HAAGA-HELIA
ammattikorkeakoulu

Verkkopankkihyökkäykset ja niiden torjunta henkilöasiakkaan näkökulmasta

Anita Cardona

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

23.4.2014

Tekijä tai tekijät Anita Cardona	**Ryhmätunnus tai aloitusvuosi** 2009
Raportin nimi Verkkopankkihyökkäykset ja niiden torjunta henkilöasiakkaan näkökulmasta	**Sivu- ja liitesivumäärä** 37
Opettajat tai ohjaajat Sirpa Marttila	

Opinnäytetyön tavoitteena oli tutkia henkilöasiakkaan verkkopankkiin kohdistuvia hyökkäyksiä Microsoft Windows -käyttöjärjestelmän pöytätietokoneissa ja kannettavissa tietokoneissa, koska huijaamiset kohdistuvat eniten Microsoft Windows -käyttöjärjestelmään. Tavoitteena oli myös koota tietoturvaohjeistus henkilöasiakkaille.

Kiinnostus opinnäytetyön aiheeseen syntyi siitä, että opinnäytetyön kirjoittaja on työntekijänä eräässä pankin yksikössä, jossa yhtenä toimintona on nykyään verkkopankkiin kohdistuvat hyökkäykset. Työ ei ollut pankin toimeksianto johtuen pankkisalaisuudesta. Aihe on myös ajankohtainen henkilöasiakkaille.

Tutkimusongelmana oli selvittää, missä tapauksissa pankit korvaavat verkkopankkihyökkäyksistä aiheutuneita henkilöasiakkaan rahallisia menetyksiä ja milloin ei maksupalvelulain mukaan. Tavoitteena oli myös kartoittaa, millaisia verkkopankkiin kohdistuvia hyökkäyksiä on ja miten ne toimivat. Lisäksi tavoitteena oli kartoittaa, miten SSL-salaus ja käyttäjän todentamismenetelmät toimivat sekä miten hyökkäyksiä voi torjua.

Syksyn 2013 ja kevään 2014 aikana yksilötyönä toteutetun työn tutkimusmenetelmä oli kvalitatiivinen kirjallisuuskatsaus. Lähdeaineistoina käytettiin alan kirjallisuutta, lehtiartikkeleita, eri instituutioiden Internet-sivustoja ja muutamaa muuta Internet-lähdettä alan kirjallisuuden vähyyden vuoksi.

Teoriataustassa käydään läpi verkkopankkiasioinnin kehitystä 2000-luvulla, maksupalvelulain tuomia lisävastuumuutoksia henkilöasiakkaan huolellisuusvelvoitteeseen maksuvälineisiin kuuluvien pankkitunnusten säilyttämisessä ja pankkien korvausvastuuta henkilöasiakkaille väärinkäytöstapauksissa. Lisäksi työssä selvitetään tietoverkkorikollisten toiminta- ja huijaamistapoja sekä SSL-salausta että käyttäjän todentamismenetelmiä. Tietoturvaohjeistuksessa käydään läpi maksun lisävahvistusta, palomuuria, virustentorjuntaohjelmistoja ja ohjeistuksia.

Tutkimustulosten johtopäätöksessä todetaan, että tietoturvasta huolehtiminen on tärkeää. Tietoja varastavat ohjelmat ovat kehittyneitä, eivätkä virustentorjuntaohjelmat anna sataprosenttista suojaa.

Asiasanat
Verkkohyökkäykset, verkkourkinta, haittaohjelmat, sähköinen tunnistaminen, verkkopankit

HAAGA-HELIA
University of Applied Sciences

Abstract

23 April 2014

Degree Programme in Information Technology

Authors Anita Cardona	**Group or year of entry** 2009
The title of thesis Attacks on online banking and their prevention from the point of view of private customers	**Number of pages and appendices** 37
Supervisor(s) Sirpa Marttila	

The aim of the thesis was to examine private customers' online banking attacks in the Microsoft Windows operating system in desktop and laptop computers, because frauds are targeted mostly against Microsoft Windows operating system. The aim was also to gather security guidelines for private customers.

The interest in the topic of the thesis arose when the author of the thesis works as an employee in one bank unit, where one function is online banking attacks nowadays. The thesis was not commissioned by the bank mandate due to bank secrecy. The issue is also topical for private customers.

The research problem was to find out in which cases banks pay for financial losses caused by online banking attacks and when not according to the Payment Services act. The aim was also to survey what kind of private customers' online banking attacks there are, and how they work. In addition, the aim was to survey how an SSL encryption and user authentication method works as well as how attacks can be prevented.

The research method was a qualitative review of the literature and the study was conducted during autumn 2013 and spring 2014. The source material consisted of relevant literature, journal articles, various institutions' Internet pages and a few other Internet sources because of the lack of literature. The theoretical background discusses the online banking trend in the 2000s, additional responsibilities brought by the Payment Services Act for private customers' duty to take care of netbank access codes and banks' liability for private customers in misuse cases. In addition, the thesis deals with cyber criminals' method and swindles as well as SLL encryption and user authentication methods. In the instructions for security guidelines additional payment confirmation, firewalls, anti-virus software and guidelines are examined.

As a conclusion it can be stated that taking care of information security is important. Data-stealing programs are advanced and anti-virus software does not provide hundred percent protection.

Key words
Network attacks, phishing, malwares, e-identification, online banking

Sisällys

1 Johdanto

Tietoverkkorikollisten uhreiksi on joutunut 9 % maailman väestöstä. Uhreja on jopa yli miljoona päivittäin. Symantecin 24 maan tutkimustulosten mukaan suurin riski joutua uhriksi on paljon Internetissä aikaa viettävillä aikuisviihdepalveluita käyttävillä alle 30-vuotiailla miehillä. Myös kokemattomat, väärillä henkilötiedoilla esiintyvät ja langattomia yhteyksiä käyttävät joutuvat usein uhreiksi. Miespuolisia uhreja on jopa 71 % ja naisia 63 %. Jopa 41 %:lla ei ole ajan tasalla olevaa virustentorjuntaohjelmaa tietokoneellaan, eikä tietokonetta ole suojattu salasanalla. (Haasio 2013, 14.)

Monia verkkopankin henkilöasiakkaita huolettaa Internetin ja oman verkkopankin tietoturvallisuus. Kaikki henkilöasiakkaat eivät tiedä mitä verkkopankkihyökkäykset ovat ja miten niitä voi yrittää torjua ennalta hyökkäysten minimoimiseksi. Osa tietoverkkorikollisten tekemistä verkkopankkihuijauksista onnistuu, koska asiakkaat erehtyvät pitämään tietoverkkorikollisten Internet-linkkejä ja -sivustoja aitoina. On myös käyttäjiä, joilla ei ole ajantasaista virustentorjuntaohjelmaa tietokoneellaan, verkkopankkitunnuksista ei pidetä huolta tai tietokoneen sisäänkirjautumisessa ei käytetä salasanaa.

Tietoverkkorikollisten käyttämät menetelmät kehittyvät jatkuvasti vaikeuttaen virustentorjuntaa, eikä verkkopankin henkilöasiakas välttämättä huomaa rahojensa hävinneen verkkopankin istunnon aikana edes tilin saldosta. Haittaohjelma on päässyt asiakkaan tietokoneeseen esimerkiksi henkilöasiakkaan avatessa sähköpostiviestistään viruksen sisältävän linkin tai surffaillessaan saastuneella Internet-sivustolla.

Finanssialan Keskusliitto ry:n (2012a) mukaan 81 % suomalaisista maksaa laskunsa verkkopankissa. Verkkopankkiasiakkaiden haittana voivat olla tietokoneilta pankkitunnuksia varastavat erilaiset haittaohjelmat. Näistä verkkopankkiin kohdistuvista hyökkäyksistä on kuultu julkisuudessa erityisesti viime lähivuosina 2011, 2012 ja 2013 useaan otteeseen median tiedotuskanavissa. Finanssivalvonnan mukaan (Ranta 2013c) suomalaisten pankkitileiltä varastettiin noin 800 000 euroa vuonna 2012. Varkaudet kohdistuivat 300 henkilöön. Näistä rahoista noin puolet saatiin takaisin. Määrät ovat kuitenkin pieniä verrattuna verkkopankin sopimus- ja tapahtumamääriin. Viimeisinä aiheina on

ollut työn kirjoittamisen aikana Citadel-niminen Zeus-verkkopankkihuijaus-virukseen perustuva haittaohjelma MTV Uutisissa vuoden 2013 loppupuolella.

Tietotekninen kehitys ja siten elektroniset tiedonsiirtoyhteydet ovat kasvattaneet Internetin kautta tapahtuvien pankkipalveluiden tarjontaa ja asiakkaiden jokapäiväistä pankkiasiointia. Verkkopankissa tehtäviä tilisiirtoja voidaan tehdä nykyään periaatteessa missä vain ajasta ja paikasta riippumatta erilaisilla laitteilla. Pankeilla on käytössä SSL-salaus verkkopankin istunnoissa sekä asiakkaan todentamismenetelmät sisäänkirjautumisissa. Käytössä on myös matkapuhelimen tekstiviestillä tapahtuva maksun lisävahvistus. Asiakkaita koskevat huolellisuusvelvoitteet maksuvälineisiin kuuluvien pankkitunnusten säilyttämisessä ja oman tietokoneen tietoturvasta huolehtiminen, joilla on vaikutusta pankkien maksamiin korvauksiin väärinkäytöstapauksissa.

Tutkittava aihe on opinnäytetyön kirjoittajalle mielenkiintoinen ja kiinnostava, koska kirjoittaja on erään pankin työntekijänä yksikössä, jossa yhtenä pankin toimintona on nykyään verkkopankki ja siihen kohdistuvat verkkopankkihyökkäykset. Tämä opinnäytetyö ei ole pankin toimeksianto, eikä tätä työtä tehdä pankkien näkökulmasta johtuen pankkisalaisuudesta. Tämä tutkimustyö voi kuitenkin hyödyttää kirjoittajan työnantajaa ja sen työntekijöitä verkkopankin henkilöasiakkaiden lisäksi sekä muita opinnäytetyön aiheesta kiinnostuneita lukijoita. Lisäksi tällä tutkimuksella voi löytyä ajankohtaisempaa tietoa henkilöasiakkaille mitä kirjallisuudesta ei vielä löydy. Tutkittavana aiheena verkkopankkihyökkäykset on haasteellinen, koska pankit eivät ole julkaisseet omia tilastotietojaan verkkopankkihyökkäyksistä, eikä alan kirjallisuutta ole paljoa.

1.1 Tutkimuksen tavoitteet ja rajaus

Tämän tietoturvaan liittyvän opinnäytetyön tavoitteena on lisätä henkilöasiakkaiden yleistä tietoisuutta verkkopankkihyökkäyksistä sekä verkkorikollisten toimintatavoista. Tutkimustavoitteena on selvittää, missä tapauksissa pankit korvaavat verkkopankkihyökkäyksistä aiheutuneita henkilöasiakkaan rahallisia menetyksiä ja milloin ei. Tavoitteena on myös kartoittaa, millaisia henkilöasiakkaan verkkopankkiin kohdistuvia hyökkäyksiä on ja miten ne toimivat. Näiden lisäksi tutkimustavoitteena on myös kartoittaa, miten SSL-salaus ja käyttäjän todentamismenetelmät toimivat. Tuotoksena on koota

yhteen eri tietolähteisiin perustuen henkilöasiakkaille tietoturvaohjeistus, miten henkilöasiakas voi mahdollisesti tunnistaa ja torjua näitä verkkopankkihyökkäyksiä omilla toimenpiteillään.

Opinnäytetyö on rajattu koskemaan Microsoft Windows -käyttöjärjestelmän pöytätietokoneisiin ja kannettaviin tietokoneisiin kohdistuviin henkilöasiakkaiden verkkopankkihyökkäyksiin Suomessa. Petteri Järvisen mukaan tietoverkkorikollisten on helpompi hyökätä näihin tietokoneisiin, sillä ne eivät ole niin riisuttuja kuin älypuhelimet ja tablettitietokoneet (Väkimies 2013). Työn ulkopuolelle on rajattu muut käyttöjärjestelmät, puhelinpankkipalvelut, mobiiliverkkopankki, tablettitietokoneet, älypuhelimet ja langattomat verkot. Myös yritysasiakkaat on rajattu tutkimuksesta pois, vaikka tietyt perusasiat koskettavat yhtä lailla heitä kuin henkilöasiakkaita. Tarkoituksena ei ole tutkia verkkopankkia syvällisesti, vaan ainoastaan käyttäjän todentamismenetelmiä ja verkkopankin tietoturvaan liittyvää SSL-salausta.

1.2 Tutkimuskysymykset

Alla on lueteltuna opinnäytetyölle asetetut tutkimuskysymykset, joita työssä pyritään selvittämään:

- missä tapauksissa pankit korvaavat verkkopankkihyökkäyksistä aiheutuneita henkilöasiakkaan rahallisia menetyksiä ja milloin ei maksupalvelulain mukaan
- millaisia henkilöasiakkaan verkkopankkiin kohdistuvia hyökkäyksiä on ja miten ne toimivat
- miten SSL-salaus ja käyttäjän todentamismenetelmät toimivat
- miten henkilöasiakas voi mahdollisesti tunnistaa ja torjua ennalta näitä verkkopankkihyökkäyksiä vastaan omilla toimenpiteillään.

1.3 Tutkimusmenetelmä

Tämän yksilötyönä toteutetun opinnäytetyön tutkimusmenetelmä on kvalitatiivinen kirjallisuuteen perustuva katsaus. Työssä on käytetty lähdeaineistoina alan kirjallisuutta,

lehtiartikkeleita, eri instituutioiden Internet-sivustoja ja muutamaa muuta Internet-lähdettä alan kirjallisuuden vähyyden vuoksi.

1.4 Opinnäytetyön rakenne

Työn toinen luku käsittelee tietoteknisen kehityksen tuomia vaikutuksia verkkopankkiin 2000-luvulla. Luvussa käydään myös läpi lainsäädännöllisiä kohtia, jotka henkilöasiakkaan on hyvä huomioida käyttäessään maksuvälineisiin kuuluvia pankkitunnuksia. Kolmannessa luvussa tutustutaan tietoverkkorikollisten toimintatapoihin ja käydään läpi verkkopankkeihin kohdistuvia hyökkäystapoja. Neljännessä luvussa käydään läpi SSL-salausta tietoliikenteen salaamisessa, varmennetta Internet-sivuston tunnistamisessa ja henkilöasiakkaan todentamismenetelmiä verkkopankin käytössä. Viidennessä luvussa käydään läpi henkilöasiakkaan tietoturvaohjeistusta hyökkäysten minimoimiseksi. Viimeinen eli kuudes luku sisältää opinnäytetyöhön liittyvän pohdinnan. Tämä sisältää tutkimuksen yhteenvedon eli tutkimustulokset ja johtopäätökset, työn etenemisen ja oman oppimisen sekä työn tuloksen hyväksikäyttömahdollisuudet.

1.5 Käsitteitä

Yhtäläisyyden vuoksi työssä käytetään nimitystä verkkopankki, jota suurin osa suomalaisista pankeista käyttää lukuun ottamatta OP Pohjolan ja LähiTapiolan verkkopalvelua sekä Ålandsbankenin Internetkonttoria. Verkkopankkiin sisäänkirjautumisessa ja maksutapahtumien vahvistuksissa käytetään maksuvälineenä pankkitunnuksia. Yhdessä käyttäjätunnuksen kanssa käytetään tunnusta, josta yhtäläisyyden mukaan käytetään nimitystä tunnusluku. Tunnusluku löytyy tunnuslukukortista. Ainakin Nordea, S-pankki, Säästöpankki ja Ålandbanken käyttävät nimitystä tunnusluku ja tunnuslukutaulukko, LähiTapiola tunnuslukua ja tunnuslukulistaa, OP Pohjola avainlukua ja avainlukulistaa, Aktia turvalukua ja avaintunnuskorttia sekä Säästöpankki avainlukua ja avainlukukorttia.

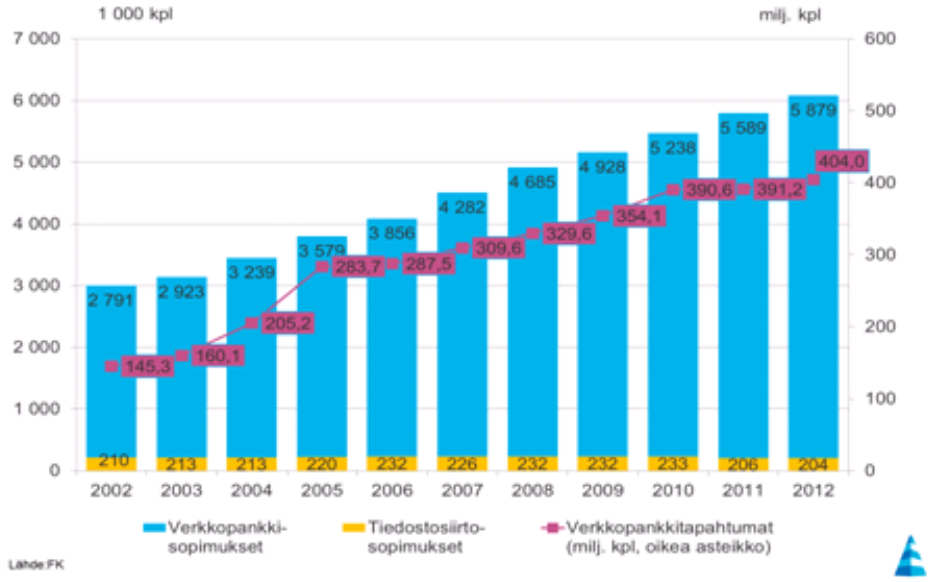
2 Verkkopankkiasioinnin kehitys ja lainsäädäntö

Tässä luvussa käydään läpi verkkopankkisopimusten ja verkkopankkitapahtumien kasvukehitystä 2000-luvulla. Lisäksi käydään läpi Euroopan Unionin maksupalveludirektiiviin perustuvan maksupalvelulain tuomia huolellisuusvelvoitteeseen liittyviä vastuita henkilöasiakkaille verkkopankin maksuvälineiden käytössä ja pankin korvausvastuuta väärinkäytöstapauksissa.

2.1 Verkkopankkiasioinnin kehitys

Suomalaiset ovat maailman kärkipäässä sähköisten pankkipalveluiden käytössä. Tietotekninen kehitys on vaikuttanut pankkien maksujärjestelmien tason kohentumiseen ja suomalaisten nykypäivän pankkiasioiden hoitamiseen. Pankkipalveluita on mahdollista käyttää konttoreiden lisäksi Internet- ja puhelinpankkipalveluiden välityksellä. Internetin verkkopankkipalvelut ovat kehittyneet tietoteknistymisen myötä nopeasti. Samalla näiden palveluiden käyttö, saatavuus sekä asiakkaiden ja pankkien väliset verkkopankkien sopimusmäärät ovat kasvaneet. (Kontkanen 2011, 13, 15, 72–74.) Verkkopankissa laskujen maksamisen teki jo 81 % suomalaisista vuonna 2012 tarkoittaen lähes kaikkia 18–44-vuotiaita ja 46 % 65–74-vuotiaista. (Finanssialan Keskusliitto ry 2012a.) Verkkopankissa tehtävät tilisiirrot siirtyvät tililtä toiselle nopeasti ja edullisesti. Tilisiirtoja voidaan tehdä periaatteessa missä vain ajasta ja paikasta riippumatta sähköisesti konttoriasioinnin sijasta. Asiakkaat käyttävät verkkopankissa eniten laskujenmaksupalveluita ja seuraavat tilitapahtumia sähköisiltä tiliotteilta. (Kontkanen 2011, 13, 72–74.)

Kuviosta 1 nähdään Finanssialan Keskusliitto ry:n (2013b) tilasto henkilöasiakkaiden verkkopankkisopimusten, yritysasiakkaiden tiedonsiirtosopimusten ja verkkopankkitapahtumien kasvukehitys vuosina 2002-2012. Henkilöasiakkaiden ja pankin välisiä verkkopankkisopimuksia oli lähes 5,9 miljoonaa vuoden 2012 lopussa. Sopimusmäärät ovat kaksinkertaistuneet vuoteen 2002 verrattuna. Tilastossa on eriteltynä myös yritysasiakkaiden ja pankin väliset tiedonsiirtosopimukset. Kaikkiaan verkkopankkitapahtumia oli tehty vuonna 2012 jo 404 miljoonaa. Tämä on lähes kolminkertainen määrä verrattuna vuoteen 2002.



Kuvio 1. Henkilöasiakkaiden verkkopankkisopimusten, yritysasiakkaiden tiedonsiirto-sopimusten ja verkkopankkitapahtumien kasvukehitys vuosina 2002-2012 (Finanssialan Keskusliitto ry 2013b, 12)

2.2 Käyttäjän huolellisuusvelvoite

Euroopan Unionin maksupalveludirektiiviin perustuva uusi maksupalvelulaki tuli voimaan Suomessa 1.5.2010. Lain noudattamista valvovat Finanssivalvonta ja kuluttaja-asiamies. Uusi laki korvaa tilisiirtolain vuodelta 1999 (Maksupalvelulaki 30.4.2010/290, 87 §; Luottokunta 2013). Maksupalvelulaki toi mukanaan mm. lisävastuuta pankin henkilöasiakkaiden huolellisuusvelvoitteeseen. Samalla henkilöasiakkaiden asema parani omavastuussa maksuvälineiden oikeudettomassa käytössä aikaisemmasta ylärajattomasta vastuusta enintään 150 euroon. (Luottokunta 2013; Maksupalvelulaki (30.4.2010) 62 §.)

Asiakkaan vastuuseen kuuluu pitää huolta maksuvälineistään (Maksupalvelulaki (30.4.2010) 53 §), joihin pankkitunnukset kuuluvat. Nämä tunnukset tulee pitää erillään toisistaan eikä niitä saa luovuttaa edes perheenjäsenille. Tunnukset eivät saa olla varkaiden ulottuvilta. (Säästöpankki 2013.) Asiakkaan tulee ilmoittaa tunnusten katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä viivytyksettä pankilleen (Maksupalvelulaki (30.4.2010) 54 §). Asiakkaan vastuu lakkaa asianmukaisen

ilmoituksen jälkeen. Tällöin pankin tulee estää maksuvälineen käyttö (Maksupalvelulaki (30.4.2010) 56 §; 62 §).

2.3 Pankin korvausvastuu

Pankit korvaavat henkilöasiakkaan menettämiä rahoja väärinkäytöissä tapauskohtaisesti vain, jos henkilöasiakas on noudattanut huolellisuusvelvoitettaan ja huolehtinut tietokoneensa virusturvasta (OP-Pohjola-ryhmä 2013c), ilmoittanut pankkitunnusten katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä pankille viivytyksettä (Maksupalvelulaki (30.4.2010)70 §). Henkilöasiakkaiden osalta pankilta saatava korvaus tarkoittaa tällöin asiakkaan rahallisia menetyksiä 150 euron omavastuuosuuden jälkeen. Pankki ei korvaa henkilöasiakkaan rahanmenetyksiä, jos henkilöasiakas on menetellyt törkeän huolimattomasti. (Säästöpankki 2013.) Pankki joutuu korvaamaan asiakkaalle pankin huolimattomuudesta johtuvan välillisen vahingon (Maksupalvelulaki (30.4.2010) 69 §).

3 Verkkopankkihyökkäykset

Tämän luvun tavoitteena on tuoda verkkopankin henkilöasiakkaiden tietoisuuteen tietoverkkorikollisten toiminta- ja huijaustapoja verkkopankkitunnusten varastamisessa.

3.1 Tietoverkkorikollisten toimintatapoja

Tietoverkkorikolliset ovat joutuneet muuttamaan toimintatapojaan sähköisten palveluiden kehittyessä. Nykypäivän verkossa tapahtuva rikollinen toiminta on usein verkostoitunutta, koska tietoverkkorikollisilta vaaditaan yhä enemmän erityisosaamista. Tietoverkkorikollisten toiminta on muuttunut harrastelusta ammattimaiseksi ja kansainväliseksi. Kansainvälinen toiminta on riippumatonta valtioiden ja oikeusjärjestelmien rajoista. (Viestintävirasto Kyberturvallisuuskeskus 2010, 2.) Tämä rajoittaa Suomen poliisia ulkomailta tulevissa huijaustapausten selvittelyissä ja rahojen takaisinsaanneissa asiakkaiden tileille poliisin toimivaltuuksien puuttuessa ulkomailla. (Poliisi 2014a.)

Tietoverkkorikollisia motivoi välitön tai välillinen taloudellinen hyöty varastamalla sekä verkkopankin henkilöasiakkaan pankkitunnuksia että Internet-selaimella käytettävien verkkolomakkeiden sisältöjä erilaisilla haittaohjelmilla kuten phishing verkkourkinnalla luvattomasti. Välitön hyöty voi olla taloudellista, ja välillinen asiakastietojen hyödyntämistä muissa rikollisissa toiminnoissa. (Viestintävirasto Kyberturvallisuuskeskus 2010, 1, 4; Linna 2012, 2.) Tietoverkkorikollinen voi saada suuria taloudellisia hyötyjä jo muutamasta onnistuneesta (Viestintävirasto Kyberturvallisuuskeskus 2010, 19) haittaohjelman avulla tehdystä hyökkäyksestä käyttämällä asiakkaalta varastettuja tietoja joko itse tai myymällä niitä eteenpäin (Poliisi 2014b). Tietoverkkorikolliset käyttävät Internetiä ja sähköpostia suurien ihmismäärien tavoittamiseen huijaamalla henkilöasiakkaita saadakseen henkilöasiakkaan verkkopankkitunnukset vetoamalla esimerkiksi hoitamattomaan maksuun, uusimis- tai muutosasiaan. (Poliisi 2014a.) F-Securen tutkimusjohtaja Mikko Hyppösen mukaan tietoverkkorikolliset kohdistavat hyökkäyksensä asiakkaiden tietokoneisiin, koska ne eivät ole niin suojattuja kuin pankkien järjestelmät (Hamunen 2012).

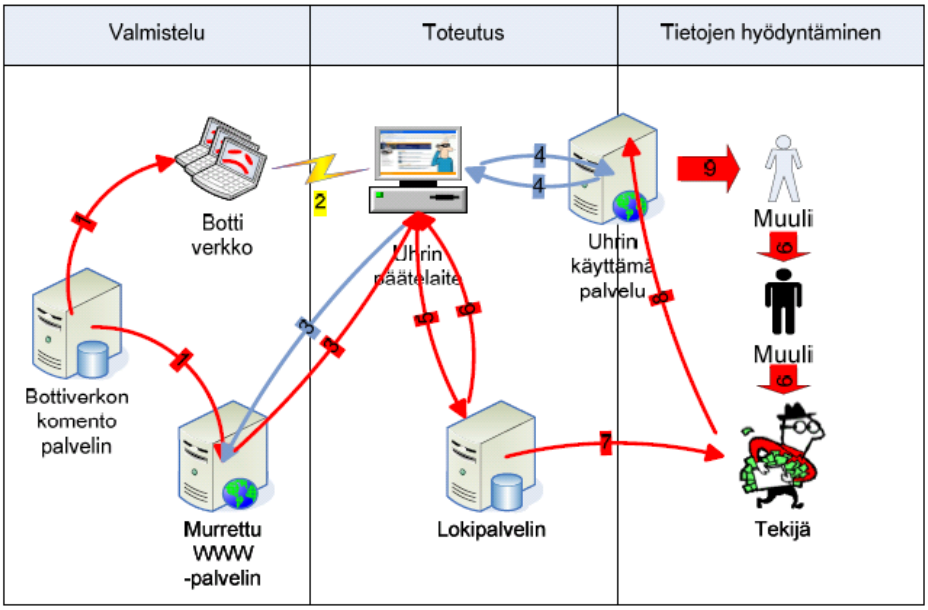
Erityisesti vanhoissa Microsoft Windows -käyttöjärjestelmäversioissa on suuri tietoturvariski. Tätä haavoittuvuutta tietoverkkorikolliset voivat käyttää hyväkseen haittaohjelmilla ja viruksilla. Esimerkiksi Microsoft Windows XP -käyttöjärjestelmän automaattiset tietoturvapäivitykset tietoturva-aukkoja vastaan päättyivät 8.4.2014. Tämä tarkoittaa haittaohjelmien tartuntariskin kasvamista. (Leppänen, 2014.) Tästä eivät kaikki tietokoneen käyttäjät ole olleet tietoisia Helsingin Sanomien mukaan. Suomessa kyseistä versiota on vielä käytössä noin 17 %:lla tietokoneissaan. (Halminen 2014, 17.) Samalla päättyi Internet Explorer -selaimen version 8 tuki sekä Windows XP:n uusien Microsoft Security Essentias lataukset viruksia, vakoiluohjelmia ja muita haittaohjelmia vastaan. (Microsoft 2014.) Muutokset tarkoittavat henkilöasiakkaille tietoturvan osalta Microsoft Windows -käyttöjärjestelmän tai toisen käyttöjärjestelmän kuten Linuxin ostamista (Leppänen 2014).

Microsoft Windows -käyttöjärjestelmän ja sovellusohjelmistojen tietoturva-aukkoja käytetään hyväksi haittaohjelmissa (Kiianmies 2010, 729). Myös Internet-selainten ja selainten laajennuksista löytyviä tietoturva-aukkoja käytetään hyväksi asettamalla haittaohjelma Internet-sivustolle esimerkiksi tietomurron yhteydessä (Järvinen 2012, 183). Selaimen toimintaa laajentavia lisäohjelmia ovat esimerkiksi ActiveX komponentit vuorovaikutteisten toimintojen tuottamiseen Internet-sivuilla (Kiianmies 2010, 781), multimedialaajennuksissa käytettävä Adoben Flash, pdf-tiedostojen lukemiseen tarkoitettu Adobe Reader ja joissain sovelluksissa ja Internet-sivustoilla käytettävä Java. Jos Javaa ei tarvita, sen voi poistaa käytöstä Ohjauspaneelista. (Järvinen 2012, 183–185, 187.)

Tietoverkkorikolliset ostavat pankkitroijalaisia erityisesti Itä-Euroopasta. Ohjelman mukana tulevan ohjeistuksen avulla pankkitroijalainen voidaan räätälöidä tunnistamaan suomalainen verkkopankki. (Järvinen 2012, 64; Ranta 2013b.) Määrittelyä varten tarvitaan vain pankkikohtainen kuvaustiedosto (Järvinen 2012, 64). Tietoverkkorikollinen voi ostaa haittaohjelman kirjoittajalta tietojen varastamiseen tarkoitetun uuden haittaohjelman tai muokatun version olemassa olevasta haittaohjelmasta, jota virustorjuntaohjelmistot eivät vielä tunnista (Viestintävirasto Kyberturvallisuuskeskus 2010, 3–4). Haittaohjelman levittämiseen uhrien tietokoneille voidaan esimerkiksi Viestintäviraston Kyberturvallisuuskeskuksen (2010, 4) mukaan käyttää bottiverkkoa, murrettua WWW-palvelinta, roskapostia tai vertaisverkossa jaettavaa tiedostoa, johon haittaohjelma on

piilotettu. Haittaohjelmat voivat tarttua tietokoneelle sähköpostin ja murrettujen verkkosivustojen lisäksi myös esimerkiksi muistitikun kautta (Hjelt 2014).

Haittaohjelman avulla tehtävään tietojen varastamiseen kuuluu eri vaiheita. Kuviossa 2 numeroidut vaiheittain etenevät punaiset nuolet esittävät haitallista verkkoliikennettä ja siniset uhrin tietoliikennettä. Valmisteluvaiheessa tietoverkkorikollinen toimittaa vakoiluohjelman murretulle WWW-palvelimelle (1). Samalla bottiverkolle annetaan käsky aloittaa roskapostiviestien lähettäminen murretulle WWW-palvelimelle (1). Toteutusvaiheessa uhri avaa roskapostiviestistä linkin murretulle WWW-palvelimelle, josta asentuu uhrin päätelaitteelle eli tietokoneelle vakoiluohjelma (3). Vakoiluohjelma seuraa uhrin käyttämiä palveluita Internetissä tämän tietämättä seurannasta (4). Vakoiluohjelma lähettää varastamansa tiedot uhrin tietokoneelta etukäteen määritetylle usein ulkomailla sijaitsevalle lokipalvelimelle (5). Tietoverkkorikollinen voi käyttää lokipalvelinta myös komentopalvelimena haittaohjelman päivittämisessä tai käskiessä haittaohjelmaa tekemään halutun toimenpiteen kuten tietojen varastamisen tai roskapostiviestin lähettämisen (6). Tietoverkkorikollinen noutaa varastetut tiedot lokipalvelimelta (7) ja käyttää kerättyjä tietoja hyväksi uhrin käyttämässä verkkopankissa (8). Tekijä häivyttää jälkensä kierrättämällä palvelun kautta hankkimansa hyödykkeet muulien kautta (9). (Viestintävirasto Kyberturvallisuuskeskus 2010, 6–7.)



Kuvio 2. Esimerkki tietojen varastamisen vaiheista (Viestintävirasto Kyberturvallisuuskeskus 2010, 6)

Tietoverkkorikolliset voivat käyttää muulina toimivia henkilöitä välikätenä laittomasti hankittujen rahojen siirroissa. Muuli nostaa saamansa rahat välittömästi tililtään ja toimittaa rahat edelleen saamansa ohjeistuksen mukaan eteenpäin esimerkiksi toiseen maahan. (Poliisi 2014c.) Käyttämällä jopa useaa muulia tietoverkkorikolliset pyrkivät välttämään kiinnijäämistä ja hankaloittamaan rikosten selvittämistä (Viestintävirasto Kyberturvallisuuskeskus 2010, 5; Poliisi 2014c). Muulit eivät useinkaan itse tiedä toimintansa olevan rikollista (Viestintävirasto Kyberturvallisuuskeskus 2010, 5).

3.2 Huijaaminen

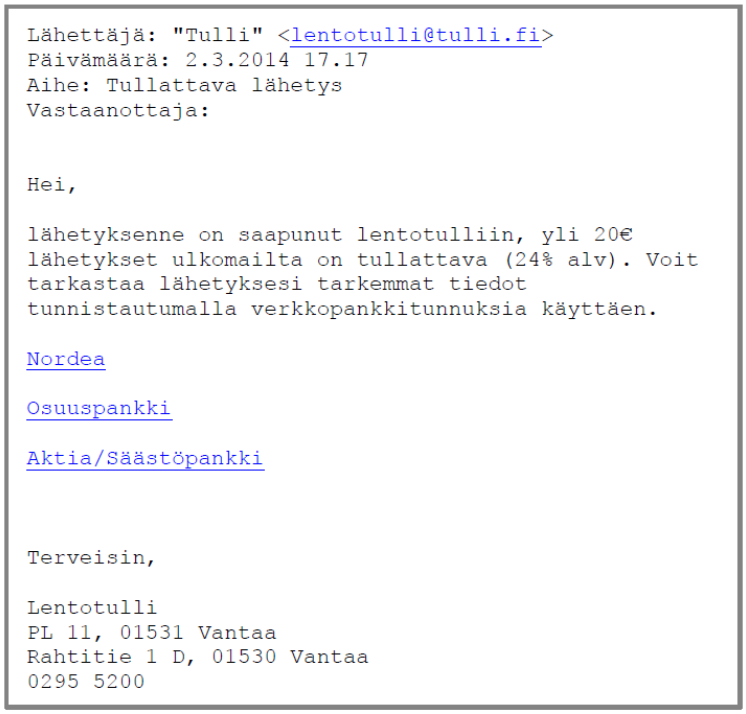
Finanssivalvonnan mukaan (Ranta 2013c) Suomeen kohdistuvissa verkkopankkihyökkäyksissä on tapahtunut huomattava muutos vuosina 2012 ja 2013. Suomalaisten pankkitileiltä varastettiin noin 800 000 euroa vuonna 2012. Varkaudet kohdistuivat 300 henkilöön. Näistä rahoista noin puolet saatiin takaisin. Vuonna 2013 Finanssivalvonnan tiedossa oli vain yksi 5 000 euron varkaustapaus, jonka pankki korvasi asiakkaalle. Hyökkäysyrityksiä oli yli 100 elokuun loppuun mennessä vuonna 2013. Tekstiviesteillä tehtävät maksun lisävahvistukset ovat vähentäneet onnistuneita huijausyrityksiä.

Haasio (2013, 38) jakaa huijaukset sähköpostitse tapahtuviin ja teknisten sovellusten avulla toteutettaviin huijauksiin. Sähköpostitse tapahtuvien huijausten tavoitteena on houkutella henkilöasiakas antamaan pankkitunnukset tai menemään tietylle Internet-sivustolle. Teknisten sovellusten, kuten troijalaisen vakoiluohjelman, tarkoituksena on vakoilla pankkitunnuksia. Verkkohuijaukset tapahtuvat yleensä sähköpostitse. Huijausviestejä lähetetään myös sosiaalisessa mediassa kuten Facebookissa (Kerkelä 2014a).

Huijaamiseen tarkoitettujen sähköpostiviestien määrät lisääntyvät. Huijausviestejä on lähetetty muun muassa pankkien, poliisin ja tunnettujen henkilöiden nimissä pankkitunnusten tietojen kalasteluissa. Sähköpostiviestien linkeistä avautuu aidoilta näyttävät huijaussivustot. (Kerkelä 2014a.) Keväällä 2014 huijausviestejä lähetettiin ainakin Itellan, Perintäpalvelun, Postin, Tullin ja Verohallinnon nimissä (Viestintävirasto Kyberturvallisuuskeskus 2014b). Tietoverkkorikolliset onnistuivat huijaamaan asiakkailta ainakin 50 000 euron edestä pikaluottoja 23 uhrin pankkitunnuksilla. Henkilöasiakkaiden

rahalliset menetykset ovat yleensä muutamista kympeistä kymmeniin tuhansiin euroihin. (Kerkelä 2014a; Kerkelä 2014b.)

Alla kuviossa 3 on esimerkki Tullin nimissä lähetetystä huijaussähköpostiviestistä. Lähettäjän sähköpostiosoite on väärennetty näyttämään siltä, kuin viesti tulisi lentotulli@tulli.fi. Viestissä pyydetään tunnistautumaan pankkitunnuksilla. (Viestintävirasto Kyberturvallisuuskeskus 2014a.)



Lähettäjä: "Tulli" <lentotulli@tulli.fi>
Päivämäärä: 2.3.2014 17.17
Aihe: Tullattava lähetys
Vastaanottaja:

Hei,

lähetyksenne on saapunut lentotulliin, yli 20€ lähetykset ulkomailta on tullattava (24% alv). Voit tarkastaa lähetyksesi tarkemmat tiedot tunnistautumalla verkkopankkitunnuksia käyttäen.

Nordea

Osuuspankki

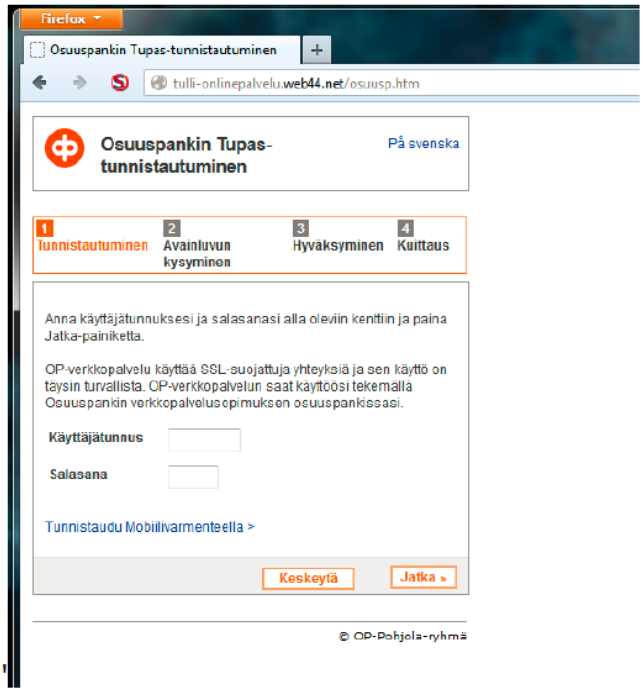
Aktia/Säästöpankki

Terveisin,

Lentotulli
PL 11, 01531 Vantaa
Rahtitie 1 D, 01530 Vantaa
0295 5200

Kuvio 3. Esimerkki Tullin nimissä lähetetystä huijaussähköpostiviestistä (Viestintävirasto Kyberturvallisuuskeskus 2014a)

Tullin nimissä lähetetyissä huijausviesteissä käytettiin myös väärennettyjä Tupas-tunnistautumissivuja. Seuraavan sivun kuvion 4 esimerkistä nähdään väärennetty Osuuspankin Tupas-tunnistautumiseen liittyvä huijaussivusto selaimen osoiteriviltä. Internet-selaimen osoiteriviltä puuttuu SSL-salattu yhteys ja lukittu lukko-ikoni. Lisäksi sivusto ei viittaa pankkiin. (Viestintävirasto Kyberturvallisuuskeskus 2014a.)



Kuvio 4. Osuuspankin väärennetty Tupas-sivusto. Internet-selaimen osoiteriviltä puuttuu SSL-salattu yhteys ja lukittu lukko-ikoni. Sivusto ei viittaa pankkiin. (Viestintävirasto Kyberturvallisuuskeskus 2014a)

Tietojen varastamisessa käytetään erilaisia haittaohjelmia kuten viruksia, matoja, Troijan hevosia, vakoilu-, mainos- ja urkintaohjelmia, rootkit-ohjelmia, selaimen kaappaajia, näppäilytallentimia ja takaovia (Kiianmies 2010, 729.) Toistaiseksi haittaohjelmien kirjoittajat kohdistavat virukset lukumäärällisesti eniten Windows-käyttöjärjestelmiin (Kiianmies 2010, 731). Haittaohjelmat on suunniteltu toimimaan vain tietyssä käyttöjärjestelmässä (Flyktman 2011, 324). Tunnetuin haittaohjelmatyyppi on virus, joita mm. takaovet, Troijan hevoset ja vakoiluohjelmat ovat (Flyktman 2011, 324–325).

Vakoiluohjelma on yksi yleisimmistä tavoista luottamuksellisten tietojen keräämisessä (Viestintävirasto Kyberturvallisuuskeskus 2010, 18). Vakoiluohjelma toimii tietokoneessa käyttäjän huomaamatta ja lähettää varastamansa tiedot ohjelman ylläpitäjän määrittelemälle lokipalvelimelle (Flyktman 2011, 337; Kiianmies 2010, 742). Vakoiluohjelma pääsee tietokoneelle esimerkiksi julkisohjelman tai huijausohjelman mukana toimien vaikkapa pelinä. Peli toimii tiedonsiirtäjänä käyttäjän tietokoneelta tietoverkkorikollisen tietokoneelle. Vakoiluohjelma voi tarttua myös Internet-selaimen tietoturva-aukon

kautta esimerkiksi Internet-sivustolta, jossa hyväksytään jokin asia painikkeella. (Flyktman 2011, 332–337.)

Vakoiluohjelma voi myös esimerkiksi seurata, mitä näppäimistöltä kirjoitetaan. Näppäilytallentimet voivat tallentaa käyttäjän kaikki tai vain tiettyyn ohjelmaan liittyvät näppäinpainallukset. Haittaohjelma lähettää näppäinpainallukset sisältävän tiedoston lopuksi eteenpäin käyttäjän tietämättä. (Kiianmies 2010, 742, 744.) Näppäimistökaappaukseen tarkoitettuja ohjelmia voi ladata Internetistä ilmaiseksi. Kaikki virustorjuntaohjelmat eivät tunnista näitä ohjelmia. Näppäimistön ja tietokoneen väliseen johtoon asennettava muistisiru tallentaa kaikki näppäinpainallukset suoraan kaapelista. (Järvinen 2012, 129.)

Troijan hevoset naamioidaan normaaleiksi ohjelmiksi, joissa on piilotettuja toimintoja (Järvinen 2012, 178; Kiianmies 2010, 739). Troijalaiset voivat avata palomuuriin tai tietokoneeseen ns. takaoven. Tällöin takaoven kautta muut haittaohjelmat pääsevät sisään uhrin tietokoneelle. (Järvinen 2012, 178; Kiianmies 2010, 739.) Tietoverkkorikollinen voi ohittaa Windowsin käyttäjätunnukset ja salasanat saadakseen tietokoneen haltuun. Myös madot voivat avata takaoven. (Kiianmies 2010, 743.)

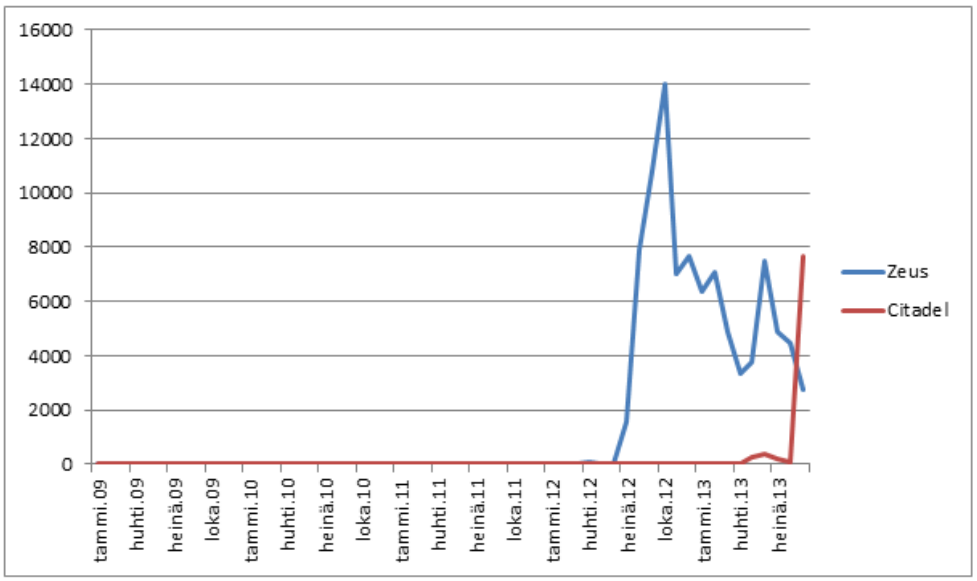
Tietokoneelle tarttunut pankkitroijalainen aktivoituu, kun henkilöasiakas kirjautuu seuraavan kerran verkkopankkiin. Haittaohjelma käynnistää varjoistunnon, jossa hyödynnetään henkilöasiakkaan käyttämiä pankkitunnuksia. Tilisiirto voi tapahtua esimerkiksi silloin, kun näytöllä on hetkellisesti teksti ”odota”, ”pieni hetki” tai ”asennetaan päivityksiä”. (MTV Oy 2012.) Henkilöasiakas ei välttämättä huomaa tietoverkkorikollisen tekemiä tilisiirtomuutoksia verkkopankki-istunnon aikana vahvistaessaan tilisiirtoa (Iranto 2012). Vasta pankkiautomaatin tiliotteesta voi selvitä ylimääräiset rahansiirrot, tai kun laskuttajalta tulee maksumuistutus (Iranto 2012; Ranta 2013b).

Verkkopankkitunnuksia urkkivien pankkitroijalaisten haittaohjelmien määrittelytiedostoista löytyi useita suomalaisia verkkopankkeja muun muassa vuonna 2011. Tavallisimmin näissä huijausyrityksissä on käytetty Zeus-haittaohjelmaperheeseen kuuluvia ohjelmia. Myös SpyEye haittaohjelmaa on tavattu suomalaisissa pankeissa Citadel-, Ice-IX ja Hermes-haittaohjelmien lisäksi. Muita yleisiä haittaohjelmaperheitä ovat Carberp,

Gozi ja Patcher. (Viestintävirasto Kyberturvallisuuskeskus 2012; Viestintävirasto Kyberturvallisuuskeskus 2011a; Viestintävirasto Kyberturvallisuuskeskus 2011c.)

MTV Oy uutisoi keskusrikospoliisin (KRP) varoittamasta Citadel-troijalaisen mahdollisesta hyökkäysaallosta joulun 2013 tienoilla. Citadel on variaatio Zeus-viruksesta. Itse Zeus on vanhimpia pankkitroijalaisia. Citadelin kirjoittaja on tunnettu venäläinen. (Ranta 2013a.) Citadel voi asentaa myös muita haittaohjelmia pankkitunnusten varastamisen lisäksi (virukset.fi 2012).

Viestintäviraston Kyberturvallisuuskeskuksen (2013) Autoreporter palvelun tuottamasta Zeus ja Citadel haittaohjelmahavainnoista nähdään alla kuviosta 5 suomalaisissa IP-osoitteissa. Zeus haittaohjelman havaintoja oli 14 010 lokakuussa 2012. Syyskuussa 2013 havaintoja oli enää 2 765. Citadel havainnot ovat nousseet huhtikuusta 2013. Havaintoja oli 7 650 syyskuussa 2013.



Kuvio 5. Autoreporterin havainnot tietoja varastavista Zeus ja Cital haittaohjelmista tammikuu 2009-heinäkuu 2013 (Viestintävirasto Kyberturvallisuuskeskus 2013)

Rootkit-haittaohjelmiin kuuluva Haxdoor voi vakoilla tietokoneelta käyttäjän tietoja ja lukea pankkisivustoihin syötettyjä pankkitunnuksia. Rootkit-ohjelmat ovat virustorjuntaohjelmien tavoittamattomissa, koska ne pystyvät piiloutumaan syvälle käyttöjärjestelmään. Rootkit-ohjelmat voivat avata muille viruksille ja haittaohjelmille takaoven tieto-

koneen hallitsemiseksi. Nämä ohjelmat voivat myös piiloutua samalla tavoin kuin Rootkit. Rootkit-ohjelman tunnistaa vain tämän etsintään erikseen luotu ohjelma kuten Microsoft Malicious Software Removal Tool ja F-Secure Blacklight. (Kiianmies 2010, 744–745.)

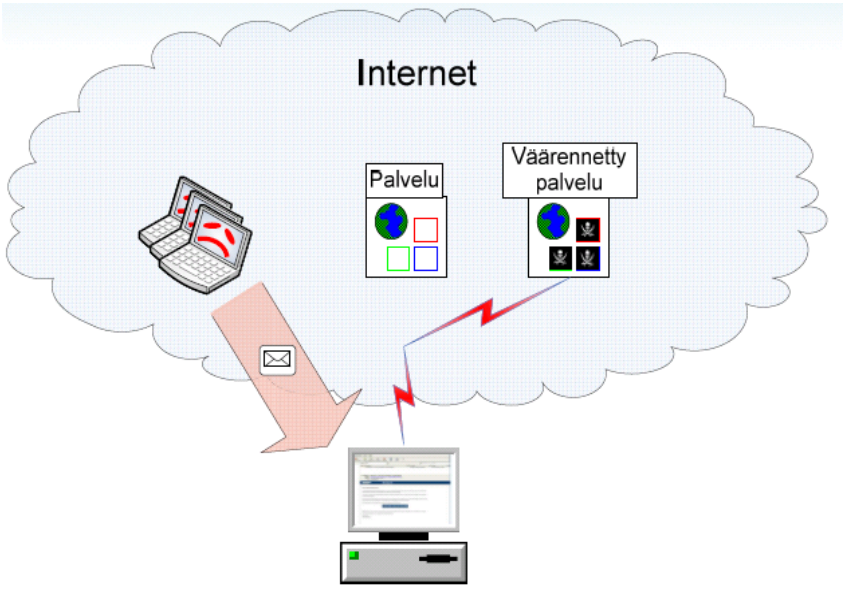
Man-in-the-Middle (MitM) eli mies välissä -hyökkäyksessä tietoverkkorikollinen kaappaa käyttäjän verkkopankin palvelimen ja käyttäjän tietokoneen välisen tietoliikenneyhteyden. Näin hyökkääjä voi seurata tietoliikennettä ja saada selville tilisiirtoihin tarvittavat pankkitunnukset. (Viestintävirasto Kyberturvallisuuskeskus 2011b.)

Phishing eli tietojen kalastelu on tietoverkkorikollisten viime vuosina nopeasti lisääntynyt henkilöasiakkaan verkkopankkiin kohdistuvana urkkimistapana. (Järvinen 2012, 73; Kiianmies 2010, 751.) Tietoverkkorikollisen tarkoituksena on kerätä laittomasti verkkopankin henkilöasiakkaan henkilökohtaiseen käyttöön tarkoitettuja pankkitunnuksia. Tiedot saadaan huijaamalla asiakas antamaan nämä tunnukset jollain sopivalla keksityllä syyllä esimerkiksi sähköpostin, väärennettyjen Internetin valesivustojen tai puhelimen kautta tietoverkkorikolliselle. (Järvinen 2012, 73; Nordea 2014.) Asiakkaan saamassa sähköpostiviestissä on mukana Internet-sivuston linkki, jota klikkaamalla asiakas ohjataan pankin sivustoa muistuttavalle sivustolle (Poliisi 2014a). Verkkopankkitietojen kalastelu on tietoverkkorikollisten suosiossa, koska jo muutama onnistunut varastamistapaus on tietoverkkorikolliselle taloudellisesti kannattavaa, ei juurikaan aiheuta kustannuksia ja on lähes riskitöntä (Viestintävirasto Kyberturvallisuuskeskus 2010, 19; Jakobsson 2012, 38).

Käytännössä tietoverkkorikollisen tekemä phishing verkkourkinta (Kuvio 6) voi tapahtua esimerkiksi siten, että tietoverkkorikollinen on luonut ensin oikeaa pankin verkkosivustoa muistuttavan valesivuston (Goodrich & Tamassia 2011, 341). Tämän jälkeen tietoverkkorikollinen lähettää huijaukseen tarkoitetun aidolta näyttävän sähköpostiviestin jollain keräämällään sähköpostin jakelulistalla usealle henkilöasiakkaalle (Kiianmies 2010, 751; Nordea 2014). Sähköpostiviestissä voidaan pyytää henkilöasiakasta kirjautumaan verkkopankissa olevalle tililleen joko tarkistamaan tai päivittämään tietojaan sähköpostissa olevan linkin kautta (Jakobsson 2012, 38). Jos henkilöasiakas valitsee sähköpostiviestistä linkin, vie linkki henkilöasiakkaan todellisuudessa väärennetyn pal-

velun valesivustolle, joka muistuttaa erehdyttävästi verkkopankin oikeaa sivustoa (Viestintävirasto Kyberturvallisuuskeskus, 20).

Valesivuston tarkoituksena on kerätä henkilöasiakkaan henkilökohtaisia verkkopankkitunnuksia siten, että henkilöasiakas antaa ensin verkkopankkitunnuksensa väärennetyn palvelun valesivustolla. Tämän jälkeen valesivusto tallentaa tunnukset asiakkaan huomaamatta itselleen ja lataa henkilöasiakkaalle oikean palvelun sivuston tai antaa esimerkiksi ilmoituksen, että sivusto on tällä hetkellä huollossa. (Goodrich & Tamassia 2011, 341; Järvinen 2012, 73.) Jos tietoverkkorikollinen onnistuu tässä tietojen kalastelussa, voi tietoverkkorikollinen siirtää näillä tiedoilla henkilöasiakkaan tililtä varoja jollekin toiselle tilille (Jakobsson 2012, 13, 38). Henkilöasiakkaan henkilökohtaisten verkkopankkitunnusten kalastelua voi tapahtua myös puhelimitse. Tässä tapauksessa rikollinen voi esiintyä pankissa työskentelevänä henkilönä ja pyytää jonkin huijauksen avulla henkilöasiakasta luovuttamaan henkilökohtaiset pankkitunnuksensa. (Nordea 2014.)



Kuvio 6. Verkkopankkitunnusten varastaminen tietojen kalastelun (phishing) eli verkkourkintahyökkäyksen avulla (Viestintävirasto Kyberturvallisuuskeskus 2010, 20)

Tietojen kalastelut onnistuvat lähinnä siksi, että kalastelun kohteena olevat verkkopankin henkilöasiakkaat erehtyvät sähköpostiviestien sekä aidoilta näyttävien että taitavasti tehtyjen Internetin valesivustojen sisältöjen olevan peräisin luotettavasta tahosta. Henkilöasiakkaat erehtyvät valesivustojen aitoudesta esimerkiksi niissä esiintyvien pankin

logojen ansiosta ja päättelevät siten niiden käytön olevan turvallista. Tietoverkkorikolliset hyötyvät tietojen kalastelussa myös siitä, että henkilöasiakkaat klikkaavat melkein mitä tahansa Internetin linkkiä, avaavat sähköpostin liitetiedostoja sekä asentavat löytämiään ohjelmia tutkimatta niitä tarkemmin. (Jakobsson 2012, 12, 38; Kiianmies 2010, 751–752.) Käännöskoneilla kirjoitetut huijaukset ovat läpinäkyviä, mutta huonosti suomea puhuvat ja verkkopankkia huonosti tuntevat henkilöasiakkaat saattavat kuitenkin erehtyä antamaan tietoverkkorikolliselle vaikka koko salasanalistan (Haasio 2013, 37; Järvinen 2012, 74).

Pharming eli huijaussivuston luominen on tietojen kalastelun vähemmän käytetty kehittyneempi muoto. Tätä huijaustapaa vastaan ei voi suojautua, sillä huijaussivustolle ohjataan suoraan ilman viestiä haittaohjelmalla. Nämä huijaussivut eivät ehdi yleensä olemaan kauan voimassa, sillä niiden toiminta huomataan yleensä melko nopeasti. Pharming tunnettiin aikaisemmin nimellä DNS-myrkyttäminen. (Kiianmies 2010, 752.) Phishingin ja pharmingin ero on siinä, että phishingissä käyttäjä suostutellaan antamaan pankkitunnuksensa. Pharmingissa taas yritetään saada pankkitunnukset ilman käyttäjän lupaa. (Finanssialan Keskusliitto ry 2012b.)

Pharmingissa tietoverkkorikollinen luo huijaussivuston, jossa käytetään hyväksi DNS-järjestelmää. DNS-järjestelmän tarkoituksena on muuntaa ihmisen ymmärtämä Internet-sivuston osoite tietokoneen ymmärtämään muotoon esimerkiksi 193.234.192.16. Luotuaan verkkopankkia muistuttavan huijaussivuston, tietoverkkorikollinen kaappaa DNS- eli verkkotunnuspalvelimen tekemän muunnoksen ts. osoitekäännöksen. Tämän jälkeen tietoverkkorikollinen kääntää huijaussivustoon tulevat kutsut oman sivustonsa tietokoneen ymmärtämään IP-osoitteeseen. Jos henkilöasiakas pitää pankkia muistuttavaa sivustoa aitona, voi henkilöasiakas antaa huijaussivustolla omat henkilökohtaiset pankkitunnuksensa. (Kiianmies 2010, 752.)

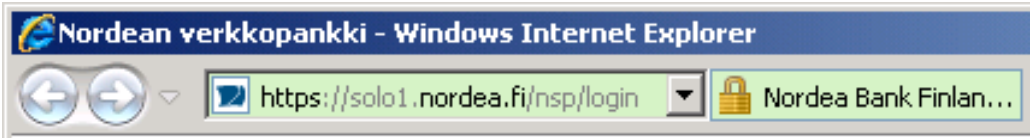
4 SSL-salaus ja käyttäjän todentamismenetelmät

Tässä luvussa käydään läpi varmenteisiin perustuvaa SSL-salausta (Secure Socket Layer) ja käyttäjän todentamismenetelmiä verkkopankin turvallisuutta lisäävinä tekijöinä.

4.1 SSL-salaus ja varmenne

Käyttäjän Internet-selain pyytää aluksi verkkopankin palvelinta todistamaan olevansa oikea palvelin. Palvelimen selaimelle esittämästä varmenteesta selviää mm. pankin nimi, osoite ja Internet-osoite. Kun selain on todennut palvelimen tiedot oikeiksi varmenteesta, selain laittaa vaikeasti murrettavissa olevan 128- tai 256-bittisen symmetrisen SSL-salauksen päälle automaattisesti kyseisen verkkopankin istunnon ajaksi Internet-selaimen ja palvelimen välille. (Järvinen 2012, 57, 59; Järvinen 2010, 155.) Tällöin muut eivät näe, mitä SSL-salatulla linjalla tapahtuu. Siksi tietoverkkorikolliset eivät yritä väärentää varmenteita vaan käyttävät huijauksissa HTTP-yhteyttä suojatun HTTPS-yhteyden sijaan. (Järvinen 2012, 58, 63.)

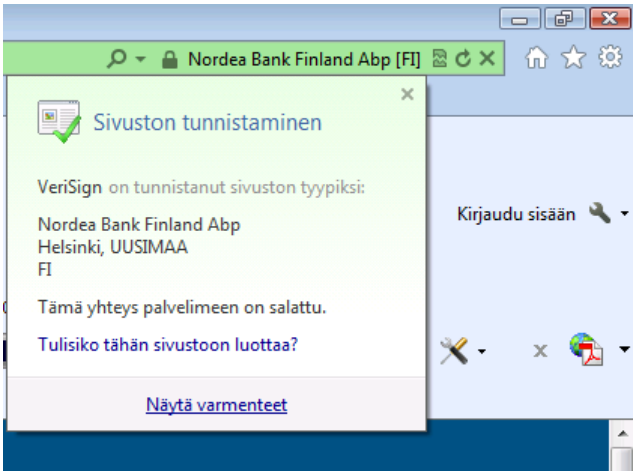
SSL-salatun yhteyden tunnistaa Internet-Explorer -selaimessa siitä, että Internet-selaimen osoiteriville tulee HTTP-yhteyden sijaan suojattu HTTPS-yhteys. Internet-selaimen osoiteriville tai alareunaan tulee lukon kuva ja osoiterivin taustaväri vaihtuu riippuen Internet-selaimesta. (Järvinen 2012, 58.) Alla kuviossa 7 on esimerkkinä Nordean SSL-salattu yhteys.



Kuvio 7. Nordean oikea sivusto, jossa on SSL-salattu HTTPS yhteys ja lukittu lukon kuva

SSL-salaus vaatii varmennetta, joka todistaa pankin aitouden. Varmenne on .cer-päätteinen tiedosto Internet-sivustolla. (Järvinen 2012, 58; Kiianmies 2010, 784.) Varmenne on voimassa tietyn ajan. Varmenteen myöntää valtuutettu varmentaja. Varmentaja takaa varmenteen aitouden ja eheyden digitaalisella allekirjoituksella. (Kiianmies 2010, 784; Järvinen 2012, 59.) Varmenteen tiedot on tarkistettavissa esimerkiksi Inter-

net Explorer -selaimessa napsauttamalla osoiterivillä olevaa lukon kuvaa ja edelleen Näytä varmenteet. Teknisistä tiedoista nähdään mm. varmenteen myöntäjä ja kenelle varmenne on myönnetty. Alla kuviosta 8 nähdään esimerkkinä Nordean verkkopankin varmenteen tietoja Internet Explorer -selaimessa. Varmenteen kirjoittaja on Verisign. (Järvinen 2012, 60–61.)



Kuvio 8. Nordean verkkopankin varmenteen tietoja, jossa varmenteen kirjoittajana on VeriSign

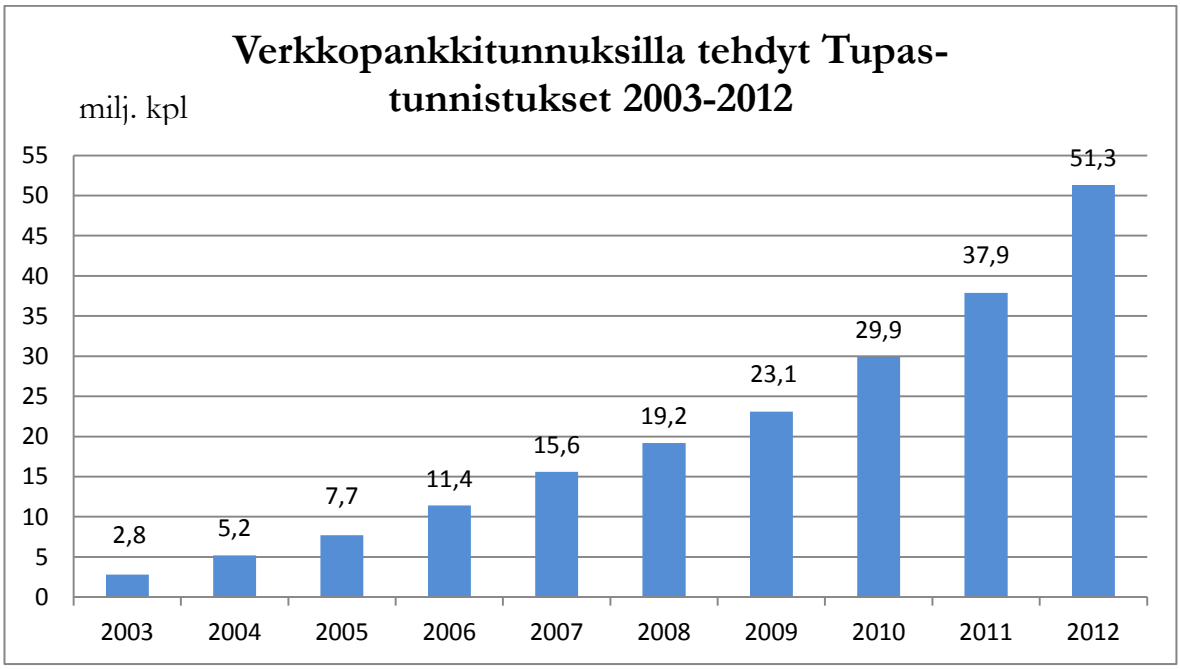
Verkkopankin henkilöasiakkaan kannalta SSL-salauksella suojatusta yhteydestä ja varmenteesta ei ole kuitenkaan hyötyä, jos tietoverkkorikollinen saa pankkitunnukset tietoja varastavan ohjelman avulla tai muutoin oikeudettomasti käyttöönsä. (Järvinen 2012, 59, 64; Wuolijoki & Hemmo 2013, 727.) Pankki pitää sekä käyttäjätunnusta että vaihtuvia tunnuslukuja käyttävää oikeana asiakkaana ja todentaa siksi tunnukset omaavan käyttäjän (Järvinen 2012, 64). Ulkopuolinen henkilö ei voi arvata näitä tunnuksia (Wuolijoki & Hemmo 2013, 727).

4.2 Käyttäjän todentamismenetelmät

Sähköisten palvelun käyttäjä pitää pystyä tunnistamaan luotettavasti. Tunnistautumista parantavat henkilökohtaiset pankkitunnukset ja erityisesti niihin kuuluvat vaihtuvat tunnusluvut. (Tietoturvaopas 2011.) Nämä maksuvälineisiin kuuluvat pankkitunnukset kuuluvat vahvaan sähköiseen tunnistamiseen. Pankkitunnuksilla todennetaan asiakkaan henkilöllisyys sähköisesti erilaisissa palveluissa kuten verkkopankissa, puhelimitse tapahtuvassa tunnistautumisessa ja Tupas-tunnistuksissa. (Viestintävirasto 2013; Wuoli-

joki & Hemmo 2013, 726.) Tupas-tunnistukset ovat pankkien kehittämä tunniste- ja varmennepalvelu yrityksille ja yhteisöille asiakkaiden tunnistamiseen. (Wuolijoki & Hemmo 2013, 726.)

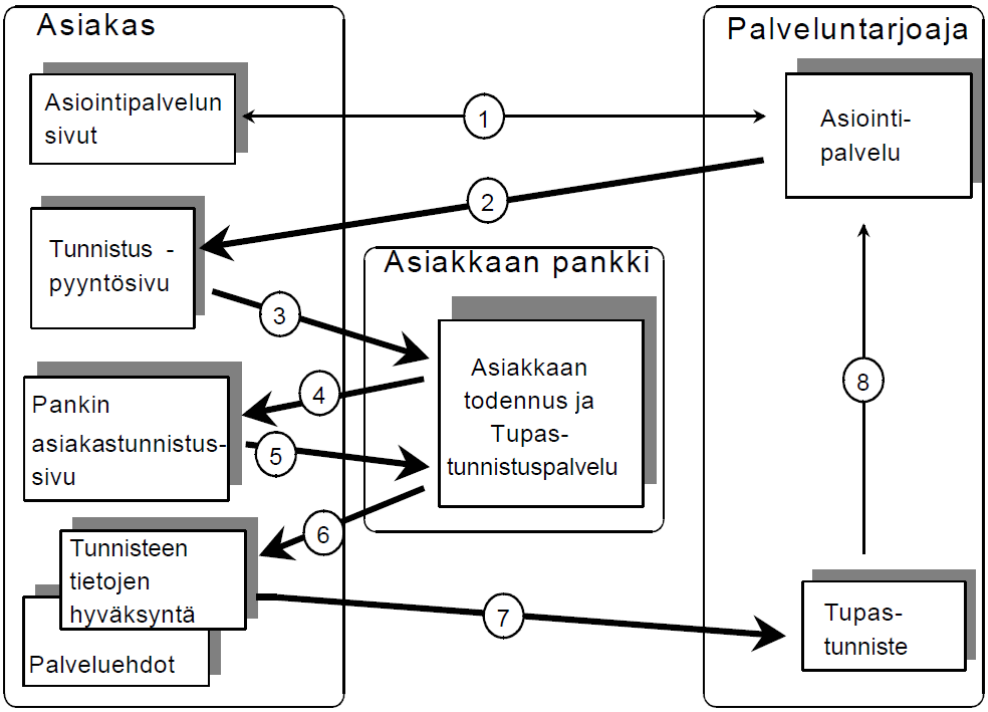
Alla kuvion 9 Finanssialan Keskusliitto ry:n (2013b, 13) tilastosta nähdään verkkopankkitunnuksilla tehtyjen Tupas-tunnistusten vuosittainen kasvukehitys vuosina 2003-2012. Trendinä on ollut jatkuva kasvu. Vuoden 2012 kasvu oli 73,88 % verrattuna edelliseen vuoteen 2011.



Kuvio 9. Verkkopankkitunnuksilla tehtyjen Tupas-tunnistuksien kehitys vuosina 2003-2012 (Finanssialan Keskusliitto ry 2013b, 13)

Seuraavan sivun kuviosta 10 nähdään Tupas-tunnistuspalvelun toiminnallinen eteneminen Finanssialan Keskusliiton ry:n (2013a, 5–6) kuvauksen mukaan. Tupas-tunnistuspalvelu alkaa siitä, kun tunnistautuva asiakas ottaa yhteyden asiointipalvelun sivuilta palveluntarjoajan asiointipalveluun SSL-suojatulla yhteydellä (1). Palveluntarjoaja vastaa asiakkaalle lähettämällä tunnistuspyynnön (2). Tunnistuspyyntösivulta asiakas pääsee oman pankkinsa Tupas-tunnistuspalveluun (3). Asiakas saa pankilta tunnistuspyynnön (4). Asiakas tunnistautuu pankin asiakastunnistussivulla (5). Asiakas saa tunnistautumisesta Tupas-tunniste-tietojen hyväksynnän (6). Tunnisteen tietojen hyväksynnässä asiakas tarkistaa tunnistustapahtuman ja hyväksyy tiedot palveluntarjoajalle

(7). Palveluntarjoaja tarkastaa Tupas-tunnisteen eheyden ja liittää tunnisteen asiakkaan palvelutapahtumaan.



Kuvio 10. Tupas-varmennepalvelun toiminnallinen kuvaus (Finanssialan Keskusliitto ry 2013a, 5)

5 Tietoturvaohjeistus henkilöasiakkaalle

Tämä tietoturvaohjeistus kertoo verkkopankin henkilöasiakkaille ennalta tehtävistä suojautumiskeinoista edellä kuvattuja huijauksia vastaan.

5.1 Maksun lisävahvistus

Maksun lisävahvistus on pankin asiakkaille maksuton tietoturvaa ja luotettavuutta lisäävä suoja verkkopankissa tehdyille maksuille kotimaassa. Maksun lisävahvistus tehdään toisella laitteella joko matkapuhelimen tekstiviestillä tai puhelimitse. (Nordea 2013b; Nordea 2013c; OP-Pohjola-ryhmä 2013b.) Tarkoituksena on paljastaa ja estää ennen maksun lisävahvistusta asiakkaan antamien maksutietojen muutokset ja rahojen siirrot väärälle tilille. Näitä verkkorikolliset yrittävät tehdä haittaohjelmilla ja huijauksilla ennen maksutietojen välittymistä pankkiin. (OP-Pohjola-ryhmä 2013a.) Maksun lisävahvistus ei poista asiakkaan tietokoneelta itse haittaohjelmia eikä anna suojaa itse tietokoneelle (OP-Pohjola-ryhmä 2011a).

Maksun lisävahvistuksen käyttöönotto edellyttää asiakkaalta voimassaolevaa verkkopankkisopimusta pankin kanssa (OP-Pohjola-ryhmä 2013b), tekstiviestejä vastaanottavaa matkapuhelinta (OP-Pohjola-ryhmä 2011b) sekä lisävahvistukseen hyväksyttyä operaattorin matkapuhelinliittymää (OP-Pohjola-ryhmä 2013b). Maksun lisävahvistuksen saa verkkopankissa käyttöön rekisteröimällä tekstiviestejä vastaanottavan matkapuhelinnumeron tekstiviestipalveluun. Numeroa on myös mahdollista muuttaa tarvittaessa jälkikäteen. (OP-Pohjola-ryhmä 2011b.)

Asiakas vahvistaa jokaisen tilisiirtona tehdyn maksun verkkopankissaan maksun teon jälkeen (Nordea 2013a). Maksun lisävahvistus tehdään vain niille maksuille, joista pankki lähettää asiakkaalle tekstiviestillä maksun lisävahvistuspyynnön asiakkaan etukäteen määrittelemään matkapuhelinnumeroon (OP-Pohjola-ryhmä 2013a) pankkien määrittelemien kriteerien mukaisesti (Pietiläinen 2010). Asiakkaan tulee varmistaa tekstiviestillä verkkopankissa antamansa maksun määrä ja saajan tilinumero, jotta pankkiin välittyneet tiedot ovat varmasti oikeat. Vasta tietojen tarkistuksen jälkeen tehdään itse maksun lisävahvistus. Jos maksussa on virheitä, asiakkaan tulee lopettaa verkkopankin

käyttö ilman maksun lisävahvistusta ja ottaa yhteyttä pankkiinsa. (OP-Pohjola-ryhmä 2013a.)

Maksun lisävahvistus tapahtuu esimerkiksi Nordeassa vastaamalla pankin lähettämään tekstiviestin lisävahvistuspyyntöön kirjaimella A viimeistään seuraavan pankkipäivän aikana. Muutoin maksu ei välity maksussa ilmoitetulle maksunsaajan tilille. Lisävahvistamisesta asiakas saa paluuviestinä kuittausviestin. (Nordea 2013b.) OP-Pohjola-ryhmässä lisävahvistus tehdään avainlukulistalta järjestysnumeroa vastaavalla avainluvulla (OP-Pohjola-ryhmä 2011b). Maksun lisävahvistuksen voi tehdä myös soittamalla asiakaspalveluun, jos asiakkaalla ei ole matkapuhelinta käytössään (Nordea 2013a).

Nordea otti ensimmäisenä käyttöön maksun lisävahvistuksen henkilöasiakkaiden verkkopankissa suurille tilisiirroille ja epäilyttäville vastaanottajille Suomessa 12.2.2010. Nordean riskienhallintajohtajan Kari Oksasen mukaan Nordean n. 1,5 miljoonan asiakkaan tekemistä tilisiirroista n. 600–700 saa maksun lisävahvistuksen päivässä Nordean tekemien testien mukaan. Nordea otti lisävahvistuksen alun perin käyttöön, koska asiakkaiden mielestä 16 000 euron tilisiirron yläraja ei ollut sopiva kaikille asiakkaille. Osa asiakkaista saattoi saada lisävahvistuksia usein riippuen esimerkiksi asiakkaan toimialasta, ja toisille asiakkaille vahvistusta ei tullut lainkaan. Myös lisääntyneet hakkeroinnit ja identiteettivarkaudet vauhdittivat lisävahvistuksen käyttöönottoa. (Pietiläinen 2010.)

Osuuspankki otti lisävahvistuksen käyttöön n. 1,3 vuotta Nordeaa myöhemmin 29.5.2011. Osuuspankki kertoo käyttöönoton syyksi verkossa maksamisen turvallisuuden lisääminen asiakkaille, sillä verkkorikollisilla on uusia keinoja huijaamiseen. Pankkien tulee olla omalta osaltaan kehityksessä mukana. (OP-Pohjola-ryhmä 2011a.) Maksun lisävahvistus on ollut käytössä lisäksi ainakin Danske Bankissa 7.12.2012 alkaen (Danske Bank 2012).

5.2 Palomuuri

Palomuuri on konekohtainen tietokoneessa oleva ohjelmallinen palomuuri tai esimerkiksi koti- ja toimistokäytössä laajakaistan ADSL-modeemiin yhdistetty laitepalomuuri

tietokoneen ja Internet-yhteyden välissä (Järvinen 2012, 189–190; Kiianmies 2010, 712). Palomuurin tarkoituksena on suojata tietokonetta rajoittamalla ja valvomalla palomuurin läpi kulkevaa julkisesta Internetistä saapuvaa ja myös Internetiin lähtevää tietoliikennettä etukäteen määriteltyjen ohjaussääntöjen eli käsittelytapojen mukaan kaappauksia, matoja ja erilaisia hyökkäyksiä vastaan estämällä näitä hyökkäyksiä käyttämästä tietokoneohjelmistojen tietoturva-aukkoja (Järvinen 2012, 189; Tietosuojavaltuutetun toimisto 2010a, 2).

Koti- ja toimistokäytössä palomuurin ohjaussäännöillä suodatetaan lähinnä vain julkisesta Internetistä tietokoneelle pyrkivät haitalliset tietoliikenteet toisin kuin yrityksissä, joissa suodatetaan myös osa lähtevästä tietoliikenteestä (Järvinen 2012, 193). Sallimattomasta liikenteestä tulee tietokoneen näytölle ilmoitus, jossa näytetään käyttöoikeutta vaativan sovelluksen nimi ja pyydetään käyttäjää joko hyväksymään tai hylkäämään lupapyyntö. Palomuuri yrittää myös piilottaa ulkopuolisia näkemästä mm. tietokonetta ja sen IP-osoitetta (Kiianmies 2010, 714–715.) Palomuuri ei anna sataprosenttista suojaa, mutta oikein asennettu palomuuri suojaa tietokoneeseen kohdistuvilta erilaisilta hyökkäyksiltä vain, jos palomuurin ohjaussääntöjä ylläpidetään säännöllisesti (Flyktman 2011, 321; Tietosuojavaltuutetun toimisto 2010a, 2).

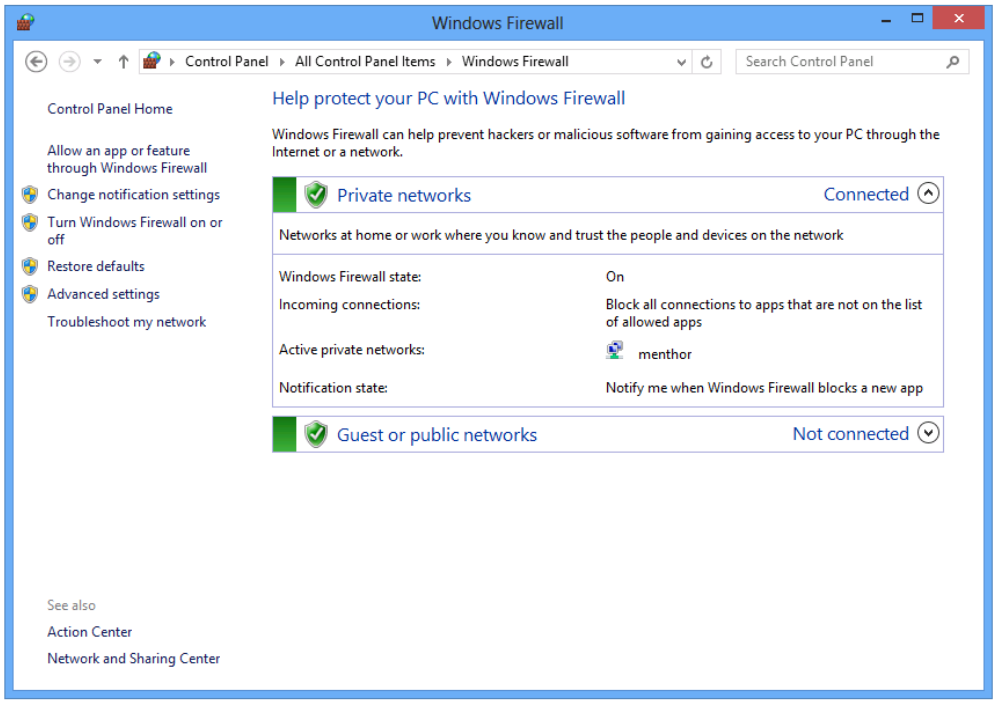
Palomuurin ohella tulee kuitenkin käyttää myös virustentorjuntaohjelmaa haittaohjelmia ja tietokoneviruksia vastaan, koska palomuuri tutkii tietoliikennettä pelkästään IP-pakettien tasolla eikä niiden sisältöjä. (Järvinen 2012, 194; Tietosuojavaltuutetun toimisto 2010a, 2.) Haittaohjelmat pääsevät palomuurin läpi tietokoneelle, jos itse palomuurissa on tietoturva-aukkoja. Palomuurin toiminnan voi pysäyttää esimerkiksi tietokoneelle sähköpostiviestin mukana päässyt haittaohjelma tai jopa käyttäjä itse, ellei käytössä ole rajoitettuja käyttöoikeuksia. (Järvinen 2012, 189.) Palomuurin ylläpitämästä lokista voidaan nähdä esimerkiksi palomuurin estämät luvattomat lähtevät ja erityisesti saapuvat tietoliikenteet tiettyyn porttiin ja IP-osoitteeseen (Kiianmies 2010, 713).

Laitepalomuuri suojaa kaikkia sisäverkossa olevia tietokoneita käyttöjärjestelmästä riippumatta ja estää kotiverkon sisällä leviäviä tartuntoja muihin verkon tietokoneisiin. Laitepalomuurissa ei ole haittaohjelmien tarvitsemia prosesseja, eikä sitä voi sammuttaa ohjelmallisesti. Siten laitepalomuuri on turvallisempi kuin ohjelmallinen palomuuri.

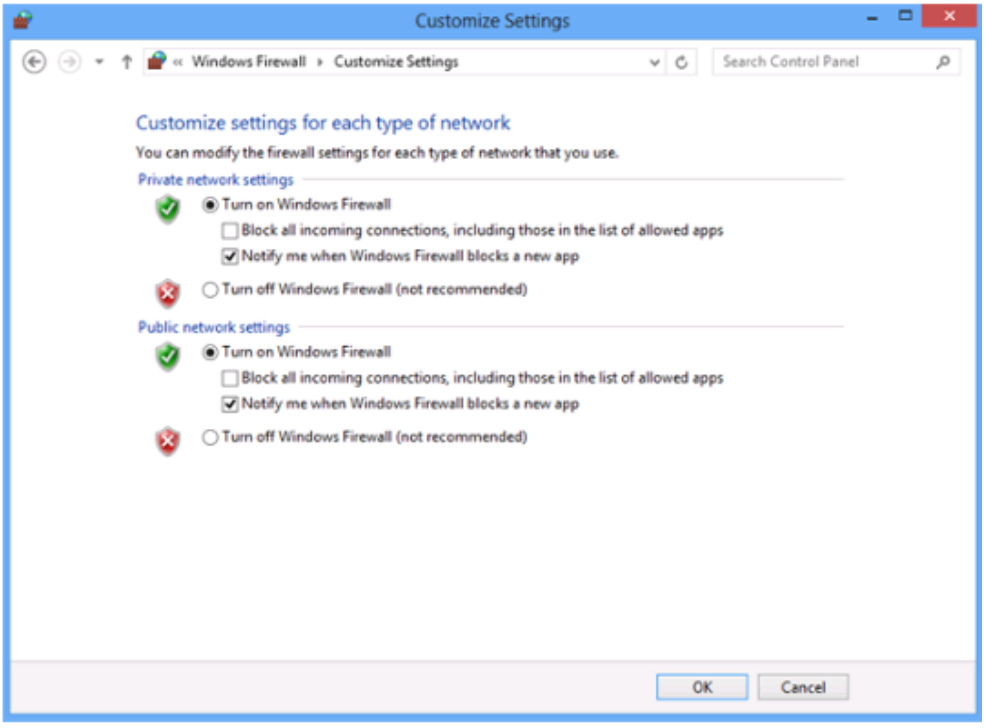
Suositeltavaa on kuitenkin käyttää konekohtaisen ohjelmallisen palomuuria lisäksi myös laitepalomuuria. On mahdollista, että tietokoneeseen saapuva haitallinen tietoliikenne estyy viimeistään tietokoneen palomuurissa sen jälkeen, jos se on päässyt laitepalomuurista läpi. (Järvinen 2012, 190.)

Lisäksi tietokoneessa on suositeltavaa käyttää vain yhtä ohjelmallista palomuuria kerrallaan, koska palomuurit saattaisivat olla eri mieltä päästääkö tietoliikenne läpi vai ei (Kiianmies 2010, 717; Rowlingson 2011, 61). Vaikka tietoturvaohjelmat poistavat automaattisesti toisen palomuurin käytöstä, on toinen palomuuriohjelmisto hyvä poistaa käytöstä jo ennen uuden asentamista (Järvinen 2012, 190; Kiianmies 2010, 717). Ohjelmavalmistajien sivuilta voi tarkistaa sopivatko eri toimittajien palomuuri- ja virustentorjuntaohjelmat yhteen omassa tietokoneessa. Käyttäjälle saattaa olla myös edullisempaa ostaa koko palomuuri- ja virustentorjuntaohjelmapaketti. (Kiianmies 2010, 717.)

Microsoft Windowsin eri käyttöjärjestelmäversioissa on oletuksena mukana palomuuriohjelma valmiiksi päällekytkettynä toisin kuin oli Microsoftin ensimmäisessä Windows XP -käyttöjärjestelmässä vuonna 2001. Silloin haittaohjelmien oli mahdollista päästä tietokoneeseen heti Internetiin yhdistymisen jälkeen. (Järvinen 2012, 190.) Windowsin palomuurin asetuksia voi tarkistaa ja muuttaa tarvittaessa esimerkiksi valitsemalla Käynnistä-valikosta Ohjauspaneeli ja kirjoittamalla vasemmalla ylhäällä olevaan hakukenttään palomuuri. Tämän jälkeen valitaan Windowsin palomuuri -linkki ja edelleen vasemmalta Ota Windowsin palomuuri käyttöön tai poista se käytöstä -linkki (Kuvio 11). Palomuurin käyttöönoton asetuksista voidaan valita halutut asetukset käyttöön (Kuvio 12). (Rowlingson 2011, 61.)



Kuvio 11. Esimerkkikuva Windows 8 palomuurin näytöstä



Kuvio 12. Palomuurin käyttöönotto Windows 8 käyttöjärjestelmässä

Maksullisia palomuuriohjelmistoja ovat esimerkiksi F-Secure Internet Security, Norton Internet Security, Sygate Personal Firewall ja ZoneAlarm (Kiianmies 2010, 717). ZoneAlarmista ja Sygatesta on olemassa myös ilmaisversiot (Flyktman 2011, 321). Muita

ilmaisia palomuuriohjelmistoja ovat esimerkiksi Outpost Firewall Free ja Kerio Personal Firewall (Kiianmies 2010, 717). Kaupallisissa ohjelmistoissa on yleensä vuoden lisenssi sisältäen päivitykset. Seuraavan vuoden päivityspaketin voi ostaa Internetistä tai ohjelmistoa myyvästä liikkeestä. Uuden ohjelmistoversion päivitys on yleensä kalliimpi. (Flyktman 2011, 321.) Palomuurin voi hankkia myös mm. laajakaistaoperaattoreilta, joilta saa tarvittaessa lisäneuvoja ohjaussääntöjen luontiin (Tietosuojavaltuutetun toimisto 2010a, 2).

Palomuurin toimintaa kannattaa testata silloin tällöin Internetistä löytyvillä palveluilla kuten Security Metricsin porttiskanneri tai Gibson Researchin ShieldsUp, eikä vain luottaa palomuurin toimivan. Esimerkiksi kotikäyttöiset edulliset laajakaistamodeemit voivat nollautua ja hukata asetukset. Testauksessa palvelu huomaa käyttäjän IP-osoitteen lähteen ja yrittää ottaa yhteyttä tämän osoitteen eri portteihin. Jos Windowsin kriittiset portit ovat 135, 139 ja 445 ovat auki, on Windows alttiina murtautumisille. Avoin-tila kertoo siis, että portti on auki, jolloin oma tietokone vastaa siihen tuleviin kyselyihin. Jollei kyseessä ole palvelin, palomuurin asetukset on tällöin syytä tarkistaa. Suljettu-tilassa tietokone tai palomuuri vastaa oven olevan suljettu. Näkymätön-tila eli parhain vaihtoehto ei anna portin kyselyihin mitään vastausta, jolloin hyökkääjä olettaa, että porttia tai konetta ei ole olemassa. (Järvinen 2012, 194–195.)

5.3 Virustentorjuntaohjelmistot

Virustentorjuntaohjelma toimii tietokoneen taustalla tarkoituksena suojata tietokonetta haittaohjelmilta (Kiianmies 2010, 748). Virustentorjuntaohjelman käyttö voi estää haittaohjelmien tarttumisen ja käynnistymisen sekä esimerkiksi tietojen varastamisen tietokoneelta (Flyktman 2011, 326). Lisäksi virustentorjuntaohjelman käyttö ennalta ehkäisevänä keinona saattaa estää hankalan haittaohjelman poistamisen. Virustentorjuntaohjelman toiminta perustuu virustunnistekannassa oleviin virusten merkkijonoihin eli sormenjälkiin. Virustentorjuntaohjelma antaa virusvaroituksen, jos löydetyn viruksen sormenjälki löytyy virustunnistekannasta. Virustentorjuntaohjelman päivityksessä virustunnistekantaan lisätään uusien virusten merkkijonot eli sormenjäljet. (Kiianmies 2010, 748–749.)

Virustentorjuntaohjelmien käyttö ja virustunnistekantojen säännölliset automaattiset päivitykset ovat välttämättömiä, jotta virustentorjuntaohjelma tunnistaa uudet haittaohjelmat. Virustentorjuntaohjelmat ja niiden virustunnistekantojen säännölliset päivitykset eivät takaa kuitenkaan 100 % suojaa haittaohjelmien torjunnassa. Tämä johtuu siitä, että mikään ohjelma ei löydä eikä pysty poistamaan kaikkia viruksia virustentorjuntaohjelmien sormenjälkikantojen päivityksistä huolimatta. Päivityksiä ei ehditä aina kirjoittamaan tai lisäämään virustunnistekantaan ajoissa. Lisäksi jotkut virukset pystyvät asettamaan virustentorjuntaohjelman pois päältä. (Kiianmies 2010, 734–735, 749.)

Virustentorjuntaohjelman havaitseman haittaohjelman voi poistaa kahdella tavalla. Virustentorjuntaohjelma saattaa antaa ilmoituksen havaitusta haittaohjelmasta tietokoneelle ja pyytää lupaa poistolle. Ajastettu tai käsin käynnistetty tietokoneen tarkistus voi löytää haittaohjelman tietokoneelta. Tällöin haittaohjelma poistetaan virustentorjuntaohjelmasta löytyvällä poistotyökalulla. (Kiianmies 2010, 746.)

Virustentorjuntaohjelmat saattavat antaa ilmoituksia myös vaarattomista ohjelmista, jolloin käyttäjä voi torjua tärkeän palvelun. Käyttäjä voi myös antaa erehdyksessä luvan haittaohjelmalle, jos käyttäjä sallii Internet-yhteyden. (Järvinen 2012, 210–211.) Viruksentorjuntaohjelmat tarvitsevat tietokoneelta muistia. Tällöin tietokoneen käynnistyminen ja toiminta saattavat hidastua. (Kiianmies 2010, 749.)

Virustentorjuntaohjelmia on saatavina sekä kaupallisina versioina että ilmaisversioina (Hjelt 2014). Kaupalliset versiot saattavat olla tehokkaampia ja niissä on monipuolisemmat asetusmahdollisuudet. Ilmaisversiot ovat kuitenkin parempi vaihtoehto kuin ei virustentorjuntaohjelmaa ollenkaan. (Flyktman 2011, 326). Kaupallisia virustentorjuntaohjelmia on muun muassa AVG Anti-Virus, F-Secure Anti-Virus ja Norton AntiVirus. Ilmaisia virustorjuntaohjelmistoja ovat muun muassa AVG Anti-Virus Free Edition, Antivir ja Avast. (Flyktman 2011, 326; Järvinen 2012, 204.)

F-Secure tietoturvayhtiöllä on ollut Internet Security 2013 -versiosta lähtien mukana lisäominaisuutena pankkitoimintojen suojausominaisuus henkilöasiakkaiden verkkopankki-istuntojen suojaamiseen erilaisilta haittaohjelmahyökkäyksiltä. Myös operaattorit tarjoavat tätä lisäominaisuutta lisäpalveluna. Toiminnon käyttöönotto ei vaadi erillisen

sovelluksen tai selainohjelman asennusta. (F-Secure 2014d.) Suojaus toimii taustalla huomaamattomasti vähintään Internet Explorer 9 -selaimessa, Firefoxin ja Chromen kahdessa viimeisimmässä pääversiossa (F-Secure 2014d; F-Secure 2014c). F-Securen (2014d) mukaan toiminto estää kaikki kyseistä verkkopankki-istuntoa vaarantavat yhteydet muiden tietoturvatoimintojen lisäksi.

Pankkitoimintojen suojauksen saa F-Securessa käyttöön avaamalla Online Safety käynnistysalustasta. Tämän jälkeen valitaan muokattava käyttäjätili ja valitaan Asetukset. Online Safety -kohdasta valitaan Pankkitoimintojen suojaus. Pankkitoimintojen suojaus -kohdan vierestä napsautetaan kytkintä ja valitaan OK. (F-Secure 2014a.)

Pankkitoimintojen suojaus aktivoituu automaattisesti verkkopankin avauksen yhteydessä. Näytön yläosaan ilmestyy lehtinen, joka ilmoittaa pankkitoimintojen suojaustilasta. Samalla kaikki uudet yhteydet estetään, jolloin tietoja varastavat ohjelmat eivät voi lähettää mitään tietoja tietoverkkorikollisille. Kaikki muut yhteydet asetetaan pitoon verkkopankki-istunnon ajaksi. Verkkopankki-istunnon aikana on kuitenkin mahdollista päästä istunnon aikana tarvittaville muille Internet-sivustoille, jotka F-Secure luokittelee turvallisiksi. (F-Secure 2014b).

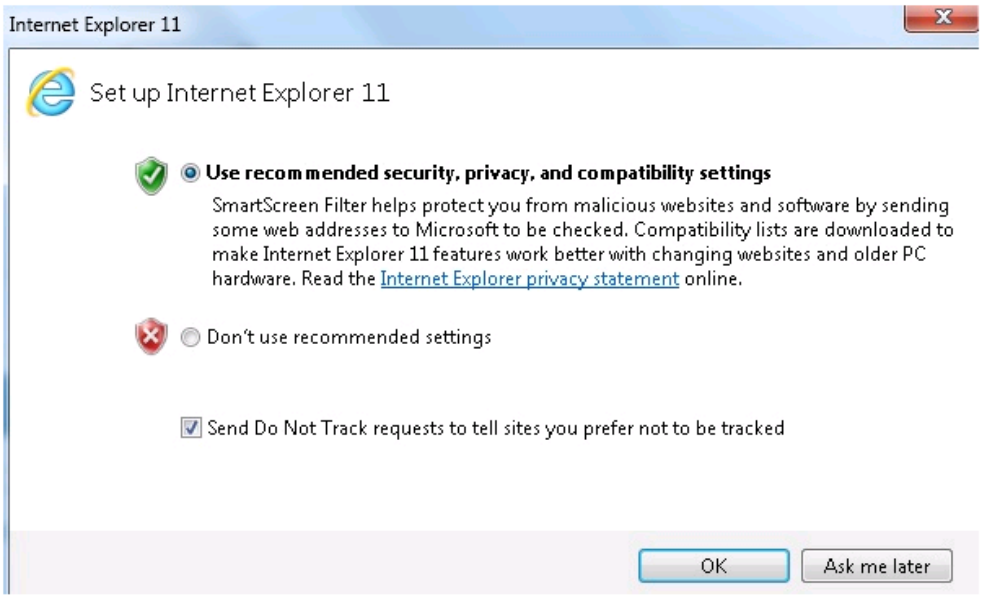
5.4 Muita ohjeistuksia

Verkkopankin henkilöasiakas saattaa tunnistaa phishing verkkourkintahyökkäykseen liittyvän huijaussivuston sen jälkeen, kun on kirjoittanut Internet-selaimen osoiteriville verkkosivun osoitteen. Valesivuston verkkopankin osoitteessa voi olla esimerkiksi vain yhden merkin ero verrattuna oikean verkkopankin Internet-osoitteeseen. Seuraavan sivun kuvion 13 esimerkistä nähdään Nordea pankin väärennetty sivusto tummennetusta osoiterivin domain-nimestä (**nordea-if.com**). Lisäksi sivuston nimestä puuttuu SSL-salaus eli HTTPS palvelinvarmenne sekä lukon kuva. (Järvinen 2012, 73.)

Kuvio 13. Esimerkki Nordea pankin huijaussivustosta, josta näkyy väärä domain-nimi nordea-if.com, puuttuva SSL-salaus eli HTTPS sekä lukon kuva (Järvinen 2012, 73)

Internet-sivuston aitoutta on syytä epäillä, jos henkilöasiakasta pyydetään valitsemaan sähköpostiviestistä pankkisivustolle vievä linkki tai jos henkilöasiakkaalta kysytään sähköpostilla verkkopankkitunnuksia. Tällaista sähköpostiviestissä olevaa linkkiä ei tule koskaan avata. (Järvinen 2012, 74; Rowlingson 2011, 66.) Myös Internet-sivustoilla olevissa linkeissä on syytä olla varovainen. Verkkopankkiin liittyvä Internet-sivuston osoite tulee kirjoittaa itse selaimen osoiteriville tai avata sivusto itse tallennetusta kirjanmerkistä. Sivuston osoite on silti vielä syytä tarkistaa, sillä haittaohjelma voi tällaisessakin tapauksessa ohjata huijaussivustolle. (Finanssialan Keskusliitto ry 2012b.) Myös pelkkä numeerinen IP-osoite ilman domain-nimeä ja maatunnusta on epäilyttävä. Sivuston aitoutta voi tarkistaa sillä, hyväksyykö sivusto kirjautumisen väärillä tunnuksilla. Oikea sivusto ei pyydä useaa verkkopankin tunnuslukua kerrallaan tai anna useaa sisäänkirjautumissivua. Jos näin tapahtuu, tulee henkilöasiakkaan kirjautua heti verkkopankista pois. (Järvinen 2012, 74–75.)

Sähköpostiviestien tietojen kalastelun torjunnassa voidaan käyttää roskapostisuodatusta, jossa suodatinohjelmalle luodaan suodatinsäännöt (Kiianmies 2010, 752). Torjuntasuodatin hidastaa hiukan selaimen käyttöä, mutta näytölle ilmestyy varoitussivu ja ilmoitus osoiteriville, jos näytöllä oleva sivusto on tietokalastelusivustojen luettelossa. (Flyktman 2010, 391.) Lisäksi Internet-selaimista ja Windows Liven sähköpostista löytyy tietojen kalastelun tunnistus- ja varoitustoimintoja (Finanssialan Keskusliitto ry 2011a; Flyktman 2011, 334). Esimerkiksi Internet Explorer -selaimen tietojen kalastelun SmartScreen torjuntasuodattimen käyttöönotto (Kuvio 14) tapahtuu Työkalut-valikosta. (Flyktman 2010, 391.)



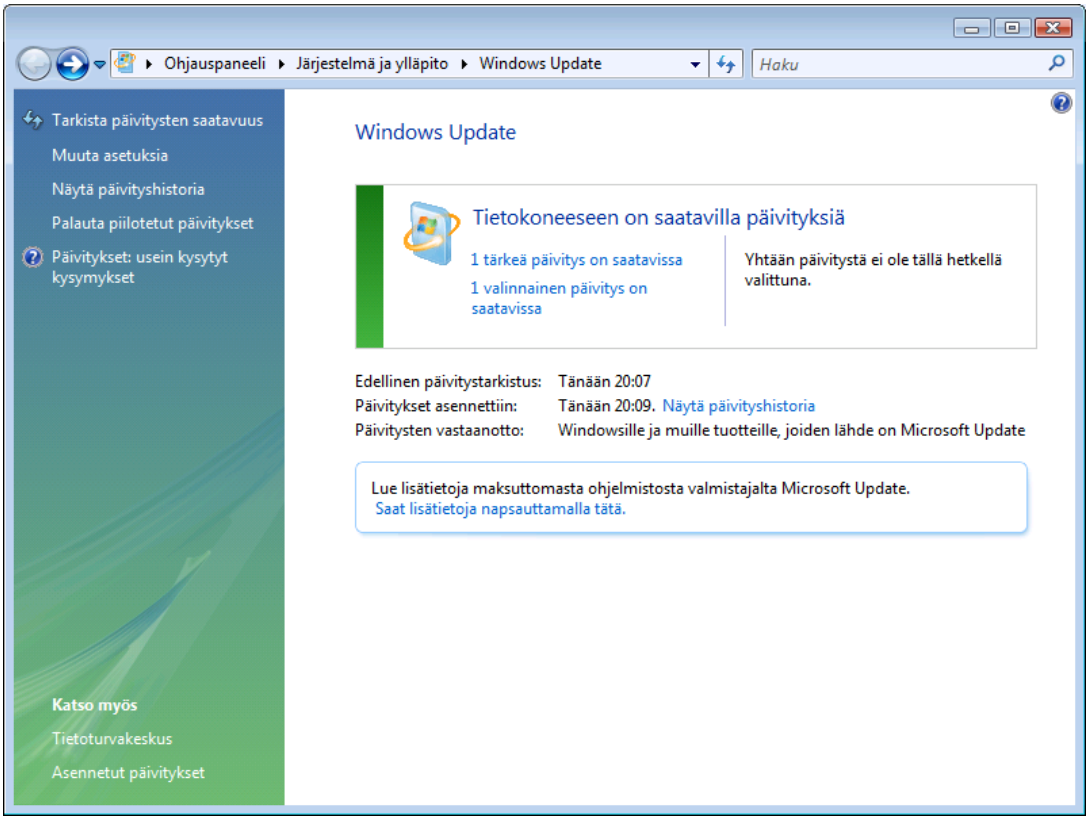
Kuvio 14. Esimerkki Internet Explorerin Työkalut-valikosta löytyvä SmartScreen torjuntasuodattimen käyttöönotto

Windows Live sähköpostin tietojen kalasteluun liittyvän torjuntasuodattimen saa päälle painamalla Alt-näppäintä -> Työkalut -> Turvallisuusasetukset -> Tietojen kalastelu. Suodattimen tarkoituksena on estää huijaukseen tarkoitetut viestit, jotka yritetään lähettää esimerkiksi jonkin tunnetun yhtiön nimissä sekä estää niihin vastaaminen. (Flyktman 2010, 410.) Tietojen kalastelun kehittyneemmän muodon eli pharming huijaussivustojen ns. ponnahdusikkunoiden torjunnassa voidaan käyttää suodatusohjelmia (Kiianmies 2010, 752; Tietosuojavaltuutetun toimisto 2010b, 3).

Internet-selaimen sivuhistorian välimuistiin jää tiedot käydyillä Internet-sivustoilla. Tällöin kuka tahansa tietokoneeseen samoilla käyttäjätunnuksilla kirjautuva voi esimerkiksi nähdä, mitä tunnuksia verkkopankissa on käytetty. Väliaikaiset Internet-tiedostot voidaan asettaa poistumaan automaattisesti, kun Internet-selain suljetaan. Esimerkiksi Internet Explorer -selaimessa tämän voi tehdä Internet-asetuksissa Lisäasetukset-välilehdeltä laittamalla ruksin kohtaan Tyhjennä Väliaikaiset Internet-tiedostot, kun selain suljetaan. (Kiianmies 2010, 776–778.)

Tietoturva- ja korjauspäivityksillä korjataan ja poistetaan Internet Explorer -selaimen, Windows-käyttöjärjestelmän ja sen eri osien tietoturva-aukkoja eli ohjelmointivirheitä, joita käytetään hyväksi haittaohjelmissa. Päivitykset asennetaan Windows Updaten

kautta. Päivitykset voivat tapahtua automaattisesti, käyttäjältä lupaa kysyen tai manuaalisesti. Windows Updaten asetuksiin pääsee esimerkiksi valitsemalla Internet Explorer -selaimesta Työkalut / Windows Update. Esimerkiksi Windows Updaten (Kuvio 15) Muuta asetuksia -linkistä voidaan valita, miten Windows asentaa päivitykset. Automaattisesti tapahtuvat päivitykset on helpoin tapa päivityksiin. (Flyktman 2011, 135; Kiianmies 2010, 537–539.)



Kuvio 15. Windows Updaten päivitykset

Käyttäjätilien valvonnalla estetään ilman käyttäjän lupaa tietokoneelle tehtävät muutokset ja ohjelmien käynnistykset. Kun tietokoneella ollaan sisäänkirjautuneena Normaali-käyttäjän oikeuksilla, käyttäjä ei voi tehdä tietokoneelle vahingossa muutoksia tai asentaa ohjelmia ilman järjestelmänvalvojan tunnuksia. Käyttäjätilien valvonnan asetuksia voidaan muuttaa Ohjauspaneelin Käyttäjätilistä. (Kiianmies 2010, 702–703).

Osa haittaohjelmista tarttuu tiedostojärjestelmän sijasta tietokoneen RAM-käyttömuistiin, joita virustentorjuntaohjelmistot eivät tunnista. Tällöin tulee käyttää muita työkaluja kuten Fitsecin pankkitroijalaisten tunnistustyökalua. (Viestintävirasto Kyberturvallisuuskeskus 2011c.) Lisäksi eri valmistajien Internet-sivustoilta voidaan käyttää

ilmaisia online-skannereita myös silloin, kun oman tietokoneen virustentorjuntaohjelma on vanhentunut. Online-skannereita ei tarvitse itse asentaa eikä päivittää. (Järvinen 2012, 205.)

Sähköpostin välityksellä asentuu tietokoneelle suurin osa haittaohjelmista liitetiedostojen ja huijausviestin välityksellä. Taulukossa 1 on ohjeistuksia sähköpostin turvalliseen käyttöön. (Kiianmies 2010, 762.)

Taulukko 1. Ohjeistuksia sähköpostin turvalliseen käyttöön (Finanssialan Keskusliitto ry 2011b; Kiianmies 2010, 762)

Ohjeistuksia sähköpostin turvalliseen käyttöön:
- älä luovuta pankkitunnuksia sähköpostitse, koska pankit eivät koskaan kysy pankkitunnuksia sähköpostitse
- älä kirjaudu verkkopankkiin sähköpostin linkistä
- poista epäilyttävä sähköposti avaamatta
- epäilyttävässä sähköpostissa voi olla tuntematon tai tunnettu lähettäjä
- tuntemasi henkilön lähettämän sähköpostin otsikko on erikoinen tai kirjoitettu vieraalla kielellä
- epäilyttävässä viestissä on tuntematon Internet-linkki, jolta saattaa käynnistyä haittaohjelma
- epäilyttävässä viestissä on liitetiedosto, joka käynnistää viruksen
- poista sähköpostin esikatselu käytöstä, koska esikatselu avaa viestin ja jotkut haittaohjelmat voivat tarttua tietokoneelle jo pelkästään esikatselusta.

6 Yhteenveto

Tämän opinnäytetyön yhteenvedossa esitetään työlle asetettujen tutkimuskysymysten tulokset ja johtopäätökset. Yhteenvedossa käydään myös läpi kirjoittajan työn etenemistä, omaa oppimista ja tuloksen hyväksikäyttömahdollisuuksia.

6.1 Tutkimustulokset ja johtopäätökset

Työn tavoitteena oli lisätä verkkopankkien henkilöasiakkaiden tietoisuutta verkkopankkihyökkäyksistä ja niiden torjuntamenetelmistä Microsoft Windows -käyttöjärjestelmän pöytäkoneiden ja kannettavien käytössä Suomessa.

Työlle asetetut tutkimuskysymykset olivat, missä tapauksissa pankit korvaavat verkkopankkihyökkäyksistä aiheutuneita henkilöasiakkaan rahallisia menetyksiä ja milloin eivät maksupalvelulain mukaan. Tavoitteena oli myös kartoittaa, millaisia henkilöasiakkaan verkkopankkiin kohdistuvia hyökkäyksiä on ja miten ne toimivat. Lisäksi tavoitteena oli kartoittaa, miten SSL-salaus ja käyttäjän todentamismenetelmät toimivat verkkopankissa sekä miten henkilöasiakas voi mahdollisesti tunnistaa ja torjua ennalta näitä verkkopankkihyökkäyksiä omilla toimenpiteillään.

Pankit korvaavat henkilöasiakkaan verkkopankkihyökkäyksistä aiheutuneita menetyksiä vain, jos asiakas on noudattanut huolellisuusvelvoitettaan pankkitunnusten käytössä ja ilmoittanut pankilleen viivytyksettä pankkitunnusten katoamisesta ja oikeudettomista käytöstapauksista. Myös tietoturvasta tulee huolehtia.

Verkkopankkihyökkäyksissä käytettävien haittaohjelmien tavoitteena on varastaa henkilöasiakkaan pankkitunnuksia ja siirtää niiden avulla henkilöasiakkaan rahoja tilisiirtona tietoverkkorikolliselle käyttämällä lokipalvelimia ja muuleja välikätenä. Tietojen varastamisessa käytetään erilaisia haittaohjelmia kuten viruksia, matoja, Troijan hevosia, vakoilu-, mainos-, ja urkintaohjelmia, rootkit-ohjelmia, selaimen kaappaajia, näppäilytallentimia ja takaovia. Tietojen kalastelussa henkilöasiakkaita huijataan tietoverkkorikollisten aitoa verkkopankkia muistuttaville Internet-sivustoille sähköpostin ja Internet-sivustojen linkeillä, joista voi asentua henkilöasiakkaan tietokoneelle haittaohjelma. Asi-

akkaita huijataan näillä sivustoilla antamaan omat pankkitunnuksensa. Lisäksi vakoiluohjelmat vakoilevat pankkitunnuksia tietokoneelta henkilöasiakkaan huomaamatta. Haittaohjelmia voidaan myös naamioida esimerkiksi peliksi. Haittaohjelmat käyttävät hyväksi Microsoft Windows -käyttöjärjestelmän, Internet-selainten ja selainten laajennuksissa olevia tietoturva-aukkoja.

SSL-salaus kytkeytyy verkkopankin sivustolla päälle sen jälkeen, kun Internet-selain on todennut palvelimen tiedot oikeiksi palvelimen varmenteesta ennen verkkopankin istuntoa. SSL-salauksen tunnistaa selaimen osoiterivillä olevasta HTTPS-protokollasta. Henkilöasiakas todennetaan henkilökohtaisilla pankkitunnuksilla ja vaihtuvilla tunnusluvuilla. Verkkopankkitunnuksilla tehtäviä tunnistautumisia käytetään myös yritysten ja yhteisöjen Tupas-tunnistautumisissa.

Henkilöasiakkaan suojautumiskeinoja verkkopankkihyökkäyksiä vastaan ovat maksun lisävahvistuksen käyttöönotto, palomuurin ja virustentorjuntaohjelmien käyttö sekä niiden kuten Windows-käyttöjärjestelmän ja Internet-selainten laajennusosien säännölliset päivitykset. Myös roskapostin ja tietojen kalastelun torjuntasuodatinta kannattaa käyttää. Osa ohjelmista pystyy myös piiloutumaan virustentorjuntaohjelmilta, jolloin on käytettävä myös muita erikseen suunniteltuja torjuntaohjelmia käyttömuistiin piiloutuvilta haittaohjelmilta.

Johtopäätöksenä voidaan todeta, että henkilöasiakkaan tehtävänä on oman tietokoneen tietoturvasta huolehtiminen. Tietoja varastavat haittaohjelmat ovat kehittyneitä ja muuntuvat koko ajan, jolloin haittaohjelmien tunnistaminen on vaikeaa. Tärkeää on myös tiedostaa, että virustentorjuntaohjelmat ja palomuurit eivät anna sataprosenttista suojaa. Virustentorjuntaohjelmien virustunnistekantoja ei ehditä aina heti päivittämään. Paras keino haittaohjelmien torjunnassa on pitää virustentorjuntaohjelma ajan tasalla ja pysyä valppaana sähköpostiviesteissä ja Internet-sivustoilla.

6.2 Työn eteneminen ja oma oppiminen

Opinnäytetyön kirjoittaminen alkoi syksyllä 2013 ja päättyi keväällä 2014. Opinnäytetyön kirjoittaminen vaatii aikaa ja pidempikestoista keskittymistä. Työn kirjoittamisen

etenemiseen vaikutti kirjoittajan perhetilanne työn laajuuteen nähden. Opinnäytetyöhön sopivia lähdeaineistoja oli aluksi hankala löytää. Osa lähteistä sisälsi vähän tietoa, joten lähdemateriaalia kertyi.

Opinnäytetyötä tehtäessä oppi tietämään miten tietoverkkorikolliset toimivat huijatessaan verkkopankin henkilöasiakkaita ja miten verkkopankkihyökkäykset toimivat. Jälkeenpäin ajatellen työssä käsiteltäviä huijaamistapoja olisi voinut tutkia jo alkuvaiheessa eikä jättää tämän osuuden kirjoittamista viimeiseksi. Tällöin olisi nähnyt selkeämmin työn laajuuden. Tutkimustyölle asetetut tavoitteet kuitenkin saavutettiin. Ilman opinnäytetyön ohjaajan avustusta työ ei olisi valmistunut ajallaan.

6.3 Tuloksen hyväksikäyttömahdollisuudet

Tästä opinnäytetyöstä hyötyvät verkkopankkien henkilöasiakkaat, jotka eivät tiedä ennen työn lukemista paljoa tietoverkkorikollisten nykyisistä toiminta- ja huijaustavoista. Työn luettuaan lukija on tietoisempi, kuinka tärkeää ennalta tehtävät omat suojautumiskeinot ovat.

Lähteet

Danske Bank 2012. Verkkopankissa käyttöön ulkomaanmaksujen lisävahvistus. Luettavissa: http://www.danskebank.fi/fi-fi/tietoa-danske-bankista/media/tiedotteet/pages/verkkopankissakayttoonulkomaanmaksujenlisavahvistus04122012.aspx. Luettu: 9.12.2013.

Finanssialan Keskusliitto ry 2013a. Pankkien TUPAS-tunnistuspalvelu palveluntarjoajille. Palvelukuvaus ja palveluntarjoajan ohje. Versio 2.4 2.12.2013. Luettavissa: http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas_varmennepalvelu_V_2.4.pdf. Luettu: 2.3.2014.

Finanssialan Keskusliitto ry 2013b. Tilastotietoja pankkien maksujärjestelmistä 2012. Luettavissa: http://www.fkl.fi/materiaalipankki/esitysaineistot/Sivut/default.aspx. Luettu: 24.9.2013.

Finanssialan Keskusliitto ry 2012a. Tiedote: Laskujen maksaminen verkossa jatkanut kasvuaan. Luettavissa: http://www.fkl.fi/ajankohtaista/tiedotteet/Sivut/Laskujen_maksaminen_verkossa_jatkanut_kasvuaan.aspx. Luettu: 28.9.2013.

Finanssialan Keskusliitto ry 2012b. Verkkopalveluiden turvallisuus. Luettavissa: http://www.fkl.fi/teemasivut/pankkiturvallisuus/kuluttajalle/Sivut/tietoturva.aspx. Luettu: 2.1.2014.

Finanssialan Keskusliitto ry 2011a. Varo huijaria! Luettavissa: http://www.fkl.fi/teemasivut/pankkiturvallisuus/vaarinkaytokset/Sivut/varo_huijaria.aspx. Luettu: 18.10.2013.

Finanssialan Keskusliitto ry 2011b. Verkkopankki. Luettavissa: http://www.fkl.fi/teemasivut/pankkiturvallisuus/kuluttajalle/Sivut/verkkopankki.aspx. Luettu: 18.10.2013.

Flyktman, R. 2011. Kannettava tietokone tehokäytössä Windows 7. Readme.fi. Helsinki.

Flyktman, R. 2010. Suuri PC-käsikirja - Windows 7. Readme.fi. Helsinki.

F-Secure 2014a. Miten pankkitoimintojen suojauksen voi ottaa käyttöön? Luettavissa: http://community.f-secure.com/t5/Tietoturvaa-PC/Miten-pankkitoimintojen/ta-p/31705. Luettu: 6.4.2014.

F-Secure 2014b. Mikä on pankkitoimintojen suojaus? Luettavissa: http://community.f-secure.com/t5/Tietoturvaa-PC/Mik%C3%A4-on-pankkitoimintojen/ta-p/31683. Luettu: 6.4.2014.

F-Secure 2014c. Mitä selaimia pankkitoimintojen suojaus tukee? Luettavissa: http://community.f-secure.com/t5/Tietoturvaa-PC/Mit%C3%A4-selaimia-pankkitoimintojen/ta-p/31685. Luettu: 6.4.2014.

F-Secure 2014d. Uutta teknologiaa F-Securelta verkkopankin turvalliseen käyttöön. Luettavissa: http://www.f-secure.com/fi/web/home_fi/news-info/product-news-offers/view/story/758833/Uutta%20teknologiaa%20F-Securelta%20verkkopankin%20turvalliseen%20k%C3%A4ytt%C3%B6%C3%B6n. Luettu: 5.4.2014.

Goodrich, M. & Tamassia, R. 2011. Introduction to Computer Security. Pearson. United States of America.

Haasio, A. 2013. Netin pimeä puoli. Suomalaisen Kirjallisuuden Seura. Helsinki.

Halminen, L. 2014. Vanha Windows voi viedä poliisin pakeille. Helsingin Sanomat, 41369, N:o 92, Kotimaa 4.4.2014, s. A17.

Hamunen, U. 2012. F-Secure: Pankkitroijalainen peräisin Venäjältä. Luettavissa: http://yle.fi/uutiset/f-secure_pankkitroijalainen_peraisin_venajalta/5053096. Luettu: 9.7.2013.

Hjelt, Y. 2014. Windows XP:n tietoturvapäivitykset loppuvat huhtikuussa – entäs siten? Luettavissa: http://yle.fi/uutiset/windows_xpn_tietoturvapaivitykset_loppuvat_huhtikuussa__entas_sitten/7144479. Luettu: 9.4.2014.

Iranto, A. 2012. Automaatin tiliote voi kertoa haittaohjelmasta. Luettavissa: http://yle.fi/uutiset/automaatin_tiliote_voi_kertoa_haittaohjelmasta/5053057. Luettu: 9.7.2013.

Jakobsson, M. 2012. The Death of the Internet. John Wiley & Sons, Inc., Hoboken. New Jersey. United States of America.

Järvinen, P. 2012. Arjen tietoturva: vinkit ja ratkaisut. Docendo. Jyväskylä.

Järvinen, P. 2010. Yksityisyys. Turvaa digitaalinen kotirauhasi. Docendo. Jyväskylä.

Kerkelä, L. 2014a. Huijausviestien määrä räjähtää käsiin. Helsingin Sanomat, 41356, N:o 79, Kotimaa 22.3.2014, s. 14.

Kerkelä, L. 2014b. Tullin nimissä lähetetyillä viesteillä huijattu jo 50 000 euroa. Luettavissa: http://www.hs.fi/kotimaa/a1396922107311. Luettu 9.4.2014.

Kiianmies, M. 2010. Suuri Windows 7 käsikirja. Readme.fi. Helsinki.

Kontkanen, E. 2011. Pankkitoiminnan käsikirja. 3. uudistettu painos. FINVA. Finanssi- ja vakuutuskustannus oy.

Leppänen, M. 2014. Microsoft lopettaa tänään Windows XP:n tietoturvapäivitykset. Luettavissa:

http://yle.fi/uutiset/microsoft_lopettaa_tanaan_windows_xpn_tietoturvapaivitykset/7178385. Luettu: 9.4.2014.

Linna, M. 2012. Tietovuodot ja -murrot ja niiden torjunta suomalaisessa yhteiskunnassa. Luettavissa: http://www.fkl.fi/kannanotot/lausunnot/Dokumentit/Tietovuodot_ja_murrot_ja_niiden_torjunta_suomalaisessa_yhteiskunnassa_15032012.pdf. Luettu: 21.1.2014.

Luottokunta 2013. Lainsäädäntö. Luettavissa: http://www.luottokunta.fi/Nets/Toimialatietoa/Lansaadanto/. Luettu: 24.1.2014.

Maksupalvelulaki 30.4.2010/290. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/2010/20100290. Luettu: 27.12.2013.

Microsoft 2014. Windows XP:n tuki on päättynyt. Luettavissa: http://windows.microsoft.com/fi-fi/windows/end-support-help. Luettu: 9.4.2014.

MTV Oy 2012. Näin pankkitroijalainen iskee koneeseesi. Luettavissa: http://www.mtv.fi/uutiset/kotimaa/artikkeli/nain-pankkitroijalainen-iskee-koneeseesi/1886216. Luettu: 10.7.2013.

Nordea 2014. Phishing. Luettavissa: http://www.nordea.fi/henkil%C3%B6asiakkaat/p%C3%A4ivitt%C3%A4iset+raha-asiat/internetpalvelut/phishing/700934.html. Luettu 24.1.2014.

Nordea 2013a. Kysymyksiä ja vastauksia maksun lisävahvistuksesta. Luettavissa: http://www.nordea.fi/Henkilöasiakkaat/Päivittäiset+raha-asi-at/Tilit+ja+maksut/Tilisiirto/40147.html?searchPhrase=Kysymyksi%u00e4+ja+vastauksia+maksun+lis%u00e4vahvistuksesta&bb=0#fa0d258c-4d1e-45f0-bc14-f1dceeeba5e3. Luettu: 25.11.2013.

Nordea 2013b. Maksun lisävahvistus on osa maksutoimeksiantoa. Luettavissa: http://www.nordea.fi/Yritykset+ja+yhteisöt/Maksuliike/Yhteys+pankkiin/Verkkopankki/942582.html?searchPhrase=maksun+lis%u00e4vahvistus&bb=0#29c18013-3dc4-4def-924e-8c6b1bc96cc3. Luettu: 26.12.2013.

Nordea 2013c. Näin toimii maksun lisävahvistus. Luettavissa: http://www.nordea.fi/Henkilöasiakkaat/Päivittäiset+raha-asi-at/Tilit+ja+maksut/Tilisiirto/40147.html?searchPhrase=n%u00e4in+toimii+maksun+lis%u00e4vahvistus&bb=0#e475f314-027b-433b-90bd-73440502bc1e. Luettu: 28.9.2013.

OP-Pohjola-ryhmä 2013a. Maksun lisävahvistus. Luettavissa: https://www.op.fi/op/henkiloasiakkaat/opastus/haku/maksun-lisavahvistus?cid=151743201&srcpl=3. Luettu: 25.11.2013.

OP-Pohjola-ryhmä 2013b. Mitä tarkoittaa maksun lisävahvistus? Luettavissa: https://www.op.fi/op/usein-kysyttya/usein-kysyttya/tietoturva/mita-tarkoittaa-maksun-lisavahvistus?cid=151724926&srcpl=3. Luettu: 9.12.2013.

OP-Pohjola-ryhmä 2013c. OP-Pohjola: Osa asiakkaista liian huolettomia sähköisissä raha-asioissaan. Luettavissa: https://www.pohjola.fi/pohjola?cid=-1052. Luettu: 27.12.2013.

OP-Pohjola-ryhmä 2011a. Avainluku ja maksun lisävahvistus lisäävät OP-verkkopalvelun turvallisuutta. Luettavissa: https://www.op.fi/op/henkiloasiakkaat/opastus/avainluku-ja-maksun-lisavahvistus-lisaavat-op-verkkopalvelun-turvallisuutta?cid=151513742&srcpl=3. Luettu: 9.12.2013.

OP-Pohjola-ryhmä 2011b. Maksun lisävahvistuksen käytön ohje. Luettavissa: https://www.op.fi/op/henkiloasiakkaat/tietoturva/maksun-lisavahvistuksen-kayton-ohje?cid=151502823&srcpl=3. Luettu: 25.11.2013.

Pietiläinen, T. 2010. Nordea vaatii vahvistuksen suurille tai oudoille nettimaksuille. Luettavissa:
http://www.hs.fi/talous/artikkeli/Nordea+vaatii+vahvistuksen+suurille+tai+oudoille+nettimaksuille/1135252928374. Luettu: 25.11.2013.

Poliisi 2014a. Huijauksen monet muodot. Luettavissa:
http://www.poliisi.fi/poliisi/krp/home.nsf/pages/5aba1cd4b1d3b896c22570fb0057ca71. Luettu: 24.1.2014.

Poliisi 2014b. Identiteettirikokset ja kohdistetut hyökkäykset tietorikosten nousevia ilmiöitä. Luettavissa:
http://www.poliisi.fi/poliisi/krp/home.nsf/Pages/4E2E3CA9B18035C8C22579E80046AC48. Luettu: 18.10.2013.

Poliisi 2014c. Älä ala muuliksi. Luettavissa:
http://www.poliisi.fi/poliisi/krp/home.nsf/pages/699DA9EC5E48CDA0C225785E0054C79C?opendocument. Luettu: 24.1.2014.

Ranta, N. 2013a. MTV selvitti: Tämä haittaohjelma uhkaa suomalaisia verkkopankkien käyttäjiä. Luettavissa: http://www.mtv.fi/uutiset/rikos/artikkeli/mtv-selvitti--tama-haittaohjelma-uhkaa-suomalaisia-verkkopankkien-kayttajia/2416416. Luettu: 18.1.2014.

Ranta, N. 2013b. Näin rahat voidaan viedä suomalaisen pankkitileiltä täysin huomaamatta. Luettavissa: http://www.mtv.fi/uutiset/rikos/artikkeli/nain-rahat-voidaan-vieda-suomalaisten-pankkitileilta-taysin-huomaamatta/2416430. Luettu: 19.1.2014.

Ranta, N. 2013c. Suomalaistileiltä katosi satojatuhansia euroja verkkohyökkäyksissä. Luettavissa: http://www.mtv.fi/uutiset/rikos/artikkeli/suomalaistileilta-katosi-satojatuhansia-euroja-verkkohyokkayksissa/2418148. Luettu 19.1.2014.

Rowlingson, R. 2011. The Essential Guide to Home Computer Security. BCS. United Kingdom.

Säästöpankki 2013. Maksupalvelulaki säätelee henkilöasiakkaan maksupalveluja. Luettavissa: https://www.saastopankki.fi/maksupalvelulaki-henkiloasiakkaan-kannalta. Luettu: 27.12.2013.

Tietosuojavaltuutetun toimisto 2010a. Palomuuri, mikä se on? Luettavissa: www.tietosuoja.fi/uploads/khezzfmwctbvp.pdf. Luettu: 27.10.2013.

Tietosuojavaltuutetun toimisto 2010b. Pharming, mitä se on? Luettavissa: http://www.tietosuoja.fi/uploads/ylrxqp2uwqra0q.pdf. Luettu: 27.19.2013.

Tietoturvaopas 2011. Palveluiden turvallinen käyttö. Luettavissa: http://www.tietoturvaopas.fi/internetinpalvelut/palveluidenturvallinenkaytto.html. Luettu: 25.11.2013.

Viestintävirasto 2013. Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne. Luettavissa: https://www.viestintavirasto.fi/tietoturva/sahkoinentunnistaminenjaallekirjoitus.html. Luettu: 2.1.2014.

Viestintävirasto Kyberturvallisuuskeskus 2014a. Tietojenkalastelukampanja jatkuu yhä aktiivisena. Luettavissa: https://www.cert.fi/attachments/tietoturvakatsaukset/FlsxtSj7M/Tietojenkalastelurapportti.pdf. Luettu: 18.4.2014.

Viestintävirasto Kyberturvallisuuskeskus 2014b. Tietoturva nyt! Huhtikuu. Luettavissa: https://www.cert.fi/tietoturvanyt/2014/04/.html. Luettu: 21.4.2014.

Viestintävirasto Kyberturvallisuuskeskus 2013. CERT-FI-tapahtumailmoitukset. Luettavissa: https://www.cert.fi/katsaukset/2013/tt_katsaus_3_13/poikkeamat3_13/cert_ilmoitukset_3_13.html. Luettu: 11.4.2014.

Viestintävirasto Kyberturvallisuuskeskus 2012. Suomalaiset verkkopankit haittaohjelmien kohteina. Luettavissa: https://www.cert.fi/katsaukset/2012/tietoturvakatsaus_1-2012/verkkopankit.html. Luettu: 2.10.2013.

Viestintävirasto Kyberturvallisuuskeskus 2011a. Kahdeksan suomalaista verkkopankkia Zeus-haittaohjelman kohteena. Luettavissa: https://www.cert.fi/tietoturvanyt/2011/07/ttn201107181108.html. Luettu: 2.10.2013.

Viestintävirasto Kyberturvallisuuskeskus 2011b. Man in the Middle -hyökkäyksen torjunta. Luettavissa: https://www.cert.fi/tietoturvanyt/2011/09/ttn201109281253.html. Luettu 22.4.2014.

Viestintävirasto Kyberturvallisuuskeskus 2011c. Työkalu yleisimpien pankkitroijalaisten tunnistukseen. Luettavissa: https://www.cert.fi/tietoturvanyt/2011/08/ttn201108231354.html. Luettu: 14.10.2013.

Viestintävirasto Kyberturvallisuuskeskus 2010. CERT-FI. Tietoja varastavat haittaohjelmat. Luettavissa: http://www.cert.fi/attachments/certtiedostot/5n8rVzH5M/Tietoja_varastavat_haittaohjelmat.pdf. Luettu: 2.10.2013.

Virukset.fi 2012. Citadel virus poistaminen. Luettavissa: http://virukset.fi/citadel-virus/. Luettu: 17.2.2014.

Väkimies, T. 2013. Asiantuntijalta yllättävä vinkki verkkopankin käyttöön. Luettavissa: http://www.mtv.fi/uutiset/rikos/artikkeli/asiantuntijalta-yllattava-vinkki-verkkopankin-kayttoon/2419612. Luettu: 17.2.2014.

Wuolijoki, S., & Hemmo, M. 2013. Pankkioikeus. 2. uudistettu painos. Talentum. Helsinki.