Tietojenkalastus ja ikäihmiset – yli 60-vuotiaiden tietoturvatietoisuus

Emilia Asikainen

2022 Laurea

Laurea-ammattikorkeakoulu

Tietojenkalastus ja ikäihmiset – yli 60-vuotiaiden tietoturvatietoisuus

Emilia Asikainen

Tietojenkäsittelyn tradenomi

Opinnäytetyö

Helmikuu, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely

Tradenomi (AMK)

Emilia Asikainen

Tietojenkalastus ja ikäihmiset – yli 60-vuotiaiden tietoturvatietoisuus

Vuosi 2022 Sivumäärä 38

Opinnäytetyön tarkoitus oli selvittää, millä tasolla yli 60-vuotiaiden tietoturvatietoisuus on tällä hetkellä. Työ keskittyi erityisesti tietojenkalastukseen, joka on tällä hetkellä yksi suurimmista tietoturvariskeistä kotikäyttäjille.

Tutkimus tehtiin nimettömänä kyselytutkimuksena, johon osallistui 18 kohderyhmän jäsentä. Tutkimuksessa käytettiin sekä määrällisen tutkimuksen metodeita että asiantuntija-arviota. Teoriapohjana ikäihmisten digikäyttäytymiselle käytettiin Tilastokeskuksen tutkimusta, ja tietojenkalastukselle erinäistä alan kirjallisuutta.

Tutkimuksessa selvisi, että yli 60-vuotiaiden tietoturvatietoisuus tietojenkalastuksen osalta on hyvällä tasolla, ja he osaavat hyvin tunnistaa sekä huijausviestit että -puhelut, ja pystyivät luetteloimaan useita piirteitä, mistä he ne tunnistavat. Sen sijaan vastaukset heidän salasanatottumuksistaan osoittivat, että sen osalta heidän tietoturvatietoisuudessaan on vielä kehittämisen varaa, sillä suurimmalla osalla vastaajista heidän salasanatottumuksensa eivät vastanneet nykyisiä asiantuntijoiden tietoturvasuosituksia. Yli 60-vuotiaille suositeltiin lisää tietoturvakoulutusta siitä, millainen hyvän salasanan pitäisi olla, oikeista tavoista kirjata salasanat ylös, sekä kaksivaiheisen tunnistuksen tärkeydestä.

Asiasanat: tietoturva, tietojenkalastus, ikäihmiset, tietoturvatietoisuus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's Thesis

Emilia Asikainen

Phishing and the elderly – information security awareness of over 60 year olds

Year 2022 Pages 38

The aim of this Bachelor's Thesis was to examine the current state of the information security awareness of over 60 year olds. The thesis focused espicially on phishing, which is among the biggest information security threats to home users at the moment.

Quantitative methods and expert analysis were applied in this thesis. A web questionnaire was made and shared among the target group, and 18 responses were received. The theory of this thesis was based on both the studies of Statistics Finland of elderly people's internet use, and on various information security books on phishing.

The results of this thesis indicate that over 60 year olds have a good grasp on information security awareness when it comes to phishing, as they were able to both recognize scam emails and scam phone calls, and list several traits of both that can be used to recognize them. However, when it comes to passwords, their information security awareness could use some improvement, as neither their most typical passwords nor their most typical methods for writing them down meet the current information security guidelines.

It is recommended that more information security awareness training be held for people of this age group, so that they can learn, among other things, the importance of good passwords and multi-factor authentication.

Keywords: information security, information security awareness, elderly, security threat

Sisällys

1 Johdanto

Tämä on opinnäytetyö tietojenkäsittelyn tradenomin tutkintoon. Siinä on tarkoitus tutkia yli 60-vuotiaiden tietoturvatietoisuutta, keskittyen erityisesti tietojenkalastukseen. Työhön kuuluva tutkimus käsittelee myös jonkin verran kohderyhmän salasanatottumuksia, sillä se on edelleen eräs kotikäyttäjän kannalta tietoturvallisuuden tärkeimmistä aiheista. Aihe valittiin sen ajankohtaisuuden ja kiinnostavuuden takia. Tämä työ on tehty ilman toimeksiantajaa.

2 Ikäihmisten digikäyttäytymisen ja tietoturvan teoria tutkimuksen takana

Tähän osioon on kirjoitettu opinnäytetyöhön liittyvää teoriaa, jota on myös käytetty tutkimuksen teossa. Ensimmäisessä alaluvussa kerrotaan ikäihmisten digikäyttäytymisestä, koska se oli oleellinen osa tätä tutkimusta niin aihetta miettiessä kuin tutkimusta tehdessä.

Toisessa alaluvussa perehdytään tietojenkalastuksen teoriaan, joka oli luonnollisesti tämän tutkimuksen teoriapuolen tärkein osa.

2.1 Ikäihmisten digikäyttäytyminen

Yleinen stereotypia on, että ikäihmiset, varsinkin 70 ikävuodesta ylöspäin olevat sellaiset, eivät käyttäisi juurikaan internetiä tai teknologiaa muuten, eivätkä siis osaisi käyttää sitä. Tilastokeskuksen Väestön tieto- ja viestintätekniikan käyttö -tutkimus vuodelta 2020 kuitenkin osoittaa, että ikäihmiset käyttävät yhä enenevissä määrin internetiä päivittäin. Tutkimuksen mukaan 65–74-vuotiaista jopa 62 prosenttia käytti internetiä useasti päivässä, joka on 6 prosenttiyksikköä enemmän kuin edellisenä vuonna. 75–89-vuotiaista internetiä useasti päivässä käyttävien osuus oli 30 prosenttia, 7 prosenttiyksikköä enemmän kuin edellisvuonna. Tutkimus myös osoitti, että 65–74-vuotiaista 25 prosenttia ja 75–89-vuotiaista 8 prosenttia oli ostanut jotain verkkokaupasta edellisen 3 kuukauden aikana. (Tilastokeskus 2020.)

Yleisin internetiä käyttävä viestintäväline on sähköposti, jota käytti 87 prosenttia 16–89-vuotiaista. Tutkimuksen mukaan samasta ikävälistä 76 prosenttia oli myös käyttänyt älypuhelintaan pikaviestimiseen edellisen 3 kuukauden aikana. Tarkkaa lukua nimenomaan yli 65-vuotiaiden viestimisestä sähköpostilla tai pikaviestimillä ei ollut, mutta muiden lukujen valossa senkin voidaan olettaa yleistyneen, luultavasti samassa suhteessa internetin käytön kanssa. Tilastokeskuksen tutkimus paljasti, että 46 prosenttia 65–74-vuotiaista ja 16 prosenttia 75–89-vuotiasta oli seurannut yhteisöpalveluluita, kuten Facebookia tai WhatsAppia, viimeisen 3 kuukauden aikana. Kokonaisuudessaan 16–89-vuotiaista 58 prosenttia käytti Facebookia, jota moni

vanhempien ikäryhmien jäsen sanoi käyttävänsä enemmän kuin muita vastaavia palveluita. Whatsappia käytti kokonaisuudessaan 50 prosenttia vastanneista. (Tilastokeskus 2020.)

Tutkimus osoitti, että yleisin verkossa asioimisen muoto oli verkkopankin käyttäminen. Tutkimuksen mukaan 16–89-vuotiaista 87 prosenttia oli käyttänyt verkkopankkia edellisen 3 kuukauden aikana. Myös esimerkiksi julkisten palveluiden käyttäminen netin kautta oli yleistynyt, samoin muiden viranomaisten palvelujen käyttö. Jopa 50 prosenttia oli varannut ajan lääkärille netissä edellisen 3 kuukauden aikana. (Tilastokeskus 2020.)

2.2 Tietojenkalastus käytännössä

Tietojenkalastelu tarkoittaa tilannetta, jossa ihmisiä eli potentiaalisia uhreja pyritään saamaan luovuttamaan tietojaan (esim. käyttäjätunnus, salasana, pankkitiedot, henkilökohtainen informaatio) erilaisin huijauskonstein. Näistä yleisimpiä ovat huijaussoitot ja -viestit, joita varsinkin näin pandemia-aikana on ilmennyt enenevissä määrin. Niistä puhutaan tässä opinnäytetyössä omissa alaluvuissaan, jotka löytyvät alempaa.

Tietojenkalastuksessa uhreilta kerättyjä tietoja, etenkin tunnistautumistietoja ja henkilökohtaista informaatiota, on usein tarkoituksena käyttää identiteettivarkauksissa, eli toiseksi henkilöksi tekeytymisessä. Tekijät voivat saadusta tiedosta riippuen ottaa haltuunsa sosiaalisen median tilejä, tehdä verkkokauppa ostoksia, tai siirtää rahaa uhrin pankkitililtä. Tietoja voidaan myös käyttää erityiseen tietojenkalastuksen muotoon, josta käytetään englanniksi termiä *spear phishing* eli suomeksi keihäskalastelu. Siinä kalastelijat tekeytyvät jonkin organisaation sijaan joksikin tietyksi henkilöksi, jonka uhri tuntee ja johon hän luottaa. Kalastelijat voisivat esimerkiksi tekeytyä halutun uhrin alaiseksi tai esihenkilöksi, mahdollisesti tämän varastetuilla tunnuksilla, ja pyytää tätä kiireellisesti kirjautumaan jollekin sivulle tai kertomaan jotain tietoa. (Dulaney & Easttom 2017.)

2.2.1 Huijauspuhelut

Huijauspuhelut ovat tietojenkalastuksen metodeista, jossa tekijät soittavat kohteilleen ja tekeytyvät joksikin toiseksi henkilöksi, esimerkiksi IT tuen edustajaksi, saadakseen kohteensa luovuttamaan tietojaan. Näitä tietoja voivat olla esimerkiksi kohteen käyttäjätunnus, salasana, tai pankkitunnukset. Suomessa soitot voivat tulla joko suomalaisista tai ulkomaisista suuntanumeroista, mutta usein niihin vastatessa soittajat puhuvat englantia. Jo pari vuotta liikkeellä ollut Microsoft-huijaus, jossa soittaja väittää olevansa Microsoftin IT-tuesta ja vastaajan tietokoneen tietoturvan olevan uhattuna, ja pyytää lataamaan jonkin ”etähallintaohjelman” ja antamaan soittajalle pääsyn koneelle, on esimerkki huijauspuhelusta.

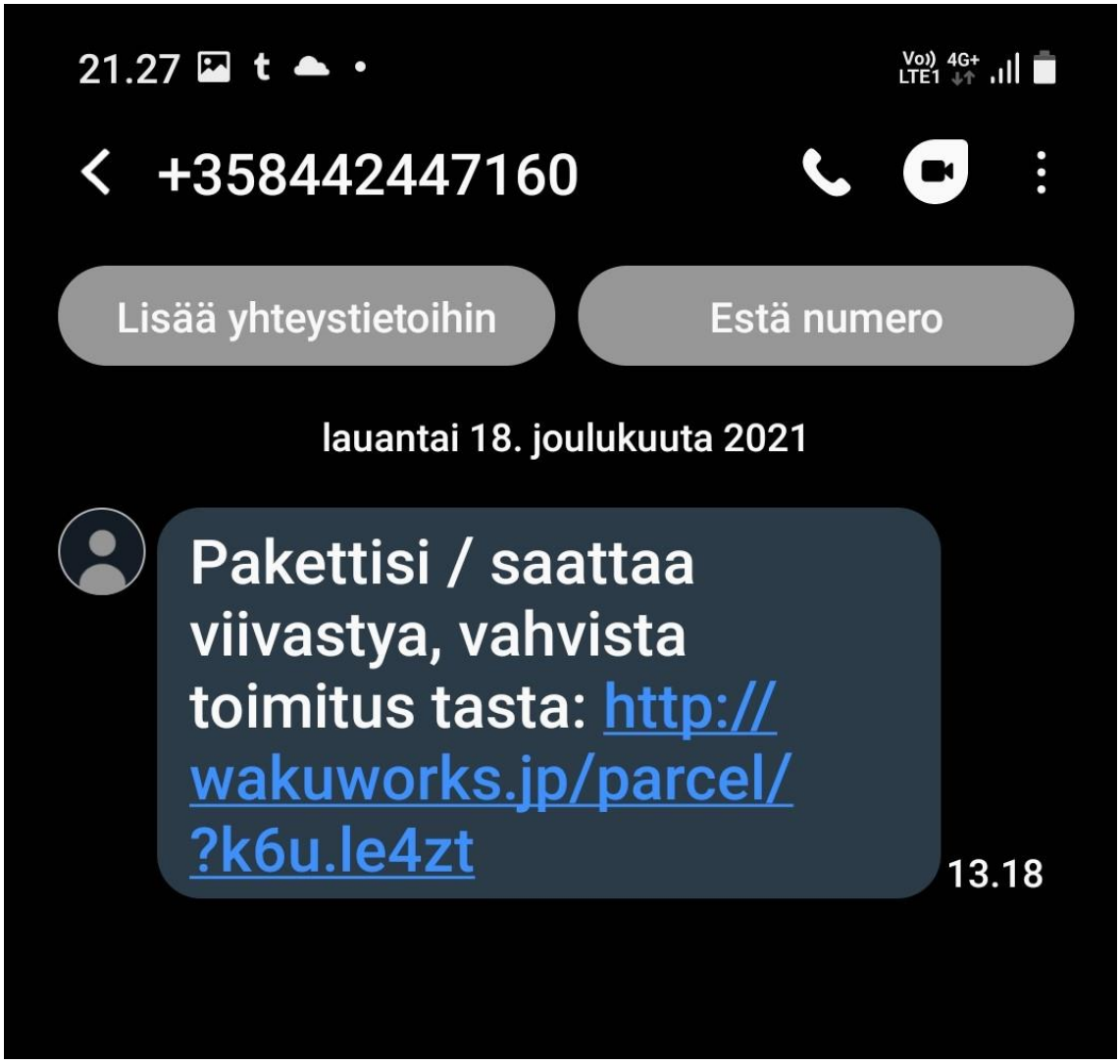
Suomen poliisin verkkosivulla olevassa uutisessa kerrotaan, että ainakin Kaakkois-Suomessa olisi tullut ilmoituksia puheluista, jossa suomea puhuva soittaja väittää olevansa poliisista, ja

pyytää vastaajan pankkitietoja. Tässäkin on kyse huijauspuhelusta, ja Poliisi muistuttaakin uutisessa, että viranomaiset eivät koskaan pyydä puhelimitse pankkitietoja tai käyttäjätunnuksia. (Poliisi, 2021.)

2.2.2 Huijausviestit

Huijausviestit ovat yksi tietojenkalastuksen metodeista, jossa tekijät lähettävät kohteilleen viestejä – usein tekstiviestillä tai sähköpostilla, mutta myös muissa viestipalveluissa – esittävänsä olevansa jostakin luotetusta organisaatiosta, kuten pankista, postista, poliisista, tai vaikkapa striimipalvelusta. Viestissä pyydetään käyttäjältä kiireellisiä toimia, esimerkiksi kirjautumaan palveluun, vaihtamaan salasanan, tai maksamaan jotain. Viestissä on linkki, jonka annetaan ymmärtää vievän organisaation tai palvelun sivulle. Todellisuudessa linkki vie valesivulle, joka usein on hyvinkin aidon näköinen kopio oikeasta sivusta. Valesivun erottaakin parhaiten kopiosta URL-osoitteen kautta, joka ei vastaa aitoa sivua. Mikäli uhri yrittää kirjautua sen kautta sisään organisaatioon tai palveluun, tekijät saavat tämän tunnistautumistiedot itselleen. Joissain tapauksissa valesivu saattaa tämän jälkeen ohjata uhrin aidolle sivustolle, jotta tämä ei huomaisi virhettään. (Hadnagy, Fincher & Dreeke, 2015.)

Viime aikoina, erityisesti nyt pandemia-aikana, on liikkunut paljon postipaketteihin liittyviä huijausviestejä. Näissä lähettäjät esittävänsä olevansa Postista tai muusta pakettipalvelusta, ja kertovat, että viestin saajan tulee tehdä jotain toimia, kuten klikata linkkiä tai maksaa postimaksu, saadakseen hänelle lähetetyn paketin. Viesti ei kuitenkaan tule Postin numerosta, vaan usein kyseessä on jokin tavallinen puhelinnumero, kuten Kuviossa 1.



Kuvio 1: Esimerkki huijausviestistä

Kuviossa 1 on kuvakaappaus yhdestä oikeasta pakettihuijausviestistä, joka on saatu viime joulukuussa. Kuten kuvasta näkyy, viestissä on kirjoitusvirheitä ja ääkköset puuttuvat, mikä on yleistä monissa huijausviesteissä. Tässä tapauksessa viestin linkki selvästi ei vie Postin sivulle, vaan jollekin japanilaisen domainin omaavalle sivulle. Viesti on tullut tavallisesta +358-alkuisesta numerosta. Kyseessä on siis melko tyypillinen huijausviesti.

3 Tutkimuksen lähtökohdat ja tavoitteet

Viime vuosina erilaisia huijausviestejä on ollut liikkeellä paljon, erityisesti nyt koronapandemian aikana, kun yhä enemmän ihmisiä on joutunut hoitamaan asioitaan etänä. Esimerkiksi posti- ja Microsoft-huijausyrityksiä on tullut monille. Usein niiden kohteena – tai ainakin yleisimpänä uhrina – vaikuttaisivat olevan vanhemmat ihmiset, joiden ajatellaan olevan

vähemmän tietoisia mahdollisista uhista. Tällaiset tapaukset ovatkin usein uutisotsikoissa. Tästä syntyi ajatus tutkimuksesta, joka pyrkisi selvittämään, millä tasolla on vanhempien ihmisten – tässä tutkimuksessa yli 60-vuotiaiden – yleinen tietoturvatietoisuus, tunnistavatko he erilaisia huijauksia, sekä sen, millaisia heidän kokemuksensa tietojenkalastelusta ja erilaisista huijauksista ovat. Tämän perusteella olisi sitten mahdollista tulevaisuudessa lähteä kehittämään tietoturvaohjeistusta, mikäli tarvetta sille ilmenee. Aihe on kiinnostava, sillä omassa lähisuvussani on paljon kohderyhmään kuuluvia, ja heille on lähetetty viimeisen vuoden aikana useita erilaisia huijausyrityksiä.

3.1 Tutkimuskohteen kuvaus ja tutkimusongelma

Opinnäytetyön muoto on tutkimustyö. Tutkimuksen kohteena ovat 60 vuotta täyttäneet ja sitä vanhemmat ihmiset, joita tässä tutkimuksessa kutsutaan myös nimellä ”ikäihmiset”. Tarkoituksena on selvittää, millä tasolla heidän tietämyksensä tietoturvasta on tällä hetkellä, keskittyen erityisesti tietojenkalastukseen sen ajankohtaisuuden vuoksi. Tutkimus on mielestäni tärkeää toteuttaa, sillä vaikka ikäihmisten yleisesti ajatellaan olevan vähemmän perehtyneitä digitaalisten laitteiden käyttöön ja internetin maailmaan, ja siten myös tietoturvaan, siitä ei näyttäisi olevan juurikaan tutkimuksia, ainakaan suomenkielisiä tai uusia sellaisia. Tutkimuksen tarkoituksena on arvioida ikäihmisten tietoturvatietämyksen nykytilaa, jotta heille tähdättyä tietoturvakoulutusta voitaisiin tulevaisuudessa mahdollisuudessa parantaa. Esimerkiksi ikäihmisille erilaisia palveluita ja ohjeistusta tuottavat tahot – mukaan lukien kunnat – voisivat hyötyä tutkimuksesta kehittäessään uusia tapoja opettaa ikäihmisille parempaa tietoturvakäyttäytymistä.

3.2 Tutkimuskysymykset

Tässä tutkimuksessa haluttiin tutkia, millä tasolla yli 60-vuotiaiden tietoturvatietoisuus on. Käytännössä tutkimuksessa kysyttiin, kuinka paljon huijauspuheluita ja -viestejä yli 60-vuotiaat (ikäihmiset) saavat, osaavatko he tunnistaa niitä, ja miten he reagoivat niihin. Samalla haluttiin selvittää, ovatko kohderyhmään kuuluvat koskaan joutuneet tietojenkalastushuijauksen uhriksi, ja jos ovat, mistä he sen huomasivat.

Lisäksi tutkimuksessa kysyttiin, millaisia salasanoihin ja kirjautumiseen liittyviä tietoturvatottumuksia yli 60-vuotiailla on. Aiheesta kysyttiin, koska yleinen stereotypia on, etteivät ikäihmisten salasanat ole usein kovinkaan vahvoja tai niiden merkitsemistavat kovinkaan tietoturvallisia. Tutkimuksessa haluttiin selvittää, pitääkö stereotypia paikkansa.

3.3 Aihealueen rajaus

Tässä työssä kohderyhmänä ja tutkimuksen kohteena ovat ainoastaan yli 60-vuotiaat, eikä sitä nuorempien tietoturvatietoisuus kuulu tähän tutkimukseen. Tässä tutkimuksessa ei myöskään

lähdetä tutkimaan, mitkä ovat tämänhetkiset suurimmat tietoturvauhat, vaan niiden suhteen tutkimus luottaa virallisten tahojen lähteisiin sekä muihin tutkimuksiin. Tässä työssä ei myöskään oteta kantaa siihen, ovatko tietojenkalastushuijaukset yleistyneet viime aikoina.

Aiheen laajuuden vuoksi tutkimus keskittyy pääasiassa nimenomaan tietojenkalastukseen, minkä lisäksi tutkitaan jonkin verran myös kohderyhmän tietoturvatottumuksia liittyen salasanoihin. Tämä rajaus on tehty siitä syystä, että tutkimuksessa haluttiin keskittyä nimenomaan käyttäjäkeskeisiin tietoturva-asioihin, joihin kohderyhmäläinen pystyy vaikuttamaan, ja jotka ovat ajankohtaisia juuri nyt.

3.4 Keskeiset käsitteet

Tietojenkalastus	Toimintaa, jossa ihmisiä eli potentiaalisia uhreja pyritään saamaan luovuttamaan tietojaan (esim. käyttäjätunnus, salasana, pankkitiedot, henkilökohtainen informaatio) erilaisin huijauskonstein. Yleisiä keinoja ovat esimerkiksi huijausviestit, huijauspuhelut, ja valeverkkosivut.
Huijausviestit	Yksi tietojenkalastuksen metodeista, jossa tekijät lähettävät kohteille viestejä, joissa esittävät olevansa joku muu, ja pyydetään klikkaamaan linkkiä ja kirjautumaan johonkin tai maksamaan tai lataamaan jotakin. Monesti viestien esitetään tulevan viralliselta taholta, esimerkiksi pankista, postista, poliisilta, tai jostain yleisestä palvelusta, kuten Netflixistä.
Huijauspuhelut	Yksi tietojenkalastuksen metodeista, jossa tekijät soittavat kohteilleen ja tekeytyvät joksikin toiseksi henkilöksi, esimerkiksi IT tuen edustajaksi, saadakseen kohteensa luovuttamaan tietojaan, kuten käyttäjätunnuksensa tai salasanansa.
Tietoturvatietoisuus	Ymmärrys siitä, mitä tietoturva on, ja miten itseään ja tietojaan voi suojata.
Identiteettivarkaus	Tapaus, jossa joku esiintyy toisena henkilönä käyttäen hänen henkilötietojaan, tunnistautumistietoja, pankkitunnuksia, tai muita tietoja, jolla henkilö yleensä tunnistetaan. Esimerkiksi sosiaalisessa mediassa toiseksi henkilöksi tekeytyminen tai toisen nimellä ja tunnuksilla tehty verkkokauppatilaus ovat identiteettivarkauksia.

Kaksivaiheinen tunnistautuminen	Tietojen suojauskeino, jossa kirjautumiseen vaaditaan kaksi eri tunnistautumismenetelmää. Yleinen esimerkki on kirjautumistietojen ja sähköpostilinkin tai tekstiviestillä lähetetyn koodin yhdistelmä. Joissakin tapauksissa tunnistautumisvaiheita on enemmän kuin kaksi.

4 Tutkimusmenetelmät

Tämä opinnäytetyö on toteutettu kyselytutkimuksena, ja käyttää siis määrällisen tutkimuksen menetelmiä. Se valittiin, koska kyselytutkimus sopii hyvin henkilöiden yksityiselämän seikkojen tutkimiseen, mihin tietoturvatietoisuus kuuluu. Lisäksi verkkokysely sopi hyvin tällaiseen tutkimukseen, jossa tutkitaan tietoturvatottumuksia, ja pyritään pitämään vastaukset mahdollisimman nimettöminä. Lisäksi tutkimus käyttää asiantuntija-arviota kyselyn vastausten kokoamiseen ja johtopäätösten tekemiseen.

4.1 Kyselytutkimuksen tekeminen

Kyselytutkimuksen tekemisessä tärkeintä on miettiä kysymykset niin, että niihin annetut vastaukset vastaavat tutkimuskysymyksiin ja antavat tarvittavaa tietoa tutkimuksen tekemiseen. Niiden on myös oltava tarpeeksi yksiselitteisiä, että käyttäjä ei voi ymmärtää niitä väärin ja vastata siis eri kysymykseen kuin kyselyn laatijalla oli tarkoitus. On myös päätettävä kyselyn pituus: tehdäkö lyhyt kysely, johon saa luultavasti enemmän vastauksia, vai pidempi kysely, jossa on pienempi vastausprosentti, mutta enemmän tietoa per vastaaja.

Myös kysymys- ja vastaustyyppien valinta on tärkeää, sillä erilaisiin tutkimuksiin ja tutkimusmetodeihin sopivat eri vastaustyypit. Esimerkiksi tämän opinnäytetyön kyselyssä enimmäkseen käytetyt monivalintakysymykset sopivat paremmin määrälliseen tutkimukseen, jossa tarvitaan tarkempia lukuja, kun taas laadulliseen tutkimukseen sopivat vapaat tekstikentät, johon vastaajat voivat kirjoittaa vastauksensa. Kummassakin kuitenkin kysymysten tulee olla tarkkoja ja selkeitä. (Hiltunen.)

4.2 Validiteetti ja reliabiliteetti

Validiteetti, joka tulee englannin kielen sanasta ”validity”, kertoo, miten hyvin tutkimus- tai mittausmenetelmä mittaa tutkittavaa asiaa tai ominaisuutta. Käytännössä siis validiteetilla katsotaan, onko tutkimuksessa mitattu oikeaa asiaa ja kysytty oikeita kysymyksiä, eikä

vahingossa tutkittu aivan muuta kuin mitä oli tarkoitus. Jos tutkimuksella ei ole validiteettia, eli siinä on tutkittu vääriä asioita, ei se ole pätevä. (Tilastokeskus.)

Reliabiliteetti, joka tulee englannin kielen sanasta ”reliability”, taas kertoo tutkimuksen luotettavuudesta, eli siitä, miten hyvin sen tuloksiin voi luottaa. Sitä käytetään erityisesti määrällisessä tutkimuksessa, mutta se on tärkeä myös muunlaisissa tutkimuksissa. Yksi reliabiliteetin tärkeimmistä merkeistä on se, että tutkimuksen tulokset on mahdollista toistaa uudella mittauksella. (Heinonen.)

5 Tutkimuksen toteutus

Tässä luvussa kerrotaan itse opinnäytetyötä varten tehdystä tutkimuksesta. Kuten aiemmin on jo kerrottu, kyseessä oli kyselytutkimus, jota laatiessa jouduttiin miettimään luvussa 4.1 kerrottuja asioita, kuten kysymysten ja vastausten tyyppiä, kysymysten selkeyttä, ja sitä, kuinka hyvin saadut vastaukset vastaisivat opinnäytetyölle asetettuihin tutkimuskysymyksiin. Koska kohderyhmänä olivat yli 60-vuotiaat, ja kyseessä oli tietoturvaan liittyvä tutkimus, kysymysten selkeyden tärkeys ja kohderyhmän tietotason huomioon ottaminen oli erityisen tärkeää. Siksi kysymysten miettimiseen käytettiin paljon aikaa jo ennen kuin itse kyselyä lähdettiin laatimaan, ja lopullinen kysely testattiin lähes kohderyhmän ikäisellä vapaaehtoisella ennen kyselyn laittamista jakoon. Tämä testaus osoittautui hyväksi ideaksi, koska annettu palaute auttoi selventämään muutamaa kysymystä selityksen lisäämällä. Kyseiset kysymykset olisivat muuten voineet aiheuttaa ongelmia tai virheitä tuloksiin kyselyyn vastaajien mahdollisten väärinymmärrysten vuoksi.

5.1 Kysely kohderyhmille

Kysely toteutettiin Google Forms-palvelulla, joka on Googlen ilmainen kyselynluomispalvelu, ja Laurea-ammattikorkeakoulussa melko runsaassa käytössä. Se valittiin työkaluksi kyselyn toteuttamiseen, koska se oli ilmaisista vaihtoehdoista tunnetuin ja siksi kohderyhmälle luotettavin vaihtoehto. Jos kyselyn luomiseen olisi käytetty jotain kohderyhmälle täysin tuntematonta työkalua tai palvelua, olisivat jäsenet voineet epäröidä vastata siihen. Tämä otettiin huomioon palvelua valittaessa. Päätökseen auttoi myös se, että Google Forms on helppokäyttöinen työkalu sitä ensimmäistä kertaa käyttävälle, ja se luo valmiiksi diagrammit osasta vastauksista, mikä helpottaa kyselyn tekijän työtä analyysivaiheessa. Lisäksi siinä on vaihtoehto, jossa käyttäjän tietoja tai sähköpostiosoitetta ei julkaista kyselyn laatijalle, mikä teki siitä optimaalisen tässä nimenomaisessa tutkimuksessa käyttämiseen.

Kyselyssä kysyttiin 15 kysymystä, jotka jaettiin kahteen osaan: Yleistä tietoturvasta-osassa kysyttiin salasanatottumuksiin liittyviä kysymyksiä, ja Huijausviestit ja -puhelut-osassa keskityttiin nimensä mukaisesti erityisesti tietojenkalastukseen huijausviestien ja puheluiden avulla.

Ensimmäisessä osassa oli 4 kysymystä, ja loput 11 olivat toisessa osassa. Toisen osan 11 kysymyksestä kolme oli tehtäviä, joissa piti erottaa, oliko kuvassa oleva viesti aito vai huijaus. Tällä tutkittiin, kuinka hyvin kohderyhmä osaa erottaa huijausviestejä aidoista.

Linkkiä kyselyyn jaettiin tutkimuksen tekijän lähipiirille, jotka jakoivat sitä eteenpäin tuntemilleen yli 60-vuotiaille henkilöille. Läheisten joukossa olevat kohderyhmään kuuluvat myös itse täyttivät kyselyn. Lopputuloksena oli se, että tutkimuksen tekijäkään ei ole varma, ketkä kaikki kyselyyn vastasivat. Kuten luvussa 7 kerrotaan tarkemmin, tämä on hyvä asia. Kaiken kaikkiaan kyselyyn vastasi 18 ihmistä, ja näistä kaikki olivat vakavasti otettavia vastauksia, eli kaikeksi onneksi niin kutsuttuja ”trollivastauksia” ei ollut. Tämä johtunee siitä, että kohderyhmään kuuluvat olivat nimenomaan yli 60-vuotiaita, joiden voisi olettaa ottavan kyselyt yleensäkin vakavammin, sekä erityisesti siitä, että kyselyyn vastaajat joko tunsivat kyselyn laatijan henkilökohtaisesti, tai tunsivat jonkun, joka tuntee laatijan. He eivät tästä syystä välttämättä halunneet antaa huonoja vastauksia.

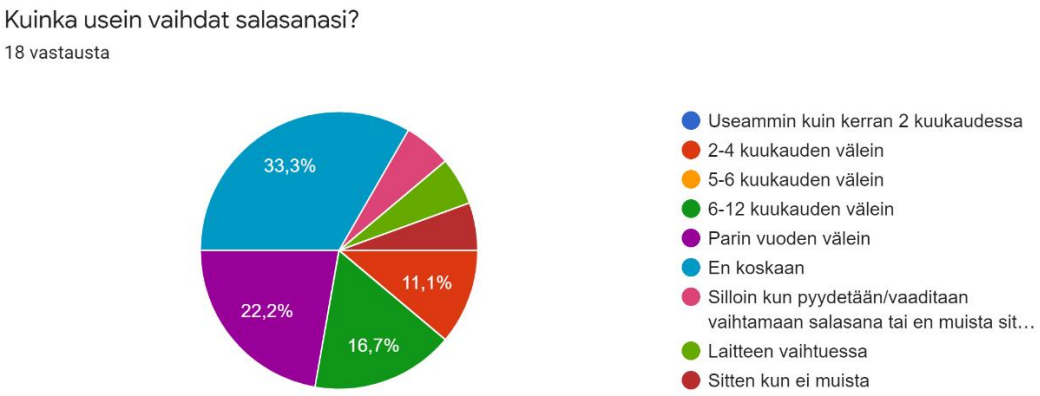
5.2 Vastaukset kyselyyn

Kuten edellisessä luvussa kerrottiin, kyselyyn vastasi kaiken kaikkiaan 18 ihmistä, mikä on tämän kokoisessa opinnäytetyötutkimuksessa melko hyvä tulos, ja riittävä antamaan kuvaa kohderyhmän tietoturvatietoisuuden nykytilasta tietojenkalastuksen ja salasanojen osalta.

Selvyyden vuoksi kohderyhmän vastaukset on jaettu kahteen alalukuun; ensimmäinen käsittelee salasanoihin liittyviä kysymyksiä ja vastauksia, ja toinen tietojenkalastusta. Näin on tehty siitä syystä, että itse kyselyn kysymyksetkin oli jaettu kahteen osaan, jotka oli jaettu samalla periaatteella. Monien kysymysten vastauksista on myös tehty diagrammeja, ja niiden kaikkien laittaminen yhteen lukuun tekisi siitä turhan pitkän.

5.2.1 Vastaukset salasanoista

Luvussa 6.1 kerrottiin, kyselyn ensimmäisessä osassa oli neljä salasanoihin ja tunnistautumiseen liittyvää kysymystä. Niistä kaikki olivat monivalintakysymyksiä, joiden vastauksista on tehty ympyrädiagrammit. Nämä diagrammit on lisätty tähän opinnäytetyöhön kuvioina yksi kerrallaan, minkä jälkeen vastauksia on avattu enemmän tekstissä.



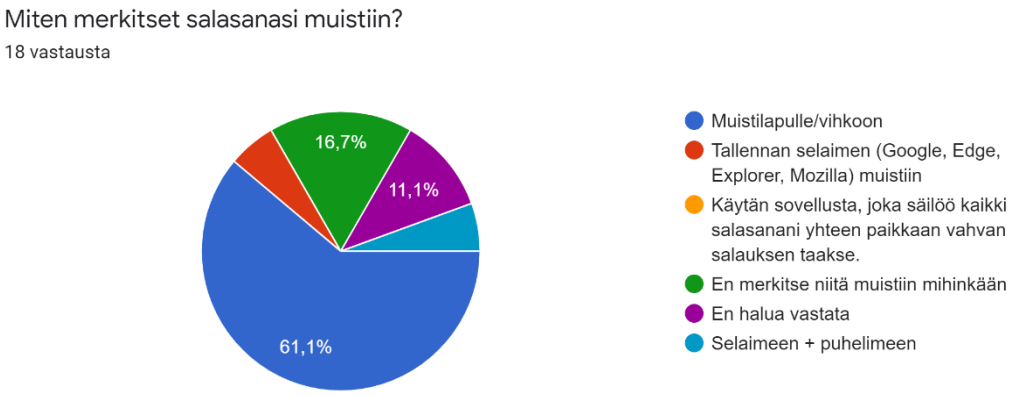
Kuvio 2: Salasanojen vaihtotiheys

Kuviosta 2 näkyy, että kyselyn ensimmäinen kysymys oli ”kuinka usein vaihdat salasanasi”. Muutama vastausvaihtoehto nousi selvästi yli muiden: 33,3% vastasi ”en koskaan”, 22,2% vastasi ”parin vuoden välein”, ja 16,7% vastasi ”6-12 kuukauden välein”. Vain 11,1% vastasi ”2-4 kuukauden välein”, mikä on yleinen tietoturva-asiantuntijoiden suosittelema salasanojen vaihtoväli. Kaksi kohderyhmäläistä kertoi vaihtavansa salasanan silloin kun ei enää muista sitä, ja toinen heistä lisäsi, että vaihtaa myös silloin, kun salasanaa vaaditaan vaihtamaan. Eräs toinen taas kertoi vaihtavansa salasanojaan silloin, kun hänen laitteensa vaihtuu.

Kuvio 3: Tyypilliset salasanat

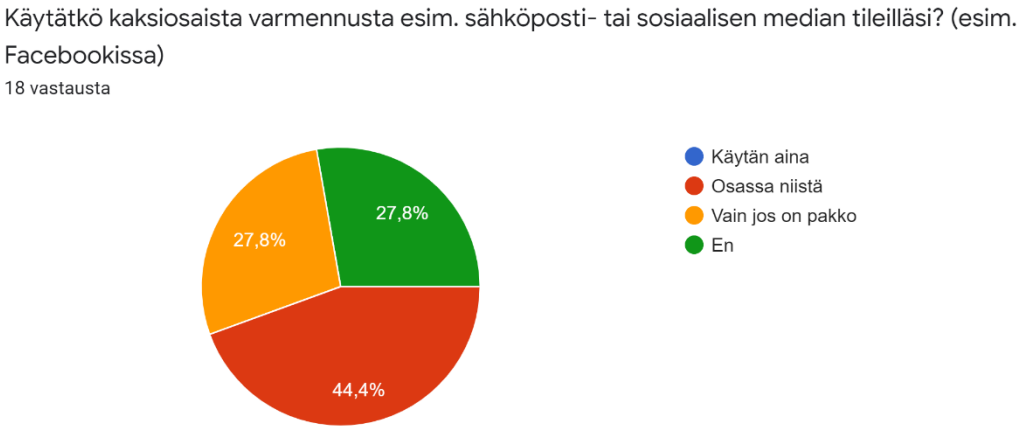
Kuviossa 3 näkyy, että toinen kyselyn kysymys oli ”Mikä näistä vaihtoehdoista muistuttaa eniten tyypillisiä salasanojasi?”. Vastausvaihtoehdoiksi oli annettu erilaisia salasana tyyppejä eri tietoturvatasoilta, joista huonoin oli ”salasana123” ja paras rivi sekalaisia numeroita ja kirjaimia. Vaihtoehtona oli myös valita ”En halua vastata”, minkä 16,6% vastaajista oli valinnutkin. Selvästi eniten vastaajista valitsi kuitenkin vaihtoehdon ”MaijaMehiläinen62” kaikkein eniten

heidän tyypillisiä salasanojansa muistuttavaksi, mikä ei ehkä kohderyhmän huomioon ottaen tullut yllätyksenä. 27,8% taas vastasi ”Matkailija54”, eli melko samanlaisen vaihtoehdon. Vain yksi vastaaja valitsi vaihtoehdon ”M4tk41l1j4”, joka oli vaihtoehtosalasanoista toisiksi tietoturvallisin. Kaikkein tietoturvallisinta vaihtoehtoa, satunnaisten kirjainten ja numeroiden sarjaa, ei valinnut kukaan.



Kuvio 4: Salasanojen muistiin merkitseminen

Kuviosta 4 näkyy, että kyselyn kolmas kysymys oli ”Miten merkitset salasanasi muistiin”. Tässä kysymyksessä vastausten trendi oli hyvin selvä: 61,1%, eli peräti 11 vastaajista, kertoi merkitsevänsä salasanansa muistilapulle tai vihkoon. Yksi vastasi tallentavansa salasanat selaimensa muistiin, yksi vastasi tallentavansa salasanat sekä selaimeensa että puhelimeensa, ja 16,7% eli 3 vastaajaa kertoi, ettei merkitse salasanojaan muistiin mihinkään. 11,1% eli 2 vastaajista valitsi vaihtoehdon ”en halua vastata”.

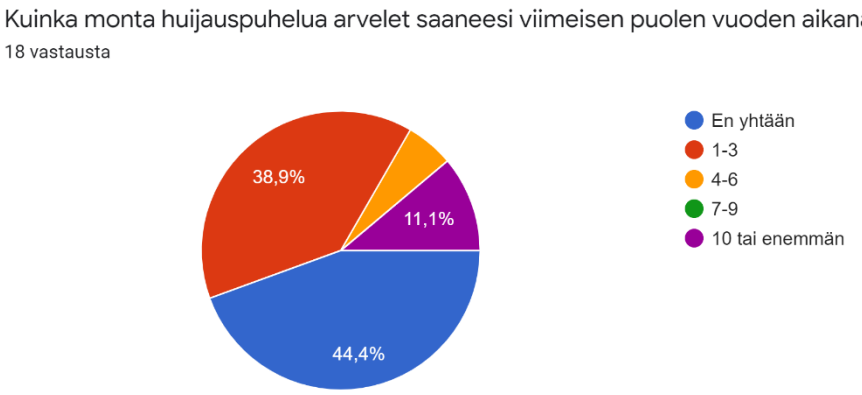


Kuvio 5: Kaksiosaisen varmennuksen käyttö

Kuten yllä olevasta Kuviosta 5 näkyy, että neljäs ja viimeinen tämän osan kysymys oli ”Käytätkö kaksiosaista varmennusta esim. sähköposti- tai sosiaalisen median tileilläsi? (esim. Facebookissa)”. Tässä kohderyhmän vastaukset jakautuivat kolmeen kategoriaan: yleisin vastaus, jonka valitsi 44,4% eli 8 vastaajista, oli ”osassa niistä”. Sen sijaan sekä ”vain jos on pakko” että ”en käytä” olivat 27,8% eli 5 vastaajan valinnat. Tämä tarkoittaa sitä, että yli puolet kohderyhmän vastaajista joko ei käytä kaksiosaista varmennusta, tai ei käyttäisi sitä, ellei olisi pakko. Vastausvaihtoehtona ollut ”käytän aina” ei saanut yhtään valintaa.

5.2.2 Vastaukset tietojenkalastelusta

Kyselyn toinen osa koostui kysymyksistä liittyen tietojenkalastukseen, tarkemmin ottaen huijausviesteihin ja -puheluihin. Tässä osassa oli 11 kysymystä, josta 9 oli monivalintakysymyksiä, ja kahdessa pyydettiin vastaamaan tekstikenttään. Kuten edellisessäkin luvussa, monivalintavastauksista on tehty diagrammit, jotka on lisätty tähän lukuun. Jokaisen jälkeen vastauksia on avattu lisää tekstimuodossa. Avoimien kysymysten vastaukset on tiivistetty muutamaan yleisimpään vaihtoehtoon, ja kerrottu jäljempänä.



Kuvio 6: Huijauspuhelut puolen vuoden aikana

Kuviossa 6 näkyy, että tämän kyselyn osan ensimmäinen kysymys oli ”Kuinka monta huijauspuhelua arvelet saaneesi viimeisen puolen vuoden aikana”. On ehkä jokseenkin yllättävää, että jopa 44,4% vastaajista kertoo, ettei ole saanut yhtään huijauspuhelua kysyttynä ajanjaksona. 38,9% vastaajista kuitenkin kertoo saaneensa 1-3 huijauspuhelua, kun taas yksi vastaaja arvelee saaneensa niitä 4-6. Kaksi vastaajaa kertoo saaneensa jopa 10 tai enemmän huijauspuhelua viimeisen puolen vuoden aikana, mikä on jo merkittävä määrä.

Kuvio 7: Huijausviestit puolen vuoden aikana

Kuvio 7 kertoo, että tämän osion toinen kysymys oli ”Kuinka monta huijausviestiä (tekstiviesti tai sähköposti) arvelet saaneesi viimeisen puolen vuoden aikana”. Tässä kysymyksessä oli enemmän hajontaa kuin edellisessä: 38,9% eli 7 vastaajista kertoi saaneensa 1-3 viestiä kysyttynä aikavälinä, kun taas 27,8% eli 5 arveli saaneensa 4-6. Jopa 22,2% eli 4 vastaajista kertoi saaneensa huijausviestejä 10 tai enemmän. Vain kaksi vastaajaa vastasi, ettei ollut saanut huijausviestejä lainkaan.

Kuvio 8: Huijausviestin tunnistus

Kuten Kuviossa 8 näkyy, osion kolmannessa kysymyksessä kysyttiin ”Onko alla olevassa kuvassa näkyvä Postin sähköpostiviesti aito vai huijaus”. Kaikki vastaajat olivat hyvin yksimielisiä: kaikki vastasivat viestin olevan huijaus, mikä oli oikea vastaus. Alla olevassa Kuviossa 9 on kysymyksessä ollut kuva.

Kuvio 9: Kyselyssä ollut huijausviesti

Kuvio 10: Aidon viestin tunnistus

Kuten Kuviossa 10 näkyy, osion neljäs kysymys oli niin ikään ”Onko tässä kuvassa näkyvä Postin viesti aito vai huijaus”. Tässä tapauksessa viesti oli aito, minkä 94,4% vastaajista tunnisti. Vain yksi vastaajista sanoi viestin olevan huijaus.

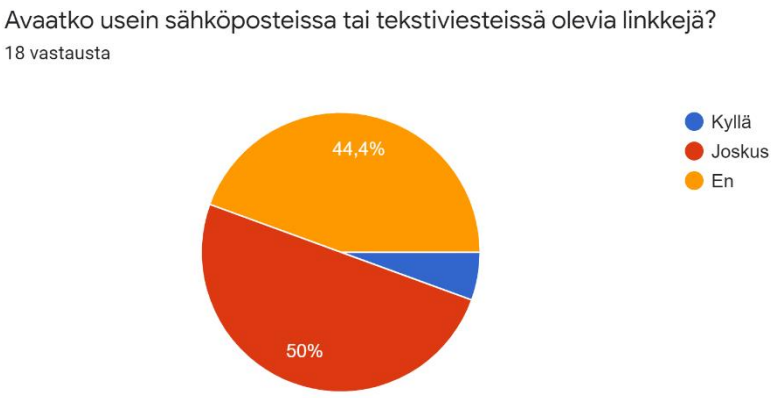
Kuvio 11: Huijausviestin tunnistamisprosentti

Kuten Kuviossa 11 näkyy, seuraava kysymys oli niin ikään viestin tunnistustehtävä, tällä kertaa tekstiviestistä. Jälleen kohderyhmän vastaajat olivat hyvin yksimielisiä: kaikki vastasivat viestin olevan huijaus, mikä oli oikea vastaus. Kysymyksessä ollut kuvakaappaus huijausviestistä on tässä opinnäytetyössä jo luvussa 3.2.2 esimerkkinä ollut Kuvio 1.

Seuraava kyselyn kysymys oli ”Mistä yleensä tunnistat huijausviestin tai puhelun?”, ja siihen oli annettu tekstikenttä, johon kyselyyn osallistujat saivat kirjoittaa vastauksensa omin sanoin. Kysymykseen tuli monenlaisia vastauksia, mutta osallistujien vastauksissa toistui useita piirteitä, mistä he tunnistavat huijausviestin tai puhelun. Tässä on lista niistä:

- Outo sähköpostiosoite tai numero
- Kirjoitusvirheet ja huono suomen kieli
- Puhelu tulee toisen maan suuntanumerosta
- Soittaja puhuu englantia, vaikka numero on suomalainen
- Pyydetään maksua tai pankkitunnuksia
- Kiire toimia
- Outo linkki, joka pyydetään avaamaan

Muutamat vastaajat viittasivat Microsoftin huijauksiin erikseen vastauksissaan, mistä voisi päätellä, että heillä saattoi olla niistä omakohtaista kokemusta, tai he ovat kuulleet niistä mediassa.

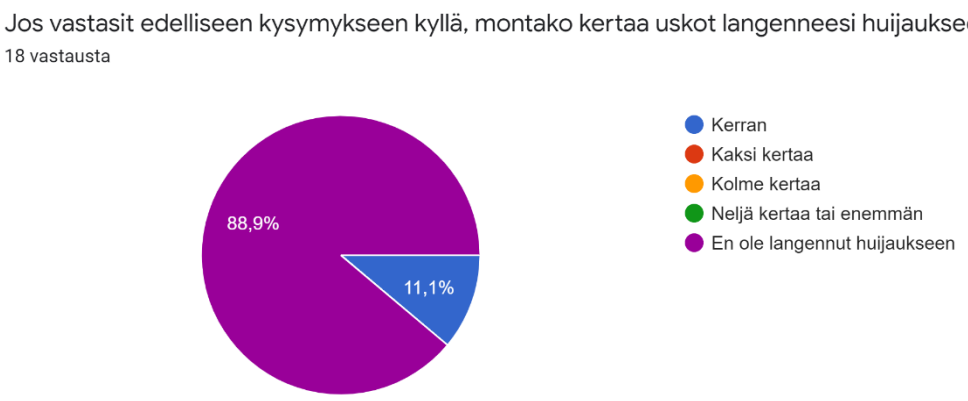


Kuvio 12: Puolet avaa joskus linkkejä

Kuten Kuviossa 12 näkyy, seuraava kysymys oli ”Avaatko usein sähköposteissa tai tekstiviesteissä olevia linkkejä”. Tämän kysymyksen vastaukset jakautuivat melko tasan: 50% sanoi avaavansa linkkejä joskus, 44,4% vastasi, ettei avaa linkkejä. Vain yksi vastaaja sanoi avaavansa usein linkkejä saamissaan sähköposteissa ja tekstiviesteissä.

Kuvio 13: Harva on tullut tietojenkalastuksen uhriksi

Kuten Kuviosta 13 näkyy, seuraava kysymys oli ”Uskotko tulleesi koskaan tietojenkalastuksen uhriksi”. Koska termi ei välttämättä ollut kohderyhmälle tuttu, kysymyksessä kerrottiin myös, mitä sillä tarkoitetaan. Tähän kysymykseen 66,7% vastasi, ettei ole tullut tietojenkalastuksen uhriksi, ja yksi vastaaja kertoi, ettei ole varma. 27,8% eli 5 vastaajaa kertoi tulleensa sen uhriksi.



Kuvio 14: Huijaukseen lankeamisesta

Kuten Kuviosta 14 näkyy, seuraavaksi kyselyssä oli jatkokysymys edelliseen kysymykseen: ”Jos vastasit edelliseen kysymykseen kyllä, montako kertaa uskot langenneesi huijaukseen”. Kuten kuviosta näkyy, tämän kysymyksen vastaukset eroavat edellisestä kysymyksestä, sillä vain 11,1% eli 2 osallistujaa sanoi langenneensa kerran huijaukseen, mikä on kolme vähemmän kuin edellisessä kysymyksessä. 88,9% vastasi, ettei ole kertaakaan langennut tietojenkalastus-huijaukseen.

Seuraavaksi oli vuorossa kysymys ”Oletko huomannut laitteessasi mitään erikoista sen jälkeen, kun olet avannut esim. tekstiviestin tai sähköpostin linkin? Jos olet, mitä?”, ja siinäkin oli annettu tekstikenttä, johon osallistujat saivat kirjoittaa vastauksensa. Heidän vastauksensa olivat melko yksimielisiä ja kertoivat samaa kuin edellinenkin kysymys: lähes kaikki sanoivat, etteivät ole huomanneet mitään erikoista, tai avanneet mitään epäilyttäviä linkkejä. Vain kaksi vastausta erosi tästä: yksi sanoi, että ”välillä Avast ilmoittaa torjutusta hyökkäyksestä”, ja toinen kertoi hänen koneelleen ilmestyneen kerran prostituoitujen tarjouksia. Tämän osallistujan ongelma kuulemma korjaantui aktivoimalla F-securen virustorjuntaohjelma.

Kuvio 15: Vain yhdellä outoja tapahtumia pankkitilissä

Kuten Kuviosta 15 näkyy, kyselyn viimeinen kysymys oli ”Oletko huomannut esimerkiksi sähköposti- tai pankkitilissäsi jotain outoa sen jälkeen, kun olet kirjautunut jollekin sivulle”. Tässäkin kohderyhmän vastaukset olivat melko yksimielisiä: 94,4% kertoi, ettei ollut huomannut mitään outoa kummassakaan. Vain yksi osallistuja sanoi huomanneensa pankkitilissään jotain outoa jollekin sivulle kirjautumisen jälkeen.

6 Tutkimuksen eettisyys ja luotettavuus

Tämän opinnäytetyön tutkimusta tehdessä oli etiikan puolesta tärkeintä ottaa huomioon tietoturvan eettiset seikat: tutkimukseen osallistuvien kohderyhmäläisten tietosuoja ja tietoturva oli turvattava tutkimuksen aikana, eli kyselyyn osallistuessa ja sen jälkeen. Siksi oli tärkeää, että kysely tehtiin nimettömänä, jotta kyselyn laatija ei tiedä, kuka vastasi mitäkin, eli tämä ei saanut tietoa esimerkiksi tiettyjen henkilöiden salasanatottumuksista. Kyselyn nimettömyys myös tarkoittaa, että myös tässä opinnäytetyössä julkaistut tulokset ovat täysin nimettömiä, ja niitä on mahdotonta yhdistää tiettyihin henkilöihin. Tämä oli jo alussa erittäin tärkeää osallistujien tietoturvan kannalta. Koska varsinkin salasanat ovat arka aihe tietoturvan kannalta, oli myös tärkeää, että kyselyyn vastaajille oli niihin liittyvissä kysymyksissä mahdollisuus valita ”En halua vastata”. Tämä tehtiin jo tutkimuksen esittelyssä selväksi, jotta vastaajat tiesivät, ettei heidän ollut pakko vastata kyseisiin kysymyksiin. Myös kyselyn nimettömyys tehtiin jo alussa selväksi osallistujille.

Luonnollisesti opinnäytetyössä on myös noudatettu tavallisia tutkimusetiikan periaatteita ja Laurea-ammattikorkeakoulun eettisiä sääntöjä. Kohderyhmästä on käytetty sosiaalisesti hyväksyttyjä termejä, kuten ’ikäihminen’ ja ’yli 60-vuotias’. Koska tutkimuksen kysely tapahtui verkossa ja nimettömänä, pienikin syrjinnän mahdollisuus sen osalta karsittiin pois.

Tutkimusten tulosten tarkkailussa on pyritty tieteelliseen analyyttisuuteen, ja on pyritty olemaan tuomitsematta esimerkiksi huonoja tietoturvatottumuksia, vaikka työssä kehitysehdotuksia tehdäänkin.

Mitä tutkimuksen luotettavuuteen tulee, tutkimuksen aikana saatiin kyselyyn 18 vastausta, mikä on tällaiselle opinnäytetyökyselylle melko hyvä tulos, ja on riittävän kokoinen otos, jotta siitä voidaan tehdä johtopäätöksiä. On kuitenkin otettava huomioon, että koska tutkimuskyselyä jaettiin suomalaiseen keskiluokkaan kuuluvan kyselyn laatijan lähipiirissä ja lähipiirin tuttujen kesken, ovat ainakin suurin osa kyselyyn vastanneista mitä luultavimmin itsekin keskiluokkaisia ja enimmäkseen korkeakoulutettuja ihmisiä. Osa heistä on edelleen työelämässä, ja osa on jäänyt eläkkeelle vasta viimeisen kymmenen vuoden aikana. Osa vastanneista on siis mahdollisesti töissään saanut jonkinasteista tietoturvakoulutusta työpaikkojensa tietoturvaan liittyen, mikä luonnollisesti korottaa heidän omaa tietoturvatietoisuuttaan. Kaikki kyselyyn vastanneet ovat myös ainakin jossain määrin digitaitoisia, sillä he osasivat vastata sähköisesti toteutettuun kyselyyn. Mikäli tutkimus olisi toteutettu lähihaastatteluna, paperisena kyselynä tai muuten paikan päällä, tai jonkun muun ihmisjoukon keskuudessa, saattaisi vastauksissa näkyä enemmän vaihtelevuutta.

Edellä kuvatut kyselyyn vastaajat voidaan kuitenkin nähdä jokseenkin keskivertoihmisinä, sillä Tilastokeskuksen vuoden 2020 tutkimuksen mukaan noin 1,5 miljoonaa suomalaista oli suorittanut vähintään alimman korkea-asteen tutkinnon (Tilastokeskus, 2020). Tarkkoja lukuja ikäihmisten osuudesta tästä luvusta ei löytynyt, mutta ottaen huomioon, että Tilastokeskuksen väestöraportin mukaan 22,7 % suomalaisista on yli 65-vuotiaita (Tilastokeskus, 2021), ja tästä luvusta puuttuvat niin ikään tutkimuksen kohderyhmään kuuluvat 60–64-vuotiaat, voidaan olettaa, että merkittävä osa noista 1,5 miljoonasta suomalaisesta korkeakoulutetusta on ikäihmisiä. Kyselyn vastausten voidaan siis katsoa antavan tarpeeksi luotettavan kuvan siitä, millä tasolla keskivertoisen ikäihmisen tietoturvatietoisuus on.

7 Tutkimuksen tulokset

Kyselyn vastauksia tarkastellessa ilmeni sekä melko odotettavia tuloksia että hyvin yllättäviäkin sellaisia. Kun kyselyn ensimmäisen osion vastauksia katsoo, on selvää, että yli 60-vuotiaiden salasanatottumukset eivät ole siitä tietoturvallisimmasta päästä, ja siinä olisi kehitettävää. Suurin kehittämisen aihe olisi monien vastaajien tyypillisissä salasanoissa: moni salasanoissa käyttää joko nimeä ja syntymävuottaan, tai jotain sanaa ja syntymävuottaan, eikä kumpaakaan pitäisi tehdä. Tietoturva-asiantuntijoiden mukaan salasanassa ei pitäisi koskaan käyttää omaa nimeään, eikä syntymävuodenkaan käyttö ole suositeltavaa. Hyvässä salasanassa on sekä kirjaimia, numeroita, että erikoismerkkejä, jos ne vain ovat sallittu, mielellään sekaisin keskenään. Kuitenkin salasanan kannattaisi olla myös sellainen, jonka käyttäjä

muistaa. Tästä syystä esimerkiksi osan kirjaimista korvaaminen numeroilla salasanassa, kuten yhdessä ko. kysymyksen esimerkkisalasanassa, on hyvä vaihtoehto. Näin salasana on helpompi muistaa, eikä sitä tarvitse kirjoittaa ylös. Salasanojen kirjoittaminen ylös, varsinkaan muistilapulle tai vihkoon, kuten moni vastaaja kertoi tekevänsä, ei ole erityisen tietoturvallista, ja siinäkin olisi siis kehitettävää. Kohderyhmästä kukaan ei vastannut käyttävänsä salasanojen säilöntäsovellusta, mikä on kaikkein tietoturvallisisin paikka säilyttää salasanoja, mikäli niitä haluaa jossain säilyttää. Selaimeen tallentaminen on toki vaihtoehto, mutta se tarkoittaa, että käyttäjän salasanat tallentuvat selainta pyörittävän yrityksen palvelimille, missä on omat ongelmansa.

Vastaukset kysymykseen salasanojen vaihtamisesta osoittivat myös kehittämisen tarvetta osallistujien salasanatottumuksissa, joskin tulos ei ollut yllättävä. Se, että monet eivät vaihda salasanaansa, ellei ole pakko, oli jokseenkin arvattavissa, eikä koske pelkästään tutkimuksen kohteena ollutta ikäryhmää. Siihen on syynsä, miksi monissa yrityksissä ja organisaatioissa, mukaan lukien Laurea-ammattikorkeakoulussa, pakotetaan vaihtamaan salasana tietyin väliajoin, ja se on nimenomaan tämä tapa olla vaihtamatta salasanoja. Kuitenkin salasanoja olisi tärkeä vaihtaa, sillä mitä pidempään sama salasana on käytössä, sitä vähemmän se on tietoturvallinen, sillä se saatetaan hyvinkin murtaa jossain vaiheessa. Etenkin, jos samaa salasanaa käyttää useassa paikassa. Tässäkin olisi siis kehitettävää kohderyhmän tietoturvatietoisuuden edistämiseksi. Samoin olisi kehitettävää, jotta kohderyhmä saataisiin käyttämään enemmän kaksivaiheista tunnistautumista, jota osa kertoi käyttävänsä joskus ja osa ei ollenkaan. Kuten salasanoihin liittyvistä kysymyksistä huomattiin, salasanat eivät aina ole kovinkaan hyvä suoja tunnuksille tai tiedolle: siksi olisi tärkeää, että kirjautumiseen vaadittaisiin aina kaksi tunnistautumisen metodia, jotta pelkkä käyttäjätunnus ja salasana ei riittäisi sisään pääsyyn. Se lisää hieman vaivaa kirjautumiseen, mutta ei paljoa, ja kuten tutkimuksen vastauksissa huomattiin, se olisi tutkimuksen ikäryhmälle erityisen tärkeää.

Kohderyhmän vastauksissa kyselyn toiseen osaan sen sijaan oli yllättäviäkin puolia. Oli positiivinen yllätys, että kaikki kohderyhmän kyselyyn osallistujat tunnistivat molemmat huijausviestit, ja osasivat kertoa monia huijausviestien ja -puheluiden piirteitä, josta ne tunnistaa. Se, että he enimmäkseen tietävät olla avaamatta tuntemattomilta tulevia linkkejä, ei ollut yhtä yllättävää, mutta positiivinen tulos sekin. Molemmat olivat osoitus siitä, että tietojenkalastuksen puolella ainakin näillä kohderyhmän jäsenillä on tietoturvatietoisuus melko hyvällä tasolla, mikä on aina hyvä uutinen. Samalla oli kuitenkin hieman yllättävää, että niin moni kertoi, ettei ollut saanut ainuttakaan huijauspuhelua puolen vuoden aikana, sillä muutama vastaajista oli saanut niitä yli 10, ja opinnäytetyön tekijän omasta kokemuksesta ne ovat melko yleisiä. Toki on otettava huomioon mahdollisuus, että osa näistä vastaajista on itse asiassa saanut huijauspuheluita jossain vaiheessa, mutta eivät vain muista sitä, sillä puoli vuotta on pitkä aika. Vaikuttaisi kuitenkin siltä, että mikäli he ovat saaneet huijauspuhelun, he ovat tunnistaneet sen sellaiseksi. Lisäksi on tietenkin mahdollista, että ero johtuu siitä, että osa

kyselyyn vastaajista ei vastaa tuntemattomiin numeroihin lainkaan, jolloin he eivät myöskään saisi huijauspuheluita. Se, että ei vastata tuntemattomiin numeroihin, on kuitenkin melko yleistä nykyään.

8 Yhteenveto

Tämän opinnäytetyön tarkoitus oli selvittää, millä tasolla yli 60-vuotiaiden tietoturvatietoisuus on tällä hetkellä tietojenkalastuksen ja jossain määrin myös salasanojen osalta. Tutkimuksen perusteella voidaan nyt sanoa, että kohderyhmän tietoturvatietoisuus on tietojenkalastuksen kannalta jokseenkin hyvällä mallilla, ja se osaa tunnistaa huijauspuhelut ja -viestit, ja reagoida niihin oikein, ja olla klikkaamatta tuntemattomia linkkejä. Se, kuinka paljon he ovat saaneet huijauspuheluita viimeisen puolen vuoden aikana vaihtelee, mutta huijausviestejä ovat saaneet lähes kaikki vähintään yhden, osa enemmän. Sen sijaan salasanatottumusten puolella heidän tietoturvatietoisuudessaan olisi vielä kehitettävää, sillä heidän tyypilliset salasanansa ja niiden ylöskirjaamistavat eivät vastaa nykyisiä tietoturvasuosituksia.

Tätä opinnäytetyötä on tehty pitkään ja hartaasti, ensin aiheen valinnan vaikeuden, ja sitten erinäisten muiden viivästysten vuoksi. Lopulta päädyin tekemään tätä samaan aikaan, kun tein harjoitteluani, johon tämä opinnäytetyö ei liity mitenkään. Nämä olosuhteet huomioiden sanoisin, että työni meni loppujen lopuksi suhteellisen hyvin. Työskentelyni seurasi loogista järjestystä, ja tutkimukseni oli itse asiassa aika mielenkiintoinen, joskaan aika ei riittänyt laajemman tutkimuksen tekemiseen. Nyt kun tämä on viimein tehty, olen tyytyväinen lopputulokseen.

Lähteet

Painetut

Dulaney E. & Easttom C. 2017. CompTIA Security+ Study Guide : Exam SY0-501. 7. painos. John Wiley & Sons, Incorporated.

Hadnagy C., Fincher M. ja Dreeker R. 2015. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. John Wiley & Sons, Incorporated.

Sähköiset

Heinonen J. Tutkimussuunnitelma, luku 7. Kyvyt.fi. Julkaistu 31.12.2012. Viitattu 16.2.2022. https://kyvyt.fi/view/artefact.php?artefact=304009&view=72174

Hiltunen L. Metodina kyselytutkimus. Jyväskylän yliopisto. Viitattu 18.2.2022. http://www.mit.jyu.fi/OPE/kurssit/Graduryhma/PDFt/kyselytutkimus2.pdf

Internetin käyttö medioiden seuraamiseen ja viestintään lisääntynyt. Tilastokeskus. Julkaistu 10.11.2020. Viitattu 18.2.2022. https://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tie_001_fi.html

Käsitteet. Validiteetti. Tilastokeskus. Viitattu 13.2.2022. https://www.stat.fi/meta/kas/validiteetti.html

Tutkinnon suorittaneiden osuus väestöstä moninkertaistunut 50 vuodessa. Tilastokeskus. Julkaistu 31.11.2021. Viitattu 17.2.2022 https://tilastokeskus.fi/til/vkour/2020/vkour_2020_2021-11-03_tie_001_fi.html

Väestö ja yhteiskunta. Tilastokeskus. Viitattu 17.2.2022. https://www.tilastokeskus.fi/tup/suoluk/suoluk_vaesto.html

Kuviot

Liitteet

Liite 1: Kysely yli 60-vuotiaiden tietoturvatietoisuudesta.

Yleistä tietoturvasta

1. Kuinka usein vaihdat salasanasi? *

Merkitse vain yksi soikio.

- ◯ Useammin kuin kerran 2 kuukaudessa
- ◯ 2-4 kuukauden välein
- ◯ 5-6 kuukauden välein
- ◯ 6-12 kuukauden välein
- ◯ Parin vuoden välein
- ◯ En koskaan
- ◯ Muu: _____

2. Mikä näistä vaihtoehdoista muistuttaa eniten tyypillisiä salasanojasi? *

Merkitse vain yksi soikio.

- ◯ Salasana123
- ◯ MaijaMehiläinen62
- ◯ Matkailija54
- ◯ M4tk41l1j4
- ◯ Ghj4GH73hj
- ◯ En halua vastata

3. Miten merkitset salasanasi muistiin? *

Merkitse vain yksi soikio.

- ◯ Muistilapulle/vihkoon
- ◯ Tallennan selaimen (Google, Edge, Explorer, Mozilla) muistiin
- ◯ Käytän sovellusta, joka säilöö kaikki salasanani yhteen paikkaan vahvan salauksen taakse.
- ◯ En merkitse niitä muistiin mihinkään
- ◯ En halua vastata
- ◯ Muu: _____

4. Käytätkö kaksiosaista varmennusta esim. sähköposti- tai sosiaalisen median tileilläsi? (esim. Facebookissa) *

Merkitse vain yksi soikio.

- ◯ Käytän aina
- ◯ Osassa niistä
- ◯ Vain jos on pakko
- ◯ En

5. Kuinka monta huijauspuhelua arvelet saaneesi viimeisen puolen vuoden aikana? *

Merkitse vain yksi soikio.

- ◯ En yhtään
- ◯ 1-3
- ◯ 4-6
- ◯ 7-9
- ◯ 10 tai enemmän

6. Kuinka monta huijausviestiä (tekstiviesti tai sähköposti arvelet saaneesi viimeisen puolen vuoden aikana? *

Merkitse vain yksi soikio.

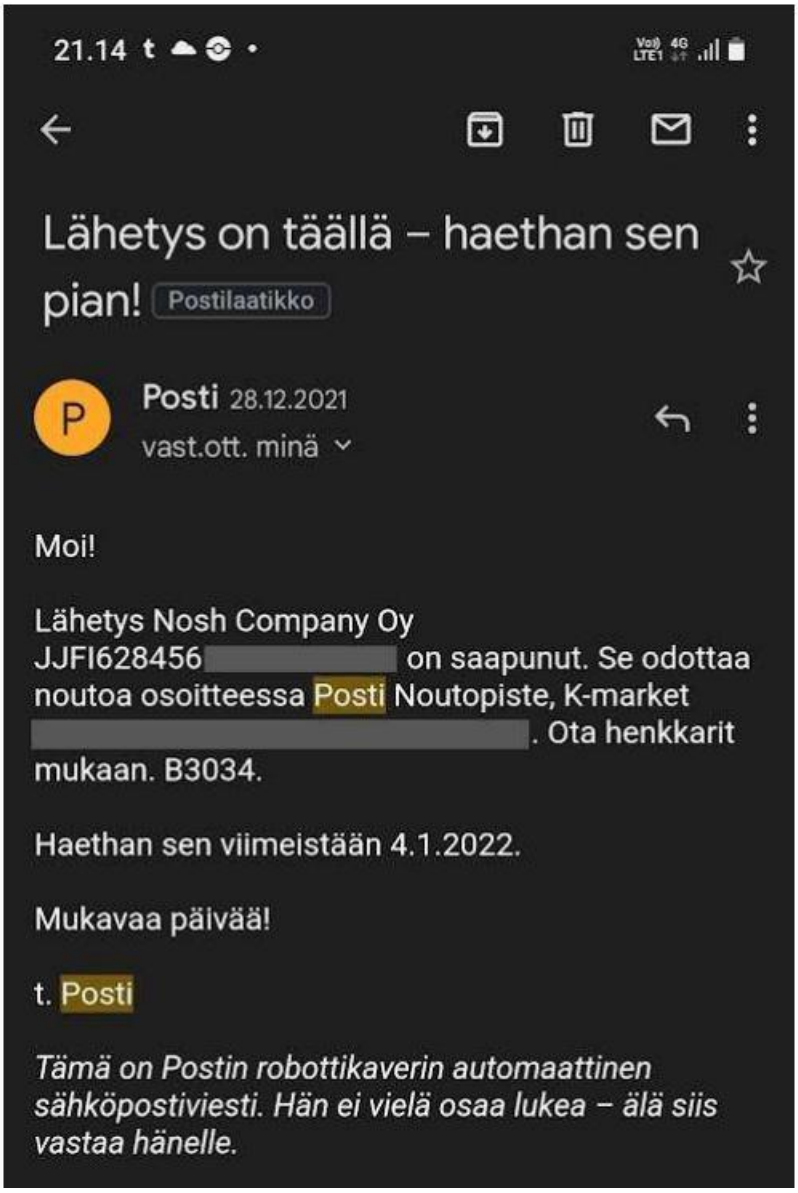
- ◯ En yhtään
- ◯ 1-3
- ◯ 4-6
- ◯ 7-9
- ◯ 10 tai enemmän

7. Onko alla olevassa kuvassa näkyvä Postin sähköpostiviesti aito vai huijaus? *

Merkitse vain yksi soikio.

- ◯ Aito
- ◯ Huijaus

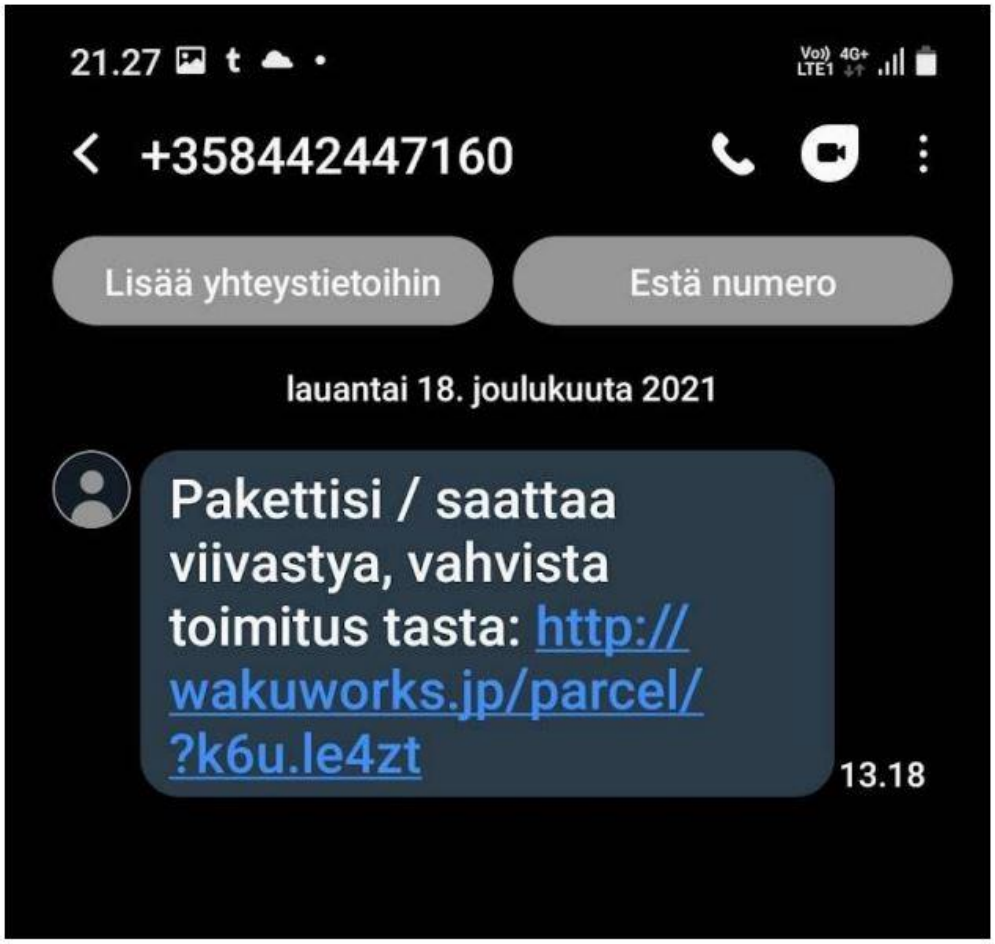
8. Entä onko tässä kuvassa näkyvä Postin viesti aito vai huijaus? *



Merkitse vain yksi soikio.

- ◯ Aito
- ◯ Huijaus

9. Onko kuvassa näkyvä tekstiviesti aito vai huijaus? *



Merkitse vain yksi soikio.

- ◯ Aito
- ◯ Huijaus

10. Mistä yleensä tunnistat huijausviestin tai puhelun? *

11. Avaatko usein sähköposteissa tai tekstiviesteissä olevia linkkejä? *

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ Joskus
- ◯ En

12. Uskotko tulleesi koskaan tietojenkalastushuijauksen uhriksi? Tietojenkalastuksella tarkoitetaan toimintaa, jossa yritetään varastaa esimerkiksi pankkitunnuksia huijaamalla uhrit luovuttamaan ne huijausviesteillä tai -puheluilla, joissa tekeydytään esim. Postiksi. *

Merkitse vain yksi soikio.

- ◯ Ei
- ◯ Kyllä
- ◯ En ole varma

13. Jos vastasit edelliseen kysymykseen kyllä, montako kertaa uskot langenneesi huijaukseen? *

Merkitse vain yksi soikio.

- ◯ Kerran
- ◯ Kaksi kertaa
- ◯ Kolme kertaa
- ◯ Neljä kertaa tai enemmän
- ◯ En ole langennut huijaukseen

14. Oletko huomannut laitteessasi mitään erikoista sen jälkeen, kun olet avannut esim. tekstiviestin tai sähköpostin linkin? Jos olet, mitä? *

_____

_____

_____

_____

_____

15. Oletko huomannut esimerkiksi sähköposti- tai pankkitilissäsi jotain outoa sen jälkeen, kun olet kirjautunut jollekin sivulle? *

Merkitse vain yksi soikio.

- ◯ Kyllä, sähköpostissa
- ◯ Kyllä, pankkitilissä
- ◯ En ole
- ◯ Muu: _____