Pankkiasiakkaisiin kohdistuvat huijaukset nyt ja tulevaisuudessa

Kiia Kairasalo

Haaga-Helia ammattikorkeakoulu
Liiketalouden koulutusohjelma
Amk-opinnäytetyö
2023

Tiivistelmä

Tekijä(t)
Kiia Kairasalo

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Pankkiasiakkaisiin kohdistuvat huijaukset nyt ja tulevaisuudessa

Sivu- ja liitesivumäärä
32+1

Tässä opinnäytetyössä tutkitaan pankkien nimissä tehtyjä huijauksia. Aihe on valitettavan ajankohtainen, sillä huijaukset ja niihin menetettyjen varojen määrät ovat kasvaneet vuodesta toiseen. Opinnäytetyön tavoitteena on selvittää, millaisia huijauksia pankkiasiakkaiden kohdistuu tällä hetkellä, miltä huijaukset tulevat näyttämään tulevaisuudessa ja kuinka niitä voidaan ennaltaehkäistä. Tutkimus on rajattu koskemaan pankkiasiakkaiden peruspalveluihin kohdistuvia huijauksia ja tulevaisuuden käsite on rajattu viiteen vuoteen.

Teoriaosuudessa on käsitelty pankkiasiakkaiden peruspalvelut, eli lyhyesti tilit, kortit, maksaminen sekä verkkopankkitunnukset. Myös opinnäytetyön rajauksen puitteissa olevat eri huijausmuodot, eli tekstiviesti- ja sähköpostihuijaukset, tietojenkalastelusivut sekä huijauspuhelut. Lisäksi katsaus lainsäädäntöön ja FINEn ratkaisuihin pankin ja asiakkaan välisistä kiistatilanteista.

Tutkimus on toteutettu kvalitatiivisella tutkimusotteella. Menetelmänä on käytetty ennakointia, joka on yksi tulevaisuudentutkimuksen menetelmistä. Ennakoinnissa on käytetty apuna etenkin asiantuntijahaastatteluita. Valitut asiantuntijat ovat työnsä takia tekemisissä huijauksien sekä huijausten uhrien kanssa päivittäin. Haastattelun avulla saatuja tuloksia on täydennetty kirjallisuudella ja verkkolähteillä.

Tutkimuksessa selvisi, että pankkiasiakkaisiin kohdistuu tietojenkalastelua eritoten tekstiviesti- ja verkkosivuhuijausten muodossa. Myös turvatilihuijaukset nousivat tämän hetken trendiksi. Uskotaan, että tulevaisuudessa huijausten teemat pysyvät nykyisen kaltaisina, mutta teknologian kehityksen myötä tulemme näkemään teknologisesti kehittyneempiä sekä yksilöidympiä huijauksia. Myös nykyiset ennaltaehkäisykeinot tulevat korostumaan tulevaisuudessa. Etenkin asiakkaiden tietoisuuden lisääminen ja teknologian hyödyntäminen huijausten ennaltaehkäisy koettiin tärkeäksi.

Asiasanat
Kyberrikollisuus, huijaus, pankki, pankkipalvelut, tietojenkalastelu

Sisällys

1 Johdanto

Lähes jokainen meistä on nykyään vähintään yhden pankin asiakas. Pankki on usein mukana elämässämme ensimmäisistä vuosista aina viimeisiin päiviimme asti. Digitalisaation myötä pankkiasiointi on siirtynyt yhä enemmän verkkoon ja omien pankkiasioiden hoitaminen on jatkuvasti helpompaa kotoa käsin. Kirjailija Brett Kingin (2019, 13) sanoin ’’Banking is no longer somewhere you go, but something you do.’’

Digitalisaatio on tuonut mukanaan monia mahdollisuuksia mutta uhkiakin. Yksi näistä uhkista on jatkuvasti yleistyvät huijaukset. Huijauksissa hyödynnetään usein teknologiaa, kuten sähköpostia, tekstiviestejä ja verkkosivuja. Huijausten laatu on teknologian kehityksen myötä vain parantunut ja valveutuneimmillakin ihmisillä saattaa olla haasteita erottaa huijaus oikeasta asiasta. Pankkiasiakkaisiin kohdistuvat huijaukset voivat aiheuttaa vakavia taloudellisia seurauksia ja vuosittain huijauksiin menetetyt summat ovat päätä huimaavia.

Moni ihminen kokee, etteivät huijarit ole kiinnostuneita juuri heistä tai heidän asioistaan, varoistaan tai tiedoistaan. Näin ei kuitenkaan ole. Huijarit käyvät kauppaa esimerkiksi toimiviksi varmistetuilla sähköpostiosoitteilla ja numeroilla, tavoittelevat pohjoismaissa pieniksi katsottuja summia ja pyrkivät hyötymään juuri meistä ihan tavallisista ihmisistä. Ei tarvitse siis olla miljonääri kuuluakseen huijarin kohderyhmään. Viime vuosina uutisointi huijauksista ja niiden uhreista on ollut jatkuvaa, mutta tietoisuuden leviämisestä huolimatta onnistuneet huijaukset eivät ole vähentyneet.

Tässä opinnäytetyössä tarkastellaan pankin asiakkaisiin kohdistuvia huijauksia, niiden nykytilannetta sekä tulevaisuuden näkymiä. Tutkitaan myös keinoja, joilla huijauksia ennaltaehkäistään tällä hetkellä ja kuinka niitä tullaan ehkäisemään tulevaisuudessa. Pankin asiakkaisiin kohdistuvat huijaukset ovat vakava ja jatkuvasti kehittyvä haaste, joka vaatii laajaa ymmärrystä ja toimenpiteitä niiden torjumiseksi.

1.1 Opinnäytetyön tavoitteet

Opinnäytetyön tavoitteena on luoda kattava katsaus siihen, millaisia pankin nimissä tehtyjä huijauksia kohtaamme ja tulemme kohtaamaan tulevaisuudessa. Opinnäytetyön tekijä työskentelee pankin asiakaspalvelussa toimihenkilönä ja kohtaa huijauksen uhreja lähes päivittäin. Usein huijausten seuraukset eivät ole vain taloudellisia, vaan ne aiheuttavat myös henkistä tuskaa ja kärsimystä uhreille.

Pankin vastuulla on tehdä pankkiasiointi mahdollisimman turvalliseksi omalta osaltaan, mutta meidän kaikkien täytyy pitää asiasta huolta myös omalta osaltamme. Useasti heikoin lenkki

pankkiturvallisuuden osalta on ihminen. Kone tunnistaa huijauksia ja lyö kortteja ja verkkopalvelutunnuksia automaattisesti lukkoon havaitessaan epätavallista toimintaa. Ihminen ei kuitenkaan toimi näin.

Opinnäytetyö voi olla hyvä katsaus siihen, miten meidän kaikkien tietoja havitellaan huijarien toimesta hyväksi, miten huijarit pyrkivät hyötymään meistä ja kaiken kaikkiaan herätys siihen, kuinka yleisiä huijaukset ovat. Meistä jokainen törmää jonkinlaisiin huijauksiin, joten on hyvä oppia ainakin jollain tasolla ymmärtämään ja tunnistamaan niitä.

Tutkimuksen kohteena on pankkiasiakkaisiin kohdistuvat huijaukset. Pääongelma on muotoiltu seuraavasti:

1. Miten pankkiasiakkaisiin kohdistuvia huijauksia voidaan ennaltaehkäistä nyt ja tulevaisuudessa?

Pääongelman tueksi asetetaan kolme alaongelmaa:

1. Millaisia pankin nimissä tehtyjä huijauksia pankkiasiakkaisiin kohdistuu tällä hetkellä?
2. Miltä huijaukset tulevat näyttämään tulevaisuudessa?
3. Kuinka huijauksia voidaan ennaltaehkäistä?

Taulukko 1 Peittomatriisi

Opinnäytetyön alaongelmat	Teoreettinen viitekehys	Haastattelujen kysymykset	Tulokset
Millaisia huijauksia pankkiasiakkaisiin kohdistuu?	2, 2.2, 2.2.1, 2.2.2, 2.2.3,	1, 2, 3,4	3.2, 3.3
Miltä huijaukset tulevat näyttämään tulevaisuudessa?	2.2.	5	3.4
Kuinka huijauksia voidaan ennaltaehkäistä?	3.5, 3.5.1, 3.5.2	6, 7, 8, 9	3.5, 3.5.1, 3.5.2, 3.6

1.2 Aiheen rajaus

Opinnäytetyössä keskitytään pankkien nimissä tehtyihin huijauksiin ja niiden ennaltaehkäisyyn. Kansainvälinen kyberrikollisuus ja pankkien nimissä tehdyt huijaukset ovat valtavan laaja ja maailmanlaajuinen ongelma, mutta keskitytään oleellisuuden takia suomalaisiin pankkeihin sekä henkilöasiakkaisiin. Poissuljetaan yritysasiakkaat ja yrityksiin kohdistuvat huijaukset. Erilaisia yksityishenkilöihin kohdistuvia huijauksia on todella paljon, joten aihe on rajattu käsittelemään pankin nimissä tehtyjä huijauksia, jotka kohdistuvat henkilöasiakkaiden peruspalveluihin, eli tileihin, kortteihin ja maksamiseen sekä vahvaan tunnistautumiseen. Mukaan luetaan kuitenkin luottokortit, sillä ne ovat usein huijausten kohteena. Aiheen rajaamiseksi jätetään siis esimerkiksi sijoitushuijaukset, toimitusjohtajahuijaukset, kiristyshuijaukset ja romanssihuijaukset käsittelemättä.

Aikajana ’’nyt ja tulevaisuudessa’’ on laaja, joten rajataan tulevaisuutta noin 5 vuotta eteenpäin, tarkennettuna vuosiin 2024–2028. Nopealla teknologian kehityksellä on vahva yhteys huijauksiin ja huijausmenetelmiin, joten on mahdotonta arvioida niiden tulevaisuutta esimerkiksi 50 vuoden päähän.

Aihe käsittelee tiettyjä pankkisalaisuuden alle lukeutuvia aiheita, joten tarkkoja kuvauksia esimerkiksi uhreista tai tietyistä ennaltaehkäisymenetelmistä ei voida antaa, vaan aiheet on kuvattu yleisellä tasolla. Opinnäytetyössä ei myöskään keskitytä yksittäisiin huijauksiin tai niiden uhreihin, eikä tutkimuksessa käytetä materiaaleja tai kuvauksia, joista tapauksen tai yksityishenkilön voi tunnistaa.

1.3 Keskeisiä käsitteitä

Kyberrikollisuus on tietoverkkojen, kuten ohjelmistojen avulla tehtyjä rikoksia. Kaikki verkossa tai verkkoa apuna käyttäen tehdyt rikokset katsotaan kyberrikollisuudeksi. (Poliisi s.a.)

Peruspankkipalvelut ovat pankin lain velvoittamana asiakkailleen tarjoamat tili, kortti sekä verkkopalvelutunnukset. (Finanssivalvonta 2018.)

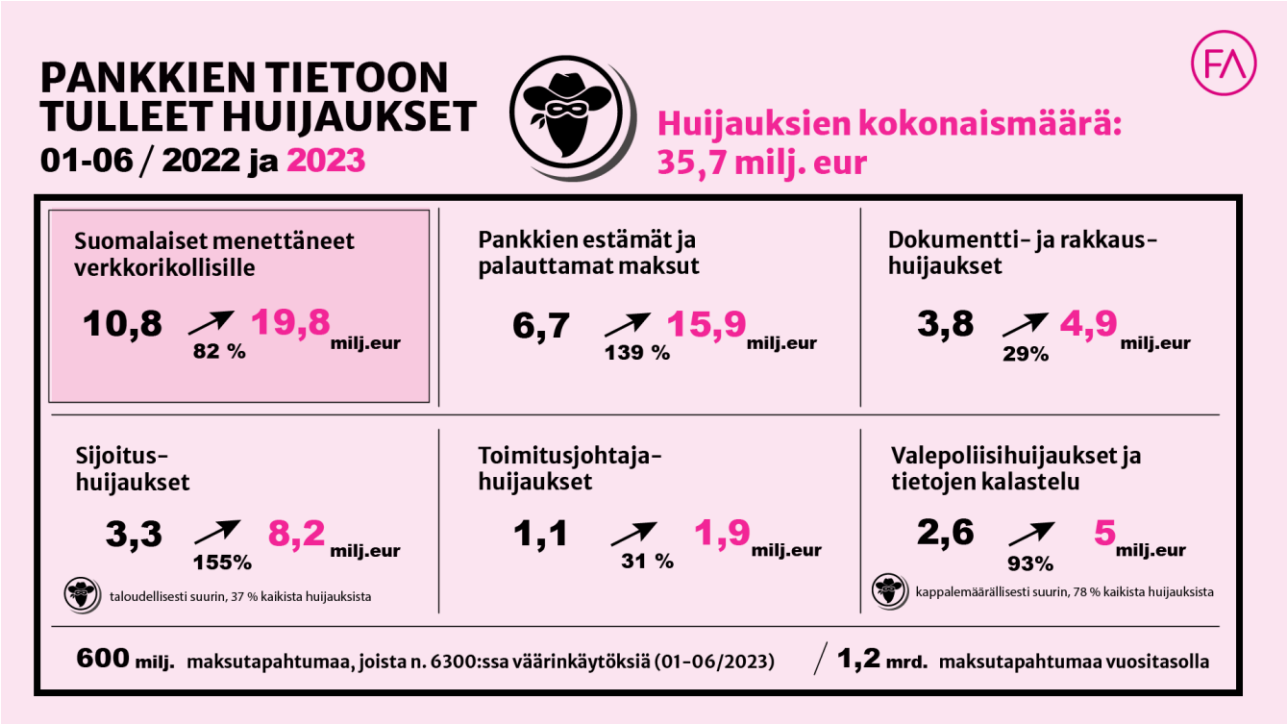
Sanalla **phishing** tarkoitetaan tietojenkalastelua. Tietojenkalastelulla pyritään esiintymään esimerkiksi viranomaisena ja saada uhri luovuttamaan esimerkiksi verkkopalvelutunnukset huijarin käsiin. (Steinberg 2022, luku 2.)

Smshing on tekstiviestitse tehtävää tietojenkalastelua. (Steinberg 2022, luku 2.)

2 Peruspankkipalvelut ja niihin kohdistuvat huijaukset

Jokaisella pankin asiakkaalla on riski joutua huijauksen uhriksi. Uhreja löytyy jokaisesta ikäluokasta, sukupuolesta ja asemasta. (Asiantuntija 1, 2023.) Vuonna 2021 tietojenkalastelun ja huijausten rikoshyöty oli huimat 30 miljoonaa euroa. Summa on noussut 60 % vuoteen 2020 verrattuna. Pelkästään verkkopalvelutunnusten kalasteluun menetetyt varat nousivat jopa 8 miljoonaan euroon. (Kyberturvallisuuskeskus 2021.)

Finanssiala Ry on julkaissut sivuillaan pankkien tietoihin tulleista huijauksista vertailun vuoden 2022 ja 2023 välillä.



Kuva 1 Finanssialan julkaisema vertailu pankkien tietoon tulleista huijauksista 2022-2023 (Finanssiala ry 2023)

Vertailusta voidaan huomata, että suomalaisten vuonna 2023 verkkorikollisille menettäneiden rahojen määrä on kasvanut huomattavasti, jopa 82 % edelliseen vuoteen verrattuna. Finanssiala ry:n petos- ja rikostorjunnasta vastaava johtaja Niko Saxholm kertoo, että nousulle ei ole yhtä selittävää tekijää, vaan rikollisten epäillään aktivoituneen huijauskampanjoissaan. (Finanssiala ry 2023.) Luvuista voidaan myös päätellä, että huijaukset ovat yleistymään päin.

Pelkästään huijaukset eivät ole kasvussa, vaan positiivisia näkymiä asiaan luo pankkien estämien ja palauttamien maksujen määrä. Huima 139 % kasvu estetyissä ja palautetuissa maksuissa

kertoo, että huijauksien estämiseksi todellakin tehdään töitä. Ennaltaehkäisy näyttäytyy yhä tärkeämpänä osana taistelussa huijareita vastaan.

2.1 Peruspalvelut ja vahva tunnistautuminen

Ymmärtääksemme huijausten ennaltaehkäisyä, on hyvä perehtyä siihen, mitä huijarit tavoittelevat. Opinnäytetyössä keskitytään peruspalveluihin kohdistuviin huijauksiin, joten tässä kappaleessa käsitellään tarkemmin, mitä peruspalvelut tarkoittavat.

Laki luottolaitostoiminnasta (8.8.2014/610) 15 luvun 6 § velvoittaa pankkeja tarjoamaan peruspalveluita syrjimättä ETA-maissa laillisesti asuville luonnollisille henkilöille. Tällaisen lain säätäminen on ollut tarpeellista, sillä nykymaailmassa pankkipalveluitta eläminen on vaikeaa. Jokainen asiakas ei ole pankin liiketoiminnan kannalta tuottava, joten jos peruspalveluiden tarjoamista koskevaa sääntelyä ei olisi, voisi moni yksityishenkilö jäädä tahtomattaan pankkipalveluiden ulkopuolelle. (Wuolijoki 2023, 99.) Peruspankkipalveluihin kuuluvat perusmaksutili ja siihen liittyvä tilinkäyttöväline, kuten debit-kortti ja verkkopankkitunnukset, mahdollisuus nostaa käteistä rahaa, maksutapahtumien toteuttaminen sekä sähköinen tunnistusväline. (Finanssivalvonta 2018.) Tässä kappaleessa käsitellään pankkien asiakkailleen tarjoamia peruspalveluita. Mukaan on kuitenkin luettu credit-kortit sekä vahvan tunnistautumisen välineet, sillä ne ovat usein huijareiden kohteena.

2.1.1 Perusmaksutili

Lain asettamiin peruspankkipalveluihin kuuluu euromääräinen perusmaksutili, eli käyttötili. Käyttötiliä voidaan käyttää maksujen vastaanottamiseen ja lähettämiseen, käteistalletuksien tekemiseen sekä käteisen nostamiseen. (Aktia Pankki Oyj 2023.) Peruspankkipalveluihin eivät siis lukeudu esimerkiksi säästötilit, kuten ASP-tili.

Käyttötiliin voidaan yleisesti ottaen liittää yleisimmät maksamiseen liittyvät palvelut. Näitä ovat esimerkiksi verkkopankin käyttö, tilisiirrot, e-laskut ja suoraveloitukset. (Alhonsuo ym. 2012, 199.)

2.1.2 Kortit

Käyttötilin maksuvälineeksi pystytään liittämään kortti. Maksukortit ovat henkilökohtaisia tilinkäyttövälineitä, eikä niitä saa luovuttaa muiden käyttöön. (Kontkanen 2015, 217.) Kortteja löytyy erilaisia, mutta ainoa peruspalveluihin sisältyvä kortti on debit-kortti. Debit-kortti on liitetty käyttötiliin, jolloin raha lähtee suoraan tililtä maksun yhteydessä. Debit-kortilla voidaan myös nostaa rahaa automaatista, tehdä verkko-ostoksia sekä maksaa ulkomailla. (Nordea Bank Oyj 2023.)

Pankit myöntävät asiakkailleen myös luotto- eli credit-kortteja. Luottokortit eivät kuulu peruspalveluihin, mutta koska huijarit usein havittelevat pankkiasiakkaiden luottokorttitietoja, on aiheellista

sisällyttää ne opinnäytetyöhön. Pankki myöntää asiakkaalle kortin tietyllä luottorajalla, jolloin asiakas pystyy joustavasti ja tarpeidensa mukaan käyttämään korttia tuohon luottorajaan asti. Luottokortilla maksaessa itse pankkitililtä ei lähde rahaa, vaan kortin luotto on lyhennettävä pois joko kerralla tai pikkuhiljaa. (Nordea Bank Oyj 2023.) Kun luottokorttia käytetään, maksetaan kortilla olevasta luotollisesta velasta korkoa (Kontkanen 2015, 218).

Jokaisella maksukortilla on oma PIN-koodi. PIN (personal indetification number), eli henkilökohtainen tunnistuskoodi auttaa varmistumaan siitä, että kortin haltijalla on oikeus käyttää korttia. Korttisopimusta tehdessä velvoitetaan kortinhaltija käyttämään korttiaan palveluehtojen mukaisesti ja säilyttämään korttitietoja sekä PIN-koodia ehtojen mukaisesti. (Kontkanen 2015, 217.)

2.1.3 Verkkopankkitunnukset ja vahva tunnistautuminen

Peruspankkipalveluihin luetaan myös verkkopankkitunnukset. Verkkopankkitunnukset sisältävät käyttäjätunnuksen, salasanan sekä tunnistautumisvälineen. Tunnistautumisväline on käyttäjätunnuksesta ja salasanasta riippumaton ja erillinen osa kaksivaiheista tunnistautumista. Esimerkiksi pankin tunnistussovellus tai avainlukulista tekevät tunnistuksesta vahvan. (Salo 2023, 69.) Verkkopankkitunnukset ovat vahvan sähköisen tunnistamisen väline, jolla voi esimerkiksi allekirjoittaa virallisia sopimuksia ja kirjautua tunnistautumista vaativille sivustoille, kuten Vero.fi tai Omakanta. Vahvan sähköisen tunnistautumisen avulla tehdyt sopimukset, toimeksiannot, viestit sekä hakemukset ovat sitovia ja tunnistautuminen vastaa allekirjoitusta. Tämän takia verkkopankkitunnukset ovat aina henkilökohtaisia, eikä niitä saa luovuttaa kenellekään muulle. (OP Ryhmä 2023.) Finanssivalvonnan mukaan pankki voi kieltäytyä antamasta sähköisen tunnistautumisen välinettä asiakkaalle, mikäli tällä ei ole henkilötunnusta tai häntä ei löydy väestötietorekisteristä. Näissäkin tilanteissa pankki on velvoitettu tarjoamaan asiakkaalle suppeampaa verkkopalvelutunnusta, jotta tämä voi käyttää perusmaksutiliä ja siihen liittyviä palveluita. (Finanssivalvonta 2023.)

2.2 Huijaustavat

Ymmärtääksemme huijausten kehitystä ja niiden ennaltaehkäisyä, on syytä paneutua siihen, millaisia huijauksia pankin nimissä tehdään. Huijareiden käyttämät tavat ovat entistä kehittyneempiä ja kohdistettuja. Tietoa potentiaalisesta uhrista löydetään esimerkiksi sosiaalisesta mediasta tai oman työpaikan verkkosivuilta, jonka jälkeen huijaus muokataan uhrille sopivaksi. Pankin nimissä tehdyillä huijausrikoksilla on kuitenkin se, että uhri pyritään saamaan luovuttamaan pankkitunnukset ja kortti- tai henkilötietoja. (Poliisi 2023.) Tässä osiossa käydään läpi opinnäytetyön rajauksen puitteissa oleviin olennaisia huijauksia esimerkkeineen.

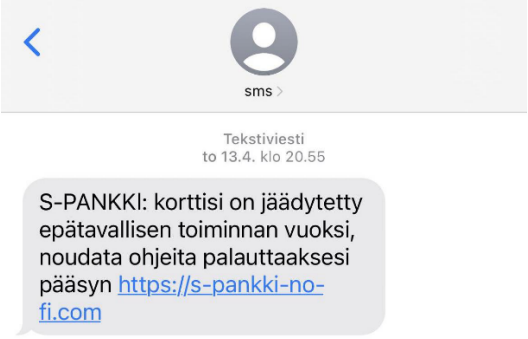
2.2.1 Tekstiviesti- ja sähköpostihuijaukset

Pankkien nimissä lähetetään jatkuvasti huijausviestejä. Usein viestit sisältävät linkkejä tai liitetiedostoja sekä kehotuksen ryhtyä toimeen esimerkiksi pankkisiirron perumiseksi, suljettujen tunnusten avaamiseksi tai henkilöllisyyden vahvistamiseksi. (Nordea Oyj 2023.) Asiantuntija B:n mukaan pankin nimissä tapahtuvista huijauksista yleisintä on viestien välityksellä tapahtuva tietojenkalastelu, eli phishing.

Tekstiviestihuijauksien, eli smshing-viestien tavoitteena on usein pankkiasiakkaiden verkkopalvelutunnukset ja pääsy asiakkaan verkkopalveluihin ja tätä kautta varoihin. Tekstiviestihuijausten kanssa täytyy olla erityisen tarkkana, sillä viestit tulevat usein samaan viestiketjuun, jossa on oikean pankin lähettämiä viestejä. Asiakkaan silmin näyttää siis siltä, että ketjun jokainen viesti on samalta lähettäjältä. Huijausviesti on yleensä lyhyt ja sillä pyritään herättämään saajan huomio ja saada tämä reagoimaan. Toivottu reaktio on yleensä viestissä tulleen linkin seuraaminen. (Salo 2023, 35.)

Kuva 2 Huijausviesti 1, tekstiviesti (OP Ryhmä 2022)

Kuvassa 2 on esimerkki Osuuspankin nimissä lähetetystä huijausviestistä. Viestissä kerrotaan, että asiakkaan maksu on kirjautunut järjestelmään. Viestistä löytyy linkki, jota kehotetaan seuraamaan, mikäli asiakas ei ole itse tehnyt maksua. Kun linkkiä seurataan, avautuu huijarin tietojen kalasteluun kehittämä verkkosivu, eli phishing-sivusto. Verkkosivulla pyydetään asiakasta syöttämään esimerkiksi verkkopalvelutunnuksensa. Kun asiakas syöttää tunnukset, saa huijari ne käsiinsä ja pyrkii näiden avulla kirjautumaan oikean pankin sivuille. Kun huijari syöttää tunnukset, lähtee uhrille tekstiviesti, jossa pyydetään avainlukulistan numeroa tai mobiilivarmennetta. Uhrin syöttäessä varmenteen pääsee huijari käsiksi uhrin verkkopankkiin. (OP Ryhmä 2023.)

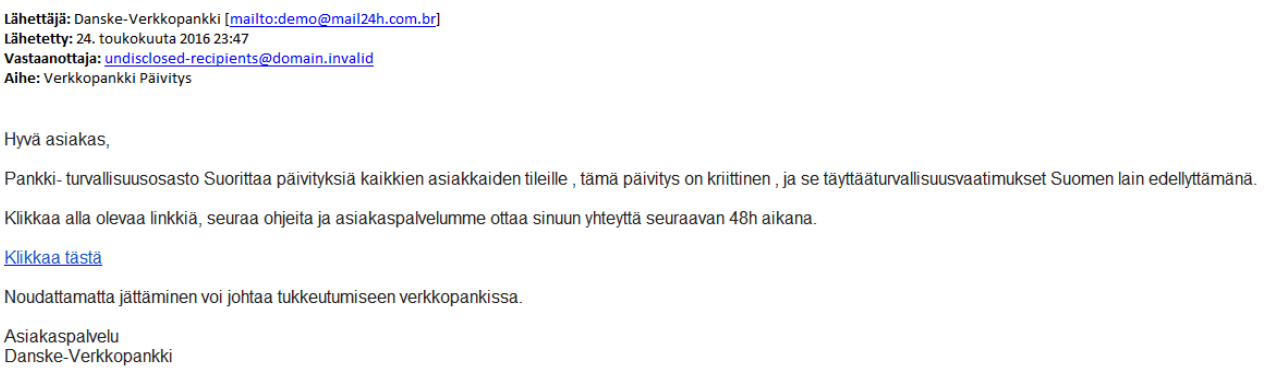


Kuva 3 Huijausviesti 2, tekstiviesti

Kuvassa 3 on S-Pankin nimissä lähetetty viesti. Viestin alkuun on kirjoitettu isoilla kirjaimilla ’’lähettäjäksi’’ pankki. Viestissä kerrotaan, että asiakkaan kortti on jäädytetty epätavallisen toiminnan vuoksi. Viestiin on liitetty linkki ja kehotus noudattaa ohjeita kortin palauttaa kortille pääsy.

Kuva 4 Huijausviesti 3, sähköposti (Alma Media Oyj 2022)

Kuvassa 4 nähdään sähköpostitse tulleen huijausviestin, joka on lähetetty Nordean nimissä. Sähköpostissa kerrotaan, että asiakkaan hyvityspyyntö on hyväksytty. Asiakasta pyydetään kuitenkin vielä klikkaamaan viestissä tullutta linkkiä vahvistaakseen hyvityksen. Aiemman tekstiviestihuijauksen tapaan linkkiä seuraamalla asiakas päätyy sivustolle, jossa pyydetään syöttämään verkkopalvelutunnukset. (Alma Media Oyj 2022.)



Lähettäjä: Danske-Verkkopankki [mailto:demo@mail24h.com.br]
Lähetetty: 24. toukokuuta 2016 23:47
Vastaanottaja: undisclosed-recipients@domain.invalid
Aihe: Verkkopankki Päivitys

Hyvä asiakas,

Pankki- turvallisuusosasto Suorittaa päivityksiä kaikkien asiakkaiden tileille , tämä päivitys on kriittinen , ja se täyttääturvallisuusvaatimukset Suomen lain edellyttämänä.

Klikkaa alla olevaa linkkiä, seuraa ohjeita ja asiakaspalvelumme ottaa sinuun yhteyttä seuraavan 48h aikana.

Klikkaa tästä

Noudattamatta jättäminen voi johtaa tukkeutumiseen verkkopankissa.

Asiakaspalvelu
Danske-Verkkopankki

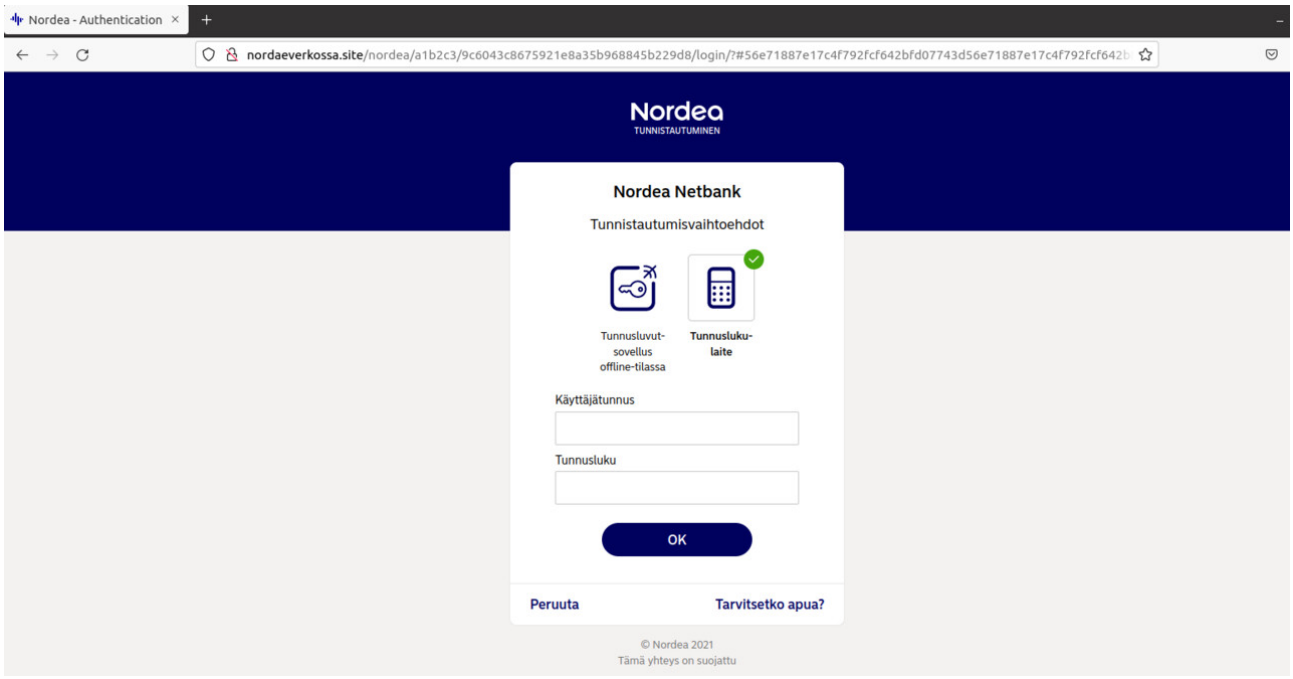
Kuva 5 Huijausviesti 4, sähköposti (Danske Bank A/S 2023)

Kuvassa 5 nähdään Danske Bankin nimissä sähköpostitse lähetetty huijausviesti. Lähettäjän nimeksi on merkitty Danske-Verkkopankki, mutta sähköpostiosoite ei ole Danske Bankin yleisesti käyttämä danskebank.fi. Huijausviestissä pyydetään asiakasta seuraamaan viestissä olevaa linkkiä ja seuraamaan ohjeita, sillä pankki suorittaa päivityksiä asiakkaidensa tileille. Ohjeiden noudattamatta jättäminen voi johtaa ongelmiin verkkopankissa. Viestin tarkoituksena on todennäköisesti kartoittaa potentiaalisia uhreja. Linkin seuraamisen jälkeen asiakkaalta kysytään todennäköisimmin verkkopalvelutunnuksia tai yhteystietoja, sillä viestissä kerrotaan asiakaspalvelun olevan vielä yhteydessä asiakkaaseen. Tulevassa puhelussa pankin virkailijana esiintyvä huijari pyytää lisää asiakkaan tietoja ja pyrkii pääsemään kiinni tämän varoihin. (Danske Bank A/S 2023.)

Tekstiviesti- ja sähköpostihuijauksissa huijari pyrkii usein luomaan kiireen tuntua lukijalle. Salon (2023, 16) mukaan yllättäen saapuvat viestit voivat herättää vastaanottajassa vahvoja tunnereaktioita: hätäännystä, ärsyyntymistä, innostusta, pelkoa – ja se on niiden tarkoituskin. Viesteillä on tarkoitus herättää paniikkia, jotta vastaanottaja saadaan toimimaan nopeasti. Epätavallinen toiminta kortilla tai järjestelmään kirjautunut maksu, jota asiakas ei itse ole tehnyt ovat omiaan herättämään huolen ja sen enempää ajattelematta klikkaamaan viestissä tullutta linkkiä.

2.2.2 Verkkosivuhuijaukset

Huijarit käyttävät toiminnassaan myös verkkosivuja. Sivulle saatetaan päätyä muun muassa tekstiviestin linkin, hakukoneen tai sosiaalisen median kautta. Usein verkkosivut ovat kopioita aidosta sivustosta, kuten pankin verkkosivusta. Huijaussivuston sisältö on usein lähes identtinen aitoon sivustoon verrattuna. Salon (2023, 101) mukaan pelkästään sivun ulkonäköön ei kannata luottaa, sillä verkkosivujen kopiointi on helppoa. Erityistä huomiota kannattaa kiinnittää sivun osoitteeseen. Usein pankeilla on yksinkertainen osoite, kuten nordea.fi, op.fi ja s-pankki.fi. Mikäli osoiterivillä lukee jotain muuta, on hälytyskellojen syytä soida.



Kuva 6 Huijaussivusto (Kyberturvallisuuskeskus 2021)

Kuvassa 6 näemme esimerkin huijaussivustosta. Tällaisen sivuston uhri voi saada esiin esimerkiksi seuraamalla viestissä tullutta linkkiä. Sivusto on hyvin samanlainen verrattaessa pankin oikeaan kirjautumissivustoon, joten eroa on vaikea huomata jollei kunnolla kiinnitä huomiota yksityiskohtiin. Yksi erottava tekijä valesivun ja oikean sivun välillä on kuitenkin verkkosivun osoite. (Kyberturvallisuuskeskus, 2021.)

2.2.3 Huijauspuhelut

Huijarit toimivat usein myös puhelimitse. Huijauspuheluita kutsutaan myös nimellä vishing, eli voice phishing. Kyberturvallisuuskeskuksen mukaan huijauspuheluita on tullut viime vuosina jopa miljoonia. Monesti huijarit soittavat ulkomailta, mutta numerot on naamioitu suomalaisiksi. (Kyberturvallisuuskeskus, 2023.) Yksi syy yleistymiseen saattaa olla se, että puhelinnumerot ovat nykyään helposti saatavissa. Ihmiset julkaisevat yhteystietojaan sosiaalisessa mediassa, puhelinnumeroja on keräilty eri verkkosivuilla vuosikymmenien ajan ja tietomurrot ovat nykypäivää. Myös teknologian avulla huijaussoittojen toteutus on helpottunut. Huijareilla on käytössään ohjelmia, jotka tekevät niin sanottuja testisoittoja koneen arpomiin numeroihin. Mikäli kone havaitsee, että numerosta joko vastataan tai esimerkiksi painetaan punaista luuria, merkataan se vahvistetuksi numeroksi. Tämä tarkoittaa sitä, että numero on toimiva ja seuraavan kerran oikea ihminen siirtyy soittamaan tällaiseen vahvistettuun numeroon. (Salo, 2023, 25–27.)

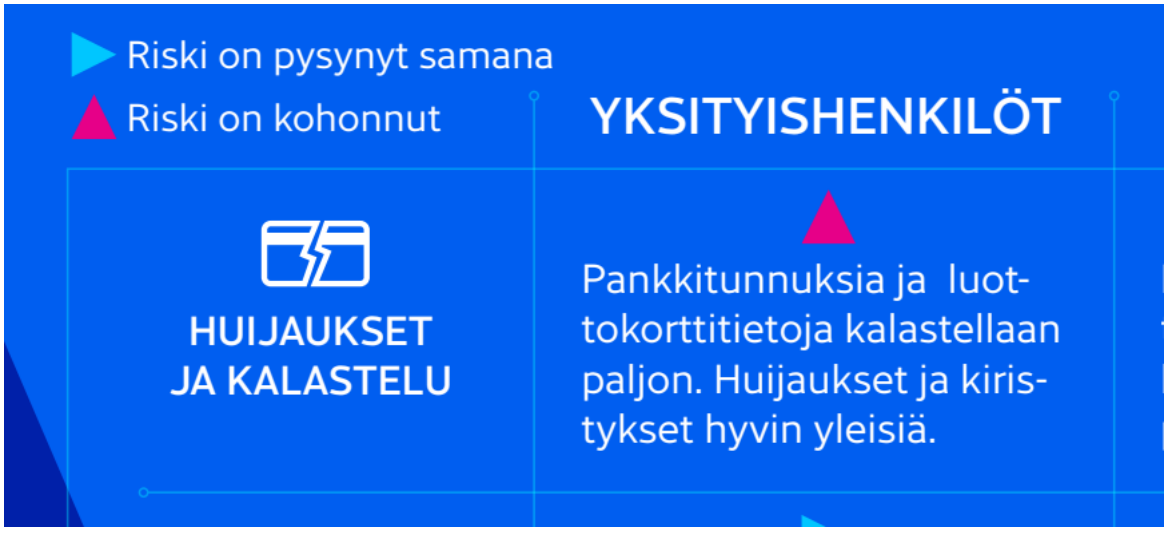
Puhelussa huijari esiintyy pankkivirkailijana ja pyrkii puhelun aikana saamaan uhrilta esimerkiksi verkkopalvelutunnukset, korttitiedot tai saada uhri tekemään tilisiirto. Eräässä tällaisessa

huijauksessa pankkivirkailijana esiintyvä huijari soittaa uhrille kertoakseen, että tämän tilin tiedot ovat vaarantuneet tai joutuneet vääriin käsiin. Puhelun aikana huijari kertoo, että tilin varat on siirrettävä ’’turvalliselle’’ tilille. Todellisuudessa rahat päätyvät huijarin omaan taskuun yleisimmin useamman tilisiirron kautta, jolloin varoja on vaikeampi jäljittää. Tällaisia huijauksia kutsutaan turvatilihuijauksiksi. (Danske Bank A/S 2023.) Huijarit käyttävät usein ns. rahamuuleja kierrättämään rahoja usean tilin kautta. Monesti muulit eivät ole edes tietoisia osallistuvansa rikokseen, vaan uskovat tekevänsä laillista työtä. Muulit on saatettu palkata ’’työsuhteeseen’’, jonka toimenkuvana on rahojen vastaanotto ja siirto jälleen seuraavalle tilille. (Asiantuntija A, 2023.)

Pankin nimissä tehtyjen huijauspuheluiden uskottavuutta lisää usein myös se, että ne ovat suomalaisten huijarien tekemiä. Enemmän epäilyjä todennäköisesti herättää se, jos englantia puhuva huijari esiintyisi suomalaisena pankkivirkailijana.

2.3 Huijausten kehitys

Opinnäytetyössä keskitytään vahvasti huijausten tulevaisuuteen, mutta miltä näyttää, jos katsomme viisi vuotta taaksepäin? Kyberturvallisuuskeskuksen vuosittain julkaisemassa Tietoturvan vuosi 2018-katsauksessa kerrotaan huijareiden siirtyneen käyttämään tekstiviestejä. Myös tietojenkalastelu on ollut vahvana ilmiönä jo kyseisenä vuonna.



Kuva 7 Kyberturvallisuuskeskus, Tietoturvan vuosi 2018

Kuvassa 7 näemme osana Tietoturvan vuosiraporttia julkaistun taulukon kohdan yksityishenkilöihin kohdistuvat huijaukset ja kalastelu. Jo vuonna 2018 pankkitunnusten ja luottokorttien tietojen kalastelu on ollut vallitsevana trendinä ja aihe on nähty kohonneena riskinä. Vuodesta 2018 eteenpäin jokaisessa raportissa on ollut mainintoja pankkien nimissä tehdyistä huijauksista tekstiviestien, sähköpostien sekä puheluiden muodossa. Katsoessa viisi vuotta taaksepäin, voidaan

huomata, että teemat ovat olleet samoja, mutta huijaukset ovat kehittyneet teknologisesti paremmiksi ja yksilöidyimmiksi. Jos peilataan historiaa tulevaisuuteen, voidaan päätellä, että samat teemat tulevat edelleenkin säilymään, mutta teknologian kehityksen seurauksena niiden laatu paranee.

2.4 Lainsäädäntö ja sen haasteet

Huijausten jatkuvan kehityksen ja uusien huijausmuotojen myötä lainsäädännöllä on haasteita pysyä perässä. Suomen laissa ei ole eriteltynä verkkorikollisuutta tai verkkohuijauksia, mutta jos verkkohuijauksen katsotaan olevan saman tyyppinen kuin perinteisen rikoksen, on käytetty perinteisen rikoksen säännöksiä. (Peltomäki & Norppa 2015, 73.) Esimerkiksi Rikoslain 19.12.1889/39 36 luvun 1 § määritellään petos seuraavasti;

> ’’Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava petoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.’’

Esimerkiksi tämän säännöksen voidaan siis katsoa soveltuvan pankkiasiakkaisiin kohdistuviin huijauksiin.

Oikeuden päätöksiä verkkohuijauksista ei kuitenkaan juurikaan ole. Yksi syy tähän on oikeudenkäyntien suuret kulut. Sen sijaan FINE Vakuutus- ja rahoitusneuvonta auttaa asiakkaita esimerkiksi pankin ja asiakkaan välisissä ongelmissa veloituksetta. Usein FINEn huijauksiin liittyvissä ratkaisussa on kiistaa siitä, kuka on korvausvastuussa huijauksesta johtuvista tappioista. Esimerkiksi ratkaisussa FINE-060698 (2023) uhri on joutunut huijarin luomalle valesivustolle, jonne on luovuttanut verkkopalvelutunnuksensa. Huijari on ottanut pankin mobiilisovelluksen käyttöön uhrin tunnuksilla, jolloin uhrille on pankin toimesta lähetetty infoviesti, jossa kerrotaan uudesta kirjautumisesta sovelluksessa. Viestissä kehotetaan myös olemaan yhteydessä pankin sulkupalveluun, mikäli vastaanottaja ei itse ole kirjautunut uudella laitteella. Uhri on kuitenkin jättänyt viestin huomiotta, jolloin huijari on päässyt siirtämään rahaa uhrin tileiltä ulkomaille yhteensä 32400 euroa. Asiakas on huomannut tilien tyhjentyneen, jonka jälkeen hän on ollut yhteydessä pankkiin sekä FINEen. Asiakas vaatii pankkia korvaamaan koko menetetyn summan. Pankin mukaan kyse on kuitenkin ollut asiakkaan omasta huolimattomuudesta etenkin sen takia, että aiempaan tekstiviestiin ei oltu reagoitu millään tavalla. FINEn pankkilautakunta on käsitellyt asian ja ei suosita asiassa hyvitystä. Kokonaisselvityksen perusteella Pankkilautakunta katsoo asiakkaan toiminnan osoittavan maksupalvelulaissa tarkoitettua törkeää huolimattomuutta. (FINE 2023.) Uhri ei ole siis tässä tapauksessa saanut minkäänlaisia korvauksia menetetyistä varoistaan.

Päättyneet riita-asiat

Lopputulos	Pankki	Sijoitus	Vakuutus	Yhteensä
Palveluntarjoajan eduksi	28/35%	14/70%	454/63 %	**496**
Asiakkaan eduksi	18/22%	4/20 %	154/21 %	**176**
Sovinto	17/21%	-	90/12 %	**107**
Jätetty käsittelemättä	13	2	11	**26**

Kuva 8 FINEn käsittelemät riita-asiat vuonna 2022 (FINE 2023)

Kuvassa 8 näemme vuonna 2022 FINEn käsittelemät riita-asiat. Tapaukset on eroteltu toimijan mukaan, mutta luvuista huomataan, että viime vuonna käsitellyistä pankkeihin liittyvistä valituksista enemmistö on päättynyt pankin eduksi. Vuoden 2022 yhteydenotot sekä vireille laitetut riita-asiat yli kaksinkertaistuivat verrattuna vuoteen 2021. Suuren nousun selittää pankkisektorilla juuri tietojenkalasteluun liittyvät riidat. (FINE Vuosikertomus 2022.)

Rikollisuus on usein myös kansainvälistä, joka luo omat haasteensa, sillä yhtenäistä sääntelyä maiden välillä ei ole (Peltomäki & Norppa 2015, 73). Mikäli uhri on suomalainen ja huijari ulkomailla, on sääntelyn puitteissa hankala saada tuomioita. Myös tutkinta on huomattavasti haastavampaa kansainvälisissä tapauksissa. Suomi liittyi vuonna 2022 Europolin yhteistyöryhmään, The Joint Cybercrime Action Taskforce eli J-CATiin. Yhteistyöryhmä tutkii ja pyrkii ennaltaehkäisemään rajat ylittävää rikollisuutta. (Poliisi 2022.) Ryhmä mahdollistaa maiden välistä yhteistyötä ja tiedonvaihtoa. Rajat ylittävää yhteistyötä on siis jo olemassa, mutta se on suhteessa pienimuotoista verrattuna kyberrikollisuuden valtavaan volyymiin.

3 Tutkimus

Opinnäytetyön tavoitteena on selvittää, miten huijauksia ennaltaehkäistään nyt ja tulevaisuudessa. Tässä kappaleessa käydään läpi opinnäytetyön tutkimusmenetelmä sekä tutkimuksen tulokset eriteltyinä tutkimuksen alaongelmien mukaisesti.

3.1 Tutkimusmenetelmä

Opinnäytetyön tutkimus on toteutettu kvalitatiivisella tutkimusotteella, käyttäen ennakointia, joka on yksi tulevaisuuden tutkimuksen menetelmistä. Tulevaisuudentutkimuksen ymmärtämiseksi käytetään tieteenfilosofian lähestymismenetelmiä. Ennakoinnin tarkoitus tai tavoite ei ole ennustaa tarkkaa tulevaisuutta, vaan tuoda esille erilaisia perusteltuja näkökulmia ja käsityksiä tulevaisuuden näkymistä. (Turun yliopisto 2022, 349 ja 351.) Valittu menetelmä tukee opinnäytetyön tavoitteita, sillä ennakoinnissa pyritään havaitsemaan ilmiöiden laadullisia ja määrällisiä muutoksia sekä nykyisiä ja menneitä trendejä, joiden perusteella voidaan arvioida tulevaisuuden näkymiä.

Ennakoinnin tavat jäsennetään yleisesti kahteen päätyyppiin; pitkän aikavälin epävarmuuksien ennakointi sekä lähitulevaisuuden riskien ja mahdollisuuksien ennakointi. Opinnäytetyön aikarajauksen kannalta jälkimmäinen sopii paremmin tutkimukseen. Lähitulevaisuuden riskien ennakoinnilla pyritään vähentämään epävarmuuksia ja hallitsemaan niitä olemassa olevan tiedon avulla. (Turun yliopisto 2022, 353.) Kun tiedossa on mahdolliset tulevaisuuden riskit, on niihin helpompi varautua.

Tutkimuksen pääasiallinen aineisto on kerätty asiantuntijahaastatteluilla, jota voidaan myös kutsua ennakointimenetelmien puitteissa asiantuntijaennakoinniksi. Asiantuntijaennakoinnissa rajattu joukko asiantuntijoita pohtii tulevaisuutta määritellyn aiheen pohjalta (Turun yliopisto 2022, 352). Asiantuntijuus on häilyvä käsite, mutta tietoyhteiskunnissa asiantuntijan piirteeksi on määritelty pitkälle erikoistunut tiede- ammatti tai instituutioperusteinen asiantuntijuus. Asiantuntijalla on aiheesta sellaista tietoa, jota maallikolla ei yleisesti ottaen ole. (Hyvärinen, Aho, Nikander & Ruusuvuori 2017, luku 9.) Kaikki tutkimukseen valitut asiantuntijat työskentelevät pankin fraud- eli petososastolla, joten ammattinsa puolesta heistä jokaisella on tietoa ja taitoa pohtia tulevaisuuden näkymiä. Haastatteluissa on käytetty yhdeksää kysymystä, joiden avulla on pyritty löytämään vastaukset tutkimusongelmiin. Haastattelut on toteutettu sähköisesti, joko sähköposti- tai Teams-haastatteluna.

Tutkimuksen tuloksena ei synny eksaktia kuvausta siitä, miltä huijaukset tai niiden ennaltaehkäisy tulevat näyttämään viiden vuoden päästä. Sen sijaan asiantuntijahaastatteluita, kirjallisuutta sekä verkkolähteitä apuna käyttäen tutkaillaan sitä, millainen tulevaisuus meitä huijausten ennaltaehkäisyn osalta saattaa odottaa.

3.2 Tutkimuksen tulokset

Tutkimuksen tulokset on saatu asiantuntijahaastatteluina joko kirjallisesti tai suullisesti, jolloin tulokset on kerätty muistiinpanoina. Tulokset on analysoitu käyttäen sisällönanalyysiä, jonka tarkoituksena on luoda sanallinen ja ymmärrettävä kuvaus tutkittavasta aiheesta (Tuomi & Sarajärvi 2018, luku 4.4.2).

Tutkimuksessa on haastateltu kolmea asiantuntijaa kahdesta eri pankista. Haastateltaville on annettu pseudonyymit, jotta vastaukset ja vastaajat pystytään pitämään mahdollisimman anonyyminä. Heidät on tutkimuksessa nimetty Asiantuntija A:ksi, Asiantuntija B:ksi sekä Asiantuntija C:ksi. Asiantuntija A ja Asiantuntija B työskentelevät pankissa X, Asiantuntija C pankissa Y. Jokaisen haastateltavan ammattinimike on yleistetty Fraud-asiantuntijaksi, sillä he työskentelevät pankkien Fraud- eli huijausten ja petosten osastoilla.

Tutkimuksen tulokset on eritelty tutkimuksen kolmen alaongelman mukaisesti.

3.3 Pankkiasiakkaisiin kohdistuvat huijaukset tällä hetkellä

Opinnäytetyön tietoperustassa on käyty perusteellisemmin läpi yleisiä pankin nimissä tehtyjä huijauksia, joten tämä alaongelma jätetään hiukan suppeammaksi. Käydään kuitenkin läpi haastatteluissa esille tulleet pääpointit.

Kaikki haastatellut asiantuntijat kertovat, että yleisimpien huijausten joukossa on viime vuosina ollut turvatilihuijaukset. Kyseiset huijaukset ovat olleet todella yleisiä muissa pohjoismaissa ja valitettavasti rantautuneet myös Suomeen. Lisäksi pankin nimissä lähetetyt kalasteluviestit ovat jatkaneet suosiossa. Kalasteluviestejä on helppo lähettää massaviesteinä, joten menetelmä on suhteellisen vaivaton huijareille.

Asiantuntija A:n (31.10.2023) mukaan huijauspuhelut ovat olleet viime aikoina huijareille tuloksellisia. Usein ennen puhelua asiakkaan tietoja on jo kartoitettu kalasteluviestillä tai -sivustolla. Kun pankkivirkailijaksi esittäytynyt huijari sitten soittaa uhrille, osaa hän jo kertoa kalastelun avulla kerättyjä tietoja, joka luo uskottavuutta asiakkaan silmissä. Asiantuntija A:n mukaan puheluissa käytetään hyväksi myös auktoriteetin tuomia etuja. Pankkivirkailijaan uskotaan ja luotetaan jopa siinä määrin, että omat käyttäjätunnukset tai korttitiedot luovutetaan puhelun aikana sen suurempia miettimättä. Tällaiset pankin nimissä tehdyt huijauspuhelut ovat usein suomalaisten rikollisten tekemiä, sillä oletusarvona on se, että suomalaisen pankin virkailijat puhuvat suomea.

3.4 Huijausten tulevaisuuden näkymät

Kaikki kolme asiantuntijaa uskovat, että tulemme seuraavan viiden vuoden aikana kohtaamaan yhä teknisesti taitavampia huijauksia. Kalastelusivustot voivat olla jo nykyään lähes identtisiä esimerkiksi pankin verkkosivujen kanssa, joten mikäli ne kehittyvät vieläkin paremmiksi, on tulevaisuuden haasteena keksiä keinoja niiden estämiseksi.

Tekstiviestihuijauksissa tullaan Asiantuntija B:n mukaan näkemään yhä uskottavampaa suomen kieltä ja viestit voivat olla entistä yksilöidympiä. Jos huijausviesti alkaakin normaalin hei:n sijaan yksilöidysti oman etunimesi kanssa ’’Hei Jarkko! Korttisi on lukittu. Otathan yhteyttä asiakaspalveluumme seuraavan linkin kautta…’’ tuntuu se huomattavasti henkilökohtaisemmalta jolloin myös uskottavuus paranee.

Asiantuntija A uskookin, että huijausten yksilöinti tulee olemaan yksi tulevaisuuden trendeistä, sillä se tekee huijauksista huomattavasti uskottavampia. Ihmiset jakavat itsestään sosiaaliseen mediaan valtavan paljon tietoa, huijarille parhaassa tapauksessa somesta löytyy yhteystiedoista lähtien kaikki. Kuvitellaan tilanne, että uhrilla on käytössään Instagram, Facebook sekä LinkedIn. Huijari löytää potentiaalisen uhrin ensin Facebookista, jossa uhrilla lukee parisuhdetiedot, lapsien nimet sekä suora linkki uhrin Instagram-tilille. Instagram-tililtä huijari näkee, että uhri on käynyt kaksi kuukautta sitten lomalla Kreikassa. Sen jälkeen huijari etsii uhrin LinkedInistä nimellä, josta löytyy uhrin työpaikkatiedot ja sähköpostiosoite sekä puhelinnumero mahdollisia yhteydenottoja varten. Huijarilla on uhrista ja hänen elämästään jo paljon tietoa, joten hän soittaa uhrilleen ja esittäytyy pankin virkailijana. Hän kertoo uhrilleen, että asiakastiedot on päivitettävä heti puhelun alussa, onko sähköpostiosoitteesi xx.xx@gmail.com? Oletko vielä vakituisessa työpaikassa yrityksessä xx? Pitääkö paikkaansa, että olet vielä naimisissa ja sinulla on kaksi alaikäistä lasta? Kun uhri on varmistanut kaikki tiedot paikkaansa pitäviksi, saattaa huijari kertoa, että uhrin kortilta on yritetty maksaa eilen Kreikkaan epäilyttävä maksu. Uhrilla nousee hätä tuntemattomasta maksusta ja kertoo että on kyllä ollut Kreikassa lomalla lähiaikoina. Huijari pyytää uhrin korttitietoja kortin sulkemiseksi ja koko puhelun perusteella uhri luottaa pankkivirkailijana esiintyvään huijariin ja antaa tiedot.

Sitä myötä, kun tietoisuus huijauksista ja niiden toteutustavoista kasvaa, on huijareiden keksittävä yhä vakuuttavimpia tapoja toimia. Asiantuntija C uskoo, että huijarit tulevat hyväksikäyttämään esimerkiksi tilaisuuksia, jolloin pankissa on meneillään julkisesti tiedossa olevia uudistuksia. Uhrille on pankin toimesta ilmoitettu tulevasta uudistuksesta, jonka jälkeen hän saa puhelun toimihenkilöksi esittäytyvältä huijarilta. Huijari osaa kertoa pankissa meneillään olevasta uudistuksesta, joka tuntuu uhrille uskottavalta.

Kannamme nykyteknologian mahdollistamana pankkisovellusta ja älylompakoita mukanamme jatkuvasti. Parilla puhelinruudun napautuksella laskumme on maksettu, ystävälle on lainattu rahaa Mobilepayssä ja ruokaostosten maksu hoituu AppleWalletin avulla fyysisen kortin unohduttua kotiin. Kirjailija Brett King (2019, 31) uskoo, että tekoäly tulee olemaan yhä suurempi osa päivittäisiä pankkipalveluitamme. Hän uskoo, että tulevaisuudessa esimerkiksi ääniohjattavia apuohjelmia, kuten Siriä ja Alexaa tullaan käyttämään laskujen maksussa, tilisiirroissa, sijoitusneuvonnassa ja verkkokauppojen tilausten tekemisessä. Asiantuntijat A ja B sitä vastoin uskovat, että voice cloning- ja deepfake-huijaukset tulevat yleistymään teknologian kehittyessä. Voice cloning, eli äänen kloonaus on nykyisen tekoälyn avulla helppoa, tarvitaan vain tarpeeksi ääninäytteitä ihmisen puheesta. Viime aikoina internetissä on pyörinyt esimerkiksi äänityksiä, joissa Sauli Niinistö laulaa tämän hetken hittikappaleita. Itse presidentti ei tietenkään ole kyseessä, vaan tekoälyn luoma ääniraita. Mikäli pelkällä äänellä pystyy tekemään tilisiirtoja, sijoituspäätöksiä ja ostoksia, kasvaa myös väärinkäytösten ja huijausten mahdollisuudet. Jos käytössäsi on vaikkapa Alexa-laite, jolla normaalisti teet tilisiirtoja sanomalla ’’Alexa, lähetä henkilölle X 50 euroa rahaa.’’, miten pystymme estämään esimerkiksi laitteen hakkeroinnin ja voice cloningin avulla tehdyn tilisiirron rikollisen toimesta?

Deepfake sen sijaan on kuva tai video, joka tekoälyn avulla saadaan näyttämään siltä, että videossa olisi sinä, minä tai vaikkapa aiemmin mainittu Sauli Niinistö. Deepfakeja ja voice cloningia voidaan käyttää esimerkiksi elokuviin, viihteeseen tai videopeleihin, mutta eniten huolta aiheuttaa niiden epäeettinen käyttö. (Lyon 2023, luku 2.) Jos mietitään, miten pankin nimissä voitaisiin käyttää deepfake-videoita, yhtenä esimerkkinä voisi olla toimitusjohtajan käyttö videossa. Pankkien toimitusjohtajat ovat asemansa puolesta julkisia henkilöitä ja heistä löytyy verkosta kuva- ja videomateriaalia. Tämän materiaalin avulla on helppo tehdä video, jossa toimitusjohtaja esimerkiksi kertoo, että asiakkaiden tilitiedot ovat vaarantuneet ja tilien varat on välittömästi siirrettävä turvatilille, joka videossa on ilmoitettu.

3.5 Huijausten ennaltaehkäisy

Tämä alaongelma on selkeyden vuoksi jaoteltu kahteen eri osioon. Ensimmäisessä osiossa käydään läpi, miten tällä hetkellä huijauksia ennaltaehkäistään. Toisessa osiossa keskitytään siihen, millaisia ennaltaehkäisyn keinoja saatamme tulevaisuudessa nähdä.

3.5.1 Ennaltaehkäisy nyt

Yksi tärkeimpiä ennaltaehkäisyn keinoja tällä hetkellä on asiakkaiden kouluttaminen ja tiedon jakaminen huijauksista. Pankissa X on pyritty pitämään huijauksista kommunikointi mahdollisimman avoimena verkkosivuilla, sosiaalisessa mediassa sekä pankin omassa sovelluksessa. Asiakkaille

tiedotetaan eri kanavoissa esimerkiksi, jos pankin nimissä liikkuu aktiivisia huijauskampanjoita. Asiantuntija A:n mukaan toistuvalla viestinnällä on myös varjopuolensa, mutta ne tunnistetaan. On esimerkiksi mahdollista, että asiakkaan kohdatessa usein viestintää erilaisista huijauksista, jäävät ne helpommin huomiotta. Myös sähköisten kanavien käytössä uutisoinnin ulkopuolelle jää etenkin vanhuksia. Huijarit hyväksikäyttävät monesti ikäihmisten puutteellista digiosaamista, joka tekee heistä alttiimpia huijauksille. Asiantuntija C kertoo, että pankissa Y pyritään informoimaan ja nostamaan tietoisuutta huijauksista asiakkaiden kesken esimerkiksi sähköisissä kanavissa, sosiaalisessa mediassa sekä erilaisissa seminaareissa. Erityisen tärkeäksi koetaan informoida asiakkaita esimerkiksi siitä, että pankki ei koskaan kysy tiettyjä asioita, kuten verkkopalvelun tunnuksia missään muualla kuin omalla kirjautumissivuillaan.

Henkilökunnan kouluttamisella pyritään ennaltaehkäisemään huijauksia. Kun toimihenkilö kohtaa työssään asiakkaan, joka on esimerkiksi joutumassa huijauksen uhriksi, on toimihenkilön tiedettävä miten menetellä. Esimerkiksi tieto erilaisista huijausmenetelmistä on tärkeässä roolissa asiakkaan kohtaamisessa. (Asiantuntija B 2023.)

Viime vuosina kerättävän datan määrä on vain kasvanut, joten työn helpottamiseksi teknologiaa ja tekoälyä pyritään käyttämään päätöksenteossa. Etenkin koneoppimista, joka on tekoälyn yksi osa-alueista, käytetään huijausten ennaltaehkäisyssä. Koneoppimisessa järjestelmä kerää dataa siitä, mikä on esimerkiksi normaalia toimintaa. Kun kone on luonut kuvan siitä, mitä normaali toiminta on, huomaa se myös poikkeavuudet. (Wilson 2021, 115–123.) Tällä hetkellä pankissa käytetään tekoälyä esimerkiksi epäilyttävän toiminnan havaitsemiseen. Jos kone havaitsee, että verkkopalvelutunnuksilla tai kortilla on epäilyttäviä tapahtumia, laittaa se automaattisesti tunnukset tai kortin lukkoon. Koneen toiminta ei ole kuitenkaan aina moitteetonta. Jos kone huomaa, että asiakas, joka ei ole vuosiin poistunut suomesta käyttää yhtäkkiä korttiaan vaikkapa Singaporessa, saattaa se katsoa tämän epäilyttäväksi toiminnaksi. Todellisuudessa asiakas on lähtenyt vain lomailemaan ja ulkomailla ollessaan huomaa, että kortti on lukittu turvallisuussyistä. (Asiantuntija A 2023.)

Tällä hetkellä pankki huomioi petosriskin mahdollisuuden palveluiden suunnittelussa, asiointikanavien muutoksissa ja muissa tuotteissaan. Esimerkiksi verkkopankkien ja tunnuslukusovellusten tietoturvaa pyritään jatkuvasti parantamaan. Myös korttien turvarajat on tehty asiakkaan varojen suojaamiseksi. Turvarajoja on kuitenkin helppo muokata verkkopankissa, joten jos huijarilla on pääsy korttiin että verkkopankkiin, ei turvarajoilla ole juurikaan merkitystä. (Asiantuntija C 2023.)

Traficom on tehnyt yhteistyötä suomalaisten operaattorien kanssa estääkseen ulkomailta tulevat puhelut, jotka on naamioitu suomalaisiksi. Uusi operaattoreita koskeva määräys on tullut voimaan lokakuussa 2023. Tällä määräyksellä on pyritty minimoimaan ulkomailta tulevia soittohuijauksia. Operaattoreilla on jatkossa velvollisuus estää naamioidut numerot. Traficomin johtavan

asiantuntijan Klaus Niemisen mukaan heti määräyksen astuttua voimaan, on päivittäin estetty jopa 200000 huijauspuhelua. (Traficom 2023.) Vaikka Traficomin operaattoreita koskeva määräys oli onnistunut, ei uskota, että soittohuijaukset tulevat loppumaan kokonaan. Etenkin pankin nimissä tehdyt soittohuijaukset tulevat lähes aina suomalaisesta numerosta, jota operaattorin järjestelmät eivät automaattisesti estä.

Tärkeäksi ennaltaehkäisykeinoksi nousi myös yhteistyö viranomaisten, kuten Poliisin ja Kyberturvallisuuskeskuksen kanssa. Tietoisuuden levittäminen ja yhteiset tavoitteet rikollisuuden estämisessä on yhteistyön myötä helpompaa. (Asiantuntija B 2023.) Viranomaiset järjestävät yhteistyössä pankkien ja muiden finanssialan toimijoiden kanssa erilaisia kampanjoita kyberturvallisuuteen liittyen. Tämän opinnäytetyön teoriaosuudessakin käytetty Finanssialan ja pankkien yhteistyönä luoma taulukko huijauksille menetetyistä varoista on oiva esimerkki siitä, miten tietoisuutta pyritään luomaan.

3.5.2 Ennaltaehkäisy tulevaisuudessa

Asiantuntija A ajattelee nykyisten ennaltaehkäisykeinojen vain korostuvan tulevaisuudessa. Pankin on luotava entistä helppokäyttöisempiä ja turvallisempia työkaluja asiakkailleen, joilla pyritään minimoimaan väärinkäytöksen riskejä.

Aiemmin mainitun Traficomin operaattoreita koskevan määräyksen lisäksi ollaan kehittelemässä myös tapoja, joilla tekstiviestihuijaukset saadaan kuriin (Traficom 2023). Tällä hetkellä huijarit pystyvät lähettämään viestin samaan viestiketjuun, josta pankki on lähettänyt viestejä. Asiakkaan silmin tämä näyttää siis siltä, että kaikki viestit ovat tulleet samasta numerosta, vaikka näin ei ole. Mikäli viesti tulisi kokonaan tuntemattomalta lähettäjältä, saattaisi tämä helpottaa huijausviestin tunnistamisessa. Tällaiset samaan viestiketjuun tulevat viestit ovat olleet erityisen yleisiä, joten niiden taklaamiseksi on välttämätöntä tehdä toimia. Uskomuksena on, että huijausviestien laatu tulee paranemaan entisestään. Yhä vakuuttavampia viestejä esimerkiksi kielellisesti ja ulkonäöllisesti tullaan todennäköisesti näkemään. (Asiantuntija B 2023.)

Tämän päivän maksuliikenne on todella nopeaa. Tilisiirron ulkomaille voi tehdä sekunneissa ja maksu menee läpi välittömästi. Asiantuntija A:n mukaan pankkien on tulevaisuudessa mietittävä, kuinka tilisiirtojen kanssa toimitaan turvallisemmin. Onko todella tarpeellista, että rahaliikenne toimii näin nopeasti? Tällä hetkellä palveluiden sujuvuus on pyritty tekemään mahdollisimman vaivattomaksi, mutta vaivattomuuden ei tulisi tulla turvallisuuden hinnalla. Pankilla ei ole juurikaan automatisoidun tarkastuksen lisäksi aikaa toimia tilisiirron estämiseksi, vaikka aihetta saattaisi olla. Maksuliikenteen seuraamisessa tullaan tulevaisuudessa todennäköisesti hyödyntämään tekoälyä entistä monipuolisemmin. Tällä hetkellä datan keräys rajoittuu pankin oman toiminnan sisälle, mutta mikäli

esimerkiksi Eurooppa-tasoisesti pystyttäisiin keräämään dataa, monipuolistuisi tekoälyn käyttö ja tehokkuus. Jatkossa myös yhteistyö yli rajojen tulee korostamaan merkitystä, sillä ongelma on maailmanlaajuinen. (Asiantuntija A 2023.)

Maksuliikenteen seuraamisen yhteydessä korostuu pankkien lain asettama velvollisuus tuntea asiakkaansa, KYC eli know your customer. Asiantuntija A uskoo, että tulevaisuudessa asiakkaiden tunteminen tulee olemaan entistä tärkeämpää rahaliikenteen monitoroinnissa. Osan huijauksista voisi parhaassa tapauksessa estää asiakkaan riittävällä seurannalla ja käyttäytymisen ymmärtämisellä. Asiantuntija C:n mukaan erilaiset monitorointitavat tulevat korostumaan tulevaisuudessa nykyistä enemmän. Teknologian tärkeys näkyy erityisesti monitoroinnissa, sillä volyymit ovat valtavia. Jokaisen asiakkaan kaikki korttiostokset, tilisiirrot ja niin sanotun normaalin käyttäytymisen seuranta olisi mahdotonta ilman toimivia ohjelmistoja.

FINE:n päätöksien perusteella voimme päätellä, että tällä hetkellä huijauksen uhrit joutuvat usein itse korvausvastuuseen menetetyistä rahoista. Asiantuntija A uskoo, että seuraamme Iso-Britannian jäljissä ja että asia tulee olemaan tulevaisuudessa eri tavalla. Payment Systems Regulator (PSR) on julkaissut 7.6.2023 tiedon siitä, että vuoteen 2024 mennessä Iso-Britanniassa otetaan käyttöön uusi säännös, joka auttaa uhreja saamaan tilisiirtona huijaukseen menetetyt rahat takaisin. Uudessa säännöksessä rahan lähettävä sekä vastaanottava pankki olisivat 50:50 korvausvelvollisia menetetyistä varoista. Jos uhri siis menettää 10000 £ huijaukseen, korvaa lähettäjäpankki siitä uhrille 5000 £ ja vastaanottava pankki 5000 £. Muutos entiseen on pankkien kannalta huomattava, sillä PSR:n mukaan vuonna 2022 Iso-Britanniassa kyseisten kaltaisille huijauksille on menetetty jopa 500 miljoonaa puntaa. Asiantuntija A uskoo, että kyseinen säännös luo pankille paineita luoda erilaisia ennaltaehkäisyn menetelmiä huijauksiin. Kuten aiemmin mainittu, tällä hetkellä rahan siirto ulkomaille onnistuu jopa sekunneissa, sillä asiointi on pyritty tekemään asiakkaan kannalta mahdollisimman sujuvaksi. Tämä pelaa myös huijareiden pussiin. PSR:n toimitusjohtaja Chris Hemsley uskoo, että uusi säännös antaa jokaiselle rahoituslaitokselle syyn toimia huijareita ja huijauksia vastaan entistä tehokkaammin. (Payment Systems Regulator 2023.) Pankeilla on siis tulevaisuudessa uhkana joutua korvausvelvollisiksi, vaikka tämän päivän säännöstelyllä huijauksen uhriksi joutuneen asiakkaan katsottaisiinkin toimineen vaikkapa törkeän huolimattomasti.

Asiantuntija A kertoo myös tulevasta maksupalveludirektiivistä. Vuonna 2018 on otettu käyttöön toinen maksupalveludirektiivi, PSD2. Tässä direktiivissä uudistuksena tuli esimerkiksi vaatimus siitä, että asiakkaan on tunnistauduttava verkko-ostoksia tehdessään. Komissio on valmistelemassa kolmatta maksupalveludirektiiviä, PSD3, joka säätelee muun muassa huijausten torjuntaa lainsäädäntötasolla. Komissio esittää uudessa ehdotuksessaan, että ennaltaehkäisytyökaluksi otettaisiin käyttöön järjestelmä, jossa voitaisiin jakaa tietoa pankkien välillä mahdollisesti rikoksiin

käytetyistä tileistä. Tällaisella tiedonvaihdolla pyritään helpottamaan huijausten torjuntaa. (Finanssiala 2023.) Tällä hetkellä pankkien välisen tiedon jakaminen on hankalaa pankkisalaisuuden takia. Jos asiakkaan tilit on esimerkiksi suljettu pankissa 1 huijauksiin liittyvän rahanpesun estämisen takia, voi hän mennä pankkiin 2 avaamaan uuden tilin ongelmitta. Tällaiset uudet muutokset eivät tule nopeasti pankkien ja muiden viranomaisten päästä, on toimittava sääntelyn ja lakien mukaisesti ja hyödyllisissä uudistuksissakin saattaa kestää vuosia. Huijaukset sen sijaan kehittyvät jatkuvasti, eikä huijareiden tarvitse välittää tietosuojasta tai GDPR:stä. (Asiantuntija A 2023.) Pankkien haasteena on siis toimia sääntelyn puitteissa jatkuvasti kehittyvässä ympäristössä.

3.6 Huijauksilta suojautuminen henkilöasiakkaan näkökulmasta

Tutkimuksessa on käyty läpi keinoja, joilla pankki ennaltaehkäisee huijauksia. Mutta mitä voimme itse tehdä pienentääksemme riskiä joutua huijauksen uhriksi?

Poliisi on julkaissut verkkosivuillaan hyvän ohjeen henkilöasiakkaille huijauksilta suojautumisesta.

Miten suojaudut huijaukselta

- Älä anna puhelimitse tai sähköpostitse henkilö- tai pankkitietojasi.
- Jos olet epävarma, onko kyseessä huijaus, sulje puhelu ja soita viranomaisen tai yrityksen omaan viralliseen numeroon.
- Älä maksa vaadittuja summia.
- Älä avaa epäilyttäviä linkkejä sähköpostissa tai puhelimessa.
- Älä luota sokeasti sähköpostin lähettäjätietoihin ja tarkista selaimen kohdeosoite.
- Vaihda salasana. Vahva salasana suojelee arvaamiseen perustuvilta hyökkäyksiltä ja tunkeutumisyrityksiltä.
- Jos on huolissaan tietokoneen tai mobiililaitteen kameran kaappaavista haittaohjelmista, voi kameran peittää esimerkiksi teipillä.
- Haittaohjelmilta voi parhaiten suojautua pitämällä tietokoneen käyttöjärjestelmä- ja ohjelmistopäivitykset ajan tasalla sekä asentamalla ohjelmia vain luotetuista lähteistä.
- Varoita läheisiäsi ja keskustelkaa petosyritysten vaaroista.

Kuva 9 Miten suojaudut huijaukselta (Poliisi 2021)

Ohjeessa käydään läpi yleisimmät huijaukselta suojautumisen keinot. Asiakkaan ei tule antaa puhelimitse tai sähköpostitse henkilö- tai pankkitietoja, tehdä tilisiirtoja tai avata epäilyttäviä linkkejä. Puhelun voi myös katkaista, jos ei ole varma, onko kyseessä oikea puhelu vai ei. Soittamalla esimerkiksi pankin asiakaspalveluun puhelun saamisen jälkeen, voi asiakas varmistaa onko puhelu aito. Tärkeää on myös olla tarkkana selaimen osoitteen kanssa. Mikäli osoite on pankkiverkkosivu.fi oikean pankki.fi osoitteen sijaan, on syytä epäillä sivuston aitoutta. Myös sähköpostin lähettäjätiedot on hyvä tarkistaa. Mikäli pankkivirkailijaksi esiintyvä henkilö lähettää sähköpostia gmail-osoitteesta, kyseessä tuskin on oikea virkailija. Tärkeää on myös varoittaa läheisiä liikkeellä olevista huijauksista. Etenkin vanhukset jäävät usein sähköisten varoitusten ulkopuolelle, joten tietoa huijauksista voidaan jakaa mahdollisuuksien mukaan.

Mutta mitä on tehtävä, jos huomaa joutuneensa huijauksen uhriksi?

Kuva 10 Toimi näin, jos tulet huijatuksi (Poliisi 2021)

Monesti huijauksen uhri huomaa tulleensa huijatuksi suhteellisen nopeasti. Etenkin kalasteluviesteissä pyritään herättämään kiireen tuntua, jolloin uhri klikkaa viestissä tullutta linkkiä ja syöttää verkkopalvelutunnuksensa huijaussivustolle sen enempää miettimättä. Kun tilanne rauhoittuu, ymmärtää uhri, että joku tässä tilanteessa oli outoa. Poliisi on julkaissut sivuillaan kuvassa 10 näkyvän listan siitä, mitä uhrin on syytä tehdä jouduttuaan huijatuksi. Mikäli uhri on syöttänyt korttitiedot tai verkkopalvelutunnukset huijaussivustolle, on syytä olla pankkiin yhteydessä välittömästi. Pankki

sulkee vaarantuneet palvelut, jotta uhrin verkkopankkiin ja korttiin ei enää päästä. On tärkeää ilmoittaa omalle pankille mahdollisimman nopeasti huijausepäilystä. Huijarit voivat tehdä verkkopankissa tilisiirtoja, hakea lainaa ja nostaa luottokortin saldon tilille. On mahdollista, että uhrin kaikki varat on siirretty pois, jos sulkutoimenpiteitä ei tehdä mahdollisimman pian. Pankille on myös syytä ilmoittaa, jos huijaus on tehty pankin nimissä. Silloin liikkeellä olevista huijauksista pystytään ilmoittamaan asiakkaille.

Huijauksen uhrilla on myös syytä tehdä rikosilmoitus. Rikosilmoitus on hyvä tehdä, vaikka taloudellista haittaa ei olisikaan huijauksesta aiheutunut. Mikäli tililtä on sen sijaan hävinnyt rahaa, monesti pankki vaatii asiakkaan tekemän rikosilmoituksen, jotta mahdollinen palautuspyyntö voidaan käsitellä.

Viimeisenä listalla on Rikosuhripäivystyksen verkkosivuille linkki. Se on palvelu, josta uhri voi saada tukea ja apua. Huijaukset aiheuttavat usein niin taloudellista kuin henkistä ahdinkoa, joten uhrien on hyvä muistaa, että apua on tarjolla.

Jokaisella asiakkaalla on vastuu pitää huoli turvallisesta pankkiasioinnista omassa päässään. Esimerkiksi verkkopalvelutunnuksen ja korttitietojen huolellinen ja vastuullinen käyttö kuuluu oleellisena osana vastuullista asiointia.

4 Yhteenveto ja pohdinta

Opinnäytetyön tavoitteena oli selvittää, millaisia pankin nimissä tehtäviä huijauksia pankkiasiakkaisiin kohdistuu ja miten niitä voidaan estää nyt ja seuraavan viiden vuoden aikana. Huijauksien lukumäärät ovat olleet jo vuosia kasvussa ja huijareille vuosittain menetetyt summat ovat valtavia.

Tietoperustassa käytiin läpi yleisimpiä pankin nimissä tehtyjä huijauksia sekä huijareiden kohteena olleet peruspalvelut. Lisäksi katsaus lakikäytäntöihin, joiden perusteella päättelimme, että huijauksiin menetetyt rahat jäävät usein uhrinsa itse korvattaviksi. Tutkimus toteutettiin käyttäen ennakointimenetelmiä. Ennakoinnissa käytettiin apuna asiantuntijahaastatteluita, kirjallisia- sekä verkkolähteitä. Tutkimuksen tuloksena saatiin kuvaus siitä, miltä huijausten ennaltaehkäisy näyttää tällä hetkellä ja kuinka sen oletetaan kehittyvän seuraavan viiden vuoden aikana.

Teknologian kehitys on vauhdittanut huijauksien kehitystä. Pankkien nimissä lähetetään tietojenkalasteluun liittyviä viestejä ja yhdistävänä tekijänä näissä tietojenkalasteluviesteissä on viestiin liitetty linkki, jota pyydetään seuraamaan. Tämänhetkisenä trendinä on nostanut päätään etenkin turvatilihuijaukset, joissa asiakkaan tilitietojen kerrotaan vaarantuneen. Pitääkseen varat turvassa, kehotetaan asiakasta siirtämään ne huijarin ilmoittamalle ’’turvatilille’’. Todellisuudessa turvatiliä ei ole, vaan asiakkaan varat päätyvät huijarin taskuun.

Myös laadukkaat verkkosivuhuijaukset ovat tätä päivää. Huijarit voivat kopioida pankkien kirjautumissivut lähes identtisesti. Jos asiakas ei ole tarkkana esimerkiksi verkkosivun osoitteen kanssa, päätyvät verkkopalvelutunnukset helposti vääriin käsiin.

Puhelimen välityksellä pankkien nimissä tehdyt huijaukset ovat etenkin suomalaisten huijarien käsialaa. Uskottava suomen kieli ja uhrista mahdollisesti hankitut ennakkotiedot lisäävät soittohuijausten onnistumisprosenttia. Traficom on kehitellyt yhdessä operaattoreiden kanssa keinoja, joilla soittohuijauksia ja tekstiviestihuijauksia saataisiin kuriin. Kampanjassa kotimaisiksi numeroksi naamioituneita ulkomaisia numeroita vastaan on nähty jo suuria onnistumisia. Kuten mainittu, pankin nimissä tehdyt soittohuijaukset tulevat kuitenkin usein suomalaisista numeroista. Tällaisten suomalaisten huijauspuheluiden ennaltaehkäisyssä korostuu asiakkaiden informointi, sillä teknologian avulla ei ole mahdollista tunnistaa, onko soittaja huijari vai ei.

Seuraavan viiden vuoden aikana asiantuntijamme uskovat, että tulemme näkemään yhä teknisesti taitavampia huijauksia. Teemat todennäköisesti tulevat pysymään samankaltaisina, mutta huijaukset kehittyvät entistä yksilöidymmiksi. Yksilöityjä huijauksia on huomattavasti vaikeampi tunnistaa, joten asiakkaiden on oltava todella tarkkoja. Myös voice cloning ja deepfake-huijaukset saattavat yleistyä vuosien varrella.

Tällä hetkellä yhdeksi tärkeimmiksi ennaltaehkäisykeinoiksi nostettiin tiedon jakaminen asiakkaille. Lähes kaikissa pankin nimissä tehdyissä huijauksissa asiakas itse on heikko lenkki turvallisuuden osalta. Asiakas syöttää verkkopalvelutunnukset tietojenkalastelusivulle tai antaa korttitiedot huijarille puhelimitse. Tietoa huijauksista jaetaan etenkin sähköisissä lähteissä, verkkosivuilla, sosiaalisessa mediassa sekä pankkien omissa sovelluksissa. On syytä kuitenkin pohtia, miten vanhimpiakin asiakkaita saataisiin informoitua liikkeellä olevista huijauksista.

Tiedon jakamisen lisäksi teknologia ja tekoäly ovat isossa roolissa ennaltaehkäisytoimissa. Mitä enemmän pankit saavat kerättyä dataa asiakkaiden maksuliikkeestä ja muodostettua kuvaa siitä, mikä normaali toiminta on asiakkaalle, sitä paremmin esimerkiksi epäilyttäviä tilisiirtoja voidaan estää. Tulevaisuuden kannalta toiveena on, että dataa ja tietoa voitaisiin jakaa vapaammin pankkien välillä. Tällä hetkellä data, jota pankit keräävät asiakkaistaan, jää pankkikohtaiseksi. Mikäli tulevaisuudessa pystyisimme jakamaan dataa esimerkiksi Eurooppatasolla, tulisi ennaltaehkäisystä helpompaa. Huijaukset ovat kansainvälinen ongelma, eivätkä huijarit suinkaan toimi vain oman maiden rajojen sisällä.

Mitä enemmän keinoja keksitään huijausten estämiseksi, sitä enemmän huijarit pyrkivät kiertämään ne. Uusia huijauksia ja huijaustapoja keksitään jatkuvasti. Huijausten ehkäisyksi tehdään jatkuvasti toimia ja ennaltaehkäisyn kannalta on tärkeää pysyä ajan tasalla siitä, millaisia trendejä on liikkeellä. Haasteita ennaltaehkäisyssä luovat pankkeja koskeva sääntely ja lait. Pankkien on toimittava pankkisalaisuuden puitteissa, eikä tällä hetkellä tietoa esimerkiksi pankkien välillä voida jakaa.

4.1 Tutkimuksen luotettavuus ja jatkokehitysideat

Validiteetti, eli luotettavuus kertoo, miten tarkasti on pystytty kertomaan siitä, mitä on lähdetty tutkimaan (Nummenmaa, Holopainen, Pulkkinen & Kimpimäki 2019, 20). Tässä kappaleessa arvioidaan opinnäytetyön luotettavuutta.

Tutkimus on toteutettu käyttäen tulevaisuuden tutkimuksen menetelmää, tarkennuksena ennakointia. Ennakointi ei anna tarkkaa vastausta siitä, miltä tulevaisuus tulee näyttämään. Tutkimuksen tulokset kannattaa siis ottaa enemmänkin kuvauksina ja aatteina siitä, miltä tulevaisuus tuo tullessaan, ennemmin kuin tarkkana totuutena. Meistä kukaan ei ole käynyt tulevaisuudessa ja kuten olemme viimeisen kolmen vuoden aikana joutuneet huomaamaan, maailmassa voi tapahtua mitä tahansa.

Tutkimukseen haastatellut asiantuntijat ovat kaikki oman alansa ammattilaisia. Kolmen ammattilaisen otanta on kuitenkin suhteellisen pieni ja vaikka monia yhteneviä mielipiteitä asioista löytyi, ei se välttämättä anna meille koko ammattikunnan mielipidettä. Asiantuntijat ovat kahdesta eri

pankista, joten myös pankkien väleillä saattaa olla eroja. Laajempi asiantuntijoiden joukko antaisi tarkemman vastauksen opinnäytetyön kysymyksiin.

Opinnäytetyössä lähdettiin tutkimaan sitä, millaisia huijauksia pankkiasiakkaisiin kohdistuu ja miten niitä ennaltaehkäistään tällä hetkellä ja kuinka niitä voidaan ennaltaehkäistä tulevaisuudessa.

Pankkiasiakkaisiin kohdistuvien huijausten kuvaus on mielestäni onnistunut ja tutkimuksen rajauksen puitteissa suhteellisen kattava esimerkkeineen. Huijausten tulevaisuudesta ja kehityksestä on tehty tavoitteiden mukaisia arvioita. Huijausten historiaa olisi voinut käsitellä opinnäytetyön teoria-osuudessa tarkemmin, mutta aikataulun puitteissa ja opinnäytetyön päätavoite mielessä se jätettiin pienehköksi.

Huijauksen ennaltaehkäisymenetelmissä sen sijaan voisi olla täydennettävää. Asiantuntijat eivät voineet salassapitovelvollisuuden vuoksi kertoa tarkemmin pankeissa käytettävistä ennaltaehkäisymenetelmistä, kuten ohjelmistoista tai tekoälyn kaikista käyttötavoista. Opinnäytetyössä on mainintoja siitä, miten tekoäly avustaa esimerkiksi maksuliiketarkkailussa tai epäilyttävien toimintojen havaitsemisessa, mutta kovin laajasti aiheesta ei ole pystytty kertomaan.

Jatkokehityksen kannalta voitaisiin tutkia, miten sähköisten kanavien ulkopuolelle jääville vanhuksille saadaan viestittyä huijauksista parhaalla mahdollisella tavalla. Tällä hetkellä aktiivinen uutisointi on keskittynyt vahvasti pankkien verkkosivuille, sosiaaliseen mediaan sekä pankkien omiin sovelluksiin. Vanhimpien asiakkaiden digitaidot eivät välttämättä ole riittävät, jolloin he ovat alttiimpia joutumaan huijauksen uhreiksi. Huijarit osaavat myös hyväksikäyttää digitaidottomuutta huijauksissaan.

Tässä opinnäytetyössä keskityttiin henkilöasiakkaiden peruspalveluihin. Luonnollisena jatkumona tutkimus voitaisiin laajentaa käsittelemään esimerkiksi sijoitus- ja toimitusjohtajahuijauksia, jotka tästä tutkimuksesta on rajattu pois. Finanssialan julkaisussa (Kuva 1) sijoitushuijauksiin menetettyjen rahojen määrä vuosien 2022–2023 välillä on noussut huimat 155 %. Asiantuntija A:n mukaan sijoitushuijauksien tyypillisimmät uhrit ovat nuoria. Aihe on siis ajankohtainen ja olisi mielenkiintoista tutkia, miksi huijaukset ovat toimivia juuri nuoremmassa ikäpolvessa.

Iso-Britanniaan viimeistään vuonna 2024 tulevaan säännökseen pankkien korvausvastuusta huijaustapauksista olisi myös hyvä jatkotutkimuksen kohde. Miten pankit tulevat reagoimaan nouseviin kuluihin? Kuinka säännös tulee vaikuttamaan esimerkiksi tilisiirtojen nopeuteen? Mikäli samankaltaisia muutoksia tullaan tulevaisuudessa kaavailemaan myös Suomeen, tutkimuksen tulokset olisivat erittäin tarpeellisia.

Työ valmistui aikataulullaan, vaikka välivaiheiden aikataulut venyivät hiukan. Lähteitä oli helppo löytää aiheen ajankohtaisuuden vuoksi ja yhteistyö asiantuntijoiden kanssa onnistui hyvin ja toi inspiraatiota opinnäytetyön loppuun saattamiseen. Aiheen valinta perustui kirjoittajan omiin mielenkiintoihin sekä urasuunnitelmiin. Tutkimusmenetelmän valinnassa oli hiukan vaikeuksia, mutta lopulta päädyttiin tulevaisuudentutkimukseen ja ennakointiin. Valinta tuntui osuvalta tavoitteiden saavuttamisen kannalta. Opinnäytetyö on toteutettu mahdollisimman eettisin menetelmin. Tutkimus ja haastattelut on suunniteltu niin, ettei niissä tule esille pankkisalaisuuden alla olevaa tai yksilöivää tietoa.

Opinnäytetyön tekeminen opetti tekijälleen kvalitatiivisen tutkimuksen tekemisestä, lähteiden oikeaoppisesta käytöstä ja tutkimuksen aiheesta paljon. Pankin toimihenkilönä kaikki oppi pankkiasiakkaisiin kohdistuvista huijauksista on kullan arvoinen etu ja koenkin pystyväni kohtaamaan huijauksen uhreja taas aavistuksen paremmin avuin.

Lähteet

Aktia Pankki Oyj. Käyttötili. Luettavissa: https://www.aktia.fi/fi/kayttotili Luettu: 17.10.2023.

Alhonsuo, S., Nisén, A., Nousiainen, S., Pellikka, T. & Sundberg, S. 2012. Finanssitoiminnan käsikirja. 2. uud. p. Helsinki: Finva.

Asiantuntija A. 31.10.2023. Fraud-asiantuntija. Pankki X. Haastattelu. Helsinki.

Asiantuntija B. 6.11.2023. Fraud-asiantuntija. Pankki X. Haastattelu. Helsinki.

Asiantuntija C. 9.11.2023. Fraud-asiantuntija. Pankki Y. Haastattelu. Helsinki.

Danske Bank A/S. Tarkkana verkossa. Luettavissa: https://danskebank.fi/sinulle/asiakaspalvelu/tarkkana-verkossa/faktat/erilaisia-huijaustapoja#accordion-0-item-1 Luettu:20.10.2023.

Danske Bank A/S. Valesähköpostit. Luettavissa: https://danskebank.fi/sinulle/asiakaspalvelu/tarkkana-verkossa/asiakaspalvelu/huijaukset-sahkopostitse#accordion-0-item-1 Luettu: 20.10.2023.

Finanssiala 2023. Kalastelut ja muut huijaukset kasvoivat räjähdysmäisesti. Luettavissa: https://www.finanssiala.fi/uutiset/kalastelut-ja-muut-huijaukset-kasvoivat-rajahdysmaisesti-alkuvuonna-pankit-saivat-estettya-huijauksia-lahes-16-miljoonan-euron-edesta/ Luettu: 20.10.2023.

Finanssiala 2023. Maksamisen sääntely uudistuu taas. Luettavissa: https://www.finanssiala.fi/uutiset/maksamisen-saantely-uudistuu-taas-finanssiala-peraankuuluttaa-kohtuullisia-siirtymaaikoja-maltillisia-kustannuksia-ja-laadukasta-saantelya/ Luettu: 12.11.2023.

Finanssivalvonta. Peruspankkipalvelut. Luettavissa: https://www.finanssivalvonta.fi/kuluttajansuoja/pankkipalvelut/peruspankkipalvelut/ Luettu: 28.9.2023.

FINE. Ratkaisu 060698. Luettavissa: https://www.fine.fi/ota-yhteytta/ratkaisutietokanta/ratkaisu/fine-060698.html?q=huijaus&asiasanat=&n=&ratkaisun_antaja=&kategoria=&asiaryhma=&vakuutuslaji=&lakipykalat=&date_from=&date_to=&elem_id=1 Luettu: 17.10.2023

FINE. Vuosikertomus 2022. Luettavissa: https://www.fine.fi/oppaat/julkaisu/fine-vuosikertomus-2022.html Luettu: 3.11.2023

Hyvärinen, M., Aho, A. L., Nikander, P. & Ruusuvuori, J. 2017. Tutkimushaastattelun käsikirja. Tampere: Vastapaino. E-kirja. Luettu: 4.11.2023.

Iltalehti. Tilitietosi yritetään kaapata – älä usko ”Nordealta” tulevaa viestiä. Luettavissa: https://www.iltalehti.fi/tietoturva/a/f8b5bbac-eb23-4566-8df4-24e4366c66f8 Luettu 17.10.2023

King, B. 2019. Bank 4.0: Banking everywhere, never at a bank. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd.

Kontkanen, E. 2015. Pankkitoiminnan käsikirja. 4. uudistettu painos. [Helsinki]: Finva.

Kyberturvallisuuskeskus. Huijarit kaappaavat pankkitunnuksia Omakannan ja Suomi.fi-palvelun nimissä. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/huijarit-kaappaavat-pankkitunnuksia-omakannan-ja-suomifi-palvelun-nimissa Luettu: 17.10.2023.

Kyberturvallisuuskeskus. Tietoturvan vuosi 2018. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf Luettu: 11.11.2023.

Kyberturvallisuuskeskus. Tietoturvan vuosi 2021. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2021.pdf Luettu: 5.11.2023.

Kyberturvallisuuskeskus. Tietoturvan vuosi 2022. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TRAFICOM_Tietoturvan-vuosi-2022.pdf Luettu: 5.11.2023

Kyberturvallisuuskeskus. Traficomin määräys lopettaa suomalaisiksi naamioidut valepuhelut lähes kokonaan. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficomin-maarays-lopettaa-suomalaisiksi-naamioidut-valepuhelut-lahes-kokonaan Luettu: 29.10.2023.

Laki luottolaitostoiminnasta 8.8.2014/610. Luettavissa: https://www.finlex.fi/fi/laki/ajantasa/2014/20140610#O4L15P6 Luettu 28.9.2023.

Lyon, B. 2023. Exploring Deepfakes: Deploy Powerful AI Techniques for Face Replacement and More with This Comprehensive Guide. Birmingham: Packt Publishing, Limited. E-kirja. Luettu: 7.11.2023.

Nordea Bank Oyj. Debit-kortti. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/nordea-debit.html#tab=Ehdot Luettu: 17.10.2023.

Nordea Bank Oyj. Erilaisia huijausmuotoja. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/tuki/erilaisia-huijausmuotoja.html Luettu: 19.10.2023.

Nordea Bank Oyj. Luottokortit. Luettavissa: https://www.nordea.fi/henkiloasiakkaat/palvelumme/maksu-luottokortit/luottokortit.html#tab=Luotto-ominaisuus Luettu: 17.10.2023.

Nummenmaa, L., Holopainen, M., Pulkkinen, P. & Kimpimäki, K. 2019. Tilastollisten menetelmien perusteet. 1.-5. painos. Helsinki: Sanoma Pro Oy. E-kirja. Luettu: 12.11.2023.

OP-Ryhmä. Tunnukset. Luettavissa: https://www.op.fi/henkiloasiakkaat/digitaaliset-palvelut/tunnukset Luettu: 17.10.2023.

OP-Ryhmä. Turvallinen asiointi. Luettavissa: https://www.op.fi/turvallinen-asiointi/mista-tunnistaa-huijausviestin Luettu: 17.10.2023.

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

Poliisi. Kyberrikollisuus. Luettavissa: https://poliisi.fi/kyberrikokset Luettu: 12.11.2023.

Poliisi 2021. Poliisi varoittaa huijausyrityksistä. Luettavissa: https://poliisi.fi/-/poliisi-varoittaa-huijausyrityksista Luettu: 12.11.2023.

Poliisi 2022. Poliisi tehosta kyberrikostorjuntaa. Luettavissa: https://poliisi.fi/-/poliisi-tehostaa-kyberrikostorjuntaa-suomi-mukaan-europolin-yhteistyoryhmaan Luettu: 11.11.2023.

Poliisi 2023. Ajankohtainen katsaus kyberrikollisuuteen. Luettavissa: https://poliisi.fi/blogi/-/blogs/ajankohtainen-katsaus-kyberrikollisuuteen- Luettu: 8.11.2023.

Payment Systems Regulator. PSR confirms new requirements for APP fraud reimbursement. Luettavissa: https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/?fbclid=IwAR37doEP1GknCLWTfL37P9yynf9G0VQw5v5UrNw3UfUY7KJJADmR1fy-XcE Luettu: 31.10.2023.

Salo, M. & Westlie, K. 2023. Digiviidakon selviytymisopas. Helsinki, Suomi: Planeetta Kustannus.

Steinberg, J. 2022. Cybersecurity for Dummies. Newark: John Wiley & Sons, Incorporated. E-kirja. Luettu 12.11.2023.

Traficom. Määräyksen velvoitteet voimaan - jopa 200 000 huijauspuhelua estetään päivässä. Luettavissa: https://www.traficom.fi/fi/ajankohtaista/maarayksen-velvoitteet-voimaan-jopa-200-000-huijauspuhelua-estetaan-paivassa Luettu: 8.11.2023.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Kustannusosakeyhtiö Tammi. E-kirja. Luettu: 11.11.2023.

Turun yliopisto. Tulevaisuuden tutkimuskeskus, j., Aalto, H., Heikkilä, K., Keski-Pukkila, P., Mäki, M. & Pöllänen, M. 2022. Tulevaisuudentutkimus tutuksi: Perusteita ja menetelmiä. Turku: Tulevaisuuden tutkimuskeskus. E-kirja. Luettu: 3.11.2023.

Wilson, D. 2021. Cybersecurity. Cambridge, Massachusetts: The MIT Press.

Wuolijoki, S. 2023. Pankkioikeus: II. 3., uudistettu painos. Helsinki: Alma Talent. E-kirja. Luettu: 4.11.2023.

Liitteet

Liite 1. Haastattelukysymykset asiantuntijahaastatteluun

Haastattelukysymykset

1. Millaisia ovat yleisimmät pankin nimissä tehtävät huijaukset tällä hetkellä?
2. Kuinka pankin nimissä tehdyt huijaukset vaikuttavat pankin toimintaan?
3. Mitä trendejä pankin nimissä tehtyjen huijausten suhteen on viime vuosina ollut?
4. Millaisilla pankin nimissä tehdyillä huijauksilla on eniten uhreja?
5. Miten uskot pankin nimissä tehtävien huijausten kehittyvän seuraavien viiden vuoden aikana?
6. Kuinka pankki ennaltaehkäisee huijauksia tällä hetkellä?
7. Mitkä ennaltaehkäisevistä toimista ovat mielestäsi tärkeimpiä?
8. Minkä asioiden uskot korostuvan ennaltaehkäisyn kannalta tulevaisuudessa?
9. Pankin ja asiakkaan vastuut ennaltaehkäisyssä?