KYBERRIKOLLISUUS IHMISEN ARJESSA

Aki Somerkallio
Mari Takkinen

03/2018

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

Tekijä	Tutkinto/kurssi ja opinnäytetyö/nimike
Aki Somerkallio Mari Takkinen	Poliisi (AMK)
Julkaisun nimi Kyberrikollisuus ihmisen arjessa	Julkisuusaste Julkinen
Ohjaajat ja opintoaine/opetustiimi Matti Hänti, ylikomisario Juha-Pekka Oskanen, ylikonstaapeli	Opinnäytetyön muoto Toiminnallinen opinnäytetyö

Tiivistelmä

Tässä opinnäytetyössä tarkastellaan kyberrikollisuutta tavallisen ihmisen näkökulmasta. Työssä nostetaan esille sellaisia verkossa tapahtuvia rikoksia ja uhkia, joita kuka tahansa verkon käyttäjä saattaa arjessaan kohdata.

Kyberrikoksilla tarkoitetaan verkkoympäristössä tapahtuvaa tai sitä ympäristönä hyväksikäyttävää rikollisuutta. Verkkoa käytetään koko ajan enemmän ja sen merkitys lähes jokaisen ihmisen arjessa on kasvanut viimeisen vuosikymmenen aikana. Verkossa käydään kauppaa, jaetaan tietoa ja se on mahdollistanut yhä useampien palveluiden käytön virtuaalisesti. Tämä digitaalinen ulottuvuus, jossa nykyään tapahtuu myös paljon rahaliikennettä, vetää puoleensa rikollisia tuottojen toivossa. Verkkoa käyttäessä ihmiset joutuvat yhä useammin rikoksien uhreiksi ja tietämättään saattavat edesauttaa rikollista toimintaa. Opinnäytetyössä käydään läpi kyberrikollisuuden tällä hetkellä yleisimpiä ilmenemismuotoja ja tarjotaan niihin teoriatietoa.

Teoriapohjaa varten on myös haastateltu aihealueen asiantuntijoita. Haastatteluiden kautta kävi ilmi, että haasteita kyberrikollisuutta torjuttaessa asettaa erityisesti kansalaisten tietoisuuden vähäisyys verkossa tapahtuvasta rikollisuudesta. Opinnäytetyön lopputuloksena syntyi kysymyspohja nettitestiin, joka toivotaan jossain vaiheessa siirrettävän verkkoon kaikkien ihmisten saataville. Testin tarkoitus on lisätä ihmisten valveutuneisuutta, tietoisuutta sekä ymmärrystä verkossa tapahtuvasta rikollisuudesta ja toimia näin myös ennalta estävänä hankkeena.

Sivumäärä	Tarkastuskuukausi ja vuosi	Opinnäytetyökoodi (OPS)
46	02/2018	AMK2015 ONT

Avainsanat

kyberrikollisuus, verkkorikollisuus, kyberrikos, verkkorikos, poliisi, ennalta estävä toiminta, EET

SISÄLLYS

TERMINOLOGIAA

Kyberrikollisuus: Tunnetaan myös nimillä tietoverkkorikollisuus ja verkkorikollisuus. Tapahtuu verkossa tai on rikollista toimintaa jonka verkon toimintaympäristö mahdollistaa.

Digitalisaatio: Tietotekniikan yleistymistä arkielämän toiminnoissa.

Sähköistyminen: Palvelut ja toimet siirtyvät verkkoon sähköisessä muodossa ollen näin riippumattomia ajasta ja paikasta.

Tor -verkko: Alun perin Yhdysvaltain ilmavoimien viestintätarpeisiin kehitetty ”Sipuli-verkko”. Tor -verkossa tietoliikenne kiertää usean eri tietokoneen kautta salattuna. Tietoliikenteen alku ja loppupäätä on näin lähes mahdoton yhdistää.

Kryptaus: Kryptauksen, eli salauksen avulla salausjärjestelmä salakirjoittaa selkotekstin, jolloin vain viestin valtuutetut ovat kykeneviä lukemaan viestin sisällön.

Virtuaalivaluutta: Digitaalista valuuttaa, jonka arvo perustuu valuutan käyttäjien sopimuksiin ja vaihtelee käyttäjien kysynnän ja tarjonnan mukaan. Ei virallinen valuutta.

Fiat -valuutta: Paperi / rautarahaa, jonka fyysinen arvo ja todellinen arvo eivät kohtaa, eli paperirahan materiaalinen arvo ei ole sama, kuin paperirahan arvo valuuttana.

Internet of Things: Esineiden internet tarkoittaa internet-verkon laajentumista ja leviämistä koneisiin ja laitteisiin, jolloin näitä voidaan ohjata, mitata ja sensoroida internet-verkon yli.

Deepweb: Internetissä olevaa sisältöä, jota ei löydä hakukoneiden avulla.

Darknet: Internetissä oleva yksityinen verkko, johon pääsevät vain luotetut ja tunnetut tahot. Tor -verkko on osa darknetiä.

Bottiverkko: Joukko tietokoneita tai laitteita, jotka on saastutettu haittaohjelmalla toimimaan haittaohjelman tekijän päämäärien mukaan.

Haittaohjelma: Ohjelma, joka ujutetaan tietokoneelle yleensä petollisesti ja joka kerää tietokoneelta tietoa tai muutoin käyttää tietokonetta haittaohjelman liikkeellelaskijan hyväksi.

Pankkihaittaohjelma: Haittaohjelma, joka tietokoneelle asennuttuaan pyrkii harhauttamaan käyttäjän antamaan verkkopankin tunnusluvun ja salasanan ohjelman tekijän käyttöön.

Ransomware: Haittaohjelma, jota hyväksikäyttäen kiristetään uhrilta rahaa.

Scareware: Haittaohjelma, jolla pelotellaan uhria toimimaan halutulla tavalla.

1 JOHDANTO

Tämä opinnäytetyö käsittelee kyberrikollisuutta ihmisten arjessa. Yhteiskunta on digitalisoitunut ja sähköistynyt jo kymmeniä vuosia. Erityistä kehitystä on tapahtunut viimeisten vuosien aikana. Digitalisaatiolla tarkoitetaan teknologisen kehityksen enenevässä määrin mukanaan tuomaa digitaalitekniikkaa ihmisen arkitoimintoihin (Koiranen ym. 2016). Sähköistymisellä tarkoitetaan erilaisten palveluiden ja toimien siirtymistä sähköisessä muodossa verkkoon, jolloin ne ovat saatavilla ajasta ja paikasta riippumatta (Vehviläinen 2017). Siinä missä digitalisaatio ja sähköistyminen tuovat elämää ja arkea helpottavia ratkaisuja, ne tuovat mukanaan myös varjopuolen kyberrikollisuuden muodossa.

Rikollisuuden muotona internetissä tapahtuvat rikokset ovat tällä hetkellä hyvin ajankohtaisia, sillä niitä tulee poliisille tutkittavaksi koko ajan enemmän. Kyberrikollisuus on noussut voimakkaammin esiin myös poliisin viestinnässä viimeisen parin vuoden aikana. Kyberrikollisuuden torjunta on huomioitu EU:n sisäisen turvallisuuden strategian yhdeksi tärkeimmistä painopistealueista vuosille 2015−2020 (Sisäministeriö 2017). Ensimmäinen kansallinen kyberturvallisuusstrategia julkaistiin vasta vuonna 2013 ja hyväksyttiin vuonna 2014. Suomen kyberturvallisuusstrategian toimeenpano-ohjelmassa 2017–2020 todetaan kyberturvallisuuden olevan yhä keskeisempää jatkuvan digitalisoitumisen myötä. (Turvallisuuskomitea 2017, 4-5.)

Opinnäytetyö pureutuu kyberrikollisuuteen ennalta estävästä näkökulmasta. Opinnäytetyössä käydään läpi mitä kyberrikollisuus on, miten se ilmenee nyky-yhteiskunnassa ja minkälaisia haasteita se tuo mukanaan. Opinnäytetyön tavoitteena on rakentaa pohja virtuaaliselle testille joka tulevaisuudessa tulisi ihmisten saataville internetiin. Testin avulla voidaan lisätä ihmisten tietoisuutta internetin kautta tapahtuvista erilaisista huijauksista ja rikoksista. Testin avulla pyritään herättämään ihmisten tarkkaavaisuutta ja lisäämään heidän valveutuneisuutta internetissä piilevien riskien havaitsemiseen. Vastaavanlainen testi on aikanaan tehty poliisin Harmaa talous - musta tulevaisuus -kampanjaan. Kyseinen testi saavutti paljon näkyvyyttä mediassa ja tavoitti esillä ollessaan suuren määrän ihmisiä. Tämän opinnäytetyön tuotoksella pyritään saamaan yhtä suurta näkyvyyttä ja levinneisyyttä ihmisten keskuudessa. Näin on myös parhaiten saavutettavissa opinnäytetyön perustana ollut ennalta estävä näkökulma.

Kyberrikollisuuden muodot kehittyvät ja muuttuvat jatkuvasti. Opinnäytetyössä pyritään käyttämään mahdollisimman ajan tasalla olevia lähteitä ja teoksia. Haasteita kyberrikollisuuteen liittyville lähteille tuokin juuri se, että ne usein jo julkaistessaan ovat ainakin osaksi vanhentuneita. Tässä opinnäytetyössä käytettyä aihealueen tarkempaa terminologiaa koskeva osio löytyy opinnäytetyön alusta. Opinnäytetyötä varten on lisäksi haastateltu Keskusrikospoliisin kyberrikostorjuntakeskuksen rikosylikomisario Tero Muurmania ja rikoskomisario Sami Siurolaa sekä Viestintäviraston kyberturvallisuuskeskuksen erityisasiantuntijaa Antti Kurittua.

2 KYBERRIKOLLISUUDEN ENNALTA ESTÄMINEN

EET eli ennalta estävä toiminta on tärkeimpiä, ellei jopa tärkein tapa taistella kyberrikollisuutta vastaan. Tietoverkkorikosten ennalta estäminen, selvittäminen ja syyteharkintaan saattaminen on pääsääntöisesti poliisin työtä, mutta poliisin lisäksi myös muita viranomaisia osallistuu kyberrikosten selvittämiseen ja niiden ennalta estämiseen. Ennalta estävää työtä tulee tehdä laajasti yhteistyössä eri tahojen kanssa, jotta sen sanoma ja levinneisyys olisi mahdollisimman tehokasta ja tavoittaisi mahdollisimman suuria ihmismääriä.

2.1 Poliisin ennalta estävä toiminta

Poliisin ennalta estävän toiminnan strategian visio kiteytyy lauseeseen "Vähemmän rikoksia, enemmän turvallisuutta - yhdessä ennakoivasti toimien". Keskeisiä asioita poliisin ennalta estävässä toiminnassa ovat ennen kaikkea väkivallan vähentäminen, tietojohtoisuuden vahvistaminen, verkostoyhteistyön tehostaminen sekä sosiaalisen median hyödyntäminen. (Poliisi 2018, B.)

Poliisin yksi tärkeistä tehtävistä on jo tapahtuneiden rikosten selvittämisen lisäksi ennalta estää uusien rikosten syntymistä. Poliisilain 1 luvun 1 § (22.7.2011/872) alkuosa määrittelee poliisille kuuluviksi tehtäviksi seuraavaa:

> *"Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä."*

Poliisin perustehtäviin kuuluu toimia kansalaisten hyvinvointiin kuuluvien turvallisuuspalvelujen tuottajana. Poliisi toimii yhteiskuntamme yleisen järjestyksen ylläpitäjänä sekä torjuu ja ennaltaehkäisee rikollisuutta. (Poliisi 2018, C.) Rikosten ennalta estäminen sekä

rikoksen uhriksi joutumisen estäminen kuuluu siis hyvin merkityksellisenä osana poliisin työhön.

Turvallisuutta voidaan pitää ihmisten yhtenä tärkeimmistä perusodotuksista. Jotta yksilö voi tuntea olonsa turvalliseksi, edellyttää se myös turvallista elinympäristöä (Rapila 2010). Nykyään tämä elinympäristö on enenevässä määrin levittäytynyt myös tietoverkkoihin, ja ihmisten turvallista asioimista verkossa tulisi myös poliisin puolelta pyrkiä edistämään niin hyvin kuin se on mahdollista.

Suomen poliisi on saanut nauttia poikkeuksellisen korkeaa luottamusta kansalaisiltaan muihin maihin verrattuna. Vuonna 2016 julkaistun poliisibarometrin mukaan 96 prosenttia kansalaisista pitää Suomen poliisia erittäin luotettavana tai melko luotettavana. Barometrin mukaan suomalaiset kokevat myös yleisen turvallisuuden parantuneen. Itseasiassa tulokset olivat vuonna 2016 myönteisempiä kuin kertaakaan aikaisemmin poliisibarometrin mittaushistorian aikana. (Poliisibarometri 2016.)

Tietoverkkorikosten määrä on suuressa kasvussa. Silti edelleen suuri osa tietoverkkorikollisuudesta jää tulematta poliisin tietoon (Sisäministeriön julkaisu 2017, 32). Yhtenä syynä tähän on varmasti se, että osa kyberrikoksista jää ihmisiltä ja yrityksiltä kokonaan huomaamatta, jolloin niistä ei yleensä myöskään ole aiheutunut erityistä haittaa. Toinen syy saattaa olla myös, ettei kaikista kyberrikoksista ilmoiteta syystä tai toisesta poliisille ollenkaan.

Suurin osa poliisin tietoon tulleista tietoverkkorikoksista on verkossa tapahtuneita petosrikoksia. Tällä hetkellä poliisi pyrkii tekemään ennalta estävää tiedottamista sellaisista esitutkintaan tulleista tietoverkkorikoksista, joiden uhreiksi voidaan epäillä myös muiden ihmisten sekä yritysten joutuvan. (Sisäministeriön julkaisu 2017, 32.)

Kyberrikollisuuden selvittämistä sekä torjuntaa varten on Keskusrikospoliisille perustettu vuonna 2015 oma ryhmä, kyberrikostorjuntakeskus.

"Tämän kyberrikostorjuntakeskuksen päätehtävinä kyberrikollisuuden torjunnassa ovat;

- vakavimpien tietoverkkorikosten tutkinta
- tietoverkkorikollisuuden tilannekuvan ylläpito
- internet- ja verkkotiedustelu
- tietotekninen tutkinta
- esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille." (Poliisi 2018, D.)

"Lisäksi kyberrikostorjuntakeskus seuraa tietotekniikan ja tietoverkkojen kehitystä, tunnistaa niissä esiintyviä uusia rikosilmiöitä, kehittää rikostorjunnan menetelmiä ja kouluttaa poliisia kybertoimintaympäristössä toteutettujen rikosten selvittämisessä" (Poliisi 2018, D).

Tietoverkkorikollisuuden torjuntaa koskevaa selvitystä koordinoinut Tiina Ferm toteaa sisäministeriön tiedotteessa, että poliisilla tulee olla keinot ja osaaminen tunnistaa tietoverkkoihin liittyviä rikoksia, ehkäistä ennalta verkossa tapahtuvia rikoksia, paljastaa verkossa toimivia rikollisia ja selvittää verkkoihin liittyviä rikosepäilyjä (Tietoverkkorikollisuuden torjuntaa koskeva selvitys 2017). Jotta tämän tyyppinen toiminta on mahdollista, tulee poliisilla olla myös tarvittavaa tietämystä ja osaamista verkossa tapahtuvien rikosten selvittämiseen sekä niiden ennaltaehkäisemiseen. Sisäministeriön julkaisun mukaan, yksi poliisihallinnon tärkeimmistä tehtävistä on juuri kehittää osaamista kyberturvallisuusstrategian saavuttamisessa (Sisäministeriön julkaisu 2017, 5).

"Kyberturvallisuusstrategian linjaus huolehtia poliisin tehokkaista kyberrikostorjunnan edellytyksistä pitää sisällään muun muassa sen periaatteen, että poliisilla tulee olla osaava ja motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristössä tapahtuvien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin oikeusvarmalla tavalla. Esitutkinta- ja turvallisuusviranomaisilla tulee olla uhan vakavuus huomioon ottaen riittävät toimivaltuudet ennalta estää, paljastaa ja selvittää kyberrikoksia sekä torjua kyberuhkia. Jatkuvasti muuttuva toimintaympäristö edellyttää lainsäädännön arviointia ja kehittämistä jatkuvana ja pysyväisluonteisena toimintana." (Sisäministeriön julkaisu 2017, 5-6.)

Muuttuvan toimintaympäristön myötä poliisien peruskoulutuksenkin on pysyttävä mukana tässä muutoksessa. Verkossa enenevissä määrin tapahtuvien rikosten määrän vuoksi kyberasioiden opetusta tullaan lisäämään poliisin peruskoulutukseen. Tämän lisäksi pyritään tarjoamaan laadukasta erityiskoulutusta kyberrikostorjuntaan erikoistuville sekä kehittämään koulutus- ja tutkimusyhteistyötä viranomaisten, korkeakoulujen sekä yliopistojen kanssa. (Sisäministeriön julkaisu 2017, 6.)

Poliisin peruskoulutukseen on jo viimeistenkin vuosien aikana kuulunut erilaisia katsauksia poliisin toiminnasta kybertoimintaympäristössä (Sisäministeriön julkaisu 2017, 35). Opinnäytetyön tekijöiden kurssi aloitti vuoden 2015 lokakuussa ja kurssin peruskoulutukseen sisältyi ainoastaan yksi luento kyberrikollisuuteen liittyen. Tulevaisuudessa tämän rikollisuuden muodon luennoille tulee varmasti olemaan tarvetta enemmänkin.

Poliisin kyberrikostorjuntatietoisuutta sekä -osaamista on pyritty kehittämään vuosien saatossa useilla eri menetelmillä. Koulutusta on järjestetty niin kotimaassa kuin ulkomaillakin suoritettavilla kursseilla. Valitettavasti tämän osa-alueen kehittäminen ja toteuttaminen ei ole poliisihallinnossa kuitenkaan ollut kovin suunnitelmallista eikä koordinoitua. Tämä puolestaan on aiheuttanut myös sen, että osaaminen ei ole sijoittunut alueittain tasaisesti, vaan kohdentuen tiettyihin sektoreihin enemmän kuin muihin, vaikka osaamiselle olisi tarvetta laajemminkin. (Sisäministeriön julkaisu 2017, 35.)

Tietoverkkorikollisuuden ulottuvuus on todella laaja ja moninainen ja se kehittyy nopealla vauhdilla. Poliisi seuraa tietoverkkorikollisuuden kuvaa ja tiedottaa aktiivisesti tällä hetkellä siihen liittyvistä ajankohtaisista uhkista ja vaaroista. Poliisi tekee myös tiivistä yhteistyötä Viestintäviraston kyberturvallisuuskeskuksen kanssa. (Poliisi 2018, D.)

Viestintäviraston pääasiallisena tehtävänä on käyttäjien suojaaminen perustuen valistavaan viestintään. Kansalaiset voivat tehdä ilmoituksen tietoturvaloukkauksesta Viestintäviraston verkkosivujen tietoturvaloukkausilmoitus -lomakkeen avulla tai olla yhteydessä Kyberturvallisuuskeskukseen sähköpostitse. Viestintävirasto selvittää ilmiöitä ja niiden vaikutuksia sekä auttaa kyberrikoksista toipumisessa. Usein kyberrikostapauksissa Viestintävirasto ei kuitenkaan voi muuta, kuin neuvoa kansalaista tekemään rikosilmoituksen. Erityisasiantun-

tija Kurittu (2018) kertoi, että neuvoja pyytävät ihmiset tiedustelevat usein, mitä hyötyä rikosilmoituksen tekemisestä on. Kurittu jatkaa, ettei hyöty aina ole välitön, koska kyberrikokset ovat usein haastavia selvittää. Yhteiskunnallinen etu rikosilmoituksen tekemisessä on kuitenkin merkittävä. Kun kyberrikoksista ilmoitetaan, samalla myös tietoisuus niistä kasvaa ja näin niitä voidaan ennalta estää paremmin.

Viestintävirasto pyrkii ennalta estämään kyberrikollisuutta viestinnällään. Viestintävirastolta pyydetään usein haastatteluja ajankohtaisiin keskusteluihin kyberrikollisuudesta. Kyberturvallisuuskeskuksesta tehdään myös julkisia esiintymisiä aihetta koskevia tilaisuuksia varten. Ajankohtaisista aiheista ja varoituksista ilmoitetaan Viestintäviraston sosiaalisessa mediassa. (Kurittu 2018.)

2.2 Muiden viranomaisten ennalta estävä toiminta

Yhteistyötä poliisin kanssa tekee Tulli ja Rajavartiolaitos, jotka kuuluvat poliisin lisäksi lainvalvontaviranomaisiin. Tulli sekä rajavartiolaitos suorittavat molemmat rikostutkintaa omilla toimialoillaan, ja kuten poliisin myös heidän tehtäviinsä kuuluu pyrkiä ennalta estämään rikosten syntymistä niin tavallisessa kuin myös tietoverkkoympäristössä. Tietoverkkorikollisuuden ja kyberuhkien torjunnassa, kuten monien muidenkin rikollisuustyyppien torjunnassa korostuu yhteistyön merkitys eri viranomaisten sekä elinkeinoelämän toimijoiden välillä. (Sisäministeriö 2017.)

Myös Puolustusvoimilla on oma tehtävänsä kansallisen kyberturvallisuuden edistämiseksi. Puolustusvoimat suojaavat järjestelmänsä, jotta he pystyvät toimimaan mahdollisimman hyvin suojattuina kybertoimintaympäristössä. Puolustusvoimat kehittävät tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä sekä harjoittelevat ja kehittävät kyberpuolustusta yhdessä keskeisten viranomaisten, järjestöjen ja elinkeinoelämän toimijoiden kanssa. Näiden lisäksi Puolustusvoimat antavat virka-apua lainsäädännön niin salliessa. (Valtioneuvosto 2013.) Puolustusvoimat ovat myös perustaneet kyberkeskuksen, johon varusmiespalvelustaan aloittavat voivat hakea suorittamaan palvelustaan (Puolustusvoimat 2018). Itse puolustuskyvyn ylläpidon lisäksi tämän voi nähdä ennalta estävänä toimintana,

koska sillä voidaan saattaa hakkerinalut oikealle polulle turvallisuusalalle sen sijaan, että taitoja alettaisiin käyttämään taitojen testaamiseen laittomilla tietoturvamurroilla.

Ensiarvoisen tärkeää on myös, että kyberrikosten ennalta estäminen otetaan huomioon muidenkin kuin viranomaisten toimesta. Esimerkkinä pohjoismaiset pankit ovat lisänneet yhteistyötään kyberrikollisuuden torjumiseksi. Vuonna 2017 pohjoismaisista pankeista muun muassa Danske Bank, Nordea, DNB, Sparebank 1 ja Eika Group ovat päättäneet keskinäisestä tiedonjaosta koskien kyberrikollisuuden torjuntaa (Nordea 2017). Kyberrikollisuuden ennalta estäminen ja torjuminen ei siis ole yksinomaan poliisin tehtävä vaan siinä on myös iso joukko muita yhteistyötahoja mukana.

3 KYBERRIKOLLISUUDEN VIITEKEHYS

Tässä osiossa avaamme kyberrikollisuuteen liittyviä peruskäsitteitä sekä sitä, miten kyberrikollisuus on kehittynyt vuosien aikana. Tuomme myös esille Poliisin näkökulmasta kyberrikollisuuden tutkintaan liittyviä haasteita sekä sitä, miten kyberrikollisuus näkyy tavallisen ihmisen arjessa.

3.1 Mitä kyberrikollisuus on?

Kyberrikollisuus tai verkkorikollisuus on tietoverkossa tapahtuvaa rikollisuutta. Nimenomaan tietoverkkorikoksista käytetään nykyään enenevässä määrin termiä kyberrikos. Tietoverkkorikosten määritteleminen sen sijaan ei ole täysin yksiselitteistä. Englanninkielinen käsite "cybercrime" tarkoittaa suomenkielelle käännettynä tietotekniikkarikosta, joka puolestaan toimii synonyymina rikoslain esitöissä käytettävälle tietoverkkorikollisuus- termille. Yhdysvalloissa kyber-alkuisten sanojen käyttö alkoi jo 1990-luvun loppupuolella. Suomeen tällä etuliitteellä varustetut termit rantautuivat vasta vuonna 2011, kun kansallisen kyberstrategian laatiminen aloitettiin. Tietoverkkorikoksista puhuttaessa tarkoitetaan siis tietoverkkoympäristöön kohdistuvia tai sitä ympäristönä hyväksi käyttäen tapahtuvia rikoksia. (Sisäministeriön julkaisu 2017, 10-11.)

Digitalisaatio on poistanut paljon rajoja, jotka sitoivat ihmisen aiemmin tiettyyn paikkaan ja aikaan. Nykyään useita asioita, jotka aiemmin vaativat siirtymistä ja ajankäytön suunnittelua, voidaan tehdä kotisohvalta muutamassa hetkessä. Myös maiden rajat ovat avautuneet uudella tavalla, kun yksi henkilö voi digitaalisesti olla monessa paikassa samaan aikaan.

Digitalisaatio on myös mahdollistanut yhteiskuntamme monipuolisen kehityksen. Digitalisaation ansiosta ihmisille pystytään luomaan eri elämäntilanteita ja elämänkaaren tarpeita varten luotettavampia ja parempia palveluketjuja, jotka ovat nopeasti saatavilla. Tutkitusti Suomesta löytyy myös tällä hetkellä EU-maiden paras digiosaaminen. (Valtiovarainministeriö 2018.) Digitalisaatiolla on kuitenkin varjopuolensa. Siinä missä digitalisaatio ja sähköistyminen ovat helpottaneet elämää, se on myös luonut pohjan nopeasti kehittyvälle kyberrikollisuudelle.

Internet tarjoaa uudenlaisen toimintaympäristön, jonka kautta ihmiset voivat helpommin löytää toisia ihmisiä ja jakaa ajatuksiaan. Internetin avulla voi kommunikoida nimettömästi ja näin pienentää riskiä tulla tunnistetuksi (Bossler & Holt 2017, 38). Tämän johdosta digitaalinen toimintaympäristö on avannut rikolliselle toiminnalle täysin uudenlaisen ulottuvuuden toimia. Verkossa tapahtuvat rikokset ovat usein valtioiden rajat ylittäviä ja kansainvälisiä. Toisin kuin perinteiset rikokset, verkossa tapahtuvat rikokset eivät vaadi tekijän ja uhrin fyysistä läheisyyttä, jolloin näiden etäisyydellä tai sijainnilla ei ole merkitystä. (Sisäministeriö 2017.) Nykyään yhä enenevässä määrin poliisin tietoon tulleet rikokset liittyvät jollain tavalla tietoverkkoympäristöihin (Sisäministeriön julkaisu 2017, 12).

3.2 Kyberrikollisuuden kehittyminen

Yhteiskunnan digitalisoituminen ja sähköistyminen ovat alkaneet kehittyä noin vuoden 1980 tietämillä, kun kotitietokoneet alkoivat yleistyä ihmisten kodeissa (Koiranen ym. 2016). 1990-luvulla suomalaisilla oli keskimäärin yksi internetyhteyttä hyödyntävä laite kotonaan. Kehitys on kiihtynyt ja jo 2000-luvulla tietoverkot ja päätelaitteet tulivat osaksi ihmisten päivittäistä elämänhallintaa. Ihmiskunta on luonut rinnakkaistodellisuuden verkkoon, jossa tieto ja raha liikkuvat samalla tavalla, tai jopa tehokkaammin, kuin reaalimaailmassa. Tämä on näkynyt myös yritysten tuottavuuden kasvussa, josta lähes 80 prosenttia on tullut viimeisen vuosikymmenyksen aikana tietoliikenneyhteyksien kehityksen ansiosta. Kaupanteko ja kuluttaminen muuttuvat vauhdilla virtuaaliseksi, joka kiihdyttää myös rahaliikennettä verkossa. Suomalaisten kotitalouksien internetyhteyttä hyödyntävien laitteiden määrä on kasvanut 1990-luvun yhdestä laitteesta helposti 10:en laitteeseen. (Peltomäki & Norppa 2015, 16-25.)

Rikosylikomisario Muurmanin (2018) mukaan verkkorikosten kehityksen myötä ne ovat muuttuneet tekotavoiltaan monimutkaisemmiksi ja ammattimaisemmiksi kuin ennen. Rikollisuus on laajentunut kotimaan sisällä ja ulottuu nykyään myös pitkälle ulkomaille saakka. Myös verkossa tapahtuvien rikosten tekeminen on helpottunut, sillä tietojärjestelmiä hyvin hallitsevat tahot tarjoavat erilaisia valmiita ohjelmia ja sovelluksia verkkorikos-

ten tekemiseen. Tämän vuoksi kynnys verkkorikosten tekemiseen on madaltunut, koska itse tekijältä ei enää vaadita teknistä osaamista vaan teknisen puolen tuottaa ulkopuolinen taho.

Digitalisaatiokauden alussa verkossa tapahtuvat rikokset tehtiin ennemminkin huvin kuin tuoton vuoksi. Tuolloin verkossa tapahtuvien rikosten päämäärä oli uusien teknisten saavutusten ja maineen luominen. Nykyään rahaa liikkuu yhtä paljon verkossa kuin reaalimaailmassa, joka on muuttanut vääryyksien siirtymistä huvista tuottoon. (Grabosky & Holt 2017, 17.)

Virtuaalivaluutat ovat myös nousseet otsikoihin viime aikoina. Virtuaalivaluutat tarjoavat rikollisille tehokkaan tavan siirtää ja tallettaa laittomasti hankittuja varoja viranomaisten ulottumattomissa. Virtuaalivaluutta eroaa virallisesta eli fyysiseen valuuttaan perustuvasta niin kutsutusta fiat -rahasta siinä, että virtuaalivaluutta ilmenee pelkästään digitaalisessa muodossa. Virtuaalivaluuttaa ei myöskään luokitella lailliseksi maksuvälineeksi. Virtuaalivaluutoissa arvo perustuu sen käyttäjien välisiin sopimuksiin. Tunnetuin virtuaalivaluutta lienee Bitcoin, joka edustaa kryptovaluuttoja. Sanalla "krypto" tarkoitetaan salausta. Kryptovaluutat perustuvat matemaattiseen salaukseen, joka tarkoittaa sitä, että kryptovaluuttamaksuun pääsee käsiksi vain omistamalla salauksen purkuun tarvittavan avaimen. Kun maksut tapahtuvat salatussa ympäristössä, kuten Tor -verkossa, jossa toimijoita ei voi yhdistää oikeisiin henkilöihin, on maksujen väliin viranomaisten hyvin vaikea päästä. (FATF 2014.)

Rikoskomisario Siurolan (2018) havaintojen mukaan tekijänoikeusloukkaukset ovat myös olleet aiempaa vähemmän pinnalla. Tekijänoikeuden tiedotus- ja valvontakeskus ry:n toiminnanjohtaja Pihkala Jaana (2018) kommentoi, ettei tekijänoikeusrikkomusten nykytilanteeseen ole yksiselitteistä vastausta. Tilanne riippuu, mistä näkökulmasta asiaa tarkastelee.

Suomalaiset piraattipalvelut, joiden avulla ladattiin ja jaettiin paljon materiaalia, ovat määrältään romahtaneet 10 vuoden takaiseen tilanteeseen. Samalla laiton lataaminen ja jakaminen verkossa on vähentyneet. Samoin on käynyt myös musiikin kulutukselle laittomista

lähteistä. Kokonaisuudessaan Suomessa laittomien lähteiden käyttö tuntuu vähentyneen siitä mitä se oli viisi tai 10 vuotta sitten. (Pihkala 2018.)

MediaVision Ab teki keväällä 2016 tutkimuksen, jonka mukaan kuitenkin kahdeksan prosenttia Suomen väestöstä eli noin 325 000 henkilöä kuukausittain käyttää laittomia lähteitä elokuvien ja TV -sarjojen hakemiseen. Tämä tarkoittaa sitä, että kyseinen osa väestöstä lataa tai suoratoistaa laittomasti vuosittain 15 miljoonaa elokuvaa ja 29 miljoonaa TV -sarjan jaksoa. Kyse on siis edelleen varsin merkittävästä ongelmasta. Tekijänoikeusloukkauksista ei kuitenkaan enää tehdä niin usein tutkintapyyntöä poliisille, eikä asiat mene tuomioistuinkäsittelyyn kuten aikaisemmin. Nykyään tekijänoikeusloukkauksia käsitellään huomattavasti aiempaa enemmän siviilioikeudellisin tiedonsaantimenetelmin ja asiat sovitellaan niin sanotuin kirjemenettelyin. Tästä saattaa johtua, ettei poliisille tule enää samalla tavalla tutkintapyyntöjä tekijänoikeusloukkauksista. (Pihkala 2018.)

Pihkala (2018) tiivistää tekijänoikeusloukkausten eli niin kutsutun piratismin vähentyneen Suomessa johtuen seuraavien tekijöiden summasta; tietoisuus tekijänoikeuksista on lisääntynyt, valvonta on kohdistunut oikein sekä lailliset palvelut ovat kehittyneet. Ongelmaa ei kuitenkaan ole selätetty, vaan tekninen ympäristö on muuttunut enemmän suoratoistoon joka tuo mukanaan omat haasteensa tekijänoikeusrintamalla. Pihkala on myös huolestunut nettipiratismin kehittymisestä yhä enemmän järjestäytyneeksi ja ammattimaiseksi. Nettipiratismi tuntuu seuraavan tuoteväärennösten kehitystä, joilla rahoitetaan kansainvälisiä rikollis- ja terroristijärjestöjä.

3.3 Haasteet kyberrikollisuuden tutkinnassa

Kyberrikollisuus on aiheena verrattain tuore osa rikollisuutta. Kriminologia tutkii rikollisuutta ilmiönä ja pyrkii selvittämään rikollisuuden taustaperiä sekä siihen johtaneita syitä. Ilmiön tuoreudesta johtuen kriminologisia tutkimuksia ei vielä juurikaan ole tehty. Haasteita kyberrikollisuuden tutkinnassa aiheuttaa muun muassa datan, eli informaation vähyys. Rikollisuuden kehitystä pyritään seuraamaan ja tulkitsemaan keräämällä statistiikkaa erilaisten rikostilastojen avulla. **(**Bossler & Holt 2017, 41.)

Kyberrikoksen tekijät tai sen mahdollistajat ovat usein lähtöisin monesta eri maasta ja vaativat näin intensiivistä ja laajaa kansainvälistä yhteistyötä. Ongelmana on, ettei ole globaaleja toimijoita, joilla voitaisiin tutkia tällaisia laajoja verkostoja. Yksittäiset teot jäävät lopulta melko vähäpätöisiksi, eikä yksittäisen maan poliisivoimat kykene niitä varten järjestämään kovin laajoja kansainvälisiä selvityksiä. Rikollisten kannalta kyberrikokset saattavat olla isoakin bisnestä, mutta uhreja on tiputellen yksittäin ympäri maailmaa, joka luo haasteen selvitystyölle. Silloin tällöin Interpol kansainvälisenä toimijana ottaa jonkin bottiverkon haaviinsa ja tekee pidätyksiä, jotka saattavat kaataa laajojakin bottiverkostoja. (Kurittu 2018).

Rikosylikomisario Muurman (2018) kommentoi, että Suomessa poliisin järjestelmillä pystytään taltioimaan statistiikkaa kyberrikoksista. Ongelmana on, ettei poliisilaitoksilla kirjata kyberrikoksia yhdenmukaisesti tai joissain tapauksissa saattaa kirjaukset tietotekniikkarikosten osalta jäädä kokonaan tekemättä. Tarvittaisiin siis lisää koulutusta kyberrikosten havaitsemiseen ja yhdenmukaiseen kirjaamiseen.

Muurman (2018) kertoo myös, että Suomessa tekninen tutkinta on hyvällä tasolla. Sen sijaan taktisen tutkinnan puolella valmiudet kyberrikosten tutkintaan vaihtelevat paljon. Haasteena on se, että kyberrikoksia koskevat jutut menevät muiden tutkintaan tulevien juttujen mukana, eikä osaamista yksittäisen tutkijan tasolla ole vielä tarpeeksi. Muurmanin mukaan olisi hyvä, jos jokaisella laitoksella olisi muutamia tietotekniikkarikoksiin erikoistuneita henkilöitä, jotka ensisijaisesti tarttuisivat kyberrikosjuttuihin. Näin heidän osaamisensa pysyisi paremmin yllä ja samaan aikaan kehittyisi.

Koulutusta kyberrikollisuuden tutkintaan on olemassa paljon, mutta vielä suhteellisen vähän Suomessa. Kursseja järjestetään paljon ulkomailla, jotka puolestaan ovat kalliita. Kotimaisen koulutuksen saatavuuteen tulisi panostaa enemmän ja näin koulutus olisi myös paremmin kaikkien saatavilla. Osaaminen poliisilaitosten välillä vaihtelee myös paljon ja se on maantieteellisesti jakautunut hyvin epätasaisesti. Poliisiammattikorkeakoulussa on olemassa hyvä suunnitelma sekä taktisen että teknisen tutkinnan kouluttamiseen. Kuitenkin poliisin perustutkinnon osalta koulutus kyberrikoksiin on vielä hyvin vähäistä. Aihe on ajankohtainen ja sitä olisi syytä lisätä myös peruskoulutukseen juurikin tästä syystä. Ky-

berrikosten tutkinnassa koulutuksella saavutettavat yhtenäiset käytännöt olisivat tärkeitä. Rikosilmoitusten kirjaustavat tulisi yhtenäistää ja tietotekniikkarikokset luokitella asianmukaisesti ilmoitusta kirjattaessa. Tämä parantaisi myös kyberrikoksista saatavaa statistiikkaa. Lisäämällä poliisien tietoisuutta erilaisin koulutuksin, saataisiin myös poliisin sisällä kyberrikoksiin liittyvää asennetta muutettua. Kyberrikosten tutkinta ei kuitenkaan ole niin hankalaa kuin sen tällä hetkellä koetaan olevan. (Muurman 2018.)

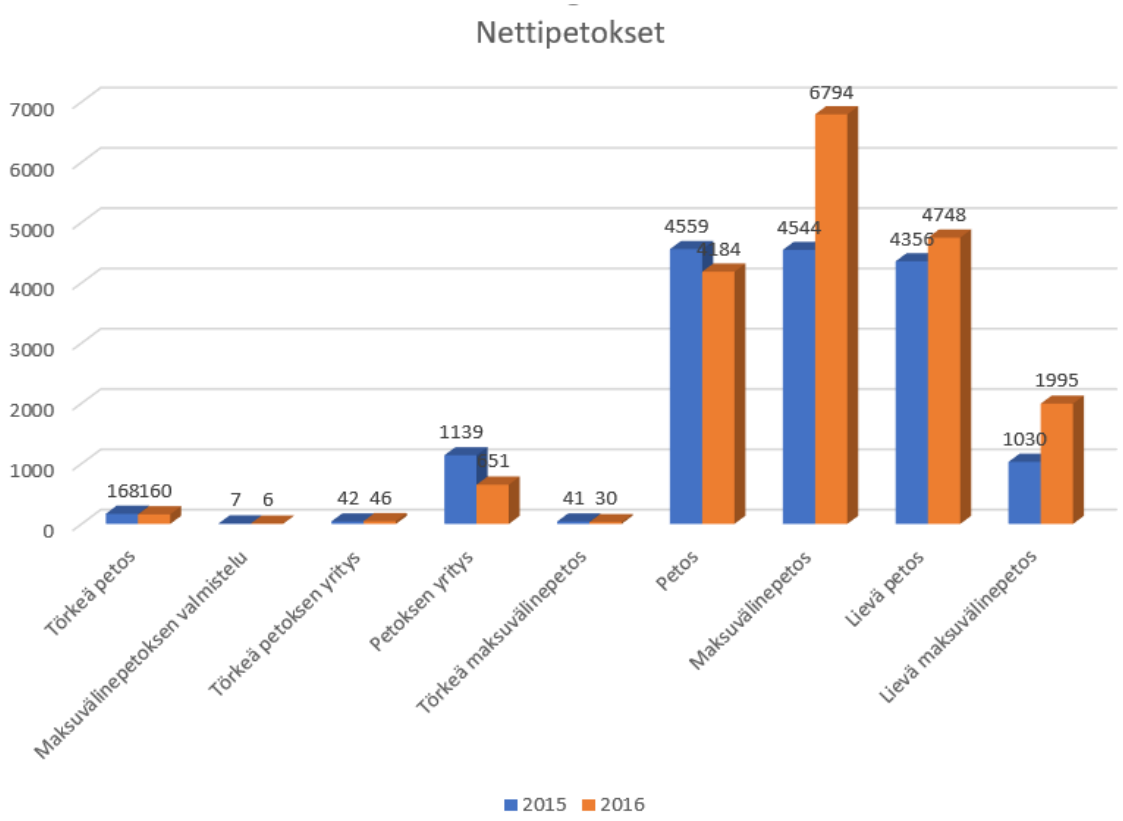
Haasteelliseksi on osoittautunut myös kyber- sekä tietoverkkorikosten tutkinnassa lakien taipumattomuus juuri näiden rikosten tutkimiseen. Suomessa lakipykälät ovat vanhoja ja tulkinnanvaraisia, erityisesti kun niitä yritetään soveltaa kyberrikostutkinnassa. Rikoslain soveltaminen ei ole niinkään haastavaa, mutta erityisesti pakkokeinolaista löytyy paljon tulkinnanvaraisuuksia. Osa pykälistä on melko toimimattomia tämän lajin rikoksia tutkittaessa. Lain mukana pysyminen kyberrikostutkinnassa on haastavaa, koska tekniikka kehittyy jatkuvasti. Uusin pakkokeinolaki tuli voimaan vuonna 2014 ja siinä on jo nyt paljon kehitettävää, mikäli sitä haluttaisiin hyödyntää enemmän kyberrikosten selvittämisessä. Pelkästään lainsäädännön muuttaminen vie vuosia, joten tällaisissa nopeasti kehittyvissä asioissa laki on usein vanha vasta valmistuttuaankin. Tästä syystä lain tulisi olla niin yleisellä tasolla avoimeksi kirjoitettua, jotta pykälät olisivat käyttökelpoisia moneen asiaan. Tietoverkkomaailmassa tapahtuva tutkinta vaatii sen maailmaan sopivat työkalut. (Muurman 2018.)

Kansallisten lakien haasteet kyberrikostutkinnassa on kuitenkin otettu huomioon EU:ssa ja osittain laajemmallakin tasolla. Euroopan neuvoston jäsenvaltiot, sekä muut allekirjoittaneet valtiot ovat vuonna 2001 tehneet yleissopimuksen koskien tietoverkkorikollisuutta. Sopimuksen tarkoitus on lähentää maiden rikospolitiikkaa kyseisten rikosten tehokkaaksi torjumiseksi sekä parantaa yhteistyötä rikosten selvittämiseksi. Tämä asetus helpottaa jäsenmaiden välistä yhteystyötä, koska sen avulla jäsenvaltiot tietävät samankaltaisten tietoverkkorikosten olevan kriminalisoituja kussakin jäsenvaltiossa. (Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus 2007.) Sopimusta ja sen ajanmukaisuutta tarkastellaan kaksi kertaa vuodessa T-CY:n (The Cybercrime Convention Committee) toimesta (Council of Europe 2018).

Suomessa ollaan rikosylikomisario Muurmanin (2018) mukaan hyvin ajan tasalla maailmalla tapahtuvista kyberrikoksista. Europolin ansiosta sen jäsenmaat pysyvät hyvin ajan tasalla rajat ylittävästä rikollisuudesta, jota kyberrikollisuus pääasiassa on. Yhteistyöverkoston kautta pystytään jakamaan tietoa tämänhetkisistä kyberrikollisuuden muodoista. Tämän tiedon avulla pystytään ennakoimaan vastaavaa toimintaa Suomessa. Euroopan ulkopuolelta puolestaan Yhdysvallat on tärkeä yhteystyökumppani Suomelle jo yksinomaan siksi, että useat verkossa sijaitsevat palvelut kuten Facebook, Twitter ja Instagram sijaitsevat siellä. Yhdysvalloissa FBI (Federal Bureau of Investigation) toimii aktiivisimmin kyberrikosten parissa, mutta myös Secret Service jakaa paljon kyberrikostietoja Suomen kanssa. Suomen sisällä puolestaan tehdään paljon yhteistyötä Viestintäviraston kanssa.

3.4 Kyberrikollisuus ihmisen arjessa

Poliisihallituksen vuoden 2017 tilastojulkistuksesta käy ilmi, että vuonna 2016 poliisille ilmoitettiin yhteensä 809 368 rikosta. Kasvua tapahtui vuodesta 2015 vuoteen 2016 kaikkien rikosten ilmoitusmäärissä 0,44 prosenttia, joka lukuna tarkoittaa 3 574 rikosta enemmän edellisvuoteen verrattuna. Kokonaisuutena omaisuusrikosten määrä on laskenut noin kolme prosenttia edelliseen vuoteen verrattuna. Kuitenkin petosten ja erityisesti internetissä tapahtuneiden maksuvälinepetosten määrä on noussut entisestään. Petosrikoksissa kasvua oli jopa huimat kahdeksan prosenttia, joka tarkoittaa lukuna 2 900 rikosta enemmän kuin vuonna 2015. (Poliisin tilastot vuosi 2016 – nettipetokset.)



Kuva 1. Poliisin kirjaamat nettipetokset vuosina 2015-2016 (Poliisin tilastot vuosi 2016 - nettipetokset).

Poliisin vuonna 2016 nettipetoksien jakautumisesta tekemän tilaston mukaan poliisin tietoon tulleet petosrikostapaukset, joiden tekopaikaksi on luokiteltu "Internet", ovat jakautuneet vuosina 2015 ja 2016 yllä näkyvän taulukon mukaisesti. Yhteensä nettipetoksia tuli poliisin tietoon vuonna 2015 15 886 kappaletta ja vuonna 2016 yhteensä 18 614 kappaletta. Vuoden 2017 tammi-syyskuun välisenä aikana poliisin tietoon on tullut yhteensä 22 579 petosrikosta, joista ei tosin ole erikseen vielä eritelty internetissä tapahtuneita petoksia (Poliisiammattikorkeakoulu 2017).

Erityistä kasvua vuosien 2015 ja 2016 välillä on ollut maksuvälinepetoksissa sekä lievissä maksuvälinepetoksissa. Näiden petostyyppien kasvua voidaan selittää esimerkiksi sillä, että ihmiset ovat ilmoittaneet korttitietojaan verkossa ilmaantuneille huijaussivustoille. (Poliisi 2017.)

"– Tyypillistä verkossa tapahtuvaa petosrikollisuutta on se, että tarjotaan myytäväksi omaisuutta, jota myyjällä ei ole. Myyjällä on yleensä kiire saada rahat tuotteesta tililleen ja hän väittää, että tuotteelle on jonossa muitakin ostajia tai pyytää maksamaan rahat jonkun kolmannen henkilön tilille tai ulkomaiselle tilille rahasiirrolla, poliisylijohtaja Kolehmainen sanoo." (Poliisi 2017.)

Suomessa poliisin tietoon tulleet nettipetokset saadaan pääosin hyvin tutkinnassa selvitettyä. Sen sijaan vaikeampia selvittää ovat maksuvälinepetokset, joissa rikosten tekopaikka on ulkomailla mutta seuraus ilmenee Suomessa. Hyvästä selvitysasteesta huolimatta rikoksen tekijät ovat valitettavan usein ehtineet myös käyttää saamansa rikoshyödyn tai ovat muuten varattomia, jolloin rikoksen uhreiksi joutuneiden korvaukset jäävät olemattomiksi. (Poliisi 2017.)

Poliisin mukaan kortti on turvallinen maksuväline myös verkossa, kunhan sitä käytetään turvallisissa verkkokaupoissa ja salatun yhteyden kera. Parhaiten tämän tunnistaa siitä, että www-sivuston kirjautumisosoite johon korttitiedot syötetään, on muotoa https://. Korttien väärinkäytösten riskejä pystytään vähentämään ja kortin käytön turvallisuutta lisäämään erilaisilla turvarajoilla. (Poliisi 2017.) Tällaisia voivat olla esimerkiksi korttiin asetettava vuorokautinen käteisnostoraja tai tilille asetettava vuorokautinen maksuraja. Kortin internetkäytön voi myös kokonaan rajoittaa pois ja ottaa käyttöön vasta, kun korttia tarvitsee internetostoissa. (Nordea 2018).

Uutena tulokkaana petosrikosten alasarjaan on vuoden 2015 syksyllä rikoslaissa rangaistavakasi voimaan tullut identiteettivarkaus. Tätä ennen identiteettivarkauksia tutkittiin muiden rikosnimikkeiden alla. Yksinkertaisimmillaan identiteettivarkaudessa on kyse siitä, että tekijä onnistuu hankkimaan käyttöönsä toisen ihmisen henkilötiedot, joiden avulla saa itselleen taloudellista hyötyä. Yleisimmin tämä ilmenee erilaisten verkossa tapahtuneiden tilausten muodossa, joiden avulla tekijät onnistuvat tekemään isoja laskuja uhrinsa kustannuksella. (Karismo 2017.)

Parhaiten nettipetoksia pystyy ennalta estämään nettiostajat ja verkossa toimijat itse. Tämä puolestaan korostaa entisestään poliisin ennalta estävän toiminnan merkitystä ja sen tar-

peellisuutta nettipetosten torjunnassa. Mitä tietoisempia ihmiset ovat verkossa tapahtuvista vaaroista, sen paremmin he pystyvät niitä tunnistamaan ja näin ollen myös välttämään.

Ideaalitilanteessa jokaisella suomalaisella olisi tietynlaiset perustaidot verkossa toimimiseen. Kaikilla tulisi olla peruskäsitys siitä, miten omaa toimintaa voisi suojata verkkoympäristössä. Esimerkiksi laitteiden ja järjestelmien mukana tulleet oletussalasanat ja tunnukset tulisi heti käyttöönottaessa muuttaa omiksi. Muurman ja Siurola (2018) toteavat, että Suomessa on paljon verkkoa käyttäviä hyvin valveutuneita nuoria, jotka ovat erittäin fiksuja, mutta sitten meillä on myös iso joukko keski-iän ylittäneitä ihmisiä, jotka eivät osaa toimia verkossa tarpeeksi valveutuneesti. Perustaidot tulisi kaikille saada tasapuolisesti paremmalle tasolle.

Tämä on ongelma, joka ei korjaudu yksinomaan ajansaatossa. Nuorten kuin myös aikuisten joukossa on sellaisia ihmisiä, jotka eivät yksinkertaisesti pysty lukihäiriön tai muun keskittymis- tai kehityshäiriön vuoksi ymmärtämään sellaisia asioita, jotka voivat vaarantaa omaa toimintaa verkossa. Nuorisolle tarvitaan tervettä epäluuloa sosiaalisessa mediassa toimimiseen. Kaikkia yksityisyyteen liittyviä tietoja ei kannata kirjoittaa omaan profiiliinsa sosiaalisessa mediassa tai muutenkaan jakaa kaikkia yksityiselämän tietoja julkisesti. Esimerkkinä voidaan nostaa esille se, että Facebookissa tehty ilmoitus lomalle lähdöstä voi olla merkki rikollisille tyhjilleen jäävästä asunnosta. (Muurman & Siurola 2018.)

Erityisasiantuntija Kurittu (2018) kertoo, että keskeiset yksityishenkilöitä koskevat huijaukset ovat sosiaaliset huijaukset, joiden määrät ovat olleet kasvussa. Sosiaalisiin huijauksiin lasketaan muun muassa tietojen kalastelut, tilausansat, romanssihuijaukset ja erilaiset petokset. Myös Kuritun mukaan ihmisten tietoisuuden vähäisyys turvallisesta verkon käytöstä on suurimpia ongelmia. Sosiaalisista huijauksistakin vain pieni osa tulee viranomaisten tietoon, joten ongelma on varmasti laajempi, kuin mitä tiedossa on.

4 KYBERRIKOLLISUUDEN ERI MUODOT

Kyberrikollisuutta esiintyy verkossa lukuisissa eri muodoissa. Jokainen tavallinenkin verkon käyttäjä kohtaa kyberrikollisuuden eri muotoja joko huomaamattaan tai tiedostaen. Seuraavissa kappaleissa olemme nostaneet esille yleisimpiä kyberrikollisuuden tyyppejä, joita ihmiset yleisimmin kohtaavat arjessaan.

4.1 Palvelunestohyökkäykset ja esineiden internet

Palvelunestohyökkäyksellä tarkoitetaan tilannetta, missä tietoon tai palveluun pääsy on vaikeutunut tai estetty kokonaan. Tietojen tai palveluiden käyttöön oikeutettujen henkilöiden tietojen saantia pyritään hankaloittamaan tai jopa estämään kokonaan palvelunestohyökkäyksien avulla. Yleisimpiä motiiveja palvelunestohyökkäyksille voivat olla esimerkiksi kiusanteko, maineen luominen, taloudellisen hyödyn tavoittelu tai haktivismi. Taloudellisen hyödyn tavoittelulla tarkoitetaan hyödyn saamista kiristämällä tai ohjaamalla palvelun käyttäjät jonkin toisen kilpailevan palvelun piiriin. Haktivismilla puolestaan tarkoitetaan tietoverkossa tapahtuvaa toimintaa, jolla pyritään aikaansaamaan muutosta tai huomiota johonkin asiaan liittyen. Yleisimmin hyökkäysten tekemiseen käytetään heikosti suojattuja laitteita, väärin määriteltyjä palvelimia tai kaapattuja tietokoneita, jotka välittävät väärennettyä liikennettä. (Viestintävirasto 2016.)

Vuonna 2000 tunnetuimpia palvelunestohyökkäyksiä oli Michael Calce, ”Mafia Boy”-nimimerkillä toimineen 16-vuotiaan nuorukaisen hyökkäys, jolla hän kaatoi Amazon, CNN, Dell, E*Trade, eBay ja Yahoo! -sivustot. Yahoo oli tuolloin maailman käytetyin hakukone. Calce kertoi tehneensä ensimmäisen hakkerointinsa jo yhdeksänvuotiaana. Tuon 2000-luvun palvelunestohyökkäyksen Calce kertoi tehneensä ottamalla haltuunsa yliopiston verkkoa. Tuota verkkoa apunaan käyttäen Calce ylikuormitti internetsivustoja suuntaamalla niihin valtavan määrän informaatiota, jolloin sivusto kaatui. Hyökkäyksillään Calce halusi osoittaa taitonsa muille hakkeriryhmittymille. (Hersher 2015.)

Nykymittapuissa Calcen hyökkäys oli suhteellisen harmiton. Tänä päivänä kyberrikollisuudessa käytetään paljon niin kutsuttuja botteja. Botilla tarkoitetaan haittaohjelmaa, joka

asentuu tietokoneelle tai laitteelle ja mahdollistaa haittaohjelman haltijan pääsyn haittaohjelman saastuttaneelle tietokoneelle tai laitteelle, jossa on internetyhteys. Nämä haittaohjelmien saastuttaneet tietokoneet tai laitteet toimivat yhdessä bottiverkostona, jonka kautta levitetään viruksia, luodaan roskapostia sekä tehdään muita rikoksia ja petoksia verkossa. (Norton 2017.) Bottiverkoilla voidaan kerätä jopa miljoonia laitteita suorittamaan tiettyä kyberrikosta. Kehittyneimmät haittaohjelmat ovat haastavia havaita tietokoneelle asennuttuaan. Haittaohjelmien tekijät kehittävät ja päivittävät ohjelmiaan jopa vuosia ja voivat tehdä niillä voittoa myymällä niitä eteenpäin rikollisille tahoille. (Soumenkov & Golovanov 2011.)

Esimerkiksi vuonna 2008 TDL:ksi nimetty haittaohjelma eteni vuoteen 2011 mennessä neljänteen versioonsa nimeltä TDL-4. Kyseistä ohjelmaa levitettiin yleisimmin aikuisviihdesivustojen, piraattisivustojen sekä videoiden ja tiedostojen varastointipalveluiden kautta. Kun bottiverkkoon on saatu iso määrä tietokoneita, voidaan internettiä käyttää nimettömästi piilottamalla verkon käyttäjän toiminta bottiverkossa olevien tietokoneiden joukkoon. Tätä ominaisuutta voidaan myydä omana palvelunaan, joka tarjoaa TDL-4:n laatijalle lisäansaitsemismahdollisuuksia. (Soumenkov & Golovanov 2011.)

Bottiverkon voi siis luoda saastuttamalla tietokoneen tai laitteen haittaohjelmalla. Internetyhteydellinen tietokone on selvä asia, mutta mitä tarkoitetaan mainitulla laitteella. Teknologiakehitys on mahdollistanut verkko-ominaisuuden lisäämisen yhä useampaan laitteeseen. Näin erilaisia laitekokonaisuuksia voidaan hallita verkon välityksellä. Useista laitteista voidaan saada hyödyllistä tietoa, kun laitteen toiminnasta voidaan koota ja lähettää tietoa verkon kautta. Tällaista kutsutaan esineiden internetiksi. Esineiden tai laitteiden yhteistoiminta verkon kautta luo paljon mahdollisuuksia niin yksityispuolella kuin kaupallisellakin. (Holt & Grabosky 2017, 29.)

Esimerkkinä tällaisesta laitteesta on Samsungin valmistama jääkaapin, jonka avulla voidaan seurata jääkaapin sisältöä ja ostokset voi tehdä suoraan jääkaapissa olevan älynäytön kautta (Samsung 2017). Tällaiset sovellukset tekevät elämästä helpompaa ja lisäävät synergiaa, mutta tarjoavat myös rikollisille jälleen uusia toimintaympäristöjä. Sen jälkeen, kun laitteen käyttäjä pääsee laitteeseen käsiksi verkon kautta, pääsee siihen mahdollisesti

käsiksi rikollisetkin. Rikollinen voi käyttää laitteen perusominaisuuksia omiin tarkoituksiinsa tai käyttäjää vastaan, tai käyttää laitteen verkko-ominaisuuksia esimerkiksi palvelunestohyökkäyksiin. (Holt & Grabosky 2017, 29.)

Vuonna 2016 tehtiin palvelunestohyökkäys käyttäen hyödyksi esineistä luotua bottiverkkoa. Kyseisellä palvelunestohyökkäyksellä kaadettiin suuria yhdysvaltalaisia palveluita kuten Spotify, Twitter ja Netflix. Tuolloin käytetty haittaohjelma bottiverkon luomiseksi oli nimeltään Mirai. Normaalista bottiverkosta poiketen Mirai saastutti internetiin kytkettyjä esineitä. Hyökkäys tehtiin käyttämällä oletussalasanoja ja käyttäjätunnuksia (Kaspersky Lab 2016).

Rikoskomisario Siurola (2018) kertoo esineiden internetin luovan lisää mahdollisuuksia kyberrikollisille. Arvokkaimmat laitteet, jotka hyödyntävät tätä esineiden internettiä, sisältävät paremmat suojat ja niitä päivitellään useammin. Tämä ehkäisee kyseisten laitteiden hyödyntämistä verkkorikoksissa. Halvemmissa laitteissa suojaukset ovat heikompia, eikä niihin tule juuri päivityksiä, joka tekee niistä helpommin hyödynnettäviä verkkorikollisuuteen. Ongelmaa lisää se, etteivät ihmiset usein muuta laitteiden oletusasetuksia, jolloin verkkorikolliset pääsevät helpommin laitteisiin käsiksi. Tällaiset laitteet ovat myös pääsääntöisesti jatkuvasti verkossa, jolloin ne altistuvat helpommin verkkorikollisuudelle.

Rikosylikomisario Muurmanin ja rikoskomisario Siurolan (2018) mukaan palvelunestohyökkäykset ovat jatkuvasti esillä. Palvelunestohyökkäyksistä kuitenkin vain jäävuoren huippu tulee poliisin tietoon. Tämä puolestaan saattaa johtua siitä, että palvelunestohyökkäykset kohdistuvat pääasiassa yrityksiin ja virastoihin, jotka maineen kärsimisen pelossa eivät halua siirtää rikoksia poliisin tutkittaviksi. Asian selvittely saatetaan myös kokea aikaa vieväksi ja kustannuksia aiheuttavaksi. Odotettavissa olevat seuraamukset koetaan vähäisiksi ja vahingonkorvausten saaminen vaikeaksi, jolloin asia mieluummin jätetään sillensä. Verkkorikokset ovat pääosin virallisen syytteen alaisia rikoksia, jonka vuoksi poliisi on ne tietoon saadessaan velvollinen tutkimaan. Tuomioistuimen käsittelyn tai tutkinnan lopettamisen jälkeen rikoksen tiedot tulevat julkisiksi, jolloin yrityksen maine saattaa kärsiä. Tämän lisäksi verkkorikosten tutkimiseen vaaditaan usein myös yrityksen oman henkilöstön apua, joka on kallista verrattuna esimerkiksi kioskimurtoihin.

4.2 Huijausviestit

Aikoinaan ihmisten välinen viestintä tapahtui pääasiassa kirjepostin ja puhelimen välityksellä. Näiden jälkeen kehittyivät faksit ja tietokoneiden myötä sähköpostit. Matkapuhelinten myötä tulivat tekstiviestit ja viimeisimpänä kehitysmuotona älypuhelimien mahdollistama sosiaalinen media. Yksi yleisimmistä huijauksista, johon hyvin moni on jossain vaiheessa elämäänsä törmännyt, on niin kutsuttu "nigerialaishuijaus". Huijaus on alun perin lähtöisin Nigeriasta, jonka mukaan ne ovat myös saaneet nimensä.

Kiistämätön tosiasia on se, että verkossa tapahtuvien huijausten määrä on kasvanut räjähdysmäisesti. Pelkästään nigerialaisia huijausviestejä lähtee Ruotsin poliisin vuonna 2007 tekemän arvion mukaan vuodessa noin 50 miljoonaa. Erityisen paljon huijausviestejä tulee Länsi-Afrikan maista, mutta yhä enenevässä määrin myös länsimaat ovat huijausviestien takana. (Salmivuori 2016, 26-27.) Nigerialaishuijaukset perustuvat pääasiassa viestin saajan hyväuskoisuuteen. Viestin vastaanottajalle uskotellaan tämän voittaneen palkinnon, saaneen perinnön kaukaiselta sukulaiselta tai vastaavan arvokkaan yllätyksen. Jotta viestin saaja voisi lunastaa luvatun rahasumman, häntä kehotetaan siirtämään rahaa erilaisten kulujen kattamiseksi. Kulujen kattamisen tarve monimutkaistuu huijauksen edetessä ja hyväuskoinen viestin vastaanottaja jatkaa rahojen lähettämistä. Viestissä luvattua rahasummaa viestin vastaanottaja ei tule kuitenkaan koskaan saamaan. (Viestintävirasto 2014, 5.)

Verkkohuijausten onnistumista ei voida yksinomaan selittää uhrien hyväuskoisuudella tai ahneudella, vaikka se helposti näin mielletäänkin. Kyseiset huijausviestit ovat yleensä hyvin uskottavia ja ne pyrkivät kehittymään ja muuntautumaan koko ajan. Tavallisen verkon käyttäjän voi olla vaikea erottaa huijausviestiä oikeasta viestistä, varsinkin jos sillä onnistutaan vetoamaan ihmisen sen hetkiseen elämässä vallitsevaan tarpeeseen. Tällöin usein skeptisenkin ihmisen epäluulot saatetaan saada hälvenemään ja kääntymään huijareiden eduksi. (Salmivuori 2016, 27.)

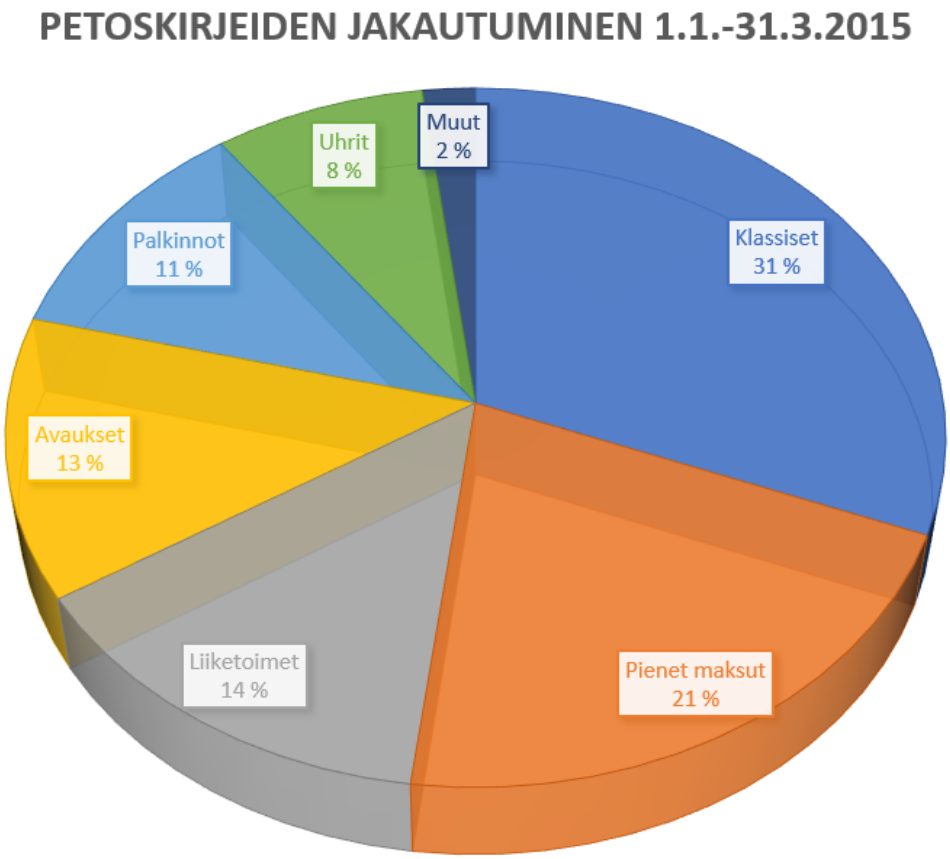
Aivan kuten Salmivuorikin toteaa kirjassaan, ovat verkkopetokset, erityisesti sähköpostitse tapahtuvat huijaukset useimmille internetin käyttäjille lähinnä ärsyttävää roskapostia, jonka

hävittäminen vie vain hetken. Salmivuori on arvioinut, että huijausviestien vastausprosentti olisi noin yhdestä viiteen prosenttia. Määrä tuntuu vähäiseltä, mutta huijausviestien määrään suhteutettuna viesteihin vastanneiden luku kasvaa huijareiden kannalta katsottuna kuitenkin kannattavaksi. (Salmivuori 2016, 27.)

Vuonna 2000 maailmalla kiersi ”I Love You” -sähköposteja, jotka houkuttelivat ihmisiä avaamaan viestejä johdatellen heitä olettamaan niiden tulleen joltain viestin saajan läheiseltä. Viestiä avattaessa kyseiselle tietokoneelle asentui virus, joka levitti samaa viestiä kaikille viestin vastaanottajan sähköpostin kontaktilistalla oleville henkilöille. Kymmenessä päivässä yli 40 miljoonaa tietokonetta oli saastunut tällä viestillä. (Holt & Grabosky 2017, 17.)

Lupaava romanssi on myös yksi tapa, jolla ihmisiltä voidaan helposti huijata rahaa internetissä. Romanssihuijauksen tekijän tavoitteena on yksinkertaisimmillaan saada huijauksen uhri lähettämään rahaa yleisimmin netissä tapahtuvan deittailun ohessa. Toiveikasta ihmistä on valitettavan helppo johtaa harhaan lupaavaksi naamioidulla ihmissuhteella. Verkon välityksellä huijarin ei tarvitse panostaa niin paljon näyttelijän taitoihin kuin kasvotusten. Verkossa pystyy helposti huijaamaan useampaa ihmistä kerralla, ja myös itse huijauksen taustalla voi olla useampia tekijöitä.
Huijauksessa pyritään luomaan ensin kontakti uhriin esimerkiksi seuranhakupalvelun kautta väärennetyllä profiililla. Uhrin löydyttyä pyritään vähitellen rakentamaan luottamuspohjaa tämän kanssa. Riittävän tunnesiteen rakennuttua, syntyy tarinalle jokin traaginen käänne, joka uhkaa suhteen jatkoa. Ongelma ratkeaa vain, jos uhri "lainaa" tai antaa rahaa huijarille. (Viestintävirasto 2014, 4.)

Salmivuori teki otantatestin luomalla uuden sähköpostitilin aikavälille 1.1−31.3.2015, jonka aikana hänen sähköpostitililleen saapui yhteensä 427 viestiä. Näiden viestien jakautuminen on osoitettu sektoreittain kuvassa 2.



Kuva 2. Sähköpostin petoskirjeiden jakautuminen sektoreittain ajalla 1.1.−31.3.2015 (Salmivuori 2016, 86.)

Suurimmaksi huijausviestiryhmäksi osoittautuivat klassiset huijaukset, joita Salmivuori sai sähköpostiinsa yhteensä 132 kappaletta. Salmivuori luonnehtii klassisia huijauksia stereotyyppisiksi "nigerialaiskirjeiksi". Näistä tyypillisin lienee perilliskäsikirjoitus, jossa klassisesti huijari esittäytyy jonkin valtiollisen elimen edustajana, lakimiehenä tai pankkiirina etsien perillistä. Tästä seuraa viestiketju, jonka lopullisena tavoitteena on tarkoitus saada vastapuoli lähettämään rahaa huijareille saadakseen itselleen luvatun palkkion. Tätä palkkiota on kuitenkin lopulta turha jäädä odottelemaan. Toinen tyypillinen esimerkki klassisesta huijauksesta on viesti, jossa vastaanottajalle luvataan likimain kirjaimellisesti laatikkokaupalla rahaa. (Salmivuori 2016, 45-47.)

Seuraavaksi suurimpana ryhmänä esittäytyy pienet maksut, joita Salmivuoren sähköpostiin tuli yhteensä 88 kpl. Luku on yli viidennes koko otannasta. Näiden viestien kaavat toista-

vat pääasiassa jo yllä lueteltuja esimerkkejä, mutta lisänä näissä esitellään yleensä jo ensimmäisen viestin kohdalla pieni, yleensä muutamien kymmenien eurojen suuruinen käsittelymaksu, jonka maksutiedot löytyvät useimmiten viestin lopusta. (Salmivuori 2016, 75-76.)

Avauksien (54 kpl) ja liiketoimien (60 kpl) lukumäärät olivat suurin piirtein samat. Avauksien tarkoituksena oli yksinkertaisimmillaan tarkoitus avata keskustelu mahdollisen uhrin kanssa. Lopputulema avausviestien takana on useimmiten kuitenkin sama kuin klassisissa huijauksissa, näissä lähestymistapa on vain hieman erilainen. Liiketoimien kohdalla huijarit puolestaan lähestyvät vastaanottajiaan pääasiassa sijoittajina tai sijoittajien edustajina, jotka etsivät itselleen luotettavaa sijoituskumppania ulkomailta. (Salmivuori 2016, 59, 77.)

Uhreille suunnatuissa huijausviesteissä pyritään jo nimenkin mukaisesti ottamaan yhteyttä joko jo kerran huijatuksi tulleisiin uuden huijauksen toivossa tai vaihtoehtoisesti kokeilla huijata uudelleen niitä, jotka ovat aiempien huijausten kohdalla kesken kaiken tajunneet olevansa tulossa huijatuksi. Nämä huijaukset ovat verkkopetosten maailmassa niin kutsuttuja uusia tulokkaita. Huijarin näkökulmasta kerran huijattua voidaan pitää niin sanottuna ihannekohteena, sillä yleensä huijatuksi tulleella on satunnaista verkonkäyttäjää suurempi motivaatio saada kerran huijarille menettämänsä rahasummansa takaisin. (Salmivuori 2016, 72-75.)

Muut huijaukset- ryhmään kuuluu karkeasti ottaen kaikki muut huijausviestit (8 kpl), joita Salmivuori ei tässä kohtaa katsonut enää asiakseen jakaa pienempiin alaryhmiin. Näihin huijausviesteihin lukeutui esimerkiksi uhkaus- ja kutsuviestejä. Oman lukunsa muodostavat myös erilaisissa verkossa tapahtuvissa kauppapaikoissa piinaavat huijarit, jotka voidaan karkealla jaolla jakaa myyjiin ja ostajiin. Nämä erilaisissa verkkohuutokaupoissa tapahtuneet petostyypit ovat kuuluneet viime vuosina Suomen poliisin yleisimpiin tietoon tulleisiin petoksiin. (Salmivuori 2016, 83-84.)

Rikoskomisario Siurola (2018) kertoo phishing kampanjoiden, eli tietojenkalasteluviestien, olevan myös nykyään paljon esillä. Ihmisiä varoitellaan tällaisesta rikollisesta toiminnasta

paljon. Esimerkiksi pankkitunnuksia ei tulisi koskaan luovuttaa kenellekään. Siitä huolimatta ihmiset sortuvat näihin tietojenkalasteluihin jatkuvasti.

4.3 Valepoliisirikokset

Valepoliisi-ilmiöllä tarkoitetaan tilannetta, missä poliiseiksi esiintyvät rikolliset käyttävät hyödykseen suomalaisten luottamusta poliisiin ja kalastelevat tätä luottamusta hyväksikäyttäen erityisesti ikäihmisten verkkopankki- ja pankkikorttitunnuksia. Poliisina valheellisesti esiintymistä kutsutaan rikosnimikkeellä virkavallan anastus. Poliisina esiintymisten lisäksi myös muiden luottamusta herättävien tahojen nimissä tehty huijaaminen on lisääntynyt. Pelkästään vuonna 2017 poliisi on kirjannut virkavallan anastuksista, niihin liittyvistä petosrikoksista sekä niiden yrityksistä 950 rikosilmoitusta, ja näistä aiheutuneet rikosvahingot ovat olleet 2017 vuoden aikana lähes miljoona euroa. (Poliisi 2018, A.)

Valepoliisien soittamat petospuhelut noudattavat pääsääntöisesti samaa kaavaa. Yleisimmin soittaja esittäytyy poliisina ja kertoo puheluun vastanneelle, että tämän tili on hakkeroitu tai sitä yritetään käyttää väärin. Uhrille kerrotaan, että poliisi yrittää tilitietojen ja pankkitunnusten avulla estää teon. Puhelun tavoitteena on siis saada puhelimeen vastannut henkilö kertomaan pankkitunnuksensa sekä tilinumeronsa, jonka jälkeen rikolliset pyrkivät tyhjentämään näiden tilit mahdollisimman nopeasti. Useimmiten soittajat osaavat puhua sujuvaa suomen kieltä ja tarvittaessa pystyvät muuttamaan tarinaansa puhelun edetessä uskottavan kuuloiseksi. (Pisto 2017.)

Valepoliisina esiintymiset lähtivät ensin liikkeelle puhelinsoittoina, mutta yhä enemmän esiintyy myös sitä, että tullaan kotiovelle ja esiinnytään valheellisesti eri ammattikuntien edustajina. Yleisimpiä peiteammatteja huijareille voivat olla poliisin lisäksi esimerkiksi katonkorjaajat, putki-, rakennus- tai asfalttimiehet. Yleisimmin ovelta ovelle- huijareina esiintyy naisia, sillä he osaavat keskustella ikäihmisten kanssa luottamusta herättävästi. Huijauksen tavoitteena on päästä asuntoon sisään ja voittaa asunnon omistajan luottamus itselleen. Jossain kohtaa huijari pyrkii saamaan asukkaan toiseen huoneeseen harhautukseksi ja poistuu lopulta itse asunnosta löytämiensä arvotavaroiden tai -omaisuuden kanssa. (Pisto 2017.)

Sisä-Suomen poliisilaitoksen rikosylikomisario Jari Kinnunen kertoo, että ikäihmisiin kohdistuneiden valepoliisihuijausten taustalla ovat lähes poikkeuksetta romanit ja selkeästi järjestäytynyttä rikollisuutta. Kinnunen kertoo, että vuoden 2017 aikana selvitettyjen valepoliisirikosten taustalta on aina löytynyt romani. Hänen mukaan romanien petostoiminta on hyvin organisoitua ja koko maan kattavaa. (Lehtinen 2017.)

4.4 Scareware ja ransomware -haittaohjelmat

Scarewarella tarkoitetaan nopeasti leviävää haittaohjelmaa, jonka tarkoituksena on pelotella tietokoneen käyttäjää esimerkiksi väärillä virustorjuntahälytyksillä. Haittaohjelma esiintyy yleisimmin erilaisina ponnahdusikkunoina tietokoneen näytöllä. Ponnahdusikkunassa ilmoitetaan varoitustekstein, että kyseisessä tietokoneessa on havaittu virus. Viestissä käyttäjää pyydetään suorittamaan maksu, jonka jälkeen virus luvataan poistaa. Vaikka kyseistä maksua ei maksaisikaan, on tietokoneen käyttäjä saattanut jo epähuomiossa sallia haittaohjelman pääsyn koneelle, jolloin ohjelmalla on pääsy tietokoneen sisältöön. Osa ohjelmista saattaa myös kopioida sisällöt talteen, jolloin koneen käyttäjä on menettänyt ne kokonaan haittaohjelman käytettäväksi. (Siciliano 2017.)

Sacreware tyyppisiä haittaohjelmia saatetaan toimittaa ihmisille myös sähköpostin välityksellä. Sähköpostiviestissä suostutellaan tavalla tai toisella henkilöä lataamaan todellisuudessa hyödytön palveluohjelma tietokoneelle. Jossain vaiheessa palveluohjelman käyttöönottoa henkilöltä kysytään luottokorttitietoja. Mikäli nämä tiedot erehtyy antamaan, voi kyseinen henkilö joutua tulevaisuudessa identiteettivarkauden uhriksi. (Kaspersky Lab 2018 A.)

Ransomware on kiristykseen perustuva haittaohjelma, joka asentuessaan uhrinsa tietokoneelle lukitsee koneen ja vaatii rahallista korvausta lukituksen poistamiseksi. Kyseisen lajityypin haittaohjelmat ovat levinneet jo useamman vuoden ajan internetissä ympäri maailmaa. Osa kiristysohjelmista on harmittomia, eivätkä todellisesti lukitse konetta. Jotkut kiristysohjelmista kuitenkin salaavat tiedostot tietokoneelta, jolloin ainut tapa päästä tiedostoihinsa käsiksi on saada salauksen purkuavain. (F-Secure ym. 2018.)

Linkkejä haittaohjelmiin saattaa olla verkossa monessa paikassa. Esimerkiksi YouTube -videotoistopalvelussa voi olla linkki Salatut Elämät -TV sarjan jaksoon. Kun jaksoa yrittää katsoa, videolla näkyy viesti joka kehottaa lataamaan videon alla olevasta linkistä ohjelman, jotta voi katsoa koko jakson. Jos käyttäjä erehdyksessä lataa ohjelman koneelleen asentaakin hän tietämättään haittaohjelman. (Kurittu 2018.)

Erityisasiantuntija Kurittu (2018) kertoo ensimmäisten kiristysohjelmien saapuneen ehkä 5 – 10 vuotta sitten. Kiristysohjelmat on mahdollistanut käytännössä kaksi asiaa. Ensinnäkin virtuaalivaluutta anonyymina valuuttana mahdollistaa varainsiirron. Toiseksi tietokoneiden arkipäiväistyminen, joka tarkoittaa, että kaikilla on sähköpostit ja sosiaalisen median tilit. Ihmisten koko digitaalinen elämä on yhdellä koneella ja useimmiten ilman varmuuskopiota. Rikolliset keksivät, että tietojen varastamisen sijaan he tekevät tiedon käyttökelvottomaksi ja myyvät salauksen purkuavaimen koneen haltijalle. 90 -luvulla tämä ei olisi ollut mahdollista, koska tiedostojen salakirjoittaminen olisi vienyt niin paljon aikaa. Nykyään sen voi tehdä hetkessä.

Rikosylikomisario Muurmanin (2018) mukaan kiristyshaittaohjelmilla on ilmeisesti tehty jo niin paljon rahaa, ettei pankkihaittaohjelmia Suomessa juurikaan enää esiinny. Myös tietokonepäätteiden käyttö on vähentynyt nykymaailmassa, koska ihmiset käyttävät matkapuhelimia aktiivisemmin ja tallettavat sinne tiedon, joka ennen tallennettiin tietokoneille. Tämä kehitys on tuonut kiristyshaittaohjelmat myös matkapuhelimiin. Matkapuhelimen sisällön menetys on nykyään jopa haitallisempaa kuin tietokoneen sisällön menetys, riippuen käyttäjästä.

4.5 Vakoiluohjelmat ja sextortion

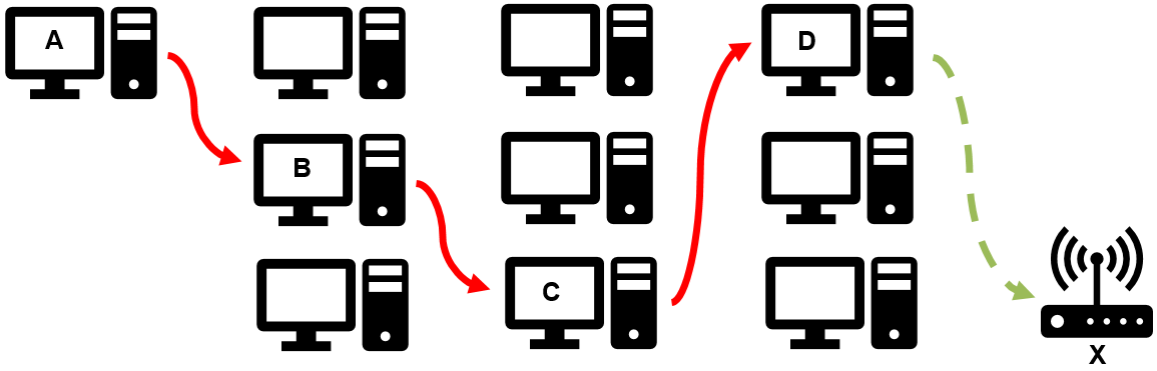
Erilaiset vakoiluohjelmat ovat myös tätä päivää. Vakoiluohjelmilla pyritään saamaan selville käyttäjän tietoja kuten salasanoja ja käyttäjätunnuksia. Yllättävän useassa parisuhderiidassa vakoillaan toisen puoliskon tekemisiä tämän tietokoneen välityksellä, ujuttamalla siihen ensin vakoilun mahdollistava haittaohjelma. (Kurittu 2018.)

Tietokoneen kameralla voidaan vakoiluohjelman tietokoneelle asentumisen jälkeen vakoilla esimerkiksi nuoria naisia. Keräämällä tällaista materiaalia, voi rikoksen tekijä kiristää uhriaan uhkaamalla julkaista kyseisen materiaalin verkossa. (Kurittu 2018.) Rikoksen tekijä voi myös lähestyä uhriaan jonkin verkon sosiaalisen kanavan kautta ja huijaa uhriaan lähettämään seksuaalista videota tai kuvaa itsestään. Kuvan tai videon saatuaan rikoksen tekijä ilmoittaa uhrilleen, että tämän täytyy maksaa tai vaihtoehtoisesti lähettää lisää vastaavanlaista materiaalia, tai rikoksen tekijä julkaisee saamansa materiaalin verkossa. Tällaista toimintaa kutsutaan sextortioniksi, eli seksikiristykseksi. (Europol 2018.) Pahimmassa tapauksessa kiristys siirtyy kasvotusten tapaamiseen, ja kiristäjä kuvaa itse uhrinsa hyväksikäyttöä ja kiristysmateriaali lisääntyy. (Kurittu 2018.)

4.6 Nimettömyys verkossa

Digitalisaatio tarjoaa kehityksen myötä rikollisille yhä paremmat mahdollisuudet toimia nimettömästi verkossa. Anonymiteettiä lupaavat ohjelmat ovat kehittyneet aina Tor (The Onion Router) -teknologiaan, joka perustuu usean tason salaukseen ja käyttäjän toiminnan kierrättämisen tuhansien vapaaehtoisten verkon käyttäjien kautta. Tällöin viestin lähettäjien ja vastaanottajien identifiointi on usein mahdotonta. (Grabosky & Holt 2017, 17.)

Kuvassa 3 havainnollistetaan Tor -verkon toimintaa. Käyttäjä A käyttää Tor -verkkoa ja haluaa salata tietoliikenteensä palvelimeen X. Käyttäjät B ja C käyttävät myös Tor -verkkoa ja tarjoavat Tor -verkon sisällä salattua tietoliikenteensiirtoa. Käyttäjä D toimii niin kutsuttuna exit nodena, eli tarjoaa tietoliikenteen Tor -verkosta ulospäin, jolloin D käyttäjän koneesta oleva yhteys palvelimeen X ei ole salattua. Kun A:n tietoliikenne kiertää Tor -verkon kautta ei A:n yhteyttä palvelimeen X voida selvittää. (Electronic Frontier Finland ry 2018.)



Kuva 3. Tor -verkon toimintamalli (Electronic Frontier Finland ry 2018).

Tor -verkko on kehitetty suojaamaan verkossa tapahtuvaa viestintää, tehden viestien lähettäjien ja vastaanottajien selvittämisestä lähes mahdotonta. Tor -verkon käyttäminen on helppoa ja käyttäjämäärät saadaan pidettyä tällä tavalla mahdollisimman suurina. Kun käyttäjiä on paljon, ei Tor -verkossa välitettävää dataa tai sen lähdettä voida jäljittää. Kun dataliikenteen määrä on käyttäjäpaljouden vuoksi suurta, on myös sen puolesta yksittäisen käyttäjän toimintojen seuraaminen erittäin haastavaa. (Ollila 2016, 6.)

Myös virtuaalivaluutat mahdollistavat nimettömänä toimimista verkossa. Rikoskomisario Siurolan (2018) mukaan virtuaalivaluuttaa hyväksikäyttävät rikolliset tekevät maksuja keskenään virtuaalivaluutassa vaikean jäljitettävyyden vuoksi. Kun varat halutaan muuttaa reaalivaluutaksi, voidaan virtuaalivaluutta muuttaa esimerkiksi arvo-omaisuudeksi. Tämän jälkeen arvo-omaisuus myydään, jolloin saadaan reaalivaluuttaa käyttöön.

4.7 Tilausansat

Tilausansoilla tarkoitetaan usein erilaisissa sosiaalisen median kanavissa esiintyviä mainoksia, joissa mainostetaan esimerkiksi muutaman euron merkkilenkkareita, uutta älypuhelinta postikulujen hinnalla tai ilmaisia tuotekokeilupaketteja. Mainoksen avattuaan kuluttaja pyritään sitomaan erilaisiin määräaikaisiin tai pitkäkestoisiin hinnakkaisiin sopimuksiin, joita kuluttaja ei aluksi välttämättä edes huomaa klikkausten vuoksi syntyneen. (Euroopan kuluttajakeskus Suomessa 2017.)

Tyypillisimmillään tilausansatapauksissa kuluttaja saa puhelinmyyjältä tai verkkokaupalta laskun tuotteesta, jota ei muista tai ole ymmärtänyt tilanneensa. Yleisimmin tiedot yllättävistä seikoista löytyy sopimusehdoista mainoksen lopusta pienellä printattuna. (Kilpailu- ja kuluttajavirasto 2014.) Kilpailu- ja kuluttajavirasto on listannut tyypillisimpiä tilanteita, joissa kuluttajan on mahdollista perua epähuomiossa tekemänsä sopimus tai tilaus ja ohjeistaa kuluttajaa toimimaan näissä tilanteissa oikealla tavalla.

4.8 Kyberrikollisverkostot

Kyberrikoksien tekijät ovat myös monimuotoistuneet ajan saatossa, enää tekijöiden ei tarvitse olla IT-asiantuntijoita. Palvelut kyberrikosten tekemiseen voi ostaa asiantuntijoilta, mikä avaa mahdollisuuksia uusille toimijoille. Tämän kaltaisia toimijoita on monenlaisia kuten perusrikollisuudessakin. Osa rikollisista toimii yksinomaan verkossa ja toisille verkkorikollisuus on vain oheistoimintaa. (Grabosky & Holt 2017, 19.) Internetissä toimii erityisesti laittomiin tarkoituksiin suunnattuja Darknettejä sekä tavanomaisten hakukoneiden tavoittamattomissa olevia Deep Webejä ja muita foorumeita. Ne ovat rikollisuuden markkina- ja kohtauspaikkoja (Sisäministeriön julkaisu 2017, 12). Deep Web ei kuitenkaan tarkoita laitonta sisältöä. Deep Web pitää sisällään esimerkiksi verkkopankin sivut, joihin pääsee kirjautumalla ja yksityiset internetissä olevat tietokannat. (Kaspersky Lab 2018 B.)

Osa verkossa toimivista ryhmistä ei ole juurikaan organisoituneita, eikä heillä ole erillistä johtoa. Tämän tyyppiset ryhmittymät keskittyvät paljolti erilaisiin ideologisiin hankkeisiin, kuten viharikoksiin ja poliittisiin vasta-asetteluihin. Tähän ryhmään kuuluu esimerkiksi tunnettu auktoriteettivastainen Anonymous -anarkistiryhmä, jonka toimintatapoihin kuuluu verkkoilkivalta. Anonymous -ryhmän jäsenet ovat niin sanottuja haktivisteja. (Grabosky & Holt 2017, 20.)

Toiset pääosin verkossa toimivat ryhmittymät ovat organisoituneempia, ja heillä on selkeämpi johto. Tämän tyyppiset ryhmittymät toimivat laajemmalla toiminta-alueella ja hyödyntävät toiminnassaan esimerkiksi piratismia, verkkourkintaa ja botteja, sekä tekevät ver-

kossa seksuaalirikoksia. Scareware-pelottelutyyppiset haittaohjelmat ovat usein näiden ryhmittymien käsialaa. (Grabosky & Holt 2017, 20.)

Jotkin kyberrikosryhmittymät ovat niin kutsuttuja ”hybridejä”, jotka toimivat sekä verkossa että verkon ulkopuolella. Nämä ovat yleensä organisoituneita ryhmiä, joiden toimet verkon ulkopuolella voivat olla esimerkiksi luottokorttien kopiointia. Rikollisin keinoin saatuja korttitietoja käytetään tämän jälkeen verkossa luvattomaan ostamiseen tai kyseiset korttitiedot saatetaan myydä eteenpäin toisille rikollisille. (Grabosky & Holt 2017, 20.)

Näiden lisäksi on rikosryhmiä, jotka toimivat pääosin verkon ulkopuolella, mutta käyttävät verkon tarjoamia mahdollisuuksia edistääkseen toimintaansa. Tällaisia toimia saattavat olla esimerkiksi aikuisviihdesivut prostituution jatkeena, järjestelmiin kohdistuvat kiristykset ja uhkailut tai yksityisten tiedostojen hankkiminen hakkeroinnilla. Verkko tarjoaa myös helpon tavan kommunikoida ja koordinoida rikollista toimintaa. (Grabosky & Holt 2017, 20.)

Rikosylikomisario Muurman (2018) toteaa rajanvedon verkkorikollisuuden ja muun rikollisuuden välillä alkavan hälventyä. Verkkorikollisuus hyödyntää osin samoja rahanpesuorganisaatioita kuin esimerkiksi huumausainerikollisuus. Rikoskomisario Siurola (2018) lisää DarkWebin eli niin kutsutun "pimeän verkon" olevan nykyään mukana yhä useammissa eri rikostyypeissä.

5 OPINNÄYTETYÖN TAVOITTEET JA MENETELMÄT

Tässä osiossa kerrotaan toiminnallisen opinnäytetyön tavoitteista ja menetelmistä, joilla asetetut tavoitteet voidaan saavuttaa.

5.1 Tavoitteet

Opinnäytetyön tavoitteena on lisätä ihmisten tietoisuutta ja valveutuneisuutta kyberrikollisuudesta sekä tietoverkossa tapahtuvista rikoksista. Kyberrikollisuus on rikollisuuden muotona verrattain tuore ilmiö, ja yhä enemmän myös tavalliset ihmiset joutuvat erilaisten tietoverkossa tapahtuvien rikosten uhreiksi.
Kyberrikollisuutta on nostettu viime aikoina paljon esille poliisin toimesta, ja siihen liittyvään ennalta estävään toimintaan on panostettu yhä enemmän. Tämä opinnäytetyö, ja sen toiminnallisena osuutena toteutettu produkti, on haluttu toteuttaa nimenomaan tavallisia verkon käyttäjiä varten parantaakseen heidän tietoisuuttaan verkossa tapahtuvasta rikollisuudesta.

5.2 Toiminnallinen opinnäytetyö

Opinnäytetyön menetelmäksi valittiin toiminnallinen opinnäytetyö, koska tarkoitus oli saada aikaan jotain konkreettista − jokin konkreettinen tuotos eli produkti. Kumpikaan opinnäytetyön tekijöistä ei ollut aiemmin tehnyt toiminnallista opinnäytetyötä, mikä myös lisäsi kiinnostusta menetelmää kohtaan.

Toiminnallisella opinnäytetyöllä tarkoitetaan työtä, jonka tavoitteena on yleensä kehittää käytännön toimintaa työelämässä. Näin ollen toiminnallisella opinnäytetyöllä on usein toimeksiantaja. Toiminnallinen opinnäytetyö poikkeaa perinteisestä tutkimuksellisesta opinnäytetyöstä siinä, että toiminnallisella opinnäytetyöllä on jokin erillinen produkti. Produktin lisäksi muodostuu opinnäytetyöraportti, eli opinnäytetyöprosessin dokumentointi. Opinnäytetyö on näin siis kaksiosainen. (Myllylä 2017.)

Tämän opinnäytetyön produktina on internetiin toteutettava testi, jonka tavoite on lisätä ihmisten tietoisuutta sekä valveutuneisuutta verkossa tapahtuvista rikoksista nimenomaan ennalta estävästä näkökulmasta. Haaste oli suuri, sillä kyberrikollisuus on aihealueena laaja ja opinnäytetyön toteutuksen aika sekä resurssit ovat rajalliset. Opinnäytetyötä suunniteltaessa sekä sen edetessä oli huomioitava, ettei valittu toteutusmenetelmä pääse kasvamaan liian suureksi ja näin vaikuttaen negatiivisesti kokonaisuuteen.

Tutkimusasetelmassa ytimenä ovat tutkimuskysymykset, joiden ympärille itse työ kootaan. Toiminnallisen opinnäytetyön ollessa kyseessä, ei kuitenkaan puhuta välttämättä niinkään tutkimuskysymyksistä, vaan esimerkiksi arviointikysymyksistä, kehittämiskysymyksistä tai pelkästään kysymyksistä. (Toikko & Rantanen 2009, 117.) Toiminnallisessa opinnäytetyössä ei välttämättä ole edes opinnäytetyölle ominaisia tutkimuskysymyksiä, jotka pysyisivät alusta loppuun samoina, vaan ne saattavat muovaantua ja kehittyä projektin aikana (Myllylä 2017).

Koko opinnäytetyöprojektin aikana tulee käyttää hyödyksi prosessiarviointia, jonka tehtävä on systemaattisin menetelmin avata tyypillisesti moniulotteisia ja tilanne-ehtoisia kehittämisprosesseja. Siinä seurantatiedon, palautteen ja reflektion pohjalta tehdään johtopäätöksiä, joilla kehittämistoimintaa ohjataan kohti projektin tavoiteltavaa visiota sekä tuotetaan tietoa kehittämistoimenpiteiden ja vaikutusten välisestä suhteesta. (Seppänen-Järvelä & Karjalainen 2003, 225.)

Tässä opinnäytetyössä prosessiarviointiin osallistuvat paitsi tekijät itse itsearvioinnilla, myös opinnäytetyön ohjaaja ulkoisena evaluaattorina. Itsearvioinnit ovat monessa asiassa elinehtona kehitykselle, niin ihmisten henkilökohtaisessa elämässä, kuin organisaatioissa. Projekteissa itsearvio on ehtona toimivalle tuotokselle. Projektin aikana pidetään kenttäpäiväkirjaa, jotta projektin kokonaiskuva pysyy selkeänä ja hallittavana. Kenttäpäiväkirjaan kirjataan mitä on tehty ja suunnitellaan mitä tullaan tekemään. Projektin aikana peilataan jo toteutettuja ja tulevaisuuden suunnitelmia, jotta fokus pysyy oikeana. (Seppänen-Järvelä & Karjalainen 2003, 229.)

Tiedon keräämisen ja suodattamisen merkitys opinnäytetyössä on kaksiosainen. Toikon ja Rantasen kirjassa ”Tutkimuksellinen kehittämistoiminta” kerrotaan kaksiosaisesta tiedontuotannon merkityksestä. Ajatuksena on, että tiedon tuotolla tavoitellaan paitsi ennalta-asetettujen tavoitteiden saavuttamista, myös tiedon tuottajien omaa oppimista sekä oman toiminnan kehittämistä. Tällainen toiminta- ja ajatusmalli on vahvasti esillä asiantuntija-ammateissa toimivilla henkilöillä. (Toikko & Rantanen 2009, 117.)

Tässä opinnäytetyössä tuotettu tieto muovautuu lopputuloksena tuotettuun testipohjaan. Miten hyvin testipohja lisää kansalaisten tietoisuutta kyberrikollisuudesta määrittelee, onko työllä tavoiteltava tavoite saavutettu. Poliisin ammatti on ehdottomasti asiantuntija-ammatti, jolloin tiedonkeruu tähän projektiin kehittää myös tekijöiden omaa ammattitaitoa, ja projekti toimii näin tuplatavoitteellisesti. Kyberrikollisuus on nykyajan alati kehittyvä rikollisuuden muoto ja sen ymmärtäminen tulee olemaan poliisin työtehtävissä merkittävää. Tiedontuotannossa tärkeää on myös kokonaisuuden hallinnointi. Tiedontuotanto toimii reflektiivisenä herättelynä tekijöiden keskuudessa.

Reflektiivinen herättely näkyy opinnäytetyön edetessä palaverikäytänteenä. Palavereissa käydään läpi kerättyä tietoa ja herätellään keskustelua sekä pyritään näiden pohjalta jatkuvasti uudelleen suuntaamaan projektia oikeaan suuntaan. Alussa ajateltu suunta ei projektin edetessä välttämättä osoittaudu lopulliseksi suunnaksi ja tämän vuoksi tällaiset reflektiiviset herättelyt ovat tärkeitä, jotta säästetään aikaa ja toimitaan mahdollisimman tehokkaasti. (Toikko & Rantanen 2009, 117.)

Ajatuksena opinnäytetyössä on tuoda tieto mahdollisimman selkeästi kansalaisten ulottuville. Tällaisessa asetelmassa on tärkeää, että tekijät tiedostavat omat suodattimensa ja tuottavat tiedon sellaisessa muodossa, että sillä saavutetaan haluttu tulos, eli kansalaisten tietoisuuden lisääminen. Tällaisten faktojen jakamisessa on tekijöiden ja kohteen erillisyys oltava lähtökohtana, kun tietoa tuotetaan asiantuntijatasolta hyvin laajalle skaalalle kansalaisia. Työtä varten kerättävä ja tuotettava tieto on oltava riippumatonta subjektiivisista tekijöistä. (Toikko & Rantanen 2009, 118.)

Projekteissa, kuten tässä opinnäytetyössä, on onnistumisen ja tehokkuuden takaamiseksi tärkeää tehdä projektisuunnitelma. Ennen itse suunnitelmaa on oltava mietittynä tarpeen tunnistaminen. On listattava käytössä olevat resurssit, aikataulu ja projektin rajoitteet. Ilman näitä alkupohdintoja voi projektin edetessä tulla haasteita esimerkiksi projektin liiasta paisumisesta tai aikataulullisista haasteista. (Kettunen 2009, 93.)

Alkujaan tämän opinnäytetyön toiminnallisena produktina oli tarkoitus järjestää jonkinlainen tapahtuma, missä ajatuksena oli tuoda esille kyberrikollisuuden uhkia ja sitä, miten kansalaisten olisi mahdollista niitä välttää. Tämän toteutustavan haasteena olisi ollut ennen kaikkea saada jaettua tietoa mahdollisimman isolle ihmismäärälle, mutta myös saada paikalle oikeaa kohdeyleisöä. Vaikka tapahtuma olisi järjestetty Helsingissä jonkin pienemmän kaupungin sijaan, olisi tietoisuuden leviäminen silti jäänyt maantieteellisesti hyvin pieneksi. Päädyimme käyttämään internetiä opinnäytetyön produktin lopulliseen jakamiseen sen mahdollistaman suuren tavoiteyleisön vuoksi.

Myös aikataulullisesti internetpohjainen tiedon jakaminen osoittautui helpommaksi tavaksi levittää tietoa. Internetissä tieto leviää nopeasti ja tavoittaa lyhyessä ajassa suuren määrän ihmisiä. Verkossa tietoa pystytään jakamaan nopeasti ja laajasti sosiaalisen median sekä muiden interaktiivisten palstojen avulla. Opinnäytetyön toiminnallisesta osuudesta täytyy saada helposti lähestyttävä ja kiinnostava tuotos, jotta sillä voidaan tavoittaa mahdollisimman suuri yleisö.

Opinnäytetyöprojektin hallinnoimisen ja seurannan helpottamiseksi opinnäytetyö jaetaan välitavoitteisiin. Välitavoitteet helpottavat opinnäytetyöprojektin toteuttamista. Tällöin tekijöiden energia ei kulu koko opinnäytetyöprojektin hallinnoimiseen, vaan tietyn kulloisenkin välitavoitteen saavuttamiseen. Välitavoitteita on kuitenkin peilattava aika ajoin kokonaisuuteen. Projektin jakaminen välitavoitteisiin helpottaa myös projektin seurantaa esimerkiksi ulkopuolisen evaluaattorin näkökulmasta. (Kettunen 2009, 108.) Opinnäytetyössä välitavoitteiden seuranta tapahtuu jo aiemmin mainitun kenttäpäiväkirjan avulla. Kenttäpäiväkirja on työn liitteenä 4. Välitavoitteet aikataulutetaan myös, jotta opinnäytetyön valmistuminen voidaan pitää suunnitellussa aikataulussa.

Suunnitteluvaiheessa on otettava huomioon myös riskit ja niiden hallinta. Riskikartoitus tässä työssä toteutetaan SWOT-analyysilla. Opinnäytetyöprojektin seurannassa on myös pidettävä riskit mielessä ja pyrittävä tunnistamaan ne riittävän ajoissa, jotta riskejä vastaan pystytään suorittamaan oikaisevat toimenpiteet ennen riskien toteutumista. (Kettunen 2009, 122.)

SWOT-analyysin tarkoitus on tuottaa kokonaiskuva analysoitavasta kohteesta. Kyseistä analyysitapaa käytetään usein yritysten tilan kartoittamiseen, mutta se toimii yhtä lailla projektien alkutilan kartoittamisessa, jotta projektin eteenpäin viemiseksi osataan tehdä strategisesti oikeita valintoja. SWOT-analyysia tehtäessä tulisi tehdä riittävä pohjatyö sen kokoamiseksi, jottei analyysiin kerätä vain latteuksia ja itsestäänselvyyksiä. Hyvin tehdyn analyysin pohjalta tulisi voida nostaa muutama keskeinen teema joihin keskitytään. (Vuorinen 2014, 88.)

SWOT-analyysi koostuu neljästä osa-alueesta S (Strengths, Vahvuudet), W (Weakneses, Heikkoudet), O (Opportunities, Mahdollisuudet) ja T (Threaths, Uhat). Näistä kahdella ensimmäisellä kuvataan organisaation, tai tässä tapauksessa tekijöiden sisäisiä asioita, eli niin sanotusti käsillä olevia työkaluja, joilla projektiin ryhdytään. Kahdella jälkimmäisellä puolestaan kuvataan ulkoisia asioita, eli projektia toteuttaessa eteen tulevia haasteita. Vahvuuksien kohdalla on mietittävä, miten niitä voisi projektin edetessä käyttää hyväksi ja vahvistaa. Heikkouksien sekä uhkien kohdalla tulisi miettiä, miten ne saisi käännettyä vahvuuksiksi tai miten ne pystyttäisiin välttämään kokonaan. Mahdollisuuksia tulisi puolestaan pyrkiä hyödyntämään mahdollisimman tehokkaasti. (Vuorinen 2014, 88.)

Tässä työssä käytetty SWOT-analyysi löytyy työn liitteenä 2. SWOT-analyysistä esille nostettava seikka on, että aihe on hyvin ajankohtainen. Tämä luo opinnäytetyölle sen suurimmat haasteet sekä samaan aikaan mahdollisuudet. Opinnäytetyölle on tarvetta, mutta kyberrikollisuuden kenttä on alati muuttuvaa, joten ajoitus ja tietolähteet on valittava tarkasti. Haastavaa on saada opinnäytetyö valmiiksi niin, että siitä on vielä hyötyä sen valmistumisajankohtana, eikä tieto ole ehtinyt oleellisesti vanhentua. Kyberrikollisuuden tuomia uhkia on viime aikoina tuotu esille medioissa paljon. Opinnäytetyö kerää sopivaan aikaan tätä tietoa yhteen ja jakaa sitä omalta osaltaan eteenpäin.

6 ENNALTA ESTÄVÄN HANKKEEN LUOMINEN

6.1 Nettitesti

Opinnäytetyön produktina valmistuu testipohja, joka pitää sisällään kysymyksiä ja vastausvaihtoehdot nettitestin toteutusta varten. Vastausvaihtoehdoista yksi vaihtoehto on oikea kuhunkin kysymykseen. Näiden lisäksi kukin kysymys pitää sisällään tietoiskun, joka ilmestyy, mikäli testiin vastaaja valitsee väärän vastauksen. Kysymyksiä tulee tämän opinnäytetyön aihealueen ilmiöistä. Jotkut ilmiöt ovat tekijöiden keksimiä ja toiset reaalimaailmasta otettuja tapahtumia, joihin tekijät ovat joko opintojensa tai elämänsä aikana törmänneet.

Nettitestin lopullinen toteutus jää tekijöiden resurssien puutteesta johtuen valmistumatta tekijöiden toimesta. Tekijät toivovat, että poliisissa testipohja otettaisiin mielenkiinnolla vastaan ja sitä käytettäisiin lopullisen nettitestin luomiseksi ja julkaistaisiin opinnäytetyön toteutumisen jälkeen. Näin työn ennalta estävä näkökulma toteutuisi parhaiten. Nettitestin pohjakysymykset ovat opinnäytetyön liitteenä 1.

6.2 Suunnittelu ja toteutus

Ennalta estävänä hankkeena toteutettavan nettitestin kysymyspohja muodostui muiden internetissä leviävien testien vaikutteista. Testin on tarkoitus olla helppolukuinen ja nopeasti vastattavissa, jottei vastaajan mielenkiinto lopahda kesken testin tai heti alkuunsa. Myös vastausvaihtoehtojen tulee olla helposti ymmärrettävissä ja sisäistettävissä. Väärästä vastauksesta pitää myös informoida vastaajaa, jotta hän tietää mikä meni pieleen ja oppii virheestään. Tästä syystä väärästä vastauksesta saa ”palkinnoksi” tietoiskun, joka kertoo, miksi vastaus oli väärin. Tietoiskun tulee myös olla ytimekäs, jotta vastaaja siihen viitsii perehtyä. Oikeasta vastauksesta testi liikkuisi vain eteenpäin, koska liika informaation syöttäminen joka käänteessä saattaisi myös olla puuduttavaa.

Testi suunnitellaan kilpailuhenkiseksi, eli mitä nopeammin vastaat oikein kaikkiin kysymyksiin, sitä paremmat pisteet saat. Tämä houkuttelee vastaajan palaamaan testin pariin uudestaan, jos ei ihan pääse esimerkiksi viikon parhaisiin tuloksiin, jotka näkyisivät sivulla. Testin tuloksen voisi jakaa sosiaalisessa mediassa, joka auttaisi testin leviämistä internetissä.

6.3 Loppusanat

Opinnäytetyön tekeminen on lisännyt ja syventänyt tekijöiden tietotasoa kyberrikollisuudesta merkittävästi. Kaikkea opittua ei ole tähän opinnäytetyöhön saatu sisällytettyä, sillä kyberrikollisuus aihealueena osoittautui yllättävän laajaksi. Asiantuntijahaastatteluiden myötä ymmärrys poliisin sisäisistä toimista kyberrikollisuuden saralla on lisääntynyt. Poliisin lisäksi kyberrikollisuuden parissa toimii myös muita ulkopuolisia toimijoita, joista osaan tekijät pääsivät opinnäytetyön ohella tutustumaan. Ennen opinnäytetyön aloittamista aihealue oli molemmille tekijöille entuudestaan vieras, mutta työn valmistuttua aiheen ajankohtaisuus ja työn merkitys on avautunut vielä enemmän.

Kyberrikollisuutta saatetaan edelleen pitää kovin erillisenä osana ihmisten jokapäiväistä toimintaa, mutta kuten tässä opinnäytetyössä on selvinnyt, koskettaa se yhä useampaa ihmistä jossain elämän vaiheessa. Aina tätä ei henkilö itsekään huomaa. Siksi on tärkeää, että aihetta saataisiin tuotua enemmän kaikkien ihmisten tietouteen ja kyberrikollisuuden mukanaan tuomat uhat huomioitaisiin myös tavallisten ihmisten keskuudessa enemmän.

Tulevaisuudessa kyberrikollisuus tulee epäilemättä olemaan yhä arkisempi käsite, kun digitalisoituminen ja sähköistyminen valtaavat palveluita. Kehitys kiihtyy ja vuodessa saavutetaan kehitysaskelia, jotka aikaisemmin ovat vieneet useita vuosia. Tulevaisuudessa tekoäly saattaa olla seuraava suuri askel kehityksessä. Tekoäly luo mahdollisesti täysin uudenlaista infrastruktuuria jolla epäilemättä on myös varjopuolensa. Verkossa tapahtuvat rikokset muuttuvat jatkuvasti ja tästä syystä opinnäytetyössä esille nostetut rikostyypit vanhenevat ja muuntuvat nopeasti. Opinnäytetyöstä oli lähes mahdotonta tehdä sellaista, joka olisi asiasisällöllisesti ajankohtainen vielä vuosienkin kuluttua. Tämä oli kuitenkin asia, joka oli hyväksyttävä jo heti opinnäytetyön aihetta valittaessa.

Opinnäytetyö tuotoksineen on tekijöiden mielestä onnistunut suunnitelmien mukaan. Testipohjan kysymyksistä on pyritty tekemään mielenkiintoisia ja riittävän haastavia iso käyttäjäkunta huomioiden. Suunnitelmasta haluttiin tehdä yksityiskohtainen ja kattava antamaan raameja testin rakennetusta varten. Itse opinnäytetyöstä oli tarkoitus tehdä selkolukuinen ja sellainen, josta tavallinenkin verkonkäyttäjä voisi hyötyä sen lukiessaan. Erityisen hyvin asetetussa tavoitteessa on onnistuttu mikäli joku yksittäinen verkon käyttäjä onnistuu välttämään verkossa rikoksen uhriksi joutumisen opinnäytetyön ansiosta.

LÄHTEET

Electronic Frontier Finland ry 2018. Miten Tor toimii? Luettavissa: http://tor.effi.org/ Luettu 25.01.2018

Euroopan kuluttajakeskus Suomessa 2017: Näin vältät verkon tilausansat – uusi tutkimus Euroopan kuluttajakeskukselta. Luettavissa: https://www.ecc.fi/Ajankohtaista/Tiedotteet/2017/nain-valtat-verkon-tilausansat--uusi-tutkimus-euroopan-kuluttajakeskukselta/ Luettu: 10.1.2018

Europol 2018. Online sexual coercion and extortion is a crime. Luettavissa: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime Luettu 19.01.2018.

FATF Report 2014. Virtual Currencies Key Definitions and Potential AML/CTF Risks. Luettavissa: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf Luettu 15.01.2017

F-Secure, Poliisi & Viestintävirasto 2018. Mitä on ransomware? Luettavissa: http://www.ransomware.fi/ Luettu 13.1.2018

Golovanov Sergey, Soumenkov Igor 2011. TDL4 – Top Bot. Kaspersky Lab, SecureList. Luettavissa: https://securelist.com/tdl4-top-bot/36152/ Luettu 31.10.2017.

Heino, Anne 2017: Valepoliisitoimintaa johtaa järjestäytynyt rikollisryhmä. Uutinen. Luettavissa: https://yle.fi/uutiset/3-9941287 Luettu: 5.1.2018

Hersher Rebecca 2015. Meet Mafiaboy, The 'Bratty Kid' Who Took Down The Internet. NPR. Luettavissa: http://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet Luettu 30.10.2017

Holt Thomas J. & Bossler Adam M. & Grabosky Peter 2017: Cybercrime through an Interdisciplinary Lens. New York, Routledge.

Karismo, Anna 2017: Identiteettivaras vaanii verkossa - Tässä kuusi käytännön ohjetta, joilla vaikeutat huijaajien työtä. Uutinen. Luettavissa: https://yle.fi/uutiset/3-9448910 Luettu: 28.11.2017

Kaspersky Lab 2018 A. What is Scareware? Luettavissa: https://www.kaspersky.com/resource-center/definitions/scareware Luettu 10.01.2018

Kaspersky Lab 2018 B. Cyber Threats and Dangers on the Deep (Dark) Web. Luettavissa: https://usa.kaspersky.com/resource-center/threats/deep-web Luettu 05.02.2018

Kaspersky Lab 2016. IoT: You become responsible for what you have deployed. Luettavissa:
https://www.kaspersky.com/blog/iot-ddos/6210/ Luettu 29.11.2017

Kettunen Sami 2009. Onnistu projektissa. Juva, WS Bookwell Oy.

Kilpailu- ja kuluttajavirasto 2014: Lasku ilman tilausta ja tilausansa. Luettavissa:
https://www.kkv.fi/Tietoa-ja-ohjeita/Ostaminen-myyminen-ja-sopimukset/huijaukset/lasku-ilman-tilausta-ilmaiset-naytepakkaukset/ Luettu: 10.1.2018

Koiranen Ilkka, Räsänen Pekka & Caj Södergård 2016. Talous ja Yhteiskunta 3/2016, Mitä digitalisaatio tarkoittaa kansalaisen näkökulmasta? Luettavissa:
http://www.labour.fi/ty/tylehti/talous-yhteiskunta-32016/mita-digitalisaatio-on-tarkoittanut-kansalaisen-nakokulmasta/ Luettu 09.01.2018

Lehtinen, Pekka 2017: Poliisi: Valepoliisihuijausten romanien järjestäytynyt rikollisuus – petostoiminta kattaa koko maan. Uutinen. Luettavissa:

https://www.mtv.fi/uutiset/rikos/artikkeli/poliisi-valepoliisihuijausten-taustalla-romanien-jarjestaytynyt-rikollisuus-petostoiminta-kattaa-koko-maan/6676522#gs.sLN6dd0
Luettu: 4.1.2018

Myllylä Markku 2017: Tutkimuksellinen kehittämistoiminta ammattikorkeakoulun opinnäytteenä, luentomateriaali. Tampere, Poliisiammattikorekakoulu.

Mäntymaa, Eero 2016: Suomalaisten luotto poliisiin ei horju – yli puolet luottaa poliisiin erittäin paljon. Uutinen. Luettavissa: https://yle.fi/uutiset/3-9210735 Luettu: 16.1.2018

Nordea 2017: Henkilöasiakkaat->päivittäiset raha-asiat -> internet-mobiili- ja puhelinpalvelut - > turvarajat. Luettavissa:
https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/internet-mobiili-ja-puhelinpalvelut/turvarajat.html Luettu: 25.11.2017

Nordea 2017. Pohjoismaiset pankit torjuvat kyberrikollisuutta yhdessä. Luettavissa:
https://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/press-releases/2017/04-10-08h00-pohjoismaiset-pankit-torjuvat-kyberrikollisuutta-yhdessa.html Luettu 23.01.2018.

Norton 2017. Botit ja bottiverkot – kasvava uhka. Luettavissa:
https://fi.norton.com/botnet Luettu 31.10.2017

Nurmi Juha, Kaskela Teemu 2015. Silkkitie, päihteiden suomalaista nappikauppaa. Yhteiskuntapolitiikka. Luettavissa:
https://www.julkari.fi/bitstream/handle/10024/129562/nurmi.pdf Luettu 06.11.2017

Ollila Mikko 2016. Tor-verkko. HAMK Ammattikorkeakoulu, Riihimäki. Opinnäytetyö. Luettavissa:
http://www.theseus.fi/bitstream/handle/10024/120440/Ollila_Mikko.pdf?sequence=1&isAllowed=y Luettu 06.11.2017

Osterwalder Alex, Pigneur Yves 2010: Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. USA New Jersey, Wiley & Sons.

Peltomäki Juha & Norppa Kati 2015: Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki, Talentum Media Oy.

Pihkala, Jaana 2018: Tekijänoikeuden tiedotus- ja valvontakeskus ry:n toiminnanjohtaja. Sähköposti 21.01.2018.

Pisto, Ville 2017: Ole tarkkana, jos kylään pyrkii poliisi, putkimies tai kotipalvelun hoitaja - näin sinua yritetään huijata kotiovellasi. Luettavissa:

https://yle.fi/uutiset/3-9902977 Luettu: 4.1.2018

Poliisi 2017: Poliisin vuosi 2016 – Rikosten määrä pysytteli edellisen vuoden tasolla – nettipetokset jatkoivat kasvuaan. Luettavissa:

http://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/poliisin_vuosi_2016_rikosten_maara_pysytteli_edellisen_vuoden_tasolla_-_nettipetokset_jatkoivat_kasvuaan_56212

Luettu 4.11.2017

Poliisin tilastot vuosi 2016, nettipetokset. Luettavissa:

http://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/polisenaxwwwstructure/56209_Poliisin_tilastot_vuosi_2016_nettipetokset.pdf?19fce54b8a46d488

Luettu 4.11.2017

Poliisi 2018 A: Huijauksen monet muodot. Luettavissa:
https://www.poliisi.fi/rikokset/huijaukset Luettu 20.1.2018'

Poliisi 2018 B: Poliisin ennalta estävä toiminta
https://www.poliisi.fi/rikokset/ppoliisin_ennalta_estava_toiminta Luettu 25.1.2018

Poliisi 2018 C: Ennalta estävä poliisitoiminta Helsingissä. Luettavissa:
http://www.poliisi.fi/helsinki/ennaltaestava Luettu 25.1.2018

Poliisi 2018 D: Kyberrikollisuus. Luettavissa:
http://www.poliisi.fi/rikokset/kyberrikollisuus Luettu: 25.1.2018

Poliisiammattikorkeakoulu 2017: Tilastotietoa poliisin toiminnasta ja rikollisuudesta, loka-kuu 2017. Luettavissa:
http://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/64914_Polstat_tilastot_loka2017.pdf?51cd5dfe081dd588
Luettu 25.11.2017

Puolustusvoimat 2018: Kybervarusmies, Puolustusvoimien johtamisjärjestelmäkeskus. Luettavissa:
http://varusmies.fi/palvelustehtavat-ja-paikat/-/services/506 Luettu 06.11.2017

Rapila, Pekka 2010: Yksilön ja yhteiskunnan turvallisuus. Luettavissa: http://www.edu.fi/turvallisuus_ja_liikenne/turvanetti/yksilon_ja_yhteiskunnan_turvallisuus
Luettu 22.10.2017

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

Samsung 2018: Family Hub. Luettavissa: https://www.samsung.com/us/explore/family-hub-refrigerator/overview/ Luettu 29.11.2017

Seppänen-Järvelä Riitta ja Karjalainen Vappu 2009: Kehittämistyön risteyksiä. Jyväskylä, Gummerus kirjapaino Oy.

Siciliano, Robert 2017: What is Scareware? Luettavissa:

https://www.thebalance.com/what-is-scareware-4019121 Luettu 3.1.2018

Sisäministeriö 2016: Poliisibarometri 2016. Luettavissa:
http://intermin.fi/julkaisut/julkaisu?pubid=URN:ISBN:978-952-324-107-7
Luettu: 20.10.2017

Sisäministeriö 2017: Kyberrikollisuus ylittää rajat tietoverkoissa. Luettavissa: http://intermin.fi/poliisiasiat/kyberrikollisuus Luettu: 25.11.2017

Sisäministeriö 2017: Sisäministeriön julkaisu 14/2017. Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Luettavissa:
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1 Luettu 19.01.2017.

Sisäministeriö 2018. Kyberrikollisuutta torjutaan yhteistyöllä. Luettavissa:
http://intermin.fi/poliisiasiat/kyberrikollisuus/kyberrikollisuuden-torjunta Luettu 23.01.2018.

Turvallisuuskomitea 2017. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020. Luettavissa:
https://www.turvallisuuskomitea.fi/index.php/files/10/lataukset/66/Toimeenpano-ohjelma%202017-2020%20final.pdf Luettu 20.01.2018.

Toikko Timo ja Rantanen Teemu 2009. Tutkimuksellinen kehittämistoiminta. Tampere, Tampereen Yliopisto Oy – Juvenus Print.

Valtioneuvosto 2013. Suomen kyberturvallisuus-strategia. Luettavissa: http://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30 Luettu 24.01.2017

Valtiovarainministeriö 2018. Digitalisaatio. Luettavissa: http://vm.fi/digitalisaatio Luettu 13.06.2017

Vehviläinen Anu 2017. Apua digitaalisiin kansalaistaitoihin. Luettavissa: https://suomidigi.fi/apua-digitaalisiin-kansalaistaitoihin/ Luettu 16.01.2018.

Viestintävirasto 2017. Näin meitä huijataan! Luettavissa: https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Nain_meita_huijataan.pdf Luettu 31.10.2017.

Vuorinen Tero 2014. Strategiakirja 20 työkalua. Helsinki, Talentum Media Oy.

WhatsApp 2018. WhatsAppin turvallisuus. Luettavissa: https://www.whatsapp.com/security/?l=fi Luettu 21.01.2018.

Internetissä tarjotaan kännykkää 2 eurolla, tartutko tarjoukseen?

1. Kyllä, noin halvalla ei saa kännykkää mistään!
2. Klikkaisin tarjousta ja lukisin ehdot ennen ostamista.
3. Miksikäs ei, jos voi hävitä vain 2 euroa?
4. Kuulostaa liian hyvältä ollakseen totta, en ostaisi!

Väärin! Kahden euron kännyköitä ei ole. Kyseessä saattaa olla tilausansa, joka ottaa tietosi ja laskuttaa esimerkiksi luottokorttiasi kuukausittain. Tai kyseessä saattaa olla vain tietojenkalastelua, jolloin tietosi joutuvat vääriin käsiin.

Mitä tarkoitetaan tietojenkalastelulla?

1. Sitä, että selvittää, missä on parhaat kalapaikat.
2. Tietojenkalastelu on poliisin operaatio, jossa satunnaisilta ohikulkijoilta kysellään tietoja rikoksista.
3. Kun joku koittaa harhauttamalla saada toisen paljastamaan esimerkiksi pankkitunnuksensa.
4. Kun kysyt vaikka Googlesta?

Väärin! Tietojenkalastelulla tarkoitetaan toimintaa, jossa yritetään harhauttaa henkilöä paljastamaan henkilökohtaisia tietojaan, kuten pankkitunnuksiaan.

Saat sähköpostin, jossa kerrotaan sinun voittaneen miljoona euroa, sinun täytyy vain antaa henkilökohtaisia tietojasi voiton lunastamiseksi, annatko tiedot?

1. Tottakai, miljoonalla eurolla eläisin leveästi!
2. Klikkaisin linkkiä varmistaakseni, että juttu pitää paikkansa.
3. En, kuulostaa huijaukselta!
4. Kertoisin oikein vain tilinumeroni, jonne rahan voisi siirtää.

Väärin! Kukaan ei lähestyisi sinua miljoonan euron voitosta tuntemattomasta sähköpostista. Mieti myös oletko edes osallistunut tällaiseen arvontaan, todennäköisesti et. Jo linkin klikkaaminen voi vaarantaa tietokoneesi tietoturvan! Poista siis viesti sitä avaamatta.

Sinulla on Tori.fi-palvelussa myytävänä omaisuuttasi. Huonoa englanninkieltä käyttävä ostaja ottaa sinuun yhteyttä ja kertoo olevansa kiinnostunut myytävästäsi. Hän kertoo, että voidakseen ostaa tuotteen sinun tulisi vain maksaa rahtikulut ulkomaille ja tämän jälkeen hän maksaa tuotteen tilillesi, miten toimit?

1. Jatkaisin viestittelyä varmistuakseni siitä, että ostaja varmasti maksaa tuotteen rahdin maksettuani.
2. En jatka yhteydenpitoa ostajaan, kuulostaa huijaukselta!
3. Maksan rahdin ja pyydän tämän jälkeen maksun tuotteesta tililleni.
4. Tarjoan, että maksaisimme rahtikulut puoliksi, jonka jälkeen pyydän maksun tuotteestani.

Väärin! Älä suostu kauppoihin, jossa sinun pitäisi etukäteen maksaa jotain, ilman että voit varmistua ostajan oikeellisuudesta. Ostaja todennäköisesti haluaa vain tuon rahtikulun verran rahojasi ja et kuule hänestä tai rahoistasi enää.

Selailen Huuto.net-palvelua ja löydän sieltä etsimäni tuotteen. Otan yhteyttä myyjään, joka ilmoittaa postittavansa tuotteen minulle, kun maksan ennakkoon puolet sovitusta hinnasta.

1. En suostu maksamaan, pyydän toimitusta postiennakolla.
2. Maksan puolet hinnasta, sehän kuulostaa järkevältä vaihtoehdolta molempien kannalta!
3. Tinkaan etumaksun yhteen neljäsosaan ja maksan sen.
4. Pyydän myyjää lähettämään kuvia tuotteesta varmistuakseni, että se on varmasti olemassa. Kuvat saatuani maksan summan.

Väärin! Älä suostu kauppoihin, jossa sinun pitäisi etukäteen maksaa jotain, ilman että voit varmistua myyjän rehellisyydestä. Vaikka myyjällä olisi kuva tuotteesta ei se tarkoita, että hän on myyntiaikeissa. Kaupat kannattaa sopia aina toteutettavaksi kasvotusten, jos se on mahdollista ja tuote testata ennen kauppojen toteutumista.

Puhelimeni soi, soitto tulee minulle tuntemattomasta numerosta. Soittaja kertoo olevansa Hämeen poliisista ja ilmoittaa, että omistamani pankkitili on hakkeroitu. Estääkseen jatkorikosten syntymisen poliisi pyytää verkkopankkitunnuksiani.

1. Hätäännyn ja annan tunnukset soittajalle pikimmiten.
2. Kysyn ensin, mistä ovat tiedon hakkeroinnista havainneet ja vastauksen saatuani annan tunnukset.
3. Kerron soittajalle etten aio luovuttaa pankkitunnuksiani ja suljen puhelimen.
4. Annan tunnukset ja kysyn, ovatko rahat tililläni vielä tallessa?

Väärin! Älä koskaan anna verkkopankkitunnuksiasi kenellekään. Verkkopankkitunnukset ovat henkilökohtaisia, eikä kenelläkään ole syytä niitä tietää, ei edes poliisin.

Seuraamasi TV -sarja jäi jännään kohtaan, seuraava jakso julkaistaan vasta viikon kuluttua. Joku tuntematon henkilö on kuitenkin jakanut koko sarjan ilmaiseksi internetissä!

1. Huippua, nyt saan katsoa koko sarjan yhdeltä istumalta, lataukseen siis!
2. Lataan vain yhden jakson, jäihän se jännään kohtaan…
3. Hetkinen, kuulostaa epäilyttävältä, maltan mieleni enkä lataa.
4. Lataan sarjan ja jaan sen vielä parhaalle ystävälleni.

Väärin! TV -sarjoja, elokuvia tai vastaavaa audiovisuaalista sisältöä ei lähtökohtaisesti ole internetissä tarjolla ilmaiseksi. Mikäli kaupallisen sarjan lataa laittomasti internetistä kyseessä on tekijänoikeusloukkaus. Jos kyseisen latauksen vielä jakaa eteenpäin on kyseessä myös tekijänoikeusloukkaus. Laittomasti jaossa olevat sisällöt saattavat pitää sisällään myös viruksia.

Löysin matkapuhelimeeni applikaation, jonka avulla saan Spotify -musiikkitoistopalvelun maksullisen sisällön ilmaiseksi.

1. Kyseessä ei voi olla laiton applikaatio, koska se on ladattu monta kertaa ja saanut satoja hyviä arvosteluja, lataan applikaation.
2. Ostan kaikki kuuntelemani musiikin myös CD -levyinä, olen siis kertaalleen maksanut sisällöstä ja voin ladata tämän applikaation huoletta.
3. Tarvitsen musiikkia vain yhdeksi illaksi, sen jälkeen poistan applikaation, se on varmasti ok!
4. Tuolla varmaan säästäisi, mutta en halua tuntemattomasta lähteestä olevia ohjelmistoja matkapuhelimeeni, en lataa.

Väärin! Kyseessä on laittomasti tehty modifikaatio, jonka lataamalla loukkaat musiikin tekijöiden tekijänoikeuksia.

Huuto.netissä on myynnissä lähes käyttämätön 400 euroa maksava matkapuhelin 150 eurolla.

1. Hieno tilaisuus saada itselleni edullisesti hyvä matkapuhelin, teenpä heti ostotarjouksen!
2. Teen ostotarjouksen, mutta suostun maksamaan vasta, kun näen kuvan puhelimesta.
3. Teen ostotarjouksen, mutta maksan vasta, kun saan puhelimen käteeni.
4. Kuulostaa liian hyvältä ollakseen totta, en osta.

Tarjous, joka kuulostaa liian hyvältä ollakseen totta, ei yleensä ole totta. Vaikka saat matkapuhelimesta kuvan, voi henkilö myydä samaa matkapuhelinta useille henkilöille kenellekään sitä kuitenkaan oikeasti myymättä. Pelkkä matkapuhelimen näkeminenkään ei tee kaupasta totta, puhelin saattaa olla toimimaton.

Löysit internetistä halvalla auton renkaat, olet tekemässä maksua luottokortilla ja vilkaiset osoiteriviä, jossa lukee http://www.tästähalvatrenkaat.net, miten jatkat?

1. Ostan renkaat, koska joku oli internetissä kehunut sivustoa toimivaksi.
2. Lopetan välittömästi luottokorttitietojeni syöttämisen, koska http:// tarkoittaa, ettei sivusto ole suojattu.
3. Otan riskin, on sen verran edulliset renkaat ja tuttu rengasmerkki!
4. Internet on pullollaan edullisia renkaita, miksi tämä poikkeaisi muista? Ostan renkaat.

Väärin! Varmistu aina, ettei luottokorttitietosi mene vääriin käsiin. Tähän saa varmistusta, kun selvittää, että kauppa josta olet ostamassa, on rekisteröity, sivustolta löytyy luottokorttiyhtiön logot, sivuston osoiterivin alussa lukee https:// joka tarkoittaa, että salaus on päällä.

Olet ostanut uuden jääkaapin, joka tietää älyominaisuuksiensa ansiosta onko jääkaapissasi puutteita ruoan suhteen ja saa yhteyden internettiin, vau! Mitä sinun tulee ottaa kuitenkin huomioon jääkaappia asentaessasi?

1. Tosi siistiä, vedän töpselin seinään ja liitän koneen langattomaan verkkoon, avot!
2. No huhuh, tiedän kyllä jääkaappini sisällön ilman, että jääkaappini siitä minulle kertoo. En liitä konetta verkkoon.
3. Jes, nyt kauppareissut sujuvat mutkitta, kun voin soittaa jääkaapilleni. Täytyy kyllä ensin vaihtaa oletus käyttäjätunnukset ja salasanat, ennen verkkoon liittämistä.
4. Jääkaappi vaan langattomaan verkkoon, jos joku haluaa kyberanastaa ostoslistani niin antaa palaa!

Väärin! Mikäli oletus käyttäjätunnusta ja salasanaa ei vaihda, on jääkaappiasi helppo käyttää esimerkiksi palvelunestohyökkäyksissä apuna tietämättäsi. Edesautat siis kyberrikollisuutta vahingossa!

Voi surku! Surffailit jännillä sivuilla ja koneesi ruutuun hyppäsi virusvaroitus! Mutta kylläpäs lykästi, kun samassa huomautuksessa on viruksen poistava ohjelma ladattavissa!

1. Stop, Seis, Stannar! Kyseessä on haittaohjelma, joka yrittää saada sinua valheellisella tarinalla lataamaan itsensä koneelle, älä vain lataa!
2. No kylläpä lykästi tosiaan, siitä vain ohjelma koneelle ja virukset pois!
3. Omat virusturvani on niin hyviä, että vaikka lataisin tuon ohjelman ei se voisi vahingoittaa konettani.
4. Ei hitto, parasta polttaa koko kone varmuuden vuoksi.

Väärin! Haittaohjelmat pyrkivät pelottelemaan käyttäjää erilaisin tavoin, jotta käyttäjä lataisi haittaohjelman koneelleen, älä putoa tähän ansaan äläkä siis asenna moisia ”virusturvia”. Mikään virusturva ei ole jatkuvasti 100 % ajan tasalla uusista viruksista, älä siis sokeasti luota aina virusturvaasi vaan käytä myös maalaisjärkeä. Äläkä nyt kuitenkaan polta sitä konettasi…

Selailit seuranhakusovellusta ja löysit sielunkumppanisi, joka on täys 10. Olette keskustelleet jo jonkin aikaa ja nyt hän haluaa sinusta kuvan vähissä vaatteissa.

1. Olen tutustunut jo hyvin sielunkumppaniini, voin huoletta lähettää kuvan.
2. Pyydän ensin häneltä vastaavan kuvan ja suostun sitten lähettämään oman kuvani.
3. En lähde tähän mukaan, en ole tavannut henkilöä kasvotusten ja internetissä kuka vain voi esiintyä kenenä tahansa.
4. Lähettäisin kuvan, mutta sellaisen jossa ei ole kasvojani.

Väärin! Netissä kuka vain voi esiintyä kenenä tahansa, pahimmassa tapauksessa henkilö saattaa kiristää sinua uhkaamalla julkaista kuvasi internetissä.

Tekstiviesti: ”Lähettäjä S-market, Hei Sinulla on (1) paketti odottamassa. Katso se täältä >>> lataa esikatselu napauttamalla”.

1. Mikäli pakettiautomaattiin tulisi paketin noutokoodi samassa viestissä, epäilyttävää että pitäisi klikkailla erikseen. En avaa!
2. Viestin lähettäjä on S-Market, jossa on postipakettien noutopiste ja satun odottamaan pakettia, katson siis pakettini tiedot napauttamalla.
3. Kyseessä on tekstiviesti, tekstiviestit eivät sisällä vaarallisia liitteitä, voin huoletta klikata.
4. Otan mobiilidatan pois päältä ennen kuin klikkaan, en voi saada viruksia jos mobiilidata ei liiku!

Väärin, tekstiviestitse tulevat paketteja koskevat viesti sisältävät itsessään tarvittavat tiedot paketin noutamiseen. Älä klikkaile epäilyttävissä tekstiviesteissä olevia linkkejä missään tilanteessa. Linkin takaa saattaa latautua haittaohjelma matkapuhelimeesi.

Junassa joku on peittänyt kannettavansa kameran tarralla, mistähän tämä johtuu?

1. Kameraohjelman avatessa on kurja katsella omaa naamaansa, siksi ihmiset peittävät kameran tarralla.
2. Kameran tarralapulla peittämällä voi estää kameraohjelmaa hyväksikäyttävien haittaohjelmien vakoilun.
3. Kamera sattuu olemaan siinä kohdassa mihin ihmiset tykkäävät liimailla tarroja.
4. Henkilö haluaa näyttää muille ettei kuvaa heitä, eikä voi saada syytteitä salakuvaamisesta.

Väärin! Kameran peittämällä voi varmistua, ettei haittaohjelmat voi käyttää tietokoneen kameran kuvaa hyväkseen.

Tor -verkon käyttäminen on laitonta.

1. Ei pidä paikkaansa, Tor -verkko ei ole itsessään laiton.
2. Oikein, Tor -verkkoa käytetään rikolliseen toimintaan ja sen käyttäminen näin on laitonta.
3. Jo Tor -verkon mahdollistaman sovelluksen koneelle lataaminen on laitonta.
4. TOR = Tämä On Rikollista, sanoohan sen jo nimikin!

Väärin! Tor (The Onion Router) -verkon käyttäminen ei ole laitonta, vaikka siihen liittyy myös paljon rikollista toimintaa, koska se mahdollistaa verkon käyttämisen anonyymisti.

Virtuaalivaluutta on laitonta valuuttaa.

1. Virtuaalivaluutta ei ole minkään lainsäädännön mukaista valuuttaa, joten se on laitonta.
2. Virtuaalivaluutta ei lueta lailliseksi valuutaksi, muttei se ole laitontakaan.
3. Virtuaalivaluutta on laillista Kiinassa ja useissa muissa Aasian maissa, ei kuitenkaan Suomessa.
4. Virtuaalivaluutta on laillista, jos sitä ei muuta euroiksi.

Väärin! Virtuaalivaluutta ei ole laitonta. Myös erinäisissä tietokonepeliympäristöissä käytetään ns. virtuaalivaluuttaa pelissä tehtävien ostosten tekemiseksi. Jotkut kaupatkin jo hyväksyvät virtuaalivaluutat maksutapana.

15 -vuotiasta Siniä on lähestynyt aikuinen mies internetissä. Mies on pyytänyt Siniltä vähäpukeisia kuvia. Sini ei tähän suostu ja kertoo asiasta vanhemmilleen. Mikä on oikea toimintatapa?

1. Vanhemmat saavat Siniltä miehen puhelinnumeron ja soittavat miehelle kertoen, että on laitimmainen kerta, kun tällaista tekee. Vanhemmat kertovat tekevänsä asiasta ilmoituksen poliisille.
2. Vanhemmat toruvat Siniä, kun tämä on tuollaisten miesten kanssa tekemisissä internetissä. Pitäisihän Sinin tietää paremmin!
3. Vanhemmat selvittävät Siniltä saadun miehen puhelinnumeron perusteella miehen osoitteen ja menevät paikanpäälle selvittämään asian.
4. Vanhemmat eivät ota mieheen yhteyttä vaan kertovat tiedot poliisille.

Väärin! Vaikka tunteet ovat varmasti pinnassa, ei tällaiseen henkilöön tulisi olla itse yhteyksissä, eikä varsinkaan käydä itse tällaista henkilöä tapaamassa. Henkilö saattaa kadota, mikäli pelkää kiinni jäämistä. Asiasta tulisi tehdä heti ilmoitus poliisille ja antaa poliisien hoitaa tilanne.

Saat yhtäkkiä ilman syytä todella hyvän näköiseltä vastakkaista sukupuolta edustavalta henkilöltä kaveripyynnön Facebookissa. Henkilöllä on erikoinen nimi etkä tunne häntä.

1. Olenhan itsekin aika vetävän näköinen, en siis ylläty, että hänkin on minusta kiinnostunut. Hyväksyn pyynnön ja kysyn mikä on meininki!
2. Erittäin vetävän näköinen henkilö, jota en tunne lähestyy minua yhtäkkiä ilman syytä. Haiskahtaa epätodelliselta. Poistan pyynnön.
3. No, no, täytyyhän tämä naru kokeilla, hyväksyn pyynnön, mutta olen varuillani.
4. Jätän pyynnön vähäksi aikaa odottamaan, hyväksyn sen sitten myöhemmin, etten vaikuta liian innokkaalta.

Väärin! Näin toimii niin kutsutut botit Facebookissa. Jos hyväksyt kaveripyynnön alkaa botti lähettämään sinulle viestejä ja linkkejä jotka sisältävät haittaohjelmia tai ohjaavat sinut vastaamaan kyselyihin joista botin tekijät saavat rahaa.

Päivitetyn virustorjuntaohjelman avulla voit huoletta surffata internetissä. Mikään virus ei voi päästä koneellesi, koska virustorjuntaohjelmasi on ajantasalla.

1. Ei pidä paikkaansa. Käyttäjän on itse oltava myös huolellinen internetissä.
2. Juuri näin, maksan virustorjunnastani paljon, se pitää internetin haitat loitolla.
3. Pidän virustorjuntaohjelmani ajan tasalla ja tarkistan aika ajoin koneeni viruksien varalta. Voin näillä menetelmillä huoletta selata internetistä mitä vain.
4. Minulla on kaksi virustorjuntaohjelmaa, mikään ei läpäise tuplavarmistusta!

   Väärin! Mikään virustorjuntaohjelma ei pysy niin aallonharjalla virusten kehitysmuodoista, että se tarjoaisi 100% suojan tietokoneellesi. Käyttäjän on oltava itse huolellinen internettiä käyttäessään.

Palvelunestohyökkäyksellä tarkoitetaan?

1. Kun esimerkiksi tietylle sivustolle kohdennetaan tuhansittain kirjautumisyrityksiä tai muuta toimintaa jolloin informaatiotulvan vuoksi sivusto lakkaa toimimasta.
2. Sitä, kun mennään kioskin ovelle, eikä päästetä ihmisiä sisään.
3. Kun lähetetään huijausviestejä tuntemattomille ihmisille ja koitetaan saada heitä paljastamaan pankkitunnukset.
4. Annetaan sivustoille huonoa palautetta, niin ettei ihmiset enää luota siihen sivustoon.

   Väärin! Palvelunestohyökkäyksellä tarkoitetaan tilannetta, jossa kohdennetaan valtava määrä informaatiota, esimerkiksi kirjautumisyrityksiä tietylle sivustolle, jolloin informaatiotulvan vuoksi sivusto lakkaa toimimasta.

Minkälainen käyttäjätunnus ja salasana ovat parhaat?

1. Sellaiset jotka muistaa helpoiten, esimerkiksi oma nimi ja syntymävuosi käyttäjätunnukseksi ja salasanaksi vaikka 12345.
2. Käyttää kahta erilaista satunnaista numero, kirjain ja merkkisarjaa salasanana ja vaihtelee niitä kahden eri käyttäjätunnuksen kanssa.
3. Jokaiseen paikkaan erilainen salasana ja käyttäjätunnuspari. Salasana sisältää kirjaimia isoina ja pieninä, numeroita ja merkkejä ja on ainakin 8 merkkiä pitkiä.
4. Käytää samaa naapurin kanssa, jos ei itse muista niin naapuri voi muistaa!

   Väärin! Jokaiseen paikkaan tulisi käyttää erilaista salasana ja käyttäjätunnusparia. Salasanan tulisi koostua isoista ja pienistä kirjaimista, numeroista ja merkeistä ja sen tulisi olla ainakin 8 merkkiä pitkä. Vaikka salasanasi olisi kuinka hyvä voi se joutua vääriin käsiin ja tällöin kaikki palvelut mitä käytät samalla salasanalla ja käyttäjätunnuksella ovat muiden käytettävissä.

Luottokortin turvallista käyttämistä internetostoksissa voi lisätä.

1. Pitämällä luottokortin aina kotona, niin siihen ei kukaan pääse käsiksi.
2. Säilyttämällä luottokorttia aina suojakotelossa, jolloin siitä on vaikeampi havaita numeroita.
3. Kytkemällä luottokortin asetukset verkkopankissa niin, ettei sitä voi käyttää ulkomailla ja nettiostoksissa vain, kun kytken kyseisen ominaisuuden erikseen päälle.
4. Kirjoittamalla luottokortin tiedot johonkin ylös ja viilaamalla numerot kortista pois.

Väärin! Luottokortin tiedot voivat joutua vääriin käsiin jos ne vahingossa vaikka vain kirjoittaa johonkin internetsivulle joka ei ole turvallinen. Verkkopankissa kannattaa kytkeä luottokortin ominaisuudet niin, ettei luottokortti toimi kuin esimerkiksi Suomessa ja asettaa internetkäytön ominaisuus kortissa päälle vain, kun sitä käyttää internetissä itse. Aina tulee myös olla varma verkkosivun oikeellisuudesta, johon luottokortin tiedot syöttää.

Olet kirjautumassa verkkopankkiin ja näytölle avautuu ikkuna, jossa kysytään turvaluvun tarkistamista. Mitä teet?

1. Tilanne poikkeaa normaalista verkkoasioimisesta, en anna enempää tietoja ja soitan pankkiin ilmoittaakseni tapahtuneesta.
2. Pankki voi satunnaisesti tehdä niin sanotun tuplavarmistuksen, jolloin joudun antamaan turvaluvun kahteen kertaan. Annan siis turvaluvun.
3. Outoa, ei pankin sivustot yleensä kysy erillisellä ikkunalla mitään. Jätän homman tähän ja yritän myöhemmin uudelleen.
4. Kyseessä on varmasti huijausyritys haittaohjelman avulla. Annan väärän turvaluvun hämätäkseni haittaohjelmaa, jonka avulla voin jatkaa asiointia pankissa normaalisti.

Väärin! Tällaiset tuplavarmistukset eivät ole oikeita. Lopeta tietojen syöttö välittömästi ja ole yhteydessä pankkiisi, jotta pankki voi ryhtyä tarvittaviin toimiin mahdollisimman nopeasti.

Huomaat internetissä väärennetyn verkkosivun, jolla yritetään kalastella henkilökohtaisia tietojasi, onneksi et ole ehtinyt mitään tietoja vielä syöttämään. Miten toimit?

1. Otan verkkosivun tiedot ylös ja lähetän tiedot Viestintäviraston kyberturvallisuuskeskukseen ja näin ennalta ehkäisen muiden joutumista kyseisen sivuston uhriksi.
2. Huokaisen helpotuksesta, etten ehtinyt syöttää tietojani ja jatkan internetin selailua.
3. Kirjoitan sivustolle herjaviestin ja toivon, että sivuston pitäjät häpeissään vetäytyisivät internetistä.
4. Selvitän hakkeroinnin salat, värvään itselleni bottiarmeijan ja suoritan palvelunestohyökkäyksen kyseiselle sivustolle, jolloin sivusto kaatuu ja olen estänyt rikoksen syntymisen!

Väärin! Ilmoitus Viestintäviraston kyberturvallisuuskeskukselle tai poliisille on hyvä liike havaitessasi huijaussivuston internetissä. Tällöin viranomaiset voivat päästä estämään sivuston harhauttavan toiminnan.

Kyberrikollisuus ihmisen arjessa SWOT -analyysi

	+ VAHVUUDET	- HEIKKOUDET
NYKYTILA	-Ajankohtainen aihe -Asiantuntijaverkosto -Mielenkiinto aiheeseen sekä into saada aikaiseksi työ, jolla voisi olla oikeasti merkitystä kyberrikollisuuden ennalta estämisessä tavallisten ihmisten keskuudessa -Työ toteutuessaan palvelee poliisin EET toimintaa -Kaksi tekijää	-Tietotekninen tietämättömyys -Toiminnallinen opinnäytetyö uutta molemmille tekijöille -Molemmille tekijöille melko uusi aihealue -Vaikea saada tarkkaa tilastotietoa aiheesta poliisin tietojärjestelmistä -Oikean asiantuntijaverkoston saaminen -Materiaalin hankkiminen (helposti vanhentunutta, kielelliset haasteet kun suuri osa materiaalista englanninkielistä)

	MAHDOLLISUUDET	UHAT
TULEVAISUUS	-Ajankohtainen aihe -Ihmisten mielenkiinto -Itsensä kehittäminen -Ennalta estävä toiminta (vähemmän nettipetoksen uhreja tulevaisuudessa) -Tilaston tekeminen testin pohjalta -Työn jatkojalostaminen	-Aikataulu -”Puhkikulunut” aihe? - Tietotekninen toteutus -Työaikojen sovittelu -Testin epäonnistuminen -Vanhentunut aineisto -Nettirikosten jatkuva muuntuminen -Tavoittaako testi toivottua kohdeyleisöä

LIITE 3

Haastattelun runkokysymyksiä:

Haastattelu Keskusrikospoliisissa

Rikosylikomisario Muurman Tero ja Rikoskomisario Siurola Sami

1. Miten kyberrikokset ovat mielestäsi kehittyneet viimeisten vuosien aikana?

2. Mitkä ovat tämän hetken trendit kyberrikollisuudessa?

3. Seuraako trendit jotain tiettyä kehitystä?

4. Pysyykö poliisi kuinka hyvin perässä kyberrikollisuuden ilmiöissä?

5. Mitä haasteita kyberrikollisuuden tutkinnassa on nykyään? (Järjestelmät, koulutus jne)

6. Miten näitä haasteita on suunniteltu käsiteltävän tulevaisuudessa?

7. Minkälainen innovointi voisi edistää poliisin kyberrikollisuuden tutkintaa?

8. Kyberrikollisuuden vaaroista on pyritty valistamaan ihmisiä, mistä luulet johtuvan, että uhrimäärä kyberrikoksissa on edelleen melko suuri, vai onko se?

9. Ketkä ovat yleisimmin kyberrikosten uhreina?

10. Minkälaisilla menetelmillä voisi kyberrikollisuuden uhriksi joutumista mielestäsi vähentää?

11. Eroaako oikeusturva kyberrikoksessa ja ns. katurikoksessa? (lainsäädäntö? haasteet saada oikeutta)

12. Suomi on ollut teknologiakehitykseltään tunnettu maa, mutta kyberrikollisuuden tutkinnassa ja selvittelyssä olemme vielä varsin alkutekijöissä, mistä tämä johtuu?

LIITE 3

Haastattelu Viestintävirastossa

Erityisasiantuntija Kurittu Antti

1. Minkälaisia tietoturvauhkia on tällä hetkellä olemassa tavallisen ihmisen näkökulmasta? Viestintäviraston sivuilla olevat top5-tietoturvauhat suunnattu selkeästi lähinnä yrityksille. Sivuilla kerrottiinkin, että yksityishenkilöä koskevat uhat tullaan luettelemaan myöhemmin, mitä ne ovat ja miten niitä voisi estää?

2. Minkälaista kehitys on ollut viimeisten vuosien aikana? Miten uhat ovat muuttuneet?

3. Miten kyberrikollisuus näkyy viestintäviraston toiminnassa?

4. Mistä tieto erilaisista tietoturvauhista tulee viestintävirastolle?

5. Minkälaisilla menetelmillä kyberrikollisuutta pyritään viestintäviraston toimesta ennalta ehkäisemään?

6. Paljosta uutisoinnista ja valistuksesta huolimatta ihmisiä joutuu edelleen verkkorikosten uhreiksi, mistä näet tämän johtuvan, miten verkkorikosten uhriksi joutumista voisi mielestäsi ehkäistä?

7. Kuinka paljon viestintävirasto tekee yhteistyötä poliisin kanssa?

8. Osaatko sanoa miten tietorikosten uhrit jakautuvat kun vertaillaan tavallisia ihmisiä ja yrityksiä?

9. Millä tasolla näet Suomen valmiuksien olevan verkkorikollisuutta torjuntaan?

LIITE 4

Päivämäärä	Toiminto		Osallistuu	Lopputulos
05.09.2017	Opinnäytetyöseminaari 1		Aki Somerkallio Mari Takkinen	To Do Lista
05.09.2017	Toiminnallinen opinnäytetyö -kurssi		Aki Somerkallio	Toiminnallisen opinnäytetyön teoriaosuus opinnäytetyöhön
04.01.2018	KRP, Asiantuntijahaastattelu rikosylikomisario Tero Muurman		Aki Somerkallio Mari Takkinen	Haastatteluosio opinnäytetyöhön
04.01.2018	KRP, Asiantuntijahaastattelu komisario Sami Siurola		Aki Somerkallio Mari Takkinen	Haastatteluosio opinnäytetyöhön
16.01.2018	Opinnäytetyö 70% valmiudessa ohjaajalle ja opponoijille		Aki Somerkallio Mari Takkinen	Valmistautuminen toiseen seminaariin
18.01.2018	Seminaari 2		Aki Somerkallio Mari Takkinen	To Do Lista
18.01.2018	Viestintävirasto, asiantuntijahaastattelu, eritysiasiantuntija Antti Kurittu		Aki Somerkallio Mari Takkinen	Haastatteluosio opinnäytetyöhön
06.02.2018	Opinnäytetyö 99% valmiudessa ohjaajalle ja opponoijille		Aki Somerkallio Mari Takkinen	Valmistautuminen viimeiseen seminaariin
13.02.2018	Seminaari 3		Aki Somerkallio Mari Takkinen	Työ 99% valmis