Turvallinen pankkiasiointi ja pankkihuijaukset

Ines Haapalainen

Haaga-Helia ammattikorkeakoulu
Liiketalouden koulutusohjelma
Amk-opinnäytetyö
2022

Tiivistelmä

Tekijä(t)
Ines Haapalainen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Turvallinen pankkiasiointi ja pankkihuijaukset

Sivu- ja liitesivumäärä
26 + 11

Tämä toiminnallinen opinnäytetyö ja sen liitteenä oleva Turvallinen pankkiasiointi ja pankkihuijaukset -opas käsittelee peruspankkipalveluita ja niiden turvallista käyttöä henkilöasiakkaan näkökulmasta.

Opinnäytetyössä käsitellään henkilöasiakkaan peruspankkipalveluita, joita ovat käyttötili, maksukortti ja verkkopankkitunnukset, joihin sisältyy vahva sähköinen tunnistautuminen. Näiden palveluiden tunteminen on oleellista turvallisen pankkiasioinnin kannalta. Opinnäytetyössä käsitellään pankkihuijauksia, joissa sivutaan ohuesti peruspankkipalveluiden lisäksi myös sijoitustuotteita.

Opinnäytetyön liitteenä olevan oppaan tarkoitus on toimia henkilöasiakkaan apuna pankkipalveluiden käytössä digitaalisessa käyttöympäristössä. Opas sisältää ohjeita, joita henkilöasiakkaan olisi hyvä noudattaa arjessaan käyttäessään pankkipalveluitaan. Nyky-yhteiskunnassa pankkipalveluihin kohdistuu paljon erilaisia huijausmuotoja, jotka asiakkaan on hyvä osata tunnistaa. Oppaasta löytyy yleisimpien huijauksien tunnusmerkit sekä ohjeet, miten toimia, jos joutuu pankkihuijauksen uhriksi.

Opinnäytetyö alkaa johdannosta, jossa on kuvattu aiheen valintaa ja rajausta. Lisäksi käydään läpi opinnäytetyön rakenne sekä keskeiset käsitteet. Toisessa luvussa on tietoperusta. Ensimmäisenä käydään läpi tietosuojaa sekä kyberturvallisuutta, jotka ovat osa digitaalisia palveluita. Työssä tutustutaan pankkien tarjoamiin peruspankkipalveluihin tuotekohtaisesti sekä pankkitoimintaa sääntelevään lainsäädäntöön, joka auttaa tarkemmin ymmärtämään pankkien tuotetarjoamaa ja tuotteiden käyttöä. Toisen luvun lopussa avataan huijauksia, joihin henkilöasiakas voi törmätä käyttäessään peruspankkipalveluita sekä niiden tunnusmerkkejä.

Kolmannessa luvussa käydään läpi liitteenä löytyvän oppaan tarpeellisuutta ja toteutusta. Neljännessä eli viimeisessä luvussa tarkastellaan oppaan lopputulosta ja kehitysehdotuksia. Tämän luvun lopussa on oman oppimisen arviointi.

Opinnäytetyö on toteutettu vuoden 2022 elo – marraskuun aikana.

Asiasanat
Pankki, peruspankkipalvelut, verkkohuijaus, pankkihuijaus

Sisällys

1 Johdanto

Vuoden 2022 kesä oli poikkeuksellista aikaa pankkimaailmassa. Erilaisia huijausyrityksiä, joissa kalastellaan ihmisten verkkopankkitunnuksia, esiintyi laajalti. Verohallinto tiedotti 7.6.2022, että Verohallinnon nimissä kiersi huijausviestejä niin sähköpostitse kuin tekstiviestitse, joissa luvattiin Verohallinnolta hyvitystä viestin vastaanottajalle. Sen lisäksi suomalainen pankki S-Pankki tiedotti ensimmäisen kerran kesäkuussa 2022, että huijausviestejä levisi pankin nimissä tekstiviestitse. Viesteissä varoitettiin asiakkaita oudosta toiminnasta tilillä ja ohjattiin painamaan viestissä olevaa linkkiä, joka ohjasi verkkopankin näköiselle huijaussivustolle. Kyseisessä tekstiviestihuijauksessa valitettavaa oli se, että huijausviestit näkyivät samassa viestiketjussa kuin pankin itse lähettämät viestit. (Poliisi 2022.)

Teknologian kehityksen mukana myös rikollisuus on muuttunut, ja erilaiset huijausyritykset ovat harmillisesti lähes arkipäivää. Pankkipalveluihin kohdistuvat huijaukset voivat pahimmillaan aiheuttaa suurta taloudellista haittaa uhrille. Tämän takia huijauksista pyritään varoittamaan kansalaisia aktiivisesti. Esimerkiksi lokakuussa vietetään vuosittain Euroopan kyberturvallisuuskuukautta (ECSM) ja vuonna 2022 pääteemoina olivat tietojenkalastelu ja kiristyshaittaohjelmat. Kyseisen kampanjan tavoitteena on parantaa kyberturvallisuutta ja tarjota ajantasaista tietoa tietoturvasta. (Kyberturvallisuuskeskus 20.10.2022) Suomessa finanssialan toimijat, Poliisi, Kyberturvallisuuskeskus, Kuluttajaliitto, Digi- ja väestötietovirasto, Kela sekä Microsoft järjestivät yhteistyössä vuoden 2021 lopussa Varo, varmista, varoita -kampanjan, jonka tarkoituksena oli varoittaa rikollisista huijauksista. Kampanjan materiaalien mukaan lokakuuhun 2021 mennessä suomalaiset olivat menettäneet verkkorikollisuudelle 35 miljoonaa euroa. Huijauksien osuus, jossa tekijä esiintyi pankkina, oli 9 miljoonaa euroa. (Digi- ja väestötietovirasto 2021.)

Vaikka pankit ja viranomaiset pystyivät vuonna 2021 lokakuuhun mennessä estämään tai palauttamaan rikollisille siirtymässä ollutta rahaa noin 20 miljoonan euron edestä, on huijauksien kautta saatu rikoshyöty edelleen korkea. Myöskään kaikkia huijauksia ei raportoida poliisille, joten tarkkaa huijausten määrää tai niistä aiheutuvaa taloudellista menetystä ei ole tiedossa. (Digi- ja väestötietovirasto 2021.)

Uutisointi pankkihuijauksista on mediassa usein näyttävää, mutta silti huijauksen uhriksi päätyy monia suomalaisia. Arkielämässä esiintyy huijauksien lisäksi muitakin pankkipalveluihin kohdistuvaa väärinkäyttöä, kuten maksukortin lainaamista perheenjäsenten tai kavereiden kesken. Koronapandemian seurauksena pankkipalvelut ja asiakastapaamiset ovat vahvemmin siirtyneet sähköisiin kanaviin. Silloin pankkien fyysisiä konttoreita suljettiin tai asiakkaita palveltiin vain ajanvarauksella. (Palmgren 9.9.2020.) Asiakas siis pystyy avaamaan perinteisen konttorilla käynnin li-

säksi palvelunsa verkkopankissa itsenäisesti. Vaikka konsepti on asiakkaan näkökulmasta joustava ja kätevä, ei hänellä ole pankkialan ammattilaista kertomassa tuotteiden toiminnasta tai yleisistä sopimusehdoista, jolloin palveluiden turvallinen käyttö saattaa olla puutteellista.

1.1 Tavoitteiden kuvaus

Opinnäytetyön päätavoitteena on luoda opas turvallisesta pankkiasioinnista. Opas on suunnattu kaikille peruspankkipalveluita käyttäville pankin henkilöasiakkaille Suomessa. Oppaassa kuvataan, miten peruspankkipalveluita käytetään turvallisesti sekä miten henkilöasiakas voi tunnistaa yleisimmät pankkipalveluiden käyttöön kohdistuvat huijausmuodot, kuten dokumenttihuijauksen ja tietojenkalastelun. Tarkoituksena on, että henkilöasiakas saa selkeän kokonaiskuvan peruspankkipalveluiden turvallisesta käytöstä sekä osaa tunnistaa ja välttää yleisimmät pankkihuijaukset.

Päätavoitteen lisäksi opinnäytetyön alatavoitteena on löytää vastaukset seuraaviin kysymyksiin:

- Mitä on turvallinen pankkiasiointi?
- Mitä riskejä pankkiasiointiin liittyy?
- Miten pankkipalveluihin kohdistuvilta riskeiltä voi suojautua?
- Mitä vastuita ja velvollisuuksia henkilöasiakkaalla on turvalliseen pankkiasiointiin liittyen?
- Mitä vastuita ja velvollisuuksia pankilla on turvalliseen pankkiasiointiin liittyen?

1.2 Opinnäytetyön aiheen rajaus ja rakenne

Opinnäytetyön aihe on rajattu henkilöasiakkaiden peruspankkipalveluiden käyttöön Suomessa. Kyse on vähittäispankin toiminnasta, eli pankista, joka tarjoaa palveluita tavallisille ihmisille (Pulkkinen 2019). Lähes jokainen suomalainen on vähintään yhden pankin asiakas, joten aiheen kohderyhmä on kattava.

Laki luottolaitostoiminnasta (8.8.2014/610) 15 luvun 16 § säätää, että talletuspankilla on velvollisuus tarjota peruspankkipalveluita Euroopan unionin (EU) ja Euroopan talousalueella (ETA) laillisesti asuvalle luonnolliselle henkilölle. Sama laki ei siis koske esimerkiksi pankin yritys- tai yhdistysasiakkaita. Kyseiseen lakiin nojaten aiheen rajaus on tehty koskettamaan vain peruspankkipalveluita, koska ne ovat lähes kaikkien asiakkaiden käytössä.

Vaikka kyseinen laki säätää velvollisuudesta tarjota palveluita EU- ja ETA-alueella laillisesti asuville, on aiheen rajaus rajattu Suomeen myös kansallisen säädännön tarkastelun takia. Pankkien toimintaa ohjaa luottolaitostoimintalain lisäksi Suomessa Finanssivalvonta, joka on rahoitus- ja vakuutustoiminnan valvontaviranomainen ja se toimii Suomen Pankin yhteydessä (Finanssivalvonta 2022). Finanssivalvonnan toiminta perustuu lakiin Finanssivalvonnasta (19.12.2008/878), 1 luvun 3

§:n mukaan Finanssivalvonnan tehtävä on esimerkiksi seurata ja arvioida peruspankkipalveluiden saatavuutta ja hinnoittelua sekä yleisesti valvoa finanssimarkkinoita.

Aihe on rajattu peruspankkipalveluihin niiden yleisyyden takia ja koska peruspankkipalveluiden tuotteet ovat yleisesti pankkihuijausten ja muun väärinkäytön kohteina. Muita pankin tuotteita ovat esimerkiksi luottotuotteet, kuten luottokortti ja laina. Markkinoilla on tarjolla lisäksi erilaisia sijoitustuotteita, joihin voi kohdistua sijoitushuijauksia.

Tämä opinnäytetyö koostuu neljästä osasta, joista ensimmäinen on johdanto. Johdannossa käsitellään opinnäytetyön taustaa, tavoitteet sekä rakenne ja keskeisimmät käsitteet. Pääluvussa kaksi perehdytään tietoperustaan. Alaluvuissa käydään läpi yleisesti, miten tietoturva näkyy pankkitoiminnassa ja mitä ovat peruspankkipalvelut. Näiden lisäksi alaluvuissa käsitellään yleisimpiä pankkihuijauksia sekä niiden tunnusmerkkejä.

Luvussa kolme esitellään opinnäytetyön liitteenä oleva tuote eli opas peruspankkipalveluiden turvalliseen käyttöön henkilöasiakkaalle. Tässä luvussa käydään myös läpi opinnäytetyön kirjoittamisprosessin vaiheet ja oppaan toteutus. Neljännessä eli viimeisessä luvussa on yhteenveto opinnäytetyöprosessista, joka sisältää oppaan ja koko opinnäytetyöprosessin onnistumisen tarkastelun, kehitysehdotukset sekä oman oppimisen tarkastelun.

1.3 Keskeiset käsitteet

Pankki on rahoitusmarkkinoiden osa, joka mahdollistaa rahan liikkumisen kotitalouksien ja yritysten välillä. Talletuspankki on pankki, joka vastaanottaa asiakkailta rahatalletuksia ja myöntää lainoja. (Pohjola 2019, 205). Pankilla on luottolaitoslain (8.8.2014/610) 15 luvun 6 §:n mukaan velvollisuus tarjota peruspankkipalveluita ETA-alueella laillisesti asuvalle henkilölle. Saman lain toisessa momentissa todetaan, että peruspankkipalveluiden tarjoamisesta saa kieltäytyä rahanpesuun ja terrorismin rahoittamiseen tai eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä annetusta laista (29.12.1967/659) johtuvasta syistä.

Peruspankkipalveluita ovat pankkitili sekä siihen kytketyt tilinkäyttövälineet, kuten debit-maksukortti ja verkkopankkitunnukset vahvalla sähköisellä tunnistautumisella. Peruspankkipalveluihin kuuluu mahdollisuus toteuttaa tilisiirtoja ja nostaa sekä tallettaa käteistä. (Finanssivalvonta 5.9.2018.)

Verkkohuijaus tarkoittaa yleisesti verkossa tehtyä huijausta, jossa esimerkiksi huijari pyrkii saamaan rahaa uhrilta vaikka myymällä jotain, josta uhri maksaa etukäteen, muttei koskaan saa tuotetta (Albrecht 2017).

Yleisesti pankkihuijauksina voidaan pitää sellaisia huijaustyyppejä, jossa huijarin tavoitteena on saada käyttöön uhrin pankkipalvelut tai niiden osa. Pankkihuijaukset ovat samaan aikaan myös verkkohuijauksia. Yleisimpiä henkilöasiakkaaseen kohdistuvia pankkihuijauksen tyyppejä ovat sähköposti- ja tekstiviestihuijaukset (phishing- ja smishing-huijaukset), rakkaushuijaus, huijauspuhelu, sijoitushuijaus, verkkokauppahuijaukset, identiteettivarkaus tai toimiminen muulina, eli rikollista rahaa pyritään siirtämään eteenpäin tilien kautta, jolloin rahan alkuperää pyritään peittelemään. (Nordea 2022.)

2 Turvallinen pankkiasiointi

Jotta pankkipalveluiden väärinkäytön vaikutukset ja pankkihuijausten riskit voidaan ymmärtää, on ensimmäiseksi tarkasteltava, mitä tietosuoja ja tietoturva tarkoittavat pankkimaailmassa sekä mitä pankkien peruspalvelut tarkalleen ovat. Pankkiasioinnin turvallisuutta on hyvä pohtia, sillä finanssialaan kohdistuvat häiriöt ja epävarmuudet vaikuttavat nopeasti yksilön ja yhteiskunnan arkeen (Huoltovarmuuskeskus 2020).

2.1 Tietosuoja pankkimaailmassa

Euroopan unionin yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) (2016/679/EU) sai alkunsa Euroopan komission ehdotuksesta vuonna 2012, kun huomattiin, ettei tietosuojalainsäädäntö vastannut nykyaikaisia digitaalisen ympäristön tarpeita. Asetus tuli voimaan vuonna 2016 ja sitä alettiin soveltamaan 25.5.2018 siirtymäkauden päättymisen jälkeen (Korpisaari, Pitkänen & Warma-Lehtinen 2022, 1). Ennen tätä aikaa, Suomessa noudatettiin henkilötietolakia (22.4.1999/523). Henkilötietolain 1 luvun 1 §:n mukaan sen tarkoituksena on turvata yksityisyyden suojaa henkilötietoja käsiteltäessä ja edistää hyvän tavan mukaista tietojenkäsittelytavan kehittämistä ja noudattamista.

Tietosuoja-asetuksen 4 artiklan mukaan henkilötiedoilla tarkoitetaan sellaisia tietoja, jotka voidaan yhdistää yksittäiseen luonnolliseen henkilöön. Sellaisia tietoja ovat esimerkiksi nimi, henkilötunnus, osoite, henkilöllisyysasiakirjan tiedot ja IP-osoite.

Tietoturva on osa tietosuojaa. Sillä tarkoitetaan tietojen, palveluiden, järjestelmien sekä tietoliikenteen suojaamista teknisin keinoin niin, että tiedot ovat saatavilla ja käytettävissä vain niitä käsitteleville henkilöille. Tietoturvaa on esimerkiksi järjestelmien käyttöoikeuksien määrittely, käsittelytapahtumien kirjaukset sekä järjestelmien turvaaminen muilta tietoturvauhkilta kuten viruksilta ja haittaohjelmilta. Koprisaaren, Pitkäsen ja Warma-Lehtisen (2022, 371) tulkinnan mukaan tietoturvan katsotaan olevan kokonaisuus, joka koostuu tietojen luottamuksellisuudesta, eheydestä, saatavuudesta, todennuksesta, vastuullisuudesta ja kiistämättömyydestä.

Vuonna 2020 Huoltovarmuuskeskus teki kyberturvallisuusselvityksen, jossa selvitettiin eri toimialojen kyberturvallisuuden taso. Kyseisessä selvityksessä finanssiala sai parhaimman tuloksen, joka viittaa siihen, että kyberturvallisuus on johdonmukaisesti toteutettu. Finanssialalla on yleisesti hyvin varmistettu ja resursoitu perustietoturva ja tietoturvallisuutta kehitetään jatkuvasti. Toisaalta on hyvä huomioida, että digitaalinen toimintaympäristö muuttuu nopeasti, joka asettaa jatkuvan tar-

peen turvallisuuden ylläpitämiselle sekä riskienhallinnalle. Yli-Huttulan (16.9.2022) mukaan pankeilla on muutenkin korostunut velvollisuus suojata asiakastietoja sekä asiakkaiden varoja, jonka takia pankkien tietoturvaratkaisut ovat asiakkaiden luottamuksen ansaitsemiseksi tärkeitä.

Pankeilla on olemassa velvollisuuksia, joiden noudattamisessa yhdistyy tietosuoja-asetuksen tunteminen. Pankeilla on rahanpesulakiin (laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444) perustuva velvollisuus tuntea asiakkaansa. Asiakkaan tunteminen tarkoittaa rahanpesulain 3 luvun 3 §:n mukaan sitä, että pankin on tiedettävä esimerkiksi asiakkaan henkilötiedot, taloudellinen asema ja asiakkaan tunnistamiseen käytetyn henkilöllisyysasiakirjan tiedot. Pankin on pystyttävä jälkeenpäin osoittamaan viranomaisille, kuten Finanssivalvonnalle, kuinka asiakas on tunnistettu ja mihin tietoihin tunnistaminen perustuu (Tietosuoja 2022). Asiakkaan tunnistaminen on oleellinen osa pankkipalveluiden tarjoamista, josta kerrotaan lisää luvuissa 2.2. ja 2.3.

Rahanpesulain 3 luvun 3 §:n mukaan asiakkaan tuntemistietojen kuuluu olla ajankohtaisia sekä olennaisia, ja tietoja kuuluu säilyttää viisi vuotta vakituisen asiakassuhteen päättymisen jälkeen. Tietosuoja-asetuksen artikla 17 säätää, että henkilöllä on oikeus tulla unohdetuksi, eli pyytää rekisterinpitäjää poistamaan häntä koskevat tiedot. Pankilla on kuitenkin velvollisuus säilyttää tietoja myös asiakassuhteen päättymisen jälkeen, mutta asiakkaalla on mahdollisuus pyytää henkilötietojen käsittelyn rajoittamista (Euroopan Komissio s.a.).

Pankin henkilökunnalla on velvollisuus noudattaa pankkisalaisuutta henkilötietoja käsitellessä. Pankkisalaisuudesta on säädetty luottolaitoslain 15 luvun 14 §:n ja se tarkoittaa, ettei pankkitoimihenkilö tai toimielimen jäsen saa kertoa asiakastietoja ulkopuolisille. Pankkisalaisuuden alaista tietoa ovat esimerkiksi sellaiset tiedot asiakkaasta, joilla asiakas voidaan yksilöidä tiedon perusteella. (Finanssiala 2021.)

2.2 Peruspankkipalvelut

Peruspankkipalveluiden katsotaan muodostuvan pankkitilistä, jossa rahaa voi säilyttää, sekä tilin käyttövälineistä, joilla rahaa pystyy hyödyntämään. Peruspankkipalveluihin liittyvät tilin käyttövälineet ovat debit-maksukortti sekä pankkitunnukset. Pankista riippuen peruspankkipalvelut voivat olla maksuttomat tai niihin voi kuulua kuukausimaksu. Erilaisia palvelumaksuja saattaa pankista riippuen tulla tilinkäyttövälineiden kautta, esimerkiksi kortin käyttö euroalueen ulkopuolella aiheuttaa valuutanmuunnosmaksuja. Pankkipalvelut voi avata joko pankin konttorissa tai yhä useammin pankin verkkopankissa, tunnistautuneena toisen pankin verkkopankkitunnuksilla. (Finanssivalvonta 5.9.2018.)

Turvallisen pankkiasioinnin kannalta on erittäin olennaista, että lähtökohtaisesti pankkipalvelut ovat henkilökohtaisia. Asiakkaalla on mahdollisuus kuitenkin esimerkiksi avata yhteinen tili, vaikka taloustili perheenjäsenen kanssa, tai alaikäiselle voi hankkia rinnakkaiskortin vanhemman luottokorttiin. Näistä huolimatta, pankkitunnukset sekä maksukortti ovat aina henkilökohtaisia. (Nordea s.a.a.)

2.2.1 Käyttötili

Tilityyppejä on olemassa erilaisia, kuten käyttötili, säästötili, ensiasunnon ostajalle suunnattu säästötili eli ASP-tili ja määräaikaistili. Tässä opinnäytetyössä tutustaan näistä ensimmäiseen, eli käyttötiliin. Käyttötilillä tarkoitetaan sellaista tiliä, jossa voi säilöä rahaa sekä tehdä käteistalletuksia ja -nostoja. Käyttötiliin pystyy yhdistämään maksukortin ja pankkitunnukset. Näiden palveluiden avulla tililtä pystyy esimerkiksi hoitamaan laskujen maksun verkkopankissa ja maksamisen kortilla kaupparessun yhteydessä. (Alhonsuo, Nisén, Nousiainen, Pellikka, Sundberg 2012, 199.)

Tiliä avattaessa allekirjoitetaan tilisopimus, jossa lukee sopimusehdot. Pankilla on mahdollisuus maksaa asiakkaan tilille korkoa. Talletuskorko on niin ikään pankin korvaus asiakkaalle siitä, että asiakas on laittanut rahaa pankkitililleen. Koron ajatus on kannustaa asiakkaita tallettamaan rahaa tilille. Pankkitileillä olevaa rahaa pankki hyödyntää myöntämällä muille asiakkaille esimerkiksi lainoja tai sijoittamalla. Pankit, jotka toimivat kokonaan verkossa, maksavat lähtökohtaisesti enemmän korkoja, koska rahaa ei mene asiakaskonttoreiden ylläpitämiseen. (Woodard 31.5.2022.) Kesäkuun 2022 lopussa suomalaisten kotitalouksien talletuskanta oli 113 miljardia euroa ja keskikorko käyttötileillä oli 0,02 prosenttia. Suomalaisten kotitalouksien talletustilien varoista 92 prosenttia on käyttötileillä. (Suomen Pankki 2022.)

Tilillä olevia rahoja suojaa talletussuojajärjestelmä, josta Suomessa vastaa Rahoitusvakausvirasto. Tämän järjestelmän tarkoituksena on suojella tilillä olevia varoja, jos talletuspankki todetaan pysyvästi maksukyvyttömäksi. Talletussuoja kattaa 100 000 euroa tallettajan yhdessä pankissa olevista varoista. (Rahoitusvakausvirasto s.a.)

2.2.2 Maksukortti

Henkilöasiakkaalle tyypilliset tarjottavat korttituotteet ovat debit- tai credit-kortteja, tai näiden yhdistelmiä eli yhdistelmäkortteja. Debit-kortilla maksaessa maksu veloitetaan korttiin liitetyltä tililtä (Alhonsuo ym. 2012, 208). Credit-kortti sisältää luotto-ominaisuuden, eli pankin myöntämää lainaa, jolla asiakas pystyy maksamaan ja hyödyntämään luottokortin tarjoamaa maksuaikaa. Asiakkaan maksukyky on oltava riittävä ja pankki tarkasteleekin asiakkaan maksukykyä luottohakemuksen yhteydessä. (Alhonsuo ym. 2012, 207).

Kortilla maksaessa on asiakkaan annettava nelinumeroinen varmennuskoodi eli PIN-koodi. Debitkortilta löytyy sen lisäksi mahdollisuus lähimaksuun, eli maksamiseen ilman tunnuslukua. Ilman tunnuslukua on mahdollista maksaa alle 50 euron ostoksia. Silti PIN-koodia kysytään satunnaisesti turvallisuussyistä. (OP s.a.a.) Lähimaksamisen lisäksi viime vuosina on yleistynyt mobiilimaksamisen palvelut, eli kortin pystyy yhdistämään älylaitteeseen ja maksun voi näin ollen hoitaa älypuhelimella tai -kellolla. Lähimaksusta poiketen, mobiilimaksamisella voi tehdä yli 50 euron ostoksia ilman PIN-koodia. (OP s.a.b.)

Asiakas pystyy vaikuttamaan kortin turvalliseen käyttöön itse asettamalla kortille turvarajoituksia. Turvarajoja voi asettaa kortin euromääräiseen käyttöön käteisnostoissa, verkko-ostoksissa sekä tavallisissa korttiostoksissa, kun korttia käytetään fyysisesti kaupassa. Ostorajat ovat vuorokausikohtaisia. Kortille pystyy asettamaan myös maakohtaisia rajoituksia. Kun kortille valitaan käyttöalueeksi esimerkiksi Suomi, ei kortti toimi ulkomailla. Kortin turvarajoja asiakas voi hallita verkkopankistaan. (OP s.a.c.)

2.2.3 Verkkopankkitunnukset

Verkkopankkitunnuksilla tarkoitetaan palvelua, joiden avulla asiakkaalla on mahdollisuus kirjautua pankkinsa verkkopalveluun ja sieltä käsin hallita omia pankkipalveluitaan. Pankkitunnukset koostuvat usein eri osista, ja tunnistautumisen tapoja verkkopankkiin voi olla useita. Perinteiset pankkitunnukset koostuvat jonkin muotoisesta käyttäjätunnuksesta, salasanasta ja varmennuksesta, joka voi olla esimerkiksi tunnuslukutaulukko. Esimerkiksi Nordea tarjoaa tunnistautumiseen erillistä tunnuslukulaitetta, jolla varmennetaan kirjautuminen. (Nordea s.a.b.)

Verkkopankkitunnuksilla voi kirjautua omiin tietoihin joko pankin verkkosivujen kautta tai käyttämällä pankin tarjoamaa mobiilisovellusta. Sovelluksessa voidaan käyttäjätunnuksen ja salasanan lisäksi tunnistaa asiakas älylaitetta käyttäessä biometrisellä tunnisteella, esimerkiksi kasvojen tunnistuksella tai sormenjäljellä. (Kyberturvallisuuskeskus 11.3.2022.)

2.2.4 Alaikäisen asiakkaan peruspankkipalvelut

Verrattuna täysi-ikäiseen asiakkaaseen, on alaikäisten käytössä olevat peruspankkipalvelut rajatummat. Lisäksi palveluiden suhteen on paljon pankkikohtaisia eroja. Alaikäiselle palveluiden avaamisesta vastaa alaikäisen edunvalvojat, jotka ovat yleensä alaikäisen huoltajia. Tämä tarkoittaa sitä, että kun edunvalvojia on kaksi, molemmilta tarvitaan suostumus palveluiden avaukselle. Suostumuksen voi antaa valtakirjalla, mikäli molemmat edunvalvojat eivät kykene asioimaan pankissa. (Välimäki 10.3.2022.)

Alaikäisen tilin avauksen yhteydessä edunvalvojille annetaan käyttöoikeus tiliin. Edunvalvoja voi käyttöoikeudellaan tarkistaa esimerkiksi tilin saldon tai tilitapahtumia. (Danske Bank s.a.). Edunvalvojilla on myös oikeus saada tietoja alaikäisen pankkipalveluista, vaikka tilin käyttöoikeus olisi yksin alaikäisellä (Finanssiala 2021). Huoltajien käyttöoikeus poistuu automaattisesti alaikäisen tilistä, kun alaikäinen täyttää 18 vuotta, ja sen jälkeen hän voi hoitaa pankkipalveluitaan itsenäisesti (Danske Bank s.a.).

Nordeassa on mahdollista tilata maksukortti edunvalvojien suostumuksella 6-vuotiaalle, kun taas S-Pankissa ja OP:ssa kortin saa 7-vuotiaana, myöskin edunvalvojien suostumuksella. (Nordea s.a.a; S-Pankki 2018; Välimäki 10.3.2022.) Myös pankkitunnuksien kohdalla on pankkikohtaisia eroja etenkin alaikäisille tarjottavien palveluiden suhteen. Esimerkiksi OP tarjoaa alaikäisille asiakkailleen pääsyn rajoitetusti verkkopankkiin jo 7-vuotiaana, jossa pystyy katsomaan tilin saldon sekä tekemään maksuja tililtä, johon alaikäisellä on käyttöoikeus. Danske Bankissakin alaikäinen pääsee harjoittelemaan jo 8-vuotiaana verkkopankin käyttöä (Danske Bank s.a.). Vahvan sähköisen tunnistamisen alaikäinen saa käyttöön vasta 12-vuotiaana (OP s.a.d).

2.3 Vahva sähköinen tunnistaminen

Suomalaisessa yhteiskunnassa vahva sähköinen tunnistus on arkipäivää. Joillakin toimialoilla asiakas on tunnistettava vahvasti lakisääteisten vaatimusten takia, kuten pankki- ja terveyspalveluita hoitaessa. Vahva tunnistaminen on yleistä myös muilla aloilla sen tietoturvallisuuden takia. (Signicat 28.5.2021.)

Pankkitunnukset toimivat vahvan sähköisen tunnistautumisen välineenä. Se tarkoittaa sitä, että oman henkilöllisyyden pystyy todistamaan verkossa tunnistautumalla oman pankkinsa verkkopankkitunnuksilla. Pankkitunnuksien lisäksi vahvan tunnistuksen saa käyttöön teleoperaattorien mobiilivarmenteen avulla sekä Digi- ja väestötietoviraston kansalaisvarmenteella, mikä on kylläkin harvinaisempaa. (Signicat 28.5.2021.) Pankki toimii tunnistuspalvelun tarjoajana, jolloin toimintaa säätelee laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (tunnistus- ja luottamuspalvelulaki 7.8.2009/617). Tunnistus- ja luottamuspalvelulain 5 luvun 42 a §:n mukaan tunnistautumisen palveluita sekä niiden palveluntarjoajien toimintaa valvoo Suomessa Liikenne- ja viestintävirasto Traficom.

Kun hakijalle myönnetään vahvan sähköisen tunnistuksen väline, tulee hänet tunnistus- ja luottamuspalvelulain 3 luvun 17 §:n mukaan ensitunnistaa henkilökohtaisesti Suomen, ETA-alueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämästä passista tai henkilökortista tai vaihtoehtoisesti verkkopankissa toisen pankin vahvoilla verkkopankkitunnuksilla. Mikäli hakijan henkilöllisyyttä ei voida todeta luotettavasti, ensitunnistuksen tekee poliisi. Tällöin asiakkaan tulee

hakeutua poliisilaitokselle voimassa olevan passin tai henkilökortin kanssa, jossa täytetään hakemus tunnistautumisesta tunnistusvälinettä varten. Jos hakija pystytään poliisin toimesta tunnistamaan, annetaan henkilön tunnistamisesta todistus, joka postitetaan suoraan tunnistuspalvelun tarjoajalle. Todistus muodostuu myös siinä tilanteessa, mikäli hakijaa ei pystytä tunnistamaan. (Poliisi s.a.)

Tunnistus- ja luottamuspalvelulain 3 luvun 23 § säätää tunnistusvälineen haltijan velvollisuuksista, joita ovat tunnistusvälineen sopimusehtojen mukainen käyttö sekä huolellinen säilytys. Tunnistamisen välinettä ei saa luovuttaa muiden henkilöiden käyttöön. Siinä missä tunnistusvälineen haltijalla on velvollisuus ilmoittaa viipymättä tunnistusvälineen katoamisesta tai väärinkäytöstä tunnistusvälineen tarjoajalle, on tarjoajalla saman lain 3 luvun 25 §:n mukaan velvollisuus tarjota mahdollisuus ilmoittaa tällaisesta toiminnasta milloin tahansa sekä peruuttaa tai estää tunnistusvälineen käyttö viipymättä. Lisäksi saman lain 3 luvun 26 §:n mukaan tunnistusvälineen tarjoaja voi peruuttaa tai estää tunnistusvälineen käytön esimerkiksi silloin, kun epäillään, että tunnistusvälinettä käyttää joku muu, tunnistusvälinettä käytetään sopimusehtojen vastaisesti vai tunnistusvälineen käytön turvallisuus on muuten vaarantunut. Tällainen tilanne on esimerkiksi tekstiviestihuijaus, johon asiakas luovuttaa pankkitunnuksensa.

Tilanteessa, jossa on antanut tarkoituksella tai vahingossa pankkitunnuksensa toisen käyttöön, on ilmoitettava välittömästi pankille. Tämä johtuu siitä, että tunnistus- ja luottamuspalvelulain 3 luvun 27 §:n mukaan tunnistusvälineen haltija vastaa tunnistusvälineen oikeudettomasta käytöstä silloin, jos hän on luovuttanut tunnistusvälineen jollekin toiselle, tunnistusväline on kadonnut tai huolimattomuudesta johtuen päätynyt toisen henkilön käsiin tai ei ole ilmoittanut tunnistusvälineen katoamisesta tai toisen haltuun joutumisesta välittömästi. Tunnistusvälineen haltija ei ole vastuussa tunnistusvälineen oikeudettomasta käytöstä silloin, kuin tunnistusvälinettä on käytetty haltijan tekemän ilmoituksen jälkeen.

Pankin on tärkeää puuttua pankkitunnuksiin liittyvään väärinkäyttöön välittömästi, sillä tunnistus- ja luottamuspalvelulain 5 luvun 45 §:n perusteella Liikenne- ja viestintävirasto voi antaa huomautuksen ja uhkasakon lain rikkomisesta. Saman lain 5 luvun 45 a §:n mukaan Liikenne- ja viestintävirasto voi kieltää tai keskeyttää esimerkiksi tunnistautumismenetelmän tarjoamisen vahvan sähköisen tunnistautumisen välineenä, mikäli kyseistä lakia tai tunnistautumisesta ja luottamuspalveluista annettua Euroopan unionin asetusta (Euroopan parlamentin ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 2014/910/EU) ei noudateta. Kyseessä on väliaikainen toimi, joka on voimassa enintään kolme kuukautta.

2.4 Pankkimaailman huijaukset

Henkilöasiakkaan pankkipalveluihin kohdistuvia huijauksia on monenlaisia. Usein niiden taustalla on järjestäytynyttä kansainvälistä rikollisuutta, ja rikokset tehdäänkin suurimmilta osin ulkomailta käsin (Rikosuhripäivystys s.a.a).

Kyberrikollisuus voidaan jakaa kahteen alalajiin: tietoverkkoihin ja tietotekniikkaan kohdistuvat tietotekniikkarikokset sekä tietotekniikkaa ja tietoverkkoja hyväksikäyttäen tehdyt rikokset. Tässä opinnäytetyössä tutustutaan näistä jälkimmäiseen. Tietotekniikkaa ja tietoverkkoja hyväksikäyttäen tehdyt rikokset kattavat erilaiset petokset ja tietojen kalastelun, mutta myös rahanpesun, kiristyshaittaohjelmat ja huumausainerikollisuuden. (Rikosuhripäivystys s.a.b.)

Petoksiin luetellaan useita huijaustyyppejä. Yksiä vanhimpia huijausmuotoja on dokumenttihuijaukset, kansan kielellä tutummin rakkaushuijaus tai nigerialaishuijaus. Kyseisessä huijaustyypissä huijari ottaa yhteyttä uhriin esimerkiksi sosiaalisen median kautta esittäen toista henkilöä. Huijari voi esittää olevansa kaukainen sukulainen, joka lupaa uhrille suurta perintöä, kunhan maksaa perinnöstä ennakkosumman. Huijari pyrkii saamaan rahaa uhrilta, eikä pyri saamaan haltuunsa uhrin pankkituotteita. Todellisuudessa uhrille luvattua perintöä ei ole olemassa. Tämä huijausmuoto on rikollisille tuottoisa. Vuoden 2022 tammi-kesäkuun välisenä aikana erilaisien pankkihuijauksien rikoshyöty on ollut 10,8 miljoona euroa, josta dokumenttihuijauksien osuus on ollut 3,8 miljoonaa euroa. (Manninen 21.9.2022.) Alla olevasta taulukosta 1 näkyy kokonaisuudessaan onnistuneet sekä estetyt pankkihuijaukset kyseisellä aikavälillä. Prosenttiosuudet kuvastavat jakaumaa kokonaismäärään nähden.

Taulukko 1. Pankkien tietoon tulleet huijaukset tammi-kesäkuussa 2022 (mukaillen Finanssiala 2022)

Huijaustapa	*Tapauksien kokonais-määrä*	*Arvo (asiakkaiden me-netetty arvo)*
Dokumentti- ja rakkaushuijaukset	716 kpl / 39 %	3 832 154 € / 35 %
Sijoitushuijaukset	172 kpl / 9 %	3 266 076 € / 30 %
Valepoliisi ja tietojenkalastelu	898 kpl / 49 %	2 602 496 € / 25 %
Toimitusjohtajahuijaukset	55 kpl / 3 %	1 133 207 € / 10 %
Huijaukset yhteensä	1 841 kpl	10 833 933 €
Estetyt ja palautuneet maksut	712 kpl / 39 %	6 675 303 € / 62 %

Tietojenkalastelu eli kansainvälisesti ”phishing” tarkoittaa huijausta, jossa huijari pyrkii samaan käyttöön uhrin henkilötietoja tai pankkitietoja. ”Smishing” tarkoittaa tietojenkalastelua erityisesti tekstiviestin tai pikaviestipalveluiden avulla. Tietojenkalasteluviestejä voi tulla myös sähköpostiin. Tyypillistä viesteissä on se, että viestin lähettäjä on ennestään tuntematon tai lähettäjän nimi on kirjoitettu väärin. Myös viestin oikeinkirjoitus saattaa olla puutteellista. Usein viestissä on linkki, jota huijari kannustaa uhria painamaan ja sitä kautta luovuttamaan tietonsa. Jotta uhri painaisi linkkiä, viestissä voidaan varoittaa pankkitilillä havaitusta oudosta toiminnasta tai luvata valtiolta saatavaa ylimääräistä korvausta – jota johdannossa käsitellyissä tosielämässä tapahtuneissa huijauksissa tehtiin. Vaikka yritys voi tavoitella asiakasta viestitse, eivät yritykset yleensä käytä suoria linkkejä. (Federal Trade Commission 2022.)

Huijausviestien lisäksi huijarit voivat käyttää puhelinhuijausta, josta käytetään kansainvälisesti termiä ”vishing”. Viestien kautta tapahtuvien huijauksien kaltaisesti huijauspuhelussa voidaan esittää pankin toimihenkilöä, viranomaista tai myös teknisen tuen työntekijää. IT-tuen työntekijänä esiintyvä henkilö saattaa ohjata uhria asentamaan laitteelleen haittaohjelman. (F-Secure 18.6.2022.)

Sijoitushuijauksessa uhria yritetään huijata sijoittamaan esimerkiksi osakkeisiin, joukkolainoihin tai kryptovaluuttoihin. Huijauksessa esimerkiksi uhri luulee sijoittavansa todelliseen osakkeeseen, mutta rahat menevätkin huijarille. (FINE Vakuutus- ja rahoitusneuvonta s.a.) Pyramidihuijaus on eräänlainen sijoitushuijaus, jossa sijoittajalle luvataan epärealistisen suuria voittoja kuvitteellisesta

sijoituskohteesta. Ensimmäiset sijoittajat saavat sijoitusvoittoja, jolloin he alkavat suosittelemaan sijoituskohdetta myös uusille sijoittajille. Verkosto kasvaa, ja uusien sijoittajien aloitusmaksut menevät heitä aikaisempien sijoittaneiden taskuihin. Pyramidihuijaukset romahtavat yleensä nopeasti, koska uusimmat sijoittajat eivät usein saa heille luvattua tuottoa. (Bloomenthal 30.9.2022.)

Muiden huijaustyyppien lailla myös sijoitushuijauksissa tyypillistä on kiireen tunteen luominen, jossa luodaan kuvaa rajoitetusta tarjouksesta, joka on liian hyvää ollakseen totta. Yhteydenotto voi tulla ulkomailta tai muuten tuntemattomalta taholta. FINE Vakuutus- ja rahoitusneuvonnan (s.a.) mukaan varmin merkki sijoitushuijauksesta on se, ettei palveluntarjoajalla ole toimilupaa. Finanssivalvonta ylläpitää rekisteriä palveluntarjoajista, joilla on toimilupa Suomessa ja jotka ovat tehneet ilmoituksen toiminnastaan. (FINE vakuutus- ja rahoitusneuvonta s.a.)

Taulukossa 1 on viimeisimpänä huijaustyyppinä mainittu toimitusjohtajahuijaus. Toimitusjohtajahuijaus on yrityksiin kohdistettu huijaus, jossa verkkorikollinen esittää olevansa yrityksen johdossa ja pyytää alaistaan äkkiä tekemään esimerkiksi tilisiirron tai maksamaan laskun. Kuten muissakin huijaustyypeissä, viesti saattaa tulla oudosta osoitteesta ja siinä vedotaan kiireeseen. Huijari saattaa myös pyytää, että hänen pyyntönsä pysyy luottamuksellisena ja painostaa alaistaan toimimaan nopeasti. Tällaisen viestin saatua on tärkeä olla toimimatta kiireen alla ja tarvittaessa keskustella oman yrityksen asiantuntijoiden kanssa, mikäli epäilee saaneensa huijausviestin. (Laakso 21.6.2022.)

Monissa pankkihuijauksissa yhdistyy rahanpesun piirteitä. Esimerkiksi jos asiakas luovuttaa verkkopankkitunnukset huijarin käyttöön tietojen kalasteluviestin kautta, voi huijari yrittää siirtää rahaa eteenpäin muiden uhrien tilille. Kyseessä on silloin rahanpesua, koska rikollisella toiminnalla hankitun rahan alkuperää pyritään häivyttämään. Kyseisessä tilanteessa muiden uhrien tilit toimivat muulitileinä. Tilin omistaja ei välttämättä tiedä joutuneensa muuliksi. (Erkkilä 5.12.2019.)

Pankkihuijaukset ovat harmillisia monelta eri näkökulmalta. Pahimmassa tapauksessa henkilöasiakas voi esimerkiksi tietojenkalastelun yhteydessä menettää rahansa sekä verkkopankkitunnuksensa, joilla huijarit voivat tehdä mittavaa vahinkoa. Mikäli joutuu pankkihuijauksen uhriksi, on tästä tärkeää ilmoittaa oman pankin asiakaspalveluun tai vaihtoehtoisesti sulkupalveluun välittömästi. Pankki pystyy sulkemaan verkkopankkitunnukset ja kortin, jotta niitä ei voi käyttää. Huijarit saattavat olla todella nopeita tekemään haluamiaan toimenpiteitä, joten palveluiden sulkeminen pikimmiten on usein ratkaisevaa. Kun palvelut on suljettu, on tapauksesta hyvä ilmoittaa poliisille ja tehdä tarvittaessa rikosilmoitus. (Rikosuhripäivystys s.a.a.)

Huijauksen uhrina saattaa jäädä tilanteessa yksin, joten on hyvä tietää se, että apua on saatavilla. Esimerkiksi Rikosuhripäivystys tarjoaa apua rikoksen uhreille ja auttavaan puhelimeen tai viestipalveluun voi olla yhteydessä myös pankkihuijauksen tapahtuessa. (Rikosuhripäivystys s.a.a.)

2.5 Pankkipalveluiden turvallinen käyttö ja väärinkäytön seuraukset

Turvallinen pankkiasiointi on monien tekijöiden summa. Se koostuu asiakkaan näkökulmasta tuotteiden ja palveluiden turvallisesta käytöstä sekä pankkihuijausten tunnistamisesta ja välttämisestä. Pankin palveluita käyttäessä on asiakkaan vastuulla, ettei asiakas esimerkiksi näytä tai anna korttiaan ja sen PIN-koodia tai pankkitunnuksiaan muiden käsiin. (S-Pankki s.a.) Pankin tehtävä turvallisen pankkiasioinnin takaamiseksi on huolehtia itse omien tietojärjestelmien kehityksestä sekä ylläpidosta (Yli-Huttula 16.9.2022). Niin asiakas kuin pankkikin voidaan heidän velvollisuuksiansa laiminlyödessään asettaa korvausvastuuseen.

Pankkien toimintaa valvoo Suomessa Finanssivalvonta ja vahvaa sähköistä tunnistautumista valvoo Suomessa Liikenne- ja viestintävirasto Traficom (Finanssivalvonta 2022, Kyberturvallisuuskeskus 11.3.2022). Pankkien velvollisuuksia ja niiden rikkomisesta aiheutuvia seurauksia sähköisen tunnistautumisen tarjoamisesta on käyty läpi opinnäytetyön alaluvussa 2.3.

Rikoslain (39/1889) 37 luku käsittelee maksuvälinerikoksia. Maksukortti on henkilökohtainen ja siinä lukee aina kortin omistajan nimi. On tärkeää, ettei korttia käytä kukaan muu kuin sen omistaja, koska sen väärinkäyttö on rikos. Rikoslain 37 luvun 8 §:n mukaan sellainen henkilö, joka esimerkiksi käyttää maksuvälinettä ilman sen haltijan lupaa tai käyttää väärennettyä maksuvälinettä on tuomittava maksuvälinepetoksesta sakkoon tai enintään kahdeksi vuodeksi vankeuteen. Saman lain 9 §:n mukaan törkeän maksuvälinepetoksen piirteitä ovat huomattava tai erityisen tuntuvan vahingon aiheuttaminen, teon erityinen suunnitelmallisuus sekä järjestäytynyt rikollisuus, joiden täyttyessä tuomio on vähintään neljä kuukautta ja enimmillään viisi vuotta vankeutta.

Toisen henkilön verkkopankkitunnusten käytössä on usein identiteettivarkauden piirteitä. Rikoslain 38 luvun 9 a §:n mukaan identiteettivarkauden tunnusmerkki on taloudellisen vahingon tai muun vähäistä suuremman haitan aiheuttaminen, jolloin tekijä on tuomittava sakkoon.

3 Opas turvalliseen pankkiasiointiin

Henkilöasiakas voi vaikuttaa pankkipalveluidensa turvalliseen käyttöön. Teot, joilla asiakas voi taata palveluiden turvallisen käytön, voivat vaikuttaa pieniltä, mutta niillä on suuri vaikutus palveluiden käytön kokonaisturvallisuuteen. Tässä luvussa tutustutaan opinnäytetyön liitteenä 1 olevaan turvallisen pankkiasioinnin oppaaseen, joka on suunnattu peruspankkipalveluita käyttävälle henkilöasiakkaalle.

3.1 Oppaan tarve

Nykyajan digitaalisessa ympäristössä pankkiasiointi onnistuu verkossa. Peruspankkipalvelut eli pankkitili, maksukortti ja verkkopankkitunnukset vahvalla tunnistautumisella ovat ETA-alueen vakituiselle asukkaalle kuuluva oikeus luottolaitostoimintalain (8.8.2014/610) 15 luvun 16 §:n mukaan. Nämä palvelut ovat avainasemassa arkisten toimintojen kannalta, ja etenkin ilman sähköistä vahvaa tunnistautumista on suomalaisessa yhteiskunnassa vaikea toimia. Se toimii välineenä niin laskujen maksussa verkkopankissa kuin myös henkilöllisyyden todentamisessa viranomaispalveluissa. (Signicat 28.5.2021.)

Nämä palvelut ovat henkilöasiakkaan arjen sujuvoittamiseksi tärkeät, jonka takia niihin kohdistuva väärinkäyttö ja riskit aiheuttavat suurta haittaa yksityishenkilön arkeen. Henkilöasiakas pystyy tehokkaasti ehkäisemään riskien vahingot noudattamalla hyväksymiään sopimusehtoja ja olemalla tarkkana esimerkiksi käyttäessään vieraita verkkopalveluita tai saadessaan pankin tai viranomaisen nimissä viestin. Henkilöasiakas voi palveluita käyttäessään törmätä erilaisiin huijausyrityksiin, mutta palveluiden väärinkäyttöön voidaan kannustaa esimerkiksi lähipiirissäkin, esimerkiksi lainaamalla maksukorttia toiselle henkilölle. Asiakkaan tulee tunnistaa kyseiset riskit sekä suojautua ja minimoida ne.

Tämän opinnäytetyön liitteenä olevan oppaan tarkoituksena on tutustua tiivistetysti peruspankkipalveluiden turvalliseen käyttöön sekä niihin riskeihin, joihin henkilöasiakas voi törmätä palveluita käyttäessään.

3.2 Tiedonhankinta ja aikataulu

Oppaan teoria perustuu opinnäytetyön tietoperustaan eli lukuun 2. Pankkipalveluihin liittyvää materiaalia on saatavilla paljon ja monipuolisesti. Jokaisella Suomessa toimivalla pankilla on omat verkkosivut, joista löytyy niin yleistä tietoa pankkipalveluiden käytöstä, kuin myös pankin tarjoamista palveluista. Peruspankkipalveluiden suhteen tarjottavat ominaisuudet ovat lähtökohtaisesti pankista riippumatta samat, pieniä vivahde-eroja lukuun ottamatta. Selkeimmin nämä eroavaisuudet näkyvät alaikäiselle tarjottavissa peruspankkipalveluissa. Toisaalta lähteiden samankaltaisuus luo

uskottavuutta tietoperustalle, koska ne eivät ole keskenään ristiriidassa. Pankkitoiminnasta säädetään Suomen laissa, joten osa oppaan tiedonkeruusta sisälsi lakitekstien läpikäymistä ja tiedon jalostamista helposti ymmärrettäväksi kokonaisuudeksi.

Kyberturvallisuus ja tietoturva ovat teemoina nousseet enemmän pinnalle, joka on huomattavissa esimerkiksi aiheeseen liittyvästä kampanjoinnista. Erilaiset kampanjat, kuten aikaisemmin mainitut Euroopan kyberturvallisuuskuukausi ja Suomessa eri alojen yhteiskampanja Varo, varmista ja varoita -verkkorikollisuutta ehkäisevä kampanja, tarjosivat hyvää tietoperustaa aiheesta, sillä niiden kohdeyleisönä on tavalliset kansalaiset, joille halutaan levittää tietoisuutta.

Opinnäytetyön aiheista löytyi paljon suomenkielisiä lähteitä, joita on pääosin myös hyödynnetty työssä. Englanninkielisiä lähteitä oli haastavampi löytää etenkin suoraan pankkitoimintaan liittyen, sillä suomalainen ja ylipäätänsä EU-alueen pankkitoiminta perustuu pitkälti EU-tason lainsäädäntöön, jolloin materiaalit ovat saatavilla kaikilla Euroopan unionin virallisilla kielillä. Suomessa pankkitoiminta perustuu myös kansalliseen lainsäädäntöön ja pankkien toimintaa valvoo Suomen viranomaistahot. Tästä syystä englanninkielisiä lähteitä on hyödynnetty etenkin kyberturvallisuutta ja pankkihuijauksia käsittelevissä luvuissa, koska kyseiset aiheet ovat universaaleja kaikissa maissa, joissa on vastaavan kaltaista pankkitoimintaa.

Aikataulullisesti opinnäytetyön suunnittelu alkoi elokuussa 2022 ja itse kirjoitusprosessi alkoi syyskuun aikana. Suunnitelmavaiheessa ajatuksena oli, että opasta toteutetaan samaan tahtiin kuin tietoperustaakin. Tämä kuitenkin osoittautui haasteelliseksi, sillä tietoperustassa teoriaa käsitellään eri laajuudessa kuin oppaassa. Kokonaiskuvaa tietoperustasta oli vaikea hahmottaa, ennen kuin se oli lähestulkoon valmis. Kun tietoperusta alkoi valmistumaan, oli sen ohella helppoa miettiä olennaista sisältöä opasta varten. Oppaan kokoaminen alkoi vasta lokakuussa, kun tietoperusta oli valmistunut. Taulukossa 2 on kuvattu tarkemmin opinnäytetyöprosessin aikataulu ja vaiheet.

Taulukko 2. Opinnäytetyöprosessin aikataulu ja vaiheet

Viikot	*Prosessin vaiheet*
1-2	Suunnittelu, aiheen rajaus, johdanto
3-6	Tietoperustaan perehtyminen ja kirjoittaminen
7	Oppaan kokoaminen
8-9	Oppaan tarkastelu, oman oppimisen tarkastelu

3.3 Toteutus

Opas on suunnattu henkilöasiakkaalle, jonka takia turvallista pankkiasiointia aiheena on pyritty lähestymään mahdollisimman yksinkertaisesta näkökulmasta. Oppaan on tarkoitus olla tiivis, helppolukuinen ja informatiivinen, jotta se tarjoaisi kaikille pankkipalveluita käyttäville yleiskäsityksen siitä, mitä turvallinen pankkiasiointi on ja miten siihen kohdistuvia riskejä voidaan ehkäistä. Oppaan tärkeimpiä tavoitteita on se, että se palvelee nimenomaan henkilöasiakkaan käyttötarkoitusta.

Oppaan ensimmäisellä puoliskolla käydään läpi kolme peruspankkipalveluiden tuotetta, eli pankkitili, maksukortti ja verkkopankkitunnukset, joihin sisältyy vahva tunnistautuminen. Oppaan neljänneltä sivulta löytyy kahden sivun verran vinkkejä henkilöasiakkaalle, miten hän voi käyttää näitä edellä mainittuja palveluitaan turvallisesti.

Sivut kuusi ja seitsemän oppaassa sisältävät tietoa siitä, millaisia pankkihuijaukset voivat esimerkiksi olla ja mistä pankkihuijauksen voi esimerkiksi tunnistaa. Viimeisellä sivulla on lisätietoa sekä apua huijauksen uhrille. Sivulta löytyy esimerkiksi toimintaohjeet huijauksen tapahtuessa ja yhteystiedot Rikosuhripäivystykseen avun hakemisen helpottamiseksi.

Itse opas on toteutettu Canva-nimisellä graafisen suunnittelun sivustolla. Visuaalisessa ilmeessä haettiin henkilöasiakasta kiinnostavaa, mutta myös helppolukuista ja selkeää lopputulosta.

4 Pohdinta

Tässä luvussa tarkastellaan liitteenä olevaa opasta sekä sitä, päästiinkö opinnäytetyössä asetettuihin tavoitteisiin. Lisäksi käydään läpi kehitysehdotuksia ja sitä, mitä seuraavaksi voisi opinnäytetyön pohjalta tutkia. Viimeinen alaluku keskittyy oman oppimisen tarkasteluun.

4.1 Oppaan tarkastelu

Oppaan tavoitteena oli olla selkeä ja helppolukuinen kohderyhmää ajatellen. Oppaan kohderyhmä on laaja, sillä aihe koskee kaikkia peruspankkipalveluita käyttäviä henkilöasiakkaita. Oppaan kokoamisessa kohderyhmää pyrittiin huomioimaan yksinkertaisella teorialla ja selkeillä ohjeistuksilla, jonka pohjana toimii opinnäytetyön luvun 2 tietoperusta. Alun perin tarkoituksena oli sisällyttää oppaaseen enemmän tietoperustan asioita esimerkiksi lainsäädäntöön liittyen, mutta jotta opas palvelisi tarkoituksessaan, koin parhaimpana vaihtoehtona pitää oppaan mahdollisimman tiiviinä. Näin prosessin edetessä oppaasta muovautui enemmänkin pika-opas. Kun opas on helposti saatavilla ja tarpeeksi kompakti, tarttuu asiakas siihen paljon todennäköisemmin.

Opas on tehty digitaaliseen muotoon, joten sen jakaminen onnistuisi helposti digitaalisissa kanavissa. Näitä voisivat olla esimerkiksi sosiaalinen media tai pankkien verkkosivut. Esimerkiksi oppaan sivut neljä ja viisi, jotka kertovat turvallisesta pankkiasioinnista, toimivat hyvin myös sellaisenaan, jolloin asiakkaille voisi jakaa tärkeimmät ohjeet hyvinkin kompaktisti ja helposti. Oppaasta saisi helposti tehtyä painetun version, jolloin sen voisi antaa vaikka asiakkaan matkaan, kun asiakas asioi fyysisesti pankkikonttorilla.

Yhtenä haasteena oli oppaan tuottaminen niin, että se palvelisi mahdollisimman monia. Opas itsessään on tehty suomeksi, joten olennainen kehitysehdotus olisi saada samanlainen opas myös ruotsin ja englannin kielellä. On kuitenkin huomioitavaa, että pankkipalveluita käyttävät esimerkiksi maahanmuuttajat, joilla ei välttämättä ole suomen, ruotsin tai englannin kielitaitoa. Kyseiselle asiakasryhmälle olisi tärkeää saada tietoisuutta näistä asioista, sillä heille länsimaalainen pankkitoiminta saattaa olla vierasta.

4.2 Jatkokehitysehdotukset

Tämä opinnäytetyö ja sen tuotteena syntynyt opas on suunnattu kaikille peruspankkipalveluita käyttäville henkilöasiakkaille. On kuitenkin tiedostettava se, että kaikki pankkipalveluita käyttävät eivät välttämättä käytä digipalveluita. Etenkin ikäihmisten digitaidot eivät välttämättä ole riittävät, joka aiheuttaa yhteiskunnallisella tasolla digitaalista epätasa-arvoa. Digitaalisia palveluita suunnitellessa on tärkeää huomata myös tarpeet selkokielisyydestä ja saavutettavuudesta. (Liikenne- ja

viestintävirasto 2.11.2022.) Aihe on ajankohtainen, sillä yhä useampi palvelu on siirtynyt digitaaliseen muotoon, ja olisi varmaan hyvä tutkia suomalaisten pankkien verkkopalveluiden saavutettavuutta eri käyttäjäryhmissä.

Luonnollisena jatkokehitysehdotuksena näen, että seuraavana tulisi yrityspankkipalveluiden käyttö ja niiden riskit. Myös mielenkiintoinen näkökulma on peruspankkipalveluiden ulkopuolelle jäävät tuotteet. Tässä opinnäytetyössä on sivuttu sijoitushuijauksia, sillä niiden toteutuminen usein vaatii verkkopankkitunnusten käytön, jotta tilisiirto voidaan toteuttaa. Sijoitustuotteet sekä erilaiset rahoitustuotteet ovat peruspankkipalveluita monimutkaisempia, ja niiden käyttöön kohdistuu myös erilaisia riskejä verrattuna peruspankkipalveluihin.

Kuten jo aikaisemmin on todettu, rikollisuus muuttaa aina muotoaan. Tämän takia tulevaisuuden riskienhallintaa kyberuhkilta on hyvä pohtia ja ennakoida. Jäin itse miettimään sitä, miten verkkohuijaukset muuttuvat tekniikan kehittyessä tai onko jopa realistista saada rikollisuus kytkettyä pois kokonaan verkkohuijauksiin liittyen. Toisaalta, aina kun osapuoli on ihminen, on mahdollisuus inhimilliseen virheeseen, josta rikolliset osaavat ottaa hyödyn irti.

4.3 Oman oppimisen tarkastelu

Opinnäytetyöprosessin avulla pystyin syventämään osaamistani etenkin opinnäytetyön aiheen suhteen. Lisäksi pääsin kehittämään taitojani tiedonkeruun ja prosessinhallinnan kannalta. Prosessinhallinnan näkökulmasta koen opinnäytetyönprosessin olleen onnistunut. Pysyin asettamassani aikataulussa ja opinnäytetyö valmistui ajallaan. Koen, että avain tähän onnistumiseen on ollut hyvä ennakkotietämys opinnäytetyön aiheesta, jolloin pystyin syventymään entistä enemmän esimerkiksi lainsäädäntöön ja tietosuoja-asetuksen teemoihin. Olen jo opinnäytetyöprosessin aikana huomannut, että oppimani asiat ovat päässeet käyttööni työelämässä.

Luin opinnäytetyön aiheeseen tutustuessa paljon verkkoartikkeleita, joiden alla oli kommentointimahdollisuus. Monissa tilanteissa kommentoija kuvasi tilannetta lähipiiristä, jossa esimerkiksi läheinen on antanut huijaussivustolle pankkitunnuksensa, huijari on pystynyt tunnuksilla ottamaan käyttöön kyseisen pankin puhelinsovelluksen ja sitä kautta suorittamaan maksuja uhrin huomaamatta. Kommenteissa ihmetellään pankin vastuuta tai enemmänkin sitä, miten sellaista ei tunnu olevan, koska pankki vierittää vastuun asiakkaan harteille huolimattomuuden takia eikä korvauksia tilanteesta ole saatavilla. On ymmärrettävää, että kyseinen tilanne herättää keskustelua, sillä tapahtumien vaikutukset uhriin sekä hänen taloudelliseen tilanteeseensa ja henkiseen hyvinvointiinsa saattavat olla suuret. Tilanteita on vaikea lähteä kommentoimaan ulkopuolisena tietämättä tarkkaa tapahtumankulkua, mutta kommenttien kaltaiset kuvaukset ovat tärkeitä motiiveja tämän opinnäytetyön syntymiselle.

Tutustuin aihetta tutkiessani esimerkiksi FINE Vakuutus- ja rahoitusneuvonnan ratkaisusuosituksiin, jotka löytyvät heidän verkkosivuiltaan vapaasti luettavissa. FINE on antanut 31.8.2022 päätöksen asianumerolla FINE-046898 yllä olevan kommentin kaltaisesta tilanteesta. Ratkaisu oli Pankkilautakunnan yksimielisesti laatima, ja tarkka päätöksentekoprosessi auttoi ymmärtämään hyvin pankkihuijauksien yleistä tapahtumankulkua sekä miten pankkitoimintaa säätelevää lainsäädäntöä hyödynnetään esimerkiksi pankkihuijauksia tutkiessa.

Opinnäytetyön aiheen valitseminen oli helppoa, sillä aihe oli itselleni mielenkiintoinen, ja valitettavasti yhteiskunnallisesti ajankohtainen. Nyt opinnäytetyön valmistumisen myötä koen, että haluan oppia pankkimaailmasta vain entistä enemmän ja olla tulevaisuudessa luomassa niitä ratkaisuja, jotka takaavat pankkipalveluiden turvallisen käytön. Toivon kovasti, että opinnäytetyöni ansiosta voin osaltani pelastaa ainakin yhden asiakkaan pankkihuijaukselta.

Lähteet

Albrecht, M. 2017. Verkkorikollisuus. Rikosuhripäivystys. Luettavissa: https://www.riku.fi/content/uploads/su_file/1883__RIKU_2_2017.pdf. Luettu: 11.9.2022.

Alhonsuo, S., Nisén, A., Nousiainen, S., Pelikka, T. & Sundberg, S. 2012. Finanssitoiminnan käsikirja. Finva. Jyväskylä.

Bloomenthal, A. 30.9.2022. What is a pyramid scheme. Investopedia. Luettavissa: https://www.investopedia.com/insights/what-is-a-pyramid-scheme/. Luettu: 22.10.2022.

Danske Bank s.a. Pankkipalvelut lapselle. Luettavissa: https://danskebank.fi/sinulle/asiakaspalvelu/lapsen-pankkiasiointi#accordion-0-item-3. Luettu: 4.10.2022.

Digi- ja väestötietovirasto 2022. Varo, varmista ja varoita: Suomalaisilta viety tänä vuonna jo kymmeniä miljoonia nettihuijauksilla. Näin suojaudut. Luettavissa: https://dvv.fi/-/varo-varmista-ja-varoita-suomalaisilta-viety-tana-vuonna-jo-kymmenia-miljoonia-nettihuijauksilla-nain-suojaudut. Luettu: 1.10.2022.

Erkkilä, J. 5.12.2019. Pankit ja poliisi jahtaavat rahamuuleja. Luettavissa: https://www.salkunrakentaja.fi/2019/12/pankit-rahamuuli/. Luettu: 2.10.2022.

Euroopan Komissio. Milloin voin käyttää oikeuttani henkilötietojeni käsittelyn rajoittamiseen? Luettavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_fi. Luettu: 26.9.2022.

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EU) 2016/679. Annettu 27.4.2016.

Euroopan parlamentin ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (EU) 2014/910. Annettu 23.7.2014.

F-Secure 18.6.2022. Puhelinhuijaukset ja miten toimia, jos uskot joutuneesi huijauksen kohteeksi. Luettavissa: https://community.f-secure.com/common-home-fi/kb/articles/6350-puhelinhuijaukset-ja-miten-toimia-jos-uskot-joutuneesi-huijauksen-kohteeksi. Luettu: 2.10.2022.

Federal Trade Commission 2022. How to recognize and avoid phishing scams. Luettavissa: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams. Luettu: 2.10.2022.

Finanssiala ry 2021. Pankkisalaisuusohje 2021. Luettavissa: https://www.finanssiala.fi/wp-content/uploads/2021/03/FA_Pankkisalaisuusohjeet_2021_lopullinen.pdf. Luettu: 4.10.2022.

Finanssiala ry 2022. Pankkien tietoon tulleet huijaukset. Luettavissa: https://www.finanssiala.fi/wp-content/uploads/2022/09/fa_huijaukset_pankit_01_06_2022.png. Luettu: 16.10.2022.

Finanssivalvonta 2022. Tietoa Finanssivalvonnasta: Luettavissa: https://www.finanssivalvonta.fi/finanssivalvonta/. Luettu: 11.09.2022.

Finanssivalvonta 5.9.2018. Peruspankkipalvelut. Luettavissa: https://www.finanssivalvonta.fi/kuluttajansuoja/pankkipalvelut/peruspankkipalvelut/. Luettu: 11.9.2022.

FINE Vakuutus- ja rahoitusneuvonta s.a. Säästä ja sijoita viisaasti – Eväitä sijoittamiseen tutustuvalle. Luettavissa: https://www.fine.fi/oppaat/julkaisu/saasta-ja-sijoita-viisaasti-evaita-sijoittamiseen-tutustuvalle. Luettu: 22.10.2022.

Henkilötietolaki 22.4.1999/523.

Huoltovarmuuskeskus 2020. Kyberturvallisuuden tila eri toimialoilla – Kartoituksen keskeiset havainnot. Huoltovarmuusorganisaation Digipooli. Helsinki. Luettavissa: https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf. Luettu: 16.10.2022.

Kyberturvallisuuskeskus 20.10.2022. Euroopan kyberturvallisuuskuukausi. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month. Luettu: 22.10.2022.

Kyberturvallisuuskeskus 11.3.2022. Sähköinen tunnistaminen. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen. Luettu: 26.9.2022.

Laakso, M. Mikä on toimitusjohtajahuijaus? Luettavissa: https://tietojesiturvaksi.fi/blogi/mika-on-toimitusjohtajahuijaus. Luettu: 30.10.2022.

Laki Finanssivalvonnasta 19.12.2008/878.

Laki luottolaitostoiminnasta 8.8.2014/610.

Liikenne- ja viestintävirasto Traficom 2.11.2022. Enemmistö kuluttajista hallitsee arjen digipalveluiden käytön. Luettavissa: https://www.traficom.fi/fi/ajankohtaista/enemmisto-kuluttajista-hallitsee-arjen-digipalveluiden-kayton. Luettu: 2.11.2022.

Manninen, L. 21.9.2022. Takkaushuijaus on roistolle tuottoisa petos – Näin kalliiksi ne käyvät suomalaisille. Talouselämä. Luettavissa: https://www.talouselama.fi/uutiset/rakkaushuijaus-on-roistolle-tuottoisa-petos-nain-kalliiksi-ne-kayvat-suomalaisille/87a38eac-9d7d-4765-a000-2d9bd5785598. Luettu: 2.10.2022.

Nordea 2022. Erilaisia huijausmuotoja. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/tuki/erilaisia-huijausmuotoja.html#tab=Sahkoposti--ja-tekstiviestihuijaus. Luettu: 11.9.2022.

Nordea s.a.a. Rinnakkaiskortit. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/rinnakkaiskortit.html. Luettu: 26.9.2022.

Nordea s.a.b. Pankkitunnukset. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/palvelumme/verkko-mobiilipalvelut/pankkitunnukset.html. Luettu: 26.9.2022.

OP s.a.a. Lähimaksaminen on nopeaa ja turvallista. Luettavissa: https://www.op.fi/henkiloasiakkaat/paivittaiset/maksaminen/lahimaksaminen-nopeaa-ja-turvallista. Luettu: 20.9.2022.

OP s.a.b. Mobiilimaksaminen. Luettavissa: https://www.op.fi/mobiilimaksaminen. Luettu: 20.9.2022.

OP s.a.c. Turvallista maksamista kortilla. Luettavissa: https://www.op.fi/turvallinen-asiointi/turvallista-maksamista-kassalla-ja-verkossa. Luettu: 26.9.2022.

OP s.a.d. Miten lapsi tai nuori saa OP:n tunnukset. Luettavissa: https://www.op.fi/henkiloasiakkaat/digitaaliset-palvelut/alaikaisen-mobiili. Luettu: 26.9.2022.

Palmgren, J. 9.9.2020. Korona lisäsi sähköisten pankkipalveluiden käyttöä jopa kymmenillä prosenteilla. Finanssi-ala. Luettavissa: https://www.finanssiala.fi/uutiset/korona-aika-lisasi-sahkoisten-pankkipalvelujen-kayttoa-jopa-kymmenilla-prosenteilla/. Luettu: 2.10.2022.

Pohjola, M. 2019. Taloustieteen oppikirja. SanomaPro. Helsinki.

Poliisi 2022. Poliisi varoittaa huijausyrityksistä pankin nimissä. Luettavissa: https://poliisi.fi/-/poliisi-varoittaa-huijausyrityksista-pankin-nimissa. Luettu: 1.10.2022.

Poliisi s.a. Todistus ensitunnistuksesta. Luettavissa: https://poliisi.fi/todistus-ensitunnistuksesta. Luettu: 26.9.2022.

Pulkkinen, V. 2019. Miten pankit toimivat, rautalangasta vääntäen. Luettavissa: https://www.inderes.fi/fi/miten-pankit-toimivat-rautalangasta-vaantaen. Luettu: 26.9.2022.

Rahoitusvakausvirasto. Talletussuoja Suomessa. Luettavissa: https://rvv.fi/talletussuoja. Luettu: 26.9.2022.

Rikoslaki 19.12.1889/39.

Rikosuhripäivystys s.a.a. Nettihuijaus voi tapahtua kenelle tahansa. Luettavissa: https://www.riku.fi/erilaisia-rikoksia/nettihuijaus/. Luettu: 2.10.2022.

Rikosuhripäivystys s.a.b. Kyberrikollisuudella on monta eri muotoa. Luettavissa: https://www.riku.fi/erilaisia-rikoksia/nettihuijaus/kyberrikollisuus/. Luettu: 2.10.2022.

Signicat 28.5.2021. Vahva sähköinen tunnistaminen ja tunnistautuminen. Signicatin blogi. Luettavissa: https://www.signicat.com/fi/blogi/vahva-s%C3%A4hk%C3%B6inen-tunnistaminen-ja-tunnistautuminen. Luettu: 26.9.2022.

S-Pankki 2018. Oma pankkikortti lapselle. Luettavissa: https://www.s-pankki.fi/fi/artikkelit/oma-pankkikortti-lapselle/. Luettu: 26.9.2022.

S-Pankki s.a. Turvallinen pankkiasiointi. Luettavissa: https://www.s-pankki.fi/fi/arjen-raha-asiat/turvallinen-pankkiasiointi. Luettu: 2.11.2022.

Suomen Pankki 2022. Kotitalouksien talletuskannan kasvuvauhti hidastunut. Luettavissa: https://www.suomenpankki.fi/fi/Tilastot/saastaminen-ja-sijoittaminen/tiedotehistoria/2022/kotitalouksien-talletuskannan-kasvuvauhti-hidastunut/. Luettu: 2.10.2022.

Tietosuoja 2022. Usein kysyttyä pankkitoiminnasta. Luettavissa: https://tietosuoja.fi/usein-kysyttya-pankkitoiminta. Luettu: 20.9.2022.

Van der Kleut, J. 2022. Vishing. Nortonin blogi. Luettavissa: https://us.norton.com/blog/online-scams/vishing. Luettu: 2.10.2022.

Verohallinto 2022. Verohallinnon nimissä liikkuu edelleen huijaustekstiviestejä. Luettavissa: https://www.vero.fi/tietoa-verohallinnosta/uutishuone/lehdist%C3%B6tiedotteet/2022/verohallinnon-nimiss%C3%A4-liikkuu-edelleen-huijaustekstiviestej%C3%A4---tuhoa-viesti-ilmoita-oma-tilinumero-omaverossa/. Luettu: 1.10.2022.

Välimäki, M. 10.3.2022. Mikä ikäisenä saa omat verkkopankkitunnukset, tilin, ja pankkikortin? OP Media. Luettavissa: https://www.op-media.fi/omat-rahat/lasten-ja-nuorten-pankkiasiointi-eri-ikaisena/. Luettu: 4.10.2022.

Woodard, S. 31.5.2022. What Is a Deposit Interest Rate? Luettavissa: https://www.thebalance-money.com/what-is-a-deposit-interest-rate-5213644. Luettu: 1.10.2022.

Yli-Huttula, T. 16.9.2022. Suomalaisten pankkien tietoturva on kansainvälisesti korkeatasoista. Luettavissa: https://www.finanssiala.fi/kolumni/suomalaisten-pankkien-tietoturva-on-kansainvalisesti-korkeatasoista/. Luettu: 22.10.2022.

Liitteet

Liite 1. Turvallinen pankkiasiointi ja pankkihuijaukset -opas

Turvallinen pankkiasiointi ja pankkihuijaukset

Henkilöasiakkaan opas tunnistamaan ja välttämään pankkipalveluiden käytön riskit

Ines Haapalainen, 2022

Tämä opas on tiivis tietopaketti pankin henkilöasiakkaille peruspankkipalveluista ja niiden turvallisesta käytöstä. Tässä oppaassa tutustutaan lisäksi yleisimpiin pankkihuijauksiin ja siihen, miten toimia, jos joutuu huijauksen uhriksi.

Sisällys

Peruspankkipalvelut

Pankkitili

Pankkitilejä on erilaisia, kuten käyttötili ja säästötili. Tilillä pystyy säilyttämään rahaa. Tilille voi lisätä rahaa käteistalletuksilla ja tilisiirroilla. Rahaa voi käyttää tekemällä käteisnostoja tai yhdistämällä tiliin maksukortin ja verkkopankkitunnukset, joilla pystyy käyttämään tilillä olevia varoja.

Debit-maksukortti

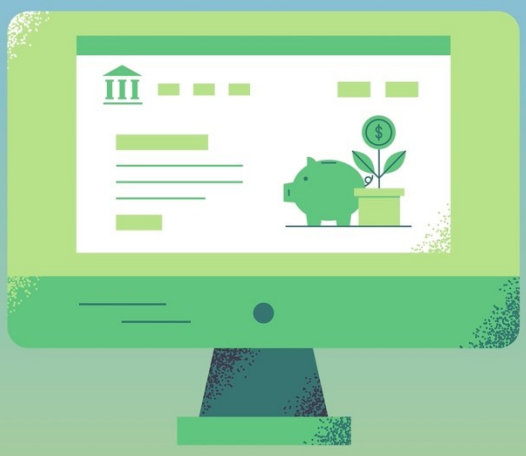
Debit-maksukortilla voi maksaa tilillä olevista varoista. Maksuja voi tehdä fyysisesti vaikka kaupan kassalla tai verkossa kortin numerolla, voimassaolopäivällä sekä kortin takana olevalla CVV-luvulla.

Maksukortissa on yleensä lähimaksu, eli kortilla voi maksaa sirun NFC-tekniikkaa hyödyntäen alle 50 euron ostoksia ilman PIN-koodia. Yli 50 euron ostokset tulee maksaa käyttäen kortin PIN-koodia.

Verkkopankkitunnukset

Verkkopankkitunnukset ovat väline pankkipalveluiden hoitamiseen verkossa. Verkkopankkitunnukset koostuvat yleensä käyttäjätunnuksesta, salasanasta ja kolmannesta varmistustavasta, kuten tunnuslukutaulukosta tai erillisestä tunnistusaplikaatiosta.

Verkkopankkitunnuksiin sisältyy vahva tunnistautuminen, jolla voi todistaa henkilöllisyyden verkkopalveluissa.



Näin hoidat pankkiasiat turvallisesti

Kortti ja pankkitunnukset ovat aina henkilökohtaiset, älä koskaan luovuta niitä muiden käyttöön!

Suosi lähimaksua ja mobiilimaksua.

Peitä kädellä maksupääte, kun näppäilet kortin tunnuslukua.

Älä kirjoita kortin tunnuslukua ylös.

Pidä kortissa sellaiset turvarajat, jotka sopivat sinun arkikäyttöön.

Näin hoidat pankkiasiat turvallisesti

Kirjaudu verkkopankkiin vain pankin virallisten sivujen tai pankin oman mobiilisovelluksen kautta.

Suosi biometrisiä tunnisteita, kuten sormenjäljen lukijaa ja kasvojen tunnistusta.

Säilytä pankkitunnukset turvallisessa paikassa, muiden katseilta piilossa.

Jos korttisi tai pankkitunnukset joutuvat toisen henkilön käsiin, ota välittömästi yhteyttä pankkisi sulkupalveluun.

Tunnista huijaus!

Huijaus voi olla...

- tekstiviesti tai soitto
- sähköpostiviesti
- yksityisviesti sosiaalisessa mediassa
- linkki

Huijari voi esittää olevansa...

- pankin työntekijä
- viranomainen, kuten poliisi
- rahan tarpeessa oleva, ennestään tuntematon henkilö
- julkisuuden henkilö,

...jolloin huijari voi pyytää kortin tai pankkitunnusten tietoja tai tekemään tilisiirron vieraalle tilille.

Tunnista huijaus!

Huijauksessa tyypillistä on...

- kirjoitusvirheet, huono suomen kielen taito tai vieraskielinen viesti suomalaiselta lähettäjältä
- kiireen tai hädän tunteen luominen
- viesteissä tuntematon lähettäjä tai kyseenalainen lähetysosoite, soitoissa tuntematon numero, jota ei löydy palvelun omilta sivuilta, oudon näköinen linkki
- sijoitushuijauksessa painostaminen nopeaan sijoituspäätökseen, ainutlaatuisen ja henkilökohtaisen edun tarjoaminen, isojen voittojen lupaaminen tai vieras palveluntarjoaja

Jos joudut huijauksen uhriksi

- Ilmoita välittömästi pankkiisi kortin tai pankkitunnusten ollessa toisen henkilön käytössä, jossa palvelut suljetaan
- Tee rikosilmoitus verkossa tai poliisiasemalla
- Kysy pankiltasi lisätietoja ja ohjeita korttireklamaation täyttämiseen

Jos pankki tai viranomainen ottaa sinuun yhteyttä ja epäilet yhteydenoton oikeellisuutta, voit olla itse yhteydessä kyseiseen tahoon. Varmista aina yhteystiedot tahon omilta virallisilta verkkosivuilta.

Lisätietoa ja apua huijauksen uhreille

Tutustu myös

Poliisin verkkosivut

Lisää ohjeita huijauksen uhrille sekä rikosilmoituksen täyttäminen

poliisi.fi/petosrikokset

Rikosuhripäivystys RIKU

Rikosuhripäivystys puhelimessa ja chatissa

riku.fi/erilaisia-rikoksia/nettihuijaus

Kuluttajaliitto

Kuluttajaliiton jäsenille lakineuvontaa digihuijauksen tapahtuessa

kuluttajaliitto.fi/neuvonta