Markus Sippo

KOTIKÄYTTÄJÄN TIETOTURVAKÄYTTÄYTYMINEN JA TIETOTURVATIETOISUUS

JYVÄSKYLÄN YLIOPISTO
2017

TIIVISTELMÄ

Sippo, Markus
Kotikäyttäjän tietoturvakäyttäytyminen ja tietoturvatietoisuus
Jyväskylä: Jyväskylän yliopisto, 2017, 32 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Moilanen, Panu

Tämän tutkielman tarkoitus on selvittää, millainen on kotikäyttäjä, mitä tarkoittaa kotikäyttäjän tietoturvakäyttäytyminen ja mistä tekijöistä se koostuu. Lisäksi tutkimuksessa tarkastellaan kotikäyttäjän tietoturvatietoisuutta, sen rakentumista ja sen vaikutuksia tietoturvakäyttäytymiseen. Tutkimuksen tuloksena löydettiin useita eri tekijöitä, jotka vaikuttavat tietoturvakäyttäytymiseen ja tietoturvatietoisuuteen. Myös yhteys tietoturvatietoisuuden ja tietoturvakäyttäytymisen välillä löydettiin. Löydösten pohjalta muodostettiin uudenlainen malli kotikäyttäjän tietoturvakäyttäytymisen muodostumisesta. Tutkimus on toteutettu kirjallisuuskatsauksena, jonka lähteinä on käytetty tieteellisiä julkaisuja ja tutkimuksia, jotka on julkaistu erilaisissa akateemisissa julkaisuissa.

Asiasanat: tietoturva, kotikäyttäjä, tietoturvakäyttäytyminen, tietoturvatietoisuus

ABSTRACT

Sippo, Markus
Home user's information security behavior and information security awareness
Jyväskylä: University of Jyväskylä, 2017, 32 p.
Information system science, bachelors degree
Supervisor(s): Moilanen, Panu

The purpose of this study is to find out, what is a home user, what home user's information security behavior is and from what factors it consists of. Additionally, the second purpose of this study is to describe home user's information security awareness, from what factors it consists of and how it affects information security behavior. Based on the findings of this study, many different factors, that affects information security behavior and information security awareness, were found. The connection between information security awareness and information security behavior was also found. Based on the findings of this study, a new model was created to describe the formation of home user's information security behavior. This study is a literature review. The sources used in this study are mostly scientific articles and studies published in different academic journals.

Keywords: information security, home user, information security behavior, information security awareness

KUVIOT

SISÄLLYS

1 JOHDANTO

Tässä johdantoluvussa pyritään kuvaamaan tutkielman aihepiiri mahdollisimman tarkasti sekä tutkielman aiheen merkitys kotikäyttäjälle. Tässä luvussa esitellään myös tutkimuskysymykset, tutkielman yleiset tavoitteet sekä tutkielman rakenne. Lopuksi käsitellään vielä tutkimuksen toteutusta sekä tiedonhakua. Kuvaan myös kehitystä, joka on johtanut nykyiseen tilanteeseen, ja minkä takia tutkimus tästä aihealueesta on erityisen tärkeää.

Internetin rooli yhteiskunnassamme ja suomalaisten jokapäiväisessä elämässä on saavuttanut lähtemättömän aseman. Alle 55-vuotiaista suomalaisista noin 90 prosenttia käyttää internetiä päivittäin. Nuoremmista, alle 24-vuotiaista suomalaisista, internetiä käyttää päivittäin lähes jokainen (SVT, 2016.)

Tietoturva ei ole kuitenkaan pysynyt mukana internetin nopeassa kehityksessä, etenkään kotikäyttäjien osalta. Kotikäyttäjiin internetissä tyypillisesti kohdistuvat uhat, kuten tietojenkalastelusähköpostit ja haittaohjelmat, lisääntyivät merkittävästi vuonna 2016. Erityisen huolestuttavaa on haittaohjelmien määrän nousu mobiililaitteilla. Vuonna 2016 uudenlaisia variaatioita haittaohjelmista löydettiin 77 prosenttia enemmän kuin vuotta aikaisemmin (Symantec, 2016.)

Kotikäyttäjien ongelmat tulevat korostumaan jatkossa nykyistä enemmän, ellei muutosta nykyisessä tilanteessa tapahdu. Kotikäyttäjien tietoturvaa pitäisi parantaa tietoisesti lisäämällä koulutusta tietoturvasta ja sen merkityksestä yksilön turvallisuuteen. Useimmiten kotikäyttäjien suurin ongelma tietoturvan suhteen on tiedon puute (Kritzinger & von Solms, 2010).

Tietoturvakäyttäytymistä on tutkittu laajasti yrityskontekstissa, mutta kotikäyttäjien tutkiminen ei ole saanut osakseen yhtä paljon huomiota. Tutkimuksen puute aiheesta on huolestuttavaa, sillä on todettu, että kotikäyttäjät ovat suurin yksittäinen kohderyhmä verkkorikollisille.

Tulevaisuudessa voidaan olettaa, että riskien määrä tulee nousemaan entisestään sekä uudenlaisia haittaohjelmia ja entistä parempia tietojenkalasteluhuijauksia tullaan kehittämään. Lisäksi verkkoon kytkettyjen laitteiden määrä kasvaa jatkuvasti. Tästä syystä on erityisen tärkeää, että kotikäyttäjän tietoturvaa

tutkitaan laajasti, jotta kotikäyttäjän tietoturvakäyttäytymistä voidaan tulevaisuudessa myös parantaa.

1.1 Tutkimuskysymykset ja tavoitteet

Tutkielmassani pyrin vastaamaan seuraaviin tutkimuskysymyksiin:

- Millainen on kotikäyttäjä?
- Mitä on tietoturvakäyttäytyminen ja mitkä tekijät siihen vaikuttavat?
- Mitä on tietoturvatietoisuus ja mitkä tekijät siihen vaikuttavat?
- Miten tietoturvatietoisuus vaikuttaa kotikäyttäjän tietoturvakäyttäytymiseen?

Tutkielmassani pyrin myös antamaan konkreettisia esimerkkejä kotikäyttäjään kohdistuvista uhista internetissä. Yleisimpien riskien esittely on tarpeellista, jotta voimme ymmärtää kotikäyttäjän tietoturvakäyttäytymistä paremmin. Avaan lukijalle myös tietoturvan käsitteen ja pyrin kertomaan, miten ja miksi yksilön käyttäytyminen kotona eroaa yksilön käyttäytymisestä organisaatiossa.

Tutkielmani tavoitteena on antaa lukijalle kokonainen tietokatsaus kotikäyttäjän tietoturvakäyttäytymisestä, tietoturvatietoisuudesta ja mistä tekijöistä kyseiset käsitteet kotikäyttäjän osalta muodostuvat. Tämän tutkielman perusteella voidaan tulevaisuudessa saavuttaa laajempi ymmärrys tietoturvan muodostumisesta ja myös kehittää yksilön tietoturvakäyttäytymistä parempaan suuntaan.

1.2 Tutkielman rakenne

Tutkielma jakaantuu kuuteen eri osaan. Johdantoon, kolmeen eri asialukuun, yhteenvetoon sekä lähdetietoihin.

Ensimmäisessä asialuvussa käsitellään ja määritetään mitä kotikäyttäjällä ja tietoturvalla tarkoitetaan tässä tutkimuksessa. Luvussa myös pohditaan tietoturvan eroja kotikäyttäjän sekä yrityksen työntekijän välillä. Luvussa tarkastellaan myös kotikäyttäjään kohdistuvia yleisimpiä tietoturvauhkia ja pohditaan syitä niihin.

Toisessa asialuvussa tutkitaan kotikäyttäjän tietoturvakäyttäytymistä. Luvussa pyritään vastaamaan tutkimuskysymyksiin; mitä tietoturvakäyttäytyminen on ja mitkä tekijät siihen vaikuttavat. Luvussa myös eritellään kotikäyttäjälle tyypillistä käyttäytymistä.

Kolmannessa ja viimeisessä asialuvussa tutkitaan kotikäyttäjän tietoturvatietoisuutta. Luvussa pyritään vastaamaan tutkimuskysymyksiin; mitä tietotur-

vatietoisuus on, mitkä tekijät siihen kotikäyttäjillä vaikuttavat ja mikä on tietoturvatietoisuuden ja tietoturvakäyttäytymisen välinen suhde.

Tutkielmani viimeinen luku on yhteenveto, jossa eritellään tutkimuksessa saadut keskeiset tulokset, mahdolliset rajoitteet sekä pohditaan aiheen jatkotutkimusmahdollisuuksia.

1.3 Tutkimuksen toteutus ja tiedonhaku

Tämä tutkimus on toteutettu kirjallisuuskatsauksena. Allekirjoittanut on tutustunut aiheeseen liittyvään lähdemateriaaliin ja pyrkinyt valitsemaan tutkimuskysymysten pohjalta sopivia lähteitä.

Tiedonhaku on toteutettu etsimällä, erilaisia hakukoneita hyödyntäen, aiheeseen liittyvää tieteellistä tutkimusta. Käytettyjä hakusanoja ovat esimerkiksi: information security awareness, information security, home user ja information security behavior. Myös näiden sanojen erilaisia yhdistelmiä on käytetty. Lähteitä on haettu pääosin englannin kielisillä termeillä. Lisäksi muutamia lähteitä on löydetty erilaisten tietokantojen suositusominaisuuksien perusteella, jotka ehdottavat käyttäjälle muita saman aihealueen tutkimuksia. Lähteitä on etsitty myös muiden tutkimusten lähdeluettelojen perusteella. Tiedonhaussa on käytetty pääosin Google Scholar -palvelua, mutta myös muita hakukoneita sekä tietokantoja on pyritty hyödyntämään.

Tutkimuksen lähdemateriaalina on pääosin käytetty artikkeleita ja tutkimuksia, jotka on julkaistu tieteellisissä julkaisuissa. Julkaisujen taso on varmistettu Julkaisufoorumi -sivustoa käyttäen. Tässä tutkimuksessa on käytetty pääosin tason 1 tai korkeamman luokituksen omaavia julkaisuja. Tutkielman lähdemateriaaliksi on pyritty valitsemaan mahdollisimman paljon viimevuosina julkaistuja tutkimuksia, jotta mahdollisesti vanhenneelta tiedolta vältytään. Lisäksi lähteiden laatu on varmistettu arvioimalla lähteen tunnettuutta, kirjoittajaa sekä viittausten määrää.

2 KOTIKÄYTTÄJÄN TIETOTURVA

Tässä luvussa on tarkoitus määritellä tutkimukseni kannalta keskeiset käsitteet, kuten tietoturva ja kotikäyttäjä. Tutkimukseni erittelee myös kotikäyttäjälle tyypillisimpiä tietoturvariskejä sekä tuo esille eroja kotikäyttäjän ja yrityksen työntekijän välillä.

2.1 Tietoturva käsitteenä

Tietoturva on käsite, josta on puhuttu jo pitkään, niin organisaatioissa kuin kotioloissakin. Kuitenkin tietoturvan käsite on vaikeasti määriteltävä. Tässä luvussa tutkimukseni tarjoaa lukijalle erilaisia määritelmiä tietoturvalle, joiden perusteella voimme ymmärtää, mitä tietoturva oikeastaan on ja mitä tietoturvalla tarkoitetaan.

Tietoturvasta puhuttaessa on tärkeää huomioida, että tietokoneiden ja tietoverkkojen käyttö on muuttunut valtavasti viime vuosikymmeninä. Samalla myös suojauskeinot, joilla tietokoneita ja laitteita pyritään suojaamaan, ovat muuttuneet. Tietoturva ei tarkoita enää pelkästään teknisiä ratkaisuja, vaan se on laajentunut tarkoittamaan koko tiedonsuojauksen prosessia ja sen kaikkia osatekijöitä (von Solms & van Niekerk, 2013.) Eikä tietoturvaa voi saavuttaa pelkästään teknisillä ratkaisuilla (Herath & Rao, 2009).

Whitman ja Mattord (2011) määrittelevät tietoturvan tarkoittavan tiedon ja sen kriittisten elementtien suojaamista. Kriittisiä elementtejä ovat järjestelmät ja laitteet, jotka käyttävät, varastoivat ja lähettävät tietoa (Whitman & Mattord, 2011).

Whitman ja Mattord (2011) myös selittävät tietoturvaa C.I.A -mallilla. Se selittää tiedolle tyypillisiä ominaisuuksia, joita ihmisten ja organisaatioiden tulisi suojella omassa toiminnassaan. C.I.A -malli tyypillisesti koostuu tiedon luottamuksellisuudesta (confidentiality), eheydestä (integrity) ja saatavuudesta (avaibility). Tämän mallin mukaan tietoturva toteutuu, kun kaikki edellä mainitut kriteerit ovat kunnossa ja otettu huomioon.

Tiedon luottamuksellisuus tarkoittaa, että tietoon ei ole pääsyä muilla kuin valtuutetuilla ihmisillä ja järjestelmillä (Whitman & Mattord, 2011). Tiedon eheys tarkoittaa, että tieto on ehjä ja virheetön kokonaisuus (Whitman & Mattord, 2011). Eheyttä uhkaavat esimerkiksi tiedostojen korruptoituminen ja tietyn tyyppiset virukset. Tiedon saatavuus puolestaan tarkoittaa, että valtuutetut käyttäjät saavat tiedon käyttöönsä ilman ongelmia ja halutussa tiedostoformaatissa (Whitman & Mattord, 2011).

Perinteistä C.I.A -mallia on kuitenkin kritisoitu sen kyvyttömyydestä selittää nykypäivän nopeasti muuttuvia ympäristöjä. Whitman ja Mattord (2011) jatkavat, että C.I.A -malli ei pysty selittämään nykypäivän ilmiöitä, kuten tiedon vahingoittamista, tuhoamista, varastamista tai tiedon sisällön muuttamista.

Ratkaisuna edellä mainittuun ongelmaan he ehdottavat malliin lisättäväksi uusia tiedon ominaisuuksia, joita on tietoturvan toteutumisen kannalta otettava huomioon ja suojeltava. Uusia ominaisuuksia olisivat: tiedon tarkkuus (accuracy), aitous (authenticity), käyttökelpoisuus (utility) ja omistus (possession) (Whitman & Mattord, 2011.)

Tiedon tarkkuudella tarkoitetaan, että tieto on sisällöltään virheetöntä ja se vastaa käyttäjän odotuksia (Whitman & Mattord, 2011). Tiedon aitous tarkoittaa, että tieto on aitoa ja alkuperäistä, ja että tietoa ei ole kopioitu, jäljitelty tai väärennetty (Whitman & Mattord, 2011). Tiedon käyttökelpoisuudella tarkoitetaan, että tietoa voidaan aidosti käyttää ja sillä on jokin tarkoitus (Whitman & Mattord, 2011). Tiedon omistus puolestaan tarkoittaa, että tiedolla on omistaja tai sitä kontrolloidaan muilla keinoilla (Whitman & Mattord, 2011).

Nämä uudet tiedon ominaisuudet tekevät tietoturvan määrityksestä huomattavasti nykyaikaisemman ja laajemman. Pelkkä C.I.A -malli ei pysty selittämään nykyisiä tietoturvan ongelmia, mutta laajennuksen avulla malli sopii tähän tarkoitukseen paremmin. Laajennetussa mallissa on ominaisuuksia, jotka huomioivat, että kaikki tietoturvan ongelmat eivät liity tiedon luotettavuuteen, eheyteen ja saatavuuteen.

2.2 Kotikäyttäjä ja tietoturva

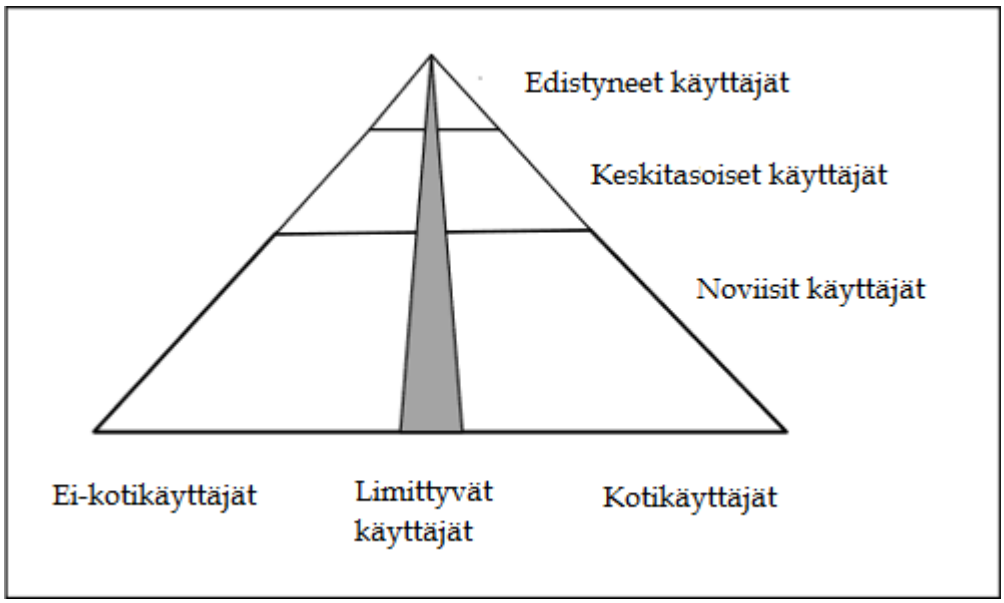
Kun puhutaan kotikäyttäjästä, täytyy ymmärtää, että kohderyhmä on valtava ja hyvin monipuolinen, eikä tarkan määritelmän antaminen ole mahdollista. Käyttäjät voivat olla lapsia, aikuisia ja vanhuksia. (Howe, Ray, Roberts, Urbanska & Byrne, 2012.) Edellä mainituista syistä on ensiarvoisen tärkeää tiedostaa, mitä kotikäyttäjällä tarkoitetaan tässä tutkimuksessa.

Kritzinger ja von Solms (2010) määrittelevät kotikäyttäjän tarkoittavan henkilöä, jonka ikä ja teknologinen osaaminen vaihtelevat, ja joka käyttää informaatioteknologiaa työympäristön ulkopuolella. Alasuutari (2016) toteaa väitöskirjassaan, että kotikäyttäjät käyttävät teknologioita myös kotinsa ulkopuolella, esimerkiksi kahviloissa ja kirjastoissa.

Tämän tutkimuksen kannalta on myös tärkeää huomioida, että erilaisilla kotikäyttäjillä on erilaiset tekniset kyvykkyydet ja osaaminen. Furnell, Bryant ja

Phippen (2007) jakavat tutkimuksessaan internetin käyttäjät kolmeen eri kategoriaan teknisen osaamisen perusteella: noviiseihin-, keskitasoisiin- ja edistyneisiin käyttäjiin. Edellä mainittu luokitus sopii erittäin hyvin myös tähän tutkimukseen, jossa pyrimme keskittymään kotikäyttäjiin, joiden teknologinen kyvykkyys on matala eli noviiseihin.

Kritzinger ja von Solms (2010) käyttävät apunaan Furnellin, Bryantin ja Phippenin (2007) jakoa teknologisesta osaamisesta, ja tuovat mukaan jaottelun kotikäyttäjän ja ei-kotikäyttäjän välillä (kuvio 1). Kritzinger ja von Solms (2010) myös erottelevat käyttäjiä heidän työtehtäviensä mukaan. Usein työtehtävissä, joissa käsitellään arkaluontoista informaatiota, pidetään myös huolta työntekijöiden tietoturvasta, ja usein työntekijöille järjestetään erilaisia tietoturvakoulutuksia. Tällaiset henkilöt eivät ole enää puhtaasti kotikäyttäjiä, vaan he sijoittuvat kuvion keskiosaan ja ovat limittyviä käyttäjiä (kuvio 1). Ei-kotikäyttäjät -alue (kuvio 1) tarkoittaa puolestaan henkilöitä, jotka käyttävät informaatioteknologiaa ainoastaan työympäristössä.



KUVIO 1 Käyttäjien jakaminen osaamisen ja käyttöpaikan välillä (Kritzinger & von Solms, 2010; suomentanut Sippo, 2017)

Tässä tutkimuksessa kotikäyttäjällä tarkoitetaan siis henkilöä, joka käyttää informaatioteknologiaa. Lisäksi kotikäyttäjän teknologinen osaaminen ei ole kovin suuri (noviisi käyttäjä), eikä hän ole saanut työnsä puolesta tietoturvakoulutusta.

2.3 Kotikäyttäjän erot verrattuna yrityksen työntekijään

Yrityksissä tietoturvan merkitys ja vaikutukset on tiedostettu jo pitkään. Tästä syystä yrityksissä tietoturvaan kiinnitetään huomiota. Tässä luvussa on tarkoi-

tus erotella tekijöitä tietoturvan suhteen, jotka erottavat kotikäyttäjän yrityksen työntekijästä.

Usein yrityksen työntekijät saavat työnpuolesta todennäköisemmin pakollista koulutusta tietoturvaan liittyvistä asioista. Heidän käyttäytymistään myös tarkkaillaan, jotta yrityksen tietoturvan toteutumista voidaan arvioida. He ovat jatkuvasti siis niin sanotun ”valvovan silmän alla” (Kritzinger & von Solms, 2010.) Kotikäyttäjien osalla tilanne on kuitenkin toisenlainen. Kotikäyttäjiltä puuttuu yrityksen kaltainen valvova taho, joka mittaisia tietoturvan toteutumista käytössä ja varmistaisi paremman tietoturvakäyttäytymisen (Kritzinger & von Solms, 2010).

Voidaankin sanoa, että kotikäyttäjien turvallisuus kärsii huomattavasti yksinomaan siitä syystä, että valvontaa ei ole. Tästä syystä myös motivaatio tietoturvan parantamiseen puuttuu. Usein yrityksissä käytetään motivoivina keinoina joko rangaistuksia tai palkitsemisia. Kotikäyttäjillä motivaatio tietoturvaa kohtaan täytyy herätä jotakin muuta kautta. Valitettavan usein näin ei kuitenkaan tapahdu. On todettu, että kotikäyttäjät eivät ole kovinkaan motivoituneita omaa tietoturvaansa kohtaan (Furnell, Tsaganidi & Phippen, 2008).

Yrityksen sisällä tietoturvasta vastaa usein yrityksen oma yksikkö, jonka tehtävänä on huolehtia ohjelmistojen asentamisesta ja päivityksistä. He myös huolehtivat erilaisten tietoturvaratkaisujen asentamisesta (Anderson & Agarwal, 2010.) Kotikäyttäjien tilanne on toinen. He joutuvat henkilökohtaisesti asentamaan kyseiset suojaukset ja ohjelmistot, elleivät he halua maksaa niiden erillisestä asentamisesta. Kotikäyttäjien osalta tietoturva on täysin vapaaehtoista (Li & Siponen, 2011). Erilaisia tapoja suojautua uhilta internetissä on todella paljon, mutta käyttäjä joutuu itse käyttämään omaa harkintakykyään miettiessään mitä eri tietoturvapalveluita hän ottaa käyttöön (Alasuutari, 2016).

Kotikäytössä laitteet ovat yleensä myös jaettuja, joka tarkoittaa sitä, että yhtä laitetta käyttää monta eri henkilöä. Li ja Siponen (2011) pitävät todennäköisenä, että useat käyttäjät samalla laitteella heikentävät laitteen tietoturvaa. Edellä mainittu on hypoteesi, mutta voidaan olettaa, että se on oikean suuntainen. Kun käyttäjien määrä kasvaa, on laitteen turvallisuutta hankalampi hallita. Lisäksi yhden käyttäjän turvaton käyttäytyminen vaarantaa myös kaikki muut käyttäjät. Yritysmaailmassa usein laitteet ovat henkilökohtaisia, joten tätä ongelmaa ei ole.

Edellä mainituista syistä voimme päätellä osasyitä miksi yritysten tietoturva on lähtökohtaisesti jo paljon paremmalla tasolla kuin kotikäyttäjien. Yrityksen työntekijät saavat useita tietoturvaratkaisuja valmiina, kun taas kotikäyttäjät joutuvat itse vastaamaan koko käyttöönotosta aina päätöksenteosta asentamiseen asti. On selvää, että tämä on suuri ongelma, varsinkin kun tekninen osaaminen kotikäyttäjillä on yleensä suhteellisen heikko.

2.4 Kotikäyttäjän yleisimmät tietoturvariskit

Viestintäviraston raportissa (2017) eritellään vuoden 2016 aikana tyypillisimpiä verkkouhkia, jotka kohdistuivat suomalaisiin kotikäyttäjiin. Viisi yleisintä uhkaa verkossa raportin mukaan olivat;

- Huijaukset ja tilausansat
- Kiristysohjelmat
- Tietoturvapuutteet Internet of Things -laitteissa
- Yksityisyyden puute sosiaalisessa mediassa
- Saman salasanan käyttäminen useassa palvelussa

Raportin löydökset ovat linjassa muiden tilastojen kanssa, esimerkiksi Symantec (2016).

2.4.1 Huijaukset ja tilausansat

Erilaisia tapoja huijata kotikäyttäjiä internetissä on lukemattomia. Huijauksia kuitenkin yhdistää tiedonkalastelu (phishing). Lähes aina, jotta huijaus voidaan toteuttaa, tarvitaan uhrista jotakin tietoa, esimerkiksi nimi tai pankkitunnukset. Tällaista tietojenkalastelua esiintyy niin verkkosivujen kuin sähköpostienkin muodossa. Tietojenkalastelusivustot pyrkivät ohjaamaan käyttäjän sivustolle ja näyttämään mahdollisimman luotettavilta, jotta käyttäjä syöttäisi omat tietonsa kyseiselle sivulle. Tietojenkalastelusähköpostit puolestaan lähestyvät uhria sähköpostin välityksellä ja pyytävät tietoja suoraan tai ohjaavat käyttäjän sivustolle, jolla tietoja pyritään keräämään.

Kotikäyttäjillä suurin ongelma liittyen erilaisiin huijauksiin internetissä on se, että tietojenkalastelun välineitä ei tunnisteta. Dahamija, Tygar ja Hearst (2006) totesivat, että hyvin rakennettu huijaussivusto onnistui huijaamaan yli 90% prosenttia koehenkilöistä.

Kun kotikäyttäjät joutuvat arvioimaan internet sivun luotettavuutta he kiinnittävät usein huomiota vääriin asioihin. Kotikäyttäjät pitävät usein sivun ulkoasuun liittyä asioita, kuten animaatioita ja kuvia, takeena sivun turvallisuudesta ja luotettavuudesta (Dahamija ym., 2006.) On sanomattakin selvää, että tämän kaltainen käyttäytyminen johtaa ennen pitkää ongelmiin.

2.4.2 Kiristysohjelmat

Kiristysohjelmat (ransomware) ovat haittaohjelmia, jotka pyrkivät lukitsemaan käyttäjän tiedostot tai itse laitteen ja jonka jälkeen käyttäjälle esitetään maksuvaatimus tiedostojen tai laitteen avaamisesta (Mercaldo, Nardone & Santone, 2016).

Tietojen lukitseminen tapahtuu salaamalla tiedostot jotakin salausmenetelmää käyttäen. Avatakseen laitteen käyttäjän on saatava salaus murrettua eli saatava haltuunsa salausavain, jota salauksessa on käytetty. Muitakin menetelmiä ja työkaluja on olemassa, mutta niiden tehokkuudesta tai toimivuudesta ei ole takeita. Usein noviisien käyttäjien ainut vaihtoehto on maksaa kiristäjille tai delegoida asian hoitaminen osaavammalle henkilölle.

Useimmiten kiristysohjelmia pyritään levittämään sähköpostin liitetiedostona. On myös yleistä, että uhri asentaa itse haittaohjelman tietokoneeseensa usein huijausviestin motivoimana (Viestintävirasto, 2016.)

Vaikka erilaiset kiristysohjelmat ovatkin yleistyneet ja saavuttaneet enemmän huomiota viime vuosina, eivät ne ole kovinkaan uusi ilmiö. Ensimmäiset havainnot kiristysohjelmista esiintyivät jo yli kymmenen vuotta sitten (Gazet, 2010). Symantecin (2016) raportin mukaan erilaiset kiristysohjelmat lisääntyivät vuonna 2015 yli 35% vuoden 2014 lukuihin verrattuna. Kasvun odotetaan jatkuvan myös tulevaisuudessa.

Tänä päivänä kiristysohjelmat ovat yleistyneet vauhdilla myös mobiililaitteissa (Mercaldo ym., 2016). Tämä kehitys on täysin loogista. Ihmiset käyttävät yhä enemmän mobiililaitteita perinteisten tietokoneiden sijasta, jolloin myös mobiililaitteista tulee kohde tämän tyyppisille hyökkäyksille.

2.4.3 Tietoturvapuutteet Internet of Things -laitteissa

Internet of Things (IoT) tarkoittaa internetiin kytkettyjä jokapäiväisiä laitteita ja kodinkoneita ja niiden muodostamaa verkostoa. Usein kyseiset laitteet sisältävät myös jonkinlaista laskentaa tai tietoa (Xia, Yang, Wang & Vinel, 2012.) Tällaiset laitteet yleistyvät jatkuvasti niin suomalaisten kodeissa kuin myös maailmalla. Mukanaan kyseiset laitteet tuovat loistavia ominaisuuksia ja mahdollisuuksia, mutta myös vakavia tietoturva ongelmia.

Usein IoT -laitteet ovat suurimmanosan ajasta valvomatta, jolloin hyökkääjillä on paljon aikaa toteuttaa itse hyökkäys. Lisäksi langattoman verkon kuuntelu on teknisesti todella helppoa toteuttaa (Atzori, Lera & Morabito, 2010.) IoT -laitteet ovat myös erittäin haavoittuvia Man-in-the-middle tyyppisille tietoturvahyökäykselle (Atzori ym., 2010). Man-in-the-middle hyökkäys tarkoittaa hyökkäystä, jossa käyttäjän ja palvelimen välinen liikenne kaapataan, ja sen sisältöä muokataan halutulla tavalla. Tämän jälkeen viesti naamioidaan ja lähetetään pyyntönä palvelimelle, jolloin palvelin kuvittelee palvelevansa laitteen omistajaa, vaikka todellisuudessa pyynnöt on lähettänyt hyökkääjä.

Kun laitteiden huono tietoturva ja yksityisen datan kerääminen IoT -laitteissa yhdistyvät, on tuloksena vakavia tietoturvapuutteita. Tulevaisuudessa IoT:n tietoturva tulee korostumaan entisestään, kun tällaisten laitteiden määrä jatkaa kasvuaan suomalaisissa kodeissa.

2.4.4 Yksityisyyden puute sosiaalisessa mediassa

Sosiaalinen media sisältää paljon tietoa käyttäjästä. Osa tästä tiedosta on julkista, mutta usein sosiaalisessa mediassa on saatavilla käyttäjästä erittäin yksityiskohtaista tietoa. Tämä avaa paljon ovia erilaisille häiriköille tai rikollisille. Esimerkiksi liian tarkat ja jatkuvat sijaintitiedot voivat altistaa kotisi varkaille tai sähköpostiosoitteen ilmoittaminen julkisessa profiilissa voi altistaa sähköpostinviesteihin perustuviin huijauksiin. Yksityisen tiedon väärinkäytölle on lukemattomia mahdollisuuksia ja lähinnä rikollisen mielikuvitus on rajana.

Sosiaalisesta mediasta louhitaan paljon tietoa myös yritysten käyttöön. Tämän tiedon pohjalta käyttäjälle kohdennetaan markkinointia. Tiedonkeruulta on lähes mahdotonta välttyä, mutta olisi hyvä muistaa ja tiedostaa, että näin tehdään.

Sosiaalisen median käytössä tulisi siis muistaa, että liian yksityiskohtaista tai arkaluontoista informaatiota ei tulisi näihin palveluihin tallentaa, ainakaan kaikille näkyviin julkisiin profiileihin.

2.4.5 Saman salasanan käyttäminen useassa palvelussa

Viestintäviraston (2017) raportissa mainitaan myös salasanojen heikkous merkittävänä uhkana yksilön tietoturvan kannalta. Raportti on täysin linjassa salasanoihin liittyvän tieteellisen tutkimuksen kanssa. Kotikäyttäjillä on usein kymmeniä erilaisia palveluita, joihin vaaditaan käyttäjätunnus ja salasana. Erilaisia palveluita on usein niin paljon, että jos jokaiseen palveluun laadittaisiin oma salasana, olisi niiden muistaminen liian vaikeaa (Florencio & Herley, 2007.)

Ratkaisu edellä mainittuun ongelmaan on usein muutama erilainen salasana, joita käytetään eri palveluissa (Florencio & Herley, 2007). Tällöin käyttäjän ei tarvitse muistaa kymmeniä erilaisia salasanoja, ja salasanojen hallinta helpottuu. Tietoturvan kannalta huonoin tilanne on, jos jokaisessa palvelussa käytetään samaa salasanaa. Tällöin yhden palvelun kirjautumistietojen varastaminen vaarantaa myös kaikki muut palvelut, joihin käyttäjä on rekisteröitynyt samalla salasanalla.

Toinen ongelma kotikäyttäjän salasanoissa on niiden huonous. Usein käyttäjät valitsevat tietoisesti heikon salasanan, erityisesti jos he eivät pidä palvelua tärkeänä. Kotikäyttäjät myös tiedostivat usein salasanan heikkouden, mutta eivät olleet motivoituneita korjaamaan kyseistä ongelma. (Egelman, Sotirakopoulos, Muslukhov, Beznosov & Herley, 2013.) Alasuutari (2016) on todennut, että vahvan salasanan laatiminen aiheuttaa käyttäjälle vaivannäköä, koska usein vahvat salasanat ovat hankalampia muistaa.

Kotikäyttäjät siis valitsevat huonon salasanan, koska huono salasana on helpompi muistaa, he eivät pidä palvelua tärkeänä ja hyvän salasanan keksiminen ja muistaminen aiheuttaa käyttäjälle ylimääräistä vaivaa.

3 TIETOTURVAKÄYTTÄYTYMINEN

Tässä luvussa tarkastellaan kotikäyttäjän tietoturvakäyttäytymistä kokonaisuutena. Luvun jälkeen lukijalla on selkeä käsitys siitä, mitä tietoturvakäyttäytyminen tarkoittaa ja mistä eri tekijöistä se kotikäyttäjillä tyypillisesti rakentuu.

3.1 Tietoturvakäyttäytymisen määritelmä

Tietoturvakäyttäytyminen tarkoittaa tässä tutkimuksessa kotikäyttäjän tapaa, jolla hän käyttäytyy kotilaitteellaan ja tietoverkoissa ja kuinka hän huomioi tietoturvaa käyttäytymisessään.

Tietoturvakäyttäytyminen viittaa myös aktiviteetteihin, joita loppukäyttäjien noudatettava tietoturvan ylläpitämiseksi, ja jotka on määritetty tietoturvaohjeissa (Padayachee, 2012). Kotikäyttäjillä tietoturvaohjeista ei kuitenkaan vastaa kukaan muu kuin yksilö itse.

Tietoturvakäyttäytymisestä puhuttaessa on myös huomioitava niin sanottu suunniteltu käyttäytyminen (planned behaviour) ja todellinen käyttäytyminen (actual behaviour) (Thomson & von Solms, 1998). Vaikka yksilö tiedostaa ongelmia ja hän aikoo käyttäytyä tietyllä tavalla, on eri asia noudattaako hän jatkossa suunnitelmaansa paremmasta käyttäytymisestä Kotikäyttäjän osalta tämä tarkoittaa sitä, että vaikka hän miettii tietoturvaansa ja muodostaa aikomuksen parantaa sitä jollakin tavalla, ei voida olla varmoja noudattaako hän loppupeleissä tekemäänsä suunnitelmaa.

3.2 Kotikäyttäjälle tyypillinen tietoturvakäyttäytyminen

Useimmat tietokoneen kotikäyttäjät pystyvät nimeämään joitakin internetin uhista, kuten virukset, ja ainakin ymmärtämään yhteyden kyseisen uhan ja tietoturvan välillä. Useimmat myös tiedostavat olevansa itse vastuussa omasta tietoturvastaan. Siitä huolimatta perustason käyttäjät pystyvät hyvin harvoin

nimeämään ratkaisuja tai parempia toimintatapoja tuntemiinsa tietoturvaongelmiin. Lisäksi käyttäjät eivät vaikuta kovinkaan kiinnostuneilta parantamaan omaa tietoturvaansa, vaikka ymmärtävätkin että ongelmia on olemassa. (Furnell, Tsaganidi & Phippen, 2010.)

Usein kotikäyttäjä käyttää internetiä henkilökohtaiselta laitteeltaan, joka on hyvin usein tietokone, kannettava tietokone, älypuhelin tai tablettitietokone. Edellä mainitut laitteen sisältävät usein arkaluontoista tiedostoja ja informaatiota, kuten kuvia, viestejä, laskuja, työhakemuksia ja monia muita arkaluontoisia tiedostoja (Alasuutari, 2016.)

Kun tällaista tietoa sisältävät laitteet ovat yhteydessä internetiin riskit tietojen varastamisesta tai menettämisestä kasvavat. Lisäksi edellä mainittujen laitteiden omistaja on usein henkilökohtaisesti vastuussa laitteen tietoturvasta (Alasuutari, 2016).

Perinteisiä pöytätietokoneita ja kannettavia tietokoneita kuitenkin suojataan usein paremmin, kuin esimerkiksi älypuhelimia ja tablettitietokoneita (Alasuutari, 2016). Älypuhelimien tietoturvaan tulee jatkossa kiinnittää yhtä paljon huomiota kuin tietokoneidenkin, sillä usein älypuhelimia käytetään tietokoneen tavoin ja molemmat sisältävät käyttäjän kannalta arkaluontoista informaatiota.

Kotikäyttäjät suojautuvat usein paremmin erilaisia uhkia vastaan, mikäli he tuntevat olevansa omistussuhteessa suojattavaan laitteeseen tai järjestelmään (Anderson & Agarwal, 2010). Esimerkiksi kotikäyttäjät usein suojaavat henkilökohtaista tietokonettaan paremmin kuin esimerkiksi jotakin internetin palvelua, koska heillä on psykologinen omistussuhde tietokoneeseen, mutta internetiin ja sen palveluihin tällaista suhdetta ei ole. Puhun psykologisista tekijöistä lisää myöhemmin tässä luvussa.

Kotikäyttäjälle tyypillistä käyttäytymistä on suhteellisen vaikea kuvailla, koska kohderyhmä on niin laaja. Tärkeintä on kuitenkin muistaa, että suurin osa kotikäyttäjistä käyttää internetiä tietokoneen tai mobiililaitteen välityksellä. Kotikäyttäjät myös tiedostavat, että kybermaailmassa on olemassa erilaisia riskejä, mutta he eivät yleensä osaa ratkaista tai torjua kyseisiä riskejä.

3.3 Tietoturvakäyttäytymiseen vaikuttavat tekijät

Kotikäyttäjän tietoturvakäyttäytymiseen vaikuttaa monia erilaisia tekijöitä. Tässä alaluvussa kuvataan tietoturvaan vaikuttavia tekijöitä yksityiskohtaisesti.

3.3.1 Asenne ja motivaatio

Asenteella ja motivaatiolla on suuri merkitys tietoturvakäyttäytymisen rakentumisessa. Mutta kuten edellä jo todettiin, kotikäyttäjillä ei ole takanaan yritystä, joka motivoisi parempaan tietoturvaan, vaan kotikäyttäjillä motivaation ja asen-

teen on löydyttävä jostain muualta. Oikeanlaisen asenteen merkitys on kuitenkin suuri tietoturvan kannalta.

Useissa eri tutkimuksissa on todettu, että asenteella on positiivinen vaikutus tietoturvakäyttäytymiseen (Ng & Rahim, 2005; Anderson & Agarwal, 2010). Asenne ja motivaatio ovat varmasti yksi merkittävimmistä tekijöistä, jotka vaikuttavat tietoturvakäyttäytymiseen.

Furnell ym. (2008) toteavat, että osa käyttäjistä ei ole motivoituneita tai kiinnostuneita parantamaan tietoturvaansa, vaikka ymmärtävätkin, että riskejä on olemassa. Kotikäyttäjillä asenteen ja motivaation puuttuminen on huolestuttavaa, sillä kuten aiemmin todettiin, kotikäyttäjiltä puuttuu täysin ulkoiset motivaattorit oman käyttäytymisen parantamiseen.

Positiivinen asenne ja motivaatio siis vaikuttavat positiivisesti tietoturvakäyttäytymiseen, mutta mitä tapahtuu, jos asenne on lähtökohtaisesti todella huono tai sitä ei ole lainkaan. Voidaan olettaa, että negatiivinen asenne vaikuttaa tietoturvaan passivoivasti. Ne kotikäyttäjät, joilla ei ole motivaatiota tai asennetta tietoturvaa kohtaan, käyttäytyvät välinpitämättömästi ja jättävät tietoturvan huomioimatta omassa käyttäytymisessään.

Edellisen perusteella voidaan olettaa, että kotikäyttäjän motivaatio ja asenne ovat erittäin tärkeitä elementtejä, kun halutaan siirtyä suunnitellusta tietoturvakäyttäytymisestä todelliseen tietoturvakäyttäytymiseen. Asenteet ja motivaatio toimivat eräänlaisena mahdollistajina paremmalle tietoturvakäyttäytymiselle. Voidaan olettaa, että lähtökohtaisesti jokaisen kotikäyttäjän tietoturvatietoisuuden kohotessa myös tietoisuus siitä, kuinka hänen tulisi käyttäytyä tietoturvallisesti nousee, mutta vain henkilöt, jotka ovat motivoituneita ja asennoituneet oikealla tavalla, alkavat käyttäytyä turvallisemmin. Puolestaan ne henkilöt, jotka eivät omaa samanlaista asennetta tai motivaatiota tietoturvaa kohtaan, eivät muuta käyttäytymistään turvallisemmaksi.

3.3.2 Hyödyt, haitat ja kustannukset

Tietoturvakäyttäytymiseen vaikuttavat myös oleellisesti käyttäjän kokemat hyödyt ja haitat (Beautement, Sasse, & Wonham, 2008). Esimerkiksi jos käyttäjä haluaa ottaa käyttöön virustorjunnan hän arvioi ohjelmiston mahdollisia hyötyjä (tietoturvan paraneminen, jne.) ja vertaa niitä ohjelmiston käytöstä ilmeneviin haittoihin ja kustannuksiin (ärsyttävät ilmoitukset, tietokoneen hidastuminen, palvelun hinta, jne.). Mikäli haitat tai kustannukset koetaan liian suuriksi saatavaan hyötyyn nähden, on usein tilanne se, että käyttäjä ei ota palvelua käyttöön. Lisäksi tutkimuksissa on todettu, että käyttäjät haluavat hyötyä mahdollisesti turvattomasta käyttäytymisestä (Howe ym., 2012).

3.3.3 Kognitiiviset, sosiaaliset ja psykologiset tekijät

Anderson ja Agarwal (2010) ovat todenneet, että käyttäjän tietoturvakäyttäytymiseen vaikuttaa joukko kognitiivisia, sosiaalisia ja psykologisia tekijöitä.

Anderson ja Agarwal (2010) erittelevät erityisesti kaksi sosiaalista tekijää, jotka vaikuttavat käyttäjän tietoturvakäyttäytymiseen: subjektiivinen normi (subjective norm) ja deskriptiivinen normi (descriptive norm). Subjektiivinen normi tarkoittaa asioita, joita käyttäjä uskoo muiden ihmisten odottavan häneltä. Deskriptiivinen normi puolestaan tarkoittaa asioita, joita käyttäjä olettaa muiden käyttäjien tekevän (Anderson & Agarwal, 2010.) On tärkeää kuitenkin tiedostaa, että edellä mainittujen tekijöiden vaikutukset eivät välttämättä ole positiiviset turvallisuuden kannalta. Lisäksi on huomioitava, että edellä mainitut normit eivät välttämättä toimi kaikissa tilanteissa.

Kuten edellä jo todettiin, tietoturvakäyttäytymiseen vaikuttavat myös psykologiset omistussuhteet. Mitä suurempaa psykologista omistuksen tunnetta käyttäjä tuntee suojattavaa kohdetta kohtaan, sitä turvallisempaa hänen käyttäytymisensä todennäköisesti on (Anderson & Agarwal, 2010). Esimerkiksi kotikäyttäjä yleensä tuntee vahvaa omistuksen tunnetta omaa henkilökohtaista tietokonettaan kohtaan, jolloin tätä tietokonetta myös suojataan paremmin. Mutta esimerkiksi internetiä kohtaan käyttäjällä ei juuri ole omistussuhdetta. Internet mielletään käyttäjien osalta yleensä ”yhteisenä hyvänä” (Anderson & Agarwal, 2010). Tällöin myös turvallisen tietoturvakäyttäytymisen todennäkösyys internetissä pienenee.

Psykologisista tekijöitä tarkastellessa tulee myös huomioida yksilön kyky tehdä päätöksiä. Leach (2003) toteaa yksilön kyvyn tehdä päätöksiä vaikuttavan tietoturvakäyttäytymiseen. Useimmat päätökset tehdään ei kriittisissä tilanteissa, joissa päätöksenteko kestää myös jonkin verran poikkeamaa optimaalisesta tietoturvakäyttäytymisestä. Jotkin päätökset tehdään kuitenkin kriittisissä tilanteissa, joissa aikaa reagoida on vähemmän. Tällöin myös marginaali huonojen päätösten siedon osalta pienenee (Leach, 2003.) Kotikäyttäjillä tällainen kriittinen tilanne voisi olla esimerkiksi virustorjuntaohjelmiston hälyttäminen viruksen havaitsemisesta, tällöin käyttäjä joutuu tekemään nopeita päätöksiä käyttäytymisensä suhteen.

Voidaankin todeta, että kotikäyttäjillä tietoturvakäyttäytymiseen vaikuttaa joukko erilaisia kognitiivisia, sosiaalisia sekä psykologisia tekijöitä. Täytyy myös huomioida, että kyseiset tekijät ovat erittäin vahvasti yksilöllisiä.

3.3.4 Minäpystyvyys

Anderson ja Agarwal (2010) toteavat, että minäpystyvyys (self-efficacy) on merkittävä tekijä tietoturvakäyttäytymisessä. Minäpystyvyys tarkoittaa sitä, että kotikäyttäjä tuntee osaavansa ja pystyvänsä ratkaisemaan jokapäiväisessä käytössä kohdattuja ongelmia tietoturvaan liittyen. Minäpystyvyyttä voidaan pitää siis motivoivana tekijänä, joka kannustaa parempaan tietoturvakäyttäytymiseen.

Rhee, Kim ja Ryu (2009) toteavat tutkimuksessaan, että henkilöt joiden minäpystyvyyden taso on korkeampi, ottavat myös todennäköisemmin käyttöön tietoturvaohjelmistoja ja käyttäytyvät ylipäätään turvallisemmin verkossa kuin henkilöt, joiden minäpystyvyys on heikompi. Käyttäjät jotka omaavat kor-

keamman minäpystyvyyden myös ylläpitävät ja kehittävät tietoturvaosaamistaan paremmin (Rhee ym., 2009).

Kun puhutaan minäpystyvyydestä ja sen vaikutuksista kotikäyttäjiin tässä tutkimuksessa, on kuitenkin huomioitava mistä asioista se tietoturvan kontekstissa koostuu. Edwards (2015) toteaa, että tietoturvatietoisuus on merkittävä tekijä yksilön minäpystyvyyden kannalta. Rhee ym. (2009) puolestaan määrittelevät minäpystyvyyden, informaatioteknologian kontekstissa, koostuvan kolmesta asiasta; yleisestä kokemuksesta tietokoneisiin ja internetiin liittyen, mahdollisesti tapahtuneista tietoturvaongelmista ja yleisestä hallittavuudesta. Totesimme kuitenkin kotikäyttäjiä tarkastellessa, että useilla kotikäyttäjillä tekniset taidot eivät ole kovin hyvät. On siis huomioitava, että minäpystyvyys saattaa puuttua kotikäyttäjiltä lähes kokonaan tai osittain. Tästä syystä ei voida sanoa, että se vaikuttaisi aina tietoturvakäyttäytymiseen kotikäyttäjillä. Mutta jos kyvykkyyttä on olemassa, ei sen vaikutuksia käyttäytymiseen voida kiistää.

3.3.5 Tietoturvatietoisuus

Tietoturvatietoisuus on oleellinen osa yksilön tietoturvakäyttäytymistä. Useissa tutkimuksissa on todettu, että tietoturvatietoisuuden paraneminen vaikuttaa positiivisesti yksilön tietoturvaan (Howe ym., 2012; Öğütçü, Testik, & Chouseinoglou, 2016). Tietoturvatietoisuutta ja sen vaikutuksia tietoturvakäyttäytymiseen tarkastelemme syvemmin tämän tutkimuksen seuraavassa pääluvussa.

3.3.6 Tilannesidonnaisuus

Tietoturvakäyttäytymisen rakentumista tarkastellessa on myös tärkeää huomioida, että tietoturvakäyttäytyminen ei aina ole samanlaista. Alasuutari (2016) toteaa väitöskirjassaan, että tietoturvakäyttäytyminen on tilannesidonnaista ja että käyttäjä voi suojaustoimen käyttöönoton jälkeen joissain tilanteessa poiketa siitä, varsinkin jos hän kokee, että turvallisesta käyttäytymisestä poikkeaminen on hänelle hyödyllistä.

Tällaisessa tilanteessa käyttäjä kokee tarpeiden välisen ristiriidan ja priorisoi tarpeitaan. Tämän seurauksena käyttäjä väliaikaisesti tai pysyvästi muuttaa käyttäytymistään ja luopuu suojaustoimesta (Alasuutari, 2016.) Tämä on oleellinen huomio, sillä useat tutkimukset ovat olettaneet, että tietoturvakäyttäytyminen on tilanteesta riippumatta aina samanlaista.

Kotikäyttäjien osalta tilannesidonnaisuus siis tarkoittaa sitä, että kotikäyttäjien tietoturvakäyttäytyminen ei ole aina samanlaista, vaan se vaihtelee ja on erilaista eri tilanteissa.

4 TIETOTURVATIETOISUUS

Tässä kappaleessa käsittelen tietoturvatietoisuutta kokonaisuutena. Pyrin antamaan tietoturvatietoisuudelle selkeän määritelmän kotikäyttäjän osalta, erittelemään tekijöitä, joista tietoturvatietoisuus koostuu ja lopuksi arvioimaan tietoturvatietoisuuden vaikutuksia kotikäyttäjän tietoturvakäyttäytymiseen.

4.1 Tietoturvatietoisuuden määritelmä

Tietoturvatietoisuus on käsitteenä erittäin laaja ja se sisältää paljon erilaisia näkökulmia. Siponen (2001) on jakanut tietoturvatietoisuuden viiteen erilaiseen ulottuvuuteen (dimension), jotka käsittelevät tietoturvatietoisuutta eri näkökulmasta. Näitä ulottuvuuksia ovat: organisatorinen ulottuvuus (organizational dimension), julkinen ulottuvuus (general public dimension), sosiopoliittinen ulottuvuus (socio-political dimension), tietokoneen eettinen ulottuvuus (computer ethical dimension) ja institutionaalinen koulutus ulottuvuus (institutional education dimension) (Siponen, 2001).

Tässä tutkimuksessa keskitymme julkiseen ulottuvuuteen, jonka sisällä käsittelemme tarkemmin tietoturvatietoisuutta juuri kotikäyttäjän näkökulmasta. Tästä huolimatta on kuitenkin ymmärrettävä, että tietoturvatietoisuus ei ole yksiselitteinen käsite ja sen määritelmä saattaa vaihdella erilaisten kohteiden välillä, koska tietoturvan tarpeet ovat erilaiset.

Bulgurcu, Cavusoglu, ja Benbasat (2010) määrittelevät tietoturvatietoisuuden seuraavasti: “General information security awareness is defined as an employee's overall knowledge and understanding of potential issues related to information security and their ramifications.”

He siis määrittelevät tietoturvatietoisuuden (information security awereness) tarkoittavan yrityksen työntekijän yleistä tietämystä ja ymmärrystä mahdollisista ongelmista, jotka liittyvät tietoturvaan, ja niiden seuraamuksista.

Vaikka he määrittelevät tietoturvatietoisuuden yrityskontekstissa on määritelmä erittäin pätevä ja paikkansapitävä myös kotikäyttäjien osalta. Kotikäyt-

täjienkin osalta tietoturvatietoisuus tarkoittaa juurikin yleistä tietämystä tietoturvasta ja tietoturvan vaikutusten ymmärtämistä laajemmassa mittakaavassa. Määritykseen on kuitenkin lisättävä myös ymmärrys erilaisista ratkaisuista tietoturvaongelmiin. Tämä on tärkeää siksi, että kotikäyttäjät ovat itse vastuussa omasta tietoturvastaan ja joutuvat itse ratkaisemaan kohtaamansa ongelmat kybermaailmassa.

Tässä tutkimuksessa kotikäyttäjän tietoturvatietoisuudella tarkoitetaan siis kotikäyttäjän yleistä ymmärrystä tietoturvasta, sen ongelmista ja niiden vaikutuksista yksilöön ja ongelmien ratkaisujen olemassaolon tiedostamisesta.

4.2 Tietoturvatietoisuuden rakentuminen kotikäyttäjillä

Tietoturvatietoisuus on kokonaisuudessaan usean eri muuttujan summa. Kotikäyttäjillä tietoturvatietoisuuteen vaikuttavia tekijöitä tyypillisimmin ovat elämänkokemus ja yksilölliset erot. Tietoturvaan liittyvä koulutus on erinomainen keino ja tapa lisätä tietoturvatietoisuutta kotikäyttäjillä, mutta todella harvat kotikäyttäjät pystyvät osallistumaan tietoturvakoulutuksiin. Seuraavaksi tarkastelemme tietoturvatietoisuuden rakentumiseen vaikuttavia tekijöitä yksityiskohtaisemmin.

4.2.1 Koulutus ja tietoturvakoulutus

Pattinson, Butavicius, Parsons, McCormac & Calic (2015) toteavat tutkimuksessaan, että yleinen koulutuksen taso ei vaikuta merkittävästi yksilön tietoturvatietoisuuteen. Koulutuksella tarkoitetaan siis yleistä koulutusta, ei tietoturvaan liittyvää koulutustaustaa.

Tietoturvaan liittyvä koulutustausta korreloi puolestaan selvästi tietoturvatietoisuuden kanssa. Tietoturvaan liittyvän koulutuksen ongelmana kotikäyttäjien osalta on kuitenkin sen maksullisuus ja ongelmat saatavuudessa. Hyvin harvat kotikäyttäjät pystyvät osallistumaan tietoturvakoulutukseen (Li & Siponen, 2011.) Usein kotikäyttäjät eivät edes tiedosta koulutuksen mahdollisuutta, koska he eivät ymmärrä tietoturvan merkityksellisyyttä tai osaa etsiä koulutusta. Tulevaisuudessa kotikäyttäjien koulutukseen tulisi kiinnittää enemmän huomiota, koska koulutuksella olisi laajat vaikutukset koko valtion tasolla tietoturvaan.

4.2.2 Elämänkokemus

Bulgurcu, Cavusoglu, ja Benbasat (2010) toteavat, että tietoturvatietoisuuden yksi osatekijä on elämänkokemus. Elämänkokemus tarkoittaa, että käyttäjä on voinut joutua aikaisemmin esimerkiksi viruksen uhriksi ja on siksi kiinnostunut omasta tietoturvastaan. Elämänkokemus pitää myös sisällään kaiken tiedon ja tietämyksen, jota käyttäjä on voinut lukea esimerkiksi lehdistä, uutisista tai

muista ulkoisista lähteistä (Bulgurcu ym., 2010). Myös Li ja Siponen (2011) ovat todenneet, että kotikäyttäjillä tietoturvatietoisuus pääosin koostuu itseoppimisesta ja omista henkilökohtaisista kokemuksista.

Kotikäyttäjien osalta elämänkokemuksen mukana tuoma tietämys tietoturvasta on selvästi merkittävin tekijä, kun tarkastellaan tietoturvatietoisuuden rakentumista kotikäyttäjillä. Täytyy myös muistaa, että osa elämänkokemuksen mukana tuomasta tiedosta voi olla hyvinkin virheellistä. Tässä tutkimuksessa elämänkokemus pitää sisällään myös massamedian, perheen sekä kollegoiden vaikutuksen tietoturvatietoisuuteen, jonka on todettu olevan varsin suuri (Ng & Rahim, 2005).

4.2.3 Yksilölliset erot

McCormac ym. (2017) ovat eritelleet tutkineet yksilöllisten erojen merkitystä tietoturvatietoisuuden rakentumisessa yrityskontekstissa. Voidaan kuitenkin olettaa, että yksilölliset erot vaikuttavat myös kotikäyttäjien tietoturvatietoisuuden rakentumiseen.

Tutkimuksessaan he tarkastelivat iän ja sukupuolen vaikutuksia tietoturvatietoisuuden. He havaitsivat, että ikä vaikuttaa merkittävästi tietoturvatietoisuuteen. Mitä korkeampi yksilön ikä on, sitä tietoisempi hän on tietoturvasta (McCormac ym., 2017.) Ikä puolestaan korreloi elämänkokemuksen kanssa, joten voidaan sanoa, että havainnot tukevat toisiaan. He havaitsivat myös, että sukupuoli vaikuttaa tietoturvatietoisuuteen. Naisilla havaittiin korkeampia tuloksia tietoturvatietoisuudessa, mutta erot miehiin verrattuna eivät olleet kovin suuria (McCormac ym., 2017).

He tutkivat myös persoonallisuuden, henkilökohtaisten erojen sekä yksilön riskienoton vaikutuksia tietoturvatietoisuuteen. Henkilöt, jotka ovat enemmän tietoisia, avoimempia ja joilla on taipumus ottaa vähemmän riskejä, ovat usein tietoisempia myös tietoturvan suhteen (McCornac ym., 2017). Myös muut tutkijat ovat saaneet samankaltaisia tuloksia. Pattinson ym. (2015) erittelevät tietoturvatietoisuuteen vaikuttavia yksilöllisiä tekijöitä olevan iän, avoimuuden, tietoisuuden, hyväksynnän sekä kyvyn kontrolloida impulsiivista käytöstä.

Bulgurcu ym. (2010) puolestaan argumentoivat, että tietoturvatietoisuus pitää sisällään erilaisia taustatekijöitä, joita ovat esimerkiksi demograafinen asema, kokemus, luonne ja tietämys, ja että nämä tekijät vaikuttavat epäsuorasti yksilön tietoturvakäyttäytymiseen. Voidaankin sanoa, että yksilölliset erot siis selvästi vaikuttavat kotikäyttäjän tietoturvatietoisuuteen, ja sitä kautta myös tietoturvakäyttäytymiseen.

4.3 Tietoturvatietoisuuden vaikutukset kotikäyttäjien tietoturvakäyttäytymiseen

Tutkimuksissa on todettu, että tietoturvatietoisuus ja tietoturvakäyttäytyminen kulkevat usein käsi kädessä. Kun käyttäjän tietoisuus erilaisista riskeistä ja uhista kasvaa, myös hänen suhtautumisensa tietoturvaan muuttuu ja yksilön käyttäytymisestä verkossa tulee turvallisempaa (Öğütçü, Testik, & Chouseinoglou, 2016.)

Myös muut tutkijat ovat saaneet vastaavia tuloksia. Howe ym. (2012) toteavat tutkimuksessaan, että kotikäyttäjien ollessa tietoinen uhista he välittävät tietoturvastaan enemmän ja tuntevat olevansa henkilökohtaisesti vastuussa tietoturvastaan. Tietoturvatietoisuus on siis selvästi liitoksissa tietoturvakäyttäytymiseen.

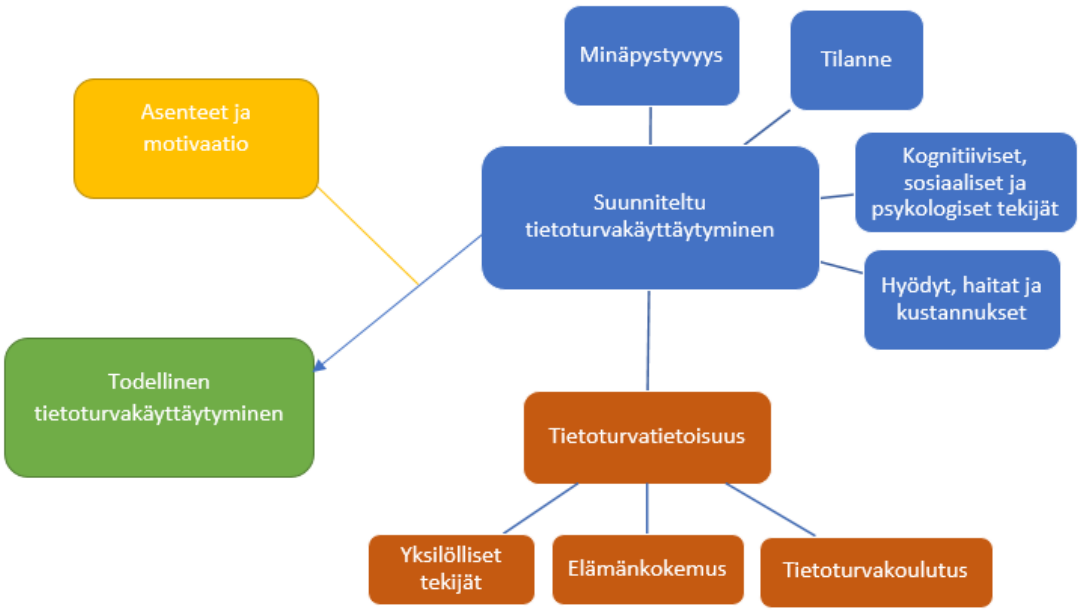
Toisaalta aina näin ei tapahdu. Anderson ja Agarwal (2010) toteavat, että tietoturvatietoisuus ei ole ainut asia, joka vaikuttaa tietoturvakäyttäytymiseen. Jossain tapauksissa tietoturvakäyttäytymisessä ei tapahdu muutosta, vaikka tietoturvatietoisuus kasvaisi tai se olisi lähtökohtaisesti korkea (Öğütçü, Testik, & Chouseinoglou, 2016). Useissa tutkimuksissa on todettu, että käyttäjä ei todennäköisesti paranna tietoturvaansa merkittävästi, vaikka heille tarjottaisiin tietoa eri riskeistä ja tietoturvaratkaisuista ja heidän tietoturvatietoisuutensa kasvaisi (Aytes & Connolly, 2004; Edwards, 2015).

Syitä tähän tulisi tutkia enemmän. Voidaan olettaa, että tällöin kotikäyttäjällä muut tekijät vaikuttavat tietoturvakäyttäytymiseen ja estävät sen paranemisen. Esimerkiksi jos käyttäjä tulee tietoisemmaksi tietoturvasta ja sen uhista, mutta hänellä ei ole motivaatiota parantaa tietoturvaa, on hyvin todennäköistä, että tietoturvakäyttäytyminen ei muutu paremmaksi.

Tietoturvatietoisuus on siis selvästi yksi osatekijä tietoturvakäyttäytymisen rakentumisessa kotikäyttäjillä, mutta se ei välttämättä yksin riitä parantamaan tietoturvakäyttäytymistä merkittävästi. Jotta parempi tietoturvakäyttäytyminen voidaan saavuttaa, tarvitaan myös muiden tekijöiden vaikutusta.

4.4 Malli kotikäyttäjän tietoturvakäyttäytymisen rakentumisesta

Tutkimuksen tulosten pohjalta on muodostettu malli tietoturvan rakentumisesta kotikäyttäjällä (kuvio 2). Mallissa esitetään kotikäyttäjän tietoturvakäyttäytymisen prosessi uudella tavalla, joka erittelee tietoturvakäyttäytymiseen sekä tietoturvatietoisuuteen vaikuttavia tekijöitä kotikäyttäjällä. Lisäksi mallissa todetaan asenteiden ja motivaation vaikutus ja tärkeys suunnitellun sekä toteutuneen tietoturvakäyttäytymisen välillä. Mallin pohjalta on helpompi ymmärtää tietoturvakäyttäytymisen kokonaisuutta sekä hahmottaa yksittäisiä asioita laajemmassa mittakaavassa.



KUVIO 2 Malli kotikäyttäjän tietoturvakäyttäytymisen rakentumisesta.

Mallin ydin koostuu suunnitellusta tietoturvakäyttäytymisestä. Suunniteltu tietoturvakäyttäytyminen tarkoittaa siis kotikäyttäjän aikomusta käyttäytyä turvallisesti (Thomson & von Solms, 1998). Suunniteltuun tietoturvakäyttäytymiseen vaikuttavia tekijöitä löydettiin useita. Ensimmäinen niistä on minäpystyvyys, jolla tarkoitetaan henkilön osaamista sekä uskoa omaan osaamiseen (Anderson & Agarwal, 2010; Rhee, Kim & Ryu, 2009).

Toinen tietoturvakäyttäytymiseen vaikuttavat tekijä on tilanne. Alasuutarin (2016) mukaan tietoturvakäyttäytyminen ei suinkaan aina ole samanlaista, vaan se voi muuttua tilanteen mukaan. Joissain tilanteissa kotikäyttäjä saattaa käyttäytyä turvallisesti, mutta joissain toisissa tilanteissa ollaan valmiita ottamaan riskejä oman turvallisuuden kustannuksella.

Kolmantena tietoturvakäyttäytymiseen vaikuttavana tekijänä tunnistettiin joukko kognitiivisia, sosiaalisia ja psykologisia tekijöitä (Anderson & Agarwal, 2010; Leach, 2003). Näitä tekijöitä ovat esimerkiksi omistussuhteet ja sosiaaliset odotukset.

Kotikäyttäjä joutuu myös arvioimaan tietynlaisen tietoturvakäyttäytymisen mukanaan tuomia hyötyjä ja vertaamaan niitä haittoihin (Beautement ym., 2008). Hyödyt, haitat ja kustannukset ovat siis yksi tietoturvakäyttäytymiseen vaikuttavista tekijöistä.

Tietoturvatietoisuus on selvästi yksi osatekijä tietoturvakäyttäytymisen rakentumisessa, vaikkakin tutkimuksissa on saatu eriäviä tuloksia. Osa tutkimuksista totesi tietoturvatietoisuuden vaikuttavan positiivisesti tietoturvakäyttäytymiseen (Howe ym., 2012; Öğütçü ym., 2016). Osa tutkimuksista puolestaan totesi, että tietoturvatietoisuuden kasvaminen ei paranna tietoturvakäyttäytymistä merkittävästi (Aytes & Connolly, 2004; Edwards, 2015).

Tässä tutkimuksessa tarkasteltiin myös tarkemmin, mistä tietoturvatietoisuus koostuu. Tietoturvatietoisuuden todettiin kotikäyttäjillä koostuvat pääosin

kahdesta eri tekijästä; yksilöllisistä tekijöistä (McCormac ym. (2017) sekä elämänkokemuksesta (Bulgurcu ym., 2010). Tietoturvakoulutus olisi erinomainen tapa vaikuttaa yksilön tietoturvatietoisuuteen, mutta vain todella harvat kotikäyttäjät pystyvät osallistumaan tietoturvakoulutukseen (Li & Siponen, 2011).

Todellinen tietoturvakäyttäytyminen puolestaan tarkoittaa kotikäyttäjän toteutunutta tietoturvakäyttäytymistä. Ideaalitilanteessa suunniteltu tietoturvakäyttäytyminen ja todellinen tietoturvakäyttäytyminen ovat samanlaisia, mutta läheskään aina näin ei ole. On mahdollista, että kotikäyttäjä suunnittelee käyttäytyvänsä tietyllä tavalla, mutta lopulta käyttäytyy toisin. Tämä tarkoittaa sitä, että edellä mainitut tietoturvakäyttäytymiseen vaikuttavat tekijät eivät yksinomaan riitä parantamaan kotikäyttäjän tietoturvakäyttäytymistä.

Avuksi tarvitaan asennetta ja motivaatiota, joilla on havaittu olevan positiivinen vaikutus tietoturvakäyttäytymiseen (Anderson & Agarwal, 2010; Ng & Rahim, 2005). Mutta jos asenne tietoturvaa kohtaan on huono, voidaan olettaa, että todellinen tietoturvakäyttäytyminen ei parane. Voidaankin sanoa, että asenteet ja motivaatio ovat eräänlainen mahdollistaja suunnitellun ja toteutuneen tietoturvakäyttäytymisen välillä.

5 YHTEENVETO

Tässä tutkimuksessa tarkasteltiin kotikäyttäjän tietoturvakäyttäytymistä ja siihen vaikuttavia tekijöitä sekä kotikäyttäjän tietoturvatietoisuutta, sen rakentumista ja sen vaikutuksia tietoturvakäyttäytymiseen. Tutkimus toteutettiin kirjallisuuskatsauksena. Lähteinä käytettiin pääosin aihealueeltaan sopivia ja vertaisarvioituja tieteellisiä tutkimuksia.

Ensimmäisessä luvussa käsiteltiin kotikäyttäjää ja tietoturvaa. Luvussa vastattiin tutkimuskysymykseen: millainen on kotikäyttäjä? Kotikäyttäjä määriteltiin henkilöksi, joka käyttää informaatioteknologiaa, hänen tekniset taitonsa eivät ole kovin hyvät ja hän ei ole saanut työnsä puolesta tietoturvakoulutusta. Tutkimuksessa eriteltiin myös kotikäyttäjälle yleisimpiä tietoturvauhkia ja pohdittiin mistä kyseiset ongelmat johtuvat.

Toisessa luvussa tarkasteltiin kotikäyttäjän tietoturvakäyttäytymistä. Luvussa vastattiin tutkimuskysymyksiin: mitä on tietoturvakäyttäytyminen ja mitkä tekijät siihen vaikuttavat? Tietoturvakäyttäytyminen todettiin jakautuvat suunniteltuun tietoturvakäyttäytymiseen ja todelliseen tietoturvakäyttäytymiseen. Kotikäyttäjän tietoturvakäyttäytymiseen vaikuttavia tekijöitä tunnistettiin olevan: minäpystyvyys, tilanne, kognitiiviset, sosiaaliset ja psykologiset tekijät, hyödyt, haitat ja kustannukset sekä tietoturvatietoisuus.

Kolmannessa ja viimeisessä asialuvussa käsiteltiin kotikäyttäjän tietoturvatietoisuutta. Tietoturvan todettiin tarkoittavan kotikäyttäjän kykyä ymmärtää tietoturvaa, sen ongelmia ja niiden vaikutuksia sekä hahmottaa ratkaisuja tietoturvaongelmiin. Tietoturvatietoisuuden havaittiin koostuvan kotikäyttäjillä usein elämänkokemuksesta ja yksilöllisistä tekijöistä. Tietoturvakoulutuksen havaittiin olevan erinomainen tapa lisätä tietoturvatietoisuutta, mutta kotikäyttäjät eivät yleensä pysty osallistumaan tällaisiin koulutuksiin. Tietoturvatietoisuuden havaittiin vaikuttavan tietoturvakäyttäytymiseen, vaikka saadut tutkimustulokset ovat pienimuotoisessa ristiriidassa keskenään. Lisäksi luvun lopussa esitettiin malli tietoturvakäyttäytymisen rakentumisesta kotikäyttäjällä.

Tämän tutkimuksen rajoitteita ovat juuri kotikäyttäjiin kohdistuvan tieteellisen tutkimuksen vähyys. Useat tutkimukset, joita tässä tutkimuksessa on käytetty lähdemateriaalina tarkastelevat yksilön tietoturvakäyttäytymistä ja

tietoturvatietoisuutta organisaation sisällä. Voidaan kuitenkin olettaa, että kotikäyttäjien osalta tulokset olisivat samansuuntaisia, mutta täyttä varmuutta asiasta ei ole.

Akateemisen tutkimuksen vähyys osoittaa, että suurin kiinnostus tietoturvasektorilla on keskittynyt organisaatioiden tietoturvaan. Tulevaisuudessa kotikäyttäjien tutkiminen tulee olemaan tärkeää monestakin syystä. Ensinnäkin jotta kotikäyttäjien tietoturvallisuutta voidaan kokonaisvaltaisesti parantaa, tulee ensin ymmärtää kotikäyttäjien ongelmat verkossa. Toisaalta tulevaisuudessa yhä useampi laite tulee olemaan kytkettynä verkkoon, jolloin myös riskit tiedon väärinkäytölle kasvavat.

Tieteellisen tutkimuksen vähyys asettaa myös hyvät jatkotutkimusmahdollisuudet tälle tutkimukselle. Tiedonhaku prosessin aikana en löytänyt lainkaan luotettavia empiirisiä tutkimuksia, joissa olisi tarkasteltu kotikäyttäjien kykyä havaita riskejä verkkomaailmassa tai mitattu tietoturvatietoisuuden tasoa.

Kuten edellä todettiin, tämä tutkimus on toteutettu kirjallisuuskatsauksena, joten saatuja tuloksia ei ole voitu varmistaa käytännössä. Lisäksi kirjallisuuskatsaus asettaa tutkimukselle myös muita rajoitteita. On mahdollista, että joitakin asioita, jotka vaikuttavat kotikäyttäjän tietoturvakäyttäytymiseen tai tietoturvatietoisuuteen on jäänyt käsittelemättä tässä tutkimuksessa, koska lähdemateriaalia ei välttämättä ole löydetty. Edellä luetellut tutkimuksen rajoitteet tulee tiedostaa tutkimuksen tuloksia tarkastellessa.

LÄHTEET

Alasuutari, M. (2016). Prosessiteoreettinen näkökulma, joka selittää henkilökohtaisen tietokoneen käyttöön liittyvää tietoturvakäyttäytymisen muutosta. Jyvskylä: University of Jyvskylä.

Anderson, C. L., Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *Management Information Systems : Mis Quarterly, 34*(3), 613-643.

Atzori, L., Lera, A., Morabito, G. (2010). The Internet of Things: A survey, *Computer Networks,* Volume 54, Issue 15, 28 October 2010, Pages 2787-2805, ISSN 1389-1286

Aytes, K., & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing (JOEUC), 16*(3), 22-40.

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (NSPW '08). ACM, New York, NY, USA, 47-58.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548

Dahamija, R., Tygar, J. D., Hearst, M. (2006). Why Phishing Works. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '06), ACM, New York, NY, USA, 581-590.

Edwards, K. (2015). Examining the security awareness, information privacy, and the security behaviors of home computer users. Nova Southeastern University, College of Engineering and Computing. (947)

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., Herley, C. (2013). Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13). ACM, New York, NY, USA, 2379-2388

Florencio, D., Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (WWW '07). ACM, New York, USA, 657-666.

Furnell, S., Tsaganidi, V. & Phippen, A. (2008). Security beliefs and barriers for novice internet users. *Computers & Security, 27*(7–8), 235-240

Furnell, S., Bryant M., P. & Phippen, A. D. (2007). Assessing the security perceptions of personal internet users. *Computers & Security, 26*(5), 410-417

Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal of Computer Virology* (2010) 6: 77.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Howe A. E., Ray I., Roberts M., Urbanska M. & Byrne Z. (2012). The psychology of security for the home computer user, *IEEE Symposium on Security and Privacy 2012.*

Kritzinger, E., von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

Leach, J. (2003). Improving User Security Behavior. *Computers & Security,* 22(8), 685-692.

Li, Y., Siponen, M. (2011) A Call For Research On Home Users' Information Security Behaviour. PACIS 2011 Proceedings, 112

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156

Mercaldo F., Nardone V., Santone A., Visaggio C.A. (2016) Ransomware Steals Your Phone. Formal Methods Rescue. FORTE 2016: Formal Techniques for Distributed Objects, Components, and Systems. 212-221.

Ng, B.Y., Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. PACIS 2005 Proceedings. 20.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers & Security, 31(5), 673-680

Pattinson M., Butavicius M., Parsons K., McCormac A., Calic D. (2015) Factors that Influence Information Security Behavior: An Australian Web-Based Study. *Human Aspects of Information Security, Privacy, and Trust,* HAS 2015, 231-241

Rhee, H., Kim, C. & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826

Siponen, M. (2001) Five dimensions of information security awareness. *Computers and society, 31(2)*, 24-29

Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. ISSN=2341-8699. 2016, Liitetaulukko 9. Internetin käyttö ja käytön useus 2016, %-osuus väestöstä . Helsinki: Tilastokeskus [viitattu: 13.2.2017]. Saantitapa: http://www.stat.fi/til/sutivi/2016/sutivi_2016_2016-12-09_tau_009_fi.html

Symantec, (2016). ISTR, Internet security thread report, volume 21, april 2016. [viitattu 13.2.2017]. Saantitapa :https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Thomson, M. E. & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173

Viestintävirasto, (2017). Tietoturvan vuosi 2016. [viitattu 14.2] Saantitapa : https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102

Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security. Boston, United States of America: Course technology, Cengage learning

Xia, F., Yang, L. T., Wang, L. and Vinel, A. (2012), Internet of Things. *International Journal of Communication Systems*., 25: 1101–1102.

Öğütçü, G., Testik, Ö. M., Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.