Ada Jakosuo

KOTIKÄYTTÄJÄN TIETOTURVAKÄYTTÄYTYMISEEN VAIKUTTAVAT TEKIJÄT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Jakosuo, Ada
Kotikäyttäjän tietoturvakäyttäytymiseen vaikuttavat tekijät
Jyväskylä: Jyväskylän yliopisto, 2022, 26 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Riekkinen, Janne

Teknologian nopea kehitys on johtanut siihen, että informaatioteknologian käyttö on arkipäiväistynyt ihmisten jokapäiväisessä elämässä. Kuitenkaan ihmisten osaaminen ja tietoturvatietoisuus eivät ole pysyneet tässä kehityksessä mukana, joka on ongelmallista alati lisääntyvien tietoturvauhkien vuoksi. Tässä kirjallisuuskatsauksessa määritellään, millainen on kotikäyttäjä tietoturvan kontekstissa, sekä tarkastellaan tietoturvakäyttäytymiseen vaikuttavia tekijöitä. Tutkimuskirjallisuus osoitti, että käyttäjän merkittävimmät tietoturvakäyttäytymiseen vaikuttavat tekijät ovat tietoturvatietoisuus, asenne, minäpystyvyys, subjektiiviset ja kuvailevat normit sekä käyttäjän aiemmat kokemukset. Olemassa oleva tietoturvatutkimus on keskittynyt lähinnä organisaatiokontekstiin, mutta myös kotikäyttäjien tietoturvaa tulisi tutkia, sillä etätyöskentely on yhä yleisempää ja tietoturva on pitkälti riippuvainen käyttäjästä.

Asiasanat: tietoturva, tietoturvakäyttäytyminen, kotikäyttäjä,
suojelumotivaatioteoria

ABSTRACT

Jakosuo, Ada
Factors Affecting Home User Security Behavior
Jyväskylä: University of Jyväskylä, 2022, 26 p.
Information Systems, Bachelor's Thesis
Supervisor: Riekkinen, Janne

The rapid development of technology has led to the use of information technology becoming more commonplace in people's daily lives. However, people's skills and security awareness have not kept pace with this development, which is problematic due to increasing security threats. This literature review defines the home user in a security context and examines the factors that affect security usage. The literature research showed that the most significant factors influencing a user's security behavior are information security awareness, attitude, self-efficacy, subjective and descriptive norms, and the user's previous experiences. Existing security research has focused on the organizational context, but the security of home users should also be explored, as remote working is becoming more common and information security is highly user dependent.

Keywords: information security, cybersecurity, information security behavior, home user, protection motivation theory

KUVIOT

SISÄLLYS

1 JOHDANTO

Informaatioteknologian käytöstä on tullut erottamaton osa ihmisten jokapäiväistä elämää. Tekniikan nopeasta kehityksestä huolimatta, käyttäjien kohtaamat tietoturvaongelmat ovat edelleen merkittävässä roolissa niin organisaatio- kuin kotikontekstissa. ENISA:n (2021) uhkaraportin mukaan Covid-19 pandemian seurauksena haitalliset toimijat kohdistivat yhä enemmän monimutkaisia hyökkäyksiä kotiverkkoihin. Muun muassa palvelunestohyökkäykset lisääntyivät vuonna 2020 1,6 miljoonalla ja kiristyshyökkäykset 125 prosentilla verrattuna vuoteen 2019. Myös tahattomat tapaukset kasvoivat vuosina 2020 ja 2021, kun Covid-19-pandemiasta tuli inhimillisten virheiden kerrannaistekijä ja suurin osa tietoturvaloukkauksista johtui tietokoneen käyttäjien virheistä. (ENISA, 2021). Tietoturvallisuutta pidetäänkin usein ihmiskysymyksenä ja ihminen on yleensä tietoturvan heikoin lenkki (White, Ekin & Visinescu, 2017).

Tietoturvakäyttäytymisen tutkimuksen tärkeys on tunnistettu viimeisen vuosikymmenen aikana ja tukijat ovat pyrkineet ymmärtämään aihetta useista teoreettisista näkökulmista. Perinteisesti tietoturvakäyttäytymisen tutkimus on keskittynyt työntekijöihin ja organisaatiokontekstiin. Teknologian kehitys on kuitenkin muuttanut ihmisten tapaa työskennellä ja olla yhteydessä toisiinsa ja esimerkiksi etätyöskentely on lisääntynyt merkittävästi viimeisten vuosien aikana. Kotitietokoneet ovat kehittymässä tuottavuustyökaluista niin sanotuiksi elämänhallintakeskuksiksi ja monet kotitietokoneet ovat myös kodin ulkopuolisten palvelimien hallinnassa ja vuorovaikutuksessa muiden verkkojen kanssa. Lisääntyneestä Internetin ja informaatioteknologian kulutuksesta huolimatta, ihmisillä ei ole tarpeeksi tietoa turvallisuusuhista tai suositelluista tietoturvatoimista.

Vaikka tekninen valvonta on välttämätöntä, tietoturvallisuus riippuu lopulta yksilöiden turvallisuuskäyttäytymisestä (Ng, Kankanhalli & Xu, 2009). Tästä syystä on tärkeää selvittää, mitkä tekijät vaikuttavat ihmisen harjoittamaan tietoturvakäyttäytymiseen.

Tämän kirjallisuuskatsauksen tavoitteena on saada vastaus seuraaviin tutkimuskysymyksiin:

- Millainen on kotikäyttäjä tietoturvan kontekstissa?
- Mitkä tekijät vaikuttavat kotikäyttäjän tietoturvakäyttäytymiseen?

Tutkielman ensimmäinen luku käsittelee tietoturvaa erityisesti kotikäyttäjän näkökulmasta. Luvussa määritellään tietoturva, tietoturvauhka ja kotikäyttäjä, sekä esitetään tyypillisimmät kotikäyttäjän kohtaamat tietoturvauhat. Tässä luvussa vastataan tutkielman ensimmäiseen tutkimuskysymykseen ”Millainen on kotikäyttäjä tietoturvan kontekstissa?”.

Tutkielman toisessa luvussa taas syvennytään tietoturvakäyttäytymiseen. Luvussa paneudutaan tietoturvakäyttäytymisen määritelmään yleisellä tasolla ja teoreettiselta pohjalta suojelumotivaatioteorian näkökulmasta. Kolmas luku käsittelee tietoturvakäyttäytymiseen vaikuttavia tekijöitä, eli kyseisessä luvussa vastataan tutkielman toiseen tutkimuskysymykseen. Viimeinen osuus tutkielmasta käsittää yhteenvedon, jossa tiivistetään tutkielman havainnot ja vastataan kertaalleen tutkimuskysymyksiin. Yhteenvedossa esitetään myös jatkotutkimusehdotus sekä perustellaan aiheen tutkimuksen tärkeys.

Tutkielma on toteutettu kirjallisuuskatsauksena ja tutkimusaineistoa on haettu pääasiassa Google Scholar -palvelusta ja Jykdokin tietokannoista. Hakusanoina on käytetty muun muassa seuraavia;” information security”,” information security behavior”, ”information security awareness”, ”information security” ja “home user”. Tutkielman lähdemateriaalina on pyritty käyttämään mahdollisimman tuoreita ja relevantteja tieteellisiä artikkeleita ja tutkimuskirjallisuutta.

2 TIETOTURVA

Tässä luvussa määritellään tietoturvan ja tietoturvauhan lisäksi kotikäyttäjä tietoturvan kontekstissa, sekä käsitellään yleisimpiä yksilöön kohdistuvia tietoturvauhkia. Tietoturvan käsite on tärkeä määritellä, jotta voidaan ymmärtää ihmisen tietoturvakäyttäytymistä.

2.1 Tietoturva ja tietoturvauhka

Tietoturva on tiedon ja tietojärjestelmien suojaamista luvattomalta käytöltä, häiriöiltä, paljastamiselta, muuttamiselta tai tuhoamiselta luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi (Guttman & Roback, 1995). Mattordin ja Whitmanin (2012) mukaan tietoturva on tiedon, järjestelmien ja laitteiston suojaamista niiden toimesta, jotka käyttävät, tallentavat ja välittävät kyseistä tietoa.

Tietoturvaa määriteltäessä puhutaan usein myös kolmesta tiedon ominaisuudesta, joita ovat luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Nämä tunnetaan myös tietoturvan kulmakivinä (C.I.A triangle). Tiedon luottamuksellisuudella tarkoitetaan sitä, että vain luvan saaneet henkilöt voivat nähdä tietyn tiedon. Kun tiedot ovat suojattu paljastamiselta, ovat ne tällöin luottamuksellisia. Tieto on eheää, kun se on kokonaista, täydellistä ja korruptoimatonta. (Mattord & Whitman, 2012). Tietoa käyttävien ihmisten tulee siis voida luottaa tietojen aitouteen ja siihen, ettei niitä ole esimerkiksi muokattu ilman lupaa. Saatavuus taas mahdollistaa valtuutettujen henkilöiden tai tietojärjestelmien päästä käsiksi tietoihin ilman häiriöitä tai esteitä ja vastaanottaa ne vaaditussa muodossa (Mattord & Whitman, 2012). Jos tietojärjestelmä ei pysty tarjoamaan sen lupaamaa tietoa, on saatavuus tällöin estetty ja turvallisuutta loukattu.

Vaikka C.I.A kolminaisuuden elementit ovatkin tärkeitä ja niitä tulee suojella tiedon turvaamiseksi, on kyseistä mallia kuitenkin arvosteltu sen kyvyttömyydestä perustella nopeasti muuttuvia turvallisuusvaatimuksia. Whitman ja Mattord (2012) ovat esittäneet tähän ongelmaan ratkaisun, jossa mallia

laajennetaan lisäämällä siihen uusia tiedon ominaisuuksia, joita täytyy ottaa huomioon ja suojeltava tietoturvan toteutumiseksi. Näitä ominaisuuksia ovat; tiedon tarkkuus (accuracy), aitous (authenticity), käyttökelpoisuus (utility) ja hallinta (possession). Tiedon tarkkuus merkitsee sitä, että tieto on virheetöntä sekä vastaa käyttäjän odotuksia. Tiedon aitoudella tarkoitetaan tiedon alkuperäisyyttä, kopioimattomuutta ja jäljittelemättömyyttä. Tieto on käyttökelpoista, kun tietoa voidaan käyttää tarkoituksenmukaisesti. Tiedon hallinnalla taas tarkoitetaan sitä, että tiedolla on omistaja tai se on muilla tavoin kontrolloitua (Whitman & Mattord, 2012).

Perinteistä tietoturvan mallia ovat haastaneet myös Yin, Fang, Guo, Sun ja Tian (2020), jotka jakavat tietoturvan neljään eri kerrokseen: fyysiseen, toiminnalliseen, data- ja sisältöturvallisuuteen. Näistä kahden ensimmäisen kerroksen turvallisuus riippuu todennuksesta ja käytettävyydestä palvelujen näkökulmasta. Kolmas kerros taas nojaa tietojen luottamuksellisuuteen, autentikointiin ja saatavuuteen datan itsensä näkökulmasta ja neljäs kerros riippuu ohjattavuudesta, saatavuudesta ja todennuksesta käytön kannalta. Heidän mukaansa tietoturva on prosessi, jolla varmistetaan, että järjestelmät tarjoavat odotetun palvelun suojaamalla käytettävyyttä ja todennusta järjestelmäkerroksessa. Prosessi varmistaa, että tiedot lähetetään ja vastaanotetaan oikein suojaamalla luottamuksellisuus, saatavuus ja todennus tietokerroksessa. Prosessin tulee myös suojata odotetulla tavalla käytettävää tietoa varmistamalla käyttötasojen saatavuus, ohjattavuus ja todennus. (Yin ym., 2020).

Sanastokeskuksen (2018) mukaan kyberuhka tai tietoturvauhka on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua toteutuneista tietoturvauhkista tai digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista. Kyberuhkat voivat kohdistua yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin tai kansalaisiin, joko suoraan tai välillisesti.

2.2 Kotikäyttäjä tietoturvan kontekstissa

Koska käsittelen tässä tutkielmassa erityisesti kotikäyttäjän tietoturvaa, on tarpeellista eritellä kotikäyttäjän ja työntekijän erot informaatioteknologian käyttäjinä. Kritzinger & Solms (2010) ovat määritelleet kotikäyttäjän on henkilöksi, jonka ikä ja tekninen tietämys voi vaihdella, ja joka käyttää tietokonetta ja Internetiä missä tahansa työympäristön ulkopuolella ja on vastuussa tietokoneensa suojaamisesta ja päivittämisestä. Kotikäyttäjien ei välttämättä tarvitse hankkia tietoturvatietoa tai -koulutusta, elleivät he itse halua.

Informaatioteknologian käyttäjiä voidaan kuitenkin jaotella myös heidän osaamistasonsa mukaan, kuten Furnell, Bryant & Phippen (2007) tekivät tutkimuksessaan. He jakoivat käyttäjät osaamistasonsa mukaan noviiseihin, keskitasoisiin ja edistyneisiin. Kritzinger & Solms (2010) esittivät tutkimuksessaan, että

kotikäyttäjien ja ei-kotikäyttäjien määritelmät voivat niin sanotusti limittyä keskenään, joka tarkoittaa sitä, että käyttäjä voi esimerkiksi käyttää informaatioteknologiaa sekä kotona, että organisaatioympäristössä. Kyseisiin tutkimuksiin nojaten voidaan siis todeta, että käyttäjät voivat olla joko kotikäyttäjiä, ei-kotikäyttäjiä tai molempia, ja jokainen näistä käyttäjäryhmistä voi olla tasoltaan noviisi, keskitasoinen tai edistynyt. Tässä tutkielmassa pyritään tarkastelemaan erityisesti noviiseja sekä keskitasoisia kotikäyttäjiä.

Kotikäyttäjän tietoturvakäyttäytymistä tutkittaessa ei voida täysin soveltaa samoja kysymyksiä, kuin työntekijän tietoturvakäyttäytymisen tutkimuksessa. Kotikäyttäjä ei esimerkiksi ole yleensä saanut tietoturvakoulutusta, tietoturvan toteutumista kotona ei valvota, eikä käyttäjällä ole IT-tukea apunaan ongelmatilanteissa, toisin kuin organisaatioympäristössä (Anderson & Agarwal, 2010). Organisaatiot ovat panostaneet tietoturvaan huomattavan paljon aikaa, rahaa ja huomiota, joka on johtanut myönteisiin tuloksiin (Dupuis, Crossler & Endicott-Popovsky, 2012). Organisaatioiden panostukset sisältävät investointeja tietoturvakoulutukseen ja -tietoisuusohjelmiin, mutta samanlaisia panostuksia ei ole tehty kotikäyttäjille (Crossler & Bélanger, 2009). Kotikäyttäjät eivät ole homogeeninen ryhmä, eikä useimmilla heistä ole organisoituja keinoja saada tietoturvakoulutusta, tai -tietoisuutta. Lisäksi on olemassa vain vähän tietoa siitä, mitä tehokas tietoturvakasvatus, -koulutus ja -tietoisuus kotikäyttäjälle tarkoittaisi. Ennen kuin tiedetään konkreettisempaa tietoa heidän käyttäytymistään liittyvistä ominaisuuksista, on haastavaa ja todennäköisesti turhaa käyttää merkittäviä resursseja kotikäyttäjien tietoturvakoulutukseen, ja -tietoisuusohjelmiin.

Jokainen tietokoneen käyttäjä edustaa päätepistettä tietokoneverkossa tai tietojärjestelmässä, ja ilman kunkin käyttäjän tietoturvan mukaista käyttäytymistä, verkko ei ole turvallinen. Turvallisia toimia ovat muun muassa säännöllinen varmuuskopiointi, salasanojen vaihtaminen, sovellusten päivittäminen, palomuurien määrittäminen ja virusohjelmien käyttäminen (Whitman, 2003; Rosenthal, 2002). Tietoturvatiedon puute on usein yksi suurimmista riskeistä, jolle kotikäyttäjät altistuvat informaatioteknologiaa käyttäessään ja yksityishenkilöt altistuvatkin yhä useammin tietoturvauhille käyttäessään Internetiä kotitietokoneillaan (Furnell ym., 2007).

2.3 Kotikäyttäjiin kohdistuvat tietoturvauhat

Kyberrikollisuuden kehittyminen ja monipuolistuminen on ollut huomattavaa digitaalisessa toimintaympäristössä. Tietoverkkoihin sekä tietojärjestelmiin kohdistuvien hyökkäysten, tietoturvaloukkausten sekä haittaohjelmatartuntojen määrä on kasvanut merkittävästi. Pelkästään haittaohjelmien määrä on lisääntynyt 100 miljoonasta yli 1,1 miljardiin vuosien 2012 ja 2020 välisenä aikana. (Neittaanmäki, Lehto & Savonen, 2021). Liikenne- ja viestintäviraston kyberturvallisuuskeskus on listannut vuoden 2021 yleisimmiksi tietoturvauhiksi huijaukset, tietojenkalastelun sekä haittaohjelmat. Nurse (2018) jakaa yksilöihin kohdistuvat tietoturvarikokset neljään kategoriaan;

2.3.1 Sosiaalinen manipulointi ja verkkohuijaukset

Järjestelmiä voidaan hyödyntää petoksissa ”automatisoimalla” perinteisiä petosmenetelmiä tai hyödyntämällä uusia menetelmiä. Petoksia voivat tehdä niin sanotut sisäpiiriläiset, eli valtuutetut käyttäjät tai ulkopuoliset. Sosiaalinen manipulointi on tekniikka, jota käytetään tietojenkalastelussa (phishing). Sosiaalinen manipulointi perustuu ihmisen vuorovaikutukseen, jotta yksilö saataisiin rikkomaan suojausprotokollaa ja rohkaisemaan henkilöä paljastamaan luottamuksellisia tietoja. Tällaiset hyökkäykset tehdään yleensä puhelimitse tai verkossa. (Nieles, Dempsey & Pillitteri, 2017)

Tietojenkalastelu tapahtuu käyttämällä sähköistä viestintää, kuten sähköpostia tai verkkosivustoa. Siinä rikollinen lähettää sähköpostin tai luo verkkosivuston, joka näyttää legitiimiltä, tarkoituksenaan houkutella henkilöitä paljastamaan arkaluontoisia tietoja tai suorittamaan haluttuja toimia. Kohdennettu tietojenkalasteluhyökkäys (spear-phishing), on räätälöity muiden tärkeiden ja asiaankuuluvien tietojen, kuten syntymäajan, pankin, Internet-palveluntarjoajan tai sähköpostiosoitteen perusteella. Tätä lisätietoa käytetään parantamaan legitimiteettiä ja siten lisäämään huijauksen tehokkuutta. (Nurse, 2018).

2.3.2 Identiteettivarkaudet

Identiteettivarkauksissa rikolliset keräävät tietoja henkilöistä ja käyttävät sitä perustana heidän henkilöllisyytensä varastamiseen. Kyberrikolliset suosivat yleensä kahta tiedonkeruutekniikkaa, joista toinen on henkilöiden seuraaminen sosiaalisessa mediassa, kun he tekevät julkaisuja ja ovat vuorovaikutuksessa verkossa. Toisen tekniikan avulla henkilötietoja kerätään aikaisemmista tietoturvaloukkauksista. Ensimmäisessä tekniikassa hyödynnetään tietojenkalasteluun henkilön heikkoa tietoturvan ja yksityisyyden hallintaa. (Nurse, 2018).

2.3.3 Hakkerointi

Hakkerointi on yksi perinteisimmistä kyberrikollisuuden muodoista, ja se sisältää toimintoja, jotka johtavat tietokonejärjestelmien ja digitaalisen tiedon vaarantumiseen. Hakkerointiprosessissa Internetiä skannataan, jotta päästäisiin huonosti suojattuihin sekä väärin määritettyihin järjestelmiin. Kun järjestelmä on saastutettu, hakkeri voi etäohjata tartunnan saaneen järjestelmän ja lähettää komentoja, jotta järjestelmä toimisi hyökkääjien vakoojana ja muiden järjestelmien häiritsemisessä. (Uma & Padmavathi, 2011).

Hakkeroinnin alle lukeutuu monia eri rikoksia, joista yleisimpänä ovat haittaohjelmat. Haittaohjelmat ovat sovelluksia, jotka rikolliset ovat kehittäneet ja joita he käyttävät vaarantaakseen järjestelmien tietojen luottamuksellisuuden tai eheyden. Vuonna 2017 Symantec raportoi uusien haittaohjelmatyyppien lisääntymisestä verkossa kolminkertaiseksi, kun taas vuonna 2018 uusien haittaohjelmatyyppien määrä nousi 88 %. Yleisimmin yksityishenkilöihin käytettyjä haittaohjelmatyyppejä ovat virukset, madot, Troijan hevoset sekä vakoiluohjelmat.

Kiristyshaittaohjelma (ransomware) on haitallista koodia, joka estää tai rajoittaa pääsyä järjestelmään lukitsemalla koko näytön tai salaamalla tiettyjä tiedostoja, kunnes lunnaat maksetaan. Kiristyshaittaohjelmahyökkäyksiä on kahta eri tyyppiä – salaajia ja säilytyskaappeja. Salaajat estävät järjestelmätiedostot ja vaativat maksua näiden tiedostojen eston poistamiseksi. Kaapit on suunniteltu lukitsemaan käyttäjät käyttöjärjestelmistä. Käyttäjillä on edelleen pääsy laitteeseen ja muihin tiedostoihin, mutta tartunnan saaneen tietokoneen lukituksen avaamiseksi käyttäjää pyydetään maksamaan lunnaita. Lunnaiden maksu ei kuitenkaan takaa sitä, että hyökkääjä avaisi tartunnan saaneen järjestelmän. (Nieles, Dempsey & Pillitteri, 2017).

Haittaohjelmien lisäksi tilien ja salasanojen hakkerointi on yleistynyt kyberuhka yksilöille ja se on kyberrikollisten käyttämien tekniikoiden ansiosta usein jopa automatisoitua. Rikolliset hakkeroivat tilit tyypillisesti varastamalla käyttäjien salasanoja ja käyttäjätunnuksia, esimerkiksi asentamalla uhrin tietokoneeseen haittaohjelman, joka kirjaa kaikki näppäimistössä tapahtuvat painallukset talteen tai käyttämällä sosiaalisen manipuloinnin tekniikoita. (Nurse, 2018).

2.3.4 Palvelunestohyökkäykset

Palvelunestohyökkäykset (Distributed Denial of Service, DDoS) kohdistuvat järjestelmän ja tiedon saatavuuteen. Palvelunestohyökkäyksessä hyökkääjä lähettää suuren määrän yhteys- tai tietopyyntöjä kohteeseen. Pyyntöjä tehdään niin paljon, että kohdejärjestelmä ylikuormittuu, eikä pysty vastaamaan laillisiin palvelupyyntöihin. Järjestelmä saattaa kaatua tai yksinkertaisesti epäonnistua tavallisten toimintojen suorittamisessa. (Mattord & Whitman, 2012).

ENISA:n (2021) uhkaraportin mukaan perinteiset palvelunestohyökkäykset ovat siirtymässä kohti mobiiliverkkoja ja esineiden Internetiä (IoT), joka asettaa myös kotikäyttäjät yhä alttiimmaksi kyseiselle uhalle. Liikenne- ja viestintävirasto Traficom (2020) totesi tietoturvaraportissaan, että runsas etätöihin siirtyminen vuoden 2020 keväällä toi esiin palvelunestohyökkäysten vaikutukset organisaatioiden sisäisiin palveluihin, kuten Skypeen ja VPN-ratkaisuihin.

3 TIETOTURVAKÄYTTÄYTYMINEN

Tässä luvussa määritellään tietoturvakäyttäytyminen sekä esitellään laajasti tietoturvatutkimuksessa käytetty teoria. Lopuksi tarkastellaan kyseistä teoriaa tietoturvakäyttäytymisen tutkimuksessa.

3.1 Tietoturvakäyttäytymisen määritelmä

Koska ihmisen tietoturvakäyttäytymisen tutkimus on kompleksi ja laaja aihe, ei sille ole olemassa universaalisti hyväksyttyä määritelmää. Tietoturvakirjallisuudessa tietoturvakäyttäytyminen voidaan luokitella kontekstinsa mukaan, eli organisaatiokäytön tai ei-työkäytön mukaan. Vaikka tietoturvakäyttäytymisessä voi olla yhtäläisyyksiä työympäristön ja kodin välillä, on niiden erot kuitenkin hyvä tunnistaa, jotta kotikontekstia koskeva tutkimus voi kehittyä (Li & Siponen, 2011). Usein tietoturvakirjallisuudessa tietoturvakäyttäytyminen on määritelty kuvaamalla suositeltua turvallisuuskäyttäytymistä. Suositeltavat turvatoimet ovat yleisesti hyväksyttyjä tietoturvatoimia, joilla pyritään tehostamaan ihmisten tietoturvaa.

Padayacheen (2012) mukaan tietoturvakäyttäytyminen tarkoittaa joukkoa keskeisiä tietoturvatoimintoja, joita loppukäyttäjien on noudatettava ylläpitääkseen tietoturvakäytäntöjen määrittelemää tietoturvaa. Yksittäiset tietoturvatoimet voivat olla esimerkiksi virustorjuntaohjelmistojen ja palomuurin käyttämistä, laitteiden ja ohjelmistojen päivittämistä, tuntemattomista lähteistä tulevien sähköpostien epäilyä ja tehokkaiden salasanojen käyttämistä sekä niiden suojaamista (Anderson & Agarwal, 2010).

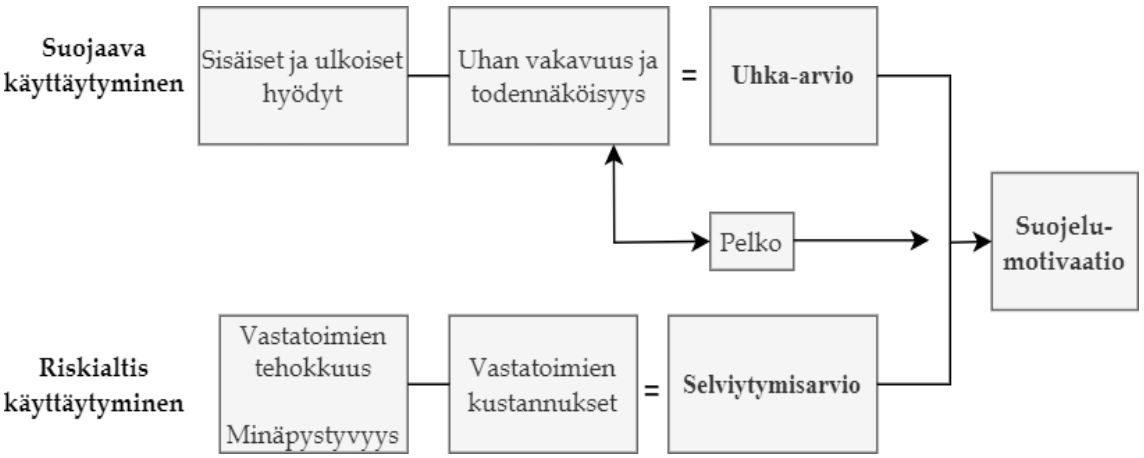
Tässä tutkielmassa tietoturvakäyttäytymisellä tarkoitetaan tapaa, jolla käyttäjä toimii työpaikan ulkopuolella tietoverkoissa, tietokoneella tai älypuhelimella ja kuinka hän ottaa huomioon tietoturvan ylläpitämisen.

3.2 Teoreettinen malli tietoturvakäyttäytymiselle

Suojelumotivaatioteoria (Rogers, 1975, 1983) on luotu selittämään ihmisen reaktiota uhkaan tai vaaraan ja niitä toimintatapoja, joita ihminen valitsee kohdatessaan uhan. Suojelumotivaatioteorian mukaan ihmiset suojelevat itseään kahden kognitiivisen prosessin avulla, joita ovat uhka-arvio (Threat Appraisal) ja selviytymisarvio (Coping Appraisal). Näiden prosessien välityksellä tieto uhasta käynnistää suojelumotivaation, eli aikomuksen suojautua uhalta. Kuviossa 1 esitellään suojelumotivaatioteoria kaavion muodossa.

Uhka-arvioprosessissa arvioidaan riskialttiin käyttäytymisen aloittamista tai sen jatkamista. Tässä prosessissa uhan vakavuutta sekä sen toteutumisen todennäköisyyttä verrataan kyseessä olevaan käyttäytymiseen liittyviin hyötyihin. Uhka-arvioprosessi koostuu: 1) havaitun uhan vakavuudesta, 2) uhan toteutumisen todennäköisyydestä sekä 3) sisäisistä ja ulkoisista palkinnoista, joita voi olla esimerkiksi henkilökohtainen tyytyväisyys tai sosiaalinen hyväksyntä ikätovereilta. Mikäli uhan vakavuuden ja todennäköisyyden merkitys ylittää käyttäytymisestä saatavat hyödyt, arvioidaan sen madaltavan riskialttiin käyttäytymisen todennäköisyyttä. Jos taas käyttäytymisestä saatavat hyödyt koetaan tärkeämmiksi, todennäköisyys riskialttiiseen käyttäytymiseen kasvaa. (Rogers, 1983).

Selviytymisarvioprosessissa arvioidaan uhalta suojautumiseen ryhtymistä ja suojaavan käyttäytymisen omaksumista. Myös selviytymisarvioprosessi perustuu kolmeen tekijään: 1) minäpystyvyyteen, 2) vastatoimien tehokkuuteen ja 3) kustannuksiin. Minäpystyvyydellä viitataan henkilön käsitykseen omasta kyvystään suorittaa suojaavaa käyttäytymistä. Vastatoimien tehokkuus tarkoittaa henkilön arviota vastatoimien tehokkuudesta uhalta suojautumiseksi. Kustannuksilla taas viitataan suojakäyttäytymisestä aiheutuviin kustannuksiin, kuten suojaavan käyttäytymisen vaikeuteen tai siihen kuluvaan aikaan. Jos henkilö uskoo, että hänellä on kyky ryhtyä tarvittaviin toimiin, suojaava käyttäytyminen on tehokasta ja vastatoimien kustannukset ovat kohtuulliset, ryhtyy hän todennäköisemmin suojaavaan käyttäytymiseen. (Rogers, 1983).



KUVIO 1 Suojelumotivaatioteoria (mukaillen Rogers, 1983)

3.3 Suojelumotivaatioteoria tietoturvatutkimuksessa

Alun perin Rogersin (1975) kehittämää suojelumotivaatioteoriaa on käytetty jo pitkään tietoturvakäyttäytymisen tutkimuksessa. Usein sitä on tosin muokattu tai yhdistetty muiden teorioiden kanssa, koska yksinään suojelumotivaatioteoria ei pysty täysin ennustamaan henkilön tietoturvakäyttäytymistä.

Tsai ym. (2016) tutkivat muokatun suojelumotivaatioteorian avulla käyttäjien turvallisuusaikeita. Tutkimuksessa selvitettiin, kuinka alkuperäiset ja uudet suojelumotivaatioteorian muuttujat ennustivat turvallisuusaikeita. Selviytymisarviomuuttujat olivat tutkimuksen mukaan vahvimpia turvallisuusaikeiden ennustajia, erityisesti tottumuksen vahvuus, vastatoimien tehokkuus ja henkilökohtainen vastuu. Uhan vakavuus oli myös merkittävä ennustaja. Uusien muuttujien (aiemmat kokemukset, subjektiiviset normit, tottumuksen vahvuus, koettu turvallisuustuki ja henkilökohtainen vastuu) lisääminen alkuperäiseen suojelumotivaatiomalliin lisäsi mallin selittävyyttä 15 %.

Woon, Tan ja Low (2005) tekivät tutkimuksen kodin langattoman verkon turvallisuudesta, jossa he käyttivät suojelumotivaatioteoriaa teoreettisena perustana. Tutkimustulokset osoittivat, että minäpystyvyys, vastatoimien tehokkuus, vastatoimien kustannukset sekä uhan havaittu vakavuus olivat tärkeimmät käyttäytymisen ennustajat. Toisaalta he osoittivat myös, että havaittu haavoittuvuus ei ollut merkittävä suojaavan käyttäytymisen ennustaja.

Tu ym. (2015) puolestaan tutkivat, kuinka ihmiset kehittävät selviytymis- ja uhka-arvioita mobiililaitteiden katoamisen tai varkauksien suhteen. Tutkimuksessaan he yhdistivät suojelumotivaatioteoriaa sekä sosiaalisen oppimisen teoriaa. Tulokset osoittivat, että käyttäjien aikomuksiin ryhtyä vastatoimiin vaikuttivat heidän arvionsa uhista, uskomuksista omaan kykyyn käyttää vastatoimia, sekä arviot vastatoimien tehokkuudesta.

Suojelumotivaatioteoriaa on hyödynnetty paljon myös työntekijöiden turvallisuuskäyttäytymisen tutkimuksessa. Vance, Siponen ja Pahnila (2012) yhdistivät suojelumotivaatioteorian ja tavan (rutinoitunut aikaisemman käytöksen muoto) tutkiakseen työntekijöiden tietoturvakäytäntöjen noudattamista. Empiirinen testi osoitti, että tavanomaisen tietoturvan noudattaminen vahvisti voimakkaasti suojelumotivaatioteorian kognitiivisia prosesseja, sekä työntekijöiden aikomusta noudattaa prosesseja tulevaisuudessa. Tutkimuksesta kävi myös ilmi, että lähes kaikki suojelumotivaatioteorian osat vaikuttivat merkittävästi työntekijöiden aikomukseen noudattaa tietoturvakäytäntöjä.

Suojelumotivaatioteoriaa on myös kritisoitu, koska se ei huomioi riittävästi pelkoa välittävien viestien aikaansaamia tunnereaktioita (Tanner ym., 1991). Tannerin ym. (1991) mukaan alkuperäinen suojelumotivaatioteoria keskittyy pelon sijaan ainoastaan kognitiivisiin tekijöihin ja että sen ennustuskyky paranisi, jos mallissa tunnistettaisiin myös tunneperäisten prosessien merkitys uhka-arvioiden tekemisessä.

4 TIETOTURVAKÄYTTÄYTYMISEEN VAIKUTTAVAT TEKIJÄT

Tässä luvussa eritellään lähdekirjallisuuden perusteella merkittävimpiä tietoturvakäyttäytymiseen vaikuttavia tekijöitä.

4.1 Tietoturvatietoisuus

Tietoturvatietoisuus on yksilön tietämystä tietyistä turvallisuusuhkista ja mahdollisista vastatoimenpiteistä niitä vastaan (Siponen, 2000; Thomson & von Solms, 1998). Siponen (2000) määritteli tietoturvatietoisuuden tilaksi, jossa organisaation alaiset käyttäjät ovat tietoisia ihanteellisesti sitoutumisesta turvallisuustehtävistään. Vaikka kyseinen määritelmä onkin suunnattu organisaatioympäristöön, se on silti hyödyllinen kotikäyttäjän kontekstissa. Hanus ja Wu (2016) toteavat käyttäjän sitoutuneisuuden tärkeäksi osaksi tietoturvatietoisuutta.

Bulgurcu ym. (2010) määrittelee tietoturvatietoisuuden yleiseksi tietämykseksi ja ymmärrykseksi turvallisuusongelmista ja niiden potentiaalisista seurauksista, sekä organisaatioiden asettamista vaatimuksista tietoturvakäytäntöjä koskien. Tsohou ym. (2015) taas käsittää tietoturvatietoisuuden prosessina, jonka tarkoituksena on muuttaa yksilöiden käsityksiä, arvoja, asenteita, käyttäytymistä, normeja, työtapoja sekä organisaatiokulttuuria ja rakenteita tietoturvakäytäntöjä koskien.

Hanus ja Wu (2016) tutkivat tietoturvatietoisuuden vaikutusta turvallisuuskäyttäytymiseen hyödyntäen suojelumotivaatioteoriaa. Tutkimuksen tulokset osoittivat, että tietoturvatietoisuus vaikuttaa merkittävästi koettuun uhan vakavuuteen, vastatoimien tehokkuuteen, minäpystyvyyteen ja vastatoimien kustannuksiin. Selviytymisarvioprosessin osatekijät puolestaan havaittiin vaikuttavan merkittävästi suositeltuun tietoturvakäyttäytymiseen.

4.2 Minäpystyvyys

Minäpystyvyydellä tarkoitetaan ihmisen arvioita tai uskomuksia omista kyvyistään suorittaa jokin tehtävä (Bandura, 1986). Ihmisillä, joilla on korkea minäpystyvyys, on vahvempi itseluottamus kyvystään motivoida kognitiivisia resursseja ja toimintatapoja, joita tarvitaan tehtävän menestyksekkääseen suorittamiseen (Stajkovic ja Luthans, 1998).

Tietoturvan kolme keskeistä attribuuttia ovat luottamuksellisuus, eheys ja saatavuus (Smith, 1989), joiden perusteella Rhee, Kim ja Ryu (2009) ovat määritelleet minäpystyvyyden tietoturvakontekstissa uskoksi omaan kykyyn suojella tietoja ja tietojärjestelmiä luvattomalta paljastamiselta, muuttamiselta, katoamiselta, tuhoutumiselta ja saatavuuden puutteelta.

Tutkimuksessaan Rhee ym. (2009) selvittivät, että henkilöt, joilla oli korkea minäpystyvyys, käyttivät enemmän suojausohjelmistoja ja -ominaisuuksia. Korkea minäpystyvyys korreloi myös tärkeimpien tietoturvasovellusten ja tietoturvatyökalujen käyttöönottoasteen kanssa. Lisäksi korkean minäpystyvyyden omaava käyttäjäryhmä käytti tietoturvapäivityksiä ja -korjauksia useammin kuin henkilöt, joilla on alhainen minäpystyvyys. Henkilöt, joilla on korkea minäpystyvyys, tekivät useammin varmuuskopioita tärkeistä tiedostoista, käyttivät vahvoja ja useita salasanoja eri verkkotileille, tarkistivat, salaako sivusto siirretyt tiedot lähettäessään henkilökohtaisia tietojaan, eivätkä jakaneet tietokoneitaan muiden kanssa. Lisäksi käyttäjät, joilla oli korkea minäpystyvyys, osoittivat aikovansa jatkaa ja vahvistaa näitä turvatoimia.

Yoon, Hwang ja Kim (2012) esittivät opiskelijoiden tietoturvakäyttäytymistä koskevassa tutkimuksessaan suojelumotivaatioteoriaan perustuvan mallin ja identifioivat minäpystyvyyden muuttujaksi, joka vaikuttaa merkittävästi langattoman kodin verkon käyttäjien päätökseen ottaa käyttöön suojausominaisuuksia verkoissaan. He havaitsivat, että minäpystyvyydellä on myös merkittävä vaikutus opiskelijoiden aikomuksiin harjoittaa tietoturvaa.

4.3 Asenne

Ajzen ja Fishbein (1975) ovat määritelleet asenteen suotuisuudeksi ryhtyä tiettyyn käyttäytymiseen. Monet käyttäytymistutkimukset ovat käyttäneet asennetta käyttäytymisaikomusten selittämiseen, koska sillä on havaittu olevan suora vaikutus aikomuksiin ryhtyä turvalliseen käyttäytymiseen. On tutkittu, että jos käyttäjä ajattelee jonkin toiminnon parantavan hänen turvallisuuttaan, hän pitää toimintoa hyödyllisenä, esimerkiksi vakoiluohjelmien torjuntaohjelmiston hyödyllisyyden havaittiin vaikuttavan merkittävästi asenteeseen (Ng & Rahim, 2005).

4.4 Subjektiiviset ja kuvailevat normit

Subjektiiviset ja kuvailevat normit ovat sosiaalisia tekijöitä, jotka vaikuttavat ihmisen tietoturvakäyttäytymiseen. Subjektiivinen normi on perustava käsite perustellun toiminnan teoriassa (Theory of Planned Behavior), joka on suojelumotivaatioteorian tavoin usein käytetty teoria tietoturvakäyttäytymisen tutkimuksessa. Subjektiivisilla normeilla tarkoitetaan asioita, joita yksilö uskoo tiettyjen henkilöiden tai ryhmien odottavan häneltä (Fishbein & Ajzen, 1975). Kuvaava normi taas viittaa käsityksiin siitä, mitä henkilö uskoo muiden tekevän turvallisuuden parantamiseksi (Anderson & Agarwal, 2010).

Subjektiivisten normien tai kuvailevien normien roolia henkilökohtaisessa tietoturvakäyttäytymisessä on tutkittu vähän, mutta on todennäköistä, että ne ovat olennaisia, koska organisaation käyttäjien muodollisia lähestymistapoja turvallisuuskäyttäytymisen parantamiseen ei löydy henkilökohtaisesta käyttäytymisestä (Anderson ja Agarwal, 2010). Laitteet ja ohjelmistot on yleensä varustettu vain vähäisellä dokumentaatiolla, ja käyttäjien odotetaan etsivän itsenäisesti lisätietoja verkosta. Käytettävyyskehittäjät pyrkivät tuotteisiin, jotka uusi käyttäjä voi yksinkertaisesti ottaa käyttöön ja aloittaa heti toimintansa. Tämä helppokäyttöisyys tulee kuitenkin maksamaan, koska käyttäjillä saattaa olla puutteita tietoturvatiedoissaan. Näitä aukkoja voidaan tämän seurauksena täyttää keskustelemalla tuotteista ystävien ja sukulaisten kanssa, mikä lisää subjektiivisen normin ja kuvailevan normin mahdollista roolia. (Thompson, McGill & Wang, 2017).

Anderson ja Agarwal (2010) tarkastelivat subjektiivisia ja kuvailevia normeja ja havaitsivat, että subjektiivinen normi vaikutti aikomukseen suorittaa turvallisuuteen liittyviä toimintoja kotitietokoneilla, mutta ei Internetin suojaamiseen liittyviin toimiin. Päinvastoin kuvaileva normi oli merkittävä tekijä aikeissa ryhtyä turvalliseen käyttäytymiseen Internetin suojaamiseksi, mutta ei oman kotitietokoneen suojaamiseksi. Kyseinen ilmiö voidaan selittää sillä, että ihmiset voivat menettää enemmän, jos hei eivät suojaa tietokonettaan. Yksilöt voivat myös ajatella, että heidän tehtävänsä on suojata omia laitteitaan, kun taas Internetin suojaaminen on yhteisesti kaikkien vastuulla.

Tu ym. (2015) tutki myös sosiaalisten tekijöiden roolia henkilökohtaisten laitteiden suojaamisessa varkauksilta ja havaitsi, että niillä oli tärkeä rooli määritettäessä käyttäjien tietämystä uhkiin vastaamisesta, käsityksiä uhan asteesta ja aikeista ryhtyä suojatoimenpiteisiin. Tutkimuksen mukaan laitteiden ollessa henkilökohtaisessa omistuksessa, käyttäjät eivät yleensä saa muodollista tietoturvakoulutusta, joka johtaa siihen, että oppiminen perustuu pääasiassa epävirallisiin tietolähteisiin, kuten työtovereihin, henkilökohtaisiin kokemuksiin ja mediaan.

4.5 Aiemmat kokemukset

Aiempien kokemuksien vaikutusta tulevaan käyttäytymiseen on tarkasteltu tietoturvakontekstissa yleisellä tasolla. Lee ym. (2008) tutki aiempien virustartuntojen vaikutusta yksilön aikomukseen omaksua virustorjuntakäyttäytymistä. Aytes ja Connolly (2004) tarkastelivat aikaisempia kokemuksia selvittämällä, onko tutkimuksen osallistujilla koskaan ollut negatiivisia seurauksia tietyn tietoturvatehtävän suorittamatta jättämisestä ja jos on, kuinka äskettäin. Aiemmat kokemukset eivät kuitenkaan olleet merkittävä osa heidän tutkimustaan tai analyysiään. Aiemmat kokemukset elämässä koostuvat yleensä kahdesta osasta: 1) aikaisempien kokemuksien tiheydestä ja 2) vakavuudesta (Dupuis ym., 2012).

Henkilökohtaista tietoturvauhille altistumista pidetään yhtenä hankitun tiedon muotona, joka voi vaikuttaa koettuun haavoittuvuuteen ja sitä kautta käyttäytymiseen (Weinstein ym., 2000). Boss (2007) havaitsi, että sekä henkilökohtainen kokemus, että tieto muiden altistumisesta tietoturvauhille vaikuttivat koettuun haavoittuvuuteen. Aiempi kokemus tietoturvauhista voi olla sitäkin merkittävämpi vaikuttaja kotiympäristössä, koska kotikäyttäjillä on saattanut saada vähän tai ei ollenkaan tietoturvakoulutusta (Furnell ym., 2007), jonka vuoksi he voivat olla enemmän riippuvaisia henkilökohtaisista kokemuksistaan muodostaessaan omaa tietoturvakäyttäytymistään ja reaktioitaan.

5 YHTEENVETO

Tämän kirjallisuuskatsauksen tavoitteena oli selvittää, millainen on kotikäyttäjä tietoturvan kontekstissa ja mitkä tekijät vaikuttavat kotikäyttäjän tietoturvakäyttäytymiseen. Ensimmäisessä luvussa käsiteltiin tietoturvaa yleisesti, jotta tietoturvakäyttäytymistä ja siihen vaikuttavia tekijöitä voitaisiin ymmärtää paremmin. Ensimmäisessä luvussa tarkasteltiin myös kotikäyttäjää tietoturvakontekstissa sekä yleisimpiä kotikäyttäjien kohtaamia tietoturvauhkia.

Työntekijöitä koskevaa tietoturvatutkimusta ei voida täysin soveltaa kotikäyttäjiin, sillä olosuhteet ja lähtökohdat ovat usein varsin erilaiset. Erot työntekijän ja kotikäyttäjän välillä voidaan nähdä esimerkiksi siinä, että kotikäyttäjä ei ole yleensä saanut tietoturvakoulutusta, tietoturvan toteutumista kotona ei valvota, eikä käyttäjällä ole IT-tukea apunaan ongelmatilanteissa, toisin kuin työympäristössä (Anderson & Agarwal, 2010). Tutkielmassa kotikäyttäjä määriteltiin henkilöksi, jonka ikä ja tekninen tietämys voi vaihdella, ja joka käyttää tietokonetta ja Internetiä missä tahansa työympäristön ulkopuolella ja on vastuussa tietokoneensa suojaamisesta ja päivittämisestä (Kritzinger & Solms, 2010).

Toisessa pääluvussa tarkasteltiin tietoturvakäyttäytymistä yleisesti sekä teoreettisen mallin pohjalta. Kolmannessa luvussa vastattiin toiseen tutkimuskysymykseen erittelemällä tietoturvakäyttäytymiseen vaikuttavia tekijöitä.

Tietoturvakäyttäytymistä on pyritty selittämään useiden eri teorioiden pohjalta, sekä monesti myös teorioiden yhdistelmillä ja niiden muokatuilla versioilla. Halusin tarkastella tietoturvakäyttäytymistä suojelumotivaatioteorian näkökulmasta, sillä se on yksi laajimmin käytetyistä teorioista tietoturvatutkimuksessa. Suojelumotivaatioteorian keskeinen periaate on, että yksilön on tunnettava huolta mahdollisesta uhasta (Rogers, 1975). Huoli edustaa suojelumotivaatioteoriassa uhkien arviointia, joka on liittynyt tietoturvatutkimuksessa muun muassa kodin palomuurikäyttäytymiseen (Woon ym., 2005), turvallisuuskäyttäytymiseen (Tsai ym., 2016) ja turvallisuusvaatimusten noudattamiseen (Vance ym., 2012; Pahnila ym., 2007). Mitä suuremmalta ja merkityksellisemmältä uhka vaikuttaa, sitä todennäköisemmin yksilöllä on positiivinen asenne ryhtyä tietoturvatoimiin (Woon ym., 2005). Tämä positiivinen asenne johtaa vahvempiin toiminta-aikomuksiin ja pienempään todennäköisyyteen siitä, että yksilö jättää

huomioimatta turvallisuuskäyttäytymisen (Workman ym., 2008). Suojelumotivaatioteorian on havaittu olevan yksi tehokkaimmin selittävistä teorioista, joka ennustaa yksilön aikomuksia ryhtyä suojatoimiin (Agarwal & Anderson, 2010). Tästä huolimatta, suojelumotivaatioteoria ei yksinään riitä selittämään käyttäjän aikomuksia ryhtyä suojaavaan käyttäytymiseen.

Kirjallisuuskatsauksen perusteella voidaan todeta, että tietoturvakäyttäytymiseen vaikuttavat merkittävästi asenne, minäpystyvyys, subjektiiviset ja kuvailevat normit ja käyttäjän aiemmat kokemukset.

Tutkielma sisältää joitakin rajoitteita liittyen tietoturvakäyttäytymiseen vaikuttaviin tekijöihin. Ihmisen käyttäytyminen on laaja aihe, johon vaikuttavat yllä mainittujen lisäksi lukemattomat eri tekijät, kuten ikä, sukupuoli, kulttuuri, koulutus ja sosioekonominen asema. Tutkielmassa ei siis oteta huomioon kaikkia tietoturvakäyttäytymiseen mahdollisesti vaikuttavia tekijöitä. On olemassa tutkimuksia, jotka tutkivat sitä, miten esimerkiksi kulttuuri, ikä tai sukupuoli vaikuttavat tietoturvakäyttäytymiseen, mutta tähän tutkielmaan päätin rajata tarkasteltavaksi yleisimmin tutkimuskirjallisuudessa toistuvat tekijät selkeyden vuoksi. Lähdemateriaalin perusteella esittelemäni tekijät ja suojelumotivaatioteorian muuttujat ovat myös erittäin relevantteja ja vahvoja tietoturvakäyttäytymisen ennustajia.

Kotikäyttäjien tietoturvakäyttäytymisen tutkimuksen tärkeys on selvästi tunnistettu tietoturva-alalla, mutta tutkimus on yhä vähäistä. Työskentely ei tapahdu enää pelkästään organisaatioympäristössä, vaan enenevissä määrin myös työpaikan ulkopuolella, joka lisää tietoturvariskejä. Jatkotutkimuksen avulla voitaisiin ymmärtää paremmin ihmisten tietoturvakäyttäytymistä ja tutkijat voisivat antaa suosituksia ratkaisuista, jotka puuttuvat käyttäytymisen aiheuttajaan. Jos esimerkiksi heikko uhkien havaitseminen johtaa siihen, että käyttäjä jättää suorittamatta annettuja turvallisuustehtäviä, tutkijat voisivat suositella ratkaisuja, jotka lisäävät uhkien havaitsemista.

LÄHTEET

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, *82*(2), 261–277. https://doi.org/10.1037/h0076477

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Aytes, K., & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. 20.

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of social and clinical psychology*, *4*(3), 359-373.

Boss, S. R. (2007). Control, Perceived Risk and Information Security Precautions: External and Internal Motivations for Security Behavior. 237.

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. https://doi.org/10.2307/25750690

Crossler, R. E., & Bélanger, F. (2009). The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security*, *5*(3).

Dupuis, M., Crossler, R., & Endicott-Popovsky, B. (2012). The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information.

Enisa Threat Landscape. (2021). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001

Guttman, B., & Roback, E. (1995). An Introduction to Computer Security: The Nist Handbook. *DIANE Publishing.*

Hanus, B., & Wu, Y. "Andy". (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. 21.

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. https://doi.org/10.1016/j.cose.2010.08.001

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, *45*(2), 109–119. https://doi.org/10.1016/j.im.2008.01.002

Liikenne- ja viestintävirasto. (2020). Tietoturvan vuosi 2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Ng, B.-Y., & Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. 15.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security (NIST SP 800-12r1; s. NIST SP 800-12r1). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-12r1

Nurse, J. R. C. (2019). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit (ss. 662–690). https://doi.org/10.1093/oxfordhb/9780198812746.013.35

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 767-A4.

Rhee, H.-S., 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. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenthal, D. A. (2002). Intrusion detection technology: leveraging the organization's security posture. *Information Systems Management*, *19*(1), 35-44.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Stajkovic, A., & Luthans, F. (1998). Self-Efficacy and Work-Related Performance: A Meta-Analysis. *Psychological Bulletin*, *124*, 240–261. https://doi.org/10.1037/0033-2909.124.2.240

Symantec: Internet Security Threat Report. (2017). https://docs.broadcom.com/doc/istr-22-2017-en

Tanner Jr, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *Journal of marketing*, *55*(3), 36-45.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Thomson, M. E., & von, S. R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38–58. https://doi.org/10.1057/ejis.2013.27

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52*(4), 506–517. https://doi.org/10.1016/j.im.2015.03.002

Uma, M., & Padmavathi, G. (2013). *A Survey on Various Cyber Attacks and Their Classification*. 7.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198.

Viestintävirasto, Kyberturvallisuuskeskus. (2018). Kyberturvallisuuden sanasto. http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Weinstein, N., Lyon, J., Rothman, A. & Cuite, C. (2000) Changes in Perceived Vulnerability Following Natural Disaster. Journal of Social and Clinical Psychology, 19(3), 327- 395.

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of Protective Behavior and Security Incidents for Home Computers. *Journal of Computer Information Systems*, *57*(4), 353–363. https://doi.org/10.1080/08874417.2016.1232991

Whitman, M. E., & Mattord, H. J. (2012). *Roadmap to Information Security: For IT and Infosec Managers*. Cengage Learning.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91-95.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). *A Protection Motivation Theory Approach to Home Wireless Security*. 14.

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*.

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks*, *16*(1), 1550147719899374.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). *Exploring Factors That Influence Students' Behaviors in Information Security*. *23*, 10.