Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VALTTERI VIERIMAA

Satakunnan ammattikorkeakoulun opiskelijoiden tietämys ja kokemukset turvallisesta pankkiasioinnista ja pankkihuijauksista

OPINNÄYTETYÖ

LIIKETALOUDEN TUTKINTO-OHJELMA
2025

TIIVISTELMÄ

Vierimaa, Valtteri: Satakunnan ammattikorkeakoulun opiskelijoiden tietämys ja kokemukset turvallisesta pankkiasioinnista ja pankkihuijauksista
Opinnäytetyö, AMK
Liiketalouden tutkinto-ohjelma
Helmikuu 2025
Sivumäärä: 55

Pankkihuijaukset ovat yleistyneet todella paljon viime vuosina muun muassa jatkuvan digitalisaation myötä myös finanssialalla. Pankkipalvelut ovat nykyään suureksi osaksi verkossa, jonka myötä turvallinen pankkiasiointi on noussut yhä tärkeämpään rooliin huijausten estämisessä. Pankkihuijaukset ovat yhä vaikeammin havaittavissa, jonka vuoksi aiheesta on tärkeä tuoda esiin tietoa ja keskustella.

Tämän opinnäytetyön tavoitteeksi asetettiin selvittää Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkielisten päiväopiskelijoiden tietämyksen taso liittyen pankkihuijauksiin ja turvalliseen pankkiasiointiin sekä selvittää opiskelijoiden kokemuksia aiheeseen liittyen.

Työn teoriaosa koostuu kahdesta pääluvusta, jotka ovat turvallinen pankkiasiointi ja pankkihuijaukset. Ensimmäisessä teorialuvussa käytiin läpi eri pankkipalvelut, tietoturvallisuutta ja vahvaa sähköistä tunnistautumista, jotka ovat keskeisiä turvallisen pankkiasioinnin kannalta. Toisessa teorialuvussa käsiteltiin erilaiset pankkihuijaustavat ja mitä seurauksia pankkihuijauksista seuraa.

Tutkimuksen toteutuksessa käytettiin määrällistä tutkimusmenetelmää. Tutkimuksen aineistonkeruu toteutettiin strukturoidulla sähköisellä internet kyselyllä. Kyselytutkimukseen vastasi 59 kohderyhmän opiskelijaa. Kyselytutkimuksessa selvisi, että yksi kyselyn vastaaja on joutunut pankkihuijauksen uhriksi. Kyselyyn vastanneista 19 henkilöön oli kohdistunut huijausyritys. Tutkimustulosten perusteella selvisi, että tutkimukseen vastanneilla opiskelijoilla on hyvä tietämys turvallisesta pankkiasioinnista ja he tunnistavat melko hyvin eri huijaukset. Vaikka tutkimus osoitti, että kohderyhmän opiskelijoiden tietämys aiheesta on hyvä, niin noin puolet vastaajista koki, ettei aiheesta ole saatavilla riittävästi tietoa. Tutkimuksesta selvisi, että myös nuoriin kohderyhmän opiskelijoihin kohdistuu paljon pankkihuijausyrityksiä, vaikka he osaavatkin havaita niitä melko hyvin.

Avainsanat: Pankki, pankkipalvelut, pankkihuijaus, kyberrikollisuus, turvallinen pankkiasiointi, verkkourkinta

ABSTRACT

Vierimaa, Valtteri: Satakunta University of Applied Sciences students' knowledge and experiences of safe banking and bank scams
Bachelor's thesis
Business Administration
February 2025
Number of pages: 55

Bank fraud has become significantly more common in recent years, partly due to the ongoing digitalization of the financial sector. Banking services are now largely online, making secure banking increasingly important in preventing fraud. Bank fraud schemes are becoming harder to detect, which is why raising awareness and discussing the topic is essential.

The objective of this thesis was to assess the level of knowledge among Finnish-speaking full-time students at Satakunta University of Applied Sciences' Rauma campus regarding bank fraud and secure banking, as well as to explore their experiences related to the topic.

The theoretical part of the study consists of two main sections: secure banking and bank fraud. The first section examines different banking services, cybersecurity, and strong electronic authentication, which are crucial for safe banking. The second section discusses various types of bank fraud and their consequences.

A quantitative research method was used in this study. Data collection was conducted through an online survey, with 59 students from the target group responding. The survey revealed that one respondent had been a victim of bank fraud, while 19 respondents had experienced attempted fraud. The results indicate that the students who participated in the study have a good understanding of secure banking and can recognize different types of fraud relatively well. However, despite their knowledge, about half of the respondents felt that there was not enough information available on the topic. The study also showed that young students are frequently targeted by bank fraud attempts, even though they are fairly skilled at identifying them.

Keywords: Bank, banking services, bank fraud, cybercrime, secure banking, phishing

SISÄLLYS

1 JOHDANTO

Eri toimijoiden, kuten esimerkiksi pankkien, poliisin, postin, verohallinnon ja yksityisten yritysten nimissä liikkuu tänä päivänä valtava määrä huijausviestejä, joilla pyritään saamaan tietoon ihmisten verkkopankkitunnuksia tai muutoin huijata ihmisiltä rahaa. Tämä on valitettava todellisuus. Muutaman viimevuoden aikana erilaiset huijaukset ovat yleistyneet räjähdysmäisesti. Vuonna 2023 suomalaisilta on yritetty huijata huimat 76,9 miljoonaa euroa. Pankit saivat kuitenkin estettyä huijausyrityksistä 32,7 miljoonaa euroa, jotka olisivat päätyneet huijareille. Vuonna 2022 suomalaisilta yritettiin huijata erilaisilla huijauksilla 46,5 miljoonaa euroa. Huijausyritysten määrä on siis yhden vuoden aikana kasvanut noin 30 miljoonalla eurolla. Vuonna 2024 pelkästään tammikesäkuussa huijausyritykset ovat 45,7 miljoonaa euroa. Pankkihuijaukset ovat siis selkeässä kasvussa, joten pankkiturvallisuudesta tiedottaminen ja pankkien asiakkaiden kouluttaminen tunnistamaan ja suojautumaan huijauksilta on todella tärkeää, jotta huijauksia pystytään ehkäisemään tulevaisuudessa (Finanssiala ry, 2024).

Turvallinen pankkiasiointi ja ihmisten tietämys sekä osaaminen sen osalta on kriittisen tärkeää pankkihuijauksien estämisessä. Vaikka huijausten määrä on ollut kasvussa, niin myös pankkien kyky estää huijauksia on parantunut. Huijarit käyttävät luovia ja monenlaisia eri keinoja, jotta he saavat kalastettua ihmisten pankkitunnuksia tai maksukorttien tietoja. Tietoja voidaan kalastella esimerkiksi tekstiviestillä, sähköpostilla ja sosiaalisessa mediassa, joissa huijarit käyttävät psykologisia keinoja. Lisäksi huijarit voivat luoda luotettavan näköisiä pankkien tai verkkokauppojen sivuja, jotka voi olla vaikea erottaa oikeasta sivustosta (Finanssiala ry, 2024). Tässä opinnäytetyössä pyritään selvittämään Satakunnan ammattikorkeakoulun opiskelijoihin kohdistuneiden huijausten määrää ja opiskelijoiden tietämyksen tasoa turvallisesta pankkiasioinnista.

2 TUTKIMUKSEN TAVOITTEET

2.1 Tarkoitus, tavoite ja tutkimusongelma

Opinnäytetyössä on tarkoitus selvittää Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkielisten päiväopiskelijoiden tietoisuutta pankkiturvallisuudesta ja kuinka paljon heihin on kohdistunut pankkihuijauksia. Työstä hyötyy finanssiala ja sen toimijat, sillä he saavat tietoa korkeakouluopiskelijoiden tieto- ja taitotasosta liittyen pankkiturvallisuuteen ja pankkihuijauksiin. Tarkoituksena on lisäksi kartoittaa kokevatko nuoret opiskelijat tietävänsä tarpeeksi turvallisesta pankkiasioinnista ja miten he mahdollisesti haluaisivat tietää asiasta lisää. Tästä tiedosta on hyötyä finanssialalle, sillä näin he saavat kuvaa mikä on tietoisuus pankkiturvallisuudesta nuorten keskuudessa. Aihe on tärkeä, sillä pankkihuijauksien määrä on kasvanut joka vuosi viimevuosien aikana. Suomalaisilta on saatu pankkihuijauksilla vietyä jo pelkästään vuoden 2024 tammi-kesäkuun aikana 27,5 miljoonaa euroa (Finanssiala ry, 2024). Tietoisuuden lisääminen pankkihuijauksista ja turvallisesta pankkiasioinnista on tärkeää, jotta pankkihuijauksia voidaan tulevaisuudessa estää paremmin finanssialan toimijoiden toimesta sekä ihmisten paremmalla kyvyllä havaita huijausyrityksiä.

Työn konkreettisena tavoitteena on tehdä selvitys korkeakouluopiskelijoiden ja tarkemmin Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkielisten päiväopiskelijoiden tietoisuudesta turvallisesta pankkiasioinnista, ja pankkihuijauksista sekä miten heihin on kohdistunut pankkihuijauksia.

Opinnäytetyössä on tavoitteena saada vastaukset seuraaviin kysymyksiin:

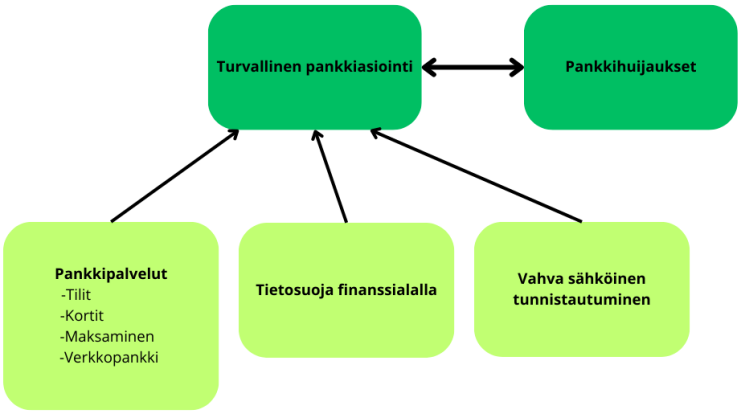
- Mikä on Satakunnan ammattikorkeakoulun opiskelijoiden tietoisuus pankkihuijauksista ja turvallisesta pankkiasioinnista?

- Onko Satakunnan ammattikorkeakoulun opiskelijoihin kohdistunut pankkihuijauksia tai -huijausyrityksiä ja miten niitä on esiintynyt?

- Miten ja mistä korkeakouluopiskelijat haluaisivat saada lisätietoa turvallisesta pankkiasioinnista?

2.2 Opinnäytetyön aiheenrajaus ja viitekehys

Opinnäytetyön teoriaosassa on tarkoitus käydä läpi turvallista pankkiasiointia ja pankkihuijauksia. Työssä käydään läpi suomalaisten pankkien henkilöasiakkaiden peruspankkipalvelut, joiden oikea käyttö on osa pankkiturvallisuutta. Työssä ei käsitellä yritysasiakkaiden pankkipalveluita tai alaikäisten pankkipalveluita, sillä tutkimuksen kohderyhmän henkilöt ovat suureksi osaksi pankkien henkilöasiakkaita. Aihe on rajattu suomalaisiin henkilöasiakkaisiin, jotta työstä ei tule liian laaja ja pinnallinen. Opinnäytetyössä ei myöskään käsitellä tarkemmin lainaamista ja siihen liittyviä huijauksia, sillä suurin osa pankkihuijauksista kohdistuu henkilöasiakkaisiin ja peruspankkipalveluihin, kuten verkkopankkitunnuksiin.



Kuvio 1. Käsitteellinen viitekehys

Kuviossa 1 esitetyssä käsitteellisessä viitekehyksessä esitetään opinnäytetyön teoriaosan tärkeimmät käsitteet ja niiden yhteys toisiinsa. Opinnäytetyön teoriaosassa käydään läpi turvallista pankkiasiointia eli niin sanottua

pankkiturvallisuutta. Turvalliseen pankkiasiointiin kuuluvat peruspankkipalvelut, kuten tilit, kortit, maksaminen ja verkkopankki. Pankkipalveluiden turvallinen käyttö on tärkeä osa turvallista pankkiasiointia. Turvalliseen pankkiasiointiin kuuluu myös osaksi tietosuoja finanssialalla. Tietosuoja määrittää, että mitä tietoa pankit kysyvät, sekä kuinka tietoa käsitellään. Lisäksi turvalliseen pankkiasiointiin kuuluu osaksi vahva sähköinen tunnistautuminen. Se on tärkeää, kun halutaan käyttää turvallisesti pankkipalveluita tai tunnistautua esimerkiksi valtion palveluihin. Turvallinen pankkiasiointi on suoraan yhteydessä pankkihuijauksiin ja pankkihuijaukset yhteydessä turvalliseen asiointiin. Pankkihuijaukset perustuvat turvallisen pankkiasioinnin puutteisiin ja hyödyntävät heikkouksia. Turvallinen pankkiasiointi ja sen oikea toteuttaminen ehkäisee pankkihuijauksien toteutumista.

2.3 Keskeiset käsitteet

Pankit ovat finanssialan toimijoita, jotka ottavat vastaan talletuksia ja myöntävät luottoja. Lisäksi pankit voivat hoitaa asiakkaidensa sijoituksia ja varallisuutta. Pankkien tärkeänä tehtävänä on myös välittää maksuja (Finanssiala ry, 05.01.2024). Pankit myöntävät luottoja, joista asiakkaat maksavat korkoa, johon pankit lisäävät oman marginaalinsa ja näin ollen tekevät voittoa. Finanssialan toimijoiden toiminta on tarkasti säädelty luottolaitoksia koskevassa lainsäädännössä.

3 TURVALLINEN PANKKIASIOINTI

Tässä luvussa käydään läpi turvallista pankkiasiointia tietosuojan ja tietoturvan kannalta. Lisäksi käydään läpi peruspankkipalvelut, kuten tilit, kortit, maksaminen ja verkkopankki sekä niillä turvallista pankkiasiointia. Luvussa käydään myös läpi verkkopankkitunnuksilla tapahtuvaa vahvaa sähköistä tunnistautumista ja siihen liittyvää turvallista pankkiasiointia.

3.1 Tietosuoja finanssialalla

Tietosuojalla tarkoitetaan ihmisen henkilötietojen suojaa. Tietosuoja määrittää ketkä saavat kerätä ihmisten henkilötietoja ja milloin sekä miten niitä käsitellään. Henkilötietoja ovat kaikki tiedot, joita voidaan käyttää tunnistamaan henkilö. Henkilötietojen käsittelystä määritellään laissa (Tietosuojavaltuutetun toimisto, n.d.b).

Tietosuojasta on määritelty Euroopan Unionin yleisessä tietosuojalaissa eli GDPR asetuksessa. GDPR on lyhenne sanoista general data protection regulation. Laki on viimeksi päivitetty vuonna 2018 ja se sääntelee henkilötietojen käsittelyä. Lakia sovelletaan kaikissa EU-maissa. Asetuksen tavoitteena on varmistaa, että muun muassa finanssialan toimijat ja muut tahot käsittelevät henkilötietoja turvallisesti, vastuullisesti ja asianmukaisin perustein. Pankit käsittelevät erityisen arkaluontoisia henkilötietoja sekä asiakkaiden tili- ja maksutietoja, joten on tärkeää, että finanssialan toimijat käsittelevät tietoja huolella (Tietosuojavaltuutetun toimisto, n.d.a).

Finanssialla toimivilla pankeilla on lakiin perustuvia velvollisuuksia kerätä asiakkaidensa henkilötietoja ja muita tarvittavia tietoja. Rahanpesulaissa (laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017) määritellään pankkien velvollisuudesta tuntea asiakkaansa ja heidän liiketoimensa. Kun pankit keräävät tietoa asiakkaistaan, niin ne muodostavat kuvan asiakkaalle tavanomaisista liiketoimista. Asiakkaan tuntemisen avulla pankit voivat havaita, mikäli asiakkaiden tileillä tai palveluissa tapahtuu huomiota herättäviä normaalista poikkeavia liiketoimia, kuten esimerkiksi suuria tilisiirtoja ulkomaiseen pankkiin tai suuria käteisnostoja. Näin pankit voivat havaita, että asiakkaan pankkiturvallisuus on vaarantunut ja joku tuntematon ihminen on saattanut saada haltuun asiakkaan pankkitunnukset tai korttitiedot. Rahanpesulaissa on määritelty, että pankeilla on oltava ajantasaiset ja päivitetyt henkilöiden sekä yritysten asiakastiedot (Laki rahanpesun ja terrorismin rahoittamisen estämisestä, 444/2017, 3 luku).

Tietoturva

Tietoturva on yksi keino suojata tietoja ja toteuttaa tietosuojaa. Tietoturvan avulla finanssialalla suojataan asiakkaiden henkilötietoja ja muita arkaluonteisia tietoja ja tietojärjestelmiä. Käytännössä tietoturva varmistetaan organisaatioissa erilaisin teknisin järjestelmin, jotka varmistavat tiedon luottamuksellisuuden ja suojan ulkopuolisilta toimijoilta (Tietosuojavaltuutetun toimisto, n.d.b).

”Tietoturvallisuudella tarkoitetaan sitä, että yrityksen tiedot, palvelut, järjestelmät ja tietoliikenne on suojattu ja varmistettu sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä” (Finanssivalvonta, 2014, s. 23).

Pankeille tietoturva tarkoittaa käytännössä asiakkaiden tietosuojan varmistamista eli asiakkaisiin liittyvän tiedon, kuten henkilötietojen, maksutietojen ja tilitietojen suojaamista. Tietoturvallisuus on todella tärkeää finanssialan toimijoille, sillä heidän käsittelemä tieto on arkaluonteista. Pankkeihin kohdistuu vuosi vuodelta enemmän hyökkäyksiä, joten pankeille on tärkeää jatkuvasti valvoa ja kehittää tietoturvallisuuttaan. Tietoturvariskien hallinnoiminen on tärkeää, jotta pankit säilyttävät luottamuksen asiakkaisiinsa. Tietoturvan toteuttamisessa käytetään monia keinoja, kuten vahvaa salaus- ja tunnistustekniikkaa, pääsynvalvontaa, palomuureja sekä tietomurtojen ja kyberhyökkäysten havaitsemista varten kehitettyjä monitorointijärjestelmiä. Tietoturvan kannalta on tärkeää, että myös pankin asiakkaan laitteet, joilla pankkipalveluja käytetään, on turvattu tietoturvaohjelmistoilla (Finanssivalvonta, 2014, luku 6).

3.2 Pankkipalvelut

Tässä opinnäytetyössä käsitellään pankkiturvallisuutta ja pankkihuijauksia kohdistuen pääasiassa peruspankkipalveluihin. Peruspankkipalveluihin kuuluvat Debit-maksukortti, perusmaksutili ja verkkopankkitunnukset. Peruspankkipalveluilla on myös mahdollisuus suorittaa maksutapahtumia, nostaa käteistä rahaa ja tunnistautua sähköisesti. Peruspankkipalveluihin ei kuulu osaksi luottokortit tai luotolliset tilit. Pankkien on tarjottava kaikille henkilöasiakkaille

peruspankkipalveluita tasapuolisesti edellyttäen, että asiakas asuu laillisesti ETA-valtiossa (Finanssivalvonta, 2018).

Tilit

Pankit tarjoavat erilaisia tilejä, joita ovat useimmiten käyttötili, säästötili, ASP-tili ja erilaiset määräaikaistilit. Eri tilityyppien nimet voivat vaihdella eri pankkien välillä. Käyttötili on päivittäiseen käyttöön tarkoitettu tili, johon voi liittää maksukortin ja tehdä käteisnostoja tai talletuksia. Useimmat pankit eivät maksa käyttötilille korkoa. Säästötili on taas säästämiseen tarkoitettu tili, johon useat pankit maksavat korkoa. Säästötileihin ei saa liitettyä maksukorttia. Pankit haluavat maksaa säästötileille korkoa, jotta ne saavat asiakkaat tallettamaan tilille heidän varojansa. Asiakkaiden talletetut varat kasvattavat pankkien talletuskantaa. Pankit hyödyntävät asiakkaidensa tallettamia varoja ja myöntävät näistä luottoja muille asiakkailleen (Alhonsuo ym., 2009, s.185-186).

Määräaikaistilit ovat tilejä, jotka ovat sovitun määräajan voimassa. Määräaikaistilille maksetaan usein korkeampaa korkoa kuin säästötilille. Määräaikaistilissä tilin korko sovitaan tilin luomisen yhteydessä pankin kanssa. Määräaikaistilit voivat olla esimerkiksi vuoden pituisia, jolloin sovittu korko on koko vuoden sama tilin eräpäivään saakka. Määräaikaistilissä tilille talletetut varat ovat sidottuina tiliin koko sen määräajan, joten varoja ei voi siirtää tilitä pois kesken määräaikaisuutta. Tilin korko määräytyy yleisen korkotason, talletussumman ja määräajan mukaan (Nordea, n.d.a).

ASP-tili eli asuntosäästöpalkkiotili on tarkoitettu ensiasunnon ostoa varten säästämiseen. ASP-tilille maksetaan vuotuista korkoa. ASP-tilin ideana on, että sinne säästetään 10 % ensiasunnon ostohinnasta. Kun pankin asiakas on säästänyt 10 % ensiasunnon ostohinnasta, niin asuntoa ostaessa pankki myöntää loput varat asunnon ostoa varten ASP-lainana. ASP-tilin tarkoitus on tehdä ensiasunnon ostosta helpompaa. ASP- lainassa oman rahan osuus asunnon ostossa on matalampi kuin normaalissa asuntolainassa. ASP-tiliä voi hyödyntää vain ensi asunnon ostossa 15-44-vuotiaat henkilöt (Op, n.d.a).

Kortit

Pankkitileihin on mahdollista liittää maksukortteja, joita on erilaisia eri pankeilla. Korttivaihtoehtoja ovat Debit-pankkikortti, Credit-luottokortti tai yhdistelmäkortti, jossa on molemmat maksuvaihtoehdot. Lisäksi pankeilla on olemassa alaikäisille sopivia kortteja. Debit kortilla maksaessa maksu veloitetaan pankkitililtä. Maksukorteilla voi tehdä verkko-ostoksia verkkokaupoista, maksaa maksupäätteillä kaupoissa ja nostaa käteistä automaateista (Aktia, n.d.).

Luottokortti on kortti, johon luottoyhtiö on myöntänyt luottoa tiettyyn luottorajaan saakka. Luottokortilla maksaessa ostosta ei tarvitse heti maksaa omalta tililtään, vaan siitä syntyy luottovelkaa luottoyhtiölle. Luottovelkaa lyhennetään yleensä kuukausittain laskuilla, joita luottoyhtiö lähettää asiakkaalleen. Luottovelan lyhennyksen määrä vaihtelee sopimuksen mukaan. Luotto-ominaisuuden voi yhdistää myös tavalliseen pankkikorttiin, jolloin kyseessä on yhdistelmäkortti. Credit/Debit yhdistelmäkortilla maksaessa on valittava kummalla vaihtoehdolla maksaa (Kuluttajaliitto, n.d.).

Maksukorteilla maksettaessa käytetään korttiin liitettyä nelinumeroista PIN-tunnusta, jolla maksut vahvistetaan maksupäätteessä. Korteissa on myös mahdollista olla lähimaksuominaisuus, jolloin kortilla voi maksaa ilman tunnusluvun syöttämistä. Lähimaksua voi käyttää vain alle 50 euron kertaostoihin. Maksukortin tiedot voi liittää myös älypuhelimeen erilaisiin maksusovelluksiin, jolloin maksaminen onnistuu puhelimella ilman fyysistä korttia ja PIN-tunnuksen käyttöä. Maksukorteilla voi lisäksi tehdä verkko-ostoksia syöttämällä kortin numerosarjan, voimassaoloajan ja turvaluvun verkkokaupassa maksaessa. Verkossa maksaessa on tärkeää, että verkkokauppa on luotettava, jotta kortin tiedot eivät vaarannu. Pankkien asiakkaisiin kohdistuvissa huijausyrityksissä huijarit voivat monesti pyrkiä saamaan tietoonsa luotto- tai pankkikortin korttitiedot, jotta he voivat tehdä kortilla ostoksia. Korttien turvallisessa käsittelyssä on huomioitava, ettei kortin tietoja ja PIN-tunnusta luovuta ulkopuolisille tahoille (Nordea, n.d.b).

Maksukortit ovat aina henkilökohtaisia. Kortin haltijan on huomioitava, ettei kukaan muu saa korttia haltuun, tietoon kortin PIN-tunnusta tai muita korttitietoja. Kortteihin on mahdollista asettaa vuorokausikohtaisia ostorajoituksia, jotka on hyvä asettaa normaalin käytön mukaisesti. Ostorajat ovat tärkeä turvallisuustekijä, mikäli joku tuntematon henkilö saa kortin tiedot haltuunsa. Kortteihin on lisäksi mahdollista asettaa maa tai maanosa kohtaisia turvarajoja, jolloin kortin käyttö voidaan esimerkiksi sallia vain Suomessa (Nordea, n.d.c).

Mikäli pankin asiakkaan kortilla on tehty tapahtumia, joita asiakas ei tunnista tai asiakas epäilee, että korttitiedot ovat vaarantuneet, niin tulee asiakkaan heti ilmoittaa asiasta pankilleen, jotta kortti voidaan sulkea. Tapahtumista, joita asiakas ei tunnista, tulee tehdä korttireklamaatio eli oikaisupyyntö, jotta tehdyt tapahtumat voidaan mahdollisesti palauttaa. Mikäli pankin asiakas kokee olevansa rikoksen uhri, ja kortti tai korttitiedot on varastettu häneltä, niin asiasta tulee myös tehdä rikosilmoitus poliisille. Mikäli kortilla on katevaraus mitä kortinhaltija ei tunnista, niin sen perusteella ei vielä voi tehdä korttireklamaatiota (Oma Säästöpankki, n.d.a).

Maksaminen

Pankkien asiakkailla on yleensä käytössä kaikki yleisimmät maksutavat, kun asiakkaalla on käytössään käyttötili ja verkkopankki. Verkkopankissa pankkien asiakkaat voivat maksaa laskuja ja tehdä tilisiirtoja. Tilisiirroissa käytetään laajalti nykyään kansainvälistä IBAN-muotoa. IBAN on lyhenne, joka muodostuu sanoista International Bank Account Number eli kansainvälinen tilinumero. IBAN-muotoinen tilinumero koostuu perinteisestä tilinumerosta, jonka eteen liitetään maakohtainen tunnus ja kaksi tarkistenumeroa. Suomessa maakohtainen tunnus on FI. IBAN-muotoista tilinumeroa on käytettävä, kun halutaan tehdä tilisiirto Suomen ulkopuolelle (OP, n.d.b).

Laskujen maksu ja tilisiirrot kotimaahan ja euroalueeseen kuuluviin valtioihin tapahtuu SEPA-maksuna. SEPA (Single Euro Payment Area) eli yhtenäinen euromaksualue on Euroopan pankkien yhteinen maksuliikenteen välitysalue (Alhonsuo ym., 2009, s. 223). SEPA-maksut ovat siis euroalueen sisällä

tehtäviä tilisiirtoja, joissa maksu siirtyy vastaanottajalle viimeistään seuraavana pankkipäivänä. SEPA-tilisiirrossa käytetään saajan tilinumeroa IBAN-muodossa ja saajan pankin BIC-koodia. SEPA-maksuista on mahdollista tehdä SEPA-pikasiirtoja, jolloin maksu välittyy saajalle sekunneissa (Säästöpankki, n.d.).

Pankki voi suorittaa ulkomaanmaksuja tai niitä voi tehdä myös pankkien verkkopankissa. Ulkomaanmaksun suorittamiseen maksuun täytyy merkitä tilinumero IBAN-muodossa sekä maksun saajan pankin BIC- tai SWIFT-koodi. BIC- ja SWIFT-koodi tarkoittavat samaa asiaa, mutta niitä kutsutaan joissakin maissa eri nimillä. Maksuun on lisäksi merkittävä summa ja maksun saavan pankin- sekä asiakkaan tiedot (Alhonsuo ym., 2009, s.198).

SEPA-suoraveloitus on maksutapa, jossa pankin asiakas antaa suostumuksen pankille ja laskuttavalle yritykselle veloittaa laskuja suoraan asiakkaan pankkitililtä. Suoraveloituksia tehdään usein toistuvista maksuista, kuten asunnon vastikkeen maksusta. Suoraveloitus on asiakkaan kannalta huoleton tapa hoitaa laskuja, sillä ne veloitetaan eräpäivänä ilman asiakkaan toimia. Pankkien välillä on eroja suoraveloitusten hinnoittelussa (Alhonsuo ym., 2009, s. 226).

Verkkopankissa pankkien asiakkaiden on mahdollista tehdä laskuistaan e-laskuja eli verkkolaskuja. Tällöin lasku ei tule asiakkaalle paperisena kotiin, vaan laskusta tehdään pankissa e-laskusopimus, jolloin lasku tulee näkyviin verkkopankkiin. E-laskusopimukseen voidaan määritellä, että veloitetaanko maksu suoraan pankkitililtä vai vaatiko se vahvistusta verkkopankissa. Paperilaskut ovat nykypäivänä monesti maksullisia, joten e-lasku on kätevä tapa saada maksut sähköisesti verkkoon (Alhonsuo ym., 2009, s.188).

Maksaminen onnistuu myös verkkomaksuna. Verkkomaksut ovat tapa tehdä ostoksia verkkokaupoissa. Verkkomaksuissa käytetään maksun hyväksymiseen verkkopankkitunnuksia, joilla asiakas tunnistautuu ja hyväksyy maksun veloituksen tililtään. Verkkomaksuissa on usein välissä kolmas osapuoli, joka

toimii palveluntarjoajana ja välittää maksun yritykselle, jonka verkkokaupassa ostos on tehty (Alhonsuo ym., 2009, s.190).

Laskujen maksua ja tilisiirtoja on mahdollista tehdä myös pankkien konttoreissa. Lisäksi osa pankeista tarjoaa asiakkaillensa maksupalvelua. Asiakas voi lähettää laskun tai tilisiirtolomakkeen pankin maksupalveluun, jossa lasku tai tilisiirto kirjataan pankin järjestelmään. Maksupalveluun lähetettävässä laskussa on oltava merkitty asiakkaan tili, jolta lasku maksetaan sekä asiakkaan allekirjoitus. Maksupalvelua hyödyntävät usein pankkien vanhempi asiakaskunta, mikäli heillä ei ole mahdollista käydä maksamassa laskuja pankin konttorissa tai heillä ei ole käytössään verkkopankkitunnuksia. Pankit veloittavat maksupalvelu toimeksiannoista usein palvelumaksuja (Alhonsuo ym., 2009, s. 191-192).

Verkkopankki

Verkkopankki on kaikilla pankeilla käytössä oleva palvelu. Verkkopankissa pankin asiakas näkee kokonaisvaltaisesti kaikki pankkipalvelunsa ja voi hoitaa pankkiasioitansa. Verkkopankissa voi muun muassa tarkastaa tilin saldon, tehdä tilisiirtoja, maksaa laskuja ja tarkastella sijoituksia sekä lainoja (Oma Säästöpankki Oyj, n.d.b). Eri pankkien verkkopankit eroavat toisistaan hieman ja niissä voi olla eri palveluita. Verkkopankkiin kirjaudutaan verkkopankkitunnuksilla, jotka koostuvat usein käyttäjätunnuksesta ja salasanasta tai PIN-koodista. Verkkopankkiin kirjautuminen vahvistetaan jollakin lisätunnisteella, kuten esimerkiksi avainlukulistasta kertakäyttöisellä koodilla, tekstiviestillä tai tunnistuslaitteella. Pankkien käyttämät nimet tunnuksista vaihtelevat. Lisäksi pankkien käytössä olevat lisätunnisteet myös vaihtelevat pankeittain. Verkkopankkitunnuksia käyttämällä voi tehdä ostoksia verkkokaupoissa. Suurimmalla osalla pankeista on käytössä myös pankin mobiilisovellus ja osalla myös jonkinlainen erillinen tunnistus- tai vahvistussovellus, jolla voi vahvistaa maksuja tai kirjautumisen verkkopankkiin. Mobiiliverkkopankissa voi olla vähemmän palveluita kuin verkkopankin selain versiossa. Mobiiliverkkopankkien ominaisuudet vaihtelevat myös pankkien välillä (Solla, 2017).

Pankkien asiakkaisiin kohdistuu nykypäivänä paljon huijausyrityksiä, joissa yritetään saada selville varsinkin pankin asiakkaan verkkopankkitunnuksia. Verkkopankkitunnukset ovat henkilökohtaiset ja niitä ei tule antaa kenellekään. Verkkopankkiin kirjautuessa on tärkeää olla varma, että kyseessä on pankin oma sivu. Verkko-ostoksia tehdessä kannattaa olla tarkkana, että verkkokauppa on luotettava, jotta siellä on turvallista tehdä ostoksia verkkopankkitunnuksilla. Verkkopankkitunnusten turvallisessa käytössä on hyvä muistaa, että oman pankin sivuille siirryttäessä kirjoittaa selaimen hakupalkkiin pankin nettisivujen osoitteen muodossa www.pankki.fi. Mikäli verkkopankkitunnukset päätyvät, jonkun muun tietoon niin pankin asiakkaan tulee olla välittömästi yhteydessä omaan pankkiin, jotta tunnukset voidaan lukita. Kaikkien pankkien käytössä on myös korttien ja verkkopankkitunnusten sulkupalvelu, johon voi soittaa ympäri vuorokauden. Sulkupalvelun puhelinnumero on +358 20 333. Mikäli pankin asiakkaalta saadaan kalastettua verkkopankkitunnukset, niin tunnukset tietoon saanut huijari voi tehdä asiakkaan tileiltä tilisiirtoja omille tileillensä, jotka ovat usein ulkomailla. Tällöin maksujen peruuttaminen ja estäminen ei välttämättä ole mahdollista. Mitä nopeammin tuntemattomat tilitapahtumat havaitaan, niin sitä paremmalla todennäköisyydellä pankki pystyy estämään ja palauttamaan maksun (Oma Säästöpankki Oyj, n.d.b).

3.3 Vahva sähköinen tunnistautuminen

Vahva sähköinen tunnistautuminen tarkoittaa sähköisesti henkilön identiteetin tunnistamista. Vahvaa sähköistä tunnistautumista käytetään tunnistautuessa erilaisiin sähköisiin palveluihin, kuten valtion sähköisiin palveluihin ja muihin asiointipalveluihin, joissa palveluntarjoajien on tunnistettava asiakas. Traficom liikenne- ja viestintäviraston kyberturvallisuuskeskus valvoo tunnistautumista tarjoavia palveluja. Valvontaa tehdään, jotta voidaan varmistaa tunnistuspalveluiden luotettavuutta ja tietoturvallisuutta. Vahvoja sähköisen tunnistautumisen palveluita ovat Suomessa pankkien verkkopankkitunnukset, puhelinoperaattoreiden mobiilivarmenteet ja vähemmän käytössä olevat Digi- ja väestöviraston kansalaisvarmenteet (Traficom, n.d.).

Pankkien verkkopankkitunnuksilla tunnistautuessa on riskinä, että sivut joihin pankkitunnukset syötetään ovat valesivustoja. Huijarit voivat luoda sivustoja, jotka esittävät ja näyttävät pankkien sivuilta. Huijarit voivat saada valesivulle syötetyt verkkopankkitunnukset haltuun ja tällöin kirjautua tunnuksilla verkkopankkiin. Verkkopankista he voivat kavaltaa pankin asiakkaan varat. Verkkopankkitunnuksilla sähköisesti tunnistautuessa eri asiointipalveluihin on tärkeää muistaa kirjoittaa sivuston osoite suoraan selaimen hakukenttään, sillä hakukoneilla haettaessa voi huomaamattaan avata valesivuston.

Vahvasti sähköisesti tunnistautuessa on mahdollista myös käyttää teleoperaattoreiden tarjoamaa mobiilivarmennetta. Mobiilivarmenne on matkapuhelimissa toimiva tunnistautumisväline, joka on liitetty SIM-korttiin ja puhelinnumeroon. Mobiilivarmenne perustuu kaksivaiheiseen tunnistamiseen, jossa tunnistus tapahtuu PIN-koodilla ja puhelimen SIM-kortilla. Mobiilivarmenteen etuna on se, että mikäli sitä käyttää huijaussivustolla, niin verkkopankkitunnukset ja henkilön varat eivät tällöin vaarannu. Mobiilivarmennetta suositellaan käytettävän sähköiseen asiointiin ja verkkopankkitunnuksia käytettävän vain kirjautuessa pankkien sivustoille (Mobiilivarmenne, n.d.).

Digi- ja väestöviraston myöntämä kansalaisvarmenne on vähemmän käytössä oleva vahva sähköisen tunnistautumisen väline. Digi- ja väestövirasto myöntää varmennekortteja ja varmenteita kansalaisille, sosiaali- ja terveydenhuollolle sekä organisaatioille. Kansalaisvarmenteita käytetään pääasiassa erilaisten dokumenttien sähköiseen allekirjoittamiseen (DVV, n.d.).

4 PANKKIHUIJAUKSET

Pankkien palveluiden käyttöön kohdistuu paljon riskejä väärinkäytöksiin ja nykypäivänä pankkien asiakkaisiin kohdistuu valitettavan paljon huijausyrityksiä. Pankkihuijauksissa huijarit voivat lähestyä pankin asiakasta monesta eri kanavasta, kuten esimerkiksi puhelimitse, sähköpostitse, sosiaalisessa mediassa

ja muissa viestintäkanavissa. Pankkihuijauksille tyypillistä on, että ne vaikuttavat liian hyvältä ollakseen totta tai niissä pyydetään toimimaan nopeasti. Pankkihuijauksissa huijarit yrittävät yleensä saada tietoonsa ihmisten pankkitunnuksia tai maksukorttien tietoja. Huijarit käyttävät psykologisia keinoja saadakseen ihmisen luottamuksen, jotta he esimerkiksi siirtäisivät rahaa huijarille. Tässä kappaleessa käydään läpi yleisimmät pankkihuijauskeinot, joita ovat hakukonehuijaus, huijauspuhelu, rakkaushuijaus, sijoitushuijaus ja tietojenkalastelu. Näistä huijaustyypeistä voidaan käyttää erilaisia nimityksiä. (Finanssivalvonta, 2024). Luvun lopussa käydään läpi pankkihuijauksista aiheutuvia seuraamuksia.

4.1 Hakukonehuijaus

Hakukonehuijauksessa tyypillistä on, että haettaessa jollain hakukoneella, esimerkiksi Google tai Bing, hakutulosten joukossa voi esiintyä valesivustoja, jotka näyttävät ja vaikuttavat oikeilta sivustoilta. Huijarit luovat valesivustoja, jotka näyttävät usein esimerkiksi pankkien, Kelan, Omakannan, verottajan tai poliisin sivuilta. Myös erilaisista verkkokaupoista tai kaupankäyntisivustoista, kuten tori.fi esiintyy huijaussivustoja. Huijarit pyrkivät saamaan nämä valesivustot näkyviin hakutuloksiin, kun tietyllä hakukoneella haetaan oikeaa sivustoa. Tällöin ihmiset voivat huomaamattaan siirtyä huijaussivustolle ja täten esimerkiksi pankin sivulta näyttävän valesivuston kautta huijari saa tietoon pankkitunnukset. Hakukonehuijauksia voi välttää kirjoittamalla aina selaimen osoitekenttään haluamansa sivuston koko osoite esimerkiksi www.vero.fi. Mikäli tunnistaudut pankkisi sivulle, niin on hyvä varmistaa aina tunnistautuessasi pankin tunnistussovelluksella, että mitä tapahtumaa olet vahvistamassa (Nordea Oyj, n.d.d).

Valeverkkokauppoihin voi päätyä huomaamattaan hakukonehuijauksen kautta. Verkkokauppa huijaussivustot voivat vaikuttaa aivan samanlaisilta, kuin oikeat sivustot. Huijaussivustoissa voi kuitenkin havaita usein kielioppivirheitä tai muuten tökeröä suomen kieltä, mikäli sivustot on luotu käyttäen kääntäjää. Tällaiset virheet sivustoissa voivat paljastaa sivuston valesivustoksi.

Verkkokauppahuijauksissa huijauksen uhrit usein syöttävät sivustolle maksukorttiensa tiedot tai verkkopankkitunnuksensa. Verkkokauppahuijauksessa ostetusta tuotteesta veloitetaan, mutta maksusta ei ikinä tule vahvistusta ja tuotetta ei ikinä saada. Vaihtoehtoisesti huijaussivusto voi tehdä maksun yhteydessä pienen alkuveloituksen, jonka myötä maksaja hyväksyy palveluntarjoajan ehdot ja kortilta voi alkaa menemään esimerkiksi kuukausittainen veloitus, joista voi olla vaikea päästä eroon (Nordea Oyj, n.d.d).

4.2 Huijauspuhelu

Huijauspuhelu huijaus eli ”vishing” tarkoittaa huijausta, jossa huijari lähestyy esimerkiksi pankin asiakasta väärentämällä puheluita. Huijari voi esittäytyä pankin työntekijänä tai viranomaistahona. Puheluissa huijarit pyrkivät saamaan tietoonsa pankin asiakkaan pankkitunnukset, muita henkilökohtaisia tietoja tai pyytävät siirtämään rahaa huijarin tilille. Yleisimpiä menetelmiä huijauspuheluissa on turvatilihuijaus. Tällaisessa huijauksessa huijari esittäytyy pankin työntekijänä tai viranomaisena ja kertoo, että huijauksen uhrin tili tai pankkitunnukset ovat vaarantuneet. Huijari pyytää tällöin toimimaan nopeasti ja siirtämään uhrin tililtä varat niin sanotulle ”turvatilille”, joka on kuitenkin huijarin tili. Huijauspuhelussa huijari voi esittäytyä myös jonkun yrityksen, kuten esimerkiksi Microsoftin tai Applen asiakaspalveluna. Tällöin puhelussa huijari pyytää paljastamaan palveluiden käyttäjätunnuksen ja salasanan. Huijauspuheluita havaittaessa on hyvä muistaa, että pankit eivät ikinä kysy asiakkailtaan puhelimitse verkkopankkitunnuksia tai muitakaan arkaluontoisia tietoja (Danske Bank, n.d.).

4.3 Rakkaushuijaus

Rakkaushuijaus tai rakkauspetos on huijaus, jossa huijari lähestyy uhriaan usein sosiaalisen median kautta tai seurustelupalstoilla. Huijarit ovat usein taitavia manipuloimaan ihmisiä ja käyttävät psykologisia keinoja luottamuksen rakentamiseen. Rakkaushuijauksessa uhri rakastuu tai ihastuu viestittelemänsä henkilön kanssa. Viestittelijänä on kuitenkin huijari, joka pyrkii

rakentamaan luottamuksen uhrin kanssa ja pyytää tätä lähettämään tilisiirtona rahaa. Rakkaushuijauksissa on hankalaa tunnistaa, että onko tutustumassa oikeaan ihmiseen vai huijariin. Rakkaushuijauksissa huijari kertoo usein olevan varakas ja haluaa yhteisen tulevaisuuden uhrin kanssa. Huijarit kuitenkin asuvat usein ulkomailla ja eivät syystä tai toisesta pysty videokeskusteluun. Rakkaushuijauksessa huijari usein myös pyytää uhria lähettämään hänelle rahaa kertomalla, että tarvitsee sitä sairaalakuluihin, läheisen kuolemaan, lentolippuihin tai muuhun äkilliseen hätään. Kun uhri haluaa tavata huijarin, niin tapaamisen estämiseksi huijari esittää aina erilaisia syitä. Rakkaushuijaukset ovat usein pitkäkestoisia ja huijari pyytää useaan eri tarpeeseen rahaa. Rikosten uhrit eivät usein heti havaitse joutuneensa rikoksen uhriksi, sillä he ovat rakastuneet huijariin (Poliisi, n.d.). Rakkaushuijausten määrä on laskenut vuodesta 2023 verrattuna 2024 vuoteen. Muut huijaustavat ovat kuitenkin yleistyneet (Finanssiala ry, 17.09.2024).

4.4 Sijoitushuijaus

Sijoitushuijaukset ovat huijauksia, joissa uhria lähestytään tarjoamalla mahdollisuutta sijoittaa varojaan esimerkiksi virtuaalivaluuttahuijauksiin tai käymään kauppaa kaupankäyntihuijaussivustoilla. Sijoitushuijauksissa voidaan tarjota mahdollisuutta moninkertaistamaan sijoitetut rahat. Sijoitushuijaukset kuulostavat usein todella houkuttelevilta. Sijoitushuijauksissa rahaa sijoittanut henkilö voi huomata tulleensa huijatuksi usein vasta, kun hän haluaa nostaa sijoituksensa pois, eikä se jostain syystä onnistukkaan. Sijoitushuijari voi tällöin pyytää asiakasta maksamaan hänelle jonkin ”provision” sijoitettujen varojen tuotosta ennen kuin varat voidaan nostaa. Huijari ei kuitenkaan maksa varoja milloinkaan takaisin ja tällöin uhri voi siirtää rahaa huijarille useaan kertaan siinä toivossa, että saa varansa takaisin. Huijarit voivat lisäksi myöhemmin lähestyä uhriaan esittäytymällä erilaisina viranomaisina tai muun luotettavan tahon nimissä, joka tarjoaa apua sijoitushuijauksessa menetettyjen varojen takaisin saamisessa. Tällaisten palveluiden tarjoaminen on kuitenkin usein myös huijaus, jolloin uhri voi joutua uudelleen huijatuksi ja jälleen siirtää huijarille varoja. (FINE, 2024). Sijoitushuijaukset ovat olleet vuonna 2023 ja 2024

toiseksi yleisin huijauskeino, jolla rikolliset ovat saaneet pankkien asiakkailta huijattua varoja. Huijausten määrä on ollut kasvussa viimevuosina (Finanssiala ry, 17.09.2024).

4.5 Tietojenkalastelu

Tietojenkalastelu eli ”phishing” on rikollisten toimintaa, jossa huijarit yrittävät saada tietoonsa ihmisten verkkopankkitunnuksia, maksukorttien tietoja tai henkilötietoja laittomaan tarkoitukseen. Tietojenkalastelussa huijarit lähestyvät usein uhrejaan tekstiviestitse, puhelimitse tai sähköpostitse. Nämä huijausviestit näyttävät usein pankkien, viranomaisten, postin tai muiden tahojen lähettämiltä viesteiltä. Viesteissä voidaan pyytää toimimaan välittömästi kirjautumalla viestissä olevan linkin kautta huijaussivustolle verkkopankkitunnuksilla. Viestissä, joka voi näyttää pankin viestiltä, voidaan kertoa, että pankkitili on vaarantunut tai siinä voidaan uhata tilin lopetuksella. Huijausviestin linkkiä klikkaamalla avautuu pankin sivulta näyttävä huijaussivusto, jossa pyydetään kirjautumaan verkkopankkitunnuksilla. Tällöin huijari saa tietoonsa verkkopankkitunnukset ja voi siirtää pankin asiakkaan kaikki varat omille tileilleen (Poliisi, n.d.).

Tietojenkalastelua tapahtuu nykypäivänä todella paljon internetissä. Tietojenkalastelulta suojautumisessa on hyvä muistaa, että epäilyttäviä linkkejä ja tiedostoja ei kannata avata. Eri palveluissa on hyvä käyttää vahvoja ja pitkiä salasanoja ja samaa salasanaa ei tulisi käyttää monessa palvelussa. Mikäli saat sähköpostiviestin jonkun yrityksen nimissä, niin kannattaa tarkistaa viestin lähettäjän tiedot ja osoite, josta viesti on lähetetty. Älä anna kenellekään verkkopankkitunnuksiasi tai muita henkilökohtaisia tietoja viestin välityksellä. Pankit eivät esimerkiksi ikinä kysy verkkopankkitunnuksia tekstiviestien tai sähköpostin välityksellä. Käytä aina kaksivaiheista tunnistautumista, kun se on mahdollista. Kaksivaiheinen tunnistautuminen, jossa kirjautuminen vahvistetaan esimerkiksi vielä tekstiviestillä lähetettävällä tunnuksella, vahvistaa turvallista asiointia erilaisissa palveluissa. Jos jokin tarjous tai viesti kuulostaa liian hyvältä ollakseen totta, niin se on useimmiten huijaus (Rikosuhripäivystys, n.d.).

Tietojenkalastelun kautta rikolliset voivat saada pankkitunnusten lisäksi tietoonsa myös henkilötietoja, kuten henkilötunnuksen tai osoitetietoja. Tällaisia tietoja hyödyntämällä rikolliset voivat tehdä identiteettivarkauksia. Identiteettivarkaus tarkoittaa toimintaa, jossa rikollinen on saanut tietoon johonkin henkilöön yhdistettäviä tietoja, joita rikollinen käyttää rikolliseen tarkoitukseen. Identiteettivarkaudesta aiheutuu uhrille usein taloudellista vahinkoa. Identiteettivaras voi esimerkiksi tilata uhrinsa nimissä tuotteita tai palveluja. Identiteettivarkauksissa rikollinen voi esittäytyä jonain muuna tahona, joka kysyy henkilötietoja. Identiteettivarkauksilta suojautuessa kannattaakin siis muistaa, että henkilötietoja ei tule ikinä luovuttaa kenellekään, mikäli ei ole aivan varma tietojen vastaanottajasta (Poliisi, n.d.).

Sosiaalisessa mediassa, kuten Facebookissa, WhatsAppissa ja Instagramissa esiintyy myös huijauksia. Tällaisissa huijauksissa rikollinen esittäytyy usein uhrin jonain tuttuna ystävänä ja lähestyy näin uhriaan. Rikollinen voi kertoa uhrille esimerkiksi arvonta voitosta, jonka haluaa jakaa uhrin kanssa. Tällöin rikollinen voi pyytää esimerkiksi uhrin pankkitunnuksia, korttitietoja tai henkilötietoja, jotta voi jakaa voiton. Rikollinen kuitenkin yrittää ystävän nimissä saada vain kalastettua tietoja ja huijata uhrilta rahaa. Sosiaalisen median huijauksissa rikolliset voivat yrittää myös kaapata sosiaalisen median tilejä (FINE, 2024).

Finanssiala ry:n (17.09.2024) pankeilta kerätyn tiedon mukaan tietojenkalastelu on 2024 alkuvuoden tammi-kesäkuussa tapahtuneista huijauksista yleisimpiä. Tietojenkalastelulla rikollisten saamat varat ovat 2024 alkuvuoden aika yli kaksinkertaistuneet verrattuna samaan ajanjaksoon alkuvuodesta 2023. Tietojenkalastelu pankkihuijauksien keinona on siis valtavasti kasvussa.

4.6 Pankkihuijausten seuraukset

Pankin asiakas, joka joutuu pankkihuijauksen tai tietojenkalastelun uhriksi, on rikoksen uhri. Vaikka huijaustapaus on rikosoikeudellinen niin se ei suoraan tarkoita, että pankki olisi vastuussa asiakkaan huijauksessa menettämistä

varoista. Ensisijaisesti vastuussa on rikoksentekijä. Pankkihuijauksista pankin asiakkaan tulee ilmoittaa tapahtuneesta pankille ja tehdä rikosilmoitus poliisille. Osa pankkihuijauksista pystytään estämään pankin toimesta (FINE, 2024).

Finanssi ry:n (17.09.2024) pankeilta keräämän tiedon mukaan vuoden 2024 tammi-kesäkuussa pankit saivat pysäytettyä ja palautettua huijauksiin liittyviä maksuja 18,2 miljoonaa euroa. Samana aikavälinä pankkien asiakkaat menettivät rikollisille 27,5 miljoonaa euroa. Pankit siis pystyivät estämään noin kolmasosan maksuista, mutta kuitenkin suurinta osaa ei ole voitu estää.

Suurimmassa osassa huijaustapauksissa rikoksen tekijää ei saada siis kiinni. Tällöin pankin ja sen asiakkaan välinen vastuu menetetyistä varoista määräytyy pankin ja asiakkaan välisten sopimusehtojen ja maksupalvelulain mukaan (FINE, 2024). Asiakkaiden vastuu viimevuosina huijauksissa on ollut todella suuri. Suomen pankin mukaan pankit hyvittivät vuonna 2023 ainoastaan 4 % oikeudettomista tilisiirroista ja pankkien asiakkaiden vastuulle jäi 92 % (Yle, 18.11.2024).

Palveluntarjoajan eli pankin ja maksupalvelun käyttäjän eli asiakkaan välisestä vastuunjaosta säädetään maksupalvelulain (290/2010) 62 §:ssä. Mikäli maksupalvelun käyttäjä on luovuttanut maksuvälineen jollekin oikeudettomalle, huolehtinut siitä huolimattomasti tai jättänyt ilmoittamasta maksuvälineen katoamisesta tai vaarantumisesta palveluntarjoajalle, niin tällöin pankin asiakkaan vastuu on enintään 50 euroa. Tämä ei kuitenkaan päde, mikäli pankin asiakas on toiminut törkeän huolimattomasti tai tahallaan (FINE, 2024).

Suurimmassa osassa pankkihuijaustapauksissa pohditaan, että onko pankin asiakas toiminut törkeän huolimattomasti. Mikäli asiakas on toiminut vain huolimattomasti, niin hänen osuutensa hävityistä varoista on vain 50 euroa ja pankin on korvattava loput. Mikäli taas asiakkaan todetaan toimineen törkeän huolimattomasti, niin asiakas on itse vastuussa huijauksessa hävityistä varoista ja pankki ei ole lainkaan korvausvelvollinen. Suurimmassa osassa huijaustapauksissa pankit toteavat asiakkaansa toimineen törkeä huolimattomasti

käyttäessään pankkitunnuksiaan tai pankkikorttia, joten pankit eivät joudu korvausvelvolliseksi. Törkeän huolimattomuuden määritelmää voi tulkita laissa eri tavoin. Sitä tarkastellaankin tapauskohtaisesti esimerkiksi oikeuteen viedyissä tapauksissa (FINE, 2024). Viime vuosina osa huijauksen kohteeksi joutuneista pankkien asiakkaista ovat haastaneet pankkinsa oikeuteen, koska vastuu menetetyistä varoista on jäänyt asiakkaalle. Asiakkaat ovat kokeneet, että vastuu menetetyistä varoista on ollut pankilla.

Esimerkki pankkihuijaukseen liittyvästä oikeustapauksesta

Honkajoen Osuuspankin asiakkaana oleva pariskunta joutui vuonna 2021 Omakanta-huijauksen uhriksi. Pariskunta menetti verkkopankkihuijauksessa tileiltään noin 45 000 euroa. Pankin asiakas oli halunnut kirjautua Omakantaan tarkastellakseen terveystietojaan. Hän erehtyi kuitenkin klikkaamaan itsensä Omakannan sivua esittäneelle valesivustolle. Pankin asiakas syötti valesivustolle verkkopankkitunnuksensa ja aktivointitunnuksen, jonka myötä rikollinen sai asennettua pankin sovelluksen asiakkaan nimissä. Tämän jälkeen huijari teki tilisiirtoja pariskunnan tileiltä. Pankki sai estettyä osan siirroista, mutta huijari sai vietyä yli 25 000 euroa pariskunnalta. Pariskunta koki, että pankki on velvollinen hyvittämään hävinneet varat. Pankki oli kuitenkin asiasta eri mieltä, jonka vuoksi pariskunta vei tapauksen Satakunnan käräjäoikeuteen. Käräjäoikeus päätti, että pariskunta ei ole toiminut tapauksessa vakavan piittaamattomasti, jonka vuoksi he eivät toimineet törkeän huolimattomasti. Käräjäoikeus siis päätti, että Honkajoen Osuuspankki on velvollinen korvaamaan asiakkailleen hävityt varat. Pankki valitti tapauksesta Vaasan hovioikeuteen. Hovioikeus taas päätti, että pariskunta on toiminut törkeän huolimattomasti ja he ovat itse vastuussa huijatuista varoista. Päätös perusteltiin sillä, että kun huijari oli saanut asiakkaan verkkopankkitunnukset, niin hän oli ottanut pankin mobiilisovelluksen käyttöön. Mobiilisovelluksen aktivoinnista oli lähtenyt pankin asiakkaalle tekstiviesti pankin nimissä, jossa luki, että asiakas on aktivoimassa pankin mobiilisovellusta. Hovioikeuden mukaan pankin asiakkaan olisi pitänyt havaita viestistä, että mobiilisovelluksen aktivointi ei voi liittyä Omakantaan kirjautumiseen. Pankin asiakkailta huijauksessa viedyt yli 25 000 euroa jäivät siis

pariskunnan omaksi vastuuksi eikä pankki ole korvausvelvollinen (Edilex, 23.09.2024).

Monet päätökset korvausvelvollisuudesta erilaisissa pankkihuijauksiin liittyvistä oikeustapauksista ovat jääneet pankkien asiakkaille. Tapauksia, joissa pankin asiakas on voittanut oikeudenkäynnin, löytyy kuitenkin myös muutamia. Pankkihuijauksen uhriksi joutuminen voi siis aiheuttaa monesti pankin asiakkaalle suuriakin taloudellisia tappioita ja psyykkistä vahinkoa.

5 TUTKIMUKSEN TOTEUTUS

5.1 Tutkimusmenetelmä

Empiirinen tutkimus on tutkimus, joka perustuu tutkittavan kohteen mittaamiseen, havainnointiin ja analysointiin. Empiiriset tutkimukset voidaan jakaa kahteen eri tyyppiin tutkimusmenetelmän mukaan. Nämä kaksi tutkimusmenetelmää ovat kvalitatiivinen eli laadullinen ja kvantitatiivinen eli määrällinen tutkimus. Laadullisessa tutkimuksessa pyritään ymmärtämään tutkittavaa ilmiötä ja selvittämään syvällisempiä syitä ilmiölle. Laadullisessa tutkimuksessa tutkimusaineistoa kerätään yleensä erilaisilla henkilö- tai ryhmähaastatteluilla. Laadullisen tutkimuksen otanta on usein pieni. Määrällisessä tutkimuksessa taas selvitetään lukumääräisesti tutkittavat ilmiön laajuutta suuremmalla otannalla. Määrällisessä tutkimuksessa kerätään yleensä aineistoa erilaisilla kyselyillä (Heikkilä, 2014, s.12–15).

Tässä tutkimuksessa käytetään kvantitatiivista eli määrällistä tutkimusmenetelmää. Tätä tutkimusmenetelmää voidaan kutsua myös tilastolliseksi tutkimukseksi. Määrällisessä tutkimuksessa tutkimusdataa kerätään usein strukturoidulla kyselytutkimuksella, jossa on etukäteen määritellyt kysymykset, jotka ovat samat kaikille kyselyyn vastaajille. Kyselyssä on usein valmiit vastausvaihtoehdot. Määrällisessä tutkimusmenetelmässä otannan on oltava riittävä,

jotta tutkimustuloksia voidaan yleistää tai analysoida vastausten ja asioiden välisiä riippuvuuksia. Määrällisen tutkimusmenetelmän avulla voidaan selvittää määrällisesti ja numeerisesti eri tutkimustuloksia ja analysoida niitä käyttäen taulukoita ja kuvioita. Määrällisen tutkimuksen avulla saadaan kartoitettua olemassa oleva tilanne, mutta syvällisempiä syitä asioille ei usein saada (Heikkilä, 2014, s.16).

Tämän opinnäytetyön tutkimukseen on valittu määrällinen tutkimusmenetelmä, koska tutkimuksessa halutaan selvittää määrällisesti, kuinka paljon opiskelijoihin on kohdistunut huijauksia tai huijausyrityksiä. Määrällisellä tutkimuksella saadaan kartoitettua lukumäärältään enemmän opiskelijoiden kokemuksia ja tietämystä aiheesta, sillä määrällisessä tutkimuksessa otanta on laajempi kuin laadullisessa tutkimuksessa. Laajemman otannan pohjalta saadaan käsitys pankkihuijausten ja huijausyritysten laajuudesta opiskelijoiden keskuudessa.

5.2 Tutkimuksen toteuttaminen ja kyselylomake

Tämän opinnäytetyön aineistonkeruumenetelmäksi on valittu sähköinen internet kysely. Kyselytutkimus on yleisin määrällisessä tutkimuksessa käytetty aineistonkeruumenetelmä. Sähköisen kyselyn etuna on, että sen avulla voidaan saada laaja otanta, sillä se voidaan lähettää esimerkiksi sähköpostilla tutkimuksen kohderyhmälle. Kyselytutkimuksen ongelmana voi olla, että vastausprosentti jää alhaiseksi, jolloin tutkimuksen otanta voi jäädä liian pieneksi (Heikkilä, 2014, s.17). Kysely sopii paremmin tämän opinnäytetyön tutkimuksen tutkimusmenetelmäksi kuin haastattelut, sillä kyselyn avulla saadaan enemmän otantaa ja aineistonkeruu vie vähemmän aikaa. Tutkimuksen aineiston keruuseen valittiin sähköinen strukturoitu kyselylomake, koska tutkimuksen kohderyhmän jäsenillä on kaikilla käytettävissä oppilaitoksen sähköposti, johon kyselylomake voidaan lähettää. Sähköinen kyselytutkimus on myös helppo ja nopea toteuttaa ja sopii siksi tähän tutkimukseen, sillä tutkimuksen aikataulu sekä budjetti on rajallinen. Strukturoidussa kyselylomakkeessa kysymykset ja vastausvaihtoehdot ovat ennalta määriteltyjä, jolloin tutkimuksen

tuloksia voidaan vertailla paremmin. Strukturoitu kysely sopiikin tulosten vertailukelpoisuuden vuoksi hyvin tähän tutkimukseen.

Opinnäytetyön tutkimuksellinen osa on toteutettu kyselytutkimuksena Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkielisille päiväopiskelijoille. Kohderyhmän ulkopuolelle rajataan englanninkieliset opiskelijat ja tutkintolinjat, jotta kohderyhmä ei ole liian suuri ja kyselytutkimus on helpompi toteuttaa. Kohderyhmäksi valikoitui Satakunnan ammattikorkeakoulun opiskelijat, koska kohderyhmältä saadaan tutkimusdataa helposti sähköisen kyselyn avulla. Tutkimuksen yhtenä kohderyhmävaihtoehtona oli vanhemmat ihmiset ja vanhukset. Vanhempiin ihmisiin kohdistuvia pankkihuijauksia olisi ollut myös mielenkiintoista tutkia, sillä voisi olettaa, että heihin kohdistuu paljon huijauksia, sillä heillä ei ole usein niin hyvät digitaidot kuin nuorilla. Vanhemmilta ihmisitä olisi kuitenkin ollut todennäköisesti vaikeampi saada tutkimusdataa, sillä sähköisellä kyselylomakkeella heiltä ei välttämättä olisi saatu riittävästi vastauksia. Tämän vuoksi kohderyhmäksi valikoitui opiskelijat.

Kyselytutkimuksessa selvitetään kohderyhmän opiskelijoiden tietoisuuden tasoa pankkihuijauksista ja turvallisesta pankkiasioinnista. Lisäksi selvitetään, kuinka paljon opiskelijoihin on kohdistunut huijauksia tai huijausyrityksiä. Tutkimuksessa myös selvitetään, miten ja mistä nuoret opiskelijat haluaisivat saada lisätietoa pankkihuijauksista. Tutkimustiedon perusteella tehdään selvitys, mikä on Satakunnan ammattikorkeakoulun opiskelijoiden tietämyksen taso pankkihuijauksista ja miten niitä on heihin kohdistunut. Kyselytutkimuksessa ei kerätä henkilötietoja ja kyselyyn vastaaminen on täysin vapaaehtoista. Kyselytutkimuksen tulokset käsitellään asianmukaisesti ja hävitetään tutkimuksen jälkeen. Kyselytutkimuksen toteuttamiseen ja lähettämiseen Satakunnan ammattikorkeakoulun opiskelijoille haettiin tutkimuslupa Satakunnan ammattikorkeakoululta.

Kysely toteutettiin Microsoft Forms -kyselylomakkeella, sillä se on helppokäyttöinen ohjelma kyselylomakkeen tekemiseen. Forms -kyselylomakkeen avulla saadaan myös kerättyä helposti tutkimusdataa, joka voidaan suoraan viedä Microsoft Exceliin, jossa aineistosta voidaan luoda erilaisia taulukoita ja

kuvioita, joilla voidaan havainnollistaa tutkimuksen tuloksia. Kyselylomakkeen laatimisessa käytettiin apuna tekoälyä kysymysten ideointiin ja vastausvaihtoehtojen luontiin.

Kyselylomake (Liite 2) lähetettiin Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkielisille päiväopiskelijoille sähköpostilla saatekirjeen (Liite 1) kanssa 13.01.2025. Kyselyyn oli aikaa vastata 20.01.2025 saakka. Kyselylomakkeeseen vastaaminen tapahtui anonyymisti ja vastaaminen oli täysin vapaaehtoista. Kyselylomakkeen aukioloajaksi valittiin yksi viikko, jotta mahdollisimman moni opiskelija ehtii vastata kyselyyn, mutta tutkimuksen aikataulu ei kuitenkaan veny liian pitkäksi. Kyselyn vastausajan sulkeuduttua aloitettiin tutkimustulosten käsittely ja analysointi.

Kyselylomakkeeseen valittiin kysymyksiä, joihin vastataan eri vastausvaihtoehtojen perusteella. Osassa kysymyksistä on mahdollisuus valita useampi vaihtoehto ja osassa taas vain yksi. Kysymyksiin haluttiin strukturoituja kysymyksiä, joissa vastataan vaihtoehtojen mukaan, jotta kyselyn kysymyksien avulla saadut tuloksia voidaan vertailla ja esittää erilaisin kuvioin tutkimuksen tulosten käsittelyvaiheessa. Kyselylomakkeessa käytettiin myös muutamia avoimia kysymyskenttiä, mikäli vastaajilla on mielessä jokin muu vastausvaihtoehto.

Kyselylomakkeen (Liite 2) kolme ensimmäistä kysymystä keräsivät tietoa vastaajien taustasta. Kysymyksissä kysyttiin ikää, sukupuolta ja opiskelualaa. Kysymyksessä viisi ja kuusi pyydettiin vastaajia arvioimaan oman tietämyksen tasoa liittyen pankkihuijauksiin ja turvalliseen pankkiasiointiin. Seuraavassa kysymyksessä kysyttiin, mitkä eri pankkihuijaustavoista ovat vastaajille tuttuja. Kysymyksissä 7–9 kysyttiin, kokevatko vastaajat, että pankkihuijauksista ja turvallisesta pankkiasioinnista on tarpeeksi tietoa saatavilla ja mistä sekä miten he haluaisivat saada lisätietoa. Seuraavissa kolmessa kysymyksessä testattiin vastaajien tietämystä pankkihuijauksista ja turvallisesta pankkiasioinnista. Ensimmäisen osan viimeisenä kysymyksenä tiedusteltiin, mikäli vastaajat ovat joutuneet pankkihuijauksen uhriksi tai onko heihin kohdistunut huijausyrityksiä. Mikäli vastaaja valitsi, että hän on joutunut huijatuksi, niin hän siirtyi

lisäkysymyksiin, joilla kysyttiin tarkemmin tietoa huijauksesta. Jos taas vastaaja vastasi, että häneen on kohdistunut huijausyritys, niin hän siirtyi huijausyrityksestä tiedusteleviin kysymyksiin. Jos vastaajaan ei ole kohdistunut kumpaakaan, niin hän siirtyi viimeiseen osaan. Viimeisessä osassa oli avoin kysymyskenttä, jossa voi kertoa muita ajatuksia tai kokemuksia aiheeseen liittyen.

5.3 Tutkimuksen reliabiliteetti ja validiteetti

Tutkimuksien tekemisessä on pyrittävä miettimään tutkimuksen luotettavuutta ja pätevyyttä. Kaikkien tutkimuksien tekijöiden pitäisi pyrkiä välttämään virheitä, mutta niitä voi vääjäämättä syntyä tutkimuksen tekemisen aikana. Tutkimuksen luotettavuutta voidaan arvioida reliabiliteetin ja validiteetin kautta. Tutkimuksen reliabiliteetti tarkoittaa tutkimuksen tulosten toistettavuutta. Se tarkoittaa siis, että jos joku muu henkilö tekisi saman tutkimuksen, niin päätyisikö hän myös samaan tulokseen. Reliabiliteetti tarkoittaa siis tutkimuksen kykyä antaa luotettavia ja ei sattumanvaraisia tuloksia. Tutkimuksen validiteetti eli pätevyys tarkoittaa, että tutkimus mittaa sitä asiaa, jota on tarkoitus mitata. Tutkimuksen kyselylomakkeessa voidaan kysyä erilaisia kysymyksiä tutkimusongelmaan liittyen, mutta tutkimuksen tekijä on voinut tehdä kysymykset esimerkiksi liian monitulkintaisiksi, jolloin vastaajat voivat vastata eri kysymykseen kuin mitä tutkija on ajatellut. Tällöin tutkimus ei ole pätevä, sillä tutkimuksen kyky mitata haluttua asiaa ei toteudu (Hirsjärvi, 2007, s.226).

Tässä tutkimuksessa on pyritty toimimaan hyvä tieteellisen käytännön mukaan. Tutkimuksen luotettavuutta on mietitty tutkimusta tehdessä ja tehty ratkaisuja, jotka tukevat tutkimuksen toistettavuutta. Tutkimuksen kyselyn kysymysten laadintaan on käytetty aikaa ja kysymykset on pyritty asettelemaan niin, että ne ovat selkeästi ymmärrettävissä. Kyselylomake on lähetetty enne aineistonkeruuta läheisille ja ystäville, jotta he voivat tarkastaa, että tutkimuksen kysymykset ovat selkeitä sekä helposti ymmärrettäviä. Tutkimuksen kyselyyn vastasi 59 henkilöä, joten tutkimusotanta jäi hieman pieneksi. Tutkimusotannan matala määrä on otettu huomioon tutkimuksen tuloksia analysoidessa. Tutkimuksen teossa on myös mietitty eettisiä kysymyksiä.

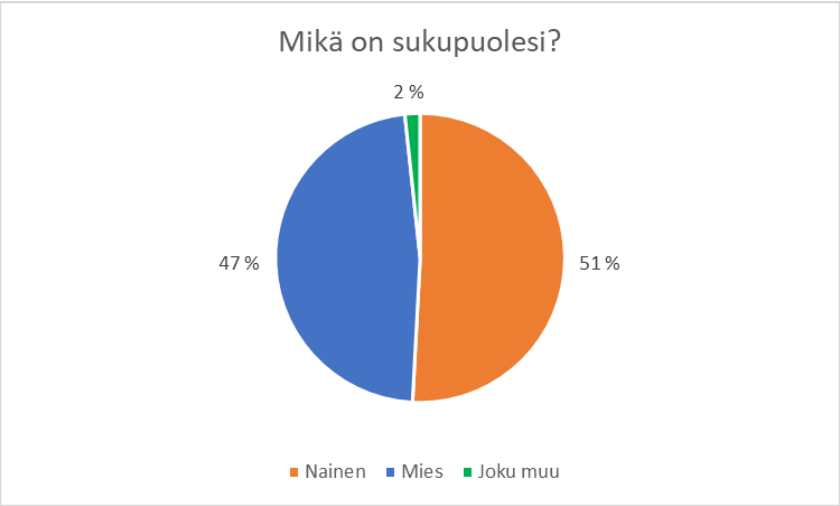
Esimerkiksi tutkimuksen kyselyssä ei kerätä vastaajien henkilötietoja, joilla heidät voitaisiin tunnistaa. Kyselyssä kerätään vain tutkimuksen kannalta oleellisia tietoja ja kyselyyn vastaaminen on vapaaehtoista. Kyselytutkimuksen vastaukset hävitetään asianmukaisesti, kun tutkimustulokset on käsitelty. Tutkimuksen kyselylomake lähetettiin sähköisesti sähköpostilla kohderyhmälle saateviestin kanssa. Saateviestissä kerrottiin tutkimuksen aihe ja, että kyselyyn vastaaminen tapahtuu anonyymisti ja vastaaminen on vapaaehtoista. Lisäksi saateviestissä tuotiin esille, että kyselyn vastaukset hävitetään tutkimuksen valmistuttua. Tutkimuksen aiheen vuoksi tutkimuksessa on käytetty paljon verkkolähteitä, sillä aiheesta ei löydy paljon kirjallisuutta. Tutkimuksen tiedonhankinnassa on kuitenkin pyritty käyttämään lähteenä luotettavia tahoja.

6 TUTKIMUSTULOKSET

Tässä luvussa käydään läpi sähköisen kyselylomakkeen avulla saatu tutkimusaineisto ja tutkimustulokset. Tulokset on esitelty ja havainnollistettu erilaisin kuvioin, kuten pylväs- ja ympyrädiagrammein. Kyselytutkimus lähetettiin yhteensä 498:lle Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkieliselle päiväopiskelijalle. Kyselyn vastausaika oli 13.1. -20.1.2025. Kyselyyn vastasi 59 opiskelijaa, joten kyselyn vastausprosentti oli alle kymmenen prosenttia, joka on melko matala vastausprosentti. Kyselylomake löytyy liitteestä 2 työn lopusta.

6.1 Vastaajien taustatiedot

Kyselylomakkeen alussa kysyttiin vastaajien sukupuolta, ikää ja opiskelualaa. Kyselyyn vastanneista naisia oli 51 %, miehiä 47 % ja muu sukupuoli 2 %. Kyselyyn vastasikin siis melkein yhtä paljon naisia ja miehiä, joten sukupuolijakauma on tasainen. Sukupuolijakauma on esitetty kuviossa 2.



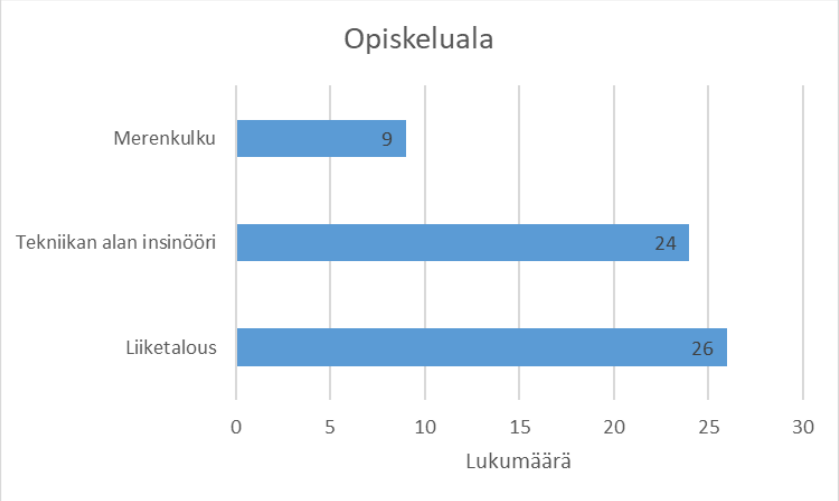
Kuvio 2. Sukupuolijakauma.

Seuraavaksi kyselylomakkeessa kysyttiin vastaajien ikää. Kyselyyn vastasi laajasti monen ikäisiä opiskelijoita. Eniten kyselyyn kuitenkin vastasi 21–24-vuotiaita, joita vastanneista oli 43 %. Toiseksi eniten kyselyyn vastanneista olivat 25–30-vuotiaita, joita oli 32 % vastanneista. Kyselyn ikäjakauma on esitetty kuviossa 3.

Kuvio 3. Ikäjakauma.

Kolmannessa kyselyn kysymyksessä selvitettiin vastanneiden opiskelijoiden opiskelualaa. Satakunnan ammattikorkeakoulun Rauman kampuksella opiskeltavia kohderyhmän opintoaloja ovat Liiketalous, Merenkulu ja tekniikan alan insinöörityötkinnot, kuten tuotantotekniikka, tuotantotalous ja logistiikka. Vastanneista suurin osa ovat liiketalouden opiskelijoita tai tekniikan alan

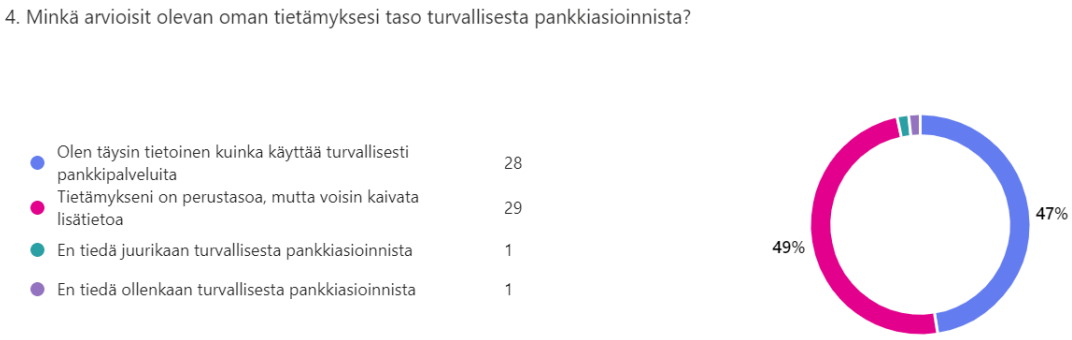
insinööriopiskelijoita. Liiketalouden opiskelijoita vastasi kyselyyn 26 kappaletta ja tekniikan alan insinööriopiskelijoita 24 kappaletta. Vähiten vastauksia saatiin merenkulun alan opiskelijoilta, joita kyselyyn vastanneista oli 9 kappaletta. Opiskelualan jakauma vastanneiden kesken on esitetty kuviossa 4.



Kuvio 4. Opiskeluala.

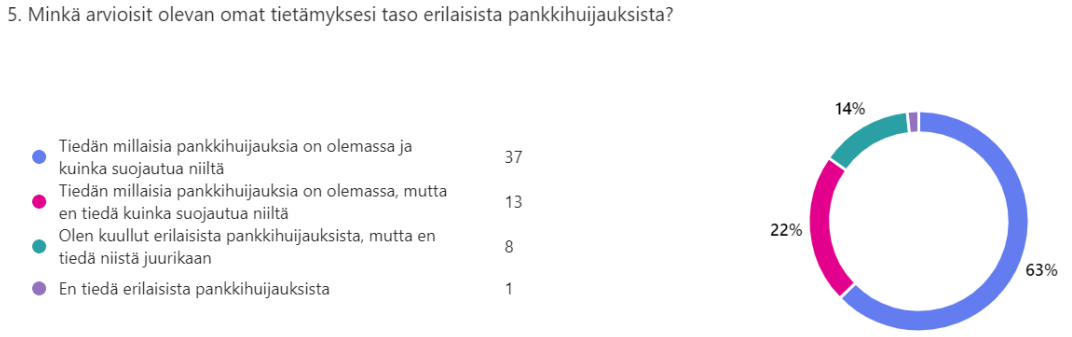
6.2 Vastaajien tietämys pankkiturvallisuudesta ja pankkihuijauksista

Kyselylomakkeen seuraavassa vaiheessa tiedusteltiin vastaajien tietämystä turvallisesta pankkiasioinnista ja erilaisista pankkihuijauksista. Kysymyksessä neljä, vastaajia pyydettiin arvioimaan oman tietämyksen taso turvallisesta pankkiasioinnista. Kuten kuviosta 5 voi havainnoida, niin vastaajista 47 % kokee olevansa täysin tietoinen, kuinka käyttää turvallisesti pankkipalveluita. Vastaajista kuitenkin 49 % uskoo tietämyksensä olevan hyvällä perustasolla, mutta kaipaisivat lisätietoa aiheesta. Vain yksi henkilö vastasi, että ei tiedä juurikaan turvallisesta pankkiasioinnista. Lisäksi yksi henkilö vastasi, ettei tiedä ollenkaan turvallisesta pankkiasioinnista. Vastausten perusteella siis noin puolet vastanneista opiskelijoista kokevat tietävänsä kuinka käyttää turvallisesti pankkipalveluita. Toinen noin puolikas osa vastanneista kokee, että voisi kaivata lisätietoa, mutta heidän tietämyksensä on perustasolla. Vastanneet siis kokevat tietävänsä kuinka käyttää turvallisesti pankkipalveluita.



Kuvio 5. Oman tietämyksen tason arviointi turvallisesta pankkiasioinnista.

Kysymyksessä viisi, joka on esitetty kuviossa 6, kyselyn vastaajat arvioivat omaa tietämyksen tasoa liittyen erilaisiin pankkihuijauksiin. Vastaajista 63 % (37 kappaletta) kokee tietävänsä, millaisia pankkihuijauksia on olemassa ja kuinka niiltä voi suojautua. Vastaajista 22 % (13 kappaletta) taas kokee tietävänsä, millaisia huijauksia on olemassa, mutta ei tiedä kuinka suojautua niiltä. Kysymykseen vastanneista 14 % (8 kappaletta) on vastannut, että on kuullut erilaisista pankkihuijauksista, mutta ei tiedä niistä juurikaan. Vain yksi henkilö on vastannut, ettei ole tietoinen erilaisista pankkihuijauksista. Suurin osa kyselyyn vastanneista opiskelijoista siis kokee ja uskoo tietävänsä, millaisia pankkihuijauksia on liikkeellä.



Kuvio 6. Oman tietämyksen tason arviointi erilaisista pankkihuijauksista.

Seuraavassa kysymyksessä eli kuudennessa kysymyksessä (kuvio 7) selvitettiin tarkemmin, että mitkä yleisimmistä pankkihuijaustavoista ovat vastaajille tuttuja. Kysymykseen kuusi oli mahdollista valita vaihtoehdoista monta vaihtoehtoa. Vastausten perusteella tutuin pankkihuijauksien keino vastanneille on tietojenkalastelu tekstiviestillä tai sähköpostilla, sillä sen vaihtoehdon valitsi 56

henkilöä 59:stä kyselyyn vastanneesta. Myös huijauspuhelut ovat tuttu huijauskeino suurimmalle osalle, sillä sen valitsi 53 henkilöä. Vähiten tuttu pankkihuijaustapa on ollut rakkaushuijaus, jonka on valinnut 28 henkilöä vastanneista. Kukaan kyselyyn vastanneista ei ole kokenut, että mikään valittavista huijaustavoista ei ole heille tuttu.

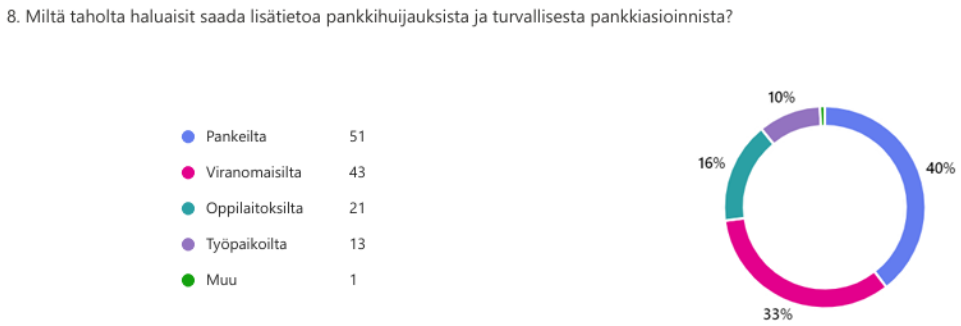
Kuvio 7. Pankkihuijaustapojen tuttavuus.

6.3 Tiedon saatavuus pankkiturvallisuudesta ja pankkihuijauksista

Kyselytutkimuksen seuraavissa kolmessa kysymyksessä selvitettiin, että onko vastaajien mielestä turvallisesta pankkiasioinnista ja pankkihuijauksista tarpeeksi tietoa saatavilla ja miten sekä keneltä vastaajat haluaisivat saada aiheista lisätietoa. Kysymyksessä seitsemän selvitettiin, että onko opiskelijoiden mielestä pankkihuijauksista ja turvallisesta pankkiasioinnista saatavilla tarpeeksi tietoa. Vastanneista 53 % (31 kappaletta) kokee, että aiheesta on tarpeeksi tietoa saatavilla. Vastanneista taas 47 % (28 kappaletta) kokee, että aiheesta ei ole saatavilla tarpeeksi tietoa. Noin puolet siis kokevat, että pankkihuijauksista ja turvallisesta pankkiasioinnista pitäisi olla enemmän tietoa saatavilla tai aiheista pitäisi kertoa enemmän.

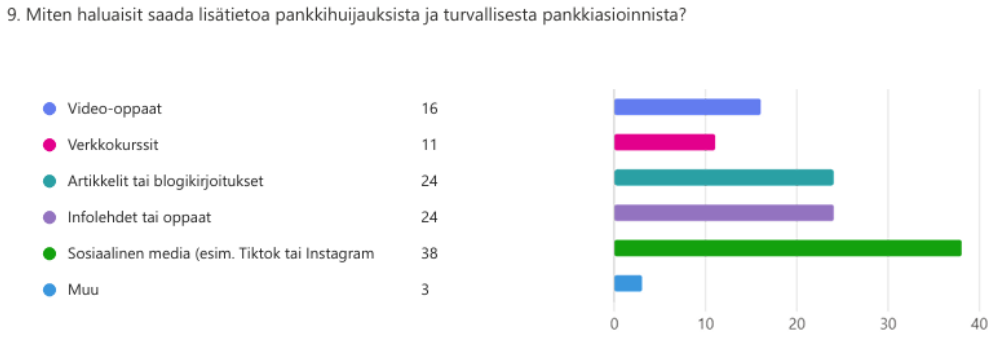
Kysymyksessä kahdeksan (kuvio 8) selvitettiin, että miltä eri tahoilta opiskelijat haluaisivat saada lisätietoa pankkihuijauksista ja turvallisesta pankkiasioinnista. Kysymyksessä vastaajat pystyivät valitsemaan monta eri vaihtoehtoa, mutta vähintään yksi vaihtoehto oli pakollinen valittava. Lisäksi yksi

vastausvaihtoehdoista oli vaihtoehto ”muu”, joka oli avoin vastauskenttä. Vastaukset jakautuivat niin, että opiskelijoista 40 % haluaisi saada aiheista lisätietoa pankeilta. Viranomaisilta tietoa aiheista haluaisivat saada 33 % vastanneista. Oppilaitoksilta tiedon saamiseksi vastanneista valitsi 16 % ja työpaikoilta 10 %. Yksi kysymykseen vastanneista henkilöistä vastasi avoimeen vastauskenttään, johon hän kertoi, että haluaisi saada mediasta konkreettisia esimerkkejä millaisia huijauksia on liikkeellä.



Kuvio 8. Pankkihuijauksista ja turvallisesta pankkiasioinnista lisätiedon saanti eri tahoilta.

Seuraavassa kyselyn kysymyksessä eli kysymyksessä yhdeksän (kuvio 9) selvitettiin, miten opiskelijat haluisivat saada lisätietoa huijauksista ja turvallisesta pankkiasioinnista. Kysymyksessä vastaajat pystyivät valitsemaan monta haluamaansa vaihtoehtoa, joista yksi oli avoin vastauskenttä. Vastaukset jakautuivat melko tasaisesti, mutta eniten vastauksia sai vastausvaihtoehto ”lisätietoa sosiaalisen median, kuten Tiktokin tai Instagramin kautta”, jonka valitsi 38 kappaletta vastanneista. Opiskelijoista 24 kappaletta haluaisi saada lisätietoa erilaisista artikkeleista tai blogeista sekä infolehdistä tai oppaista. Video-oppaista lisätietoa aiheesta haluaisi saada 16 kappaletta vastanneista ja 11 kappaletta haluaisi saada tietoa verkkokursseista. Avoimeen vastauskenttään vastasi 3 henkilöä. Avoimissa vastauksissa nousi esille, että lisätietoa halutaan saada pankeilta esimerkiksi henkilökohtaisena ohjauksena pankkivirkailijoiden toimesta.



Kuvio 9. Pankkihuijauksista ja turvallisesta pankkiasioinnista lisätiedon halun saanti tapojen jakautuminen.

6.4 Tietämyksen selvittäminen pankkihuijauksista ja -turvallisuudesta

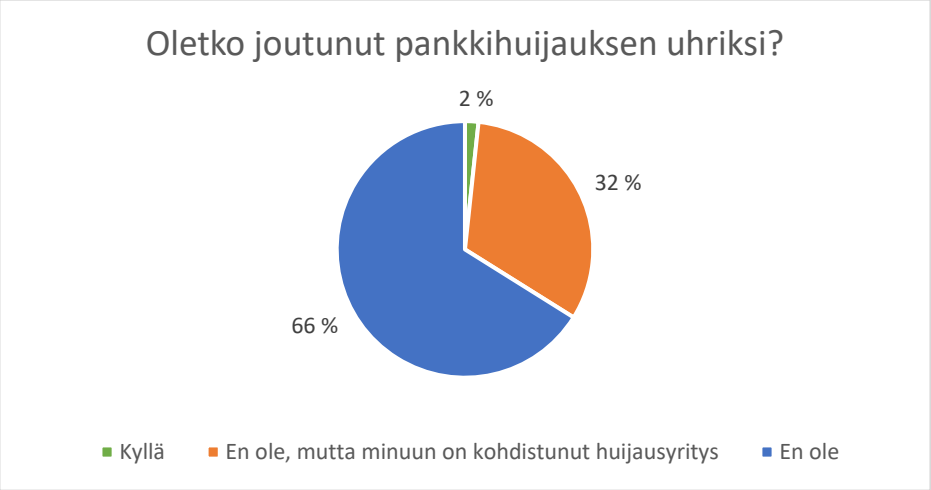
Kyselylomakkeen seuraavissa kolmessa kysymyksissä selvitettiin esimerkkitapauksin ja kysymyksin vastanneiden opiskelijoiden todellista tietämystä pankkihuijauksista ja turvallisesta pankkiasioinnista. Kysymyksessä kymmenen testattiin, että tunnistavatko opiskelijat esimerkkitapauksesta, että millainen pankkihuijaus on kyseessä. Kysymyksen esimerkki on seuraava: ”Henkilö A haluaa päästä Omakantaan ja hakee Googlesta "Omakanta". A erehtyy klikkaamaan Omakannan sivun näköiselle valesivustolle, jonne syöttää verkkopankkitunnuksensa ja vahvistuskoodin. Valesivustolle syötettyjen tietojen avulla huijari pääsee käsiksi A:n verkkopankkiin ja siirtää sieltä A:n varat ulkomaalaiselle tilille”. Kyseisen esimerkin mukainen tapaus on hakukonehuijaus. Vastanneista opiskelijoista 81 % (48 kappaletta) vastasi kysymykseen oikein. Vääriä vastauksia tuli 10 % (6 kappaletta) vastausvaihtoehdolle ”tietojenkalastelu” ja 9 % (5 kappaletta) vaihtoehdolle ”identiteettivarkaus”. Suurin osa opiskelijoista vastasi kysymykseen siis aivan oikein.

Kysymyksessä yksitoista vastaajilta kysyttiin, että miten he voivat varmistaa, että he ovat kirjautumassa pankin oikealle verkkosivustolle. Kysymykseen vastasi oikein 97 % (57 kappaletta) opiskelijoista. Oikea vastaus on, että henkilö tarkastaa, että verkkosivuston osoite alkaa ”https://” ja sisältää pankin nimen. Vain kaksi vastanneista henkilöistä vastasi kysymykseen väärin.

Seuraavassa kysymyksessä eli kahdennessatoista kysymyksessä vastaajilta kysyttiin, että onko pankki koskaan oikeutettu pyytämään verkkopankkitunnuksia puhelimessa tai sähköpostilla. Oikea vastaus kysymykseen on ei. Oikein vastasi myös 97 % (57 kappaletta) vastanneista, kuten aiempaankin kysymykseen. Kaksi henkilöä, jota vastasivat väärin, valitsivat vastaukseksi ”kyllä” ja ”vain, jos on hätätilanne”.

6.5 Pankkihuijauksen ja -huijausyrityksen kohteeksi joutuminen

Kysymyksessä kolmetoista, joka on esitetty kuviossa 10, vastaajilta kysyttiin ovatko he joutuneet pankkihuijauksen uhreiksi. Yksi vastanneista opiskelijoista on joutunut huijauksen uhriksi. Huijausyrityksiä on kohdistunut puolestaan 32 % (19 kappaletta) opiskelijoista. Noin kaksi kolmasosaa vastanneista (66 %, 39 kappaletta) ei ole joutunut pankkihuijauksen uhriksi tai huijausyrityksen uhriksi. Pankkihuijauksen uhriksi joutuneelle vastaajalle seurasi kysymyksen jälkeen lisäkysymyksiä huijaukseen liittyen. Myös huijausyritysten uhreille seurasi eri lisäkysymykset huijausyritykseen liittyen. Henkilöille, jotka eivät ole joutuneet kummankaan uhriksi seurasi vielä kyselyn viimeinen vapaamuotoinen kysymys, mikäli heillä oli jotain mielessä aiheeseen liittyen.



Kuvio 10. Pankkihuijauksen uhriksi joutuneiden määrä.

Pankkihuijauksen uhriksi joutuneelta henkilöltä selvitettiin seuraavassa kysymyksessä, millaisen huijauksen uhriksi hän on joutunut. Vastaaja kertoi

tulleensa hakukonehuijauksen uhriksi. Vastaaja kertoi avoimessa kysymyksessä huijauksesta seuraavanlaisesti: "Huijari yritti tyhjentää luottokortin, mutta pankki laittoi kortit automaattisesti kiinni, kun epäilyttävä taho yritti käyttää luottokorttia. En menettänyt siis mitään." Lisäksi huijauksen uhri kertoi, että hänelle aiheutui tästä psyykkistä haittaa. Seuraavassa kysymyksessä selvitettiin, että onko hän kertonut huijaukseen joutumisesta muille. Vastaaja kertoi, että on kertonut asiasta muille, kuten läheisilleen.

Kysymyksessä kolmetoista vastaajat, jotka ovat kertoneet joutuneensa huijausyrityksen uhriksi, saivat seuraavaksi kysymyksen, jossa selvitettiin, että millainen huijausyritys heihin on kohdistunut. Kysymyksessä seitsemäntoista (kuvio 11) vastaajat saivat valita halutessaan monta vaihtoehtoa, mikäli he ovat joutuneet monen eri huijausyrityksen kohteeksi. Huijausyrityksen kohteeksi joutuneista kaikki eli 19 henkilöä vastasivat, että he ovat joutuneet tekstiviesti tai sähköposti tietojenkalastelun kohteeksi. Vastanneista 8 henkilöä vastasi, että heihin on kohdistunut huijauspuhelu. Muiden huijausyritystapojen kohteeksi vastanneista 5 henkilöä on joutunut hakukonehuijausyrityksen kohteeksi, 3 henkilöä sijoitushuijausyrityksen kohteeksi, 2 henkilöä rakkaushuijausyrityksen kohteeksi ja 2 henkilöä sosiaalisen median kautta tietojenkalasteluyrityksen kohteeksi. Kukaan vastanneista ei vastannut avoimeen vastauskenttään, johon sai kertoa jostain muusta mahdollisesta huijausyrityksestä.

Kuvio 11. Erilaiset huijausyritykset.

Toiseksi viimeisessä kysymyksessä eli kysymyksessä kahdeksantoista, tiedusteltiin, että kuinka moni huijausyrityksen kohteeksi joutunut henkilö on kertonut epäillystä huijauksesta eteenpäin. Huijausyrityksen kohteeksi joutuneista 19 henkilöstä 17 henkilöä ei ole kertonut asiasta eteenpäin. Kuitenkin kaksi henkilöä vastasi kertoneensa asiasta pankillensa.

Kyselylomakkeen viimeinen kysymys oli avoin, johon kaikki kyselyyn vastaajat saivat vapaasti kertoa ajatuksiaan tai kokemuksiaan aiheeseen liittyen. Kysymykseen vastasi kolme henkilöä. Yksi avoimeen kysymykseen vastanneista kertoi, että hän käyttää pankki- ja sijoitusasioihin vain sovelluksia, joten hän välttyy helposti huijaussivustoilta. Lisäksi hän käyttää mobiilivarmennetta. Hänen mielestään sovelluksia tulisi markkinoida pankkien asiakkaille luotettavina ratkaisuina digihuijauksia vastaan. Hän on myös suorittanut hyödylliseksi kokemansa STAR-kurssin työelämässä. Toisen avoimeen kysymykseen vastanneen henkilön mielestä vanhemmille ihmisille pitäisi järjestää helposti saatavilla olevia koulutuksia, sillä esimerkiksi tekoälyn myötä huijaukset ovat kehittyneet todella uskottaviksi. Tämä parantaisi vanhempien ihmisten turvallista pankkiasiointia.

6.6 Johtopäätökset

Tutkimuskyselyyn vastasi 59 henkilöä, joten tutkimuksen otanta jäi hieman toivottua matalammaksi. Vastauksia tuli kuitenkin riittävästi, jotta tutkimustuloksista voidaan tehdä joitakin johtopäätöksiä, muttei täysin yleistäviä tulkintoja. Tutkimustulosten analysoinnissa on otettu huomioon otannan määrä ja johtopäätökset on tehty sen mukaan.

Ennen tutkimuksen tutkimuksellista osaa oletuksenani oli, että nuorilla opiskelijoilla on yleisesti hyvä tietämys pankkihuijauksista ja turvallisesta pankkiasioinnista. En kuitenkaan osannut arvioida kuinka moni opiskelijoista on joutunut huijauksen uhriksi tai heihin on kohdistunut pankkihuijausyritys. Tutkimustuloksista voidaan havainnoida, että opiskelijat kokevat tietävänsä turvallisesta pankkiasioinnista hyvin ja he myös kokevat tietävänsä sekä tunnistavansa

melko hyvin erilaiset pankkihuijaukset. Kyselytutkimuksen muutamassa kysymyksessä testattiin opiskelijoiden kykyä tunnistaa esitetystä esimerkistä oikea pankkihuijaustapa ja oikea turvallinen tapa asioida pankin sivuilla. Opiskelijat osasivat tunnistaa kuinka turvallisesti asioida pankin palveluissa. Suurin osa eli noin 80 % opiskelijoista lisäksi tunnisti esimerkkitapauksesta oikean pankkihuijaustavan. Tästä voidaankin todeta, että kohderyhmän opiskelijoilla on hyvä tietämys turvallisesta pankkiasioinnista ja pankkihuijauksista. Tätä vahvistaa myös se, että kyselyssä kävi ilmi, että vain yksi henkilö vastasi joutuneensa pankkihuijauksen uhriksi.

Kyselyyn vastanneista opiskelijoista noin 30 prosenttiin on kohdistunut pankkihuijausyritys, joten huijauksia on selkeästi liikkeellä paljon myös kohdistuen nuoriin. Usein pankkihuijauksien oletetaan kohdistuvan vain vanhempiin ihmisiin, joilla ei ole usein niin hyviä digitaitoja. Nuorilla opiskelijoilla on usein hyvät taidot tietotekniikassa ja yleisesti parempi ymmärrys sosiaalisen media sekä internetin eri alueista verrattuna vanhempiin ihmisiin. Nuoret ovat kasvaneet elektronisten laitteiden ja internetin maailmassa, jolloin heille on kertynyt myös parempi ymmärrys, millaisia huijauksia internetissä liikkuu.

Opiskelijoista, joihin kyselyn mukaan on kohdistunut pankkihuijausyritys, on kaikkiin kohdistunut tietojenkalastelua tekstiviestillä tai sähköpostilla. Kaikki huijausyritysten kohteena olleet opiskelijat ovat siis tunnistaneet saaneensa tiedonkalasteluviestejä tekstiviestillä tai sähköpostilla. Tietojenkalastelu on viime vuosina noussut yleisimmäksi huijauskeinoksi, kuten työn teoriaosassakin kerrottiin. Tämän tutkimuksen vastaukset vahvistavat myös, että tietojenkalastelu tekstiviestillä ja sähköpostilla on tällä hetkellä yleisin pankkihuijareiden käyttämä huijauskeino. Moneen kyselyn vastaajaan on myös kohdistunut monia eri pankkihuijausyrityksiä, sillä kaikkiin kyselyssä vaihtoehtona olleisiin huijaustapoihin tuli vastauksia.

Kyselyyn vastanneet opiskelijat vastasivat lisäksi, että tietojenkalastelu tekstiviestillä ja sähköpostilla sekä huijauspuhelut ovat heille tutuimpia huijaustapoja. Tietojenkalastelu tekstiviestillä ja sähköpostilla onkin siis tullut mahdollisesti tutuksi opiskelijoille, sillä heihin on kohdistunut näitä huijaustapoja eniten.

Huijauspuhelut ovat toiseksi tutuimpia opiskelijoille vastausten perusteella. Tämän voi johtua siitä, että huijaustapa on melko yksiselitteinen ja huijauspuheluista on varoiteltu uutisissa jo pitkään.

Huijausyrityksen kohteeksi joutuneista opiskelijoista 89 % ei ilmoittanut heihin kohdistuneesta huijausyrityksestä eteenpäin esimerkiksi pankille tai poliisille. Tämä voi selittyä sillä, että huijausyrityksiä on liikkeellä paljon ja moni opiskelija varmasti saakin sähköpostiin sekä muihin kanaviin niin paljon tietojenkalasteluviestejä, että he eivät vain reagoi niihin. Pankkihuijausyritysten ja tietojenkalasteluviestien tapoja olisi kuitenkin hyvä raportoida eteenpäin esimerkiksi omalle pankille, jotta pankit saavat tietoon millaisia huijauksia on milläkin hetkellä liikkeellä. Tällä tavoin pankit voivat levittää tietoa ajankohtaisista huijauksista. Pankkihuijausyrityksissä huijarit voivat lähettää viestiä esiintyen jonain pankkina. Tämän vuoksi pankkienkin olisi hyvä saada tietoon, mikäli heidän nimissään yritetään huijata asiakkaita.

Tutkimuksesta kävi ilmi, että noin 50 % kyselyyn vastanneista opiskelijoista kokee, että turvallisesta pankkiasioinnista ja pankkihuijauksista on tarpeeksi tietoa saatavilla. Kuitenkin toinen puolikas vastanneista kokee, ettei tietoa ole tarpeeksi saatavilla, joten aiheista tulisi selkeästi olla enemmän tietoa liikkeellä. Kyselyn mukaan suurin osa opiskelijoista haluaisi saada lisätietoa pankeilta ja viranomaisilta. Pankeilla ja viranomaisilla on paras tietämys, millaisia pankkihuijauksia on liikkeellä ja miten niiltä voi välttyä, joten tiedon saaminen heiltä on loogista. Kyselystä kävi myös ilmi, että opiskelijat haluaisivat saada tietoa eniten sosiaalisen median kanavien kautta, jotka ovatkin nuorille usein helpoin ja sopivin tapa saada tietoa eri aiheista. Sosiaalisen median kautta levitetään valitettavasti myös paljon väärää ja virheellistä tietoja, jonka vuoksi voi olla vaikea tunnistaa, että mikä tieto on luotettavaa ja oikeaa.

Kyselyyn vastanneet vastasivat myös haluavansa saada pankkihuijauksista ja turvallisesta pankkiasioinnista tietoa artikkeleista, blogeista, infolehdistä ja erilaista oppaista, joten tietoa aiheista tulisi opiskelijoiden näkökulmasta saada monella eri tavalla laajasti. Jotta tietoisuus pankkihuijauksista ja turvallisesta pankkiasioinnista paranisi, niin aiheesta tulisi puhua avoimesti sekä kertoa

esimerkkien kautta millaisia huijauksia on liikkeellä. Viime vuosina uutisiin on noussut jo jonkin verran esimerkkitapauksia ihmisistä, jotka ovat joutuneet pankkihuijauksen uhriksi. Tutkimukseen vastanneiden opiskelijoiden mukaan siis tietoa tulisi saada pankeilta ja viranomaisilta sosiaalisen median kanavien kautta. Tällöin luotettavien tahojen levittämä tieto saavuttaisikin varmasti parhaiten nuoret opiskelijat.

Tutkimuksen tuloksiin ja niiden luotettavuuteen on voinut vaikuttaa opiskelijoiden opiskeluala. Liiketalouden opiskelijoilla voisi olettaa olevan parempi tietämys aiheesta opiskelualan vuoksi, mutta koska liiketalouden ja tekniikan alan opiskelijoilta saatiin melkein saman verran vastauksia, niin uskon, että opiskelualalla ei ole suurempaa merkitystä tutkimuksen tuloksiin. Myös tutkimuksen sukupuolijakauma oli tasainen, joten en usko myöskään sukupuolen vaikuttaneen tuloksiin.

7 POHDINTA JA YHTEENVETO

Opinnäytetyöprosessin alkaessa työ tuntui melko suurelta projektilta, mutta kun sen jakoi pieniin osiin, niin työ eteni oikein hyvin. Koen, että opinnäytetyötä tehdessäni opin kuinka laajemmissa kirjoitustöissä kannattaakin jakaa työ palasiin, joita lähtee yksi kerrallaan tekemään. Näin työ ei ala tuntumaan ylitsepääsemättömän suurelta. Työn alussa ehkä haastavin tehtävä oli valita työn aihe. Koen, että työn aiheeksi on tärkeä valita aihe, josta on oikeasti kiinnostunut, jotta työn teko säilyy mielekkäänä ja työ on helpompi saattaa loppuun. Aiheen valinta oli vaikea päätös, mutta päädyin tähän aiheeseen, sillä olen itse pankissa töissä ja vastaani tulee tällä hetkellä valitettavan paljon pankkihuijauksia. Aihe onkin siis todella ajankohtainen tällä hetkellä. Töissä minulle on tullut vastaan juuri samantyyppisiä pankkihuijauksia, joita tässäkin työssä on käsitelty. Olen oppinut työn teon aikana erilaisista huijaustavoista lisää, mistä on hyötyä työelämääni.

Minun ei ole aiemmin tarvinnut hakea tietoa näin laajaan työhön, joten hyvien lähteiden etsintä oli aluksi vaikeaa. Koen kuitenkin, että työn teoriaosaa tehdessä kehityin tiedon ja lähteiden etsinnässä sekä luotettavien lähteiden arvioinnissa. Lisäksi uskon tai ainakin toivon, että näin pitkän kirjoitusprosessin olen myös kehittynyt kirjoittajana hieman. Sitä on kuitenkin vaikea itse arvioida, mutta ehkä se voi näkyä työstäni.

Opinnäytetyön yhtenä tutkimuskysymyksenä oli selvittää, mikä on Satakunnan ammattikorkeakoulun opiskelijoiden tietoisuus pankkihuijauksista ja turvallisesta pankkiasioinnista. Onnistuin mielestäni vastaamaan tähän tutkimuskysymykseen, sillä tutkimuskyselyn avulla selvisi, kuinka hyvin opiskelijat tietävät erilaisista pankkihuijauksista. Lisäksi kyselystä selvisi, että opiskelijat osaavat toimia hyvin turvallisen pankkiasioinnin osalta. Toisena tutkimuskysymyksenä oli selvittää, onko Satakunnan ammattikorkeakoulun opiskelijoihin kohdistunut pankkihuijauksia tai -huijausyrityksiä ja miten niitä on esiintynyt. Kyselystä selvisi, että noin kolmasosaan on kohdistunut huijausyrityksiä ja yksi henkilö on joutunut huijauksen uhriksi. Kyselystä selvisi myös, millaisia huijauksia vastanneisiin on kohdistunut. Kolmannessa tutkimuskysymyksessä selvitettiin, miten ja mistä Satakunnan ammattikorkeakoulun opiskelijat haluaisivat saada lisätietoa turvallisesta pankkiasioinnista. Tähänkin kysymykseen onnistuttiin selvittämään vastaus, sillä kyselyn mukaan opiskelijat haluaisivat saada lisätietoa aiheesta pankeilta ja viranomaisilta sosiaalisen median kautta. Tutkimuskysymyksiin ja ongelmaan onnistuttiin saamaan mielestäni vastaukset, joten tutkimuksen empiirinen osa onnistui siltä osin hyvin ja tavoitteisiin päästiin.

Opinnäytetyön aikana haastavimpana tehtävänä oli kyselylomakkeen ja sen kysymysten määrittely. Lomakkeen kysymysten ja niiden asettelun sekä vastausvaihtoehtojen miettiminen oli hankalaa. Oli vaikea valita, että millaisia kysymyksiä kyselyyn laitetaan, jotta tutkimuskysymyksiin ja -ongelmaan saataisiin parhaiten vastauksia. Jos tekisin työn uudelleen, niin voisin lisätä kyselylomakkeeseen vielä lisäkysymyksiä, jotta kyselystä saataisiin vielä tarkempia vastauksia. Lisäksi muutaman kysymyksen vastausvaihtoehtoja voisi muuttaa monipuolisemmiksi, jotta tutkimustulokset eivät ainakaan vääristy vastausvaihtojen laadun vuoksi. Monessa kysymyksessä toki oli yhtenä

vastausvaihtoehtona avoin vastauskenttä, johon pystyi kirjoittamaan jonkin muun vastauksen, jota ei vaihtoehdoista löytynyt. Näihin avoimiin kysymyksiin vastaamisessa on vain monelle vastaajalle isompi kynnys, sillä he eivät välttämättä jaksa kirjoittaa omaa vastausta, vaan heidän on helpompi valita esitetyistä vaihtoehdoista parhaiten sopiva.

Tutkimuksessa valittiin tutkimusmenetelmäksi määrällinen tutkimus, joka toteutettiin kyselytutkimuksena. Koen, että tämä oli hyvä valinta, jotta asettamiini tutkimuskysymyksiin saatiin vastaukset. Tutkimuskysymyksissäni kuitenkin haluttiin selvittää muun muassa, miten paljon määrällisesti opiskelijoihin on kohdistunut huijausyrityksiä. Tutkimuksen olisi kuitenkin voinut myös toteuttaa laadullisena tutkimuksena, jolloin tutkimuksessa olisi voitu haastatella muutamia opiskelijoita ja saada tietoon laajemmin heidän näkemyksensä turvallisesta pankkiasioinnista ja selvittää tarkemmin mitä he tietävät eri pankkihuijaustavoista. Tällöin ei toisaalta voisi saada tietoon, että miten paljon ja kuinka laajalti opiskelijoihin on kohdistunut huijauksia, vaan vain yksittäisten henkilöiden kokemuksia.

Valittuun määrälliseen tutkimusmenetelmään liittyi se ongelma ja rajoite, että tulokset voivat jäädä liian pinnallisiksi, mikäli tutkimusta ja kyselyä ei toteuteta hyvin. Riskinä oli myös, että mikäli tutkimuksen kyselyyn ei saada vastauksia riittävästi, niin tutkimustuloksista ei voida vetää johtopäätöksiä. Koen kuitenkin saaneeni kyselyyni vastauksia sen verran, että tutkimustuloksista voidaan tehdä johtopäätöksiä ainakin kyselyyn vastanneiden osalta. Yleismaailmallisia yleistyksiä ei voitu tehdä, mutta tutkimuksen kohderyhmäni oli myös rajattu pienempään joukkoon.

Uskon, että tutkimustulokset onnistuivat kartoittamaan hyvin kohderyhmän tilanteen. Tutkimuksen myötä sain selvitettyä miten pankkihuijauksia ja huijausyrityksiä on kohdistunut kohderyhmän opiskelijoihin sekä mikä on heidän tietoisuutensa turvallisesta pankkiasioinnista. Tutkimuksen tulokset ovat mielestäni luotettavia, sillä tutkimukseen vastaaminen oli opiskelijoille vapaaehtoista ja se tapahtui anonyymisti. Tutkimuksen otanta jäi hieman matalaksi, mutta uskon, että se oli kuitenkin riittävä, jotta sain selvitettyä kohderyhmän

kokemukset ja tietoisuuden aiheesta. Sähköpostilla lähetettäviin kyselytutkimuksiin on usein melko hankala saada paljon vastauksia, sillä esimerkiksi opiskelijat saavat paljon sähköposteja ja heille tulee useita muitakin kyselyjä opiskeluvuoden aikana. Tämän vuoksi monet opiskelijat eivät välttämättä ehdi tai viitsi vastata kyselyihin.

Tutkimukseni tulokset antavat hieman osviittaa siitä mikä voisi olla yleisestikin nuorten opiskelijoiden tietoisuus ja kokemukset aiheeseen liittyen. En kuitenkaan tekisi tästä yleistystä kaikkiin nuoriin opiskelijoihin Suomessa. Opinnäytetyön aihepiiristä olisi mielenkiintoista saada vielä lisätietoa ja tehdä jatkotutkimuksia eri kohderyhmille. Jatkotutkimuksessa voisi esimerkiksi selvittää, että mikä on vanhempien ihmisten ja vanhusten tietoisuus pankkihuijauksista sekä miten paljon heihin kohdistuu huijauksia. Vanhemmilla ihmisillä voidaan olettaa olevan heikommat digitaidot, jonka vuoksi voisi ajatella, että heihin kohdistuu paljon huijauksia ja he joutuvat helpommin niiden uhreiksi. Olisi mielenkiintoista selvittää, että mikä on asian todellisuus.

En valinnut tähän tutkimukseen kohderyhmäksi vanhempia ihmisiä, sillä tutkimuksen toteutus olisi ollut haastavaa. Opinnäytetyöaikatauluni olisi ollut myös pidempi ja vienyt enemmän resursseja, sillä tutkimuksen aineiston keruu olisi ollut haastavampaa. Tämän vuoksi en valinnut vanhempia ihmisiä kohderyhmäksi, vaan valitsin kohderyhmäksi Satakunnan ammattikorkeakoulun opiskelijoita. Tutkimus oli helpompi toteuttaa opiskelijoille, sillä pystyin lähettämään kyselytutkimuksen sähköisenä ja suoraan opiskelijoiden sähköpostiin.

Kokonaisuudessaan opinnäytetyöprosessi oli mielestäni onnistunut, sillä onnistuin pääsemään tavoitteisiini eli saamaan tietoon opiskelijoiden tietämystä ja kokemuksia pankkihuijauksista sekä turvallisesta pankkiasioinnista. Onnistuin myös viemään tutkimuksen kunnialla maaliin. Pankkihuijausten määrä on kasvanut räjähdysmäisesti viimevuosina, jonka vuoksi aiheesta on mielestäni tärkeä levittää tietoa. Tämä on tärkeää, jotta ihmisten tietoisuus aiheesta paranisi ja he osaisivat käyttää turvallisesti pankkipalveluitaan. Pankkihuijausten määrän vähentämiseksi myös pankkien ja viranomaisten on tärkeä levittää aiheesta tietoa. Toivon, että olen työni avulla edesauttanut tiedon levittämistä

aiheesta ja luettuasi tämän opinnäytetyön ymmärrät hieman paremmin, millaisia pankkihuijauksia on olemassa ja miten suojautua niiltä sekä kuinka käyttää pankkipalveluita turvallisesti.

LÄHTEET

Aktia. (n.d.). Monipuoliset maksuvälineet arkeen ja lomalle. Haettu 19.11.2024 osoitteesta https://www.aktia.fi/fi/kortit

Alhonsuo, S., Nisén, A. & Pellikka, T. (2009). Finanssitoiminnan käsikirja. Hakapaino Oy.

Danske Bank. (n.d.). Yleisimmät huijaustavat. Haettu 26.11.2024 osoitteesta https://danskebank.fi/sinulle/asiakaspalvelu/tarkkana-verkossa/faktat/erilaisia-huijaustapoja#accordion-0-item-1

Digi- ja väestövirasto. (n.d.). Varmenteet ja kortit. Haettu 15.11.2024 osoitteesta https://dvv.fi/varmenteet

Edilex. (23.09.2024). Hovioikeus äänesti ja kumosi käräjäoikeuden tuomion verkkopankkihuijausasiassa: Pankin henkilöasiakas vastasi maksuvälineen oikeudettomasta käytöstä. Haettu 20.12.2024 osoitteesta https://www-edilex-fi.lillukka.samk.fi/uutiset/92627

Finanssiala ry. (17.09.2024). Huijaukset kovassa kasvussa – pankit onnistuivat pysäyttämään yli 18 miljoonaa euroa huijattua rahaa. Haettu 1.11.2024 osoitteesta https://www.finanssiala.fi/uutiset/huijaukset-kovassa-kasvussa-pankit-onnistuivat-pysayttamaan-yli-18-miljoonaa-euroa-huijattua-rahaa/

Finanssiala ry. (06.02.2024). Huijareilla oli aktiivinen vuosi 2023 – Pankit saivat estettyä digihuijauksia lähes 33 miljoonan euron edestä. Haettu 1.11.2024 osoitteesta https://www.finanssiala.fi/uutiset/huijareilla-oli-aktiivinen-vuosi-2023-pankit-saivat-estettya-digihuijauksia-lahes-33-miljoonan-euron-edesta/

Finanssiala ry. (05.01.2024). Pankit ja rahoitus. Haettu 1.11.2024 osoitteesta https://www.finanssiala.fi/aiheet/pankit-ja-rahoitus/#/

Finanssivalvonta. (14.08.2024). Huijaukset. Haettu 18.11.2024 osoitteesta https://www.finanssivalvonta.fi/kuluttajansuoja/huijaukset/

Finanssivalvonta. (05.09.2018). Peruspankkipalvelut. Haettu 11.11.2024 osoitteesta https://www.finanssivalvonta.fi/kuluttajansuoja/pankkipalvelut/peruspankkipalvelut/

Finanssivalvonta. (2014). Määräykset ja ohjeet 8/2014: Operatiivisen riskin hallinta rahoitussektorin valvottavissa. https://www.finanssivalvonta.fi/globalassets/fi/saantely/maarayskokoelma/2014/08_2014/08_2014.m6.pdf

FINE. (2024). Huijausten selvittäminen ja ratkaisukäytännöt FINEssä. Haettu 26.11.2024 osoitteesta https://www.fine.fi/oppaat/julkaisu/huijausten-selvittaminen-ja-ratkaisukaytannot-finessa.html

Heikkilä, T. (2014). Tilastollinen tutkimus. 9. uudistettu painos. Edita.

Hirsjärvi, S., Sinivuori, E., Remes, P., & Sajavaara, P. (2007). Tutki ja kirjoita (13. osin uud. laitos.). Tammi.

Kuluttajaliitto. (n.d.). Maksukortit. Haettu 11.11.2024 osoitteesta https://www.kuluttajaliitto.fi/materiaalit/maksukortit/

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017. Haettu 11.11.2024 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2017/20170444#L3

Liikenne- ja viestintävirasto Traficom kyberturvallisuuskeskus. (n.d.). Sähköinen tunnistaminen. Haettu 15.11.2024 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Maksupalvelulaki 290/2010. Haettu 20.12.2024 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2010/20100290#L7P63

Mobiilivarmenne. (n.d.). Näin Mobiilivarmenne toimii. Haettu 15.11.2024 osoitteesta https://mobiilivarmenne.fi/nain-mobiilivarmenne-toimii/

Nordea Oyj. (n.d.a). Määräaikainen sijoitustili. Haettu 11.11.2024 osoitteesta https://www.nordea.fi/henkiloasiakkaat/palvelumme/saastaminen-sijoittaminen/saastamisen-tilit/maaraaikainen-sijoitustili.html

Nordea Oyj. (n.d.b). Turvallinen verkkomaksaminen. Haettu 19.11.2024 osoitteesta https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/kortin-turvallinen-kaytto/nain-ostat-turvallisesti-verkossa.html

Nordea Oyj. (n.d.c). Käteisnostoraja ja kortin muut turvarajat – varmista kortin turvallinen käyttö. Haettu 11.11.2024 osoitteesta https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/kortin-turvallinen-kaytto/#tab=Ohjeita-kortin-turvalliseen-kayttoon

Nordea Oyj, (n.d.d). Erilaisia huijausmuotoja. Haettu 26.11.2024 osoitteesta https://www.nordea.fi/henkiloasiakkaat/sinun-elamasi/turvallisuus/erilaisia-huijausmuotoja/

Oma Säästöpankki Oyj. (n.d.a.). Korttireklamaatio. Haettu 20.12.2024 osoitteesta https://www.omasp.fi/henkiloasiakas/arjen-raha-asiat/kortit/tietoa-kortin-kaytosta/korttireklamaatio

Oma Säästöpankki Oyj. (n.d.b). Verkkopankissa hoidat pankkiasiasi missä ja milloin vain. Haettu 12.11.2024 osoitteesta https://www.omasp.fi/henkiloasiakas/digitaaliset-palvelut/digiasiointi/verkkopankki

OP. (n.d.a). ASP-tili. Haettu 11.11.2024 osoitteesta https://www.op.fi/henkiloasiakkaat/paivittaiset/tilit/asp-tili

OP. (n.d.b). IBAN-tilinumero ja BIC-koodi. Haettu 12.11.2024 osoitteesta https://www.op.fi/henkiloasiakkaat/paivittaiset/tilit/iban-tilinumero

Poliisi. (n.d.). Petosrikokset. Haettu 26.11.2024 osoitteesta https://poliisi.fi/petosrikokset

Rikosuhripäivystys. (n.d.). Tietojenkalastelu. Haettu 3.12.2024 osoitteesta https://www.riku.fi/nettihuijaus/tietojenkalastelu/

Solla, K. (09.08.2017). Digitreenit: Miten pankkiin mennään puhelimella? Viisi kysymystä pankkien mobiilisovelluksista. Yle artikkeli. https://yle.fi/aihe/artikkeli/2017/08/09/digitreenit-miten-pankkiin-mennaan-kannykalla-viisi-kysymysta-pankkien

Säästöpankki. (n.d.). SEPA-maksut. Haettu 12.11.2024 osoitteesta https://www.saastopankki.fi/fi-fi/tilit-kortit-ja-maksaminen/maksaminen/sepa-maksut

Tietosuojavaltuutetun toimisto. (n.d.a). EU:n tietosuoja-asetus. Haettu 04.11.2024 osoitteesta https://tietosuoja.fi/usein-kysyttya-gdpr

Tietosuojavaltuutetun toimisto. (n.d.b). Tietosuoja. Haettu 04.11.2024 osoitteesta https://tietosuoja.fi/tietosuoja

Yle. (18.11.2024). Pankkien edunvalvoja vertaa nettihuijaukseen lankeamista ryöstöön Rion karnevaaleilla: ”Ei se ole Finnairin vastuu”. Haettu 20.12.2024 osoitteesta https://yle.fi/a/74-20124331

LIITE 1

Kyselylomakkeen saatekirje

Hei!

Olen neljännen vuoden liiketalouden opiskelija ja teen opinnäytetyötä, jossa selvitän Satakunnan ammattikorkeakoulun Rauman kampuksen suomenkielisten päiväopiskelijoiden tietämystä ja kokemuksia turvallisesta pankkiasioinnista ja pankkihuijauksista.

Arvostaisin suuresti, jos vastaisit kyselyyn. Kyselyyn vastaaminen vie vain muutaman minuutin ajastasi, mutta siitä on minulle valtava apu, jotta saan tarvittavaa tutkimusmateriaalia. Vastaaminen on vapaaehtoista ja kyselyyn vastaaminen tapahtuu anonyymisti. Vastaukset kerätään opinnäytetyötäni varten ja hävitetään tutkimuksen valmistuttua.

Voit vastata kyselyyn tästä: xxxx

Kysely on auki 13. – 20.1.2025

Mikäli sinulle tulee tutkimukseeni liittyen kysyttävää, niin voit ottaa minuun yhteyttä sähköpostitse osoitteessa xxxx.

Kiitos paljon ajastasi!

Ystävällisin terveisin
Valtteri Vierimaa

LIITE 2

Kyselylomake

1. Mikä on sukupuolesi?
- Nainen
- Mies
- Joku muu

2. Minkä ikäinen olet?
- 18–20
- 21–24
- 25–30
- Yli 30

3. Mikä on opiskelualasi?
- Liiketalous
- Merenkulku
- Tekniikanalan insinööri (Tuotantotekniikka ja tuotantotalous, logistiikka)

4. Minkä arvioisit olevan oman tietämyksesi taso turvallisesta pankkiasioinnista?
- Olen täyin tietoinen, kuinka käyttää turvallisesti pankkipalveluita,
- Tietämykseni on perustasoa, mutta voisin kaivata lisätietoa,
- En tiedä juurikaan turvallisesta pankkiasioinnista,
- En tiedä ollenkaan turvallisesta pankkiasioinnista.

5. Minkä arvioisit olevan omat tietämyksesi taso erilaisista pankkihuijauksista?
- Tiedän, millaisia pankkihuijauksia on olemassa ja kuinka suojautua niiltä,
- Tiedän, millaisia pankkihuijauksia on olemassa, mutta en tiedä kuinka suojautua niiltä

- Olen kuullut erilaisista pankkihuijauksista, mutta en tiedä niistä juurikaan,
- En tiedä erilaisista pankkihuijauksista.

6. Mitkä seuraavista pankkihuijaustavoista ovat sinulle tuttuja?
- Hakukonehuijaus
- Huijauspuhelut
- Rakkaushuijaus
- Sijoitushuijaus
- Tietojenkalastelu tekstiviestillä tai sähköpostilla
- Tietojenkalastelu sosiaalisen median kautta
- Muu, (vapaakenttä)

7. Onko pankkihuijauksista ja turvallisesta pankkiasioinnista mielestäsi saatavilla tarpeeksi tietoa?
- Kyllä
- Ei

8. Miltä taholta haluaisit saada lisätietoa pankkihuijauksista ja turvallisesta pankkiasioinnista?
- Pankeilta
- Viranomaisilta
- Oppilaitoksilta
- Työpaikoilta
- Muu (vapaakenttä)

9. Miten haluaisit saada lisätietoa pankkihuijauksista ja turvallisesta pankkiasioinnista?
- Video-oppaat
- Verkkokurssit
- Artikkelit tai blogikirjoitukset
- Infolehdet tai oppaat
- Sosiaalinen media (esim. Tiktok tai Instagram)
- Muu (vapaakenttä)

10. Minkälainen pankkihuijaus on kyseessä? "Henkilö A haluaa päästä Omakantaan ja hakee Googlesta "Omakanta". A erehtyy klikkaamaan Omakannan sivun näköiselle valesivustolle, jonne syöttää verkkopankkitunnuksensa ja vahvistuskoodin. Valesivustolle syötettyjen tietojen avulla huijari pääsee käsiksi A:n verkkopankkiin ja siirtää sieltä A:n varat ulkomaalaiselle tilille."
- Sijoitushuijaus
- Tietojenkalastelu
- Rakkaushuijaus
- Hakukonehuijaus
- Identiteettivarkaus
- Huijauspuhelu

11. Miten voit varmistaa, että olet kirjautumassa pankin oikealle verkkosivustolle?
- Klikkaamalla ensimmäistä Googlen hakutulosta "pankin nimi kirjautuminen"
- Tarkistamalla, että verkkosivuston osoite alkaa "https://" ja sisältää pankin nimen
- Kirjautumalla sisään sivustolla, joka näyttää pankin viralliselta sivulta
- Tarkistamalla verkkosivuston taustavärin

12. Onko pankki koskaan oikeutettu pyytämään sinulta verkkopankkitunnuksia puhelimitse tai sähköpostilla?
- Kyllä
- Ei
- Vain, jos on hätätilanne

13. Oletko joutunut pankkihuijauksen uhriksi?
- Kyllä
- En ole, mutta minuun on kohdistunut huijausyritys
- En ole

14. Minkä tyyppinen pankkihuijaus oli kyseessä, jonka uhriksi jouduit?

- Hakukonehuijaus
- Huijauspuhelut
- Rakkaushuijaus
- Sijoitushuijaus
- Tietojenkalastelu tekstiviestillä tai sähköpostilla
- Tietojenkalastelu sosiaalisen median kautta
- Muu, (vapaakenttä)

15. Mitä siitä seurasi, kun jouduit pankkihuijauksen uhriksi?
- Taloudellinen tappio
- Identiteettivarkaus
- Psyykkistä haittaa
- Muu (vapaakenttä)

16. Mikäli olet joutunut hujauksen uhriksi, niin oletko kertonut asiasta muille?
- Kyllä
- Kyllä, mutta vain läheisille
- En

17. Minkälainen huijausyritys tai -yrityksiä sinuun on kohdistunut?
- Hakukonehuijaus
- Huijauspuhelut
- Rakkaushuijaus
- Sijoitushuijaus
- Tietojenkalastelu tekstiviestillä tai sähköpostilla
- Tietojenkalastelu sosiaalisen median kautta
- Muu, (vapaakenttä)

18. Oletko ilmoittanut epäillystä huijauksesta eteenpäin?
- Kyllä, pankille
- Kyllä, poliisille

- En ilmoittanut

19. Onko sinulla muita ajatuksia tai kokemuksia turvallisesta pankkiasioinnista?
- Muu (vapaakenttä)