Tampereen yliopisto

Eveliina Hietaniemi

KATSAUS VERKKO- JA MOBIILI-PANKKIEN TIETOTURVAUHKIIN

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Elokuu 2023

TIIVISTELMÄ

Eveliina Hietaniemi: Katsaus verkko- ja mobiilipankkien tietoturvauhkiin
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Elokuu 2023

Pankkiasiointi tapahtuu nykypäivänä yhä enenevissä määrin tietoverkkojen kautta, verkko- ja mobiilipankeissa. Pankkitunnuksia käytetään myös moniin muihin palveluihin kirjautuessa. Tämä on väistämättä luonut haavoittuvuuksia ja rikollisille uusia tapoja huijata uhreja sekä toteuttaa pankkeihin kohdistuvia hyökkäyksiä. Vaikka vahvan sähköisen tunnistautumisen järjestelmien vaatimukset ovat korkealla tasolla, mikään tietojärjestelmä ei ole täysin turvallinen tai aukoton. Käyttäjien on hyvä olla tietoisia erilaisista uhkista, joita kuka tahansa voi kohdata.

Tämä tutkielma on toteutettu kirjallisuuskatsauksena, jossa vastataan seuraaviin tutkimuskysymyksiin: miten verkko- ja mobiilipankit ovat kehittyneet nykyiseen muotoonsa, ja millaisia tietoturvauhkia niihin erityisesti liittyy? Pankkipalveluita alettiin tarjota etänä jo 80-luvulla, mutta verkkoselaimen ja Internet-yhteyden vaativat verkkopankit yleistyivät 2000-luvun vaihteessa. Mobiilipankkisovellukset ovat kasvattaneet suosiotaan tasaisesti vuodesta 2010 alkaen. Katsauksen perusteella verkkopankkeihin kohdistuu etenkin haittaohjelmahyökkäyksiä. Mobiilipankkisovelluksissa yleisiä uhkia ovat muun muassa kolmannen osapuolen peukaloimat sovellukset. Sovellusten haavoittuvuudet liittyvät usein varmenteiden vahvistukseen, arkaluonteisen tiedon salaukseen ja välitykseen, sekä kuvakaappausten mahdollisuuteen. Väliintulohyökkäys ja tietojenkalastelu uhkaavat pankkien asiakkaita yleisesti.

Avainsanat: kyberturvallisuus, verkkopankki, mobiilipankki, tietoturva, uhka

SISÄLLYSLUETTELO

1 Johdanto 1

2 Tutkimusmenetelmä 3

3 Pankkien tietoturva yleisesti 4

3.1 Pankit ja tietoturva 4

3.2 SSL/TLS 5

3.3 Autentikointi 5

4 Verkkopankkien tietoturva 7

4.1 Verkkopankin lyhyt historia 7

4.2 Verkkopankkeihin liittyviä tietoturvauhkia 7

5 Mobiilipankkien tietoturva 10

5.1 Mobiilipankin lyhyt historia 10

5.2 Mobiilipankkeihin yleisesti liittyviä tietoturvauhkia 10

5.3 Android-laitteet 11

6 Keskustelu 13

7 Yhteenveto 15

Lähdeluettelo 16

1 Johdanto

Pankit ovat instituutioita ja pääasiassa yksityisen sektorin keskenään kilpailevia yrityksiä, jotka tarjoavat finanssipalveluja. Näihin palveluihin kuuluvat muun muassa talletusten vastaanotto, maksuliikenteen hoito ja luotonanto. Pankeilla on korostunut velvollisuus asiakkaidensa varojen ja tietojen huolelliseen säilytykseen (Yli-Huttula, 2022). Lähes jokaiselta löytyy tili jostakin pankista, joten pankkien turvallisuus koskettaa meitä kaikkia. Kun 1990-luvun alun laman aikana Suomessa tehtiin pahimmillaan yli sata pankkiryöstöä vuodessa, nykyään ryöstöt ovat käytännössä loppuneet – tästä voidaan kiittää sekä tehokkaita turvatoimia että käteisen rahan käytön vähenemistä (Palmgren, 2020).

Digitalisaation myötä yhä useampi asiakas hoitaa pankkiasioinnin sähköisesti verkkopankissa ja/tai mobiilipankkisovelluksessa. Tämä helpottaa asiakkaiden elämää, mutta samalla rahaliikenteen siirtyminen verkkoon luo erilaisia uhkia. Jos aikana ennen Internetin yleistymistä pankkeihin kohdistetut rikokset olivat lähinnä ryöstöjä, tänä päivänä rikollisten ei tarvitse yrittää mitään yhtä riskialtista. Suurien summien saaminen voi onnistua verkon välityksellä, hyökkäystä voidaan suunnitella huolella pitkäänkin ja kiinnijäämisen todennäköisyys on pienempi. Pankkeihin kohdistuvan kyberrikollisuuden voidaan ajatella olevan tietoverkkojen mahdollistamaa rikollisuutta, koska pankkiasioinnin siirtyminen verkkoon on luonut sekä hyökkäyspintoja että -vektoreita, joita ei aiemmin ollut käytössä.

Pankit ovat erityisen kiinnostava ja tuottoisa kohde rikollisille siitä syystä, että hyökkäysketju on tällöin mahdollisimman lähellä rahallisia tuottoja. Kun kyberrikollisuuden vuosittaisia kustannuksia tarkastellaan toimialoittain, pankkiala on listan kärjessä. (Zimba, 2022) Suomessa pankit hallinnoivat turvallisuusratkaisujaan ja vastaavat tietojärjestelmien kehityksestä ja ylläpidosta itse. Järjestelmiä koskevat vaatimukset ovat tiukimmasta päästä, ja Traficomin mukaan vahvan sähköisen tunnistuksen järjestelmät ovat Suomessa kansainvälisesti vertailtuna korkeatasoisia. Pankkitunnuksia käytetään paljon myös muihin kuin pankin palveluihin kirjautumiseen, joten kirjautumisen luotettavuus on siinäkin mielessä hyvin tärkeää. (Yli-Huttula, 2022) Tietojärjestelmistä ja kyberturvallisuudesta huolehtiminen on merkittävässä osassa pankkien toimintaa ja investointeja: esimerkiksi viime vuonna OP Ryhmällä ICT-kulut olivat henkilöstökulujen jälkeen suurin yksittäinen kuluerä (OP Ryhmä, 2022).

Tässä tutkielmassa tarkastellaan pankkien kyberturvallisuutta. Tutkimuskysymykseni ovat, miten verkko- ja mobiilipankit ovat kehittyneet, ja millaisia tietoturvauhkia niihin erityisesti kohdistuu. Työssä ei keskitytä pintaraapaisua enempää uhkilta suojautumiseen, joka itsessään voisi olla toisen tutkielman aihe. Kirjallisuuskatsauksen perusteella nettiselaimella toimivat verkkopankit syntyivät 90-luvun lopulla Internetin saatavuuden para-

nemisen myötä, ja vuosituhannen vaihduttua useimmat pankit tarjosivat verkkopankkipalveluita. Mobiilipankkisovellukset alkoivat yleistyä vuodesta 2010 eteenpäin ja kasvattivat suosiotaan nopeasti: tänä päivänä suurin osa pankkitapahtumista tehdään mobiilipankkien kautta. Verkkopankkien yleisin uhka on haittaohjelma, joka tarttuu esimerkiksi sähköpostiviestin välityksellä. Mobiilipankkisovelluksista on löydetty monia haavoittuvuuksia. Varmenteiden virheellinen tai puutteellinen käyttö altistaa väliintulohyökkäykselle. Lisäksi on hyvä huomioida tietojenkalastelu, joka ei vaadi onnistuakseen monimutkaisia teknisiä toteutuksia.

Luvussa 2 kerron tiedonhankintaprosessista ja tutkimusmenetelmästä. Luvussa 3 kuvataan muutama keskeinen käsite sekä tietoturvauhkia, jotka liittyvät pankkeihin yleisellä tasolla. Luvussa 4 kerrotaan lyhyesti verkkopankin historiasta ja sille ominaisista tietoturvauhkista. Luvussa 5 kuvataan vastaavasti mobiilipankin kehitystä ja uhkia. Luku 6 sisältää keskustelua ja pohdintaa löydetyistä tuloksista, ja luvussa 7 vielä tiivistetään.

2 Tutkimusmenetelmä

Tutkielma on toteutettu kirjallisuuskatsauksena. Pyrin löytämään mahdollisimman tuoreita tutkimuksia aiheesta, ja suurin osa tieteellisistä lähteistä onkin viimeisen 5 vuoden ajalta, vanhimmat vuodelta 2015. Aihetta on viime vuosina tutkittu kohtalaisesti. Vapaasti saatavilla olevia lähteitä löytyi tutkielmaa varten riittävästi, muttei mitenkään runsaasti. Tieteellisten artikkelien lisäksi käyttämiäni lähteitä ovat muun muassa Ylen uutiset ja Finanssialan nettiartikkelit, jotka koen luotettaviksi.

Tiedonhankinnan alussa aiheeni oli vielä yleisellä tasolla pankkien tietoturvauhat. Joitakin tieteellisiä lähteitä selailtuani aloin huomata, että niissä toistuivat termit *online banking* ja *mobile banking*. Tämä on loogista, koska kyberturvallisuuteen liittyvät uhat kohdistuvat juuri näihin eivätkä fyysisiin pankkeihin. Myöhemmin aloin käyttää näitä termejä tiedonhaussa, mikä helpotti sopivien artikkelien löytämistä. Tiedonhaussa näkyi viime vuosien aikana kehittynyt siirtymä verkkopankeista mobiilipankkisovelluksiin, koska jälkimmäisestä tuntui löytyvän helpommin tuoreita lähteitä. Online banking viittaa monessa tapauksessa kaikkeen sähköiseen pankkiasiointiin, mukaan lukien mobiilipankit, joten saadakseni tuloksia juuri verkkopankista tein hakuja myös vaihtamalla onlinemääritteen tilalle home tai web.

Käyttämiäni tietokantoja olivat Andor, ACM Digital Library, Computer Science Database ja IEEE Xplore. Erityisen toimivaksi hakulausekkeeksi osoittautui (”online bank” OR ”mobile bank”) AND (security OR threat). Etsin artikkeleja, jotka olivat korkeintaan 5–10 vuotta vanhoja ja vapaasti saatavilla. Pariin pääsin käsiksi Tunin tunnusten avulla. Tulosten alustava karsiminen tapahtui otsikon perusteella. Lupaavimpia artikkeleja olivat sellaiset, joissa käyttämäni hakusanat esiintyivät jo otsikossa. Halusin tulosten kuvaavan aihetta yleisellä tasolla ja olevan kansainvälisesti vertailukelpoisia, joten alustavasti pyrin karsimaan artikkelit, joissa tutkimus kohdistui yksittäiseen maahan. Lopulta pari tämän kaltaista laadukasta artikkelia valikoitui mukaan.

Avattuani lupaavalta vaikuttavan artikkelin esittelysivun luin abstraktin tai tiivistelmän, ja tämän perusteella jatkoon päässeet tallensin tietokoneelle. Välillä merkitsin muistiin, mistä tietokannasta ja millä hakusanoilla lähde löytyi. Kaikki tähän asti selvinneet artikkelit luin läpi. Osa tuloksista karsiutui vielä tässäkin vaiheessa, jos kyseessä olikin kooste muiden tekemistä tutkimuksista eikä kirjoittajan itsensä tekemä, tai sisältö ei suoraan vastannutkaan tutkimuskysymykseeni. Tällaisten kohdalla hyviä lähteitä saattoi kuitenkin löytyä lähdeluettelosta.

3 Pankkien tietoturva yleisesti

Tässä luvussa avataan keskeisimpiä tietoturvan termejä ja sähköisiin pankkijärjestelmiin yleisesti liittyviä uhkia.

Aluksi on hyvä määritellä CIA-malli eli kolme osa-aluetta, joiden huomioimiseen tietoturvallisuus keskittyy: *luottamuksellisuus* (confidentiality), *eheys* (integrity) ja *saatavuus* (availability). Luottamuksellisuus tarkoittaa sitä, että tieto on saatavilla vain niille, joille on myönnetty lupa: muussa tapauksessa tieto pysyy salassa eikä pääse sellaisten käsiin, joille sen ei haluta päätyvän. Pankkikontekstissa luottamuksellisuutta on se, että vain asiakas itse ja tarvittaessa pankin työntekijät tai poliisi saavat tarkastella tiliotteita. Eheydellä tarkoitetaan sitä, että tieto pysyy muuttumattomana ja on juuri sitä, mitä sen kuuluisikin olla. Esimerkiksi tilisiirron yhteydessä tulisi varmistaa, että kaikki maksun tiedot ovat oikein. Saatavuus taas viittaa siihen, että tieto on saatavilla aina silloin kun sitä tarvitaan. Siispä esimerkiksi tietoliikenneverkkojen toimivuus on tärkeää ja osa tietoturvallisuutta.

Tutkielman aiheen kannalta tärkeitä termejä ovat *uhka* (threat) ja *haavoittuvuus* (vulnerability). Uhka on ”mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku” (TEPA, 2023). Tietoturvauhalla viitataan siis vahingolliseen tapahtumaan, joka toteutuessaan rikkoo tietoturvaa. Haavoittuvuus on ”alttius tietoturvaan kohdistuville uhkille”. Haavoittuvuuksia voidaan hyväksikäyttää vahingon aiheuttamisessa ja niitä voi esiintyä niin tietojärjestelmissä, prosesseissa kuin ihmisten toiminnassa. (TEPA, 2023)

3.1 Pankit ja tietoturva

Pankkeihin liittyy erityisesti kahden tyyppisiä turvallisuusongelmia: haavoittuvuuksien hyväksi käyttäminen ja toimintahäiriöistä johtuvat tahattomat tapahtumat. Haavoittuvuuksille ja toimintahäiriöille alttiita voivat olla useat sähköiseen pankkiasiointiin liittyvät tekijät, kuten tietojärjestelmät, laitteisto, IT-henkilöstö, järjestelmien käyttäjät, järjestelmien ja laitteiden valmistajat, sekä maksupalveluita tarjoavat yritykset. (Geramiparvar & Modiri, 2015) Tutkimukset ovat osoittaneet, että yleisin hyökkäysvektori pankkeja ja muita rahoituslaitoksia vastaan kohdistetuissa kyberrikoksissa on haittaohjelma. Muita vektoreita ovat muun muassa sähköpostien liitteet, heikot ja varastetut tunnistetiedot sekä käyttäjän manipulointi. (Zimba, 2022)

Suomessa on säännöllisin väliajoin uutisoitu pankkeihin kohdistuvista *palvelunestohyökkäyksistä* (denial-of-service attack). Keväällä 2022 Nordeaan kohdistettu hyökkäys aiheutti verkko- ja mobiilipankeissa häiriöitä poikkeuksellisen pitkään. F-Securen tutkimusjohtaja Mikko Hyppösen mukaan pankkien kaltaisiin järjestelmiin tehdyt hyökkäykset eivät nykypäivänä aiheuta ongelmia yleensä pitkäksi aikaa. Pidempään kestävät häiriöt ovat vakavia erityisesti siksi, että moni käyttää pankkitunnuksia sähköiseen tunnistautumiseen muissakin palveluissa. (Lindholm, 2022) Palvelunestohyökkäys vaikuttaa tietoturvan osa-alueista saatavuuteen. Usein asiakkaiden tilit ja rahat eivät ole vaarassa,

mutta esimerkiksi verkkopankkiin kirjautuminen ei onnistu. En löytänyt tieteellisiä artikkeleja nimenomaan pankkeihin kohdistetuista hyökkäyksistä; siinäpä siis mahdollinen tutkimuksen aihe.

Perinteisten pankkien lisäksi on olemassa rahoitusalan yrityksiä, joilla ei ole lainkaan fyysistä konttoria ja jotka eivät käsittele käteistä rahaa, vaan kaikki palvelu tapahtuu digitaalisessa muodossa, usein sovelluksen kautta. Tällaisia palveluja tarjoavista yrityksistä käytetään termiä *fintech*, joka tulee sanoista financial technology. Vaikka paperisten asiakirjojen puuttuminen poistaa niiden varastamisen tai kadottamisen uhan, täysin digitaaliset tietueet aiheuttavat lisää tietosuoja- ja tietoturvaongelmia, mikä edellyttää erityistä harkintaa sovellusten kehittämisessä, tiedonsiirrossa ja tietojen tallentamisessa (Botacin et al., 2019). Tässä tutkielmassa fintech jätetään syvemmän tarkastelun ulkopuolelle.

3.2 SSL/TLS

Yksi keskeinen termi turvalliseen verkkoyhteyden käyttöön liittyen on suojausprotokolla *SSL* (Secure Sockets Layer). SSL-varmenne on digitaalinen varmenne, joka todentaa verkkosivuston ja mahdollistaa verkkopalvelimen ja selaimen välille luodun salatun yhteyden. SSL siis suojaa verkkoyhteyden ja estää rikollisia lukemasta tai muokkaamasta tietoja, joita kahden järjestelmän välillä siirretään. Protokolla otettiin käyttöön yli 20 vuotta sitten. Vuosien varrella siitä on tullut useita eri versioita, joissa on kuitenkin ilmennyt tietoturvaongelmia ennemmin tai myöhemmin. Nykyään käytössä on parannettu versio, josta käytetään nimitystä *TLS* (Transport Layer Security). Lyhenne SSL on kuitenkin edelleen myös yleisesti käytössä. (Kaspersky, 2023)

Monessa tapauksessa sähköisen pankkijärjestelmän haavoittuvuudet liittyvät juuri SSL/TLS-varmenteen virheelliseen vahvistukseen. SSL/TLS-istunnon heikkous altistaa etenkin *väliintulohyökkäykselle* (man-in-the-middle attack), jossa ulkopuolinen voi seurata verkkoliikennettä asiakkaan ja palvelimen välillä, ja ilman eheyden tarkastusta jopa muokata ja lähettää väärennettyjä tietoja jommallekummalle osapuolelle (Reaves et al., 2015).

HTTP (Hypertext Transfer Protocol) on protokolla, joka suunniteltiin verkkoselaimen ja -palvelimen väliseen kommunikointiin ja tiedonsiirtoon. *HTTPS* (Hypertext Transfer Protocol Secure) on HTTP- ja SSL/TLS-protokollien yhdistelmä, joka varmistaa suojatun yhteyden. Riippulukko osoiterivin URL-osoitteen vieressä on osoitus siitä, että sivusto on suojattu SSL/TLS:n avulla. HTTP:ssä kaikki kommunikaatio tapahtuu selkotekstillä (plaintext), kun taas HTTPS salaa tekstin. (Awati, 2022)

3.3 Autentikointi

Autentikointi eli todentaminen tarkoittaa menettelyä, ”jolla varmistutaan kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä sekä tiedon eheyden säilymisestä”

(TEPA, 2023). Autentikoinnilla siis tarkastetaan sisäänkirjautuvan käyttäjän henkilöllisyys. Käsittelen tässä verkko- ja mobiilipankeissa käytössä olevia autentikointitapoja, jotka ovat oleellinen osa pankkien turvallisuutta, koska kirjautumisprosessi on yksi istunnon kriittisimmistä hetkistä.

Kiljan ja muut toteuttivat laajan, kansainvälisen tutkimuksen, jossa he tarkastelivat samojen sähköisten pankkijärjestelmien autentikointia ensin vuonna 2013 ja myöhemmin 2015. Identiteetin todentaminen (entity authentication) on pakollinen vaihe, joka käyttäjän on suoritettava ennen varsinaista verkko- tai mobiilipankki-istuntoa. Tapahtumien todentaminen (transaction authentication) on mahdollinen ylimääräinen todennus rahansiirron yhteydessä. Todentamisen tapoja ovat muun muassa tieto (jotain, mitä käyttäjä tietää), omistus (jotain, mitä käyttäjällä on hallussaan) sekä biometriikka (jotain, mitä käyttäjä on tai tekee). Todentaminen voi olla yksi-, kaksi- tai monivaiheista, riippuen siitä montako eri tapaa istunto vaatii. Vuonna 2015 Euroopassa oli lähes yksinomaan käytössä monivaiheinen todennus. (Kiljan et al., 2016)

Tutkituista verkkopankeista 21 %:ssa ja mobiilipankeista 38 %:ssa autentikointi perustui vain tietoon. Tietoon perustuvan autentikoinnin toteutuksia olivat tekstipohjaiset salasanat ja PIN-koodit. Salasanoja yksinään käytettiin jonkin verran, kun taas PIN-koodit olivat useammin osana monivaiheista todennusta. Näiden käyttö yksivaiheisessa todennuksessa on melko turvatonta, koska ne usein pysyvät pitkään muuttumattomina, jolloin rikolliset voivat näppäilytallentimen avulla saada tunnukset talteen ja pystyä suoraan hyödyntämään niitä. Muutamassa mobiilipankkisovelluksessa PIN-koodin tilalla käytettiin vaihtoehtoisena autentikointitapana biometriikkaa sormenjälkitunnistuksen muodossa. (Kiljan et al., 2016) Tässä on luultavasti tapahtunut kehitystä vuoden 2015 jälkeen.

Omistukseen perustuvaa todennusta ei juurikaan käytetty yksinään, vaan sen käyttö oli huomattavasti yleisempää monivaiheisessa todennuksessa. Verkkopankeissa yleisin toteutustapa oli, että asiakkaalle lähetetään tekstiviestillä kertakäyttösalasana. Mobiilipankeissa taas käyttäjä rekisteröi tilinsä sovelluksen kautta ja sitoo sen käytön tiettyyn laitteeseen. Tapa tuo kuitenkin turvallisuusriskin, koska mobiililaite itse edustaa hallussapitotekijää epäluotettavassa digitaalisessa ympäristössä, jolloin hyökkääjä saattaa haittaohjelman avulla kopioida tämän tekijän. Toinen yleinen omistukseen perustuva autentikointitapa oli jokin ulkoinen hallussapitotekijä, kuten paperisen/muovisen avainlukulistan käyttö. (Kiljan et al., 2016)

4 Verkkopankkien tietoturva

Tämä luku käsittelee verkkopankin kehityskaarta ja siihen kohdistuvia tietoturvauhkia nykypäivänä. Verkkopankit tarjoavat pankkien palveluja niiden omilla verkkosivuilla. Palvelun käyttö vaatii sopivan laitteen, Internet-yhteyden ja verkkopankkitunnukset. Verkkopankissa päivittäisten raha-asioiden hoito onnistuu missä ja milloin tahansa, joten ei ole ihme, että monelle se on mieluisampi vaihtoehto kuin paikan päällä konttorissa asioiminen.

4.1 Verkkopankin lyhyt historia

1980-luvun alussa pankkiasiointi onnistui etänä puhelimitse: asiakas soitti pankkiin ja puhui työntekijälle. Työntekijöiden palkkaaminen erikseen tätä tehtävää varten oli kuitenkin kallista, joten pankit alkoivat miettiä tapoja, joilla työntekijä voitaisiin poistaa prosessista. Ilmeisin tapa oli kehittää tietokone, jonka kanssa asiakas kommunikoisi työntekijän sijaan. Ensimmäiset sähköiset pankkijärjestelmät otettiin käyttöön myöhemmin 80-luvulla. Järjestelmään pääsy vaati tietynlaisen kotitietokoneen ja modeemin. Tiedonsiirto tapahtui puhelinlinjoja pitkin. 80- ja 90-lukujen taitteessa kehitettiin niin sanottu ”kotipankkiohjelmisto” (home banking software), jonka avulla asiakas saattoi nähdä tilin tapahtumahistorian ja saldon sekä suorittaa rahansiirtoja. (Kiljan et al., 2016)

90-luvun lopulla Internetin saatavuus parani ja osa pankeista päivitti kotipankkiohjelmistonsa tukemaan Internetin käyttöä niin, että asiakas saisi omalla tietokoneellaan yhteyden pankkiin. Jotkin pankit taas näkivät potentiaalia World Wide Webissä, jolloin ei tarvittaisi erillistä asiakaspuolen ohjelmistoa, vaan asiointi onnistuisi verkkoselaimella pankin omilla sivuilla. Tämä myös säästäisi pankeilta ohjelmiston kehittämisen, ylläpidon ja jakelun vaivan. Vuosituhannen vaihduttua suuri osa pankeista tarjosi verkkopankkipalveluita. Verkkopankki kasvatti tasaisesti suosiotaan, ja esimerkiksi vuonna 2015 Pohjoismaissa verkkopankkia käyttävien osuus väestöstä oli yli 85 %. (Kiljan et al., 2016)

4.2 Verkkopankkeihin liittyviä tietoturvauhkia

Syksyllä 2022 uutisoitiin S-Pankin tietojärjestelmähäiriöistä, mikä herätti kysymyksiä pankkitunnistautumisen luotettavuudesta. Osa pankin asiakkaista pääsi kolmen kuukauden ajan käsiksi toistensa verkkopankkeihin. Joiltakin tileiltä tehtiin oikeudettomia tilisiirtoja, mikä onnistui tietojärjestelmästä löytynyttä haavoittuvuutta hyväksi käyttäen. Tapaus on poikkeuksellinen, koska epäiltyjen joukko asuu ja teot on tehty Suomessa, ja rikokset ovat onnistuneet ilman asianomistajien myötävaikutusta. Poikkeuksellisuudesta huolimatta Kuluttajaliitto epäilee, että tämä yksittäinen tapaus saattaa aiheuttaa epäluottamusta myös muuhun digitaaliseen pankkiasiointiin, vaikka finanssiala on pitkään tehnyt töitä rakentaakseen luottamusta. (Helpinen, 2022)

Yksi esimerkki juuri verkkopankkeihin kohdistuvista turvallisuusuhkista oli hakkerointikampanja Operation Emmental. Vuonna 2015 Emmental-niminen haittaohjelma oli

yksi vaarallisimmista ja monimutkaisimmista siihen mennessä tunnetuista viruksista ja hyökkäyksistä: se pystyi tunkeutumaan kaksivaiheisen tunnistautumisjärjestelmän läpi. Tapauksia ilmeni muun muassa Ruotsissa, Sveitsissä, Itävallassa ja Japanissa, ja hyökkäysten havaittiin tulleen venäjänkielisistä maista. Hyökkäys alkoi käyttäjän saamalla sähköpostilla, jonka lähettäjä vaikutti olevan hyvämaineinen yritys kuten Google, Microsoft tai eBay. Jos käyttäjä erehtyi avaamaan viestin liitteenä olevan tiedoston, haittaohjelma aktivoitui. Seuraavassa vaiheessa käyttäjä päätyi pankkitapahtumaa varten väärennetylle sivulle, johon tuli syöttää verkkopankkitunnukset. Kirjautuminen vaati lisäksi PIN-koodin, joka tavallisesti lähetetään tekstiviestinä. Tekstiviesti ei tullutkaan perille, joten käyttäjä joutui klikkaamaan “No SMS received from the bank”, minkä jälkeen hän sai kehotuksen ladata sovellus koodin saamiseksi, tai muuten verkkopankin käyttö ei onnistuisi. Mikäli käyttäjä latasi kyseisen sovelluksen ja syötti sen generoiman salasanan verkkosivustolle, PIN-koodin sisältämä tekstiviesti tulikin hyökkääjälle, joka onnistui saamaan käyttäjän verkkopankkitunnukset käyttöönsä. Tämän jälkeen haittaohjelma itse poisti itsensä, mikä teki sen löytämisestä haastavaa. (Geramiparvar & Modiri, 2015)

Viimeisin uutinen Emmental-haittaohjelmasta on vuodelta 2017, mutta samankaltaisia ja kehittyneempiä hyökkäyksiä ilmaantuu jatkuvasti. Kenties tämän hetken yleisin ja levinnein haittaohjelma finanssialalla on GameOver Zeus -niminen bottiverkko, joka pystyy hyödyntämään pilvilaskennan ympäristöjä tiettyjen haavoittuvuuksien esiintyessä. GameOver Zeusin edeltäjä on pankkitroijalainen Zeus, joka esiintyi ensimmäisen kerran vuonna 2007. Ensisijaisesti Zeus poimii pankkitunnuksia tartunnan saaneista järjestelmistä. Alun perin tartuntavektoreita olivat sähköpostien roskaposti- ja tietojenkalasteluviestit. GameOver Zeusin hyökkäysmalli on erilainen kuin alkuperäisen Zeusin. Se käyttää tekniikkaa, joka luo suuren määrän verkkotunnuksia – jopa 10 000 päivässä – jotka toimivat ”tapaamispisteinä” Command & Control -tason ja bottiverkon välillä. (Zimba, 2022)

Jansen ja Leukfeldt haastattelivat onnistuneiden haittaohjelmahyökkäysten ja tietojenkalastelun uhreiksi joutuneita alankomaalaisia verkkopankkiasiakkaita. Nämä kaksi ovat Alankomaissa yleisimpiä verkkopankkipetoksiin liittyviä rikoksia, ja kaikkialla maailmassa merkittäviä kyberrikollisuuden lajeja myös pankkikontekstin ulkopuolella. Molemmissa tapauksissa huijareiden tavoitteena on huijata uhria tai järjestelmää saadakseen uhrin laitteen ja/tai pankkitunnukset käyttöönsä. Suurin osa haastatelluista oli käyttänyt verkkopankkia vähintään 5 vuotta ja käytti sitä vähintään viikottain, joten heitä voisi kuvata kokeneiksi verkkopankin käyttäjiksi. (Jansen & Leukfeldt, 2016)

Tietojenkalastelutapauksissa hyökkäys alkoi yleensä sähköpostiviestistä, joka liittyi verkkopankin turvallisuuteen tai autentikointiin. Sähköpostia seurasi usein puhelu. Puhelussa hyökkääjä saattoi mainita, että asiakkaan tulisi tarkistaa tai suorittaa jokin toimenpide, joka käynnistyisi sähköpostiin vastaamalla. Hyökkäyksen onnistuttua kaikki paitsi

yksi uhreista ymmärsi, missä kohtaa oli mennyt pieleen ja miten hyökkääjä sai arkaluonteista tietoa. He kuitenkin kokivat, että hyökkääjä ja tämän tarina vaikuttivat luotettavilta, tai eivät itse olleet tarpeeksi valppaina torjuakseen hyökkäystä. (Jansen & Leukfeldt, 2016)

Haittaohjelmahyökkäykset olivat erilaisia muun muassa siten, että uhrit eivät jälkikäteen osanneet rekonstruoida hyökkäysprosessia. Nämä hyökkäykset eivät vaatineet suoraa kontaktia uhriin. Hyökkäys jäi osalta jopa täysin huomaamatta, kun taas osa ilmoitti huomanneensa jonkin poikkeaman, muttei osannut yhdistää sitä mahdolliseen hyökkäykseen. Poikkeamia olivat esimerkiksi näytön häiriö, selaimen toiminnan lakkaaminen tai ongelmat kirjautumisessa. Haittaohjelma latautui käyttäjän laitteelle, jos tämä vieraili saastuneella verkkosivustolla. Tartunnan jälkeen käyttäjän tehdessä tilisiirtoja puolet summasta siirtyi oikealle vastaanottajalle, ja puolet niin sanotun muulin eli välikäden tilille, josta muuli siirtäisi rahat hyökkääjälle. Kaikki vilpillinen tapahtui käyttäjältä piilossa, eikä ylimääräinen siirto näkynyt maksun yhteenvetonäkymässä. Se oli havaittavissa vain laitteella, joka ei ollut saanut tartuntaa. (Jansen & Leukfeldt, 2016)

Yksi mahdollinen uhka on näppäimistön ”nuuskinta” (keyboard sniffing). Lee ja Yim tarkastelivat tuoreessa tutkimuksessa PS/2-liittimellä varustettuihin näppäimistöihin kohdistuvia hyökkäystekniikoita, joiden avulla rikolliset voivat kerätä näppäimistön dataa ja saada haltuunsa muun muassa verkkopankkitunnuksia. Kyseisten näppäimistöjen sisältämä laitteistosiru ei tarjoa turvallisuutta parantavia ominaisuuksia. Monissa maissa verkkopankkisivut eivät sisällä näppäimistöä suojaavaa ohjelmistoa (secure keyboard software/program). Lee ja Yim testasivat hyökkäyksiä korealaisilla verkkosivuilla, joissa suojaavia ohjelmistoja sovellettiin. He huomasivat, että ohjelmistoista huolimatta useat eri virustorjuntaohjelmat eivät havainneet hyökkäyksissä käytettyjä työkaluja. (Lee & Yim, 2023) Tätä uhkaa kuitenkin lieventää se, että viime vuosina USB-liitäntä ja langattomuus ovat olleet näppäimistöissä yleisempiä.

5 Mobiilipankkien tietoturva

Tämä luku käsittelee mobiilipankin kehitystä ja siihen kohdistuvia tietoturvauhkia nykypäivänä. Mobiilipankilla viitataan pankkiasiointiin mobiililaitteella, kuten älypuhelimella, mikä vaatii erikseen ladattavan mobiilipankkisovelluksen. Tämä sovellustyyppi kuuluu turvallisuuskriittisimpiin ja tietoherkimpiin, ottaen huomioon mahdolliset turvallisuusriskit ja haavoittuvuuksien aiheuttamat taloudelliset tappiot (Chen et al., 2020).

5.1 Mobiilipankin lyhyt historia

Mobiilipankin historia ulottuu peräti 1990-luvun lopulle. Tuolloin käytössä oli Wireless Application Protocol eli WAP, eräänlainen kevyempi versio WWW:stä, joka mahdollisti verkkosivujen lataamisen matkapuhelimissa. Sen käyttö oli paikasta riippumattomampaa kuin verkkopankin käyttö kotitietokoneella. WAP oli aikanaan mullistava teknologia, mutta melko kallis, käytettävyydeltään heikko ja vain rajoitetun käyttäjäkunnan saatavilla. (Kiljan et al., 2016)

Mobiilipankkisovellukset alkoivat yleistyä vuodesta 2010 eteenpäin. Sovellusten kehittäminen ja julkaiseminen on suhteellisen helppoa, ja nykyään useimmat pankit tarjoavat sovellukset niin Androidille kuin iOS:lle. Vielä joitakin vuosia sitten mobiilipankin käyttö ei ollut yhtä yleistä kuin perinteisen verkkopankin käyttö, mutta sen suosio kasvaa ja suosion odotetaan kiihtyvän entisestään. Verkkopankki on kuitenkin edelleen laajassa käytössä mobiiliversion ohella, vaikka suuri osa pankkitapahtumista tehdään jo mobiilipankeissa. (Kiljan et al., 2016) Syitä mobiilipankkien suosion nopealle kasvulle ovat muun muassa käyttö etenkin 18–32-vuotiaiden keskuudessa, saavutettavuus, vaivattomuus ja helppokäyttöisyys, sekä usein hyvän käyttökokemuksen tarjoaminen (Wazid et al., 2019).

5.2 Mobiilipankkeihin yleisesti liittyviä tietoturvauhkia

Wazid ja muut listaavat neljä mobiilipankkien turvallisuuteen liittyvää uhkaa, jotka huolestuttavat potentiaalisia käyttäjiä. Ensimmäinen on mobiililaitteiden haittaohjelmat: mobiilipankin käytön yleistyttyä hyökkääjät ovat kehittäneet haittaohjelmia, jotka kohdistuvat erityisesti mobiilipankkisovelluksiin. Haittaohjelmien määrän ja tyyppien odotetaan kasvavan tulevaisuudessa. Toinen listattu uhka on kolmannen osapuolen sovellukset, joista osa on huijareiden kehittämiä. Kolmas uhka on suojaamattoman Wi-Fin käyttö esimerkiksi ostoskeskuksissa ja lentokentillä, minkä seurauksena voi olla muun muassa väliintulohyökkäys. Neljäs mainittu uhka on ihmisten käytös, eli käyttäjien toimiminen tavoilla, jotka mahdollistavat hyökkäysten tavoitteet ja helpottavat rikollisia: sovellusten lataaminen, linkkien avaaminen ja suojaamattoman verkkoyhteyden käyttö. Wazid ja muut listaavat myös kahdeksan haittaohjelmatyyppiä, jotka voivat uhata mobiilipankkei-

hin liittyviä järjestelmiä. Nämä ovat näppäilytallennin, vakoiluohjelma, virus, mato, troijalainen, piilohallintaohjelma, selaimen kaappaaja ja kiristyshaittaohjelma. (Wazid et al., 2019)

5.3 Android-laitteet

Reaves ja muut julkaisivat vuonna 2015 ensimmäisten joukossa syvällisen analyysin mobiilipankkisovellusten turvallisuudesta. Tutkimukseen valitut Android-sovellukset olivat käytössä kehitysmaissa, joissa mobiiliraha on erityisen tärkeässä asemassa käteisen rahan ryöstöjen takia. Analyysin perusteella selvisi, että yleisin haavoittuvuus oli ongelmat SSL/TLS-varmenteen vahvistamisessa tai peräti SSL/TLS-protokollan hyödyntämättä jättäminen. Osassa sovelluksista kryptografiset algoritmit eli salausjärjestelmät olivat heikosti toteutettuja, mikä uhkaa tiedon eheyttä ja altistaa tilitapahtumien vakoilulle ja väärentämiselle. Lisäksi joidenkin sovellusten pääsynvalvonta oli puutteellisella tasolla: esimerkkinä tiedon välitys tekstiviestitse, minkä on todettu olevan huono käytäntö viestien sieppausten riskin vuoksi. (Reaves et al., 2015)

Chen ja muut laativat vuonna 2020 laajimman siihen mennessä tehdyn tutkimuksen Android-laitteiden mobiilipankkisovelluksista. He keräsivät yli 2000 haavoittuvuutta tai heikkoutta (weakness) 693 sovelluksesta, joiden takana oli 470 pankkia 83 eri maasta. He muun muassa huomasivat, että pankkien tytäryhtiöiden omistamat sovellukset ovat usein vähemmän turvallisia kuin emopankkien omistamat. Hyökkääjät voivat käyttää hyväkseen erityisesti sovellusten vanhentuneista versioista tai kolmannen osapuolen kirjastoista johtuvia heikkouksia. Maailmanlaajuisesti tarkasteltuna mobiilipankkisovellukset ovat turvallisimpia Euroopassa ja Pohjois-Amerikassa, joissa löytyi keskimäärin 0,27 haavoittuvuutta yhtä sovellusta kohden, kun Afrikassa luku oli 4,6 ja Aasiassa 6,4. (Chen et al., 2020)

Roottaus (rooting) on Android-laitteille tehtävä prosessi, jolla saa pääkäyttäjän oikeudet eli niin sanotut root-oikeudet koko käyttöjärjestelmään. Näillä oikeuksilla käyttäjä voi esimerkiksi poistaa laitteen esiasennettuja sovelluksia. Roottaus muuttaa puhelimen luontaista suojausta ja aiheuttaa turvallisuusriskejä etenkin, jos käyttäjä ei tiedä mitä tekee. Roottauksen myötä käyttäjä on siis itse vastuussa käyttöjärjestelmän ja sovellusten turvallisuudesta ja eheydestä. (Hildenbrand, 2022)

Chen ja muut huomasivat, että tiettyjä heikkouksia esiintyi juuri rootatuissa laitteissa. He luokittelivat löytämänsä haavoittuvuudet neljään eri kategoriaan sen mukaan, millä tavoin arkaluonteisia henkilötietoja voisi päätyä hyökkääjien käsiin. Ensimmäinen on syötteen kerääminen (input harvest), jolla tarkoitetaan salassa pidettävien syötteiden tai arkaluonteisten tietojen keräämistä käyttöliittymän kuvakaappauksilla, mikä voi olla mahdollista rootatuissa laitteissa haitallisten sovellusten toimesta. Tämä oli yleisin haavoittuvuus, sillä peräti 88 %:ssa sovelluksista pystyi ottamaan kuvakaappauksia. Tiedontallennukseen (data storage) liittyvissä heikkouksissa hyökkääjä voi rootatuissa laitteissa

hankkia dataa tallennustilasta, tai ilman root-oikeuksia esimerkiksi SD-muistikortilta, .txt-tiedostoista tai järjestelmälokista. Kolmas kategoria on tiedonsiirto (data transmission), johon liittyviä heikkouksia oli esimerkiksi arkaluonteisen tiedon välittäminen tekstiviestitse, sillä haittaohjelmat voivat siepata viestejä. Viestintäinfrastruktuuriin (communication infrastructure) liittyviä heikkouksia taas olivat kehnojen varmenteiden käyttö, sopimattoman tai epävarman salauksen käyttö, sekä vain HTTP-protokollan käyttäminen suojatun HTTPS:n sijaan. Nämä altistavat väliintulohyökkäykselle. (Chen et al., 2020)

Zhengin ja muiden artikkeli keskittyy myös Android-laitteisiin. He tutkivat erityisesti mobiilipankkisovelluksiin liittyvää uhkaa, jossa rikolliset muokkaavat jostakin Android-sovelluskaupasta löytyvän sovelluksen koodia ja sitten lisäävät tämän manipuloidun, mutta alkuperäistä muistuttavan version pahaa-aavistamattomien käyttäjien ladattavaksi. Kyseessä on repackaging attack, jolla ei vaikuta olevan vakiintunutta suomenkielistä termiä, mutta käytetään tässä yhteydessä nimeä *uudelleenpakkaushyökkäys*. Zheng ja muut toteuttivat ja demonstroivat kolme erilaista hyökkäystä, joiden avulla hyökkääjä voi saada käsiinsä esimerkiksi uhrin tekstiviestit, yhteystiedot, sijainnin tai muuta arkaluonteista tietoa. Etenkin epävirallisissa, kolmannen osapuolen sovelluskaupoissa sovelluksia voi kehittää ja ladata lähes kuka tahansa, jolloin riski peukaloidun sovelluksen lataamiselle on suurempi. Edes virusohjelma ei kaikissa tapauksissa suojaa käyttäjää. Useimmiten vain valveutuneimmat käyttäjät suhtautuvat vakavasti mahdolliseen järjestelmän antamaan varoitukseen ja lukevat tekstin huolellisesti. (Zheng et al., 2017)

Botacin ja muut tutkivat Androidille saatavilla olevia mobiilipankkisovelluksia Brasiliassa, jossa uusien pankkiteknologioiden varhainen ja laaja käyttöönotto on ollut tavallista. Tutkituista sovelluksista moni oli altis väliintulohyökkäykselle, koska ne hyväksyivät tekaistun varmenteen avulla luodun ”salatun” yhteyden. Osassa sovelluksista arkaluonteista tietoa ei tallennettu salattuna, jolloin hyökkääjä voi saada tunnukset käsiinsä selkotekstinä. Näytöntallennus ja kuvakaappaukset olivat mahdollisia, kuin myös niin sanottu overlay-hyökkäys, jossa oikean kirjautumiskentän päällä on huijarin lisäämä overlay tunnusten saamiseksi. Sovellusten itsesuojauksessa oli puutteita, koska ne toimivat rootatuissa laitteissa; toivottavaa olisi, että epästandardissa ympäristössä turvallisuuskriittisen sovelluksen suoritus estettäisiin. Tutkijat mainitsevat myös uudelleenpakkaushyökkäyksen ja huolensa siitä, kuinka helposti sovellusten koodi on purettavissa ja peukaloitavissa. (Botacin et al., 2019)

6 Keskustelu

Tässä tutkielmassa selvitettiin, millaisia tietoturvauhkia verkko- ja mobiilipankkeihin kohdistuu. Tulosten valossa voidaan todeta, että sähköisissä pankkijärjestelmissä ja asiakkaiden toiminnassa olisi vielä parannettavaa. Etenkin mobiilisovelluksista löytyy haavoittuvuuksia, vaikka kehitystä on tapahtunut. Maailmanlaajuisesti tarkasteltuna Euroopassa turvallisuuden taso on kuitenkin korkealla.

Tunnistettujen (ja ennalta tuntemattomien) uhkien torjuminen on oma aiheensa, jonka kanssa pankkien kyberturvallisuuden ammattilaiset taistelevat päivittäin. Tutkielmassa ei syvennytty tähän, mutta tulosten perusteella voidaan kuitenkin tiivistetysti todeta, että pelkästään asiakkaiden tietoisuuden lisääminen ehkäisisi monia rikoksia. Etenkään tietojenkalastelun kohdalla edes huipputurvallinen tekninen toteutus ei auta, jos asiakas haksahtaa huijaukseen ja luovuttaa itse pankkitunnuksensa ulkopuoliselle. Lisäksi virusohjelmien lataaminen ja ohjelmistojen päivittäminen on helppo tapa parantaa käyttäjän tietoturvaa.

Yksi huomionarvoinen asia on, kuinka pankit itse suhtautuvat löydettyihin haavoittuvuuksiin ja muihin tietoturva-aukkoihin. Reaves ja muut (2015) ilmoittivat palveluntarjoajille löytämänsä haavoittuvuudet ja tarjosivat myös hyväksyttyjä käytäntöjä näiden korjaamiseksi, mutta eivät saaneet juuri vastauksia. Jansen & Leukfeldt (2016) huomauttavat, että myös pankeilla on vastuunsa tietoisuuden lisäämisessä ja siten tietoturvan parantamisessa: pankkien tulisi informoida asiakkaitaan mahdollisista hyökkäyksistä ja esimerkiksi muistuttaa, ettei pankin työntekijä koskaan kysyisi arkaluonteista tietoa sähköpostitse tai puhelimitse. Tämän tutkielman kirjoittamisen aikaan ainakin OP-mobiilin kirjautumissivulla oli varoitus OP:n nimissä pankkitunnuksia kalastelevista rikollisista ja OP:n verkkosivuilla julkaistiin laajempi tiedote huijausviesteistä.

Mobiilipankkien tietoturvaa koskevasta luvusta huomataan, että lähteiksi löytyi erityisesti Android-laitteiden turvallisuutta käsitteleviä artikkeleja, mutta ei Applen iOS-käyttöjärjestelmää koskevia. Tälle on ainakin kaksi mahdollista selitystä. Yksi on, että Android-laitteita on yksinkertaisesti tutkittu enemmän, koska niiden määrä on ollut suurempi. Reaves ja muut toteavatkin vuoden 2015 artikkelissaan, että he valitsivat tutkimuskohteeksi Androidin sovellukset, koska sen markkinaosuus oli suurin ja siihen saatavilla olevia sovelluksia oli enemmän. Applen markkinaosuus ei ollut yhtä merkittävä vielä 5–10 vuotta sitten, vaan Android oli selvä ykkönen. Toinen mahdollinen selitys taas on, että Applen tuotteet ovat turvallisempia, joten iOS-laitteiden tietoturvauhkista ei löydy vastaavaa näyttöä. Tämäkin voi kuitenkin johtua laitteiden suosiosta: rikollisten on kannattavampaa iskeä tuotteisiin, joiden markkinaosuus on suurin, joten Applen tuotteet ovat pitempään saaneet olla hyökkäyksiltä rauhassa. Suosion kasvun myötä rikollisten kiinnostus ja haittaohjelmien ynnä muiden uhkien määrä voi kasvaa. Reaves ja muut (2015) huomauttavat, etteivät voi esittää väitteitä iOS-sovellusten turvallisuudesta, ja

Android-sovelluksista löytyneet virheet ovat mahdollisia myös iOS-laitteissa, eivät vain Androidille ominaisia.

Botacin ja muut huomasivat, että globaalien pankkien mobiilisovellukset eri maissa erosivat toisistaan. Sovellusten koodi oli osittain samaa, mutta niiden ydin oli sidottu tukemaan paikallisten asiakkaiden tarpeita, paikallisten tiimien kehittäminä ja pankkiviranomaisten omistamilla varmenteilla allekirjoitettuina. Tämä mahdollistaa asiakaslähtöisemmät tuotteet, mutta johtaa haasteisiin sovellusten hallinnassa, koska tietyssä versiossa havaittuja vikoja ei voida taata saada korjatuksi toisessa, erillisen tiimin ylläpitämässä versiossa. (Botacin et al., 2019) Tämän perusteella kansainvälisten pankkien olisi parempi pitää yksi yhteinen, eri kielille käännetty sovellusversio, mikä vähentäisi haavoittuvuuksien määrää ja siten parantaisi tietoturvaa.

Lähivuosina fintech-yritykset ja palveluiden sähköistyminen tulevat luultavasti lisääntymään. Yle uutisoi heinäkuussa 2023 pankkikonttorien verkoston harvenemisesta. Uutisen julkaisuhetkellä yli 15 % Suomen kunnista oli ilman omaa konttoria, palveluiden keskittyessä suuriin kaupunkeihin. Pankit ovat viime vuosina investoineet digitaalisiin palveluihin vahvasti. Finanssivalvonta on kuitenkin ilmiöstä huolissaan, sillä kaikki asiakkaat eivät voi käyttää digitaalisia kanavia, jolloin palveluiden yhdenvertaisuus ei välttämättä toteudu. (Björklund & Kluukeri, 2023) Jää nähtäväksi, kuinka merkittävästi konttorien määrä tulee lopulta vähenemään ja onko tällä vaikutuksia pankkien turvallisuuteen.

7 Yhteenveto

Pankkiasiointi on muutaman vuosikymmenen aikana siirtynyt yhä vahvemmin sähköiseen muotoon. Verkkopankki on edelleen pitänyt pintansa, vaikka mobiilipankki on nopeasti kasvattanut suosiotaan etenkin nuorempien keskuudessa. Pankkien autentikointikäytännöt vaihtelevat, mutta kiistämättä on selvää, että monivaiheinen, useampaan todennustapaan nojaava kirjautumisprosessi on turvallisempi kuin yksivaiheinen. Kertakäyttösalasanan välittämiseen tekstivestitse liittyy riski, koska viestejä voidaan siepata.

Tietojärjestelmien haavoittuvuudet liittyvät usein SSL/TLS-varmenteiden virheelliseen vahvistukseen, mikä altistaa väliintulohyökkäykselle niin verkko- kuin mobiilipankeissa. Verkkopankeissa merkittävin tietoturvauhka on haittaohjelmat, jotka voivat jopa jäädä käyttäjiltä huomaamatta. Viime vuosien yleisimpiä haittaohjelmia ovat olleet pankkitroijalainen Zeus ja sen variantit. Mobiilipankeissa yksi yleisimmistä haavoittuvuuksista on mahdollisuus ottaa kuvakaappauksia. Lisäksi kolmannen osapuolen muokkaamat haitalliset sovellukset voivat uhata varomattomia käyttäjiä. Android-laitteiden roottaus ei ole suositeltavaa lisääntyneiden turvallisuusriskien takia. Tietojenkalastelu on edelleen suuressa osassa sitä, kuinka rikolliset onnistuvat pääsemään uhrien tileihin ja rahoihin käsiksi.

Lähdeluettelo

Awati, R. (2022). *Hypertext Transfer Protocol Secure (HTTPS)*. TechTarget. https://www.techtarget.com/searchsoftwarequality/definition/HTTPS (Haettu 31.7.2023)

Björklund, S. & Kluukeri, I. (2023). *Pankkikonttoreiden harveneminen jatkuu – Finanssivalvonta jo huolissaan perinteisten palveluiden vähentymisestä*. Yle. https://yle.fi/a/74-20039904 (Haettu 16.8.2023)

Botacin, M., Kalysch, A. & Grégio, A. (2019). The Internet banking [in]security spiral: past, present, and future of online banking protection mechanisms based on a Brazilian case study. *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19),* 1–10. https://doi.org/10.1145/3339252.3340103

Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., Liu, Y. & Xu, L. (2020). An empirical assessment of security risks of global Android banking apps. *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering (ICSE '20)*, 1310–1322. https://doi.org/10.1145/3377811.3380417

Geramiparvar, S. & Modiri, N. (2015). Security as a serious challenge for E-banking: A review of Emmental malware. *International Journal of Advanced Computer Research*, *5*(18), 62–67. https://www.proquest.com/compsci-jour/docview/1718578976/fulltext/26E390F430DD44F8PQ/4?accountid=14242

Helpinen, V. (2022). *Lukuisilta S-pankin tileiltä on viety rahaa laittomasti – Poliisi: maksuvälinepetoksia ainakin 53, tietomurtoja noin 150*. Yle. https://yle.fi/a/3-12623785 (Haettu 18.5.2023)

Hildenbrand, J. (2022). *Everything you need to know about rooting your Android phone.* Android Central. https://www.androidcentral.com/root (Haettu 17.6.2023)

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: a qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79–91. DOI: 10.5281/zenodo.58523

Kaspersky. (2023). *SSL-varmenne – määritelmä ja selitys*. https://www.kaspersky.fi/resource-center/definitions/what-is-a-ssl-certificate (Haettu 20.7.2023)

Kiljan, S., Simoens, K., De Cock, D., van Eekelen, M. & Vranken, H. (2016). A survey of authentication and communications security in online banking. *ACM Computing Services*, *49*(4), 1–35. https://doi.org/10.1145/3002170

Lee, K. & Yim, K. (2023). Vulnerability analysis and security assessment of secure keyboard software to prevent PS/2 interface keyboard sniffing. *Sensors 2023, 23*(7)*,* 3501. https://doi.org/10.3390/s23073501

Lindholm, P. (2022). *Nordeaan kohdistunut kyberhyökkäys oli "poikkeuksellisen hyvin toteutettu", sanoo asiantuntija – hyökkääjän taustoista ei tietoa.* Yle. https://yle.fi/a/3-12340081 (Haettu 20.8.2023)

OP Ryhmä. (2022). *OP Ryhmän toimintakertomus ja tilinpäätös 2022*. https://vuosi.op.fi/siteassets/pdf/2022/op-ryhman-toimintakertomus-ja-tilinpaatos-2022-pdf.pdf

Palmgren, J. (2020). *Laittoman uhkauksen siirtyminen virallisen syytteen alaiseksi on*

oiva päätös pitkälle uralle. Finanssiala. https://www.finanssiala.fi/uutiset/laitto-man-uhkauksen-siirtyminen-virallisen-syytteen-alaiseksi-on-oiva-paatos-pitkalle-uralle/ (Haettu 12.6.2023)

Reaves, B., Scaife, N., Bates, A., Traynor, P. & Butler, K. (2015). Mo(bile) money, mo(bile) problems: analysis of branchless banking applications in the developing world. *Proceedings of the 24th USENIX Security Symposium,* 17–32. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/reaves

TEPA. (2023). *Autentikointi.* TEPA-termipankki. https://termipankki.fi/tepa/fi/haku/autentikointi (Haettu 4.8.2023)

TEPA. (2023). *Haavoittuvuus*. TEPA-termipankki. https://termipankki.fi/tepa/fi/haku/haavoittuvuus (Haettu 9.8.2023)

TEPA. (2023). *Uhka*. TEPA-termipankki. https://termipankki.fi/tepa/fi/haku/uhka (Haettu 9.8.2023)

Wazid, M., Zeadally, S. & Das, A. K. (2019). Mobile banking: evolution and threats: malware threats and security solutions. *IEEE Consumer Electronics Magazine*, *8*(2), 56–60. https://doi.org/10.1109/MCE.2018.2881291

Yli-Huttula, T. (2022). *Suomalaisten pankkien tietoturva on kansainvälisesti korkeatasoista*. Finanssiala. https://www.finanssiala.fi/kolumni/suomalaisten-pankkien-tietoturva-on-kansainvalisesti-korkeatasoista/ (Haettu 18.5.2023)

Zheng, X., Pan, L. & Yilmaz, E. (2017). Security analysis of modern mission critical Android mobile applications. *Proceedings of the Australasian Computer Science Week Multiconference (ACSW '17)*, 1–9. https://doi.org/10.1145/3014812.3014814

Zimba, A. (2022). A bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks. *International Journal of Computer Network and Information Security*, *15*(1), 25–39. https://doi.org/10.5815/ijcnis.2022.01.03