SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Joona Hautalaakso

# Digitalisaation riskit asiakkaalle pankkialalla

Miten asiakasta huijataan?

Opinnäytetyö
Syksy 2023
Tradenomi (AMK), Liiketalous

SEINÄJOEN AMMATTIKORKEAKOULU

## Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Tradenomi (AMK), Liiketalous

Tekijä: Joona Hautalaakso

Työn nimi alaotsikoineen: Digitalisaation riskit asiakkaalle pankkialalla: Miten asiakasta huijataan?

Ohjaaja: Margit Mannila

Vuosi: 2023 Sivumäärä: 36 Liitteiden lukumäärä: -

Opinnäytetyön tavoitteena oli selvittää, miten digitalisaatio ilmenee pankkialalla, millaisia riskejä digitalisaatio on tuonut asiakkaalle pankkialalla ja miten asiakasta huijataan. Digitalisaatio näkyy jokapäiväisessä elämässä, ja sen vaikutukset koskettavat meitä jokaista. Pankkialalla digitalisaation vaikutukset näkyvät erityisesti digitaalisten palveluiden lisääntymisenä.

Digitalisaatio on tuonut paljon mahdollisuuksia pankkialalle, mutta samanaikaisesti asiakkaan riskit ovat kasvaneet. Kyberrikollisuus on räjähtänyt käsiin viimeisten vuosien aikana, eikä sille ole löytynyt pysäyttäjää. Asiakkaat joutuvat nykypäivänä entistä useammin nettirikollisen uhriksi, ja uusia huijausyrityksiä ilmenee jatkuvasti lisää.

Opinnäytetyön teoriaosuudessa hyödynnettiin eri aineistoja laajasti, muun muassa alan ammattijulkaisuja sekä artikkeleita, uutisia, verkkosivuja ja tilastoja. Opinnäytetyön teoriaosuutta tutkittiin asiakkaan näkökulmasta. Lisäksi yhteenvedossa on lueteltu tärkeitä neuvoja pankin asiakkaille nettihuijausten ehkäisemiseksi.

[1] Asiasanat: digitalisaatio, pankkiala, riskit, kyberrikollisuus

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

## Thesis abstract

Degree programme: Bachelor of Business Administration

Author: Joona Hautalaakso

Title of thesis: Risks of digitalization for customers in the banking sector: How customers are scammed?

Supervisor: Margit Mannila

Year: 2023 Number of pages: 36 Number of appendices: -

The aim of this thesis was to find out how digitalization appears in the banking sector, what kind of risks digitalization has brought to the customer in the banking sector, and how customers are scammed. Digitalization is visible in day-to-day life, and its effects touch each of us. In the banking sector, the impacts of digitalization are particularly evident in the increase of digital services.

Digitalization has brought many opportunities to the banking sector, but at the same time, the risks for customers have increased. Cybercrime has exploded in recent years, and no solution has been found for it. Nowadays, customers are more often victims of cybercriminals, and new scam attempts are constantly emerging.

In the theoretical part of the thesis, a wide range of materials was utilized, including professional publications in the field, as well as articles, news, websites, and statistics. The theoretical part of the thesis was examined from the customer's point of view. In addition, the summary lists important advice for customers to prevent online scams.

[1] Keywords: digitalization, banking, risks, cybercrime

**SISÄLTÖ**

## Kuva-, kuvio- ja taulukkoluettelo

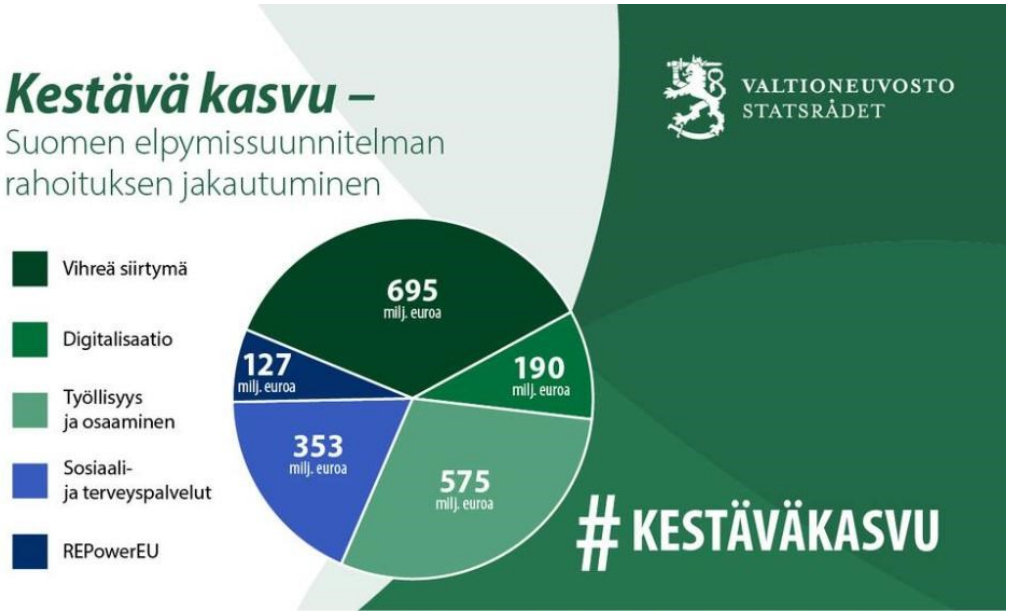
## Käytetyt termit ja lyhenteet

| | |
|---|---|
| **Digitalisaatio** | Digitaalitekniikan yleistyminen jokapäiväisen elämän toiminnoissa. |
| **Riski** | Epävarmuuden vaikutus tavoitteisiin. Vaikutus on myönteinen tai kielteinen odotettuun vaikutukseen verrattuna. |
| **Kyberrikollisuus** | Rikokset, jotka kohdistuvat tietotekniikkaan tai tietoverkkoihin. Tietotekniikkaa tai tietoverkkoja voidaan käyttää myös rikoksentekovälineinä. |

# 1 JOHDANTO

Digitalisaatio on ollut esillä jo useiden vuosien ajan ja sen varaan on asetettu suuria tavoitteita sekä odotuksia (Neittaanmäki ym., 2021, s. 11). Digitalisaatio näkyy jokapäiväisessä elämässämme, kuten työpaikoilla, kouluissa ja terveydenhuollossa. Suomalaisessa yhteiskunnassa on tapahtunut todella isoja rakenteellisia muutoksia, mikä on nostanut digitalisaation yhteiskunnallisen keskustelun puheenaiheeksi. Digitalisaatio käynnistyi Suomessa 1980-luvulla, jolloin digitaalinen teknologia yleistyi arkielämän toiminnoissa, mutta nykyään Suomi on yksi digitalisaation kärkimaista (mts. 15). Viime vuosina on alettu ymmärtämään enemmän digitalisaation yhteiskunnallista merkitystä ja miten pystymme varmistamaan digitaalisen kehityksen tulevaisuudessa. Digitalisaatio tuo myös mukanaan monia riskejä, jotka liittyvät erityisesti ihmisten yksityisyyteen ja tietosuojaan. Vaikka riskit sekä uhat liittyvät vahvasti digitalisaatioon, niistä on silti haastavaa löytää tietoa.

Suomen kestävän kasvun ohjelma on valtiovarainministeriön julkaisema ohjelma, jonka tavoitteena on tukea kestävää kasvua ekologisesti, sosiaalisesti ja taloudellisesti hallitusohjelman mukaisesti (Valtiovarainministeriö, i.a.-a). Ohjelma pyrkii myös kasvattamaan kilpailukykyä, investointeja, osaamistasoa ja innovaatioita. Suomen kestävän kasvun ohjelma perustuu neljään kokonaisuuteen, joista yksi kohta liittyy digitalisaatioon: digitalisaation ja datatalouden avulla tuottavuutta vahvistetaan ja palvelut tuodaan kaikkien saataville.




Kuva 1. Kestävä kasvu – Suomen elpymissuunnitelman rahoituksen jakautuminen (Valtiovarainministeriö, i.a.-b).

Kuvassa 1. selviää Suomen elpymissuunnitelman rahoituksen jakautuminen eri osa-alueisiin (Valtiovarainministeriö, i.a.-b). Elpymis- ja palautussuunnitelma kuuluu Suomen kestävän kasvun ohjelmaan. Valtiovarainministeriö linjaa Suomalaisen yhteiskunnan olevan murrosvaiheessa, sillä mittavat rakenteelliset muutokset ovat jo käynnissä (Valtiovarainministeriö, i.a.-c). Digitalisaatio on yksi tärkeimmistä palasista muutosten onnistumisen kannalta. Digitalisaation seurauksena toimintatavat joudutaan luomaan uudelleen, mutta se tulee lisäämään tehokkuutta sekä joustavuutta entistä enemmän. Käytännön tasolla digitalisaatio tuo kansalaiset ja yritykset julkisten palveluiden kehityksen keskiöön. Digitaalisuudesta puhuttaessa, puheenaiheeksi nousee usein tekoäly, jonka suosio on räjähtänyt viime aikoina. Tekoälyä pyritään hyödyntämään jatkuvasti yhä enemmän ja käyttökohteet kasvavat huimalla vauhdilla.

Perinteinen rikollisuus alkaa jäämään taka-alalle kyberrikollisuuden noustessa kansainväliseksi uhaksi. Digitalisaatio on edesauttanut kyberrikollisuuden lisääntymistä ympäri maailmaa eikä sen pysäyttämiseksi ole riittävästi resursseja saatavilla. Kyberturvallisuuskeskuksen tietoturva-asiantuntija Könösen mukaan (2023) rikosten teko verkossa on muuttunut entistä helpommaksi, sillä nykyään erilaisia verkkohuijauksia pystyy jopa ostamaan pimeästä verkosta omaan käyttöönsä. Se ei pakosta vaadi rikolliselta edes minkäänlaista osaamista koodaamisesta. Ennen stereotyyppinen hakkeri oli huppupäinen henkilö, joka ymmärsi tietokoneista kaiken, mutta nykyään rikoksen tekijä voi myös olla alaikäinen. Keskusrikospoliisin kyberrikostorjuntakeskuksen päällikkö Rauhamaa (2023) kertoo jopa alaikäisten ostaneen palvelunestohyökkäyksiä pimeästä verkosta. Verkkorikoksen uhriksi voi joutua kuka tahansa iästä tai asemasta riippumatta ja suomalaisiin kohdistuneita rikoksia tehdään myös ulkomailta.

### 1.1 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena on selvittää, millaisia riskejä digitalisaatio on tuonut asiakkaille pankkialalle ja miten asiakasta yritetään huijata. Digitalisaatio on aiheena hyvin ajankohtainen pankkialalla ja minulla on siitä myös henkilökohtaista tuntemusta sekä kokemusta. Olen pankissa työskennellessäni kohdannut, mitä haasteita digitalisaatio on tuonut pankkialalle. Digitalisaation tuomista muutoksista ovat kärsineet etenkin ikäihmiset. Lisäksi he voivat joutua muuta ikäluokkaa useammin verkkorikollisen uhriksi.

Opinnäytetyön tutkimuskysymykset ovat määritelty seuraavasti:

1. Miten digitalisaatio ilmenee pankkialalla?

2. Mitkä ovat digitalisaation riskit asiakkaalle pankkialalla?

3. Miten asiakasta huijataan?

Kyberrikollisuus on pankkialalla isoin riski asiakkaille. Kyberrikollisuus on kasvanut räjähdysmäisesti digitalisaation seurauksena, ja rikolliset käyttävät entistä ovelampia keinoja huijatakseen, esimerkiksi pankin asiakasta. Huijausten perimmäinen motiivi on yleensä raha, mutta se voi olla aivan muutakin. LähiTapiolan tietoturvajohtaja Niemelä (2023) kertoo, että melkein puolet suomalaisista ovat joutuneet nettihuijauksen kohteeksi. Tämä ilmenee LähiTapiolan julkaisemasta Arjen katsaus -kyselystä. Kyselyn mukaan 47 prosenttia suomalaisista on kohdannut huijausyrityksiä internetissä. Huijaukseen joutuminen saattaa aiheuttaa uhrille häpeän tunnetta, mutta on kuitenkin tärkeää muistaa, ettei sen asian kanssa tarvitse jäädä yksin. Ihmisten internetin ja digitaalisten palveluiden lisääntynyt käyttö on muuttanut rikollisuuden ilmentymistä. Rikollinen on aina siellä, missä ihmisetkin ovat.

### 1.2 Opinnäytetyön rakenne

Opinnäytetyö koostuu johdannosta, teoriasta ja yhteenvedosta. Johdannossa kerrotaan digitalisaatiosta yleisesti ja kyberrikollisuuden lisääntymisestä nykypäivänä. Myös opinnäytetyön tavoite ja tutkimuskysymykset käydään läpi johdannossa. Varsinainen teoriaosuus on jaettu kolmeen päälukuun, joita ovat digitalisaatio, digitalisaation riskit asiakkaalle ja miten asiakasta huijataan. Vielä lopuksi on yhteenveto, joka sisältää omaa pohdintaa työn lopputuloksista. Lisäksi yhteenvedossa on kerrottu mahdolliset jatkotutkimusaiheet.

# 2 DIGITALISAATIO

## 2.1 Digitalisaation määritelmä

Digitalisaatio on käsitteenä todella ajankohtainen eikä siltä ole voinut välttyä, mutta ilmiötä voi olla vaikea ymmärtää kokonaisuudessaan. Alasoini (2015, s. 26) kertoo digitalisaation tarkoittavan digitaalitekniikan integrointia jokapäiväisen elämän toimintojen osaksi hyödyntämällä digitoinnin mahdollisuuksia kokonaisvaltaisesti. Digitalisaatio luokitellaan yhteiskunnallisiin prosesseihin, jossa hyödynnetään teknologisen kehityksen tuomia uusia mahdollisuuksia yhteiskunnan jokaisella osa-alueella, muun muassa liiketoiminnassa. Pohjola huomauttaa (2014), että digitalisaatio on yksi tärkeimmistä tekijöistä teknologian kehityksen kannalta ja vertaa sitä James Wattin höyrykoneen merkitykseen teollisen vallankumouksen aikana.

Digitalisaatio koskettaa meitä jokaista ja se on nähtävillä niin arjessa kuin työpaikallakin (Digitaalinen Helsinki, i.a.). Digitalisaatio tuo arkeen helpotusta, vaikka sen vaikutusta ei aina huomaakaan. Esimerkiksi, oma lähibussivuoro voi näyttää ulospäin samalle, mutta sen kaiken taustalla on kuitenkin tapahtunut suuria muutoksia. Jokaisen bussin sijainti on jatkuvasti liikenteen suunnittelijoiden saatavilla. Lisäksi eri pysäkkien suosiosta saadaan reaaliaikaista tietoa ja matkustaja näkee pysäkin näytöstä, milloin oma bussi on lähettyvillä.

Digitalisaatiota voidaan pitää aikakautemme suurimpana muutosvoimana, sillä se on muuttanut ihmisten toimintatapoja sekä käyttäytymistä eri tilanteissa (Ilmarinen & Koskela, 2015, s. 13). Digitalisaatio on vaikuttanut erityisesti informaation hankkimiseen, tuotteiden ostamiseen, palveluiden kuluttamiseen ja vuorovaikutustilanteisiin. Digitalisaatio on muovannut yritysten kilpailuympäristöä ja poistanut perinteisiä toimialarajoja, mikä on pakottanut yrityksiä uudistamaan toimintatapojaan sekä osaamistaan. Tämä vaikuttaa myös siihen, miten yritykset ovat vuorovaikutuksessa asiakkaiden kanssa.

Neittaanmäki ym. (2021, s. 11) kertovat, että digitalisaatio voidaan kokea muutoksena, jossa perinteiset toimintatavat muokkautuvat täysin uuteen muotoon, mikä johtaa uusien palveluiden sekä liiketoimintamallien syntyyn. Digitalisaatio pohjimmiltaan asiakaslähtöistä

toiminnan muutosta, jonka kehittynyt teknologia on mahdollistanut. Digitalisaatio ei kuitenkaan näyttäydy kaikkialla maailmalla samalla tavalla, sillä monella ei ole käytössään toimivaa internetyhteyttä. Monella on yleinen harhaluulo digitalisaation tarkoittavan ainoastaan tietokoneiden käytön lisääntymistä. Digitalisaation vaikutukset ovat todella laajat ja ne koskettavat koko yhteiskuntaa. Digitalisaation yhteiskunnallisia vaikutuksia ovat muun muassa:

1. Digitaaliset palvelut
2. Digitaalinen koulutus
3. Digitaalinen terveydenhoito
4. Digitaalinen liikenne
5. Digitaaliset teollisuus- ja palvelurobotit

Tämän opinnäytetyön keskiössä ovat erityisesti digitaaliset palvelut. Organisaatiotasolla vanhat käytännöt korvataan uusilla ja palveluita tarjotaan asiakkaille uudella sekä modernilla tavalla, esimerkiksi pankkien digitaaliset palvelut ovat korvanneet perinteisen konttorissa asioimisen (Neittaanmäki ym., 2021, s.13). Digitaalisia sovelluksia ja työkaluja hyödynnetään yhä enemmän, mikä poistaa manuaalisia työvaiheita. Aikoinaan teollistuminen muutti maailmaa, mutta nykyään se johtuu digitalisaatiosta ja tekoälyn lisääntymisestä.

### 2.2 Digitalisaatio pankkialalla

Digitalisaatio on muokannut useita eri toimialoja, mutta varsinkin pankkialaa. Alasoini (2021, s. 298) mainitsee digitalisaation olevan olennainen osa pankkien strategiaa, jonka avulla pankit pyrkivät vaikuttamaan muuttuvaan toimintaympäristöön. Digitalisaatio ilmenee pankkialalla erityisesti perinteisten liiketoimintamallien muuttumisena, mikä on tuonut pankkien harjoittamaan liiketoimintaan paljon uusia mahdollisuuksia (Finanssialalle, i.a.-a). Tämä ei kuitenkaan tapahdu hetkessä, sillä se vaatii yrityksiltä ja organisaatioilta runsaasti uutta osaamista, jotta he pärjäävät markkinoilla muita kilpailijoita vastaan. Markkinoilla pärjääminen vaatii mukautumiskykyä ja ymmärrystä, miten asiakkaille sekä sidosryhmille saadaan tuotettua uutta arvoa. Teknologia kehittyy hurjaa vauhtia ja tulevaisuudessa menestyvät erityisesti sellaiset yritykset sekä organisaatiot, jotka osaavat liittää toisiinsa liiketoimintaan vaikuttavat tekijät, joita ovat:

- Asiakkaat
- Digitaaliset alustat
- Työntekijät
- Tehokkaat toimintatavat

Lisäksi se vaatii asiakkaiden tarpeisiin vastaamista globaalissa liiketoiminnassa, sillä digitalisaatio on mahdollistanut kansainväliset liiketoiminta-alustat.

Pulkkisen (2021) mukaan pankkipalveluiden tekoäly tulee helpottamaan asiointia tulevaisuudessa. Pankkien tietoteknologia kehittyy koko ajan ja tekoälystä on tullut tärkeä työkalu yrityksille. Tekoälystä on myös apua pankin asiakkaille, sillä sen avulla asiakas voi saada neuvoja, esimerkiksi säästämiseen ja sijoittamiseen. Koronapandemia edisti pankkien digitalisaatiota, joka tuli ilmi muun muassa pankin mobiilisovelluksen käytön merkittävä kasvuna. OP-yritysmobiilin kirjautumiset kasvoivat puolella, kun taas yksityisasiakkaiden OP-mobiilin kirjautumiset kasvoivat kolmanneksella verrattuna edelliseen vuoteen. Myös yli puolet neuvotteluista hoidettiin etänä. Digitaaliset palvelut helpottavat taloudenhallintaa ja OP tarjoaa asiakkailleen yhä enemmän sähköisiä palveluja, joita ovat esimerkiksi OP Yritystalous ja OP sijoituskumppani. Digitaalisten palveluiden lisäksi chatbotit kehittyvät jatkuvasti, jotta ne pystyvät ratkaisemaan entistä monimutkaisempia kysymyksiä. Tulevaisuudessa pankkipalvelut ovat yhä enemmän personoitu yksityis- ja yritysasiakkaille. Lisäksi palveluiden käytöstä tulee helppokäyttöisempää, sillä tekoälysovellukset pystyvät tarjoamaan asiakkaan tarpeisiin ajankohtaisia palveluja. Tekoälyn kehittyessä puheella ohjattavat palvelut ovat mahdollisia finanssialalla. Verkostoitumisen tärkeyttä ei saa unohtaa, sillä se on tulevaisuudessa avainasemassa tekoälysovellusten lisääntyessä.

Finanssipalvelut tavoittavat nykyään laajemman asiakaskunnan digitalisaation myötä, sillä ennen palvelut olivat vain tietyn asiakaskunnan saatavilla, esimerkiksi sijoitusneuvonta (Finanssialalle, i.a.-b). Nykyiselle kuluttajasukupolvelle digitaalisten palveluiden käyttö on varsin luonnollista, mutta se voi tuottaa hankaluuksia vanhemmalle väestölle. He saattavat tarvita palveluiden omaksumiseen ulkopuolista apua. Finanssiala on ollut aikoinaan varsin suljettu liiketoimintaympäristö, mutta markkinarakenteet sekä liiketoimintamallit ovat muuttuneet digitalisaation seurauksena. Digitalisaatio on mahdollistanut eri toimijoiden pääsyn markkinoille, joten kilpailu on koventunut finanssialalla. Kansainvälisistä

teknologiayrityksistä erityisesti Apple on lähtenyt mukaan finanssialan kehitykseen. Apple tunnetaan finanssialalla erityisesti Apple Pay -lähimaksupalvelustaan, joka on hyvin suosittu myös Suomessa. Apple on tehnyt yhteistyötä usean eri toimijan kanssa ja Apple Pay:n käyttö on maailmanlaajuista.

Arkilahden (2019) mukaan pankkialan muutosta tulisi katsoa mahdollisuutena eikä haasteena tai uhkana. Pankin on tärkeää tiedostaa digitalisaation vaikutukset asiakkaan kannalta, sillä digitalisoituvassa ympäristössä yhteys asiakkaaseen on entistä ratkaisevampi. Asiakas voi jopa luulla, että pankki etääntyy asiakkaistaan. Asiakkaiden suhtautuminen digitaalisiin palveluihin voi olla varsin erilainen, joten pankin pitää kohdata asiakas yksilönä ja tunnistaa heidän tarpeensa. Kuitenkin pankin perimmäinen tehtävä on tarjota asiakkailleen turvallista, helppoa ja saatavilla olevaa palvelua kanavasta riippumatta. Toimiva asiakassuhde perustuu ennen kaikkea luottamukseen ja myönteiseen asiakaskokemukseen koko asiakassuhteen aikana.

Suomi sekä muut pohjoismaat ovat Euroopan kärkeä digitalisaation kehityksessä ja digitaalisten taitojen taso on korkea (Grym ym., 2018, s. 3). Tämä on helpottanut digitaalisten rahoituspalveluiden integroimisen osaksi muita palveluja. Ihmiset liikkuvat paikasta toiseen, joten on helppoa, että pankkipalvelut ovat mukana verkossa ja mobiilissa. Pankkien on olennaista tehdä digi-investointeja ja kehittää palveluitaan, jotta he eivät jää kehityksestä jälkeen. On tärkeää, että asiakkailla on digitaalista talousosaamista (Rajas, 2020, s. 3). Digitaaliseen talousosaamiseen kuuluvat muun muassa digitaalisen ympäristön toimintalogiikan osaaminen ja turvallisuusasioiden, kuten tietoturvan sekä kyberturvallisuuden huomioiminen.

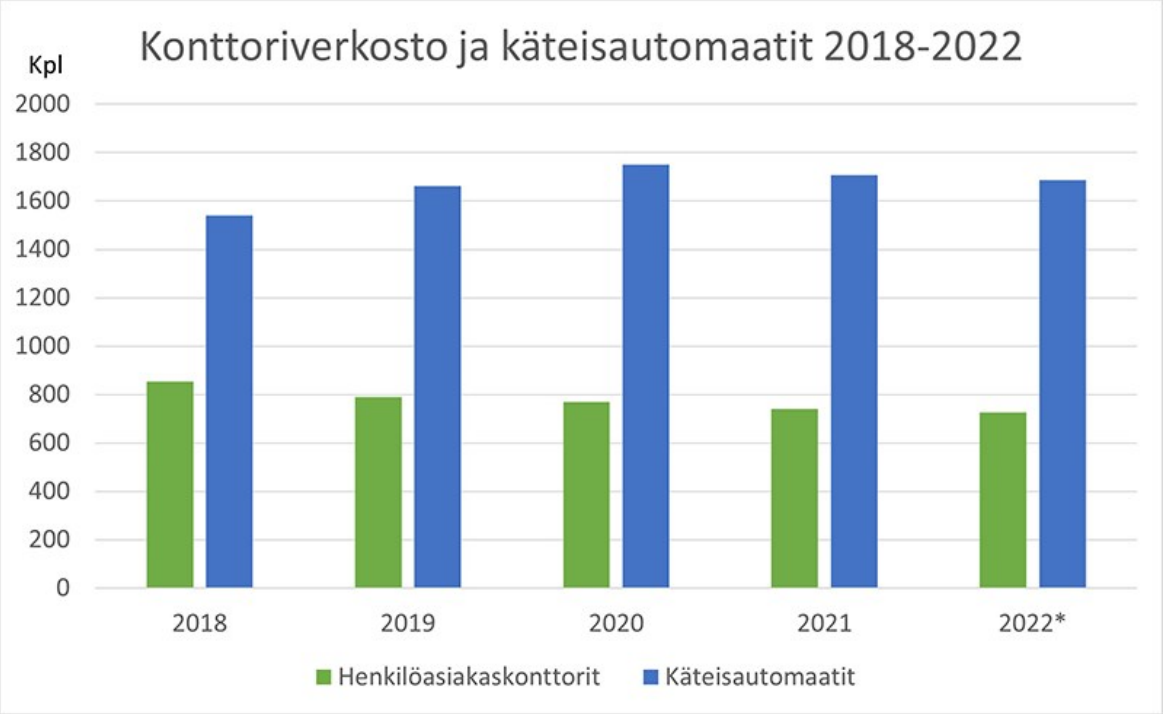
Digitalisaatio on tuonut useita muutoksia maksamiseen (Takala, 2022, s. 5). Ensin korttimaksut syrjäyttivät käteismaksun, mutta nykyään korttimaksut ovat siirtymässä älylaitteisiin. Maksutapojen muutoksiin ovat vaikuttaneet monet tekijät, kuten koronapandemia, etätyön kasvu ja kulutustottumusten muuttuminen. Yhä useampi tilaa esimerkiksi ruokaa ja vaatteita verkkokaupasta, mikä edellyttää sähköistä maksamista. Voi kuitenkin olla, että tulevaisuudessa ei enää tarvitse fyysistä maksuvälinettä, vaan maksaminen tapahtuu esimerkiksi kasvojentunnistuksella.

## 2.3 Pankkipalveluiden saatavuus

Pankkipalvelut ovat muuttuneet viime vuosien saatossa entistä enemmän digitaaliseen muotoon, mikä on vaikuttanut vääjäämättä pankkipalveluiden saatavuuteen (Finanssivalvonta, 2022). Digitalisaation seurauksena pankit ovat panostaneet digitaalisten palveluiden kehittämiseen. Tämä on johtanut yhä useamman pankkikonttorin sulkemiseen. Myös koronapandemialla on ollut oma osuutensa konttoripalveluiden saatavuuden suhteen ja muutos on tullut jäädäkseen. Koronapandemian aikaan digitaalisten palveluiden käyttö kasvoi merkittävästi. Kuitenkin ongelmaksi on noussut etenkin ikäihmisten päivittäisten raha-asioiden hoitaminen, sillä he ovat tottuneet hoitamaan pankkiasioitaan konttorissa paikan päällä. Päivittäisiä raha-asioita ovat muun muassa käteisen nostaminen, laskujen maksaminen sekä tilisiirrot. Lisäksi pankkeihin on usein pitkät jonotusajat ja palveluhinnasto on noussut suhteellisen korkealle.

Peruspankkipalveluihin kuuluvat muun muassa mahdollisuus käteisen rahan nostamiseen, verkkopankkitunnukset, perusmaksutili ja siihen liittyvä tilinkäyttöväline (Finanssivalvonta, 2018). Finanssivalvonta arvio vuosittain peruspankkipalveluiden saatavuutta ja hinnoittelua henkilöasiakkaille. Vuosittaisen selvityksen tavoite on arvioida sekä varmistaa kuluttaja-asiakkaiden oikeuden toteutuminen peruspankkipalveluiden suhteen. Peruspankkipalveluiden oikeuden toteutumisen perusteet ovat määritelty luottolaitoslaissa (Laki luottolaitostoiminnasta 610/2014, 15 luku, 6 §).

Vuoden 2012 selvityksen mukaan pankkikonttoreita oli jopa 1411, mutta monessa konttorissa oli supistettu käteispalveluja rajaamalla palvelu, jotta käteistä pystyi nostamaan vain tiettynä kellonaikana (Finanssivalvonta, 2023). Tämän takia pankkipalveluiden saatavuus oli paikallisesti heikentynyt etenkin sellaisten asiakkaiden kohdalla, joilla ei ollut käytössä verkkopankkia tai maksukorttia. Näin tapahtui erityisesti iäkkäämpien asiakkaiden kohdalla. Lisäksi muutamat pankit velvoittivat laskun maksamisesta konttorissa enimmillään 7–12 euroa, mikä vaaransi asiakkaan oikeuden saada peruspankkipalveluita kohtuulliseen hintaan. Seuraavasta kuviosta ilmenee pankkikonttorien ja käteisautomaattien määrän lasku, mikä vaikuttaa myös asiakkaan peruspankkipalveluiden saatavuuteen.



Kuvio 1. Konttoriverkosto ja käteisautomaatit 2018–2022 (Finanssivalvonta, 2023).

Kuten kuviosta 1 huomaa, henkilöasiakaskonttoreiden määrä on laskenut tasaisesti vuodesta 2018 lähtien (Finanssivalvonta, 2023). Käteisautomaattien määrä on kääntynyt lievään laskuun vuodesta 2021 lähtien. Suomessa oli vuoden 2022 lopulla yhteensä 1687 käteisautomaattia.

Vuoden 2022 selvityksessä ilmeni, että pankkipalveluja oli saatavilla hyvin ja palveluja tarjottiin pääosin kohtuuhintaisesti (Finanssivalvonta, 2023). Digitaaliset palvelukanavat ja muut etäkanavissa tarjottavat palvelut olivat palvelutarjonnan suurin lähde. Pankkikonttoreiden lukumäärä oli vuoden 2022 lopussa 726, jotka palvelivat henkilöasiakkaita. Pankkikonttoreiden määrä on puolittunut 10 vuoden takaisesta Finanssivalvonnan selvityksestä. Konttoreiden lukumäärän vähentyminen johtuu erityisesti digitaalisten palvelukanavien suosien myötä ja kysynnän vähentymisellä tietyillä maantieteellisillä alueilla. Digitaalisten pankkipalveluiden kanssa kamppaileville, pankit antoivat suurimmaksi osaksi maksutonta sekä monimuotoista digitukea. Tämä mahdollistaa sen, että monet käyttäjäryhmät, kuten iäkkäät ja muuta erityistukea tarvitsevat asiakkaat, pystyisivät käyttämään digitaalisia palveluja helpommin.

## 2.4 Suomen kestävän kasvun ohjelma

Suomen kestävän kasvun ohjelmassa painotetaan digitalisaation merkitystä tulevaisuudessa (Valtiovarainministeriö, i.a.-d). Kestävän kasvun ohjelman mukaan digitalisaation ja datatalouden asema vahvistuu sekä julkisissa että yksityisissä palveluissa, mikä johtaa kustannustehokkuuden ja tuottavuuden paranemiseen. Digitalisaatio mahdollistaa kilpailukykyisen toimintaympäristön yrityksille ja samalla palvelut tuodaan kaikkien saataville turvallisuutta painottaen.

Digitalisaation osalta, kestävän kasvun ohjelman tavoitteena on nostaa Suomi maailman kärkeen datavetoisten palveluiden sekä niiden turvallisten ratkaisujen kehittäjänä (Valtiovarainministeriö, i.a.-d). Yhteiskunnan digitaalisen siirtymän tukena käytetään digi-, teknologia- ja datainvestointeja. Kestävän kehityksen ohjelmassa on listattu merkittäviä digitalisaation hankkeita, jotka vahvistavat Suomen asemaa maailman johtavana digitaalisena yhteiskuntana. Hankkeita ovat muun muassa:

- Kyber- ja tietoturvallisuuden tutkimuksen investoinnit
- Kärkiteknologian investoinnit (tekoäly, 6G-verkot, mikroelektroniikka ja kvanttilaskenta)
- Reaaliaikatalous, jossa liiketoiminnan prosessit siirtyvät digitaalisiksi sekä reaaliaikaiseksi (esimerkiksi laskut ja kuitit)
- Huippunopeat nettiyhteydet koko maahan

Hankkeiden tavoitteena on helpottaa digitaalista siirtymää koko yhteiskunnassa, joten jokaisen hankkeen hyöty on valtavan suuri (Valtiovarainministeriö, i.a.-d). Digitalisaatio on mahdollistanut teknologiakehityksen, joka etenee hurjalla vauhdilla, mutta on todella tärkeää varmistaa kansalaisten kyber- ja tietoturvallisuus. Uudet digitaaliset palvelut lisääntyvät, joten on varmistettava, että kansalaiset osaavat käyttää niitä oikeaoppisesti ja turvallisesti.

Kärkiteknologian kehittämisen ansiosta yritykset saavat käyttöönsä entistä kehittyneempää teknologiaa, jota pystyy hyödyntämään täysin uudella tavalla (Valtiovarainministeriö, i.a.-d). Etenkin tekoälyllä on suuri merkitys tulevaisuuden työelämässä. Suomeen on tarkoitus luoda osaamista uuden teknologian käytölle, mikä avaisi täysin uusia mahdollisuuksia

opiskeluun sekä työelämään. Osaamisen ollessa korkeatasoista Suomi pärjäisi globaalissa kilpailussa.

# 3 DIGITALISAATION RISKIT ASIAKKAALLE

Digitalisaatio on muuttanut pankkialaa merkittävästi, sillä se on tuonut mukanaan monia mahdollisuuksia ja uusia toimintatapoja pankkialalle. Siitä huolimatta digitalisaatio on asettanut pankkialalle paljon uusia riskejä, joihin pankkien täytyy varautua. Pankkien on tärkeää tunnistaa sekä hallita näitä riskejä perusteellisesti.

Asiakkaiden turvallisuusriskien lisäksi pankkien tulee valmistautua asiakkaiden ja sijoittajien uskoon vaikuttaviin tekijöihin (Finanssialalle, i.a.-c). Sen sijaan pankkien verkkosivuilla on todella niukasti tietoa riskeistä, joita asiakas voi kohdata. Asiakkaan riskit liittyvät pääosin kyberrikollisuuden eri muotoihin.

## 3.1 Kyberrikollisuus

Kyberrikollisuus eli tietotekniikkarikollisuus tarkoittaa rikoksia, jotka kohdistuvat tietotekniikkaan tai tietoverkkoihin (Sisäministeriö, i.a.-a). Tietotekniikkaa sekä tietoverkkoja käytetään myös rikoksentekovälineinä. Kyberrikollisuus on nopeimmin kasvava rikollisuuden ala maailmalla. Nykymaailmassa tietoverkot ovat toimintaympäristönä sekä rikollisuudelle että rikostorjunnalle. Lisäksi nykypäivän rikoksista tehdään yhä enemmän tietoverkoissa tai tietojärjestelmissä. Kansainvälisyys on usein kyberrikoksien keskeinen tekijä, koska verkossa tapahtuvat rikokset ylittävät tyypillisesti kansalliset rajat. Verkossa tapahtuvat rikokset eroavat perinteisistä rikoksista, sillä verkossa ei ole fyysisiä rajoitteita. Vaikka kyberrikollisuutta tapahtuu jatkuvasti, suurin osa rikoksista ei tule poliisin tietoon tai rikokset jäävät monesti selvittämättä, vaikka esitutkinta olisi aloitettu. Tämä johtuu siitä, että kyberhyökkäyksen tekijän tunnistaminen on usein todella haastavaa. Hyökkääjä peittää usein jälkensä hyvin taitavasti, mutta myös ammattirikolliset tekevät joskus virheitä (Sisäministeriö, i.a.-b). Hyökkääjä voi käyttää eri keinoja johtolankojen peittämiseksi:

- Hyökkäyksen reitittäminen useiden kaupallisten palvelimien kautta
- Tunkeutumistyökalujen anonymisointi
- Tahallinen harhauttaminen
- Välikäsien käyttäminen (kyberrikollisryhmät)

Pankkialalla kyberriskit ovat merkittäviä, sillä ne voivat vaikuttaa laajasti niin pankkien toimintaan kuin asiakkaidenkin luottamukseen (Finanssialalle, i.a.-c). Kyberrikollisuus on lisääntynyt pelottavan nopeasti teknologian kehittyessä, joten rikolliset löytävät entistä edistyneempiä tapoja päästä käsiksi asiakkaiden tärkeisiin tietoihin. Tämän takia finanssialan yritykset ovat siirtyneet passiivisesta kyberpuolustuksesta aktiiviseen puolustukseen globaalilla tasolla. Muun muassa useat finanssialan yritykset palkkaavat kyberpuolustuksen asiantuntijoita, jotka pyrkivät estämään kyberrikollisuutta.

Ennen pankkitilien hakkerointia pidettiin suurimpana uhkana, mutta nykyään kyberuhkia on lukuisia ja toimintatavaltaan erilaisia (Kyberturvallisuuskeskus, 2020a, s. 4). Finanssialan yritykset joutuvat kamppailemaan kyberrikollisuuden kanssa kaiken aikaa ja heidän tavoitteenaan on turvata sekä oma että asiakkaidensa turvallisuus. Kyberuhat vaikuttavat organisaation toimintaan, talouteen ja sen hallussa olevaan tietoon. Pahimmassa tapauksessa kyberuhat ovat vaaraksi koko organisaation liiketoiminnalle ja sen jatkuvuudelle.

### 3.1.1 Tietojenkalastelu

Tietojenkalastelulla tarkoitetaan tilannetta, jossa huijarit yrittävät esimerkiksi sähköpostin tai tekstiviestin avulla saada käsiinsä ihmisten henkilötietoja, kuten verkkopankkitunnuksia ja käyttäjätunnuksia (Kilpailu- ja kuluttajavirasto, i.a.-a). Sähköpostit ja tekstiviestit ovat usein aidon kaltaisia. Lisäksi viesteissä on tyypillisesti linkki, joka pyydetään avaamaan vedoten esimerkiksi maksamattomiin kuljetusmaksuihin. Kuitenkin linkki koostuu monesti kirjaimista sekä numeroista, mikä voi paljastaa huijauksen.

Erilaisia huijaustapoja ovat muun muassa lahjakortti- ja arvontahuijaukset, väärennetyt seurantaviestit tai paketin saapumisilmoitukset ja asiakastutkimukset sekä kyselyt (Kilpailu- ja kuluttajavirasto, i.a.-a). Huijausviestejä lähetään yleensä isojen yritysten nimissä, mutta tietojenkalastelulta voi välttyä, kunhan ei avaa oudolta kuulostavia linkkejä eikä anna henkilötietoja kenellekään.

### 3.1.2 Haittaohjelmat

Haittaohjelmat ovat muun muassa viruksia ja vakoiluohjelmia, joita verkkorikolliset käyttävät sekä levittävät (F-Secure, i.a.-a). Haittaohjelmien tarkoituksena on esimerkiksi arkaluonteisen tiedon ja rahan varastaminen. Myös niiden avulla aiheutetaan vahinkoa uhrin laitteelle. Haittaohjelmien tunnistaminen on hyvin tärkeää, sillä ne vaarantavat uhrin kyberturvallisuutta. Haittaohjelman voi tunnistaa oudoista ponnahdusikkunoista, laitteen hitaudesta ja laitteen normaalista poikkeavasta toiminnasta. Kuitenkin vahinko on usein jo tapahtunut ennen kuin uhri huomaa sitä. Haittaohjelmilta suojautuessa on todella tärkeää käyttää virustorjuntaohjelmaa, pitää päivitykset ajan tasalla, välttää yllättävien ponnahdusikkunoiden avaamista, ei yhdistä avoimiin wifi-verkkoihin ja lataa sovelluksia vain virallisista sovelluskaupoista.

Haittaohjelmat luokitellaan toiminnan, leviämisen ja haittatyypin perusteella (F-Secure, i.a.-a). Tietokoneiden lisäksi haittaohjelmat voivat levitä myös mobiililaitteisiin. Suojautumisen kannalta on tärkeää tunnistaa eri haittaohjelmat ja niiden tunnusmerkit. Haittaohjelmat voidaan jakaa seuraavasti:

- Virus
- Troijalainen
- Vakoiluohjelma
- Kiristysohjelma
- Mainosohjelma
- Tietokonemato

Tietoturvayhtiö Check Point (2023) julkaisi heinäkuussa listan yleisimmistä haittaohjelmista maailmalla. Yleisimmäksi haittaohjelmaksi nousi Qbot-pankkitroijalainen, joka varastaa käyttäjien pankkitunnuksia ja tallentaa käyttäjien näppäinpainalluksia käyttäjätunnusten ja salasanojen viemiseksi. Viime aikoina haittaohjelmahyökkäyksiä on tehty maailmalla erityisesti koulutus- ja tutkimusalalla.

### 3.1.3 Palvelunestohyökkäykset

Palvelunestohyökkäykset ovat lisääntyneet viimeisten vuosien aikana Suomessa ja niitä tehdään vuositasolla yli 10 000 kappaletta (Kyberturvallisuuskeskus, 2022). Esimerkiksi Suomen Pankin ja Verohallinnon sivustoille kohdistui palvelunestohyökkäyksiä lokakuussa (Pietarinen, 2023). Venäläinen hakkeriryhmä ilmoittautui hyökkäysten tekijäksi. Palvelunestohyökkäyksellä tarkoitetaan tietoverkkohyökkäystä, jolla estetään verkkosivun tai -palvelun normaali toiminta (Kyberturvallisuuskeskus, 2022). Tietoverkkohyökkäys saadaan aikaan, kun sivustolle tai palveluun ohjataan suuria määriä liikennettä.

Palvelunestohyökkäyksen takana voi olla muun muassa kyberrikolliset, yksittäiset ihmiset tai valtiolliset toimijat (Kyberturvallisuuskeskus, 2022). Hyökkäyksen tavoitteena on usein ilkivalta tai julkisuuden tavoittelu. Kuitenkin hyökkäyksen kesto on usein lyhytaikainen. Palvelunestohyökkäys on palvelun tai sivuston käyttäjälle harmillinen, mutta konkreettista vahinkoa onnistutaan aiheuttamaan todella harvoin.

### 3.1.4 Identiteettivarkaudet

Identiteettivarkaudet ovat nousseet esiin digitalisoitumisen myötä (OP, i.a.-a). Identiteettivarkaudella tarkoitetaan tilannetta, jossa asiaton henkilö käyttää toisen henkilön henkilötietoja tai pankkitietoja ilmaan lupaa. Tietomurtojen ja tietojenkalastelun avulla rikolliset voivat saada käsiinsä heille kuulumatottomia toisten ihmisten henkilötietoja. Asiaton henkilö voi muun muassa esiintyä uhrin henkilöllisyydellä tai tehdä verkkokauppatilauksia uhrin laskuun.

Mikäli epäilee joutuneensa identiteettivarkauden kohteeksi, on tärkeää tehdä rikosilmoitus poliisille (Kyberturvallisuuskeskus, 2020b). Mikäli rikollisella on pankkitietojasi käytössä, tulee ottaa yhteyttä omaan pankkiin. Muita mahdollisia keinoja suojata tietojasi on tehdä rekisteröintikielto, osoitteenmuutoskielto ja osoitetietojen suojaaminen.

Identiteettivarkauden kohteeksi voi joutua lähes kuka tahansa (Rikosuhripäivystys, i.a.-a). Kuitenkin kohteeksi joutumista voi välttää muutamalla tapaa. Henkilötunnusta ja muita henkilötietoja ei saa antaa ulkopuolisille. Silppua henkilötietoja sisältävät paperit, äläkä

laita niitä lehtikeräykseen tai muualle, jossa ne voivat joutua vääriin käsiin. Käytä maksu- ja nostorajoja tileilläsi sekä maksukorteillasi. Suosi e-laskuja paperisten laskujen sijaan.

### 3.2 Tekniset häiriöt

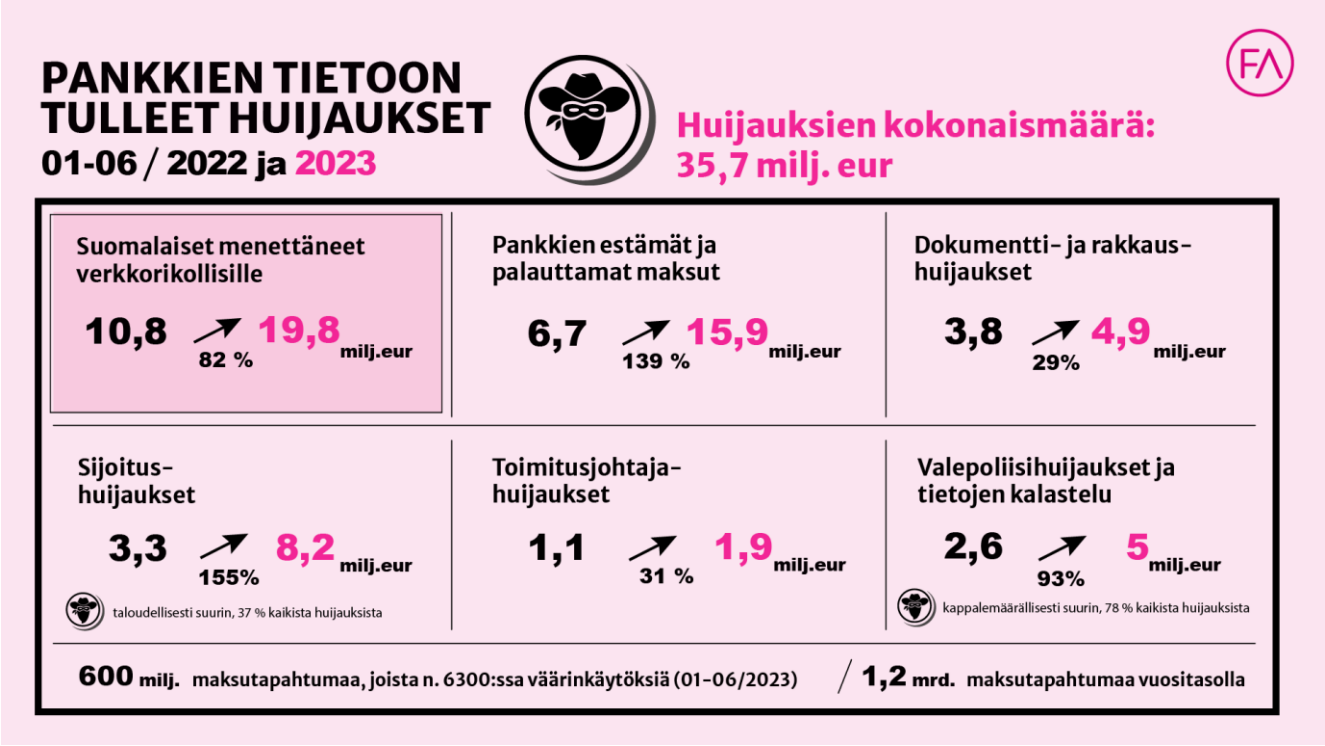
Erilaiset laitteiden sekä palveluiden tekniset häiriöt ovat jo arkipäivää nykymaailmassa. Siitä huolimatta ne voivat olla riski asiakkaalle, vaikka todellista vaaraa on harvoin. Jos häiriö ei korjaannu, kannattaa olla yhteydessä oman pankin asiakaspalveluun. Yleisiä teknisiä häiriöitä ovat maksukorttien toimimattomuus maksutilanteissa. Esimerkiksi Nordean palveluissa oli hiljattain häiriö, jossa monen asiakkaan tilin saldo näytti tyhjää jopa tuntien ajan (Pitkänen, 2023). Häiriö näkyi pääosin säästämisen tileillä mobiili- ja verkkopankissa. Jotkut asiakkaat luulivat, että heidät on ryöstetty. Myös OP:n maksuliikenteessä oli kesällä tekninen häiriö, joka vaikutti asiakkaiden palkkojen, eläkkeiden ja etuuksien saamiseen (Näveri, 2023). Muun muassa Kelan etuudet ja eläkkeensaajan eläkkeet eivät ilmestyneet asiakkaiden tileille. Häiriö vaikutti noin 115 000 tuhanteen Kelan asiakkaaseen.

Tekniset häiriöt eivät kuitenkaan johdu aina ulkopuolisten toiminnasta, vaan vika voi myös olla omissa laitteissa. Esimerkiksi pankin asiakas ei pääse kirjautumaan omaan mobiilipankkiinsa, koska hän ei ole päivittänyt sovelluksen uusinta versiota. Asiakas luulee ongelman johtuvan pankista, vaikka se johtuu omasta huolimattomuudestaan.

# 4 MITEN ASIAKASTA HUIJATAAN?

## 4.1 Yleisimmät huijaustavat ja niiden tunnistaminen

Digitalisaatio on nostanut kyberrikollisuuden aivan uudelle tasolle. Rikolliset löytävät koko ajan uusia tapoja ihmisten huijaamiseen. Nummi (2023) muistuttaa, että pankki ei koskaan lähetä asiakkaalleen linkkiä, johon pitäisi kirjautua verkkopankkitunnuksilla tai antaa muita henkilökohtaisia tietoja. Ei edes poliisi ole koskaan yhteydessä ja pyydä kertomaan käyttäjätunnuksia tai salasanoja. Vain rikolliset tekevät näin, mutta silti moni sortuu rikollisten huijauksiin.




Kuva 2. Pankkien tietoon tulleet huijaukset (Palmgren, 2023).

Huijausten määrä on kasvanut huolestuttavan paljon viimeisen vuoden aikana. Suomalaiset ovat menettäneet huijareille vuoden 2023 ensimmäisellä puoliskolla peräti 19,8 miljoonaa euroa, joka on melkein kaksinkertaistunut edeltävään vuoteen verrattuna (Palmgren, 2023). Toisaalta pankit ovat onnistuneet estämään huijauksia vuoden 2023 ensimmäisen puoliskon aikana 15,9 miljoonan euron edestä. Edellisenä vuonna määrä oli 6,7 miljoonaa euroa. Huijausten kokonaismäärä on peräti 35,7 miljoonaa euroa. Isoimmat menetykset

ovat syntyneet sijoitushuijauksista, joissa asiakkaat menettivät 8,2 miljoonaa euroa. Pitää kuitenkin muistaa, että kaikki huijaukset eivät tule pankkien tietoon.

### 4.1.1 Huijausviestit ja -soitot

Huijausviestit ja -soitot ovat yleinen tapa saada vastaanottajalta haluttuja tietoja, kuten pankkitunnuksia sekä muita henkilökohtaisia tietoja (Europol, 2022). Huijausviestejä voivat olla esimerkiksi arvonnassa voittaminen tai tilauksen saapuminen, vaikka ei olisi itse osallistunut mihinkään tai tilannut mitään. Viestit näyttävät usein samankaltaisilta kuin aidot viestit mikäli niitä vilkaisee vain pikaisesti. Lisäksi viesteissä vedotaan yleensä tilanteen kiireellisyyteen.

Huijaussoitoilla huijari yrittää urkkia uhriltaan tärkeitä tietoja, kuten pankkitietoja (Europol, 2022). Huijaussoitto voi tulla lähes mistä tahansa puhelinnumerosta, minkä takia väärennettyä puhelinnumeroa on vaikea tunnistaa. Vaikka huijarilla olisi uhrin tiedot hallussa, ei saa olettaa hänen olevan aito, koska huijari voi saada uhrin perustiedot selville internetistä.

### 4.1.2 Väärennetyt pankin nettisivut ja verkkokauppahuijaukset

Väärennetyillä pankin nettisivuilla tarkoitetaan nettisivuja, joiden tarkoitus on saada uhreilta verkkopankkitunnuksia tai muita henkilökohtaisia tietoja (OP, i.a.-b). Huijausten ehkäisemisessä on tärkeää välttää tekaistuja linkkejä, joiden avulla asiakas yritetään saada väärennetyille nettisivuille. Huijarit voivat upottaa hakutuloksiin kalastelusivuja, jotka ovat täysin aidon näköisiä ja tulevat hakutuloksiin ensimmäiseksi (Nordea, i.a.). Sivustot ovat lähes identtisiä alkuperäisten sivustojen kanssa, esimerkiksi nordea.fi ja kalastelusivusto nordeda.fi. Kun on kirjautumassa johonkin sivustolle, on tärkeää tarkistaa sivuston aitous tai kirjoittaa sivuston koko verkko-osoite selaimen osoitekenttään. Myös sivuston hakukentässä oleva lukkoikoni ja https:// -alkuinen verkko-osoite kertoo sivuston turvallisuudesta. Vaihtoehtoisesti usein käytetyt sivustot on mahdollista lisätä selaimessa kirjanmerkkeihin.

Yhä useampi tilaa nykypäivänä verkkokaupasta tuotteita. Kuitenkaan kaikki verkkokaupat eivät ole luotettavia, joten asiakkaan pitää olla aina todella tarkkana (Kilpailu- ja kuluttajavirasto, i.a.-b). Verkkokauppahuijauksesta on kyse silloin, kun asiakkaan tilaamia ja

maksamia tuotteita ei ikinä saavu perille tai tilatun tuotteen sijasta tulee väärä tuote. Verkkokauppahuijauksen hälyttäviä merkkejä ovat verkkokaupan puutteelliset tiedot, poikkeuksellisen halvat hinnat ja muiden asiakkaiden varoittavat kommentit. Mikäli jokin asia kuulostaa paremmalta, mitä se voisi olla, kyseessä on todennäköisesti huijaus. Verkkokauppahuijauksessa reklamaation tekeminen on tyypillisesti mahdotonta tai yritys on lopettanut toimintansa. Jos tilaama tuote ei ikinä saavu tai myyjä ei vastaa yhteydenottoihin, kannattaa olla yhteydessä omaan pankkiin.

### 4.1.3 Sijoitushuijaukset

Sijoitushuijauksilla tarkoitetaan olemattomia sijoituksia, jotka kertomansa mukaan olisivat korkeatuottoisia, vaikka eivät todellisuudessa tuota mitään (OP, i.a.-c). Jos joku sijoitus vaikuttaa liian hyvältä ollakseen totta, sitä se todennäköisesti on. Sijoitushuijaukset ovat olleet kasvussa viime aikoina Suomessa (Nordea, 2023). Sijoitushuijarit tekevät aidon näköisiä valeverkkosivuja, huijaussähköposteja sekä yhteydenottokampanjoita. Huijari esiintyy usein sijoituspalvelun tarjoajana tai rahoitusneuvojana. Huijareihin voi törmätä esimerkiksi sosiaalisessa mediassa.

Uhria voidaan huiputtaa monella eri tapaa (Nordea, 2023). Muun muassa uhria voidaan neuvoa lataamaan tietokoneelleen etähallintaohjelma, jonka avulla sijoituksissa pystytään neuvomaan. Todellisuudessa huijari saa pääsyn uhrin tietokoneelle ja voi saada käyttöönsä uhrin henkilökohtaisia tietoja, kuten pankkitunnuksia. Lisäksi uhria voidaan kehottaa avaamaan ulkomaille tilejä tai virtuaalisia lompakoita kryptovaluutta-alustoilla, joita huijari hallinnoivat. Tuottojen lunastamiseksi uhria pyydetään maksamaan erilaisia palkkioita, vaikka todellisuudessa hän ei tule saamaan rahojaan. Myös tämän jälkeen huijari voi esiintyä pankin edustajana ja esittää auttavansa uhria rahojen saamiseksi, vaikka huijarin tarkoitus on vain saada uhrilta lisää rahaa.

Sijoitushuijauksen voi kuitenkin tunnistaa eri merkeistä (OP, i.a.-c). Näitä merkkejä ovat esimerkiksi tarjous, joka on liian hyvä ollakseen totta tai kauppaavalla yrityksellä ei ole asianmukaista toimilupaa. Finanssivalvonnan sivuilla on lista yrityksistä, joita on syytä epäillä huijauksesta (Finanssivalvonta, i.a.). Uskottavuutta lisätäkseen sijoitusmainoksissa

käytetään julkisuuden henkilöitä, vaikka he eivät ole huijauksessa mukana millään tavalla. Kaikkein tärkeintä on kuitenkin, ettei luovuta pankkitunnuksia kenellekään.

### 4.1.4 Toimitusjohtaja- ja romanssihuijaukset

Toimitusjohtajahuijauksessa huijari lähestyy uhrejaan sähköpostitse tai soittamalla esittäen yrityksen korkea-arvoista henkilöä, kuten toimitusjohtajaa (Europol, 2022). Huijarin tarkoituksena on saada rahaa valelaskun tai muun siirron avulla yritykseltä. Huijari kertoo usein maksun kiireellisyydestä, tietää paljon yrityksestä, jonka johtajana esiintyy ja pyytää uhria toimimaan tavanomaista poikkeavilla valtuuskäytännöillä.

Romanssihuijauksessa huijari etsii uhreja usein seuranhakupalveluista ja muilta sosiaalisen median alustoilta (Rikosuhripäivystys, i.a.-b). Huijari voi myös ottaa yhteyttä sähköpostitse. Seuraa hakevan ihmisen voi olla vaikea tunnistaa onko kyseessä huijari vai tavallinen tutustuminen toiseen. Yleisiä romanssihuijauksen tunnusmerkkejä ovat huijarin työskentely arvostetussa ammatissa, sovittujen tapaamisten peruuntuminen erilaisten syiden vuoksi, videoyhteyden ottaminen ei onnistu, mutta yhteyden saa soittamalla. Lisäksi huijari voi pyytää rahaa, esimerkiksi sairaalakuluihin. Huijari pyrkii usein saamaan uhrin luottamuksen ensimmäiseksi, jossa voi mennä moniakin kuukausia. Vasta sen jälkeen hän pyytää muun muassa rahaa ja pankkitietoja. Uusiin ihmisiin tutustuessa onkin tärkeää olla valppaana ja kiinnittää huomiota epätavallisiin asioihin.

## 4.2 Miten parantaa omaa tietoturvaansa?

Huolellisuus ja maalaisjärjen käyttö on erityisen tärkeää internettiä käytettäessä (Rikosuhripäivystys, 2022). Tunnistautuminen mobiilivarmenteella, verkkopankkitunnuksilla tai sähköisellä henkilökortilla on turvallista, kunhan muistaa olla huolellinen. Jos on epävarma jostakin asiasta, muun muassa puhelusta, sähköpostista tai tekstiviestistä, asia kannattaa aina varmistaa esimerkiksi omasta pankista. Huijauksissa luodaan usein paineen ja kiireen tunne, mikä edesauttaa mahdolliseen huijaukseen sortumista (Nordea, i.a.). Ennen kuin klikkaa esimerkiksi sähköpostissa saapunutta linkkiä, kannattaa pysähtyä hetkeksi miettimään linkin luotettavuutta. Lisäksi on tärkeää pysyä kärryillä digitalisaation muutoksissa.

Digitukea saa muun muassa omasta pankista. Myös monet kirjastot ja kunnat tarjoavat digitukea sitä tarvitseville.

Virustorjuntaohjelmat, kuten F-Secure tarkistaa kaikki käyttämäsi sivustot ja pitää yhteytesi suojattuna, jotta kukaan ei pääse tietoihisi käsiksi (F-Secure, i.a.-b). Rikolliset pyrkivät saamaan tietokoneille haittaohjelmatartuntoja muun muassa väärennettyjen sovellusten sekä päivitysten avulla. Käyttöjärjestelmien ja ohjelmien päivittäminen on todella tärkeä asia kyberturvallisuuden kannalta (Kyberturvallisuuskeskus, 2020c). Päivitykset usein korjaavat järjestelmien haavoittavuuksia. Kuitenkin myös väärennettyjä päivityksiä voi esiintyä, jotka ilmestyvät esimerkiksi selaimen ponnahdusikkunaan. Väärennetyissä päivityksissä voidaan uskotella käyttäjälle, että selain pitää päivittää. Todellisuudessa kyseessä ei ole päivitys vaan haittaohjelma. Haittaohjelman avulla huijari voi esimerkiksi anastaa käyttäjän maksutiedot.

Salasanan on tarkoitus estää tilien luvaton käyttö (Kyberturvallisuuskeskus, 2023). Salasanan pituuden, erikoismerkkien ja suurien kirjainten vähimmäismäärä riippuu usein palvelusta. Salasanan tulisi kuitenkin olla pitkä ja yksilöllinen, jotta se ei olisi arvattavissa. On tärkeää käyttää eri salasanoja eri palveluissa, jolloin kirjautuminen muihin palveluihin on estettävissä, koska monet käyttävät juuri samaa salasanaa joka paikassa. Monivaiheisella tunnistautumisella pystytään estämään luvattoman henkilön pääsy tietoihisi, vaikka hänellä olisi hallussa salasanasi. Monivaiheisessa tunnistautumisessa henkilöllisyys tulee varmistaa käyttämällä kahta tai useampaa tunnistautumistapaa, esimerkiksi salasanalla ja sormenjäljellä.

# 5 YHTEENVETO

## 5.1 Loppupohdinta

Digitalisaatio on muuttanut maailmaa pysyvästi ja tulevaisuudessa digitalisaation vaikutukset ovat entistä suurempia. Tekoäly tulee olemaan yhä merkittävämpi osa digitalisaatiota, mahdollistaen älykkäämmät ja itseoppivat järjestelmät. Tämä kehitys voi tehostaa päätöksentekoa, automatisoida rutiinitehtäviä ja tarjota henkilökohtaisempia asiakaskokemuksia. Digitalisaation laajetessa kyberturvallisuuden tarve tulee kasvamaan entisestään.

Digitalisaation riskit ovat jo nyt todellinen uhka asiakkaille, mutta voidaan vain kuvitella, mitä ne ovat tulevaisuudessa. Asiakkaan riskit liittyvät erityisesti nopeasti kasvavan kyberrikollisuuden eri muotoihin. Kaiken tämän lisäksi asiakkaat kohtaavat entistä enemmän nettihuijareita, joiden huijaukset saavat jatkuvasti täysin uusia piirteitä. Mitä jos huijauksiin saadaan lisättyä todella kehittynyt tekoäly, joka osaa muun muassa matkia uhrin perheenjäsenen ääntä? Tekoäly on loistava keksintö, mutta rikollisten käsissä sillä saa vain tuhoa aikaan.

Tämän opinnäytetyön aihe on erittäin ajankohtainen ja tärkeä asiakkaan näkökulmasta. Digitalisaatio on ilmiönä todella laaja ja sen vaikutukset ulottuvat koko yhteiskuntaan. Digitalisaatio on tuonut haasteita etenkin vanhemmalle väestölle. Digitalisaation mahdollisuuksista puhutaan paljon, mutta riskien kartoittaminen on jäänyt taka-alalle. Digitalisaation riskeistä täytyy puhua enemmän. Se on yksi syy, miksi valitsin juuri tämän aiheen.

Pankin tärkein tehtävä on huolehtia asiakkaidensa turvallisuudesta ja varoittaa mahdollisista riskeistä. Myös asiakkaan tulee olla todella varovainen asioidessaan verkossa (OmaSp, i.a.-a). Vielä lopuksi on lueteltu tärkeitä neuvoja pankin asiakkaille turvalliseen verkkoasiointiin, jotka pienentävät riskiä joutua huijatuksi:

- Kirjaudu verkkopankkiin ainoastaan pankin kotisivujen kautta tai pankin mobiilisovelluksella
- Kun kirjaudut verkkopankkiin, kirjoita pankin koko osoite selaimen osoitekenttään

- Älä varsinkaan kirjaudu verkkopankkiin tekstiviestillä tai sähköpostilla saapuneen linkin kautta
- Käytä pankin mobiilisovellusten lataamiseen vain virallista sovelluskauppaa, älä lataa niitä muualta verkosta
- Älä missään nimessä luovuta pankkitunnuksiasi kenellekään muulle, ei edes lähiomaiselle
- Lue pankin lähettämät viestit ja varsinkin maksujen vahvistuspyynnöt erittäin tarkasti sekä huolellisesti ennen vahvistusta
- Suhtaudu varauksella pankista tuleviin viesteihin ja kiinnitä huomiota epäilyttäviin ja epätavallisiin viesteihin
- Älä avaa mitään linkkejä tai liitteitä hätiköiden
- Mikäli epäilet tulleesi huijatuksi, ota yhteys pankkiin välittömästi ja sulje tunnuksesi
- Jos havaitset huijauksia, varoita niistä lähipiiriäsi ensimmäisenä

### 5.2 Jatkotutkimusaiheet

Opinnäytetyössä tutkittiin nimenomaan asiakkaan riskejä pankkialalla, mutta vaihtoehtoisesti riskejä voisi tutkia pankin näkökulmasta. Digitalisaation riskit voivat vaikuttaa koko organisaation liiketoimintaan. Tämän hetken yksi puhutuimmista puheenaiheista on Psykoterapiakeskus Vastaamon tietomurto, jolla on valtavia vaikutuksia, erityisesti yrityksen maineeseen (Kerkelä, 2023). Tekijä sai käsiinsä peräti 33 000 tuhannen asiakkaan potilastiedot. Aluksi tekijä vaati rahaa Vastaamolta, jonka jälkeen siirtyi kiristämään yksittäisiä ihmisiä, joiden potilastietoja hänellä oli hallussaan. Kyberrikoksen tekijä on usein haastavaa yhdistää tekemiinsä rikoksiin, mikä ilmenee myös tässä tapauksessa.

Riskienhallinta on pankin kannalta hyvin tärkeää, sillä se on kriittinen osa pankin liiketoimintaa ja sisäistä valvontaa (OmaSp, i.a.-b). Riskienhallinnan tehtävänä on varmistaa, jotta keskeiset riskit tunnistetaan, arvioidaan ja mitataan. Lisäksi riskejä pitää seurata sekä hallita päivittäisen liiketoimintojen johtamisen ohella. Riskejä täytyy arvioida säännöllisesti yhdessä yhtiön hallituksen kanssa.

OmaSp:n sivuilla on määritelty tarkasti yhtiön eri riskit ja niiden hallinta (OmaSp, i.a.-b). Pankin riskejä ovat muun muassa:

- Luottoriski
- Markkinariski
- Korkoriski
- Likviditeetti- ja rahoitusriski
- Operatiivinen riski

# LÄHTEET


Alasoini, T. (2015). *Digitalisaatio muuttaa työtä – millaista työelämää uudistavaa innovaatiopolitiikkaa tarvitaan? Työpoliittinen aikakauskirja.* Työ- ja elinkeinoministeriö. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/74854/tak22015.pdf#page=26

Alasoini, T. (2021). Pankkien asiantuntijatyö digitalisaation ja EU-sääntelyn puristuksessa. *Työelämän tutkimus, 19*(3), 296–321. https://doi.org/10.37455/tt.100399

Arkilahti. (28.1.2019). Voiko pankki olla yhtä aikaa digitaalinen ja tavoitettavissa? *Finanssiala.* https://www.finanssiala.fi/kolumni/voiko-pankki-olla-yhta-aikaa-digitaalinen-ja-tavoitettavissa/

Check Point. (9.8.2023). *July 2023's most wanted malware: Remote Access Trojan (RAT) Remcos climbs to third place while Mobile Malware Anubis returns to top spot.* https://blog.checkpoint.com/security/july-2023s-most-wanted-malware-remote-access-trojan-rat-remcos-climbs-to-third-place-while-mobile-malware-anubis-returns-to-top-spot/

Digitaalinen Helsinki. (i.a.). *Mitä digitalisaatio tarkoittaa?* https://digi.hel.fi/esittely/mika-digi/

Europol. (12.5.2022). *Take control of your digital life. Don't be a victim of cyber scams!* https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%e2%80%99t-be-victim-of-cyber-scams

Finanssialalle. (i.a.-a). *Digitaaliset liiketoimintamallit.* https://www.finanssialalle.fi/opintomateriaalit/finanssialan-perusteet/innovaatiot/digitaaliset-liiketoimintamallit.html

Finanssialalle. (i.a.-b). *Digitalisaatiosta finanssialalla.* https://www.finanssialalle.fi/opintomateriaalit/finanssialan-perusteet/innovaatiot/digitalisaatiosta-finanssialalla.html

Finanssialalle. (i.a.-c). *Kyberriskit finanssialalla.* https://www.finanssialalle.fi/opintomateriaalit/tulevaisuuden-finanssiala/tulevaisuuden-pankki/kyberriskit-finanssialalla.html

Finanssivalvonta. (i.a.). *Luvattomia palveluntarjoajia koskevat varoitukset.* Haettu 30.11.2023, https://www.finanssivalvonta.fi/rekisterit/varoituslistat/luvattomia-palvelun-tarjoajia-koskevat-varoitukset/

Finanssivalvonta. (5.9.2018). *Peruspankkipalvelut.* https://www.finanssivalvonta.fi/kuluttajansuoja/pankkipalvelut/peruspankkipalvelut/

Finanssivalvonta. (1.4.2022). *Pankkien tärkeää huolehtia ei-digitaalisten palveluiden saatavuudesta ja palveluiden kohtuullisesta hinnoittelusta.*

https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2022/pankkien-tarkeaa-huolehtia-ei-digitaalisten-palveluiden-saatavuudesta-ja-palveluiden-kohtuullisesta-hinnoittelusta/

Finanssivalvonta. (6.7.2023). *Fivan selvitykset peruspankkipalveluista.* https://www.finanssivalvonta.fi/kuluttajansuoja/pankkipalvelut/peruspankkipalvelut/fivan-selvitykset-peruspankkipalveluista/

F-Secure. (i.a.-a). *Mikä on haittaohjelma?* https://www.f-secure.com/fi/articles/what-is-malware

F-Secure. (i.a.-b). *F-Secure Internet Security.* https://www.f-secure.com/fi/internet-security

Grym, A., Koskinen, K. & Manninen, O. (2018). Pohjoismaiset pankit muuttuvat digiaikaisiksi. *Euro & talous, 26*(2). https://urn.fi/URN:NBN:fi:bof-201805171549

Ilmarinen, V., & Koskela, K. (2015). *Digitalisaatio: Yritysjohdon käsikirja.* Talentum.

Kerkelä, L. (3.11.2023). ”Jotain osaan tietokoneella tehdä” – Vastaamo-epäilty kertoi kuulustelussa, ettei hallitse ohjelmointia. *Helsingin Sanomat*. https://www.hs.fi/kotimaa/art-2000009944567.html

Kilpailu- ja kuluttajavirasto. (i.a.-a). *Tietojenkalastelu.* https://www.kkv.fi/kuluttaja-asiat/huijaukset/tietojenkalastelu/

Kilpailu- ja kuluttajavirasto. (i.a.-b). *Verkkokauppahuijaus.* https://www.kkv.fi/kuluttaja-asiat/huijaukset/verkkokauppahuijaus/

Kyberturvallisuuskeskus. (2020a). *Kyberturvallisuus ja yrityksen hallituksen vastuu*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuuskeskus. (2020b). *Neuvoja identiteettivarkauden tai tietovuodon uhrille.* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-identiteettivarkauden-tai-tietovuodon-uhrille

Kyberturvallisuuskeskus. (.2020c). *Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen!* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen

Kyberturvallisuuskeskus. (10.8.2022). *Palvelunestohyökkäykset ovat arkipäivää Suomessa.* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa

Kyberturvallisuuskeskus. (19.6.2023). *Salasanat haltuun – Kuka käyttää tiliäsi?* https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun

Laki luottolaitostoiminnasta 610/2014. https://www.finlex.fi/fi/laki/ajantasa/2014/20140610#O4

Neittaanmäki, P., Lehto, M., & Savonen, M. (2021). *Yhteiskunnan digimurros.* Jyväskylän yliopiston IT-tiedekunta. Yliopistopaino. https://urn.fi/URN:ISBN:978-951-39-8647-6

Niemelä, L. (5.10.2023). Lähes puolet suomalaisista joutunut nettihuijauksen kohteeksi – näin huijareilta voi suojautua. *LähiTapiola.* https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/ajankohtaista/1509582383689/

Nordea. (i.a.). *Seitsemän ajankohtaista neuvoa turvalliseen pankkiasiointiin.* https://www.nordea.fi/henkiloasiakkaat/tuki/seitseman-ajankohtaista-neuvoa-turvalliseen-pankkiasiointiin.html

Nordea. (18.9.2023). *Sijoitushuijaukset nousussa.* https://www.nordea.com/fi/uutiset/sijoitushuijaukset-nousussa

Nurmi, P. (4.12.2023). Verkkorikollisuus kasvussa – miten tunnistan huijausyrityksen? *OmaSp.* https://www.omasp.fi/ajankohtaista/omastoori/verkkorikollisuus-kasvussa-miten-tunnistan-huijausyrityksen

Näveri, A. (1.6.2023). OP:n häiriö korjattu – eläkkeitä, palkkoja ja Kelan etuuksia viivästyi häiriön vuoksi. *Yle.* https://yle.fi/a/74-20034565

OmaSp. (i.a.-a). *Vinkit turvalliseen verkkoasiointiin.* https://www.omasp.fi/henkiloasiakas/arjen-raha-asiat/turvallinen-asiointi/turvallinen-asiointi-verkossa

OmaSp. (i.a.-b). *Riskienhallinta kuuluu pankin liiketoimintaan.* https://www.omasp.fi/sijoittajalle/johto-ja-hallinnointi/riskienhallinta-ja-riskit

OP. (i.a.-a). *Identiteettivarkaus*. https://vahinkoapu.pohjola.fi/henkiloasiakkaat/tietoa/identiteettivarkaus

OP. (i.a.-b). *Huijaussivustot*. https://www.op.fi/turvallinen-asiointi/verkkorikollisuus/huijaussivustot

OP. (i.a.-c). *Sijoittaja, muista maltti ja vältä huijarit!* https://www.op.fi/turvallinen-asiointi/verkkorikollisuus/sijoitushuijaus

Palmgren, J. (13.9.2023). Kalastelut ja muut huijaukset kasvoivat räjähdysmäisesti alkuvuonna – pankit saivat estettyä huijauksia lähes 16 miljoonan euron edestä. *Finanssiala.* https://www.finanssiala.fi/uutiset/kalastelut-ja-muut-huijaukset-kasvoivat-rajahdysmaisesti-alkuvuonna-pankit-saivat-estettya-huijauksia-lahes-16-miljoonan-euron-edesta/

Pietarinen, H. (5.10.2023). Suomen Pankki ja Verohallinto palvelunestohyökkäyksen kohteena – venäläishakkerit ilmoittautuivat tekijäksi. *Helsingin Sanomat*. https://www.hs.fi/talous/art-2000009901387.html

Pitkänen, P. (18.11.2023). Nordean palveluissa oli häiriö – tilit näyttivät nollaa tuntien ajan. *Ilta-Sanomat*. https://www.is.fi/taloussanomat/art-2000010000679.html

Pohjola, M. (2015). *Digitalisaatio ja tuottavuus finanssialalla.* Aalto-yliopiston kauppakorkeakoulu. https://www.finanssiala.fi/wp-content/uploads/2015/06/Digitalisaatio_ja_tuottavuus_finanssialalla.pdf

Pulkkinen, M. (13.7.2022). Pankkipalveluiden tekoäly helpottaa ja sujuvoittaa asiointia. *OP Media.* https://www.op-media.fi/digitalisaatio/pankkipalveluiden-tekoaly-helpottaa-ja-sujuvoittaa-asiointia/

Raijas, A. (2020). Digitaalisuus talousosaamisessa. *Euro & talous.* https://urn.fi/URN:NBN:fi:bof-202006082176

Rikosuhripäivystys. (i.a.-a). *Miten voin suojautua identiteettivarkaudelta ja vähentää siitä koituvien muiden rikosten riskejä?* https://www.riku.fi/oppaat-ja-ohjeet/identiteettivarkaus/

Rikosuhripäivystys. (i.a.-b). *Rakkauspetokset ja romanssihuijaukset verkossa.* https://www.riku.fi/erilaisia-rikoksia/rakkauspetokset-verkossa/

Rikosuhripäivystys. (1.11.2022). *Verkkopankkihuijauksen sattuessa pankki saattaa vastata menetyksistä.* https://www.riku.fi/verkkopankkihuijauksen-sattuessa-pankki-saattaa-vastata-menetyksista/

Sisäministeriö. (i.a.-a). *Kyberrikollisuus ylittää rajat tietoverkoissa.* https://intermin.fi/poliisiasiat/kyberrikollisuus

Sisäministeriö. (i.a.-b). *Kyberturvallisuus osana kansallista turvallisuutta.* https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

Takala, K. (2022). Digitalisaatio muuttaa maksamistapoja Suomessa. *Euro & talous.* https://urn.fi/URN:NBN:fi:bof-202208301350

Tillaeus, J. (13.11.2023). *Jopa lapset tekevät palvelunestohyökkäyksiä – kohteena pelialustat ja koulumaailman Wilma*. Yle. https://yle.fi/a/74-20059527

Valtiovarainministeriö. (i.a.-a). *Suomen kestävän kasvun ohjelma – vauhtia uudistuksiin ja investointeihin.* https://vm.fi/kestava-kasvu

Valtiovarainministeriö. (i.a.-b). *Suomen elpymis- ja palautussuunnitelma.* https://vm.fi/suomen-elpymis-ja-palautumissuunnitelma

Valtiovarainministeriö. (i.a.-c). *Julkisen hallinnan digitalisaatio.* https://vm.fi/digitalisaatio

Valtiovarainministeriö. (i.a.-d). *Digitalisaatio – elpymis- ja palautussuunnitelma.* https://vm.fi/digitalisaatiokk