Eero Lempinen

# SALASANAT, SALASANANHALLINTASOVELLUKSET JA NIIDEN KÄYTTÖÖNOTTO

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

# TIIVISTELMÄ

Lempinen, Eero
Salasanat, salasananhallintasovellukset ja niiden käyttöönotto
Jyväskylä: Jyväskylän yliopisto, 2022, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Halttunen, Veikko

Salasanojen käyttöön liitetty yleinen ongelma on useiden salasanojen muistaminen ja samanaikaisesti vahvojen salasanojen suositusten noudattaminen. Ratkaisuna ongelmaan tarjotaan usein salasananhallintasovelluksia, jotka luovat, tallentavat ja muistavat vahvat salasanat käyttäjän puolesta. Salasananhallintasovellukset eivät silti ole näyttäneen saavuttavan kovinkaan suurta suosiota käyttäjien keskuudessa. Moni ei vaikuta luottavan salasananhallintasovellusten toimintaan, ja suuri osa ei ole edes tietoinen niiden olemassaolosta. Tämän tutkielman tarkoituksena on selvittää salasananhallintasovellusten käyttöönottoon vaikuttavia syitä, sitä miksi ihmiset kertovat käyttävänsä hallintasovelluksia, sekä lisäksi tarkastella salasanoja ja niihin tutkimuksissa liitettyjä ongelmia. Tutkielma pyrkii vastaamaan tutkimuskysymykseen ”Mitkä ovat tutkimuksissa havaitut yleisimmät syyt sille, että käyttäjät ottavat (tai eivät ota) salasananhallintasovellusta käyttöönsä?”. Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielman tuloksena havaittiin, että salasananhallintasovellusten käyttöönottoa käsittelevissä tutkimuksissa päällimmäiset syyt käyttämättömyydelle ovat käyttäjien luottamusongelmat sovelluksia kohtaan, koettu ajanpuute, huonosta salasanaturvallisuudesta aiheutuvien uhkien ja haavoittuvuuksien välittömyyden puute, ja oman salasanaturvallisuuden yliarviointi. Merkittävimpänä syynä salasananhallintasovelluksien käytölle todettiin sovelluksien tuomat helpotukset salasanojen kanssa elämiseen, pääasiassa niiden muistamiseen ja hallintaan. Yllättävän harva käyttäjä mainitsi käyttävänsä salasananhallintasovelluksia salasanaturvallisuuden parantamiseen. Lisäksi melko harva salasananhallintasovelluksien käyttäjistä oli edes tietoinen niiden tarjoamista mahdollisuuksista vahvempien salasanojen käyttämiseen.

Asiasanat: salasanat, salasananhallintasovellukset, tunnistautumismenetelmät

# ABSTRACT

Lempinen, Eero
Passwords, password management applications and their adoption
Jyväskylä: University of Jyväskylä, 2022, 31 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Halttunen, Veikko

A widespread problem associated with the use of passwords is the need to remember multiple passwords and at the same time follow the recommendations for strong passwords. As a solution to this problem, password management applications are often offered that create, store, and remember strong passwords on behalf of the user. However, password management applications do not seem to have gained much popularity among users. Many do not seem to trust them, and many are not even aware of their existence. The purpose of this thesis is to explore the reasons for adopting password management applications, why people choose to use them, and to examine passwords and the problems associated with them in research. This thesis aims to answer the research question "What are the most common reasons found in studies for people adopting (or not adopting) password management applications?". The thesis has been conducted as a literature review. The result of the thesis is that the main reasons for non-adoption found in studies on password management application adoption are lack of trust in the application by users, perceived lack of time, lack of immediacy of threats and vulnerabilities from poor password security, and overestimation of one's own password security. The most important reason found for using password management applications was the comfort they brought to living with passwords, mainly for remembering and managing them. Surprisingly few users mentioned using password management applications to improve password security. Moreover, relatively few users of password management applications were even aware of the possibilities they offer for using stronger passwords.

Keywords: passwords, password management applications, authentication methods

# SISÄLLYS

# 1 JOHDANTO

Salasana on lukuisista erilaisista tunnistautumismenetelmistä ylivoimaisesti eniten käytetty, vaikka monet muut menetelmät (kuten sormenjälkitunnistus) eivät aiheuta käyttäjille läheskään yhtä suurta kognitiivista kuormitusta (Zimmermann & Gerber, 2020). Hyvän salasanan ohjeiden noudattaminen ja useiden kymmenien salasanojen muistaminen muodostaa haasteita käyttäjille (Notoatmodjo & Thomborson, 2009). Muun muassa Bill Gates ennusti jo 2000-luvun alkupuoliskolla salasananpohjaisten tunnistautumisjärjestelmien tulevan katoamaan lähivuosina (Kotadia, 2004), mutta lukuisia vastaavia ennustuksia vasten salasana on silti yhä vallalla. 2000-luvun aikana onkin noussut useita salasananhallintasovelluksia ratkaisemaan salasanaan liitettyjä ongelmia, pääasiassa niiden muistamisen haastavuutta.

Herleyn ja van Oorschotin (2012) mukaan huolimatta vuosikymmenien aikana ehdotetuista lukuisista vaihtoehdoista, salasanat ovat pysyneet käytetyimpänä tunnistautumistapana, ja vaihtoehdot ovat epäonnistuneet yhtä suuren käyttöasteen saavuttamisessa. 15 vuotta sitten internetin käyttäjällä oli jo keskimäärin 25 eri tiliä (Florencio & Herley, 2007), ja lukumäärä on nykyhetkellä hyvin todennäköisesti vielä suurempi. Heikot ja yksinkertaiset salasanat sekä niiden uudelleenkäyttö ovat yhä tunnistettuja ongelmia tietoturvallisuudessa, joista ensimmäinen havaittiin jo 1970-luvulla (Morris & Thompson, 1979). Erityisesti salasanojen uudelleenkäyttö on laaja ja käyttäjien tietoturvaa heikentävä ongelma verkossa (Florencio & Herley, 2007). Syyksi uudelleenkäytölle on oletettu käyttäjien vaikeus muistaa useita monimutkaisia salasanoja (Florencio ym., 2014; Notoatmodjo & Thomborson, 2009). Samanaikaisesti hyvän, vahvan salasanan ominaisuuksien täyttäminen ja useiden erilaisten salasanojen muistaminen on hankalaa.

Salasananhallintasovellukset pyrkivät ratkaisemaan käyttäjien raportoimia ongelmia tallentamalla käyttäjän salasanat yhteen palveluun, useimmiten yhden pääsalasanan taakse (monesti yhdistettynä kaksivaiheiseen tunnistautumiseen). Salasanat säilytetään sovelluksesta riippuen joko salatussa tietokannassa laitteella, jolle sovellus on asennettu tai verkossa pilvipalvelussa. Eri sovellustyyppeihin ja tallennusmuotoihin liittyy erilaisia haavoittuvuuksia. Suuri osa

sovelluksista tarjoaa ominaisuuden vahvojen salasanojen generoimiseen ja siten salasanaturvallisuuden parantamiseen. Konseptin salasananhallintasovellukselle, salasanojen tallentamiselle tietokantaan kryptatussa muodossa yhden pääsalasanan taakse, esittelivät todennäköisesti ensimmäisenä Luo ja Henry (2003). Nykyisin salasananhallintasovelluksia on markkinoilla useita, niin ilmaisia kuin maksullisia sekä suljetun ja avoimen lähdekoodin vaihtoehtoja vaihtelevilla ominaisuuksilla.

Salasananhallintasovelluksiin kohdistunut tutkimus on pirstaleista, mutta pääasiassa keskittynyt selvittämään sovelluksien konkreettista tietoturvallisuutta niiden hyödyntämissä tallennusmenetelmissä ja automaattisen täytön turvallisuudessa. Muutamat salasananhallintasovelluksien käyttöön kohdistuneet tutkimukset ovat selvittäneet tekijöitä, jotka vaikuttavat sovelluksien käyttöönottoon (Alodhyani ym., 2020; Aurigemma ym., 2017; Ayyagari ym., 2019; Fagan ym., 2017; Pearman ym., 2019; Ray ym., 2021). Tutkimusten näkökulmana on ollut lähtökohtaisesti, miksi salasananhallintasovelluksia ei käytetä.

Tämän tutkielman tarkoituksena on selvittää kyseisissä tutkimuksissa havaittuja syitä sille, miksi vaikuttaa siltä, että kovin moni ei päätä käyttää salasananhallintasovelluksia, vaikka niiden avulla olisi mahdollista helpottaa useiden salasanojen kanssa elämistä ja parantaa salasanaturvallisuutta. Tämä kandidaatintutkielma pyrkii vastaamaan seuraavaan tutkimuskysymykseen: Mitkä ovat tutkimuksissa havaitut yleisimmät syyt sille, että käyttäjät ottavat (tai eivät ota) salasananhallintasovellusta käyttöönsä?

Kandidaatintutkielma on toteutettu kirjallisuuskatsauksena. Tutkielmaan on etsitty lähteitä käyttäen Google Scholar, JYKDOK ja IEEE Xplore-hakupalveluita. Tietokantahauissa on käytetty hakusanoina seuraavia: *password(s), password reuse, password manager(s), password manager use, password manager usage* ja *password manager adoption.* Tutkielmaan valittujen lähteiden luotettavuus on pääasiassa tarkistettu käyttämällä julkaisufoorumi-palvelua. Lähteiksi on pyritty lähtökohtaisesti valitsemaan jufo-luokitukseltaan vähintään tason 1 julkaisuja, mutta tutkielmaan soveltuvan aineiston rajallisen määrän takia myös tason 0 ja julkaisufoorumista löytymättömiä julkaisuja on valittu muutamia. Niiden tapauksessa julkaisusta on pyritty etsimään mahdollisimman paljon tietoa verkosta, ja arvioimaan luotettavuutta tapauskohtaisesti.

Tutkielma koostuu viidestä luvusta. Johdannossa esitellään tutkielman aihepiiri, tutkimuskysymys ja tutkielman tekotapa. Toisessa luvussa pohjustuksena salasananhallintasovelluksille tarkastellaan salasanoja ja vaihtoehtoisia tunnistautumismenetelmiä, ja käydään läpi tutkimuksissa havaittuja ongelmia salasanojen käytössä. Kolmannessa luvussa esitellään salasananhallintasovelluksien perustoimintaa, niiden eri muotojen luokittelua ja käsitellään lyhyesti salasananhallintasovelluksien vaikutusta niitä käyttävien salasanaturvallisuuteen. Neljännessä luvussa tarkastellaan salasananhallintasovellusten käyttöönoton syitä, lähtökohtana se, miksi hallintasovelluksia ei käytetä. Viimeisessä yhteenvetoluvussa käydään läpi tutkielmassa tehtyjä päähavaintoja, ja niistä tehtävissä olevia johtopäätöksiä.

# 2 SALASANAT TUNNISTAUTUMISMENETELMÄNÄ

Salasanat ovat käytössä olevista tunnistautumismenetelmistä yhä ylivoimaisesti laajimmalle levinnyt ja eniten käytetty, vaikkei välttämättä lähellekään helppokäyttöisin, yksinkertaisin tai ongelmattomin vaihtoehto (Zimmermann & Gerber, 2020). Salasanoihin liittyvää tutkimusta on suoritettu valtavasti jo vuosikymmenien ajan useista eri näkökulmista, kuten turvallisuuden tai käytettävyyden kannalta, ja niiden käytöstä ja toiminnasta on esitetty kritiikkiä ja ongelmakohtia jo ensimmäisistä käyttökohteista lähtien. Ensimmäisissä salasanoja hyödyntäneissä järjestelmissä havaittiin samoja salasanoihin liittyviä ongelmia, mitä yhäkin nykypäivänä pyritään ratkaisemaan, kuten käyttäjien taipumusta valita heikoiksi luokiteltavia salasanoja (Morris & Thompson, 1979). Tässä luvussa tarkastellaan ensin salasanojen alkuperää osituskäyttöjärjestelmissä. Sen jälkeen käsitellään tutkimuksissa havaittuja salasanoihin yleisesti liitettäviä ongelmia. Viimeisessä alikappaleessa käydään läpi muutamia vaihtoehtoisia tunnistautumismenetelmiä, joita on nykyisin käytössä salasanojen rinnalla.

## 2.1 Salasanojen alkuperä tietotekniikan kontekstissa

Salasanojen historia on linkittynyt vahvasti tietokoneiden historiaan. Osituskäyttöjärjestelmien keksiminen ja ilmaantuminen keskustietokoneisiin 1960- ja 70-luvuilla teki ensimmäistä kertaa mahdolliseksi sen, että usea käyttäjä pystyi samanaikaisesti hyödyntämään keskustietokoneen toimintoja ja laskentatehoa (Denning, 1992). Lähes samanaikaisesti huomattiin tarve käyttäjien pääsyn rajoittamiselle, jotta pystyttiin rajaamaan tiedostoja ja toimintoja vain tietyille käyttäjille. Kyseisen tarpeen täyttämiseen hyödynnettiin sarjaa kirjaimia ja/tai numeroita, jotka käyttäjän täytyi kirjoittaa tietokoneelle päästäkseen sisään järjestelmään. Tämä tapahtui nähtävästi ensimmäistä kertaa Massachusetts Institute of Technologyn CTSS-tietokonejärjestelmän yhteydessä 1960-luvulla (McMillan, 2012).

Ensimmäisissä muodoissaan, esimerkiksi CTSS-järjestelmässä, eri käyttäjien salasanoja tallennettiin sellaisenaan yksittäiseen avoimeen salasanatiedostoon, josta järjestelmä pystyi lukemaan ja tarkistamaan salasanojen oikeellisuuden (Morris & Thompson, 1979). Avoin tallennusmenetelmä oli luonnollisesti herkkä haavoittuvuuksille. Tämän huomasivat CTSS:n käyttäjät 60-luvulla, kun järjestelmän toiminnasta johtuvan virheen takia salasanatiedoston sisältö oli hetkellisesti nähtävissä kaikkien käyttäjien kirjautumisruuduilla. Salasanatiedoston sisältöön oli kyseisessä järjestelmässä myös pääsy useilla eri ohjelmilla, ja lisäksi kuka tahansa, joka pääsi käsiksi varmuuskopion sisältävään magneettinauhaan, saattoi suoraan lukea tiedoston sisällön. (Morris & Thompson, 1979)

Ratkaisuksi turvallisuusongelmaan ehdotettiin tallennusmenetelmän muuttaminen siten, että salasanat tallennetaan salasanatiedostoon kryptattuina niiden näkymättä järjestelmässä ollenkaan (Morris & Thompson, 1979). Ehdotuksessa käytetty kryptausmenetelmä lainattiin osittain Yhdysvaltain armeijan käyttämästä salakirjoituskoneesta, ja verrattuna nykyaikaisiin menetelmiin, oli se toiminnaltaan ja turvallisuudeltaan melko alkeellinen. Pohja salasanan hyödyntämiselle tietokonejärjestelmissä oli kuitenkin luotu, ja toimintaperiaatteeltaan salasana säilyi melko muuttumattomana pari seuraavaa vuosikymmentä. 1980-luvulla osituskäytön ja keskustietokoneiden siirryttyä pois henkilökohtaisten tietokoneiden yleistymisen tieltä, kehittyneempiä menetelmiä, kuten erilaisia kryptografisia verkkoprotokollia, liitettiin salasanojen yhteyteen käyttäjien autentikoinnissa paikallisverkon sisällä (Denning, 1992).

Siirryttäessä kohti nykypäivää salasanojen käyttö on räjähtänyt internetin yleistymisen johdosta. Lähtökohtaisesti jokainen käyttäjäpohjainen internetin palvelu hyödyntää salasanoja jossain käyttötarkoituksessa, joko käyttäjätunnuksen ohessa tunnistautumismenetelmänä, tai tukena muiden vaihtoehtoisten menetelmien, kuten erilaisten kaksivaiheisten tunnistautumisten ohessa. Morrisin ja Thompsonin (1979) ehdottaman kryptausmenetelmän vaikutus palveluntarjoajien toimintaan on yhä nähtävissä, sillä esimerkiksi U.S. National Institute of Standards and Technology (NIST) vaatii säilyttämään salasanoja kryptattuina avainjohdannaisfunktioita (key derivation function) käyttäen (Grassi ym., 2017).

## 2.2 Salasanoihin yleisesti liitettyjä ongelmia

Zimmermann ja Gerber (2020) selvittivät eri käyttäjien preferenssejä liittyen erilaisiin autentikointimenetelmiin. Tutkimukseen valitusta 12 menetelmästä vastaajat sijoittivat salasanan ja sormenjälkitunnistautumisen menetelmien kärkeen. Tuloksissa ilmeni mielenkiintoinen havainto: vaikka salasana oli vastaajien suosituin menetelmä, sen käyttöön liitettiin silti suuri kognitiivinen kuormitus, aiheutuen mahdollisesti monimutkaisten ja lukuisien salasanojen muistamisesta.

Bonneaun, Herleyn, van Oorschotin ja Stajanon (2012) mukaan salasanojen jatkuva suosio teknologian ja vaihtoehtoisten menetelmien kehittyessä on ollut ”valtavaksi häpeäksi turvallisuustutkijoille”. Turvallisuuden kannalta salasanat ovat alttiita niin ulkopuoliselle tarkkailulle kuin mahdollisille vuodoille

verkon palveluissa, ja lisäksi muun muassa kalastelua hyödyntäville hyökkäyksille. Johtuen käyttäjien ennalta-arvattavista salasanavalinnoista ja salasanojen uudelleenkäytöstä, eivät salasanat ole turvassa yksinkertaiselta arvailulta (esimerkiksi datasettejä apuna hyödyntäen), ja erityisesti heikot salasanat ovat alttiita väsytyshyökkäyksille (brute-force-attack).

Yhdysvaltain kyberturvallisuusvirasto CISA tarjoaa verkkosivuillaan ohjeistusta salasanojen oikeaan ja turvalliseen käyttöön (CISA, 2019), pohjautuen NIST:in julkaisuun autentikoinnista (Grassi ym., 2017). Eri palveluissa ja tietojärjestelmissä täytyisi käyttää aina eri salasanoja. Salasanojen pitäisi olla myös pitkiä (minimissään 8 merkkiä), esimerkiksi satunnaisista sanoista koostuvia lauseita. Toisaalta salasanojen luonnissa kannattaa välttää suoraan sanakirjoista löytyvien sanojen käyttämistä sanakirjahyökkäyksiltä suojautumiseksi. Salasanat eivät myös saisi koskaan sisältää mitään henkilökohtaisia, käyttäjään liitettäviä tietoja, kuten syntymäpäivää.

CISA:n Ohjeistusta tarkastellessa kaikki vaatimukset ovat loogisia ja täysin ymmärrettäviä, mutta käytännössä niiden täydellinen noudattaminen on työlästä ja haastavaa. Uuden pitkän, satunnaisen salasanan keksiminen joka rekisteröitymisen yhteydessä käy nopeasti turhauttavaksi, ja ellei salasanoille keksi helposti muistettavia muistisääntöjä, joutuu nopeasti turvautumaan erilaisiin selviytymiskeinoihin, kuten salasanojen uudelleenkäyttöön.

Salasanojen uudelleenkäyttö on itsessään laajasti tunnistettu salasanoihin liitetty ongelma (Das ym., 2014; Florencio & Herley, 2007; Wash ym., 2016). Uudelleenkäyttö on käyttäjistä lähtöisin oleva ilmiö, joka altistaa käyttäjiä useille tietoturvariskeille. Moninaiset, ja ajoittain kooltaan valtavat tietoturvavuodot verkon palveluissa eivät vielä yksinään aiheuttaisi suuria ongelmia käyttäjille, mutta ongelmia ilmaantuu, kun yhdessä palvelussa käytettyä vuodettua salasanaa voidaan käyttää muihinkin palveluihin kirjautumiseen. Silloin yhden salasanavuodon johdosta käyttäjän kaikki muut tilit, jotka käyttävät samaa salasanaa, ovat alttiita murrolle.

Suuria salasanadatasettejä hyödyntäneessä tutkimuksessa Das, Bonneau, Caesar, Borisov ja Wang (2014) tarkastelivat salasanojen uudelleenkäyttöä verkossa. Tuloksista kävi ilmi, että täydellinen salasanan kopiointi palveluiden välillä ei usein ole täysin mahdollista, sillä eri palveluissa on erilaisia vaatimuksia salasanoille. Tutkimuksen päätavoitteena oli hyödyntää vuodettuja salasanoja muiden salasanojen arvaamisessa arvausalgoritmin tukena, jolloin jopa 30 % salasanoista oli arvattavissa 100 yrityksellä. Datasettien tarkastelussa havaittiin, että 43 % verkon käyttäjistä hyödyntää samoja salasanoja suoraan niitä muuttamatta muissa palveluissa.

Uudelleenkäytön on katsottu johtuvan siitä, että käyttäjillä on yksinkertaisesti liikaa salasanoja muistettavana, ja siksi uudelleenkäyttäminen on eräänlainen selviytymismekanismi, jolla helpotetaan muistamisesta aiheutuvaa kognitiivista kuormaa. Uudelleenkäytölle on havaittu useita erilaisia menetelmiä. Käyttäjät saattavat hyödyntää samaa salasanaa samaan kategoriaan sijoittuvissa palveluissa, esimerkiksi yhtä salasanaa kaikilla uutissivustoilla ja vastaavasti yhtä salasanaa kaikilla sähköpostitileillä. (Notoatmodjo & Thomborson, 2009).

Salasanoja saatetaan ryhmitellä myös sen mukaan, liittyvätkö palvelut työhön, vapaa-aikaan tai perheeseen (Notoatmodjo & Thomborson, 2009). Silloin samaa salasanaa käytetään kaikissa palveluissa, jotka liittyvät jollain tavoin käyttäjän työhön, ja samaa salasanaa vapaa-ajan palveluihin. Lukuisat erilaiset uudelleenkäyttömenetelmät osoittavat, että käyttäjät vaikuttaisivat kokevan useiden salasanojen muistamisen työlääksi, ja joutuvat siksi kehittelemään omia strategioita ratkaisuna, jotka kuitenkin johtavat salasanaturvallisuuden heikentymiseen.

Woods ja Siponen (2018) tutkivat salasanojen muistamista ihmisen muistin näkökulmasta. Johtopäätöksenä oli, että salasanojen unohtaminen ei johtuisi suinkaan käyttäjän muistamiskyvyistä, vaan korreloi enemmän sen kanssa, kuinka tärkeäksi käyttäjä arvioi salasanan ja kuinka motivoitunut hän on sen muistamiseen. Tärkeimpiä salasanoja, joiden muistamiseen on suurin motivaatio (kuten verkkopankki) unohdetaan vähemmän verrattuna salasanoihin, jotka arvioidaan vähemmän tärkeiksi, ja siten niiden muistamiseen on vähemmän motivaatiota. Luonnollisesti myös ne salasanat, joita käytetään eniten, esimerkiksi päivittäin, ovat helpommin muistettavissa kuin salasanat, joita tarvitsee vain kerran kuukaudessa.

Notoatmodjo ja Thomborson (2009) huomioivat käyttäjän arvioiman salasanan tärkeyden vaikuttavan myös siihen, kuinka turvallinen salasana itsessään on. Käyttäjillä on heidän mukaansa yleisenä taipumuksena luoda turvallisempia ja monimutkaisempia salasanoja tileille ja palveluihin, jotka he näkevät erityisen tärkeinä. Vastaavasti vähemmän tärkeissä palveluissa käyttäjät hyödyntävät yksinkertaisempia salasanoja, tai suoraan samoja salasanoja kuin muualla. Tärkeänä huomiona tutkimuksessa oli, että monet käyttäjien luokittelemista ”tärkeistä” salasanoista eivät välttämättä ole kuitenkaan kovin turvallisia, sillä käyttäjillä on taipumus yliarvioida oma turvallisuutensa ja tehdä virhearvioita huonosta salasanaturvallisuudesta aiheutuvista uhista.

Florencio, Herley ja van Oorschot (2014) ovat esittäneet poikkeavia näkemyksiä salasanoihin liitetyistä ongelmista. Myös he havaitsivat, että vahvojen (satunnaisten ja uniikkien) salasanojen muistaminen on käyttäjille hyvin hankalaa, kun muistettavien salasanojen määrä kasvaa. Kuten Notoatmodjo ja Thomborson (2009), myös Florencio ym. (2014) näkevät salasanojen uudelleenkäytön, sekä lisäksi tavallista yksinkertaisempien salasanojen hyödyntämisen ilmiöinä, jotka johtuvat useiden salasanojen muistamisen hankaluudesta. Tosin Florencion ym. (2014) mukaan ohjeistukset ja strategiat, jotka kehottavat välttämään heikompia salasanoja ja salasanojen uudelleenkäyttöä eivät ole optimaalisia. Johtopäätös on ymmärrettävä, sillä tälläkin hetkellä huolimatta lukuisten toimijoiden, virastojen ja ryhmien tavoitteista valistaa verkon käyttäjiä toimista salasanaturvallisuuden parantamiseksi, eivät uudelleenkäyttö ja heikkojen salasanojen suosiminen vaikuttaisi vuosien aikana vähentyneen.

Florencion ym. (2014) mukaan käyttäjien kannalta parhain menetelmä olisi kompromissi helppouden ja turvallisuuden välillä. Kannustaminen salasanojen ryhmittelyyn palveluiden tärkeyden pohjalta, ja salasanojen vahvuuden ja uudelleenkäytön arviointiin ryhmittelyyn perustuen vähentäisi muistamisen

vaivaa. Kuten aiemmin mainittiin, käyttäjien on jo havaittu hyödyntävän vastaavan kaltaista strategiaa arjessaan salasanojen käytössä (Notoatmodjo & Thomborson, 2009).

Vaihtoehtoista näkemystä ehdottavat myös Wash ym. (2016), joiden mukaan pienen skaalan salasanojen uudelleenkäyttö olisi itseasiassa käyttäjien kannalta positiivinen asia. Wash ym. (2016) väittävät, että jos käyttäjillä on muutama ennestään vahvempi salasana, joita he hyödyntäisivät eri palveluiden välillä, olisi se salasanaturvallisuuden ja käytettävyyden kannalta parempi vaihtoehto. Tosin ehdotuksessa nähdään myös olennaisia aukkoja, sillä olisi hankalaa arvioida, millä sivuilla käytetään salasanoista turvallisempia ja millä taas heikompia. Lisäksi ehdotus ei ratkaise millään tavalla uudelleenkäyttöön liittyvää keskeistä ongelmaa, joka on muiden vuotanutta tai murrettua salasanaa hyödyntävien tilien altistuminen.

## 2.3 Vaihtoehtoisia tunnistautumismenetelmiä

Salasanoille on ajan saatossa ehdotettu useita erilaisia korvaavia tunnistautumismenetelmiä, ja tälläkin hetkellä on käytössä monia muita menetelmiä. Erityisesti mobiilialustoilla, kuten älypuhelimissa, on jo pitkään ollut useita vaihtoehtoja salasanalle käyttäjän tunnistautumista varten. Salasanaan rinnastettavissa olevat PIN-koodit, usein neljän numeron mittaisia, ovat käytössä useissa eri käyttökohteissa, kuten älylaitteiden ja tietokoneiden lukituksen avauksessa, jo pitkään SIM-korttien yhteydessä, sirullisten pankki- ja luottokorttien todentamisessa ja esimerkiksi erilaisissa elektronisissa lukoissa.

Älypuhelinten maailmassa sormenjälkeä, yhtä muotoa biometrisesta tunnistautumisesta, on ollut mahdollista käyttää 2010-luvun alkupuolelta asti. Apple toi sormenjälkitunnistautumisen iPhone-älypuhelimiinsa ensimmäistä kertaa vuonna 2013 (AppleInsider, 2022). Niin älylaitteissa kuin tietokoneissakin sormenjälkitunnistautuminen ei kuitenkaan toimi aina ainoana menetelmänä, vaan usein sille vaaditaan varalle salasana tai numerokoodi. Biometrisiä tunnistautumismenetelmiä on olemassa toki muitakin, esimerkiksi allekirjoituksen tunnistaminen, jossa päätelaite tunnistaa käyttäjän hänen yksilöllisen allekirjoituksen perusteella, tai kirjoitustyylin tunnistaminen, jossa käyttäjät pystytään erottamaan toisistaan heidän kirjoitustyyliensä perusteella (Zimmermann & Gerber, 2020).

Nopeasti yleistyvältä vaikuttava kaksivaiheinen tunnistautuminen on keino parantaa turvallisuutta vaatimalla kirjautumisten yhteydessä erillistä, usein kertakäyttöistä koodia, joka voidaan noutaa erillisestä sovelluksesta tai vaikkapa tekstiviestistä. Token-pohjainen tunnistautumismenetelmä on verrattavissa kaksivaiheiseen tunnistautumiseen, mutta se ei välttämättä vaadi salasanan käyttämistä kirjautumisen yhteydessä. Token-tunnistautumisessa käyttäjältä vaaditaan usein erillinen laite, jonka avulla voidaan suorittaa käyttäjän todentaminen hyödyntäen jokaiselle käyttäjälle yksilöllistä avainta (Zimmermann & Gerber, 2020).

Monessa palvelussa on myös mahdollista käyttää tunnistautumiseen fyysistä USB-muistitikkua, joka koneeseen syöttämällä tunnistaa käyttäjän. Ehkä perinteisempi esimerkki token-pohjaisesta tunnistautumisesta saattaisi olla sirukortti (tai älykortti), jota käyttämällä voidaan kirjautua sisään tietokonejärjestelmään tai muuhun käyttökohteeseen. Korttitunnistautuminen ei välttämättä vaadi ollenkaan muita pääsytietoja, mutta silloin täytyy olla riittävä varmuus siitä, että kortti ei päädy ulkopuolisen tahon käsiin.

Moni kaksivaiheinen tunnistautumismenetelmä on rinnastettavissa token-menetelmään, ja menetelmien ero ei ole ehkä aina täysin selkeä. Esimerkiksi Nordean ID-sovellus, jota vaaditaan verkkopankin asioinnissa, on käytännössä esimerkki kaksivaiheisesta tunnistautumismenetelmästä, mutta nykyisin se tarjoaa mahdollisuuden kirjautumiseen käyttämällä vain QR-koodin skannausta ja sovellukseen asetettua PIN-koodia tai biometristä tunnistautumista, sivuuttaen siten verkkopankin käyttäjätunnuksen ja salasanan.

# 3 SALASANANHALLINTASOVELLUKSET

Ratkaisuksi muutamiin salasanoihin liittyviin ongelmiin kuten muistamiseen, heikkojen salasanojen valintaan ja uudelleenkäyttöön, on usein ehdotettu salasananhallintasovelluksia. Hallintasovellukset mainostavat itseään työkaluna salasanojen muistamiseen ja samanaikaisesti vahvojen salasanojen luomiseen hyödyntämällä salasanageneraattoreita, joita useat niistä tarjoavat. Salasananhallintasovelluksia on tällä hetkellä markkinoilla useita erilaisia ja ne eroavat toiminnallisuuksiltaan, kehitysmenetelmiltään ja kaupallisuudeltaan melko laajasti. Osa yleisimmistä hallintasovelluksista on maksullisia, toiset ilmaisia tarjoten maksusta lisäominaisuuksia. Moni hallintasovellus on myös avointa lähdekoodia ja täysin ilmainen, mutta kaupallisista vaihtoehdoista useat ovat suljettua lähdekoodia. Tässä luvussa käydään ensin läpi salasananhallintasovellusten luokittelua eri kategorioihin ja niihin liittyviä toiminnallisuuseroja. Sen jälkeen tarkastellaan lyhyesti, mitä tavoitteita salasananhallintasovelluksilla käytännössä on, ja lopuksi pohditaan salasananhallintasovellusten vaikutusta käyttäjien salasanaturvallisuuteen.

## 3.1 Salasananhallintasovelluksien luokittelua

Salasanhallintasovelluksien historiasta ei ole olemassa kovin tarkkaa tietoa tai tutkimusta. Vuonna 2003 Luo ja Henry esittelivät konseptin ohjelmasta, jonne voi yhdellä pääsalasanalla salattuun tietokantaan tallentaa useita muita salasanoja. Samana vuonna julkaistiin ensimmäinen versio avoimen koodin KeePass-salasananhallintasovelluksesta, joka Luevanosin, Elizarrarasin, Hirschin ja Yehn (2017) mukaan oli ensimmäinen julkaisu yleiseen käyttöön tarkoitetusta salasananhallintasovelluksesta. Suuri osa nykyisin yleisimmin suositelluista hallintasovelluksista on julkaistu 2010-luvulla (mm. Bitwarden, Dashlane, NordPass), poikkeuksina ovat 1Password ja LastPass (julkaistu 2006 ja 2008).

Li, He, Akhawe ja Song (2014) ovat kuvanneet yksinkertaisen salasananhallintasovelluksen toimintaa. Olennaisimmat toiminnallisuudet

salasananhallintasovelluksessa ovat tietokanta, jonne sovellus tallentaa käyttäjän lisäämät tiedot, ja jonkinlainen pääsalasana, jolla salasanatietokanta salataan. Li ym. (2014) mukaan tietokantaan tallennetaan käyttäjän pääsytietoja, jotka ovat yhdistelmä käyttäjätunnuksesta, salasanasta ja sivustosta jonne niillä kirjaudutaan. Hallintasovellus vaatii myös luonnollisesti käyttöliittymän, jonka kautta käyttäjä voi pääsalasanaa käyttämällä lisätä ja hakea pääsytietoja tietokannasta. Riippuen sovelluksesta, käyttöliittymä voi olla verkkosivu, selainliitännäinen tai erillinen asennettava sovellus.

Karolen, Saxenan ja Christinin (2011) mukaan salasananhallintasovellukset voidaan jakaa pääosin kolmeen eri kategoriaan: työpöytäsovellukset, verkkopohjaiset sovellukset ja mobiilisovellukset. Työpöytäsovellukset asennetaan ja ne tallentavat tietokantansa käyttäjän omalle tietokoneelle. Suurin haittapuoli työpöytäsovelluksissa on tietokannan lokaali sijainti, jolloin salasanojen hakeminen muualla kuin kyseisellä tietokoneella ei ole mahdollista.

Verkkopohjaiset sovellukset tallentavat salasanatietokannan verkko- tai pilvipalvelimelle, joka turvallisuuden näkökulmasta tekee niistä alttiita sovelluksien käyttämiin palvelimiin kohdistuviin hyökkäyksiin. Verkkopohjaisuus tosin mahdollistaa salasanojen noutamisen miltä tahansa laitteelta, joka tukee kyseistä hallintasovellusta.

Mobiilisalasananhallintasovelluksia ovat puhelimille asennettavat sovellukset, jotka tallentavat salasanatietokannan lokaalisti puhelimen muistiin, sekä USB-pohjaiset sovellukset, jotka asennetaan ja ne tallentavat tietokannan USB-muistille. Kumpaakin tyyppiä on yhä saatavilla, esimerkiksi KeePass-sovelluksesta on saatavilla epävirallisia, avoimen lähdekoodin mobiilisovelluksia, jotka ovat täysin lokaaleja, sekä myös USB-muistilta toimivia versioita. Niin kutsutut offline-hallintasovellukset ovat tosin luultavasti menettäneet suosiota verkkopohjaisten, sulavasti laitteiden kanssa synkronoivien vaihtoehtojen yleistyttyä. Kaikki suosituimmat hallintasovellukset, kuten LastPass, Dashlane ja Bitwarden tarjoavat virallisia mobiilisovelluksia niin Androidille kuin iOS:lle.

Nykyisin myös suuri osa suosituimmista verkkoselaimista tarjoaa oman vaihtoehdon salasanojen hallinnalle. Google Chrome tallentaa käyttäjän niin halutessaan salasanat lokaaliin salattuun tietokantaan. Käyttäjä voi myös Google-tiliä hyödyntämällä synkronoida salasanat eri laitteille asennettujen selaimien ja Android-käyttöjärjestelmän välillä (Google, 2022). Mozillan Firefox-selaimessa on saatavilla myös vastaavanlainen ominaisuus, jossa selaimeen tallennettuja salasanoja on mahdollista synkronoida laitteiden välillä Firefox Sync-ominaisuudella (Mozilla, 2022). Myös Firefox tallentaa salasanat ainakin tietokoneympäristössä lokaalisti salattuun tietokantaan. Firefoxissa on myös mahdollista asettaa tietokanta pääsalasanan taakse hieman samaan tapaan kuin erillisissä salasananhallintasovelluksissa.

## 3.2 Salasananhallintasovellusten tavoitteet

Mitä ongelmia salasananhallintasovelluksilla pyritään käytännössä ratkaisemaan? Luo ja Henry (2003) pyrkivät vastaamaan kysymykseen esitellessään versionsa hallintasovelluksesta. Heidän mukaansa suurin ongelma käyttäjien turvallisuudessa verkkopalveluiden käytössä on salasanojen ja käyttäjätunnuksien, eli pääsytietojen, uudelleenkäyttäminen. Syynä kyseiselle toiminnalle ovat käyttäjien vaikeudet muistaa kasvavia määriä pääsytietoja.

Salasananhallintasovellus, josta Luo ja Henry (2003) käyttivät nimitystä common password method, ratkaisee kyseistä ongelmaa seuraavilla tavoilla: käyttäjän tarvitsee muistaa vain yksi käyttäjätunnus ja salasana, eli pääsalasana, jota käytetään hallintasovellukseen kirjautumiseen; jokaisen lisätyn palvelun pääsytiedoissa käytetään eri salasanaa, joka generoidaan sovelluksella; jokainen pääsytieto on salattu hallintasovelluksen tietokannassa, ja salaus voidaan purkaa vain pääsalasanaa käyttämällä.

Salasananhallintasovellus on siis siten kätevä ratkaisu monien pääsytietojen muistamiseen, ja parantaa myös samalla käyttäjien verkkoturvallisuutta. Vähentämällä salananojen muistamiseen ja turvallisten salasanojen luomiseen liitettyä vaivaa, eivät käyttäjät ole välttämättä niin taipuvaisia uudelleenkäyttämään pääsytietoja. Jos yhden palvelun pääsytiedot vuotavat tai ne saadaan muulla tavoin selville, eivät muut palvelut ole heti murron uhan alaisia. (Luo & Henry, 2003).

Luon ja Henryn (2003) versiossa perusoletuksena oli, että hallintasovellusta hyödyntävä käyttäjä generoi jokaisen uuden salasanan sovellusta käyttämällä, ja siten varmistetaan, että käyttäjä hyödyntää palveluissaan vahvoja salasanoja. Salasananhallintasovellukset eivät tosin suinkaan vaadi vahvojen salasanojen käyttöä, sillä käyttäjät pystyvät lisäämään salasanoja sovelluksiin täysin vapaasti ilman rajoituksia. Siksi, vaikka hallintasovellusten tavoitteena olisi muistamisen helpottaminen ja lisäksi vahvojen salasanojen käyttäminen, eivät salasananhallintasovellukset välttämättä kuitenkaan paranna käyttäjien salasanaturvallisuutta.

## 3.3 Salasananhallintasovellusten vaikutus salasanaturvallisuuteen

Lyastani, Schilling, Fahl, Backes ja Bugiel (2018) havaitsivat salasananhallintasovelluksia käsittelevässä tutkimuksessaan, että salasanojen uudelleenkäyttämiseen vaikutti huomattavasti se, mitä tapaa käyttäjät hyödynsivät pääsytietojen täyttämiseen. LastPass-salasananhallintasovellusta käyttäneiden keskuudessa salasanojen uudelleenkäyttämisen todennäköisyys oli 2.85 kertaa matalampi verrattuna ilman teknologisia apuvälineitä toimiviin käyttäjiin. Kokonaisuudessaan

47 % LastPass-sovelluksen tai selainliitännäisen kautta syöteistä salasanoista oli uudelleenkäytettyjä, ja keskiarvoltaan LastPass-salasanat olivat vahvimpia.

Yhtenä tutkimuksen syöttötavoista oli Chrome-selaimen automaattinen täyttö, joka on käytännössä sama menetelmä kuin aiemmin luokittelussa mainittu Google Chromen salasananhallintaominaisuus. Chromen automaattitäytön kautta syötetyt salasanat olivat 1.65 kertaa todennäköisemmin uudelleenkäytettyjä, ja kaikkiaan huomattavan suuri osa (80 %) salasanoista oli uudelleenkäytettyjä. Lyastanin ym. (2018) mukaan syynä saattoi olla se, että Chrome ei ehdottanut vahvoja salasanoja käyttäjille tilien luontien yhteydessä, vaan salasanangenerointi oli oletuksena pois käytöstä. Siten salasanan luominen ja sen vahvuus oli täysin käyttäjän vastuulla.

Käyttäjillä on toiminnassaan yleensä taipumuksena olla koskematta sovelluksien ja palvelujen oletusasetuksiin (Shah & Kesan, 2008). Siksi on tärkeää, että salasananhallintasovellukset oletuksena pyrkivät kannustamaan käyttäjää luomaan turvallisia salasanoja, ja välttämään uudelleenkäyttöä. Tätä tukee toisessa tutkimuksessa tehdyt havainnot siitä, että selaimiin sisäänrakennettujen salasananhallintasovellusten käyttäjät ovat usein tietämättömiä mahdollisuudesta generoida salasanoja, kun taas erillisten salasananhallintasovellusten käyttäjät mielsivät ominaisuuden hyödylliseksi ja käteväksi. (Pearman ym., 2019).

Vastuu salasanaturvallisuudesta näyttäisi lankeavan loppukädessä hallintasovelluksien käyttäjille. Alodhyanin, Theodorakopouloksen ja Reinecken (2020) tutkimuksen mukaan salasananhallintasovelluksia käyttävistä vain 51 % hyödynsi salasanageneraattoreita salasanojen luomisessa. Tukien Pearmanin ym. (2019) havaintoja, 42 % heistä, jotka eivät käyttäneet generaattoreita, ilmoitti olleensa tietämättömiä kyseisestä ominaisuudesta salasananhallintasovelluksissa.

# 4 SALASANANHALLINTASOVELLUSTEN KÄYTTÖÖNOTTO

Tässä luvussa tarkastellaan muutamassa keskeisessä tutkimuksessa havaittuja syitä sille, miksi ihmiset joko haluavat, tai eivät halua käyttää, tai ottaa käyttöönsä salasananhallintasovelluksia. Käyttöönottoon negatiivisesti vaikuttavien tekijöiden tarkastelussa turvaudutaan vahvasti Aurigemman, Matsonin ja Leonardin (2017) suorittamaan tutkimukseen, sillä se vaikuttaisi olevan salasananhallintasovellusten käyttöönottoa käsittelevistä tutkimuksista kyselytutkimuksen otokseltaan yksi laajimmista. Negatiivisten tekijöiden ohessa tarkastellaan lisäksi tarkemmin salasananhallintasovelluksiin kohdistuvia luottamusongelmia ja monien niiden ongelmana mainitsemaa yhden pisteen haavoittuvuutta.

## 4.1 Salasananhallintasovellusten käytön syyt ja käyttöönottoa edistävät tekijät

Salasananhallintasovellusten käytölle on Faganin ym. (2017) tutkimuksen mukaan kaksi syytä ylitse muiden: kätevyys ja turvallisuus. Suuri osa tutkimukseen vastanneista salasananhallintasovelluksia käyttäjistä, 80 %, vaikutti ymmärtäneen väärin hallintasovellusten ydinidean. Salasananhallintasovellukset nähtiin vain yksinkertaisena työkaluna helpottamaan salasanojen muistamista, eräänlaisena korvaavuutena salasanojen kirjoittamiselle muistikirjaan tai tekstitiedostoon. Vain 25 % kertoi käyttämisen syyksi turvallisuuden ja sen, kuinka salasananhallintasovelluksilla voidaan edistää salasanaturvallisuutta käyttämällä vahvempia salasanoja. Turvallisuuteen liittyen vain pieni osa mainitsi mahdollisuuden generoida vahvoja salasanoja hallintasovelluksessa, viitaten mahdolliseen tietämättömyyteen kyseisestä olennaisesta ominaisuudesta käyttäjien keskuudessa.

Ayyagari ym. (2019) tutkivat salasananhallintasovellusten käyttöönottopäätöksen tekemiseen vaikuttavia tekijöitä suojelumotivaatioteoriaan (protection motivation theory) pohjautuen. Heidän mukaansa kaksi suurinta havaittua

motivaatiota hallintasovellusten käyttöönottoon ovat käyttäjien kokema haavoittuvuus (perceived vulnerability) ja uhkan koettu vakavuus (perceived severity). Tutkimuksen havainnot tarkoittavat käytännössä sitä, että mitä haavoittuvammaksi käytetyt salasanat ja oma salasanaturvallisuus koetaan, ja mitä vakavammiksi uhat, kuten tietovuodot ja tietomurrot nähdään, sitä suurempi motivaatio käyttäjillä on ottaa salasananhallintasovellus käyttöön. Ihmisten inhimilliset erheet kuitenkin hankaloittavat kyseistä arvioita, sillä usein mahdollisten uhkien ja haavoittuvuuksien todennäköisyys aliarvioidaan reilusti, ja vastaavasti oma turvallisuus verkon palveluissa saatetaan yliarvioida (Ayyagari ym., 2019). Ihmiset siis näkevät käyttämänsä salasanansa turvallisempina ja palveluihin kohdistuvat uhat epätodennäköisempinä kuin mitä ne oikeasti ovat.

Macleanin ja Ophoffin (2018) mukaan salasananhallintasovellusten käyttöönottoon vaikuttaa pääasiassa vain kolme olennaista tekijää: suoritusodotukset, tavat ja tottumukset, sekä luottamus. Suoritusodotuksilla tarkoitetaan sitä, kuinka paljon hyötyä käyttäjä kokee saavansa salasananhallintasovelluksesta arjessa tai työelämässä. Suoritusodotukset ovat verrattavissa Faganin ym. (2017) havaitsemaan hallintasovellusten kätevyyteen niiden käytön syynä. Kuten sillä, myös suoritusodotuksilla oli vahva vaikutus käyttöönottoon. Tapojen ja tottumuksien havaittiin vaikuttavan siten, että mitä enemmän hallintasovelluksia käyttää ja integroi osaksi salasanatottumuksia (kuten generoimalla uudet salasanat aina sovelluksessa), sitä hyödyllisemmäksi hallintasovellus koetaan. Kuten edellä alaluvussa 4.3 todetaan, luottamuspuute voi merkittävästi vaikuttaa hallintasovellusten välttämiseen, mutta luottamuksella on Macleanin ja Ophoffin (2018) mukaan myös suuri merkitys käyttöönottoon. Luottamusta ja läpinäkyvyyttä edistävät tekijät, kuten mahdollisuus hallintasovellusten auditoinnille, vaikuttavat positiivisesti käyttöönottoon. Lisäksi sovelluksia tarjoavien yritysten maineella on vaikutusta mahdollisten käyttäjien näkemyksiin sovelluksista.

Alkaldin ym. (2019) havaintojen mukaan kolme suurinta syytä salasananhallintasovellusten asentamiseen ja käyttöön ovat salasanojen muistaminen, tiedon tallentaminen turvallisesti ja salasanojen synkronointi laitteiden välillä. Tutkimuksessa ylivoimaisesti suurin mainittu syy oli salasanojen muistaminen (90 % vastaajista). Havainnot tukevat siten Faganin ym. (2017) tekemiä johtopäätöksiä siitä, miten suuri osa hallintasovellusten käyttäjistä on todennäköisesti ymmärtänyt niiden käyttötarkoituksen väärin, ja käyttää sovelluksia kätevyyssyistä sen sijaan, että hyödyntäisivät niitä oman salasanaturvallisuutensa parantamiseen.

Alkaldin ym. (2019) tutkimuksessa tarkasteltiin myös itseohjautuvuusteorian (self-determination theory) näkökulmasta sen vaikutusta salasananhallintasovellusten käyttöönottoon. Itseohjautuvuusteorian mukaan ihmisillä on kolme perustarvetta: omaehtoisuus, kyky ja yhteisöllisyys (Ryan & Deci, 2000). Alkaldin ym. (2019) mukaan itseohjautuvuusteorian perustarpeista omaehtoisuudella ja yhteisöllisyydellä on eniten vaikutusta motivoidessa käyttäjiä ottamaan hallintasovelluksia käyttöönsä. Käyttäjien kyvyillä, eli arvioilla omista valmiuksista ja osaamisesta salasananhallintasovellusten käyttöön ei havaittu olevan suurta merkitystä.

Omaehtoisuutta voidaan hyödyntää käyttöönottokehotuksissa välttämällä suoria vaatimuksia ja pakkokeinoja (esimerkiksi yritysympäristöissä), ja sen sijaan pyrkimällä antamaan käyttäjille itselleen päätösvalta ja eri vaihtoehtoja päätöksentekoon. Yhteisöllisyyttä taas voidaan edistää hyödyntämällä referral- ja word of mouth-markkinointia salasananhallintasovelluksissa, sillä käyttöönottoon vaikuttaa positiivisesti, jos asennuskehotus tulee jo sovellusta käyttävältä ihmiseltä. (Alkaldi ym., 2019). Toisaalta täytyy huomioida, että Macleanin ja Ophoffin (2018) tutkimuksen mukaan muiden ihmisten ehdotuksilla ja ympäröivän sosiaalisen piirin mielipiteillä ei ole salasananhallintasovellusten kontekstissa paljoa vaikutusta käyttöönottoon.

## 4.2 Salasananhallintasovellusten käyttöä estävät tekijät

Aurigemma ym. (2017) selvittivät tutkimuksessaan kyselyn avulla 372:n kandidaatintutkinto-opiskelijan salasananhallintasovelluksen. Opiskelijoille esitettiin aluksi huonon salasananhallinnan vaaroja, joiden välttämiseen ehdotettiin ratkaisuna muutamaa erilaista hallintasovellusta. Tutkimuksen ensimmäisessä vaiheessa selvitettiin vastaajien käyttäytymisaikomuksia ja toisessa vaiheessa käytännön toimintaa salasanaturvallisuuteen liittyen, mukaan lukien kysymyksiä vastaajan valitsemasta hallintasovelluksesta. Kaksivaiheisuuden avulla pyrittiin selvittämään, toteutuivatko ensimmäisessä vaiheessa todetut vastaajien aikomukset salasananhallintasovelluksen käyttämiseen käytännössä. Kvalitatiivisessa analyysissä kyselyiden vastauksille suoritettiin koodaus kahden tutkimuksen tekijöiden toimesta.

Aurigemman ym. (2017) tutkimuksen tuloksissa data-analyysin ja koodauksen jälkeen havaittiin kahdeksan salasananhallintasovelluksen käyttöönottoon vaikuttavaa tekijää, jotka tutkimuksessa nimettiin käyttäytymisinhibiittoreiksi. Neljä näistä lajiteltiin yksilöllisiksi inhibiittoreiksi, ja niitä havaittiin 72 %:lla tutkimukseen osallistuneista. Aurigemma ym. (2017) määrittelevät yksilöllisiksi inhibiittoreiksi ne tekijät, jotka aiheuttavat konfliktia tai kuluttavat aineellisia resursseja tai kognitiivista kapasiteettia. Yksilöllisiä inhibiittoreita olivat ajanpuute, välittömyyden puute, liiallinen vaiva ja matala itseluottamus.

Suurin osa, 41 % vastaajista, raportoi ajanpuutteen pääsyyksi, mikä käytännössä tarkoitti sitä, että vaikka vastaaja olisi kokenut käyttöönoton tärkeäksi toimeksi, muut asiat olivat silti tärkeysjärjestyksessä korkeammalla. 15 % mainitsi syyksi välittömyyden puutteen, eli hallintasovelluksen käyttöönottoa ei nähty niin tärkeäksi, että vastaaja olisi ryhtynyt heti toimeen, ja siten unohti asian. 12 % vastaajista näki salasananhallintasovelluksen asentamisen toimenpiteenä, joka olisi vaatinut liikaa vaivaa, ja täten eivät olleet halukkaita ryhtyä toimeen. Yksilöllisistä inhibiittoreista viimeistä, matalaa itseluottamusta, raportoi 5 % vastaajista. Kyseisten vastaajien näkökulmasta heidän tietotekniset taitonsa eivät olleet tarpeeksi edistyneitä, jotta he olisivat osanneet ottaa salasananhallintasovelluksen käyttöön. Ongelmakohdaksi vastaajat kokivat joko sovelluksen asentamisen tai sen käyttämisen.

Erilliseksi osa-alueeksi käyttäytymisinhibiittoreissa erotettiin uhka-apatia, jonka mainitsi 25 % osallistujista. Tutkimuksen kontekstissa Aurigemman ym. (2017) mukaan uhka-apatialla tarkoitetaan osallistujien näennäistä piittaamattomuutta huonon salasananhallinnan aiheuttamista uhkista. Se tarkoittaa käytännössä sitä, että vaikka tutkimukseen osallistuneille viestitettiin uhkien vakavuudesta, eivät he silti kokeneet salasananhallintasovelluksen asentamista niin tärkeäksi toimeksi, että olisivat sitä tehneet. Osassa uhka-apatiaan luokitelluista vastauksista vastaajat kokivat myös, että he pystyvät jo nykyisellään hallitsemaan ja muistamaan salasanansa riittävän hyvin, ja siten eivät tarvinneet hallintasovellusta. Hyvin pieni osa (2 %) oli sitä mieltä, että heidän salasanansa ovat niin hyviä, että niihin ei kohdistu minkäänlaista uhkaa.

Yksilöllisten inhibiittorien ja uhka-apatian lisäksi kolmantena osa-alueena Aurigemman ym. (2017) tutkimuksessa olivat teknologiainhibiittorit, joita tunnistettiin 20 %:lla vastaajista. Teknologiainhibiittoreiksi laskettiin käytössä olevat vaihtoehtoiset ratkaisut, luottamuksen puute ja puutteellinen tietoisuus. 10 % ilmaisi olleensa kiinnostunut salasananhallintasovelluksen asentamisesta ja käytöstä, mutta vaativat lisää tietoa kyseisistä toimista ja yleisesti sovelluksen toiminnasta. 7 % mainitsi, että heillä oli käytössä jo jonkinlainen vaihtoehtoinen ratkaisu salasanojen hallintaan, joten eivät siten tarvinneet erillistä sovellusta. Esimerkkinä eräs vastaaja antoi fyysisen muistikirjan, jossa oli kirjattuna ylös kaikki käytössä olevat pääsytiedot. Viimeisenä tutkimuksessa havaittuna inhibiittorina oli luottamuksen puute. 5 % vastaajista oli epäileväisiä hallintasovelluksia kohtaan. Salasanojen tallentaminen sovellukseen tai verkkoon kuulosti heille mahdollisesti jopa vaaralliselta, ja he eivät olleet halukkaita ottamaan sovellusta käyttöön.

Ray, Wolf, Kuber ja Aviv (2021) tutkivat salasananhallintasovellusten käyttöä vanhemman ikäluokan ihmisten (yli 60-vuotiaiden) keskuudessa. Tutkimuksessa esiintyi paljon samankaltaisia havaintoja kuin Aurigemman ym. (2017), ja yksittäisten syiden kategorioihin ryhmittelyn jälkeen havaittiin neljä laajaa pääsyytä, jotka estävät salasananhallintasovellusten käyttöönottoa. Kuten Aurigemman ym. (2017) toteama ajanpuute, myös Ray ym. (2021) havaitsivat ajankäyttöön liittyvät ongelmat merkittävänä syynä olla asentamatta hallintasovelluksia. Useat vastaajista mainitsivat, että asentaminen veisi liian paljon aikaa ja vaivaa, ja eivät siten olleet halukkaita käyttöönottoon. Myös minäpystyvyyden puute mainittiin vastauksissa, vertautuen Aurigemman ym. (2017) havaitsemaan matalaan itseluottamukseen. Tosin vanhempien ihmisten keskuudessa minäpystyvyydellä oli huomattavasti suurempi merkitys, sillä vastaajat olivat laajemmin epäileväisiä omista taidoistaan käyttää ja asentaa salasananhallintasovelluksia.

## 4.3 Luottamusongelmat ja turvallisuushuolet salasananhallintasovelluksia kohtaan

Yksi erillisenä huomioitava, käyttöönottoon merkittävästi vaikuttava tekijä on mahdolliset käyttäjien luottamusongelmat liittyen salasananhallintasovelluksien toimintaan ja turvallisuuteen. Fagan, Albayram, Khan ja Buck (2017) tutkivat käyttöönoton harkintaa, ja havaitsivat tutkimustuloksissaan, että suuri osa eikäyttäjistä (46 %) mainitsi turvallisuushuolet syyksi olla käyttämättä hallintasovelluksia. Muut syyt olivat suurelta osin vastaavia kuin Aurigemman ym. (2017), kuten tyytyväisyys muihin hallintakeinoihin, hallintasovelluksen näkeminen tarpeettomana, ajan tai motivaation puute, ja sovellusten näkeminen vaikeina tai hankalina. Vastaajien mainitsemat luottamusongelmat liittyivät Faganin ym. (2017) mukaan lähinnä tietämättömyyteen salasananhallintasovellusten toiminnasta.

Suurinta huolta esitettiin siitä, kuinka hallintasovelluksissa kaikki salasanat ovat yhdessä paikassa ja siten muodostuu suuri uhka niiden täydelliselle menettämiselle. Moni vastaaja oli myös tarkemmin määrittelemättä sitä mieltä, että hallintasovellukset eivät ole yleisesti turvallisia. Faganin ym. (2017) tuloksista täytyy lisäksi nostaa esille, että myös osa hallintasovelluksia käyttävistä vastaajista mainitsi turvallisuushuolista. Kyseiset käyttäjät eivät esimerkiksi tallentaneet kaikkia salasanojaan hallintasovellukseen, syynä pelko niiden menettämiselle tai haavoittuvuudelle. Tärkeimpiä salasanoja säilytettiin joko omassa muistissa tai esimerkiksi fyysisesti ylös kirjoitettuna.

Käyttäjien turvallisuushuolia ovat huomioineet myös Alodhyani ym. (2020). Heidän tutkimuksessaan suurin havaittu syy olla käyttämättä hallintasovelluksia oli luottamuksen puutteeksi kategorisoidut vastaukset. Myös heidän havainnoissaan luottamuspula oli lähtökohtaisesti peräisin tiedon ja ymmärryksen puutteesta, tukien Faganin ym. (2017) havaintoja. Käyttäjät eivät olleet tietoisia salasananhallintasovellusten perustoiminnasta. Perimmäisiä huolia olivat muun muassa kuinka salasanat ovat tallennettu sovellukseen, missä sijainnissa salasanoja säilytetään, ja mitä tapahtuu, jos menettää pääsyn sovellukseen tai unohtaa pääsalasanan.

Myös Ray ym. (2021) ja Pearman ym. (2019) ovat todenneet tutkimuksissaan luottamusongelmat yhtenä syynä, miksi ihmiset eivät käytä tai ole halukkaita ottamaan käyttöön salasananhallintasovelluksia. Rayn ym. (2021) tutkimuksessa vanhemmat aikuiset olivat epäileväisiä hallintasovellusten toiminnasta ja osoittivat huolta siitä, kenellä on tosiasiassa pääsy verkkoon tallennettuihin salasanoihin. Moni mainitsi huolia salasanojen tallentamisesta yhteen paikkaan, ja siitä mahdollisesti aiheutuvista vaaroista. Mielenkiintoisesti moni vastaaja ei täysin luottanut siihen, että salasananhallintasovellukset muistavat kaikki sinne tallennetut salasanat, ja osoittivat huolta siitä, että jotkut salasanat saattavat kadota sovelluksesta. Pearmanin ym. (2019) tutkimuksessa turvallisuuteen ja luottamukseen liittyvät huolet olivat vastaavanlaisia. Syinä käytön välttämiseen mainittiin muun muassa epäluottamus sovelluksia tarjoaviin yrityksiin ja

siihen, pitävätkö ne salasanat todellisesti turvassa ja poissa muiden (mukaan lukien yrityksen) käsistä. Lisäksi monella oli huoli salasananhallintasovelluksiin ja niitä tarjoaviin yrityksiin kohdistuviin hyökkäyksiin, ja siten salasanojen vuotamiseen tai menettämiseen.

Alodhyanin ym. (2020) mukaan turvallisuushuolia olisi mahdollista vähentää edistämällä läpinäkyvyyttä salasananhallintasovellusten toiminnassa. Suuri osa markkinoilla käytössä olevista ja eniten mainostetuista hallintasovelluksista ovat suljetun lähdekoodin sovelluksia (lukuun ottamatta joitakin avoimen lähdekoodin vaihtoehtoja). Siten niiden hyödyntämät toimintaperiaatteet, salausmenetelmät ja algoritmit ovat vain kehittävän yrityksen tiedossa, toisin kuin avoimen lähdekoodin sovelluksissa. Samasta syystä kyseisten sovellusten turvallisuusauditointi on huomattavasti hankalampaa kuin avoimeen lähdekoodiin perustuvien, joiden toimintaan kuka tahansa ulkopuolinen voi halutessaan tutustua.

Luottamuksen vaikutuksesta käyttöönottoon on tosin myös eriäviäkin havaintoja. Ayyagarin ym. (2019) tutkimuksen mukaan luottamuksen vaikutus käyttöönottoaikomukseen on vähintäänkin epäselvä. Ottaen huomioon muut tutkimuksessa hyödynnetyt muuttujat, luottamuksella oli loppukädessä vain pieni merkitys, ja esimerkiksi käyttäjien näkemillä haavoittuvuuksilla ja koetuilla uhkilla huonosta salasanaturvallisuudesta johtuen oli merkittävästi suurempi vaikutus käyttöönottoon. Luottamus saattaa vaikuttaa käyttäjien tekemiin valintoihin enemmän esimerkiksi silloin, kun he vertailevat erilaisia salasananhallintasovelluksia ja tekevät päätöksiä niiden välillä. Lisäksi aikaisemmin tarkastellussa Aurigemman ym. (2017) tutkimuksessa vain 5 % kaikista vastaajista mainitsi luottamusongelmat yhtenä syynä, miksi he eivät käyttäneet salasananhallintasovellusta.

## 4.4 Salasananhallintasovellusten yhden pisteen haavoittuvuus

Käsiteltyihin luottamusongelmiin liittyvissä tutkimuksissa vastaajat nostivat usein esille salasananhallintasovellusten yhden pisteen haavoittuvuuden (Alodhyani ym., 2020; Aurigemma ym., 2017; Pearman ym., 2019). Oletettu käyttötapa salasananhallintasovelluksille on sellainen, jossa käyttäjä tallentaa ja luo kaikki salasanansa hallintasovelluksen kautta. Siten, jos käyttäjä unohtaa tai menettää pääsytietonsa salasananhallintasovellukseen, ovat kaikki tietokantaan tallennetut palveluiden pääsytiedot saavuttamattomissa. Vastaavasti, jos käyttäjän pääsytiedot hallintasovellukseen vuotavat esimerkiksi sovellukseen kohdistuneen tietomurron myötä, kaikki tallennetut tiedot voivat mahdollisesti päätyä jonkun ulkopuolisen haltuun.

Esitetty huoli on täysin ymmärrettävä, sillä säilyttämällä salasanoja omassa muistissa, fyysisessä muistikirjassa, sähköisessä tekstitiedostossa tai muussa yhdessä monista tallennustavoista, joita käyttäjät hyödyntävät, on silloin vastuu turvallisuudesta ja tallessapidosta täysin itse käyttäjällä. Käyttämällä salasananhallintasovellusta, varsinkin sellaista, joka synkronoi tietokannan verkon kautta,

on vastuu turvassa pidosta usein sovellusta tarjoavalla yrityksellä. Suuret tietomurrot ja -vuodot saavat usein mediassa paljon huomiota, ja siten saattaa tuntua erityisen huolestuttavalta antaa kaikki pääsytiedot ulkopuolisen säilytettäväksi. Moni käyttäjä ei myös ehkä täysin ymmärrä salasananhallintasovellusten toimintaa, josta aiheutuen he ovat epäluuloisia esimerkiksi niiden turvallisuudelle.

Tutkimuksissa todettu tosiasia on, että verkon käyttäjien salasanaturvallisuus on yleisesti ottaen huonoa: käyttäjät luovat heikkoja, yksinkertaisia ja nopeasti arvattavissa olevia salasanoja, ja turvallisuutta edelleen heikentäen käyttävät samoja heikkoja salasanoja uudelleen monissa muissa palveluissa (Das ym., 2014; Florencio & Herley, 2007). Käyttäjistä lähtöisin oleva ongelma on tietotekniikan ajankäsityksellä ikivanha. Jo ensimmäisten salasanojen ilmaantuessa tietokoneisiin huomattiin, että yksi suurimmista turvallisuusongelmista oli heikkotasoiset salasanat. Vuonna 1979 havaintona oli, että 86 % osituskäyttöjärjestelmän käyttäjien salasanoista oli luokiteltavissa liian yksinkertaisiksi, ja kolmasosa salasanoista oli löydettävissä suoraan sanakirjasta ja siten alttiita sanakirjahyökkäyksille (Morris & Thompson, 1979).

Salasanaturvallisuus on kompromissien tekemistä. On todettu, että yksinkertaisesti salasanan pidentäminen nostaa salasanan turvallisuutta (Kelley ym., 2012), ja useissa salasanojen luontiin ja käyttöön liittyvissä ohjeistuksissa pyritäänkin neuvomaan pitkien salasanojen hyödyntämiseen sen sijaan, että käyttäisi esimerkiksi täysin satunnaisia kirjaimia, numeroita tai erityismerkkejä. Voisi ajatella, että pitkät salasanat ovat automaattisesti vaikeampia muistaa käytössä, mutta havaintojen mukaan muistettavien salasanojen lukumäärällä näyttäisi olevan enemmän vaikutusta muistivaikeuksiin (Pilar ym., 2012). Monet käyttäjät turvautuvat siten melko luonnollisesti salasanojen ylös kirjoittamiseen, kuten muistikirjaan, ratkaisukeinona useiden salasanojen muistamiseen (Stobert & Biddle, 2014).

Salasananhallintasovellukset eivät ole suinkaan täydellinen ratkaisu erittäin yleiseen ongelmaan, joka monille aiheutuu useiden salasanojen muistamisesta. Kuitenkin, vaikka moni mainitsee päällimmäisenä syynä sovellusten välttämiseen luottamusongelmat ja mahdolliset turvallisuushuolet, ovat salasananhallintasovellukset parempi keino salasanojen kanssa elämiseen kuin suurin osa muista vaihtoehdoista. Ison-Britannian kyberturvallisuuskeskuksen mukaan salasananhallintasovellukset vähentävät niin kutsuttua turvallisuuskitkaa tekemällä turvallisuudesta helpompaa ja kätevämpää (NCSC, 2017). Salasananhallintasovelluksia hyödyntämällä pystytään välttämään käyttäjien itse aiheuttamia turvallisuusriskejä, jotka usein aiheutuvat heikoista salasanoista, sillä ne mahdollistavat vahvojen, uniikkien salasanojen luomisen ja niiden muistamisen. Myös Yhdysvaltain kyberturvallisuusvirasto CISA kehottaa hyödyntämään salasananhallintasovelluksia salasanojen muistamisessa, mutta erityisesti turvallisten salasanojen luomisessa niiden avulla (CISA, 2019).

Microsoft Regional Director ja tunnetun Have I Been Pwned-sivuston luoja Troy Hunt kehottaa myös salasananhallintasovellusten käyttöön huolimatta mahdollisista niihin liittyvistä turvallisuushuolista (Hunt, 2017). Hänen mukaansa käyttäjien muistiongelmat ja turvallisuusvaatimukset johtavat

kompromisseihin, kuten salasanojen uudelleenkäyttöön ja heikkoihin salasanoihin. Salasananhallintasovellukset ovat yksi sellainen kompromissi, joka hyötyjä ja haittoja vertaamalla vaikuttaisi kuitenkin positiiviselta. Vahvojen salasanojen käyttäminen kaikissa palveluissa ja prosentuaalisesti minimaalinen riski hallintasovellukseen kohdistuvaan (onnistuneeseen) hyökkäykseen verrattuna useiden heikkojen salasanojen käyttäminen monissa palveluissa ja riski mihin tahansa kyseisistä palveluista kohdistuvaan iskuun tai tietovuotoon – loogisesti arvioiden salasananhallintasovellusten käyttö näyttäisi huomattavasti paremmalta vaihtoehdolta.

# 5 YHTEENVETO JA POHDINTA

Salasanaturvallisuus on tietoturvallisuuden alue, josta käyttäjiä pyritään usein valistamaan. Toistuvasti pyritään kehottamaan käyttämään verkossa vain vahvoja ja turvallisia salasanoja, mutta kyseinen toiminta on kuitenkin usein hankalaa, sillä keskivertoisella nykyajan käyttäjällä on kymmeniä palveluita ja siten kymmeniä muistettavia salasanoja (Florencio & Herley, 2007). Samanaikaisesti useiden salasanojen muistamisen kerrotaan olevan hankalaa, ja sen on tutkimuksissa havaittu olevan yhtenä pääsyistä sille, miksi ihmiset käyttävät samoja salasanoja uudelleen useissa palveluissa (Florencio ym., 2014; Notoatmodjo & Thomborson, 2009). Silti salasananhallintasovellusten hyödyntäminen käyttäjien ongelmien helpottamiseksi vaikuttaisi olevan harvinaista, ja niiden käyttäjämäärä melko vähäistä.

Tämän tutkielman tavoitteena oli tarkastella salasanoja yleisesti tunnistautumismenetelmänä, tutkia salasanoihin liitettyjä ongelmia, sekä tutkia syitä miksi ihmiset käyttävät tai päättävät olla käyttämättä salasananhallintasovelluksia. Tutkimuskysymys, johon pyrittiin hakemaan vastausta, oli ”Mitkä ovat tutkimuksissa havaitut yleisimmät syyt sille, että käyttäjät ottavat (tai eivät ota) salasananhallintasovellusta käyttöönsä?”. Motivaationa tutkielmalle toimi halu saavuttaa parempi, laaja-alainen käsitys siitä, mikä vaikuttaisi estävän ihmisiä käyttämästä salasananhallintasovelluksia.

Luvussa neljä käsiteltyjen käytön ja käyttöönottoa estävien syiden perusteella voidaan salasananhallintasovelluksien käytöstä tehdä muutamia olennaisia johtopäätöksiä. Käyttöönottoa estävät syyt vaikuttaisivat johtuvan ennemmin käyttäjistä itsestään kuin hallintasovelluksista. Tarkastelluissa tutkimuksissa useasti toistuneet syyt kuten ajanpuute, käyttäjien omien muistimenetelmien toimivuus, koettujen uhkien arvioitu harvinaisuus tai niiden vakavuuden koettu mataluus, tietoisuuden puute ja erityisesti hallintasovelluksiin kohdistuneet luottamusongelmat olivat päällimmäisiä syitä, joiden takia salasananhallintasovelluksia ei käytetä (Alodhyani ym., 2020; Aurigemma ym., 2017; Fagan ym., 2017; Pearman ym., 2019; Ray ym., 2021).

Pyrittäessä motivoimaan käyttäjiä hyödyntämään salasananhallintasovelluksia salasanojen organisoinnissa, luonnissa ja yleisen salasanaturvallisuuden

parantamisessa, olisi todennäköisesti parhainta kiinnittää huomiota mainittuihin käyttöä estäviin syihin. Niin salasananhallintasovelluksia tarjoavissa yrityksissä kuin tulevaisuuden salasananhallintasovelluksia käsittelevissä tutkimuksissa olisi kenties hyvä tarkastella, millä strategioilla on mahdollista onnistuneesti viestiä ihmisille, jotka eivät käytä hallintasovelluksia, miksi heidän olisi oman salasanaturvallisuutensa parantamiseksi hyvä käyttää hallintasovelluksia.

Salasananhallintasovelluksia tarjoavien ja kehittävien yritysten ja organisaatioiden kannattaisi myös kohdistaa huomionsa ihmisten sovelluksiin liittämiin luottamusongelmiin, olivat ne sitten realistisia tai eivät. Osa luottamusongelmista vaikuttaisi johtuvan siitä, että ihmiset eivät täysin ymmärrä salasananhallintasovellusten toimintaa, ja ovat siten epätietoisia esimerkiksi siitä, missä salasanoja säilytetään ja keillä niihin on pääsy (Alodhyani ym., 2020; Fagan ym., 2017; Pearman ym., 2019). Mahdollisiin käyttäjiin kohdistuvassa viestinnässä, mainonnassa ja yleisesti sovelluksista annettavassa tiedossa olisi siis syytä mahdollisimman yksinkertaisesti ja selkeästi viestiä, kuinka hallintasovellukset käytännössä toimivat.

Kysyttäessä pääsyytä salasananhallintasovelluksen käyttämiseen, valtaosa käyttäjistä kertoo sen olevan yksinkertaisesti ratkaisu liian monien pääsytietojen muistamiseen, ja vain pieni osa käyttää hallintasovellusta oman salasanaturvallisuuden parantamiseen (Alodhyani ym., 2020; Fagan ym., 2017). Salasananhallintasovellusten tavoitteiden ollessa muistamisen helpottaminen sekä turvallisuuden parantaminen, vaikuttaisi siltä, että käyttäjät nähtävästi arvostavat hallintasovellusten tuomaa kätevyyttä merkittävästi enemmän kuin niiden tarjoamia turvallisuushyötyjä. Moni ei lisäksi ole edes tietoinen turvallisuutta edistävistä ominaisuuksista, kuten salasanageneraattoreista (Alodhyani ym., 2020).

Näyttäisi myös siltä, että hallintasovellusten markkinoinnissakin on viime vuosina ryhdytty korostamaan enemmän kätevyys- ja helppousaspekteja, ja turvallisuus on siirtynyt rinnakkaistavoitteesta toissijaiseksi eduksi. Esimerkiksi LastPass ja Bitwarden painottavat kotisivuillaan hyvin vahvasti salasananhallintasovellusten tuomia helpotuksia salasanojen käyttöön ja toimintaan (Bitwarden, 2022; LastPass, 2022)

Helppouden korostaminen turvallisuuden sijaan (tai sen kustannuksella) on verrattavissa pankkikorttien käytössä tapahtuneeseen mullistukseen 2000-luvun aikana lähimaksamisen ilmaannuttua kortteihin. Moni lähimaksamista kokeillut todennäköisesti suhtautui aluksi sen turvallisuuteen epäluulolla, mutta kuitenkin arvosti sen tuomaa helppoutta enemmän. Salasananhallintasovellusten käyttäjistäkin merkittävä osa raportoi epäluottamuksestaan niitä kohtaan, mutta käyttämisen syiksi kertoo päällimmäisenä helppouden ja kätevyyden.

Tutkimushavaintojen pohjalta olisi siis toisaalta syytä pohtia, onko aiemmin ehdotettu salasanaturvallisuuden tärkeydestä valistaminen siten edes kannattavaa. Jos merkittävä osa mahdollisista käyttäjistä ei vaikuttaisi arvostavan hallintasovellusten tuomia turvallisuusetuja, ei ole mitenkään yllättävää, että sovelluksia tarjoavat yritykset pyrkivät vastaamaan käyttäjien päällimmäisiin tarpeisiin. Yritysten näkökulmasta on luonnollisesti turha panostaa markkinoinnissa sellaisiin ominaisuuksiin, joista suuri osa käyttäjistä ei ole kiinnostunut.

Tosin on myös mahdollista, että salasananhallintasovelluksien markkinoinnissa on jo ennestään keskitytty turvallisuuden edistämisen kannalta vääriin asioihin. Jos tutkimushavaintojen perusteella iso osa käyttäjistä ei ole tietoisia turvallisuutta edistämistä ominaisuuksista, voisivat he silti olla niiden käyttämisestä kiinnostuneita. Toinen lähestymistapa olisi keskittyä enemmän juuri niiden ominaisuuksien markkinointiin, joiden olemassaolosta käyttäjät eivät tiedä, ja siten mahdollisesti saataisiin suurempi osa käyttäjistä parantamaan salasanaturvallisuuttaan hallintasovelluksia hyödyntämällä.

# LÄHTEET


Alkaldi, N., Renaud, K. & Mackenzie, L. (2019). Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 10.

Alodhyani, F., Theodorakopoulos, G. & Reinecke, P. (2020). Password Managers—It's All about Trust and Transparency. *Future Internet*, *12*(11), 189. https://doi.org/10.3390/fi12110189

AppleInsider. (2022). *Touch ID | iPhone, iPad, Mac*. Noudettu 26. toukokuuta 2022, osoitteesta https://appleinsider.com/inside/touch-id

Aurigemma, S., Mattson, T. & Leonard, L. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4061–4070. https://doi.org/10.24251/HICSS.2017.490

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. https://doi.org/10.7903/cmr.19394

Bitwarden. (2022). *Bitwarden Open Source Password Manager*. Bitwarden. Noudettu 12. kesäkuuta 2022, osoitteesta https://bitwarden.com/

Bonneau, J., Herley, C., Oorschot, P. C. van & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

CISA. (18.11.2019). *Choosing and Protecting Passwords*. Noudettu 12. kesäkuuta 2022, osoitteesta https://www.cisa.gov/uscert/ncas/tips/ST04-002

Das, A., Bonneau, J., Caesar, M., Borisov, N. & Wang, X. (2014). The Tangled Web of Password Reuse. *Proceedings 2014 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2014.23357

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), 12. https://doi.org/10.1186/s13673-017-0093-6

Florencio, D. & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web - WWW '07*, 657–666. https://doi.org/10.1145/1242572.1242661

Florencio, D., Herley, C. & van Oorschot, P. C. (2014). Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. *Proceedings of the 23rd USENIX Security Symposium*, 575–590.

Google. (2022). *Use passwords across your devices - Computer - Google Chrome Help*. Noudettu 12. huhtikuuta 2022, osoitteesta https://support.google.com/chrome/answer/6197437

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K. & Theofanos, M. F. (2017). *Digital identity guidelines: authentication and lifecycle management* (NIST SP 800-63b; s. NIST SP 800-63b). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Herley, C. & Van Oorschot, P. (2012). A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy Magazine*, *10*(1), 28–36. https://doi.org/10.1109/MSP.2011.150

Hunt, T. (4.4.2017). *Password managers don't have to be perfect, they just have to be better than not having one*. Troy Hunt. Noudettu 25. toukokuuta 2022, osoitteesta https://www.troyhunt.com/password-managers-dont-have-to-be-perfect-they-just-have-to-be-better-than-not-having-one/

Karole, A., Saxena, N. & Christin, N. (2011). A Comparative Usability Evaluation of Traditional Password Managers. Teoksessa K.-H. Rhee & D. Nyang (toim.), *Information Security and Cryptology - ICISC 2010* (Vsk. 6829, s. 233–251). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-24209-0_16

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F. & Lopez, J. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. *2012 IEEE Symposium on Security and Privacy*, 523–537. https://doi.org/10.1109/SP.2012.38

Kotadia, M. (25.2.2004). Gates predicts death of the password. *CNET*. Noudettu 12. huhtikuuta 2022, osoitteesta https://www.cnet.com/tech/services-and-software/gates-predicts-death-of-the-password/

LastPass. (2022). *#1 Password Manager & Vault App with Single-Sign On & MFA Solutions*. Noudettu 12. kesäkuuta 2022, osoitteesta https://www.lastpass.com/

Li, Z., He, W., Akhawa, D. & Song, D. (2014). *The Emperor's New Password Manager: Security Analysis of Web-based Password Managers:* Defense Technical Information Center. https://doi.org/10.21236/ADA614474

Luevanos, C., Elizarraras, J., Hirschi, K. & Yeh, J. (2017). Analysis on the Security and Use of Password Managers. *2017 18th International Conference on Parallel and Distributed Computing, Applications and*

*Technologies (PDCAT)*, 17–24. https://doi.org/10.1109/PDCAT.2017.00013

Luo, H. & Henry, P. (2003). A common password method for protection of multiple accounts. *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, 2749–2754. https://doi.org/10.1109/PIMRC.2003.1259242

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. *Proceedings of the 27th USENIX Security Symposium*, 19.

Maclean, R. & Ophoff, J. (2018). Determining Key Factors that Lead to the Adoption of Password Managers. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 1–7. https://doi.org/10.1109/ICONIC.2018.8601223

McMillan, R. (27.1.2012). The World's First Computer Password? It Was Useless Too. *Wired*. Noudettu 23. toukokuuta 2022, osoitteesta https://www.wired.com/2012/01/computer-password/

Morris, R. & Thompson, K. (1979). Password security: a case history. *Communications of the ACM*, *22*(11), 594–597. https://doi.org/10.1145/359168.359172

Mozilla. (2022). *Password Manager - Remember, delete and edit logins and passwords in Firefox | Firefox Help*. Noudettu 12. huhtikuuta 2022, osoitteesta https://support.mozilla.org/en-US/kb/password-manager-remember-delete-edit-logins

NCSC. (24.1.2017). *What does the NCSC think of password managers?* Noudettu 25. toukokuuta 2022, osoitteesta https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

Notoatmodjo, G. & Thomborson, C. (2009). Passwords and Perceptions. *Conferences in Research and Practice in Information Technology*, *98*, 71–78.

Pearman, S., Zhang, S. A., Bauer, L., Christin, N. & Cranor, L. F. (2019). Why people (don't) use password managers effectively. *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, 319–338.

Peter J. Denning. (1992). The Science of Computing: Passwords. *American Scientist*, *80*(2), 117–120.

Pilar, D. R., Jaeger, A., Gomes, C. F. A. & Stein, L. M. (2012). Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. *PLoS ONE*, *7*(12), e51067. https://doi.org/10.1371/journal.pone.0051067

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

Ryan, R. M. & Deci, E. L. (2000). Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. *American Psychologist*, 11.

Shah, R. C. & Kesan, J. P. (2008). SETTING ONLINE POLICY WITH SOFTWARE DEFAULTS. *Information, Communication & Society*, *11*(7), 989–1007. https://doi.org/10.1080/13691180802109097

Stobert, E. & Biddle, R. (2014). *The Password Life Cycle: User Behaviour in Managing Passwords*. 13.

Wash, R., Rader, E. & Berman, R. (2016). Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. *Proceedings of the Twelfth Symposium on Usable Privacy and Security*, 15.

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. https://doi.org/10.1016/j.ijhcs.2017.11.002

Zimmermann, V. & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006