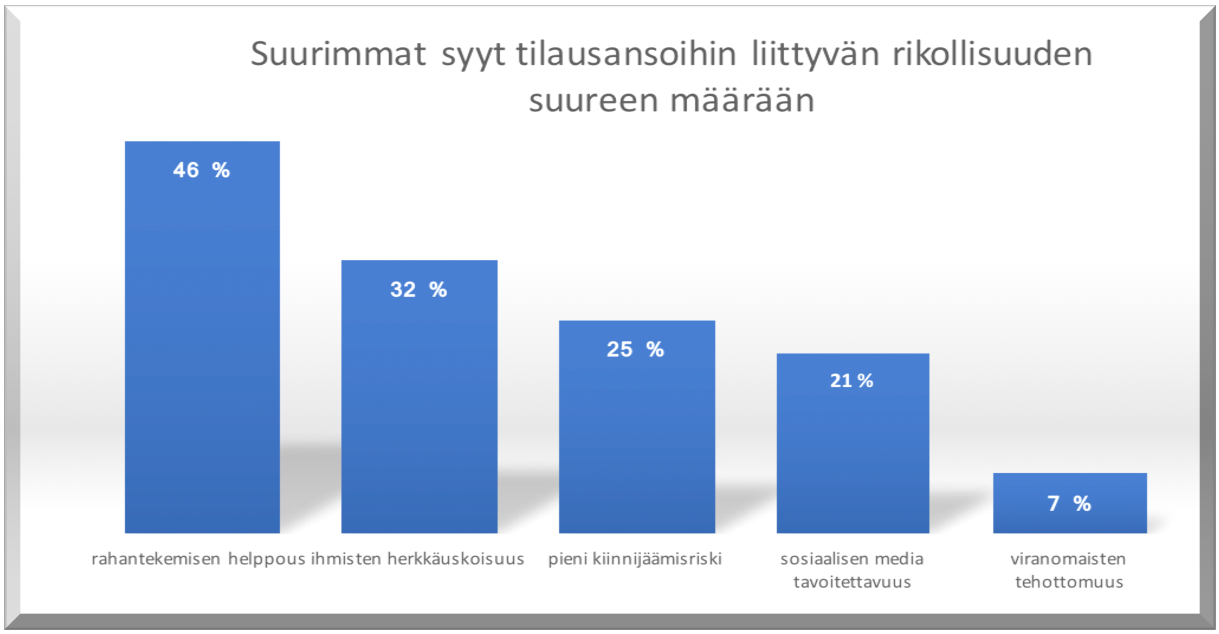
Kyselyssä tuli ilmi se tosiasia, että suurin osa tilausansoihin liittyvistä reklamaatioista on ns. turhaa työtä ja usein aikaa vievää, vaikka taustalla on viime kädessä asiakkaan hyväuskoisuus ja huolimattomuus.

Yhteenvetona haastateltavien vastauksista ja kyselyn tuloksista voidaan todeta, kuinka sosiaalinen media, sähköiset alustat sekä maksamisen digitalisoituminen ovat antaneet pohjan tilausansojen synnylle ja kasvulle. Rikolliset ovat pystyneet kehittämään erityisen kannattavan huijaustavan ja pyrkineet tekemään siitä koko ajan monimuotoisempaa ja aggressiivisempaa. Tilausansasivusto on helppo ja nopea perustaa, ja houkutteleviin mainoksiin tarttuu nopeasti iso määrä ihmisiä. Riski tilausansalla saatujen rahojen menettämisestä on pieni. Ongelmana on myös sosiaalisten medioiden lisääntyminen, herkkäuskoisuus, linkit luotettavalta kaverilta ja se, että useimmissa maissa kyse ei ole rikollisesta toiminnasta, vaan kuluttajan harhaanjohtamisesta, jos edes siitä. Monissa netissä olevissa ”arvonnoissa” ehdot kerrotaan selkeästi, kunhan kortinhaltija jaksaa lukea myös pienen tekstin. Euroopassa ei ole

selkeätä kuvaa siitä, onko tilausansa laillista vai laitonta. Kuluttajien sekä ammattilaisten toimesta ei tunnisteta selkeää rikoslakipykälää, jonka perusteella tilausansat olisivat laittomia, koska tilausansat eivät aina täytä petoksen tunnusmerkistöä. Siitä, kenelle viranomaiselle asia kuuluu, ei ole täyttä selvyyttä. Isona ongelmana etenkin finanssimaailman edustajien puolelta on ollut kauppiaiden liian löyhä seulonta kauppiassopimuksia tehtäessä. Korttijärjestöt, kuten VISA ja Mastercard, eivät myöskään torju riittävän pontevasti ja nopeasti väärinkäytöksiä. Kohdennetun markkinoinnin tarjoavalla verkkoalustalla/medialla tulisi olla vastuunsa tilausansoihin liittyvässä rikostorjunnassa. Yksinkertaisesti sanottuna, jos tilausansoilla ei ole markkinapaikkaa, ei näitä äärimmäisen hyviä yhden euron tarjouksiakaan olisi. Tälläkin hetkellä tilausansoihin liittyviä kampanjoita markkinoidaan aggressiivisesti sähköpostitse, Facebookissa ja Instagramissa, ja ne löytävät kohdemarkkinat helposti digitaalisessa maailmassa.

5.4 Tilausansojen haasteet

Tutkimuksen tulokset osoittivat, että viranomaisilla on puutteellinen keinovalikoima torjua näitä rikoksia. Ongelmaksi on havaittu se, että poliisi ei tutki tilausansoja, koska tilausansat ovat rajat ylittävää toimintaa verkossa. Kyseisiin rikoksiin ei kannata eikä muutenkaan pystytä käyttämään vähäisiä resursseja. Kun ei tutkita, ei saada kiinni rikollisia eivätkä rangaistukset ole riittäviä. Poliisi ohjaakin tapauksia usein myös muille viranomaisille käsiteltäviksi. Moni ilmaisi myös huolensa suomalaisten herkkäuskoisuudesta. Moni kuluttaja uskoo siihen, että joskus saa sen voittavan arvan omalle kohdalleen. Suomessa ollaan auktoriteettiuskoisia ja luotetaan siihen, että kaupan tuotteessa näkyvä hinta on se, mitä siitä kassalla maksetaan. Harva suomalainen retkahtaa nykypäivänä ilmiselviin nigerialaiskirjeisiin, mutta kun sama huijaus muunnetaan pienempään mittakaavaan ja satunnaisen nettisivun mainoksessa luvataan uusinta Iphone-mallia yhdellä eurolla, nousee huijattavien määrä vähintään 100-kertaiseksi.



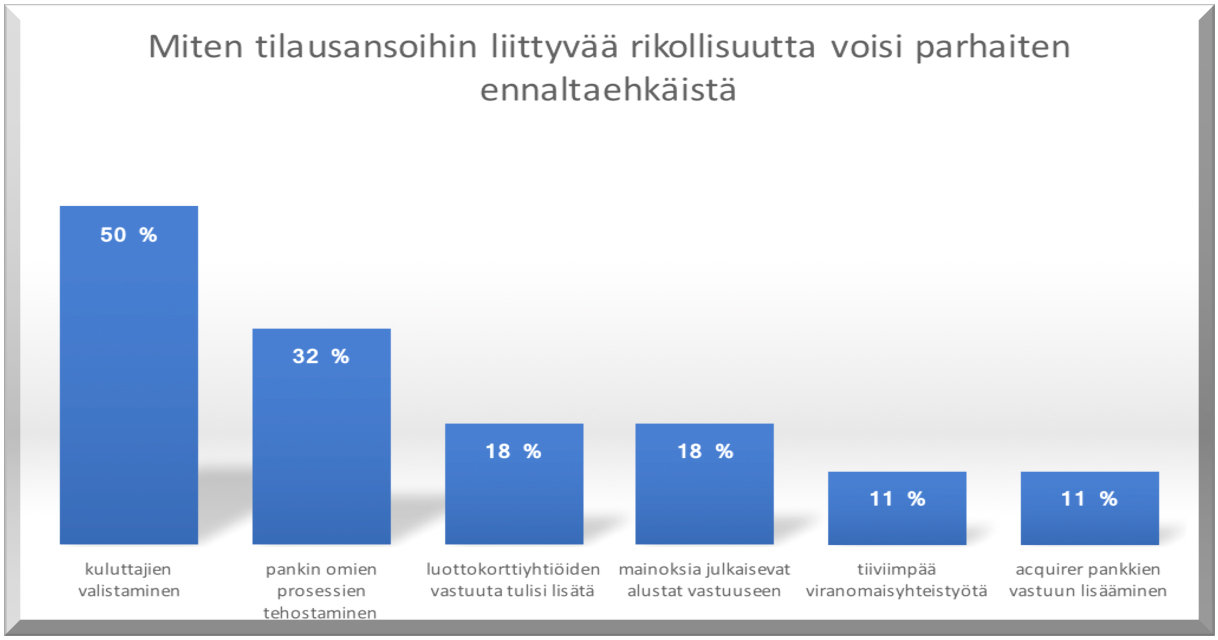
Taulukko 11: Kyselyyn vastanneet asiantuntijat, jotka tietoihinsa perustuen kertoivat syyt tilausansojen suureen määrään (N=73)

Tämän suomalaisten piirteen ovat huomanneet myös ulkomaiset nettihuijarit, ja niin kauan kuin huijattavia löytyy, houkuttelee se uusia toimijoita tekemään tilausansoja. Asiakkaat tuntuvat luottavan siihen, että maksaminen on turvallista, jos sivulla on MasterCardin tai Visan logo ja sivuston kielenä on oman maan kieli. Tilausansojen rakentajat ovat nopeampia kehittämään ansoja kuin pankit torjumaan niitä. Kortin käyttäjien hyväuskoisuus ja ahneus yhdistettynä tasokkaaseen nettigrafiikkaan helpottaa asiaa. Moni vastaaja ilmoitti myös, että suuri osa tilausansoihin liittyvistä reklamaatioista tulee yli 50-vuotiailta asiakkailta. Vanhempia ihmisiä pidetään netissä helpompina kohteina kuin nuoria ja varsinkin kohdennetulla markkinoinnilla tavoitellaan tätä kohdeyleisöä.

5.5 Ennaltaehkäisy ja rikostorjunnan kehittäminen

Kyselyyn osallistuneiden vastausten perusteella voidaan todeta, että pankit ovat lisänneet käytäntöjä poistaa yritykseltä veloitusoikeus, mikäli jollekin yritykselle tulee vaihtoon nähden merkittävästi reklamaatioita. Tässä on kuitenkin monia ongel-

mia, kun veloittajat vaihtavat nimeä ja acquiring-pankkia tasaisin väliajoin. Vaikutusta olisi sillä, jos tilanne saataisiin ehkäistyä jo acquiring-pankissa eli kauppiaita seulottaisiin tarkalla kädellä jo ennen korttiveloittajaksi hyväksymistä ja veloittajia sekä saapuvia reklamaatioita seurattaisiin jatkuvasti. Haastateltavat korostivat, että tärkeänä asiana nähdään, että sosiaalisen median yhtiöt ja muut harhaanjohtavia mainoksia julkaisevat alustat saataisiin laajempaan vastuuseen sisällöstä. Ongelmaa ei pitäisi nähdä yhden ansaan joutuneen ihmisen muutamien kymmenien eurojen menetyksenä, vaan painopiste pitäisi siirtää siihen, miten suuria voittoja toiminnalla tehdään.



Taulukko 12: Kyselyyn vastanneet asiantuntijat vastasivat miten tilausansa rikollisuutta voisi parhaiten ennaltaehkäistä (N=73)

Vastaajat finanssialalta sekä viranomaisista olivat samaa mieltä siitä, että rikostorjunnan kehittämisessä poliisille halutaan paremmat työkalut esitutkintaan ja syyllisille rikossyytteet asiakasmanipuloinnista ja harhaanjohtamisesta. Vastaajat haluavat kehittää kuluttajien valistamista sekä tukea tehokasta kansainvälistä viranomaisyhteistyötä. Uhri yleensä ymmärtää tulleensa huijatuksi, mutta hän ei uskalla eikä osaa vastustaa vaatimuksia. Uhrien auttaminen nähdään tärkeäksi silloin, kun heihin

kohdistetaan voimakasta perinnällä uhkaamista. Myös pankit voisivat tiedottaa näkyvämmin erilaisista huijauksista ja ansoista. Monissa maissa tiedotetaan yleensä ahkerasti muista kyberturvallisuuden ongelmista, mutta tilausansoihin ei kiinnitetä samalla tavalla huomiota. Haastatteluvastauksissa esille nousi pankkien vastuu, jotta nämä kehittäisivät pankkijärjestelmiään siten, että ne entistä paremmin pystyisivät tunnistamaan tilausansat ja estäisivät kortin käytön huijaussivustoilla.

Myös poliisin vaikutukset nousivat esiin vastauksissa, joissa koettiin, että poliisi ei vaikuta tekevän yhteistyötä sisäisesti tai erityisesti eri maiden välillä, vaikka kyse on sadoista tuhansista euroista vuosittain vain Suomen mittakaavassa yhden pankin sisällä. Tutkinta päätetään välittömästi, kun kyseessä on ulkomainen veloittaja ja yksittäisten asiakkaiden menetykset kymmeniä tai satoja euroja. Maksupalveluiden tarjoajilla on omat seulansa kauppiaiden hyväksymiseen, eivätkä nämä epämääräiset kauppiaat ole yleensä läpäisseet esimerkiksi PayPalin seulaa. Toimintaan pitäisi pystyä puuttumaan niin nopeasti, ettei se olisi houkuttelevaa. Jos tilausansa perustuu korttiveloituksiin, pitäisi rahojen liikkuminen päästä pysäyttämään.

Yhteenvetona haastattelun tuloksista käy selville, kuinka tärkeää olisi asennemuutos: tilausansaa ei pitäisi nähdä yhden erehtyneen ihmisen omana ongelmana. Toistuvat maksut pitäisi todentaa erikseen siten, ettei kuluttajalta voida tämän tietämättä veloittaa joka kuukausi usean kymmenen euron summaa. Liiketoiminta perustuu nimenomaan siihen, että kuluttajaa lypsetään, kunnes tämä huomaa, että rahaa häviää tilitä joka kuukausi. Harhaanjohtavan markkinoinnin kulut pitäisi saada acquirerin vastuulle, jolloin vastuu ja ennalta ehkäisy siirtyisivät alkuvaiheeseen. Ilmoituskäytännön tulisi olla nopea, ja sen tulisi johtaa toimenpiteisiin sekä korttiohjelmassa eri osapuolille ja poliisille. Tieto rikoksista tulisi jakaa poliiseille erityisesti sillä alueella, jossa kauppias sijaitsee. Moni kokee, että yksi tehokkaimmista keinoista on poliisitutkinta, johon liitetään takavarikoita ja muita pakkotoimenpiteitä. Rahavirtojen pysäytys on käytännössä tehokkain keino lopettaa tilausansa. Tilausansoja tehtailevat yritykset toimivat pääasiassa Suomen rajojen ulkopuolella, ja poliisin pitäisi tehdä yhteistyötä muiden maiden viranomaisten kanssa verkkosivujen sul-

kemiseksi. Kyseessä on merkittävä kuluttajaongelma, mutta jos lähtökohdaksi otetaan tässä selvityksessä mainittu nettirikollisuus, olisi syytä pohtia, missä määrin asia kuuluu kuluttajaviranomaisille ja missä määrin muille tahoille. Esimerkiksi kuluttajaviranomaisten keinovalikoima ja toimintatavat on luotu sellaisia toimijoita ja markkinointia silmällä pitäen, jotka haluavat pitkällä tähtäimellä toimia markkinoilla ja noudattaa kulloinkin voimassa olevaa lainsäädäntöä.

5.6 Tulosten yhteenveto

Tutkimuksen tulokset osoittavat, että kyselyyn vastaajat ymmärtävät, kuinka tärkeää rikostorjunta tilausansoja vastaan on. Vastaajat olivat hyvin yksimielisiä siitä, miksi tilausansarikollisuus kannattaa. Kyselyn tuloksena aineistosta nousi viisi keskeistä ydinkohtaa, joita pidettiin kehityksen perusteina verrattuna nykytilanteeseen. Nämä viisi ydinkohtaa ovat:

1. Tilausansayritys on suhteellisen helppo perustaa internetiin, ja valmiita sovelluksia ja sivustoja saatetaan muokata hyvin vähän uusiin yrityksiin.
2. Viranomaisten tehottomuus nousi keskeiseksi aiheeksi kyselyssä. Huolta aiheutti se, että ei ole löydetty työkaluja rikostorjuntaan tilausansoja vastaan.
3. Verkossa rikolliset ovat anonyymejä ja voivat tehdä tämänlaista rikollisuutta käytännössä mistä päin maailmaa tahansa. Toivomuksena onkin, että viranomaiset, pankit ja muut finanssilaitokset voisivat vaihtaa tiiviimmin tietoja uusista tilausansoista.
4. Viestintää tulisi pankkien ja maksupalveluiden tarjoajien välillä kehittää, jotta kommunikointi olisi tällaisen rikollisuuden torjuntaan liittyvien tapausten kanssa avoimempaa ja informaatio liikkuisi nopeammin.
5. Rikostorjuntaan pitäisi ensin saada selkeä oikeuskäytäntöön perustuva rangaistavuus, ja tämän jälkeen tilausansoja tehtailevat yritykset voitaisiin sulkea.

6 Pohdinta ja johtopäätökset

Tässä luvussa käydään läpi tutkimuksen johtopäätöksiä ja luotettavuutta. Tässä tehdään johtopäätökset ja tarkastellaan, onko tutkimukselle asetettuun kysymykseen löydetty vastaus ja onko tavoitteet saavutettu. Lisäksi käsitellään opinnäytetyön tekijän omaa pohdintaa, jonka tarkoitus on lisätä tilausansoihin liittyvien ongelmien käsittelyn näkökulmia. Tuloksissa arvioidaan myös opinnäytetyön eettisyyttä ja luotettavuutta

6.1 Tulosten tarkastelu

Tutkimusprosessi antoi paljon vastauksia kysymyksiin, mutta uudet vastaukset toivat mukanaan myös uusia kysymyksiä. Nettirikollisuus elää koko ajan, ja uusia huijauksia tulee jatkuvasti esille. Yhtenä havaintona on ollut se, kuinka lainsäädäntö ei pysy nettirikollisuuden mukana ja rikolliset osaavat käyttää tätä hyödykseen. Vastaajilta sai arvokkaita näkemyksiä rikostorjunnan vaiheista ja etenkin sen haasteista. Koska tilausansa on aiheena hyvin poikkeuksellinen ja asiantuntijoita on vähän, oli tärkeätä löytää ihmiset, jotka ovat näitä rikoksia tutkineet sekä tätä rikollisuutta vastaan taistelleet. Kyselyn tulokset auttoivat löytämään tilausansojen keskeisiä ja kriittisiä kysymyksiä sekä sijoittamaan kysymykset oikeisiin mittasuhteisiin. Kyselyyn olisi voinut valita enemmän virkavallan edustajia erityisesti Suomesta, mikä olisi tuonut tutkimukseen lisää syvyyttä ja vähentänyt poliisien ja finanssimaailman vastakkaisasettelua. Tutkimuskysymyksiä analysoin ja käsittelin pääasiassa rikostorjunnan, yhteistyön ja tilausansojen kasvun myötä sekä tilausansojen kuormittavuuden, kansainvälisen vertailun ja aikaisempien tutkimusten kautta. Vastaajien käsitykset rinnastettiin teoreettiseen viitekehykseen. Tutkimusta varten kyselyyn osallistuneet olivat yhtä mieltä siitä, että tätä rajat ylittävää rikollisuutta vastaan on vaikea taistella, varsinkin kun vastassa on kasvottomia vihollisia. Asiantuntijoiden vastaukset toivat esiin subjektiivisia mutta perusteltuja näkemyksiä tilausansojen haasteellisuudesta rikostorjunnassa. Kyselyssä ilmeni hajontaa sen suhteen, kuinka yhteistyötä tulisi kehittää. Yksityinen sektori painotti enemmän yhteistyötä viranomaisten kanssa ja tie-

donvaihtoa. Viranomaiset painottivat puolestaan enemmän sitä, että tulisi saada selkeämpi oikeuskäytäntöön perustuva rangaistavuus, jotta tilausansoja tehtailevat yritykset luopuisivat toiminnastaan. Yksityinen sektori nosti esille viranomaisia enemmän tilausansojen taustalla olevia yhtiöitä, jotka ovat vuosien aikana saaneet miljoonia euroja rikoshyötynä. Yksityisen sektorin mielestä poliisi päättää tutkimukset heti, kun kyseessä on ulkomainen veloittaja ja menetetty summa on kymmeniä tai korkeintaan satoja euroja.

Kannattaa pohtia, miksi tilausansat ovat saaneet suhteellisen rauhassa toimia Suomessa ja Euroopassa ilman, että niiden toimintaan olisi puututtu vuosien aikana. Tilausansojen toiminta on kasvanut vuosi vuodelta suuremmaksi, ja uhreja näillä tapauksilla on valtavasti. Maailmanlaajuiseen tietoverkkoteknologiaan tukeutuva monimuotoinen verkkorikollisuus on erityisen voimistuva uhka EU:ssa. Kun tarkastellaan kansainvälisen järjestäytyneen rikollisuuden selvittämistä, kohteena on yleensä tietoverkkoihin kohdistuva tutkinta. Tietoverkkoteknologiaan tukeutuva monimuotoinen ja usein pienistä osateoista koostuva järjestäytynyt verkkorikollisuus on voimistuva uhka ja kasvava haaste Euroopan eri viranomaisille ja yksityiselle sektorille. On ensiarvoisen tärkeää huomata, että viranomaisten ja elinkeinoelämän tulisi tehostaa yhteistyötä yli rajojen.

Yksityisten ihmisten ja finanssialan rikosilmoitusaktiivisuus on melko alhaista siihen määrään suhteutettuna, kuinka paljon huijauksia tehdään. Petoksiin ja huijauksiin on vaikea löytää pitävää näyttöä, rikosprosessi etenee hitaasti ja rikosten rajat ylittävä tekotapa pitää huolen siitä, että poliisin tietoon tulee vain marginaali osa tapauksista. Vuonna 2015 Heleniuksen (2017) mukaan maksuvälinepetosten tekopaikkana oli internet noin 70% tapauksista poliisin tilastojen mukaan. Vuonna 2016 luku nousi hieman (76 %). Kuluttajien asenne on usein se, että verkossa tapahtuviin rikoksiin ei ole suojaa, mikäli kysymyksessä on ns. pikkurikos. Poliisille ilmoitetuista maksuvälinepetoksista vuonna 2015 yhteensä 3,5% johti tuomioon oikeudessa (Taulukko 2 & Taulukko 6). Vuonna 2016 luku putosi 2,3% (Taulukko 2 & Taulukko 6). Vaikka poliisille ilmoitetaan enemmän maksuvälinepetoksia ja internetin käyttö rikoksissa lisääntyy, tuomioita jaetaan kuitenkin erittäin harvoin tekijöille.

Pankit ja finanssilaitokset ovat jo monta vuotta ihmetelleet sosiaalisen median kyvyttömyyttä torjua huijausmainoksia. Sosiaaliselle medialle tämä ongelma lienee yhdentekevä, sillä se saa mainostuloja eikä varsinaista riskiä ole. Sosiaalisen median alustoilla pystytään hyvin kohdentamaan mainoksia halutuille kohderyhmille. Kuten aikaisemmin todettiin, miehet tarttuvat paremmin elektroniikkaan, kun taas naiset lankeavat useammin tilasuansoihin, joissa tarjotaan kosmetiikkaa ja laihdutustuotteita. Kun miehet menettävät keskimäärin 147 euroa tilausansoille ja naisten keskimääräinen tappio on 74 euroa (Theorell 2017, 29.), voidaan sanoa, että tilausansat ovat varsinaisia rahantekokoneita. Pelkästään Suomessa yksittäinen pankki voi käsitellä tuhansia pelkkiä tilausansoja koskevia reklamaatioita vuodessa.

Moni tilausansa on yrittänyt vaikeuttaa kuluttajien yhteydenottoja, jotka koskevat rahojen palautusta. Ehdoissa on muun muassa kerrottu, kuinka järjestelmän automaattiajojen vuoksi jäsenyyttä ei voi irtisanoa ensimmäisten 24/48 tunnin aikana tai yhteydenottoa varten oleva sähköposti ei ota vastaan kuluttajien viestejä. Rekisteröitymiseen kuuluu useimmiten oheistarjous. Tutustumistarjousta ei lähetetä automaattisesti veloittajan taholta, vaan asiakas joutuu näkemään tässä vaivaa. Yleensä yhden euron iPhone-tarjouksissa ei luvata asiakkaille varsinaista puhelinta, vaan mahdollisuus voittaa se arvonnassa tietyn kestotilausjakson jälkeen. Asiakkaan pitää vahvistaa tiedot x (yleensä 3–5) päivän kuluessa profiilin kautta. Mikäli asiakas peruuttaa jäsenyyden x päivän sisään tai mikäli veloittaja ei pysty veloittamaan maksukorttia, menettää asiakas oikeuden tervetuliaislahjaan. Osoite pitää vahvistaa lähettämällä kopio jostakin laskusta, josta ilmenee nimi ja osoite.

Ongelmasta on hyvin vaikea päästä eroon, sillä vastassa on vain ns. kasvottomia vihollisia. Tärkein ja ehdottomasti suurin vaikutus on meillä jokaisella kortin käyttäjällä. Huolellisuus sekä turvallisuus ovat meille kaikille tärkeitä asioita, ja niihin kannattaa kiinnittää huomiota. Olemmeko yhtä huolellisia käyttäessämme korttia kuin lompakossa olevia seteleitä? Kumppanuusmarkkinointi on tuonut tilausansaongelmaan oman ulottuvuutensa. Se, mikä alkoi pop up -ikkunoina ja mobiilisisältöinä useita vuosia sitten, on siirtynyt ensin Facebookiin ja viime vuosina myös erilaisten bloggaajien ja kumppanuusmarkkinointiyhtiöiden kautta välttyviin mainoksiin sekä

sähköpostitarjouksiin. Useimmat mainoksista ovat asiallisia ja lainmukaisia, mutta kenellä on vastuu, jos tällainen mainos johtaakin tilausansaa. Aina ei ole helppoa selvittää, kuka tilausansan takana on, varsinkin kun jäljet johtavat usein ulkomaille.

6.2 Tutkimuksen etiikka

Eettinen ajattelu on kyvykkyys pohtia sekä omien että yhteisöjen arvojen kautta sitä, mikä jossain olosuhteessa on oikein tai väärin. Lakien ja eettisten kriteerien tuntemus auttaa konkreettisten päätöksien tekemisessä, mutta tutkimustyössä tehtävistä ratkaisusta ja valinnoista kantaa jokainen itse vastuun. Analyyttisessä etiikassa pohditaan sitä, onko jokin normatiivinen väite oikea tai väärä, kuvailevassa etiikassa taas tutkitaan moraalisen elämän eri rakenteita. Totuuden tavoittelua ja tiedon luotettavuutta ilmentävät normit määrittävät tutkijoita noudattamaan tieteellisen tutkimuksen menetelmiä ja esittämään totuudenmukaisia tuloksia, joiden oikeellisuus on tiedeyhteisön arvioitavissa. Tutkimusaineistojen kerääminen, käsittely ja asianmukainen arkistointi liittyvät olennaisesti tiedon luotettavuuteen ja tarkistettavuuteen. (Kuula 2011, 21–24.)

Internet voidaan ymmärtää sekä tutkimuksen subjektina, tutkimusvälineenä että aineiston alkuperänä. Internettutkimuksella voidaan mainita käytettävyystutkimukseen, mediahistorialliseen tutkimukseen, tekniseen kehitystyöhön, käyttäjähaastatteluihin tai teoreettiseen pohdintaan. Eettisesti internetin analysoiminen on erityisellä tavalla haasteellista. Todellisuuden, paikan, julkisen ja yksityisen tulkinta vaikuttaa internetin käyttäjien ja tutkijoiden käsitykseen virtuaalisesta ympäristöstä ja sen luonteesta. Samalla se vaikuttaa siihen, miten eettiset kysymykset internettutkimuksen yhteydessä luokitellaan. (Kuula 2011, 169, 193.)

Internet on nykyään käytetyin tiedonhankinnan väline. Internetin avulla on saatavissa paljon asiantuntijoiden tekemiä tilastoja, raportteja sekä opinnäytetöitä. Suurin osa internetin materiaalista on kuitenkin kaupallista tai yksittäisten henkilöiden tuottamaa eikä siten kovin luotettavaa tietoa. Internetissä olevan aineiston käytön vaikeus on usein myös se, että aineisto muuttuu nopeasti, joten siihen ei voi aina palata

myöhemmin. Toisaalta kehittämistyössä kannattaa hakea internetistä ja muista lähteistä muuta kuin tutkittua tietoa. Tiedonhankinnassa vaaditaan kriittisyyttä ja informaation lukutaitoa. Pitää osata havaita tiedontarve ja erilaisia tietolähteitä, arvioida tietoa kriittisesti, pohtia ja käyttää erilaisia tiedonhankintatapoja, erottaa tosiasiat, mielipiteet ja näkemykset toisistaan sekä valita ongelman ratkaisuun soveltuvin tieto ja mukauttaa sitä käytännön tarpeisiin. (Ojasalo ym. 2009, 31–32.)

6.3 Luotettavuus

Tapaustutkimuksessa toteutetun tutkimuksen mukaan laatua mitataan validiteetilla ja reliabiliteetilla. Reliabiliteetti ja validiteetti ovat Yinin (2009) mukaan lohkottavissa neljään eri osaan: ulkoiseen validiteettiin, reliabiliteettiin, sisäiseen validiteettiin sekä konstruktiovaliditeettiin. Tutkimuksellisuudessa reliaabelius eli luotettavuus viittaa mittaustulosten toistettavuuteen, joka on mahdollista todistaa oikeaksi erilaisilla menetelmillä. Reliaabeli tutkimus antaa toistettavia, ei sattumanvaraisia tuloksia. Validi eli pätevä tutkimus on puolestaan sellainen, jossa asetettu tutkimusmenetelmä mittaa oikeita asioita, yleensä mitä on tarkoitettu mitattavaksi. Kyseessä olevat käsitteet ovat peräisin kvantitatiivisen tutkimuksen maailmasta, kvalitatiivisessa tutkimuksessa niitä yleensä pyritään välttämään. Lähtökohtana kaikissa tutkimuksissa on se, että niissä arvioidaan luotettavuutta ja pätevyyttä. (Hirsijärvi ym. 2007, 226–228.)

Kyseinen taulukko perustuu Yinin (2009, 41) esittämään taulukkoon.

Vaatimus	Vaatimuksen toteutustapa	Tutkimuksen vaihe missä toteutetaan	Miten toteutettu tässä tutkimuksessa
Konstruktiovalideetti	Usean lähteen käyttäminen aineiston hankinnassa	Aineistonkeruu Raportin	Kyselyyn valittu henkilöitä eri organisaatioista eri puolilta Eurooppaa

	Todistusketjun luominen Tutkimusraportin arvioittaminen tärkeimmillä tiedonantajilla	kokoaminen	Monipuolinen taustamateriaali Tutkimusaineiston huolellinen käsittely Tutkimusraportin luetuttaminen asiantuntijoilla
Sisäinen validiteetti	Mallin soveltaminen Selityksen rakentaminen Kilpailevien selitysten toteaminen	Aineiston analyysi	Selityksien luonti tutkimusaineiston analysoinnilla
Ulkoinen validiteetti	Teorian käyttö yksittäistapaustutkimuksessa	Tutkimussuunnitelma	Tutkimustulosten vertailtavuus, keskeiset käsitteet ja tutkimuskohde on kuvattu ja määritelty
Reliabiliteetti	Tapaustutkimusprotokollan käyttö	Aineistonkeruu	Tutkimusaineiston huolellinen ja järjestelmällinen kerääminen ja käsittely

Taulukko 13: Validiteetin ja reliabiliteetin osa-alueiden testaaminen

Suunnitellessani tutkimusaineiston keräämistä tiesin sen olevan haastavaa tutkimuskohteen erityislaatuisuuden vuoksi. Aineistoa ei ollut saatavilla valmiina, vaan suurin osa kerättiin kyselyillä, haastatteluilla ja datan analysoinnilla. Kyselyyn osallistuvat vastasivat omien kokemuksiensa ja mielikuviensa perusteella, sillä he ovat työelämässä tutkineet tilausansoja. Osalla kyselyyn vastaajista oli kokemusta tilausansoista, eivätkä kaikki vastaajat olleet mukana suorassa rikostorjunnassa. Tutkimusaineisto perustui omaan subjektiiviseen näkemykseen tilausansojen merkityk-

sestä nettirikollisuuteen. Kyselylomakkeen vaarana on aina se, että vastaajat ymmärtävät kysymykset väärin, mikä voi heikentää aineiston luotettavuutta. Tässä tutkimuksessa kaikki kysymykset olivat tarkoituksella avoimia kysymyksiä, sillä vastausvaihtoehdoilla ei haluttu ohjata kyselyä tiettyyn suuntaan.

Aineistoon liittyviä mahdollisia puutteita yritin vähentää kahdella eri tavalla. Tavoittelin Euroopan alueelta mahdollisimman laajaa vastaajajoukkoa, joilla olisi erilaisia kokemuksia tilausansoista. Toinen tutkimusaineiston luotettavuutta lisäävä asia oli keskittyminen kyselylomakkeeseen. Keskityin kysymyksien selkeyteen, niiden muotoon sekä ymmärrettävyyteen. Kysymykset muotoituivat testaajien kanssa tehtyjen lopputulosten, kuten prosessikuvausten sekä selvittelyyn liittyvien tekijöiden, pohdinnan tuloksena. Tavoitteena oli tehdä kysymyksistä mahdollisimman selkeitä ja yksiselitteisiä, jotta tulkinnanvaraa ei syntyisi.

Keskusrikospoliisin edustaja kommentoi yhteistyötä tämän opinnäytetyön ja Keskusrikospoliisin välillä tilausansojen rikostorjunnassa.
”Tämä opinnäytetyö on täydellinen esimerkki monialaisesta lähestymistavasta Euroopan unionin monimutkaisiin turvallisuuskysymyksiin. Tutkimus on toteutettu käyttämällä useita tietojenkäsittelymenetelmiä uutispalveluista, internet hakukoneista, poliisin organisaatioista ja rahoituslaitoksista EU:ssa. Tutkimuksessa korostetaan, että rahan ja palvelujen vapaassa liikkumisessa EU:ssa on olemassa toimijoita, jotka yrittävät naamioida yrityksensä lailliseksi, mutta aiheuttavat edelleen huomattavia taloudellisia menetyksiä EU kansalaisille. Tämä johtuu toisinaan Euroopan oikeudellisen kehyksen ja poliisin käytäntöjen haasteista Euroopassa. Tutkimus on auttanut Suomen Keskusrikospoliisia ilmoittamaan uusien tietojenkalastelumenetelmien ilmiöstä laajemmalle eurooppalaiselle lainvalvontayhteisölle, ja se on erinomainen täydentävä tieto tulevaisuuden työlle EMPACT:in (European Multidisciplinary Platform Against Criminal Threats) lainvalvontaviranomaisten ryhmälle, joka kokoontuu säännöllisesti Euroopan lainvalvontavirastossa Europolissa, EU:n poliittisen toimintatavan 2018-2021 puitteissa” (Keskusrikopoliisi 2018.)

Opinnäytetyö esitetään kesäkuussa 2018 myös Oslossa, European Conference on Cyber Warfare and Security tilaisuudessa. Tähän liittyen konferenssin henkilöstö antoi arvionsa (Liite 22) opinnäytetyöstä heille lähetetyn tekstin perusteella.
” Tämä on erittäin mielenkiintoinen ja ajankohtainen tutkimus. Tämän tutkimuksen on kiireellisesti kiinnitettävä lainvalmistajien huomio ympäri maailmaa. Lisää vielä pohdintoja siitä, miten tämä voitaisiin saavuttaa” (European Conference on Cyber Warfare and Security 2018.)

6.4 Johtopäätökset

On selvää, että vastaajilla, joista useilla on vuosien kokemus tilausansoista, osaavat määritellä ongelmakohdat ja kehitysehdotukset. Opinnäytetyön tavoitteena oli tuottaa lisäinformaatiota nettirikollisuudesta, turvallisuudesta ja tilausansoista. Kerättyjen tietojen perusteella viranomaisille, pankeille sekä muille finanssilaitosten edustajille annetaan ideoita ja kehitystyökaluja, kuinka tilausansarikollisuutta vastaan voi taistella.

Internetissä tapahtuvat rikokset ovat lisääntyneet räjähdysmäisesti viime vuosien aikana, ja niiden määrä kasvaa tulevaisuudessa entisestään. Erityistä tukea ja valistusta tulisi keskittää ihmisille, joiden digitalisaation taidot eivät ole valtaväestön tasolla. Tällaisia kohderyhmiä on erityisesti ikäväestö ja digitalisaation ulkopuolelle jäävä väestö. Valistaminen ja tiedottaminen nousevat usein esille, kun puhutaan rikollisuudesta ja rikoksien torjunnasta. Kenelle kuuluu vastuu kuluttajien valistamisesta? Finanssiala usein ajattelee, että valistaminen ja tiedottaminen kuuluvat viranomaisille, joiden resurssiongelmat nousevat yleensä esteiksi laajamittaisessa kuluttajien valistamisessa.

Kyselyn perusteella oli selkeästi havaittavissa tietyt maat, joista tilausansoja johdetaan, tai ne ovat muulla tavalla linkittyneitä näihin maihin. Luvut eivät edusta acquirer-pankkeja, sillä nämä vaihtuvat usein tilausansayrityksillä, eikä sitä kautta voida tehdä johtopäätöksiä, mihin maahan jäljet johtavat. Myös IP-osoitteita on tut-

kittu, mutta ne ovat samalla tavalla vaihdettavissa olevia ja siksi epätarkkoja määrittelemään, mistä yrityksiä johdetaan. Kyselyn perusteella oli havaittavissa selkeä rakenne maiden välillä, mitä tuotteita tarjotaan. Yhdysvalloista ja Pohjois-Amerikasta tulee pääasiassa laihdutus- ja kosmetiikkatuotteita. Yhdysvalloista tulevia yrityksiä on myös huomattavasti hankalampi tutkia, sillä veloittajanimenä saattaa olla vain pitkä epämääräinen numerosarja.

Tutkimuksissa on nähty tilausansa sivustoja, joissa on ainoastaan muutettu sivustolla olleita värejä ja tilausansatuote on vaihdettu. Samana on pysynyt sivuston fontit, muu ulkoasu, yhteystiedot ja sama veloittajanimi. Moni ihmetteleekin ihmisten hyväuskoisuutta tilata tuotteita kyseisiltä yrityksiltä. Osa kuluttajista ei osaa aavistaa huijausta siitäkin huolimatta, että mediassa kirjoitetaan paljon tilausansoista. Viranomaiset varoittelevat ihmisiä tasaisin väliajoin omilla sivuillaan, ja pankit valistavat asiakkaitaan tilausansoista ja muista netin vaaroista. Minkälaista valistusta tarvittaisiin Euroopassa, jotta jokainen kuluttaja ymmärtäisi välttää näitä tilausansoja? Ovatko rikolliset keksineet todellisen lypsylehmän, johon riittää koko ajan uusia uhreja, ja tulovirta on sitä kautta takuuvarmaa?

Rikolliset ovat ymmärtäneet, kuinka pieni kiinnijäämisriksi tilausansoissa lopulta on. Yleinen keskustelu siitä, kuuluvatko nämä rikoslain vai kuluttajalain piiriin, ei ainakaan edesauta rikostorjunnan tehostamista. Tähänkin asiaan tulisi selkeästi määritellä, kuinka tilausansoja käsitellään lain näkökulmasta. Suurelle osalle viranomaisista ja pankkien edustajistakin on epäselvää, minkälaisista rikoksista on kysymys ja ovatko nämä edes rikoslain alaisia tekoja. Moni pankki on myös siirtänyt tilausansat asiakkaan omalle vastuulle ja vetoaa siihen, että asiakas ei ole lukenut ehtoja. Maksupalvelulain mukaan kortinhaltijan törkeä huolimattomuus tai myötävaikutus vahingon syntyyn voidaan katsoa sellaiseksi, että vastuu on kortinhaltijalla. Jos antaa maksukorttinsa tiedot lukematta tilausehtoja, voi kysymyksessä olla huolellisuusvelvoitteen laiminlyönti. Toisaalta moniko pankki tai finanssilaitos voi täysin kiistatta sanoa, että asiakas on käynyt samoilla sivuilla, joista pankki löytää tilaus- ja toimi-

tusehdot. Tämä asia on myös noussut esille muutamissa tutkinnoissa, eli ovatko yritykset tehneet kahdet erilaiset sivut yrityksestään ja pankille näytetään aidot ja lailliset sivut, joissa kaikki ehdot ja muut oikeudet ovat selkeästi esillä.

Tilausansoista on tehty erilaisia toimintamalleja, kuinka kuluttajia lähestytään. Tilausansan toiminta voi perustua ainakin kahteen eri malliin. Henkilö syöttää maksukorttinsa tiedot, jonka jälkeen kortille ilmaantuu veloituksia, joista ei ole sovittu. Tällaisessa tilanteessa pankilla/maksupalveluiden tarjoajalla on myös rooli tilanteen selvittämisessä. Toinen malli on lähettää ansaan joutuneelle perinteinen lasku ja jatkaa saatavien perintää jopa tuomioistuinkäsittelyyn asti. Näissä tilanteissa keskeinen toimija on mahdollinen perintäyhtiö tai muu taho, joka saatavia velkoo, sekä käräjäoikeudet.

Tilausansayritykset ovat saaneet vuosien aikana paljon kuluttajien maksukorttitietoja, ja aiheellinen huoli on, yrittävätkö nämä yritykset jalostaa tietoja eteenpäin. Myyvätkö yritykset asiakkaiden korttitietoja cardaus-sivustoille tai muille halukkaille? Ovatko tilausansat edelleen pinnalla tulevaisuudessa, vai onko jokin toinen ilmiö ajanut näistä ohi? Kuinka lainsäädäntöä voidaan muuttaa, jotta verkkorikollisia voidaan tuomita tehokkaammin eri oikeusasteissa? Miten pankit, finanssilaitokset ja eri viranomaiset tehostavat rikostorjuntaa? Tarjotaanko kuluttajille parempia palveluita, joissa turvallisuus on samalla tasolla kuin käyttäjäystävällisyys? Miten kuluttajat reagoivat? Tuleeko meistä kuluttajina entistä tietoisempia verkkorikollisuuden vaaroista ja osaammeko varoa uusia vaaroja, jotka odottavat jo nurkan takana? Onko tilausansarikollisuus sellaista, jolla rahoitetaan muunlaista rikollisuutta?

6.5 Kehittämisehdotukset

Jatkotutkimuksena tulisi tutkia samaa ilmiötä muutaman vuoden kuluttua lisää. Aihetta on tutkittu vähän opinnäytetyön näkökulmasta, aihe on ajankohtainen ja varmasti sitä myös lähitulevaisuudessa. Jatkotutkimus olisi tärkeää myös siitä näkökulmasta, että ilmiöstä ei ole tarpeeksi tutkimustietoa, kuinka rikostorjunnan vaikutukset näkyvät finanssilaitoksissa ja viranomaisissa. Tutkimuksen tuloksista nousi esille viisi tärkeää yksityiskohtaa kehittämisehdotukseksi. Nämä viisi yksityiskohtaa ovat:

1. Viranomaisten tulisi tiivistää yhteistyötä ja pyrkiä Euroopan laajuisesti selvittämään tekijät tilausansojen takana ja lopettamaan heidän toimintansa
2. Pankkien ja muiden finanssilaitoksien tulisi parantaa ennalta ehkäisevää toimintaa, ja pyrkiä minimoimaan veloitukset tilausansa yrityksiltä.
3. Kuluttajat tarvitsevat koko ajan valistusta kyseisenlaisista huijauksista ja erityistä huomiota tulisi kiinnittää kuluttajiin, joiden nettitaidot eivät ole muun väestön tasolla
4. Jos tilausansa perustuu korttiveloituksiin, pitäisi rahojen liikkuminen päästä pysäyttämään mahdollisimman nopeasti. Korttijärjestöt ja acquirer pankit suurempaan vastuuseen kenet hyväksytään kauppiaiksi
5. Sosiaalinen media ja muut harhaanjohtavia mainoksia julkaisevat alustat laajempaan vastuuseen sisällöstä.

Koska tutkimuksilla saadaan lisää tietoa tilausansoista, pystytään finanssilaitoksille antamaan parempaa tietoa reklamaatioiden kuormittavuudesta, joka taas vaikuttaa työmäärään ja työjonoihin. Finanssilaitokset ja korttijärjestöt hyötyvät tutkimuksista siten, miten ilmiötä tulisi ennalta ehkäistä, jotta se vaikuttaisi asiakkaisiin mahdollisimman vähän. Viranomaiset saavat tutkimuksista lisätietoa, jonka avulla pystytään parantamaan yksittäisten työntekijöiden osaamista sekä tietämystä erityisesti poliisissa. Näin päästään tehokkaammin vaikuttamaan mahdollisiin Suomessa oleviin toimijoihin.

Lähteet

Kirjat

Akerlof, G., Shiller, R. 2015. Phishing for Phools: The Economics of Manipulation and Deception. New Jersey: Princeton University Press

Benbasat, I., Goldstein D.K, & Mead M. 1987. The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 369-385.

Dubé, L. & Paré, G. 2003. Rigor in Information Systems Positivist. Case Research: Current practices, Trends and Recommendations. MIS Quartely. Vol. 27 No. 4, 597-635.

Eisenhardt, K. 1989. Building Theories from Case Study Research. Academy of Management Review.

Forss, M. 2014. Fobban sosiaalisen median selviytymisopas. Helsinki: CrimeTime

Gummesson, E. 2000. Qualitative methods in management research. Sage. Thousand Oaks

Haasio, A. 2013. Netin pimeä puoli. Helsinki: Suomalaisuuden kirjallisuuden seura

Heikkilä, T. 2014. Tilastollinen tutkimus. Helsinki: Edita Publishing Oy

Helopuro, S., Perttula, J., & Ristola, J-P. 2009. Sähköisen viestinnän tietosuoja. Helsinki: Talentum

Hietanen, M. 2015. Miten tunnistaa nettihuijari: Perusteellinen opas huijausten välttämiseen. Books on Demand

Hirsijärvi, S., Remes, P.& Sajavaara, P.2005.Tutki ja Kirjoita. Jyväskylä: Kustannusosakeyhtiö Tammi

Hirsijärvi, S., Remes, P.& Sajavaara, P.2007.Tutki ja Kirjoita. 13., osin uudistettu painos. Helsinki: Kustannusosakeyhtiö Tammi

Ilmarinen, V., Koskela, K.2015. Digitalisaatio: yritysjohdon käsikirja. Helsinki: Talentum Media Oy

Järvinen, P. 2010. Yksityisyys – turvaa digitaalinen kotirauhasi. Jyväskylä: WSOYPro

Kananen, J. 2010. Opinnäytetyön kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän Ammattikorkeakoulu

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyö. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän Ammattikorkeakoulu

Kuula, A. 2011. Tutkimusetiikka: aineistojen hankinta, käyttö ja säilytys. Tampere: Vastapaino

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo

Metsämuuronen, J. 2001. Laadullisen tutkimuksen perusteet. Helsinki: Methelp Ky.

Miles, M., Huberman, A. & Saldana, J. 2014. Qualitive Data Analysis – A Methods Sourcebook. 3. painos. Arizona: SAGE

Mäkelä, K. 2001. Talouselämän rikokset, rikosoikeus ja kriminaalipolitiikka. Saarijärvi: Gummerus Kirjapaino Oy

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: SanomaPro Oy.

Peltomäki, J., Norppa, K. 2015. Rikos meni verkkoon. Helsinki: Talentum.

Schmalleger, F., Pittaro, M. 2008. Crimes of the Internet. New Jersey: Pearson Education Ltd.

Pirinen, R. 2013. Towards Realization of Research and Development in a University of Applied Sciences. University of Eastern Finland.

Tolvanen, M., Kukkonen, R. 2011. Esitutkinta-ja pakkokeino-oikeuden perusteet. Helsinki: Talentum

Tuomi, J., Sarajärvi, A. 2012. Laadullinen tutkimus ja sisällönanalyysi. Vantaa: Kustannusosakeyhtiö Tammi

Trivers, R. 2011.Petos ja itsepetos ihmiselämässä. Helsinki: Hakapaino Oy

Virolainen, J., Pölönen, P. 2003. Rikosprosessin perusteet. Helsinki: WSOY Lakitieto

Yin, R.K.2009. Case Study Research Design and Methods. 4.painos. California: SAGE

Internet lähteet

Capgemini & BNP Paribas. 2017. World Payments Report. Viitattu 23.9.2017. https://www.worldpaymentsreport.com

Danske Bank. Maksupalvelulain keskeiset muutokset. Viitattu 30.8.2017. https://danskebank.fi/fi-fi/Sivut/maksupalvelulaki/Pages/Maksupalvelulainkeskeinensisältö.aspx

Eduskunta HE 32/2008 vp. 2008. Viitattu 22.8.2017. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_32+2008.pdf

Enforcement and European Consumer Centres. 2016. Misleading ”free” trials and subscription traps. Viitattu 28.8.2017. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=25915&no=8

ETLA raportit. 2015. Suomalainen teollinen internet – haasteesta mahdollisuudeksi. Viitattu 11.9.2017. https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-42.pdf

Euroopan Kuluttajakeskus Suomessa. 2014. Turvallinen maksaminen. Viitattu 26.9.2017. https://www.ecc.fi/Teemat/verkkokauppa/turvallinen-maksaminen/

European Banking Authority. 2014. Ohjeet internet-maksujen turvallisuudesta. Viitattu 22.8.2017. https://www.eba.europa.eu/documents/10180/1004450/EBA%202015%20Fl+Guidelines+on+internet+Payments.pdf/da6a28d2-505d-46c8-9a33-2c6a2ad3d0f8

European Comission. 2017. The European Comission and Member States consumer authorities ask social media companies to comply with EU consumer rules. Viitattu 26.9.2017. http://europa.eu/rapid/press-release_IP-17-631_en.htm

Eurostat. 2017. Internet users who bought or ordered goods or services for private use over the internet in the previous 12 months by age groups. Viitattu 20.8.2017. http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Internet_users_who_bought_or_ordered_goods_or_services_for_private_use_over_the_internet_in_the_previous_12_months_by_age_groups,_EU-28,_2007-2016_(%25_of_internet_users).png

Finanssiala. 2015. Suomi johtaa korttimaksamisessa. Viitattu 30.8.2017. http://www.finanssiala.fi/uutismajakka/Sivut/Suomi_johtaa_korttimaksamisessa.aspx

Heinonen, S. 2009. Sosiaalinen media, avauksia nettiyhteisöjen maailmaan ja vuorovaikutuksen uusiin muotoihin. TUTU-eJulkaisuja. Viitattu 11.9.2017. https://www.utu.fi/fi/yksikot/ffrc/julkaisut/e-tutu/Documents/eTutu_2009-1.pdf

Henkilötietolaki 22.4.1999/523. 1999. Viitattu 12.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Tietoyhteiskunnan kehittämiskeskus ry.2012. Fur ex machina. Viitattu 5.9.2017. https://www.slideshare.net/Tieke/fur-ex-machina

Kajantie, S. 2010. Ammattimainen rikollisuus tietoverkossa. Haaste 03/2010, 43. Viitattu 9.9.2017. http://www.haaste.om.fi/fi/index/lehtiarkisto/haaste32010/ammattimainenrikollisuustietoverkossa.html

Kauppalehti. 2016. Tällaisiin tilausansahuijauksiin pohjoismaalaiset astuvat. Viitattu 12.9.2017. https://m.kauppalehti.fi/uutiset/tallaisiin-tilausansahuijauksiin-pohjoismaalaiset-astuvat/jNrTHZ3j

Keskusrikospoliisi Tiedusteluosasto. 2013. Petosrikollisuus mukaan lukien vilpillinen ja harhaanjohtava markkinointi. Viitattu 23.9.2017. https://kauppakamari.fi/wp-content/uploads/2012/03/Yritysturvallisuuden-teematilannekuva-2013-petosrikollisuus.pdf

Kilpailu-ja kuluttajavirasto. 2016. Lausunto yleisen tietosuoja-asetuksen tietoyhteiskunnan palveluihin liittyvän lapsen suostumusta koskevasta 8 artiklasta. Viitattu 29.8.2017. https://www.kkv.fi/ratkaisut-ja-julkaisut/aloitteet-lausunnot-ja-kannanotot/2016/1.12.2016-lausunto-yleisen-tietosuoja-asetuksen-tietoyhteiskunnan-palveluihin-liittyvan-lapsen-suostu-musta-koskevasta-8-artiklasta/

Kilpailu-ja kuluttajavirasto. 2016. Viikon vinkki: Jos tarjous kuulostaa liian hyvältä ollakseen totta, se on harvoin totta. Viitattu 15.2.2018. https://www.kkv.fi/ajankohtaista/Uutiset/2016/viikon-vinkki-jos-tarjous-kuulostaa-liian-hyvalta-ollakseen-totta-se-on-harvoin-totta/

Kilpailu-ja kuluttajavirasto. 2018. Varo huijareita verkossa – kampanja varoittaa nettimaailman saalistajista. Viitattu 16.3.2018. https://www.kkv.fi/ajankohtaista/Tiedotteet/2018/varo-huijareita-verkossa--kampanja-varoittaa-nettimaailman-saalistajista/

Korttiturvallisuus.fi.2012. Olet tärkein osa maksukorttisi turvallisuutta. Viitattu 30.8.2017. https://www.korttiturvallisuus.fi/Ajankohtaista/Olet-tarkein-osa-maksukorttisi-turvallisuutta/

Korttiturvallisuus.fi. 2012. Laihdutuspillerit, ihovoiteet ja muut ravintolisät. Viitattu 15.2.2018. https://www.korttiturvallisuus.fi/Verkossa/Laihdutuspillerit-ihovoiteet-ja-muut-ravintolisat/

Kuluttajansuojalaki 1211/2013. 2013. Viitattu 28.8.2017. http://www.finlex.fi/fi/laki/alkup/2013/20131211#Lidp451516208

Lardot, R., Kaartinen. K. 2014. Rikoksia verkossa. Haaste 2/2014, 36. Viitattu 7.9.2017. http://www.haaste.om.fi/fi/index/lehtiarkisto/haaste22014/rikoksiaverkossa.html

Liikenne-ja viestintäministeriö. 2011. Kohti esteetöntä tietoyhteiskuntaa, toimenpideohjelma 2011-2015. Viitattu 11.9.2017. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78143/Ohjelmia_ja_strategioita_1-2011_Kohti_esteetonta_tietoyhteiskuntaa_lukulaite.pdf?sequence=2

Minilex. Maksuvälipetos on oikeudetonta käyttämistä. Viitattu 14.9.2017. https://www.minilex.fi/a/maksuvälinepetos-on-oikeudetonta-käyttämistä

Nets Group. 2017. Nets Rolls Out Preventative Fraud Service to Protect Online Consumers Across the Nordics. Viitattu 16.8.2017. https://www.nets.eu/Media-and-

press/news/Pages/Nets-Rolls-Out-Preventative-Fraud-Service-to-Protect-Online-Consumers-Across-the-Nordics.aspx

Perustuslaki 11.6.1999/731. 1999. Viitattu 12.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Poliisi. Makukorttirikollisuus on kasvava rikosilmiö. Viitattu 20.9.2017. http://www.poliisi.fi/rikokset/rikosilmioita/maksukorttirikollisuus

Rikoslaki 1 luku 1§ (16.8.1996/626). Viitattu 23.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=rikoslaki%2037#L1

Rikoslaki 1 luku 1§ (16.8.1996/626). Viitattu 23.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=rikoslaki%2037#L1

Rikoslaki 1 luku 5§ (16.8.1996/626). Viitattu 23.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=rikoslaki%2037#L1

Rikoslaki 1 luku 7§ (16.8.1996/626). Viitattu 23.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=rikoslaki%2037#L1

Rikoslaki 1 luku 10§ (16.8.1996/626). Viitattu 23.9.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=rikoslaki%2037#L1

Rikoslaki 37 luku (24.8.1990/769). 2017.Viitattu 16.8.2017. http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=maksuvälinepetos#L37

Suomen Pankki. 2016. Millä tavoin maksamme 2020-luvulla? Näkökulmia tulevaisuuden maksamisratkaisuihin. Viitattu 11.9.2017. https://www.suomenpankki.fi/globalassets/fi/raha-ja-maksaminen/maksujarjestelmat/suomen-pankki-katalystina-maksuneuvosto/maksuneuvoston_e_kirjanen_2016.pdf

Theorell, C. 2017. Subscription traps in 6 EU countries 2017. KANTAR SIFO. Viitattu 16.8.2107. https://forbrukereuropa.no/wp-content/uploads/2017/05/Summary_Subscription_traps_6_EU_countries_170424_Final_sifo_ECC.pdf

Tietosuojavaltuutetun toimisto. Sanastoa. Viitattu 12.9.2017. http://www.tietosuoja.fi/fi/index/sanasto.html

Tilastokeskus. Eräiden rikostyyppien kehitys 2012-2016. 2017. Viitattu 20.8.2017. http://www.stat.fi/til/rpk/2016/13/rpk_2016_13_2017-03-23_tau_001_fi.html

Tilastokeskus. Rangaistukset rikoksittain, 2009-2015 (käräjäoikeudet ja hovioikeus ensimmäisenä oikeusasteena. Viitattu 9.9.2017. http://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/StatFin__oik__syyttr/010_syyttr_tau_109_fi.px/table/tableViewLayout1/?rxid=46249e30-6373-49c0-96ab-3d829d64d42c

Tulli. 2016. Netistä ostamisen opas yksityishenkilölle. Viitattu 28.8.2017. http://tulli.fi/documents/2912305/3755702/Netistä+ostamisen+opas+yksityishenkilölle/9ffbd67d-9322-4b48-a3e0-e7e77715ee9a

Viestintävirasto – Kyberturvallisuuskeskus. 2017. Näin meitä huijataan, verkossa yleisesti tavattuja huijausmenetelmiä. Viitattu 14.8.2017. https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Nain_meita_huijataan.pdf

Viestintävirasto – Kyberturvallisuuskeskus. 2017. Vakavia seurauksia yrityksiin kohdennetusta sähköpostitunnusten kalastelusta. Viitattu 12.9.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/09/ttn201709051702.html

Julkaisemattomat lähteet

Sähköpostikeskustelut European Conference on Cyber Warfare and Security henkilön kanssa (Tulosteet kirjoittajan hallussa)

Sähköpostikeskustelut Europol henkilön kanssa (Tulosteet kirjoittajan hallussa)

Sähköpostikeskustelut Keskusrikospoliisin henkilön kanssa (Tulosteet kirjoittajan hallussa)

Sähköpostikeskustelut Poliisiammattikorkeakoulun henkilön kanssa (Tulosteet kirjoittajan hallussa)

Sähköpostikeskustelu Poliisihallituksen henkilön kanssa (Tulosteet kirjoittajan hallussa)

Kuviot

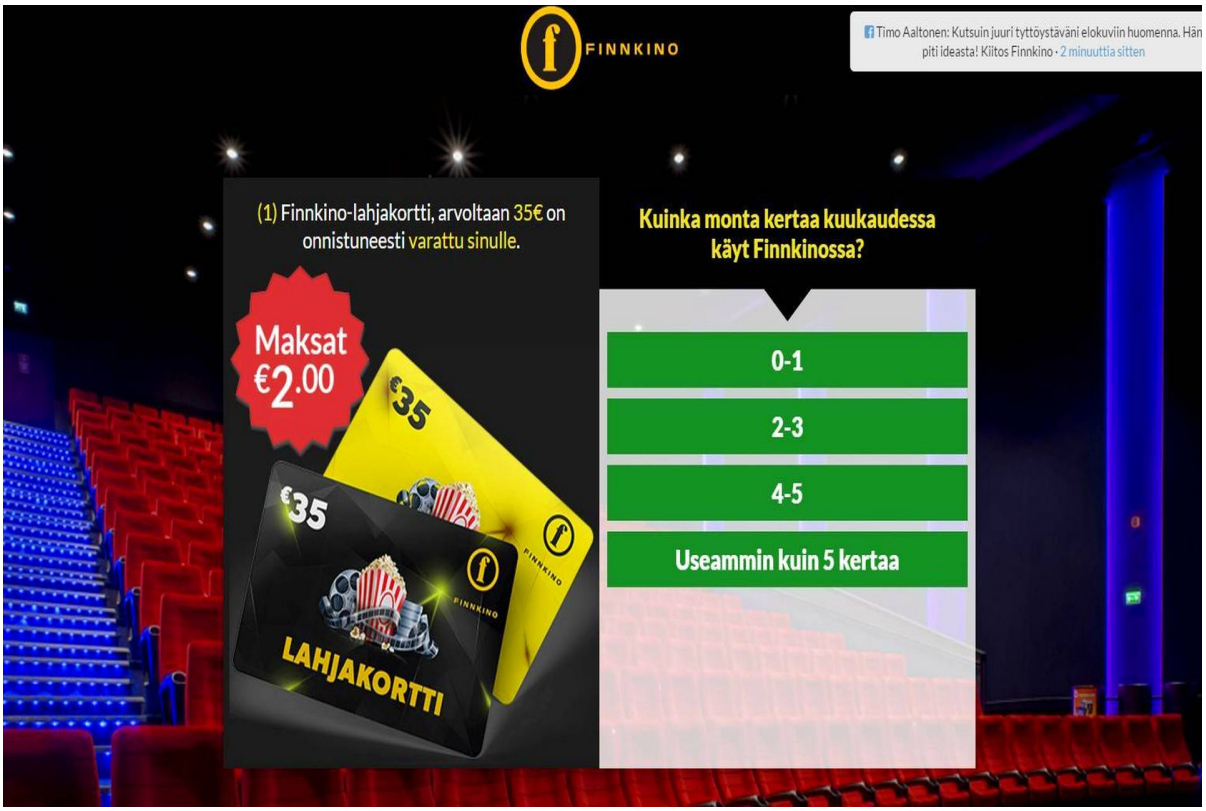
Taulukot

Liitteet

Liite 1: Tutkimuksen attribuutit. Tutkimuksen attribuutit on koottu oman näkemykseni mukaisesti mukaillen lähdeaineistoa (Dubé & Paré 2003; Miles & Huberman 1994; Pirinen 2013).

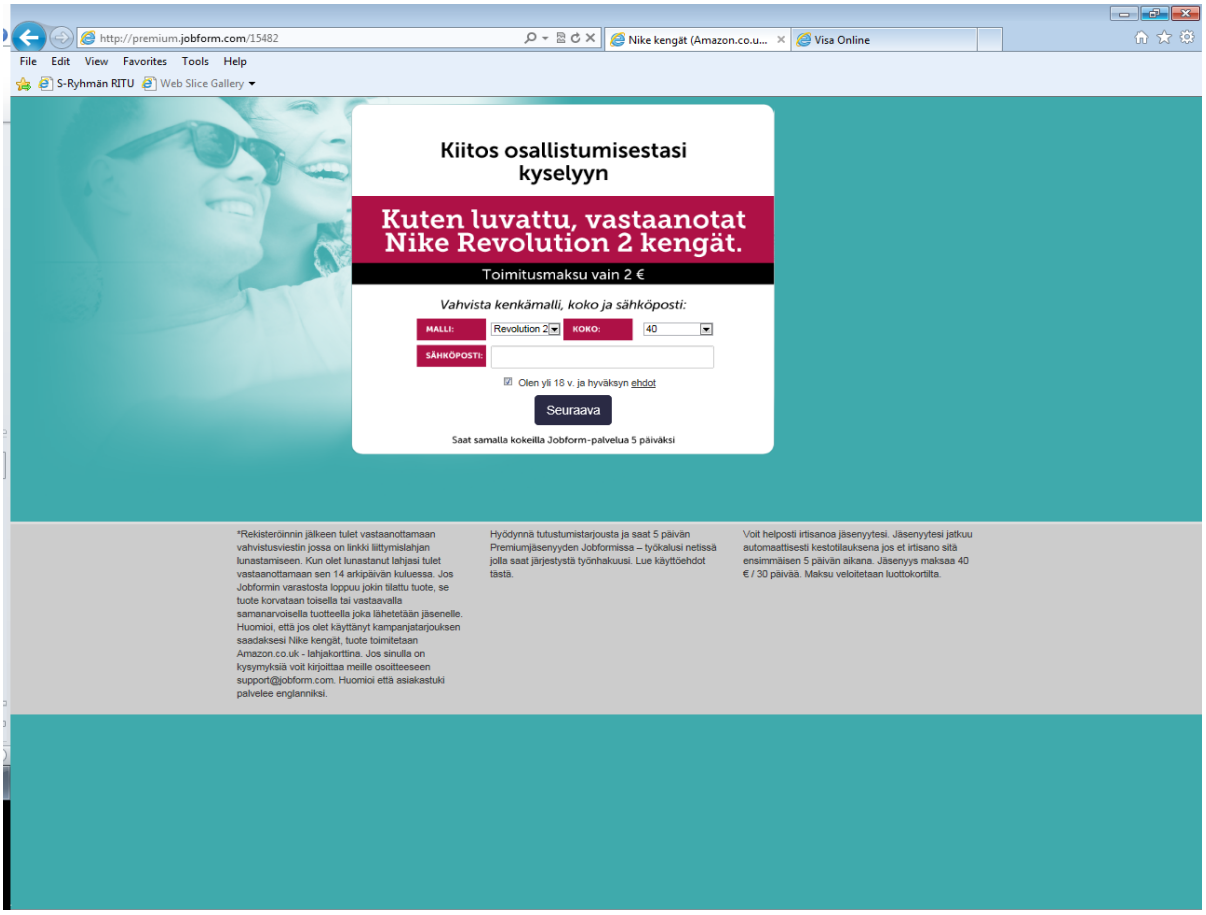
1. Tutkimuksen otsikko	Tilausansojen rikostorjunnan kehittämistä viranomaisten ja finanssialan yhteistyöllä
2. Tutkimuskysymykset	Mikä on suurin syy tilausansoihin liittyvän rikollisuuden suureen määrään? Miten tilausansoihin liittyvää rikollisuutta voisi parhaiten ennaltaehkäistä? Miten poliisi/pankki/maksupalveluiden tarjoaja voisi paremmin ennaltaehkäistä kyseisenlaista rikollisuutta? Minkälaista yhteistyötä poliisin/pankin ja maksupalveluiden tarjoajan pitäisi tehdä tilausansoihin liittyen?
3. Analysointiyksikkö	Rikostorjunnan kehittäminen tilausansoja vastaan digitaalisessa ympäristössä
4. Tutkimuksen luonne	Laadullinen ja määrällinen tutkimus
5. Tutkimuksen lähestymistapa	Induktiivinen ilmiötä kuvaileva tutkimus (rikollisuuden muuntautuminen digitalisaation myötä ja tilausansojen vaikutus petosrikollisuuden nousuun).
6. Metodologia	Tapaustutkimus (Case Study Analysis).
7. Tutkimuksen suunnittelukirjallisuus	Benbasat, Golstein & Mead 1987. Yin 2009. Dubé & Paré 2003.
8. Teoreettiset näkökulmat	Digitalisaatio, maksaminen ja rikollisuus
9. Tiedon keruumenetelmä	Haastattelukysymykset (n=73), haastateltavat (n=2).
10. Kyselylomake	Teemahaastattelu. Puolistrukturoidut haastattelukysymykset.
11.Analysointikirjallisuus	Miles, Huberman ja Saldaña 2014, Yin 2009.
12. Analyysin muoto	Haastatteluvastauksien jaoteltu/luokiteltu samankaltaisuus ja eriäviin vastauksiin. Aineiston tiivistys. Tiivistetystä aineistosta yhteenveto ja tutkimuksen päätulokset. Analyysi pohjautuu olemassa olevaan teoriaan.
13. Tuloksen merkitys	Luotu uusi näkökulma tilausansojen rikostorjuntaan. Tilausansojen torjunnan kehittämisen viitekehys, jossa yhteistyön, lainsäädännön, teknologian sekä kriittisten menestystekijöiden huomioiminen on pohjana rikostorjunnan analysoinnille ja kehittämiselle.
14. Tutkijan rooli	Haastatteluaineistosta analyysien ja johtopäätösten työstäminen.

Liite 2: Finnkinon nimissä tehty tilausansa kuva 1

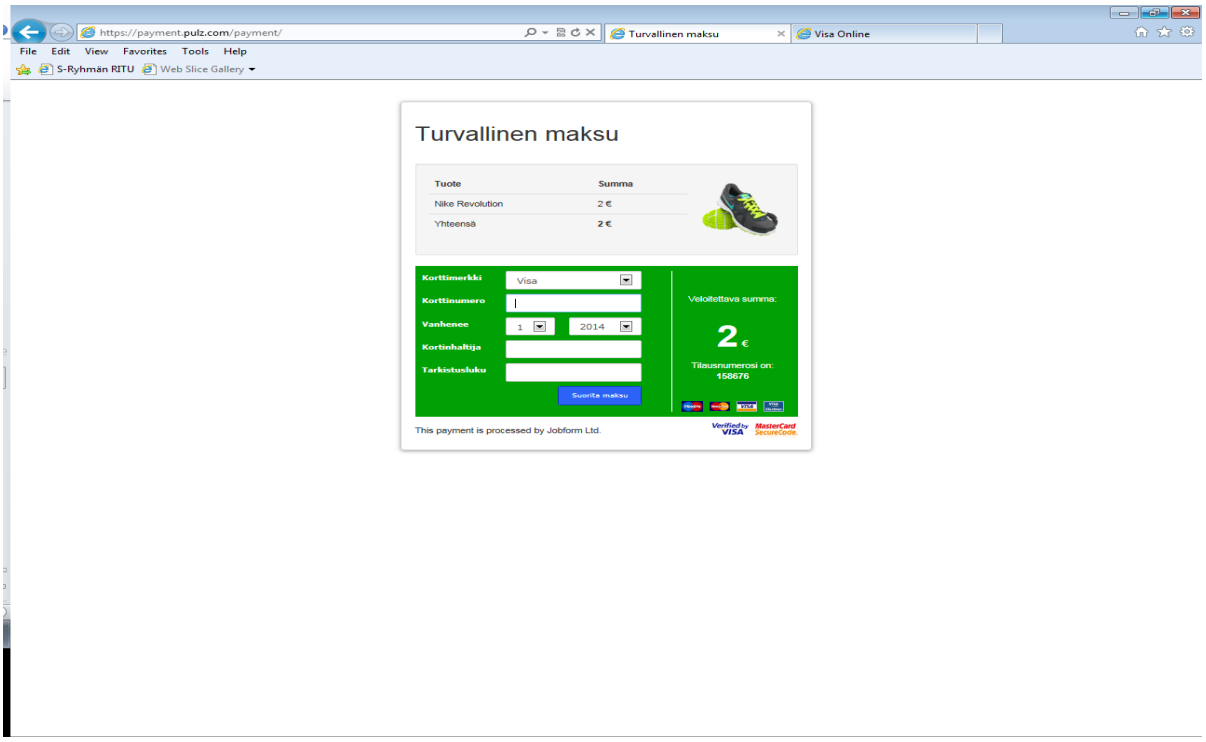


Liite 3: Finnkinon nimissä tehty tilausansa kuva 2

Liite 4: Jobform.com osallistumissivu



Liite 5: Jobform.com maksutietojen vahvistamissivu



Liite 6: Facebook mainos tilausansasta

Liite 7: Pointworldin nimissä tehty huijaussivusto

Liite 8: Henkilöhaastattelulla luodaan luottamusta huijattaviin

varustettuja Iphone 7 -puhelimia Suomen kansalaisille vain yhden euron hintaan. Apple toteuttaa tämän erikoistarjouksen yhteistyössä jakelukumppaninsa PointWorldin kanssa, ja voi näin **jakaa Iphone 7 -puhelimia likimain ilmaiseksi.** Mutta miksi näin käsittämätön kampanja on ylipäätään toteutettu?

Itä-Suomen yliopiston professori Paavo Kettunen vastaa kysymykseen seuraavasti: "Kolmessa vuodessa Applen markkinaosuus Suomessa putosi 21,4%, ja maailmanlaajuisesti se jäi selvästi Android-laitteiden jälkeen. Apple yrittääkin houkutella käyttäjiä takaisin leiriinsä tarjoamalla edullisia -puhelimia, jotka saatuaan kuluttajat kertoisivat Apple-tuotteista myös ystävilleen."

Itä-Suomen yliopiston professori Paavo Kettunen. (KUVA: © Perttu Pitkänen)

Liite 9: Toinen henkilöhaastattelu Pointworldin huijauksessa

Iphone 7 -puhelimensa kolmen päivän kuluttua.

"Ajattelin ensin, että tämä on varmaan joku vitsi, mutta tein omaa tutkimustani ja selvitin että **PointWorld** todella toteuttaa Apple-tuotteiden promootioita. Päätinkin siis sijoittaa yhden euron, koska eihän sillä nykyään saa edes aterian. Neljä päivää myöhemmin tutkin postiani ja siellähän se kiiltelevä laatikko Apple-logolla varustettuna olikin", kertoo Jarmo.

Jarmo Hyvärinen kertoi meille miten hän sai Applen puhelinta vain eurolla. (KUVA: © Perttu Pitkänen)

Ilmeisesti tällainen “käytännössä ilmainen“ markkinointitekniikka on suuressa suosiossa ulkomaalaisten suuryritysten keskuudessa. Esimerkiksi McDonald’s käynnisti samankaltaisen kampanjan vuonna 2013, tarjoten 20,000 ilmaista hampurilaista Facebookin kautta.

Liite 10: Tekaistuja käyttäjäkokemuksia Pointworldin huijauksessa

Liite 11: Esittelysivu tutkimuksesta kyselyyn vastaajille

Sivu 1

Hei,

Olen tekemässä ylemmän korkeakoulututkinnon lopputyötä, aiheena rikollisuuden muuntautuminen digiaikana ja pääpainona on tutkia tilausansoja. Lopputyön tavoitteena on saada parempi ja kattavampi kuva tilausansojen vaikutuksesta Euroopassa, lisätietoa viranomaisille kyseisestä ilmiöstä, sekä miettiä parannusehdotuksia rikoksentorjuntaan.

Kyselyssä on yhteensä 9 kysymystä ja kaikkia vastauksia käsitellään ehdottoman luottamuksellisesti. Organisaatioita ja yksittäisiä vastauksia ei tulla tässä työssä julkaisemaan, vaan tarkoitus on saada lisätietoa organisaatioilta jotka ovat ongelman ytimessä. Vastauksia ei myöskään käytetä missään muussa yhteydessä.

Mikäli asiasta herää kysymyksiä tai kommentteja, vastaan mielelläni lisäkysymyksiin.

Kiitos ajastasi ja osallistumisestasi!

Ystävällisin terveisin

Vesa Hietanen
vesa.hietanen@yahoo.com
Twitter: @vebekka
www.linkedin.com/in/vesa-hietanen-6965

Liite 12: Esitietojen kyselysivu tutkimuksessa

Rikollisuuden muuntautuminen digiaikana (Case: Tilausansat) 33 %

Minkä organisaation edustaja olet? *

pankki

Ammattinimike / Titteli *

Edell. Seur.

(muuta)

Liite 13: Tutkimuksen kysymyksiä

Haastattelukysymys 1: Milloin ensimmäisen kerran olit tekemisissä tilausansoihin liittyvän rikollisuuden kanssa?
Samankaltaisia vastauksia: **I**lmiö on alkanut 2010-luvulla ja vastaajat olivat tulleet tutuksi asian kanssa eri vuosina 2010-luvulla.
Huomiot ja eriävät vastaukset: Ensimmäiset tapaukset ovat tapahtuneet noin 20 vuotta sitten

Liite 14: Tutkimuksen kysymyksiä

Haastattelukysymys 2: Kuinka paljon tilausansoihin liittyvistä oman organisaatiosi reklamaatioista, asiakkaat EIVÄT ole tehneet rikosilmoitusta poliisille? (% arvio)
Samankaltaisia vastauksia: Noin 80-95%
Huomiot ja eriävät vastaukset: Noin 10-20%

Liite 15: Tutkimuksen kysymyksiä

Haastattelukysymys 3: Osaatteko omien tutkimuksien perusteella sanoa, mistä kyseinen rikollisuus tulee? (maa, kaupunki)
Samankaltaisia vastauksia: USA, Tanska, Iso-Britannia, Kypros, Viro, Saksa ja Slovakia
Huomiot ja eriävät vastaukset: Joitakin Afrikan maita, Curacao, Kiina, Romania, Ukraina, Venäjä ja Makedonia

Liite 16: Tutkimuksen kysymyksiä

Haastattelukysymys 4: Kuinka paljon tilausansoihin liittyvät reklamaatiot työllistävät itseäsi/osastoasi?
Samankaltaisia vastauksia: Kyseessä on monen finanssilaitoksen kohdalla ollut suurin yksittäinen aihe, josta asiakkaat ovat reklamoineet, Arvio on noin 30-35 % kaikista reklamaatioista. Moni tilausansoihin osallistuneista ei kuitenkaan koskaan tee asiasta rikosilmoitusta tai reklamaatiota.
Huomiot ja eriävät vastaukset: Arviona on että 10%-15 % reklamaatioista koskee tilausansoja.

Liite 17: Tutkimuksen kysymyksiä

Haastattelukysymys 5: Mikä on mielestäsi suurin syy tilausansoihin liittyvän rikollisuuden suureen määrään?
Samankaltaisia vastauksia: Sosiaalisten medioiden lisääntyminen, kuluttajien herkkäuskoisuus, linkit ns. luotettavilta tahoilta sekä se, että useimmissa maissa kyse ei ole rikollisesta toiminnasta, vaan kuluttajan harhaanjohtamisesta. Tilausansasivusto on helppo ja nopea pistää pystyyn ja houkutteleviin mainoksiin tarttuu nopeasti iso määrä ihmisiä. Riski tilausansalla saatujen rahojen menettämisestä on pieni ja olematon kiinnijäämisriski erityisesti rajat ylittävissä huijauksissa.
Huomiot ja eriävät vastaukset: Tilausansojen rakentajat ovat nopeampia kehittämään ansoja kuin pankit torjumaan niitä. Kortin käyttäjien hyväuskoisuus ja ahneus yhdistettynä tasokkaaseen nettigrafiikkaan helpottaa asiaa. Suomessa on kasvettu olemaan auktoriteettiuskoisia, sekä luottamaan siihen, että kaupassa tuotteessa näkyvä hinta on se, mitä joudut siitä kassalla maksamaan.

Liite 18: Tutkimuksen kysymyksiä

Haastattelukysymys 6: Miten mielestäsi tilausansoihin liittyvää rikollisuutta voisi parhaiten ennaltaehkäistä?
Samankaltaisia vastauksia: Ihmisiä on syytä jatkuvasti tiedottaa ilmiöstä. Muita mahdollisuuksia olisi saada esim. Facebook ja muut harhaanjohtavia mainoksia julkaisevat alustat laajempaan vastuuseen sisällöstä. Kehittämällä pankkien järjestelmiä siten, että ne entistä paremmin pystyvät tunnistamaan tilausansat ja estämään kortin käytös ko. sivustoilla.
Huomiot ja eriävät vastaukset: Esitutkinta ja rikossyytteet asiakasmanipuloinnista ja harhaanjohtamisesta. Myös varoitukset mediassa toimivat. Tilausansa yritykset käyttävät härskisti hyväksi esim. tunnettuja brändejä huijauksiin.

Liite 19: Tutkimuksen kysymyksiä

Haastattelukysymys 7: Miten toivot, että poliisi/pankki/maksupalveluiden tarjoaja voisi paremmin ennaltaehkäistä kyseisenlaista rikollisuutta?
Samankaltaisia vastauksia: Poliisi ei vaikuta tekevän yhteistyötä sisäisesti tai erityisesti eri maiden välillä, vaikka rikoshyödyt ovat miljoonia euroja. Hyvä globaali yhteistyö pankkien ja poliisin välillä on tarpeen. Toimintaan pitäisi pystyä puuttumaan niin nopeasti, ettei se olisi houkuttelevaa. Jos tilausansa perustuu korttiveloituksiin, pitäisi rahojen liikkuminen päästä pysäyttämään mahdollisimman nopeasti.
Huomiot ja eriävät vastaukset: Poliisitutkinta, johon liitetään takavarikoita ja muita pakkotoimenpiteitä. Rikostorjunnan keskittäminen tämän tyyppisiin rikollisuuden muotoihin, jotka varmasti muuttavat muotoaan ja kasvavat. Uhrien auttaminen silloin, kun heihin kohdistetaan voimakasta perinnällä uhkaamista.

Liite 20: Tutkimuksen kysymyksiä

Haastattelukysymys 8: Minkälaista yhteistyötä toivoisit poliisin/pankin/maksupalveluiden tarjoajan kanssa tilausansoihin liittyen?
Samankaltaisia vastauksia: Laajaa tiedonvaihtoa, jotta uuteen huijaukseen pystyttäisiin reagoimaan etupainotteisesti. Laajempi yhteinen info-foorumi, jossa tiedon vaihtoa ilmiön vähentämiseksi ja kitkemiseksi (tiedon keruu, eri kokemukset, toimenpide-ehdotukset). Palvelee kaikkia toimijoita ja vähentää turhaa työtä ja tehostaa ajankäyttöä. Poliisille paremmat mahdollisuudet tunnistaa ja sulkea väärinkäyttöön valjastettuja palvelimia. Poliisien olisi hyvä pysyä ajan tasalla liikkeellä olevista huijauksista, jotta tiedottaminen asioista olisi myös poliisin kohdalta ajantasaista.
Huomiot ja eriävät vastaukset: Asiaan pitäisi ensin saada selkeä oikeuskäytäntöön perustuva rangaistavuus, ja tämän jälkeen tilausansoja tehtailevat firmat pitäisi pistää kiinni. Rangaistavuuden kautta eri viranomaisilla olisi mahdollisuus lähettää tilausansasivustoista alasottopyyntöjä. Nyt sellaista mahdollisuutta ei ole, sillä kyseessä ei ole tietoturvaongelma, koska teko ei ole sinänsä laitonta. Kyseessä on enemmän kuluttajariitaasia. Turvallisuuspaketteja lisämaksusta riskiryhmäläisille.

Liite 21: Tiivistelmä opinnäytetyöstä ECCWS konferenssissa Oslossa

Crime prevention: How to avoid subscription traps?

Vesa Hietanen and Jyri Rajamäki
Laurea University of Applied Sciences, Research, Innovative Digital Services of the Future, Finland
vesa.hietanen@yahoo.com
jyri.rajamaki@laurea.fi

In Europe, 3.5 million consumers are estimated to have been affected by subscription traps over the past three years. This is more frequently the case now than ever before due to digital evolution which offers more opportunities to communicate and gather information from consumers. Subscription traps are offers on cheap products that lead to costly subscriptions for those who accept them. Usually, the consumer needs to pay with a debit or credit card to claim the offer. Although each free trial should be examined on a case-by-case basis, some practices are considered illegal upfront. Subscription traps include practices that are breaches of EU law or include grey zone practices that push the boundaries of what is legal or are currently untested by EU law.

This case study focuses on two research questions: 1) what circumstances creates subscription traps? and 2) how do we fight against them? A survey was conducted to professionals who had experience in subscription traps and cybercrime. The respondents (n=73) consisted of lawyers, prosecutors, police officers, risk specialists, payment card specialists, credit managers and product specialists from 14 countries. Furthermore, two individuals who did not participate in the survey were interviewed.

Research findings explain why the phenomenon of subscription traps has exploded exponentially in Europe. Furthermore, the study suggests that in the prevention of such traps the police should have better tools and methods for pre-trial investigations and charges should be made to criminals for customer manipulation and misrepresentation. Support, awareness, and education should be focused on the individuals whose digitalization skills are not on a par with the majority.

This case study concludes that legislative changes should be made. Legislation should include clear penalties based on legal practices through which the activities of the responsible parties behind these subscription traps can be shut down. The authorities and the private sector should consider forms of cooperation in order to enhance the prevention of such crime. Additionally, it was found out that for a large number of authorities and financial representatives, the kind of crime to which subscription traps belong remained unclear.

Keywords: cybercrime, subscription traps, digitalization, phishing, payments, legislation

Liite 22: ECCWS palaute opinnäytetyöstä

ECCWS

17th European Conference on Cyber Warfare and Security
28 - 29 June 2018, Oslo, Norway

Double Blind Review Form

Thank you for agreeing to be a reviewer. We are keen to ensure a high standard of papers for this conference. We are eager to help authors who may not yet have achieved a suitable skill in writing academic papers to the necessary quality. To this end we would be grateful if you would, wherever possible, provide constructive advice as to how they can make the paper more acceptable for presentation at a quality academic conference.

Please complete the table below and rate the paper on the issues described. As with all double-blind reviewing any comments you make will be passed to the authors on an anonymous basis.

We try to give feedback to authors within 2 weeks. Please try to complete the review within that time.

Reviewer reference	EWS-42	Review Due Date	ASAP
Paper Title	Crime prevention: How to avoid subscription traps?		
Conference Track		Submission Type	**masters**

To check the relevance of the paper you may like to consult the call for papers which you can find here:
http://www.academic-conferences.org/conferences/icickm/icickm-call-for-papers/
Which category or categories best describes this paper:

Empirical research	√
Theoretical paper that advances/challenges/adapts current theory	
Theoretical paper reviewing and/or synthesising current theory	
Other - please specify	

	Please rate the following: (5 excellent, 1 poor)	5	4	3	2	1	N/A
1	Relevance to the themes of this conference	√					
2	Contribution to academic debate	√					
3	Structure of the paper	√					
4	Standard of English – indicate below if you think the paper needs proof-reading		√				
5	Appropriateness of abstract as a description of the paper	√					
6	Appropriateness and number of keywords/key phrases	√					
7	Appropriateness of the research/study method	√					
8	Literature review adequately provided		√				
9	Relevance and clarity of drawings, graphs and tables	√					
10	Results and findings adequately reported	√					
11	Discussion and conclusions	√					
12	Reference list, adequate and correctly cited	√					

Taking into consideration the type of submission and the track the paper has been submitted to (see above), please give an overall rating out of 10 for this paper in terms of its contribution to this conference.	9

Can this paper be accepted for presentation at the conference?

Yes - no changes		Yes - with minor revisions	√	Yes - with major revisions		No	

Thank you for your help.
Please return this form to kelly.proctor@academic-conferences.org