Ville Erkkilä

SALASANOJEN HALLINTASOVELLUSTEN VAIKUTUS SALASANOJEN KÄYTTÖÖN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Erkkilä Ville
Salasanojen hallintasovellusten vaikutus salasanojen käyttöön
Jyväskylä: Jyväskylän yliopisto, 2022, 66 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Käyttäjätilin vaativien verkkopalveluiden lisääntyessä vuosi vuodelta, kasvaa myös ihmisten tarve salasanoille. Käyttäjien turvallisuuden takaamiseksi salasanojen täytyy olla tarpeeksi vahvoja, niiden tulisi olla uniikkeja eri palveluissa, eikä niitä tulisi säilyttää muiden ihmisten ulottuvilla. Salasanakäyttäytyminen ei kuitenkaan ole juurikaan muuttunut ajan saatossa, sillä käyttäjien yleisimmiksi salasanoiksi paljastuu toistuvasti pitkät listat heikkoja salasanoja, jotka ovat murrettavissa sekunnin murto-osissa. Tähän johtaa muun muassa se, että ihmiset usein valitsevat käytännöllisyyden ja helppouden ennen turvallisuutta, ja haluavat säästää muistikapasiteettiaan tietoturvan kustannuksella. Tähän vastaamaan on luotu salasanojen hallintasovelluksia, joiden avulla voidaan luoda, varastoida ja syöttää salasanoja. Salasanojen hallintaa helpottavista ominaisuuksista huolimatta hallintasovellusten käyttö on kuitenkin jäänyt vähäiseksi verkkopalveluiden käyttäjien keskuudessa. Lisäksi niiden käyttäminen pelkkinä salasanalompakoina ei vielä tarkoita salasanojen vahvuuden tai monimuotoisuuden parantumista. Salasanojen hallintasovelluksiin liittyen tutkimusta on paljon niiden käyttöön, käytettävyyteen ja turvallisuuteen osalta. Hallintasovellusten varsinaista vaikutusta käyttäjien salasanoihin on kuitenkin tutkittu vähän. Tässä tutkimuksessa täydennettiin kyseistä aukkoa selvittämällä, miten salasanojen hallintasovellusten ottaminen käyttöön on vaikuttanut käyttäjien salasanojen vahvuuteen, uniikkiuteen, sekä yleisesti niiden hallintaan. Tutkimuksessa toteutettiin teemahaastattelu 13 salasanojen hallintasovellusta käyttäneelle henkilölle selvittäen heidän näkemyksiään salasanojen käyttönsä muutoksista. Haastattelut analysoitiin temaattisella analyysillä. Tutkimuksen tulosten mukaan salasanojen hallintasovellusten käytön myötä käyttäjien salasanat ovat vahvempia ja monimuotoisempia. Keskeisinä syinä tälle ovat hallintasovellusten tarjoamat työkalut kuten salasanageneraattori sekä salasanojen vahvuusmittari. Lisäksi käyttäjien vähemmän turvalliset tavat hallita salasanojaan, kuten niiden kirjoittaminen paperille tai salaamattomaan digitaaliseen muotoon, ovat hallintasovellusten käytön myötä joko vähentyneet tai jääneet kokonaan. Tulokset täydentävät aiempaa tutkimusta salasanojen hallintasovellusten osalta. Ne indikoivat, että hallintasovelluksen käyttöön ottamisella on myös käytännössä useita vaikutusmekanismeja parantuneeseen salasanakäyttäytymiseen.

Asiasanat: salasana, salasanojen hallinta, salasanojen hallintasovellus,
salasanojen vahvuus, salasanojen uniikkius, salasanojen uudelleenkäyttö

ABSTRACT

Erkkilä Ville
Password managers' influence on use of passwords
Jyväskylä: University of Jyväskylä, 2022, 66 pp.
Cyber Security, Master's Thesis
Supervisor: Siponen, Mikko

As the number of online services demanding user accounts grows every year, so does the people's need for passwords. To guarantee the safety of users, the passwords must be strong enough, they need to be unique in different services, and they shouldn't be stored accessible to other people. However, password behavior has not changed much over time, as users' most common passwords are repeatedly revealed to be a long list of weak passwords that can be cracked in fractions of a second. This stems from, among other things, the fact that people often choose convenience and ease before security and want to save their memory capacity at the expense of information security. Password managers have been created to answer this challenge. They can be used to create, store, and fill in passwords. Despite the features that facilitate password management, the use of password managers has remained low among users of online services. In addition, using them as password wallets does not yet mean an improvement in the strength or diversity of passwords. There is a lot of research related to password managers regarding their use, usability, and security. However, the actual effect of password managers on users' passwords has been little studied. This study was used to fill that gap by researching how the adoption of password managers has affected the strength and uniqueness of users' passwords, as well as password management in general. In the study, a semi-structured interview was conducted with 13 password manager users, finding out their views on changes in their use of passwords. The interviews were analyzed using thematic analysis. The results of the study show that with the use of password managers, users' passwords are stronger and more unique. The main reasons for this are the tools provided by the password managers, such as the password generator and the password strength meter. In addition, users' less secure ways of managing their passwords, such as writing them down on paper or in an unencrypted digital format, have either decreased or completely disappeared due to the use of password managers. The results complement previous research on password managers. They indicate that implementing a password manager has several impact mechanisms on improved password behavior in practice as well.

Keywords: password, password management, password manager, password strength, password uniqueness, password reuse

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Salasanat pysyvät laajasta kritiikistä huolimatta yleisimpänä tunnistautumismenetelmänä, vaikka esimerkiksi biometristä tunnistautumista helpottavat älylaitteet ovat lisänneet vaihtoehtoisten kirjautumistapojen määrää viime vuosina – joskin salasanataso on usein piilotettu biometrisen tunnisteen taakse, jolloin tunnistautumistapa lähinnä helpottaa kirjautumista eikä niinkään poista salasanojen ongelmia (Furnell, 2022).

Salasanojen heikon kohdan aiheuttavat käyttäjät (Furnell, 2022). Cerniauskaiten (2021) mukaan vuoden 2021 vuodettujen salasanojen listoilla kolme ensimmäistä sijaa menee numerosarjoille *123456*, *12345* ja *123456789*, minkä lisäksi ensimmäiset kirjaimia sisältävät salasanat ovat yksinkertaisia kuten *qwerty* tai *password.* Myös nimet – olivat ne sitten ihmisten tai esimerkiksi yhtyeen tai urheiluseuran nimiä – sijoittuvat listoilla korkealle. NordPassin tekemän analyysin mukaan vuodetuista salasanoista jopa 84,5 prosenttia voidaan murtaa alle sekunnissa (Cerniauskaite, 2021). Mahdollisella hyökkääjällä voi olla monia syitä toiminnalleen: yleisimmät motiivit kyberrikollisilla ovat rahallinen hyöty sekä kosto (Neufeld, 2010).

Salasanojen ongelmaksi muodostuu ristiriita muistettavuuden ja turvallisuuden välillä (Qureshi, Younus & Khan, 2009). Käyttäjät valitsevat mieluummin muistettavan kuin turvallisen salasanan (O'Hanley & Tiller, 2014). Heikon yksittäisen salasanan lisäksi myös käyttäjien yleisessä salasanahallinnassa on ongelmallisuuksia. Samoja salasanoja käytetään useissa palveluissa, mikä aiheuttaa yhden tilin sijaan usean käyttäjäprofiilin vaarantumisen kerralla (Egelman, Sotirakopoulos, Muslukhov, Beznosov & Herley, 2013; O'Hanley & Tiller, 2014). Lisäksi käyttäjät kirjoittavat salasanojaan muistiin esimerkiksi muistivihkoon tai johonkin digitaaliseen tiedostoon (Stobert & Biddle, 2018).

Näiden haasteiden ratkaisemiseksi markkinoille on tullut salasanojen hallintasovelluksia, joiden tarkoituksena on helpottaa yksittäisen käyttäjän koko ajan kasvavan salasanamäärän mukana tuomaa haastetta muistamisen osalta (Aurigemma, Mattson & Leonard, 2017; Herley & Van Oorschot, 2012; Qureshi ym., 2009). Ne auttavat käyttäjää monilla eri tavoilla, joista keskeisimmät ovat

salasanojen varastointi ja organisointi, vahvojen salasanojen generoiminen sekä käyttäjätietojen automaattinen syöttäminen kirjautuessa (Huaman, Amft, Oltrogge, Acar & Fahl, 2022). Usein käytettyjä salasanojen hallintasovelluksia ovat muiden muassa LastPass, 1Password, Dashlane, KeePass ja BitWarden (Theodorakopoulos & Reinecke, 2020). Erikseen asennettavien hallintasovellusten lisäksi eri selaimilla ja käyttöjärjestelmillä on omia hallintajärjestelmiään (Ray, Wolf, Kuber & Aviv, 2021).

1.1 Tutkimuksen tarkoitus ja tarve

Tämä pro gradu -tutkielma pyrkii vastaamaan siihen, miten salasanojen hallintaohjelmien käyttö vaikuttaa käyttäjien salasanojen vahvuuteen ja muuhun salasanakäyttäytymiseen kuten salasanojen uudelleenkäyttöön.

Valtaosa aiemmasta salasanojen hallintasovellusten tutkimuksesta on keskittynyt joko niiden käytön tai käyttämättömyyden syihin (ks. esim. Ayyagari, Lim & Hoxha, 2019; Mayer, Munyendo, Mazurek & Aviv, 2022; Ray ym., 2021), erilaisiin käyttötapoihin (ks. esim Oesch, Ruoti, Simmons & Gautam, 2022; Pearman, Zhang, Bauer, Christin & Cranor, 2019; Seiler-Hwang ym., 2019) tai niiden teknisiin ratkaisuihin (ks. esim. Fahl, Harback, Otrogge, Muders & Smith, 2013; Fukumitsu, Hasegawa, Iwazaki, Sakai & Takahashi, 2016; Z. Li, He, Akhawe & Song, 2014). Tutkimusta ohjelmien käytön vaikutuksesta käyttäjän salasanoihin on kuitenkin hyvin vähän (Lyastani, Schilling, Fahl, Backes & Bugiel, 2018).

Lyastani ym. (2018) selvittivät, käytetäänkö hallintasovelluksia ainoastaan niin sanottuina lompakoina vai onko käytöllä myös vaikutusta käyttäjien salasanoihin. He vertailivat hallintasovelluksien kontekstissa käyttäjien ja ei-käyttäjien salasanoja keskenään ja havaitsivat, että käyttäjillä on sekä vahvempia että vähemmän käytettyjä salasanoja. Kyseinen tutkimus esitellään tarkemmin luvussa 3. Sen erot tähän tutkimukseen ovat näkökulma – käyttäjien ja ei-käyttäjien vertailu tarkastelee aihetta hieman eri näkökulmasta kuin käyttäjän oman toiminnan muuttuminen hallintasovelluksen käyttöönoton myötä – sekä tutkimusmenetelmä – Lyastanin ym. (2018) tutkimuksessa vaikutusta tutkittiin määrällisesti, tämä tutkimus puolestaan pyrkii löytämään vaikutuksen lisäksi syitä, joita aiemmin ei olla otettu huomioon.

Laajemmassa tietoturvatutkimuksen kontekstissa tämä tutkimus täydentää vähemmän tutkittua osa-aluetta: kotikäyttäjien tietoturvaa. Li ja Siponen (2011) ovat esittäneet huolensa siitä, että suurin osa tietoturvaan liittyvien inhimillisten tekijöiden tutkimus koskettaa työympäristöä. Heidän mukaansa ympäristöillä on eroa yksilön toimenpiteiden kannalta, joten he peräänkuuluttavat myös henkilökohtaisen käytön tutkimusta.

1.2 Tutkimusongelmat ja tutkimusmenetelmä

Tämän tutkimuksen päätutkimuskysymyksenä on: Miten salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen käyttöön?

Päätutkimuskysymys on jaettu kolmeen sitä suoraan tukevaan alakysymykseen: 1) Miten salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen vahvuuteen? 2) Miten salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen uniikkiuteen? ja 3) Miten salasanojen hallintasovellusten käyttäminen vaikuttaa muuhun salasanahallintaan?

Tutkimuksen kirjallisuuskatsauksen pääasialliset lähteet ovat tieteellisiä aikakauslehtiä, jotka suomalainen tieteellisten julkaisujen luokitusjärjestelmä Julkaisufoorumi on noteerannut vähintään tasolle 1, sekä täydentämiseksi sekä ajankohtaisemman tiedon hankkimiseksi artikkeleja eri konferenssijulkaisuista.

Kyseessä on laadullinen tutkimus, jonka tiedonkeruumenetelmänä käytettiin teemahaastattelua Zoom-videokonferenssipalvelun avulla. Tutkimukseen osallistui 13 henkilöä, jotka käyttivät tai olivat käyttäneet salasanojen hallintasovellusta. Aineisto on analysoitu temaattisella analyysillä.

1.3 Keskeiset tulokset ja niiden merkitys

Tutkimuksen keskeisempänä tuloksena on, että salasanojen hallintasovelluksella on salasanojen vahvuutta, uniikkiutta ja niiden hallinnan turvallisuutta parantava vaikutus. Tähän suurimpina syinä ovat hallintasovellusten tarjoamista työkaluista salasanageneraattori ja salasanavahvuusmittari sekä yleisesti hallintasovelluksen tarjoama mahdollisuus varastoida salasanat säilöön niiden muistamisen sijaan. Työkalujen avulla käyttäjät luovat itselleen vahvempia ja monimuotoisempia salasanoja, ja varastointimahdollisuus on poistanut salasanojen kirjoittamisen paperille tai digitaaliseen muotoon joko osittain tai kokonaan.

Tulokset ovat merkittäviä, koska aiempaa tutkimusta yksittäisen käyttäjän salasanojen käytön muutoksesta hallintasovelluksen käyttöönoton myötä ei ole löydettävissä.

1.4 Rajaukset

Tässä tutkimuksessa ei tutkita sitä, ovatko käyttäjien salasanat oikeasti, mitatusti, vahventuneet (mikä toisaalta on myös vaikeasti määriteltävä aihe, ks. luku 2), vaan mikä on käyttäjien oma käsitys asiasta. Toisin sanoen on mahdollista, että tutkittavat ainoastaan luulevat tietävänsä heikon ja vahvan salasanan erot, mutta oikeasti pohjaavat vastauksensa väärinkäsityksiin. Esimerkiksi Pittmanin & Robinsonin (2020) mukaan käyttäjät tunnistavat heikon salasanan, mutta vahvan salasanan tunnistaminen ei ole yhtä selvää. Tämä ei kuitenkaan ole tutkimuksen

kannalta ongelma, sillä tavoitteena on tutkia salasanakäyttäytymistä tarkkojen salasanaominaisuuksien sijaan.

Lisäksi tässä tutkimuksessa rajataan pois selaimen tai käyttöjärjestelmän sisäiset hallintajärjestelmät ja tutkitaan erillisiä, erikseen asennettavia hallintasovelluksia.

1.5 Tutkielman sisältö

Tutkielma koostuu kahdeksasta pääluvusta. Pääluku yksi on johdanto, jossa esitellään aihe ja tutkimuksen keskeisimmät osa-alueet. Pääluvun 2 tarkoituksena on taustoittaa, miksi ja miten käyttäjiltä vaaditaan toimenpiteitä salasanoihin liittyen. Siinä käsitellään salasanojen vahvuutta sen mittareiden sekä erilaisten salasanavaatimusten kautta. Lisäksi kyseisessä pääluvussa esitellään lyhyesti salasanojen murtamistavat sekä vaihtoehtoja salasanojen käytölle tunnistautumismenetelmänä. Pääluku 3 puolestaan liittyy salasanojen hallintaan: siinä käydään läpi erilaisia haasteita, joita usean salasanoja vaativan palvelun käyttäminen tuottaa, minkä lisäksi tälle tutkimukselle tärkeänä osana esitellään salasanojen hallintasovelluksiin liittyvää aiempaa tutkimusta. Pääluvussa 4 käsitellään ihmisten tietoturvallisuuskäyttäytymistä laajemmin, jotta kyetään paremmin ymmärtämään syitä erilaisille valinnoille tietoturvakontekstissa. Pääluku 5 kuvaa tutkimuksen menetelmän ja tutkimusprosessin, pääluku 6 tulokset sekä pääluku 7 tuloksiin liittyvän pohdinnan. Lopuksi pääluvussa 8 tehdään yhteenveto koko tutkimuksesta ja esitetään jatkotutkimusaiheita.

2 SALASANOJEN VAHVUUS

Tässä pääluvussa käsitellään salasanojen vahvuuden erilaisia mittareita sekä eri instanssien antamia salasanasuosituksia. Lisäksi esitellään tapoja murtaa salasanoja sekä vaihtoehtoisia tunnistautumismenetelmiä salasanojen tilalle tai täydennykseksi.

Salasanan kaltaisia menetelmiä on käytetty aina antiikin Roomasta ja Kreikasta lähtien (Eve, Bogost & Schaberg, 2019). Nykypäivänä salasanojen merkitys jokapäiväisessä elämässämme on niin suuri, että niiden tuottamat hankaluudet hyväksytään (Eve ym., 2019). Riittävän ajan ja resurssien myötä mikä tahansa salasana voidaan murtaa, mutta salasanan vahvistamisella voidaan merkittävästi vaikuttaa sen murtamistodennäköisyyteen (Vacca, 2013).

Even ym. (2019) mukaan salasanojen käyttämiseen liittyen ajatellaan usein väärin, että niillä voidaan varmasti todentaa ihmisen henkilöllisyys. Lisäksi jotta salasanaa voidaan käyttää, on luotava yhteys palveluun jo etukäteen, jotta molemmilla osapuolilla on oikea tieto jatkossa käytettävästä salasanasta (Eve ym., 2019). Kolmantena ongelmakohtana salasanojen suhteen on, että niiden tulee olla samaan aikaan sekä helposti muistettavia että vaikeasti arvattavia tai murrettavia (Qureshi ym., 2009).

2.1 Vahvan salasanan vaatimukset

2.1.1 Salasanan vahvuuden mittarit

Man, Campbellin, Tranin ja Kleemanin (2010) mukaan salasanan käyttäminen turvallisena tunnistautumismenetelmänä riippuu käyttäjän valitseman salasanan vahvuudesta, joka ei kuitenkaan ole täysin selkeästi määriteltävä mittari. Usein laadukkaan salasanan synonyyminä pidetään salasanaa, jolla on suuri entropia. Se tarkoittaa, että salasana on mahdollisimman vaikeasti ennustettava (Ma ym., 2010). Yleisesti informaatiotieteessä entropialla tarkoitetaan viestin sisältämän informaation odotusarvoa (Taneski, Kompara, Hericko & Brumen, 2021).

Ma ym. (2010) kuitenkin toteavat, että entropia ei ole salasanan laadun mittari, sillä entropiaa mitataan niin kutsutulla Markov-prosessilla, joka puolestaan pohjautuu käytetyn kielen sanojen tilastolliseen jakaumaan. Salasanoja ei heidän mukaansa kuitenkaan voi tarkastella kommunikaatiojärjestelmän mittarin avulla. (Ma ym., 2010, s. 583) Taneski ym. (2021) toisaalta toteavat, että Markov-mallin käytön laadukkuus salasanojen kontekstissa riippuu käytettävästä datasetistä.

Toinen lähestymistapa salasanan vahvuudelle on mitata todennäköisyyttä sille, että salasana pystytään murtamaan, sillä käyttäjät eivät usein luo täysin satunnaisia salasanoja, vaan toiminnassa on tiettyjä malleja (Boonkrong, Kitthimon, Koksoungnoen & Jenprakhon, 2021; Lyastani ym., 2018). Myös Egelman ym. (2013) tarkastelevat asiaa murrettavuuden kannalta. Heidän näkemyksensä on, että salasanan vahvuutta määrittää sen tuottama vaikeus murto-ohjelmille (Egelman ym., 2013). Esimerkiksi eri kokoisia kirjaimia, numeroita ja erikoismerkkejä sisältäviä 10-merkkisiä salasanoja voi olla yli 60 miljoonaa miljardia erilaista kappaletta (Eve ym., 2019).

Galbally, Coisel ja Sanchez (2017) puolestaan jakavat salasanan vahvuuden arvioinnin kolmeen kategoriaan: hyökkäysperustaisiin, heuristisuusperustaisiin sekä todennäköisyysperustaisiin menetelmiin. Myös nämä kaikki tarkastelevat asiaa hieman eri näkökulmista (Galbally ym., 2017).

Komanduri ym. (2011) toteavat, että vertailtaessa kahta yleistä ohjeistustyyppiä – 16-merkkistä salasanaa ilman muita vaatimuksia ja 8-merkkistä salasanaa, joka sisältää myös isoja kirjaimia, erikoismerkkejä ja numeroita, ensin mainittu on huomattavasti vaikeampi ennustaa huolimatta ohjeistustyyppien lähes samanlaisesta entropiasta. Hu (2018) puolestaan yksinkertaistaa, että salasanan vahvuuden maksimoinniksi tulisi lisätä sekä salasanan pituutta että mahdollisimman erilaisia merkkityyppejä.

Voidaankin todeta, että salasanan vahvuudelle ei ole selkeää yksittäistä mittaria.

2.1.2 Salasanasuositukset ja -vaatimukset

Komandurin ym. (2011) mukaan käyttäjien salasanojen vahvistamiseksi salasanoilta vaaditaan usein erilaisia ominaisuuksia: minimipituutta, isoja ja pieniä kirjaimia ja erikoismerkkejä. Mahdollisena vaatimuksena on myös, että salasanat eivät sisällä tietosanakirjasta löytyvää sanaa tai sanoja (Komanduri ym., 2011, s. 2595). Useat palvelut tarjoavat tämän helpottamiseksi visuaalisen palautteen salasanan vahvuudesta, mikä myös johtaa parempiin salasanoihin (Egelman ym., 2013; Ur ym., 2012).

Toisaalta Furnell (2022) toteaa, että jokavuotiset listat käytetyimmistä salasanoista paljastavat, että käyttäjät tekevät vuodesta toiseen samankaltaisia virheitä. On siis selvää, että käyttäjät jäävät usein ilman toteuttamiskelpoisia ohjeita vahvojen salasanojen osalta – tai vaihtoehtoisesti vastakkaisesta suunnasta katsottuna käyttäjiltä hyväksytään liian yksinkertaisia salasanoja eri palveluihin. Edistystä on kuitenkin nähtävissä erityisesti salasanan minimipituuden vaatimisen osalta (Furnell, 2022).

Salasanaohjeistuksella voi Komandurin ym. (2011) mukaan olla myös kääntöpuolensa. Liian vaikeita salasanoja vaativat ohjeistukset voivat johtaa muihin huonoihin salasanakäytäntöihin, kuten lapulle kirjoittamiseen tai kerran muistiin painetun salasanan käyttämiseen pitkän aikaa. Tutkimuksen puutteesta johtuen on myös vaikea arvioida, kuinka arvattavia salasanoja jonkin tietyn ohjeistuksen myötä muodostuu (Komanduri ym., 2011).

Esimerkiksi yhdysvaltalainen virasto NIST (National Institute of Standards and Technology) ja Yhdistyneiden kuningaskuntien NCSC (National Cyber Security Centre) ovat luopuneet erikoismerkkien käytön vaatimuksesta, sillä se lisää käyttäjien salasanaratkaisujen suoraviivaistumista: kun salasana vaaditaan tekemään monimutkaisemmaksi – ja täten vaikeammin muistettavaksi, käyttäjä tekee ennustettavia muutoksia jo olemassa oleviin salasanoihin (esimerkiksi kirjaimia vaihdetaan saman näköisiin numeroihin kuten o -> 0) tai käyttää samaa salasanaa useammassa palvelussa (NIST, 2020; NCSC, 2018).

Toinen ristiriitaisia suosituksia muodostava käytäntö on salasanojen säännöllinen vaihtaminen. O'Hanley ja Tiller (2014) suosittavat, että organisaatiossa vaaditaan salasanojen vaihtamista aina tietyn ajanjakson jälkeen, koska samojen salasanojen käyttö on niin yleistä, ja sen myötä salasanavuoto jossain toisaalla asettaa myös organisaation sisäiset järjestelmät alttiiksi hyökkäykselle. NIST (2020) ja NCSC (2018) puolestaan molemmat vastustavat tätä suositusta. NIST:n (2022) mukaan vaatimukset salasanojen kierrättämisestä johtaa vain pieneen salasanan muokkaukseen ja näin ollen lisävaatimuksesta saatava hyöty on vain näennäinen ja jopa väärässä mittakaavassa turvallisuuden tunnetta lisäävä. Tätä näkemystä tukevat myös Zhang, Monrose ja Reiter (2010), joiden mukaan yli neljäkymmentä prosenttia vaihdetuista salasanoista voidaan murtaa edellisen salasanan pohjilta. He suosittelevatkin säännöllisen vaihtamisen muuttamista vahvempien salasanojen suositukseksi (Y. Zhang ym., 2010).

Taulukoissa 1 ja 2 on yhteenveto Suomen (Kyberturvallisuuskeskus), Yhdysvaltojen (NIST), Yhdistyneiden kuningaskuntien (NCSC) ja Australian (ACSC) viranomaisten antamista suosituksista sekä käyttäjille että palveluntarjoajille liittyen salasanoihin ja niiden hallintaan. Ensimmäisessä taulukossa on yhteenveto kyseisten toimijoiden ohjeista ja toisessa taulukossa vertaillaan keskeisten teemojen näkymistä ohjeissa. Huomattavaa on, että esimerkiksi Kyberturvallisuuskeskus (2022) suosittelee edelleen erikoismerkkien käyttöä muiden (NIST, 2020; NCSC, 2018; ACSC, 2021) ollessa joko luopuneita kyseisestä suosituksesta tai jopa suositusta vastaan. ACSC:n suositusten erikoisuutena on suora ohjeistus käyttää niin kutsuttua salalausetta (engl. *passphrase*), joka on useasta sanasta koostuva pidempi yhdistelmä (ACSC, 2021). ACSC:n minimipituussuositus onkin vähintään 14 merkkiä, joka on selvästi pidempi kuin esimerkiksi NISTin mainitsema 8 merkkiä (NIST, 2020; ACSC, 2021).

TAULUKKO 1 Kolmen turvallisuusviranomaisen suositukset salasanoista (ACSC, 2021; Kyberturvallisuuskeskus, 2022; NCSC, 2018; NIST, 2020).

Organisaatio	**Salasanasuositukset**	**Vaihtoväli, uniikkius ja muut suositukset**
Kyberturvallisuuskeskus	”Mitä pidempi salasana on, sitä turvallisempi se on.” ”Hyvä salasana on helppo muistaa, mutta vaikea arvata.” ”Kokonainen lause on hyvä salasana.” ”Käytä salasanassasi isoja kirjaimia ja erikoismerkkejä.” ”Kirjoitusvirheet, murre. [SIC] puhekielen ilmaisut ja muu sanojen rikkominen vahventavat salasanaa.”	”Tee jokaiseen palveluun oma salasana.” ”Panosta tärkeisiin salasanoihin, joita käytät unohtuneiden salasanojen palautukseen, kuten sähköpostin salasanaa.” ”Älä koskaan kerro kenellekään salasanojasi – edes viranomaiset eivät niitä sinulta kysy!” ”Käytä salasanojen hallintaohjelmaa” ”Käytä kaksi- tai monivaiheista tunnistautumista”
NIST	Salasanan tulee olla vähintään 8 merkkiä pitkä. Muita salasanan muodostamisen vaatimuksia, kuten erikoismerkkien käyttöä, ei suositella palveluille.[1] Palvelun tulisi tarkastaa syötetty salasana esimerkiksi tietomurto- ja sanakirjalistojen sekä toistuvien tai peräkkäisten merkkijonojen osalta. Palveluiden tulisi tarjota käyttäjälle apua salasanamittarin muodossa.	Salasanojen säännöllistä muuttamista ei suositella. Salasanan vaihtaminen tulisi tehdä tietomurron yhteydessä. [2]
NCSC	Salasanan minimipituudelle ei anneta suositusta, mutta palveluita suositetaan määrittämään kuitenkin jokin minimipituus. Salasanan kompleksisuutta – kuten erikoismerkkien käyttöä – ei suositella vaatimaan.	Salasanojen säännöllistä muuttamista ei suositella. Salasanan vaihtaminen tulisi tehdä tietomurron yhteydessä. Salasanojen hallintaohjelman käyttöä suositellaan.
ACSC	Vähintään nelisanainen ja 14-merkkinen salalause. ”Mitä vähemmän ennustettava salalauseesi on, sen parempi”	Uniikki salalause jokaiselle tärkeälle tilille. Salasanojen hallintaohjelmaa suositellaan. Jos salalause vuotaa, se tulee vaihtaa heti.

[1] NIST (2022) perustelee suositustaan erillisessä Q&A-julkaisussa kahdella tavalla: Toisaalta käyttäjät valitsevat ennustettavia tapoja vaatimusten täyttämiseen ja toisaalta vaatimukset lisäävät samojen salasanojen käyttöä eri palveluissa (NIST, 2022).

[2] NIST:n (2022) mukaan salasanan säännöllisen vaihtamisen luovan valheellista turvallisuuden tunnetta, koska käyttäjät usein muuttavat salasanaansa vain vähän jollain tunnistettavalla tavalla (NIST, 2022).

TAULUKKO 2 Yhteenveto keskeisimmistä suosituksista (Kyberturvallisuuskeskus, 2022; NIST, 2020; ACSC, 2021; NCSC, 2018)

Organisaatio	Minimipituus	Kompleksisuus	Säännöllinen vaihto	Salasanojen hallintaohjelma
TRAFICOM	√	√	-	√
NIST	√	×	×	-
NCSC	√	×	×	√
ACSC	√	-	-	√

2.2 Salasanojen murtaminen

Suo, Zhu ja Owen (2005) luettelevat salasanojen murtamiskeinoiksi väsytyshyökkäyksen (engl. *brute force*), sanakirjahyökkäykset, arvaamisen, vakoiluohjelmat, olan takaa vakoilun (engl. *shoulder surfing*) ja käyttäjän manipuloinnin (engl. *social engineering*).

Kuo, Romanovsky ja Cranor (2006) yksinkertaistavat jakoa neljään kokonaisuuteen:

> Hyökkääjät tavallisesti murtavat salasanoja yhdellä neljästä tavasta:
> 1. Keräämällä tarpeeksi informaatiota käyttäjistä arvatakseen heidän salasanansa;
> 2. Käyttäjän manipuloinnilla, esimerkiksi huijaamalla käyttäjät paljastamaan käyttäjätunnuksensa ja / tai salasanansa;
> 3. Kaappaamalla käyttäjien salasanoja, esimerkiksi olan takaa vakoilulla tai vakoiluohjelmalla; ja
> 4. Murtamalla salasanoja käyttämällä ohjelmistoa, kuten John the Ripper. (Kuo ym., 2006, s. 68)

Väsytyshyökkäys tarkoittaa sitä, että järjestelmällisesti kokeillaan kaikkia mahdollisia salasanavaihtoehtoja, jolloin mahdollisimman suuri entropia on murtoyrityksen kohteena olevalle salasanalle hyödyksi (Eve ym., 2019; Tanni, Taharat, Parvez, Rumee & Zaber, 2022).

Arvaaminen jaetaan kahtia online- ja offline-hyökkäyksiin (Murray & Malone, 2020). Online-arvaushyökkäyksessä hyökkääjällä on usein tietty määrä yrityskertoja, kun offline-hyökkäyksessä puolestaan käytetään yleensä sanalistoja sekä jo vuodettujen salasanojen listoja, jotta koko salasana-avaruuden kaikista mahdollisista vaihtoehdoista löydettäisiin todennäköisimmät. Tämä parantaa hyökkäystyypin tehokkuutta verrattuna normaaliin väsytyshyökkäykseen (Murray & Malone, 2020). Ma ym. (2010) kuitenkin toteavat arvaamista hankaloittavaksi asiaksi sen, että arvauksen tulee olla aina täysin oikein. Tällöin ei ole hyötyä laskea arvauksen entropiaa sen sisältämistä merkeistä, sillä salasanojen kohdalla seuraavaa merkkiä ei voi päätellä edellisestä (jonka oikeudesta ei ole tietoa) (Ma ym., 2010).

Vakoiluohjelma voi olla esimerkiksi näppäimistön painalluksia tallentava haittaohjelma, josta saa tallentamisen myötä selville käyttäjän käyttäjätunnuksia

ja salasanoja (Chandrashekhar & Chakravarthy, 2022). Olan takaa vakoilu puolestaan on samankaltainen metodi, mutta fyysisessä maailmassa: siinä nimensä mukaisesti katsotaan, kun käyttäjä syöttää salasanansa järjestelmään (Gokhale & Waghmare, 2016). Käyttäjän manipuloinnissa hyökkääjä pyrkii saamaan vuorovaikutuksen kautta salasanan suoraan käyttäjältä itseltään (Kalnins, Purins & Alksnis ym., 2017).

On kuitenkin huomattava, että kaikki mainitut hyökkäystyypit eivät ole riippuvaisia salasanan vahvuudesta. Esimerkiksi käyttäjän manipuloinnissa salasanan vahvuudella ei ole väliä, mikäli käyttäjä antaa sen omatoimisesti hyökkääjälle.

2.3 Vaihtoehdot salasanoille

Tunnistautumistavat voidaan jakaa karkeasti kolmeen osaan:

1. tietämysperustainen tunnistautuminen
2. biometrinen tunnistautuminen
3. hallintaperustainen tunnistautuminen (Suo ym., 2005)

Nämä tunnetaan myös yksinkertaistettuna nimillä: *jotain-mitä-tiedät*, *jotain-mitä-olet* sekä *jotain-mitä-omistat* (Boonkrong ym., 2021). Suon ym. (2005) mukaan salasanat kuuluvat näistä ensimmäiseen kategoriaan: käyttäjältä pyydetään tunnistautumisen välineeksi jokin tieto, jonka molemmat osapuolet tietävät jo etukäteen. Biometriikka puolestaan liittyy ihmiskehon ominaisuuksiin kuten sormenjälkeen tai kasvojentunnistukseen. Valtuusperustaiseen tunnistautumiseen liittyy jokin fyysinen esine, jonka hallussapito antaa valtuuden tunnistautumiselle. Näitä tunnistautumistapoja voidaan käyttää myös yhdistelmänä, jolloin puhutaan monivaiheisesta tunnistautumisesta (Suo ym., 2005). O'Hanley ja Tiller (2014) mainitsevat vielä neljännen kategorian: *jotain-missä-olet*. Se on kuitenkin internet-aikakauden palveluissa vähemmän käytetty osamenetelmä tunnistautumiseen.

2.3.1 Biometriikka

Biometrinen tunnistautuminen on lisääntynyt huomattavasti viime vuosina (Furnell, 2022). Biometrisessa tunnistautumisessa käytetään jotain käyttäjän fyysistä ominaisuutta (Garfinkel & Lipford, 2014). Sen huonoja puolia ovat kuitenkin prosessin mahdollinen hitaus ja epäluotettavuus (Suo ym., 2005). Koska mittausympäristö voi muuttua suurestikin, on biometrisessä tunnistautumisessa otettava huomioon virhemarginaali, mikä puolestaan voi johtaa useisiin vääriin positiivisiin tuloksiin, eli oikeudeton käyttäjä saada pääsyn sisään järjestelmään (O'Hanley & Tiller, 2014). Myös tunnistuslaitteisto voi olla altis hyökkäyksille, jolloin tunnisteita voi olla mahdollista kopioida ja käyttää vääriin tarkoituksiin (O'Hanley & Tiller, 2014). Lisäksi ihmisen biometristä tunnistetietoa ei voi itse

(useimmissa tapauksissa) muuttaa, ja osalla ihmistä ei ole kykyä käyttää jotain tiettyä fyysistä tunnistetta (Garfinkel & Lipford, 2014). Biometrisellä tunnistautumisella on kuitenkin potentiaalia olla turvallisin vaihtoehto kolmesta (Suo ym., 2005).

2.3.2 Hallintaperustainen tunnistautuminen

Hallintaperustaista tunnistautumista käytetään paljon, sillä se on esimerkiksi pankki- ja luottokorttien tai erillisten yksittäisiä salasanoja tarjoavien kirjautumislaitteiden toimintatapa (O'Hanley & Tiller, 2014; Suo ym., 2005). Toisin kuin tieto, fyysinen valtuustekijä voi olla vain yhdessä paikassa kerrallaan, mikä toisaalta on myös menetelmän huono puoli: mikäli tunnistautumiseen tarvittava asia ei ole käyttäjän mukana, hän ei pysty kirjautumaan (O'Hanley & Tiller, 2014).

Vaccan (2013) mukaan fyysinen valtuustekijä voi olla joko erillinen laitteisto tai ohjelmisto esimerkiksi matkapuhelimessa. Fyysiset valtuustekijät toimivat joko aika- tai tapahtumasynkronoidusti tai niillä vastataan johonkin annettuun haasteeseen (Vacca, 2013). Garfinkelin ja Lipfordin (2014) mukaan aikasynkronoinnissa sekä tunnistautujan fyysinen valtuustekijä että palvelun oma järjestelmä suorittavat tietyin aikavälein funktion, joita sitten verrataan keskenään kirjautumishetkellä. Haasteeseen vastaamisessa puolestaan palvelun antamaan haasteeseen vastataan esimerkiksi sirukortilla, joka todentaa sisältävänsä sekä oikean yksityisen avaimen että oikein valtuutetun julkisen avaimen (Garfinkel & Lipford, 2014).

2.3.3 Monivaiheinen tunnistautuminen

Vacca (2013) jakaa tunnistautumisen vahvuuden karkeasti kahtia: Ainoastaan yhtä aiemmin mainitusta kolmesta tunnistautumistavasta käytettäessä on kyseessä heikko tunnistautuminen. Kun käytetään kahta – tai useampaa – tunnistautumistapaa yhdessä, tunnistautuminen on vahva (Vacca, 2013).

Monivaiheinen tunnistautuminen ei olekaan varsinaisesti vaihtoehto salasanojen käytölle, vaan useimmiten niiden käyttöä täydentävä menetelmä (ACSC, 2021). Se tarkoittaa siis useamman yllä mainitun tunnistautumismenetelmän yhteiskäyttöä, usein salasanaa ja vaikkapa mobiililaitteelta löytyvän autentikointiapplikaatiota (Garfinkel & Lipford, 2014). Yksinkertaisena esimerkkinä voidaan mainita pankkikortin käyttö maksupäätteellä: käyttäjän tulee paitsi tietää oma PIN-koodinsa (jotain-mitä-tiedät), myös hallittava kyseistä korttia (jotain-mitä-omistat) maksuhetkellä (Eve ym., 2019).

Vaccan (2013) mukaan turvallisin tapa onkin juuri tietämysperustaisen ja hallintaperustaisen tunnistautumisen yhdistelmä. Usein tällainen toteutustapa on seuraava: "Valtuustekijä on myönnetty tietylle käyttäjälle yhdistämällä sen sarjanumero käyttäjätietoihin […]. Kun käyttäjä kirjautuu tililleen […] hänelle esitetään haaste, johon tulee vastata myönnetyllä valtuustekijällä" (Vacca, 2013, s. 76).

Älypuhelinten aikakaudella kaksivaiheinen tunnistautuminen on tullut laajasti käyttöön joko tekstiviestiperustaisesti tai erillisellä applikaatiolla (Garfinkel & Lipford, 2014).

3 SALASANOJEN HALLINTA

Tämän pääluvun tarkoituksena on luoda katsaus niihin ongelmakohtiin, jotka muodostuvat, kun käytetään salasanoja tunnistautumismenetelmänä useissa palveluissa, sekä tarkastellaan salasanojen hallintasovellusten tarjoamaa mahdollista ratkaisua näihin ongelmiin.

Tietoturvallisuuden heikoimmaksi osaksi mielletään usein ihminen (ks. esim. Suo ym., 2005; Garfinkel & Lipford, 2014), ja salasanojen osalta tämä näkyy salasanojen vahvuudessa: helpoiten muistettavat salasanat ovat myös helpoimpia arvata tai murtaa (Garfinkel & Lipford, 2014). Kääntäen: mitä turvallisempi salasana on, sen todennäköisempää on, että sitä ei muista (O'Hanley & Tiller, 2014). Tämä voi johtaa turvallisuuden näkökulmasta huonoon salasanojen hallintatapaan: mikäli vaaditaan vaikeasti muistettavan salasanan luontia, käyttäjä saattaa kirjoittaa sen itselleen muistiin johonkin fyysisesti turvattomaan paikkaan (Adams & Sasse, 1999; O'Hanley & Tiller, 2014). Choong (2014) haastaa kuitenkin näkemyksen heikoimmasta lenkistä. Hänen mukaansa inhimillisiin tekijöihin liittyvä tutkimus on osoittanut, että käyttäjiltä vaaditaan salasanojen osalta kognitiivisesti kohtuuttomuuksia (Choong, 2014).

Zhang, Luo, Akkaladevi ja Ziegelmayer (2009) luokittelevat salasanat niiden ominaisuuksien mukaan pidemmälle: vahvojen ja muistettavien salasanojen lisäksi he mainitsevat kategorian salaiset salasanat. Se tarkoittaa salasanojen pysymistä piilossa muilta (J. Zhang ym., 2009). Salasanojen hallinnan kannalta oleellinen kysymys onkin, missä käyttäjä säilyttää salasanojaan. Stobertin ja Biddlen (2018) tutkimuksessa selvisi, että 78 % tutkittavista kirjoitti salasanansa muistiin joko digitaalisesti tai fyysisesti. Useimmat heistä kertoivat käyttävänsä menetelmää lähinnä muistia tukevana toimena (Stobert & Biddle, 2018).

3.1 Salasanojen uudelleenkäyttö

O'Hanleyn ja Tillerin (2014, s. 99) mukaan salasanojen uudelleenkäyttö tarkoittaa ”saman salasanan käyttämistä monessa järjestelmässä tai vaaditun salasanan

vaihtamisen jälkeiseksi nopeaksi takaisin muuttamiseksi". Kyseinen toimenpide on sekä hyvin yleistä että hyvin riskialtista (O'Hanley & Tiller, 2014).

Egelman ym. (2013) tutkivat salasanojen käyttöä ja heidän tulostensa mukaan yli puolet ihmisistä uudelleenkäyttää salasanojaan. Pearmanin ym. (2017) mukaan jopa yli neljä viidestä käyttäjästä käyttää joko osittain tai kokonaan salasanaansa useissa palveluissa. Heidän tutkimuksessaan 11 % osallistujista käytti pääasiallisena menetelmänään täsmälleen samaa salasanaa kaikkialla (Pearman ym., 2017).

Lyastani ym. (2018) toteavat, että usea käyttäjäprofiili vaarantuu jo yhdestä tietomurrosta, mikäli samaa salasanaa käyttää useassa palvelussa. Dasin, Bonneaun, Caesarin, Borisovin ja Wangin (2014) mukaan uudelleenkäyttöä on myös hankala torjua, koska sivuston sisäisistä turvallisuussyistä salasanojen vertailu eri palveluiden kesken ei usein onnistu. Toisaalta nk. SSO-menetelmät (Single sign-on, kertakirjautuminen), joissa yhdellä kirjautumisella pääsee tunnistautumaan useaan palveluun kerrallaan, ovat samasta syystä haasteellisia turvallisuuden kannalta: myös SSO:ta käytettäessä yhden salasanan paljastuminen altistaa useamman palvelun tunkeutujalle (Das ym., 2014).

Washin, Raderin, Bermanin ja Wellmerin (2016) tutkimuksen mukaan salasanojen uudelleenkäyttö ilmenee kahdessa kontekstissa: vahvempia salasanoja ja useimmin vierailtujen sivustojen salasanoja käytetään useimmin uudelleen. Tutkijat arvioivat, että vahvat salasanat, joita syötetään palveluihin usein, jäävät mieleen ja sitä kautta tulevat valituksi myös muilla sivustoilla (Wash ym., 2016). Toisaalta Woodsin (2017) tutkimuksen tuloksien mukaan on mahdollista, että salasanojen syöttämisen määrällä ei ole vaikutusta salasanojen muistamiseen. Hän kuitenkin toteaa, että aiheesta tulisi tehdä syvällisempää tutkimusta (Woods, 2017).

Washin ym. (2016) mukaan uudelleenkäyttö ei kuitenkaan välttämättä ole joka tapauksessa huono asia, esimerkiksi silloin kun mieleen painettua vahvaa salasanaa käytetään useammissa palveluissa. Toimintatapa voi tilanteesta riippuen olla parempi kuin heikompien salasanojen käyttö (Wash ym., 2016).

3.2 Salasanojen jakaminen

Singh, Cabraal, Demosthenous, Astbrink ja Furlong (2007) toteavat, että palveluiden turvallisuutta suunniteltaessa ei oteta huomioon, että salasanojen jakaminen on suosituksista huolimatta yleinen ilmiö. Heidän tutkimuksensa mukaan pankkipalveluissa salasanojen tai PIN-koodien jakaminen on yleistä parisuhteissa sekä kaukana palveluista asuvien ja joidenkin vammaisten ihmisten kohdalla (Singh ym., 2007).

Whittyn, Doodsonin, Creesen ja Hodgesin (2015) tutkimuksen mukaan hieman yli puolet tutkittavista kertoivat jakaneensa joskus salasanoja. Jakamiseen liittyen tilastollisesti merkittävästi esiin nousivat nuoret verrattuna vanhoihin käyttäjiin (nuoret jakoivat salasanoja enemmän) sekä persoonallisuuden puolelta korkea itsetarkkailun määrä oli salasanojen jakamista lisäävä tekijä. Tutkijat

nostivat mielenkiintoisena esimerkkinä esiin sen, että tietoturvatietoisuus ei ollut vaikuttava tekijä salasanojen jakamisessa (Whitty ym., 2015).

Van Ouytsel ja De Groote (2022) tutkivat nuorten käytöstä liittyen salasanojen jakamiseen, ja heidän mukaansa jakaminen voi olla joko hyvin tarkoituksellinen tai täysin spontaani teko. Se koetaan kuitenkin normatiiviseksi käytökseksi nuorten keskuudessa (Van Ouytsel & De Groote, 2022).

3.3 Salasanojen muistaminen

3.3.1 Muistamisen haasteet

J. Zhangin ym. (2009) mukaan ihmisen muistin kapasiteetti on lähes varmasti liian vajavainen nykypäivän salasanojen vaatimuksiin sekä niiden koko ajan kasvavaan määrään, mikä tuottaa ongelmia koko tunnistautumismenetelmälle. Yksittäinen salasana ei ole suurin ongelma, vaan käyttäjän tulee monen salasanan muistamisen lisäksi myös osata yhdistää ne oikeaan käyttäjäprofiiliin (J. Zhang ym., 2009). Myös Duggan, Johnson ja Grawemeyer (2012) uskovat muistin rajoitteiden olevan salasanojen turvallisuuteen liittyen relevantimpi aihealue kuin tietoturvakäyttäytyminen. Heidän mukaansa ihminen joutuu valitsemaan salasanansa muistin rajoitteiden puitteissa (Duggan ym., 2012).

Toisaalta Woodsin (2016) mukaan uniikit salasanat osataan yhdistää paremmin oikeaan käyttäjätunnukseen kuin muokatut tai uudelleen käytetyt salasanat. Lisäksi muokattuja ja uudelleen käytettyjä salasanoja syötetään useammin väärin kuin täysin uniikkeja salasanoja ja niitä on ylipäätään vaikeampi muistaa (Woods, 2016). Tamin, Glassmanin ja Vandenwauverin (2010) tutkimuksessa puolestaan käyttäjillä ei ollut ongelmia salasanojen muistamisessa.

Salasanan muistaminen ei ole yksioikoista, sillä se tulee ensin painaa mieleen ja pitää siellä ennen kuin on mahdollista käyttää sitä muistamalla se tunnistautumistilanteessa (Woods & Siponen, 2018). Usean salasanan muistaminen onkin ihmisen pitkäkestoiseen muistiin liittyvä haaste (J. Zhang ym., 2009).

Woods ja Siponen (2018) eivät kuitenkaan löytäneet tilastollista yhteyttä hyvän muistin ja oikeiden salasanojen muistamisen välillä. Lisäksi he tutkivat ihmisen niin sanottua metamuistia, joka koostuu ymmärryksestä ihmismuistiin liittyvistä strategioista, kapasiteetista ja tehtävistä. Myöskään metamuistilla ei ollut yhteyttä salasanojen muistamiseen (Woods & Siponen, 2018).

3.3.2 Muistamisen helpottaminen

Salasanojen muistamisen parannuskeinoja on kuitenkin tutkittu. Woodsin ja Siposen (2019) mukaan salasanan luomisvaiheessa vaaditut vahvistuskerrat lisäävät salasanan muistettavuutta. Mikäli salasana pitää vahvistaa kolme kertaa, salasanan muistettavuus kasvaa 70 prosenttiin aiemmasta (yhden vahvistuskerran) hieman yli 40 prosentista. Tämä ei tutkimuksen mukaan toisaalta vähennä merkittävästi ihmisten kokemaa käyttömukavuutta (Woods & Siponen, 2019). Vu ym.

(2007) ehdottavat hieman samankaltaista lähestymistapaa. Heidän mukaansa salasanan luomisen jälkeen tulisi vaatia useampi sisäänkirjautuminen, jotta salasana jää paremmin mieleen (Vu ym., 2007).

Vu ym. (2007) esittävät myös niin sanotun "alkukirjainlauseen" (engl. *first-letter sentence*) luomista. Siinä muodostetaan mielessä lause, josta otetaan jokaisen sanan ensimmäinen kirjain ja lisätään erikoismerkki sekä numero johonkin mielekkääseen kohtaan. Näin luodaan salasana, joka ei suoraan sisällä mitään sanakirjahyökkäyksellä vaarannettavaa sanaa (Vu ym., 2007).

Woods ja Silvennoinen (2022) tutkivat värien vaikutusta muistamiseen salasanojen kontekstissa. Heidän mukaansa valittavan värin lisääminen salasanaan ei ainoastaan lisää salasanan muistettavuutta, vaan tekee myös salasanasta turvallisemman lisäämällä sen entropiaa. He ehdottavat myös muiden visuaalisten elementtien lisäämisen tutkimusta (Woods & Silvennoinen, 2022).

Kuten viime luvussa todettiin, ainakin Australiassa on siirrytty suosittelemaan salasanalauseita (engl. *passphrase*) (ACSC, 2021). Ne ovat enemmän merkkejä sisältäviä, mutta paremmin muistettavia kokonaisia fraaseja, joiden turvallisuutta voidaan parantaa esimerkiksi tekemällä ne kaksikielisiksi (Maoneke, Flowerday & Isabirye, 2020). Käytännössä salasanalauseissa vaihdetaan eri merkkityyppien tuottama entropia merkkijono pituuden mukanaan tuomaan lisäturvallisuuteen (Bhana & Flowerday, 2020). Salasanalauseidenkin suhteen on kuitenkin ongelmia: käyttäjät valitsevat usein jonkun tutun fraasin esimerkiksi musiikista tai elokuvista, jolloin sanakirjahyökkäystä voidaan käyttää myös luomalla sanalistat kyseisen kaltaisista tunnetuista kulttuurituotteista (Kuo ym., 2006).

3.4 Salasanojen hallintasovellukset

3.4.1 Hallintasovellukset yleisesti

Salasanojen muistamiseen liittyvät haasteet ovat johtaneet salasanojen hallintasovellusten luomiseen – ensi kertaa jo 1990-luvulla (Woods & Siponen, 2019). Lyastanin ym. (2018) mukaan niiden kautta pyritään tuomaan käytettävyys ja turvallisuus lähemmäksi toisiaan salasanojen ympäristössä. Hallintasovellukset ovat yksinkertaisimmillaan niin sanottuja salasanalompakoita, jotka tallentavat käyttäjän kaikki salasanat yhden pääsalasanan taakse ja syöttävät ne automaattisesti palveluiden kirjautumisikkunoihin. Tämän lisäksi hallintasovellukset voivat auttaa käyttäjään luomaan turvallisia ja uniikkeja salasanoja eri palveluihin (Lyastani ym., 2018). Usean salasanan sijaan hallintasovellusta käytettäessä tarvitsee muistaa enää yksi, niin sanottu pääsalasana (Seiler-Hwang ym., 2019). Salasanojen luonnin ja säilyttämisen lisäksi salasanojen hallintasovellukset auttavat käyttäjää syöttämällä salasanan suoraan eri palveluihin (Oesch ym., 2022). Lisäksi sovelluksissa on useita työkaluja – kuten salasanavuodoista ilmoittaminen, monivaiheinen tunnistautuminen, salasanojen turvallisuusanalyysi sekä salasanojen jakomahdollisuus – jotka tukevat käyttäjien salasanakäyttäytymistä

(Seiler-Hwang ym., 2019). Erillinen hallintasovellus voidaan jakaa vielä kahteen alatyyppiin: tiedot pilveen tallentaviin sekä paikalliset tietokannat käyttäjän omiin laitteisiin tallentaviin järjestelmiin (Chaudhary, Schafeitel-Tähtinen, Helenius & Berki, 2019). Osa palveluista mahdollistaa molemmat talletustyypit.

Erillisen sovelluksen lisäksi yleinen salasanojen hallintajärjestelmän tyyppi on selainlaajennus (Ray ym., 2021). Selainlaajennus voi kuitenkin vaikuttaa salasanakäyttäytymiseen jopa negatiivisesti, mikäli se ei mahdollista vahvojen salasanojen luomista (Lyastani ym., 2018). Lisäksi selainlaajennuksena toimivista salasanojen hallintajärjestelmistä on löydetty haavoittuvuuksia (ks. esim. Barua, Zulkernine & Weldemariam, 2013), etenkin mikäli laajennus ei vaadi pääsalasanaa (Zhao & Yue, 2014). Kolmas suosittu hallintajärjestelmätyyppi on käyttöjärjestelmän sisäinen hallintapalvelu, kuten Applen Keychain (Ray ym., 2021; Stobert & Biddle, 2018).

Tässä tutkimuksessa tutkitaan nimenomaan erillistä hallintasovellusta selainlaajennuksen tai käyttöjärjestelmän sisäisen palvelun sijaan. Tutkimus ei erittele erillistä sovellusta talletustyypin (sisäinen vai pilvi) tai sen käyttölaitteen tai -järjestelmän mukaan.

3.4.2 Hallintasovellusten käyttö ja käyttämättömyys

Salasanojen hallintasovellusten käyttö on kuitenkin vähäistä (Ayyagari ym., 2019; Seiler-Hwang ym., 2019; Stobert & Biddle, 2018). Jonkinlaisen hallintajärjestelmän käyttäjistä suurin osa käyttää joko selainlaajennuksia tai käyttöjärjestelmän omaa järjestelmää (Mayer ym., 2022; Stobert & Biddle, 2018). Mayer ym. (2022) arvioivat selainlaajennusten suosion johtuvan siitä, että ne ovat valmiiksi käyttäjän käytettävissä ilman erillistä asentamista. Seiler-Hwangin ym. (2019) mukaan suurin osa tutkimukseen osallistuneista tiesi hallintasovelluksista, mutta vasta koittamisen jälkeen päätti itsekin alkaa käyttää sellaista.

Faganin, Albayramin, Khanin ja Buckin (2017) mukaan salasanojen hallintasovellusten käyttäjät ovat todennäköisemmin tietotekniikka- ja tietoturvaorientoituneempia kuin ne, jotka eivät järjestelmiä käytä. Osin vastakkainen näkemys on Alodhyanilla, Theodorakopoulosilla ja Reineckella (2020), joiden mukaan tietotekniikkaan tai tietoturvaan liittyvä koulutus ei lisää hallintasovellusten käyttöä. Suurin osa käyttää hallintasovelluksia käytön helppouden ja tietoturvallisuuden yhdistelmän vuoksi (Stobert & Biddle, 2018). Pearmanin ym. (2019) mukaan nimenomaan erillisten hallintasovellusten käyttäjät ajattelevat ensisijaisesti tietoturvaa, salasanojen muistamisen rajoitteita sekä sovellusten tarjoamia työkaluja. Lisäksi käyttöön ohjaavat sosiaalinen vaikutus, ajan ja oman muistikapasiteetin säästäminen sekä kokemukset aiemmista tietovuodoista.

Käyttämättömyyteen on monenlaisia syitä. Stobertin ja Biddlen (2018) tutkimuksen mukaan suurimmat syyt ovat luottamuksen puute, tarpeen puute sekä haluttomuus tilin alkujärjestelyyn (l. omien salasanojen syöttämiseen kerralla). Pearman ym. (2019) lisäävät listaan riskinarvioinnin ja tiedon puutteen. Ayyagarin ym. (2019) mukaan koettu helppokäyttöisyys oli – tutkijoiden mukaan epäintuitiivisesti – yhteydessä käyttämättömyyteen. He arvioivat, että käyttäjät kokevat helppokäyttöisyyden heikkouden osoituksena puhuttaessa ohjelmasta, jossa

on säilössä kaikki heidän salasanansa. Turvattomuus on keskeinen tekijä käyttämättömyydessä myös Faganin ym. (2017) tutkimuksen mukaan. Salasanojen hallintasovelluksia ei yksinkertaisesti mielletä turvallisiksi niiden toimesta, jotka eivät käytä kyseisiä järjestelmiä.

Eri tutkimuksissa esitetään useita ehdotuksia ja näkemyksiä käyttäjämäärien nostamiseksi. Farooq, Dubinina, Virtanen ja Isoaho (2021) toteavat, että palveluntarjoajan maine sekä riskejä vastaan annetut vakuudet lisäävät luottamusta ohjelmaan. Seiler-Hwangin ym. (2019) mukaan ohjelmat eivät tarjoa tarpeeksi hyvää ohjeistusta käyttöä varten. Lisäksi turvallisuuden ja turvallisuusviestinnän parantaminen madaltaisi heidän näkemyksensä mukaan kynnystä aloittaa ohjelman käyttö. Stobert ja Biddle (2018) jakavat näkemyksen tietoturvaviestinnästä. Lisäksi he toteavat, että sovellusten integrointi eri käyttöjärjestelmiin ja selaimiin lisäisi käyttäjien määrää. Pearman ym. (2019) puolestaan painottavat käytettävyyden parantamista ja testaamista sekä vähemmän tietoturvaorientoituneiden käyttäjien huomioon ottamista. Samaa mieltä ovat myös Alodhyani ym. (2020), joiden mielestä paitsi sovellusten sisältämä työkalujen määrä myös niiden käyttämä kieli on liian teknistä, mikä vähentää aloittelijoiden halua aloittaa käyttö. Toinen näkökulma käytön lisäämiseen on sovellusten suositteleminen tai vaatiminen. Oesch ym. (2022) toteavat, että eräs suurimmista syistä käytön aloittamiseen on se, että sitä vaaditaan työympäristössä. Myös Mayerin ym. (2022) mukaan ympäristöllä on vaikutusta suosituksen muodossa: organisaation jäsenet luottavat paremmin sovellukseen, jota suositellaan ylhäältä päin. Alkaldin, Renaudin ja Mackenzien (2019) tulokset täydentävät tätä koskemaan kaikilla tasoilla tapahtuvaa suosittelemista jo sovelluksia käyttävien henkilöiden toimesta. Albayramin, Liun ja Cangonjin (2021) mukaan suosittelumuodollakin on merkitystä. Video osoittautui moninkertaisesti tehokkaammaksi suosittelutavaksi kuin teksti. Lisäksi autonomia – esimerkiksi mahdollisuus vaikuttaa itse siihen, mitä sovellusta alkaa käyttää – on keskeisessä osassa ihmisen päätöksessä ottaa hallintasovellus käyttöön (Alkaldi ym., 2019).

3.4.3 Hallintasovellusten käytön haasteet

Toisaalta Faganin ym. (2017) mukaan hallintasovellusten käyttäjätkään eivät aina miellä järjestelmiä turvallisiksi, vaan helppous on heidän pääsyynsä käyttää sovelluksia. Tämä on johtanut muun muassa siihen, että osa käyttäjistä ei talleta hallintasovellukseen kaikkein tärkeimpien tiliensä salasanoja, koska ei luota järjestelmään. Sen myötä osa hallintasovelluksen käytön hyödyistä turvallisuuden näkökulmasta katoaa (Fagan ym., 2017). Tämä on kuitenkin Pearmanin ym. (2019) mukaan nähtävissä lähinnä sisäänrakennettujen hallintajärjestelmätyyppien käyttäjien osalta, sillä erillisten sovellusten käyttäjät ajattelevat lähtökohtaisesti turvallisuusnäkökulma edellä.

Hallintasovelluksen käyttö ei kuitenkaan vielä tarkoita, että käyttäjä loisi turvallisen salasanan käyttäen ohjelman tarjoamaa generaattoria. Seiler-Hwang ym. (2019) toteavat, että yli 70 prosenttia käyttäjistä loi salasanan itse. Syiksi he luettelivat tiedon, mielenkiinnon sekä luottamuksen puutteet. Pearmanin ym. (2019) tutkimuksessa osa kertoi käyttävänsä omia salasanoja, koska heidän

mielestään oli tärkeätä hallita ja muistaa ne itse. Lisäksi käyttäjät käyttivät vanhoja salasanojaan erityisesti, kun järjestelmän käytön kanssa oli ongelmia. Myös Oeschin ym. (2022) tutkimuksessa selvisi, että osa käyttäjistä on huolissaan, että he eivät kykene käyttämään generoituja salasanoja niillä alustoilla, joilla sovellus ei ole käytössä. Alodhyani ym. (2020) toteavat, että käyttäjistä suuri osa jättää salasanageneraattorin käytön väliin, sillä heidän pääasiallinen sovellusten käyttötarkoitus on salasanojen säilöntä ja kirjautumisikkunoiden automaattinen täyttö. Generoinnin lisäksi käyttäjät eivät aktiivisesti käytä muitakaan palveluiden tarjoamia lisätyökaluja (Oesch ym., 2022; Pearman ym., 2019).

Hallintasovellukset sisältävät myös sellaisia turvallisuuteen ja käytettävyyteen liittyviä ongelmia, jotka suoraan tai välillisesti haittaavat niiden käyttöä. Pearmanin ym. (2019) mukaan salasanojen keskitetty hallinnointi johtaa siihen, että kaikki käyttäjän kirjautumistiedot ovat saatavilla samasta paikasta. Tällöin kaikki vaarantuvat esimerkiksi pääsalasanan päätyessä vääriin käsiin. Myös heikko pääsalasana voi täten muodostua ongelmaksi (Chaudhary ym., 2019). Seiler-Hwang ym. (2019) mainitsevat joidenkin sovellusten mahdollisiksi ongelmakohdiksi muiden muassa tietokannan riittämättömän suojauksen sekä automaattisen täytön turvattomuuden. Myös Silver, Jana, Boneh, Chen ja Jackson (2014) ovat todenneet automaattisen täytön olevan ongelmakohta. Lisäksi avainten varastaminen sekä väliaikaisten tiedostojen käyttäminen hyökkäysvektorina ovat tunnettuja heikkouksia hallintasovelluksissa (Huaman ym., 2022).

Oesch ym. (2022) sekä Chaudhary ym. (2019) nostavat esiin käytettävyyden haasteet. Mobiilisovellusten ongelmat automaattisen täytön, laitteiden välisen synkronoinnin ja pysyvän kirjautumisen kohdalla vähentävät niiden käyttöä (Oesch ym., 2022). Myös usean erityyppisen hallintajärjestelmän (esimerkiksi sekä selainlaajennuksen että erillisen hallintasovelluksen) käyttö saattaa vähentää turvallisuutta. Chaudhary ym. (2019) ovat huolissaan hallintasovelluksiin liittyvästä tutkimuksesta, joka on heidän mielestään liian teknispainotteista käyttäjäkeskeisyyden kustannuksella. He esittävätkin, että käytettävyys nähtäisiin välttämättömänä turvallisuuden mahdollistajana sen sijaan että ne koettaisiin vastakohdiksi.

3.4.4 Hallintasovellusten vaikutus salasanoihin

Lyastani ym. (2018) toteuttivat tutkimuksen salasanojen hallintasovellusten käytön vaikutuksesta salasanojen vahvuuteen ja uudelleenkäyttöön. Tutkijat yhdistivät kvalitatiivista ja kvantitatiivista dataa, tarkoituksenaan selvittää käytetäänkö hallintasovelluksia vahvojen, todennäköisesti generaattorilla luotujen, salasanojen vai luultavasti heikompien, itse tehtyjen salasanojen säilyttämiseen sekä vaikuttaako sovelluksen käyttö myös salasanojen uniikkiuteen eri palveluissa.

Lyastanin ym. (2018) keskeisin löydös on, että hallintasovelluksen käyttö lisää sekä salasanojen vahvuutta että niiden uniikkiutta. Molempiin vaikutti erityisesti sovelluksen tarjoaman – tai joissain tapauksissa ulkopuolisen – salasanageneraattorin käyttäminen apuna salasanan luonnissa. Lisäksi tutkijat havaitsivat, että käyttäjän itse ilmoittama salasanan vahvuus indikoi vahvaa salasanaa

myös mittauksen kautta, eli käyttäjät ovat tietoisia käyttämiensä salasanojen vahvuudesta. Toisaalta heidän havaintojensa mukaan uniikkiuden käsite on hankalampi ymmärtää: käyttäjät arvioivat salasanojensa ainutlaatuisuutta sen osalta, käyttävätkö he henkilökohtaisesti kyseistä salasanaa useammissa palveluissa, kun tutkijoiden näkemys uniikkiudesta sisälsi kaikkien mahdollisten käyttäjien kaikki mahdolliset salasanat.

Lyastani ym. (2018) esittävät jatkokysymyksen sen osalta, miksi hallintasovellusten käyttäjillä silti on joissain palveluissa heikkoja tai uudelleen käytettyjä salasanoja. He pohtivat, että syynä saattavat olla vähemmän tärkeille sivustoille luodut salasanat, yhteiskäyttösalasanat tai hallintasovelluksen käyttöä edeltäneeltä ajalta periytyneet salasanat.

Samankaltaisuuksista huolimatta Lyastanin ym. (2018) tutkimustavoitteet eivät ole yksi yhteen tämän tutkimuksen kanssa, sillä he vertasivat hallintasovellusten käyttäjiä niihin, jotka eivät sovelluksia käyttäneet. Tässä tutkimuksessa puolestaan selvitetään, onko yksittäisen henkilön salasanakäyttäytyminen muuttunut hallintasovelluksen käyttöön ottamisen seurauksena. Kuten Fagan ym. (2017) toteavat, hallintasovellusten käyttäjät ovat tietoturvaorientoituneempia kuin niitä käyttämättömät. On siis mahdollista, että eroa salasanakäyttäytymisessä – sekä salasanojen vahvuuden että uniikkiuden osalta – on voinut olla jo ennen hallintasovellusten käyttöönottoa. Lisäksi kvalitatiivisen menetelmän avulla tässä tutkimuksessa pyritään selvittämään, millaisilla eri tavoilla hallintasovelluksen käyttö vaikuttaa salasanoihin.

4 TIETOTURVALLISUUSKÄYTTÄYTYMINEN

Tässä pääluvussa tarkastellaan syitä sille, miksi ihmiset eivät tee optimaalisia asioita salasanaturvallisuutensa eteen. Lisäksi esitellään tietoturvatutkimuksessa esille noussut ilmiö kotikäyttäjien tietoturvan tutkimuksen vähäisyydestä.

Yildirimin ja Mackien (2019) mukaan ”inhimilliset tekijät ovat avainasemassa salasanaturvallisuudessa” (Yildirim & Mackie, 2019, s. 742). Furnell (2022) laajentaa salasanakäyttäytymisen ongelmat yleisesti kyberturvallisuuden ongelmiksi: vuosia ja vuosia tunnistettu ongelma salasanojen heikkoudessa ei ole näkynyt tarpeeksi hyvin käyttäjien valistamisessa vahvojen salasanojen ja turvallisen salasanahallinnan osalta. Koko tietoturvakentän kontekstissa inhimillisiin tekijöihin kiinnitetään aiempaa enemmän huomiota, mutta ne jäävät silti sivurooliin (Furnell, 2022).

Tietoturvallisuuskäyttäytyminen on kompleksinen ilmiö, sillä siihen liittyvät useat eri vaikutteet, kuten turvallisuusympäristö sekä yksilön kognitiiviset kyvyt, persoonallisuuden piirteet ja suhde riskiin (Parsons, McCormac, Butavicius & Ferguson, 2010). Tietoturvakenttääkään ei toisaalta voi inhimillisten tekijöiden kyseessä ollessa niputtaa yhdeksi kokonaisuudeksi, sillä esimerkiksi eri kulttuureissa tarvitaan erilaisia lähestymistapoja tietoturvavalistuksen osalta (Karjalainen, Siponen, Puhakainen & Sarker, 2013).

Grawemeyer ja Johnson (2011) löysivät salasanoihin liittyen kolme syytä ”heikkoon turvallisuuteen inhimillisestä näkökulmasta: turvallisuustiedon puute, väärä tieto sekä huonot strategiat salasanaylikuormituksen käsittelemiseksi” (Grawemeyer & Johnson, 2011, s. 263). He toteavatkin, että inhimillisten tekijöiden huomioon ottaminen on keskeisessä roolissa tietoturvaohjeistuksessa ja -koulutuksessa.

4.1 Tietäminen vs. tekeminen

Puhakaisen (2006) mukaan tietoturvaohjeistuksen noudattamiseen kannustaminen jaetaan kahteen kategoriaan: kognitiivisiin ja behavioralistisiin

lähestymistapoihin. Ensin mainittu keskittyy yksilön ymmärryksen parantamiseen tietoturvan merkityksestä. Yrityksissä työntekijöiden tietoturvaymmärrystä pyritään usein parantamaan kahdella erillisellä tavalla – tehokkaalla viestinnällä sekä käyttäjien osallistamisella tietoturvallisuuden suunnitteluun. Behavioralistisesti asiaa voidaan puolestaan lähestyä joko palkinnoin tai rangaistuksin (Puhakainen, 2006).

Yildirimin ja Mackien (2019) mukaan suurin osa ihmisistä ymmärtävät vahvojen salasanojen merkityksen, mutta eivät saa tarpeeksi tukea tai motivointia niiden tekemiseen. Vaikka ohjeita on esimerkiksi verkkosivuilla tarjolla, ne eivät ole riittäviä, koska ihmiset eivät noudata niitä. Pelkästään salasanarajoituksiin perustuva lähestymistapa toimiikin huomattavasti huonommin, kuin käyttäjän tukeminen ja visuaalisen palautteen antaminen salasanan luomishetkellä. Myös esimerkit heikon salasanan vaikutuksesta voivat vaikuttaa salasanaa luodessa sen vahvuuteen parantavasti (Yildirim & Mackie, 2019). Vance, Eargle, Eggett, Straub ja Ouimet (2022) toteavat, että pelkkä passiivinen viesti heikon salasanan uhkista ei riitä, vaan viestinnässä tulee olla interaktiivisuutta. Heidän mukaansa vahvuusmittarinkaan käyttö ei johda vahvempiin salasanoihin, vaan menetelmän pitäisi lisäksi opastaa käyttäjä paremman salasanan luontiin (Vance ym., 2022) Myös Furnell (2022) sysää vastuuta nimenomaan palveluntarjoajien suuntaan sekä ohjeiden että vaatimusten osalta. Toisaalta Tamin ym. (2010) mukaan ”käyttäjät ymmärtävät eron hyvän ja huonon salasanan välillä sekä huonon salasanojen hallinnan seuraukset” (Tam ym., 2010, s. 242).

Kaleta, Lee ja Yoo (2019) tutkivat abstraktin ja konkreettisen ajattelun eroja salasanojen muodostamisessa nk. *Construal level theory*n kautta. Heidän mukaansa abstraktimmalla tasolla ajattelevat ihmiset muodostavat vahvempia salasanoja. Tutkijat ehdottavatkin, että salasanojen luontivaiheessa käyttäjää tulisikin motivoida ennemmin ylemmän tason ”miksi”-kysymyksillä pelkän oikean toimintatavan opastamisen sijaan (Kaleta ym., 2019).

Mazurek ym. (2013) esittivät kaksi kognitiivista syytä heikommille salasanoille joidenkin yliopiston laitosten henkilökunnan kohdalla. Ensimmäinen liittyi yksinkertaisesti siihen, että he eivät olleet saaneet tarpeeksi tietoa hyvästä salasanakäyttäytymisestä. Toiseen mahdolliseen selitykseen – käyttäjän kokemukseen siitä, että he eivät henkilökohtaisesti tee vahvalla salasanalla mitään – vastattiin ehdottamalla nimenomaan kollektiiviseen tietoturvaan liittyvää koulutusta (Mazurek ym., 2013).

Myös sekä Egelman ym. (2013) että Tam ym. (2010) toteavat, että käyttäjät tietävät vahvan salasanan vaatimukset. Esimerkiksi vähemmän tärkeiden tilien kohdalla heikon salasanan valitseminen johtui puhtaasti motivaation puutteesta vahvaa salasanaa kohtaan (Egelman ym., 2013). Käyttäjät saattavat siis ajatella, ettei kyseisen salasanan heikkous johda negatiivisiin seurauksiin, joten käytettävyys voittaa turvallisuuden (Tam ym., 2010). Syyksi huonoihin tapoihin salasanojen valinnassa Zhang ja McDowell (2009) toteavat ihmisen taipumuksen säästää kognitiivista kapasiteettiaan. Sen vuoksi motivaatio on isossa roolissa, jotta käyttäjä olisi valmis luomaan – ja muistamaan – vahvan salasanan (L. Zhang & McDowell, 2009).

Pohjimmiltaan kyseessä on kamppailu käytettävyyden ja turvallisuuden välillä, johon syvennytään seuraavassa alaluvussa.

4.2 Käytettävyys vs. turvallisuus

Garfinkel ja Lipford (2014) toteavat, että salasanojen poistuminen ei ole lähiaikoina näköpiirissä, sillä ihmiset haluavat internetin käytöstään sujuvaa ja mahdollisimman viiveetöntä. Salasanojen käyttäminen on edelleen ”vähiten huono” vaihtoehto, kun otetaan huomioon nimenomaan käytettävyyden ja turvallisuuden välinen suhde. Salasanaan liittyvät ongelmat kuitenkin kasvavat jatkuvasti palveluiden määrän ja murtautumiseen käytettävien tietokoneiden tehojen kasvaessa (Garfinkel & Lipford, 2014). Heikkojen salasanojen yhteys käytettävyyteen on todettu ensi kertaa jo viime vuosituhannen puolella (Adams & Sasse, 1999).

Qureshi ym. (2009, s. 11) nimeävät salasanan muistettavuuden ja turvallisuuden välisen ristiriidan “klassiseksi salasanaongelmaksi”. Näennäisen satunnaisuuden ja vaikeasti arvattavuuden lisäksi turvallisuutta tulisi parantaa säännöllisellä salasanojen vaihtamisella ja uniikkiudella eri palveluissa. Turvallisuuteen vedoten näitä erilaisia salasanoja ei myöskään tulisi kirjoittaa tai tallentaa mihinkään selkokielisinä. Tämä ristiriita aiheuttaa kompromisseja käytettävyyden ja turvallisuuden välille (Qureshi ym., 2009).

Myös Yildirim ja Mackie (2019) mainitsevat käytettävyyden ongelmasta. Heidän mukaansa helposti muistettavat salasanat ovat yleensä lyhyitä tai korkeintaan hieman yleiskielen sanoja muuttavia, jolloin ne on helpompi murtaa – tai vaihtoehtoisesti sisältävät arvaamista helpottavia henkilökohtaisia tietoja. Salasanojen käyttö tunnistautumismenetelmänä ei olekaan ongelma teknisestä näkökulmasta, vaan haasteet kumpuavat nimenomaan ihmisestä käyttäjänä (Yildirim & Mackie, 2019).

Käyttäjien vastaus tähän ristiriitaan on selkeä: muistettavuus valitaan lähtökohdaksi turvallisuuden kustannuksella (Kanta, Coray, Coisel & Scanlon, 2021). Lisäksi salasana luodaan pääosin tilanteessa, jossa halutaan päästä käyttämään palvelua, eikä luodun salasanan hyvälle mieleen painamiselle ole aikaa (Brown, Bracken, Zoccoli & Douglas, 2004). Usein muistettavuus ohjaa salasanan osittamiseen, jolloin salasana on pituutensa puolesta laskettavissa turvalliseksi, mutta sen sisältö voidaan pilkkoa helpommin murrettaviksi kokonaisuuksiksi kuten nimiksi tai yleiskielen sanoiksi (Kanta ym., 2021).

Heikot salasanat eivät ole ainoa seuraus: vaatimukset aiheuttavat ihmisissä muitakin käytettävyyteen liittyviä huonoja toimintatapoja, kuten salasanojen kirjoittamista muistiin ja saman salasanan käyttämistä eri palveluissa (J. Zhang ym., 2009).

Toisaalta Bonneau, Herley, Van Oorschot ja Stajano (2012) muistuttavat, että käytettävyyden ja turvallisuuden suhde ei ole yksioikoinen, vaan molemmat ovat monipuolisia kokonaisuuksia. Yksi syy salasanojen käytön jatkumiselle onkin, että uusien tunnistautumistapojen osalta ei osata nähdä kunnolla

kokonaiskuvaa, vaan tarkastellaan aihetta vain yhdestä näkökulmasta kerrallaan (Bonneau ym., 2012).

Myös Wash ym. (2016) toteavat ideaaliuteen pyrkimisen muodostavan enemmän ongelmia kuin parantunutta turvallisuutta. Mikäli mitään mahdollista haavoittuvaisuutta ei sallita, saattaa käyttäjien todellisen käytöksen syyt ja seuraukset hämärtyä (Wash ym., 2016).

Haaste onkin niin laaja, että sitä on tutkittu pian puoli vuosisataa (ks. esim. Morris & Thompson, 1979), mutta käytettävyyden ja salasanan vahvuuden välisen suhteen parantamisesta – eli miten parantaa salasanaa enemmän kuin miten se hankaloittaa muistamista – on kuitenkin vähän tutkimusta (Egelman ym., 2013).

Brown ym. (2004) antavat suoraan vinkiksi käyttäjälle erotella tärkeät tilit vähemmän tärkeistä. Ainoastaan erityistä turvallisuutta vaativille tileille tulisi luoda vahvempi salasana, joka painetaan eri keinoin mieleen (Brown ym., 2004). Tämä vaikuttaakin olevan käyttäjien toimintatapa, sillä vähemmän tärkeiden sivustojen tarjoamana salasanan vahvuusmittari ei johda vahvempiin salasanoihin (Egelman ym., 2013). Toisin sanoen salasanojen laatu on yhteydessä käyttäjien arvioimaan riskiin sen suhteen, kuinka arvokkaaksi he kokevat salasanan turvaaman tiedon (Creese, Hodges, Jamison-Powell & Whitty, 2013).

Kuten edellisessä pääluvussa havaittiin, käytettävyyden ja turvallisuuden välinen tasapainottelu on läsnä myös salasanojen hallintasovellusten kontekstissa. Kun ilman hallintasovelluksia käytettävyys on näyttäytynyt helposti muistettavina salasanoina, sovellusten kanssa se ilmenee koettuna hankaluutena ottaa erillinen ohjelma käyttöön. Toisaalta tasapainottelu näkyy myös käänteisesti: käyttäjät kokevat, että ohjelmien mukanaan tuoma helppous tai käytettävyys ei riitä voittamaan heidän epäilyksiään kaikkien salasanojensa luovuttamisesta yksittäiselle toimijalle.

4.3 Työympäristö vs. henkilökohtainen käyttö

Työympäristöön liittyvää tutkimusta tietoturvaohjeistuksien noudattamisesta on paljon (ks. esim. Bulgurcu, Cavusoglu & Benbasat, 2010; Crossler ym., 2013; Karjalainen, Sarker & Siponen, 2019; L. Li ym., 2019; Liu, Huang, Wang & Liu, 2019; Vance ym., 2022).

Li ja Siponen (2011) kuitenkin toteavat, että niin sanotun kotikäytön tutkimusta on siihen nähden hyvin vähän, eivätkä kyseiset kaksi ympäristöä ole kaikissa tietoturvakontekstin osa-alueissa samankaltaiset. Heidän mukaansa tietoturvatutkimus ei ole ottanut näitä eroavaisuuksia huomioon. Tutkijat esittävät yhdeksän eri kontekstia, joissa yksilön tietoturvakäyttäytyminen saattaa erota työpaikan ja kodin välillä: tietoturvakoulutuksen rooli, toimintakäytänteet, IT-tuki, monitorointi, pelkotekijät, turvallisuusilmasto, vaadittu kontrolli, verkkoturvallisuus sekä tietokoneiden jakaminen. Näiden myötä ihmisen käytöstä tietoturvan näkökulmasta ei voi tarkkailla vain yhdessä ympäristössä (Y. Li & Siponen, 2011).

Li, Xin ja Siponen (2022) täydentävät tätä näkökulmaa puhumalla "kansalaisen kyberturvallisuuskäyttäytymisestä". Heidän mukaansa viimeistään COVID-19-pandemian mukanaan tuoma etätyöskentelyn lisääntyminen aiheuttaa haasteita ainakin kodin tietoverkon turvattomuuden, yhteiskäyttötyökalujen sekä perheenjäsenien käytöksen osalta. Lisäksi käyttäjien välillä on demografisia, tiedollisia sekä näkökulmallisia eroja, jotka näkyvät eri lailla työ- ja kotiympäristöissä. Tutkijat toteavat, että henkilökohtaisen tietoturvakäyttäytymisen parantaminen vaatii koulutusta, jollaista on usein tarjolla työympäristöissä, mutta ei kotikäyttäjille. He ehdottavat, että parhaana vaihtoehtona koulutusta tarjoaisi valtio, mikä tarkoittaisi joitain muutoksia hallinnon tasolla, sekä erilaisia kampanjoita eri ihmisille (Y. Li ym., 2022).

Andersonin ja Agarwalin (2010) mukaan kotikäyttäjät ovat heikko lenkki tietoturvallisuudessa juuri sen takia, että he eivät saa töiden puolesta koulutusta tai IT-osaston tuomaa tukea. Heidän tutkimuksensa mukaan kognitiiviset, psykologiset ja sosiaaliset tekijät vaikuttavat kotikäyttäjien aikeisiin tietoturvakontekstissa, ja kyseisiä tekijöitä pystyy muokkaamaan positiivisen viestinnän avulla. Toisaalta heidän mukaansa tulee ottaa huomioon myös kohde, johon nähden kotikäyttäjän tietoturvakäyttäytymistä arvioidaan, sillä toiminta johtuu eri tekijöistä, jotka vaihtelevat sen mukaan, kokevatko käyttäjät suojaavansa esimerkiksi fyysistä tietokonetta vai digitaalista dataa. Tutkijat toteavat, että ymmärtämällä kotikäyttäjien käyttäytymistä, myös organisaatiot voivat luottaa esimerkiksi verkkokaupan toimivuuteen (Anderson & Agarwal, 2010).

5 TUTKIMUSMENETELMÄ

Tässä pääluvussa esitellään tutkimuksessa käytetty tutkimusmenetelmä. Ensin perustellaan menetelmän valinta, minkä jälkeen esitellään tutkimusprosessi aineiston keräämisen ja analysoinnin osalta. Lopuksi arvioidaan tutkimuksen luotettavuutta sen validiteetin ja reliabiliteetin kautta.

5.1 Tutkimusmenetelmän valinta

Kvalitatiivisessa eli laadullisessa tutkimuksessa tutkimuksen tekijä on keskeinen osa tutkimusprosessia hänen myös tulkitessaan dataa sen keräämisen lisäksi (Corbin & Strauss, 2015). Corbin ja Strauss (2015) listaavat asioita, joiden vuoksi laadullinen tutkimus voidaan valita kvalitatiivisen eli määrällisen tutkimuksen sijaan. Heidän mukaansa laadullista tutkimusta voidaan tehdä muun muassa

- tutkittavien sisäisten kokemusten tutkimiseksi
- merkitysten muotoutumisen ja muuttumisen tutkimiseksi
- alueiden, joita ei ole vielä tutkittu läpikotaisin, tutkimiseksi
- totta löydettäisiin olennaisia muuttujia, joita myöhemmin voidaan testata kvantitatiivisilla tutkimustavoilla
- holistisen tai kokonaisvaltaisen lähestymistavan ottamiseksi ilmiön tutkimukseen (Corbin & Strauss, 2015, s. 5).

Kuten aiemmin on todettu, hallintasovellusten vaikutusta salasanoihin ei ole juurikaan tutkittu. Sen vuoksi on perusteltua valita tutkimukselle kvalitatiivinen lähestymistapa, jotta uuden aihealueen tutkimisen lisäksi tuloksia voidaan käyttää pohjana jatkotutkimukselle eri menetelmin. Kvantitatiivisella menetelmällä olisi ollut mahdollista saada eri vaikutusten suuruusluokat selville, mutta joitain syitä ja käyttötapauksia olisi voinut jäädä selviämättä. Lisäksi Lyastani ym. (2018) olivat jo toteuttaneet samankaltaisia tutkimuskysymyksiä sisältävän tutkimuksen määrällisesti.

Jotta voidaan selvittää, miten hallintasovellusten käyttäjien salasanakäyttäytyminen on muuttunut ohjelman käytön myötä, aineiston keruumenetelmäksi valikoitui haastattelu. Kyselyyn verrattuna haastattelu muun muassa mahdollistaa syventymisen haastateltavien henkilökohtaisiin kokemuksiin sekä auttaa selventämään vastauksia tarvittaessa (Hirsjärvi ym., 2009). Kyseiset edut hyödyntävät myös tätä tutkimusta, koska aiheena on vähäisesti tutkittu ilmiö.

Corbinin ja Straussin (2015) mukaan haastattelut jaetaan kolmeen alakategoriaan: strukturoimattomaan, semistrukturoituun sekä strukturoituun haastatteluun. Nimiensä mukaisesti ne eroavat siis siinä, miten haastattelun rakenne on suunniteltu etukäteen. Mitä vähemmän rakennetta haastatteluun on luotu, sen vapaammin haastateltavat pystyvät itse määrittämään kulloisenkin keskustelunaiheen. Tarkoituksena ei kuitenkaan usein ole täysi vapaus aiheiden sisällä, vaan haastattelija voi ohjata keskustelua takaisin aiheen äärelle, mikäli olennaisesta poiketaan selvästi (Corbin & Strauss, 2015).

Semistrukturoidussa haastattelussa puolestaan mahdollistetaan tutkijalle kyky ”säilyttää johdonmukaisuutta konsepteista, joita käsitellään joka haastattelussa” (Corbin & Strauss, 2015, s. 39). Haastattelurungon avulla saadaan halutut teemat käytyä läpi kaikkien haastateltavien kanssa. Strukturoimattomuuden piirteenä haastattelija voi kuitenkin syventyä johonkin teemaan pidemmäksi aikaa tiettyjen haastateltavien kanssa. Lisäksi haastateltavalle annetaan mahdollisuus lisätä olennaisiksi kokemiaan asioita, mikäli ne eivät ole tulleet haastattelussa aiemmin esiin (Corbin & Strauss, 2015).

Corbinin ja Straussin (2015) mukaan stukturoidussa haastattelussa kaikki kysymykset on ennalta suunniteltu. Heidän mukaansa se on keino johdonmukaisuuteen haastateltavien välillä, mutta se ei mahdollista joustavuutta, mikäli se koetaan aineiston keräämiseksi tarpeelliseksi. Strukturoitu haastattelu onkin hyvin lähellä strukturoitua kyselyä (Hirsjärvi ym., 2009).

Suomessa tietynlaisesta epästrukturoidun ja stukturoidun haastattelun väliltä löytyvästä haastattelutyypistä käytetään nimeä teemahaastattelu (Eskola, Lätti & Vastamäki, 2018). Se valikoitui tämän tutkimuksen aineistonkeruumenetelmäksi, koska alaluvussa 1.2 esitellyt alatutkimuskysymykset muodostavat selkeät teemalliset kokonaisuudet. Lisäksi sen avulla on mahdollista päästä haastattelutilanteessa syvemmälle johonkin tiettyyn aihealueeseen, mikäli siitä nousee pintaan asioita, joihin ei etukäteen ole valmistauduttu.

Tekstiaineiston – tässä tapauksessa haastatteluaineiston litteraatioiden – työstämiseen on Flickin (2009) mukaan kaksi perusstrategiaa: koodaaminen, jolla pyritään kategorisoimaan aineistoa sekä sekvenssianalyysi, jolla tekstin ja tapauksen rakenne pyritään järjestelemään uudelleen.

Tässä tutkimuksessa alatutkimuskysymyksiin vastaaminen ohjaa käyttämään koodausta. Sen myötä mahdollistetaan temaattinen analyysi, jolla voidaan Aronsonin (1995) mukaan keskittyä ”[…] käyttäytymisen tunnistettaviin teemoihin ja kaavoihin” (Aronson, 1995, s. 1). Koska salasanojen vahvuus ja hallinta perustuu käyttäjän omiin valintoihin ja toimiin kulloisessakin salasanasyklin vaiheessa – eli luomisessa, varastoinnissa ja syöttämisessä (ks. esim. Lyastani ym.,

2018; Stobert & Biddle, 2018) –, temaattinen analyysi sopii tutkimusaineiston analysointiin eri käyttäytymismallien löytämiseksi.

5.2 Tutkimusprosessi

5.2.1 Aineiston kerääminen

Teemahaastattelun runko luotiin alatutkimuskysymysten ympärille. Teemoiksi valikoituivat salasanojen vahvuus, salasanojen erilaisuus sekä salasanojen hallinta. Näiden lisäksi kehitettiin joukko tukikysymyksiä, jotka mahdollistivat haastateltavan salasanojen käytön taustan hahmottamisen. Taustatekijöinä kysyttiin tutkittavan ikää, toimenkuvaa, käytettävää ohjelmaa sekä heidän omaa kokemustaan omasta tietoturvaosaamisestaan salasanojen kontekstissa. Teemahaastattelun periaatteiden mukaisesti teemojen sisälle luotiin apukysymyksiä, mutta jätettiin myös tilaa keskustelun mahdollisen laajenemisen mahdollistamiseksi. Haastattelurungon muodostamista – ja myöhemmin itse haastattelua – helpotti se, että tutkijalla oli aihealueesta myös käytännön tietämystä käytettyään salasanojen hallintasovellusta itse yli vuoden.

Tutkimuksessa haastateltiin yhteensä 13 henkilöä. Kohdejoukko tutkimukseen valittiin kahdella tapaa: suurin osa tutkittavista vastasi Jyväskylän yliopiston informaatioteknologian opiskelijoiden sähköpostiryhmään lähetettyyn viestiin, jossa ilmoitettiin etsittävän salasanojen hallintasovellusta käyttäviä kohdehenkilöitä tutkimusta varten. Sen lisäksi samankaltainen viesti välitettiin muutamalle suomalaiselle ei-tietotekniikka-aiheiselle keskustelupalstalle. Tämän tarkoituksena oli saada varianssia haastateltavien taustoihin ja mahdolliseen tietoturvakokemukseen. Haastateltavien toimenkuvat on esitelty taulukossa 3.

TAULUKKO 3 Haastateltavien toimenkuvat

Haastateltava	Toimenkuva
H1	opiskelija
H2	opiskelija
H3	tuotepäällikkö
H4	Information Security Officer
H5	tuottaja / sisältökoordinaattori
H6	tietoturvakonsultti
H7	teknisen tuen asiantuntija
H8	integraatiokehittäjä
H9	Information Technology Manager
H10	IT-projektipäällikkö
H11	AY-liikkeen asiantuntija
H12	turvakeskuksen tilannepäivystäjä
H13	tietoturva-asiantuntija

Haastateltavat valittiin ilmoittautumisjärjestyksessä, eli hallintasovelluksen käyttämisen lisäksi muita etukäteiskriteerejä ei tarkasteltu tarkemman

valikoinnin toteuttamiseksi. Suurimmalla osalla tutkittavista oli hallintasovellus vain henkilökohtaisessa käytössä. Osa mainitsi käyttävänsä niitä sekä töissä että kotikäytössä. Yksi vastaajista käytti sovelluksia ainoastaan työkontekstissa. Hallintasovellukset olivat olleet osallistujilla käytössä vaihtelevan pituisia aikoja puolesta vuodesta yli 12 vuoteen. Suurin osa haastateltavista kertoi käyttävänsä hallintasovellusta päivittäin, mutta joukossa oli myös harvemmin käyttäviä. Haastateltavien käyttämät salasanojen hallintasovellukset on esitelty taulukossa 4.

TAULUKKO 4 Käytössä olevat salasanojen hallintasovellukset

Haastateltava	**Salasanojen hallintasovellus**
H1	LastPass
H2	BitWarden, LastPass
H3	LastPass
H4	F-Secure ID Protection
H5	LastPass
H6	F-Secure ID Protection, KeePass
H7	KeePass
H8	KeePass, MacPass
H9	BitWarden, LastPass
H10	LastPass
H11	BitWarden
H12	Avira Password Manager
H13	KeePass

Osa jo sovituista haastatteluista peruuntui, minkä myötä aiemmin mielen kiintonsa ilmaisseilta kysyttiin mahdollisuutta osallistumiseen. Ennen haastatteluja haastateltaville toimitettiin sähköpostitse tutkimuksen tietosuojailmoitus sekä suostumuslomake tutustuttaviksi etukäteen. Tietosuojailmoituksessa luonnehdittiin tutkimuksen pääteemoja, mutta muuten haastatteleville ei annettu tarkempaa etukäteistietoa kysymyksistä.

Haastattelut toteutettiin COVID-19-pandemiatilanteen vuoksi Zoom-videokokouspalvelun kautta huhti–toukokuussa 2022. Palvelu mahdollisti haastattelujen nauhoittamisen, joten erillistä nauhuria tai vastaavaa ei tarvittu, joskin varamenetelmänä haastattelija oli varautunut kirjoittamaan keskeisimmät kohdat teemoittain paperille. Yksi haastateltavista osallistui ainoastaan puheen välityksellä, jolloin tilanne oli verrattavissa puhelinhaastatteluun.

Haastattelutilanteen alussa nauhoitettiin suostumuslomakkeen hyväksyminen suullisesti. Tämä mahdollisti suostumuksen tietoturvallisen käsittelyn, eikä henkilötietoja tarvinnut lähettää sähköpostitse. Sekä suostumus että varsinainen haastattelu talletettiin Jyväskylän yliopiston tutkimusaineiston käsittelyä koskevien tietoturvakäytänteiden mukaisesti. Haastattelun jälkeen tallenteet litteroitiin ja haastateltavat pseudonymisoitiin peitenimillä H1–H13. Sen myötä kaikki henkilötiedot poistuivat aineistosta ja molemmat videot kyettiin tuhoamaan.

Haastattelut noudattivat pääasiassa samaa teemojen mukaan jaoteltua haastattelurunkoa, mutta runko täydentyi prosessin aikana muutamin

lisäkysymyksin, jotta saatiin varmistettua, että kaikki vastaajat ottavat kantaa myös uusina esiin nousseisiin aiheisiin. Lisäksi haastattelurungon järjestyksestä voitiin poiketa, mikäli haastateltavat siirtyivät omatoimisesti puhumaan seuraavasta teemasta tai jos haastattelija havaitsi luontaisen siirtymän johonkin toiseen ennalta suunniteltuun aiheeseen.

TAULUKKO 5 Analyysin teemat ja alateemat vastaajittain

Aihe	**H1**	**H2**	**H3**	**H4**	**H5**	**H6**	**H7**	**H8**	**H9**	**H10**	**H11**	**H12**	**H13**
Vahvuus													
Generointi vahvistanut	√	√	√	√		√	√	√	√	√	√	√	√
Itse luodut vahvempia	√		√	√									
Ei vahvistunut					√								
Osa salasanoista vanhoja, vain muistissa	√					√					√		
Osa salasanoista vanhoja, sovelluksessa					√		√				√	√	
Uniikkius													
Generointi paransi selvästi	√	√	√	√		√	√		√	√	√		√
Itse luodut parantuivat selvästi	√												
Osittain					√			√				√	
Hallinta													
Vanhat menetelmät poistuneet		√	√	√	√	√	√		√	√		√	√
Vanhat menetelmät jääneet osittain	√							√			√		
Muut													
Muutos tehty kerralla	√								√	√			
Muutos tehty pikkuhiljaa		√		√			√	√			√	√	√
Työkalujen käyttö	√			√	√	√	√		√		√		√

5.2.2 Aineiston analysointi

Aineiston analysoinnissa käytettiin temaattista analyysiä, jonka avulla pyrittiin löytämään kaikki erilaiset tavat, joilla hallintasovelluksen käyttäjien salasanakäyttäytyminen on muuttunut. Teemahaastattelun aiheet toimivat temaattisen analyysin runkona.

Analyysin ensimmäisessä vaiheessa tutustuttiin kaikkiin litterointeihin huolella. Seuraavaksi avoimen koodauksen menetelmällä jaoteltiin aineisto pääasiassa lauseisiin ja pidempiin tekstinpätkiin, jotka sisälsivät jonkin tietyn salasananhallinnallisen kontekstin. Nämä koodatut osuudet yhdisteltiin luokittain, minkä jälkeen niistä luotiin edelleen alateemoja ja teemoja. Taulukossa 5 esitellään eri teemat ja niiden alateemat sekä tutkittavien sijoittuminen niihin.

Teemoittelun lopuksi tarkasteltiin eri käyttäjäryhmiä tarkemmin, etsien sekä syitä muutokselle tai muuttumattomuudelle sekä erilaisia näiden teemojen ilmenemistapoja. Tulokset esitellään seuraavassa pääluvussa.

5.3 Tutkimuksen luotettavuus

Tämän tutkimuksen validiteetin osalta suurin ongelmakohta on tutkimuksen kohdejoukko. Myersin ja Newmanin (2007) mukaan tutkimuksessa tulisi olla mahdollisimman monipuolinen joukko tutkittavia. Kun osallistujat olivat joko tietotekniikan opiskelijoita tai internetin keskustelupalstojen käyttäjiä, ainakin ensin mainitulta ryhmältä voi mahdollisesti olettaa keskivertokansalaista korkeampaa valveutuneisuutta myös tietoturva-asioista. Haastattelutilanteessa tulikin ilmi, että moni oli myös työtehtäviensä puolesta perehtynyt tietoturvakenttään. Vaikka Faganin ym. (2007) mukaan hallintasovellusten käyttäjät ovat lähtökohtaisesti tietoturvaorientoituneempia jo muutenkin, olisi aineiston monimuotoisuuden kannalta ollut eduksi etsiä haastateltavia vielä laajemmin. Toisaalta tälläkin kohdejoukolla tulokset olivat monipuolisia ja tutkittavilla esiintyi erilaisia salasanakäyttäytymisen malleja.

Tutkimuksen validiteettia tarkasteltaessa on otettava lisäksi huomioon salasanojen vahvuuden arviointi. Koska käyttäjien tosiasiallisia salasanoja ei erikseen mitattu ja vertailtu, jää niiden vahvuuden arviointi käyttäjälle itselleen. Kuten alaluvusta 4.1 voidaan havaita, käyttäjien kyvystä arvioida oman salasanansa vahvuutta on ristiriitaisia näkemyksiä. Lisäksi Washin ym. (2016) mukaan ihmisten kertomus salasanavaatimusten täyttämisestään ei mittaa heidän todellista salasanakäyttäytymistään. Tässä tutkimuksessa lähes kaikki salasanat, joita tutkittavat kuvailivat vahvemmiksi, oli luotu hallintasovellusten tarjoamilla generaattoreilla. Tästä ei kaikkien vastaajien osalta voida vielä vetää johtopäätöstä salasanojen objektiivisesta vahventumisesta, sillä useissa sovelluksissa on generaattorin ohessa salasanamittari, josta voidaan säätää luotavan salasanan laskennallista vahvuutta. Osa tutkittavista, mutta eivät kaikki, kertoi asettavansa generaattorissa salasanan mahdollisimman vahvaksi.

Reliabiliteettia arvioitaessa keskeinen asia on salasanojen henkilökohtaisuus. On mahdollista, että haastateltavat eivät halua mennä yksityiskohtaisuuksiin kuvaillessaan salasanojensa käyttöä, koska se saatetaan kokea liian yksityiseksi aiheeksi. Tähän pyrittiin vaikuttamaan viestimällä aineiston turvallisesta käsittelystä ja säilytyksestä, sekä painottamalla haastattelun alussa, että yksityiskohtiin (l. salasanoihin teknisesti tai esimerkiksi niiden tarkkaan säilytyspaikkaan) ei tarvitse missään vaiheessa ole tarpeen mennä. On myös mahdollista, että erityisesti tietotekniikan opiskelijat sekä tietoturvakentällä työskentelevät haastateltavat vastasivat sosiaalisesti hyväksyttäviä vastauksia omasta tietoturvakäyttäytymisestään.

Videohaastattelu – joka toteutui kaikkien paitsi yhden osallistujan osalta – menetelmänä mahdollisti pelkän puheen sijasta paremman vuorovaikutuksen haastateltavien kanssa. Sanattoman viestinnän havainnoinnin osalta tilanne muistutti kasvotusten toteutettua haastattelua. Puhelinhaastattelun tyyppisesti toteutettu videoton Zoom-puhelu ei toisaalta oletettavasti myöskään aiheuttanut haasteita esimerkiksi kysymysten ymmärtämiseen liittyen. Kaikki osallistujat olivat aktiivisia ja arvion mukaan vastasivat avoimesti eri kysymyksiin. Moni vaikutti pohtineen salasanojen hallintasovellusten käyttöään jo etukäteen luettuaan tietosuojalomakkeesta tutkimuksen pääteemat. Lisäksi osa kävi haastattelun aikana tarkistamassa hallintasovelluksesta esimerkiksi käyttämiensä salasanojen määrään. Tämä ei todennäköisesti olisi ollut mahdollista kasvotusten toteutetussa haastattelussa, ellei erikseen olisi pyydetty ottamaan hallintasovelluksen sisältämiä laitteita mukaan.

Kokonaisuudessaan arvio tutkimuksen luotettavuudesta – edellä mainitut kohdat huomioon ottaen – on hyvä, suurimpana heikkoutena työtehtäviltään ehkä liian homogeeninen kohdejoukko.

6 TULOKSET

Tässä pääluvussa esitellään tutkimuksen tulokset teemoittain. Pääteemat muodostavat alaluvut, joiden sisällä tarkastellaan kutakin ilmiötä alateemojensa kautta.

6.1 Salasanojen vahvuus

Salasanojen hallintasovelluksen käyttäminen on vaikuttanut positiivisesti salasanojen vahvuuteen yhtä lukuun ottamatta kaikilla haastatelluilla. Merkittävin tekijä on ollut salasanojen luonti sovellusten tarjoamilla generaattoreilla. Vastaajista kuusi kertoi, että kaikki heidän salasanansa ovat nykyisin salasanageneraattoreilla tuotettuja. Kaikki kaksitoista generaattoria käyttänyttä kertoivat, että se on ollut avainasemassa salasanojen vahvuuden paranemisessa.

> H9: Aina generaattorilla. Olen lukenut tilastotiedettä jonkin verran, ja se minkä ihminen luulee satunnaiseksi, ei ole satunnaista. Tämä menee ehkä sinne foliohattupuolelle, mutta kun hakataan näppäimistöä ja on tarpeeksi iso massa, sieltä löytyy aina rakenteita. Eli aina generaattorilla ja niin pitkä kuin vain palvelu sallii. Yleensä 20–30 merkkiin asti. Joskus ottaa päähän, jos palvelu ei anna tehdä pidempiä kuin 10 merkkiä, jolloin toki tietää myös palvelun laadusta, että sinne ei kannata mitään kovin salaista laittaa.

Osa käyttäjistä kertoi, että generoinnin lisäksi he ovat keksineet edelleen myös itse salasanojaan, jotka he ovat hallintasovelluksen käytön myötä voineet lähtökohtaisesti tehdä pidemmiksi ja kompleksisemmiksi, koska niitä ei tarvitse muistaa itse.

> H3: Sitten jos se on joku semmoinen, jossa minun täytyy antaa ne tunnukset johonkin muualle, niin sitten se voi olla siinä alkuun joku sellainen helpommin kommunikoitava eikä vaan joku random merkkijonopätkä.

Hallintasovelluksen käyttö ei kuitenkaan kaikkien osalta tarkoittanut sitä, että jokainen salasana olisi tallennettuna sinne. Tämä on johtanut siihen, että osalla vastaajista oli heikompia salasanoja vielä järjestelmän ulkopuolella, vaikka sovellukseen tallennetut olisivatkin olleet vahvoja. Eräs vastaajista kertoi syyksi sen, että hän oli ollut hetkellisesti tehtävässä, jonka mukana oli tullut useita uusia salasanoja, jotka hän oli tallentanut silloin hankkimaansa hallintasovellukseen. Tehtävässä toimimisensa ajan hän oli tallentanut myös uudet henkilökohtaiset kirjautumistietonsa sinne. Kun tehtävä loppui, loppui myös sovelluksen käyttäminen muiden kuin käyttöaikana tallennettujen salasanojen osalta. Vanhat salasanat pysyivät edelleen samoina, heikompina, versioina. Toisaalta hän koki hetkellisen salasanakäyttäytymisen paranemisen – eli hallintasovelluksen käytön – lopulta parantaneen toimintaansa myös käytön jälkeen:

> H1: Musta ehkä tuntuu siltä, että sen jälkeen, kun mä otin sen käyttöön, niin nekin salasanat, jotka mä olen luonut sitten joihinkin paikkoihin, joita mä en ole tallentanut sinne, niin mä oon tehnyt niistä jotenkin monimutkaisempia. Että jotenkin se oli semmoinen inspiraatio sitten semmoiseen.

Toisena syynä vanhojen salasanojen säilyttämiseen hallintasovelluksen ulkopuolella mainittiin kyseisten tilien luonne ja tärkeys: esimerkiksi verkkopankkipalveluihin liittyvien tunnusten säilömisen osalta kaikilla haastatelluilla ei ollut luottamusta palveluntarjoajiin, vaan itselle tärkeimpien tilien salasanat haluttiin pitää vain omassa muistissa. Henkilökohtaisen merkityksen lisäksi muistin käyttöön ohjasivat myös käytännöllisyys ja joidenkin käyttäjätunnusten turvaluokitus.

> H6: Pyrin joitain useimmin käytössä olevia salasanoja, vaikeammin kaivettavissa olevia salasanoja, esimerkiksi hostin tai bitlockerin salasanoja, sekä sellaisia, joita ei esimerkiksi turvaluokituksesta johtuen viitsi laittaa mihinkään, muistamaan itse.

Vastaajista kolme kertoi, että vaikka he olivatkin alkaneet luomaan hallintasovelluksen käytön myötä uusia salasanoja generaattorin avulla, heidän vanhat salasanansa olivat edelleen alkuperäisiä. Syy tähän oli pääasiassa se, että ne oli ollut tarkoitus vaihtaa, mutta sitä ei ollut vielä toteutettu. Yksi vastaajista kertoi käyttävänsä sähköpostitiliä, jonka salasanan unohtuminen johtaisi koko tilin tuhoutumiseen, eikä sen vuoksi ole vaihtanut alkuperäistä uuteen.

> H11: ProtonMailissa käytän vielä vanhaa salasanaa, kun se on aika ilkeä, jos salasana unohtuu, niin tuhoutuu sitten täysin se sähköpostin sisältö. Käytännössä kaikki muut olen vaihtanut.

Eräs vastaajista totesi, että hänen salasanansa eivät olleet hallintasovelluksen käyttöön ottamisen jälkeen muuttuneet vahvemmiksi. Hän oli tietoinen mahdollisuudesta generoida salasanoja, mutta kertoi käyttäneensä sitä ”turhan harvakseltaan”. Kyseinen haastateltava kertoi salasanojensa luonnissa olevan ajatuksena tehdä salasanasta vahva, mutta kuitenkin sellainen, jonka voisi edelleen muistaa itse.

> H5: Lähinnä se [hallintasovellus] on ollut itselle salasanapankki käytännössä. […] Tavoite on aina tehdä sellainen salasana, jonka itse muistaa ja on tarpeeksi vahva ja että se täyttäisi niitä määritteitä mitä eri sivuilla on, että pitää olla isoja ja pieniä kirjaimia ja erikoismerkkejä ja vaikka numeroita ja sitten joissain tapauksissa se ei välttämättä ole edes salasana vaan että se on joku lause. Mutta kuitenkin yrittää tehdä siitä itse sellaisen mahdollisimman vahvan, mutta että sitten myös muistaisi itse. Arvioisin, että salasanat ovat pysyneet yhtä vahvana kuin ennenkin ohjelman käyttöä. Ero on se, että jos aiemmin yritti jotain viittätoista salasanaa ennen kuin pääsi sisään, niin nyt voi käydä katsomassa sen sieltä.

Toisaalta kyseinen haastateltava mainitsi myöhemmin, että hän on salasanoja luodessaan käyttänyt hyväksi sovelluksen tarjoamaa työkalua, joka antaa palautetta salasanan vahvuudesta, ja muuttanut kyseisiä salasanoja vahvemmiksi palautteen perusteella. Tätä ja muita työkaluja käsitellään laajemmin alaluvussa 6.4.

Käyttäjien salasanojen muuttumiseen vahvemmiksi liittyy olennaisesti myös hallintasovelluksen käyttöä edeltäneet tavat luoda salasanoja. Generaattoria käyttämällä käyttäjä voi itse usein määritellä luotavan salasanan vahvuuden pelkän liukusäätimen avulla, mutta hallintasovellusta edeltäneenä aikana haastateltavilla on ollut monia syitä heikompiin salasanoihin. Myös yksittäisellä tutkittavalla saattoi olla useampia syitä.

Kyseiset syyt voidaan jaotella kahteen kategoriaan: *miksi* ja *miten* salasanat ovat olleet heikompia. Lähes kaikki haastateltavat ilmoittivat vähintään yhdeksi vastaukseksi *miksi*-kysymykseen, että aiemmin oma muistikapasiteetti ei ole riittänyt vahvempiin salasanoihin.

> H12: Kun en ole aiemmin käyttänyt manageria, niin olen pyrkinyt tekemään salasanoista sellaisia, että muistaisin ne, jonkinlaisten muistisääntöjen lomassa.

> H1: Mä sekä käytin sitä generaattoria että mä keksin itse pidempiä, ja tuossa kohtaa toi mun mielestä auttaa tosi paljon, koska jotkut niistä on itse ainakin mahdottomia muistaa. Erityisesti jos on joku semmoinen palvelu, johon kirjautuu harvemmin, vaikka se olisi joku looginen salasana itselle, jonka olisi keksinyt jostakin asiasta.

Muita mainittuja syitä olivat tiedon puute, mielenkiinnon puute, sekä viitseliäisyys luoda vahvempia salasanoja. Taulukossa 6 esitellään uusien salasanojen luonnissa pääasiassa generaattoria käyttäneiden haastateltavien mainitsemat syyt, miksi heidän salasanansa ovat aiemmin olleet heikompia.

Miten tutkittavien salasanat sitten olivat aiemmin heikompia kuin nykyisin? Haastatteluissa ilmeni neljä erilaista tapaa: pääteltävyys, arvattavuus, olemassa olevia lauseiden tai sanojen sisältäminen sekä vähäisempi pituus.

> H8: Niissä on varmasti aina ollut joku pääteltävissä oleva elementti, uskoisin. Vaikka yrittää tehdä niistä jotenkin kryptisiä, niin sitten kun ne pitäisi yrittää myös muistaa, niin sitten niihin tulee aina joku semmoinen elementti minkä perusteella ehkä sen pystyisi kräkkään.

> H10: Ne on ollut lyhyitä plus ne on ollut jonkun näköisiä lause-numero-yhdistelmiä tai sana-numero-yhdistelmiä, että ne on kuitenkin ihmisenkin vaikka olan yli suhteellisen helppo lukea tai sitten ihan murtaa voimalla.

On huomioitava, että haastatteluissa ei ollut tarkoitus mennä salasanojen yksityiskohtiin, joten tutkittavilta ei kysytty spesifisti sitä, millaisia heidän salasanansa ovat olleet ennen ohjelman käyttöä. Haastattelussa käytettiin nimenomaan *miksi*-kysymystä, johon osa vastaajista kuvaili aiemmin mainitun kaltaisesti aiempia tapojaan.

TAULUKKO 6 Syyt, miksi aiemmat salasanat ovat olleet heikompia

Haastateltava	**Muistamisen hankaluus**	**Tiedon puute**	**Mielenkiinnon puute**	**Viitseliäisyys**
H1	√			
H3	√			
H4	√			
H6		√		
H7	√	√	√	
H8	√[3]			
H9	√			√
H10	√[4]			
H11	√			
H12	√			
H13	√			

6.2 Salasanojen uniikkius

Kaikilla vastaajista salasanat olivat parantuneet uniikkiuden osalta. Kymmenen haastateltavaa kertoi salasanojen generoimisen vaikuttaneen selvästi salasanojensa monimuotoisuuteen.

> H6: Sanoisin, että ne ovat niin uniikkeja kuin olla ja voi. Ehkä ainoa mitä voisi vielä muuttaa olisi tehdä niistä eri pituisia. Satunnaisgeneraattorilla kun tekee niin ovat pseudosatunnaisia joka tapauksessa.

> H11: Kyllä. Aiemmin on ollut samoja salasanoja aika paljonkin. Toki sijoitus- ja pankkipalveluihin ja vastaaviin on ollut omat salasanansa, mutta käytännössä muissa tileissä on ollut kolme kiertävää salasanaa.

[3] Muistamisen hankaluudesta johtuen salasanaan on lisätty ”pääteltävissä oleva elementti”.

[4] Haastateltava ei mainitse suoraan syyksi muistettavuutta, mutta kertoo käyttäneensä aiemmin lyhyempiä lause-numero- tai sana-numeroyhdistelmiä salasanoina.

Yksi vastaajista kertoi luoneensa hallintasovelluksen käyttöaikanaan salasanoja sekä generaattorilla että omatoimisesti siten, että sovelluksen käyttö mahdollisti monimuotoisuuden lisäämisen molemmilla tavoilla.

Kolmella vastaajista hallintasovelluksen käyttö oli parantanut uniikkiutta osittain. Pääsyynä osittaisuuteen oli se, että vanhoja salasanoja ei ollut vielä muutettu, mutta todettiin kuitenkin hallintasovelluksen edesauttavan uniikkiuden toteutumista joko vähän kerrallaan tai esimerkiksi pelkkien työhön liittyvien salasanojen muuttamisen kautta. Myös haastateltava H5, joka totesi aiemmin, että hänen salasanojensa vahvuus ei ole parantanut, kertoi kehitystä tapahtuneen kuitenkin monimuotoisuuden osalta:

> H5: No joo. Nyt ainakin tietää, että siihen on hyvä mahdollisuus. Turvallisemmin mielin voi lähteä kokeilemaan spessumpia salasanoja kuin vaikka ennen.

Kysyttäessä syitä hallintasovellusten käyttöä edeltäneen ajan vähäisempään monimuotoisuuteen, muistaminen nousi vielä voimakkaammin esiin kuin vahvuuteen liittyen. Useampi vastaaja kertoi palveluita olevan nykypäivänä niin paljon, että salasanojen määrä tuntuu ylittävän muistikapasiteetin, ellei salasanoissa ole jotain säännönmukaisuutta.

> H13: Oikeestaan se muistaminen on ollut se isoin syy. Ainakin itse kokee, että se muisti on ollut siinä haasteena.

> H1: Joskus saattoi, jos oli vaikka kaks eri jotain nettiostopalvelua, niin saattoi tehdä niihin salasanan siten, että muutti vain pieniä osia siitä, että muistaisi sen.

> H12: Kun en ole aiemmin käyttänyt manageria, niin olen pyrkinyt tekemään salasanoista sellaisia, että muistaisin ne, jonkinlaisten muistisääntöjen lomassa. […] ne voivat mukailla toisiaan jonkin muistisäännön takia. Ne eivät ole ihan samoja mutta riittävän samoja. […] jos joku kohdistaisi oikeasti vaivaa niin salasanat olisivat johdettavissa tai murrettavissa.

Valtaosalla vastaajista oli aiemmin ollut yksinkertaisesti sama salasana useassa palvelussa:

> H4: Ihmisen kapasiteetin muistaa vuoksi. Jos on se 142 salasanaa eri palveluissa, niin pitää olla se Dustin Hoffman ja Sademies -tyyppi, että muistaa tuommoisia geneerisiä lauseita tai salasanoja.

> H2: Kyllä mä oon aiemminkin pyrkinyt siihen, että olisi useammilla sivuilla eri salasanat, mutta sitten kuitenkin se vei aika paljon muistitilaa ihan omasta päästäkin, että muisteli kaikkiin eri paikkoihin salasanat. Musta tuntuu, että aika usein niissä useimmin käytetyissä palveluissa saatto käyttää samaa salasanaa ihan vaan sen takia, että se on helpompaa itselle.

> H9: Mitä nyt muistaa, niin kyllä kaikkein tärkeimmissä paikoissa kuten nettipankeissa on ollut uniikkeja salasanoja, mutta sitten jos mennään joihinkin sosiaalisen median tileihin, mitkä nyt tavallaan nykyään on vielä tärkeämpiä, mutta kuitenkin, niin

> sanotaan että ehkä viisi neljästäkymmenestä oli uniikkeja, että ei se kauhean häävi silloin ole.

Vain yksi vastaajista mainitsi muistamisen lisäksi myös muita syitä aiempien tapojen heikkouteen uniikkiuden näkökulmasta. Hänellä oli ollut käytössä aiemmin sekä selaimen että käyttöjärjestelmän tarjoama salasananhallintajärjestelmä, mutta niiden integrointihaasteiden vuoksi käytettävyys ei ollut mahdollistanut monimuotoista salasana-avaruutta kyseisen haastateltavan tarpeisiin:

> H11: Ei ole suoraan sanottuna välittänyt niistä, miten hyviä ne ovat aiemmin ollut. […] Käytän paljon eri alustoja, eli mulla on Linux-tietokone, Windows-tietokone ja Mäkki ja sitten kännykkä on iPhone, niin siinä vaiheessa alkaa tulla vastaan se, että jos haluaisi käyttää tosi sujuvasti ylipäätään mitään palvelua, niin se pitäisi olla tavallaan tarjolla kaikilla alustoilla, mikä taas ei toteudu monen selaimen tai käyttöjärjestelmän omilla salasanahallinnoinneilla.

6.3 Salasanojen hallinta

Haastatelluista kymmenen mainitsi säilyttäneensä ainakin aiemmin vähintäänkin joitain salasanojaan kirjoitettuna muistiin johonkin, joko fyysisesti tai digitaalisena tai molempina versioina. Seitsemällä haastateltavalla oli ollut käytössään kynä ja paperi -menetelmä, eli salasanoja oli joko yksittäisillä paperilapuilla tai vihkossa.

> H12: On ollut jotain sellaisia tilejä, joissa on ollut syytä pitää salasana, mutta ei ole ollut kauhean merkittävää, että se on salainen, kuten esimerkiksi kotiverkon salasana. Niin se on saattanut olla meillä sitten saatavilla kotona sellaisessa paikassa, josta vieraatkin tietää sen sitten tarkastaa. Jotain vastaavia voi olla. Mitään varsinaista muistikirjaa en niistä pitänyt.

Kuusi haastateltavaa kertoi pitäneensä salasanoista kirjaa sähköisesti. Säilytyspaikkoja oli monia: teksti- tai taulukkolaskentatiedosto tietokoneella, selainlaajennustyyppinen hallintajärjestelmä, sähköpostin lähtevien viestien kansio sekä matkapuhelimessa lähtevissä tekstiviesteissä. Osalla oli salasanat vain yhdessä paikassa, toisilla useammassa:

> H9: Hyvin pystyn kuvittelemaan, että on ollut salasanoja esimerkiksi jossain tekstitiedostossa työpöydällä, mikä on tyhmin idea ikinä. Sitten varmaan jossain paperillakin ja kännykän muistissa lähtevissä tekstiviesteissä tai sähköpostilaatikon lähtevissä viesteissäkin on voinut olla jotain muistiinpanoja.

Kaikki eivät kuitenkaan olleet sitä mieltä, että hallintasovellus olisi välttämättä ollut turvallisempi tapa säilyttää salasanoja, sillä yksi vastaajista kertoi kiinnittäneensä huomiota tietoturvaan myös aiemmassa menetelmässään:

> H10: On ollut aiemmin, eli aiemmin kun otin tämän LastPassin käyttöön, niin käytin Exceliä, jonne olin tallentanut kaikki salasanat, joka oli sitten kryptattuna omalla ulkoisella kovalevyllä. Ei kovin käytännöllinen tapa, mutta toisaalta oli se tietoturva ihan huomattavasti parempi kuin sitten se, että käyttäisi jotain ihan perus salasanaa vaan joka ikisessä palvelussa. Siellä oli varsinkin tärkeimpien palveluiden salasanat jo tässä vanhassa Excelin kryptattu kovalevy -tyylissä tommoisia merkkihirviöitä varmuuden vuoksi.

Kolme vastaajista ilmoitti hallinneensa aiemmin salasanojaan vain omaan muistiinsa tukeutuen. Kuten edellisissä alaluvuissa tuli ilmi, hallintasovelluksella onkin ollut merkittävä vaikutus oman muistin käyttämiseen salasanojen säilytyspaikkana:

> H12: Toki palveluiden määrä, joihin salasanoja tarvitsee, alkoi räjähtää niihin aikoihin, kun aloin tätä käyttää. Se määrä oli vielä 2010–2015 maltillinen, mihin tarvitsin salasanaa, mutta yksi syy ottaa manageri käyttöön oli se, että niiden määrä alkoi laajenemaan niin paljon.

Kolmea lukuun ottamatta jokainen haastateltava ilmoitti luopuneensa vanhoista hallintamenetelmistään kokonaan salasanojen hallintasovelluksen käyttöön ottamisen myötä. Heistä seitsemän oli sellaisia, jotka olivat aiemmin kirjoittaneet salasanoja muistiin.

> H7: Kyllä näiden hallintaohjelmien käyttöönoton myötä on siirrytty pois paperilapuista ja notepadeista ja niin poispäin.

> H13: Vapaa-ajan käytössä käytti suunnilleen samaa salasanaa vähän muunneltuna – vaikka hyvä ja pitkä olikin – ja sen muuttuvan osan olin tallentanut jossain muodossa itselleni kännykkään. Työkäytössä niitä oli ihan Excelissä, kun oli toistakymmentä tiliä siellä. Nyt molemmat tavat ovat poistuneet käytöstä.

Kyseiset haastatellut kokivat, että hallintasovelluksen käyttö oli joko käytettävyyden tai turvallisuuden – tai molempien – suhteen hyvä vaihtoehto ainoaksi hallintamenetelmäksi.

> H11: Lähinnä se, että salasanojen hallinnointi on muuttunut paljon helpommaksi. Että kun nimenomaan on Android-kännykkä, on iPhone-kännykkä, on Linuxia, on hirveän paljon eri järjestelmiä käytössä, niin kun on saanut yhden joka toimii suhteellisen samaan tapaan kaikilla, niin on se syy miksi on alkanut käyttämään salasanahallinnointia.

> H2: No aiemmin olen kirjoittanut ihan paperille niitä johonkin vihkoon, mikä ei toisaalta ole kyllä kovin tietoturvallista silleen, että kuka vaan voi sen ottaa, mutta nykyään mä laitan kaikki sinne ohjelmaan.

Kolmesta vanhoja menetelmiä edelleen käyttävästä osallistujasta yksi ei mainitse haastattelussa tarkempaa syytä toiminnan jatkumiselle, mutta hän sanoo salasanojen muualle muistiin kirjoittamisen vähentyneen hallintasovelluksen käyttöönoton myötä. Kaksi muuta heistä perusteli toimintaansa sillä, että he eivät

pitäneet hallintasovelluksen käyttöä täysin luotettavana tapana pitää muistissa tärkeimpiä salasanojaan.

> H1: Jotenkin aloin ajattelemaan sitä sillä tavalla, että aina sanottiin, että ei saa säilyttää salasanoja missään paperilla kotona jossakin laatikossa, ja sitten mä aloin miettimään, että kun se on mun koneella selaimella pluginina ja sen saa yhdellä klikkauksella auki, jos mä oisin sisäänkirjautunut sinne, niin miten se eroaa siitä. Niin se lähinnä vaikutti siihen miksi mä en en halunnut laittaa sinne esimerkiksi omia salasanoja, jotka liittyy johonkin pankkipalveluihin tai sellaisiin. Tai no ehkä pankki on huono koska on se sovellus. Mutta sen tyylisiin kuitenkin, koska mitä jos mun kone on jossakin auki ja minä olen juuri kirjautunut sinne, senhän saa yhdellä klikkauksella auki, miten se eroaa siitä paperista, joka minulla on kotona.

> H11: En lähtökohtaisesti käytä ulkopuolisia ohjelmistoja rahaan tai sellaisiin vähän herkempiin henkilötietoihin liittyviin salasanoihin, ne olen kirjannut vanhanmallisesti paperille.

Kaikkiin kolmeen mainittuun teemaan – salasanojen vahvuuteen, uniikkiuteen ja hallintaan – liittyen yksi esiin noussut alateema oli toimintaan liittyvien parannusten aikautus. Kolme haastateltavaa kertoi tehneensä vanhojen tilien salasanojen parannuksen kerralla:

> H9: Kun tajusin ohjelman hyvyyden, kävin yksitellen salasanat läpi ja vaihdoin suoraan vahvempiin.

Haastateltavista seitsemän totesi tehneensä muutokset jonkin aikavälin puitteissa. He eivät siis pyrkineetkään saamaan kaikkia tilejä kerralla kuntoon. Tämä on tapahtunut esimerkiksi siten, että uusi salasana on luotu aina siinä vaiheessa, kun on tarvinnut kirjautua johonkin palveluun muista syistä.

6.4 Muita vaikutuksia

Salasanageneraattorin avulla parantunut salasanojen vahvuus ja uniikkius sekä mahdollisuus varastoida salasanoja turvallisesti olivat kolme selvästi suurinta vaikutusta, joita salasanojen hallintasovellusten käytöllä oli salasanojen käyttöön.

Neljäntenä olivat erilaiset sovelluksissa tarjolla olevat työkalut. Niistä eniten käytetyksi mainittu apuväline oli vahvuusmittari, jonka avulla pystyy tarkastelemaan joko luontivaiheessa tai jo olemassa olevan salasanan vahvuutta. Sitä oli käyttänyt seitsemän vastaajaa, ja kaikki heistä kertoivat myös vahvistaneensa salasanansa sitä käyttämällä. Tämän työkalun käyttö liittyykin kiinteästi ensimmäiseen alalukuun, eli salasanojen vahvuuteen.

Toiseksi eniten oli käytetty sovellusten tarjoamaan palvelua, jossa voi tarkastella ilmi tulleita tietovuotoja salasanojen osalta ja verrata, onko omat käyttäjätiedot vuotojen joukossa. Yksi neljästä kertoi kerran saaneensa sen kautta indikaation vaarantuneesta tilistään, mutta hän oli ehtinyt jo kauan sitä ennen muuttamaan kyseisen palvelun salasanan.

> H3: Yksi epätärkeä salasana mikä mulla on ollut joskus käytössä, oli vuodettu ja sitten siitä tuli indikaatio että se oli useammallakin listalla, mutta mä olin vaihtanut sen jo siinä vaiheessa, kun siltä palveluntarjoajalta tuli se että ”hei meidän systeemiin on murtauduttu”, mikä oli siis vuosia sitten jo.

Näiden lisäksi yksi haastateltavista kertoi käyttävänsä työkalua, joka näyttää hallintasovelluksen tietokannassa olevat samanlaiset salasanat sekä työkalua, jolla voi muuttaa olemassa olevia salasanoja suoraan hallintasovelluksen holvista. Taulukossa 7 on koonnos haastateltujen käyttämistä työkaluista. Yksikään käyttäjä ei ollut käyttänyt kaikkia kolmea työkalua. Lisäksi haastatelluista kahdeksan oli käyttänyt joko vain vahvuusmittaria tai ei työkaluja ollenkaan.

TAULUKKO 7 Haastateltujen käyttämät työkalut hallintasovelluksissa

	Salasanan vahvuusmittari	**Duplikaattien tunnistus**	**Tietovuotoilmoitukset**	**Salasanan muuttaminen holvista**
H1	√			
H3			√	
H4	√			
H5	√			
H6	√		√	
H7	√			
H9		√	√	√
H10				
H12	√		√	
H13	√			

Viides esiin noussut tapa hallintasovelluksen vaikutuksesta salasanojen hallintaan oli salasanojen jakaminen. Haastatelluista kaksi kertoi käyttäneensä hallintasovelluksen tarjoamaa turvallisempaa tapaa jakaa omia tai työhön liittyviä salasanojaan. Toinen haastatelluista mainitsi nimenomaan henkilökohtaisessa käytössä olevien tilien – esimerkiksi suoratoistopalveluiden – salasanan jakamisen, toinen käsitteli aihetta työkontekstiin liittyvässä keskustelussa:

> H8: Ehkä yhteiskäytössä olevien ohjelmien tai muiden tunnusten jakaminen on turvallisempaa nykyisin. Pystyy jakamaan sitten niitä KeePass-tiedostoja, se on ehkä isoin ero.

Lopuksi, kaksi vastaajista totesi hallintasovellusten käytön vähentäneen huomattavasti salasanan nollaus -toiminnon käyttöä eri palveluissa. He kertoivat, että aiemmin salasanan unohtaminen oli pakottanut käyttämään kyseistä toimintoa, kun varastointiratkaisua kaikille salasanoille ei ollut käytössä.

7 TULOSTEN TULKINTA JA POHDINTA

Tässä pääluvussa tarkastellaan saatuja tuloksia, ja peilaten niitä sekä tutkimuskysymyksiin että aiempaan tutkimukseen pohditaan niiden merkitystä sekä luotettavuutta. Ensin käydään läpi keskeisimmät tulokset alatutkimuskysymyksittäin ja sen jälkeen kootaan havainnot yhteen päätutkimuskysymyksen kontekstissa. Kyseisessä vaiheessa tehdään myös havaintoja liittyen aiempaan tutkimukseen yleisesti sekä Lyastanin ym. (2018) tekemään samankaltaisia tutkimusongelmia sisältäneeseen tutkimukseen. Kappaleen lopuksi esitetään jatkotutkimusaiheita.

7.1 Hallintasovellukset ja salasanojen vahvuus

Ensimmäisenä alatutkimuskysymyksenä oli ”miten salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen vahvuuteen?” Tulosten mukaan salasanojen hallintasovelluksen käyttö vaikuttaa salasanojen vahvuuteen joko positiivisesti tai ei lainkaan. Tässä tutkimuksessa kaksitoista kolmestatoista sovelluksen käyttäjästä kertoi salasanojen vahventuneen sovelluksen käytön myötä.

Kaikki, joiden salasanoista oli tullut vahvempia, kertoivat pääasiallisen syyn olleen hallintasovelluksen sisältämä salasanageneraattori. Puolet heistä käytti vain generaattoria uusien salasanojen luomisessa, ja puolet mainitsivat tekevänsä osan salasanoistaan yhä itse. Salasanageneraattorin käytön hyödyt totesivat myös Lyastani ym. (2018), joiden tulosten mukaan salasanojen generointi teki salasanoista vahvempia. Heidän tuloksensa myötäilee tämän tutkimuksen tuloksia myös niiltä osin, että pelkkä salasanojen hallintatyökalujen käyttö ei riitä merkittävään parantumiseen salasanojen vahvuudessa, vaan mukana toimintatavoissa pitää olla nimenomaan salasanojen generoiminen.

Vaikka kyseessä ei olekaan määrällinen tutkimus ja haastateltavien määrä oli verrattain vähäinen, on kuitenkin aiheellista huomioida, että yhtä vaille kaikki osallistujat käyttivät generointia säännöllisesti. Tämä on huomattavasti suurempi osa kuin Seiler-Hwangin ym. (2019) tutkimuksessa, jossa yli 70 prosenttia

hallintasovellusta käyttävistä vastaajista kertoi luovansa salasanansa edelleen itse. Myös Alodhyanin ym. (2020) mukaan alle puolet vastaajista oli käyttänyt generaattoria. He eivät myöskään löytäneet tilastollisesti merkittävää eroa asiantuntijoiden ja ei-asiantuntijoiden käyttömäärän välillä. Toisaalta heidän tutkimuksessaan erillisen salasanojen hallintasovelluksen käyttäjät käyttivät generaattoria useammin kuin selaimen sisäisen hallintajärjestelmän käyttäjät.

Kuten todettua, tämän tutkimuksen haasteltavista vain yksi kertoi käyttävänsä sovellusta pääasiassa salasanojen varastoimiseen, ei niinkään niiden parantamiseen – joskin hän mainitsi tietäneensä mahdollisuudesta generoida salasanoja erillisellä työkalulla. Kuitenkin myöhemmin hän toisen kysymyksen yhteydessä mainitsi, että luodessaan uusia salasanoja, hän on muokannut niitä vahvemmiksi tarjotun salasanamittarin arvion perusteella. Näin ollen voitaneen päätellä, että sovellus on ainakin osittain parantanut myös kyseisen käyttäjän salasanojen vahvuutta.

Salasanamittarin hyödyntämisestä salasanojen vahvuuteen mainitsivat myös kuusi muuta haastateltavaa. Kaikki olivat myös muuttaneet toimintaansa mittarin mukaan, eli he vahvensivat jo syöttämäänsä salasanaa mittarin palautteen perusteella. Tämä myötäilee Yildirimin ja Mackien (2019) havaintoja siitä, että visuaalinen palaute salasanaa luotaessa tukee käyttäjän valintoja paremmin kuin esimerkiksi pelkkä rajoitusten listaaminen. Toisaalta ainakin Vance ym. (2022) sekä Egelman ym. (2013) ovat ainakin osittain eri mieltä vahvuusmittareiden tehosta. Egelmanin ym. (2013) mukaan käyttäjän tulee olla motivoitunut suojaamaan juuri kyseistä tiliä, eikä mittari riitä salasanakäyttäytymisen parantamiseen, mikäli tiliä ei koeta tärkeäksi.

Tämän tutkimuksen osalta on otettava huomioon, että vastaajat eivät kertoneet käyttävänsä salasanamittaria joka kerta, vaan ainoastaan mainitsivat, että ovat sitä joskus käyttäneet. Toisaalta esimerkiksi Pearmanin ym. (2019) mukaan (sekä joidenkin tämän tutkimuksen haastateltavien mukaan) salasanojen hallintasovellusten käyttäjien yksi syy käyttöön on salasanojen muistamisen rajoitteet. Edellä mainitut tutkimukset (Egelman ym., 2013; Vance ym., 2022; Yildirim & Mackie, 2019) käsittelevätkin salasanoja yleisesti, eivät salasanojen hallintasovelluksia, joten esimerkiksi muistamiseen liittyvät motivaatiotekijät eivät luultavasti päde sovellusten kontekstissa. Lyastani ym. (2018) eivät käsittele tutkimuksessaan hallintasovelluksista löytyviä salasanojen vahvuusmittareita, joten tutkimuslöytö niiden tosiallisesta positiivisesta vaikutuksesta käyttäjien salasanojen vahvuuteen on uusi ja merkittävä.

Selvästi eniten haastatteluissa esiin noussut syy heikommille salasanoille aiemmin, oli muistikapasiteetin rajoitteet. Tätä tukevana huomiona J. Zhang ym. (2009) totesivat jo 13 vuotta sitten silloisten salasanavaatimusten olevan liian haastavia ihmisen muistikapasiteetille. Myös Duggan ym. (2012) ajattelivat, että salasanojen kontekstissa käyttäjän muisti rajoittaa hänen tekemiään ratkaisuja turvallisuuteen liittyen. Vastakkaisia näkemyksiä ovat esittäneet ainakin Tam ym. (2010), joiden tutkimuksessa salasanojen muistamisen suhteen ei ollut ongelmia. Tämän tutkimuksen puitteissa on vaikea arvioida, onko muisti ollut oikeasti

rajoittava tekijä kaikilla sen vastanneilla haastateltavilla, vai onko esimerkiksi oma mielipide oman muistin rajoista ollut epäilevämpi kuin todelliset rajat.

Muut mainitut heikompien salasanojen syyt, eli tiedon ja mielenkiinnon puute sekä viitseliäisyys, ovat myös löydettävissä aiemmasta tietoturva- ja salasanatutkimuksesta. Yildirim ja Mackie (2019) peräänkuuluttavat palveluntarjoajilta lisätukea käyttäjille, jotta he ovat tietoisia vahvan salasanan ominaisuuksista. Motivaatiotekijät puolestaan ovat olennaisia salasanoissa silloin kun ihminen kokee, ettei niiden heikkoudella ole negatiivisia seurauksia (Tam ym., 2010).

7.2 Hallintasovellukset ja salasanojen uniikkius

Toinen alatutkimuskysymys kuului ”miten salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen uniikkiuteen?” Kaikkien haastateltujen osalta salasanojen monimuotoisuus parani hallintasovelluksen käytön myötä vähintään jossain määrin. Myös salasanojen uniikkiuden osalta salasanageneraattorilla oli suuri rooli positiivisessa vaikutuksessa. Aiempien – joko kokonaan samojen tai samoja ominaisuuksia sisältäneiden – salasanojen tilalle oli pääasiassa vaihtunut salasanageneraattorilla luodut tunnukset. Tämän myötä käyttäjät kertoivat pääosan salasanoistaan olevan uniikkeja. Salasanojen generointiin liittyvä vertailu aiempaan tutkimukseen on tehty pääosin edellisessä alaluvussa. Lisäksi Lyastani ym. (2018) totesivat tutkimuksessaan, että salasanageneraattorin käyttäminen vaikutti merkitsevästi salasanojen uniikkiuteen.

Yksi vastaajista kertoi luoneensa myös itse monimuotoisempia salasanoja hallintasovelluksen käytön seurauksena. Myös tämä vaikutus ilmeni Lyastanin ym. (2018) tutkimuksessa, sillä heidän mukaansa ”käyttäjät kykenivät manuaalisesti luomaan uniikimpia salasanoja hallitessaan salasanoja digitaalisesti tai hallintasovelluksella” (Lyastani ym., 2018, s. 215).

Hallintasovelluksen käyttöä edeltäneen ajan osalta salasanojen monimuotoisuuden vähyyteen vaikutti monella vastaajalla muistikapasiteetti – useammin kuin salasanojen heikkouteen. J. Zhang ym. (2009) mainitsevatkin salasanojen vaatimusten lisäksi myös niiden määrän. Moni haastateltava mainitsikin nykyään omistavansa niin monta käyttäjätiliä eri palveluissa, että määrä on liikaa muistettavaksi ilman samankaltaisuuksia salasanoissa. Woods (2016) on tämän suhteen kuitenkin eri linjoilla: hänen tutkimuksensa mukaan nimenomaan uniikit salasanat on helpommin muistettavissa kuin esimerkiksi hieman muokatut. Kuten edellisessä alaluvussa todettiin, kyseessä voi olla haastateltavien alakanttiin osuva arvio omasta muistikapasiteetistaan. Toisaalta edellä mainituista tutkimuksistakin on kulunut aikaa, joten palvelujen – ja sitä myötä tarvittavien salasanojen – määrään voi olettaa entistä suuremmaksi.

Työkaluista yksi haastateltava mainitsi tähän liittyen hallintasovelluksen tarjoaman duplikaattien tunnistustyökalun. Sitä käyttämällä hän on pystynyt muuttamaan eri palveluissa olleet samat salasanat uniikeiksi. Myöskään tätä työkalua ei ole mainittu Lyastanin ym. (2018) tutkimuksessa, joten sen vaikutus salasanojen uniikkiuteen ainakin yhden haastateltavan kohdalla on uusi tieto.

7.3 Hallintasovellukset ja muu salasanahallinta

Viimeinen alatutkimuskysymys oli ”miten salasanojen hallintasovellusten käyttäminen vaikuttaa muuhun salasanahallintaan?” Stobertin ja Biddlen (2018) tutkimuksessa 78 % vastaajista kirjoitti salasanansa johonkin muistiin. Osa heistä teki sen digitaalisesti ja osa perinteisemmin paperille kirjoittaen. Tämän tutkimuksen tulosten mukaan kaikki, jotka kyseisiä menetelmiä olivat aiemmin käyttäneet, lopettivat sen vähintään osittain salasanojen hallintasovelluksen käytön myötä. Vastaajista valtaosa kertoi luopuneensa kokonaan muista salasanojen hallintamenetelmistä. Adamsin ja Sassen (1999) mukaan salasanojen kirjoittaminen muistiin suurentaa niiden paljastumisen mahdollisuutta. Mikäli salasanojen hallintasovellusten tietoturva on kunnossa (ks. esim. Chaudhary ym., 2019; Pearman ym., 2019; Seiler-Hwang ym., 2019), niiden käyttö parantaa turvallisuutta vähentämällä käyttäjien tarvetta salasanojensa säilömiseen vähemmän turvallisessa paikassa.

Hallintasovelluksen sisältämistä työkaluista tietovuotojen ilmoitustyökalua kertoi käyttäneensä neljä haastateltavaa, joista yksi oli löytänyt sen kautta ilmoituksen jo tiedossaan olleesta vanhasta vuodosta. Kenenkään kyseisistä tutkittavista ei ollut tarvinnut tehdä työkalun käytön myötä muutoksia salasanoihinsa, mutta vuotojen seuraaminen mahdollistaa reagoinnin tarvittaessa. Kaksi näistä neljästä haastateltavasta toisaalta käytti muitakin olemassa olevia palveluja tietovuotojen seuraamiseen.

Vaikka salasanoja ei suositellakaan jakamaan muille ihmisille, sitä kuitenkin tapahtuu säännöllisesti (Singh ym., 2007). Tässä tutkimuksessa kaksi osallistujaa kertoi käyttävänsä hallintasovellusten tarjoamaa turvallisempaa salasanojen jakoa. Koska Whittyn ym. (2015) mukaan tietoturvatietoisuus ei vaikuta salasanojen jakamiseen muutenkaan, voidaan todeta hallintasovelluksen lisäävän turvallisuutta salasanojen jakamisen osalta.

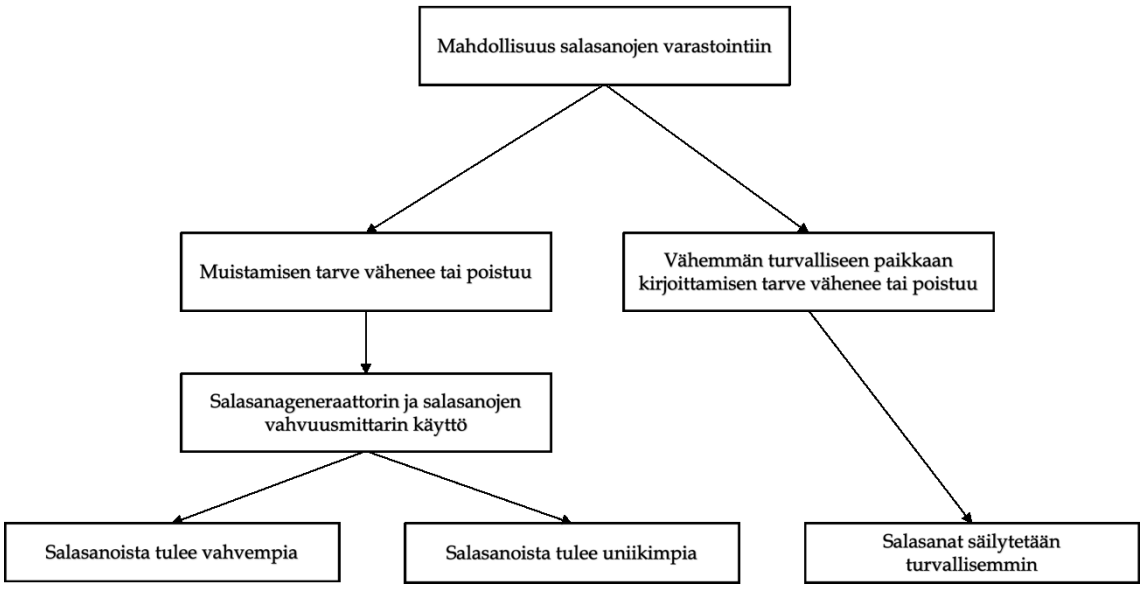
Lisäksi eräs vaikutus salasanahallintaan oli kahden tutkittavan osalta se, että he eivät enää käyttäneet yhtä paljoa salasanan nollaus -toimintoa eri palveluissa.

On huomion arvoista, että hallintasovelluksen käyttöönotto ja salasanojen parantaminen ei vaadi toteutusta kerralla. Moni haastateltavista kertoi toteuttaneensa sekä salasanojen varastoinnin että parantamisen hiljalleen, usein sitä mukaa kuin kyseisille käyttäjätunnuksille tuli tarvetta. Eräs syistä olla ottamatta hallintasovellusta käyttöön oli Stobertin ja Biddlen (2018) mukaan nimenomaan haluttomuus tehdä alkujärjestelyt tilin osalta. Aihe on tämän tutkimuksen varsinaisten tutkimusongelmien ulkopuolella, mutta hallintasovellusten portaittaisessa käyttöönotossa voisi olla potentiaalia lisäperusteeksi suositeltaessa kyseisiä ohjelmia uusille käyttäjille.

7.4 Hallintasovellukset ja salasanojen käyttö

Päätutkimuskysymys kuului: ”miten salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen käyttöön?” Siihen vastaamiseksi koostetaan alatutkimuskysymysten vastaukset sekä pohditaan tärkeisiin käyttäjätileihin liittyvien salasanojen hallinnan kysymystä.

Salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen käyttöön siten, että sovellusten käytön myötä salasanat ovat sekä vahvempia että monimuotoisempia ja niitä säilytetään turvallisemmin kuin aiemmin – käyttäjät ovat jättäneet salasanojen kirjoittamisen paperille tai digitaaliseen muotoon joko kokonaan tai osittain. Tärkeimpinä syinä tähän ovat erityisesti hallintasovellusten tarjoamista työkaluista salasanageneraattori ja salasanojen vahvuusmittari. Kaiken taustalla on sovelluksen tarjoama turvallinen varastointipaikka, jonka avulla kaikkia salasanojaan ei tarvitse muistaa itse. Tuloksissa keskeisimmin esiin nousseet hallintasovellusten vaikutusmekanismit salasanojen käyttöön on kuvattu kuviossa 1.



KUVIO 1 Salasanojen hallintasovellusten keskeisimmät vaikutusmekanismit salasanojen käyttöön

Hallintasovelluksen positiivinen vaikutus vahvuuteen ja uniikkiuteen vahvistaa Lyastanin ym. (2018) tehdyn tutkimuksen tuloksia. Heidän tutkittuaan eroja hallintasovellusten käyttäjien ja ei-käyttäjien välillä, tämä tutkimus täydentää tuloksia ottamalla huomioon yksittäisen käyttäjän salasanojen käytön ennen ja jälkeen hallintasovelluksen käyttöönoton. Muina täydentävinä elementteinä kyseisen tutkimuksen tuloksiin ovat tarkentuneet syyt vahvuuteen ja uniikkiuteen: hallintasovellusten tarjoamat työkalut – muut kuin salasanageneraattori – kuten vahvuusmittari ja duplikaattien tunnistus.

Lyastanin ym. (2018) tutkimusaiheiden ulkopuolelta tämä tutkimus valottaa muutoksia myös muussa salasananhallinnassa. Käyttäjät jakavat

salasanojaan entistä tietoturvallisemmin, seuraavat enemmän esiin tulleita tietovuotoja sekä käyttävät vähemmän salasanojen nollaus -toimintoa.

Lyastani ym. (2018) esittivät tutkimuksessaan kysymyksen ”miksi salasanojen hallintasovellusten käyttäjät edelleen uudelleenkäyttävät salasanojaan sekä käyttävät heikkoja salasanoja?” (Lyastani ym., 2018, s. 215). Kysymys kumpuaa heidän tuloksestaan, jonka mukaan, vaikka hallintasovelluksen käyttö on yhteydessä parempiin ja uniikimpiin salasanoihin, niiden käyttäjät eivät ole kummassakaan lähelläkään täydellistä. Tämän tutkimuksen tuloksista on mahdollisesti löydettävissä vastaus heidän pohdinnalleen: Kaksi haastatelluista kertoi vanhojen salasanojensa olevan vielä ajalta ennen hallintasovelluksen käyttöä. Niiden vaihtaminen oli molemmilla vähintäänkin aikeena.

Kaksi tämän tutkimuksen osallistujista mainitsi pitävänsä itselleen tärkeimmät salasanat mieluummin hallintasovelluksen ulkopuolella. Luottamus palveluntarjoajaa kohtaan on noussut esiin aiemmassakin tutkimuksessa. Kuten esimerkiksi Stobert ja Biddle (2018) sekä Pearman ym. (2019) mainitsevat, yksi keskeinen syy olla ottamatta käyttöön salasanojen hallintasovellusta on luottamuksen puute. Fagan ym. (2017) täydentävät tätä myös sovellusta jo käyttävien näkökulmasta: osa käyttäjistä jättää tärkeimmät salasanansa palvelun ulkopuolelle. Alodhyanin ym. (2020) tutkimuksessa 46 % vastaajista sanoi, ettei tallentaisi hallintasovellukseen pankki- tai passitietojaan. Yleisesti salasanojen vahvuuteen liittyen Tamin ym. (2010) mukaan salasanojen vahvuus vertautuu käyttäjätilien tärkeyteen: esimerkiksi verkkopankkien osalta käyttäjien salasanat ovat vahvempia kuin vähemmän tärkeiden tilien. Tämä johtuu heidän mukaansa turvallisuus–käytännöllisyys-vaihtokaupasta, jossa vähemmän turvallinen salasana on muistettavuuden vuoksi heikompi. Kuitenkin tämän tutkimuksen kontekstissa hallintasovellusten tarjoama mahdollisuus varastoida salasanoja muokkaa kyseisen vaihtokaupan käytännöllisyysaspektia, koska niitä ei tarvitse muistaa itse.

Suojattavan tilin tärkeyden ja salasanan vahvuuden välinen suhde nostaakin esiin kiinnostavan kysymyksen salasanojen hallintasovellusten kontekstissa: mikäli käyttäjä päättää säilyttää itselleen tärkeimpien (esimerkiksi pankkipalveluihin liittyvien) tilien salasanat sovelluksen ulkopuolella, ja hän luo useimmat hallintasovellukseen tallennettavat salasanansa generaattorilla (kuten valtaosa tämän tutkimuksen haastatelluista), onko lopputuloksena mahdollisesti tilanne, jossa hänen tärkeimmät salasanansa ovatkin heikompia kuin vähemmän tärkeät? Mikään ei toki estä luomasta tärkeimpiäkin – sovelluksen ulkopuolisia – salasanoja generaattorilla, kuten esimerkiksi yksi haastatelluista kertoi toimivansa, mutta silloin haasteeksi muodostuu kuitenkin turvallinen säilytys.

7.5 Jatkotutkimusaiheet

Koska salasanojen hallintasovelluksista on tehty paljon tutkimusta, mutta vain pieni osa siitä on keskittynyt hallintasovellusten todelliseen vaikutukseen käyttäjien salasanojen käytössä, tulisi tutkimusta jatkaa kyseisen teeman sisällä. Tämän tutkimuksen tulokset ovat laajennettavissa määrälliseen tutkimukseen siitä,

kuinka paljon hallintasovellusten käyttöönotto on vahvistanut tai monimuotoistanut yksittäisen käyttäjän salasanoja, ja mitkä ovat olleet tärkeimmät syyt muutosten takana. Erityishuomiota tulisi kohdistaa tutkittavien erilaisiin tietoturvaosaamistaustoihin. Lisäksi eri työkalujen vaikutusta salasanojen laatuun tulisi tutkia tarkemmin, sillä sen avulla olisi mahdollista saada tärkeää tietoa vaikuttavimmista apuvälineistä käyttäjien salasanakäyttäytymisen tukemisessa. Tulosten muuttamiseksi käytännön hyödyksi tulisi tutkia myös sitä, miten tuloksia voidaan hyödyntää pyrittäessä saamaan hallintasovelluksille uusia käyttäjiä.

Tulosten analysoinnin aikana esiin nousseista, mutta tämän tutkimuksen tutkimusongelmien ulkopuolisista asioista olisi hyvä tutkia salasanojen hallintasovelluksia käyttämättömien ihmisten ajatuksia ja asenteita sitä työmäärää kohtaan, jonka he ajattelevat aiheutuvan salasanahallinnan parantamiseksi hallintasovelluksen avulla. Kuten aiemmin todettiin, lähestymistapa omiin salasanoihin ja niiden parantamiseen voi olla pidemmän aikavälin projekti sen sijaan, että kaikki tulisi tehdä kerralla valmiiksi.

Lisäksi salasanojen hallintasovellusten yleistyessä mielenkiintoinen tutkimusaihe voisi olla, säilyttävätkö käyttäjät hallintasovelluksen ulkopuolella vahvempia vai heikompia salasanoja kuin sen sisällä.

8 YHTEENVETO

Sekä salasanojen vuosi vuodelta kasvava määrä että niiden murtamistapojen kehittymisestä johtuvat entistä kovemmat vaatimukset haastavat eri verkkopalveluita käyttävien ihmisten muistikapasiteettia (Garfinkel & Lipford, 2014; J. Zhang ym., 2009). Tämä asettaa käyttäjän usein tilanteeseen, jossa tulee tehdä valinta mukavuuden ja turvallisuuden välillä (Tam ym., 2010). Valintaan vaikuttaa usein halu tai tarve päästä käyttämään palvelua mahdollisimman pian sekä näkemys juuri kyseisen palvelun merkittävyydestä käyttäjälle itselleen (Brown ym., 2004; Egelman ym., 2013). Vaikka ihmiset ymmärtäisivätkin tarpeen vahvoille salasanoille, käytettävyys ajaa useimmin turvallisuuden edelle (Kanta ym., 2021; Yildirim & Mackie, 2019).

Salasanojen hallintasovellusten on toivottu tuovan tähän ongelmaan ratkaisu niiden tarjoaman turvallisen säilytystilan – ja sitä kautta ihmisen oman muistamistarpeen vähenemisen – myötä (Seiler-Hwang ym., 2019). Niiden käyttöönottoaste on kuitenkin todettu matalaksi, sillä ihmiset eivät esimerkiksi koe tarvitsevansa apua salasanojensa hallintaan, eivät tiedä niistä tarpeeksi tai eivät luota palveluntarjoajiin riittävästi (Pearman ym., 2019; Stobert & Biddle, 2018). Lisäksi palvelut käyttöön ottaneiden osalta niiden käyttöä vähentää muun muassa eri alustojen välisen integraation puute, sovellusten erilaiset ongelmatapaukset sekä ihmisten halu myös muistaa omat salasanansa (Oesch ym., 2022; Pearman ym., 2019). Moni käyttäjistä pitääkin hallintasovellusta ainoastaan säilömispaikkana vanhoille salasanoilleen (Alodhyani ym., 2020).

Salasanojen hallintasovellusten tutkimus on keskittynyt pääasiassa käytön, käytettävyyden ja turvallisuuden haasteisiin, ja paljon vähemmän tutkimusta on tehty niiden varsinaisesta vaikutuksesta käyttäjien salasanoihin (Lyastani ym., 2018). Tämän tutkimuksen tarkoituksena on ollut täydentää tuota aukkoa selvittämällä, miten hallintasovellusten käyttöön ottaminen on vaikuttanut ihmisten salasanojen käyttöön. Alatutkimusongelmina on selvitetty hallintasovellusten vaikutusta salasanojen vahvuuteen, uniikkiuteen sekä yleisesti niiden hallintaan. Käyttäjän oman toiminnan muuttumiseen keskittyvä lähestymistapa on eronnut Lyastanin ym. (2018) aiemmasta tutkimuksesta, jossa vertailtiin hallintasovellusten käyttäjiä ja ei-käyttäjiä.

Tutkimukseen osallistui 13 salasanojen hallintasovelluksia käyttänyttä henkilöä, joilla oli käyttöhistoriaa puolesta vuodesta yli kahteentoista vuoteen. Suurin osa osallistujista käytti hallintasovelluksia henkilökohtaisten tiliensä salasanojen hallintaan, mutta mukana oli myös työympäristössä niitä käyttäviä henkilöitä. Tutkimusaineisto kerättiin teemahaastatteluin jokaiselta osallistujalta erikseen. Haastatteluissa kysyttiin osallistujien näkemyksiä salasanojen käyttönsä muuttumisesta hallintasovelluksen käyttöönoton myötä. Heidän oikeita salasanojaan eri palveluissa ei tarkasteltu. Aineiston analysointiin käytettiin temaattista analyysiä.

Tutkimuksen tulosten mukaan salasanojen hallintasovellusten käyttäminen vaikuttaa salasanojen käyttöön siten, että sovellusten käytön myötä salasanat ovat sekä vahvempia että monimuotoisempia, ja käyttäjien vähemmän turvalliset tavat säilyttää salasanoja ovat vähentyneet tai loppuneet kokonaan. Syinä tähän ovat erityisesti hallintasovellusten tarjoama salasanageneraattori sekä turvallisen salasanojen varastoinnin myötä vähentynyt tarve muistaa salasanat itse. Lisäksi hallintasovellusten tarjoamat erilaiset työkalut ovat mahdollistaneet turvallisemman salasanojen jakamisen sekä tehneet osasta käyttäjistä valveentuneempia tietovuotojen osalta.

Tulokset täydentävät Lyastanin ym. (2018) tutkimuksen löydöksiä salasanojen hallintasovellusten ja salasanageneraattoreiden käyttäjien vahvemmista ja monimuotoisemmista salasanoista ei-käyttäjiin nähden. Lisähavaintoina ovat loppunut tai vähentynyt salasanojen kirjoittaminen muistiin vähemmän turvallisiin paikkoihin sekä eri työkalujen positiivinen vaikutus salasanojen turvallisuuteen.

Tutkimuksen suurimpana rajoituksena on sen kohdejoukko, jonka taustat painottuivat vahvan tietoturvatietoisuuden ja -osaamisen suuntaan. Vaikka tutkimukseen osallistui henkilöitä myös tietotekniikan opiskelijoiden ulkopuolelta, suurin osa koki olevansa tietoturvaan ja erityisesti salasanoihin liittyvissä kysymyksissä valveutuneita. Tämä voi johtaa tutkimuksen heikkoon yleistettävyyteen kaikkien hallintasovellusten käyttäjien osalta, joskin Faganin ym. (2017) mukaan hallintasovelluksia käyttävät ovat lähtökohtaisesti keskimääräistä tietoturvaorientoituneempia. Toisena rajoituksena on se, että osallistujien oikeita salasanoja ei mitattu, vaan tulokset muodostettiin heidän omien näkemystensä pohjalta. On mahdollista, että haastateltavat eivät osanneet tai halunneet arvioida entisiä tai nykyisiä salasanojen käyttönsä aspekteja realistisesti.

Kaiken kaikkiaan tämä tutkimus täytti vähemmälle huomiolle jäänyttä osaaluetta salasanojen hallintasovellusten tutkimuksessa: niiden varsinaista vaikutusta käyttäjien salasanoihin. Tulokset antavat lisäperusteita näkemykselle, että hallintasovellus on hyvä väline parantaa ihmisten salasanakäyttäytymistä sekä henkilökohtaisessa käytössä että työkontekstissa. Aihepiirin sisällä tulisi tutkimusta jatkaa selvittämällä, miten vaikutus näkyy tietoturvaosaamisen kannalta eritaustaisilla ihmisillä, sekä miten saatuja tuloksia voitaisiin tehokkaasti hyödyntää uusien käyttäjien saamiseksi salasanojen hallintasovellusten pariin.

LÄHTEET

ACSC. (2021, 6. lokakuuta). Creating Strong Passphrases. Haettu 27.8.2022 osoitteesta https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Creating%20Strong%20Passphrases%20%28October%202021%29.pdf

Adams, A. & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.

Albayram, Y., Liu, J., & Cangonj, S. (2021). Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager. Teoksessa *Proceedings of the EuroUSEC '21: European Symposium on Usable Security*, 89–104. Karlsruhe, Germany, October 11–12, 2021.

Alkaldi, N., Renaud, K. & Mackenzie, L. (2019). Encouraging password manager adoption by meeting adopter self-determination needs. Teoksessa *Proceedings of the 52nd Hawaii International Conference on System Sciences* (4824–4833). Grand Wailea, United States, January 8–11, 2019.

Alodhyani, F., Theodorakopoulos, G. & Reinecke, P. (2020). Password Managers—It's All about Trust and Transparency. *Future Internet*, *12*(11), 189–238.

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.

Aronson, J. (1995). A Pragmatic View of Thematic Analysis. *The Qualitative Report*, *2*(1), 1–3.

Aurigemma, S., Mattson, T. & Leonard, L. N. K. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? Teoksessa *50th Hawaii International Conference on System Sciences, HICSS 2017,* 1–10. Hilton Waikoloa Village, Hawaii, USA, January 4-7, 2017.

Ayyagari, R., Lim, J. & Hoxha, O. (2019). Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers. *Contemporary Management Research*, *15*(4), 227–245.

Barua, A., Zulkernine, M. & Weldemariam, K. (2013). Protecting Web Browser Extensions from JavaScript Injection Attacks. Teoksessa *18th International Conference on Engineering of Complex Computer Systems*, (188–197). Singapore, Singapore, July 17–19, 2013.

Bhana, B. & Flowerday, S. (2020). Passphrase and keystroke dynamics authentication: Usable security. *Computers & Security*, *96*, 101925.

Bonneau, J., Herley, C., Van Oorschot, P. C. & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Teoksessa *Proceedings - IEEE Symposium on Security and Privacy*, (553–567). San Francisco, USA, May 20–23, 2012.

Boonkrong, S., Kitthimon, A., Koksoungnoen, P. & Jenprakhon, K. (2021). Password Strength Metre Application. *International Journal of Interactive Mobile Technologies*, *15*(15), 59–73.

Brown, A. S., Bracken, E., Zoccoli, S. & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, *18*(6), 641–651.

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.

Cerniauskaite, P. (2021, 23. marraskuuta). Are we still lazy with our passwords? The 2021 top 200 most common passwords list is here. Haettu 13.11.2022 osoitteesta https://nordpass.com/blog/are-we-still-lazy-with-passwords/

Chandrashekhar, B. N. (2022, 3. toukokuuta). Focus: Try Scapy for Cyber Security. Haettu 22.8.2022 osoitteesta https://www.opensourceforu.com/2022/05/try-scapy-for-cyber-security/

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M. & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, *33*, 69–90.

Choong, Y.-Y. (2014). A Cognitive-Behavioral Framework of User Password Management Lifecycle. Teoksessa T. Tryfonas & I. Askoxylakis (Toim.), *Human Aspects of Information Security, Privacy, and Trust* (127–137). Springer International Publishing.

Corbin, J. & Strauss, A. L. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (Fourth edition). SAGE Publications.

Creese, S., Hodges, D., Jamison-Powell, S. & Whitty, M. (2013). Relationships between Password Choices, Perceptions of Risk and Security Expertise. Teoksessa L. Marinos & I. Askoxylakis (Toim.), *Human Aspects of Information Security, Privacy, and Trust* (80–89). London: Springer Heidelberg.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

D. J. Neufeld. (2010). Understanding Cybercrime. *2010 43rd Hawaii International Conference on System Sciences*, 1–10.

Das, A., Bonneau, J., Caesar, M., Borisov, N. & Wang, X. (2014). The Tangled Web of Password Reuse. Teoksessa *Proceedings of NDSS 2014*. San Diego, United States, February 23–26, 2014.

Duggan, G. B., Johnson, H. & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, *70*(6), 415–431.

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. Teoksessa *Proceedings of the SIGHCHI Conference on Human Factors in Computing Systems* (2379–2388). Paris, France, April 27 – May 2, 2013.

Eskola, J., Lätti, J. & Vastamäki, J. (2018). Teemahaastattelu: Lyhyt selviytymisopas. Teoksessa *Ikkunoita tutkimusmetodeihin 1* (5. uud. painos). Jyväskylä: PS-kustannus.

Eve, M. P., Bogost, I. & Schaberg, C. (2019). *Password*. London: Bloomsbury Academic.

Fagan, M., Albayram, Y., Khan, M. M. H. & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, *7*(1), Art. 1.

Fahl, S., Harbach, M., Oltrogge, M., Muders, T. & Smith, M. (2013). Hey, you, get off of my clipboard: On how usability trumps security in android password managers. Teoksessa Sadeghi, A.-R. (Toim.) *FC 2013, LNCS 7859* (144–161). Berlin: Springer-Verlag.

Farooq, A., Dubinina, A., Virtanen, S., & Isoaho, J. (2021). Understanding Dynamics of Initial Trust and its Antecedents in Password Managers Adoption Intention among Young Adults. Teoksessa *Proceedings of the 12th International Conference on Ambient Systems, Networks and Technologies*, 266–274. Warsaw, Poland, March 23–26, 2021.

Flick, U. (2009). *An Introduction to Qualitative Research*. SAGE Publications.

Fukumitsu, M., Hasegawa, S., Iwazaki, J.-Y., Sakai, M. & Takahashi, D. (2016). A Proposal of a Password Manager Satisfying Security and Usability by Using the Secret Sharing and a Personal Server. Teoksessa *IEEE 30th International Conference on Advanced Information Networking and Applications* (661–668). Crans-Montana, Switzerland, 23–25 March, 2016.

Furnell, S. (2022). Assessing website password practices – Unchanged after fifteen years? *Computers & Security*, *120*, 102790.

Galbally, J., Coisel, I. & Sanchez, I. (2017). A New Multimodal Approach for Password Strength Estimation-Part I: Theory and Algorithms. *IEEE Transactions on Information Forensics and Security*, *12*(12), 2829–2844.

Garfinkel, S. & Lipford, H. R. (2014). *Usable Security: History, Themes, and Challenges*. Switzerland: Springer.

Gokhale, Mrs. A. S. & Waghmare, V. S. (2016). The Shoulder Surfing Resistant Graphical Password Authentication Technique. *Procedia Computer Science*, *79*, 490–498.

Grawemeyer, B. & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267.

Herley, C. & Van Oorschot, P. (2012). A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, *10*(1), 28–36.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.

Hu, G. (2018). On Password Strength: A Survey and Analysis. Teoksessa Lee, R. (Toim.), *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, Studies in Computational Intelligence 721. Springer International Publishing

Huaman, N., Amft, S., Oltrogge, M., Acar, Y. & Fahl, S. (2022). They Would Do Better If They Worked Together: Interaction Problems Between Password Managers and the Web. *IEEE Secur. Priv.*, *20*(2), 49–60.

Kaleta, J. P., Lee, J. S. & Yoo, S. (2019). Nudging with construal level theory to improve online password use and intended password choice: A security-usability tradeoff perspective. *Information Technology & People (West Linn, Or.)*, *32*(4), 993–1020.

Kalniņš, R., Puriņš, J. & Alksnis, G. (2017). Security Evaluation of Wireless Network Access Points. *Applied Computer Systems*, *21*(1), 38–45.

Kanta, A., Coray, S., Coisel, I. & Scanlon, M. (2021). How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts. *Forensic Science International: Digital Investigation*, *37*(6), 301186.

Karjalainen, M., Sarker, S. & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*, *30*(2), 687–704.

Karjalainen, M., Siponen, M., Puhakainen, P. & Sarker, S. (2013). One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. Teoksessa *PACIS 2013 Proceedings*. Jeju Island, Korea, June 18–22, 2013.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M., Bauer, L., Christin, N., Cranor, L. & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. Teoksessa *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (2595–2604). Vancouver, Canada, May 7–12, 2011.

Kuo, C., Romanosky, S. & Cranor, L. (2006). Human selection of mnemonic phrase-based passwords. Teoksessa *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, (67–78). Pittsburgh, USA, July 12–14, 2006.

Kyberturvallisuuskeskus. (2022, 3. toukokuuta). Pidempi parempi—Näin teet hyvän salasanan. Haettu 27.8.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Li, L., He, W., Xu, L., Ash, I., Anwar, M. & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24.

Li, Y. & Siponen, M. (2011). A Call For Research On Home Users' Information Security Behaviour. Teoksessa *PACIS 2011 – 15th Pacific Asia Conference on Information Systems: Quality Research in Pacific*. Brisbane, Australia, 7–11 July, 2011.

Li, Y., Xin, T. & Siponen, M. (2022). Citizens' Cybersecurity Behavior: Some Major Challenges. *IEEE Security & Privacy*, *20*(1), 54–61.

Li, Z., He, W., Akhawe, D. & Song, D. (2014). The Emperor's new password manager: Security analysis of web-based password managers. Teoksessa *Proceedings of the 23rd USENIX Security Symposium*, (465–479). San Diego, United States, August 20–22, 2014.

Liu, X., Huang, Q., Wang, H. & Liu, S. (2019). Employment security and employee organizational citizenship behavior: Does an 'iron rice bowl' make a difference? *International Journal of Human Resource Management*, *30*(13), 2077–2096.

Lyastani, S. G., Schilling, M., Fahl, S., Backes, M. & Bugiel, S. (2018). Better managed than memorized? Studying the impact of managers on password strength and reuse. Teoksessa *Proceedings of the 27th USENIX Security Symposium*, (203–220). Baltimore, USA, August 15–17, 2018.

Ma, W., Campbell, J., Tran, D. & Kleeman, D. (2010). Password Entropy and Password Quality. Teoksessa *Proceedings of the Fourth International Conference on Network and System Security*, (583–587). Melbourne, Australia, 1–3 September, 2010.

Maoneke, P. B., Flowerday, S. & Isabirye, N. (2020). Evaluating the strength of a multilingual passphrase policy. *Computers & Security*, *92*, 101746–14.

Mayer, P., Munyendo, C. W., Mazurek, M. L. & Aviv, A. J. (2022). Why Users (Don't) Use Password Managers at a Large Educational Institution. Teoksessa *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, (1849–1866). Boston, USA, August 10–12, 2022.

Mazurek, M., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L., Kelley, P., Shay, R. & Ur, B. (2013). Measuring password guessability for an entire university. Teoksessa *Proceedings of the ACM Conference on Computer and Communications Security.* Berlin, Germany, November 4–8, 2013.

Morris, R. & Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, *22*(11), 594–597.

Murray, H. & Malone, D. (2020). Convergence of Password Guessing to Optimal Success Rates. *Entropy*, *22*(4), 378.

Myers, M. & Newman, M. (2007). The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization*, *17*(1), 2–26.

NCSC (2018, 19. marraskuuta). Password administration for system owners. Haettu 27.8.2022 osoitteesta https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

NIST (2020, 2. maaliskuuta). NIST Special Publication 800-63B Digital Identity Guidelines. Haettu 27.8.2022 osoitteesta https://pages.nist.gov/800-63-3/sp800-63b.html

NIST (2022, 3. maaliskuuta). NIST Special Publication 800-63: Digital Identity Guidelines Frequently Asked Questions. Haettu 27.8.2022 osoitteesta https://pages.nist.gov/800-63-FAQ/

Oesch, S., Ruoti, S., Simmons, J. & Gautam, A. (2022). "It Basically Started Using Me:" An Observational Study of Password Manager Usage. Teoksessa *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, (1–23). New Orleans, USA, 29 April – 5 May, 2022.

O'Hanley, R. & Tiller, J. S. (2014). *Information Security Management Handbook, Volume 7*. Boca Raton: Auerbach Publications.

Parsons, K., McCormac, A. & Butavicius, M. A. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment Executive Summary*. (DSTO-TR-2484). Commonwealth of Australia, Defence Science and Technology Organisation.

Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelmany, S. & Forgetz, A. (2017). Let's Go in for a closer look: Observing passwords in their natural habitat. Teoksessa *Proceedings of the ACM Conference on Computer and Communications Security*, (295–310). Dallas, USA, 30 October – 3 November, 2017.

Pearman, S., Zhang, S. A., Bauer, L., Christin, N. & Cranor, L. F. (2019). Why people (don't) use password managers effectively. *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*, (319–338). Santa Clara, USA, August 12–13, 2019.

Pittman, J. M. & Robinson, N. (2020). *Shades of Perception- User Factors in Identifying Password Strength*. arXiv:2001.04930.

Puhakainen, P. (2006). *A design theory for information security awareness* (Väitöskirja). Oulun yliopisto. Haettu osoitteesta http://urn.fi/urn:isbn:9514281144

Qureshi, M. A., Younus, A. & Khan, A. A. (2009). Philosophical Survey of Passwords. *International Journal of Computer Science Issues*, *2*, 8.

Ray, H., Wolf, F., Kuber, R. & Aviv, A. J. (2021). Why Older Adults (Don't) Use Password Managers. Teoksessa *Proceedings of the 30th USENIX Security Symposium,* (73–90). Vancouver, Canada, August 11–13, 2021.

Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D. & Becker, C. (2019). *"I don't see why I would ever want to use it": Analyzing the Usability of Popular Smartphone Password Managers*. Teoksessa *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security,* (1937–1953). London, United Kingdom, November 11–15, 2019.

Silver, D., Jana, S., Boneh, D., Chen, E. & Jackson, C. (2014). Password managers: Attacks and defenses. *Proceedings of the 23rd USENIX Security Symposium*, (449–464). San Diego, United States, August 20–22, 2014.

Singh, S. Cabraal, A., Demosthenous, C., Astbrink, G. & Furlong, M. (2007). Password sharing: Implications for security design based on social practice. Teoksessa *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* (895–904). San Jose, USA, 28 April – 3 May, 2007.

Stobert, E. & Biddle, R. (2018). The password life cycle. *ACM Transactions on Privacy and Security*, *21*(3), 1–32.

Suo, X., Zhu, Y. & Owen, G. S. (2005). Graphical passwords: A survey. Teoksessa *Proceedings of the 21st Annual Computer Security Applications Conference*. Tucson, USA, 5–9 December, 2005.

Tam, L., Glassman, M. & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour and Information Technology*, *29*(3), 233–244.

Taneski, V., Kompara, M., Heričko, M. & Brumen, B. (2021). Strength Analysis of Real-Life Passwords Using Markov Models. *Applied Sciences*, *11*(20), 9406.

Tanni, T., Taharat, T., Parvez, M., Rumee, S. & Zaber, M. (2022). Is My Password Strong Enough?: A Study on User Perception in The Developing World. *EAI Endorsed Transactions on Creative Technologies*, *9*(30), 173452.

Theodorakopoulos, G. & Reinecke, P. (2020). Password Managers—It's All about Trust and Transparency. *Future Internet*, *12*(11), 189.

Ur, B., Kelly, P., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. & Cranor, L. (2012). How does your password measure up? The effect of strength meters on password creation. Teoksessa *Proc. Security '12, USENIX Association*. Bellevue, USA, August 8–10, 2012.

Vacca, J. (2013). *Computer and Information Security Handbook* (2. uud. painos) Burlington: Morgan Kaufmann.

Van Ouytsel, J. & De Groote, D. (2022). Research brief: Early adolescents' perceptions of the motivations and consequences of sharing passwords with friends in Belgium. *Journal of Children and Media*, 1–12.

Vance, A., Eargle, D., Eggett, D., Straub, D. & Ouimet, K. (2022). Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength. *MIS Quarterly*, *46*(3), 1721.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. (Belin), Cook, J. & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744–757.

Wash, R., Rader, E., Berman, R. & Wellmer, Z. (2016). Understanding Password Choices: How Frequently Entered Passwords Are Re-Used across Websites. Teoksessa *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, (175–188). Denver, USA, June 22–24, 2016.

Whitty, M., Doodson, J., Creese, S. & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior and Social Networking*, *18*(1), 3–7.

Woods, N. (2016). *Improving the security of multiple passwords through a greater understanding of the human memory* (Väitöskirja). Jyväskylän yliopisto. Haettu osoitteesta http://urn.fi/URN:ISBN:978-951-39-6846-5

Woods, N. (2017). Frequently Using Passwords Increases Their Memorability — A False Assumption or Reality? Teoksessa *AMCIS 2017: Proceedings of the Twenty-third Americas Conference on Information Systems*, (1–5). Boston, USA, 10–12 August, 2017.

Woods, N. & Silvennoinen, J. (2022). Enhancing the user authentication process with colour memory cues. *Behaviour & Information Technology,* 1–20.

Woods, N. & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, *111*, 36–48.

Woods, N. & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, *128*, 61–71.

Yildirim, M. & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759.

Zhang, J., Luo, X., Akkaladevi, S. & Ziegelmayer, J. (2009). Improving multiple-password recall: An empirical study. *European Journal of Information Systems*, *18*(2), Art. 2.

Zhang, L. & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce*, *8*(3–4), 180–197.

Zhang, Y., Monrose, F. & Reiter, M. K. (2010). The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. Teoksessa *Proceedings of the 17th ACM Conference on Computer and Communications Security*, (176–186). Chicago, USA, October 4–8, 2010.

Zhao, R. & Yue, C. (2014). Toward a secure and usable cloud-based password manager for web browsers. *Computers & Security*, *46*, 32–47.