Arjen salasanat

Kia Berg

Haaga-Helia ammattikorkeakoulu

Amk-opinnäytetyö

2021

Tradenomin tutkinto

Tiivistelmä

Tekijä(t)
Kia Berg

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Arjen salasanat

Sivu- ja liitesivumäärä
30 + 4

Moneen sivustoon ja sovellukseen on rekisteröidyttävä, jotta palvelun saa käyttöön. Käyttäjätunnuksia ja salasanoja kertyy valtavasti ja on keksittävä keino hallinnoida niitä. Lisääntyneet tietovuotouutiset ja yhä taidokkaammat kalasteluviestit saavat pohtimaan omien salasanojen turvallisuutta.

Tutkimuksen tavoitteena oli selvittää, kuinka ihmiset hallinnoivat eri palvelujen salasanoja arjessa ja kuinka turvallisia käytössä olevat salasanat ovat. Tutkimuksesta rajattiin pois ne kyberrikollisuuden ja -turvallisuuden alueet, jotka eivät suoraan liity salasanoihin. Tutkimuksesta rajattiin pois myös yritysten käytössä olevat ratkaisut.

Teoriaosuudessa käsitellään syitä siihen, miksi salasanoista kannattaa huolehtia. Uhkina ovat erilaiset tietomurrot, tietojenkalastelu ja haittaohjelmat. Lisäksi käydään läpi, kuinka vahva salasana muodostetaan ja millaisia asioita on syytä välttää. Lisäksi tutustutaan kertakäyttöiseen salasanaan, kaksivaiheiseen tunnistautumiseen ja salasanojen hallintaan.

Tutkimus toteutettiin osin kvalitatiivisena ja osin kvantitatiivisena tutkimuksena kyselylomakkeella ja puolistrukturoiduilla haastatteluilla. Kohderyhmä oli 18–50-vuotiaat aikuiset. Kysely tehtiin keväällä 2021 ja haastattelut syksyllä 2021.

Tutkimuksen tulosten perusteella tilanne oli hyvä. Tuloksista kävi ilmi, että kaikkien vastanneiden salasanat sisälsivät viitteitä vahvoista salasanoista. Salasanojen heikkouksia tutkittaessa, vastaukset tukivat sitä näkemystä, että useimmat tutkittujen salasanat ovat vahvoja. Lisäksi monet vastaajista käyttivät salasanojen hallintasovellusta salasanojen hallinnan ja vahvuuden tueksi.

Asiasanat
Salasanat, kyberrikollisuus, kyberturvallisuus

Sisällys

1 Johdanto

Moneen sivustoon ja sovellukseen on rekisteröidyttävä, jotta palvelun saa käyttöön. Käyttäjätunnuksia ja salasanoja kertyy arjessa valtavasti ja on keksittävä keino hallinnoida niitä. Lisääntyneet tietovuotouutiset ja yhä taidokkaammat kalasteluviestit saavat pohtimaan omien salasanojen turvallisuutta. Ihmiset todennäköisesti käyttävät samoja keinoja salasanojen hallintaan myös työssään, joten asialla on isommat vaikutukset kuin mitä tässä tutkimuksessa saadaan selville.

Aihe on yllättävän vähän tutkittu, kun ottaa huomioon kuinka paljon salasanoja jokainen ihminen hallitsee. Tämän tutkimusten tuloksista voidaan päätellä, tulisiko tutkia ja kehittää jokin keino houkutella ihmisiä huolehtimaan salasanojensa turvallisuudesta. Manninen (2020, 45–46) sai opinnäytetyössään selville, että yhden kurssin aikana opiskelijoiden salasanatottumuksiin ei tullut merkittäviä muutoksia, vaikka kurssi sisälsi opetusta salasanoista.

Tässä tutkimuksessa keskitytään ihmisten arkielämän valintoihin salasanojen hallinnassa ja niitä valitessa. Salasanan vahvuuteen vaikuttaa useampi tekijä, esimerkiksi se, kuinka helposti salasana on arvattavissa ja kuinka pitkä salasana on. Useiden vahvojen ja pitkien salasanojen hallintaan on olemassa erilaisia salasananhallintaohjelmia, joiden ansiosta kaikkia salasanoja ei tarvitse muistaa ulkoa. Siltainsuu (2020, 60) havaitsi Pro gradu-tutkielmassaan, että pilvipohjainen salasananhallintaohjelma palvelee parhaiten peruskäyttäjiä, koska se toimii useilla laitteilla ja on siten helppo käyttää.

Tutkimuskysymykset ovat:

- Kuinka ihmiset hallinnoivat eri palvelujen salasanoja arjessa?
- Kuinka turvallisia käytössä olevat salasanat ovat?

Tutkimuksesta on rajattu pois ne kyberrikollisuuden ja -turvallisuuden alueet, jotka eivät suoraan liity salasanoihin, jotta tutkimuksen laajuus pysyy kohtuullisena. Tutkimuksessa ei myöskään perehdytä yritysten käytössä oleviin ratkaisuihin salasanojen hallinnassa, koska tavoitteena on selvittää ihmisten valintoja ilman sovittuja käytäntöjä.

Työn keskeisiä käsitteitä ovat salasana, kyberrikollisuus ja kyberturvallisuus. Salasana on sana tai merkkijono, jota käytetään käyttäjätunnuksen parina päästäkseen käyttämään järjestelmää (Kotimaisten kielten keskus 2020). Kyberrikollisuus on rikollisuutta, joka kohdistuu tietoverkkoihin ja tietojärjestelmiin tai tehdään niitä hyödyntäen. Kyberrikoksia ovat esimerkiksi tietojenkalastelu, palvelunestohyökkäykset ja identiteettivarkaudet ja ne kohdistuvat sekä yksityisiin henkilöihin että organisaatioihin. (Turvallisuuskomitea 2018, 26.) Kyberturvallisuus on tilanne, jossa kybertoimintaympäristön toiminta on turvattu ja siihen

voidaan luottaa. Kyberturvallisuuteen sisältyy toimenpiteet, joilla voidaan ennaltaehkäistä ja sietää kyberuhkia ja niiden aiheuttamia vaikutuksia. (Turvallisuuskomitea 2018, 22.)

2 Syitä salasanoista huolehtimiseen

Tietomurrot, haittaohjelmat ja sosiaaliset huijaukset ovat tyypillisimpiä keinoja varastaa ja hyväksikäyttää salasanoja. Salasanavarkauksia ja niiden haittavaikutuksia voi jokainen käyttäjä ennaltaehkäistä itse. (Kyberturvallisuuskeskus s.a. 8.)

Kaikki internetiä käyttävät ovat verkkorikollisten kohteita. Rikolliset tavoittelevat rahaa, identiteettiä, tietoa tai yhteyttä arvokkaaseen tietoon. He voivat myös hyödyntää luvatta käyttöönsä saanutta nettiyhteyttä rikolliseen toimintaan. Jokaisella internetiä käyttävällä on jotain menetettävää kuten rahaa, henkilöllisyys, arvokasta tietoa tai muuta rahanarvoista omaisuutta. (Kyberturvallisuuskeskus 2020c.)

Yksityisellä henkilöllä voi olla monenlaista hyödynnettävissä olevaa omaisuutta. Uhrin sähköpostiosoitetta voidaan käyttää roskapostin levitykseen ja sähköpostitilillä voidaan kiristää uhria. Sähköpostista saadaan myös muiden sähköpostiosoitteita. Tietokoneen kautta hyökkääjä voi päästä käsiksi myös työnantajan sähköpostiin. Koneen avulla voidaan jakaa laitonta sisältöä ja konetta voidaan hyödyntää palvelunestohyökkäyksissä ja tietomurroissa. (Norppa & Peltomäki 2015, 62.)

Aiemmin mainittujen lisäksi henkilöillä voi olla virtuaalivaluuttaa esimerkiksi bitcoineja, virtuaalisia luottokortteja tai internetistä ostettuja lisenssejä. Internetin kautta voi päästä käsiksi myös pankkitunnuksiin ja rahaan sekä pankki- ja luottokorttitietoihin. Useilla on myös henkilötietoja sosiaalisen median profiileissa, joita voidaan hyödyntää identiteettivarkauksissa. (Norppa & Peltomäki 2015, 62.)

Hyötyjen lisäksi rikolliset voivat myös tavoitella huomiota tai tehdä vain kiusaa. Uhrien nimiin tehdyt rikokset ja vahingonteot ovat kiusallisia sekä haitallisia maineelle. Aiheutuneiden haittojen lisäksi verkkorikollisten jälkien korjaaminen voi olla kallista ja työlästä, eikä kaikkea menetettyä välttämättä saa enää takaisin. Lisäksi arkaluonteisen tiedon leviäminen on harmillista. (Kyberturvallisuuskeskus 2020c.)

2.1 Tietomurto

Tietomurrolla tarkoitetaan sitä, että joku tunkeutuu luvatta johonkin tietojärjestelmään. Rikoslaissatietomurto määritellään toiminnaksi, jossa käytetään luvatta käyttäjätunnusta tai ohitetaan turvajärjestely, jotta päästään murtautumaan järjestelmään. Sekä tietomurto että sen yritys ovat rikoksia, joista tulisi aina tehdä rikosilmoitus poliisille. (Poliisi s.a.)

Kirjautumistietojen varastaminen käyttäjältä on yleisin tapa tehdä tietomurto. Lisäksi käytetään erilaisia keinoja turvajärjestelmien ohittamiseksi, jotta järjestelmästä löytyvää tietoa päästään hyödyntämään esimerkiksi petoksien tekemiseen. Tietoa voidaan varastaa myös sen arkaluontoisuuden vuoksi. (Poliisi s.a.)

Kun tietomurto kohdistuu yksityiseen henkilöön, tavoitteena voi olla esimerkiksi identiteettivarkaus. Tällöin pyrkimys on esiintyä kohteena olleena henkilönä. Lisäksi yksityishenkilöön kohdistuvasta tietomurrosta voi koitua uhrille harmia esimerkiksi toimimattomista järjestelmistä. (Kyberturvallisuuskeskus 2021a.)

Kaikkia tietomurtoja ei voi estää, mutta niihin voi varautua seuraavasti:

- Käytä jokaisessa käyttäjätilissä vahvaa ja ainutkertaista salasanaa.
- Käytä kaksivaiheista tunnistautumista aina, kun se on mahdollista.
- Pohdi mitä tietoja haluat antaa eri käyttäjätileille.
- Älä säilytä turhia käyttäjätilejä, vaan poista ne, kun et enää tarvitse niitä. (F-Secure s.a.)

Mikäli tietomurto osuu kohdalle, tulisi mahdolliset kiristysviestit dokumentoida ottamalla viesteistä kuvakaappaukset. Kiristysviesteihin ei kannata vastata eikä kiristäjälle tule maksaa kiristettävää summaa, vaan asiasta tulee tehdä rikosilmoitus poliisille. (F-Secure s.a.) Suomessa toimii kyberturvallisuuskeskus, jonka tehtävänä on muun muassa kehittää ja valvoa viestintäverkkojen turvallisuutta (Kyberturvallisuuskeskus 2021a). Ilmoittamalla tietomurrosta myös kyberturvallisuuskeskukselle, autat heitä muodostamaan turvallisuudesta tilannekuvaa. Tietomurron tapahduttua, käy vaihtamassa salasanat, jotta voit suojata käyttäjätileillä olevia tietojasi. (F-Secure s.a.)

Lisäksi itselleen voi tarvittaessa hankkia luottokiellon. Se on maksullinen, mutta se estää rikollista ottamasta varastetuilla luottokorttitiedoilla erilaisia luottokortteja ja lainoja. (F-Secure s.a.) Postille voi tehdä kevyen muuttosuojauksen, jonka ansiosta muuttoilmoituksen tekeminen on mahdollista vain sähköisesti vahvasti tunnistautumalla. Vaihtoehtona on myös muuttosuojaus, joka estää muuttoilmoituksen tekemisen myös sähköisesti eikä edes vahva tunnistautuminen riitä muuttoilmoituksen tekoon. Muuttosuojaus kannattaa tehdä, jos henkilötiedot ovat joutuneet tietomurron seurauksena vääriin käsiin. (Posti s.a.)

2.2 Tietojenkalastelu

Tietojenkalastelu eli phishing on tunnetuin tapa varastaa käyttäjätunnus ja salasana. Se toteutetaan esimerkiksi aidolta näyttävällä kirjautumissivulla, johon uhri syöttää kirjautumistiedot, jonka jälkeen saatuja tietoja käytetään rikolliseen toimintaan. (Poliisi s.a.)

Yleensä tietojenkalastelun välineenä toimii sähköpostiviesti, jonka avulla pyritään saamaan käyttäjän kirjautumistiedot. (Kyberturvallisuuskeskus 2019, 7). Uhrille voidaan lähettää esimerkiksi varoitus, jonka mukaan tiliä on yritetty käyttää ennestään tuntemattomasta IP-osoitteesta tai -maasta. Tämän tavoitteena on säikäyttää tilin omistaja ja saada hänet kiireellisesti klikkaamaan viestissä olevaa linkkiä, joka vie valesivulle ja jonne uhri syöttää kirjautumistunnukset vaihtaakseen salasanan. Tämän virheen välttämiseksi salasana tulisi aina vaihtaa palvelun omilta sivuilta eikä viestin linkin kautta. (Järvinen 2018, 307–308.)

Tietojenkalastelun avulla saatuja sähköpostitilejä voidaan käyttää esimerkiksi uusien kalasteluviestien lähettämiseen tai viestien lukemiseen. Lopuksi tietomurron tehnyt voi tuhota tai salata saamansa tiedostot, jonka jälkeen murron kohteena oleva laite on käyttökelvoton. (Kyberturvallisuuskeskus 2020c.)

Toinen keino tiedonkalasteluun on niin sanottu human engineering, jossa urkkija soittaa uhrille ja valehtelee olevansa esimerkiksi viranomainen, kuten poliisi (Järvinen 2018, 308). On kuitenkin hyvä tietää, ettei mikään viranomainen tai pankki pyydä kenenkään henkilö- tai pankkitietoja puhelimitse eikä sähköpostitsekaan. Mikäli on epävarma soittajan oikeellisuudesta, puhelu kannattaa katkaista ja soittaa viranomaisen julkisesti tiedossa olevaan numeroon. (Poliisi 2021.)

2.3 Haittaohjelmat

Valitettavasti verkkorikolliset hyödyntävät salasanojen lisäksi myös haittaohjelmia päästäkseen käsiksi henkilötietoihin ja pankkitunnuksiin (Kyberturvallisuuskeskus 2020c). Haittaohjelmat ovatkin yleinen keino varastaa salasanoja. Niiden avulla tutkitaan laitteen tiedostoja ja voidaan löytää selaimiin ja ohjelmiin tallennettuja salasanoja. Haittaohjelma voi hyödyntää myös näppäimistölukijaa eli niin sanottua keylogger:ia, joka lukee, tallentaa ja lähettää kirjoitukset hyökkääjälle. Haittaohjelmia voi ennaltaehkäistä huolehtimalla päivityksistä ja käyttämällä ajantasaista antivirusohjelmaa. (Kyberturvallisuuskeskus s.a. 8–9.)

Termillä haittaohjelma tarkoitetaan kaikentyyppisiä haitallisia ohjelmistoja, joiden tarkoitus on vahingoittaa tai hyödyntää laitteitta, palveluja tai verkkoa. Haittaohjelmien avulla kyberrikolliset pyrkivät saamaan haltuunsa tietoja, joilla he voivat kiristää uhreja. Tällaisia tietoja ovat esimerkiksi luottokorttitiedot, potilasasiakirjat, sähköpostit tai salasanat. Hyökkäystapoina toimivat esimerkiksi sähköpostin liitteet, haittamainokset, ohjelmistojen väärennetyt asennukset, USB-muistitikut ja tietojenkalasteluviestit. (McAfee s.a.)

Tietokoneessa saattaa olla haittaohjelma, mikäli se toimii hitaasti, sen käynnistämisessä ja sammuttamisessa on ongelmia, näytölle ilmestyy ponnahdusmainoksia tai jos näytölle

ilmestyy tartunnasta kertovia varoituksia, jotka houkuttelevat ostamaan jonkin tuotteen sen poistamiseksi. Lisäksi selain saattaa uudelleenohjata käyttäjän sivulle, jonne ei ollut tarkoitus mennä. (McAfee s.a.)

Haittaohjelmia on erilaisia, jonka takia myös suojautumiskeinoja on erilaisia. Haittaohjelmilta voi suojautua muun muassa seuraavasti:

- Haavoittuvuuksia etsitään vanhentuneista ohjelmistoista, joten huolehdi, että käyttöjärjestelmä ja sovellukset ajan tasalla.
- Älä paina ponnahdusikkunassa olevaa linkkiä, vaan sulje se ja siirry pois sivustolta.
- Asenna vain sellaisia sovelluksia, joita käytät ja poista sellaiset sovellukset, joita et enää tarvitse.
- Käytä luotettavaa tietoturvaohjelmistoa.
- Älä koske tuntemattomiin tai epäilyttäviin linkkeihin.
- Pyri käyttämään ainoastaan tunnettuja ja luotettavia sivustoja.
- Ole varovainen sähköpostien linkkien kanssa. Ne saattavat näyttää luotetun palvelun lähettämiltä, mutta älä paina linkkiä vaan kirjaudu suoraan palveluntarjoajan sivustolta.
- Lataa vain hyvämaineisia ja luotettavia ohjelmistoja ja käytä niiden lataamiseen virallisia sovelluskauppoja. (McAfee s.a.)

3 Salasanat

Salasanoja voidaan kutsua avaimiksi, joilla avataan pääsy tietojärjestelmiin, tietoihin ja laitteisiin, jonka takia salasanojen turvallisuus on yksi tietoturvan peruspilareista (Järvinen 2018, 305). Salasanat säilyttävät suosionsa, vaikka uusia menetelmiä tunnistamiseen on tullut vaihtoehdoiksi. Salasanat ovat edullinen ratkaisu ja niiden käyttäminen on helppoa ja tuttua. Lisäksi salasana on helppo ja nopea vaihtaa, mikäli se unohtuu, vanhenee tai joutuu vääriin käsiin. (Kyberturvallisuuskeskus s.a. 10–11.)

On huomattu, että salasanat ovat hyvin ennustettavissa ja sanastojen sekä todennäköisyysmallien avulla hyökkääjät voivat rajata salasanavaihtoehtoja. Lisäksi on huomattu, että jos palvelu ei aseta vaatimuksia salasanan vahvuudelle, heikot salasanat ovat yleisiä. (Dell'Amico, Michiardi & Roudier 2010.)

Joissain palveluissa on mahdollista käyttää salasanoja tukevia todennusmenetelmiä, joiden avulla käyttäjät voivat lisätä tunnistautumisen turvallisuutta. Näitä on suositeltava hyödyntää ja yksi hyvä menetelmä on monen palveluntarjoajan tarjoama kaksivaiheinen tunnistus, jossa käyttäjätunnuksen ja salasanan lisäksi käyttäjä tunnistetaan esimerkiksi tekstiviestivarmennuksella. (Kyberturvallisuuskeskus s.a. 10–11.)

Topi Manninen (2020, 46) sai opinnäytetyössään selville, että opiskelijoiden salasanavalinnat olivat heikkoja eivätkä ne kehittyneet Orientaatio ICT-infrastruktuuri-kurssin aikana. Lisäksi suurin osa opiskelijoista laiminlöi salasanojen säännöllisen vaihtamisen, ellei palvelut vaatineet säännöllistä salasanan vaihtamista. Edistystä tapahtui kuitenkin siinä, että salasananhallintaohjelmien käyttö kasvoi merkittävästi.

3.1 Vahvan ja heikon salasanan ominaisuuksia

Heikkoja salasanoja ovat esimerkiksi oma nimi, helppo sana, jonka perään on laitettu 123, qwerty, joka muodostuu näppäimistön ylimmältä kirjainriviltä kuusi ensimmäistä kirjainta peräkkäin, tai syntymäaika. Lisäksi on yleistä korvata kirjaimet numeroilla esimerkiksi o=0 ja i=1. (Kyberturvallisuuskeskus 2021b.)

Salasanan ei myöskään tulisi olla sama kuin käyttäjätunnus eikä käyttäjätunnus takaperin kirjoitettuna ole sen parempi. Palvelun nimi, johon salasanaa käytetään, on myös huono vaihtoehto. (Järvinen 2012, 118.)

Vahva salasana on sen sijaan pitkä, mieluiten 15 merkkiä, joka sisältä myös erikoismerkkejä ja on mieluummin lause kuin pelkkä sana (Kyberturvallisuuskeskus 2021b). On hyvä huomioida, että mitä pidempi salasana on, sitä turvallisemmaksi se tulee. Salasanan

kannattaa sisältää erikoismerkkien lisäksi myös isoja kirjaimia ja erilaiset kirjoitusvirheet, murteet ja muut tavat rikkoa sanoja, tekevät salasanasta vahvemman. (Kyberturvallisuuskeskus 2020d.)

3.2 Salasanojen turvallisuus

Salasana tulisi olla riittävän vahva, ettei sitä pysty arvaamaan tai selvittämään kokeilemalla järjestelmällisesti kaikkia merkkiyhdistelmiä, joka on niin sanottu brute force-menetelmä. Lisäksi tulee kiinnittää huomiota siihen, kuinka salasanan kirjoittaa. Jos mahdollista, kannattaa kirjautua esimerkiksi sormenjälkitunnistuksella, jolloin kukaan ei vahingossakaan näe salasanaa. (Järvinen 2018, 305–306.)

On tärkeää, että jokaiseen palveluun käyttää eri salasanaa ja ettei salasanaa koskaan luovuteta kenenkään muun tietoon. On kuitenkin hyvä huomioida, että salasana voidaan varastaa palveluntarjoajalta, jolloin olisi hyvä olla käytössä kirjautumisilmoitukset. Näiden avulla voidaan seurata tapahtumia, jolloin kirjautuminen tapahtuu poikkeuksellisesta paikasta tai laitteella, jolla ei ole aiemmin kirjauduttu. Tämä helpottaa huomaamaan, mikäli tunnukset ovat päätyneet vääriin käsiin huomaamattomasti. Jos salasana on joutunut vääriin käsiin, se tulisi vaihtaa välittömästi, jotta mahdollinen väärinkäyttö estyy. (Kyberturvallisuuskeskus 2021b.)

Salasana tulee vaihtaa säännöllisesti eikä tulisi käyttää samaa salasanaa, jota on aiemmin käyttänyt. Tällä voidaan vaikuttaa siihen, että jos salasana onkin joutunut vääriin käsiin, voidaan väärinkäyttö katkaista. Vanhan salasanan käyttö lisää riskiä väärinkäytölle. Mikäli salasanan pituus on 15–18 merkkiä, salasanan vaihtoväli voi olla jopa 6–9 kuukautta. Tätä lyhyemmät salasanat kannattaa vaihtaa esimerkiksi kolmen kuukauden välein. (Rousku 2014, 179.)

Salasanat voidaan jakaa kolmeen ryhmään: kriittiset-, tärkeät- ja peruspalveluissa käytettävät salasanat. Luokitus riippuu siitä, kuinka kriittinen ja tärkeä palvelu on kyseessä. Mitä kriittisempi palvelu, sitä ainutkertaisempi ja laadukkaampi salasanan tulisi olla. Esimerkiksi sähköpostin avulla unohtuneen salasanan voi palauttaa, joten sähköpostin salasana on kriittinen. Samoin kaikki ne palvelut, joissa käsitellään luottokorttitietoja tai joiden avulla voidaan kirjautua toisiin palveluihin. Sen sijaan tärkeisiin palveluihin, joissa käsitellään lähinnä henkilötietoja, voidaan käyttää samankaltaisia salasanoja. Täytyy kuitenkin huomioida, ettei ne ole niin samankaltaisia, että yhden salasanan päätyminen vääriin käsiin, avaa pääsyn myös muihin tärkeisiin palveluihin. Peruspalveluissa, joissa ei käsitellä mitään aiemmin mainittuja, voivat salasanat olla jopa samoja, mutta silloinkin tulee käyttää vahvaa salasanaa. (Rousku 2014, 184–185.)

3.3 Kertakäyttöinen salasana

Kertakäyttöisen salasanan (One time password eli OTP) sisältävät tekstiviestit ovat yleisesti käytetty menetelmä henkilön todentamiseen mobiilisovelluksissa. Monet suositut sovellukset käyttävät niitä jopa ainoana todentamiskeinonaja (One-Factor Authentication One-Time Passwords eli 1FA OTP) korvaavat niillä salasanapohjaiset todentamismallit. Vaikka kertakäyttösalasanat helpottavat käyttäjiä, on niillä myös turvallisuusriskejä. (Lei, Nan, Fratantonio & Bianchi 2021, 1.)

Tekstiviestillä saadun kertakäyttösalasanan käyttäminen ainoana todentamisena toimii niin, että käyttäjää pyydetään todistamaan oma puhelinnumeronsa, joka toimii pääasiallisena käyttäjätunnuksena eli kun omistaa puhelinnumeron, omistaa myös käyttäjätilin. Tämä menetelmä toteutetaan kysymällä käyttäjältä puhelinnumero, johon tunnuskoodi lähetetään. Lopuksi käyttäjää pyydetään antamaan vastaanotettu tunnuskoodi, tai sovellus lukee sen automaattisesti saapuneesta viestistä ja lähettää sen sovelluksen taustalle eli backend:iin. Tällä tavoin käyttäjä todistaa omistavansa puhelinnumeron. (Lei ym. 2021, 1.)

Tämä menetelmä helpottaa käyttäjää erityisesti siksi, että käyttäjän ei tarvitse taas luoda ja muistaa uutta salasanaa kirjautuessaan uuteen sovellukseen. Tämän takia menetelmä on laajasti käytetty ja esimerkiksi suosittu viestintäsovellus Telegram käyttää tätä menetelmää. Google Play:n 100 suosituimmasta sovelluksesta 24 sovellusta käyttää tätä menetelmää ainoana käyttäjän todentamisena. (Lei ym. 2021, 1.)

Valitettavasti tämä menetelmä on myös haavoittuva, koska puhelinverkko on useasti osoittautunut epävarmaksi. Hyökkääjät ovat useamman kerran kohdistaneet hyökkäyksen puhelinverkkoihin ja uudelleenohjannut kertakäyttöiset salasanat vastaanottajalle, jolle ne eivät kuulu. Merkittävin esimerkki on SIM kortin vaihtohyökkäys, jossa hyökkääjä onnistuu saamaan puhelinyhtiöltä uhrin puhelinnumeroon liittyvän SIM kortin. (Lei ym. 2021, 1.)

Puhelinverkkoon liittyvien hyökkäysten lisäksi uhkana on paikalliset hyökkäykset, joissa hyökkääjä hallitsee uhrin laitteeseen asennettua kolmannen osapuolen haittaohjelmaa. Haittaohjelman tavoitteena on varastaa tekstiviestillä lähetetyt kertakäyttöiset salasanat. Tämä on erityisen haitallista niissä tapauksissa, joissa kertakäyttöinen salasana on ainoa menetelmä käyttäjän kirjautuessa sovellukseen. Nämä hyökkäykset heikentävät myös kaksivaiheisen tunnistautumisen turvallisuutta, koska hyökkääjä saa käyttöönsä toisen kahdesta tekijästä, joilla kirjautuminen suoritetaan. (Lei ym. 2021, 1–2.)

Viime aikoina käyttöjärjestelmiin on tehty kuitenkin muutoksia, joiden ansiosta kirjautuminen kertakäyttösalasanoilla on turvallisempaa. Esimerkiksi iOS ei salli kolmansien osapuolten sovellusten lukea tai käyttää tekstiviestejä. Android-laitteissa puolestaan kolmansien osapuolten sovellukset pyytävät lupaa lukea tekstiviestejä. (Lei ym. 2021, 2.)

3.4 Kaksivaiheinen tunnistautuminen

Kaksivaiheinen tunnistautuminen eli Two-factor authentication, lyhyemmin 2FA tuo salasanalle lisää turvaa. 2FA on ylimääräinen turvallisuustaso, jolla varmennetaan, että ihminen on se, kuka hän sanoo olevansa käyttäjätunnuksen ja salasanan kautta (Twilio Authy s.a.). Aiemmin esiteltyjä kertakäyttösalasanoja käytetään yleisesti myös kaksivaiheisessa tunnistautumisessa (2FA). Tämä tarkoittaa sitä, että käyttäjätunnuksen ja salasanan lisäksi käyttäjä saa tekstiviestillä kertakäyttöisen salasanan, jonka hän antaa kirjautumisen yhteydessä. (Lei ym. 2021, 1.)

Ylimääräisellä tunnistautumisen lisääminen auttaa suojaamaan käyttäjätiliä uhilta, kuten tietojenkalastelun ja salasanojen uudelleenkäyttöhyökkäyksien seurauksilta. (Golla, Ho, Lohmus, Pulluri & Redmiles 2021, 109). Kun käyttäjä kirjautuu palveluun, hän ei käyttäjätunnuksen ja salasanan syöttämisen jälkeen pääsekään palveluun heti, vaan hänen täytyy vahvistaa todennus vielä toisella tapaa. Tapoja on kolmenlaisia: jotain, mitä tiedät tai jotain, mitä sinulla on tai jotain mitä olet. (Twilio Authy s.a.)

Jotain, mitä tiedät voi olla esimerkiksi PIN-koodi tai vastaus salaiseen kysymykseen. Jotain, mitä sinulla on voi olla esimerkiksi luottokortti tai muistitikku. Jotain mitä olet, voi perustua esimerkiksi sormenjälkitunnistukseen tai iiriksen skannaukseen. On epätodennäköistä, että vaikka salasana varastettaisiin, varas saisi käyttöönsä myös tämän toisen tunnisteen. (Twilio Authy s.a.)

Joissakin sovelluksissa käytetään biometriikkaa salasanojen täydentämiseen lisätäkseen sovellusten tietoturvaa. Nämä fyysiset biometriset ominaisuudet ovat kehon eri ominaisuuksia kuten sormenjäljet ja kasvot. Sormenjälkiä tunnistaessaan, jotkut tekniikat jäljittelevät perinteistä poliisin tapaa kuvantaa sormenjäljen pienet yksityiskohdat, kun taas toiset käyttävät kuviosovitusta. Lisäksi jotkut tekniikat havaitsevat onko sormi elävä. Sormenjälkitunnistimien valikoima on suurempi kuin muiden biometristen tunnistuslaitteiden ja nykyään sormenjälkitunnistin onkin tavanomainen ominaisuus matkapuhelimissa. (Saleem & Ordonez, 2020, 1–2.)

Osassa matkapuhelimista on käytössä sormenjälkitunnistuksen sijaan kasvojentunnistus, joka analysoi kasvojen ominaisuuksia. Se vaatii digikameran, jolla käyttäjä voi luoda

kasvokuvan todennusta varten. Teknologia mahdollistaa nykyään myös kasvojen termografian eli kasvojen lämpötilojen jakautumisen ja kasvojen kolmiulotteisen kuvaamisen. (Saleem & Ordonez, 2020, 3)

Esimerkiksi uusimpien iPhone puhelinten Face ID on turvallinen todennustapa, koska se hyödyntää TrueDepth-kamerajärjestelmää ja kehittyneitä tekniikoita. Lisäksi Face ID:n tiedot ovat salattu ja suojattu avaimella, joka on ainoastaan Secure Enclave -turva-alueen käytettävissä. TrueDepth-kamera analysoi tuhansia pisteitä ja luo kasvoista syvyyskartan sekä tallentaa infrapunakuvan. Useita siruja hyödyntävä Neural Engine muuttaa syvyyskartan ja infrapunakuvan matemaattiseksi kuvaksi verraten sitä tallennettuihin kasvotietoihin. Tämä tekniikka sopeutuu kasvojen ulkoisiin muutoksiin, kuten meikkiin ja parran kasvamiseen. Sitä pystyy käyttämään muun muassa hattujen, huivien ja silmälasien kanssa sekä eri valoisuuksissa, kuten auringossa ja täysin pimeässä. (Apple, 2021.)

Golla, Ho, Lohmus, Pulluri ja Redmiles (2021, 120) tutkivat voisivatko he parantaa käyttäjien motivaatiota ottaa käyttöön kaksivaiheista tunnistautumista suunnittelemalla erilaisia kehotteita testiä varten. Tutkimuksen tuloksena he huomasivat, että huolellisesti suunnitellut kehotteet, joissa kannustettiin käyttäjiä ottamaan kaksivaiheinen tunnistautuminen käyttöön, voivat lisätä 2FA käyttäjien määrää. Tehokkaimmin toimivat ne kehotteet, joissa painotettiin henkilökohtaista vastuuta suojaavista toimista, kuin ne, joissa ei mainita vastuuta lainkaan tai jotka korostavat yritysten vastuuta.

3.5 Salasanojen hallinta

Salasanojen hallintaohjelmalla voi luoda ja säilyttää salanoja, jolloin on helpompi ylläpitää useita vahvoja salasanoja, joita ei pysty muistamaan. Salasananhallintaohjelma säilöö salasanat yhden salasanan takana. Salasananhallintaohjelmia on erilaisia ja niissä on eroja, jotka on hyvä tunnistaa. Jotkin ohjelmat tallentavat salasanat pilvipalveluun, josta ne ovat kätevästi käytössä eri laitteilla, osa tallentaa salasanat paikalliselle tietokoneelle ja osa niille laitteille, jolle ohjelma on asennettu. (Kyberturvallisuuskeskus 2021b.)

Yksi maailmanlaajuisesti suurimmista kuluttajateknologiaan erikoistuneista arvostelijoista TechRadar testasi useita kymmeniä kuluttajille tarkoitettuja salasanan hallintaohjelmia. Kokonaisuudessaan salasanojenhallintasovelluksia on tarjolla yli 250 ja useissa on tarjolla sekä ilmainen että maksullinen versio. TechRadarin testin mukaan kolme parasta salasanan hallintasovellusta olivat Dashlane, LastPass ja NordPass. (Pikkarainen, Mesiä & Turner 2021.)

Kun valitsee itselle sopivaa salasanan hallintasovellusta, kannattaa miettiä mitä ominaisuuksia sovellukselta haluaa. Saako sovellus maksaa vai haluaako ilmaisen? Kuinka monta salasanaa sovellukseen voi tallentaa? Haluaako, että sovellus tukee kaksivaiheista tunnistautumista? Entä haluaako, että salasanat tallentuvat vain yhdelle laitteelle vai pilvipalveluun, jossa ne ovat useamman laitteen käytössä? (Kyberturvallisuuskeskus 2020b.)

Pilvipalvelua käyttävä salasanan hallintasovellus on helpottaa salasanojen käyttöä eri laitteilla, mutta pääsalasanan hukkaaminen tai salasanan väärinkäyttäminen voi johtaa kaikkien salasanojen päätymisen vääriin käsiin. Mikäli käyttää sovellusta, joka tallentaa salasanat paikallisesti, salasanat pysyvät varmemmin poissa ulkopuolisilta, mutta silloin niiden säilyvyyteen vaikuttaa päätelaitteen toiminta, varmuuskopioista huolehtiminen ja niiden turvallinen säilytys. (Kyberturvallisuuskeskus 2021b.)

Salasanojen hallintasovellus suojaa salasanoja arvailevilta hyökkäyksiltä ja yksittäisiltä salasanavuodoilta, mikäli hyödyntää salasanasovelluksen mahdollistavia vahvoja ja yksilöllisiä salasanoja eri palveluihin. Monet salasanasovellukset myös ehkäisevät salasanojen kalasteluyrityksiä tunnistamalla aidon kirjautumissivun osoitteen. (Kyberturvallisuuskeskus 2020b.)

4 Tutkimus arjen salasanavalinnoista

4.1 Tutkimusmenetelmä

Tutkimus on tehty kahdessa vaiheessa. Ensimmäisessä vaiheessa aineisto kerättiin Google Forms kyselylomakkeella (liite 1) keväällä 2021. Tutkimuksen kohderyhmä oli 18–50-vuotiaat aikuiset, jotta sukupolvien väliset erot eivät korostu. Tämä osa tutkimuksesta toteutettiin kvantitatiivisena eli määrällisenä tutkimuksena. Määrällisessä tutkimuksessa tuloksia tulkitaan numeroiden avulla, joihin ilmiöt perustuvat (Jyväskylän yliopisto 2015). Tämä on luonteva tapa tarkastella kyselyn tuloksia, kun tavoitteena on tutkia, kuinka suurella osalla vastaajista toteutuu erilaiset kriteerit ja ominaisuudet.

Toisessa vaiheessa aineistoa kerättiin syksyllä 2021 puolistrukturoiduilla haastatteluilla (liite 2). Haastatteluja tehtiin yhteensä viisi. Haastateltavat olivat 26–45-vuotiaat, koska valtaosa kyselyyn vastanneista olivat siitä ikäryhmästä ja näin saatiin täydennettyä jo kyselyssä saatuja vastauksia. Tämä osa tutkimuksesta toteutettiin kvalitatiivisena eli laadullisena tutkimuksena. Tähän osaan tutkimusta valittiin kvalitatiivinen menetelmä, koska tutkimuksessa haluttiin selvittää myös sitä, miksi vastaajat päätyvät kyseisiin ratkaisuihin salasanojen valinnassa. Kvalitatiivisessa tutkimuksessa ei päätellä tuloksia numeerisen määrän perusteella, vaan käytetään aineistona esimerkiksi tekstejä ja numeraalistakin aineistoa tutkitaan laadullisesti (Juhila 2021).

Puolistrukturoidussa haastattelussa kysymykset laaditaan ennakkoon ja ne esitetään haastateltavalle jokseenkin samassa muodossa, jonka jälkeen haastateltava saa vastata kysymyksiin vapaassa muodossa haluamallaan tavalla (Hyvärinen, Suoninen & Vuori 2021). Haastatteluja varten oli laadittu tärkeimpiä kysymyksiä, joiden lisäksi oli vapaampaa keskustelua aiheesta. Haastatteluja tehtiin yhteensä viisi, joista kaksi toteutettiin kasvotusten ja loput kolme Teams-haastatteluna. Kaikki haastattelut tallennettiin ja litteroitiin. Litteroinnilla tarkoitetaan puheen ja toiminnan kirjoittamista tekstimuotoon (Kallio 2021).

Lopuksi vastaukset analysoitiin. Tulokset analysoitiin sisällönanalyysina. Sisällönanalyysia suositellaan käytettävän tapauksessa, jossa tutkimuksen aihe on konkreettinen ja kertoo mihin aineisto viittaa (Vuori 2021a). Sisällönanalyysille ei ole tiettyjä sääntöjä eikä sitä ohjaa tietyt menetelmälliset käsitteet (Vuori 2021b). Tuloksia käsiteltiin ensin koodaamalla aineiston ryhmiin, jonka jälkeen tulokset analysoitiin. Koodausta käytetään analyysin pohjana, jolloin aineistoa käydään tarkasti läpi etsien samoja seikkoja tuloksista (Vuori 2021b). Analyysivaiheessa tuloksista tehtiin johtopäätöksiä, jotka vastaavat tutkimuskysymyksiin.

4.2 Tutkimustulokset

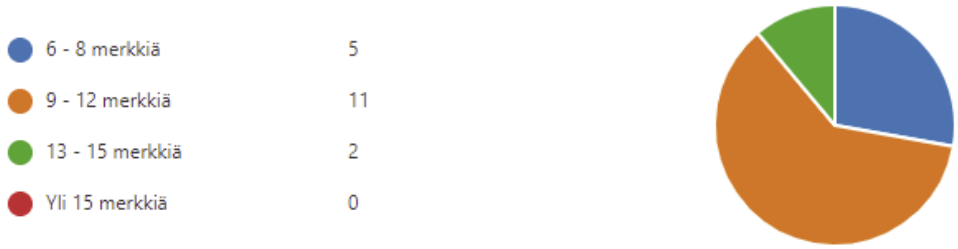
4.2.1 Kyselyn tulokset

Kyselyyn vastasi 18 henkilöä eri ammateista. Vastaajista reilu puolet olivat naisia ja kaksi kolmasosaa olivat 36–45-vuotiaita (kuva 1). Alle 26-vuotaita ei ollut lainkaan ja neljä henkilöä oli 45–50-vuotiaita.

Kuva 1. Kyselytutkimukseen osallistuneiden ikäjakauma

Salasanan vahvuutta tutkittiin eri kysymyksillä. Ensimmäisessä kysymyksessä kysyttiin, löytyykö jompi kumpi tai molemmat tyypillisestä salasanasta? A) Salasanassa on lause tai lauseesta on tehty merkkijono. B) Salasana sisältää kolme asiaa seuraavista: iso kirjain, pieni kirjain, numero tai erikoismerkki. Puolet vastaajista kertoi, että salasanasta löytyvät molemmat ja toinen puolikas vastaajista kertoi, että toinen näistä löytyy tyypillisestä salasanasta.

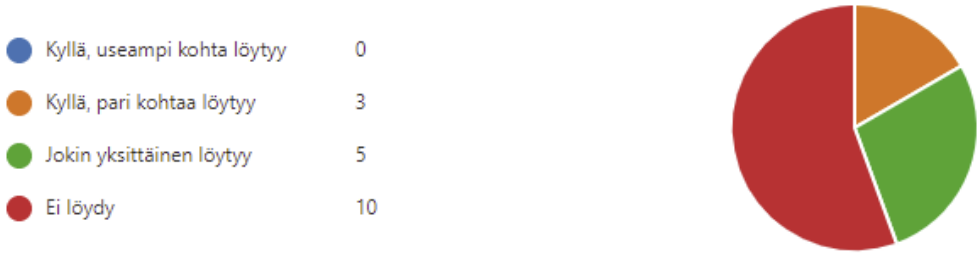
Kyselyssä selvitettiin myös salasanojen pituuksia kysymällä, kuinka pitkä tyypillinen salasana on, jos pituuden saa itse valita? Lähes kaksi kolmasosaa eli 11 henkilöä vastasi, että salasana olisi 9–12 merkkiä ja viisi vastasi, että se olisi 6–8 merkkiä pitkä (kuva 2). Kaksi henkilöä valitsisi salasanan pituudeksi 13–15 merkkiä, mutta kukaan ei valitsisi pidempää salasanaa.



Kuva 2. Omavalintainen salasanan pituus

Salasanan mahdollisia heikkouksia selvitettiin kysymällä, löytyykö tyypillisestä salasanasta jokin seuraavista: syntymäaika, rekisterinumero, julkisuuden henkilö, läheisen nimi, käyttäjätunnus etuperin tai takaperin tai kyseisen palvelun nimi, johon salasana käy? Reilu puolet eli 10 henkilöä vastasi, ettei sisällytä mitään näistä tyypilliseen salasanaansa (kuva

3). Viisi vastasi, että jokin yksittäinen näistä on käytössä ja kolme vastasi, että pari kohtaa löytyy.



Kuva 3. Salasanojen mahdollisia heikkouksia

Lisäksi kysyttiin, käyttävätkö ihmiset samaa salasanaa useammassa kuin yhdessä palvelussa, johon viisi vastasi, että ei ja toiset viisi vastasi, että kyllä (kuva 4). Kuusi henkilöä vastasi käyttävänsä samankaltaista, johon tekee pienen muutoksen käyttäessään sitä uudelleen. Kaksi vastasi käyttävänsä kahta tai kolmea salasanaa vuoroin eri palveluissa.

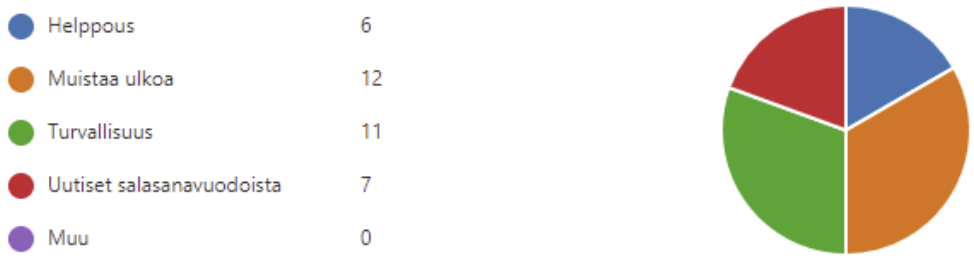
Kuva 4. Salasanojen käyttö useammassa kuin yhdessä palvelussa

Kyselyssä kysyttiin myös sitä, mitkä tekijät vaikuttavat salasanavalintoihin. Tähän pystyi valitsemaan yhden tai useamman kohdan. Vaihtoehdot olivat helppous, muistaa ulkoa, turvallisuus, uutiset salasanavuodoista tai sai kertoa jonkun muun listasta puuttuvan vaihtoehdon. 12 henkilöä piti tärkeänä sitä, että salasanan muistaa ulkoa ja 11 henkilöä kertoi turvallisuuden vaikuttavan salasanan valintaan (kuva 5). Kuusi henkilöä vastasi, että helppous ja seitsemän vastasi, että valintaan vaikuttaa uutiset salasanavuodoista. Kukaan ei ilmoittanut muuta vaihtoehtoa, mutta kolme henkilöä kertoi avovastauksena tarkemmin salasanaan vaikuttavista tekijöistä seuraavasti:

”*Riippuu paljon rekisteröitymistä vaativan palvelun luotettavuudesta tai sen vaikutelmasta. 2 vaiheista tunnistautumista tarjoavissa sovelluksissa salasanana tulee käytettyä ehkä yksinkertaisempia kuin jossain kiinalaisessa verkkokaupassa.*”

”*Salasanojen hallintaohjelman avulla salasana voi olla aivan erilainen kaikissa paikoissa.*”

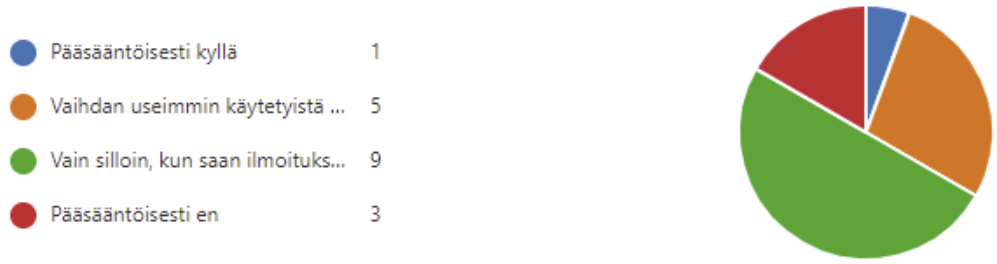
”*Satunnainen merkkijono paras.*”



Kuva 5. Salasanoihin vaikuttavat tekijät

Koska salasanoja kertyy useita ja joukkoa vahvoja salasanoja on lähes mahdoton muistaa ulkoa, kyselyssä kysyttiin, onko ihmisillä käytössä salasananhallintasovellus. Reilu puolet vastaajista eli 10 henkilöä kertoi, että heillä on käytössä salasanojenhallintasovellus ja seitsemän vastasi, ettei ole. Yksi vastaajista ei ollut varma, onko hänellä käytössä sellaista. Lisäksi kyselyssä kysyttiin, tallentavatko ihmiset salasanoja selaimeen, johon lähes kaksi kolmasosaa vastasi kyllä ja kuusi vastasi ei. Yksi ei ollut varma, tallentaako hän salasanat selaimeen.

Salasanojen hallintaan liittyen kysyttiin vielä, vaihtavatko ihmiset salasanoja säännöllisesti, vaikka palvelu ei sitä vaadi. Tähän puolet eli yhdeksän henkilöä vastasi vaihtavansa salasanan ainoastaan silloin, kun saa ilmoituksen, että salasana on mahdollisesti joutunut vääriin käsiin ja kolme ei pääsääntöisesti vaihda salasanoja (kuva 6). Yksi henkilö vastasi, että hän pääsääntöisesti vaihtaa salasanat ja viisi henkilöä vastasi vaihtavansa useimmin käytettyjen palvelujen salasanat säännöllisesti.



Kuva 6. Salasanojen vaihtaminen

Lopuksi selvitettiin vielä turvallisuuskäyttäytymistä kysymällä, käyttävätkö ihmiset kaksiosaista tunnistautumista, jos se on mahdollista. Enemmistö, eli 15 henkilöä vastasi kyllä ja vain yksi vastasi ei. Loput kaksi vastasi, että joskus.

4.2.2 Haastattelujen tulokset

Ensimmäisenä haastateltavat pyydettiin palaamaan mielikuvaan siihen tilanteeseen, kun heidän tulee luoda uusi salasana. Se tehtiin kysymällä, että kun he rekisteröityvät uuteen

palveluun ja heidän täytyy luoda uusi salasana niin, mitä ajatuksia tai tunteita heille nousee ensimmäisenä mieleen. Kolme haastateltavaa kertoi tuntevansa turhautuneisuutta luodessaan uutta salasanaa. Neljä viidestä kertoivat, että he alkavat ensimmäisenä miettiä salasanan monimutkaisuutta eli kuinka vaikea salasana tulisi olla kyseiseen palveluun. Kolme vastaajista pohtii myös kyseisen palvelun luotettavuutta siitä näkökulmasta, haluavatko he antaa palvelulle henkilökohtaisia tietoja ja kuinka suuri riski on, että palveluntarjoaja käyttää tietoja väärin tai heiltä vuotaa tiedot esimerkiksi tietovuodon seurauksena eteenpäin.

Seuraavaksi selvitettiin, kuinka usein haastateltavat törmäävät sähköpostissa kalasteluviesteihin tai epäilyttäviin linkkeihin. Vain yksi haastateltavista kertoi, että kalasteluviestejä tai epäilyttäviä linkkejä tulee sähköpostilla joka päivä. Loput vastasivat, että hyvin harvoin, jonka tulkinta vaihteli kerran kuukaudesta kerran vuoteen. Kaksi vastaajista kertoi, että näitä viestejä suodattuu todella paljon roskaposti-kansioon, mutta yksi haastateltava kertoi, ettei edes roskaposteista löydy tällaisia viestejä.

Kolmannella kysymyksellä selvitettiin missä haastateltavat törmäävät tietoon salasanojen turvallisuudesta ilman, että he etsivät tietoa tai ovat luomassa uutta salasanaa. Kaksi henkilöä muisti lehtikirjoituksia aiheeseen liittyen ja yksi muisti nähneensä jossain F-Securen työntekijöiden haastattelun. Kaksi haastateltavaa kertoivat törmäävänsä aiheeseen työn puolesta.

Seuraavaksi kysyttiin, mitä kautta haastateltavat haluaisit saada tietoa hyvistä salasanakäytännöistä ja saavatko he tietoa riittävästi ilman, että etsivät sitä. Kolme haastateltavaa kertoivat, että he haluaisivat saada tietoa sähköpostilla. Kuitenkin kaksi vastasi, että sähköpostilla saatu tieto jäisi lukematta ja hukkuisi muuhun sähköpostivirtaan. Kaksi vastasi, että some olisi hyvä kanava saada tietoa hyvistä salasanakäytännöistä ja kaksi haluaisi, että tietoa tulisi työn kautta. Kaksi vastasi, että haluaisi saada tietoa hyvistä salasanakäytännöistä niistä palveluista, joita käyttää. Yksi vastaajista kertoi, että haluaisi saada tällaiset tiedot Kyberturvallisuuskeskukselta tai viranomaisilta. Miettiessään vastausta kaksi totesi, että hyvin vähän aihe tulee etsimättä eteen.

Viidentenä haastateltavilta kysyttiin salasanojen ohjeistuksen selkeydestä eli kun on luomassa uutta salasanaa, lukevatko he ohjeet salasanan muodostamiseksi ja millaisiksi he ohjeet kokivat. Kolme viidestä vastasi, ettei lue ohjeita luodessaan uutta salasanaa ja loput kaksi vastasivat, että he vilkaisevat ohjeesta minimivaatimuksen salasanan pituudelle. Pitkät ohjeet koettiin huonoina ja hyvän ohjeen merkkejä olivat lyhyyden lisäksi selkeys ja ohjetekstin suuri koko. Lisäksi kaksi henkilöä mainitsi visuaalisuuden tuovan helppoutta salasanaa luodessa. Kummatkin mainitsivat viisarin, joka matkaa punaisesta vihreään sitä

mukaan, kun käyttäjä kirjoittaa salasanaa, jolloin punainen kuvastaa heikkoa salasanaa ja vihreä vahvaa salasanaa.

Lopuksi kysyttiin, onko jokin tapahtuma tai tieto saanut haastateltavia muuttamaan aiempaa salasanakäytäntöä ja millainen tilanne oli. Kolme haastateltavaa kertoi, ettei mikään ole muuttanut salasanakäytäntöjä, mutta siitä huolimatta yksi heistä tunnisti, että salasanakriteerit ovat muuttuneet ja siten myös salasanat. Yksi haastateltava, joka ei ole muuttanut salasanakäytäntöään kertoi, että asia on mietityttänyt yleisellä tasolla, kun on kuullut, että ihmiset ovat joutuneet pulaan tietovuodon takia. Kaksi haastateltavaa kertoi, että työpaikan muuttuneet salasanakäytännöt, kuten salasanojen vaihtotiheys ovat muuttaneet omaa vapaa-ajan käytäntöä salasanojen suhteen.

5 Pohdinta

5.1 Pohdintaa tuloksista

Tutkimuksen tavoitteena oli selvittää, kuinka ihmiset hallinnoivat eri palvelujen salasanoja arjessa ja kuinka turvallisia käytössä olevat salasanat ovat. Tutkimuksessa lähdettiin selvittämään vastauksia näihin kysymällä erilaisia kysymyksiä liittyen vahvojen ja heikkojen salasanojen tunnusmerkkeihin sekä kysymällä kysymyksiä salasanojen hallintaan liittyen. Tutkimuksessa selvitettiin myös turvallisuuskäyttäytymistä salasanoihin liittyen ja sitä, miten tieto saavuttaa käyttäjät.

Teoriaosuudessa kävi ilmi, että vahva salasana on pitkä, joka sisältää erikoismerkkien lisäksi myös isoja kirjaimia. Lisäksi salasanan tulisi olla mieluummin lause kuin pelkkä sana. Kun salasanan vahvuutta selvitettiin kyselyssä, kävi ilmi, että kaikkien vastanneiden salasanat sisälsivät lauseen/lauseesta tehdyn merkkijonon tai kolme asiaa seuraavista: iso kirjain, pieni kirjain, numero tai erikoismerkki. Tämä tieto oli yllättävä, mutta toisaalta nykyiset salasanavaatimukset ovat hyviä useimmissa kirjautumista vaativissa palveluissa. Jopa puolella 18:sta vastanneesta oli molemmat ominaisuudet salasanoissa. Tämä vaikuttaa epäuskottavalta, mutta voiko tämä pitää paikkansa?

Vahva salasana on pitkä, mieluiten 15 merkkiä ja on myös hyvä huomioida, että mitä pidempi salasana on, sitä turvallisemmaksi se tulee. Tämän teorian pohjalta tutkittiin vastaajien salasanojen tilanne kysymällä, kuinka pitkä tyypillinen salasana on, jos pituuden saa itse valita? Oli yllättävää, että vain viisi valitsisi salasanan pituudeksi 6–8 merkkiä. Tämä on useimpien palveluiden salasanan pituusvaatimus, joten olettamuksena oli, ettei ehkä kovin moni valitsisi pidempää salasanaa vapaaehtoisesti. Kuitenkin lähes kolmasosa vastaajista valitsisi 9–12 merkkiä, joka on jo aika hyvä pituus salasanalle. Kuitenkin vain kaksi valitsisi teorian mukaan suositellun salasanan pituuden 15 merkkiä. Tämän tutkimuksen perusteella voidaan todeta, että tilanne on huomattavasti parempi kuin vuonna 2010, jolloin huomattiin, että jos palvelu ei aseta vaatimuksia salasanan vahvuudelle, heikot salasanat ovat yleisiä.

Kyselystä saatujen vastausten perusteella tilanne on vielä hyvä, mutta asiaa tutkittiin myös toisesta näkökulmasta eli siitä, löytyykö salasanoista joitain heikkouksia, jolloin vastausten luotettavuus mahdollisesti vahvistuu. Teorian mukaan heikkoja salasanoja ovat esimerkiksi oma nimi, helppo sana tai syntymäaika. Salasana ei myöskään tulisi olla sama kuin käyttäjätunnus tai käyttäjätunnus takaperin kirjoitettuna eikä palvelun nimi, johon salasanaa käytetään. Tämän pohjalta kysyttiin, löytyykö tyypillisestä salasanasta jokin seuraavista: syntymäaika, rekisterinumero, julkisuuden henkilö, läheisen nimi, käyttäjätunnus

etuperin tai takaperin tai kyseisen palvelun nimi, johon salasana käy. Vastaukset tukivat aiempia vastauksia, koska kymmenen vastaajista kertoi, että mitään luetelluista ominaisuuksista ei löydy tyypillisestä salasanasta. Kysymys ei paljasta käyttääkö joku jotain luetelluista asioista ainoana tai yhdistettyinä, joten se, että viisi vastasi, että jokin yksittäinen löytyy tai että kolme vastasi, että pari kohtaa löytyy, ei suoraan kerro, onko käytetyt salasanat heikkoja. Kuitenkin hieman yli puolet vastasi, että mitään näistä ei löydy, joka kertoo, että todennäköisesti heidän salasanansa ovat vahvoja.

Kukin palvelu ohjeistaa omat kriteerit salasanan muodostamiselle ja sitä kautta voi saada tietoa vahvan salasanan kriteereistä. Haastattelussa syvennyttiin tietoisuuteen salasanoista ja selvitettiin mistä muualta haastateltavat saavat tietoa hyvistä salasanakäytännöistä ja vahvoista salasanoista. Kävi ilmi, että lähes jokainen joutui miettimään vastausta pidempään ja kaksi totesikin, että aihe tulee hyvin vähän etsimättä eteen. Ilmiö on huolestuttava, koska kyseessä on hyvin arkinen asia.

Haastatteluissa selvitettiin lukevatko haastateltavat ohjeen salasanan muodostamiseksi, koska sieltä voisi saada tietoa, kuinka vahva salasana muodostetaan. Kuitenkin kolme henkilöä kertoi, ettei lue näitä ohjeita ja loput kaksi kertoivat vilkaisevansa vaatimuksen salasanan pituudelle eli siinäkään kohtaa tieto ei välttämättä tavoita. Haastateltavat kertoivat, että he luovat uuden salasanan kokeilemalla, kunnes kriteerit täyttyvät ja luominen onnistuu. Yksi haastateltava kertoi, että hän ei siinä kohtaa halua jäädä lukemaan ohjetta, koska hän haluaa päästä itse palveluun mahdollisimman nopeasti. Esimerkkinä hän kertoi ohjelmapalvelun. Hän saa ajatuksen, että haluaa katsoa jonkun elokuvan ja löytää palvelun, josta sen näkee. Hän avaa palvelun ja törmää kirjautumiseen. Tähän hän ei etukäteen ajatellut käyttävänsä aikaa, joten hän hoitaa asian mahdollisimman nopeasti ja vaivattomasti pois alta.

Ohjelmoijan näkökulmasta on kiinnostava tietää, mitkä ovat ne keinot, joilla voidaan rekisteröitymishetkellä kannustaa asiakkaita kiinnittämään huomiota salasanaturvallisuuteen. Kaksi haastateltavaa nostivat esille salasanan vahvuusmittarin. Heidän kehonkielestään ja innostuneesta puheestaan huomasi, että tämä on asia, joka on herättänyt positiivisesti huomion. Värien käyttö, joissa punainen on heikko ja vihreä on vahva sekä viisari tähän asteikkoon, antavat välittömän palautteen salasanaa kirjoittaessa. Vaikka viisari olisikin jo vihreän puolella, käyttäjässä voi herätä tahto saada viisari aivan huippuunsa, jolloin hän vahvistaa salasanaa entisestään. Lisäksi yksi haastateltava kertoi pitävänsä listasta, jossa on kriteerit ja aina, kun salasanasta löytyy joku näistä kriteereistä, se kriteeri poistuu näkyvistä. Selvää on, että tässä viiden henkilön haastattelun otannassa kukaan ei pitänyt perinteisestä ohjetekstistä, vaan se jäi lukematta.

Haastatteluissa kävi ilmi, että oli useampaa näkemystä siitä, mistä tietoa halutaan saada. Tähän ei varmasti ole yhtä oikeaa vastausta, vaan tietoa täytyy jakaa eri kanavista ja eri tavoin, jotta se välittyy kaikille. Vastauksista selviää, että kun kyseessä on jo tapahtunut tietovuoto, tieto tulisi esittää selkeästi ja ytimekkäästi, jotta se varmasti luetaan. Palvelun-tarjoajat voivat tuottaa yleistä tietoa oman näköisellä tavalla omaa brändiä hyväksikäyttäen. Sosiaalisessa mediassa tieto voi olla modernissa muodossa esimerkiksi meemien ja lyhyiden hauskojen videoiden muodossa. Uskottavuutta tuo se taho, joka sisällön on tuottanut. Poliisi tai valtioneuvosto voivat tuottaa saman tiedon eri kanavissa eri tavoin. Verohallinnon sosiaalinen media oli herättänyt yhden haastateltavan mielenkiinnon, joka osoittaa, että vakavasti otettava viranomainen voi olla myös houkutteleva:

”Esimerkiks siis verohallinnon somehan on nykyään niinku aivan priimaa.”

Koska salasanoihin liittyvää turvallisuutta voidaan tukea muillakin keinoilla, kun salasanan vahvuudella, tutkittiin myös näihin liittyviä käytäntöjä. Teorian mukaan jokaiseen palveluun olisi hyvä käyttää eri salasanaa ja vaihtaa ne säännöllisesti. Tutkimuksessa kysyttiin käyttävätkö ihmiset samaa salasanaa useassa palvelussa, johon viisi vastasi, että ei ja toiset viisi vastasi kyllä. Kuusi henkilöä vastasi käyttävänsä samankaltaista, johon tekee pienen muutoksen käyttäessään sitä uudelleen. Kaksi vastasi käyttävänsä kahta tai kolmea salasanaa vuoroin eri palveluissa.

Teorian mukaan salasanat voidaan jakaa kolmeen ryhmään: kriittiset-, tärkeät- ja peruspalveluissa käytettävät salasanat. Luokitus riippuu siitä, kuinka kriittinen ja tärkeä palvelu on kyseessä. Esimerkiksi tärkeissä palveluissa, voidaan käyttää samankaltaisia salasanoja, mutta on hyvä huomioida, että ne eivät voi olla niin samankaltaisia, että yhden salasanan päätyminen vääriin käsiin, avaa pääsyn myös muihin tärkeisiin palveluihin. Peruspalveluissa, joissa ei käsitellä mitään aiemmin mainittuja, salasanat voivat olla jopa samoja, mutta silloinkin tulee käyttää vahvaa salasanaa. Tämän valossa katsottuna on mahdollista, että vaikka vain viisi kielsi käyttävänsä samaa salasanaa useammassa palvelussa, tilanne ei välttämättä ole kovin huono. Vastauksista ei selviä, onko useassa paikassa käytetyt salasanat peruspalveluihin vai ei. Myöskään vaihtoehto ”käytän samankaltaista, johon teen pienen muutoksen käyttäessäni sitä uudelleen”, ei kerro, onko ero tarpeeksi suuri, ettei yhden salasanan vuoto paljasta myös muita salasanoja liian helposti.

Kysymykseen, vaihtavatko ihmiset salasanoja säännöllisesti, vaikka palvelu ei sitä vaadi, puolet eli yhdeksän henkilöä vastasi vaihtavansa salasanan ainoastaan silloin, kun saavat ilmoituksen, että salasana on mahdollisesti joutunut vääriin käsiin. Kolme ei pääsääntöisesti vaihda salasanoja ja vain yksi henkilö vastasi, että pääsääntöisesti vaihtaa salasanat. Viisi henkilöä vastasi vaihtavansa useimmin käytettyjen palvelujen salasanat

säännöllisesti. Tämä on siinä mielessä ymmärrettävää, että salasanoja on hyvin paljon ja monesti käytössä on automaattinen kirjautuminen useimmin käytettyihin palveluihin. Tällöin salasanojen olemassaolon voi melkein unohtaa. Kuitenkin huolestuttavan harva vaihtaa salasanojaan säännöllisesti, koska vaihtamalla salasanat, mahdollinen väärinkäyttö voidaan katkaista, mikäli salasana on huomaamatta päätynyt vääriin käsiin. Voi myös olla, että salasanaa ei keretä murtaa, jos se vaihdetaan tarpeeksi usein.

Salasanojen hallintasovelluksen avulla voidaan luoda ja säilyttää useita vahvoja salanoja, joita ei pysty muistamaan. Reilu puolet vastaajista, eli 10 henkilöä kertoi, että heillä on käytössä salasanojenhallintasovellus. Tämä voi olla yksi syy siihen, miksi tässä otannassa salasanojen vahvuus on niin hyvä. Seitsemän kuitenkin vastasi, ettei käytä tällaista sovellusta, joka tukee niitä vastauksia, joissa salasanoissa on käytetty helppoja apusanoja/numeroita ja niitä vastauksia, joissa salasanaa käytetään useamman kerran.

Vaikka haastattelussa ei kysytty salasanojen hallintasovelluksista, kaksi haastateltavaa kuitenkin kertoi, ettei luota salasanojen hallintasovellukseen, koska kokee, että sen palveluntarjoaja tulisi olla niin luotettava, että antaisi kaikki salasanat heille. Lisäksi salasanan hallintasovellukset nostivat yhdessä haastateltavassa ajatuksen, että lähtökohta sovelluksen käytölle olisi se, että luottaisi toimijaan enemmän kuin itseensä. Lisäksi hän koki sovelluksen hieman loukkaavana sillä ajatuksella, että hän ei muka itse osaisi luoda salasanaa ja olisi niin laiska, että tarvitsisi generaattorin tekemään sen työn hänen puolestaan. Tämä on mielenkiintoinen näkökulma, että sovelluksen käytön voi kokea myös laiskuutena. Haastateltava kuitenkin lisäsi puheenvuoronsa perään, että todennäköisesti kone osaa luoda parempia salasanoja kuin ihminen.

Teorian mukaan kaksivaiheinen tunnistautuminen on ylimääräinen turvallisuustaso, jolla varmennetaan, että ihminen on se, kuka hän kertoo olevansa käyttäjätunnuksen ja salasanan avulla. Kun käyttäjä kirjautuu palveluun, hän ei käyttäjätunnuksen ja salasanan syöttämisen jälkeen pääsekään palveluun, vaan hänen täytyy vahvistaa todennus vielä toisella tapaa. Tämä auttaa suojaamaan käyttäjätiliä erilaisilta uhilta, kuten tietojenkalastelun ja salasanojen uudelleenkäyttöhyökkäyksen seurauksilta. Enemmistö kyselyyn vastanneista, eli 15 henkilöä vastasi käyttävänsä kaksiosaista tunnistautumista, jos se on mahdollista. Tämä on aika iso lukema siihen nähden, että vastausvaihtoehtona oli myös joskus. Tämä kuitenkin kertoo siitä, että moni haluaa turvata käyttäjätilinsä ja ovat kiinnostuneita tietoturvasta.

Teorian mukaan verkkorikolliset hyödyntävät haittaohjelmia päästäkseen käsiksi henkilötietoihin ja pankkitunnuksiin esimerkiksi tutkimalla laitteen tiedostoja. Lisäksi haittaohjelmat ovat yleinen keino varastaa salasanoja, jotka ovat tallennettu selaimiin.

Tutkimuksessa selvisi, että lähes kaksi kolmasosaa vastaajista tallentaa salasanat selaimeen ja kuusi ei tallenna. Salasanojen tallentaminen selaimeen on helppo ja nopea tapa käyttää salasanoja, mutta ei silloin, jos käytössä on useampia laitteita.

Teorian mukaan tietomurrolla tarkoitetaan sitä, että joku tunkeutuu luvatta johonkin tietojärjestelmään esimerkiksi käyttämällä luvatta käyttäjätunnusta tai ohittamalla turvajärjestelyn, jotta päästään murtautumaan järjestelmään. Tietojenkalastelu käyttäjältä sähköpostiviestin avulla on yleisin ja tunnetuin tapa tehdä tietomurto ja usein se toteutetaan houkuttelemalla uhri aidolta näyttävälle kirjautumissivulle, jossa uhri syöttää kirjautumistiedot antaen ne tietämättään väärälle taholle. Uhrille voidaan lähettää esimerkiksi jokin varoitus, jonka tavoitteena on säikäyttää tilin omistaja ja saada hänet kiireellisesti klikkaamaan viestissä olevaa linkkiä. Tämän valossa oli huolestuttavaa kuulla, että yksi haastateltava toivoisi tietovuotoilmoituksen sähköpostilla ja kertoi, että olisi hyvä, jos ilmoituksen ohessa olisi linkki, josta salasanan voisi käydä nopeasti vaihtamassa.

Tämän välttääkseen on syytä mennä palvelun oman verkkosivun kautta kirjautumaan palveluun eikä klikata sähköpostissa olevaa linkkiä. Kalasteluviestit ja linkit valesivuille ovat yleisiä ja on tärkeää saada välitettyä tietoa salasanaturvallisuudesta, jotta ihmiset eivät vahingossa anna salasanaa väärälle taholle. Vaikka vain yksi kertoi saaneensa näitä viestejä päivittäin ja muut harvemmin, niin yksikin viesti riittää siihen, että erehdyksissä annat käyttäjätunnuksen ja salasanan eri taholle kuin oli tarkoitus.

Toinen huolestuttava yksityiskohta nousi esille yhdessä haastattelussa, jossa haastateltava kertoi käyttävänsä samoja salasanoja sekä töissä että vapaa-ajalla. Muissakin haastatteluissa ilmeni sitä, että samoja salasanoja käytetään useammassa palvelussa. Henkilöllä saattaa olla esimerkiksi muutama salasana, jota käyttää eri palveluissa tehden niihin hieman variaatioita, jotta ne ovat kuitenkin erilaisia. Työnantajan näkökulmasta on iso riski, jos työntekijät käyttävät samoja salasanoja työssä ja vapaa-ajalla. Työsähköposti on lisäksi monissa paikoissa julkisesti tarjolla, joka on usein myös käyttäjätunnus. Jos vapaa-ajan palvelun kautta rikollinen saa salasanan, hänellä on mahdollisesti työsähköpostin kirjautumiseen vaadittavat tiedot kasassa. Jos näin käy, rikollinen pääsee hyödyntämään todellisen yrityksen nimissä lähteviä sähköposteja, jotka voivat vakuuttaa saajan viestin oikeellisuudesta.

Teorian mukaan tekstiviestillä saadun kertakäyttösalasanan käyttäminen ainoana todentamisena toimii niin, että käyttäjältä pyydetään puhelinnumero, johon tunnuskoodi lähetetään. Sen jälkeen käyttäjä antaa tekstiviestillä saadun tunnuskoodin, tai sovellus lukee sen automaattisesti saapuneesta viestistä, jonka jälkeen käyttäjä pääsee palveluun. Tämä menetelmä helpottaa käyttäjää, koska käyttäjän ei tarvitse luoda ja muistaa uuden

palvelun salasanaa. Erään haastateltavan tilanteessa palveluntarjoajat eivät välttämättä tarjoa kertakäyttösalasanaa tunnistautumiskeinona, mutta hän ei useinkaan muista luomiaan salasanoja ja valitsee ”unohditko salasanan”, jolloin hän saa kertakäyttösalasanan kirjautuakseen palveluun.

Toisessa tapauksessa haastateltava kertoi, että hän tarvitsee menetelmää silloin, kun salasanaa luodessa ei ole sitä silmää valittavissa, jota painamalla saa luettua antamansa salasanan. Eli rekisteröitymisen yhteydessä ei näe, minkä salasanan juuri kirjoitti, mutta onnistuu kuitenkin luomaan salasanan. Seuraavan kirjautumisen yhteydessä salasana on väärä, joten täytyy tilata kertakäyttösalasana ”unohditko salasanan” kautta. Usein palveluissa on kuitenkin toinen kohta, johon salasana syötetään uudelleen, joka ehkäisee näitä tilanteita. Kertakäyttösalasana tunnistautumisena kerää varmasti kannattajia sen helppouden takia. Jos harvoin kirjautuu palveluun, voi olla stressaavaa miettiä löytääkö sen palvelun salasanaa mistään. Etenkin tapauksissa, joissa ei käytä salasanan hallintasovellusta, jossa kaikki on tallessa, vaikka niitä ei usein käyttäisikään.

Teorian mukaan tulee kiinnittää huomiota siihen, kuinka salasanan kirjoittaa. Sormenjälkitunnistautumista tai muuta biometristä tunnistautumistapaa tulisi käyttää aina, jos se on mahdollista, jotta kukaan ei vahingossakaan näe salasanaa. Eräässä haastattelussa haastateltava kertoi, ettei käytä mobiililaitteessa sormenjälkitunnistinta, vaan syöttää joka kerta numerokoodin käsin. Numerokoodi on kuitenkin vakoiltavissa ja siten laite on helpompi varastaa ilman, että tilanne saa suurta huomiota esimerkiksi junassa. Puolustuksena numerokoodille oli se, että varas voi pakottaa antamaan sormenjäljen varastamisen yhteydessä. Se kuitenkin herättää helposti ulkopuolisten huomion. Numerokoodin voi huomaamattomasti vakoilla etukäteen ja varastaa puhelin taskusta tai laukusta ruuhkassa, vaikka junasta poistuttaessa ja paeta paikalta.

5.2 Oma oppiminen ja opinnäytetyöprosessi

Haastattelujen jälkeisissä keskusteluissa ja luettuani heikoimpien salasanojen listoja, huomasin, että ihmisen luomissa salasanoissa ilmenee tiettyjä inhimillisiä piirteitä, kuten arkisia sanoja tai asioita, joita näkee ympärillään. Myös niiden muuntamisessa voi olla vaikeaa keksiä ennustamattomampaa variaatiota kuin i=1. Haastatteluiden jälkeen osassa keskusteluissa tuli yllätyksenä, että hakkerit voivat käyttää avukseen erilaisia sanastoja salasanojen ratkaisemiseen eli niin sanottua Brute force-menetelmää. Suomen kielessä on onneksi runsaasti taivutusmuotoja ja murteita, joita voi käyttää avukseen, jos haluaa keksiä salasanan itse ja haluaa huomioida tämän riskin.

Tutkimusta tehdessä ajattelin, että salasanojen tilanne olisi huonompi, mitä vastaukset kertoivat. Ymmärsin kuitenkin sen, että salasanavaatimukset ovat lähes kaikissa palveluissa jo aika hyvät, joka ohjaa vastaajien valintoja ja tottumuksia. Haastattelut toivat lisää syvyyttä ja sai minut pohtimaan sovelluksen tekijän näkökulmasta, mitkä keinot voisivat edesauttaa hyvien salasanojen valintaan. Lisäksi mieleeni jäi hyvin vahvasti se, että tietoisuutta tulisi lisätä ja miettiä mitkä kanavat ja keinot olisivat siihen hyviä, jotta tieto houkuttelee pysähtymään asian ääreen.

Kun olin tehnyt ensimmäisen version kyselylomakkeesta, lähetin sen kommentoitavaksi kahdelle henkilölle, joka osoittautui todella hyväksi ratkaisuksi. Ensimmäinen versio kyselystä oli liian sensitiivinen eikä olisi ollut eettistä asetella kysymyksiä sillä tavalla. Olisi ollut todennäköistä, että kysely olisi jätetty kesken, eikä sen vastauksia olisi lähetetty minulle takaisin. Julkaistu versio oli mielestäni onnistunut ja keksin ratkaisut siihen, miten voin kysyä näin arkaluonteisia tietoja ilman, että syntyy suurempaa pelkoa siitä, että saan väärinkäytettyä tuloksia.

Opinnäytetyötä tehdessä opin, että on kahdenlaista näkemystä siitä kannattaako salasanaa vaihtaa tiheästi. Niissä lähteissä, joissa salasanaa ei suositella vaihdettavan, perustuu siihen, että salasanan vaihtaminen heikentää salasanoja. Kun käyttäjä tietää, että salasana on pian vaihdettava, hän valitsee heikkoja ja helposti muistettavia salasanoja. Ne lähteet, joissa salasanaa suositeltiin vaihtamaan mahdollisimman usein, perusteena oli salasanan väärinkäytön estäminen tai viimeistään katkaiseminen, jos salasana on joutunut vääriin käsiin. Tämä ristiriita ratkeaa käyttämällä salasananhallinta sovellusta, josta voi luoda vahvoja salasanoja helposti ja ottaa vaihdetut salasanat käyttöön suhteellisen vaivatta.

Lisäksi opin erilaisista kasvojen- ja sormenjälkien tunnistustekniikoista. Käsitykseni oli, ettei kasvojen tunnistustekniikka mobiililaitteissa osaa vielä hyödyntää infrapunakuvaa eikä tunnistus siten toimisi pimeässä. Opin myös erilaisista tavoista tehdä tietomurto sekä mitä eroavaisuuksia erilaisilla salasanan hallintasovelluksilla voi olla eli mihin paikkoihin salasanat eri sovelluksissa tallentuvat.

Minulla oli teoriaosuuden puolivälissä hankaluuksia tiedonhaussa, mutta opittuani eri termejä englanniksi, alkoi tietoa löytymään ihan eri tavalla. En ole aiemmin käyttänyt juurikaan tässä opinnäytetyössä ilmenneitä termejä, koska käytän vain niitä termejä, joiden merkityksen ymmärrän. Nyt sain sanastooni paljon uusia termejä ja lisäksi ymmärrystä siitä, mitä termit käytännössä tarkoittavat. Rohkaistuin myös kiinnostumaan alan ammattisanastosta ihan uudella tavalla, kun huomasin lopulta ymmärtäväni niiden merkityksen.

5.3 Jatkotutkimusehdotukset

Tutkimuksessa selvisi, että tietoutta salasanojen turvallisuudesta jaetaan liian vähän ja se ei ole nykyisessä muodossaan tarpeeksi houkuttelevaa. Ehdotukseni on, että tutkittaisiin millainen tieto tavoittaisi ihmiset mahdollisimman laajasti. Voisi myös tutkia erilaisien ohjeiden kiinnostavuutta salasanaa luodessa. Lisäksi voisi tutkia minkälaista opetusta peruskoulut antavat salasanaturvallisuudesta. Peruskoulujen oppilailla on kuitenkin laajasti käytössä mobiililaitteet jo hyvin varhaisesta iästä alkaen.

Lisäksi voisi tutkia lisää sitä, mitkä asiat vaikuttavat salasanaturvallisuutta vahvistavasti. Mitkä ovat ne keinot ja tekijät, joilla saadaan ihmiset tekemään parempia ratkaisuja luodessaan salasanoja? Tämä tutkimus antaa kuitenkin viitettä siitä, että ihmiset miettivät asiaa ja haluavat huolehtia salasanaturvallisuudesta ja ovat tietoisia vahvuuteen vaikuttavista tekijöistä.

Lähteet

Apple 2021. Tietoja edistyksellisestä Face ID -tekniikasta. Luettavissa: https://support.apple.com/fi-fi/HT208108. Luettu: 26.9.2021.

Dell'Amico, M., Michiardi, P. & Roudier, Y. 2010. Password Strength: An Empirical Analysis. IEEE Xplore. Luettavissa: https://ieeexplore.ieee.org/abstract/document/5461951. Luettu: 22.4.2021.

Golla, M., Ho, G., Lohmus, M., Pulluri, M. & Redmiles, E. 2021. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. Luettavissa: https://www.usenix.org/system/files/sec21-golla.pdf. Luettu: 25.9.2021.

F-Secure s.a. Tietomurto-opas: Näin reagoit ja varaudut uhkiin. Luettavissa: https://www.f-secure.com/fi/home/articles/tietomurto-opas-nain-reagoit-ja-varaudut-uhkiin. Luettu: 10.11.2021.

Hyvärinen, M., Suoninen, E. & Vuori, J. Tutkimusmenetelmien verkkokäsikirja: Laadullisen tutkimuksen verkkokäsikirja: Laadullisen tutkimuksen aineistot: Haastattelut. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/haastattelut/#Strukturoitu-puolistrukturoitu-vai-vahan-strukturoitu. Luettu: 7.9.2021.

Juhila, K. 2021. Tutkimusmenetelmien verkkokäsikirja: Laadullisen tutkimuksen verkkokäsikirja: Laadullisen tutkimuksen ominaispiirteet. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-ominaispiirteet/#Kvalitatiivisen-aineiston-suosiminen. Luettu: 17.4.2021.

Jyväskylän yliopisto 2015. Avoimet: Humanistis-yhteiskuntatieteellinen tiedekunta: Menetelmäpolkuja humanisteille: Menetelmäpolku: Tutkimusstrategiat: Määrällinen tutkimus. Luettavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/maarallinen-tutkimus. Luettu: 6.11.2021.

Järvinen, P. 2012. Arjen tietoturva: vinkit & ratkaisut. Docendo. Jyväskylä.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Docendo. Jyväskylä.

Kallio, A. 2021. Tutkimusmenetelmien verkkokäsikirja: Laadullisen tutkimuksen verkkokäsikirja: Laadullisen tutkimuksen prosessi: Litterointi. Luettavissa:

https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-prosessi/litterointi/. Luettu: 7.9.2021.

Kotimaisten kielten keskus 2020. Kielitoimiston sanakirja. Luettavissa: https://www.kielitoimistonsanakirja.fi/#/. Luettu: 16.4.2021.

Kyberturvallisuuskeskus 2020a. Kyberturvallisuuden perussanasto. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto. Luettu: 17.4.2021.

Kyberturvallisuuskeskus 2020b. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon?toggle=Huomioitavia%20ominaisuuksia&toggle=Esimerkkisovelluksia. Luettu: 12.9.2021.

Kyberturvallisuuskeskus 2020c. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla. Luettu: 11.9.2021.

Kyberturvallisuuskeskus 2020d. Pidempi parempi – Näin teet hyvän salasanan. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan. Luettu: 17.4.2021.

Kyberturvallisuuskeskus 2021a. Näin suojaudut tietomurroilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta. Luettu: 11.9.2021.

Kyberturvallisuuskeskus 2021b. Salasanat haltuun – Kuka käyttää tiliäsi? Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun. Luettu: 17.4.2021.

Kyberturvallisuuskeskus s.a. Salasanat haltuun: Neuvoja salasanojen käyttöön ja hallintaan. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf. Luettu: 16.4.2021.

Lei, Z., Nan, Y., Fratantonio, Y. & Bianchi, A. 2021. On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices. Luettavissa: https://www.ndss-symposium.org/wp-content/uploads/2021-212-paper.pdf. Luettu: 24.9.2021.

Manninen, T. 2020. Salasanahallintakäytänteet ja salasanatiivisteiden murtaminen Hashcat-ohjelmalla. AMK-opinnäytetyö. Haaga-Helia ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/360041/Salasanahallintak%C3%A4yt%C3%A4nteet-ja-salasanatiivisteiden-murtaminen-Hashcat-ohjelmalla_Topi-Manninen.pdf?sequence=2. Luettu: 18.4.2021.

McAfee s.a. Mikä on haittaohjelma? Luettavissa: https://www.mcafee.com/fi-fi/antivirus/malware.html. Luettu: 7.11.2021.

Mesiä, M., Pikkarainen, J. & Turner, B. 2021. Paras salasanan hallintaohjelma 2021: turvallisimmat ilmaiset ja maksulliset vaihtoehdot suojaukseen. Luettavissa: https://global.techradar.com/fi-fi/best/paras-salasanan-hallintaohjelma. Luettu: 12.9.2021.

Norppa, K. & Peltomäki, J. 2015. Rikos meni verkkoon: näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Talentum. Helsinki.

Poliisi s.a. Tietomurrot. Luettavissa: https://poliisi.fi/tietomurrot. Luettu: 11.9.2021.

Poliisi 2021. Poliisi varoittaa huijausyrityksistä. Luettavissa: https://poliisi.fi/-/poliisi-varoittaa-huijausyrityksista. Luettu: 11.9.2021.

Posti s.a. Muuttosuojaus ja kevyt muuttosuojaus – valitse sopivin vaihtoehto. Luettavissa: https://www.posti.fi/fi/henkiloille/kirjeet-ja-postipalvelut/jakelu-ja-muuttaminen/muuttaminen-henkiloille/muuttosuojaus. Luettu: 10.11.2021.

Rousku, K. 2014. Kyberturvaopas: Tietoturvaa kotona ja työpaikalla. Talentum. Helsinki.

Saleem, A. & Ordonez, J. 2020. Biometric authentication. Luettavissa: https://d1wqtxts1xzle7.cloudfront.net/63289512/Biometric_Ordonez_Saleem20200512-22129-1yna3jx.pdf?1589323672=&response-content-disposition=inline%3B+filename%3DBiometric_authentication.pdf&Expires=1632565296&Signature=Mrv2F7h6-CNcw-pkEGiQdO3EjSSIcJ1FFWJuVod7wP0BsN6gNAt-BOIB~bxTi02IW~BaJJ6VXfyu7m8dUf5cr5cA-aWaEtgcuz629LC2epyFI5FJW0FQ7c4xqFfwMV0kJvzU4B0qhR6CMnHCqMoZCEdya8j7b

49CV20p3rdD2pj5FbFqHD-bLHxyRbRZKjvloX8zw~fmL795rVUvG1lVJgcBvSfPeLJLWq1XwBCYdSeFiKhCk-RACCY0aKAXURXe8KBXmqQEkH38GOklBTlH8wgoC0FCtFO-jQkxpgoEqjxs5bruapyebP6shG2DTWmkA60DQeH6I2UdiACgrjq3AYNRGg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Luettu: 25.9.2021.

Siltainsuu, J. 2020. Salasanan hallintamenetelmien käyttöönoton mahdollistajat ja esteet. Pro gradu-tutkielma. Jyväskylän yliopisto, informaatioteknologian tiedekunta. Luettavissa: https://jyx.jyu.fi/bitstream/handle/123456789/70094/URN%3ANBN%3Afi%3Ajyu-202006224297.pdf?sequence=1&isAllowed=y. Luettu: 22.4.2021.

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. Luettu: 12.9.2021.

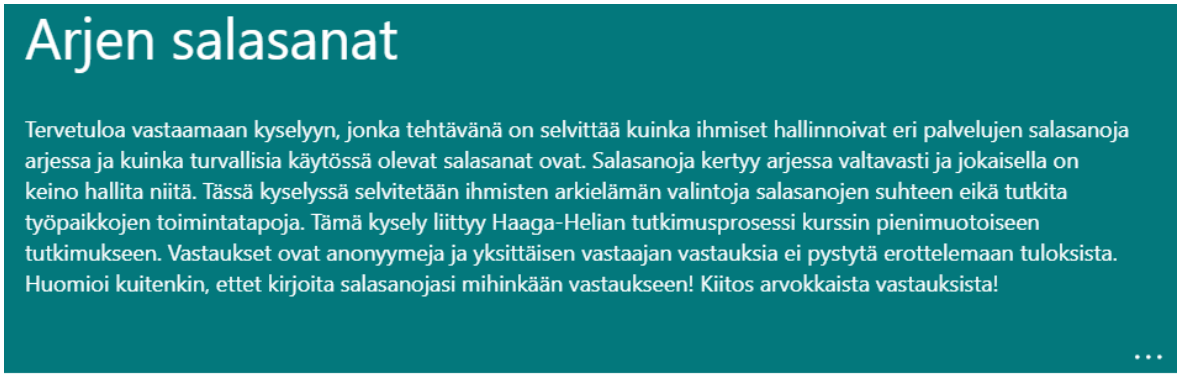
Twilio Authy s.a. What Is Two-Factor Authentication (2FA)? Luettavissa: https://authy.com/what-is-2fa/. Luettu: 12.9.2021.

Vuori, J. 2021a. Tutkimusmenetelmien verkkokäsikirja: Analyysitavan valinta ja yleiset analyysitavat: Yleiset analyysitavat. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/yleiset-analyysitavat/. Luettu: 18.4.2021.

Vuori, J. 2021b. Tutkimusmenetelmien verkkokäsikirja: Analyysitavan valinta ja yleiset analyysitavat: Laadullinen sisällönanalyysi. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/laadullinen-sisallonanalyysi/. Luettu: 18.4.2021.

Liitteet

Liite 1. Kyselylomake



* Pakollinen

1. Ikä *

- ◯ 18 - 25
- ◯ 26 - 35
- ◯ 36 - 45
- ◯ Yli 45

2. Sukupuoli *

- ◯ Nainen
- ◯ Mies
- ◯ Muu, tai en koe tarpeelliseksi kertoa

3. Löytyykö jompi kumpi tai molemmat tyypillistä salasanastasi? A) Salasanassa on lause tai lauseesta on tehty merkkijono. B) Salasana sisältää kolme asiaa seuraavista: iso kirjain, pieni kirjain, numero tai erikoismerkki. *

- ◯ Molemmat löytyy
- ◯ Toinen löytyy
- ◯ Ei löydy kumpikaan

4. Löytyykö tyypillisestä salasanastasi jokin seuraavista: syntymäaika, rekisterinumero, julkisuuden henkilö, läheisen nimi, käyttäjätunnus etuperin tai takaperin tai kyseisen palvelun nimi, johon salasana käy? *

- ◯ Kyllä, useampi kohta löytyy
- ◯ Kyllä, pari kohtaa löytyy
- ◯ Jokin yksittäinen löytyy
- ◯ Ei löydy

5. Kuinka pitkä tyypillinen salasanasi on jos saat itse valita? *

- ◯ 6 - 8 merkkiä
- ◯ 9 - 12 merkkiä
- ◯ 13 - 15 merkkiä
- ◯ Yli 15 merkkiä

6. Käytätkö samaa salasanaa useassa palvelussa? *

- ◯ Kyllä
- ◯ En. Pyrin, että eri palveluihin on eri salasanat
- ◯ Käytän samankaltaista, johon teen pienen muutoksen käyttäessäni sitä uudelleen
- ◯ Käytän kahta tai kolmea salasanaa vuoroin eri palveluissa

7. Mitkä tekijät vaikuttavat salasanavalintoihisi? Voit valita yhden tai useamman. *

- ☐ Helppous
- ☐ Muistaa ulkoa
- ☐ Turvallisuus
- ☐ Uutiset salasanavuodoista
- ☐ Muu

8. Haluatko kertoa lisää salasanaan vaikuttavista tekijöistä?

Kirjoita vastaus

9. Onko sinulla käytössä salasananhallintasovellus? (Erikseen ladattava sovellus, joka tallentaa useat salasanat yhden salasanan taakse) *

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

10. Tallennatko salasanoja selaimeesi? *

- ◯ Kyllä
- ◯ En
- ◯ En tiedä

11. Vaihdatko salasanat säännöllisesti vaikka palvelu ei vaadi sitä? *

- ◯ Pääsääntöisesti kyllä
- ◯ Vaihdan useimmin käytetyistä palveluista
- ◯ Vain silloin, kun saan ilmoituksen, että salasanani on mahdollisesti joutunut vääriin käsiin
- ◯ Pääsääntöisesti en

12. Käytätkö kaksiosaista tunnistautumista, jos se on mahdollista? *

- ◯ Kyllä
- ◯ En
- ◯ Joskus

Lähetä

Älä koskaan luovuta salasanaa kenellekään. Ilmoita väärinkäytöstä

Liite 2. Haastattelukysymykset

- Kun rekisteröidyt uuteen palveluun ja sinun tulee luoda uusi salasana, mitä ajatuksia tai tunteita sinulle nousee ensimmäiseksi mieleen?
- Kuinka usein törmäät sähköpostissa kalasteluviesteihin tai epäilyttäviin linkkeihin?
- Missä törmäät tietoon salasanojen turvallisuudesta ilman, että etsit sitä tai olet luomassa uutta salasanaa? (Esimerkiksi radio, some, tv, työpaikka jne.)
- Mitä kautta haluaisit saada tietoa hyvistä salasanakäytännöistä ja saako tietoa riittävästi ilman, että sitä varsinaisesti etsit? (Esimerkiksi radio, some, tv, työpaikka jne.)
- Kun luot uutta salasanaa, luetko ohjeet salasanan muodostamiseksi ja millaisia ne ohjeet sinusta ovat?
- Onko jokin tapahtuma tai tieto saanut sinua muuttamaan aiempaa salasanakäytäntöä? (Jos on, jatkuu kysymyksellä) Voitko kuvailla tilannetta?