Janne Siltainsuu

SALASANAN HALLINTAMENETELMIEN KÄYTTÖÖNOTON MAHDOLLISTAJAT JA ESTEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Siltainsuu, Janne
Salasanan hallintamenetelmien käyttöönoton mahdollistajat ja esteet
Jyväskylä: Jyväskylän yliopisto, 2020, 72 s.
Kyberturvallisuus, Pro gradu-tutkielma
Ohjaaja: Niemenmaa, Marko

Tämä pro gradu- tutkielma käsittelee salasanan hallintajärjestelmiä. Tutkielmassa käsiteltävät salasanan hallintajärjestelmät ovat salasanojen hallinta muistamalla, salasanojen hallinta paperilla ja salasanan hallinta digitaalisella salasanan hallintajärjestelmällä. Digitaaliset salasanan hallintajärjestelmät jaetaan kahteen pääluokkaan sen perusteella, tallennetaanko salasanat sisältä tietokanta käyttäjän oman laitteen kiintolevylle vai palveluntarjoajan pilvipalveluun. Pro gradu- tutkielmassa käsitellään ensin salasanoihin liittyviä seikkoja, kuten salasanojen käsittelyä verkkopalveluissa, käyttöä ihmisten näkökulmasta sekä yleisesti haitallisimpia salasanan hallintatapoja. Salasanan hallintajärjestelmät esitellään pääpiirteittäin. Tutkimuksen empiirisessä vaiheessa haastateltiin laadullisen tutkimuksen keinoin salasanan hallintajärjestelmiä käyttäviä ja niitä ei käyttäviä henkilöitä. Keskeisimmät löydökset tutkimuksessa esittävät, että tällä hetkellä salasanoihin liittyvät suurimmat uhat ovat salasanojen heikko laatu sekä salasanojen uudelleen käyttäminen. Salasanojen uudelleen käyttäminen asettaa käyttäjän salasanat laadusta riippumatta uhan alaisuuteen, sillä salasanoja varastetaan jatkuvasti verkkopalveluista. Kun käyttäjä uudelleen käyttää salasanoja, on silloin yhdestä palvelusta vuotanut salasana avain kaikkiin käyttäjän muihin palveluihin. Tätä voidaan välttää käyttämällä ainutlaatuisia salasanoja jokaisessa palvelussa, joka väistämättä ajaa käyttäjän ongelmaan, jossa hänen on mahdotonta muistaa kaikkia salasanojaan. Tähän vastauksena on otettava käyttöön jokin digitaalisessa ympäristössä toimiva salasanan hallintajärjestelmä. Tutkimuksessa todettiin, että käytettävyyden ja tietoturvan näkökulmasta parhaaseen ja käytettävimpään lopputulokseen päästään, kun salasanan hallintajärjestelmä on pilvipohjainen, siihen on asetettu vahva pääsalasana, joka ei ole käytössä muualla sekä palvelussa on käytössä kaksi vaiheinen tunnistaminen. Näin voidaan välttää salasanojen uudelleen käyttäminen sekä käyttää generoituja merkityksettömiä salasanoja joka palvelussa. Näin voidaan toimia sillä, käyttäjän ei tarvitse muistaa salasanoja itse. Käyttäjän tarvitsee enää muistaa ainoastaan yksi salasana, jonka avulla hän pääsee käsiksi muihin salasanoihin. Empiirisen osion mukaan käyttäjät myös kokevat tämän käytännölliseksi ja järkeväksi tavaksi käsitellä käyttäjätunnuksia ja salasanoja.

Asiasanat: Salasanan hallinta, salasana, salasanan hallintaohjelma, tietomurto, salasanavuoto, pilvipohjainen salasanan hallinta, salasanojen uudelleenkäyttö.

ABSTRACT

Siltainsuu, Janne
Password managers promoters and blockers of using
Jyväskylä: University of Jyväskylä, 2020, 72 p.
Cyber security, Master's Thesis
Supervisor: Niemenmaa, Marko

This pro gradu thesis is focusing in password management systems. Thesis will go through three different password management systems, which are remembering passwords, writing passwords down and using a digital password management software. Digital password management systems are divided in to two main groups by the meaning which they save users passwords. These two ways are saving them to the users' hard drive and to a cloud service provided by the password management system. Thesis will first handle password related topics and then go through the three ways to handle the passwords. The study was made by interviewing persons that used a digital password management software and people who did not. These results were compared to each other. Important findings during the study were that password related threats focus on password reuse and using weak passwords. Password reuse is harmful because of the fact that passwords get stolen from the services databases all the time. When passwords are reused and the password leaks from one service, it means that the password can be used to log in as the user to multiple services. This can be managed by using a different password to every service that the user uses. This creates a problem, that the users cannot remember many passwords and the answer to that is to use a password manager that works in the digital environment. The findings suggest that the best way when balancing usability and information security is to use a cloud-based password manager, generate meaningless strings of characters as passwords to services, have a strong master password to the manager and have two factor authentications enabled in the service. By using this technique, the user can avoid password reuse and still maintain usability. This also means, that the user has to remember only one password in order to access all the other passwords. The interview part suggests also that this kind of a way to handle passwords is found practical and reasonable by users using it as way to handle their passwords.

Keywords: Password management, password, password management software, password data breach, password leak, cloud-based password management, password reuse

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Vuonna 2006 todettiin, että käyttäjien hallinnoitavat tunnusmäärät tulevat kasvamaan merkittävästi. Hallinnoitavien tunnusten määrä tulee johtamaan väistämättä siihen, että käyttäjät valitsevat huonompia salasanoja, käyttävät salasanoja uudelleen useissa palveluissa sekä kirjoittavat niitä ylös turvattomasti. (Chiasson, Van Oorschot, & Biddle, 2006). Tällä hetkellä salasanoihin liittyvät asiat koskettavat väistämättä verkossa kaikkia käyttäjiä. Salasanoihin liittyvät tietomurrot yleistyvät jatkuvasti ja useissa verkkopalveluissa ainut mikä erottaa hyökkääjän käyttäjän henkilökohtaisista tiedoista on ainoastaan käyttäjän tiedossa olevat käyttäjätunnukset. Näitä tunnuksia kuitenkin varastetaan jatkuvasti verkkopalveluista ja niiden tietoturvassa ei voida enää luottaa yksin verkkopalveluiden ylläpitäjiin. Salasanojen hallintaan on olemassa useita eri työkaluja, mutta käyttäjät silti edelleen uudelleen käyttävät salasanoja sekä jättävät ottamatta kaksivaiheisen tunnistautumisen käyttöön verkkopalveluissa. Tutkimusten mukaan kaksi kolmesta käyttäjästä uudelleen käyttää samaa salasanaa, tai ainakin lähes samaa salasanaa useissa eri verkkopalveluissa. Puolet käyttäjistä eivät edes vaihda salasanaansa, vaikka ovat kuulleet palvelun, jota käyttävät joutuneen tietomurron uhriksi. 42% käyttäjistä myös pitää tärkeämpänä salasanan helppoa muistamista, kun sen turvallisuutta. 42% käyttäjistä myös kuvittelee olevansa hyökkääjälle hyödytön, sillä heillä ei ole mitään arvokasta tietoa. (LogMeIn, 2020b). Vuonna 2019 Suomessa 138000 henkilö joutui identiteettivarkauden uhriksi, joka on yli neljäkertaa enemmän kuin vuotta aiemmin. (Fagerlund, 2019). Käyttäjätunnusten kasvun ja niiden merkityksen korostuminen jatkuu nykyisessä yhteiskunnassa ennen näkemätöntä vauhtia ja tästä syystä tähän on löydettävä jokin järkevä ratkaisu, kuinka salasanoja voidaan hallinnoida turvallisesti ja käyttäjäystävällisesti. Samaan aikaan päivittäin uutisoidaan käyttäjätietokantojen vuotamisista ja tietomurroista. Salasanojen hallinnan tulisi olla käyttäjän näkökulmasta helpompaa kuin uudelleen käyttäminen sekä niiden muistaminen. Toisin sanoen, käyttäjän tulisi luottaa mahdollisimman vähän palveluun ja sen ylläpitäjään ja pyrkiä itse suojautumaan. Suojautumiseen paraskeino näyttää olevan eri salasanan käyttäminen joka palvelussa, näin yhdestä palvelusta vuotaneet tunnukset eivät vaaranna muita. Tässä tutkimuksessa on tarkoitus löytää vastauksia seuraaviin tutkimuskysymyksiin:

- Minkälaisia tapoja on hallinnoida salasanoja?
- Minkälainen tapa hallinnoida salasanoja on käytettävyyden ja tietoturvan näkökulmasta suositeltavin?
- Minkälaiset tekijät edesauttavat tai hidastavat salasanan hallintajärjestelmien käyttöönottoa?

Tutkimuksessa käsitellään ensin salasanoihin liittyviä asioita peilaten niitä historiaan ja nykypäivään. Tutkimuksessa käsitellään salasanojen historiaan liittyvät asiat pääpiirteittäin, sillä ne selittävät syyt sen takana miksi olemme päätyneet tähän tilanteeseen. Lyhyesti voidaan todeta, että salasanoja ei koskaan suunniteltu näin laajamittaiseen käyttöön vaan tilanteeseen ajauduttiin verkkopalveluiden kasvaessa, sillä parempaa tapaa tunnistaa käyttäjää ei ole helposti saatavilla. Tutkimuksessa esitellään salasanoihin liittyvät tietomurrot, jotka liittyvät suoraan salasanoihin ja tavat, jolla tietomurroissa salasanoja varastetaan. Tutkimuksessa käydään lyhyesti läpi salasanojen muodostaminen turvallisesti. Salasanojen hallintatapojen osalta esitellään kolme eri tapaa, jotka ovat muistaminen, paperilla hallinnointi sekä digitaalinen hallinnointi. Digitaalinen hallinnointi on jaettu kahteen osaan. Jaon perusteena on käytetty eroa siinä, tallennetaanko salasanat verkossa olevalle pilvipalvelimelle vai paikallisesti käyttäjän omalle laitteelle. (Huth, Orlando, & Pesante, 2013).

Varsinaisessa tutkimusosuudessa haasteltiin yhteensä 12 henkilöä, jotka ovat työskennelleet tai työskentelevät sosiaali- ja kasvatusalalla. Näistä henkilöistä puolet käyttivät jotain digitaalista salasanan hallintajärjestelmää ja puolet eivät käyttäneet. Tarkoituksena on löytää mahdollisesti tekijöitä, jotka ovat saaneet käyttäjät ottamaan käyttöön salasanan hallintajärjestelmiä sekä mahdollisia esteitä, jotka hidastavat niiden käyttöönottoa. Haastatteluiden perusteella salasanan hallintajärjestelmän käyttöönottamista edistävät muiden henkilöiden suosittelu sekä käyttökokemuksen helppous. Salasanan hallintajärjestelmän käyttöönottamista hidastaa koettu vaiva ja tarpeettomaksi näkeminen, vaikka todellisuudessa jokainen haastateltava olisi kertomansa mukaan salasanan hallintajärjestelmän tarpeessa.

2 SALASANAT

Salasanat ovat ehdottomasti yleisin tapa tunnistaa käyttäjä sekä verkossa, että lähiverkon palveluissa. Salasanat ovat laajalle levinnyt tapa tunnistaa käyttäjät ja salasanoille ei ole lähipiirissä varsinaista reaalista haastajaa, joten salasanojen käyttö tulee todennäköisesti jatkumaan pitkään. Tutkimukset ovat osoittaneet, että käyttäjät eivät pysty muistamaan useita salasanoja ja tästä syystä he pyrkivät helpottamaan niiden muistamista käyttämällä salasanoja uudelleen. (Woods & Siponen, 2018). Salasanojen rinnalle on yritetty tuoda erilaisia vaihtoehtoja, kuten erilaisia älykortteja, julkisen avaimen infrastruktuuriin ja kryptografiaan perustuvia vaihtoehtoja sekä muita vastaavia, mutta mikään näistä ei ole levinnyt kuluttajamarkkinoilla yhtä suosituksi. (Pinkas & Sander, 2002). Näyttää siltä, että älykortteja ja muita vahvemman tunnistautumisen menetelmiä käytetään lähinnä kriittisissä järjestelmissä sekä viranomaiskäytössä. Nykyisin käyttäjät tarvitsevat useita kymmeniä, ellei satoja salasanoja. Näillä salasanoilla kirjaudutaan palveluihin, jotka vaihtelevat viihdepalveluista, verkkopankkien kautta suurten yritysten ja mahdollisesti jopa ihmishenkiä käsittelevien palveluiden hallintaliittymiin. Käytännössä kaikki internet palveluita käyttävät tietävät, että salasanojen turvallisuus on tärkeä asia ja siihen tulisi kiinnittää huomiota.

Salasanoja on käytetty käytännössä aina ja sotilaskäytössä tunnussanat ja tunnuslauseet ovat olleet käytössä jo pitkään. Tunnussana perinteisesti on toiminut niin, että on päätetty esimerkiksi kaksiosainen tunnussana, kuten ”suokuokka” ja tunnussanaa kysyttäessä kysyjä sanoo ”suo” johon vastaaja vastaa ”kuokka.” Näin ollen molemmat osapuolet voivat varmistua siitä, että molemmat tietävät tunnussanan ja ovat näin oikeutettuja kanssa käymiseen. Tietojärjestelmissä ensimmäisiä salasanoja otettiin käyttöön Massachusetts Institute of Technologyssä vuonna 1961. Salasanojen käyttö verkkopalveluissa toimii niin, että käyttäjä saapuu johonkin palveluun joko työasemalla tai verkossa. Käyttäjä syöttää käyttäjätunnuksensa sekä salasanansa. Tämän jälkeen järjestelmä vertaa taustalla olevassa tietokantapalvelimessa olevaan käyttäjätietokantaan löytyykö sieltä vastaava pari. Mikäli löytyy, käyttäjä on tällöin oikeutettu pääsemään järjestelmään. Käyttäjätunnus- ja salasanayhdistelmä ei edusta vahvaa tunnistautumista, vaikka näin usein ajatellaan olevan. Vahvalla tunnistautumisella tarkoitetaan tilannetta, jossa käyttäjä tunnistautuu käyttäen vähintään kahta seuraavista faktoreista:

1. Käyttämällä jotain mitä käyttäjä tietää, esimerkiksi käyttäjätunnus ja salasana
2. Käyttämällä jotain mitä käyttäjällä on mukana, esimerkiksi vaihtuva numeropari puhelimessa tai muussa mukana kannettavassa laitteessa
3. Käyttämällä jotain mitä käyttäjä itse fyysisesti on, eli käyttämällä biometristä tunnistetta, joista yleisimmät ovat sormenjälki tai kasvojen tunnistus
4. Käyttämällä toista henkilöä, joka tunnistaa käyttäjän. Eli toinen henkilö todentaa käyttäjän valtuudet. (Brainard, Juels, Rivest, Szydlo, & Yung, 2006).

Verkkopalveluista valtaosa ei vaadi vahvaa tunnistautumista ja vain harvat käyttäjät ottavat sen käyttöön. (LogMeIn, 2020b). Tämä saattaa selittyä sillä, että käyttäjät kokevat sen ylimääräisenä vaivana ja saattavat jättää koko verkkopalvelun käyttämättä. Yleisesti käyttäjät eivät halua käyttää verkkopalveluita, jotka koetaan vaivalloiseksi. (Ketola & Krug, 2006). Vaikka se kuitenkin realistisesti kestää vain muutamia sekunteja. Valtaosa pankkipalveluista käyttää vahvaa tunnistautumista, johon kuuluu usein käyttäjätunnus, salasana sekä tunnuslukukortti tai tunnuslukuohjelma mobiililaitteessa. Vain alle 10% käyttäjistä on esimerkiksi ottanut sen käyttöön verkon suosituimmassa sähköpostipalvelu gmailissa. (Ong, 2018).

2.1 Salasanojen käsittely

Salasanalla tarkoitetaan sanaa, jolla käyttäjä tunnistetaan ja hänelle annetaan oikeus käyttää jotakin järjestelmää, johon hänellä ei ilman salasanaa olisi oikeutta. Tällaisia järjestelmiä ovat mm. verkkopalvelut, palvelimet sekä erilaiset hallintajärjestelmät. Usein salasanan parina käytetään käyttäjätunnusta, jolloin voidaan erotella käyttäjät toisistaan. (Techterms, 2020). Tämä myös tietyllä tapaa parantaa salasanan tietoturvaa, sillä potentiaalisen hyökkääjän tulee tällöin tietää myös käyttäjätunnus. Käyttäjätunnuksen merkitys tietoturvassa on kuitenkin todellisuudessa varsin vähäinen, sillä valtaosalla henkilöistä käyttäjätunnus on joko etu- ja sukunimi erotettuna esimerkiksi pisteellä tai se on henkilön pääsähköposti osoite, esimerkiksi matti.meikalainen@gmail.com. Salasanan pituutta tai merkistöä voidaan rajoittaa, mutta usein salasana saa ja on suositeltavaa sisältää kaikkia perinteisiä kirjaimia, numeroita sekä erikoismerkkejä. (viestintävirasto, 2014). Yleisesti tästä on olemassa useita eri ohjeistuksia, joissa pyritään antamaan ohjeita hyvästä salasanasta. Yleisesti salasanan tulisi olla helppo muistaa, mutta kuitenkin vaikea arvata. Tällainen salasana voidaan saavuttaa muodostamalla siitä lause. Salasanoissa ei tulisi vaatia enää erikoismerkkejä, sillä ne kasvattavat salasanan väärinkirjoittamisen todennäköisyyttä. Salasanojen tulisi olla vähintään merkkiä ja niiden pituudelle ei pitäisi asettaa ylärajaa tai ainakin sallia 64 merkkiset salasanat. Salasanat pitäisi myös saada kopioida muualta salasana kenttään ja niitä ei tulisi enää vaatia tietyin aikavälein vaihdettavaksi. (Fenton yms., 2017).

Käyttäjälle näkyvä osuus salasanasta on sen kirjoittaminen salasanakenttään, mutta tämä on niin sanotusti vain jäänvuoren huippu, kun pohditaan mitä salasanalle tapahtuu sen kirjoittamisen jälkeen muutamassa silmänräpäyksessä. Kun kyseessä on internetissä toimiva verkkopalvelu, salasana lähetetään verkossa käyttämällä http-protokollan salaamatonta tai salattua versiota. (Erdos, 2020). Mikäli käytetään salaamatonta http-protokollaa tunnusten lähettämisessä palvelimelle, on siinä mahdollisuus salasanan varastamiselle. Http- protokollasta on olemassa kaksi versiota, joista toinen http on täysin salaamaton. Tämä tarkoittaa sitä, että kun salasana siirtyy verkossa kuljetettavaksi kohti palvelinta, jossa kirjautuminen tapahtuu, kuljetetaan se verkossa täysin salaamattomana. (Fielding yms., 1999). Tämä tarkoittaa sitä, että mikäli käyttäjä on esimerkiksi

salaamattomassa langattomassa verkossa, voidaan salasana kaapata kuuntelemalla verkossa tapahtuvaa liikennettä, sillä se on selkotekstinä luettavissa. Oikea tapa käsitellä käyttäjä kirjautumista palvelimelle on käyttää http- protokollasta https- versiota, jossa on S lisättynä perään, joka tarkoittaa ”securea” eli turvallista. Tällöin käyttäjän liikenne salataan selaimen ja palvelimen välissä ja mikäli vihamielinen hyökkääjä kuuntelee liikennettä välissä, ei hän saa muuta kuin merkityksettömän kirjainjonon, josta ei ole pääteltävissä käytännössä mitään hyödyllistä. Salasana voidaan välittää http protokollassa muutamalla eri tavalla, joista yleisimmät ovat GET ja POST. Näistä GET tarkoittaa, että salasana välitetään palvelimelle käyttäen osoiteriviä, jolloin riskinä on salasanana tallentaminen selkotekstinä selaimen historioihin. Oikea tapa välittää salasanaa http protokollassa on käyttää POST- metodia, jossa se välitetään piilossa historioista ikään kuin muiden parametrien osana. (Banerjee, 2020).

Kun salasana päätyy palvelimelle siellä salasanaa, verrataan tietokantaan, jossa käyttäjätiedot ovat tallennettuna ja etsitään sieltä vastaava pari. Salasanoja tallennetaan usein kolmella eri tavalla. Selkotekstisenä, yhdensuuntaisella hash-algoritmilla salattuna, sekä ns. suolattuna hashinä. (Bauman, Lu, & Lin, 2015).

Ensimmäinen on selkotekstinä tallentaminen, jolloin salasana on tallennettuna täysin selkotekstinä ja se on luettavissa, mikäli tietokantaa päästään lukemaan. Tämä luonnollisesti on lähtökohtaisesti jo riskialtis ja vanhanaikainen tapa, sillä pelkästään ylläpitäjä, jolla on pahat aikeet voi kenenkään huomaamatta varastaa sieltä käyttäjien salasanoja. (Owasp, 2020). Selkotekstisillä salasanapaketeilla on myös rahallista arvoa verkon laittomilla markkinoilla, joten ylläpitäjä voi tienata myös myymällä käyttäjien tuoreita salasanoja. (Peltomäki & Norppa, 2015). Selkotekstisenä salasanat ovat myös haavoittuvaisia sovelluksessa oleville haavoittuvuuksille, sillä mikäli esimerkiksi tietokantakyselyyn päästään vaikuttamaan sovelluksen läpi esimerkiksi SQL-injektiolla voidaan sieltä saada takaisin vastauksena käyttäjien salasanoja. (Bauman yms., 2015).

Toinen tapa on käyttää yhden suuntaista hash- algoritmilla salattua tallennustapaa, jolloin käyttäjän salasanasta lasketaan aina samalla tavalla tietty tiiviste ja tämä tiiviste tallennetaan tietokantaan. (Greenberg, 2020). Kun salasanaa tarkistetaan, otetaan käyttäjän salasana ja lasketaan siitä uudelleen sama tiiviste, mikäli tämä juuri laskettu tiiviste on sama, kun tietokannassa oleva, voidaan varmuudella sanoa käyttäjän syöttäneen oikean salasanan. Tässä etuina on se, että salasanaa ei tallenneta selkotekstisenä ja sen takaisin laskeminen on käytännössä teoreettisesti mahdotonta. Tässä kuitenkin takaisinlaskenta on mahdollista, kun käytetään suuria määriä laskenta tehoa tai mikäli käyttäjällä on salasananaan jokin yleisesti tiedossa oleva sana, sillä silloin voidaan laskea esimerkiksi kaikista sanakirjan sanoista tiiviste käyttäen samaa algoritmia ja mikäli se löytyy tietokannasta, tiedetään mikä tähän tiivisteeseen johtanut sana oli. (Bauman yms., 2015).

Kolmas tapa on käyttää suolausta, jolloin salasanan hash- prosessiin liitetään jokin käyttäjäkohtainen tunniste, jolloin vaikka käyttäjän salasana olisikin heikko ei se vastaa enää sanakirjahyökkäyksistä löytyvää hashia, sillä salasanan tiiviste on eri. (Arias, 2020). Tälläinen prosessi käytännössä tarkoittaa sitä, että käyttäjän salasana esimerkiksi ”banaani” saapuu palvelimelle ja sen perään lisätään sana ”suola” jolloin salasanaksi muodostuu ”banaanisuola” ja tästä

lasketaan turvallisella algoritmillä kuten SHA3-256 -tiiviste, joka tässä tapauksessa olisi ”45ea7d47c92e5d6f1b32667c99f95f6e5e16898fbd6f4656cd00485100aac27b”. Mikäli hyökkääjä toteuttaa sanalla banaani tätä kohtaan sanakirjahyökkäyksen, hän saa tiivisteen ”e3c34a2fefda03809e971009d845e28084ba11292667d83ea8e104f768a21bcb” mikä on täysin erilainen, kun käyttäjän salasanasta laskettu tiiviste ja näin hyökkääjä ei saa tietoonsa käyttäjän salasanaa. (Bauman yms., 2015).

Salasanojen osalta käyttäjän tulisi luottaa mahdollisimman vähän palveluun, johon hän rekisteröityy ja pyrkiä käyttämään uniikkeja salasanoja, sillä käyttäjällä ei ole käytännössä mahdollisuutta tarkistaa, käsitteleekö ylläpitäjä salasanoja turvallisella tavalla. Valitettavasti myös suuria verkkopalveluita on vuosien varrella jäänyt kiinni salasanojen huonosta käsittelystä, myös jopa tietomurtojen kautta, jolloin käyttäjien salasanat ovat vuotaneet maailmalle. (Bauman yms., 2015).

2.2 Salasanojen käyttö ja käytännöt

Salasanojen osalta käyttäjät pyrkivät valitsemaan itselleen tuttuja salasanoja, kuten tavallisia sanakirjasta löytyvä sanoja, nimiä, automerkkejä yms. Usein käyttäjät pyrkivät myös valitsemaan itselleen merkityksellisiä asioita kuten omiin lapsiin, lemmikkieläimiin tai puolisoon liittyviä asioita. (Brown, Bracken, Zoccoli, & Douglas, 2004). Vuonna 2016 toteutetun tutkimuksen mukaan keskimääräinen salasanan pituus on 8 – 6 merkkiä, joista suurin osa 8 kirjainta. Suurin osa salasanoista on pelkkiä numeroita, joita tutkimuksen mukaan oli liki puolet, eli 45.01%. Tätä tukee myös se, että maailman kaksi yleisintä salasanaa ovat 123456 ja 123456789. (Keck, 2019). Tässä on tapahtunut muutos suhteessa vuoteen 2007, jolloin salasanoiksi valittiin usein miten ainoastaan pienistä kirjaimista koostuvia sanoja, ellei erikseen käyttäjää pakotettu valitsemaan jotakin muuta merkkiä sen sekaan. (Florencio & Herley, 2007). Tähän muutokseen syynä saattaa olla se, että vuonna 2007 käytännössä alle puoli prosenttia internetin käytöstä tehtiin mobiiliselaimella, kun nyt vuonna 2019 jo yli puolet internetin selaamisesta tehdään mobiililaitteilla. (Statscounter, 2019). Toisiksi suurin osuus salasanoista olivat numeroista ja kirjaimista koostuvat salasanat. Näitä käyttävät 39,36% käyttäjistä ja tällaisesta salasanasta voidaan pitää esimerkkinä yleistä salasanaa ”password1”. Käyttäjistä 12,35% käyttivät salasanoinaan pelkästään kirjaimista koostuvia salasanoja, kuten ”password.” Tutkimuksen mukaan vain 3,29% salasanoista käytettiin erikoismerkkejä. Erikoismerkeistä käyttäjät usein preferoivat erikoismerkkejä, jotka ovat tuttuja ja jokapäiväisessä käytössä. Kolme yleisintä erikoismerkkiä, joita käyttäjät käyttivät, olivat piste, @-symbooli sekä huutomerkki. (Shen, Yu, Xu, Yang, & Guan, 2016). Huomattavaa tutkimuksessa on, että 80% käyttäjistä käyttää ainoastaan numeroita ja kirjaimia salasanoissa, joka vähentää entropiaa merkittävästi. Kyseinen tutkimus on toteutettu kahdesti ja tutkimuksen perusteella näyttää siltä, että käyttäjät ovat kasvattaneet salasanan pituutta tutkimusten välillä. Näyttää myös siltä useimmiten käyttäjät päätyvät

salasanoihin, jotka ovat joko pelkkiä numeroita tai alphanumeerisia, eli koostuvat kirjaimista ja numeroista. Mikäli salasanoissa on erikoismerkkejä, ovat ne yleisimmin sellaisia, joihin on näppäimistöllä helppo ylettyä ja ne ovat tuttuja. On esitetty myös, että salasanoja kirjoittaessa käyttäjä voisi siirtää sormiaan yhden näppäimen oikealle tai vasemmalle, jolloin esimerkiksi edellä mainitusta salasanasta ”password” tulisi ”åsddeptf”, jolloin tämä olisi silloin turvallisempi salasana. Tämä osittain pitää paikkansa, sillä usein kun kokeillaan manuaalisesti salasanoja kokeillaan ensimmäisenä perusmuotoisia yleisesti käytettyjä salasanoja, jolloin tämän tyylinen salasanan muuttaminen toimisi, mutta koneellisessa salasanojen murtamisessa tämän tyyliset muunnokset joutuvat nopeasti erilaisille salasanalistoille. Näistä syistä tällaiset käytännöt eivät kasvata salasanan turvallisuutta merkittävästi. Tutkimusten mukaan käyttäjät uudelleen käyttävät salasanoja palveluissa ja näitä salasanoja käyttäjillä on yleensä keskimäärin 6,5 (Florencio & Herley, 2007). Näitä salasanoja käyttäjät usein hallinoivat joko muistamalla, kirjoittamalla ne ylös, yrityksen ja erehdyksen kautta kokeilemalla eri muunnelmia salasanakenttään sekä käyttämällä ”unohdin salasanani”- palvelua.

2.3 Salasanat ja tietomurrot

Salasanoihin liittyvistä tietomurroista uutisoidaan usein. Usein näissä varastetaan käyttäjätietokanta, jossa on suuria määriä käyttäjätietoja. Käyttäjätietokantojen tietovuotoja seuraavan sivuston haveibeenpwned.com:n ylläpitäjän Troy Huntin (2020) mukaan tätä kirjoittaessa vuonna 2020 yhteensä 9,5 miljardia käyttäjätiliä olivat joutuneet tietomurron uhriksi, joka tarkoittaa sitä, että käytännössä vain heidän tietoonsa on tullut tietomurtoja enemmän, kun maailmassa on ihmisiä. (Hunt, 2020). Kyseessä on ainoastaan 442 tietomurtoa, joten tämä kuvaa massiivista suuruusluokkaa ja sitä, että on hyvin todennäköistä, että valtaosa meistä on joutunut tietomurron uhriksi sen kautta, että tunnuksemme on vuotaneet ulos jostakin palvelusta.

Käyttäjätunnuksia varastetaan sen takia, että niille on tor-verkkojen kauppapaikoilla rahallinen arvo. Verkkorikollisryhmät ostavat näitä ja näiden perusteella he pyrkivät erilaisin keinoin saamaan rahallista hyötyä. (Peltomäki & Norppa, 2015). Tietomurtoja, joissa salasanoja varastetaan, toteutetaan useilla eri keinoilla. Tällaisia keinoja ovat hyökkäykset palvelin infrastruktuuria kohtaan, eli niitä laitteita, jotka käsittelevät pyyntöjä sekä joissa varsinainen tieto on varastoituna. Palvelimia vastaan voidaan hyökätä hyödyntämällä esimerkiksi vanhentuneita versioita palvelimen käyttöjärjestelmässä. Vanhentuneista versioista on usein löydetty haavoittuvuuksia ja siitä syystä ne ovat vanhentuneita versioita. Näitä kyseisiä haavoittuvuuksia löytyy verkosta varsin reilusti ja niiden avulla voidaan hyödyntää jotakin järjestelmässä olevaa heikkoutta ja saavuttaa epätavallisin keinoin ylläpitäjän oikeudet palvelimeen. (Huda, 2019).

Käyttäjätietokanta voidaan varastaa myös hyödyntämällä haavoittuvuuksia palvelimen ohjelmistoissa. Tällaisia haavoittuvuuksia voivat olla esimerkiksi haavoittuvuudet, jotka ovat esimerkiksi palvelimen ohjelmointikielissä.

Esimerkiksi PHP, jota käytetään useissa sovelluksissa taustalla, on löydetty todella paljon haavoittuvuuksia ja mikäli PHP:sta on käytössä esimerkiksi versio, josta on löydetty valmis haavoittuvuus, voidaan sitä hyödyntämällä saavuttaa myös ylläpitäjän oikeudet. (Huda, 2019). Palvelimissa on myös käytännössä aina jokin tapa päästä etähallitsemaan palvelimessa tapahtuvia prosesseja. Käytännössä nykyisin tällainen tapa on SSH eli secure shell. (Ylönen, 1996). Siinä olevia haavoittuvuuksia sekä heikkouksia voidaan myös hyödyntää, jolloin voidaan käytännössä päästä palvelimeen käsiksi, kuten ylläpitäjäkin pääsee siihen käsiksi. Tällaisissa tilanteissa saatetaan myös käyttää hyödyksi vanhoja salasana murtoja ja perinteisesti urkkia ylläpitäjän salasana niistä ja kokeilla mikäli näillä voitaisiin murtautua palvelimelle. Ylläpitäjän tunnuksia voidaan myös pyrkiä urkkimaan huijaamalla ylläpitäjä luovuttamaan ne esimerkiksi puhelimessa. Tällaiset tilanteet ovat erityisen viheliäisiä ylläpitäjän kannalta, sillä niissä usein ylläpitäjä joutuu tiedustellun hyökkäyksen kohteeksi ja häneltä urkitaan salasanoja käyttäen hyväksi hänen persoonalleen tärkeitä asioita ja näin olleen hyödyntäen niitä haavoittuvuuksina. (Mitnick, Simon, & Wozniak, 2011). Salasanoja saatetaan varastaa ylläpitäjältä myös hyödyntämällä haittaohjelmia tai haittaohjelman avulla pystytään asentamaan takaovi palvelimelle, ylläpitäjän hoitaessa normaaleja työtoimenpiteitä. Kenties eräs perinteisimmistä keinoista on myös ylläpitäjän lahjonta sekä kiristys, joiden avulla ylläpitäjä saadaan itse ajamaan mahdollisesti esimerkiksi haitallinen ohjelmakoodi palvelimeen itse.

Käyttäjätietokantoja voidaan myös varastaa hyödyntämällä haavoittuvuuksia palvelimen päällä ajettavassa sovelluksessa. (Owasp, 2017). Tällä tarkoitetaan sitä, että haavoittuvuus on kansan kielisesti siinä internet sivussa, jonka takana olevalle palvelimelle yritetään murtautua. Tällaiset haavoittuvuudet ovat todella yleisiä ja voidaankin sanoa, että jokaisessa sovelluksessa on eriasteisia haavoittuvuuksia, joiden avulla voidaan vaikuttaa sovelluksen takana olevaan palvelimeen. Tällaisia haavoittuvuudet syntyvät ohjelmointi virheistä ja niitä voidaan löytää pyrkimällä vaikuttamaan palveluun tavoilla, joita palvelun suunnittelija ei osannut odottaa. Tällaisista haavoittuvuuksista klassisimpia ovat SQL-injektiot. Näissä hyökkäyksissä kirjoitetaan esimerkiksi rekisteröitymiskenttään sähköpostin sijasta osa tietokantakyselyä. Mikäli tätä tietokantakyselyä ei käsitellä järjestelmässä oikein ja se pääsee palvelimelle asti ja se tulkitaan aitona tietokantakyselynä ja sen seurauksena voidaan saada esimerkiksi sovellus tulostamaan käyttäjätietokanta hyökkääjälle. (Janot & Zavarsky, 2008).

Salasanoja voidaan varastaa myös perinteisillä fyysisillä menetelmillä. Tällaisissa tilanteissa varastetaan laitteita, joissa käyttäjätietoja säilytetään. Tällaisia laitteita ovat yleisesti palvelimet, mutta joissain tapauksissa niitä säilytetään myös työasemilla, vaikka tämä luonnollisesti on ehdottoman väärä tapa säilöä salasanoja. (Mitnick yms., 2011).

2.4 Salasanojen hallinta

Kuten jo aiemmin on todettu, salasanoihin liittyvät tietomurrot koskettavat nykyisin kaikkia henkilöitä, jotka käsittelevät jotain tietoja mihin tarvitaan

käyttäjätunnus ja salasana. Keskimäärin käyttäjillä on 38 käyttäjätiliä, joihin tarvitaan salasana. (LogMeIn, 2020b). Käytännössä tämä tarkoittaa sitä, että jokainen henkilö on tällä hetkellä riskissä joutua salasanoihin liittyvän tietomurron uhriksi. Salasanoihin liittyvän tietomurron uhriksi joutumista tuskin voi välttää realistisesti, joten on löydettävä jokin toinen tapa suojautua siltä ja oikea tapa tällöin on käyttää uniikkeja salasanoja joka palvelussa. Tässä kappaleessa käsitellään läpi erilaiset tavat muodostaa turvallinen salasana.

2.4.1 Turvallinen tapa muodostaa ja muistaa salasana

Salasanojen tärkein ominaisuus on oikeastaan hieman epäintuitiivisesti olla olematta mikään oikea sana. Tämä johtuu siitä, että esimerkiksi suomen kielessä on perusmuotoisia sanoja noin 100 000 ja murteiden kanssa noin 350 000. (Eeronen, 1997). Joka on ihmiselle käsiteltäväksi todella suuri määrä, mutta tietokoneiden käsiteltäväksi hyvin kohtuullinen määrä. Tällaisen sanamäärän kokeileminen käyttäjätunnuksia vastaan ei ole ongelma ja mikäli käyttäjätietokanta on saatu varastettua ja sitä voidaan käsitellä paikallisesti, on selvää, että perusmuotoisten sanojen salaukset murtuvat järjellisessä ajassa. (Brumen & Makari, 2017). Salasanojen tulisi olla ennemmin, jokin lause tai lyhyt tarina, jonka käyttäjä on keksinyt itse. Tämä johtuu siitä, että mikäli lause tai lyhyt tarina on jostakin yleisesti tiedossa olevasta teoksesta tai runosta, on se myös mahdollista potentiaalisen hyökkääjän käydä koneellisesti läpi. Salasanan pituudella on väliä, joten käyttäjän keksimä lause tulisi olla yli 16 merkkiä. Tätä tukee myös viestintäviraston (2014) antama suositus, jonka mukaan salasanan tulisi olla vähintään 15 merkkiä pitkä. Viestintävirasto perustelee ohjettaan sillä, että lyhyt salasana on helpompi vakoilla käyttäjän olan yli sekä teknisesti helpompi murtaa varastetusta käyttäjätietokannasta. 15 merkkiä suojelee pakottaa käyttäjän myös keksimään jotakin muuta, kun salasanan, joka on jokin oikea sanakirjasta löytyvä sana, sillä esimerkiksi suomen sanoista suurin osa on kahdeksan merkkiä pitkiä. (Länsimäki, 2002). Esimerkiksi hakukone jätti Googlen (2020) antamien suositusten mukaan salasana voisi olla esimerkiksi, jokin kirjassa esiintyvä lause, musiikkikappaleen lyriikka tai runo. Näin se olisi helposti muistettavissa sekä vaikeasti koneellisesti arvattavissa. Näyttää siltä, että pidempi on entropian kannalta parempi. (Spacey, 2020). Tämä johtuu yksinkertaisesti siitä, että mitä enemmän salasanassa on merkkejä, sitä enemmän on luonnollisesti eri mahdollisuuksia missä järjestyksessä nämä merkit voivat olla. Käyttäjän keksimän lauseen tulisi sisältää myös numeroita, merkistön kirjainkoon vaihtelua sekä erikoismerkkejä. Näiden merkitys on kuitenkin pienempi, sillä entropiaa voidaan kasvattaa parhaiten kasvattamalla salasanan pituutta. Salasanan muistamisen kannalta tärkeätä on kuitenkin, että salasanalla on käyttäjälle jokin merkitys. Salasanojen muodostamisessa helpoksi koettu tapa avustaa muistamista on valita jokin kuva, josta salasana muodostetaan. Mikäli kuvassa esiintyy henkilöitä, muistetaan se todennäköisemmin. Esimerkiksi, jos käyttäjällä on kuva, jossa hänen puolisonsa hienon auringonlaskun edessä voisi salasana olla esimerkiksi ”RakasPuolisoniJustiinaPunaisessaAuringonlaskussa!”, jolloin salasana ei ole yksittäinen sana, se on yli 16 merkkiä pitkä, sisältää eri merkistökokoja, erikoismerkkejä sekä numeroita.

Samalla salasana on helposti palautettavissa pitkäkestoisesta muistista, kun käyttäjä vilkaisee valokuvaa. (Isola, Xiao, Torralba, & Oliva, 2011).

Salasanojen uudelleen käyttö luo kuitenkin ongelman siitä, että vaikka salasanat olisivat erittäin vahvoja, on salasanan turvallisuus kuitenkin samaan aikaan usean palvelun ylläpitäjän vastuulla, sillä salasanan turvallisuuden rikkoontuminen todennäköisesti johtuu jonkin palvelun huonosta tietoturvan tasosta. Tällöin mikäli salasana pääsee käyttäjätunnuksen kanssa vuotamaan yhdestä palvelusta, on tällöin hyökkääjällä salasanan uudelleen käytön takia kaikkien palveluiden tietoturva vaarantunut. Käytännössä käyttäjällä ei ole mahdollisuutta vaikuttaa palveluiden tietoturvan tasoon, joten käyttäjän on pyrittävä taistelemaan tätä vastaan käyttämällä uniikkeja salasanoja jokaisessa palvelussa. Tämä luonnollisesti kuitenkin asettaa suuren haasteen salasanojen muistamiselle ja käytännössä käyttäjät unohtavat salasanat ja tästä syytä salasanojen uudelleen käyttäminen on todella yleistä. Käytännössä ainut järkevä tapa on käyttää jotain salasanan hallintajärjestelmää. (viestintävirasto, 2014).

3 SALASANOJEN HALLINTATAVAT

Tässä kappaleessa esitellään erilaiset tavat hallita salasanoja. Yleisesti tällä hetkellä käyttäjillä on kymmeniä, ellei jopa satoja salasanoja, joiden perusteella he kirjautuvat verkon eri palveluihin ja tämä väistämättä ajaa tilanteeseen, jossa salasanoja on hallinnoitava jollain tavalla. (LogMeIn, 2020b). Nämä tavat ovat käytännössä mielessä muistamalla, paperille kirjoittamalla tai digitaalisella salasanan hallintaohjelmalla. Digitaalisella salasanan hallintaohjelmalla tarkoitetaan jotain ohjelmallista työkalua, jonka tietokanta on tallennettu joko käyttäjän omalle tietokoneelle tai palveluntarjoajan pilvipalveluun. Tässä kappaleessa esitellään tarkemmin nämä kaikki kolme tapaa ja punnitaan niiden hyötyjä sekä haittoja. Haittoja punnitaan tietoturvan näkökulmasta hyödyntämällä perinteistä tietoturvan kolmen ulottuvuuden: luottamuksellisuuden, saatavuuden ja muuttumattomuuden kannalta. (Hedström, Kolkowska, Karlsson, & Allen, 2011). Jokainen tapa myös arvioidaan pohtimalla sen vahvuuksia, heikkouksia sekä potentiaalisia tietoturva uhkia, jotka ovat relevantteja kyseisen hallintatavan kannalta. Kappaleen lopuksi tavasta vedetään yhteen tärkeimmät asiat. Kappaleen lopuksi salasanojen hallintatapoja vertaillaan toisiinsa.

3.1 Salasanojen hallinta muistamalla

Suuri osa käyttäjistä hallitsee salasanoja mielessään muistamalla, jolloin salasanaa tarvittaessa käyttäjä muistelee sen mielestään ja kirjoittaa itse salasana kenttään. Tällöin käyttäjä palauttaa salasanan pitkäkestoisesta muististaan työmuistiin ja suorittaa kirjautumisen ilman, että hän käyttää siihen ulkoisia apuvälineitä. Usein käyttäjät muistia käyttäessään muodostavat myös salasanansa itse. Tällöin salasana muodostetaan tutkimusten mukaan käyttäen hyödyksi itselle merkityksellisiä ja helposti muistettavia asioita. Tällöin salasanatutkimusten mukaan liittyy henkilöön itseensä, lähisukulaiseen, kuten omiin lapsiin, kotieläimeen tai puolisoon suurella todennäköisyydellä. (Brown yms., 2004).

Tietoturvan näkökulmasta salasanojen saatavuus on optimaalisessa tilanteessa muistamisessa korkea, sillä käyttäjällä on salasanat aina saatavilla muistissaan. Kuitenkin näyttää vahvasti siltä, että salasanoja unohdetaan ja käyttäjät joutuvat usein turvautumaan salasanojen palauttamispalveluun. (Florencio & Herley, 2007). Salasanan palauttaminen taas usein johtaa siihen, että käyttäjä pyrkii valitsemaan salasanan, jonka hän muistaa ja tämä salasana on joko heikompi, kun edellinen tai se on uudelleen käytettynä toisesta palvelusta. Tutkittaessa salasanamurtoja, voitiin havaita, että 52% käyttäjistä uudelleen käyttää samaa salasanaa tai ainakin lähes samaa salasanaa useissa palveluissa. (Kracker, 2018). Käyttäjät pyrkivät muuttamaan salasanojaan palvelukohtaisesti yleensä jonkin verran. Yleisimpiä käytäntöjä ovat kirjainmerkistön koon vaihtaminen, sopivien kirjainten korvaaminen saman näköisellä numerolla tai erikoismerkillä, sekä salasanan perään lisättävien lyhyiden lisänumeroiden tai erikoismerkkien lisää. Näyttää kuitenkin siltä, että salasanojen variointi lisää merkittävästi salasanojen

unohtamista, sillä käyttäjät eivät muista, mikä salasana sopii mihinkin palveluun. Tämä johtaa myös saatavuuden menettämiseen, sillä käyttäjä ei pääse ilman ulkopuolista apua kirjautumaan palveluun. Luottamuksellisuuden osalta käyttäjän salasanat ovat ainakin teorian tasolla hyvässä turvassa, sillä varsinaista realistista keinoa kiduttamisen lisäksi ei ole päästä käsiksi käyttäjän salasanoihin, mikäli ne ovat käyttäjällä omassa mielessään muistissa. Käyttäjää voidaan kuitenkin huijata luovuttamaan salasana erilaisten sosiaalisten huijausten sekä kalastelu yritysten kautta. (Hong, 2012). Kalastelulla ja sosiaalisella huijaamisella tarkoitetaan tilannetta, jossa käyttäjä ajetaan sellaiseen tilanteeseen, jossa hänelle tuntuu ainoalta järkevältä ulospääsyltä luovuttaa salasana tai muu vastaava henkilölle esimerkiksi puhelimessa. (Brainard yms., 2006). Salasanojen luottamuksellisuus voidaan menettää myös verkkopalvelun tietomurron kautta. On melko epärealistista, että käyttäjän tiedot vuotaisivat Googlen, Facebookin tai Twitterin kaltaisista verkon jättiläisistä, sillä näiden palveluiden ydinliiketoimintaa on palveluiden tietoturvan kunnossa pitäminen ja näissä palveluissa työskentelee suuriakin osastoja valvoen, testaten ja korjaten tietoturvaa. Toki näissäkin palveluissa on aikojen saatossa kohdattu suuriakin tietovuotoja, mutta niiden todennäköisyys on pienempi, kun pienemmissä palveluissa. Todellisuudessa käyttäjän salasana todennäköisesti vuotaa sellaisesta palvelusta, joka ei ole kovin suuri ja sen tietoturvan ylläpito ja valvonta ei ole palvelun ydinliiketoimintaa. Tällaisia palveluita ovat esimerkiksi erilaiset harrasteseurat, vapaaehtoisten ylläpitämät keskusteluforumit sekä pienet pelipalvelut. Tällaisissa palveluissa ei myöskään välttämättä ole kykyä havainnoida mahdollista tietomurtoa, mikäli se ei aiheuta palveluun suurta katkosta tai muuta vastaavaa. Käyttäjän kannalta ongelmaksi tämä muodostuu salasanojen uudelleen käyttämisen vuoksi, sillä nyt salasana, joka on sama sekä pienemmässä vähemmän tärkeässä palvelussa ja suuremmassa palvelussa ovat nyt hyökkääjän tiedossa. Usein miten, kun salasanoja varastetaan, ne paketoidaan useiden tuhansien salasanojen ja niihin sopivien käyttäjätunnuksien paketeiksi ja ne myydään eteenpäin verkon pimeillä markkinoilla ostajille. (Peltomäki & Norppa, 2015). Käyttäjällä ei ole realistisia mahdollisuuksia käytettävyyden ja muistamisen kannalta pyrkiä pitämään yllä useita salasanoja ja tästä syystä näytätäkin siltä, että käyttäjät turvautuvat noin kuuden salasanan käyttämiseen, joten niiden kaikkien vuotaminen on myös todellinen uhka. (Brown yms., 2004). Usein miten, mikäli käyttäjän tietojen luottamuksellisuus on menetetty, huomataan se vasta sitten kun on liian myöhistä. Organisaatioiden osalta tietomurron huomaamiseen menee tutkimusten mukaan 69 – 197 päivää (IBM, 2018), mutta yksilöiden osalta vastaavaa lukua ei ole saatavilla. Todennäköisesti kuitenkin yksilö huomaa tietojen tulleen käytetyksi väärin siinä vaiheessa, kun hänelle alkaa saapumaan ilmoituksia erääntyneistä laskuista sekä luottohäiriömerkinnän vaarasta, jolloin käytännössä potentiaalinen hyökkääjä on ehtinyt käyttämään uhrin henkilöllisyyttä useissa eri paikoissa. Tähän ei ole myöskään nykyisellään mitään järkevää tapaa suojautua tietojen menetyksen jälkeen, sillä useissa palveluissa käyttäjänä täytyy pystyä kirjautumaan johonkin palveluun tai käyttäjästä pitää olla saatavilla tietoja kuten sosiaaliturvatunnus ja kotiosoite. Nämä tiedot ovat myös olleet useissa eri tietovuodoissa ja niiden saaminen on potentiaalisen hyökkääjän näkökulmasta varsin helppo tapa, kun uhri voi valikoitua sattuman varalta sen mukaan mitä tietoja on mahdollista saada

käsiin. Tällaisia rikoksia tehtailevat kyberrikollisista usein, miten ammattirikolliset. (Peltomäki & Norppa, 2015). Erilaiset tavat saada tietoja luottotietojen kyselyistä, kuten asiakastiedon omatieto palvelu voivat tässä tapauksessa toimia eräänlaisina aikaisen varoituksen järjestelminä, joissa käyttäjää saa tiedon mahdollisten omien tietojen käytöstä jo aikaisessa vaiheessa. (Asiakastieto, 2020).

Käytettävyyden näkökulmasta, kun tarkastellaan suorituskykyä, tavan käytettävyyttä ja siitä koituvaa vaivaa on optimitilanteessa, jossa käyttäjä muistaa salasanansa käytettävyys korkea. Käyttäjän tulee kirjatuessaan ainoastaan kirjoittaa salasana sekä käyttäjätunnus ilman ulkoisia palveluita, jolloin kirjautuminen on suoraviivaista ja nopeaa. Optimaalisessa tilanteessa käyttäjä muistaa salasanansa kaikissa tilanteissa ja kirjautumiseen ei liity suurempaa vaivaa. Suorituskyky kuitenkin laskee tilanteessa, kun käyttäjän on keksittävä uusi salasana syystä tai toisesta. Tällöin käyttäjät usein päätyvät samaan salasanaan tai salasanaan, joka on ainakin hyvin lähellä jo kertaalleen käytössä olevaa. Käytettävyyden ja koetun vaivan osalta käyttäjälle salasanan muistamisesta ei synny merkittävää uutta vaivaa ja salasanan kirjoittaminenkin on käyttäjälle todennäköisesti hyvin rutinoitunut ja nopea prosessi. Lisäksi mikäli käyttäjällä on käytössä henkilökohtainen työasema, johon ei hyvien tietoturva käytänteiden mukaisesti ole muilla pääsyä on tällöin käyttäjän mahdollista asettaa selain muistamaan kirjautuminen palveluihin, jolloin salasanan kirjoittaminen jatkuvasti ei ole välttämätöntä. Tällöin kuitenkin, mikäli käyttäjä unohtaa lukita työasemansa, on hänen palveluihinsa potentiaalisella fyysisellä hyökkääjällä pääsy. Sisäisen hyökkääjän mahdollisuus kuulostaa usein pieneltä, mutta tutkimusten mukaan n. 1/3 hyökkäyksestä tapahtuu sisäisen hyökkääjän toimesta, 1/3 hyökkäyksestä on ulkopuolisen toteuttama ja 1/3 hyökkäyksestä jää epäselväksi oliko kyseessä sisäinen vai ulkoinen toimija. (Mathew, Petropoulos, Ngo, & Upadhyaya, 2010). Tästä syystä on tärkeätä muistaa, ettei selaimen tulisi kirjautumista kaikkiin palveluihin. Käyttäjän kokeman vaivan osalta salasanan kirjoittaminen ei juurikaan kasvata koettua vaivaa, mutta mikäli salasanaa ei muisteta, koetaan se hyvin vaivalliseksi.

Ehdottomasti suurin osa käyttäjistä hallinnoi salasanojaan muistamalla. Tähän myös todennäköisesti ajaudutaan aikojen saatossa, kun parempia tapoja ei ole helposti tarjolla ja kirjautumista vaativien palveluiden määrä kasvaa jatkuvasti. Näyttää siltä, että salasanan muistamiseen mielessä vahvuudet ovat käytettävyydessä ja salasanojen saatavuudessa. Kirjautuminen voidaan optimitilanteessa toteuttaa hyvin nopeasti ja salasanat ovat aina käyttäjän mielessä mukana. Kirjautuminen on tällöin helppoa ja nopeata. Mikäli käyttäjä kykenee muistamaan jonkin logiikan kautta kaikki salasanansa ja pystyy tätä kautta välttämään salasanojen uudelleen käyttämistä, on tällöin käyttäjän salasanat turvallisuuden ja käytettävyyden näkökulmasta hyvin hoidossa ja näin ollen muistaminen on käyttökelpoinen ja turvallinen tapa hallita salasanoja. Käytännössä näin kuitenkaan käytännössä missään tilanteessa ei ole. Henkilöt valitsevat itseensä helposti liitettäviä salasanoja, uudelleen käyttävät niitä sekä varioivat salasanoja helposti tunnistettavissa kaavoissa. (Brown yms., 2004). Lisäksi käyttäjiltä salasanojen huijaaminen näyttää olevan kiinni huijaajan motivaatiosta saada käyttäjästä puserrettua salasana ulos erilaisin sosiaalisen huijauksen keinoin. Salasanojen uudelleen käyttö asettaa myös käyttäjän salasanat huonoiten tietoturvaa hoitavan

palvelun varaan, jolloin tietomurron uhriksi joutuminen on käytännössä enemmän kiinni tuurista, kun hyvästä tietoturvan tasosta. Käyttäjät myös unohtavat jatkuvasti salasanojaan, joka asettaa palveluiden saatavuuden ainakin hetkellisesti ongelmalliseksi. Usein käyttäjä myös pakotetaan vaihtamaan salasanaa, jolloin käyttäjän salasanan taso usein huononee uusinta prosessin myötä. Mikäli käyttäjät pystyisivät muistamaan satunnaisesti generoituja salasanoja olisi tietoturvan taso tällöin korkeampi. Tutkimusten mukaan kuitenkin, käyttäjien on vaikeata muistaa satunnaisesti generoituja salasanoja, joten salasanojen muistamiseen on kehitettävä jokin logiikka. Näyttää siltä, että salasanojen mielessä muistaminen on keskinkertainen tapa hallinnoida salasanoja, jossa salasanojen saatavuus on korkea muistamisen ansiosta, luottamuksellisuus kohtalainen, niin kauan kun palveluista salasanat eivät pääse vuotamaan ja muuttumattomuus kohtalainen, olettaen käyttäjän pystyvän muistamaan salasanana. (Yuan, Han, & Hu, 2008).

3.2 Salasanojen hallinta paperilla

Salasanojen hallinta paperilla tarkoittaa tilannetta, jossa käyttäjä kirjoittaa salasanansa jollekin reaalimaailmassa olevalle paperiselle alustalle ja säilyttää salasanojaan näin. Yleisesti tätä tapaa käytetään tukemaan salasanan muistamista ja usein paperille salasana kirjoitetaan, kun pelätään, että salasana unohdetaan. (Grawemeyer & Johnson, 2011). Salasanojen ylös kirjoittamista käytetään myös usein sellaisissa tilanteissa, kun esimerkiksi työasema on jaettu useamman henkilön kesken ja siihen kirjaudutaan yhdellä käyttäjätunnus- ja salasanaparilla. Tämä ajaa tilanteeseen, jossa kirjautuminen on käytännössä hyödytöntä, sillä kuka tahansa riippumatta käyttöoikeuksista voi kirjautua laitteeseen sisälle tarvittaessa. Salasanan kirjoittamista harrastavat myös henkilöt, jotka pelkäävät salasanansa unohtumista, jotka myöskin mitätöivät kirjautumisen merkityksen toimimalla näin. Usein miten myös salasana, vaikka se on kirjoitettu ylös, on huonosti muodostettu ja se on jokin henkilölle itselleen merkityksellinen asia, lähisukulainen kuten lapsen nimi, lemmikkieläin tai puolisoon viittaava asia. (Brown yms., 2004).

Tietoturvan näkökulmasta salasanan ylös kirjoittaminen on saatavuuden kannalta näennäisesti hyvä, kun salasanan sisältä paperi on saatavilla. Näin kuitenkaan ei aina ole ja saatavuus voidaan mitätöidä vain sillä, että käyttäjä ja paperi ovat eri sijainnissa tai paperi on syystä tai toisesta hävinnyt tai tuhottu. Tästä syystä saatavuus salasanoja ylös kirjoitettaessa on kaikki tilanteita katsoen heikko, sillä ennemmin tai myöhemmin tulee käyttäjälle eteen tilanne, jossa hän on lukinnut itsensä ulos. Muuttumattomuus salasanoissa on kirjoittamisen kannalta erinomainen, sillä kun salasana on kirjoitettu paperille, on hyvin epätodennäköistä, että se muuttuisi. Muuttumattomuuden ollessa erinomainen olisi käyttäjällä mahdollisuus myös siirtyä tilanteeseen, jossa hänen ei tarvitsisi itse muistaa salasanaansa vaan hän voisi luottaa lapulla oleviin. Tällöin salasanat voisivat olla aidosti uniikkeja jokaisessa palvelussa, mutta tämä kuitenkin ajaa ongelmaan siinä, että käyttäjät yleisesti keksivät hyvin suppeasta skaalasta salasanoja.

Luottamuksellisuus on näennäisesti hyvä, niin kauan kun salasanat sisältävä paperi on tallessa. Kuitenkin salasanat ovat selkotekstinä tällä paperilla usein, miten ja tällöin ne ovat helposti varastettavissa niin, että käyttäjä ei itse edes huomaa niiden tuleen varastetuiksi. Tämä luonnollisesti vaatii potentiaalisen hyökkääjän fyysisen pääsyn käyttäjän lähelle, mutta 1/3 hyökkäyksestä tulee tutkimusten mukaan sisäisen toteuttajan toimesta, jolloin on todennäköistä, että näin voisi päästä käymään. (Mathew yms., 2010). Tästä syystä luottamuksellisuus salasanojen ylös kirjoittamisessa on heikko.

Käytettävyyden näkökulmasta salasanan hallinta paperille kirjoittamalla on heikko, sillä kaikissa tilanteissa käyttäjä joutuu kirjoittamaan salasanan itse kirjautuessaan salasanakenttään. Mitä vaikeampi ja harvemmin käytetty salasana on kyseessä, sitä todennäköisempää on, että käyttäjä kirjoittaa jonkin merkin väärin ja tätä kautta kirjautuminen viivästyy. Käytettävyys on samoista syistä myös heikko, sillä käyttäjä joutuu itse kirjoittamaan salasanan ja käytännön esimerkit osoittavat, että käyttäjälle tulee virheitä saman näköisten merkkien kesken. Osa kirjaimista muistuttavat eri käsialalla toisiaan ja ne aiheuttavat ongelmia kirjautumisessa. Käyttäjä ei myöskään välttämättä itse tajua kirjoittaneensa merkkiä väärin, jolloin käyttäjän ongelmaksi muodostuu se, ettei hän tiedä missä kohtaa kirjautumista mentiin vikaan. Käyttäjän kokema vaiva on näin merkittävä. Toisaalta on, jos salasanat ollaan valmiita tallentamaan luettavaan muotoon, on tällöin perusteltu syy kysyä, että miksi tällöin ei käytettäisi salasanan hallintaohjelmaa, joka vastaisi tuetuksiltaan samaa mutta vaan digitaalisessa muodossa. (Adams, Sasse, & Lunt, 1997).

Salasanojen ylös kirjoittamisen vahvuutena on, että niitä ei tarvitse käyttäjän itse muistaa ja se mahdollistaa periaatteessa salasanojen uudelleen käyttämisen vähentämisen, mikäli jokaiseen palveluun keksitään oma salasana. Sen heikkoutena on kuitenkin saatavuus, sillä on erittäin todennäköistä, että saatavuus menetetään ainakin jossain vaiheessa, kun ei ole saatavilla paperia, johon salasanat on kirjoitettu ylös. Heikkoutena voidaankin mainita todennäköisesti saatavuuden vaarantuminen ja kasvanut vaiva salasanojen kirjoittamisen myötä. Uhkana salasanojen paperille kirjoittamisessa on se, että paperi varastetaan, se hukkuu tai se kopioidaan käyttäjän tietämättä. Tämä on mahdollista sillä salasanat ovat usein, miten selkotekstinä kirjoitettuna tähän muistioon. Käyttäjä saattaa myös itse hukata tai muuten hävittää muistion, jolloin luottamuksellisuus ja pääsy salasanoihin vaikeutuu. (Adams yms., 1997).

Salasanojen paperille kirjoittamista ei voida pitää käytettävyyden, turvallisuuden ja koetun vaivan kautta kovinkaan hyvänä tapana. Optimi tilanteessa ainut huono ominaisuus on se, että ne joudutaan käsin kopioimaan paperilta salasana kenttään, mutta käytännössä käyttäjän itsensä on niin helppo vaarantaa saatavuus ja luottamuksellisuus, ettei tätä tapaa voida suositella.

3.3 Salasanojen hallinta ohjelmallisesti

Nykyisin useat tahot, kuten Viestintävirasto (2019) ja muut tietoturva-alalla toimivat organisaatiot suosittelevat salasanojen tallentamista erilaisiin digitaalisiin

salasanan hallintaohjelmiin. Salasanan hallintaohjelmat ovat tietokoneelle tai kolmannen osapuolen pilvipalveluun asennettuja salasanan hallintaohjelmia, johon on tarkoitus tallentaa käyttäjän salasanat. Kun käyttäjä tarvitsee salasanojaan, pääsee käyttäjä niihin käsiksi kirjoittamalla pääsalasanansa, joka toimii yleensä myös salauksen avaimena, jolla voidaan purkaa vahva salaus, jolla salasanaholvi on salattu. Käyttäjän tarvitsee siis muistaa ainoastaan yksi salasana, jolla hän pääsee käsiksi kaikkiin salasanan hallintaan tallennettuihin salasanoihin. Näin ollen käyttäjän ei välttämättä tarvitse muistaa itse salasanojaan, sillä salasanan hallintaohjelma muistaa ne käyttäjän puolesta. (Lastpass, 2020a). Käytännössä käyttäjän näkökulmasta salasanan hallintaprosessi toimii niin, että käyttäjä kirjautuu laitteella salasanan hallintajärjestelmään kirjoittamalla pääsalasanansa, tämä salasana purkaa ohjelmallisesti salasanojen salauksen ja käyttäjä pääsee käsiksi tallennettuihin salasanoihin ja muihin tietoihin. Kun käyttäjä haluaa kirjautua palveluun, haetaan salasana ja käyttäjätunnus salasanan hallinnasta ja liitetään palvelun salasanakenttään. Useissa palveluissa, jotka toimivat pilvipohjaisesti on myös tarjolla erilaisia selain lisäosia, jotka täydentävät salasanan automaattisesti kirjautumislomakkeeseen. Käyttäjä voi siis kirjautua palveluun ilman, että hänen tarvitsee käsin kirjoittaa salasanaa ja näin ollen, koska käyttäjä hakee salasanansa salasanan hallintaohjelmasta, ei käyttäjän edes tarvitse olla tietoinen siitä mikä salasana on sisällöltään. Selainlisäosien osalta on kuitenkin huomattava, että ne saattavat kasvattaa tietoturvan kannalta kohonnutta riskiä, sillä selaimia vastaan hyökkääminen on potentiaalinen riski. (Silver, Jana, Boneh, Chen, & Jackson, 2014). Salasanan hallintaohjelmat myös usein sisältävät mahdollisuuden generoida salasanoja rekisteröitymisen yhteydessä. Tämä tarkoittaa sitä, että kun käyttäjä on rekisteröitymässä palveluun, tarjoaa salasanan hallintajärjestelmä käyttäjälle mahdollisuutta generoida salasana ja tallentaa se suoraan salasanan hallintajärjestelmään. Hallintaohjelmien osalta voidaan myös kasvattaa salasanojen entropiaa lisäämällä niihin mukaan erikoismerkkejä, numeroita sekä eri kirjaisinkokoja. (Yuan yms., 2008). Salasanan generointi ehkäisee salasanan uudelleen käyttöä sekä salasanan ollessa täysin sattumanvarainen ja merkityksetön merkkijono, on sen ohjelmallinen murtaminen käytännössä mahdotonta. Salasanan hallintaohjelmat jaotellaan usein kahteen pääluokkaan, jotka ovat pilvipohjainen ja paikallinen salasanan hallintajärjestelmä. Pilvipohjaisena esimerkkinä tullaan käyttämään laajasti käytössä olevaa Lastpass-palvelua ja paikallisesta tullaan käyttämään esimerkkinä KeePass-palvelua, joka on myös laajasti käytössä. Pilvipohjaisella järjestelmällä tarkoitetaan salasanan hallintaa, jossa käyttäjän salasanat ovat tallennettuna kolmannen osapuolen palvelimelle, josta ne ladataan sille laitteelle, jolla käyttäjä niitä tarvitsee. Pilvipohjaisen salasanan hallintajärjestelmän selkeänä etuna on salasanojen saatavuus kaikissa tilanteissa, kun internet on saavutettavissa sekä salasanojen helppo jakaminen tarvittaessa toiselle henkilölle. Pilvipohjaisen salasanan hallintajärjestelmän käytössä selkeä heikkous on, että salasanat ovat tallennettuna muualle, kuin käyttäjän omalle laitteelle ja näin ollen tietoturvassa joudutaan luottamaan palvelun tarjoajaan. Paikallisella salasanan hallintajärjestelmällä tarkoitetaan salasanan hallintajärjestelmää, jossa salasanat ovat tallennettuna käyttäjän oman laitteen muistiin ja näin ollen tietoturva on käyttäjän vastuulla. Paikallisen salasanan hallintajärjestelmän etuna on salasanojen tietoturvan

parantuminen, sillä ei ole tarvetta luottaa kolmanteen osapuoleen. Heikkoutena on mahdolliset tilanteet, joissa salasanat sisältävä laite ei ole saatavilla tai pääsy sille on estynyt jostain muusta syystä. (Gasti & Rasmussen, 2012).

Tietoturvan näkökulmasta salasanan hallintajärjestelmissä saatavuus on erinomainen, kun tarkastellaan molempia eri hallintatapoja, kunhan lokaalissa salasanan hallintajärjestelmässä salasanat ovat saavutettaessa sillä laitteella, jolla niitä tarvitaan. Tarkasteltaessa erikseen pilvipohjaisen salasanan hallinnan saatavuus on erinomainen ja paikallisen keskitasoa. Pilvipohjaisen salasanan hallinnan selkeänä etuna on, että salasanat ovat internetin välityksellä aina saavutettavissa laitteesta riippumatta. Paikallisessa hallinnassa kääntöpuolena on salasanojen saatavuus ainoastaan, kun laite, jossa tietokanta sijaitsee, on saavutettavissa. Muuttumattomuuden ja salasanojen unohtamisen kannalta salasanojen hallinnassa on molemmissa erinomainen, sillä salasanan hallintaohjelma pitää huolta siitä, että salasanat pysyvät muuttumattomina ja tallessa. Luottamukselliseen osalta paikallisessa hallintajärjestelmässä salasanojen luottamuksellisuus on erinomainen ja pilvipohjaisessa hieman heikompi. Tämä johtuu siitä, että pilvipohjaisessa hallinnassa salasanojen luottamuksellisuus on palveluntarjoajan käsissä ja käyttäjä joutuu luottamaan johonkin kolmanteen osa puoleen. Käytännössä tämä tarkoittaa sitä, että käyttäjän on valittava palvelu, johon hän luottaa huolella ja mikäli palveluun voidaan luottaa, on silloin myös pilvipohjaisen salasanan hallinnan luottamuksellisuus erinomainen. (Gasti & Rasmussen, 2012). Pilvipohjaisen salasanan hallintajärjestelmän tietoturvan tasoa voidaan myös parantaa ottamalla käyttöön kaksivaiheinen tunnistaminen, jolloin käyttäjällä on esimerkiksi älypuhelimessan useaan kertaan minuutissa vaihtuva kertakäyttöinen numerosarja, jonka käyttäjä syöttää salasanan ja käyttäjätunnuksen lisäksi. Tällöin voidaan todeta, käyttäjän käyttävän vahvaa tunnistamista ja tällöin myös salasanan pilvipohjaisen salasanan hallintajärjestelmän tietoturva on korkeammalla tasolla.

Käytettävyyden ja suorituskyvyn näkökulmasta salasanan hallintaohjelman käyttö lisää yhden ylimääräisen askeleen kirjautumiseen, mikäli mitään selainlaajennusta tai vastaavaa ei käytetä. Kuitenkin, selainlaajennusta käytettäessä salasanan hallintaohjelman suorituskyky on kirjautumista ajatellen erittäin hyvä, sillä kun käyttäjä on selaimen käynnistäessään kirjautunut salasanan hallintaan, täyttää selainlaajennus käyttäjälle oikeat tunnukset salasana kenttään valmiiksi ja käyttäjälle ei jää muuta tehtävää, kun painaa kirjaudu. Yleisesti salasanan hallintajärjestelmä poistaa käyttäjältä tarpeen muistaa mitään muita salasanoja, paitsi sen yhden, jolla käyttäjä kirjautuu salasanan hallintajärjestelmään. Mikäli käyttäjä ei käytä selainlaajennusta on hänen käytävä kopioimassa salasana hallintaohjelmasta, joka sinänsä verrattuna salasanan muisteluun ja kirjoittamiseen nähden on vaivattomampaa tai vähintäänkin yhtä vaivalloista. Salasanojen hallinta tarjoaa käyttäjälle mahdollisuuden generoida rekisteröitymisen yhteydessä uniikkeja merkityksettömiä merkkijonoja salasanoiksi, joten silloin käyttäjältä säästyy aikaa sekä vaivaa. (LogMeIn, 2020a). Käytettävyyden osalta salasanojen hallintaohjelman valinnassa tehdään kriittinen päätös siitä, onko salasanan hallintaohjelma käytettävyydeltään hyvä. Mikäli käyttäjä valitsee salasanan hallintansa oikein, on tällöin salasanojen ja kirjautumisen hallinta parempi verrattuna edellisiin tapoihin. Tämä perustuu siihen, että käyttäjältä poistetaan vaiva, joka

liittyy muihin tapoihin hallita salasanoja. Käyttäjän kokema vaiva madaltuu myös siitä syystä, että käyttäjän ei enää tarvitse itse muistaa eikä kirjoittaa salasanojaan kirjautumisen yhteydessä, sillä salasanan hallintajärjestelmä hoitaa tämän käyttäjän puolesta. Käyttäjän tarvitsee ainoastaan muistaa yksi vahva salasana, jolla käyttäjä kirjautuu salasanan hallintajärjestelmäänsä. Käyttäjän osalta vaiva saattaa kasvaa merkittävästi, mikäli käyttäjä unohtaa salasanansa salasanan hallintaan, sillä silloin palvelu, joka huolehtii salauksesta ja tietoturvastaan riittävästi, ei pysty salasanoja enää palauttamaan, sillä salasanan holvin avaamiseen tarvitaan vanha salasana.

Salasanan hallintajärjestelmän käyttöönottamisesta edut käyttäjälle tulevat seuraavista tekijöistä. Käyttäjän ei enää tarvitse itse muistaa salasanoistaan muita paitsi yksi, jolla kirjaudutaan salasanan hallintajärjestelmään. Näin ollen käyttäjän kokema vaiva laskee. Käyttäjän ei itse tarvitse muistaa salasanojaan, joten käyttäjän salasanojen ei tarvitse enää olla sanoja vaan ne voivat olla merkityksettömiä merkkijonoja, joiden pituus voi olla ihmisen käsiteltäväksi liikaa, kuten esimerkiksi 32 merkkiä, mutta koneille ei ole merkitystä mikä salasanojen pituus on. Tietoturvan näkökulmasta käyttäjälle etuna on se, että käyttäjä voi generoida uniikin salasanan jokaiseen palveluun, joka on samalla myös erittäin turvallinen sisältäen kaikki mahdollisia merkkikokoja, erikoismerkkejä, numeroita ja näin ollen salasana voi olla näistä yhdistelmänä generoitu merkkijono. (LogMeIn, 2020a). Käyttäjän kokema etu on myös se, että mikäli jostakin palvelusta salasana vuotaa ulos on se edelleen kuitenkin vain pääsyavain tähän kyseiseen palveluun, jolloin vain tämän palvelun salasana on vaarantunut ja muiden palveluiden salasanat ovat edelleen turvassa, koska salasanaa ei ole uudelleen käytetty. Toisaalta salasanoja käsitellään nykyisin verkkopalveluissa usein miten salatussa muodossa ja täysin generoidun salasanan palauttaminen tästä salauksesta ei käytännössä ole mahdollista ja vaikka se olisikin mahdollista, näyttää se silti edelleen potentiaaliselle hyökkääjälle salatulta, johtuen satunnaisuudesta. Hyökkääjälle järkevämpää on kohdistaa aika, vaiva ja resurssit huonommin salattuihin salasanoihin, joita palveluista löytyy edelleen valtaosa. Heikkoutena salasananhallinta järjestelmän käytössä on se, että salasanat ovat yhdessä paikassa ja mikäli tämä päätyy hyökkääjän käsiin, on hyökkääjällä käytännössä pääsy kohteen kaikkiin palveluihin. Tämä on kuitenkin jo tällä hetkellä salasanan uudelleen käyttämisen vuoksi sama tilanne. On myös epätodennäköistä, että käyttäjän salasanan hallinta järjestelmä saataisiin murrettua, sillä salasanat on salattu käyttäjän omalla avaimella kaikissa palveluissa, jotka hoitavat tietoturvaansa järkevästi ja vastuullisesti. Tästä esimerkkinä voidaan käyttää Lastpass-palvelua, jossa salasanat salataan ja avataan ainoastaan käyttäjän omassa laitteessa ja ainoastaan salatut tiedot ovat tallessa Lastpassin palvelimella, jolloin niiden avaaminen ei ole mahdollista ilman käyttäjän omaa salasanaa. (Lastpass, 2020a).

Pilvipohjaisissa salasanan hallintajärjestelmien osalta ei kuitenkaan voida vähätellä sitä, että salasanat ovat kolmannen osapuolen tallennusvälineillä ja tästä muodostuu ehdottomasti luottamussuhde käyttäjän ja palvelun tarjoajan välille. Paikallisissa salasanan hallintajärjestelmissä sama vastuu on käyttäjällä itsellään. Salasanan hallintajärjestelmien käyttöön liittyvät uhat liittyvät palveluntarjoajan teknisiin haavoittuvuuksiin, väärinkäytöksiin sekä käyttäjän omiin inhimillisiin virheisiin. Salasanan hallintajärjestelmissä, kuten kaikissa

ohjelmistoissa on tavattu teknisiä haavoittuvuuksia, joiden avulla potentiaalinen hyökkääjä saattaa saada pääsyn tietoihin tai ainakin ensimmäisen jalansijan, jonka avulla käyttäjän tiedot saattaisivat olla varastettavissa. Tällaisia teknisiä haavoittuvuuksia on löydetty esimerkiksi selainlaajennuksista. (Silver yms., 2014). Näiden hyödyntämisessä kuitenkin salasanan palvelun tarjoajat ovat nopeasti korjanneet tekniset haavoittuvuudet, mutta niiden mahdollisuutta ei voi sulkea pois. Toisaalta käyttäjä saattaa itse virheellisesti luovuttaa pääsalasanansa eteenpäin tai muuten oman virheen kautta edes auttaa hyökkääjää pääsemään käsiksi tietoihin. Käyttäjä saattaa myös lukita itsensä ulos salasanan hallintajärjestelmästä, jolloin pääsy tietoihin estyy ja mikäli käyttäjä ei muista salasanaansa, on tällöin pääsy salasanoihin estynyt, sillä salausta ei voi purkaa ilman salasanaa. (Brainard yms., 2006).

Yhteenvetona salasanan hallintajärjestelmistä voidaan todeta, että niiden käyttöä suositellaan laajasti. Tällaisen suosituksen ovat antaneet Suomessa esimerkiksi viestintäviraston mukaan käyttää jotakin salasanan hallintaohjelmaa. (Viestintävirasto, 2019). Salasanan hallintajärjestelmällä tarkoitetaan ohjelmallista tapaa tallentaa salasanat joko käyttäjän omalle levylle tai palveluntarjoajan pilvipalveluun. Pilvipohjaisessa salasanan hallintajärjestelmässä hyvinä puolina on jatkuva saatavuus ja kääntöpuolena tietoturvan luottaminen kolmannen osapuolen hoidettavaksi. Paikallisessa salasanan hallintajärjestelmässä etuna on kohonnut tietoturva, sillä käyttäjän ei tarvitse luottaa kolmannen osapuolen palveluun ja kääntöpuolena on kuitenkin salasanojen saatavuuden aleneminen tilanteissa, joissa pääsyä salasanan hallintaohjelmalle ei ole. Molempien hallintatapojen osalta salasanat pysyvät muuttumattomina, sillä ohjelmallisesti niiden käsittelyssä ne eivät pääse muuttumaan tai unohtumaan. Käytettävyyden näkökulmasta salasanan hallintaohjelmat tarjoavat käyttäjälle vapauden salasanojen muistamisesta, sillä käyttäjän tarvitsee muistaa enää yksi salasana. Käyttäjän ei tarvitse enää kirjautumisen yhteydessä itse kirjoittaa salasanaa, sillä se voidaan liittää salasanan hallintajärjestelemästä. Käyttäjän ei tarvitse itse keksiä rekisteröitymisen yhteydessä salasanaa, sillä valtaosa salasanan hallintajärjestelmistä generoi käyttäjälle tarvittaessa uuden salasanan käyttäjän asettamien ehtojen perusteella. Käyttäjä voi myös generoida todella turvallisia pitkiä salasanoja, jotka ovat merkityksettömiä merkkijonoja, jotka koostuvat kaikista mahdollisista merkeistä, sillä käyttäjän ei tarvitse itse niitä muistaa tai kirjoittaa. (LogMeIn, 2020a). Käyttökokemuksen näkökulmasta käyttäjän käyttökokemus todennäköisesti paranee ja helpottuu, sillä salasanan hallintajärjestelmä hoitaa sellaiset tehtävät, jotka aiemmin ovat vaatineet käyttäjältä vaivaa. Yleisesti ottaen salasanan hallintajärjestelmät nostavat käyttäjän salasanojen tietoturvan tasoa ja parantavat käyttökokemusta. Näyttää siltä, että salasanan hallintajärjestelmän käyttöönotto on tällä hetkellä peruskäyttäjän näkökulmasta järkevää tehdä.

3.4 Salasanojen hallintatapojen vertailu

Salasanojen hallintajärjestelmien vertailussa vertaillaan salasanan hallintajärjestelmiä käytettävyydessä suorituskyvyn, sekä vaivan osalta ja tietoturvassa saatavuuden, luottamuksellisuuden ja muuttumattomuuden kannalta. (Fruhlinger, 2020). Vertailuasteikkona tullaan käyttämään laadullista asteikkoa, joka alkaa huonosta ja päättyy erittäin hyvään. Vertailua asteikossa on viisi porrasta, erittäin huono, huono, keskitaso, hyvä ja erittäin hyvä. Vertailuasteikon arvot eivät ole absoluuttisia arvoja vaan niillä pyritään antamaan helposti vertailtavaa kuva salasanan hallintajärjestelmistä ja niitä käytetään kappaleen lopussa olevassa taulukossa.

Muistamisen osalta salasanojen hallinnan suorituskyky on keskitasoa, sillä käyttäjän on itse muistettava ja kirjoitettava salasanat. Vaiva on muistamisessa pieni, sillä käyttäjän salasanat ovat aina helposti saatavilla ja käyttäjän tehtäväksi jää itse niiden kirjoittaminen salasanakenttään. Tietoturvan osalta salasanojen saatavuus on keskitasoa, sillä käyttäjät usein unohtavat salasanoja ja käyttäjien unohtaminen aiheuttaa saatavuuteen laskun. Luottamuksellisuus on muistamalla optimitilanteessa hyvä, mutta kuitenkin käytännössä tutkimusten mukaan salasanojen muistaminen on mahdollista vain uudelleen käyttämällä samaa salasanaa, jonka takia salasanojen luottamuksellisuus on huono. (Brown yms., 2004). Käyttäjät myös unohtavat jatkuvasti salasanojaan tai unohtavat logiikan, jonka perusteella muuttavat salasanojaan, joten muuttumattomuus muistamisessa on myös huono. Salasanojen muistaminen paperilla on yleisesti käytetty, mutta hyvin varsin huono tapa verrattuna muihin saatavilla oleviin tapoihin. (Stobert & Biddle, 2018).

Salasanojen muistaminen paperilla on yleisesti käytetty tukikeino salasanojen muistamisen tukemiselle. Salasanojen ylös kirjoittaminen on suorituskyvyltään huono, käyttäjän on kirjoitettava salasanat käsin paperilta salasanalomakkeeseen, tämä vie luonnollisesti aikaa sekä vaivaa. (Renaud, Kotze, & Barnard, 2001). Näin olleen salasanojen hallitseminen paperilla on suorituskyvyltään melko huono ja vaiva, jota vaaditaan sen käsittelemiseen, on keskitasoa. Tietoturvallisuuden näkökulmasta salasanojen saatavuus on huono, sillä käyttäjä ajautuu todennäköisesti ennemmin tai myöhemmin tilanteeseen, jossa salasanat sisältävä paperi on eri paikassa, kun käyttäjä. Luottamuksellisuuden osalta paperilla salasanojen muistaminen on vaihtoehtona huono sillä, salasanat ovat usein selkotekstinä paperilla. Potentiaalisen hyökkääjän toki tulee päästä fyysisesti samaan tilaan, jossa paperi sijaitsee, mutta tämä ei ole mahdotonta sillä tutkimusten mukaan kolmannes hyökkäyksistä on toteutettu organisaation sisäisen hyökkääjän toimesta. (Mathew yms., 2010). Salasanojen muuttumattomuus on paperilla hyvä, sillä on epätodennäköistä, että salasanat unohtuisivat tai ne muuttuisivat paperilla säilöttynä.

Salasanojen muistamista digitaalisesti vertaillaan kahdella eri tavalla, jotka ovat salasanojen hallinta paikallisella salasanan hallintajärjestelmällä ja pilvipohjaisella salasanan hallintajärjestelmällä. Näiden erona, kuten aiemmin on jo mainittu on, että paikallisessa salasanat hallitaan käyttäjän henkilökohtaisen laitteen kiintolevyllä ja pilvipohjaisella palveluntarjoajan pilvipalvelimella. Nämä

asettavat salasanan hallintajärjestelmät eri asemaan käytettävyyden ja tietotuvan näkökulmasta. (Gasti & Rasmussen, 2012).

Paikallisessa salasanan hallintajärjestelmässä suorituskyky on hyvä, sillä käyttäjällä on tallennettuna salasanat työasemansa kiintolevylle ja niiden saaminen sieltä on samalla laitteella helppoa ja nopeata. (Keepass, 2020). Käyttäjä voi myös asentaa salasanan hallintajärjestelmään liitännäisen selaimeen, jolla käyttäjä voi suoraan liittää salasanat ja käyttäjätunnukset automaattisesti kirjautumislomakkeeseen, joka säästää käyttäjältä vaivaa. Näin ollen näyttää siltä, että käytettävyyden osalta salasanojen hallinta paikallisella salasanan hallintajärjestelmällä on suorituskyvyltään hyvä ja käyttäjän kokema vaiva suhteessa muihin tapoihin on pieni. Tietoturvan näkökulmasta paikallisen salasanan hallintajärjestelmän kääntöpuolena on keskitason saatavuus, joka johtuu siitä, että käyttäjän paikallisen salasanan hallintajärjestelmän kääntöpuolena on se, että käyttäjän salasanat ovat aina saatavissa ainoastaan laitteella, jossa käyttäjän salasanat ovat tallessa. Tällöin saatavuuden osalta ennemmin tai myöhemmin ajaudutaan tilanteeseen, jossa käyttäjän salasanat eivät ole saatavilla, kun niitä tarvitaan. Luottamuksellisuuden osalta, koska käyttäjän salasanat ovat saatavilla ainoastaan käyttäjän laitteelta, ovat ne silloin erittäin hyvin turvassa ja niitä vastaan hyökkääminen vaatii käyttäjän pääsalasanan sekä paikallisen hyökkäyksen tai edistyneen haittaohjelman. Muuttumattomuuden osalta, salasanan hallintajärjestelmä pitää huolen siitä, etteivät salasanat pääse muuttumaan, joten salasanojen muuttumattomuus on erittäin hyvä. (KeePass, 2019).

Pilvipohjaisen salasanan hallintajärjestelmän osalta suorituskyky on hyvä sekä käyttäjän kokema vaiva pieni, sillä käyttäjän näkökulmasta käyttäjän täytyy kirjoittaa kirjautumisen yhteydessä ainoastaan yksi salasana ja tämän jälkeen salasanan hallintaohjelma pitää huolen käyttäjän salasanojen täydentämisestä. Tällöin käyttäjän kokema vaiva suhteessa ei digitaalisiin tapoihin hallita salasanoja on pieni ja suorituskyky hyvä. Tietoturvan näkökulmasta käyttäjän salasanat ovat saatavilla mistä tahansa maailmasta, millä tahansa laitteella, jossa on käytössä internet. Tällöin saatavuus on muihin tapoihin verrattuna erittäin hyvä. Saatavuuden korkea taso aiheuttaa tietojen luottamuksellisuuteen pienen alenemisen, sillä potentiaalisella hyökkääjällä on tällöin myös mahdollisuus hyökätä salasanan hallintajärjestelmään mistä tahansa maailmalta käyttäen hyödyksi palvelun korkeaa saatavuutta. Tätä vastaan voidaan kuitenkin taistella ottamalla käyttöön vahva uniikki salasana, jota ei käytetä missään muualla ja kytkemällä palvelun kaksivaiheinen tunnistaminen päälle, jolloin potentiaalisen hyökkääjän pitäisi saada käyttäjän laite sekä salasana. (Lastpass, 2020b). Tällöin hyökkäyksen hyökkäyspinta-ala jää auttamatta pieneksi ja hyökkäyksen toteuttaminen on erittäin vaikeata. Kuitenkin, on huomioitava, että luottamuksellisuus kokee tästä pienen aleneman ja tästä syystä luottamuksellisuus pilvipohjaisella salasanan hallintajärjestelmällä on hyvä, mutta ei erittäin hyvä. Salasanojen muuttumattomuuden osalta, tietokanta pitää huolen siitä, etteivät salasanat pääse muuttumaan ja tästä syystä digitaalisella salasanan hallinnalla salasanojen muuttumattomuus on erittäin hyvä. (Lastpass, 2020a).

Salasanojen hallintajärjestelmien osalta näyttää siltä, että perinteinen ja yleisesti eniten käytetty tapa, eli muistaminen antaa käyttäjälle pieniä etuja käytettävyydessä, mutta salasanojen tietoturvan näkökulma on varsin huono. (Brainard

yms., 2006). Tämä johtuu salasanojen uudelleen käyttämisestä sekä niiden heikosta muistamisesta. Salasanojen muistaminen paperilla on suorituskyvyltään sekä tietoturvaltaan varsi huono tapa, tarjoten ainoastaan etuuksia salasanojen muuttumattomuudella, sillä salasanat ovat paperilla muistissa. Digitaaliset hallintatavat näyttävät olevan parhaita vaihtoehtoja, kun verrataan käytettävyyttä ja tietoturvallisuutta. Salasanan hallintajärjestelmää päätettäessä on kuitenkin tehtävä selkeä valinta sen osalta, painotetaanko korkeaa saatavuutta vai korkeinta tietoturvan tasoa. Tällä perusteella käyttäjän tulee tehdä päätös sen osalta, onko hänelle tärkeintä saada salasanat aina käyttöön, kun on mahdollista.

Näyttää kuitenkin siltä, että salasanan hallintajärjestelmät sekä digitaalisesti, että paperilla antavat mahdollisuuden käyttää uniikkeja salasanoja jokaisessa palvelussa, jolloin niiden käyttäminen kasvattaa käyttäjän tietoturvan tasoa merkittävästi. Salasanojen muistaminen paperilla, on kuitenkin muiden osa-alueiden kannalta niin heikko, että on epätodennäköistä, että käyttäjä ottaisi niiden osalta niitä joka päiväiseen ja laajamittaiseen käyttöön. Digitaalisista salasanan hallinta järjestelmät tarjoavat käyttäjälle molemmilla osa-alueilla etuuksia. Käyttäjän tulee valita, haluaako hän painottaa korkeata tietoturvaa vai korkeata saatavuutta. Ajatellessa käyttäjää, joka käsittelee sensitiivistä materiaalia työssään, voidaan suositella ennemmin työkäytössä paikallista salasanan hallintajärjestelmää. Tämä siitä syystä, että käyttäjän tulee yleisesti käsitellä tietoja ainoastaan työnantajan laitteilla ja näin ollen saatavuutta ei tule olla muilta kuin tietyltä laitteelta, jolloin paikallinen salasanan hallinta on järkevää. Keskivertokäyttäjän näkökulmasta henkilökohtaisessa käytössä näyttää siltä, että nykymaailmassa, jossa käyttäjällä on tietokoneen lisäksi usein älypuhelin sekä mahdollisesti myös tabletti on käyttäjän päästävä usealla laitteella käsiksi samoihin salasanoihin ja yleensä mistä päin maailmaa tahansa, on tällöin peruskäyttäjän suositeltavaa käyttää pilvipohjaista salasanan hallintajärjestelmää yhdistettynä kaksi vaiheiseen tunnistamiseen. Käyttäjän kokema suorituskyky on tällöin hyvä ja koettu vaiva pieni, kun järjestelmää käytetään oikein. Tietoturvan näkökulmasta voidaan todeta, saatavuuden olevan erittäin hyvä, sillä palvelut ovat saavutettavissa internetistä mistä tahansa. Luottamuksellisuus on hyvä tai erittäin hyvä, mikäli käyttäjällä on käytössä kaksivaiheinen tunnistus ja valittu palvelu on yleisesti käytetty ja hyväksi todettu. Salasanojen muuttumattomuus on erittäin hyvä, sillä tietokanta pitää huolen salasanojen tallessa pysymisestä.

	Käytettävyys		**Tietoturva**		
	Suorituskyky	**Vaiva**	**Saatavuus**	**Luottamuksellisuus**	**Muuttumattomuus**
Muistamalla	Keskitasoa	Hyvä	Keskitasoa	Huono	Erittäin huono
Paperilla	Huono	Keskitasoa	Huono	Huono	Hyvä
Paikallinen hallinta	Hyvä	Hyvä	Keskitasoa	Erittäin hyvä	Erittäin hyvä
Pilvipohjainen hallinta	Hyvä	Hyvä	Erittäin hyvä	Hyvä	Erittäin hyvä

Taulukko 1 Salasanojen hallintatapojen vertailu

3.5 Turvallinen tapa hallita salasanoja käytettävyyden ja tietoturvan näkökulmasta

Aiemmin on tarkasteltu käyttäjän näkökulmasta salasanojen hallintaan liittyviä ongelmia ja etsitty niihin ratkaisuja käytettävyyden ja tietoturvan näkökulmasta. Käyttäjän näkökulmasta suurimmat uhat liittyvät siihen, että salasanoja vuotaa jatkuvasti palveluista verkkorikollisten tietoon ja käyttäjällä ei ole mahdollisuutta käytännössä suojautua tätä vastaan, sillä tällöin vastuu on salasanoja hallinnoivalla taholla, eli tässä tapauksessa palveluiden ylläpitäjillä. Käyttäjä itse voi suojautua salasanoihin liittyviä tietomurtoja vastaan parhaiten käyttämällä uniikkeja salasanoja jokaisessa palvelussa. (Hunt, 2020). Tällöin yksittäisen palvelun tietomurto vaikuttaa ainoastaan tähän kyseiseen palveluun ja yhdellä salasanalla ei päästä murtautumaan muihin palveluihin. Tämä luonnollisesti asettaa ongelmaksi salasanojen muistamisen, sillä käyttäjillä on nykyisin kymmeniä, jopa satoja eri palveluita, joihin heillä on käyttäjätunnukset. (LogMeIn, 2020b). Näyttää siltä, että ainoa järkevä tapa on hyödyntää jotain digitaalista salasanan hallintajärjestelmää. Tämä johtuu siitä, että se on käytännössä ainut käyttökokemuksen näkökulmasta oleva järkevä tapa hallinnoida salasanoja niin, että tietoturva pysyy riittävän korkealla tasolla. Kyseinen hallintamenetelmä myös pitää käyttökokemuksen on riittävän hyvänä, jotta käyttäjällä pysyy motivaatio käyttää palvelua. Toisin sanoen, kirjautumisen tulee olla helpompaa salasanan hallintajärjestelmällä kuin manuaalisesti. Saatavuuden näkökulmasta pilvipohjaisella salasanan hallintajärjestelmällä voidaan taata jatkuva saatavuus kaikissa tilanteissa ja pilvipohjainen salasanan hallintajärjestelmä yhdistettynä vahvaan tunnistamiseen näyttä olevan riittävän tietoturvallinen vaihtoehto vastaamaan suurimman osan käyttäjien tarpeita. Käyttäjän näkökulmasta siis käyttäjän tarvitsee enää muistaa yksi salasana, jolla käyttäjä kirjautuu salasanan hallintapalveluun ja sieltä käyttäjä kopioi salasanat niihin palveluihin, joihin hän niitä kulloinkin tarvitsee. (Lastpass, 2020a). Koska salasanat ovat muistissa salasanan hallintajärjestelmässä eikä käyttäjän niitä enää tarvitse muistaa, ei ole mitään syytä miksi nämä salasanat olisivat edes käyttäjälle kirjoitettavassa muodossa, sillä niitä hyvin harvoin tarvitsee kirjoittaa. Käyttäjä voi siis generoida jokaiseen palveluun pitkänkin, esimerkiksi 32 merkkiä pitkän merkityksettömän merkkijonon ja käyttää tätä salasanana. Tällainen 32 merkkiä pitkä merkkijono voi olla kussakin palvelussa eri ja käyttäjän ei ole mitään tarvetta uudelleen käyttää salasanoja, sillä niitä ei tarvitse enää muistaa. Käyttäjän käyttökokemusta voidaan parantaa erityisesti vielä asentamalla selaimeen lisäosa, jolla voidaan täydentää salasanat automaattisesti kirjautumislomakkeisiin, jolloin käyttäjän käyttökokemukseen liittyvää vaivaa voidaan myös merkittävästi madaltaa ja käyttäjän motivaatio käyttää salasanan hallintajärjestelmää on korkea, sillä kirjautuminen vie itseasiassa vähemmän aikaa ja vaivaa kun aiemmin. Toisin sanoen, peruskäyttäjän näkökulmasta, kun tarkastellaan tietoturvaa ja käytettävyyttä, on pilvipohjainen salasanan hallintajärjestelmä vahvalla salasanalla ja vahvalla tunnistamisella paras vaihtoehto. (Zhao & Yue, 2014).

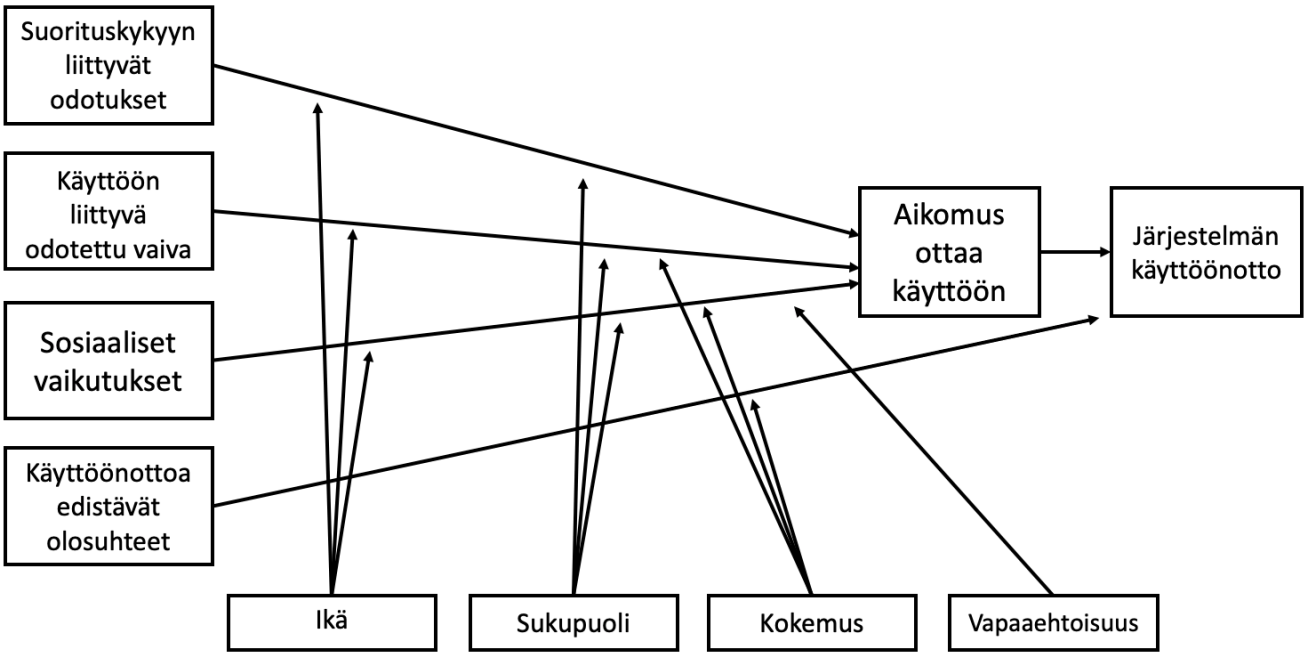
3.6 Salasanan hallintajärjestelmien käyttöönottaminen

Salasanan hallintajärjestelmät näyttävät olevan paras vaihtoehto käytettävyyden ja tietoturvan kannalta peruskäyttäjille hallita salasanoja. Käyttäjät eivät kuitenkaan ota salasanan hallintajärjestelemiä käyttöön, vaikka he tietävät, että heidän salasanansa ovat heikkoja ja he uudelleenkäyttävät salasanojaan. Tämä käy ilmi salasanan hallinta tarjoavan Lastpass (2020) tutkimuksesta, jossa 77% käyttäjistä kertoi kuullensa salasanojen hallintaan liittyvistä paremmista käytännöistä, kuitenkin 54% näistä vastaajista jatkoi samoja huonoja salasanan hallintaan liittyviä tapoja. Näyttää siis siltä, että salasanan hallintajärjestelmiä ei oteta käyttöön, vaikka niistä ollaan tietoisia.

Teknologioiden käyttöönottoa voidaan tarkastella hyödyntämällä useita eri malleja. Eräs malleista, joka käsittelee tätä, on Davidsin ja Bagozzin (1985) kehittämä Technology Acceptance Model. Kun Technology Acceptance Modeln hengessä tarkastellaan salasanan hallintajärjestelmien käyttöönottamatta jättämistä saattaa se osin johtua siitä, että henkilöt tekevät tietynlaisia oletuksia jo ennen, kun ottavat teknologioita käyttöön ja nämä olettamukset, joita käyttäjä tekee saattavat hidastaa tai toisaalta myös edistää teknologioiden käyttöönottoa. Näitä olettamuksia ohjaavat teknologian ulkoiset muuttujat, jotka ovat aiempien teknologioiden käyttöön liittyviä kokemuksia sekä teknologian ominaisuuksien vertailu. Näiden perusteella tehdään päätelmiä siitä, onko teknologiasta hyötyä käyttäjälle ja onko teknologian käyttö liittyvä oletettu vaiva suuri. Mikäli oletettu vaiva on merkittävästi liian suuri vaikuttaa se myös koettuun kokemukseen oletetusta hyödyllisyydestä. Nämä kaksi tekijää vaikuttavat asenteeseen, joka koetaan liittyvän tietyn teknologian käyttöön. Tämä asenne johtaa päätökseen, joko käyttää teknologiaa tai olla käyttämättä teknologiaa. (Davis & Bagozzi, 1985). Toisin sanoen tämän teorian perusteella, kun sitä sovelletaan salasanan hallintajärjestelmiin voidaan sanoa, että näyttää siltä, että todennäköisesti salasanan hallintajärjestelmien kohdalla käyttäjät eivät koe niitä riittävän helpoiksi käyttää ja he eivät koe niistä olevan riittävää hyötyä päivittäisessä käytössä, koska 77% käyttäjistä on Lastpassin (2020) tekemän tutkimuksen mukaan kuullut salasanan hallintajärjestelmistä, mutta silti yli puolet edelleen päättää olla käyttämättä niitä.

Teknologioiden käyttöönottoa voidaan tarkastella laajemmin hyödyttämällä uudempaa Unified Theory of Acceptance and Use of Technology (UTAUT) mallia. (Venkatesh, Morris, Davis, & Davis, 2003). Tämä malli koostuu neljästä päätekijästä, jotka ovat suorituskykyyn liittyvät odotukset, käyttöön liittyvä odotettu vaiva, sosiaalinen vaikutus ja käyttöönottoa edistävät olosuhteet. Päätekijöihin vaikuttavia sivutekijöitä on neljä, jotka ovat sukupuoli, ikä, aiempi teknologinen kokemus sekä käyttöön liittyvä vapaaehtoisuus. Käyttöön liittyvällä vapaaehtoisuudella tarkoitetaan esimerkiksi tilannetta, jossa henkilölle organisaation toimesta pakotetaan jokin järjestelmä käyttöön ja sen vertaamista vapaaehtoiseen käyttöönottoon. Suorituskykyyn liittyvät odotukset ovat asioita kuten, järjestelmän käytön kautta saadut hyödyt, tuottavuuden kasvu, positiiviset vaikutukset suoriutumiseen sekä koettu hyödyllisyys. Salasanan hallintajärjestelmien osalta tällaisia suorituskykyyn liittyviä odotuksia voivat olla esimerkiksi odotettu nopeutuminen kirjautumisprosesseissa, kohonnut tietoturvan taso ja

kasvanut tuottavuus prosesseissa, kun salasanoja ei tarvitse enää palauttaa unohdusten vuoksi. Nämä asiat näyttävät salasanan hallintajärjestelmän osalta olevan yleisiä ominaisuuksia teknologian käyttöön liittyen ja niihin ei voida juurikaan vaikuttaa valitsemalla oikeata tuotetta. Käyttöön liittyvä vaiva kuvaa niitä asioita, jotka liittyvät teknologian käyttöä vaativaan vaivaan. Tällaisia asioita ovat esimerkiksi helppokäyttöisyys, eli vaikeuttaako salasanan hallintajärjestelmä kirjautumista vai helpottaako se sitä. Koettuun vaivaan liittyy myös koettu stressi järjestelmän käytöstä, eli tunteeko henkilö salasanan hallintajärjestelmien osalta olevansa turvassa ja näin vähentääkö se tietoturvaan liittyvää stressiä. Sosiaalisella vaikutuksella tarkoitetaan asioita, jotka edistävät teknologian käyttöönoton hyväksyntää sosiaalisesti ja sen sosiaalisia vaikutuksia yhteisöön. Mikäli teknologia koetaan hyödylliseksi yhteisölle, otetaan se todennäköisemmin käyttöön ja mikäli teknologialla voidaan saada sosiaalista hyväksyntää, otetaan se silloin todennäköisemmin käyttöön. Myös erilaiset suosittelut oikealta taholta vaikuttavat teknologioiden käyttöön. Salasanan hallintajärjestelmien osalta siis todennäköisesti, mikäli sitä suosittelee oikea taho ja sillä voidaan saavuttaa sosiaalisia hyötyjä esimerkiksi erilaisten salasanan jako ominaisuuksien kautta, otetaan se todennäköisemmin käyttöön teorian mukaan. Käyttöönottoa edistävät olosuhteet tarkoittavat asioita, kuten järjestelmän saatavilla olo ja tarvittu tietotaito järjestelmän käyttöön. Salasanan hallintajärjestelmien osalta järjestelmän maksuttomuus, saatavuus eri alustoille sekä käytön helppous ovat tällaisia tekijöitä. (Venkatesh yms., 2003).



Kuva 1 Unified Theory Of Acceptance And Use of Technology (Venkatesh yms., 2003).

Salasanan hallintajärjestelmien käyttöönottamisen kannalta mielenkiintoista on tarkastella erityisesti suorituskykyyn liittyviä odotuksia, käyttöön liittyvää odotettua vaivaa, sosiaalisia vaikutuksia sekä käyttöä edistäviä olosuhteita. Näiden lisäksi todennäköisesti jonkin verran vaikuttavat käyttäjän ikä sekä aiempi kokemus teknologiasta. Sukupuolella ei todennäköisesti ole salasanan hallintajärjestelmien kannalta suurempaa merkitystä, sillä salasanan hallintaan on vaikea liittää maskuliinisia tai feminiinisiä piirteitä samaan tapaan, kun esimerkiksi joihin sosiaalisen median palveluihin. Käytön vapaaehtoisuuden osalta on mielekästä rajata pakotetut käyttäjät ulos, sillä todennäköisesti organisaationsa puolesta pakotetut käyttäjät kyllä kokevat salasanan hallinnan mielekkääksi ja hyödylliseksi, mutta samalla vääristävät tuloksia, kun tarkastelussa on erityisesti vapaaehtoinen omaehtoinen käyttöönotto. (Venkatesh yms., 2003).

4 Haastattelututkimus ja tutkimusmenetelmät

Tämän tutkimuksen pääasiallisena tavoitteena on tarkastella ihmisten tapoja hallinnoida salasanoja ja löytää tapoja, joten peruskäyttäjän tietoturvaa voitaisiin parantaa. Tutkimus toteutettiin haastattelemalla salasanan hallintajärjestelmää jo käyttäviä henkilöitä. Tässä osiossa käydään läpi tutkimuksen järjestelyihin, kohdejoukkoon, aineiston keruuseen ja haastatteluiden järjestämiseen liittyviä asioita. Salasananhallinta menetelmien haastattelututkimuksessa pyritään löytämään vastauksia seuraaviin kysymyksiin.

- Minkälaisia tapoja haastateltavilla on hallinnoida salasanoja?
- Miten henkilöiden teknologinen tausta ja mielenkiinto teknologiaa kohtaan vaikuttavat tapaan hallinnoida salasanoja?
- Kokevatko henkilöt tapansa hallita salasanoja turvalliseksi?
- Uudelleenkäyttävätkö käyttäjät salasanoja?
- Miten henkilö on päätynyt käyttämään salasanan hallintajärjestelmäänsä?
- Minkälaiset tekijät ovat edesauttaneet tai hidastaneet salasanan hallintajärjestelmän käyttöönottoa
- Minkälaisia hyötyjä tai haittoja henkilöt ovat kokeneet valitsemansa salasanan hallintajärjestelmän osalta?

Näiden tekijöiden lisäksi tutkittiin haasteltavien asenteita liittyen tietoturvaan, teknologiaan ja heidän käyttökokemukseensa.

4.1 Kvalitatiivinen haastattelu menetelmä

Venkatesh, Morris, Davis, & Davis (2003) mukaillen tutkimuksessa tutkitaan UATAT:n viitekehyksenmukaisesti laadullisesta näkökulmasta siitä syystä, että laadullisessa tutkimusmenetelmässä pyritään usein hakemaan pidemmälle menevä ymmärrys tiettyyn ilmiöön tai asiaan (Alasuutari, 2012). Tässä tutkimuksessa on päädytty laadulliseen tutkimusmenetelmään myös siitä syystä, että tutkimuksessa olevat muuttujat ovat laadultaan sellaisia, ettei niitä voida juurikaan järkevästi mitata määrällisen tutkimuksen menetelmien mukaan. Näin olleen voidaankin tehdä laadullisen tutkimuksen pohjalta pyrkiä löytämään vastausten välisiä suhteita ja yleistettävyyksiä. (Hirsjärvi & Hurme, 2008). Laadullinen haastattelututkimus toteutettiin olosuhteiden ja maailmanlaajuisen pandemia tilanteen vuoksi etähaastatteluina Zoom- kokouspalvelussa. Zoom valittiin siitä syystä, että se vaikutti olevan tutuin kaikille haasteltaville ja heidän oli helppo sitä käyttää. Zoom tarjosi myös loistavat edellytykset sisäänrakennetun haastattelun nauhoittamiselle, joka teki siitä paremman vaihtoehdon muille verkon kokouspalveluille. Käytettävällä alustalla ei nähty olevan mitään merkitystä

haastatteluun niin kauan kun se toimii ainoastaan tapana välittää kuvaa ja ääntä. Haastattelu toteutettiin puoli strukturoituna haastatteluna, jossa kysymykset oli määritelty etukäteen ja kysymykset kysyttiin kaikilta haastateltavilta samassa järjestyksessä. Puoli strukturoidun haastattelusta tekee se, että haastateltavilta voitiin kysyä haastattelun aikana tarkentavia kysymyksiä, joiden tarkoituksena oli ymmärtää haastateltavan vastaus paremmin.

4.1.1 Tutkimuskohde ja tutkimusmenetelmä

Haastatteluun valittiin henkilöitä, jotka eivät työskentele IT-alalla, mutta kuitenkin työskentelevät tällä hetkellä tai ovat työskennelleet aiemmin kasvatus- ja sosiaalialalla. Haastattelu kohdistettiin ei IT-alalla työskenteleviin siitä syystä, että lyhyen kartoituksen jälkeen IT-alalla työskentelevien motiivit eivät vaikuttaneet olevan sovellettavissa peruskäyttäjiin, sillä käytännössä kaikilla IT-alalla työskentelevillä on perustiedot salasanan hallinnasta ja tapa hallinnoida on hyvin homogeenistä. Kaikki haasteltavat ovat myös alle 35-vuotiaita, mutta kuitenkin yli 18 vuotiaita. Tämä valittiin sillä perusteella, että mikäli haasteltaisiin pitkälle yli 40 vuotiaita ei enää voitaisi enää olettaa henkilöiden käyttäneen koko työuransa moderneja tietojen käsittely välineitä. Tämä on merkityksellistä siksi, että tällöin henkilöille kirjautuminen ja kirjautumistietojen käsittely on arkipäivää ja heillä ei ole kokemusta ajasta ennen it järjestelmiä. Haastateltava populaatio koostui henkilöistä, jotka eivät työskentele IT-alalla ja ovat työskennelleet, työskentelevät tai opiskelevat lääketiedettä, sosiaali- tai kasvatusalaa. Populaatio on valikoitunut sen takia, että kaikki alalla työskentelevät ovat käsitelleet, käsittelevät tai tulevat tulevassa työssään käsittelemään henkilötietoja, terveystietoja sekä perheiden sosioekonomiseen statukseen liittyviä tietoja, jotka koetaan varsinkin länsimaisessa yhteiskunnassa todella arkaluontoisiksi. Populaatio käsittelee myös tietoja, jotka ovat myös lakisääteisesti tietynlaisen tietosuojan alaisuudessa.

Tutkimuksessa pyritään selvittämään syitä mitkä edistävät käyttäjien motivaatiota ottaa käyttöön tiettyä teknologiaa, joka tässä tapauksessa on salasanojen hallintajärjestelmä. Tätä tutkitaan käyttämällä hyväksi Unified Theory of Acceptance and Use of Technology teoriaa, jossa pohditaan teknologian käyttöön ottoon liittyviä syitä pohtimalla neljää eri avain tekijää. (Venkatesh yms., 2003). Nämä tekijät ovat:

1. Suorituskykyyn liittyvät odotukset (Performance expectancy)
2. Käyttöön liittyvä odotettu vaiva (Effort expectancy)
3. Sosiaalinen vaikutus (Social influence)
4. Käyttöönottoa edistävät olosuhteet (Faciliting confitions)

Suorituskykyyn liittyviä odotuksia tutkitaan tutkimuksessa etsimällä vastauksia haastattelussa haastateltavilta siihen mitkä he kokevat tärkeimmiksi ominaisuuksiksi salasanan hallintajärjestelmässään. Tämän lisäksi pyritään löytämään vähemmän tärkeitä ominaisuuksia. Näitä peilataan käyttäjän aiempaan tapaan hallita salasanoja.

Käyttöön liittyvää koettua vaivaa tutkitaan haastattelussa etsimällä vastauksia kysymyksiin kuten minkälaisia asioita koetaan nykyisessä tavassa hallinnoida salasanoja helpoksi tai vaikeaksi. Käyttäjää myös pyydetään kuvailemaan hänen kirjautumisprosessiaan ja siitä pyritään löytämään asioita, jotka hän kuvailee hankaliksi tai helpoiksi. Tällaisia asioita voivat olla esimerkiksi automaattisen salasanan tarjoama täydennys nopeuttavana tekijänä tai salasanan uudelleen pyytäminen unohdin salasanani palvelun avulla hidastavana tekijänä.

Sosiaalista hyväksyntää pyritään tutkimaan kysymällä haastattelussa, onko salasanan hallinta järjestelmiä suositeltu haastateltaville ja ottivatko he käyttöön niitä sen perusteella. Sosiaalista hyväksyntää pyritään myös tutkimaan kysymällä ovatko haastateltavat kohdanneet jotain positiivisia tai negatiivisia asenteita kertoessaan tavastaan hallita salasanoja. Erityisen kiinnostavaa tämä on salasanan hallintaa käyttävien henkilöiden osalta, sillä salasanan hallinta saattaa herättää negatiivisia asenteita, koska salasanoihin liittyy luottamuksellisia tekijöitä ja tämä luottamus on luovutettu kolmannen osapuolen käsiin.

Käyttöä edistäviä olosuhteita pyritään tutkimaan kysymällä haastateltavilta minkälaisia ominaisuuksia tai resursseja he pitävät tärkeinä salasanan hallintajärjestelmässään. Heiltä myös kysytään minkälaiset tekijät ovat vähemmän tärkeitä. Salasanan hallinnan osalta myös pyritään löytämään vastaus siihen ovatko he ottaneet salasanan hallinnan käyttöön vapaaehtoisesti vai jonkin kolmannen osapuolen pakottamasta syystä. Tällainen syy saattaa olla esimerkiksi työpaikalla vallitseva salasanan hallintaan liittyvä pakko tai esimerkiksi puolison salasanan hallintajärjestelmään asettama suoratoistopalvelun salasana, jolloin tiettyjen järjestelmien käyttö pakottaa käyttäjän käyttämään salasanan hallintajärjestelmää.

4.1.2 Tulosten analysointi

Tuloksia tullaan analysoimaan tässä tutkimuksessa hyödyntämällä sisältöanalyysiä. Sisältöanalyysissä pyritään luomaan tekstipohjainen näkemys tutkittavasta aiheesta. Sisältöanalyysissä haastatteluissa tuotettu aineisto kirjataan ylös sellaiseen muotoon, jossa kerätyt vastaukset ovat helpommin jäsenneltävissä kysymysten mukaan ryhmiin. (Tuomi & Sarajärvi, 2017). Ryhmittely tullaan tekemään Venkateshin, Morrisin, Davisin, & Davisin (2003) mukaisesti Unified Theory of Acceptance and Use of Technology neljään kategoriaan, jotka ovat:

1. Suorituskykyyn liittyvät odotukset (Performance expectancy)
2. Käyttöön liittyvä odotettu vaiva (Effort expectancy)
3. Sosiaalinen vaikutus (Social influence)
4. Käyttöönottoa edistävät olosuhteet (Faciliting confitions)

Näissä kategorioissa tullaan jakamaan kysymykset ensin alakategorioihin sekä sen jälkeen jakamaan vastaajat kahteen eri ryhmään sen perusteella käyttävätkö he digitaalista salasanan hallintajärjestelmää vai eivät. Kun ryhmät on jaettu näin, voidaan niistä helpommin. nähdä eroja sekä yhteneväisyyksiä molempien ryhmien välillä.

5 Tutkimuksen tulokset

Tutkimuksen toteutus tapahtui etäyhteyksiä käyttäen, johtuen vuoden 2020 koronaviruspandemiasta. Haastatteluun osallistuneet henkilöt olivat suostuneet vapaaehtoisesti. haastatteluun ja siihen oli sovittu aika ennakkoon. Haastateltaville henkilöille ei toimitettu etukäteen mitään kysymyksiä, sillä henkilöille ei haluttu antaa tutkimuksesta ylimääräisiä tietoja, jotka saattaisivat vaikuttaa heidän vastaustensa sisältöön. Kaikille henkilöille toimitettiin etukäteen tiedot haastattelusta, jossa kerrottiin haastattelun olevan luottamuksellinen ja kaikki data, jota tullaan keräämään osana tutkimusta tullaan käsittelemään, niin ettei haastateltava ole tunnistettavissa vastauksista. Haastateltaville myös kerrottiin, että mikäli he eivät halua vastata johonkin kysymykseen, he voivat päättää milloin tahansa olla vastaamatta sekä annettiin vapaus keskeyttää haastattelu missä tahansa vaiheessa, he vain tuntevat sen olevan tarpeen. Haastateltaville myös kerrottiin, että haastattelu tullaan nauhoittamaan myöhempää analysointia varten ja nauhoitteet tullaan sellaisinaan tuhoamaan tutkimuksen valmistuttua ja kun niille ei enää ole tarvetta. Tämän lisäksi itse haastattelu tilanteessa kaikille haastateltaville vakuutettiin, että kyseisessä haastattelussa ei ole olemassa mitään oikeita vastauksia, sillä tutkimuksen mielenkiinnon kohteena on yksilön tapa toimia tietyissä tilanteissa ja näin ollen henkilön tapa toimia on ehdottomasti aina oikea. Tällä pyrittiin luomaan ajatus siitä, että henkilöt voivat rentoutua ja kertoa omasta kokemuksestaan pelkäämättä vastauksen olevan väärä tai muuten epämiellyttävä. Haastateltaville kerrottiin myös, että haastattelun aikana haastattelu tulee etenemään niin, että varsinaisesti ei käydä juurikaan keskustelua asiasta vaan haastattelija tulee esittämään kysymyksiä ja kommentoimaan mahdollisimman vähän haasteltavan vastauksiin. Tällä pyrittiin rikkomaan jää muutoin epäluonnolliselle keskustelulle, missä haastateltava ei varsinaisesti saa mitään vastakaikua vastauksilleen. Haastateltaville kerrottiin myös haastattelun alku vaiheessa, että haastattelun aikana saattaa tuntua siltä, että on vastannut samantyyliseen kysymykseen jo aiemmin ja, että tämän normaalia sillä samaa asiaa lähestytään useasta eri näkökulmasta. Haastattelu tilanne itsessään eteni niin, että haastattelu tilanteen alussa henkilöltä kysyttiin lähinnä kuulumisia, jotta saatiin keskustelu yhteys avattua ja niin sanotusti jää rikottua. Tämän jälkeen siirryttiin hieman syvällisempiin asenteita liittyviin kysymyksiin, joiden tarkoituksena oli selvittää, minkälainen henkilö on kyseessä ja mikä heidän suhteensa on teknologioihin, tietoturvaan sekä salasanojen hallintaan. Asenteiden jälkeen haastattelussa tutkittiin henkilön odotuksia ja toteutuneita asioita liittyen hänen valitsemansa salasanan hallintajärjestelmän käyttöön ja sen suorituskykyyn. Tämän jälkeen haastattelussa kysyttiin kysymyksiä liittyen käyttäjän kokemaan käyttökokemukseen ja erityisesti pyrittiin löytämään sellaisia asioita, jotka käyttäjä kokee käyttöä edistäväksi, eli helpoiksi tai käyttöä estäviksi eli vaikeiksi. Käyttökokemuksen jälkeen siirryttiin pohtimaan sosiaalista elementtiä ja sitä, oliko taustalla jokin suosittelija, jonka kautta salasanan hallintajärjestelmä otettiin käyttöön. Sosiaalista elementtiä pohdittiin myös sitä kautta, ovatko kyseiset henkilöt kokeneet, että salasanan hallintajärjestelmän käyttäminen on sosiaalisesti hyväksyttävää. Viimeisenä asiana ennen, kun haastattelu päätettiin, pohdittiin sitä, mitkä

ovat käyttöä edistävät olosuhteet ja mitkä johtivat loppujen lopuksi siihen, että käyttäjä otti salasanan hallintajärjestelmän käyttöön. Haastattelu tilanteen jälkeen kaikille vastaajille annettiin mahdollisuus täydentää mahdollista vastausta sekä mikäli heillä oli jotain kysyttävää, tarjottiin heille mahdollisuus kysyä. Haastattelun jälkeen jokaista haastateltavaa kiitettiin haastattelusta ja siitä, että he olivat antaneet aikaansa sekä vaivaansa tähän tutkimukseen.

5.1 Lämmittelykysymykset ja salasanan hallintaan liittyvät kysymykset

Haastattelu alkupuolella henkilöiltä kysyttiin helppoja kysymyksiä liittyen heidän teknologiseen taustaansa sekä tapaansa hallita salasanoja. Haastattelun alkupuolen helpompien ja henkilöiden itse yksinkertaiseksi kokemien kysymysten tarkoituksena oli avata keskusteluyhteyttä sekä pyrkiä niin sanotusti rikkomaan jää haastateltavan sekä haastattelijan väliltä.

5.1.1 Teknologisen taustan tutkiminen kohderyhmissä

Haastattelun alkupuolella käyttäjiltä kysyttiin kysymyksiä liittyen heidän teknologisen taustaansa liittyviä. Tällä kysymyksellä pyrittiin saamaan käsitys siitä, minkälainen tekninen tausta haastattelun kohde henkilöillä on. Sama kysymys esitettiin molemmille haasteltaville kohderyhmille. Henkilöt, jotka eivät käyttäneet digitaalista salasanan hallintaohjelmaa vastasivat hyvin samalla tavalla kertoen, että he ovat teknologisesti keskiverto osaajia tai hieman sen yli. Monet haastateltavat mainitsivat kokevansa olevansa keskivertokäyttäjää parempi digitaalisten työkalujen käytössä sekä normaalien tavanomaisten digitaalisten asioiden hoitamisessa. Kohderyhmä käsitteli digitaalista osaamista hyvin pitkälle sillä tavalla, kun odotettiinkin, eli he kokevat olevansa peruskäyttäjiä omassa ikäluokassaan, joka vaikutti pitävän paikkansa. Vaikutti siltä, että salasana managereita käyttämätön joukko on digitaalisten työkalujen sekä teknologioiden käytössä normaalilla tasolla. Eräs vastaaja vastasi kuvaavasti ja leikkisästi kysymykseen seuraavasti: *"Mä olen tälläinen digiajan nuorukainen."* Henkilöt, jotka käyttivät digitaalista salasanan hallintajärjestelmää, kokivat toisen joukon tavoin olevansa hyvin pitkälle digitaalisten työkalujen ja teknologioiden käytössä keskitasossa tai hieman sen yli. Henkilöt kertoivat käyttäneensä teknologioita jo nuoresta pitäen ja suoristuvansa hyvin digitaalisia työkaluja vaativista tehtävistä. Eräs haasteltavista avasi hyvin samaan tyyliin keskustelun, kun toisessakin ryhmässä toteamalla seuraavasti: *"Olen ehdottomasti diginatiivi!"* Haastatteluun valittujen kohdejoukkojen välillä ei nähty mitään merkittäviä eroja teknologisten taustojen välillä. Henkilöt vaikuttivat odotetusti peruskäyttäjiltä, joilta löytyy kyky ja osaaminen suoriutua päivittäisistä digitaalisista tehtävistä ja haasteista. Kohderyhmien välillä ei havaittu tässä osassa merkittävää eroa osaamisen tasossa.

5.1.2 Teknologioiden omaksuminen ja käyttöönotto

Haastattelussa molemmilta kohdejoukoilta kysyttiin kysymys liittyen heidän tapaansa omaksua ja ottaa käyttöön uusia teknologioita. Kysymyksen tarkoituksena oli selvittää, onko kohdejoukkojen välillä merkittäviä eroja suhteessa siinä, miten henkilöt ottavat käyttöön uusia teknologioita ja voitaisiinko selittää henkilöiden salasanan hallintaohjelman käyttöä sillä, että henkilöt kokevat halua olla niin sanottuja innovoijia tai aikaisessa vaiheessa teknologioita käyttöön ottavia. (Rogers, 2010). Rogersin mallissa teknologioiden käyttäjät jaotellaan guassin käyrän mukaisesti niin, että n. 68% ottaa teknologiaa käyttöön sen yleistyessä, 16% hyvin aikaisessa vaiheessa ja 16% vasta hyvin myöhäisessä vaiheessa.

Henkilöt, jotka eivät käytä salasanan hallintaohjelmia kertoivat ottavansa yleisesti teknologioita, palveluita ja sovelluksia silloin kun ne alkavat yleistyä ja kun niistä alkaa olemaan henkilölle itselleen hyötyä. Monet haastateltavat mainitsevat myös, että ovat innokkaita kyllä kokeilemaan uusia palveluita, mutta yleensä ne tulevat käyttöön, kun joku omassa sosiaalisessa ympyrässä alkaa käyttää sovellusta ja suosittelee sitä muille. Yleisesti voidaan todeta, henkilöt, jotka eivät käyttäneet salasana manageria ottivat omien sanojensa mukaan käyttöön teknologioita niiden yleistyessä ja kun niitä käytetään laajasti. Kukaan käyttäjistä ei kokenut olevansa aikaisen tai myöhäisen vaiheen käyttöönottaja.

Salasanan hallintajärjestelmiä käyttävien henkilöiden osalta koettiin, että uusia teknologioita, palveluita ja sovelluksia otettiin käyttöön niiden yleistyessä ja kun ne ovat tarjolla kohtuulliseen rahallisen tai muuhun kustannukseen. Tässäkin kohderyhmässä mainittiin, että käyttöönottoa yleensä edeltää jonkun suosittelu ja se, että omassa sosiaalisessa ympyrässä teknologiaa otetaan käyttöön. Rogersin (2010) mallin mukaisesti myös salasanan hallintajärjestelmiä käyttöön ottavat henkilöt ottavat yleensä keskivaiheilla teknologioita käyttöön eikä kukaan haastateltavista kertonut olevansa innokkaana ensimmäisenä tai ihan viimeisten joukossa, kun otettiin käyttöön uusia teknologioita.

Yleisesti kohdejoukkojen perusteella voidaan todeta, että teknologioiden käyttöönottoon liittyvä innokkuus ei selitä henkilöiden motivaatiota ottaa käyttöön tai olla ottamatta käyttöön salasanan hallintajärjestelmiä. Kaikki vastaajat kertoivat kuuluvansa keskivaiheille käyttöönottajissa. Uusien teknologioiden käyttöönottoa molemmissa ryhmissä tuntuivat edistävän se, että henkilöt kokevat sen hyödylliseksi, se on yleisesti käytössä ja sitä käyttää joku heidän omassa sosiaalisessa ympyrässään. Kysymyksessä nähtiin mielenkiintoinen vastaus molemmissa ryhmissä, sillä molemmissa ryhmissä nimettiin oma-aloitteisesti sosiaalisen median uusi palvelu TikTok sellaisena palveluna, jota ei aiota ottaa käyttöön ikinä. Tähän varsinaisesti kohdejoukosta ei löytynyt selittävää tekijää, mutta haastattelijan näkökulmasta näyttää siltä, että kohdejoukon työskentely tausta lasten, nuorten tai muuten sosiaalialan sektorilla näkyy tässä vastauksessa siitä syystä, että TikTok on tällä hetkellä ilmiö nuorison keskuudessa ja se todennäköisesti aiheuttaa lieveilmiöitä alalla työtätekevien työssä. Tämä tosin jäi tutkimuksen valossa selvittämättä, mutta TikTok:in ja nuorten käyttöön ottamien sovellusten vaikutus alalla työskenteleviin voisi olla yksi mielenkiintoinen jatkotutkimus aihe liittyen siihen, miten teknologioita otetaan käyttöön. Kysymykseen teknologioiden käyttöön otosta voisi tiivistää hyvin erään vastaajan

vastaukseen: *"En ole kyllä ensimmäinen, mutta en kyllä viimeinenkään. Otan yleensä käyttöön, kun siitä on hyötyä ja joku lähipiirissä käyttää sitä."*

5.1.3 Salasanojen hallintamenetelmä

Kaikilta haastateltavilta kysyttiin kysymys suoraan liittyen heidän salasanan hallintajärjestelmäänsä ja kysymys oli muotoiltu molemmille kohdejoukoille samalla tavalla. Kysymyksessä ei johdateltu vaan kysyttiin miten käyttäjä hallinnoi salasanojaan.

Kohdejoukko, joka ei käyttänyt salasanan hallintajärjestelmiä kertoi huomattavasti pidemmin heidän salasanan hallintajärjestelmistään. Valtaosalla näytti olevan käytössä muutamia salasanoja, joista keksitään erilaisia variaatioita. Käytännössä tämä tarkoitti sitä, että henkilöt valitsivat jonkin salasanan tai salasanalauseen, jonka sisältöä he muuttivat hieman jokaiseen palveluun. Osa käytti suoraan samaa salasanaa joka palvelussa ja he kertoivat, että heillä on yksi mitä käyttävät usein ja muutamia mitä käyttävät harvoin. Käytännössä merkittävää tässä kohdejoukossa oli se, että henkilöt uudelleen käyttivät yhtä salasanaa joko ilman muutoksia tai pienin muutoksin useissa eri palveluissa. Henkilöt mainitsivat myös, että he saattavat hyväksyä selaimen ehdotuksen tallentaa salasana selaimeen talteen, mutta tähän useat lisäsivät sen olevan kuitenkin kehno tapa hallinnoida, sillä usein salasanaa tarvittaisiin useilla eri laitteilla. Haastateltavista muutamat myös kertoivat kirjoittavansa salasanan ylös johonkin paperiseen muotoon, jossa ne ovat turvassa.

Kohdejoukko, joka käytti salasanan hallintajärjestelmiä vastasi hyvin nopeasti ja yksiselitteisesti sen palvelun nimen, jota käyttivät eivätkä mitään muuta. Kohdejoukossa olevat henkilöt käyttivät kahta eri palvelua, jotka olivat LastPass ja F-secure Key. Kysymykseen hei eivät vastanneet monimutkaisemmin, sillä heidän tapansa hallita salasanoja oli heidän salasanan hallintaohjelmansa nimi.

Kysymyksen perusteella voidaan havaita, että jo tässä vaiheessa henkilöt myönsivät uudelleenkäyttävänsä salasanoja merkittävästi. Osa henkilöistä, jotka eivät käyttäneet salasanan hallintajärjestelmää myönsivät suoraan uudelleen käyttävänsä yhtä tai muutamaa salasanaa ja toinen osuus henkilöistä kertoi, että heillä on jokin logiikka, jonka pohjalta he luovat uusia salasanoja palveluihin. Yleinen vastaus tiivistyy erään vastaajan vastaukseen: *"Mulla on yksi yleinen mitä sitten muutan vähän vaihtamalla merkkiä tai numeroa johonkin kohtaan."*

5.1.4 Salasanojen hallinta menetelmään päätyminen

Molemmilta kohdejoukoilta kysyttiin, miten he ovat päätyneet tähän tapaan hallita salasanoja. Kysymyksellä pyrittiin löytämään eroja kohdejoukkojen välillä, sillä heidän tapansa hallita salasanoja on erilainen. Kysymykseen liittyvä odotus oli, että salasanoja uudelleen käyttävä, muistamalla niitä hallitseva populaatio on ikään kuin ajautunut tähän aikojen saatossa, eikä heidän tapaansa ole ajanut mikään tapahtuma tai muu vastaava tilanne. Salasanan hallintajärjestelmää käyttävien osalta odotus on, että joki tilanne, tapahtuma, suosittelu tai muu vastaava

on saanut heidät näkemään sen vaiva, että he ovat ottaneet salasanan hallintajärjestelmän käyttöön.

Kohdejoukko, joka ei käytä salasanan hallintajärjestelmää vastasi kysymykseen hyvin odotetun tapaisesti. Haastattelu tilanteessa ilmaantui pieni hämmennys useimmille kysymyksen ympärille, sillä vastaus vaikutti ilmeisesti haastateltavista itsestään selvältä. Tähän oli ajauduttu aikojen saatossa eikä mitään yksittäistä syytä löytynyt. Monet mainitsivat, että he eivät ole nähneet tätä tarpeelliseksi ja omalla laiskuudella on ollut tässä merkittävä rooli. Osa kertoi myös, että heillä ei varsinaisesti ole tarkkaa tietoa siitä, miten voisivat tilannetta parantaa. Lähes kaikki kuitenkin mainitsivat, että tietävät mitä salasanan hallintaohjelmat ovat, mutta niitä on ilmeisesti niin monia ja on vaikea sanoa mikä niistä on käyttäjän näkökulmasta käyttökokemuksen ja luotettavuuden kannalta hyvä.

Salasanan hallintajärjestelmää käyttävä joukko vastasi kysymykseen käytännössä kaikkien osalta kertomalla sen tilanteen, joka sai heidät ottamaan salasanana hallinta järjestelmän käyttöön. Osalla tämä tilanne oli ollut kollegan tai ystävän suosittelu, yhdellä uuden laitteiston hankkiminen ja yleisesti koettu tilanne, jossa halutaan laittaa oma henkilökohtainen tietoturva kuntoon. Erään käyttäjän kohdalla merkittävä tilanteeseen vaikuttanut yksittäinen tapahtuma oli tietomurron uhriksi joutuminen. Käyttäjä oli toisen kohdejoukon kaltaisesti uudelleen käyttänyt muutamia salasanoja, joista jokin oli vuotanut ja tämän salasanan turvin hyökkääjä oli toteuttanut automatisoidun hyökkäyksen ja täyttänyt koko uhrin Facebook seinän halpojen aurinkolasien mainoksilla. Tämä oli luonnollisesti uhrille tilanteena nolo sekä loukkasi tämän henkilökohtaista turvallisuuden tunnetta, joten uhri päätti tällä hetkellä laittaa oman henkilökohtaisen tietoturvansa kuntoon. Kohdejoukosta nousi merkittävänä osana esille opiskelijajoukko, jossa he olivat päätyneet käyttämään samaa tuotetta, koska yliopisto oli sen heille ilmaiseksi tarjonnut. Salasanan hallintajärjestelmää käyttävältä osajoukolta kysyttiin myös, kuinka suuri osa heidän käyttäjätunnuksista ja salasanoista on salasanan hallintajärjestelmiin tallennettuna ja tähän henkilöt, jotka käyttivät f-securen tuotetta vastasivat, että heidän salasanoista suurin osa, mutta eivät kaikki on tallennettuna salasanan hallintajärjestelmään. Tähän käyttäjät kertoivat syyksi käytettävyyteen liittyvät asiat, sillä he käsittelivät salasanoja pääasiallisesti puhelimen muistista. Lastpassiä käyttävä joukko vastasi, että käytännössä kaikki salasanat ovat tallessa Lastpassissä ja vain tarpeettomia ja sellaisia, mitä ei ole käytetty pitkään aikaan on sen ulkopuolella.

Näyttää siltä, että peruskäyttäjien osajoukossa käyttäjät ovat ajautuneet aikojen saatossa hallitsemaan salasanojaan muistamalla. Näyttää siltä, että mitään yksittäistä syytä ei ole sille, miksi toinen kohdejoukko on päätynyt tähän tilanteeseen. Salasanojen hallitseminen muistamalla on todennäköisesti yksinkertaisin tapa ja siksi siihen päädytään. Näin hyvin todennäköisesti on myös muun väestön keskuudessa ja haastattelusta saatu tulos voidaan suurella todennäköisyydellä yleistää myös suurempaa populaatioon. Salasanojen hallintajärjestelmän käyttöönottaneiden käyttäjien osalta vaikuttaa siltä, että yksittäisiä käyttöä edistäviä asioita ovat jonkun henkilön suosittelu sekä epämiellyttävän tietoturvatilanteen kokeminen. Mielenkiintoinen havainto oli myös se, että selkeästi näkyi hajontaa käytettävän tuotteen osalta ja F-secure key:n käyttäjät hyödynsivät salasanan hallintajärjestelmäänsä vähemmän, kun Lastpassin käyttäjät. Eräs

vastaaja vastasikin seuraavasti kysymykseen: *"Kyllä se oli vähän noloa, kun oli Facebook täynnä rayban mainoksia ja kaikki kaverit tägätty niihin. Piti tehdä jotain."*

5.1.5 Salasanojen muodostaminen

Molemmilta kohdejoukoilta kysyttiin heidän tapaansa muodostaa salasana palveluun. Kysymyksen tarkoituksena oli selvittää, eroavatko prosessit tosistaan jollakin tapaa. Kysymyksen odotuksena oli, että salasanan hallintajärjestelmää käyttävät hyödyntävät enemmän valitsemaansa digitaalista salasanan hallintajärjestelmää ja generoivat salasanan käyttäen salasanan hallintajärjestelmästä löytyvää salasana generaattoria, jolloin salasana on usein täysin satunnainen merkkijono. Toisella osajoukolla, joka hallinnoi salasanoja muistamalla oli odotettavaa, että henkilöt ottavat vanhan salasanan käyttävät sitä joko suoraan uudelleen tai sitten muokkaavat sitä jonkin verran muuttamalla merkistön kokoa tai muutamalla jonkin merkin esimerkiksi numeroksi.

Osajoukko, joka ei käyttänyt salasanan hallintajärjestelmää vastasi hyvin samalla tavalla. Valtaosa kertoi ottavansa suoraan vanhan salasanan ja uudelleen käyttävänsä sitä. Osa kertoi, että ottavat vanhan salasanan ja muuttavat sitä jollakin tavalla. Vaihtamalla esimerkiksi merkistökokoja, erikoismerkkejä lisäämällä sekä vaihtamalla kirjaimia numeroiksi. Käytännössä kaikilla haastateltavilla oli tapana käyttää muutamia eri salasanoja eri muodoissa. Muutamat haastateltavat kertoivat, että heillä on tapana keksiä eri salasana eri kategorioihin, jolloin on esimerkiksi kolme eri salasanaa ja niitä käytetään niin, että työpaikalla, opiskelupaikalla sekä henkilökohtaisessa elämässä on eri salasanat. Useissa vastauksissa nousi kysymättä esille muistamiseen liittyvät ongelmat ja se, että henkilöt kokivat vaikeaksi muistaa mikä salasanan variaatio kuului mihinkin palveluun. Osajoukolle esitettiin myös jatkokysymys, jossa kysyttiin osaavatko he nimetä jotakin yksittäistä syytä salasanojen uudelleen käytölle. Henkilöt käytännössä kaikki vastasivat muistamiseen liittyvän ongelma ja sen, että ei ole realistisia mahdollisuuksia muistaa salasanoja, sillä tilejä on niin monia, ellei salasana olisi sama monessa eri paikassa.

Salasanan hallintajärjestelmää käyttävä osanjoukko kertoi pääsääntöisesti generoivansa salasanan käyttäen digitaalista salasana generaattoria. F-secure keyn käyttäjät kertoivat keksivänsä salasanoja myös itse ja lastpassin käyttäjät kertoivat käytännössä kaikki generoivansa salasanan käyttäen salasana manageria. Lastpassin käyttäjistä osa myös mainitsi salasana generaattorissa näkyvän salasanan vahvuusmittarin kasvattaneen heidän salasanojensa turvallisuutta, sillä se antaa suoran palautteen siitä minkä vahvuinen salasana on kyseessä. Osajoukolle esitettiin myös jatkokysymyksenä kysymys, jossa kysyttiin, miten he muodostivat salasanansa, ennen hallintajärjestelmään siirtymistä. Vastaukset olivat hyvin samankaltaiset, kun toisen osajoukon. Myös hallintajärjestelmää käyttävät uudelleen käyttivät samoja salasanoja joko suoraan tai pienin muunnoksin ennen, kun he siirtyivät käyttämään salasanan hallintajärjestelmää.

Salasanojen muodostamisessa oli nähtävissä selkeä ero ryhmien välillä joukko, joka ei käyttänyt hallintajärjestelmää selkeästi uudelleen käytti suoraan tai hieman varioiden vanhoja salasanoja, kun taas joukko, jolla oli salasanan

hallintajärjestelmä käytössä, turvautui useimmiten salasanan hallintajärjestelmän tarjoamaan salasanan generointi mahdollisuuteen. Näyttää siltä, että salasana managerin käyttäjät eivät uudelleen käytä salasanoja juuri ollenkaan, kun taas salasanan hallintajärjestelmää käyttämättömät uudelleen käyttävät salasanoja jatkuvasti. Näyttää myös siltä, että salasanan hallintajärjestelmään siirtyminen odotetusti vähentää merkittävästi salasanojen uudelleen käyttämistä.

5.2 Teknologioihin, tietoturvaan ja salasanoihin liittyvät asenteet ja arvot

Tutkimusta toteutettiin käyttämällä hyväksi Unified theory of acceptance and use of technology viitekehystä a siinä voidaan nähdä yhtenä vaikuttavana tekijänä henkilön itsensä vapaaehtoiset asenteet ja arvot, jotka vaikuttavat sosiaaliseen hyväksyntään sekä toimivat käyttö edistävinä mahdollistajina. (Venkatesh yms., 2003). Tarkoituksena oli löytää yhdistäviä sekä erottelevia tekijöitä kohdejoukkojen välille.

5.2.1 Tietoturvan tärkeyden kokeminen henkilökohtaisessa elämässä

Molemmilta kohdejoukoilta kysyttiin miten tärkeänä he pitävät henkilökohtaisessa elämässä tietoturvaa. Kysymyksen tarkoituksena oli selvittää kokevatko henkilöt tietoturvan merkityksen eri tavalla eri haastatteluryhmissä. Kysymyksen odotuksena oli, että salasanan hallintajärjestelmää käyttävät kokevat tietoturvan tärkeämpänä ja salasanan hallinta järjestelmää käyttämättömät kokevat tietoturvan vähemmän tärkeänä.

Salasanan hallintajärjestelmää käyttämätön populaatio koki tietoturvan tärkeäksi tai osittain tärkeäksi. Osa henkilöistä kuitenkin kertoivat, etteivät varsinaisesti ihan täysin tiedä mitä tietoturva sinänsä tarkoittaa, joten on vaikea pitää tärkeänä, kun se vaikuttaa abstraktilta ja vaikealta kokonaisuudelta. Tässä tilanteessa voidaankin todeta, että oletus ei ollut oikea, sillä vaikka henkilöt eivät käyttäneet salasanan hallintajärjestelmää pitivät he tietoturvaa ainakin osittain tärkeänä tai hyvin tärkeänä.

Salasanan hallintajärjestelmää käyttävä osajoukossa nähtiin saman tyylistä hajontaa. Osa henkilöistä piti tietoturvaa vähemmän tärkeänä ja osa enemmän tärkeänä. Vastaajat kuitenkin kaikki kokivat, että tietoturva on nykyihmiselle sellainen perusjuttu, jonka kunnossa oleminen on ihan perus asia ja sen tulee olla kunnossa. Kahdella vastaajalla kuitenkin nousi korostunut tietoturvan merkitys esille ja he kertoivat siitä, kuinka tietoturvan kunnossa oleminen on heille tekijä henkilökohtaisen turvallisuuden tunteen osalta ja sen tulee olla kunnossa, koska se vaikuttaa tähän turvallisuuden tunteeseen. Henkilöistä ainakin toinen oli kokenut tietomurron aiemmin elämässään ja todennäköisesti tästä syystä turvallisuuden tunteeseen liittyi myös tietoturva, sillä hänen henkilökohtaisessa elämässään tietomurto oli realisoitunut.

Kysymyksen osalta voidaan sanoa, että oletukset eivät pitäneet paikkaansa, sillä molemmat osajoukot kokivat tietoturvan tärkeäksi osaksi heidän henkilökohtaista elämäänsä. Vaikutti kuitenkin ainakin osittain siltä, että salasanan hallintajärjestelmää käyttäneessä osajoukossa tietoturvan merkitys korostui ja tietotaito vaikutti olevan hieman korkeammalla tasolla, kun toisessa osajoukossa. Merkittäväksi nousi turvallisuuden tunteen korostuminen, sillä kaksi vastaajaa nosti sen esille toisistaan riippumatta kertoen, että tietoturva on osa henkilökohtaista turvallisuuden tunnetta.

5.2.2 Tietoturvan tärkeyden kokeminen työelämässä

Molemmille osajoukoille esitettiin tietoturvan merkityksen kokemiseen liittyvä kysymys, jossa pohdittiin sen merkitystä osana sitä työtä, jota tekee nyt tai sitä työtä, jota tulee tulevaisuudessa tekemään. Kysymyksen odotuksena oli, että koska osajoukko työskentelee tai, on työskennellyt aiemmin sosiaali- ja kasvatusalan tehtävässä, on heidän käsittelemänsä tiedot usein hyvin luottamuksellisia ja käsittelevät länsimaisessa yhteiskunnassa hyvin arkaluontoisiksi luokiteltuja tietoja kuten terveystietoja, perheiden ja lasten sosioekonomiseen tilaan liittyviä tietoja tai muuten henkilökohtaisesti sellaisia tietoja, jotka koetaan luottamukselliseksi. Näistä edellä mainituista syistä on oletettavaa, että henkilöt kokevat käsittelemiensä tietojen ja niiden tietoturvan merkityksen osana työtään tärkeänä.

Joukko, joka ei käyttänyt salasanan hallintajärjestelmää koki, että työssä käsiteltävät tiedot ja niiden tietoturva on merkityksellistä. Osa kuitenkin mainitsi liittyen nykyiseen työtehtävään, ettei käsittele juuri tällä hetkellä tietoja, jotka ovat erityisen luottamuksellisia, joten niiden tietoturvalla sinänsä ei ole niin merkitystä, koska ne ovat jo saatavilla julkisista lähteistä. Osa koki taas tietojen tietoturvan erittäin tärkeäksi juuri odotuksen mukaisesta syystä, eli tiedot ovat jonkun kolmannen osapuolen tietoja ja henkilöt kokivat olevansa vastuussa sekä moraalisesti, että lain näkökulmasta siitä, etteivät tiedot pääse vuotamaan muille.

Salasanan hallintajärjestelmää käyttävien henkilöiden osalta he kokivat, että tietoturva on heidän tekemässään työssä merkityksellistä johtuen hyvin pitkälti samoista syistä, kun edellä mainitussa kohdejoukossa. Useat henkilöt kertoivat haastattelussa nimenomaan huolensa siitä, että he käsittelevät työssään jonkun toisen henkilön luottamuksellisia tietoja ja niiden tulee olla turvassa sekä moraalisista, että lainsäädännöllisistä syistä.

Kysymyksen osalta odotuksen mukainen olettamus oli oikea, molemmissa osajoukoissa pidettiin tietoturvan merkitystä tärkeänä tai todella tärkeänä osana sitä työtä, jota henkilö tällä hetkellä tekee. Haastattelussa korostui myös henkilöiden moraalinen sekä lainsäädännöllinen vahvuus ja varsinaisia eroja osajoukkojen välillä ei ollut havaittavissa.

5.2.3 Kokemus salasanan hallintajärjestelmän turvallisuudesta

Molemmilta osajoukoilta kysyttiin miten he kokevat nykyisen tapansa hallita salasanoja olevan tietoturvallinen ja kokevatko he, että salasanojen hallintajärjestelmä on turvallinen. Odotuksena oli, että osajoukko, joka ei käytä

hallintaohjelmia pitäisi salasanan hallintajärjestelmäänsä ainakin osittain turvallisena ja salasanan hallintajärjestelmää käyttävä osajoukko turvallisena. Tämän päätelmän perustana on Protection Motivation Theory, jonka mukaan, kun ihmiset kokevat riskin uhkan tai toimintatavan olevan turvaton, he muuttavat toimintaansa. (Siponen & Baskerville, 2009).

Osajoukko, joka ei käyttänyt salasanan hallintajärjestelmää hieman yllättäen vastasi käytännössä jokaisen haasteltavan osalta, että he eivät koe heidän nykyisen salasanan hallintajärjestelmänsä olevan turvallinen. Kaksi vastaajaa kokivat nykyisen järjestelmän olevan osittain turvallinen, mutta eivät osanneet varsinaisesti perustalla miksi. Osittain tämä turvallisuuden tunne perustui siihen, että henkilöt kokivat heidän salasanojensa olevan perinteisillä mittareilla vahvoja, eli salasanat koostuvat useista eri sanoista, merkistönkoko vaihtelee, mukana on numeroita, erikoismerkkejä ja salasanan pituus on yli 12 merkkiä. Tämä kuitenkin luo valheellisen turvallisuuden tunteen, sillä nykyisin nimenomaan salasanojen uudelleen käyttö luo merkittävää uhkaa ja perinteisiä salasanojen väsytyshyökkäyksiä palveluita kohtaan havaitaan enää vain harvoin kuluttajien kohtaamissa palveluissa. Jokaiselle osajoukkoa edustavalle henkilölle esitettiin jatkokysymyksenä, miksi he eivät ole muuttaneet tapaansa, vaikka tietävät sen olevan turvaton. Tähän henkilöt vastasivat, että syitä ovat esimerkiksi motivaation puute, laiskuus ja se, etteivät he ole tietoisia, miten tilannetta voitaisiin parantaa ja minkälaisia työkaluja salasanan hallintaan on oikeasti tarjolla. Jokainen tiesi, että on olemassa salasanan hallintajärjestelmiä, mutta niitäkin on monia ja on vaikeata tietää mikä niistä on aidosti hyvä ja millä saadaan aikaan sekä käytettävyyden, että turvallisuuden kannalta hyvä lopputulos. Toisena jatkokysymyksenä tälle osajoukolle esitettiin kysymys, miltä heistä tuntuisi tallentaa kaikki salasanat johonkin palveluun, johon monet vastasivat, että se olisi heidän mielestään ihan käyttökelpoinen ratkaisu, mutta osa kuitenkin empi sen osalta, että onko sitten tämän palvelun turvallisuus taattu ja voiko palveluun todella luottaa. Henkilöitä kysyttiin vielä, että mikäli heille jokin luotettava tietoturvatietoinen henkilö suosittelisi palvelua, luottaisivatko he siihen silloin enemmän ja tämän jälkeen kaikki vastasivat, että kyllä se kasvattaisi heidän luottamustaan palveluun. Yksi vastaaja kuitenkin sanoi, että hän ei siltikään olisi valmis laittamaan kaikkia tärkeimpiä salasanojaan palveluun, mutta valtaosan kyllä.

Salasana managereita käyttävät henkilöt vastasivat kaikki kokevansa nykyisen tapansa hallita salasanoja olevan turvallinen tai ainakin niin turvallinen kun se kohtuullisella vaivalla voi tällä hetkellä olla. Osa salasanan hallintajärjestelmän käyttäjistä pohti valitsemansa palvelun luotettavuutta, mutta päätyivät kuitenkin siihen, ettei ole todennäköisesti tarjolla parempaakaan palvelua.

Näyttää siltä, että odotukset kysymyksen osalta olivat vääriä. Henkilöt eivät, jotka eivät käyttäneet salasanan hallintajärjestelmää kokivat, että salasanat ovat heikkoja ja heidän tapansa hallita salasanoja ei ole turvallinen. Kuitenkaan henkilöt eivät ole tehneet asialle käytännössä mitään ja salasanojen turvallisuus on uudelleen käytön vuoksi huonolla tasolla. Hälyttävää tästä osittain myös tekee se, että henkilöillä on vääränlainen turvallisuuden tunne sen osalta, että osa mainitsi kuitenkin, että käyttävät vahvoja salasanoja ja näin ainakin salasanojen taso on kunnossa, mutta uudelleen käyttö on todennäköisesti ongelma. Näyttää siltä, että henkilöiden motivaatio muuttaa toimintaa liittyy siihen, ette he eivät

koe riskin olevan riittävän suuri ja näin ollen on helppo jäädä käyttämään nyt helpoksi koettua tapaa hallinnoida salasanoja. Kaikki haasteltavat kuitenkin joko käyttivät tai olisivat valmiita käyttämään jotakin salasanan hallintajärjestelmää ja näyttääkin vahvasti siltä, että mikäli se olisi tehty helpoksi ottaa käyttöön niin henkilöt olisivat valmiita niitä ottamaan käyttöön, mikäli niitä jokin luotettava taho suosittelisi heille.

5.2.4 Tietoturvaan liittyvä henkilökohtainen uhka

Molemmilta joukoilta kysyttiin minkä he kokevat itselleen epämieluisaksi tietoturvatapahtumaksi tai uhkaksi. Kysymyksen tarkoituksena oli löytää hieman henkilöiden kokemia uhkia ja minkälainen tietoturvaan liittyvä tilanne voisi olla epämiellyttävää henkilöiden mielestä. Kysymyksen osalta odotus oli, että henkilöt kokisivat epämiellyttäväksi tilanteeksi erilaisia asioita riippuen omaan henkilökohtaiseen elämän tilanteeseensa. Kysymyksessä odotettiin nousevan taloudelliset menetykset sekä terveys- ja henkilötietoihin liittyvät tietoturva tapahtumat.

Osajoukko, joka ei käyttänyt salasanan hallintaohjelmaa nimesi käytännössä jokaisessa haastattelussa identiteettivarkauden tyyliset asiat mahdollisimman epämiellyttäväksi tietoturvatapahtumaksi ja uhkaksi. Tätä edelsivät yleensä vastaukset, jossa henkilöt kuvailivat melko tarkkaan identiteettivarkauden tyylisiä asioita kuten taloudellisten tietojen hyväksikäyttöä, henkilön rahojen tai tietojen käyttämistä hänen tietämättään sekä mikäli henkilönä voitaisiin esiintyä ja tehdä erilaisia taloudellisia sopimuksia kuten tavaroiden tilaamista. Mikäli henkilö itse kuvaili identiteettivarkautta, esitettiin heille jatkokysymyksenä, että tarkoittavatko he identiteettivarkauden tyylisiä asioita ja kaikki vastanneet reagoivat tähän vastaamalla hyvin saman tyylisesti ”kyllä, juuri sellaisia.”

Osajoukko, joka käytti salasanan hallintajärjestelmiä, kuvaili edellisen osajoukon tapaan hyvin saman tyylisiä asioita, joissa korostui identiteetti varkauden tyyliset asiat. Osa vastaajista myös kuvaili melko tarkasti tilannetta, jossa hänen mielestään yksi mahdollisimman epämiellyttävä tilanne voisi olla se, että hänen toimiensa takia työnantajana hallussa olevia tietoja pääsisi vuotamaan maailmalle.

Haastateltavissa molemmat osajoukot pitivät hyvin samanlaisia tietoturvaan kohdistuvia uhkia henkilökohtaisesti mahdollisimman epämiellyttävinä. Henkilöt pitivät erityisesti haitallisena tapahtumia, jotka voisivat vaikuttaa heidän taloudelliseen elämäänsä. Molemmissa osajoukoissa henkilöt kuvailivat hyvin tarkasti identiteettivarkauden tyylisiä asioita ja niiden olevan epämiellyttäviä sekä haitallisia. Osa henkilöistä mainitsi myös terveydelliset tiedot, jotka koetaan luonnollisesti hyvin henkilökohtaisiksi ja niiden vuotamisen erityisen epämiellyttäväksi. Osa henkilöistä myös mainitsi, että työssä käsiteltävien tietojen vuotaminen oman huolimattomuuden takia olisi erityisen epämiellyttävää. Odotusten vastaisesti näyttää siltä, että kaikki haastatteluun vastanneet pitivät identiteetti varkauden tyylisiä asioita erityisen epämiellyttävänä. Mikäli henkilöihin halutaan vaikuttaa esimerkiksi Protection Motivation Theoryn (Siponen &

Baskerville, 2009). kautta silloin identiteetti varkauksien käyttäminen esimerkkinä voisi olla sekä perusteltua, että toimivaa.

5.3 Käyttöön liittyvä vaiva

Laadullinen haastattelu tutkimus toteutettiin niin, että siinä käytettiin hyväksi Unified Theory of Acceptance And Use of Technology- viitekehystä, jossa käyttöön liittyvä vaiva on yksi tutkittavista ulottuvuuksista, kun henkilöt ottavat tai jättävät ottamatta käyttöön uusia teknologioita. (Venkatesh yms., 2003). Tarkoituksena on löytää viitekehyksen hengessä erilaisia tekijöitä, joilla voitaisiin löytää syitä henkilöiden kokemiin etuihin, kun tarkastellaan palveluiden käyttämiseen tai käyttämättä jättämiseen liittyvää koettua vaivaa.

5.3.1 Omassa hallinta tavassa koettu helppous

Haastatteluun osallistuneilta kysyttiin, miten he kokevat kirjautumisprosessiinliittyvää vaivaa ja minkä he erityisesti kokevat helpoksi liittyen valitsemaansa salasanan hallintajärjestelmään. Odotuksena kysymykselle oli, että salasanan hallintajärjestelmää käyttävät kokevat kirjautumisen nopeaksi ja helpoksi, kun taas henkilöt, jotka eivät käytä järjestelmää kokevat hallinnoimisen salasanoissa helpoksi. Tämä perustuu siihen, että yleisesti salasanan hallintajärjestelmää käyttävillä henkilöillä on usein käytössä internet selaimessa laajennus, joka täyttää heille kirjautumiseen liittyvät tiedot automaattisesti. Salasanan hallintajärjestelmää käyttämättömät henkilöt taas joutuvat muistelemaan salasanan ja mikäli siitä on useita eri versioita, kokeilemaan mikä tähän kyseiseen palveluun on sopiva salasana.

Salasanan hallintajärjestelmää ei käyttävä osajoukko koki omaan tapaansa hallinnoida salasanoja helpoksi sen, että salasana on ainakin näennäisesti aina saatavilla, kun sitä tarvitaan. Henkilöt kokivat myös, että kirjautuminen palveluihin on helppoa, sillä usein heillä on vain muutamia salasanoja, joita täytyy kokeilla ennen, kun palveluun löytyy oikea salasana. Useat henkilöt kuitenkin lisäsivät heti tämän jälkeen, että he kokevat vaikeaksi sen, että usein joutuvat sekä kokeilemaan useita eri vaihtoehtoja ja mahdollisesti myös jopa nollaamaan salasanan käyttämällä sähköpostiin tulevaa salasanan vaihtolinkkiä. Yksi haastateltavista myös koki erityisen harmillisena palvelut, jotka menevät lukkoon, kun on kokeillut salasanaa muutamia kertoja, sillä tämä on altis tapahtumaan varsinkin silloin kun täytyy kokeilla useista eri salasana muunnoksista, mikä on tähän kyseiseen palveluun sopiva salasana. Eräs vastaaja vastasi kysymykseen kuvaavasti, *"Arkielämässä ne muutamat salasanat on niin tuttuja ja iskostuneet selkärankaan, että kirjautuminen on tosi helppoa."*

Salasanan hallintajärjestelmää käyttävä osajoukko koki odotusten mukaisesti, että kirjautumisen palveluihin olevan erityisen helppoa sillä yleisesti salasanan hallintajärjestelmä täytti heille valmiiksi salasanan, jota he tarvitsivat ja

oikean palveluun. Osa myös mainitsi, että rekisteröityminen koettiin erityisen helpoksi, sillä rekisteröitymishetkellä salasanan hallintaohjelma ehdotti generoitua salasanaa käytettäväksi ja tallennettavaksi palveluun. Eräs vastaaja vastasi hyvin kuvaavasti hänen kokemustaan salasananhallintajärjestelmän käytöstä sanomalla: *"Se kirjautuminen menee vaan smuutisti!"*

Kirjautumiseen liittyvän helppouden koettiin pitkälle liittyvän salasanan muistamiseen osajoukossa, joka ei käyttänyt hallintaohjelmia ja käytettävyyden näkökulmasta tämä on hyvä asia, kuitenkin tietoturvan näkökulmasta salasanojen uudelleen käyttäminen on yksi yleisimmistä ja huonoimmista käytännöistä, johon käyttäjät syyllistyvät. Salasanan hallintaohjelmien käyttäjistä valtaosa koki, että kirjautuminen palveluihin on todella helppoa ja nopeata, kuten oletettiinkin. Tämä johtuu siitä, että käytännössä käyttäjän ei tarvitse muistaa salasanaa tai edes, onko hänellä tiliä kyseiseen palveluun, sillä salasanan hallintaohjelman selainlaajennus täyttää käyttäjätunnuksen ja salasanan automaattisesti palveluun. Näyttää haastatteluiden valossa siltä, että salasanan hallintajärjestelmän käyttämisessä on käyttäjälle tietoturvan lisäksi myös käytettävyyteen liittyviä etuja, sillä käyttäjän ei tarvitse nähdä sitä vaivaa, että hän kokeilee mahdollisesti useita eri salasanoja palveluun.

5.3.2 Omassa hallinta tavassa koettu vaikeus

Haastatteluun osallistuneilta kysyttiin, miten he kokevat kirjautumisprosessiinliittyvää vaivaa ja minkä he erityisesti kokevat vaikeaksi liittyen valitsemaansa salasanan hallintajärjestelmään. Odotuksena kysymykselle oli, että salasanan hallintajärjestelmää käyttävät eivät koe juurikaan vaikeaksi kirjautumiseen liittyviä asioita vaan vaikeaksi koetaan esimerkiksi asioita, jotka liittyvät salasanan hallintajärjestelmän toimivuuteen erikoistilanteissa, jotka ilmenevät muulloin, kun peruskirjautumisen aikana. Salasanan hallintajärjestelmää ei käyttävän osajoukon osalta odotuksena on, että he kokevat nimenomaan kirjautumisen ja siihen liittyvän salasanojen muistamisen vaikeaksi.

Osajoukko, joka ei käyttänyt salasanan hallintajärjestelmää kokivat vaikeaksi tilanteet, jossa he kirjautuvat järjestelmään, mutta eivät muista salasanaa oikein. Osajoukon vastauksissa korostui selkeästi se, että salasanoja unohdellaan ja niihin liittyy vaivaa. Yksi haastateltava myös huomautti erityisen vaikeaksi tilanteen, jossa järjestelmä pakottaa salasanan vaihdon, jolloin salasana pitäisi keksiä uudelleen ja muistaa sen jälkeen. Yksi vastaajista vastasi salasanojen unohteluun liittyvään vaikeuteen seuraavasti: *"Tänään viimeksi jouduin ressuttamaan salasanan ja se oli kyllä taas niin ärsyttävää."*

Salasanan hallintajärjestelmää käyttävä osajoukko kuvaili odotetusti erilaisia ongelmia, joita he kohtaavat valitsemansa salasanan hallintajärjestelmän käytössä. Erityisesti kahdella vastaajalla toisistaan riippumatta nousi esille F-secure key palveluun liittyen käyttöliittymän hankaluus. Eräs käyttäjä myös muisteli tilannetta, jossa oli lukinnut itsensä ulos salasanan hallintajärjestelmästä ja hän joutui uusimaan kaikki salasanansa sekä salasananhallintajärjestelmässä olevan käyttäjätilin, hän tosin myös kertoi tämän kasvattaneen luottamusta palveluun, sillä palvelussa olevat tiedot ovat niin turvassa, ettei edes palvelun ylläpito pääse

niitä näkemään. Muutamat henkilöt kuvailivat myös tilanteita, joissa heillä käytössä olevan puhelimen käyttöliittymä ei tukenut salasanan hallintajärjestelmää riittävän saumattomasti ja se aiheutti kirjautumiseen lisää hankaluuksia. Eräs vastaaja kuvasi hyvin käyttöliittymään liittyvää hankaluutta sanomalla: *"Oon monta vuotta ihmetellyt mitä ne ikonit siinä on, mutta en vieläkään tiedä."*

Kysymyksen osalta näyttää siltä, että salasanan hallintajärjestelmää käyttävät henkilöt eivät koe varsinaisesti kirjautumisprosessia hankalaksi vaan ainoastaan erikoistilanteita, joihin he saattavat joutua käyttäessään salasanan hallintaa. Salasanan hallintajärjestelmää ei käyttävä osajoukko sen sijaan kuvaili useissa tilanteissa nimenomaan kirjautumiseen liittyviä tilanteita ja tilanteita, jotka liittyvät salasanojen unohtamiseen. Nämä tilanteet ovat nimenomaan sellaisia tilanteita, joissa salasanan hallintajärjestelmä voisi auttaa käyttäjää ja poistaa tilanteen ongelman.

5.3.3 Salasanan uusiminen käyttämällä unohdin salasanani palvelua

Molemmilta osajoukoilta kysyttiin, joutuvatko he käyttämään usein unohdin salasanani palvelua verkkopalveluissa. Tällä tarkoitetaan palvelua, jolla voidaan vaihtaa salasana käyttämällä hyväksi esimerkiksi sähköpostiin tulevaa linkkiä, josta voidaan asettaa uusi salasana, kunhan käyttäjällä on pääsy palveluun rekisteröityyn sähköpostiin. Odotuksena kysymykselle oli, että koska salasanan hallintajärjestelmä muistaa salasanat ei hallintajärjestelmää käyttävä osajoukko joudu turvautumaan tähän juuri koskaan ja näin ollen kokevat tästä aiheutuvan vaivan olevan vähäistä. Toisaalta osajoukko, joka ei käytä salasanan hallintajärjestelmää todennäköisesti joutuu käyttämään kyseistä palvelua usein, sillä he eivät muista salasanojaan tai käyttävät niistä sellaisia muunnelmia, joita eivät pysty toistamaan aina tarpeen vaatiessa.

Osajoukko, joka ei käyttänyt salasanan hallintajärjestelmää käytännössä poikkeuksetta kertoi joutuvansa turvautumaan, unohdin salasanani palveluun usein. Osa vastaajista sanoi, joutuvansa turvautumaan siihen viikoittain. Kysymyksessä ei esiintynyt juurikaan minkäänlaista hajontaa, kaikki vastaajat joutuivat turvautumaan tähän vaihtoehtoon odotetusti usein.

Osajoukko, joka käytti salasanan hallintajärjestelmää ei omien kertomustensa mukaan joutunut juuri koskaan tai vain harvoin käyttämään unohdin salasanani palvelua. Valtaosa vastaajista jäivät miettimään milloin he ovat joutuneet käyttämään palvelua ja osa vastasi, että yleisesti tämä koskee sellaisia palveluita, jotka on rekisteröity ennen salasanan hallinnan käyttöönottoa ja niitä ei ole koskaan tallennettu salasanan hallintajärjestelmään. Monet vastaajat myös kertoivat, että he ovat joutuneet turvautumaan kyseiseen palveluun usein ennen hallinnan käyttöönottoa.

Näyttää siltä, että tässä osassa odotukset olivat oikeassa ja salasanan hallintaa käyttävät eivät joudu turvautumaan palveluun usein, kun taas toinen osajoukko joutuu turvautumaan usein. Tämä johtuu hyvin pitkälle jo siitä yksinkertaisesta asiasta, että salasanan hallintajärjestelmän tarkoitus on muistaa henkilön salasanat, jotta käyttäjän ei niitä tarvitse itse muistaa. Tällöin tilanne väkisin ajaa

siihen tilanteeseen, että henkilö ei joudu turvautumaan palveluun, kun salasana on digitaalisessa salasanan hallinnassa tallessa. Tässäkin tapauksessa voidaan todeta, että digitaalinen salasanan hallintajärjestelmä tuntuu vähentävän käyttäjän kokemaa vaivaa ja samalla kasvattamaan tietoturvan tasoa. Eräs vastaaja, joka käytti salasanan hallintajärjestelmää vastasi kuvaavasti: *"Mä lähinnä joudun turvautumaan sellaisissa palveluissa, mitä en ole käyttänyt sen jälkeen, kun otin lastpassin käyttöön."*

5.3.4 Kirjautumiseen liittyvä vaiva

Haastateltavilta kysyttiin suoraan, että kokevatko he palveluihin kirjautumisen vaivanloiseksi. Tämä kysymys esitettiin suoraan osajoukolle, joka ei käyttänyt salasanan hallintajärjestelmää. Osajoukolle, joka käytti salasanan hallintajärjestelmää, kysymys esitettiin muodossa, jossa kysyttiin, onko heidän näkemyksensä mukaan palvelun käyttöönottaminen vähentänyt vai lisännyt koettua vaivaa kirjautumisessa. Kysymystä esitettiin toiselle osajoukolle eri muodossa siitä syystä, että hallintajärjestelmää käyttävät olivat jo aiemmin kuvailleet käytännössä kaikissa tapauksissa kirjautumisen olevan helppoa.

Valtaosa hallintajärjestelmää käyttämättömistä henkilöistä koki, että kirjautuminen on vaivanloista ja sen olevan hankalaa. Osa koki, että itse kirjautuminen on helppoa, sillä käytössä on ainoastaan yksi salasana ja sillä pääsee sisälle joka paikkaan. Osa myös mainitsi, että tallentavat osan salasanoista selaimen salasanan hallintaan, jolloin kirjautuminen on todella suoraviivaista ja helppoa. Tämä toisaalta on juuri se, mitä voitaisiin saavuttaa salasanan hallintaohjelmalla ja salasanan hallintaohjelman etuja ei voida vielä tällä saavuttaa sillä salasanat ovat edelleen uudelleen käytettyjä.

Salasanan hallintajärjestelmää käyttävät olivat useampaan otteeseen jo kuvailleet salasanan hallinnan kautta saatua helppoutta kirjautumiseen, jolloin he kokivat kirjautumisen itsessään olevan varsin helppoa. Kysymys esitettiinkin tästä syystä tälle osajoukolle tavalla, jossa pyrittiin löytämään vastaus siihen, onko salasanan hallinnan käyttöönotto helpottanut vai vaikeuttanut heidän kirjautumistaan. Käytännössä kaikki henkilöt kokivat, että salasanan hallintajärjestelmä on helpottanut heidän kirjautumistaan. Yksi haastateltava totesi, että *"kirjautumiseen on periaatteessa tullut yksi lisä vaihe"*, mutta sen ei koettu kuitenkaan varsinaisesti kasvattanut merkittävästi koettua vaivaa.

Näyttää siltä, että henkilöt, jotka muistavat salasanat mielessään kokevat kirjautumisprosessin vaivanloiseksi ja osittain hankalaksi. Tähän mainittuja syitä ovat salasanojen unohtaminen ja eri variaatiot salasanasta, jolloin on hankala muistaa, mikä sopii juuri tähän palveluun. Salasanojen hallintajärjestelmää käyttävien käyttäjien osalta taas kirjautuminen koettiin helpoksi ja suoraviivaiseksi. Salasanan hallintajärjestelmän käyttöönoton koettiin myös helpottaneen kirjautumista ja vähentäneen siihen liittyvää vaivaa.

5.3.5 Hallintajärjestelmän käyttö verrattuna aiempaan menetelmään

Salasanan hallintajärjestelmää käyttävältä joukolta kysyttiin, miten he vertaisivat nykyistä ja aiempaa tapaansa hallita salasanoja. Haastateltavilta kysyttiin myös suoraan, onko järjestelmän käyttöönotto helpottanut vai vaikeuttanut päivittäistä kirjautumista, mikäli se ei tullut vertailussa esille. Kysymyksen odotuksena oli, että nykyisellä järjestelmällä olisi helpotettu ja nopeutettu heidän kirjautumisprosessiaan verrattuna edelliseen.

Käyttäjät kokivat, että salasanan hallintajärjestelmän käyttöön menee vaikeasta pääsalasanasta johtuen ainakin ensimmäisellä kirjautumiskerralla hieman pidempään aikaa, kun aiemmin. Käyttäjät kuitenkin kuvailivat tapahtumaan menevän muutamia sekunteja enemmän aikaa, joka sinänsä viestii siitä, että varsinaisestisalasanan hallintajärjestelmän käyttöönotto ei kasvattanut merkittävästi kirjautumiseen käytettyä aikaa, mutta kysymyksen asettelussa haastateltavaa ehkä johdatettiin siihen suuntaa. Osa käyttäjistä vastasi, että kirjautuminen on ehdottomasti nopeutunut ja eräs vastaaja sanoi, että *"nykyisin tarvii vaan klikata ja ollaan sisässä."* Osa vastaajista myös sanoi, että kirjautuminen on merkittävästi nopeutunut ja samalla muuttunut turvallisemmaksi. Eräs vastaaja korosti sitä, että samaan aikaan kun salasanojen uudelleen käyttö on loppunut, on salasanojen taso parantunut merkittävästi, koska hän generoi aina maksimimerkki määrän salasanaksi rekisteröityessään palveluihin.

Käyttäjät, joilta kysyttiin, onko salasanan hallinta helpottanut vai vaikeuttanut päivittäistä kirjatumista vastasivat odotetusti, että pääsääntöisesti nykyinen järjestelmä helpottaa kirjautumista. Eräs käyttäjä korosti myös tässä kohtaa, että salasanan hallintajärjestelmän käyttöönottaminen on ehdottomasti tehnyt kirjautumisesta turvallisempaa, joka viestii siitä, että käyttäjät kokevat olevansa paremmin turvassa käyttäessään salasanan hallintaohjelmaa. Käyttäjät myös kokivat, että kirjautumiseen on tullut toki yksi lisä vaihe lisää ainakin, kun selain käynnistetään, mutta tämä yksi vaihe vähentää vaivaa muissa kirjautumisissa. Yksi käyttäjistä, joka kertoi edelleen opiskelevansa, että hänelle päänvaivaa aiheutuu opiskelupaikkansa tietojärjestelmiin kirjautuminen, sillä silloin hänen on haettava puhelimen salasana ohjelmistolla salasana ja käsin kirjoitettava se merkkimerkiltä salasana kenttään, tämän hän koki selkeästi kasvattaneen vaivaa edelliseen nähden. Mutta hän lisäsi kuitenkin kokevansa, että muissa tapauksissa salasanan hallintaohjelma on selkeästi vähentänyt vaadittavaa vaivaa.

Näyttää siltä, että haastateltavien mielestä salasananhallintaohjelma on vähentänyt heidän kokemaansa vaivaa ja helpottanut kirjatumista suhteessa salasanojen muistamiseen. Käyttäjät kokivat, että vaikeiksi muodostuvat erikoistilanteet, jolloin salasanan kopiointia ei syystä tai toisesta päästä käyttämään. Näyttääkin siltä, että pääsääntöisesti päivittäisessä käytössä salasanan hallintaohjelma parantaa käyttäjän käyttökokemusta, vähentää vaivaa sekä nopeuttaa kirjautumista.

5.4 Sosiaalinen hyväksyntä

Laadullinen haastattelu tutkimus toteutettiin niin, että siinä käytettiin hyväksi unified theory of acceptance and use of technology viitekehystä, jossa käyttöön liittyvä sosiaalinen hyväksyttävyys on yksi tutkittavista ulottuvuuksista, kun henkilöt ottavat tai jättävät ottamatta käyttöön uusia teknologioita. (Venkatesh yms., 2003). Tarkoituksena on löytää viitekehyksen hengessä erilaisia tekijöitä, jotka henkilöt kokevat edistävän tai estävän salasanan hallinta järjestelmän käyttöönottoa sosiaalisesta näkökulmasta.

5.4.1 Toisen henkilön suositukset

Molemmilta osajoukoilta kysyttiin, onko joku henkilö suositellut heille salasanan hallintajärjestelmän käyttöönottoa. Odotuksena kysymyksessä oli, että molemmille osajoukoille tätä on suositeltu, sillä molemmat olivat joko käyttäjiä tai tietoisia siitä, mitä salasanan hallintajärjestelmät ovat. Molemmille osajoukoille esitettiin myös kysymys, joko miksi he eivät ole ottaneet hallintajärjestelmää käyttöön tai miksi he ovat ottaneet sellaisen käyttöön.

Osajoukko, joka ei käyttänyt salasanan hallintajärjestelmää vastasi kysymykseen myöntävästi ja joku henkilö oli heille suositellut salasanan hallintajärjestelmää. Kaikille sellaista oli suositeltu ja jatkokysymyksenä heille esitettiin kysymys, miksi eivät kuitenkaan olleet ottaneet järjestelmää käyttöön. Tähän kysymykseen vastaukset vaihtelivat jonkin verran ja vastauksissa näkyi se, että käyttäjät eivät oikein tienneet minkä järjestelmän ottaisivat käyttöön. Toisaalta osa käyttäjistä koki, että heidän motivaationsa ei riitä ja uhka ei vaikuta riittävän suurelta, että kannattaisi muuttaa hyväksi todettua toimintatapaa. Toisin sanoen, realistiseksi koetun uhkan puuttuessa henkilöitä tuntui puuttuvan motivaatio ottaa salasanan hallintajärjestelmää käyttöön.

Osajoukko, jolla oli käytössä salasanan hallintajärjestelmä, oli myös suositeltu salasanan hallintajärjestelmää otettavaksi käyttöön. He olivat myös käytännössä kaikki suositelleet tai ainakin maininneet asiasta eteenpäin muille henkilöille. Käyttäjille esitettiin kysymys, mikä sai heidät loppujen lopuksi ottamaan järjestelmän käyttöön. Tähän henkilöillä oli erilaisia vastuksia, osa henkilöistä vastasi, että salasanojen määrä alkoi kasvaa niin suureksi, että niiden hallinnoinnista tuli käytännössä mahdotonta ja elämästä hankalaa kirjautumisten kanssa. Eräs käyttäjä mainitsi, että hän kuuli toistavansa huonoja salasana käytäntöjä ja olevansa salasanojensa osalta juuri sellainen käyttäjä, jonka palveluihin olisi helppo murtautua ja tästä syystä hän otti palvelun käyttöön. Yksi käyttäjistä kertoi, joutuneensa tietomurron uhriksi ja sen myötä halunneensa parantaa omaa henkilökohtaista tietoturvaansa. Mielenkiintoinen vastaus, joka nousi eräältä käyttäjältä, oli hänen pohdintansa siitä, että hän ei tiennyt saako tällaista järjestelmää ottaa käyttöön työpaikalla vai onko se säätöjen vastaista. Oikein käytettynä tällainen järjestelmä parantaa merkittävästi käyttäjän tietoturvaa ja siitä syystä sen tulisi ehdottomasti olla sallittu organisaatioissa. Mielenkiintoista tässä

on se, että on helppoa ymmärtää käyttäjän käymä polku siitä, että hän tallentaa organisaation järjestelmiin sopivia salasanoja jonkin kolmannen osapuolen palveluun ja tämä saattaisi olla vastoin tietoturvapolitiikkaa. Kuitenkaan tällaiselle ei varsinaisesti ole perustetta, kun korkean turvaluokituksen yrityksissä ja tästä syystä tämä on yksi kysymys, joka olisi hyvä yritysten ottaa huomioon ja suositella käyttäjilleen salasanan hallintajärjestelmien käyttöönottoa.

Näyttää vahvasti siltä, että salasanan hallintajärjestelmistä on kuultu ja niitä on suositeltu molemmille osajoukoille. Toinen osajoukko ei ole vain kokenut riittävää motivaatiota ja riittävää realistista uhkaa, jotta olisi tarpeellista muuttaa käyttäytymistä. Näyttää myös siltä, että salasanan hallintajärjestelmän käyttöön liitetään edelleen merkittävästi vaivaa sekä opettelua, mutta ei kuitenkaan vaikuta siltä, että salasanan hallintajärjestelmien käyttöönottoa estäisi mikään sosiaalinen seikka.

5.4.2 Hallintajärjestelmän vastaanotto suositeltaessa

Salasanan hallintajärjestelmää käyttäviltä käyttäjiltä kysyttiin, minkälaisia asenteita he ovat kohdanneet kertoessaan, että he käyttävät salasanan hallintajärjestelmää. Kysymykselle ei varsinaisesti ollut mitään odotettua vastausta vaan, tavoitteena oli selvittää miten he ovat kokeneet muiden ihmisten palautteen kertoessaan käyttävänsä salasanan hallintajärjestelmää.

Käyttäjät kertoivat keskusteluissa kohdanneensa ihmetystä siitä, että miksi he toimivat näin. Kuitenkin käyttäjien selitettyä, yleisesti vastaanotto on ollut positiivista ja kannustavaa. Käyttäjät myös kertoivat, että keskusteluissa heitä on pidetty tietoturvan osalta edelläkävijöinä ja edistyneinä käyttäjinä heidän hallintatapansa vuoksi.

Varsinaisesti kysymyksen ympärillä ei havaittu mitään negatiivista tai positiivista sosiaalista vaikutusta. Näyttää siltä, ettei sosiaalisilla tekijöillä ole varsinaisesti suurta vaikutusta otetaanko hallintajärjestelmää käyttöön vai ei.

5.5 Suorituskykyyn liittyvät odotukset

Laadullinen haastattelu tutkimus toteutettiin niin, että siinä käytettiin hyväksi unified theory of acceptance and use of technology viitekehystä, jossa suorituskykyyn liittyvät odotukset ovat yksi tutkittavista ulottuvuuksista, kun henkilöt ottavat tai jättävät ottamatta käyttöön uusia teknologioita. (Venkatesh yms., 2003). Tarkoituksena on löytää viitekehyksen hengessä erilaisia tekijöitä, jotka käyttäjät kokevat olevan käyttöönotettavan teknologian suorituskyvyn kannalta merkityksellisiä. Suorituskykyyn liittyviä odotuksia käsitteleviä kysymyksiä kysyttiin ainoastaan salasanan hallintajärjestelmän käyttöönottaneelta populaatiolta, sillä heille voitiin esittää jatkokysymyksenä: toteutuivatko heidän odotuksensa liittyen järjestelmää.

5.5.1 Odotukset liittyen salasanan hallintajärjestelmään

Haastattelussa hallintajärjestelmään liittyviä odotuksia kysyttiin osajoukolta, joka oli ottanut käyttöön salasanan hallintajärjestelmän. Odotuksena oli, että henkilöt odottaisivat kyseisen teknologian helpottavan heidän kirjautumistaan, vähentävän salasanojen muistamiseen liittyviä hankaluuksia ja helpottamaan päivittäistä palveluiden käyttöä.

Osa käyttäjistä kertoi, ettei heillä juurikaan ollut suuria odotuksia liittyen salasanan hallintajärjestelmään. Kuitenkin kun henkilöille annettiin hetki pidempään aikaa pohtia he yleensä, saivat mieleensä muutamia odotuksia. Näitä odotuksia olivat salasanojen uusimisen tarpeen väheneminen, jonka käyttäjät kokivat tässä ja toisessa kysymyksessä käytännössä loppuneen kokonaan. Käyttäjät kokivat myös, että salasanojen muistamisen tarve vähenisi ja niiden laatu paranisi. Toisaalta eräs käyttäjä kertoi, että hän uskoi kirjautumisen jonkin verran hidastuvan ja vaikeutuvan kun salasanan hallintajärjestelmä otetaan käyttöön, mutta hän myös kertoi, että näin ei kuitenkaan käynyt vaan hän koki tilanteen olevan täysin päinvastainen ja kirjautumiset ovat sen sijaan nopeutuneet jonkin verran.

Käyttäjille esitettiin jatko kysymyksenä, että kokevatko he, että heidän odotuksensa toteutuivat ja käyttäjät kertoivat pääsääntöisesti odotusten toteutuneen. Eräs käyttäjä kertoi F-secure keyn käytön olevan osittain hankalaa ja hän odotti käyttävänsä sitä enemmän, mutta näin ei kuitenkaan ole vaikea käyttöisyyden vuoksi käynyt. Pääsääntöisesti kuitenkin käyttäjät kokivat, että heidän odotuksensa täyttyivät ja osa jopa kertoi, että odotukset helppoudesta, mutkattomuudesta ja nopeudesta ylittyivät.

Näyttää siltä, että käyttäjien odotukset ja todellinen käyttökokemus kohtaavat salasanan hallintajärjestelmien käyttöönottamisen myötä. Osittain näyttää siltä, että käyttäjien odotukset voidaan jopa ylittää.

5.5.2 Tärkeät ja ei tärkeät ominaisuudet valitussa järjestelmässä

Haastattelussa salasanan hallintajärjestelmää käyttävältä joukolta kysyttiin mitkä ovat heidän mielestään tärkeimpiä sekä vähiten tärkeitä ominaisuuksia valitsemassaan salasanan hallintajärjestelmässä. Kysymyksen odotettuna tuloksena oli, että käyttäjille tärkeimpiä ominaisuuksia ovat helppo käyttöisyys, salasanojen muistamisen puuttuminen ja salasanojen kirjoittamisen puuttumisesta johtuva käytön helpottuminen. Vähemmän tärkeäksi ominaisuudeksi todennäköisesti käyttäjät listaavat salasanojen jakamiseen liittyvät ominaisuudet sekä muiden, kun käyttäjätunnuksien tallentamiseen liittyvät ominaisuudet.

Käyttäjille tärkeimpiä ominaisuuksia olivat haastatteluiden perusteella salasanojen tallentamisen mahdollisuus ja se, ettei salasanoja enää tarvitse itse muistaa. Vastauksissa korostui selkeästi käyttömukavuuteen liittyvät seikat, kuten selainliitännäisen rooli kirjautumisessa ja se kautta säästetty vaiva. Käyttäjät kokivat myös tärkeäksi järjestelmän saatavuuden eri käyttöjärjestelmille, jolloin salasanat ovat saatavilla kaikilla tarpeellisilla laitteilla jatkuvasti.

Mielenkiintoista kysymyksen osalta on, että ainoastaan yksi käyttäjä vastasi tietoturvaan liittyvän seikan ja hän koki salasanan hallinnan kasvattavan henkilökohtaista turvallisuuden tunnetta.

Vähemmän tärkeiksi ominaisuuksiksi käyttäjät listasivat erilaiset henkilökohtaisen tietoturvan analysointiin liittyvät työkalut sekä muiden tietojen kuin salasanojen tallentamisen. Käyttäjät eivät varsinaisesti kokeneet mitään täysin hyödyttömäksi ja näin ollen useat myös vastasivat, etteivät osaa sanoa mitään täysin hyödytöntä ominaisuutta. Osaltaan tässä saattoi vaikuttaa myös kysymyksen asettelu, jossa haastattelija saattoi epäonnistua.

Yhteenvetona näyttää siltä, että käyttäjille heidän vaivaansa poistavat ja saatavuutta kasvattavat tekijät ovat tärkeitä. Tällaisiksi tekijöiksi käyttäjät listasivat salasanan automaattinen täyttö sekä saatavuus useilla eri laitteilla. Hyödyttömiksi ominaisuuksiksi käyttäjät tuntuivat kokevan muiden tietojen tallentamisen salasanan hallintajärjestelmään.

5.6 Käyttöä estävät ja edistävät olosuhteet

Laadullinen haastattelu tutkimus toteutettiin niin, että siinä käytettiin hyväksi unified theory of acceptance and use of technology viitekehystä, jossa käyttöä edistävät olosuhteet ovat yksi tutkittavista ulottuvuuksista, kun henkilöt ottavat tai jättävät ottamatta käyttöön uusia teknologioita. (Venkatesh yms., 2003). Tarkoituksena on löytää viitekehyksen hengessä erilaisia tekijöitä, jotka käyttäjät kokevat edes auttavan käyttöä, sekä käyttöönottoa ja toisaalta sellaisia, jotka estävät käyttöä tai käyttöönottoa.

5.6.1 Tekijät, jotka edistivät salasanahallinta ohjelman käyttöönottoa

Käyttäjiltä kysyttiin erilaisia tekijöitä, jotka he kokivat edistäneen salasanan hallintaohjelman käyttöönottoa ja työntäneen heidät viimein sen kynnyksen yli, jonka jälkeen he ottivat salasanan hallintaohjelman käyttöön. Kysymyksen odotuksena ja perusteena oli, että käyttäjät ottavat salasanan hallintajärjestelmän käyttöön sen jälkeen, kun heidän oma turvallisuuden tunteensa järkkyy tietoturvan osalta syystä tai toisesta tai kun salasanan hallintajärjestelmää suositellaan heille riittävän hyvin perusteluin.

Haastatteluissa useat käyttäjät kertoivat, että heidän käyttöönottonsa tapahtui suosittelun jälkeen. Osassa tapauksissa suosittelijana oli toiminut tietoturvasta tietoinen henkilö, joka työskentelee tietoturva-alalla. Useat käyttäjät kertoivat myös syyksi sen, että salasanojen määrä kasvoi niin suureksi, että niiden järkevä hallinta ei enää ollut mahdollista. Eräs käyttäjä kertoi myös huolestuneensa siitä, että hän käytti kuulemansa perusteella juuri niitä heikko tasoisia salasanoja, jotka ovat helposti murrettavissa ja tämän takia koki oman tietoturva tasonsa heikoksi. Yksi käyttäjistä joutui itse tietomurron uhriksi ja tästä syystä hän etsi tapoja parantaa omaa tietoturvan tasoaan.

Näyttää siltä, että käyttäjät ottavat salasanan hallintajärjestelemiä käyttöön minimoidakseen salasanojen hallinnoinnista koostuvaa vaivaa, kun salasanojen määrä kasvaa liian suureksi. Käyttäjät kokivat myös halua parantaa omaa tietoturvan tasoa esimerkiksi tietomurron kokemisen jälkeen ja kun heille selkeni, että he toistavat perinteisiä tietoturva virheitä.

5.6.2 Käyttöönottoa hidastavat tekijät

Salasanan hallintajärjestelmää käyttäviltä henkilöitä kysyttiin, minkälaiset tekijät hidastivat heidän käyttöönottoansa siltä väliltä, kun he ottivat järjestelmän käyttöön ja kuulivat sellaisesta. Odotuksena oli, että käyttöönottoa lykkäsi koettu vaiva ja järjestelmän tuntemattomuus.

Haastatteluun vastanneet henkilöt vastaivat, että heidän käyttöönottoaan lykkäsivät se, etteivät tienneet mitä sovellusta tulisi käyttää ja miten se otetaan käyttöön. Käyttöönottoon liitettiin myös merkittävää vaivaa ja opettelua. Osa käyttäjistä myös koki, että aiemmin heidän salasanansa, jota he uudelleen käyttivät palveluissa, oli jo valmiiksi vahva salasana mittareiden mukaan ja sen pitäisi riittää, joten varsinaista salasanan hallintaohjelmaa ei ollut tarve käyttää. Kuitenkin, sama käyttäjä lisäsi, että hän joutui nimenomaan vuotaneen salasanan kautta tietomurron uhriksi ja sitä kautta hän oli hieman ihmeissään, että mitä tapahtui. Yksi käyttäjistä hieman yllättäen epäili työpaikallaan, että onko sallittua tallentaa salasanoja ulkopuoliseen järjestelmään ja hän otti hallintajärjestelmän käyttöön vasta kun sai siihen luvan työpaikkansa it-palveluilta.

Näyttää siltä, että käyttöön ottamisen hidasteena on se, että käyttäjät kokevat salasanan hallintaan liittyvän paljon vaivaa, vaikka todellisuudessa käyttöönottaminen on varsin nopeata ja suoraviivaista. Käyttäjät myös kokevat, että heidän salasanansa ovat jo nyt turvallisia, mikä saattaakin olla totta, mutta salasanan uudelleen käyttämisen takia ei ole käytännössä väliä, vaikka salasanat olisivat vahvoja. Lähinnä ne vain tuhoavat käyttökokemuksen, sillä salasanat ovat vaikeita kirjoittaa. Näyttää siltä, että käyttäjät tarvitsisivat hieman opastusta alkuun, jotta salasanan hallintajärjestelmä tulisi otettua käyttöön. Ensimmäisten kirjautumisten jälkeen käyttötapaukset ovat sen verran suoraviivaisia, että niistä käyttäjä todennäköisesti selviytyy melko kevyellä vaivalla.

5.6.3 Käyttöönotossa tehtyjen ratkaisujen pitkäaikaiset vaikutukset

Kun teknologioita otetaan käyttöön, voidaan usein myöhemmin todeta, että joitakin ratkaisuja olisi voitu hoitaa järkevämmin. Myös salasanan hallintajärjestelmissä on tällaisia tilanteita ja haasteltavilta kysyttiin, olisiko heillä jotain käyttötapauksia, jotka he hoitaisivat nyt toisin, mikäli se olisi mahdollista, kun tarkastellaan palvelun käyttöönottoa. Kysymykselle ei ollut varsinaista odotettua tulosta, sillä kysymyksen osalta koettiin, että vastaukset ovat todennäköisesti hyvin subjektiivisia ja kuvaavat lähinnä yksittäisten käyttäjien subjektiivisissa tilanteissa kokemia asioita.

Valtaosalla haastateltavista esille nousi mahdollisuus kartoittaa hieman tarkemmin muita salasanan hallintaohjelmia, sillä käyttäjät valitsivat sen, josta he olivat kuulleet joltain suosittelevalta taholta. Käyttäjät mainitsivat myös, että pääsalasanan olisi voinut valita niin, että se olisi helpompi kirjoittaa mobiililaitteella sekä, että mahdollisissa ongelmatilanteissa olisi hyvä selvittää tavat palauttaa salasanan hallintaohjelman pääsy. Eräs käyttäjä kertoi, että hänen ongelmaksensa muodostui kaksivaiheisen tunnistamisen käyttöönotossa se, että hän ei tehnyt sitä riittävän hyvin, joka johti siihen, ettei käyttäjä enää päässyt salasanan hallintaansa käsiksi ja hän joutui käytännössä nollaamaan kaikki salasanat ja ottamaan koko hallinnan uudelleen käyttöön.

Näyttää siltä, ettei yksittäistä yhdistävää tekijää löydy, jonka voisi toteuttaa käyttöönotossa paremmin. Näyttää siltä, että käyttäjät tarvitsisivat yleisesti rekisteröitymisessä ja palvelun käyttöönotossa hieman ohjeistusta ja avustusta, jonka jälkeen käyttäminen olisi helpompaa ja suoraviivaisempaa. Sinänsä tämä ei ole yllättävää, sillä kaikkien uusien teknologioiden käyttöönottoon kuuluu aina jonkin verran vaivaa ja opettelua.

5.7 Yhteenveto haastatteluista

Tutkimukseen haastateltiin yhteensä 12 henkilöä, joista kaikki työskentelivät parhaillaan tai olivat aiemmin työskennelleet sosiaali- ja kasvatusalalla. Henkilöistä kahdeksan oli naisia ja neljä miehiä. Henkilöiden keski-ikä oli 25 vuotta. Henkilöistä puolet käyttivät salasanan hallintajärjestelmää ja puolet eivät käyttäneet. Haastattelut järjestettiin etänä vallitsevan koronaviruspandemian vuoksi ja haastatteluihin käytettiin alustana Zoom palvelua, jossa haastateltaviin oli sekä ääni, että puheyhteys. Ennen haastattelua henkilöille kerrottiin haastattelun kulku pääpiirteittäin sekä haastattelun luottamuksellisuuteen liittyvät asiat. Itse haastattelu tilanteessa haasteltavia muistutettiin vielä luottamuksellisuudesta ja kerrottiin haastattelu tilanteesta ja haastattelun etenemisestä. Haastatteluissa esiin tulleita eroja ja samankaltaisuuksia on esitelty taulukossa: Taulukko 2 Haastatteluiden vertailu.

Haastattelun aikana selvisi, että haastateltavilla on pääsääntöisesti kahdenlaisia tapoja hallita salasanoja. Nämä olivat hallinta muistamalla sekä hallinta digitaalisella salasanan hallintaohjelmalla. Lopputuloksena tämä ei ollut yllättävä sillä haasteltavat oli valittu tällä perusteella haastatteluihin. Haastatteluissa ei selvinnyt mitään merkittävää eroa ryhmien välillä teknologioiden omaksumisen ja teknologisen taustan suhteen. Kaikki haastateltavat olivat tekniseltä osaamiseltaan samaa tasoa ja kaikki ottivat sanomansa mukaan uusia teknologioita pääsääntöisesti käyttöön niiden yleistyessä. Salasanan hallintajärjestelmän käyttöönoton edistymistä ei siis voitu selittää sillä, että henkilöt ottaisivat uusia teknologioita alttiimmin käyttöön. Koetun tietoturvallisuuden tason osalta havaittiin selkeä ero ryhmien välillä. Käytännössä kaikki salasanan hallintajärjestelmää käyttävät henkilöt kokivat tapansa hallita salasanoja turvalliseksi. Vastavuoroisesti ei käyttävä joukko koki salasanan hallinnan muistamalla turvattomaksi. Myös salasanojen uudelleen käytössä, joka on aiemmin todettu eräänä hyvin haitallisena

tietoturva käytäntö, oli havaittavissa selkeä ero. Salananoja muistava joukko uudelleen käytti salasanoja. Osa henkilöistä kertoivat uudelleen käyttäneensä samoja salasanoja jo pitkään. Salasanan hallintaohjelmaa käyttävä osajoukko vastasi, ettei uudelleen käytä salasanoja. Tästä voidaan todeta, että salasanan hallintajärjestelmän käyttö ajaa henkilöitä pois haitallisesta salasanojen uudelleen käyttämisestä. Henkilöt päätyivät käyttämään salasanan hallintajärjestelmiä yleensä jonkun toisen henkilön suosituksesta ja sitä edesauttoi selkeät ohjeet sekä suositeltu salasanan hallintajärjestelmä. Muutamat henkilöt kertoivat päätyneensä myös tietomurron kokemisen jälkeen sekä kun salasanojen hallinta tuli mahdottomaksi liian suuren salasana määrän vuoksi. Salasanat muistava joukko koki, että heidän tapaansa hallita salasanoja oli lähinnä ajauduttu. Kenellekään ei ollut selkeätä selitystä sille, miksi he ovat päätyneet tällaiseen tapaan hallita salasanoja. On myös varsin loogista ajatella, että salasanojen uudelleen käyttäminen ja muistaminen on vähimmän vaivan vaihtoehto ja siihen on helppoa ajautua. Salasanan hallintaohjelmien käyttöönottoa hidastavat tekijät, jotka ilmenivät haastatteluissa, olivat niihin liittyvä monimutkaisuus ja sen kokeminen. Osa haasteltavista vastasi myös, että kynnys opetella uusia teknologioita, joiden käyttöön ei varsinaisesti nähdä riittävää motivaatiota on liian korkea. Osa haasteltavista myös vastasi, että he eivät tienneet mikä hallintajärjestelmä tulisi ottaa käyttöön eivätkä varsinaisesti osanneet tehdä vertailua niiden välillä, sillä ei ollut selvää mitkä ominaisuudet ovat tärkeitä. Haastatteluissa molemmilta ryhmiltä kysyttiin minkälaisia haittoja ja hyötyjä he kokivat liittyen salasanan hallintajärjestelmiin tai niiden muistamiseen. Hallintajärjestelmiä käyttävä joukko kertoi, että he kokevat kirjautumisen olevan helppoa ja nopeata sekä myös turvallista. He kokivat myös, että salasanojen muistaminen helpottaa stressaamista, kun on salasanat eivät unohdu. He myös vastasivat, etteivät joudu turvautumaan unohdin salasanani palveluun usein, joka kuvastaa, että salasanoja ei todella tarvitse unohtaa. He myös kuitenkin kokivat, että vaivaa on jonkin verran kasvattanut kirjautumiseen liittyvä yksi ylimääräinen vaihe sekä pienehkö opettelu liittyen valittuun salasanan hallintajärjestelmään. Salasanat muistamalla hallinnoiva joukko koki, että salasanojen uudelleen käyttämisen näkökulmasta kirjautuminen on helppoa ja nopeata, kunhan salasanat muistetaan. Salasanoja kuitenkin unohdetaan usein ja henkilöt kertoivat kaikki joutuvansa turvautumaan usein, unohdin salasanani palveluun. Henkilöt kokivat myös, että salasanojen muistamisesta tulee ylimääräistä vaivaa.

Haastatteluissa erona selkeästi oli havaittavissa, että muistamalla salasanoja hallinnoivan joukon tietoturvan taso on huonompi salasanojen uudelleen käytön vuoksi, kun salasanan hallintajärjestelmiä käyttävien. Joukkojen välillä oli myös huomattavissa selkeä ero suhteessa koettuun vaivaan ja käyttömukavuuteen. Myös turvallisuuden tunne oli selkeästi huonompi muistavalla joukolla. Haastatteluiden perusteella voidaan todeta, että salasanan hallintajärjestelmällä voidaan parantaa tietoturvaa sekä käyttömukavuutta.

	Salasanan hallintajärjestelmiä ei käyttävät	Salasanan hallintajärjestelmiä käyttävät
Asenteet ja arvot teknologiaa kohtaan	Ottavat teknologioita käyttöön usein niiden yleistyessä.	Ottavat teknologioita käyttöön yleensä niiden yleistyessä.
Asenteet ja arvot tietoturvaa kohtaan	Pitävät pääsääntöisesti tärkeänä, mutta eivät muuta käyttäytymistä sen perustella. Pitävät työelämässä tärkeämpänä, kun omassa elämässään.	Pitävät tietoturvaa tärkeänä ja muuttavat käyttäytymistään sen perusteella. Pitävät työelämässä tärkeämpänä, kun omassa elämässään.
Salasanoihin liittyvä vaiva	Kokevat kirjautumisen ja muistamisen vaivalloisena. Joutuvat usein palauttamaan salasanoja unohduksen vuoksi	Eivät koe kirjautumista ja salasanojen hallinnointia vaivanloisena. Eivät joudu juuri koskaan palauttamaan salasanoja unohtamisen vuoksi.
Pitävätkö tapaansa hallita salasanoja turvallisena	Kukaan haastateltavista ei pitänyt salasanojen muistamista täysin turvallisena.	Kaikki vastaajat pitivät salasanan hallintajärjestelmää niin turvallisena, kun se on mahdollista järjellisesti pitää.
Sosiaalinen hyväksyntä	Eivät koe salasanoihin tai niiden hallinnointiin liittyvää sosiaalista painetta. Ottaisivat käyttöön järjestelmän, jos luotettava taho sitä suosittelisi.	Eivät koe salasanan hallintana liittyviä sosiaalisia paineita. Valtaosa on ottanut käyttöön hallintajärjestelmänsä toisen henkilön suosituksesta.
Epämiellyttävin tietoturva tapahtuma	Kaikki vastasivat identiteettivarkaus joko nimeten sen suoraan tai kuvaillen sitä riittävän tarkasti.	Kaikki vastasivat identiteettivarkaus joko nimeten sen suoraan tai kuvaillen sitä riittävän tarkasti.
Salasanan hallintaan liittyvät suorituskyky odotukset	Salasanojen muistamisen osalta odotetaan, että ne ovat aina saatavilla, kun niitä tarvitaan.	Salasanan hallintajärjestelmältä odotetaan, että se vähentää salasanojen muistamista ja helpottaa kirjautumista.
Käyttöönottoa edistävät olosuhteet ja tekijät	Voisivat ottaa salasanan hallintajärjestelmän käyttöön, jos sitä suosittelisi heille luotettava taho.	Valtaosa on ottanut salasanan hallintajärjestelmän käyttöön, kun sitä on suositellut heille luotettava taho. Henkilökohtaisesti koettu tietomurto sekä salasanojen kasvanut määrä toimivat myös edistävänä tekijänä.
Käyttöönottoa hidastavat olosuhteet ja tekijät	Motivaation puute, tietämättömyys hallinnointi järjestelmien eroista, väärä turvallisuuden tunne nykyisestä tavasta sekä suosittelun puute.	Motivaation puute, tietämättömyys hallinnointi järjestelmien eroista, väärä turvallisuuden tunne nykyisestä tavasta sekä suosittelun puute.

Taulukko 2 Haastatteluiden vertailu

6 Pohdinta

Tässä pro gradu- tutkielmassa tutkittiin salasanoja ja niiden hallintajärjestelmiä. Tarkastelussa olivat kolme tapaa hallita salasanoja, muistaminen, paperille kirjaaminen ja digitaaliset salasanan hallintajärjestelmät. Tutkimuksessa pyrittiin löytämään vastauksia seuraaviin tutkimus kysymyksiin:

- Minkälaisia tapoja on hallinnoida salasanoja?
- Minkälainen tapa hallinnoida salasanoja on käytettävyyden ja tietoturvan näkökulmasta suositeltavin?
- Minkälaiset tekijät edesauttavat tai hidastavat salasanan hallintajärjestelmien käyttöönottoa?

Vastauksia pyrittiin löytämään tekemällä kirjallisuus katsaus salasanoihin ja hallintajärjestelmiin sekä haastattelemalla henkilöitä, jotka käyttävät salasanan hallintaa digitaalisesti ja henkilöitä, jotka eivät käytä. Haastatteluihin kutsuttiin 12 henkilöä, jotka ovat töissä tai ovat työskennelleet sosiaali- ja kasvatusalalla. Henkilöt valittiin, sillä ala on ei tekninen ja henkilöt käsittelevät tietoturvan näkökulmasta luottamuksellista materiaalia paljon työssään. Henkilöt haastateltiin verkon välityksellä käyttäen Zoom palvelua johtuen 2020 keväällä puhjenneesta covid19- pandemiasta.

6.1 Päälöydökset

Tutkimuksessa pyrittiin löytämään vastauksia tutkimus kysymyksiin, jotka on esitelty edellisessä kappaleessa ja ne käsitellään yksittäin tässä kappaleessa.

6.1.1 Tavat hallinnoida salasananoja

Tutkimuksessa selvisi, että salasanoja voidaan hallita kolmella eri tavalla, jotka ovat muistamalla mielessä, kirjoittamalla paperille ne ylös tai hallinnoimalla niitä digitaalisella salasanan hallintajärjestelmällä. Tämä näyttää olevan myös linjassa aiemman kirjallisuuden kanssa, sillä varsinaisesti muita yleisesti käytössä olevia tapoja ei löydetty. Jokaisella järjestelmällä on omat hyvät ja huonot puolensa kun niitä vertaillaan käytettävyyden ja tietoturvan näkökulmasta. Muistamalla huono puoli on salasanojen määrän rajallisuus, joka johtaa väistämättä salasanojen uudelleen käyttämiseen. Uudelleen käyttämisen riskinä on, että yhdestä palvelusta vuotanutta salasanaa voidaan käyttää muissa palveluissa ja näin käyttäjän tietoturva on uhattuna useassa palvelussa. Sama asia on myös laajalti esillä alan kirjallisuudessa sekä sen yleisyydestä kertoo myös se, että useat tietoturvapolitiikat ja tietoturva-alan artikkelit pyrkivät kertomaan sen salasana ohjeistukesssaan. Salasanoja voidaan hallita kirjaamalla niitä ylös paperille, joka kasvattaa mahdollisuutta käyttää uniikkeja salasanoja. Haastatteluissa kuitenkin

huomattiin, että vain harva käyttää tätä tapaa. Haastattelussa myös huomattiin, että henkilö, joka käytti tätä tapaa, uudelleen käytti salasanoja ainakin jonkin verran. Paperille kirjaamisen huonona puolena on myös salasanojen oleminen selkotekstinä, jolloin niiden varastaminen helpottuu merkittävästi. Salasanojen tallentaminen digitaalisesti tarkoitetaan niiden tallentamista joko käyttäjän omalla laitteelle tallennettavaan tietokantaan tai niiden tallentamista, jonkin palvelun tarjoajan tietokantaan. Salasanat tallennetaan tietokantaan salatussa muodossa ja käyttäjän oma pääsalasana toimii avaimena tähän tietokantaan. Tällöin käyttäjä tarvitsee oman pääsalasanansa, jotta hän pääsee käsiksi hänen tietokantaansa ja näin käyttäjän pääsalasana toimii avaimena. Digitaalisen salasanan hallintajärjestelmän etuina muihin nähtiin tietoturvan näkökulmasta se, että käyttäjän ei itse tarvitse muistaa salasanojaan, jolloin ne voivat olla täysin sattumanvaraisesti generoituja pitkiä merkkijonoja sekä uniikkeja jokaisessa palvelussa. Näin salasanojen uudelleen käyttö ei enää ole käyttäjän kohdalla tarpeellista. Käyttökokemuksen osalta haastatteluissa nousi esille käyttäjien kokema helppous kirjautumisessa, sillä käyttäjien ei tarvinnut itse kirjoittaa salasanoja salasana lomakkeisiin. Näin käyttäjien kirjautuminen nopeutui ja helpottui. Salasanan hallintajärjestelmissä pilvipohjaisista voitiin todeta, että tarkastelussa ollut Lastpass salaa salasanat käyttäjän laitteella ja avaa ne vasta kun ne on toimitettu käyttäjän laitteelle. Näin olleen ilman käyttäjän pääsalasanaa ne eivät ole tiedossa myöskään palvelun tarjoajalla ja tietoturvan näkökulmasta, mikäli käyttäjän pääsalasana on turvassa, on käyttäjän salasanat myös hyvin turvassa. Salasanan hallintajärjestelmän uhkana nähtiin se, että käyttäjä pystyy lukitsemaan itsensä ulos järjestelmästä unohtamalla salasanan tai hukkaamalla kaksi vaiheiseen tunnistamiseen käytettävän laitteen. Löydökset salasanojen uudelleen käytöstä ja tavoista hallita salasanoja ovat linjassa pääsääntöisesti aiemman kirjallisuuden ja tutkimuksen kanssa.

6.1.2 Tietoturvan ja käytettävyyden kannalta paras hallintatapa

Tietoturvan ja käytettävyyden näkökulmasta näyttää siltä, että pilvipohjainen useilla laitteilla toimiva salasanan hallintajärjestelmä palvelee parhaiten peruskäyttäjiä. Tämä johtuu siitä, että tällä hetkellä käyttäjiä uhkaa suurimpana uhkana salasanojen uudelleen käyttö ja muista palveluista vuotavat salasanat. Tätä uhkaa voidaan vähentää merkittävästi käyttämällä uniikkeja generoituja salasanoja jokaisessa palvelussa. Näin yhden palvelun tietomurto ei altista muita palveluita. Salasanojen muistaminen mielessä tai paperilla on kuitenkin tässä tilanteessa erittäin hankalaa, sillä nopeasti käyttäjälle muodostuu hallinnoitavaksi useita kymmeniä salasanoja, jolloin niiden järjellinen hallinta muistamalla tai kirjoittamalla ei enää ole järkevää. Pilvipohjainen salasanan hallinta tarjoaa käyttäjälle tavan muistaa ja käsitellä salasanoja järkevästi ja helposti. Haastatteluissa nousseiden vastausten mukaan käyttäjät kokivat heidän tietoturvan tasonsa nousseen merkittävästi ja kirjautumisten helpottuneen. Näin ollen voidaan todeta, että salasanan hallinta digitaalisesti pilvipohjaisella salasanan hallintajärjestelmällä on käytettävyyden ja tietoturvan kannalta tällä hetkellä parhaiten

tasapainossa, kun tarkastellaan peruskäyttäjää. Tätä tukee myös aiempi kirjallisuus, sillä kirjautumiseen liittyvät ongelmat liittyvät yleisimmin käyttäjän itse tekemiin virheisiin, kuten salasanan väärin kirjoittamiseen, epävarmuuteen mikä salasana variaatio sopii kyseiseen palveluun tai salasanan unohtamiseen. (Grawemeyer & Johnson, 2011). Nämä kaikki ongelmat ovat ratkaistavissa siirtämällä salasanan hallinnointi saatavuudeltaan hyvään järjestelmään.

6.1.3 Mitkä tekijät edes auttavat tai hidastavat salasanan hallinnan käyttöönottoa?

Haastatteluissa nousi esille useita tekijöitä, jotka edesauttavat salasanan hallinta järjestelmien käyttöönottoa sekä toimivat hidasteina käyttöönotolle.

Salasanan hallintajärjestelmän käyttöönottoa hidastavat selkeästi haastatteluiden perusteella käyttäjien motivaation puute, salasanojen hallinnan tietoturvan merkityksen aliarviointi ja tietämättömyys palvelusta, jota tulisi käyttää. Useat käyttäjät kertoivat salasanan hallintajärjestelmiä koskevissa haastatteluissa, ettei heillä ole ollut motivaatiota selvittää ja opetella käyttämään salasanan hallintajärjestelmiä. Jokainen henkilö oli kuullut sellaisen olemassa olosta ja tiesi sen toiminnan pääpiirteittäin, mutta käyttäjät eivät silti kokeneet, että sen käyttöönottaminen olisi siihen käytetyn vaivan arvoista. Käyttäjät myös kokivat, että heillä tällä hetkellä käytössä oleva järjestelmä on riittävän hyvä ja sen muuttamiseen ei ole tarvetta. Kuitenkin jokainen salasanan hallintajärjestelmää ei käyttävä henkilö vastasi kysymykseen, ”koetko salasanan hallintajärjestelmäsi tällä hetkellä turvalliseksi” kieltävästi. Joten käyttäjät tietävät, ettei heidän nykyinen salasanan hallintajärjestelmänsä ole riittävän hyvä, mutta hei eivät ole kokeneet sen olevan silti vaivan arvoista. Käyttäjät myös kertoivat, ettei heillä ole ollut riittävästi tietoa palveluiden vertailemisesta ja heillä ei ole ollut riittävästi tietoa mitä ominaisuuksia palvelusta tulisi löytää ja mikä sopisi heille. Voidaan sanoa, että salasanan hallintajärjestelmien käyttöönottoa hidastavat käyttäjien motivaation puute, tietämättömyys eri palveluista ja helppous jämähtää nykyiseen tilanteeseen.

Salasanan hallintajärjestelmiä otettiin käyttöön yleensä sen jälkeen, kun henkilöt kuulivat siitä, että he syyllistyvät tietoturvan kannalta huonoihin ratkaisuihin ja ovat riskissä joutua tietomurron uhriksi. Käyttäjät myös ottivat salasanan hallintajärjestelmiä käyttöön pian sen jälkeen, kun he itse joutuivat tietomurron uhriksi, joten tietomurron uhriksi joutuminen selkeästi kasvattaa motivaatiota, joka ei sinänsä ole kovin yllättävää. Tämä on linjassa turvallisuuteen liittyvän tutkimuksen ja aiemman kirjallisuuden kanssa. Protection Motivation Theoryn mukaan käyttäjät toimivat nimenomaan näin, kun he kokevat uhan olevan välitön, seuraukset raskaat ja käyttäytymisen muuttamisen kustannus on pieni. (Siponen & Baskerville, 2009). Käyttäjät ottivat myös salasanan hallintajärjestelmiä käyttöön, kun niitä suositteli jokin sellainen taho, jonka he itse kokivat luotettavaksi. Tämä löydös on linjassa myös alan aiemman kirjallisuuden sekä Unified Theory of Acceptance and Use of Technology (UTAUT) mallin kanssa. (Venkatesh, Morris, Davis, & Davis, 2003). Salasanan hallintajärjestelemän

käyttöönottoa myös edisti selkeästi se, kun käyttäjät joutuivat esimerkiksi työnpuolesta kasvattamaan salasanojen määrää merkittävästi. Useat käyttäjät kertoivat haastattelussa ottaneensa käyttöön salasanan hallinta järjestelmän, kun salasanojen määrä kasvoi liian suureksi ja niiden hallinnointi kävi vaikeaksi.

Näyttää siltä, että salasanojen hallinta järjestelmien käyttöönottoa viivästyttää tietämättömyys ja motivaation puute. Salasanan hallintajärjestelmien käyttöönottoa edistää tietoturvauhkan näkyväksi tekeminen ja siihen ratkaisun suosittelu.

6.1.4 Jatkotutkimusaiheet

Salasanojen hallinta näyttää olevan järkevintä hoitaa pilvipohjaisella salasanan hallintajärjestelmällä. Jatkotutkimuksen aiheina voitaisiin hakea vastauksia esimerkiksi siihen, joutuvatko salasanan hallintajärjestelmiä käyttävät useammin vai harvemmin tietomurron uhreiksi kuin niitä ei käyttävät. Näyttää siltä, että salasana vuodoissa ei juurikaan ole havaittavissa generoituja pitkiä salasanoja, vaan yleisimmin niistä löytyvät yleisimmät salasanat sekä sanakirjasanoja. Olisi mielenkiintoista nähdä, päätyvätkö yleisestikään generoidut salasanat salasana murroissa hyökkääjien tietoon.

Toinen mielenkiintoinen jatkotutkimusaihe voisi olla salasanojen hallintajärjestelmien teknisten haavoittuvuuksien ja heikkouksien kartoittaminen voisi olla mielenkiintoinen tutkimuskohde, jonka tavoitteena olisi löytää tietoturvan kannalta paras tapa tarjota salasanan hallintajärjestelmäpalvelua.

6.2 Yhteenveto pohdinnasta

Salasanoja voidaan hallinnoida muistamalla ne mielessä, kirjaamalla ne ylös paperille tai digitaalisella salasanan hallinta järjestelmällä. Muistaminen sekä paperille kirjaaminen yleensä toimivat toisiaan tukevina keinoina. Muistaminen näyttää tutkimuksen perusteella altistavan käyttäjän salasanojen uudelleen käytölle, huonojen salasanojen valitsemiselle ja näin olleen altistaa käyttäjän salasanavuodoista johtuville tietomurroille. Salasanojen kirjaaminen paperille käytännössä toimii yleensä tukevana toimenpiteenä niiden muistamiselle, mutta ei varsinaisesti näytä parantavan salasanojen laatua. Digitaalisesti salasanoja voidaan hallinnoida tallentamalla ne ohjelmallisesti salatussa muodossa joko laitteen kiintolevylle tai jonkin palveluntarjoajan pilvipalveluun. Näyttää siltä, että turvallisuuden ja käytettävyyden näkökulmasta paras tapa hallinnoida tällä hetkellä salasanoja on käyttää pilvipohjaista salasanan hallintajärjestelmää. Pilvipohjaisen salasanan hallintajärjestelmän käyttöä voidaan perustella sillä, että siinä saatavuus, luottamuksellisuus ja muuttumattomuus ovat turvallisuuden näkökulmasta hyvässä tasapainossa ja käyttäjällä on miltä tahansa laitteelta pääsy hänen käyttäjätunnuksiinsa, joka saatetaan menettää, mikäli käytetään paikallista salasanan hallintajärjestelmää. Käytettävällä salasanan hallintaohjelmalla generoidaan tilin

luonnin tai salasanan vaihdon yhteydessä uniikit esimerkiksi 32-merkkiset salasanat, jotka sisältävät isoja ja pieniä merkkejä, erikoismerkkejä ja numeroita sekä ovat merkityksettömiä merkkijonoja. Käyttäjän ei tarvitse tätä muistaa itse, joten sen sisällön ei tarvitse olla ihmiselle helposti luettavissa. Tämä parantaa myös merkittävästi salasanan varastamista, mikäli se nähdään selkotekstinä jossain nopeasti, sillä se on ihmiselle vaikea muistaa. Salasanan ainutlaatuisuudella voidaan suojautua salasanavuotoihin niin, että yksi salasana ei sovi useaan paikkaan. Toisaalta mikäli salasana ei ole sanakirjasana ja sen pituus on 32-merkkiä tai enemmän, voidaan sillä suojautua myös salasanoja hyvin käsittelevien palveluiden tietomurtoja vastaan, sillä salasanojen auki laskeminen salatusta muodosta muuttuu käytännössä mahdottomaksi suhteessa sanakirjasta löytyviin sanoihin. Salasanojen hallintajärjestelmän salasanaksi täytyy valita salasana lause, jolloin voidaan saavuttaa helposti pitkä sekä vaihteleva salasana, jota ei löydy sanakirjoista eikä näin ollen voida käyttää sanakirja hyökkäyksissä. Salasanan hallintaan tulee kytkeä päälle kaksi vaiheinen tunnistaminen, jolloin yksin salasanan varastaminen ei riitä palveluun kirjautumiseen, sillä mahdollisesti esimerkiksi mustasukkainen puoliso saattaa olla kiinnostunut käyttäjätunnuksista. Pilvipohjaisista salasanan hallintajärjestelmistä käytettäväksi voidaan suositella esimerkiksi palveluita, Lastpass, Dashlane ja F-secure key. Salasanan hallintajärjestelmien käyttöönottoa näyttävät hidastavan henkilöiden tietämättömyys eri vaihtoehdoista, minkälaisia ohjelmistoja voidaan käyttää. Sen lisäksi salasanan hallintajärjestelmiin koetaan liittyvän opettelua sekä vaivaa. Salasanan hallintajärjestelmiä otetaan käyttöön myös mieluummin, mikäli niitä suosittelee jokin luotettava taho.

7 Yhteenveto

Tässä pro gradu- tutkielmassa tutkittiin salasanan hallintajärjestelmiä tarkastellen niitä tietoturvan ja käytettävyyden näkökulmasta. Tavoitteena oli selvittää, minkälainen salasanan hallintamenetelmä toimisi parhaiten, kun sitä tarkastellaan tietoturvan ja käytettävyyden näkökulmasta. Tutkielman tutkimuskysymykset olivat:

- Minkälaisia tapoja on hallinnoida salasanoja?
- Minkälainen tapa hallinnoida salasanoja on käytettävyyden ja tietoturvan näkökulmasta suositeltavin?
- Minkälaiset tekijät edesauttavat tai hidastavat salasanan hallintajärjestelmien käyttöönottoa?

Tutkielman aluksi tarkasteltiin salasanoja yleisesti ja niihin liittyviä tietomurtoja. Näyttää siltä, että käyttäjät uudelleen käyttävät salasanoja eli käyttävät samaa salasanaa useassa eri palvelussa. Tämä asettaa kaikkien palveluiden tietoturvan yhden palvelun varaan, sillä päivittäin salasanoja varastetaan palveluista ja niiden tietokannoista. Mikäli käyttäjällä on sama salasana useassa palvelussa, altistuu näin hänen kaikki palvelunsa tietomurroille. Toisaalta salasanojen laatu ja pituus ovat tärkeitä tekijöitä salasanojen turvallisuudessa. Salasanojen tulisi olla yli 16 merkkiä pitkiä, sisältää merkistökoossa eroja, numeroita ja erikoismerkkejä. Lisäksi salasanat eivät saisi olla mistään sanakirjasta löytyviä sanoja ja näiden tulisi olla joka palvelussa ainutlaatuisia. Käyttäjän näkökulmasta näiden keksiminen ja muistaminen on mahdoton tehtävä, joten salasanojen hallintaan tarvitaan jokin menetelmä.

Tutkielmassa esiteltiin kolme tapaa hallita salasanoja, jotka olivat hallinta muistamalla, hallinta paperille kirjaamalla ja hallinta digitaalisella salasanan hallintaohjelmalla. Digitaaliset hallintaohjelmat olivat jaettu kahtia, sen perusteella tallennetaanko salasanojen tietokanta paikallisesti vai tallennetaanko se pilvipalveluun. Tarkasteltaessa käytettävyyden ja tietoturvan näkökulmasta pilvipohjainen salasanan hallintajärjestelmä, jossa on käytössä kaksivaiheinen tunnistaminen, osoittautui turvallisimmaksi ja parhaaksi järjestelmäksi. Käyttäjän tietoturvan tasoa voidaan nostaa muista menetelmistä merkittävästi, mikäli käyttäjä valitsee itselleen ainutlaatuisen ja vahvan salasanan tähän hallintajärjestelmään. Hallintajärjestelmän avulla käyttäjä generoi yli 16 merkkisiä sattumanvaraisia merkkijonoja salasanoiksi muihin palveluihin, jolloin käyttäjän salasanat ovat turvallisia ja niitä ei uudelleen käytetä muissa palveluissa. Kirjautuessaan käyttäjä käy hakemassa salasanan hallintajärjestelmästä ja kopioi sen salasanalomakkeeseen tai käyttää selainlaajennusta, joka täyttää salasanan automaattisesti.

Tutkielmassa haastateltiin 12 henkilöä, joista kuusi käytti salasanan hallintaa ja kuusi hallinnoi salasanojaan muistamalla. Haasteltavan populaation osalta voitiin todeta, että käyttäjät kokevat salasanojen hallinnasta olevan hyötyä sekä käytettävyyden, että tietoturvan osalta. Ongelmat tilanteet, kuten salasanojen unohtaminen ja siitä johtuva ylimääräinen vaiva korostui muistamalla hallinoivan populaation osalta. Haastatteluissa korostui myös turvallisuuden tunne ja

koettu helppous liittyen kirjautumiseen ja salasanan hallintaan, kun käytössä oli salasanan hallintajärjestelmä. Salasanan hallintajärjestelmien käyttöönottoa edistävät haastatteluiden perusteella, luotettavan tahon suosittelu, oman henkilökohtaisen tietoturvan haavoittuvaisuuden tason ymmärtäminen sekä käyttäjän kokemus tietomurrosta. Hallintajärjestelmien käyttöönottoa hidastavat käyttäjien motivaation puute, tietämättömyys hallintajärjestelmistä ja niiden vaihtoehdoista, valheellinen turvallisuuden tunne sekä suosittelujen puute.

Näyttää siis vahvasti siltä, että sekä teoriapainotteisen kirjallisuuskatsauksen ja empiirisen haastatteluvaiheen perusteella voidaan suositella tietoturvan ja käytettävyyden näkökulmasta pilvipohjaista digitaalista salasanan hallintajärjestelmää, johon on asetettu kaksivaiheinen tunnistaminen.

LÄHTEET

Adams, A., Sasse, M. A., & Lunt, P. (1997). Making Passwords Secure and Usable. People and Computers XII, 1–19. https://doi.org/10.1007/978-1-4471-3601-9_1

Alasuutari, P. (2012). Laadullinen tutkimus 2.0. Tampere: Vastapaino.

Arias, D. (2020). Adding Salt to Hashing: A Better Way to Store Passwords. haettu osoitteesta https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Asiakastieto. (2020). Minun Omatietoni -turvapalvelu. Haettu osoitteesta https://www.asiakastieto.fi/omatieto/fi

Banerjee, S. (2020). HTTP GET and POST Methods in PHP. haettu osoitteesta https://www.geeksforgeeks.org/http-get-post-methods-php/

Bauman, E., Lu, Y., & Lin, Z. (2015). Half a century of practice: Who is still storing plaintext passwords? Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9065, 253–267. https://doi.org/10.1007/978-3-319-17533-1_18

Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006). Fourth-factor authentication, 168. https://doi.org/10.1145/1180405.1180427

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641–651. https://doi.org/10.1002/acp.1014

Brumen, B., & Makari, T. (2017). Resilience of students' passwords against attacks. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings. https://doi.org/10.23919/MIPRO.2017.7973619

Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2006). A usability study and critique of two password managers. Proceedings of the 15th Conference on USENIX Security Symposium Volume 15, (August), 1–16. Haettu osoitteesta http://dl.acm.org/citation.cfm?id=1267336.1267337

Davis, F., & Bagozzi, R. (1985). a technology acceptance model for empirically testing new end-user information systems: theory and results.

Eeronen, R. (1997). Ennätysten kieli. Haettu osoitteesta https://www.kotus.fi/nyt/kolumnit_artikkelit_ja_esitelmat/kieli-ikkuna_%281996_2010%29/ennatysten_kieli

Erdos, M. (2020). Identity & Access Management. Haettu osoitteesta https://iam.harvard.edu/resources/behind-login-screen

Fagerlund, N. (2019). ID-VARKAUKSIEN MÄÄRÄ NELINKERTAISTUI VUONNA 2018 – SUOMALAISET MENETTIVÄT YHTEENSÄ 140 MILJOONAA EUROA. Haettu osoitteesta https://www.mysafety.fi/lehdistohuone/identiteettivarkauksien-maara-nelinkertaistui-vuonna-2018

Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., … Burr, W. E. (2017). Digital Identity Guidelines. NIST Special Publication 800-63B, 2–79. https://doi.org/10.6028/NIST.SP.800-63b

Fielding, R. T., Gettys, J., Mogul, J. C., Nielsen, H. F., Masinter, L., Leach, P. J., & Berners-Lee, T. (1999). rfc2616, Hypertext Transfer Protocol. Haettu

osoitteesta https://tools.ietf.org/html/rfc2616
Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web - WWW '07 (p. 657). New York, New York, USA: ACM Press. https://doi.org/10.1145/1242572.1242661
Fruhlinger, J. (2020). What is the CIA triad? The CIA triad components, defined. Haettu osoitteesta https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html
Gasti, P., & Rasmussen, K. B. (2012). On the security of password manager database formats. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7459 LNCS, 770–787. https://doi.org/10.1007/978-3-642-33167-1_44
Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. Interacting with Computers, 23(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007
Greenberg, A. (2020). Hacker Lexicon: What Is Password Hashing?
Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. Journal of Strategic Information Systems, 20(4), 373–384. https://doi.org/10.1016/j.jsis.2011.06.001
Hirsjärvi, S., & Hurme, H. (2008). Tutkimushaastattelu: Teemahaastattelun Teoria Ja Käytäntö. Helsinki: Gaudeamus Helsinki University Press.
Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197
Huda, S. (2019). Next Level Cybersecurity: Detect the Signals, Stop the Hack. Leaders Press.
Hunt, T. (2020). pwned accounts. Haettu osoitteesta https://haveibeenpwned.com/
Huth, A., Orlando, M., & Pesante, L. (2013). Password Security and Protection. Managing Trust in Cyberspace, 449–470. https://doi.org/10.1201/b16318-22
IBM. (2018). How much would a data breach cost your business? Haettu osoitteesta https://www.ibm.com/security/data-breach
Isola, P., Xiao, J., Torralba, A., & Oliva, A. (2011). What makes an image memorable? In CVPR 2011 (pp. 145–152). IEEE.
Janot, E., & Zavarsky, P. (2008). Preventing SQL Injections in Online Applications : Study , Recommendations and Java Solution Prototype Based on the SQL DOM. Application Security Conference.
Keck, C. (2019). It's Time to Nervously Mock the 50 Worst Passwords of the Year. Haettu osoitteesta https://gizmodo.com/its-time-to-nervously-mock-the-50-worst-passwords-of-th-1840514905
Keepass. (2020). Keepass technical FAQ. Haettu osoitteesta https://keepass.info/help/base/faq_tech.html
KeePass. (2019). Detailed information on the security of KeePass. Haettu osoitteesta https://keepass.info/help/base/security.html
Ketola, V.-P., & Krug, S. (2006). Älä Pakota Minua Ajattelemaan!: Tervejärkinen Käsitys Web-käytettävyydestä. Helsinki: Readme.fi.
Kracker, J. (2018). 52% of users reuse their passwords. Haettu osoitteesta

https://www.pandasecurity.com/mediacenter/security/password-reuse/
Länsimäki, M. (2002). Suomen yleisin sana. Haettu osoitteesta https://www.kotus.fi/nyt/kolumnit_artikkelit_ja_esitelmat/kieli-ikkuna_%281996_2010%29/suomen_yleisin_sana
Lastpass. (2020a). How it works? Haettu osoitteesta https://www.lastpass.com/how-lastpass-works
Lastpass. (2020b). LastPass MFA is a smarter way to authenticate. Haettu osoitteesta https://www.lastpass.com/products/multifactor-authentication
LogMeIn. (2020a). Generate strong, random passwords. Haettu osoitteesta from https://www.lastpass.com/password-generator
LogMeIn. (2020b). Psychology of Passwords: The Online Behavior That's Putting You at Risk. Haettu osoitteesta https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf
Mathew, S., Petropoulos, M., Ngo, H. Q., & Upadhyaya, S. (2010). A data-centric approach to insider attack detection in database systems. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6307 LNCS, 382–401. https://doi.org/10.1007/978-3-642-15512-3_20
Mitnick, K., Simon, W. L., & Wozniak, S. (2011). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Little, Brown. Haettu osoitteesta https://books.google.fi/books?id=p-nRxITKc34C
Ong, T. (2018). Over 90 percent of Gmail users still don't use two-factor authentication. Theverge. Haettu osoitteesta https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google
Owasp. (2017). Top 10 2017 Top 10. Haettu osoitteesta https://www.owasp.org/index.php/Top_10-2017_Top_10
Owasp. (2020). Password Plaintext Storage. Haettu osoitteesta https://owasp.org/www-community/vulnerabilities/Password_Plaintext_Storage
Peltomäki, J., & Norppa, K. (2015). Rikos meni verkkoon : näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum. Haettu osoitteesta https://jyu.finna.fi/Record/jykdok.1458178
Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. In Proceedings of the 9th ACM conference on Computer and communications security - CCS '02 (p. 161). New York, New York, USA: ACM Press. https://doi.org/10.1145/586110.586133
Renaud, K., Kotze, P., & Barnard, A. (2001). Hardware, software and pepoleware. SAICSIT, September(25–28). Haettu osoitteesta http://uir.unisa.ac.za/bitstream/handle/10500/24759/SAICSIT_2001_Karen.pdf?sequence=1&isAllowed=y
Rogers, E. M. (2010). Diffusion of innovations. Simon and Schuster.
Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. Computers and Security, 61. https://doi.org/10.1016/j.cose.2016.05.007
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.

Siponen, M., & Baskerville, R. (2009). Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. Economic Development and Cultural Change, (January), 1–36.

Spacey, J. (2020). What is Password entropy? Haettu osoitteesta https://simplicable.com/new/password-entropy-definition

Statscounter. (2019). Desktop browser market share. Haettu osoitteesta https://netmarketshare.com/

Stobert, E., & Biddle, R. (2018). The password life cycle. ACM Transactions on Privacy and Security, 21(3), 243–255. https://doi.org/10.1145/3183341

Techterms. (2020). Password. Haettu osoitteesta https://techterms.com/definition/password

Tuomi, J., & Sarajärvi, A. (2017). Laadullinen tutkimus ja sisällön analyysi. In Laadullinen tutkimus ja sisällön analyysi. Tammi.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425–478.

viestintävirasto. (2014). Salasanat haltuun, Neuvoja salasanojen käyttöön ja hallintaa.

Viestintävirasto. (2019). Pidempi on parempi. Haettu osoitteesta https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2018/06/ttn201806201436.html

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

Ylönen, T. (1996). SSH - Secure Login Connections over the Internet.

Yuan, H., Han, Y., & Hu, J. (2008). Password Memorability and Security : Empirical Results. 2008 International Computer Science and Software Engineering Conference, Volume 4, 25–31.

Zhao, R., & Yue, C. (2014). Toward a secure and usable cloud-based password manager for web browsers. Computers and Security, 46, 32–47. https://doi.org/10.1016/j.cose.2014.07.003

LIITE 1 HAASTATTELUKYSYMYKSET SALASANAN HALLINTAJÄRJESTLEMÄÄ KÄYTTÄVILLE HENKILÖILLE

Lämmittelykysymykset:

- Ikä?
- Miten kuvailisit teknologista taustaasi?
- Oletko joskus joutunut tietomurron uhriksi?
- Minkälaista salasanan hallintajärjestelmää käytät?
- Miksi päädyit käyttämään juuri tätä?
- Kuinka suuri osa salasanoista sinulla on hallintajärjestelmässäsi?
- Miten hallinnoit muita, jos niitä on?

Asenteisiin liittyvät kysymykset:

- Miten kuvailisit itseäsi uusien teknologioiden käyttöönottajana?
- Miten tärkeänä koet tietoturvan osana henkilökohtaista elämää?
- Kuinka tärkeänä koet tietoturvan osana työtä, jota teet?
- Minkä koet itsellesi suurimpana tietoturvauhkana?
- Pidätkö salasanan hallintajärjestelmässä muita tietoja, kun salasanoja?

Suorituskyvyn odotukset:

- Miten hallinnoit salasanojasi ennen, kun otit hallintajärjestelmän käyttöön?
- Miten odotit, että salasanan hallintajärjestelmä toimii, kun aloitit käyttämään sitä?
- Mitkä ovat tärkeimpiä ominaisuuksia liittyen salasanan hallintajärjestelmään?
- Mitkä ovat vähemmän tärkeitä ominaisuuksia, joita ilman pärjäisit?

Käyttöön liittyvä vaiva:

- Minkä koet salasanan hallintajärjestelmääsi liittyen helpoksi?
- Minkä koet salasanan hallintajärjestelmääsi liittyen vaikeaksi?
- Miten vertaat kirjautumista ja salasanojen hallintaa aiempaan tapaasi hallita salasanoja?
- Onko salasanan hallintajärjestelmän käyttö vaikeuttanut tai helpottanut päivittäistä toimintaasi?
- Uudelleen käytätkö salasanoja, eli onko sinulla sama salasana useassa eri palvelussa?
- Joudutko usein turvautumaan ”unohdin salasanani” palveluun?

Sosiaalinen hyväksyntä:

- Onko joku kannustanut sinua ottamaan hallintajärjestelmän käyttöön?
- Oletko sinä kannustanut muita ottamaan salasanan hallintajärjestelmiä käyttöön?
- Miten muut ovat reagoineet siihen?
- Oletko kohdannut negatiivisia tai positiivisia asenteita liittyen salasanan hallintajärjestelmän käyttöön?

Käyttöä edistävät olosuhteet:

- Mitkä ominaisuudet tai resurssit ovat sinulle kaikista tärkeimpiä valitsemassasi järjestelmässä?
- Mitkä asiat sinun kohdallasi edistävät/avustavat salasanan hallintajärjestelmän käyttöä?
- Mitkä asiat sinun kohdallasi estävät/hidastavat salasanan hallintajärjestelmän käyttöä?
- Jos voisit mennä takaisin siihen aikaan, kun otit käyttöön salasanan hallintajärjestelmääsi, niin mitä tekisit toisin vai tekisitkö mitään?

LIITE 2 HAASTATTELUKYSYMYKSET SALASANAN HALLINTAJÄRJESTLEMÄÄ EI KÄYTTÄVILLE HENKILÖILLE

Lämmittelykysymykset:

- Ikä?
- Miten kuvailisit teknologista taustasi?
- Oletko joskus joutunut tietomurron uhriksi?
- Miten sinä hallinnoit sinun salasanojasi?
- Miten olet päätynyt tähän tapaan hallinnoida salasanoja?
- Uudelleen käytätkö salasanoja? Eli onko sinulla sama salasana useassa palvelussa?
- Osaatko nimetä jotain syytä, miksi uudelleen käytät samoja salasanoja?
- Millä tavalla muodostat uuden salasanan, kun tarvitset sitä?
- Miten hallinnoit muita, jos niitä on?

Asenteisiin liittyvät kysymykset:

- Miten tärkeänä koet tietoturvan osana henkilökohtaista elämääsi?
- Kuinka tärkeänä koet tietoturvan osana sitä työtä mitä teet?
- Minkä koet sinulle henkilökohtaisesti suurimpana tietoturva uhkana?
- Koetko nykyisen tavan hallinnoida salasanojasi turvalliseksi?
- Jos et, niin miksi et ole muuttanut tapaa?
- Miltä sinusta tuntuu ajatus, että tallentaisit salasanasi jonkun toisen palveluun?
- Helpottaisiko jos joku, jonka tietämykseen uskoisit sanoisi, että se on turvallista?

Käyttöön liittyvä vaiva:

- Minkä koet hallintaan liittyen helpoksi?
- Minkä koet hallintaan liittyen vaikeaksi?
- Joudutko usein Käyttämään "unohdin salasanani" palvelua?
- Koetko, että palveluihin kirjautuminen on vaivalloista?

Sosiaalinen hyväksyntä:

- Onko joku kannustanut sinua ottamaan hallintajärjestelmän käyttöön?
- Et ole kuitenkaan ottanut käyttöön, miksi et?