Helsingin yliopisto
Taloustieteen laitos
Kuluttajaekonomia

Verkkopankin käyttäjien kokemuksia ja käsityksiä palvelun turvallisuudesta

MAISTERIN TUTKIELMA KULUTTAJAEKONOMIASSA MAATALOUS-METSÄTIETEIDEN MAISTERIN TUTKINTOA VARTEN

Iiris Setälä
Toukokuu 2010

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department	
Maatalous-metsätieteellinen tiedekunta	Taloustieteen laitos	
Tekijä — Författare — Author		
Iiris Setälä		
Työn nimi — Arbetets titel — Title		
Verkkopankin käyttäjien kokemuksia ja käsityksiä palvelun turvallisuudesta		
Oppiaine —Läroämne — Subject		
Kuluttajaekonomia		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Maisterin tutkielma	Toukokuu 2010	79 s. + liitteet 3 s.

Tiivistelmä — Referat — Abstract

Tämän tutkimuksen tarkoituksena on kartoittaa verkkopankin käyttäjien tietoisuutta verkkopankin käyttöön liittyvistä turvallisuusuhista. Lisäksi tarkoituksena on selvittää, onko tutkittaville muodostunut omia keinoja parantaa verkkopankissa asioinnin turvallisuutta. Tarkastelun kohteena on myös tutkittavien näkemys siitä, kenen vastuulla on korvata mahdolliset taloudelliset menetykset onnistuneen huijauksen johdosta.

Tutkimusaineisto koostuu kahdeksan tottuneen verkkopankin käyttäjän teemahaastatteluista. Aineistoa tarkastellaan faktanäkökulmasta ja analyysissä on käytetty teemoittelua ja tyypittelyä. Kuluttajahaastattelujen lisäksi tehtiin kaksi asiantuntijahaastattelua. Tätä aineistoa käytetään lähteiden tapaan eikä sitä ole tarkoitus analysoida kuten muita haastatteluja.

Phishing on rikollista toimintaa, jonka tavoitteena on saada haltuun uhrin henkilökohtaisia tietoja kuten verkkopankkitunnuksia. Tutkimuksessa selvisi, että haastateltavat olivat melko tietämättömiä erilaisista phishingin muodoista. Lähes kaikki olivat kuitenkin kuulleet kalasteluviesteistä. Niitä ei koettu uhkana itselle koska ne osattiin tunnistaa ja tiedettiin, että viesteihin ei saa vastata vaan ne tulee poistaa.

Kuluttaja voi omalla käytöksellään parantaa verkkoasioinnin turvallisuutta. Haastateltavat vaikuttivat olevan melko huolellisia asioidessaan verkkopankissa, vaikka pankista ei oltu juuri annettu ohjeistusta. Verkkopankkitunnusten eri osia säilytettiin erillään ja kiinteät osat muistettiin pääasiassa ulkoa. Verkkopankissa asiointia julkisessa käytössä olevilta koneilta vältettiin yleisesti ja moni rajoitti verkkopankin käytön ainoastaan kotiin ja työpaikalle.

Haastateltavat kokivat vastuunjaon taloudellisista menetyksistä riippuvan tilanteesta. Pankkia ei heidän mielestään voi asettaa vastuuseen jos tunnukset on itse annettu vääriin käsiin. Muissa tapauksissa koettiin kuitenkin korvausvastuun olevan pankilla. Kuluttajan suurempi tietoisuus turvallisuusuhista näyttäytyy tässä aineistossa kuluttajan vastuuta kasvattavana tekijänä.

Avainsanat — Nyckelord — Keywords

verkkopankki, turvallisuus, uhka, riski, tiedotus, vastuunjako

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — Övriga uppgifter — Further information

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department	
Faculty of Agriculture and Forestry	Department of Economics and Management	
Tekijä — Författare — Author		
Iiris Setälä		
Työn nimi — Arbetets titel — Title		
Internet bank users´ experiences and ideas about the security of the service		
Oppiaine —Läroämne — Subject		
Consumer Economics		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Master's thesis	May 2010	79p. + appendixes 3p.

Tiivistelmä — Referat — Abstract

The purpose of this study is to find out weather or not the users of internet bank are aware of the security threats concerning the use of the service. The intention is to find out also if the interviewees have created some methods of their own to raise the security level of their use of internet bank. Still, the purpose of the study is to clarify the interviewees' opinions about the economically responsible party in case of economic losses.

Research material consists of eight internet bank users' interviews. The statements of the interviewees are considered from factual point of view and analysed by dividing them under certain themes and types. In addition to the interviews of consumers, also two experts were interviewed. This material works more like source of information and it is not analysed like the other interviews. These two interviews were carried out to get information about the security level of Finnish internet banks.

Phishing is criminal activity by which the criminals' objective is to gather confidential information, such as access codes for internet bank, from the victims. This research revealed that the interviewees were quite unaware of the different forms of phishing attacks. However, almost everyone had heard of the phishing e-mails. They were not seen as a threat because the interviewees knew how to identify those e-mails and also that they should never be answered but deleted immediately.

Consumers can enhance the security of internet transactions by their own behaviour. The interviewees seemed to be quite careful when using internet bank even though they had not gotten much directions from the bank. The different parts of internet bank access codes were kept separately and the fixed parts were mostly known by heart. Some interviewees used internet bank merely at home or at work place and public computers were broadly avoided for that purpose.

The interviewees thought that the economically responsible party in the case of economical losses depends on the situation. Bank could not be held responsible if the access codes were given to outsiders by self. In other cases however the interviewees saw bank as the responsible party. Greater awareness of security threats seems in this research material to increase the responsibility of consumer. Consumers' responsibility would also increase if banks would increasingly inform consumers about these security threats.

Avainsanat — Nyckelord — Keywords

Internet bank, security, phishing, threat, risk, informing

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — Övriga uppgifter — Further information

Sisältö:

Taulukot ja kuviot:

1 Johdanto

Perinteisesti kuluttajat ovat hoitaneet pankkiasiansa konttoreissa. Viime vuosikymmenten aikana teknologia on kuitenkin kehittynyt nopeasti ja nykyään monet palvelut ovat saatavilla internetin kautta. Myös pankit ovat siirtäneet palveluitaan verkkoon, ja nykyään lähes kaikki pankkiasiat on mahdollista hoitaa itsenäisesti verkkopankissa.

Internetin käyttö on tavallista suomalaisten keskuudessa ja verkkopankkipalveluita käytetään laajalti. Vuoden 2008 lopussa suomalaisilla oli 4,7 miljoonaa verkkopankkisopimusta (FK 2009a, 21). Monissa muissa maissa verkkopankin käyttö ei ole saavuttanut yhtä suurta suosiota, ja tutkimuksia on tehty lähinnä verkkopankkipalvelujen omaksumiseen vaikuttavista tekijöistä.

Kuluttajien huolet palvelujen turvallisuudesta on nähty monissa kansainvälisissä tutkimuksissa esteenä verkkopankkipalvelujen käytölle (mm. Laforet & Li 2005; Hua 2009; Sathye 1999). Suomessa palvelun turvallisuudella ei sen sijaan ollut merkittävää vaikutusta verkkopankin käyttöönotolle (Pikkarainen ym. 2004). Eivätkö suomalaiset sitten ole huolissaan verkkopankkipalvelujen turvallisuudesta? Verkkopankkipalvelujen omaksumista käsittelevä Pikkaraisen ym. tutkimus tehtiin vuonna 2004, jolloin Suomessa ei oltu vielä tavattu phishing-viestejä. Phishing-viesteillä tarkoitetaan kuluttajille lähetettyjä väärennettyjä sähköpostiviestejä, joiden tarkoituksena on saada viestin vastaanottaja luovuttamaan lähettäjälle arkaluontoisia tietoja kuten pankkitunnuksia, luottokortin numeroa tai henkilötietoja (Sarel & Marmorstein 2006).

Lokakuussa 2005 jopa satoja tuhansia Nordean asiakkaita lähestyttiin phishing-viesteillä. Ensimmäiset viestit olivat englanninkielisiä, mutta myöhemmin asiakkaat saivat myös suomenkielisiä viestejä. Sain itsekin tällaisen viestin ja muistan sen olleen täynnä kirjoitusvirheitä ja muutenkin erittäin huonoa suomenkieltä. Tästä huolimatta osa asiakkaista luovutti tunnuksiaan huijareille, jotka onnistuivat aiheuttamaan kyseisille asiakkaille taloudellisia tappioita. Tällöin Nordea kuitenkin korvasi asiakkailleen aiheutuneet vahingot.

Pankin ja sen asiakkaiden välinen turvallisuussuhde on olennaisesti muuttunut palvelujen siirryttyä verkkoon. Aiemmin pankkiasioinnin turvallisuutta uhkasivat pankkiryöstäjät ja ryöstöt kohdistuivat suoraan pankkikonttoreihin. Nykyään taas uhreja voivat olla yksittäiset verkkopankkiasiakkaat. Rikolliset pyrkivät saamaan uhreiltaan verkkopankkiin kirjautumiseen vaadittavia tunnuslukuja esimerkiksi sähköpostitse, väärennettyjen verkkosivujen kautta tai asentamalla uhrien koneille erilaisia haittaohjelmia (Kidra & Kruegel 2006).

Millainen sitten on vastuunjako tässä uudessa tilanteessa? Turvallisuusongelman aiheuttaja on selvä; se on epäilemättä rikollinen, joka tunkeutuu asiakkaan reviirille. Uudenlainen turvallisuusuhka eli verkossa toimiva rikollinen voi kuitenkin sijaita missä päin maailmaa tahansa ja näitä henkilöitä voi olla äärimmäisen vaikea asettaa vastuuseen teoistaan. Voidaankin kysyä onko taloudellinen vahinkovastuu tällöin pankilla, joka on tarjonnut alustan rikolliselle toiminnalle vai asiakkaalla, joka on kenties ollut huolimaton ja antanut salaiset tunnuksensa rikolliselle tai ei ole pitänyt huolta kotikoneensa turvallisuudesta eli virustorjunnasta ja palomuurista ja on näin altistanut itsensä rikolliselle toiminnalle? Kysymys on ongelmallinen ja monitahoinen, mutta pyrin tässä tutkimuksessa valottamaan asiaa sekä kuluttajien että verkkoturvallisuuden asiantuntijoiden näkökulmasta.

Maisterin tutkielmani aiheena on verkkopankkipalvelujen turvallisuus. Tutkin sitä ovatko verkkopankin asiakkaat ylipäätään tietoisia turvallisuusuhista ja jos ovat, millaisia tuntemuksia nämä uhat heissä herättävät. Tarkoituksena on saada selville, onko tutkittavia tai heidän tuttaviaan lähestytty huijausviesteillä tai onko jouduttu tilanteisiin, joissa turvallisuutta olisi syytä epäillä. Selvitän myös sitä, mistä tutkittavat ovat saaneet tietoa turvallisuuteen liittyen ja ovatko he tyytyväisiä tiedotuksen tasoon. Tarkastelen tutkimuksessani myös kuluttajien näkemyksiä taloudellisesta vastuunjaosta – kokevatko he olevansa itse vastuussa mahdollisista taloudellisista menetyksistä vai onko korvausvastuu heidän mielestään pankilla.

Kiinnostuin aiheesta tehdessäni kandidaatin tutkielmaani verkkopankkipalvelujen käyttöön vaikuttavista tekijöistä vuonna 2005. Lukiessani aiempia tutkimuksia huomasin, että muualla maailmassa tehdyissä tutkimuksissa vastaajat olivat erittäin

huolissaan palvelujen turvallisuudesta toisin kuin Suomessa. Juuri ennen tutkielman valmistumista alkoi täälläkin esiintyä phishing-viestejä ja aloin pohtia onko näillä vaikutusta suomalaisten jo tuolloin hyvin yleiseen verkkopankkipalvelujen käyttöön. Koska palvelujen käyttö on kuitenkin edelleen tasaisesti lisääntynyt – vuoden 2003 lopussa 2,9 miljoonalla suomalaisella oli verkkopankkitunnukset (FK 2008, 2) – aloin miettiä sitä, ovatko suomalaiset kovinkaan tietoisia turvallisuusuhista.

Seuraavassa luvussa käyn läpi tutkimuksen lähtökohtia. Aloitan katsauksella kuluttajaekonomian tutkimusperinteeseen verkkoasioinnissa, jonka jälkeen esittelen kansainvälistä tutkimusta verkkopankkipalvelujen turvallisuudesta. Suomessa turvallisuusnäkökohtia ei ole juurikaan tutkittu, joten verkkopankkiasioinnin turvallisuutta käsitellessäni nojaan pitkälti kansainväliseen keskusteluun. Luvussa 2.2 kerron laadullisen tutkimukseni toteutuksesta eli haastateltavien valinnasta ja käyttämästäni tutkimusmenetelmästä. Päätän luvun raportoimalla aineiston analysoinnista ja tutkimuksen luotettavuudesta.

Luku kolme pohjustaa varsinaisia verkkopankin turvallisuuteen liittyviä lukuja neljä ja viisi. Siinä käyn läpi suomalaisten internetin ja verkkopankin käyttöä yleensä. Luvussa neljä käsittelen verkkopankin käyttöön liittyviä turvallisuusuhkia ja niistä tiedottamista. Luvussa viisi kerron sekä pankkien että kuluttajien mahdollisuuksista parantaa verkkopankkiasioinnin turvallisuutta ja esittelen tutkittavien näkemyksiä taloudellisesta vastuunjaosta pankin ja asiakkaan välillä. Päätän työni johtopäätöksiin luvussa kuusi.

2 Tutkimuksen lähestymistapa

Kuluttajaekonomian tutkimuksissa on tarkasteltu jonkin verran verkkopalveluita. Tutkimuksissa pohditaan paljolti sitä, mikseivät verkkopalvelut ole saaneet osakseen suurempaa suosiota toisin kuin verkkopankki. Keskustelu verkkopankin turvallisuudesta taas on hyvin kansainvälistä. Tässä luvussa esittelen ensin kuluttajaekonomian tutkimusperinnettä verkkoasioinnista ja kansainvälistä verkkoturvallisuudesta tehtyä tutkimusta. Tämän jälkeen käyn läpi tutkimuksen toteutusta ja pohdin riskin ja uhan käsitteitä. Päätän luvun kertomalla aineiston analyysistä ja arvioimalla tutkimuksen luotettavuutta.

2.1 Verkkoasioinnin tutkimusperinne

Kuluttajaekonomian tutkimuksia

Tietotekniikka on kehittynyt valtavin harppauksin kahden viimeisen vuosikymmenen aikana. Mika Pantzar (1996) käsittelee muiden laitteiden ohella tietokoneiden yleistymisen historiaa. Alun perin tietokoneet suunniteltiin lähinnä fyysikoiden ja matemaatikoiden työvälineiksi, ja niitä jopa kutsuttiin matematiikkakoneiksi. Vielä 1980-luvun lopulla arvioitiin, etteivät tietokoneet tule yleistymään kodin tarpeistossa. (Pantzar 1996, 87-90.)

Pantzar (1996, 97) on pohtinut mitä ihmisille tapahtuu kun virikkeiden määrä kasvaa jatkuvasti – johtaako tiedon määrän kasvu tiedon pinnallistumiseen vai korostuuko tietoa välittävien tahojen rooli. Itse arvioisin, että tapahtuu molempia. Toisaalta ihmisten uutisten seuraaminen on varmastikin lisääntynyt internetin myötä. Uutistoimistojen verkkosivuja päivitetään useita kertoja päivässä, joten uutiset tavoittavat ihmiset miltei reaaliajassa kun aiemmin ne on kuultu illan uutislähetyksestä tai luettu seuraavan päivän lehdestä. Toisaalta uutiset eivät kenties enää järkytä ihmisiä niin paljon kun kuvia sotien uhreista ja eri puolilla maailmaa tapahtuvista katastrofeista näkee lähes päivittäin. Nykyään informaatiotulva on niin suuri, että osa uutisista jää kuluttajilta myös täysin huomioitta – tästä saadaan esimerkki myös tässä tutkimuksessa.

Kuluttajaekonomian pro gradu –tutkielmissa on käsitelty jonkin verran sähköisiä eli internetin kautta tarjottavia palveluita. Anna Kiiskinen (2007) tutki sähköisen ostamisen ongelmia. Verkkokauppojen suosio ei ole kasvanut odotetulla tavalla, vaikka internetin käyttö on Suomessa arkipäiväistä. Tuotetietoa haetaan yleisesti verkosta, mutta tuotteita ostetaan enemmän puhelin- ja postimyynnistä kuin verkkokaupoista. (mt., 4-5.)

Verkkokaupat tarjoavat kuluttajille monia etuja verrattuna perinteisiin kauppoihin. Kiiskisen tutkimustaan varten tekemissä haastatteluissa verkkokauppojen hyödyiksi mainittiin muun muassa niiden tarjoama laaja tuotevalikoima sekä edulliset hinnat. Internetin kautta on mahdollista tilata tuotteita, joita ei ole saatavilla oman lähialueen kaupoista. Verkkokaupoista voi käytännössä tilata tavaraa mistä päin maailmaa tahansa. Lisäksi hintavertailu on helppoa kun hinnat ovat esillä verkossa. Ostokset voi myös hoitaa vuorokaudenajasta riippumatta ja kotoa poistumatta. (Kiiskinen 2007, 56-57.) Palvelujen aika- ja paikkariippumattomuus on yhteinen tekijä kaikille verkkopalveluille. Myös pankkiasiat voi hoitaa verkossa vuorokaudenajasta ja sijainnista riippumatta.

Sähköisen ostamisen ongelmiksi Kiiskisen (2007) tutkittavat nostivat muun muassa pitkät toimitusajat sekä joidenkin verkkokauppasivustojen sekavuuden. Verkkokaupassa myös mahdollisuus tuotteiden kosketteluun ja konkreettiseen tutkimiseen puuttuu. Maksuvaihtoehdoista luottokortilla maksaminen koettiin turvattomaksi, ja eräs vastaaja koki miellyttävämmäksi sellaiset verkkokaupat, joissa ostokset on mahdollista maksaa verkkopankin kautta. (mt., 53-55.) Raijaksen (2002) mukaan suurin este verkkokaupalle onkin juuri asiakkaiden haluttomuus luovuttaa luottokorttitietojaan. Raijas epäilee, että kuluttajien voimakas epäluulo luottokorttimaksamista kohtaan verkossa saattaisi johtua median uutisoinnista luottokorttitietojen väärinkäytöksistä. (mt., 204.) Itse pohdin tässä työssä osaltani sitä, tiedotetaanko verkkopankkiin liittyvistä turvallisuusuhista riittävästi. Oma näkemykseni on se, että turvallisuusuhista tulisi tiedottaa laajalti unohtamatta kuitenkaan kertoa siitä, kuinka kuluttajat voivat omalla toiminnallaan pyrkiä estämään joutumista huijauksen kohteeksi. Tiedotuksen tarkoituksena ei saisi olla

pelon lietsonta vaan ihmisten tietoisuuden lisääminen ja ohjeistaminen huolelliseen verkkoasiointiin.

Eräs sähköisen ostamisen suurista ongelmista on luottamuksen puute. Fyysisen kontaktin puuttuessa luottamuksen rakentaminen yritykseen on vaikeampaa verkkokaupassa kuin perinteisessä myymäläympäristössä. Luottamus verkkokaupassa pohjautuu siis yrityksen antamiin lupauksiin, joihin asiakkaan on voitava luottaa. Yrityksen maineella on tärkeä rooli verkkoympäristössä, ja usein kuluttajat haluavatkin asioida jo ennestään tuttujen yritysten kanssa ja toisaalta tilata jo ennestään tuttuja tuotteita. (Raijas 2002, 197-199.)

Luottamus yritykseen on äärimmäisen tärkeää myös pankkiasioinnissa. Suomessa kuluttajien luottamus pankkeihin on vahva ja se juontaa juurensa suomalaisesta pankkihistoriasta. Suomessa oli hyvin pitkään tilanne, jossa markkinoilla kilpaili vain muutama pankki ja ala oli vakaa. Kuluttajat oppivat luottamaan pankkien vakavaraisuuteen ja myös koko suomalainen yhteiskunta on luottanut pankkeihin. Pankit ovat toimineet Suomessa perinteisesti pääasiallisena rahoittajana sekä yrityksille että kuluttajille. Lisäksi palkat on maksettu työntekijöiden tileille jo 1970-luvulta lähtien ja tästä syystä valtaosalla kansalaisista on ollut asiakassuhde pankkiin jo tuolloin. Pankkien välinen kilpailu oli maltillista ja asiakkaiden pankkisuhteet ovat olleet jopa elinikäisiä. (Riipinen & Tinnilä 2004, 21.) Kansalaisten vahva luottamus pankkeja kohtaan on varmasti edesauttanut laajaa verkkopankin omaksumista Suomessa.

Mirella Lähteenmäki (2009) on tutkinut väitöskirjassaan kuluttajien henkilötietojen keräämistä markkinointitarkoituksiin. Lähteenmäki esittää, että hankkiakseen mieluisia tuotteita ja palveluita kuluttajien on joustettava yksityisyytensä suhteen kun verkkopalveluissa rekisteröityminen on pakollista (mt., 29). On totta, että verkossa asioidessa henkilötietoja on pakko luovuttaa erinäisille yrityksille. Toisaalta eikö ole myös yrityksille sallittua pyrkiä minimoimaan riskejä verkkokaupassa? Mikäli henkilötietoja ei kysyttäisi, miten kauppias voisi varmistua siitä, että hän saa myös maksun toimittamastaan tuotteesta? Oikeutus asiakkaiden henkilötietojen kysymiseen edellyttää toki tietojen huolellista säilyttämistä ja varmistumista siitä, etteivät tiedot pääse ulkopuolisten käsiin.

Myös Raijas (2002) kertoo kuluttajien olevan huolissaan yksityisyytensä vaarantumisesta, joka liittyy nimenomaan pakolliseen henkilötietojen luovuttamiseen verkkokaupoissa asioidessa. Raijaksen mukaan yritykset voivat kuitenkin lisätä kuluttajien luottamusta kertomalla asiakkailleen selkeästi, miksi tietoja pyydetään sekä mihin tarkoitukseen ja millä tavalla kerättyjä tietoja käytetään. Luottamusta lisää myös lupaus siitä, ettei luovutettuja henkilötietoja välitetä muille osapuolille. (Raijas 2002, 203-206.) Tässä tutkimuksessa näkökulma on toinen, koska tutkin rikollisin keinoin kerättäviä arkaluontoisia tietoja.

Anne Korhonen (2001) on tarkastellut WAP-pankkipalvelujen käyttöä pro gradu -tutkielmassaan. WAP eli Wireless Application Protocol -palvelut ovat matkapuhelimen kautta käytettäviä verkkopalveluita. Yhtenä tutkimuskysymyksenä on tässäkin tutkimuksessa se, mikseivät palvelut ole saaneet suurempaa suosiota. WAP-palvelujen käyttäjille verkkopankki oli tärkein kanava pankkiasioiden hoitoon. Pankkiautomaatit koettiin toiseksi tärkeimmäksi palvelukanavaksi ja WAP-palvelut kolmanneksi tärkeimmäksi. WAP-palveluita käyttämättömät henkilöt kokivat automaatit tärkeimmäksi pankkipalvelukanavaksi. Toiseksi tärkein kanava oli verkkopankki, ja kolmantena mainittiin konttorit. (Korhonen 2001.) Itsepalvelukanavat olivat siis jo tuolloin kaikille vastaajille tärkeämpiä kuin fyysiset konttorit.

Mira Lystimäen (2000) Pro gradu -tutkielman aiheena taas ovat vakuutukset verkossa. Myös hänen tutkimuksessaan pohditaan syitä siihen, mikseivät verkkopalvelut ole saaneet suurempaa suosiota. Hänen mukaansa vakuutuksiin liittyvien verkkopalvelujen yleistyminen vaatisi palvelun nopeutta ja helppokäyttöisyyttä sekä selkeitä etuja kuluttajille. Lystimäen selvityksen mukaan vakuutukset koetaan ylipäätään hankaliksi tuotteiksi, koska kuluttajien tietous niiden sisällöstä ja ehdoista on huono. Vakuutusten hankinnassa vakuuttamispäätöksen avuksi kaivataan siis henkilökohtaista palvelua. Hänen tutkimansa henkilöt kokivat, että vakuutusten hinta oli verkossa sama kuin konttorista ostettaessa. (Lystimäki 2000.) Vakuutus- ja pankkipalvelujen tarjonta verkossa eroavat jossain määrin toisistaan. Verkkopankissa asiointi on alusta alkaen ollut Suomessa edullisempaa kuin konttorissa asiointi. Lisäksi suomalaiset ovat jo ennestään tottuneet hoitamaan

pankkiasioitaan itsenäisesti – ostosten maksaminen kortilla ja automaattien käyttö rahan nostoon ja laskujen maksamiseen on ollut jo pitkään hyvin yleistä (Riipinen & Tinnilä 2004, 20.) Näin ollen pankkiasioinnin siirtyminen verkkoon on tapahtunut luontevasti.

Liisa Peura-Kapanen (2009) on tutkinut kuluttajien mielipiteitä e-laskua kohtaan. E-lasku on lasku, jonka laskuttava yritys lähettää suoraan asiakkaan verkkopankkiin. E-lasku on melko uusi innovaatio – suomalaiset ovat voineet vastaanottaa e-laskuja vuodesta 2007. E-lasku ei ole saavuttanut Suomessa yhtä suurta suosiota kuin esimerkiksi Ruotsissa ja Virossa. Peura-Kapasen tutkimukseen vastanneet arvostivat laskunmaksussa edullisuutta, vaivattomuutta ja muodostuneita rutiineja. Suurin osa vastaajista vastaanotti perinteisiä paperilaskuja, jotka sitten maksettiin verkkopankissa. Totuttuun maksutapaan oltiin tyytyväisiä, joten laskunmaksutavan muutoksiin ei koettu tarvetta. Yhtenä esteenä e-laskun käyttöönotossa on asiakkaan kokema hallinnan puute. Paperilaskuihin tottuneet uskoivat, että e-laskun maksu voi unohtua kun paperinen versio ei ole muistuttamassa maksupäivästä. Lisäksi moni vastaaja halusi maksetusta laskusta paperisen kuitin, jonka sitten voi arkistoida. E-laskujen markkinoinnissa taas yhtenä tärkeänä hyötynä on painotettu juuri laskujen sähköistä arkistointia. Henkilöt, jotka olivat jo käyttäneet e-laskua olivat kuitenkin siihen erittäin tyytyväisiä ja aikoivat käyttää sitä myös jatkossa. (Peura-Kapanen 2009.)

Kansainvälinen keskustelu verkkopankin turvallisuudesta

Edellä mainituissa kuluttajaekonomian tutkimuksissa pohditaan paljon sitä, mikseivät verkkopalvelut ole kovinkaan suosittuja, vaikka internetin käyttö Suomessa on hyvin tavallista. Verkkopankin käyttö taas on erittäin yleistä. Muualla maailmassa verkkopankin suosio on jäänyt vaisummaksi. Alunperin Fred Davisin, Richard Bagozzin ja Paul Warshawin vuonna 1989 kehittämää Technology Acceptance Modelia (TAM) on käytetty yleisesti kuvaamaan verkkopalvelujen omaksumista. Mallin perusajatuksena on, että asiakkaan kokema palvelun käytön helppous sekä palvelun hyödyllisyys vaikuttavat myönteisesti verkkopalvelun käyttöönottoon. TAM:sta on tehty monia muunnelmia ja laajennuksia. Amin (2009) tutki verkkopankkipalvelujen omaksumista Malesiassa, ja laajensi TAM:ia tutkimalla

myös palvelun käytöstä saatavan nautinnon, koetun luotettavuuden eli koetun turvallisuuden ja yksityisyyden sekä sosiaalisen paineen vaikutuksia verkkopankin käyttöönottoon. Dabholkar (1996) tutki kuluttajien odotuksia muun muassa palvelun käytön helppoudesta, nopeudesta ja nautinnollisuudesta sekä niiden vaikutusta odotetun palvelun laadun kautta itsepalvelukanavan käyttöönottoon. En tässä tutkimuksessa aio käsitellä enempää TAM:ia, koska Suomessa kuluttajat ovat omaksuneet verkkopankin hyvin laajalti.

Kansainvälisissä tutkimuksissa on käsitelty paljon verkkopankin turvallisuutta. Kuluttajien huoli verkkopankin turvallisuudesta on ollut monissa maissa suurin palvelun omaksumista hidastava tekijä (Sudha ym. 2007). Emigh (2005) esittää raportissaan, että phishing-hyökkäykset aiheuttivat vuonna 2003 yhdysvaltalaispankeille suoria kustannuksia 1,2 miljardia dollaria. Emigh määrittelee phishingin verkossa tapahtuvaksi identiteettivarkaudeksi, joka voidaan toteuttaa monin eri tavoin kuten sähköpostiviestillä, uhrin koneelle asennettavan haittaohjelman avulla tai nimipalvelinasetuksia muuttamalla (mt., 6). Palaan phishingin eri muotoihin tarkemmin luvussa neljä.

Pankeilla on omat keinonsa phishing-hyökkäysten torjumiseen. Rikollisten tunkeutumista pankkien omiin järjestelmiin pyritään estämään palomuureilla ja erilaisilla salaus- ja esto-ohjelmilla. Pankit voivat myös käyttää ohjelmistoja, jotka etsivät jatkuvasti internetistä pankkiin liittyviä tietoja kuten nimeä tai logoa. Näin pyritään tunnistamaan mahdolliset väärennetyt sivustot mahdollisimman nopeasti. (Sarel & Marmorstein 2006.) Käsittelen sekä pankkien että kuluttajien mahdollisuuksia parantaa verkkopankkiasioinnin turvallisuutta luvussa viisi.

Pankkien tiedottamisella turvallisuusasioista on merkittävä vaikutus kuluttajien luottamuksen lisäämiseen. Pankkien tulisikin aktiivisesti tiedottaa asiakkaitaan siitä, mitä toimenpiteitä ne tekevät lisätäkseen verkkopankin turvallisuutta (Liao & Wong 2008). Pankkien tulisi välittömästi tiedottaa asiakkaitaan myös havaitsemistaan turvallisuusuhista kuten väärennetyistä pankkisivustoista (Sarel & Marmorstein 2006). Casaló ym. (2007) esittävät, että pankkien tulisi yhdessä julkisen sektorin kanssa tarjota asiakkailleen koulutusta verkkopankin käyttöön, jotta he oppisivat luottamaan asioinnin turvallisuuteen. Kiinnitänkin tässä tutkimuksessa huomiota

siihen, mistä tutkittavat ovat saaneet tietoa turvallisuusasioista ja onko tiedotus heidän mielestään riittävällä tasolla. Tiedotusta ja asiakkaiden ohjeistamista käsittelen luvuissa neljä ja viisi.

Tässä tutkimuksessa pyrin vastaamaan seuraaviin tutkimuskysymyksiin:

- Kokevatko haastateltavat verkkopankin turvalliseksi ja millaisista turvallisuusuhista he ovat tietoisia?
- Pyrkivätkö haastateltavat parantamaan verkkopankin käytön turvallisuutta omalla käyttäytymisellään?
- Millaiseksi muotoutuu pankin ja asiakkaan välinen vastuunjako tilanteissa, joissa asiakas menettää varojaan onnistuneen huijauksen johdosta?

2.2 Tutkimuksen toteutus

Tutkimukseni on laadullinen ja keräsin tutkimusaineiston yksilöhaastatteluilla. Haastattelin kahdeksaa tottunutta verkkopankin käyttäjää, jotka keräsin omasta tuttavapiiristäni. He edustavat tässä tutkimuksessa kuluttajia. Näiden haastattelujen lisäksi tein kaksi asiantuntijahaastattelua. Jatkossa puhuttaessa haastateltavista, tarkoitan verkkopankin käyttäjien haastatteluja eli kuluttajahaastatteluja. Asiantuntijahaastatteluista puhuttaessa mainitsen aina, että kyse on asiantuntijoista.

Haastatteluaineistojen lisäksi käytän yritysten verkkosivuja kuvaamaan millaista tietoa kuluttajille tarjotaan verkkopankin turvallisuudesta ja omista mahdollisuuksista parantaa verkkoasioinnin turvallisuutta. Viittaan näihin verkkoaineistoihin kuten kirjallisuuteen ja ne löytyvät lähdeluettelosta kirjallisuuslähteiden jälkeen. Verkkoaineistoon lukeutuvat pankkien, Kuluttajaviraston, Viestintäviraston ja Finanssialan Keskusliiton (käytän jatkossa lyhennettä FK) verkkosivustojen turvallisuusosiot sekä näiden julkaisemat tiedotteet turvallisuuteen liittyen.

Esittelen kuluttajina haastattelemiani henkilöitä taulukossa yksi. Kaikki haastateltavat ovat käyttäneet verkkopankkia aktiivisesti lähes kymmenen vuoden ajan, ja verkkopankki on kaikille tavallisin kanava hoitaa pankkiasioita. Tekstissä viittaan heihin numerokoodeilla H1-H8. Koodeja käytän siksi, että haastateltavien

joukossa esiintyy muutama saman ikäinen naishenkilö, joten sukupuolella ja iällä viittaamalla heitä ei erottaisi toisistaan.

Taulukko 1. Kuluttajahaastateltavat

	Suku-puoli	**Ikä**	**Koulutus**	**Verkkopankin käyttökokemus**	**Verkkopankin käyttökerrat**
H1	nainen	29	VTM	7 v.	3 krt/kk
H2	nainen	32	tradenomi	10 v.	2 krt/vk
H3	nainen	29	tradenomi, teologian yo	10 v.	2-3 krt/vk
H4	mies	27	peruskoulu (ammatilliset opinnot käynnissä)	9 v.	lähes päivittäin
H5	nainen	28	KTK (maisteriopinnot käynnissä)	8-10 v.	2 krt/vk
H6	nainen	27	MMM	8 v.	lähes päivittäin
H7	nainen	28	ETM	8 v.	kerran viikossa
H8	nainen	31	TaM	6 v.	3-4 krt/vk

Haastateltavien joukkoon valikoitui vain yksi mies. En kiinnittänyt niinkään huomiota sukupuoleen etsiessäni haastateltavia, vaan halusin etsiä henkilöitä, joilla olisi aiheesta jotain kerrottavaa. En koe haastateltavien sukupuolittuneisuutta ongelmana myöskään siksi, että tutkimuksen tuloksia ei ole tarkoitus yleistää suureen joukkoon ihmisiä, vaan halusin saada syvällisempää tietoa juuri näiden henkilöiden käsityksistä verkkopankin turvallisuudesta. Vaikka haastateltavat olivat minulle ennestään tuttuja, en ollut keskustellut heidän kanssaan tämän tutkimuksen aihepiiristä. Yritin siis valikoida haastatteluihin henkilöitä, jotka ovat ylipäätään valmiita ilmaisemaan oman mielipiteensä asiasta kuin asiasta. Tällä yritin välttää tilannetta, jossa joudun ohjaamaan haastattelua liiaksi. Toivoin, että haastattelutilanteista tulisi mahdollisimman luontevia. Näin myös tapahtui, haastattelut etenivät omalla painollaan ja kaikissa käytiin läpi suunnitellut teemat. Haastattelut kestivät 20 minuutista 40 minuuttiin.

Valitsin haastattelumuodoksi teemahaastattelun eli puolistrukturoidun haastattelun. Työn suunnitteluvaiheessa pohdin vaihtoehtona myös strukturoitua eli lomakehaastattelua. Kun aloin hahmottelemaan kyselylomaketta, huomasin kuitenkin kuinka vaikeaa oli laatia yksiselitteisiä ja selkeitä kysymyksiä. Hirsjärvi ja Hurme

(2004, 45) toteavatkin kysymysten laatimisen olevan lomakehaastattelun vaikeimpia vaiheita. Teemahaastatteluun taas ei ole tarkoituskaan laatia valmiita kysymyksiä vaan teemarunko, jossa listataan haastattelussa käsiteltävät asiat. Haastattelu voi edetä vapaasti ja aiheita voidaan käsitellä eri haastateltavien kanssa eri järjestyksessä. Pääasia on, että kaikki teema-alueet käydään läpi jokaisessa haastattelussa. (Eskola & Suoranta 1998, 86.) Omissa haastatteluissani aihepiirien käsittelyjärjestys vaihteli. Annoin haastateltavan melko pitkälti määrätä järjestyksen eli kyselin aina lisää siitä aiheesta, johon haastateltava omassa puheenvuorossaan jäi ja palasin sitten myöhemmin aiheisiin, jotka olivat jääneet käsittelemättä.

Tein kaikki haastattelut joulukuun 2009 ja helmikuun 2010 välillä. Olin alun perin suunnitellut toteuttavani haastattelut vain reilun kuukauden kuluessa, mutta joidenkin kanssa aikataulujen sovittaminen oli haasteellista, joten aikataulu haastattelujen toteuttamisen osalta hieman venyi. En kuitenkaan ole missään vaiheessa asettanut itselleni ehdottomia aikarajoja työn valmistumisen suhteen, joten pieni viivästys haastattelujen suhteen ei koitunut ongelmaksi. Tein kuluttajahaastattelut kotonani, koska halusin välttää meluisia kahviloita tai julkisia tiloja. Haastattelut sujuivat mielestäni hyvin, vaikka minulla ei ollut kokemusta haastattelemisesta etukäteen. Minulle olikin varmasti paljon hyötyä siitä, että haastateltavat olivat tuttaviani. Tällöin minun ei tarvinnut jännittää haastattelutilanteita lainkaan. Lisäksi minun ei tarvinnut miettiä asioita, kuten kuinka rikon jään tuntemattoman haastateltavan kanssa tai miten täytän mahdolliset hiljaiset hetket.

Litteroin haastattelut aina ennen seuraavaa haastattelua, yleensä jo samana tai seuraavana päivänä. Tämä osoittautui hyväksi keinoksi varsinkin ensimmäisten haastattelujen kohdalla. Sain hyvän käsityksen edellisen haastattelun kulusta ja samalla huomasin jos itselläni oli haastattelemisessa parantamisen varaa. Tuntuikin siltä, että haastatteluista tuli johdonmukaisempia niiden edetessä ja oman kokemukseni lisääntyessä. Huomasin, että aluksi saatoin palata samoihin asioihin kun seurasin enemmän teemarunkoa. Loppupään haastattelut sujuivatkin sitten hyvin luonnollisesti siinä järjestyksessä, missä haastateltava asioita mainitsi. Loppuvaiheen haastattelut olivat myös kestoltaan hieman lyhyempiä.

Verkkopankin käyttäjien lisäksi haastattelin siis kahta verkkoturvallisuuden asiantuntijaa, erään teleyrityksen turvallisuuspäällikköä sekä tietoturva-asiantuntijaa. Asiantuntijahaastatteluilla halusin saavuttaa paremman käsityksen verkkopankin turvallisuustilanteesta juuri tämän päivän Suomessa. Heidän laajan tietämyksensä vuoksi haastattelin vain kahta asiantuntijaa – oletan, että useammassakin haastattelussa samat asiat olisivat nousseet esiin. Käsitykseni vahvistui haastattelujen jälkeen. Molemmat mainitsivat hyvin samanlaisia asioita, toki haastatteluissa oli myöskin eroja. Käytän näitä haastatteluja lähteenomaisesti, joten tätä materiaalia ei ole tarkoitus tulkita ja analysoida samalla tavalla kuin verkkopankin käyttäjien haastatteluja.

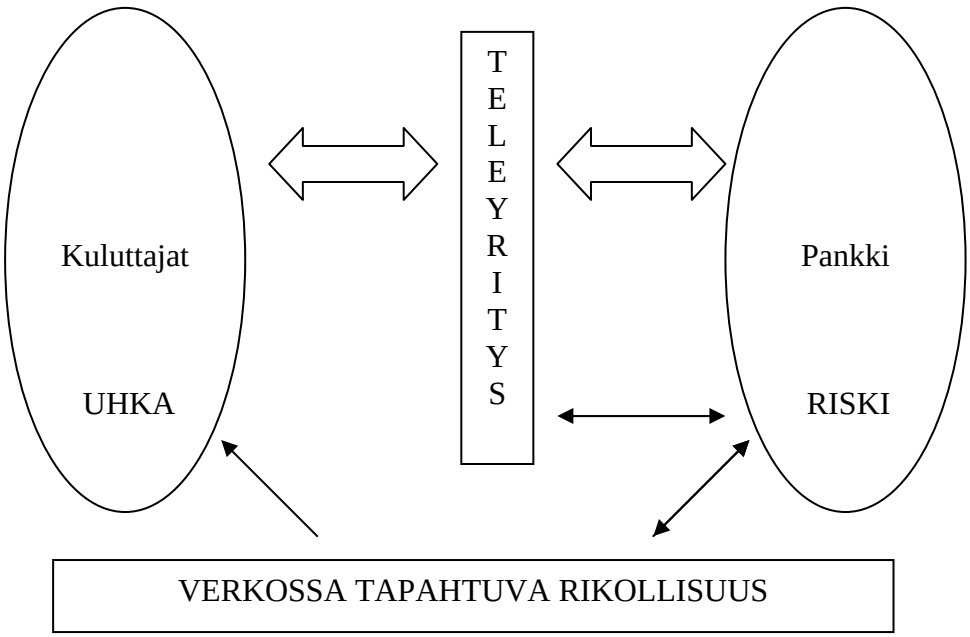
Asiantuntijahaastatteluita varten menin haastateltavien työpaikalle, josta he olivat varanneet käyttöömme neuvotteluhuoneen. Haastattelin heitä yksitellen ja molempien haastattelu kesti hieman alle puoli tuntia. Myös asiantuntijahaastatteluissa käytin apunani teemarunkoa enkä valmiiksi muotoiltuja kysymyksiä. Näin toimin myös siksi, että he tekevät työssään hyvin teknisiä toimenpiteitä ja oma tietämykseni siitä aihepiiristä on hyvin rajallinen.

En halunnut asiantuntijoiksi pankkien henkilökuntaa ristiriidan välttämiseksi. Koska yhtenä tutkimuskysymyksenä on taloudellisten vahinkojen vastuunjako kuluttajien ja pankkien välillä, pankin edustajien näkemykset olisivat mahdollisesti olleet puolueellisia. Teleyrityksen asiantuntijat voivat ilmaista vapaasti oman mielipiteensä. He tuntevat hyvin myös verkkopankkia koskevat riskit, koska teleyritykset ja pankit tekevät paljon yhteistyötä turvallisuusasioissa. Teleyritykset suodattavat tarvittaessa pankkien pyynnöstä asiakkaiden internet-liikennettä sekä poistavat internetistä rikollisten tekemiä väärennettyjä pankkisivustoja. Johdannossa esitin ajatuksen pankkien ja asiakkaiden välisen turvallisuussuhteen muuttumisesta asioinnin siirryttyä verkkoon. Teleyritykset toimivat tässä suhteessa ikään kuin kiilana pankin ja asiakkaan välissä. He tarjoavat sen alustan, jolla verkkopankin käyttäjien sekä pankkien asiakkuussuhde toteutuu.

Selvennän asiantuntijoiden roolia tutkimuksessani seuraavassa kuviossa yksi. Perinteisesti pankkisuhde on toteutunut ainoastaan kuluttajien ja pankin välillä, ja myös turvallisuussuhde on käsittänyt vain nämä alkuperäiset osapuolet. Verkkoon

siirryttäessä suhteeseen tulee kaksi osapuolta lisää: teleyritys ja verkossa tapahtuva rikollisuus. Teleyrityksellä on turvallisuussuhde sekä kuluttajiin että pankkiin. Kuluttajille tarjotaan verkkoyhteys, jonka avulla he voivat käyttää pankin palvelutarjontaan kuuluvaa verkkopankkia. Verkkoyhteyden turvallisuutta pidetään yllä viime kädessä niin, että kuluttajan internet-liikennettä suodatetaan. Tällainen varotoimi voi tulla kyseeseen yllä mainitussa tapauksessa, jossa pankki tai teleyritys löytää internetistä väärennetyn, pankin nimissä toimivan sivuston. Teleyritys voi tällöin pankin pyynnöstä estää asiakkaidensa liikenteen kyseiselle sivustolle kunnes se poistetaan. Teleyritys on siis nyt kuluttajien ja pankin välisen turvallisuussuhteen välikappale. Rikollisuus kohdistuu sekä pankkiin, että kuluttajiin. Pankki ja teleyritys toimivat yhteistyössä rikollisuutta vastaan kehittelemällä omia teknisiä järjestelmiään. Kuluttajat voitaisiin saada mukaan tähän ”taisteluun” lisäämällä tiedotusta rikollisten toiminnasta. Näin pankkien asiakkaat osaisivat varautua paremmin uhkiin, joita verkkoasiointiin liittyy. Myös kuluttajien tulisi informoida pankkia heti jos he havaitsevat jotain poikkeavaa asioidessaan verkkopankissa.

Kuvio 1. Kuluttajien, teleyrityksen ja pankin välinen suhde verkossa



Käytän tässä tutkimuksessa termiä turvallisuusuhka kuvaamaan toimintaa, jolla rikolliset pyrkivät pääsemään käsiksi uhriensa varoihin. Esittelen tässä riskiin

liittyvää käsitteistöä perustellakseni miksi olen päätynyt käyttämään uhan käsitettä riskin sijaan.

Turvallisuustason määrittelyssä voidaan käyttää apuna seuraavaa yleisesti päätösteoriassa käytettyä jaottelua, jossa kuvataan ihmisten kokemia tiloja suhteessa tulevaisuuteen:

1) Varmuus on tila, jossa tilanteen kaikki erilaiset lopputulemat ovat tiedossa.
2) Riski on tila, jossa tilanteen eri lopputulemien todennäköisyyttä voidaan arvioida.
3) Epävarmuuden tilassa tilanteen eri lopputulemien todennäköisyyttä ei voida arvioida laskennallisesti, mutta mahdolliset vaihtoehdot tiedetään.
4) Tietämättömyys on tila, jossa tilanteen eri lopputulemavaihtoehtoja ei tunneta. (Lagerspetz 1997, 94.)

Käsitän varmuuden tilanteen turvallisuuden synonyymiksi. Riski seuraa heti varmuuden perässä ja määritelmästä huomataan, että riski on tilanne, joka on oikeastaan jo hallinnassa. Eräsaari (1997, 70) esittääkin, että riskin käsittä tarvitaan epävarman tilanteen määrittelyyn, mutta oikeastaan sitä voidaan käyttää vasta kun epävarmuus on jo poistunut ja tilanne on hallinnassa. Riskin käsite on monitahoinen, eikä yhtä oikeaa määritelmää tai käyttötarkoitusta ole olemassa (mt., 79).

Eräsaaren (1997, 78) mukaan silloin kun oman toiminnan katsotaan sisältyvän riskikontekstiin, uhkiin ja vaaroihin voidaan vaikuttaa. Uhasta tulee riski kun tieto siitä lisääntyy – riski onkin siis neutraloitu uhka (mt., 76). Käytän tässä tutkimuksessa käsitettä turvallisuusuhka, koska tutkimuskohteena on kuluttaja. Haastattelemani verkkopankin käyttäjät eivät välttämättä olleet lainkaan tietoisia siitä, että verkkopankin käyttöön saattaisi ylipäätään liittyä turvallisuusuhkia. He sijoittuisivat näin ollen yllä esitetyssä jaottelussa alimpaan luokkaan, tietämättömyyden tilaan. Pankit taas tuntevat rikollisten mahdolliset huijauskeinot ja mielestäni voikin sanoa, että pankeille samaiset kuluttajia koskevat uhat ovat riskejä. Tämäkin kirkastaa johdannossa esittämääni ajatusta pankin ja asiakkaan välisen

turvallisuussuhteen muutoksesta. Pankit kohtaavat toiminnassaan hallitumpia riskejä kuluttajien ollessa kenties täysin tietämättömiä uhkien olemassaolosta.

Ulrich Beck (1992) esittää, että modernisaatio itse on riskien tuottaja. Hän määrittelee riskin modernisaation tuottamien uhkien (hazards) ja epävarmuuksien (insecurities) systemaattiseksi käsittelytavaksi. (mt., 21.) Uhasta siis muodostuu riski silloin kun sitä opitaan kontrolloimaan. Beck puhuu lähinnä teollisuuden aiheuttamista ilmastotekijöistä, mutta mielestäni sama voidaan laajentaa käsittelemään myös internetin maailmaa. Internetin aikana turvallisuusuhat ovat täysin uudenlaisia eivätkä olisi mahdollisia perinteisissä toimintaympäristöissä.

Beckin (1992) modernit riskit eivät enää ole paikallisesti sidottuja.Tässäkin esimerkkinä toimii teollisuustehdas, josta ilmansaasteet kulkeutuvat pitkiä matkoja aiheuttaen harmia myös tehdasympäristön ulkopuolella (mt., 22), mutta internet-rikollisuus on mielestäni malliesimerkki siitä, että riskit tai uhat ovat globaaleja. Internetissä toimiva rikollinen voi sijaita missä päin maailmaa tahansa kuten hänen uhrinsakin.

2.3 Aineiston analyysi ja tutkimuksen luotettavuus

Tarkastelen keräämääni aineistoa faktanäkökulmasta, jolloin on aiheellista kiinnittää huomiota haastateltavien rehellisyyteen ja saadun tiedon totuudenmukaisuuteen. Minun tulee siis jollakin tavoin varmistua siitä, että haastateltavat puhuvat totta. Tähän on kaksi menetelmää, mekanistinen ja humanistinen. Mekanistisessa menetelmässä pyritään vähentämään itse haastattelun vaikutusta saatuun informaatioon antamalla tutkittaville vain vähän tietoa tutkimuksen tarkoituksesta. Humanistisessa metodissa taas painotetaan tutkijan läheistä ja luottamuksellista suhdetta tutkittaviin ja luotetaan sitä kautta siihen, että haastateltavat haluavat olla tutkijalle rehellisiä. (Alasuutari 1999, 90-97.) Asiantuntijoiden totuudenmukaisuutta en voinut arvioida – minun oli luotettava heidän sanaansa. En kuitenkaan usko, että yksikään verkkorikollisuutta vastaan työskentelevä henkilö haluaisi valehdella näissä asioissa. Verkkopankin käyttäjien haastatteluissa taas hyödynsin molempia menetelmiä.

Mekanistisen menetelmän mukaisesti en kertonut haastateltaville etukäteen juurikaan tutkimuksestani. Kerroin vain, että haluaisin keskustella heidän käsityksistään verkkopankkipalvelujen turvallisuudesta. Pyysin heitä myös olemaan valmistautumatta haastatteluun mitenkään, koska en halunnut heidän ottavan selvää käsiteltävistä asioista etukäteen. Uskon, että tätä toivetta jopa edesauttoi se, että tunsin haastateltavat entuudestaan. He eivät varmastikaan jännittäneet haastattelutilannetta lainkaan, minkä vuoksi uskon, että he eivät myöskään kokeneet tarpeelliseksi valmistautua tilanteeseen. Lisäksi oletan, ettei heillä ollut tarvetta esittää tietävänsä asiasta enempää kuin he todellisuudessa tietävät. Haastattelutilannetta voitiin pitää lähes normaalina kanssakäymistilanteena.

Humanistisen metodin mukaisesti uskon siihen, että haastateltavat olivat minulle rehellisiä sen vuoksi, että tunnemme toisemme. Uskon, ettei heillä ollut mitään tarvetta valehdella minulle etenkään koska tutkimukseni aihe ei liity suhteeseemme millään tavoin. Koin suurimpana uhkana sen, että haastateltavat olisivat ottaneet selvää verkkopankkipalvelujen turvallisuudesta etukäteen koska halusin selvittää nimenomaan sitä tietävätkö he ylipäätään erilaisten turvallisuusuhkien olemassaolosta. Laajan uutisoinnin vuoksi oli kuitenkin syytä olettaa, että haastateltavat olisivat kuulleet marraskuun 2009 tapahtumista. Silloin Viestintävirasto epäili Zlob-troijalaisen olevan kohdennettu myös suomalaispankkien asiakkaisiin ja kehotti sen vuoksi teleyrityksiä suodattamaan asiakkaidensa internet-liikennettä. (Viestintävirasto 2009.) Toisaalta koen myönteisenä asiana sen, että haastateltavien tietämys verkkopankin turvallisuudesta lisääntyi tutkimukseni kautta. Mikäli haastateltavat eivät jostain syystä tienneet lainkaan turvallisuusuhista, kerroin niistä heille ja tiedustelin vaikuttaako tieto millään tavoin omaan verkkopankin käyttöön jatkossa.

Olen käyttänyt aineiston analyysimenetelminä teemoittelua ja tyypittelyä. Eskolan ja Suorannan (1998, 175) mukaan onnistuneesti toteutettu teemoittelu sisältää teorian ja empirian vuoropuhelua. Tämän tutkimuksen rakenne etenee teemoittain. Alustan keskustelua turvallisuudesta luvulla kolme, jossa käsittelen suomalaisten internetin ja verkkopankin käyttöä yleisellä tasolla. Luvun neljä teemana on verkkopankin turvallisuus ja luvussa viisi pääteemoja on kaksi: turvallisuusuhkiin varautuminen

sekä taloudellinen vastuunjako. Kussakin luvussa sekä esittelen aihealueeseen liittyvää tutkimusta että avaan ja tulkitsen tekemiäni haastatteluja. Näin pyrin kietomaan yhteen teorian ja empirian.

Teemoittelun vaarana on se, että sitaatteja esitetään liikaa ja itse aineiston tulkinta unohtuu. Sitaattien määrän tulisi olla kohtuullinen suhteessa tutkijan omaan tekstiin. (Eskola & Suoranta 1998, 180.) Esitän tässä tutkimuksessa jonkin verran lainauksia haastatteluista, mutta pääpaino raportissa on kuitenkin omassa tulkinnassani sekä aiemmassa tutkimuksessa.

Tyypittelyllä tarkoitetaan sitä, että aineistosta etsitään toisaalta samanlaisia ja toisaalta poikkeavia vastauksia tiettyihin kysymyksiin (Eskola & Suoranta 1998, 181). Koskisen ym. (2005, 236) mukaan poikkeavien tapausten käsittelyssä esiintyy perustavanlaatuinen ero määrällisen ja laadullisen tutkimuksen välillä; kvantitatiivisessa tutkimuksessa poikkeavat tapaukset pyritään sulkemaan tutkimuksen ulkopuolelle kun taas kvalitatiivisessa tutkimuksessa poikkeavat tapaukset voivat saada olennaisen roolin. Omassa aineistossani yksi vastaaja erottui monissa kysymyksissä muista haastateltavista. Joissakin kysymyksissä muiden vastauksissa toistuivat samat asiat, mutta tämän kyseisen haastateltavan vastaus oli täysin poikkeava. Kyseinen haastateltava on kiinnostavasti myös joukon ainoa mies. Toisaalta hänen poikkeavat vastauksensa saattavat liittyä ennemminkin hänen harrastustaustaansa. Hän on aina ollut kiinnostunut tietotekniikasta ja on näin ollen käyttänyt tietokonetta enemmän kuin muut vastaajat sekä tutustunut myös alan julkaisuihin. Hänen tietoisuutensa aihepiireistä, jota tämä tutkimus käsittelee on siis aivan toisella tasolla kuin muilla vastaajilla.

Tutkimuksen luotettavuuden arvioinnissa on perinteisesti käytetty validiteetin ja reliabiliteetin käsitteitä, jotka kuitenkin soveltuvat paremmin määrällisiin kuin laadullisiin tutkimuksiin. Validiteetti voidaan jakaa sisäiseen ja ulkoiseen validiteettiin. Sisäisesti validissa tutkimuksessa tulkinta on loogista ja ristiriidatonta. Ulkoisesti validin tutkimuksen tulkinnat taas voidaan yleistää muihinkin kuin tutkittuihin tapauksiin. (Koskinen ym. 2005, 254-255.) Alasuutarin (1999, 237) mukaan laadullisen tutkimuksen tavoitteena on tulosten yleistettävyyden sijasta jonkin ilmiön selittäminen. Tässä tutkimuksessa pyrin antamaan tarkan kuvauksen

juuri haastateltavien käsityksistä tutkittavasta ilmiöstä enkä väitäkään, että suurempi populaatio jakaisi heidän mielipiteensä.

Reliabiliteetilla viitataan eri havainnoitsijoiden yhdenmukaisuuteen tapausten luokittelussa. Kvantitatiivisessa tutkimuksessa aineisto koodataan vähintään kahden ihmisen toimesta, jolloin voidaan varmistua koodauksen oikeellisuudesta (Koskinen ym. 2005, 255-256.) Tässä tutkimuksessa en tee tilastollisia mittauksia, vaan pyrin tekemään syvällisempiä tulkintoja haastateltavien kommenteista. Jokainen lukija saa muodostaa oman mielipiteensä siitä, ovatko tulkintani johdonmukaisia.

Laadullisen tutkimuksen luotettavuutta voidaan lisätä nimenomaistamalla tutkimuksen tulkintasäännöt eli esittämällä tulkinnan lisäksi sitaatteja, joista päätelmät on tehty (Eskola & Suoranta 1998, 216). Tätä tapaa käytän myös tässä tutkimuksessa. Oman tulkintani lisäksi esitän siis joitakin katkelmia haastatteluista. Lukija voi näin ollen itse päätellä ovatko tulkintani hänen mielestään perusteltuja vai päätyisikö hän kenties itse toisenlaisiin tulkintoihin.

Kvantitatiivisissa tutkimuksissa tutkimuksen luotettavuus liittyy lähinnä määrällisten mittausten luotettavuuteen. Kvalitatiivisessa tutkimuksessa taas luotettavuus käsittää koko tutkimusprosessin tutkielman tekijän ollessa itse tärkein luotettavuuden mittari. Laadullisessa tutkimuksessa tutkija on itse osa tutkimusta ja vaikuttaa näin saatuihin tuloksiin. (Eskola & Suoranta 1998, 210-211.) Lukijan tutkimuksen arviointia helpottaakseni esitän itseni läpi tutkimuksen ensimmäisessä persoonassa. Kun esitän aineistosta tehtyjä tulkintoja, erotan ne selvästi aiemmasta tutkimuksesta. Kerron siis mitä mieltä itse olen kun taas muiden tutkimuksista puhuessani esitän aina perässä lähdeviitteen kyseiseen tutkimukseen.

Tutkimuksen vahvistuvuudella tarkoitetaan sitä, että oman tutkimusaineistoni pohjalta tekemäni tulkinnat saavat tukea aiemmin tehdyistä tutkimuksista (Eskola & Suoranta 1998, 212). Pyrinkin tässä työssä esittämään omien tulkintojeni ohella myös aiempia tutkimuksia, joissa on tehty samankaltaisia löydöksiä aineistoista.

Havaintojen toistettavuutta pidetään yhtenä vaatimuksena luotettavalle tutkimukselle. Toistettavuudella tarkoitetaan sitä, että toisella tutkijalla on mahdollista toistaa

tutkimus hyväksyäkseen aiemmat tulkinnat ja varmistuakseen tutkitun ilmiön todellisuudesta. Tutkijan tulee siis raportoida huolellisesti havaintojen tuottamisesta ja päätymisestä tehtyihin tulkintoihin. (Koskinen ym. 2005, 258.) Takaakseni tämän tutkimuksen toistettavuuden, olen edellisessä luvussa pyrkinyt kuvaamaan sekä haastateltavia että itse haastattelujen toteutusta mahdollisimman tarkasti. Lisäksi jatkossa esittämäni sitaatit haastatteluista auttavat lukijaa ymmärtämään niistä tekemiäni tulkintoja.

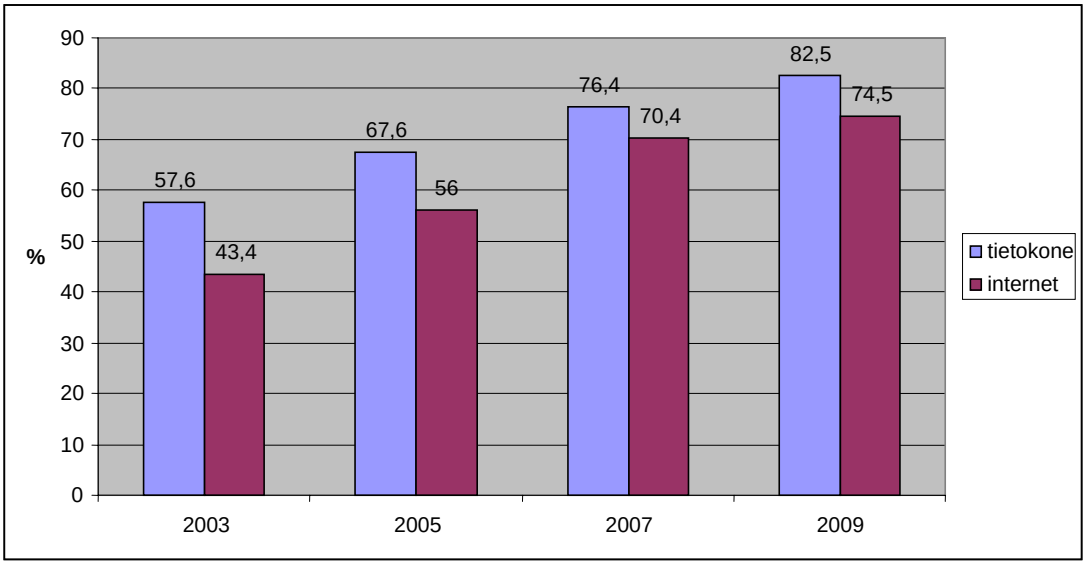
3 Internetin ja verkkopankin käyttö

Ennen siirtymistä verkkopankkipalvelujen turvallisuuden käsittelyyn, on syytä kartoittaa kuinka yleistä internetin ja verkkopankin käyttö on yleensä suomalaisten keskuudessa. Tässä luvussa tarkastelen siis palvelujen käyttöä sekä verkkopankkipalvelujen tarjoamia hyötyjä sekä pankeille että asiakkaille.

3.1 Tietokoneen ja internetin käyttö

Suomi on yksi maailman johtavia maita kuluttajien tietotekniikan omaksumisen osalta. Tietokone ja internet-liittymä kuuluvat kodin tarpeistoon suurimmassa osassa suomalaisia kotitalouksia ja niiden yleisyys on kasvanut koko 2000-luvun ajan (taulukko 2). On oletettavaa, että myös henkilöillä, joilla ei ole omaa kotikonetta ja internet-liittymää, on pääsy tietokoneelle ja internetiin työ- tai opiskelupaikallaan. Tietokone onkin nykyään perustyöväline sekä työnteossa että opiskelussa. Jo peruskouluissa, puhumattakaan ammatillisista oppilaitoksista tai korkeakouluista, tietokoneen ja internetin käyttö liittyy kiinteästi opiskeluun.

Taulukko 2: Tietokoneen ja internet-liittymän yleisyys suomalaisissa kotitalouksissa vuosina 2003-2009



Lähteet: Kuluttajabarometri 1/2006, Kuluttajabarometri 2/2007 ja Kuluttajabarometri 8/2009

Taulukosta kaksi nähdään, että vuonna 2003 tietokoneen omisti 58 prosenttia kotitalouksista ja internet-liittymän 43 prosenttia kotitalouksista (Kuluttajabarometri 1/2006). Vuonna 2009 jo 83 prosentilla kotitalouksista oli oma tietokone ja 75 prosentilla internet-liittymä (Kuluttajabarometri 8/2009). Taulukosta voidaan myös havaita, että internet-liittymien osuus on kasvanut suhteellisesti nopeammin kuin tietokoneiden. Nykyään siis yhä useammalla tietokoneen omistajalla on käytössään myös internet-yhteys.

Internetin käyttö on varsin tavallista suomalaisten keskuudessa. Vuonna 2009 internetiä käytti 86 prosenttia väestöstä. Nuorten keskuudessa internetin käyttö on kaikkein yleisintä – jopa 99 prosenttia 15–28 -vuotiaista oli internetin käyttäjiä. 15-17 -vuotiaiden ikäluokassa internetin käyttöaste on 100 prosenttia. (FK 2009b, 46.) Tämä selittyy varmasti sillä, että kyseisen ikäluokan nuoret käyvät vielä lähes poikkeuksetta koulua ja kaikissa kouluissa opetetaan tietotekniikkataitoja, joihin myös internetin käyttö saumattomasti kuuluu.

Myös ikääntyneet eli yli 65 -vuotiaat käyttävät internetiä melko yleisesti ja käyttäjien osuus on ollut viime vuosina tasaisessa kasvussa. Etenkin 65–68 -vuotiaiden keskuudessa internetin käyttäjiä on paljon, 55 prosenttia ikäryhmän edustajista käyttää internetiä. Mitä vanhemmaksi tullaan, sitä vähemmän internetiä käytetään.

80–85 -vuotiaista vain kuusi prosenttia käyttää internetiä. (FK 2009c, 13.) Tämä on mielestäni kuitenkin varsin ymmärrettävää. Työelämästä poistuttaessa ja elämäntahdin rauhoittuessa internetin käyttötarve vähenee luonnollisesti. Yli 80 -vuotiaista suuri osa on myös todennäköisesti melko sairaita ja laitoshoidossa, jolloin internetin käyttötarve laskee lähes olemattomiin.

Yleisin internetin käyttömuoto suomalaisten keskuudessa on sähköpostin lähettäminen tai vastaanottaminen; 91 prosenttia internetin käyttäjistä käyttää sähköpostia (Tilastokeskus 2009). Tämä ei ole lainkaan yllättävää. Sähköposti on monelle luonteva tapa pitää yhteyttä ystäviin ja se on myös hyvin tavallinen viestintäväline työpaikoilla. Sähköposti on ainakin oman kokemukseni mukaan monilla työpaikoilla jopa yleisempi työväline kuin puhelin. Myös tämän tutkimuksen haastateltaville yleisin internetin käyttömuoto oli sähköposti. Facebook oli toiseksi suosituin sivusto eli internet on haastateltaville tärkeä kanava sosiaalisten suhteiden ylläpitoon.

3.2 Verkkopankin käyttö

Verkkopankki on toiseksi suosituin palvelu internetin käyttäjien keskuudessa. Jopa 87 prosenttia suomalaisista internetin käyttäjistä käyttää verkkopankkia. (Tilastokeskus 2009). Vuoden 2003 lopulla 2,9 miljoonalla suomalaisella pankkien henkilöasiakkaalla oli käytössään verkkopankkitunnukset (FK 2008, 2). Vuoden 2008 lopulla verkkopankkisopimuksia oli tehty peräti 4,7 miljoonaa kappaletta (FK 2009a, 21). Sopimusten määrän suuruutta selittää varmasti osin se, että yhdellä henkilöllä voi olla verkkopankkitunnukset useaan eri pankkiin. Joka tapauksessa luku on valtava ja verkkopankin käyttäjien prosentuaalinen osuus on erittäin suuri kansainvälisesti vertailtuna. Muualla maailmassa on tehty paljon tutkimuksia, joissa pyritään selvittämään, miksi verkkopankkipalvelut eivät ole saavuttaneet kovinkaan suurta suosiota (mm. Hua 2009; Cheng ym. 2006; White & Nteli 2004).

Suomen oloissa täytyy siis olla joitakin erityispiirteitä, jotka selittävät verkkopankkipalvelujen suuren suosion kuluttajien keskuudessa. Riipinen ja Tinnilä (2004) erottelevat näitä vaikuttimia. Ensinnäkin sähköiset pankkipalvelut eli

automaatit, puhelinpalvelut ja verkkopankki sekä television kautta toimivat palvelut ovat suomalaisille melko tuttuja. Uusia jakelukanavia on tuotu markkinoille pikku hiljaa ja niitä on markkinoitu aktiivisesti. Sähköisiä palveluja on tarjottu halvemmalla kuin perinteisiä konttoripalveluja, mutta edullisuudestaan huolimatta ne ovat tarjonneet asiakkaille selkeitä etuja kätevyydellään ja hyvällä saatavuudellaan. Toiseksi suomalaisten laskunmaksuperinne on edesauttanut verkkopankkipalvelujen omaksumista koska suoraveloituksen sijaan suomalaiset ovat tottuneet maksamaan laskunsa omatoimisesti. Laskunmaksusta on muotoutunut rutiininomainen toimenpide, joka suoritetaan useita kertoja kuussa tai jopa viikossa. Viimein suomalaiset ovat ahkeria maksukorttien käyttäjiä. Tämäkin vaikuttaa itsepalvelukanavien suosioon, sillä maksut voidaan hoitaa kortilla jo kaupassa tai käteistä nostaa automaateista. Monet pankkiasiat on siis totuttu hoitamaan itsenäisesti. Suomessa on täten ollut poikkeuksellisen hyvät lähtökohdat verkkopankkipalvelujen käyttöönotolle. (mt., 20.)

Yleisimmin verkkopankkia käytetään laskujen maksamiseen. Tänä päivänä jopa 75 prosenttia 15–74 -vuotiaista maksaa laskunsa pääasiallisesti internetin kautta kun vuonna 1992 vain kaksi prosenttia väestöstä teki niin. Verkossa maksaminen on etenkin nuorten suosiossa, mutta se on lisääntynyt myös iäkkäämpien keskuudessa. Yli 65 -vuotiailla suoraveloitus on perinteisesti ollut suosituin laskunmaksutapa, mutta vuonna 2009 Internetissä maksaminen kiilasi suoraveloitusten edelle ja tästäkin ryhmästä 37 prosenttia maksaa laskunsa tavallisimmin internetissä. (FK 2009d, 40.) Tähän tutkimukseen osallistuneiden henkilöiden keskuudessa laskunmaksu oli toiseksi yleisin verkkopankin käyttömuoto. Selvästi yleisin toiminto oli saldon tarkistus.

Myös tiedon hakeminen verkkopankin kautta on tavallista. 66 prosenttia 15–74 -vuotiaista on hakenut verkkopankista tietoa tilitapahtumista ja 35 prosenttia yleisesti pankki-, vakuutus- tai rahoitusasioista. Verkkopankkien palvelutarjonta on laajaa, mutta muita palveluja käytetään suhteellisesti harvemmin. 16 prosenttia vastaajista on avannut tilin sekä hakenut maksukorttia verkkopankin kautta. (FK 2009d, 47.) Tämä voi johtua siitä, että kun kerran on haettu pankki- tai luottokorttia, se uusiutuu automaattisesti. Näin uusi korttihakemus pitää tehdä vain jos haluaa vaihtaa korttityyppiä. Myös tilinavausten suhteellisen pieni määrä on mielestäni

ymmärrettävä, koska useimmilla on oletettavasti vain yksi tai kaksi tiliä pankissa ja tilityyppiä vaihdetaan varmasti harvoin. Haastattelemistani henkilöistä kaksi oli hakenut maksukorttia verkkopankin kautta ja vain yksi oli avannut tilin verkkopankissa.

Verkkopankin kautta on mahdollista hakea myös erilaisia luottoja. Lainaa on kuitenkin hakenut verkkopankissa vain muutama prosentti 15–74 -vuotiaista suomalaisista. Kulutusluottoa on hakenut viisi prosenttia vastaajista. Opinto- sekä asuntolainaa on kumpaakin hakenut neljä prosenttia vastaajista. (FK 2009d, 47.) Lainaa haettaessa halutaankin ilmeisesti edelleen henkilökohtaista palvelua. Tässä tutkimuksessa kaksi haastateltavaa oli hakenut lainaa verkkopankin kautta. Toisella heistä oli kyse opintolainasta, toinen taas oli hakenut kulutusluottoa. Haastateltavista kolme mainitsi, että hakisi lainaa konttorissa koska haluaisi siinä tilanteessa asioida kasvotusten.

3.3 Verkkopankkipalvelujen tarjoamat hyödyt

Verkkopankki tarjoaa selkeitä hyötyjä sekä pankeille että kuluttajille. Pankit saavuttavat huomattavia säästöjä liiketoimissaan siirtämällä palveluitaan verkkoon (Polatoglu & Ekin 2001). Työvoiman käyttö tehostuu ja henkilöstön tarve pienenee verrattuna perinteiseen konttoripalvelujen tarjontaan. Myös liiketilojen tarve pienenee kun konttoreiden määrää voidaan karsia verkkopalvelujen tarjonnan lisääntyessä. (Cheng ym. 2006.)

Suomessa pankkihenkilöstön ja konttorien määrä peräti puolittui kymmenessä vuodessa 1990 -luvun alkupuolelta lähtien. Muualla Euroopassa supistukset eivät ole olleet yhtä rajuja. (Riipinen & Tinnilä 2004, 18.) Suomi on yksi maailman johtavista maista verkkopankkipalvelujen omaksumista ja käyttöä ajatellen (Pikkarainen ym. 2006). Palvelujen suuri suosio selittääkin osaltaan sen, miksi Suomessa konttoreita on vähennetty enemmän kuin muualla.

Jayawardhena & Foley (2000) esittävät, että verkkopankin suurin hyöty pankeille koituu mahdollisuudesta siirtää henkilöstön työtehtäviä asiakkaille. Tätä

mahdollisuutta käytetäänkin nykyään yleisesti hyväksi yritysten markkinoinnissa. IKEA jättää huonekalujen kokoamisen asiakkaiden tehtäväksi ja pikaruokaloissa asiakas hoitaa itse siivouksen viemällä tarjottimen ja roskat pois pöydästä. Asiakas hoitaa siis osan yrityksen työtehtävistä vapaaehtoisesti ja palkatta osallistuen näin yrityksen tuotantoprosessiin. (Zwick ym. 2008.) Asiakkaasta on tullut yritykselle ilmaista ja hyödyllistä työvoimaa.

Jayawardhenan & Foleyn (2000) mukaan verkkopalveluita tarjoavan pankin potentiaalinen asiakaskunta laajenee kun konttoreiden sijainnilla ei ole enää yhtä suurta merkitystä kuin aiemmin. Yhtenä hyötynä he mainitsevat myös muiden kuin yrityksen ydintoimintojen kehittämisen (mt.). Suomessa lähes kaikkien pankkien palvelutarjontaan kuuluukin nykyään pankkipalveluiden ohella myös vakuutuspalveluita.

Verkkopankkipalvelut tarjoavat merkittäviä hyötyjä myös pankkien asiakkaille. Palvelujen saatavuus paranee kun niitä tarjotaan internetin kautta (Järvinen & Heino 2004, 14). Asiakkaan ei enää tarvitse matkustaa konttoriin maksaakseen laskuja tai tehdäkseen tilisiirtoja, vaan hän voi suorittaa toiminnot vaikkapa kotona tai työpaikalla. Myöskään ärsyttäväksi koettuun jonottamiseen ei tarvitse varata aikaa (mt., 33). Tässäkin tutkimuksessa yksi vastaaja mainitsi verkkopankin hyödyksi jonottamisen välttämisen. Hän arvostaa myös sitä, että verkossa saa rauhassa paneutua asioiden hoitamiseen. Konttorissa asioidessa takana oleva jono tuntuu painostavalta ja tällöin omien asioiden hoitoa saatetaan kiirehtiä.

Haastateltava kertoo:

> *No ensinnäki ei tarvi jonottaa. Mä voin hoitaa mun asiat milloin mä haluan. Ja jos oon ottamassa jotain uutta palvelua käyttöön ni mä saan rauhassa tutkia kaikki ne ehdot ja dokumentit läpi ja vertailla eri palveluvaihtoehtoja ilman että tarvii miettiä kuinka pitkä jono mun takana on. (H4)*

Verkossa asiointi on riippumatonta myös vuorokaudenajasta. Konttorit ovat avoinna ainoastaan virka-aikaan, minkä on katsottu vaikeuttavan pankissa asiointia (Järvinen

& Heino 2004, 35.) Verkkopankin käyttäjät arvostavatkin palvelun aika- ja paikkariippumattomuutta sekä palvelun tasalaatuisuutta (Karjaluoto ym. 2002). Tämän tutkimuksen haastatteluissa suurimmaksi koettiin nimenomaan palvelun riippumattomuus ajasta ja paikasta. Kaikki haastateltavat mainitsivat sen vastauksissaan.

Muita verkkoasioinnista koituvia hyötyjä asiakkaille ovat palvelun nopeus, kätevyys ja edullisuus (mm. Cheng ym. 2006; Karjaluoto ym. 2002). Omissa haastatteluissani esiintyneet vastaukset tukevat edellisiä tutkimuksia. Vastaajat kokivat verkkopankin huomattavasti edullisemmaksi palvelukanavaksi konttoriin verrattuna. Myös palvelun kätevyyttä ja monipuolisuutta arvostettiin – vastaajat hoitavat lähes kaikki pankkiasiansa verkkopankissa.

Verkkopankin käytössä nähtiin muitakin hyötyjä:

> *Mulla on niitä rahastosäästöjä ja niiden arvo heilahtelee ni seuraan niitä sieltä. Ja samoin e-lasku, et voi säästää paperia ja sit tunnistautuminen muihin virallisiin palveluihin. (H8)*

Verkkopankki on siis myös ympäristöystävällinen palvelukanava. E-laskujen säästämän paperin lisäksi pankit voivat vähentää postitse lähettämäänsä materiaalia kun asiakkaan kanssa voidaan pitää yhteyttä verkkopankin sisäisellä viestijärjestelmällä. Verkkopankkitunnuksien avulla pääsee asioimaan myös muihin virastoihin. Ainakin Verotoimiston ja Kelan palveluita voi käyttää internetin kautta ja palveluihin tunnistaudutaan verkkopankkitunnuksilla.

4 Verkkopankkipalvelujen turvallisuus

Valitettavasti verkkopankeissa asiointi houkuttelee myös rikollisia, joilla on monia keinoja päästä käsiksi uhriensa varoihin. Asiakkaiden olisikin syytä tiedostaa nämä turvallisuusuhat ja kiinnittää huomiota turvalliseen verkkoasiointiin. Esittelen tässä luvussa ensin erilaisia verkkopankin käyttöön kohdistuvia turvallisuusuhkia ja haastateltavien tietoisuutta niistä. Lopuksi pohdin tiedottamisen merkitystä..

4.1 Verkkopankin käyttöön liittyviä turvallisuusuhkia

Huolet verkkopankkipalvelujen turvallisuudesta estävät monia kuluttajia käyttämästä verkkopankkia (esim. Gerrard ym. 2006). Huolestuneisuus ei ole lainkaan turhaa, sillä phishing- eli tietourkintaviestit yleistyvät jatkuvasti. Phishingillä tarkoitetaan rikollista toimintaa, jossa sähköpostiviestien ja väärennettyjen internet-sivustojen avulla yritetään saada tietoon uhrien henkilökohtaisia tietoja, kuten pankkitunnuksia ja luottokorttitietoja (Sarel & Marmorstein 2006). Vanhin phishing-hyökkäysten muoto on sähköpostiviesti, jossa vastaanottajaa pyydetään lähettämään takaisin salasanojaan ja tilitietojaan. Tällaisten viestien teho on laskenut koska verkkopankin käyttäjät ovat usein tietoisia siitä, etteivät pankit lähesty asiakkaitaan sähköpostitse. (Kidra & Kruegel 2006.)

Nykyään phishing-hyökkäykset ovatkin huomattavasti kehittyneempiä. Yleisimmin hyökkäyksissä käytetään sähköpostiviestin ja väärennetyn internet-sivuston

yhdistelmää, joka on huomattavasti pelkkää sähköpostiviestiä tehokkaampi menetelmä. Viesti lähetetään pankin nimissä ja siinä pyydetään vastaanottajaa esimerkiksi päivittämään asiakastietojaan. Viestissä on linkki, joka ohjaa uhrin taitavasti väärennetylle sivustolle. Sivusto voi näyttää erehdyttävästi samalta kuin uhrin tuntema verkkopankkinäkymä, joten tämä ei välttämättä edes ymmärrä joutuneensa huijatuksi. Jopa sivuston URL-osoite voi näyttää täysin luotettavalta. (Kidra & Kruegel 2006.)

Hyökkäykset voivat olla tätäkin taitavammin rakennettuja. Rikolliset osaavat käyttää hyödykseen internet-selainten kuten Internet Explorerin heikkouksia ja voivat asentaa uhriensa koneille haittaohjelmia, joiden kautta he keräävät näiltä arkaluontoisia tietoja. Yksi keino on asentaa ohjelma, joka pitää lokia näppäimistön painalluksista (keylogger) tai monitoroi tapahtumia tietokoneen näytöllä (screenlogger). Kun uhri kirjautuu verkkopankkiin, hakkeri saa tietoonsa kaikki kirjautumiseen tarvittavat tiedot. (Kidra & Kruegel 2006; Emigh 2005, 9.)

Esimerkkinä tällaisista haittaohjelmista haastattelemani tietoturva-asiantuntija kertoo kansainvälisessä konferenssissa kuulleestaan tapauksesta, jossa eräs pankki oli käyttänyt kaksi vuotta idioottivarman verkkopankin rakentamiseen. Kyseisessä pankissa oli käytetty kirjautumisessa kiinteää käyttäjätunnusta ja salasanaa ja rikolliset olivat onnistuneet urkkimaan tunnuksia asiakkailta. Korjatakseen tilanteen, pankki oli kehitellyt verkkopankkinsa kirjautumissivulle virtuaalinäppäimistön, jolloin asiakkaat olivat ”näppäilleet” tunnuksensa tietokoneen hiirellä näppäimistön sijaan. Vain muutaman viikon kuluttua tästä uudistuksesta löydettiin haittaohjelma, jonka avulla rikolliset pääsivät jälleen käsiksi samaisen pankin asiakkaiden tunnuksiin. Rikollisten kehittämä haittaohjelma videoi asiakkaan hiiren kursoria tietokoneen näytöllä, jolloin uhrin tunnukset päätyivät siis jälleen vääriin käsiin.

Rikolliset voivat myös ohjata uhrin internet-liikenteen kulkemaan oman palvelimensa kautta. Tällaista tekniikkaa kutsutaan man-in-the-middle –tekniikaksi ja se uhkaa jopa suojattua yhteyttä käyttäviä verkkopankkeja. (Oppliger ym. 2006.) Emighin (2005) mukaan uhrin on vaikea havaita joutuneensa man-in-the-middle –hyökkäyksen kohteeksi koska rikollinen toimii istunnossa niin sanotusti välikätenä. Rikollinen välittää asiakkaan haluaman viestin pankkiin ja jälleen pankista takaisin

asiakkaalle mutta saa samalla haltuunsa asiakkaan tunnukset ja tilitiedot (mt., 11-12). Verkkopankki toimii siis asiakkaan näkökulmasta moitteettomasti. Todellisuudessa istunnossa on kuitenkin mukana pankin ja asiakkaan lisäksi myös kolmas osapuoli, rikollinen, joka seuraa uhrinsa asiointia verkkopankissa ja saa haltuunsa tämän verkkopankkitunnukset.

Verkkopankit toimivat siis aina suojatun yhteyden kautta. Suojatulla yhteydellä tarkoitetaan Secure Sockets Layer- eli SSL- tai Transport Layer Security- eli TLS-protokollia, joiden avulla todistetaan palvelimen eli palveluntarjoajan aitous ja suojataan asiakkaan ja palvelimen välinen yhteys. (Oppliger ym. 2006.) Suojatun yhteyden merkkejä ovat ehjän riippulukon kuva näytön alalaidassa tai osoitekentässä ja sivuston URL-osoitteen alku https normaalisti käytetyn http:n sijaan. Haastattelemani teleyrityksen turvallisuuspäällikkö muistuttaa, että vasta lukkoa klikkaamalla voi varmistua sivuston aitoudesta koska vasta tällöin näkee kuka sivuston omistaa. Rikollisetkin voivat siis rekisteröidä oman sivustonsa ja saada näin lukon kuvan näkyviin.

Turvallisuuspäällikön mukaan yksi phishingin muoto on istunnon kaappaaminen. Kun asiakas on kirjautumassa verkkopankkiin, rikollinen voi kaapata istunnon ja ohjata asiakkaan väärennetylle verkkopankkisivustolle. Uhri luulee antavansa tunnuksiaan verkkopankkiin kun todellisuudessa hän luovuttaakin tunnuksensa suoraan rikollisen käsiin. Saatuaan kirjautumiseen vaadittavat tunnukset rikollinen harhauttaa uhria vaikkapa niin, että uhrin koneella näkyy teksti, jossa kerrotaan että järjestelmää päivitetään. Tänä aikana rikollinen ehtii kirjautua asiakkaan tunnuksilla todelliseen verkkopankkiin ja tehdä tilisiirtoja asiakkaan tililtä itselleen. Kun asiakasta sitten tämän ”päivityksen” jälkeen pyydetään kirjautumaan uudelleen tähän väärennettyyn verkkopankkiin, rikollinen saa haltuunsa vielä tunnuksen, jolla hän vahvistaa tekemänsä tilisiirrot. Asiakas ei ole siis tässä esimerkissä päässyt lainkaan todelliseen verkkopankkiin, vaan hän on asioinut koko ajan väärennetyllä sivustolla.

Maailmalla levisi 18.11.2009 uutinen Belbloh-troijalaisesta, joka toimii verkkopankin sisällä käyttäjän tietämättä. Asiakas voi olla maksamassa laskua ja kaikki näyttää menevän oikein, mutta rahat ohjautuvatkin huijareiden tileille. Kuluttaja ei siis huomaa virhettä ja pankki luulee, että maksu on mennyt juuri niin

kuin asiakas on sen tarkoittanut. Kauppalehden haastattelussa F-Securen tutkimusjohtaja Mikko Hyppönen kertoo, että suomalaispankit olisivat hyvin alttiita tällaisille hyökkäyksille. Suomalaisten onneksi hyökkäyksiä ei ole kohdistettu tänne, koska rikolliset pitävät suomalaispankkeja syrjäisinä ja pieninä. Hyppösen mukaan hyökkäyksiä ilmenisi varmasti mikäli rikolliset olisivat tietoisia siitä, että esimerkiksi Nordean verkkopankki on käytössä useissa eri maissa. Pankit kuitenkin varautuvat tällaisiin hyökkäyksiin monitoroimalla asiakkaidensa tilitapahtumia. Mikäli asiakas on tekemässä suurta siirtoa tilille, jolle ei koskaan aiemmin ole suorittanut maksuja, saatetaan tapahtuma tarkistaa erikseen. (Kauppalehti 19.11.2009.) Myös haastattelemani asiantuntijat, teleyrityksen turvallisuuspäällikkö ja tietoturva-asiantuntija, pitävät Suomen syrjäistä sijaintia ja pientä markkina-aluetta yhtenä syynä siihen, että suomalaispankkeihin kohdistuneita hyökkäyksiä on esiintynyt hyvin vähän.

Viestintävirasto tiedotti 24.11.2009 Zlob-troijalaisesta, jonka epäiltiin olevan kohdennettu myös suomalaisiin verkkopankkeihin. Zlob-haittaohjelma muuttaa uhrin verkkoasetuksia ja ohjaa verkkopankkiliikenteen väärennetyille sivustoille. Viestintävirasto kehotti tämän vuoksi ensimmäistä kertaa teleyhtiöitä suodattamaan kuluttajien internet-liikennettä. (Viestintävirasto 2009.) Suomalainen teleyritys tiedottikin internet-sivuillaan, että se oli rajoittanut asiakkaidensa internet-liikennettä ja että tartunnan saaneilla koneilla internet-yhteys ei täten toiminut. Haastattelemani teleyrityksen turvallisuuspäällikkö kertoo, ettei pankkien asiakkaille koitunut Zlob-troijalaisen vuoksi taloudellisia vahinkoja. Haittaohjelma oli ilmennyt uhreilla niin, että he eivät päässeet pankkinsa sivuille lainkaan. Uhrien internet-liikenteen nimipalvelinasetuksia oli muutettu niin, että kun he yrittivät päästä verkkopankkiin, heitä oltiinkin ohjaamassa rikollisten omalle nimipalvelimelle. Tällä kertaa rikolliset epäonnistuivat. Heidän oma nimipalvelimensa oli siis virheellinen eikä sivustolle päässyt. Turvallisuuspäällikkö arveleekin, ettei hyökkäystä ainakaan tässä vaiheessa oltu varsinaisesti kohdistettu suomalaispankkien asiakkaisiin vaikka nimipalvelinasetuksia olikin pankkisivustojen osalta muutettu.

Nimipalvelin on turvallisuuspäällikön mukaan kehitetty helpottamaan internetin käyttöä. Sen avulla internet-sivustot saadaan ymmärrettävään muotoon eli kirjoitetuksi kieleksi numerosarjojen eli ip-osoitteiden sijaan. Asiakkaan on

huomattavasti helpompi syöttää osoitekenttään verkko-osoite, joka on yleisimmin yrityksen nimi kuin pitkänä numerosarjana esiintyvä ip-osoite. Rikolliset voivat siis muuttaa uhrin koneen nimipalvelinasetuksia koodaamalla oman väärennetyn sivustonsa toimimaan nimellä, joka on aiemmin johdattanut asiakkaan verkkopankkiin. Tästä syystä verkkopankkiin kirjautumista linkkien kautta tulisi välttää. Mikäli rikollinen on onnistunut asentamaan uhrin koneelle haittaohjelman, hän on voinut vaihtaa myös asiakkaan suosikeiksi tallentamien verkkosivujen nimipalvelinasetuksia, jolloin ne siis johdattavatkin rikollisten omille väärennetyille sivustoille.

Teleyrityksen tietoturva-asiantuntija kertoi haastattelussa toisesta epäonnistuneesta huijaustapauksesta. Tämä troijalainen oli kohdistettu lukuisiin pankkeihin, ja myös suomalainen Sampo oli löytynyt kohdepankkien listalta. Rikolliset olivat kuitenkin olleet huolimattomia, sillä verkkopankin osoitteeksi oli asetettu www.sampo.fi. Todellisuudessa Sampo Pankin verkkopankki toimii verkko-osoitteessa www.sampopankki.fi. Tässä tapauksessa mitään uhkaa suomalaispankin asiakkaille ei siis syntynyt.

Nimipalvelinasetuksia muuttamalla tapahtuvasta phishingista voidaan käyttää nimitystä pharming (Emigh 2005, 10). Myös Finanssialan Keskusliiton avaamalla pankkiturvallisuussivustolla kerrotaan pharmingista. Siellä phishing määritellään toiminnaksi, jossa rikollinen pyytää avoimesti uhriaan luovuttamaan arkaluontoisia tietojaan kuten verkkopankkitunnuksiaan esimerkiksi sähköpostin avulla. Pharming taas määritellään toiminnaksi, jossa rikollinen pyrkii saamaan uhrilta tunnuksia tämän tietämättä eli asentamalla uhrin koneelle erilaisia haittaohjelmia tai vakoilemalla uhrin internet-liikennettä. (FK 2010.) Käytän tässä tutkimuksessa selkeyden vuoksi termiä phishing kuvaamaan yleisesti kaikkea verkossa tapahtuvaa rikollista toimintaa.

Nordean verkkopankkiasiakkaisiin kohdennettu haittaohjelma havaittiin tammikuussa 2010. Verkkopankin sisäänkirjautumissivu oli ohjelman myötä muuttunut englanninkieliseksi, ja sivuilla kerrottiin meneillään olevista huoltotoimenpiteistä. Rikolliset onnistuivat siirtämään 15:sta asiakkaan tileiltä varoja yhteensä noin 50 000 euron arvosta. Nordea korvasi asiakkailleen taloudelliset

tappiot. (Helsingin Sanomat 18.1.2010.) Nordea tiedotti asiasta verkkopankin kirjautumissivulla.

Jälleen maaliskuussa 2010 oli liikkeellä phishing-viestejä, joilla yritettiin kalastella Nordean asiakkaiden pankkitunnuksia. Myös Osuuspankin (OP) asiakkaille oli maaliskuussa lähetetty huijausviestejä, joissa pyydettiin asiakasta avaamaan tili viestissä olleen linkin kautta. Yhden viestin otsikko oli ”Turvallisuuspolitiikan H?lytt?v?t!" (OP 2010a). Jo otsikosta voi havaita, että viestit on kirjoitettu erittäin huonolla suomenkielellä. Molemmat pankit tiedottavat tapauksista omilla verkkosivuillaan. Tiedotteet ovat hyvin lyhyitä ja niissä kehotetaan asiakkaita poistamaan viestit välittömästi. Tiedotteissa ei mainita sitä ovatko jotkut asiakkaat vastanneet näihin viesteihin ja korvaako pankki asiakkaalle aiheutuneet taloudelliset vahingot tällaisissa tapauksissa. (Nordea 2010a; OP 2010a.)

Molemmat haastattelemani asiantuntijat painottavat, että Suomessa pankit ovat hoitaneet oman osansa verkkopankkien turvallisuuden kehittelyssä hyvin. Itse verkkopankkiin ei siis varsinaisesti liity turvallisuusuhkia, vaan uhkana ovat rikolliset. Vaikka pankit tekevät jatkuvasti työtä turvallisuuden parantamiseksi ja huijausten vaikeuttamiseksi, rikollisten huijauskeinot parantuvat yhtä lailla.

4.2 Haastateltavien tietoisuus turvallisuusuhista

Suurimmalla osalla tietokoneen käyttäjistä on suhteellisen heikko tietämys käyttämänsä järjestelmän turvallisuustasosta (Wang ym. 2003). Myös tämän tutkimuksen haastateltavat olivat melko tietämättömiä verkkopankin käyttöä koskevista turvallisuusuhista. Yksi haastateltavista ei ollut lainkaan tietoinen siitä, että verkkopankin käyttöön voisi liittyä turvallisuusuhkia. Kyseinen vastaaja on asunut Hollannissa vuosien ajan ja hänellä on ollut asiakkuus paikalliseen pankkiin. Siellä verkkopankkiin kirjautumiseen tarvitaan erillinen laite, joka antaa lopullisen salasanan. Laite ehkäisee phishing-viestien tehon, koska asiakas ei voi luovuttaa sähköpostitse kaikkia kirjautumiseen vaadittavia verkkopankkitunnusten osia. Mikäli käytäntö on hollantilaispankkien keskuudessa yleinen, voi olla, ettei siellä esiinny

kalasteluviestejä. Tämä selittäisi sen, että kyseinen haastateltava ei ole tietoinen viestien esiintymisestä.

Myös toinen haastateltava sanoi ensin, ettei ole tietoinen mistään turvallisuutta uhkaavista tekijöistä. Kysyessäni erikseen edellisessä luvussa mainituista uhista, hän kuitenkin muisti kuulleensa phishing-viesteistä:

> *Ainiin näistä, joo kyllä oon kuullu. Mitä saattaa tulla sähköpostilla. Totta. Niin joo pankin nimissäki saattaa tulla, että anna pankkitunnuksia. (H2)*

Loput haastateltavat osasivat heti nimetä phishing- eli kalasteluviestit kysyessäni ovatko he tietoisia verkkopankkiin liittyvistä turvallisuusuhista. Phishing-viestejä on esiintynyt Suomessakin jo muutamien vuosien ajan ja niistä on myös varoiteltu mediassa. Vastaajat arvioivat, että he tunnistaisivat tällaiset huijausviestit eivätkä lähtisi vastaamaan niihin. Tämän vuoksi viestejä ei koeta myöskään varsinaisena uhkana itselle. Kalasteluviestit ovat siis haastateltaville hallittu turvallisuusriski edistyneempien hyökkäysten muodostaessa tuntemattoman turvallisuusuhan.

Haastateltavat kertovat:

> *Uutisointii on ollu et lähetetään pankin nimis viestii et pitää lähetellä tunnuksii tai muuta vastaavaa mut ei itselle oo mikään kauheen realistinen uhka ku ei tulis mieleenkään lähettää sähköpostil yhtään mitään tunnuksia. (H5)*

> *Et onhan niit kalasteluviestei ku ihmisilt pyydetään salasanoi ja muuta mut en nyt koe et ne kauheesti mua järkyttäis et ei tulis mieleenkään antaa kellekään mitään salasanoi millään sähköpostilla. Oon iteki joskus saanu niit viestejä. Siit on kyl aikaa ja tuhosin ne saman tien. (H1)*

Pankkien ja median varoitukset phishing-viesteistä ja ohjeet siitä, ettei viesteihin saa vastata ovat siis näemmä iskostuneet haastateltaviin hyvin. Lähteenmäki (2009, 37-

41) esittelee väitöskirjassaan kuluttajien erilaisia hallintakeinoja yksityisyytensä suojelemiseksi. Hänen tutkimuksessaan käsitellään yritysten toimesta tapahtuvaa asiakkaidensa henkilötietojen keräämistä markkinointitarkoituksiin. Kyse ei siis ole laittomasta toiminnasta, joka taas on oman tutkimukseni mielenkiinnon kohteena. Mielestäni yllä esittämäni sitaatit voi kuitenkin tulkita edustamaan samankaltaista hallinnan tunnetta. Huijausviestejä ei koeta uhkana, koska ne tunnistetaan ja osataan toimia oikein eli viestit poistetaan heti. Vastaajat kokevat näin olevan tällaisten huijausyritysten ulottumattomissa.

Yksi haastateltava oli joutunut erikoiseen tilanteeseen kun hänelle oli soitettu omasta pankista:

> *En muista miks mut he halus varmaan tarkastaa jotain perustietoja, sit mult puhelimitse kysyttiin omasta pankista mun verkkopankin tunnuksia. Ja mun mielestä se oli tosi outoo, et se oli kyllä ihan oikeella asialla mut mä en suostunu antamaan niitä siinä puhelimitse... Mut et se oli tosi outoo ja sen jälkeen tätä ei oo tapahtunu... Eihän niiden pitäis tolleen niitä kysellä. Ja niidenkin pitäis se ymmärtää et hei, täähän sotii vastoin teidän omia neuvoja. (H2)*

Tässä tapauksessa pankki on toiminut erittäin kyseenalaisesti. Tietojen kalastelua harrastetaan myös puhelimitse, joten on vähintäänkin erikoista että pankin henkilöstö pyytää asiakkaaltaan verkkopankkitunnuksia tällä tavoin. Haastateltavalle oli jäänyt puhelusta hämmentynyt olo. Hän ei siis ollut suostunut antamaan tunnuksiaan ja virkailija oli sitten varmistunut hänen henkilöllisyydestään muulla tavoin. Asiakkaan ottaessa itse yhteyttä pankin puhelinpalveluun, on normaali käytäntö tunnistaa asiakas verkkopankkitunnuksilla. Tässä tapauksessa puhelu oli kuitenkin tullut nimenomaan pankin puolelta, jolloin asiakas ei voi varmistua soittajan henkilöllisyydestä. Tällaiset tapaukset ovat epäilemättä omiaan vähentämään asiakkaan luottamusta pankkia kohtaan. Jos pankista neuvotaan, ettei verkkopankkitunnuksia saa antaa kenellekään ja kuitenkin niitä kysytään pankin omasta toimesta puhelimitse, antaa tämä erittäin sekavan kuvan asiakkaalle. Voi vain

toivoa, että tässä tapauksessa on tapahtunut inhimillinen virhe eikä tällaista toimintaa harjoiteta kyseisessä pankissa yleisesti.

Yksi vastaajista osasi kertoa muitakin hyökkäysesimerkkejä. Tämä haastateltava on harrastanut tietotekniikkaa monia vuosia, joten ei sinänsä ole ihme että hänen tietämyksen tasonsa on aivan toista luokkaa kuin muiden vastaajien. Myös tietotekninen termistö on hänellä hyvin hallussa. Toisellakin haastateltavalla oli epäilyksiä, että jotakin arveluttavaa saattaisi tapahtua. Hän ilmaisee huolensa hyvin arkisella kielellä eikä tunne termejä, mutta uhkakuva muistuttaa vahvasti juuri istunnon kaappausta tai muuta tilannetta, jossa rikollinen on saanut käsiinsä uhrin verkkopankkitunnukset.

Haastateltavat kuvailevat turvallisuusuhkia:

> *...Sit on näitä virus-ja troijalaistyyppisiä softia jotka saattaa ihan kaapata sitä sun syötettä ja sitä kautta saada sun kirjautumistiedot. Sit on vielä nää ihan viimesintä tekniikkaa käsittääkseni sisältävät jotka siis tunnistaa sen ku olet verkkopankkiin kirjautuneena ja tekee sieltä siirtoja tai toimintoja ja sit peittää jälkensä tai antaa sulle eteen valheellisen version siitä ikkunasta peittääkseen ne omat siirrot. (H4)*

> *Varmaan ihan se tietoturva et ikään kun ne muurit siinä ympärillä, et sinne ei pääse kukaan muu silloin ku mä esim käytän sitä tai sillon ku en käytä mut ettei kukaan muu pääse sinne mun tilille. Et joku menis niinku minuna sinne tai varastais mun salasanat tai näin. (H1)*

Edistyneemmistä hyökkäyksistä osasi varmuudella kertoa siis ainoastaan yksi vastaaja, muilla tietämys jäi phishing-viesteihin. Tämän aineiston perusteella vaikuttaa siltä, että suurempi tietoisuus turvallisuusuhista vähentää huolestuneisuutta. Vastaajat eivät kokeneet phishing-viestien aiheuttavan uhkaa heidän verkkopankin käytölleen koska niitä vastaan osattiin toimia. Tässä valossa pankkien olisi mielestäni hyvä pyrkiä kasvattamaan asiakkaidensa tietoisuutta erilaisista turvallisuusuhista. Sähköpostiviestit ovat tosin yksinkertaisin huijausmuoto, jota vastaan on helppo toimia. Edistyneempiä hyökkäyksiä vastaan on vaikeampi varautua. Marraskuussa

2009 uutisoitiin Belbloh- (Kauppalehti 19.11.2009) ja Zlob-troijalaisista (Viestintävirasto 2009), jotka aiheuttivat huolestuneisuutta myös Suomessa. Nämä uutiset eivät siis olleet tavoittaneet haastateltavia. Seuraavassa alaluvussa käsittelenkin turvallisuusasioista tiedottamista.

4.3 Turvallisuusuhista tiedottaminen

Tämän tutkimuksen haastateltavat olivat melko tietämättömiä verkkopankin käyttöön liittyvistä turvallisuusuhista. Eräsaaren (1997, 83) mukaan viime aikoina teollisuus, vakuutusyhtiöt ja julkinen sektori ovat laskeneet liikkeelle lukuisia julkaisuja riskien ja vaarojen välttämisestä ja erottamisesta ja hän kutsuu tätä riskikasvatukseksi. Mielestäni pankit voisivat myös harjoittaa tällaista riskikasvatusta tiedottamalla asiakkaitaan erilaisista turvallisuusuhista ja kertomalla kuinka niihin voi varautua.

Edellisessä luvussa ilmeni, että pankit ja media ovat tiedotuksen avulla onnistuneet muuntamaan phishing-viestit uhasta riskiksi myös haastateltavien osalta. Uhasta tulee siis riski silloin kun uhka opitaan tuntemaan ja sitä osataan kontrolloida (Eräsaari 1997, 78). Kalasteluviestit ovat mielestäni hyvä esimerkki tästä – yhtä vastaajaa lukuun ottamatta kaikki tiesivät viestien esiintymisestä ja mikäli niitä saatiin, ne osattiin poistaa. Kommenteistakin ilmeni, ettei viestejä koettu tämän vuoksi uhkina vaan neutraalina ilmiönä, jota vastaan osataan toimia.

Haastattelemieni asiantuntijoiden mukaan suomalaispankit voisivat parantaa asiakkaidensa tiedottamista verkkopankin käyttöä koskevista turvallisuusuhista. Turvallisuuspäällikkö peräänkuuluttaa erityisesti täsmätiedottamista – mikäli pankki on tietoinen heidän asiakkaisiinsa kohdistuvasta hyökkäyksestä, asiakkaille tulisi kertoa avoimesti mistä on kyse ja antaa heille tarvittaessa toimintaohjeita tilanteeseen. Edellisessä luvussa kerroin maaliskuussa 2010 tapahtuneista phishing-hyökkäyksistä. Näistä kyllä mainittiin pankkien sivuilla, mutta hyvin lyhytsanaisesti. Tiedotteissa kerrotaan ainoastaan mitä on tapahtunut, ja että viestit tulee poistaa välittömästi. Lisäksi asiakkaita, jotka ovat luovuttaneet pankkitunnuksiaan pyydetään ottamaan välittömästi yhteyttä pankkiin. (OP 2010a; Nordea 2010a.) Mielestäni

pankit voisivat osaltaan käyttää tällaisia tapauksia hyväkseen ja tiedottaa laajemmin ilmiön taustoista ja myös muista phishingin muodoista.

Kuluttajat ovat epäilemättä kiinnostuneita omista raha-asioistaan ja haluavat välttää tilanteita, joissa heiltä viedään omaisuutta. Asiakas ei kuitenkaan voi varautua uhkaan, jonka olemassaolosta hän ei ole tietoinen. Pankeilla olisikin hyvät mahdollisuudet lisätä asiakkaidensa tietoisuutta erilaisista turvallisuusuhista tiedottamalla heitä rikollisten toiminnasta. Ilmeisesti suomalaispankit eivät ainakaan vielä ole valmiita tähän, vaikka pankkien kustannukset asian tiimoilta voisivat pudota rajustikin siinä tapauksessa, että asiakkaat tunnistaisivat rikolliset hyökkäykset ja voisivat näin ollen pienentää riskiä tulla huijatuksi. Emighin (2005) mukaan phishing-hyökkäyksistä aiheutuneet suorat kustannukset yhdysvaltalaispankeille ylsivät 1,2 miljardiin dollariin vuonna 2003 epäsuorien kustannusten noustessa tätäkin suuremmiksi. Epäsuorat kustannukset aiheutuvat asiakkaiden lisääntyvistä yhteydenotoista hyökkäyksen ilmettyä, uusien tilien avaamisesta sekä vähentyneestä verkkopalveluiden käytöstä kun asiakkaat pelkäävät uusia hyökkäyksiä. (mt., 6.)

Luvussa 4.2 ilmeni, että kukaan haastattelemistani henkilöistä ei ollut havainnut uutisointia Belbloh- ja Zlob-troijalaisista marraskuussa 2009. Haastattelemani teleyrityksen turvallisuuspäällikkö muistuttaa, että pankit eivät tiedottaneet lainkaan näistä troijalaisista vaan tiedotus tapahtui median ja operaattorien toimesta. Hän olisi toivonut, että pankit olisivat tiedottaneet asiasta kaikkia asiakkaitaan verkkopankin sisäisellä viestintäjärjestelmällä. Nykyisessä informaatiotulvassa kuluttajan on mahdotonta sisäistää kaikkea uutisointia. Monet ovat todennäköisesti jättäneet marraskuun uutiset lukematta ajatellen, että asia ei kosketa häntä itseään. On ehkä nähty troijalaisten erikoiset nimet ja ajateltu, että tietotekniikka ei kiinnosta. Jos tieto olisi tullut verkkopankin kautta, vaikutus olisi saattanut olla toinen. Tällöin uutiset olisi osattu yhdistää verkkopankissa asiointiin ja asiakkaiden mielenkiinto olisi saattanut herätä.

Tämän tutkimuksen haastateltavat olivat kuulleet turvallisuusuhista lähinnä uutisista. Vain kaksi vastaajaa kertoi saaneensa tietoa omasta pankista. Lisäksi täytyy muistaa, että kahta vastaajaa lukuun ottamatta haastateltavat olivat tietoisia ainoastaan sähköpostiviestitse tapahtuvista huijauksista. Tästä huolimatta osa heistä oli sitä

mieltä, että tiedotus on riittävää: *No mulle ne on niin päivänselviä, et on niistä kuitenkin puhuttu. Et mun mielestä se on ihan ok tasolla. (H2)* Kyseinen haastateltava puhuu nimenomaan väärennetyistä sähköpostiviesteistä. Hänelle on selvää, että viesteihin ei vastata vaan ne poistetaan heti. Haastattelun tässä vaiheessa olin kuitenkin kertonut myös muista mahdollisista hyökkäyskeinoista. Siitä huolimatta hän ei kaipaa lisää tiedotusta turvallisuusasioista.

Osa haastateltavista taas oli sitä mieltä, että pankkien tulisi lisätä tiedotusta:

> *Kyl mun mielest todellaki pitäis kertoo, just et minkälaisia ne viestit on ja miten ne tunnistaa. Et ei sen mun mielest näin pitäis mennä et mä aan tän tiedon tutkimuksen kautta, johon mä sattumalta ajaudun. (H8)*

> *No tääl Suomes nyt eletään vähän tälleen niinku herran kukkarossa, et ei oikeestaan mietitä et on mitään uhkia ennen ku se sattuu omalle kohdalle. Et siin mielessä ehkä sitä tiedotusta vois olla enemmän. Et veikkaan et vaikka se tieto siel nettisivuilla on ni en oo ainoo joka sitä ei sieltä itse kaiva. (H5)*

Tiedotuksen pitäisi siis haastateltavien mielestä olla aktiivista. Pankkien sivuilta löytyy kyllä tietoa turvallisuusasioista, mutta yksikään haastateltava ei ollut huomannut näitä turvallisuusosioita. Ensimmäinen kommentti on haastateltavalta, joka ei ollut koskaan kuullut edes phishing-viesteistä. Hän on olettanut verkkopankin olevan turvallinen siksi, että pankkitunnuksia käytetään tunnistautumiseen myös tärkeissä julkisissa palveluissa kuten verotoimiston sivuilla. Hän oli hyvin ihmeissään kerrottuani erilaisista turvallisuusuhista, joita verkkopankin käyttöön liittyy. Kommentista kuvastuu pettymys siitä, että pankista ei ole kerrottu mitään aiheesta. Toinen kommentti osuu mielestäni asian ytimeen – jotta kuluttajat kiinnostuisivat asiasta ja alkaisivat omatoimisesti etsiä siitä tietoa, pitäisi todennäköisesti joutua itse huijauksen kohteeksi. Rikollisen hyökkäyksen kohteeksi joutuminen voisi muuttaa mielipiteitä myös niiden vastaajien osalta, jotka eivät nykyisellään kaivanneet enempää tiedotusta aiheesta. Lisäksi se, että aiheesta kuullaan muualta kuin palvelun tarjoajalta, voi heikentää luottamusta pankkeihin.

Paras kanava tiedottamiseen olisi haastateltavien mielestä verkkopankin sisäinen viestijärjestelmä. Pankin lähettämiä kirjeitä ei aina edes avata, joten perinteinen posti ei välttämättä tavoittaisi haastateltavia.

Tutkittavat kommentoivat:

> *Aluks tuli mieleen se joku vihkonen mut mä harvoin jaksan avata mitään pankin kirjeitä tai tiliotteita. Ehkä ku on kyse just verkkopankin käytöstä ni se vois olla sellanen popuppi tai vastaava, tai siin etusivulla selkeesti ja isolla jonku puol vuotta, et lue tää, tähän menee max kaks minuuttii ja tiedät asiasta vähän enemmän. (H7)*

> *Tos mun verkkopankis on kätevä ku siihen tulee ihan etusivulle jos on joku ilmotus, et sen pakosti huomaa. Et vanhas pankissa näky vaan et on joku viesti ni aika usein tuli skippailtua ne. Et en menny ees kattoo niitä ku aika usein pankin viestit on vähän sellasii et blaah, pitäiskö mun ymmärtää täst jotain? Ja sit mä oon sillee et ehkä ei. (H1)*

Viestin pitäisi siis olla selkeä ja helposti huomattavissa. Kommenteista voi havaita, että haastateltavat eivät itse halua nähdä vaivaa tiedon etsimiseen. Viesti tulisi lähettää niin, että sitä ei voi olla havaitsematta. Myös viestin kielelliseen muotoon tulisi kiinnittää huomiota. Liian tekninen kieliasu voi aiheuttaa toisessa kommentissa esille tulevan ilmiön, jossa viestiä ei edes jakseta lukea kun ajatellaan, että sisältöä ei kuitenkaan ymmärretä. Tiedotteiden tulisi siis olla kielellisesti hyvin yksinkertaisia. Kuluttajien tietotekniset taidot vaihtelevat suuresti, joten tiedotteet tulisi laatia niin, että myös vähemmän tietokonetta käyttäneet asiakkaat ymmärtäisivät sisällön. Nämä vähiten tietokonetta käyttäneet muodostavat myös eniten tiedotusta tarvitsevan ryhmän. Tietotekniikan ammattilaiset ja harrastajat ovat epäilemättä jo valmiiksi tietoisempia turvallisuusuhista ja omista mahdollisuuksista varautua niihin. Casaló ym. (2007) painottavat sitä, että verkkopankin pitäisi ylipäätään olla selkeä ja yksinkertainen, jotta asiakkaat kokevat sen miellyttäväksi ja turvalliseksi.

5 Turvallisuuden parantaminen

Pankeilla on monia keinoja parantaa verkkopankin turvallisuutta. Suuri osa näistä keinoista vaatii kuitenkin myös kuluttajien osallistamista (Sarel & Marmorstein 2006). Pankkien vastuulla on toki omien järjestelmien luominen viimeisimpien päivitysten mukaisiksi, mutta myös kuluttajilla on oma roolinsa turvallisuusasioissa. Tässä luvussa käsittelen ensin pankkien keinoja parantaa verkkopankkien turvallisuutta ja siirryn sitten kuluttajiin eli kerron ohjeistuksesta, jota kuluttajille on tarjolla turvalliseen verkossa asiointiin. Lopuksi käsittelen kysymystä taloudellisesta vastuunjaosta tilanteissa, joissa asiakas menettää varojaan onnistuneen huijauksen johdosta. Tässä luvussa esitän useita viittauksia käyttämiini verkkoaineistoihin, jotka on lueteltu lähdeluettelossa kirjallisuusviitteiden jälkeen.

5.1 Pankkien keinoja parantaa turvallisuutta

Edellisessä luvussa mainitsin, että verkkopankit toimivat aina suojatun yhteyden kautta. Lisäksi palomuurit ja muut tekniset ratkaisut, joita pankit käyttävät turvallisuuden ylläpitoon, ovat kehittyneet viime aikoina ja monet pankit ovatkin kasvattaneet investointejaan tietotekniseen osaamiseen. Pankkien sisäisten järjestelmien kehittäminen vaikeuttaa rikollisten tunkeutumista pankin järjestelmään, muttei poista phishing-hyökkäysten aiheuttamaa uhkaa asiakkaille. (Sarel &

Marmorstein 2006.) Pankki ei voi toimillaan estää kalasteluviestien tai muiden phishingin muotojen esiintymistä.

Casalón ym. (2007) mukaan pankkien tulisi parantaa turvallisuutta asiakkaiden näkökulmasta. Asiakkaiden luottamus pankkia kohtaan kasvaa mikäli he kokevat verkkopankin turvalliseksi. Asiakkaiden kokemaa turvallisuutta voidaan parantaa tarjoamalla kuluttajille aiheeseen liittyvää koulutusta. Myös verkkopankin ulkoasu voi vaikuttaa asiakkaiden kokemaan turvallisuuden tunteeseen. Sivuston tulisi olla mahdollisimman yksinkertainen ja helppokäyttöinen, jotta kuluttajan ei tarvitse keskittyä toimintojen tekniseen puoleen vaan hän saa hoidettua pankkiasiansa sujuvasti. Lisäksi pankkeja kannustetaan tarjoamaan sivustoillaan linkkejä kuluttajajärjestöjen sivuille, jotta asiakkaalle välittyisi kuva että hänen hyvinvoinnistaan kannetaan huolta. (Casaló ym. 2007.)

Turkkilaispankit tarjoavat asiakkailleen mahdollisuuden käyttää virtuaalista näppäimistöä. Näppäimistön käytön eli nappien painalluksien sijaan asiakkaat syöttävät salasanansa näytöllä näkyvän virtuaalinäppäimistön kautta. Tällä estetään sellaisten haittaohjelmien toiminta, jossa rikollinen pitää lokia uhrin näppäimistön painalluksista. On kuitenkin olemassa myös haittaohjelmia, jotka pitävät lokia näytöllä tapahtuvista toimista ja niihin virtuaalinäppäimistö ei luonnollisestikaan auta. (Sayar & Wolfe 2007.) Tämä huomattiin luvussa 4.1, jossa haastattelemani teleyrityksen tietoturva-asiantuntija kertoi todellisuudessa tapahtuneesta esimerkistä virtuaalinäppäimistön tehottomuudesta. Teleyrityksen turvallisuuspäällikkö kertookin, että turvallisuuden parantaminen pankkien osalta ja rikollisten omien teknisten ratkaisujen kehittäminen toimivat eräänlaisessa kierteessä. Kun pankit kehittävät teknisen ratkaisun johonkin tietoturvaongelmaan, rikolliset yrittävät heti keksiä siihen kiertotoimen.

Pankit voivat myös pyrkiä tunnistamaan turvallisuusuhat mahdollisimman nopeasti. Ne voivat käyttää hyväkseen ohjelmistoja, jotka etsivät internetistä sivustoja joissa esiintyy yrityksen nimi tai tuotemerkki. Tällaiset ohjelmistot tarkkailevat myös internetin nimipalvelimia ja voivat näin löytää väärennettyjä sivustoja. Mikäli ohjelmistot löytävät turvallisuusaukkoja, pankkien tulisi tiedottaa asiakkaitaan vallalla olevasta uhasta. Pankit ovat kuitenkin usein haluttomia tähän. (Sarel &

Marmorstein 2006.) Edellisessä luvussa mainitun vuoden 2009 marraskuun Zlob-troijalaisen ilmettyä yksikään pankki ei tiedottanut siitä asiakkaitaan. Haastattelemani turvallisuuspäällikkö arvelee tämän johtuvan siitä, että media ei yksilöinyt sitä pankkia, jonka asiakkaille troijalainen olisi voinut aiheuttaa haittaa. Näin ollen pankit halusivat pysyä vaitonaisina, jotta niitä ei yhdistettäisi hyökkäykseen.

Koko rahoitusala voi tehdä yhteistyötä rikollisuuden estämiseksi. Yritysten aktiivisuus tiedonjakamisessa johtaa parhaillaan uhkien nopeaan tunnistamiseen. Kun petosyrityksiin puututaan nopeasti, ne voidaan myös tehdä nopeasti tehottomiksi. (Sarel & Marmorstein 2006.) Haastattelemani tietoturva-asiantuntijan mukaan eri tahojen yhteistyö toimii Suomessa hyvin. Pankit, operaattorit ja viranomaiset pyrkivät yhteisvoimin estämään ja korjaamaan internetissä tapahtuvia rikoksia. Pankit pystyvät rikollista toimintaa havaitessaan estämään epäillyttävät tilisiirtoyritykset. Pankit voivat myös pyytää operaattoreita estämään asiakkaidensa pääsy väärennetyille internet-sivustoille. Operaattorit taas keskustelevat Viestintäviraston kanssa riskien laajuudesta ja yhteisistä toimintamalleista. Tietoturva-asiantuntijan mukaan yhteistyö toimii myös kansainvälisellä tasolla eli suomalaisoperaattorit saavat tietoa väärennetyistä sivustoista ympäri maailman, muun muassa muilta operaattoreilta.

Yksi tehokas keino pankeille on parantaa verkkopankkiin kirjautumisen eli asiakkaan tunnistautumisen turvallisuustasoa. Tunnistautumisen tasot voidaan jakaa kolmeen osaan: yksiportainen (single factor), kaksiportainen (2-factor) ja moniportainen (multi-factor) tunnistautuminen. Turvallisuustaso on parhaimmillaan moniportaisessa mallissa. Yksiportaisessa mallissa kirjautuminen tapahtuu asiakkaan tiedossa olevien asioiden perusteella, kuten käyttäjätunnuksella ja salasanalla. Kaksiportaisessa mallissa tarvitaan lisäksi jotakin konkreettista asiakkaan hallussa olevaa esinettä, kuten pankkikorttia tai erillistä laitetta. Moniportaisessa järjestelmässä tarvitaan edellisten lisäksi jotakin asiakkaan fyysisesti yksilöivää elementtiä, kuten sormenjälkeä, allekirjoitusta tai ääninäytettä. (Gupta ym. 2004.) Suomen malli sijoittuu oman näkemykseni mukaan ensimmäisen tason yläpäähän. Suomalaispankkien kirjautumismallit ovat melko yhtäläisiä. Asiakkaat tarvitsevat tunnistautumiseen yleisimmin käyttäjätunnuksen, salasanan sekä avainlukutaulukon,

josta löytyvät kertakäyttöiset salasanat. En kuitenkaan tulkitsisi avainlukutaulukkoa toisen portaan erilliseksi laitteeksi, koska rikolliset voivat saada kertakäyttöisiä salasanoja haltuunsa phishing-viesteillä. Itse tunnuslukutaulukkoa ei siis tarvita kirjautumiseen, ainoastaan sen sisältämää tietoa.

Weir ym. (2009) selvittivät tutkimuksessaan erilaisten verkkopankkiin kirjautumiseen käytettävien ulkoisten laitteiden toimivuutta kuluttajien näkökulmasta. He testasivat kolmea eri tavoin toimivaa laitetta; ensimmäinen laite antoi salasanan napin painalluksella, toinen laite antoi salasanan kun siihen syötettiin kortti ja kolmanteen laitteeseen piti kortin lisäksi syöttää kortin pin-koodi ja salasanan sai vasta tämän jälkeen. Tutkittaville annettiin ohjeet laitteiden käyttöön sekä muutama yksinkertainen tehtävä suoritettavaksi verkkopankissa. Mikäli tutkittava epäonnistui kolmesti kirjautumisessa verkkopankkiin, hänen tuli lukea ohjeet uudelleen ennen seuraavaa yritystä. Eniten virheitä kirjautumisessa tapahtui laitteella, johon piti syöttää sekä kortti että kortin pin-koodi saadakseen salasanan. Tutkittavat ärsyyntyivät mikäli he joutuivat palaamaan ohjeen lukuun kun kirjautuminen ei onnistunut. Suosituimmaksi nousikin yksinkertaisin laite, josta salasanan sai yhdellä napin painalluksella. Turvallisuudeltaan tämä laite oli huonoin testatuista laitteista. Vaikeimmaksi koettiin turvallisin laite, johon siis piti syöttää sekä kortti että kortin pin-koodi. Tutkimuksessa testattiin laitteiden käyttöä myös toistamiseen. Toisella kerralla laitteisiin suhtauduttiin myönteisemmin ja kirjautuminen sujui vaivattomammin kuin ensimmäisellä kerralla. (Weir ym. 2009.) Mikäli pankki haluaa ottaa käyttöön erillisen laitteen, jonka avulla verkkopankkiin kirjaudutaan, onkin ensisijaisen tärkeää kouluttaa asiakkaita huolellisesti laitteen käyttöön.

Kysyin oman tutkimukseni haastatteluissa tutkittavien suhtautumista tällaisiin ulkoisiin laitteisiin. Turvallisuuspäällikön asiantuntijahaastattelussa tuli esille myös mahdollisuus käyttää matkapuhelinta kirjautumisessa. Käytännössä tämä vaihtoehto toimisi niin, että kun asiakas on kirjautumassa verkkopankkiin, pankki lähettäisi hänelle tekstiviestin matkapuhelimeen ja lopullinen kirjautuminen verkkopankkiin onnistuisi puhelimen nappia painamalla. Kysyin siis haastateltavien suhtautumista seuraaviin vaihtoehtoihin:

1) ulkoinen laite, joka antaa salasanan
2) ulkoinen laite, johon syötetään kortti ja kortin pin-koodi ja joka sitten antaa salasanan
3) matkapuhelin, johon tulee tekstiviesti ja kirjautuminen tapahtuu puhelimen nappia painamalla

Yksi haastattelemistani henkilöistä on asunut Hollannissa vuosien ajan ja hänellä on ollut asiakkuus pakalliseen pankkiin. Sieltä hänellä on jo ollut käytössä laite, johon syötetään pankkikortti ja kortin pin-koodi ja saadaan sitten laitteesta verkkopankkiin kirjautumiseen tarvittava salasana.

Hän kommentoi laitteen käyttöä seuraavasti:

> *Se on kyl tosi helppokäyttönen et ainoo mikä siin on et siin välil loppu patterit siin laitteessa et se oli tosi ärsyttävää jos oli just hoitamas jotain asiaa ja sit ne yhtäkkii loppu ni se oli tosi harmittavaa. Ja sit jos oon unohtanu sen laitteen ku en sitä kuljettanu aina mukana ni siin mieles se avainlukulista on kätevämpi ku se kulkee aina lompakossa. (H8)*

Itse laitteen käytettävyys on siis ollut hyvä eikä käytön kanssa ole koitunut ongelmia. Verkkopankin käytettävyys on kuitenkin kokonaisuudessaan heikentynyt laitteen myötä. Laitteen kanssa asiakkaan tulee ottaa huomioon asioita, joita ei Suomen kirjautumissysteemissä ole tarvinnut ajatella kuten pattereiden loppuminen. Pankkiasioiden hoidon keskeytyminen laitteen teknisten ominaisuuksien johdosta aiheuttaa voimakasta ärtymystä.

Turvallisuuden parantamiseksi tehdyt tekniset ratkaisut saavat usein osakseen vastustusta kuluttajien osalta, minkä on katsottu johtuvan ratkaisujen vaikutuksesta palvelun käytettävyyteen (Schultz ym. 2001). Tämä tuli hyvin esille myös tekemissäni haastatteluissa, joissa yleinen suhtautuminen ehdottamiini vaihtoehtoihin oli melko penseä ja epäilevä.

Ensimmäistä laitevaihtoehtoa kommentoitiin muun muassa seuraavasti:

> *No suhtautuisin tosi huonosti, koska sit mul pitäis aina olla se laite siinä ja sit se ois just aina vääräs paikassa tai sit se ois kiinteesti kotona ja sit tulis kotiin yks uus laite ja en hirveesti tykkää mistään laitteista. Et mun mielestä ku se verkkopankki toimii niin hyvin ja en oo ainakaan tietonen mistään kauheist tietoturvaongelmista ni en kyllä missään nimessä haluis sellasta. (H1)*

> *Miksei mut toisaalt se ois taas yks laite lisää täs maailmassa, ja eks siihenki joku voi päästä väliin? Et en kauheen innostunu oo. Et mun mielest verkkopankin suurimpii etuja on se et se on niin helppokäyttönen ja sä voit tehä sen missä vaan, ni sit et tulisko sitä kannettuu mukana ja olisko se mukana ku pitäis mennä sinne asioimaan. Tai sit jos siihen tulee joku vika ni hommaat sit pattereita tai muuta. (H7)*

Kommentit ovat samassa linjassa kuin Peura-Kapasen (2009) löydökset e-laskuja käsittelevässä tutkimuksessa. Hän huomasi, että totuttuja käytäntöjä ollaan haluttomia muuttamaan mikäli niihin ollaan tyytyväisiä (mt., 13-14). Kaikissa haastatteluissa verrattiin laitetta nykyiseen käytäntöön, johon ollaan totuttu ja joka koetaan hyväksi. Myös ylipäätään ajatus laitteesta oli monelle vastemielinen. Haastateltavien kommenteista paistaa läpi se, että laitteita on jo kotona tarpeeksi eikä niitä haluta lisää. Lisäksi he tuntuvat kokevan, että verkkopankin käytettävyys huonontuisi koska laitetta ei haluttaisi kantaa jatkuvasti mukana toisin kuin avainlukulistaa. Tätä kautta laite rajoittaisi verkkopankin käytön kotiin.

Toinen tarjoamani vaihtoehto eli laite, johon syötettäisi kortti ja kortin pin-koodi sai osakseen esimerkiksi seuraavanlaisia kommentteja:

> *No siin mieles epäilyttää et jos kortis ois jotain ongelmaa ni se käytännös estäis kaiken toiminnan. Et korttei kuitenki hukkuu ja menee*

> *rikki, et mä en siit niinku ihan kauheen mielissäni ois et kaikki ois sen yhen kortin varassa. (H5)*

> *En mä tiedä, mul on enemmän pointti se et sen pitää olla mahdollisimman nopeeta. Et mä oon sekunnis kattonu sen jos mä haluun tietää saldon tai muuta. Et ei sais hankaloitua. Ihan ok se kortti, mut mä käyn kuitenki nettipankis eri koneilla, et en mä nyt jaksais raahata sitä mukanani. Ja jos häviää kortti ni sit sä oot taas täysin ilman mitään. (H6)*

Kuten Weirin ym. (2009) tutkimuksessa, tämänkin tutkimuksen haastateltavat suhtautuivat varauksellisimmin tähän monimutkaisimpaan vaihtoehtoon. Suurinta huolta ei kuitenkaan aiheuttanut se, että laitetta olisi vaikea käyttää vaan päällimmäisenä oli ajatus siitä, että kortti voi kadota tai se voidaan varastaa, jolloin pankkiasioita ei pääsisi hoitamaan lainkaan. Ilmeisesti tämän tutkimuksen haastateltavat ovat erittäin tottuneita siihen, että verkkopankki on käytettävissä ympäri vuorokauden ja jokaisena viikonpäivänä. Pankkiasioiden hoito vaikuttaisi olevan hyvin arkipäiväinen toiminto, jonka täytyy onnistua ongelmitta. Konttorissa asioinnin mahdollisuutta ei edes mainita vaihtoehtona tilanteeseen, jossa kortti on kateissa vaan siinä vaiheessa oltaisiin ikään kuin tyhjän päällä.

Mainitsin haastatteluissa siis kaksi laitetta peräkkäin vaihtoehtoina nykyiselle avainlukulistan avulla kirjautumiselle. Osa haastateltavista vaikutti jopa turhautuvan tästä kun oli jo ensimmäisen laitteen osalta maininnut, ettei haluaisi mitään muutosta kirjautumiseen. Laitteen ominaisuuksilla ei juurikaan nähty olevan merkitystä, kun ajatusta ylimääräisestä laitteesta vieroksuttiin alun perinkin. Pankeilla saattaisi olla vaikeuksia perustella ylimääräistä laitetta näille vastaajille. Yleisestikin voisi kuvitella, että asiakkaat eivät olisi kovin halukkaita erillisten laitteiden käyttöönottoon. Etenkin kuluttajat, joilla on asiakkuus moneen pankkiin, voisivat olla harmissaan jos jokaisesta pankista saisi vielä erillisen laitteen kotiin. Tämän tutkimuksen haastateltavat käyttivät kuitenkin pääasiallisesti vain yhden pankin verkkopankkia. Jos asiakkuuksia olikin useampaan pankkiin, yksi niistä oli selvästi pääasiallinen pankki ja muissa asiakkuus oli melko passiivista. Tästä johtuen en

kysellyt heiltä enää mielipidettä tilanteeseen, jossa eri pankeista saisi vielä erilaiset laitteet.

Viimeiseen vaihtoehtoon eli kännykän käyttöön kirjautumisessa suhtauduttiin ristiriitaisesti:

> *No ehkä parantais turvallisuutta joo, mut mitäs sitte ku kännykkä oiski jossain muualla. Ei ois mukana tai virta pois tai akku loppu tai jotain. (H2)*

> *No kännykän toimintavarmuuden tuntien ni toi ois mun mielestä semmonen mihin suhtautuisin ainaki lievällä varauksella, ihan sen takia et sä oisit tavallaan siitä kännykästä riippuvainen käyttäessäs verkkopankkia, et mitä jos kännykkä häviää ja sun pitäis saada just samana tai seuraavana päivänä hoidettua jotain tärkeitä pankkiasioita. (H4)*

Osa tuntee epäilyä matkapuhelinta kohtaan. Akku voi olla lopussa tai kännykkä kadoksissa. Ylipäätään vaikuttaa, että haastateltavat eivät halua kirjautumiseen muutoksia. Avainlukulistaa pidetään hyvänä käytäntönä eikä mainitsemistani vaihtoehdoista koeta saatavan lisäarvoa palvelun käyttöön. Osa mainitsee kyllä, että turvallisuus parantuisi, mutta huonot puolet käytettävyyden heikentyessä tuntuisivat painavan vaakakupissa enemmän. Mielenkiintoista on mielestäni se, että moni mainitsee kortin ja kännykän katoamisen mahdollisuuden mutta kukaan ei tunnu ajattelevan, että yhtä lailla nykyään käytössä oleva avainlukulista voisi kadota. Samalla tavalla tällä hetkellä ollaan riippuvaisia avainluvuista kuin mitä oltaisiin kortista tai kännykästä jos niitä tarvittaisi kirjautumiseen. Osa haastateltavista kertoi kantavansa avainlukulistaa lompakossa, jossa varmasti myös kortti kulkee. Kortin katoamisesta ollaan kuitenkin enemmän huolissaan. Toisaalta nykytilanteessa avainlukulistan kadotessa asiakkaalla on edelleen käytössä maksukortti, jolla voi hoitaa maksuja kaupassa ja maksuautomaatilla sekä nostaa käteistä rahaa. Jos taas kortti katoaa, asiakkaalla on edelleen käytössään verkkopankki, jonka avulla pankkiasiat saa hoidettua. Jos korttia tarvittaisiin myös kirjautuessa verkkopankkiin, kortin kadotessa asiakkaan ainoa mahdollisuus maksuihin olisi käteinen raha ja

pankkiasiat olisi pakko hoitaa konttorissa. Tässä valossa on ymmärrettävää, että haastateltavat eivät halua kaiken asioinnin olevan yhden kortin varassa.

Haastattelemani asiantuntijat kertovat tällaisten erillisten laitteiden parantavan turvallisuutta joissakin tilanteissa. Tietoturva-asiantuntija kuitenkin muistuttaa, että mahdollisia malleja on lukuisia ja että yksikään niistä ei ole vielä osoittautunut sellaiseksi, jota ei voisi millään tavalla murtaa. Turvallisuuspäällikkö taas vertaa tarvetta ulkoiseen varmenteeseen osuvasti oman kotiovensa lukkoon. Hän kertoo jättäneensä ovensa myös lukitsematta, eikä kotoa ole silti viety mitään. Se ei silti tarkoita, että lukko on ovessa turhaan. Hän tekeekin retorisen kysymyksen, kannattaako ensin tehdä lukko vai antaako jonkun ensin murtautua sisään? Suomalaispankkien pohdittavana on siis kysymys kannattaako kirjautumisen turvallisuutta parantaa hyökkäysten ollessa täällä vielä harvinaisia vai tehdäkö ratkaisuja vasta siinä vaiheessa kun tietoturvaongelmat mahdollisesti lisääntyvät.

Tällä hetkellä pankkien voisi olla vaikea perustella laitteiden käyttöönottoa kuluttajille, jotka eivät välttämättä tiedä rikollisten toimista mitään. Nordea on vastikään ottanut käyttöön maksujen lisävahvistuspalvelun, joka toimii tekstiviestillä tai puhelinsoitolla. Lisävahvistus tarvitaan poikkeuksellisiin tilisiirtoihin kuten erityisen suurten summien siirtoon. (Nordea 2010b.) Nordea ei perustele toiminnon käyttöönottoa millään lailla. Olen itse Nordean asiakas ja toiminnosta on tullut minulle tieto ainoastaan verkkopankkiin kirjautumisen yhteydessä. Tässä on epäilemättä kyse rikollisen toiminnan estämisestä, mutta siitä ei mainita tiedotteessa mitään.

Tässä luvussa olen käynyt läpi keinoja, joita pankeilla on käytössään turvallisuuden parantamiseen. Seuraavaksi keskityn kuluttajiin ja heidän mahdollisuuksiinsa vaikuttaa verkkopankkiasioinnin turvallisuuteen omilla käytännöillään.

5.2 Ohjeistus turvalliseen verkkopankin käyttöön

Finanssialan keskusliitto on avannut pankkiturvallisuutta käsittelevän sivuston osoitteeseen www.pankkiturvallisuus.fi. Sivusto tarjoaa kattavaa tietoa

pankkiturvallisuudesta ja se on tarkoitettu sekä kuluttajien että ammattilaisten käyttöön. Kuluttajille suunnatussa osiossa tarjotaan tietoa verkkopankin turvallisuuden ohella myös korttimaksamisen ja verkkokaupoissa asioinnin turvallisuudesta sekä kerrotaan asiakkaan oikeuksista ja velvollisuuksista verkkoasioinnissa.

Sivustolla muistutetaan, että on kuluttajan velvollisuus pitää huolta oman kotikoneen tietoturvasta eli palomuurista ja ajantasaisesta virustorjunnasta. Virustorjuntaohjelmisto tulee myös päivittää säännöllisesti. Kuluttajille tarjotaan muitakin keinoja parantaa oman verkkopankkiasiointinsa turvallisuutta. Kuluttajia ohjeistetaan säilyttämään verkkopankkitunnusten osat huolellisesti ja erillään sekä välttämään verkkopankkiin kirjautumista linkkien kautta. Siinäkin tapauksessa että verkko-osoite on kirjoitettu sille tarkoitettuun osoitekenttään itse, se kehotetaan tarkistamaan ennen varsinaista kirjautumisvaihetta. Haittaohjelma voi nimittäin siitä huolimatta ohjata asiakkaan viime hetkellä väärennetylle sivustolle. Lisäksi muistutetaan aina suhtautumaan vakavasti varoituksiin, joita selainohjelma antaa varmenteen ja sivuston osoitteen yhteensopimattomuudesta. (FK 2010.) Viimeisessä ohjeessa tarkoitetaan mitä ilmeisimmin tilannetta, jossa rikollinen on naamioinut väärennetyn sivuston näyttämään siltä, että se toimii suojatun yhteyden kautta. Tällöin siis sivun alalaidassa voi näkyä ehjä lukko merkkinä suojatusta yhteydestä, mutta todellisuudessa sivusto ei ole rekisteröity pankin nimiin. Sivuston omistajasta voi varmistua ainoastaan tuplaklikkaamalla tätä ehjän lukon kuvaa, jolloin palveluntarjoajan nimi tulee esiin.

Opastusta turvalliseen verkkoasiointiin on tarjolla myös Kuluttajaviraston ja Viestintäviraston sivuilla. Kuluttajaviraston sivuilla on erillinen osio huijauksista. Sinne on koottu tietoa erilaisista internetissä tapahtuvista huijauksista avunpyyntöviesteistä ja verkkokauppahuijauksista phishing-viesteihin ja haittaohjelmiin. Sivuilla muistutetaan, että uhrin mahdollisuus saada menetettyjä varojaan takaisin on usein heikko. Tässä kuitenkin viitataan todennäköisesti sen kaltaisiin huijauksiin, jossa uhri on jonkin avunpyyntöviestin perusteella lähettänyt rahaa huijarille. Sivustolla opastetaan kuluttajia huijausten tunnistamiseen ja kerrotaan kuinka huijauksilta voi välttyä. Tärkeimpinä keinoina esitetään palomuurin ja virustorjunnan ajantasaisuuden ylläpito sekä terve järki asioinnissa. Epäilyttäviin

viesteihin ei ole syytä vastata eikä henkilö- tai muita arkaluontoisia tietoja luovuttaa. Kaikista huijausyrityksistä pyydetään raportoimaan Kuluttajaviraston vuonna 2007 käynnistämälle huijausten vastaiselle yhteistyöverkostolle, johon kuuluvat muun muassa Finanssialan Keskusliitto, Finanssivalvonta, Keskusrikospoliisi ja Luottokunta. (Kuluttajavirasto 2010.)

Viestintävirasto on koonnut kuluttajille tietoturvaoppaan, joka toimii osoitteessa www.tietoturvaopas.fi. Siellä kerrotaan hyvin kattavasti erilaisista huijauksista sekä opastetaan kuluttajaa varautumaan niihin. Kuten Kuluttajavirasto, myös Viestintävirasto käsittelee laajasti internetissä tapahtuvaa rikollista toimintaa, ei ainoastaan verkkopankkiin liittyviä turvallisuusuhkia. Tälläkin sivustolla painotetaan kuluttajan omaa vastuullisuutta verkkopalveluja käytettäessä. (Viestintävirasto 2010.)

Ohjeita turvalliseen asiointiin verkkopankissa löytyy myös pankkien verkkosivuilta. Nordea kehottaa asiakkaitaan muun muassa huolehtimaan palomuurista ja ajantasaisesta virustorjuntaohjelmistosta. Lisäksi muistutetaan pankkitunnusten säilyttämisestä huolellisesti ja varoitetaan henkilökohtaisten tietojen lähettämisestä sähköpostitse. Sivuilla kerrotaan myös phishing-viesteistä ja ohjeistetaan, ettei viesteihin saa missään nimessä vastata vaan ne tulee poistaa välittömästi. Asiakkaita kehotetaan lisäksi tarkistamaan tilitapahtumansa ja varmistamaan, että kaikki tapahtumat ovat asiakkaan itsensä tekemiä. Melko laajasta tietoturvaosiosta löytyy myös ohjeet suojatun yhteyden tarkistamiseen. (Nordea 2010c.)

Osuuspankin sivuilla kehotetaan muun muassa tyhjentämään tietokoneen välimuisti mikäli verkkopankkia käytetään yleiseltä koneelta ja ohjeistetaan miten tyhjennys tapahtuu. Asiakasta muistutetaan verkkopankkitunnusten henkilökohtaisuudesta ja siitä, että tunnusten eri osat on syytä säilyttää erillään. Lisäksi painotetaan, että pankki ei koskaan kysy asiakkaan verkkopankkitunnuksia sähköpostitse tai puhelimitse, eikä tunnuksia saa muutenkaan luovuttaa kenellekään muulle. Sivuilla kerrotaan myös suojatusta yhteydestä ja kuinka siitä voi varmistua. (OP 2010b.)

S-Pankki kertoo sivuillaan kuinka asiakas voi tarkistaa suojatun yhteyden. Lisäksi asiakasta pyydetään huolehtimaan kotikoneen virustorjunnasta sekä säilyttämään

pankkitunnusten eri osat erillään ja opettelemaan salasana ulkoa. Sivuilla varoitetaan myös sähköpostitse ja puhelimitse tapahtuvista phishing-yrityksistä. Asiakasta kehotetaan asioimaan mieluiten kotikoneella ja annetaan toimintaohjeita tilanteisiin, joissa verkkopankkia käytetään julkisella koneella. (S-Pankki 2010a.)

Kuluttajia siis opastetaan turvalliseen verkkopankissa asiointiin melko avoimesti vaikkakin mielestäni kohtalaisen lyhytsanaisesti. Lisäksi tietoa joutuu useimmiten etsimään – vain Nordean sivuilta linkki turvallisuusosioon on heti etusivulla. Aktian sivuilla turvallisuutta koskeva tieto on asetettu verkkopankin yleisen käyttöohjeen yhteyteen (Aktia 2010), jota harva tottunut verkkopankin käyttäjä tuskin koskaan edes avaa. Säästöpankin verkkosivujen turvallisuusosio sisältää ainoastaan kolme linkkiä – yksi on päivätty vuonna 2008 ja kaksi muuta vuonna 2007. Toinen vuonna 2007 lisätyistä tai päivitetyistä linkeistä johtaa sivulle, jossa kerrotaan verkkopankin turvallisuudesta (Säästöpankki 2010). Ilmeisesti sivustoa ei siis tosiaan ole päivitetty muutamaan vuoteen, vaikka viime vuosina on esiintynyt lukuisia phishing-viestihyökkäyksiä.

Haastatteluissa selvisi, että tutkittavat olivat hyvin tietämättömiä saatavilla olevasta ohjeistuksesta turvalliseen verkkoasiointiin. Kaikille oli kuitenkin selvää, että verkkopankkitunnusten eri osia säilytetään erikseen. Verkkopankkitunnusten kiinteät osat eli käyttäjätunnus ja salasana muistettiin lähes poikkeuksetta ulkoa eikä niitä oltu kirjoitettu ylös. Tähän vaikuttaa varmasti myös aiempi kokemus maksu- ja automaattikorttien käytöstä. Korttien käytössäkin on selvää, että pin-koodia ei kanneta mukana vaan se on opeteltu ulkoa.

Toisilla avainlukulista kulki aina mukana lompakossa, toiset säilyttivät listaa kotona. Verkkopankin käyttö rajoitettiin enimmäkseen kotiin ja työpaikalle, jossa oli henkilökohtaisessa käytössä oleva tietokone. Verkkopankkiasiointia julkisessa käytössä olevilta tietokoneilta vältettiin yleisesti ja jos sellaisia jouduttiin käyttämään pankkiasiointiin, välimuisti yleensä tyhjennettiin. Kaksi vastaajaa kertoi tosin käyttäneensä verkkopankkia opiskelupaikassaan tyhjentämättä välimuistia tai kirjautumatta erikseen ulos palvelusta.

Haastateltavat luettelevat omia käytäntöjään:

> *En kuljeta mukana niit tunnuksia, et en oikeestaan käytä julkisilt koneilta enkä yleensäkään vieraiden ihmisten läsnäollessa mee verkkopankkiin. Ja sit tyhjennän sivuhistorian jos oon käyttäny vaik työpaikalta. (H3)*

> *En kanna mukana sitä avainkorttia ja tyhjennän välimuistin jos käytän muualta ku kotoa. Käyttäjätunnusta ja salasanaa mul ei oo missään muualla ku mun päässä, et mä muistan ne. Ja kyl sit koitan vaik käytän muualta joskus ni ihan viimeseen asti välttää jotain koulun koneita ku ne on julkisii. (H5)*

Huolestuttava löydös oli se, että ainoastaan yksi haastateltava osasi tarkistaa suojatun yhteyden. Kyseinen henkilö oli sama, joka tiesi myös muita turvallisuusuhkia kuin phishing-viestit ja on siis harrastanut tietotekniikkaa jo vuosien ajan. Muutama muukin puhui haastattelun aikana suojatusta yhteydestä, mutta kysyessäni miten he varmistuvat siitä paljastui, että he eivät osanneet tarkistaa asiaa. Yksi heistä mainitsi avaimen kuvasta näytöllä, kun tosiasiassa suojatun yhteyden merkkejä ovat ehjä riippulukko ja verkko-osoitteen muoto https yleensä käytetyn http:n sijaan. Lisäksi täytyy muistaa, että pelkkä lukon kuva ei vielä kerro suojatusta yhteydestä, vaan lukkoa pitäisi myös klikata, jolloin näkee kenen nimiin sivusto on rekisteröity.

Lähes kaikilla vastaajilla oli kotikoneelle asennettuna palomuuri ja virustorjuntaohjelma. Yksi vastaaja kuitenkin myönsi, ettei muista päivittää ohjelmistoa kovinkaan usein. Kaksi vastaajaa kertoi, ettei omalla koneella ole virustorjuntaa koska heillä oli käytössään Applen Mac. Mac käyttää eri käyttöjärjestelmää kuin yleisimmin käytössä oleva Windows, johon suuri osa tietoturvaongelmista on kohdistunut. Myös haastattelemani turvallisuuspäällikkö kertoo, että tähän asti tietoturvaongelmilta on voinut välttyä siirtymällä toiseen käyttöjärjestelmään. Hän sanoo, että viime aikoina Microsoft on kuitenkin kehittänyt käyttöjärjestelmänsä tietoturvaa huomattavasti. Tämä taas on johtanut siihen, että

rikolliset eivät enää pyri murtamaan itse käyttöjärjestelmää vaan kohdistavat haittaohjelmat yleisesti käytettyihin sovelluksiin kuten Adobe- tai Acrobat Readeriin tai valtavan suosion saavuttaneeseen Facebookiin.

Haastattelemani asiantuntijat kertovat myös, että virustorjuntaohjelmien teho on ylipäätään heikentynyt koska virukset ovat nykyään polymorfisia eli jokainen yksittäinen virus on hieman erilainen. Turvallisuuspäällikkö kertoo virustorjunnan toimivan niin, että virustorjuntayhtiö saa kopion viruksesta ja koodaa ohjelmistonsa tunnistamaan tämän kyseisen viruksen. Tällä hetkellä jokaisen viruksen ollessa toisistaan hieman poikkeava, ei yhtiöillä ole mitään mahdollisuuksia saada haltuunsa kopiota kaikista yksittäisistä viruksista. Tietoturva-asiantuntija kertoo, että prosentuaaliset osuudet virustorjuntaohjelmien tunnistamista viruksista ovat jopa masentavaa katsottavaa. Hän mainitsee esimerkkinä yhden tarkastelemansa viruksen, jonka oli pystynyt edes jollain tasolla tunnistamaan kahdeksan 45:stä virustorjuntaohjelmistosta. Marraskuussa 2009 esiintynyt Zlob-troijalainen taas oli kaksi vuotta vanha haittaohjelma eivätkä virustorjuntaohjelmistot silti tunnistaneet sitä. Molemmat asiantuntijat kuitenkin painottavat, että virustorjunnasta on edelleen tärkeä huolehtia koska ohjelmat tunnistavat kuitenkin osan esiintyvistä viruksista.

Kuluttajan on siis entistä vaikeampaa huolehtia oman koneensa tietoturvasta. Näin ollen on entistä tärkeämpää kiinnittää huomiota omaan käyttäytymiseen verkossa. Haastattelemani asiantuntijat toivoisivat kuluttajien olevan erityisen tarkkana erilaisten linkkien ja tiedostojen lataamisen kanssa. Linkit voivat johtaa väärennetyille sivustoille ja ladattavat tiedostot voivat sisältää viruksia ja haittaohjelmia.

Tämän tutkimuksen haastateltavat tuntuivat olevan kaiken kaikkiaan huolellisia asioidessaan verkkopankissa ja internetissä yleensä, vaikka vain kaksi vastaajaa kertoi saaneensa ohjeita pankista. Pankista saatu ohje oli lisäksi ainoastaan se, että verkkopankkitunnusten osat on säilytettävä huolellisesti ja erillään toisistaan. Toisaalta on hyvinkin mahdollista myös se, että haastateltavat ovat unohtaneet pankista kenties annetut ohjeet. Kaikki tutkittavat ovat siis käyttäneet verkkopankkia vähintään kuuden vuoden ajan. Tuolloin Suomessa ei vielä ollut esiintynyt kalasteluviestejä puhumattakaan edistyneemmistä phishingin muodoista. Tässä

valossa on myös ymmärrettävää, ettei pankista välttämättä ole saatukaan muuta ohjeistusta.

Haastateltavat kertovat:

> *Silloin ku sai sen verkkopankin ni on lukenu ne tarkkaan ku oli sillee et mikäs juttu tää on? Ja se oli sellanen uus asia et silloin luki tarkkaan ne ohjeet. Mut en mä sen jälkeen oo mitään lukenu et sit vaan on sillee et jaaha, mennääs kattoo miten tää toimii. (H1)*

> *Verkkopankkitunnuksistaki on tullu niin jokapäiväst touhuu ku niit on käytetty monii vuosii, et huomaa et liian helpolla on vaan jatkanu sitä samaa eikä oo miettiny näit juttuja. Eikä oo pankiltakaan tullu sellast lähentymistä, et tavallaan maailma ympärillä on kuitenki koko ajan eläny ja kasvanu ja vois kuvitella et huijausten mahdollisuus on aika paljon isompi ku 2000-luvun alussa. (H7)*

Ensimmäisestä kommentista ilmenee, että uuteen palveluun on paneuduttu aluksi huolellisesti. Käytön jatkuessa vastaajasta on kuitenkin tullut luottavaisempi eikä hän enää mieti ohjeistusta. Toisen kommentin esittänyt vastaaja alkoi haastattelun kuluessa selvästi miettiä turvallisuusasioita ja huomasi, ettei ole aiemmin pohtinut asiaa lainkaan. Hän huomaa omien käytäntöjensä pysyneen samoina ja tiedostaa samalla ympäröivän maailman muuttuneen. Hän vaikuttaa hieman pettyneeltä siitä, ettei pankkikaan ole muistuttanut tästä muutoksesta. Pankkien olisikin ehkä hyvä tiedottaa asiakkaitaan turvallisuusasioista nyt, kun erilaisia hyökkäyksiä on alkanut esiintyä. Monet muutkin tottuneet verkkopankin käyttäjät saattavat luottaa omaan kokemukseensa palvelun käytöstä eivätkä osaa ajatella, että ajat ovat muuttuneet siitä, kun palvelu on otettu käyttöön.

5.3 Vastuunjako taloudellisista menetyksistä

Luvussa neljä esittelin erilaisia verkkopankin käyttöön kohdistuvia turvallisuusuhkia ja niistä tiedottamista. Aiemmin tässä luvussa olen kertonut pankkien keinoista

parantaa verkkopankin turvallisuutta ja toisaalta kuluttajien ohjeistamisesta turvalliseen verkkoasiointiin. Tämän osion tarkoituksena on selvittää pankin ja asiakkaan välistä vastuunjakoa tilanteissa, joissa asiakas menettää varojaan huijauksen seurauksena. Aineistosta kävi ilmi, että pankin tiedotuksen ja ohjeistuksen tasolla on selkeä vaikutus haastateltavien näkemyksiin korvausvastuullisesta osapuolesta.

Verkkopankin yleisissä palveluehdoissa kerrotaan asiakkaan vastuusta. Niiden mukaan asiakkaan tulee säilyttää pankkitunnusten eri osat huolellisesti ja erillään toisistaan. Niitä ei saa luovuttaa ulkopuolisten tietoon ja jos asiakas epäilee tunnusten olevan jonkin ulkopuolisen tahon tiedossa, siitä on ilmoitettava välittömästi ympäri vuorokauden palvelevaan tunnusten sulkupalveluun. Asiakas vastaa tunnusten oikeudettomasta käytöstä siihen asti, kunnes pankki on vastaanottanut pyynnön tunnusten sulkemisesta. Lisäksi ehdoissa kerrotaan, että asiakas vastaa verkkopankkitunnusten väärinkäytöstä vain siinä tapauksessa, että pankkitunnusten joutuminen vääriin käsiin johtuu asiakkaan muusta kuin lievästä huolimattomuudesta. (Nordea 2010d.) Käytännössä suomalaispankit ovat korvanneet asiakkailleen phishing-hyökkäyksistä koituneet varojen menetykset. Palveluehdot eivät kuitenkaan takaa vahinkojen korvaamista kaikissa tapauksissa. Korvauspäätöksessä huomioidaan asiakkaan huolellisuus tai huolimattomuus tunnusten säilyttämisen osalta. Tavoista saattaa verkkopankkitunnukset ulkopuolisten tietoon ei kuitenkaan mainita erikseen. Tunnusten eri osien säilyttäminen lompakossa on epäilemättä huolimatonta. Entä onko huolimatonta vastata kalasteluviesteihin ja sisältyykö huolellisuuteen kotitietokoneen tietoturvan ylläpito?

Laforet & Li (2005) mainitsevat yhdeksi verkkopankin hyödyksi takuun siitä, että asiakkaan varat ovat turvassa. Tämä ei kuitenkaan toteudu mikäli rikolliset onnistuvat huijaamaan asiakasta. Molemmat haastattelemani asiantuntijat ovat sitä mieltä, ettei pankkeja voi asettaa korvausvastuuseen mikäli asiakkaat menettävät varojaan rikollisen toiminnan seurauksena. Poikkeuksena he mainitsevat tilanteen, jossa pankki itse on selkeästi laiminlyönyt tietoturvan rakentamisen verkkopankkiympäristöön. Laiminlyönniksi he katsovat esimerkiksi sen, että verkkopankkiin kirjautumiseen tarvitaan ainoastaan kiinteä käyttäjätunnus ja salasana.

Teleyrityksen turvallisuuspäällikön mielestä asiakkaan vakuutusyhtiö voisi olla taho, joka korvaisi taloudelliset tappiot. Hän perustelee mielipidettään sillä, että onnistunut huijaus ei ole pankin syy. Kuluttajaakaan ei oikeastaan voi syyttää, koska häneltä ei voi odottaa laajaa tietoteknistä osaamista. Mielipide kuvastaa mielestäni hyvin tämän hetkistä tilannetta, jossa vastuunjaon määritelmä on epäselvä. Jos pankki ei ole tiedottanut asiakkaitaan mahdollisista verkkopankin käyttöön liittyvistä uhista, kuluttajalla ei myöskään ole mahdollisuutta varautua niihin. Toisaalta voiko pankkia syyttää siitä, että kuluttaja käyttäytyy huolimattomasti verkossa? Omalla käyttäytymisellä voi kuitenkin vaikuttaa asioinnin turvallisuuteen.

Myös haastattelemani verkkopankin käyttäjät näkevät käytöksellään olevan vaikutusta korvausvastuullisen osapuolen määrittelyyn. Omasta huolimattomuudesta johtuvat varojen menetykset ovat heidän mielestään asiakkaan itsensä vastuulla. Heistä suurin osa katsoo kuitenkin huolimattomuuden liittyvän vain verkkopankkitunnusten säilyttämiseen. Oman tietokoneen turvallisuuden ylläpitämisestä ei puhuta. Haastateltavien vastauksista huomaa sen, että perinteiset phishing-viestit ovat heille tuttuja. Kaikki kalasteluviesteistä kuulleet olivat sitä mieltä, että jos asiakas luovuttaa verkkopankkitunnuksensa sähköpostitse, ei pankkia voi asettaa korvausvastuuseen menetetyistä varoista.

Pankki olisi seuraavan vastaajan mielestä kuitenkin vastuussa mikäli asiakas on säilyttänyt tunnuksensa huolellisesti:

> *No jos mä oon niin tyhmä et mä meen antamaan tunnukseni jolleki sähköpostilla, ni kyl se on mun mielestä sit mun omaa tyhmyyttä. Mut jos joku kaappaa mun koneen, tavallaan sillä tavalla pääsee heidän palomuurin läpi ni silloin se on mun mielestä pankin vastuulla. Et kaikki muut tilanteet paitsi omasta tyhmyydestä johtuvat ois pankin vastuulla. (H2)*

Yllä esitetyssä kommentissa vastaaja sekoittaa oman tietokoneensa turvallisuuden pankin järjestelmän turvallisuuteen. Hänen mielestään pankin järjestelmään on murtauduttu mikäli hänen verkkopankki-istuntonsa kaapataan. Todellisuudessa

istunnon kaappaamisessa on kyse asiakkaan oman tietokoneen tietoturvaongelmista. Tällöin siihen on onnistuttu asentamaan jokin haittaohjelma, jonka kautta rikollinen pääsee vakoilemaan uhrin internet-liikennettä. Haastateltavan mielestä on siis asiakkaan vastuulla tunnistaa kalasteluviestit ja olla vastaamatta niihin. Asiakkaan oman koneen tietoturvan ylläpito ei hänen mielestään kuitenkaan ole vastuunjakoa määrittelevä tekijä.

Seuraavien vastaajien kommenteista ilmenee myös pankin ja asiakkaan välisen turvallisuussuhteen muutos. Ensimmäisen mielestä muutosta ei tosin saisi tapahtua. Koska pankki on aiemminkin kantanut vastuun asiakkaiden varoista, täytyy sen toimia niin myös verkkopalvelujen osalta. Toinen vastaaja taas näkee pankin tiedotuksen edellytyksenä sille, että vastuunjako voisi muuttua.

Haastateltavat pohtivat:

> *Kyl ku vastuu kasvaa ni se kasvaa nimenomaan pankeilla, et ei se voi siirtää asiakkaille sitä vastuuta minkä ne aikasemmin on kantanu ku asiat on hoidettu konttorissa. (H3)*

> *Et se vois pankilleki tuoda tiettyy turvaa et ne on käyny käsiks tähän asiaan ja on tiedottanu kaikkia asiakkaita. Jos asiakas ei oo sit sitä lukenu ni sit se pallo on tavallaan myös enemmän sil asiakkaalla. (H7)*

Weirin ym. (2009) mukaan asiakkaat kokevat turvallisuuden ylläpidon laajalti pankin tehtäväksi. Kuten aiemmin tässä luvussa olen kertonut, pankki ei kuitenkaan voi mitenkään vaikuttaa phishing-viestien esiintymiseen tai asiakkaidensa kotikoneiden tietoturvaan. Internet on maailmanlaajuisen kommunikoinnin helpottamiseksi kehitetty toiminta-alusta, jossa ketään yksittäistä toimijaa ei voida asettaa vastuuseen turvallisuuden ylläpidosta tai menetetyistä varoista (Hutchinson & Warren 2003). On siis tärkeää, että jokainen internetin käyttäjä kantaa oman vastuunsa toimiessaan tällä alustalla. Pankki on verkkopalvelun tarjoaja ja asiakas sen käyttäjä. Pankin vastuulla on väistämättä luoda palvelusta turvallinen, mutta voiko pankkia pitää vastuussa kaikkien asiakkaidensa verkkokäyttäytymisestä?

Haastattelemani turvallisuusasiantuntijat muistuttavat, että moni internetin käyttäjä on verkossa äärimmäisen huolimaton. Epämääräisiin linkkeihin ei aina osata suhtautua varauksella ja samaa, pahimmillaan suojaamatonta kotikonetta saattavat käyttää kaikki perheenjäsenet kukin omiin tarkoituksiinsa. Tietoturva-asiantuntija toivoisikin, että kuluttajat pohtisivat enemmän omaa käyttäytymistään internetissä ja tiedostaisivat paremmin siellä vaanivat uhat.

Yksi haastattelemistani verkkopankin käyttäjistä on vaastuunjaossa samoilla linjoilla kuin haastattelemani asiantuntijat. Hänen mielestään käyttäjän on itse kannettava vastuu omasta toiminnastaan verkossa. Myös hän väläyttää ajatuksen vakuutusyhtiöiden mahdollisuudesta laajentaa vakuutuksiaan verkkopankkirikoksiin.

Hän vertaa väärennettyjä verkkopankkisivustoja piraattivaatteisiin:

> *Et kyl se menee omaan piikkiin jos sulla ei oo ollu koneen suojaus tarpeeks korkeella tai tietotaito ei oo riittäny tunnistamaan ton tyyppistä uhkaa. Et se on vähän sama ku joku myis mulle piraattivaatteet, ni en mä voi mennä sitä alkuperästä valmistajaa syyttää et miksette opettanu mua erottaa väärää oikeesta. (H4)*

Kyseisellä vastaajalla oli haastateltavien joukosta eniten kokemusta tietokoneen käytöstä. Vaikka kaikki olivat käyttäneet tietokonetta jo lapsuudesta asti, tämä henkilö mainitsi tietotekniikan harrastuksekseen. Näin ollen on ymmärrettävää, että koska hän itse kokee tunnistavansa verkkopankin käyttöön kohdistuvat uhat, hän olettaa myös muiden pystyvän samaan tai ei ainakaan koe vääräksi mahdollisuutta, että pankki olettaisi niin. Nykyään pankit ajavat kuitenkin asiakkaitaan yhä vahvemmin käyttämään itsepalvelukanavia. Verkkopankki on usein maksuton tai hyvin edullinen palvelukanava kun taas konttorissa asioinnista peritään erilaisia palvelumaksuja. Yllä mainittu vertauskuva on mitä ilmeisimmin tarkoituksellisesti kärjistetty, mutta mielestäni kuitenkin melko raadollinen. Onhan täysin eri asia ostaa erehdyksessä aitoihin kappaleisiin nähden hyvin edullinen kopio merkkivaatteesta kuin tulla huijatuksi niin, että tili on eräänä päivänä tyhjennetty. Piraattivaatteen voi myös tunnistaa epäilyttävän edullisesta hinnasta, kun taas edistyneempiä phishing-hyökkäyksiä on hyvin vaikea havaita. Haastattelun edetessä tämäkin vastaaja oli

tosin sitä mieltä, että etenkin tottumattomia tietokoneen käyttäjiä tulisi huolellisesti opastaa turvalliseen verkkopankin käyttöön.

Ylipäätään vastaajat näkivät vastuunjaon melko hankalana asiana. Kaikki olivat yhtä mieltä siitä, että asiakas on itse vastuussa varojensa menetyksestä mikäli verkkopankkitunnuksia on säilytetty huolimattomasti. Muissa huijaustapauksissa mielipiteet vastuussa olevasta osapuolesta vaihtelivat. Mielestäni vastauksista näkyy selkeästi tiedotuksen rooli. Phishing-viestejä on esiintynyt pitkään ja niistä on tiedotettu. Haastateltavien mielestä viesteihin vastaamisesta johtuneita menetyksiä ei voi vaatia pankeilta koska heille on itsestään selvää se, ettei näihin viesteihin vastata. Viestit olivat myös ainoa tietoturvaongelma, jonka vastaajat osasivat varmasti mainita yhtä haastateltavaa lukuun ottamatta. Ainoa haastateltava, joka tiesi muistakin turvallisuusuhista oli myös ainoa, jonka mielestä pankkia ei voi syyttää asiakkaiden varojen menetyksestä muissakaan huijaustapauksissa mikäli pankki on huolehtinut oman järjestelmänsä turvallisuudesta. Suurempi tietoisuus turvallisuusuhista näyttää siis tämän aineiston osalta kasvattavan asiakkaan vastuuta ja vastaavasti pienentävän pankin vastuuta. Tässä valossa vaikuttaa siltä, että pankkien kannattaisi tiedottaa avoimesti muistakin phishingin muodoista kuin sähköpostiviesteistä. Haastateltavat kokisivat sen vastuullisena toimintana ja kommenteista saa kuvan, että myös luottamus pankkiin kasvaisi avoimen tiedottamisen myötä.

6 Johtopäätökset

Tämän tutkimuksen tarkoituksena oli tarkastella haastateltavien kokemuksia ja käsityksiä verkkopankkipalvelujen turvallisuudesta sekä sitä, onko heille muotoutunut omia keinoja parantaa verkkopankissa asioinnin turvallisuutta. Lisäksi halusin kartoittaa heidän näkemyksiään pankin ja asiakkaan välisestä vastuunjaosta tapauksissa, joissa asiakas menettää varojaan rikollisen toiminnan seurauksena.

Väitän, että pankkien ja heidän asiakkaidensa välinen turvallisuussuhde on muuttunut verkkopankkiasioinnin osalta. Perustelen väitettä kolmesta eri näkökulmasta. Ensinnäkin pankit kohtaavat verkkopankissa turvallisuusriskejä ja kuluttajat turvallisuusuhkia. Toiseksi pankkien ja kuluttajien keinot verkkopankin ja siellä asioinnin turvallisuuden parantamiseksi ovat eriytyneet. Kolmanneksi pankin ja sen asiakkaiden välinen taloudellinen vastuunjako on tällä hetkellä epäselvä.

Haastattelemieni asiantuntijoiden mukaan suomalaispankit ovat kehittäneet omat järjestelmänsä turvallisuuden kannalta kestäviksi. Rikollisten hyökkäysten kohteina ovatkin tässä uudessa tilanteessa yksittäiset pankkien asiakkaat. Ristiriita piilee siinä, että pankit ovat tietoisia verkkopankin käyttöön kohdistuvista turvallisuusriskeistä, mutta kuluttajat eivät välttämättä ole. Eräsaaren (1997, 78) mukaan uhasta tulee riski siinä vaiheessa, kun se opitaan tuntemaan. Pankit kohtaavat siis turvallisuusriskejä ja kuluttajat turvallisuusuhkia. Pankit voisivat tiedotusta lisäämällä kasvattaa asiakkaidensa tietoisuutta turvallisuusuhista ja pyrkiä näin muuntamaan uhat hallitummiksi turvallisuusriskeiksi. Näin kuluttajat pystyisivät varautumaan niihin paremmin. Kalasteluviestien osalta tämä on mielestäni jo toteutunutkin, mutta muiden phishingin muotojen osalta tästä tilanteesta ollaan vielä kaukana.

Tietokoneen käyttäjät ovat yleisesti suhteellisen tietämättömiä käyttämiensä järjestelmien turvallisuustasosta (Wang ym. 2003). Myös tämän tutkimuksen haastateltavat olivat melko tietämättömiä verkkopankin käyttöön liittyvistä turvallisuusuhista. Edistyneemmistä phishingin muodoista tiesi varmuudella vain yksi vastaaja. Hän osasi luetella käytännössä kaikki luvussa 4.1 esittelemäni phishing-hyökkäysten lajit. Kyseinen vastaaja mainitsi tietotekniikan harrastuksekseen ja kertoi seuraavansa alan kirjoituksia mediassa. Hänen laaja tietämyksensä selittyy täten omalla mielenkiinnolla aiheeseen.

Yhtä haastateltavaa lukuun ottamatta kaikki osasivat kuitenkin mainita phishing-viestit. Niiden ei koettu aiheuttavan todellista uhkaa itselle koska kaikki viesteistä kuulleet osasivat myös kertoa, ettei niihin tule missään nimessä vastata. Osa tutkittavista oli myös saanut tällaisia huijausviestejä, mutta ne oli poistettu välittömästi. Kalasteluviestejä on esiintynyt Suomessa jo monen vuoden ajan ja niistä on ollut laajaa uutisointia mediassa. Myös pankit ovat kertoneet verkkosivuillaan avoimesti tällaisten viestien esiintymisestä. Tiedotus on siis tavoittanut lähes kaikki tähän tutkimukseen osallistuneet henkilöt ja johtanut siihen, että viesteihin osataan reagoida oikein eli ne poistetaan heti – uhasta on tullut riski.

Kuluttajat pitävät turvallisuuden ylläpitoa laajalti pankkien tehtävänä (Weir ym. 2009). Monet pankkien mahdolliset toimet turvallisuuden parantamiseksi vaativat kuitenkin myös kuluttajien osallistamista (Sarel & Marmorstein 2006). Yksi tällainen pankin asiakkaat osallistava keino olisi lisätä verkkopankin kirjautumisvaiheeseen erillinen laite, joka antaisi lopulliseen kirjautumiseen vaadittavan salasanan. Kysyin haastateltavilta heidän mielipiteitään kolmeen eri vaihtoehtoon: kahteen erilaiseen ulkoiseen laitteeseen sekä matkapuhelimen käyttöön tunnistautumisvaiheessa. Kaikkiin vaihtoehtoihin suhtauduttiin epäilevästi. Haastateltavat pitävät verkkopankkia turvallisena ja ovat tyytyväisiä nykyiseen käytäntöön, jossa kertakäyttöinen salasana saadaan helposti mukana kulkevasta avainlukulistasta.

Nordea otti helmikuussa 2010 käyttöön maksujen lisävahvistuspalvelun. Poikkeuksellisiin verkkopankin kautta suoritettaviin tilisiirtoihin vaaditaan siis asiakkaan vahvistus puhelinsoitolla tai tekstiviestillä. Poikkeukselliseksi maksun voi

tehdä erityisen suuri siirrettävä summa tai siirron kohdistuminen vieraalle tilille. (Nordea 2010b.) Nordea ei ole erikseen tiedottanut asiakkailleen syytä palvelun käyttöönottoon, vaikka kyse on mitä ilmeisimmin turvallisuuden parantamisesta. Tämän uudistuksen yhteydessä olisi ollut oivallinen mahdollisuus tiedottaa asiakkaita edistyneistä phishingin muodoista. Olisi mielenkiintoista tietää, miten asiakkaat ovat suhtautuneet kyseisen palvelun käyttöönottoon. Osa asiakkaista on kenties soittanut kiukkuisena asiakaspalveluun, osa taas on mahdollisesti tiedustellut uudistuksen syistä ja ollut sitten tyytyväinen kehitykseen.

Pankkien ja heidän asiakkaidensa keinot parantaa verkkopankkipalvelun turvallisuutta ovat siis suurelta osin eriytyneet. Rikollisten hyökkäysten onnistumiseen vaikuttaa tällä hetkellä eniten kuluttajien oma käyttäytyminen pankkien järjestelmien ollessa ajan tasalla. Lagerspetz (1997) erottaa kolme mahdollista menetelmää epävarmuuden hallitsemiseen yksilötasolla:

1) Ennakointi ja uuden tiedon hankinta
2) Yksityinen varautuminen riskeihin
3) Riskien välttäminen teknologiaa ja rutiineja parantamalla (mt., 98.)

Kuluttaja voi siis parantaa verkkopankkiasioinnin turvallisuutta etsimällä itsenäisesti tietoa turvallisuusuhista, jotka siis tietämyksen tason lisääntyessä muuttuvat kontrolloitaviksi riskeiksi. Näihin riskeihin on mahdollista varautua esimerkiksi oman kotitietokoneen tietoturvaa parantamalla, tarkistamalla aina verkkopankissa käytettävä suojattu yhteys ja välttämällä linkkejä ja tuntemattomien tiedostojen lataamista internetistä. Erilaisten tiedostojen lataamisessa ja linkkien seuraamisessa on riski saada omalle tietokoneelle haittaohjelmia tai joutua ohjatuksi väärennetyille sivustoille. Suomessa edistyneitä phishing-hyökkäyksiä ei ole juurikaan esiintynyt, mutta tähän turvallisuudentunteeseen ei voida tuudittautua lopullisesti. F-Securen tutkimusjohtaja Mikko Hyppönen arvioi Kauppalehden haastattelussa, että mikäli rikolliset olisivat tietoisia siitä, että esimerkiksi Nordean verkkopankkia käytetään useissa maissa, hyökkäykset Nordean asiakkaita kohtaan lisääntyisivät varmasti (Kauppalehti 19.11.2009).

Tämän tutkimuksen haastateltavat vaikuttivat olevan melko huolellisia asioidessaan verkkopankissa. Tunnuksia säilytettiin erillään ja salasana muistettiin yleensä ulkoa. Verkkopankkia käytettiin mieluiten kotoa tai työpaikalta ja pankkiasioiden hoitoa julkisessa käytössä olevilta tietokoneilta vältettiin. Lähes kaikilla vastaajilla oli kotikoneella myös virustorjunta ja palomuuri. Huolestuttavaa oli kuitenkin se, että vain yksi vastaaja osasi tarkistaa suojatun yhteyden. Lisäksi vain kaksi vastaajaa kertoi saaneensa ohjeistusta pankista ja ainoa sieltä saatu ohje oli tunnusten säilyttäminen erillään.

Kaikki haastattelemani henkilöt ovat käyttäneet verkkopankkia vähintään kuusi vuotta. Kalasteluviestejä tai muita phishing-hyökkäyksiä ei vielä tuolloin ollut esiintynyt Suomessa. Pankeilla ei ole täten ollut tarvetta kertoa asiakkailleen phishing-hyökkäyksistä tai niihin varautumisesta. Tällä hetkellä tilanne on kuitenkin toinen. Pankkien olisikin hyvä lähestyä asiakkaitaan turvallisuusaiheen tiimoilta nyt, kun phishing-viestit ovat yleistyneet ja myös edistyneempiä hyökkäyksiä on esiintynyt. Sekä haastattelemani asiantuntijat että verkkopankin käyttäjät kokivat tiedottamisen olevan nimenomaan pankkien tehtävä phishing-hyökkäysten kohdistuessa heidän tarjoamiinsa palveluihin.

Pelkän median uutisointi ei myöskään välttämättä tavoita kaikkia verkkopankin käyttäjiä. Tämän tutkimuksen haastateltavista kukaan ei ollut kiinnittänyt huomiota marraskuun 2009 uutisiin, joissa kerrottiin verkkopankin asiakkaita uhkaavista Belbloh- ja Zlob-haittaohjelmista. Näistä troijalaisista tiedottivat siis media ja teleyritykset, mutta eivät pankit. Haastateltavien mielestä pankeille sopivin tiedotuskanava olisi verkkopankin sisäinen viestijärjestelmä. Sinne tulevat viestit huomataan ja myös luetaan helpommin kuin perinteiset kirjeet, joita ei välttämättä edes avata. Pankkien toimesta tapahtuva aktiivinen tiedottaminen olisi tärkeää myös siksi, että haastateltavat olivat haluttomia itsenäiseen tiedonhankintaan.

Pankin ja asiakkaan välinen vastuunjako on mielestäni tällä hetkellä epäselvä. Verkkopankkipalvelujen yleisissä ehdoissa puhutaan kuluttajan vastuusta, johon sisältyy tunnusten huolellinen säilyttäminen ja kielto tunnusten luovuttamisesta ulkopuolisten käsiin. Kuluttajan vastuulla on myös verkkopankkitunnusten sulkeminen mikäli tunnukset ovat kateissa tai on syytä epäillä niiden joutuneen

vääriin käsiin. (Nordea 2010d.) Ehdoissa ei kuitenkaan eritellä sitä, millä tavoin tunnukset voivat päätyä ulkopuolisille. Se, sisältyykö huolellisuuteen myös esimerkiksi taito tunnistaa phishing-viestit ja olla vastaamatta niihin, jää hämärän peittoon.

Haastattelemani turvallisuusasiantuntijat olivat sitä mieltä, ettei pankkia voi asettaa vastuuseen onnistuneista phishing-hyökkäyksistä mikäli pankin omat järjestelmät ovat ajan tasalla ja turvallisuuteen on panostettu. Suomalaispankit ovat heidän mielestään hoitaneet oman osansa hyvin. Kuluttajahaastatteluissa oma tietoisuus turvallisuusuhista näyttäytyi selvästi kuluttajan vastuuta kasvattavana tekijänä. Henkilö, jolla oli laajin tietämys phishingin muodoista, oli ainoana vastaajana samoilla linjoilla turvallisuusasiantuntijoiden kanssa. Myöskään hänen mielestään pankin ei tarvitsisi korvata asiakkailleen taloudellisia menetyksiä mikäli syy ei ole pankin.

Toinen ääripää oli haastateltava, joka ei ollut tietoinen mistään phishingin muodoista. Hänen mielestään pankin tulisi korvata kaikki phishingistä johtuvat taloudelliset menetykset. Loput haastateltavat kokivat korvausvastuun olevan pankilla vain edistyneempien phishing-hyökkäysten osalta. Kuluttajan omalle vastuulle jäisivät phishing-viesteihin vastaamisesta aiheutuneet menetykset. Kaikki haastateltavat esittivät yhtenäisen näkemyksen siitä, että kuluttaja on itse vastuullinen osapuoli tapauksissa, joissa hän on säilyttänyt verkkopankkitunnusten eri osia lompakossa, joka on sitten kadonnut tai varastettu.

Kuluttajan vastuuta näyttäisi tämän aineiston perusteella kasvattavan myös pankkien korkeampi tiedotuksen taso. Vastaaja, joka ei ollut kuullut mistään verkkopankin käyttöön liittyvistä turvallisuusuhista sanoi olevansa myös tyytyväinen: *Siin mielessä on hyväki ettei pankki oo tiedottanu noista koska oletan et pankki ottaa sit myös vastuun aika pitkälle. (H8)* Vastuun jakautuminen määräytyy siis pitkälti pankin tiedotuksen tasosta. Yleisesti katsottiin, että jos pankki tiedottaa asiakkaitaan avoimesti turvallisuusuhista ja antaa ohjeita turvalliseen verkkopankissa asiointiin, se voi odottaa asiakkailtaan huolellisempaa käyttäytymistä. Tiedotuksen lisääminen oli kuitenkin myös edellytys sille, että asiakkaan vastuuta voi kasvattaa.

Uusi EU-direktiiviin perustuva Maksupalvelulaki astui Suomessa voimaan 1.5.2010. Sen myötä pankkien tarjoamien verkkopankkipalvelujen ehdot muuttuvat joiltakin osin. Pankkien velvollisuus maksupalveluista tiedottamisesta lisääntyy. Toisaalta myös kuluttajan velvollisuus säilyttää verkkopankkitunnuksiaan huolellisesti kasvaa. Huolellisen kuluttajan vastuu lakkaa hetkellä, jolla pankki saa tiedon tunnusten sulkemisesta. Huolimaton kuluttaja voi kuitenkin joutua itse vastuuseen tunnusten mahdollisesta väärinkäytöstä. (S-Pankki 2010b.) Kuten vanhoissa ehdoissa, tässäkään ei erotella tekijöitä, joilla kuluttajan huolellisuus määritellään. Mahdolliset korvauskysymykset taloudellisista menetyksistä käsitellään mitä ilmeisimmin tapauskohtaisesti.

On mielenkiintoista nähdä lisääntyykö pankkien tiedotus uuden Maksupalvelulain myötä. Tiedottavatko pankit jatkossa turvallisuusasioista paremmin vain uusia sopimuksia tehdessä vai aktivoidaanko vanhojakin asiakkaita tutustumaan uusiin palveluehtoihin? Entä jääkö tiedotus muuttuneista ehdoista kertomiseen vai tiedotetaanko asiakkaita yleisesti turvallisuusteeman ympäriltä? Pankeilla olisi hyvä mahdollisuus aloittaa laajempi ”turvallisuuskampanja” tämän uudistuksen yhteydessä, kun jonkin tasoista tiedotusta vaaditaan joka tapauksessa.

Itse koen pankkien olevan tällä hetkellä pitkälti vastuussa verkkorikollisuudesta aiheutuneista taloudellisista menetyksistä. Olen samaa mieltä haastateltavien kanssa siitä, että kuluttajan vastuun kasvattaminen edellyttäisi aktiivista ja laajamittaista tiedottamista turvallisuusasioista. Kuten olen aiemmin maininnut, tuntemattomaan uhkaan on mahdoton varautua. Aika näyttää, ovatko suomalaispankit valmiita tiedotuksen lisäämiseen vai jäävätkö ne odottelemaan mahdollisesti lisääntyviä phishing-hyökkäyksiä. Tähän mennessä asiakkaille aiheutuneet vahingot on korvattu ja korvaamista todennäköisesti jatketaan ainakin siihen asti, että voidaan olettaa kaikkien olevan tietoisia verkossa asiointiin liittyvistä turvallisuusuhista.

Suomessa verkkopankin turvallisuutta ei ole juurikaan tutkittu johtuen todennäköisesti verkkopankin suuresta suosiosta ja siitä, että olemme suurilta osin välttyneet etenkin edistyneemmiltä phishing-hyökkäyksiltä. Ylipäätään tutkimuksia on tehty hyvin vähän kuluttajien näkökulmasta. Jatkossa olisikin mielenkiintoista lukea laajemman populaation käsityksistä palvelun turvallisuudesta ja

korvausvastuullisesta osapuolesta tapauksissa, joissa kuluttajat menettävät varojaan. Myös uusi Maksupalvelulaki tuo tullessaan jatkotutkimusaiheita. Sen avulla pyritään yhtenäistämään eurooppalaisia maksukäytäntöjä, joten tutkimusta sen vaikutuksista voisi tehdä useampaan maahan ulottuvalla otoksella.

Lähteet:

Kirjallisuus:

Alasuutari, Pertti 1999. Laadullinen tutkimus. Vastapaino. Tampere.

Amin, Hanudin 2009. An Analysis of Online Banking Usage Intentions: an Extension of the Technology Acceptance Model. International Journal of Business and Society 10 (1), p. 27-42.

Beck, Ulrich 1992. Risk Society: Towards a New Modernity. Sage Publications.

Casaló, Luis V.; Flavián, Carlos & Guinaliu, Miguel 2007. The role of security, privacy, usability and reputation in the development of online banking. Online Information Review 31 (5), 583-603.

Cheng T.C. Edwin, Lam David Y.C. & Yeung Andy C.L. 2006. Adoption of Internet banking: An empirical study in Hong Kong. Decision Support Systems 42 (3), 1558–1572.

Dabholkar, Pratibha A. 1996. Consumer evaluations of new technology-based self-service options: An investigation of alternative models of service quality. International Journal of Research in Marketing 13 (1), p. 29-51.

Davis, F.; Bagozzi, R. & Warshaw, P. 1989. User acceptance of computer technology: A comparison of two theoretical models. Management Science 35 (8), p. 982-1003.

Emigh, Aaron 2005. Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures. DHS Report. Saatavilla osoitteesta
http://www.antiphishing.org/resources.html#articles
Luettu 17.3.2010.

Eräsaari, Risto 1997. Mitä riskin käsitteellä organisoidaan? Teoksessa Ahponen, Pirkkoliisa (toim.). Riskikirja. Uhat, mahdollisuudet ja asiantuntijuus epävarmuuden yhteiskunnassa. Yhteiskuntatieteiden, valtio-opin ja filosofian julkaisuja 9. Jyväskylän yliopisto. s. 67-89.

Eskola, Jari & Suoranta, Juha 1998. Johdatus Laadulliseen tutkimukseen. Vastapaino. Jyväskylä.

FK 2008. Maksaminen Suomessa ja Euroopassa. Finanssialan keskusliiton julkaisuja 2008. Helsinki.

FK 2009a. Finanssiala 2009. Finanssialan Keskusliiton julkaisuja 2009. Helsinki.

FK 2009b. Nuorten rahankäyttötutkimus. Tutkimusraportti, kesäkuu 2009. Finanssialan keskusliitto. Helsinki.

FK 2009c. Senioritutkimus. Tutkimusraportti, kesäkuu 2009. Finanssialan keskusliitto. Helsinki.

FK 2009d. Säästäminen ja luotonkäyttö. Tutkimusraportti, toukokuu 2009. Finanssialan keskusliiton julkaisuja. Helsinki.

Gerrard, Philip; Cunningham, J. Barton & Devlin, James F. 2006. Why consumers are not using internet banking: a qualitative study. Journal of Services Marketing 20 (3), 160-168.

Gupta, Manish; Rao, Ragharv & Upadhyaya, Shambhu 2004. Electronic Banking and Information Assurance Issues: Survey and Synthesis. Journal of Organizational and End User Computing 16 (3), 1-21.

Helsingin Sanomat 18.1.2010. Nordea lupaa korvata haittaohjelman aiheuttamat vahingot. Saatavilla osoitteesta http://www.hs.fi/talous/artikkeli/Nordea+lupaa+korvata+haittaohjelman+aiheuttamat+vahingot/1135252215702
Luettu 20.1.2010

Hirsjärvi, Sirkka & Hurme, Helena 2004. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Yliopistopaino. Helsinki.

Hua, Guangying 2009. An Experimental Investigation of Online Banking Adoption in China. Journal of Internet Banking and Commerce Vol. 14 Issue 1, p. 1-12.

Hutchinson, Damien & Warren, Matthew 2003. Security for Internet banking: a framework. Logistics Information Management 16 (1), 64-73.

Jayawardhena, Chanaka & Foley, Paul 2000. Changes in the banking sector – the case of Internet banking in the UK. Internet Research: Electronic Networking Applications and Policy 10 (1), 19-31.

Järvinen, Raija & Heino, Heli 2004. Kuluttajien palvelukokemuksia vakuutus- ja pankkisektorilta. Kuluttajatutkimuskeskus, julkaisuja 2004:3. Savion Kirjapaino Oy. Kerava.

Karjaluoto, Heikki; Mattila, Minna & Pento, Tapio 2002. Electronic banking in Finland: Consumer beliefs and reactions to a new delivery channel. Journal of Financial Services Marketing 6 (4), 346-362.

Kauppalehti 19.11.2009. Suomen pankit suojattomia tilit tyhjentävälle virukselle. Saatavilla osoitteesta http://www.kauppalehti.fi/5/i/talous/uutiset/etusivu/uutinen.jsp?oid=2009/11/28036 Luettu 26.11.2009.

Kidra, Engin & Kruegel, Christopher 2006. Protecting users against phishing attacks. The Computer Journal 49 (5), 554-561.

Kiiskinen, Anna 2007. Kuluttaja ja sähköisen ostamisen ongelmat. Kuluttajaekonomian pro gradu –tutkielma. Helsingin yliopisto.

Korhonen, Anne 2001. Mobiilipalveluiden valintatilanne – Case: Leonia Pankin kyselytutkimus WAP-pankkipalveluista. Kuluttajaekonomian pro gradu –tutkielma. Helsingin yliopisto.

Koskinen, Ilpo; Alasuutari, Pertti & Peltonen, Tuomo 2005. Laadulliset menetelmät kauppatieteissä. Vastapaino. Tampere.

Kuluttajabarometri 8/2009. Joidenkin laitteiden yleisyys kotitalouksissa haastatteluhetkellä, prosenttia kotitalouksista. Kuluttajabarometri: taulukot 2009, elokuu. Tulot ja kulutus 2009. Tilastokeskus. Helsinki.

Kuluttajabarometri 2/2007. Joidenkin laitteiden yleisyys kotitalouksissa haastatteluhetkellä, prosenttia kotitalouksista. Kuluttajabarometri: taulukot 2007, helmikuu. Tulot ja kulutus 2009. Tilastokeskus. Helsinki.

Kuluttajabarometri 1/2006. Joidenkin laitteiden yleisyys kotitalouksissa. Kuluttajabarometri 2006 tammikuu. Tulot ja kulutus 2006. Tilastokeskus. Helsinki.

Laforet, Sylvie & Li, Xiaoyan 2005. Consumers´ attitudes towards online and mobile banking in China. The International Journal of Bank Marketing 23 (4/5), 362-381.

Lagerspetz, Eerik 1997. Epävarmuuden aika. Teoksessa Ahponen, Pirkkoliisa (toim.). Riskikirja. Uhat, mahdollisuudet ja asiantuntijuus epävarmuuden

yhteiskunnassa. Yhteiskuntatieteiden, valtio-opin ja filosofian julkaisuja 9. Jyväskylän yliopisto. s. 91-105.

Liao, Z. & Wong, W. K. 2008. The determinants of customer interactions with internet-enabled e-banking services. The Journal of the Operational Research Society 59 (9), 1201-1210.

Lystimäki, Mira 2000. Vakuutukset verkossa – kuluttajien odotuksia ja kokemuksia. Kuluttajaekonomian pro gradu –tutkielma. Helsingin yliopisto.

Lähteenmäki, Mirella 2009. Henkilötietojen hyödyntäminen markkinoinnissa kuluttajien tulkitsemana. Diskurssianalyyttinen tutkimus kuluttajan tietosuojasta. Helsinki School of Economics. HSE Print 2009.

Oppliger, Rolf; Hauser, Ralf & Basin, David 2006. SSL/TLS session-aware user authentication – Or how to effectively thwart the man-in-the-middle. Computer Communications 29 (12), 2238-2246.

Pantzar, Mika 1996. Kuinka teknologia kesytetään. Kuluttajatutkimuskeskuksen tutkimuksia. Karisto Oy:n kirjapaino. Hämeenlinna.

Peura-Kapanen, Liisa 2009. ”Jos siitä olisi minulle selvää taloudellista hyötyä, ainakin kokeilisin sitä.” Kuluttajien mielipiteitä e-laskusta. Työselosteita ja esitelmiä 121/2009. Kuluttajatutkimuskeskus. Helsinki.

Pikkarainen, Tero; Pikkarainen, Kari; Karjaluoto, Heikki & Pahnila, Seppo 2004. Consumer acceptance of online banking: an extension of the technology acceptance model. Internet Research 14 (3), 224-235.

Pikkarainen, Kari; Pikkarainen, Tero; Karjaluoto, Heikki & Pahnila, Seppo 2006. The measurement of end-user computing satisfaction of online banking services: empirical evidence from Finland. International Journal of Bank Marketing 24 (3), 158-172.

Polatoglu, Vishuda Nui & Ekin, Serap 2001. An empirical investigation of the Turkish consumers' acceptance of Internet banking services. International Journal of Bank Marketing 19 (4), 156-165.

Raijas, Anu 2002. Luottamus sähköisessä kaupassa. Teoksessa Uusitalo, Liisa (toim.). Kuluttaja virtuaalimarkkinoilla. Edita. Helsinki. s. 194-211.

Riipinen, Toni & Tinnilä, Markku 2004. Trust in the New Economy – The Case of Finnish Banks. Liikenne- ja viestintäministeriön julkaisuja 17/2004. Helsinki.

Sarel, Dan & Marmorstein, Howard 2006. Addressing consumer's concerns about online security: A conceptual and empirical analysis of banks' actions. Journal of Financial Services Marketing 11 (2), 99-115.

Sathye, Milind 1999. Adoption of Internet banking by Australian consumers: an empirical investigation. International Journal of Bank Marketing Vol. 17 Issue 7, 324-334.

Sayar, Ceren & Wolfe, Simon 2007. Internet banking market performance: Turkey versus the UK. International Journal of Bank Marketing 25 (3), 122-141.

Schultz, E. Eugene; Proctor, Robert W.; Lien, Mei-Ching & Salvendy, Gavriel 2001. Usability and security: an appraisal of usability issues in information security methods. Computers and Security 20 (7), 620-634.

Sudha, Raju; Thiagarajan, A.S. & Seethamaran, A. 2007. The Security Concern on Internet Banking Adoption Among Malaysian Banking Customers. Pakistan Journal of Biological Sciences 10 (1), 102-106.

Tilastokeskus 2009. Internetin käyttötarkoitukset. Saatavilla osoitteesta www.stat.fi/til/sutivi/2009/sutivi_2009_2009-09-08_tau_001.html .
Luettu 6.11.2009.

Wang, Yi-Shun; Wang, Yu-Min; Lin, Hsin-Hui & Tang, Tzung-I 2003. Determinants of user acceptance of Internet banking: an empirical study. International Journal of Services Industry Management 14 (5), 501-519.

Weir, Catherine S.; Douglas, Gary; Carruthers, Martin & Jack, Mervyn 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security 28 (1-2), 47-62.

White, Helen & Nteli, Fotini 2004. Internet Banking in the UK: Why are there not more customers? Journal of Financial Services Marketing 9 (1), 49-57.

Zwick, Detlev; Bonsu, Samuel K. & Darmody, Aron 2008. Putting Consumers to Work: `Co-Creation` and new marketing govern-mentality. Journal of Consumer Culture 2008 (8), 163-196.

Verkkoaineistot

Aktia 2010. Internet-pankin käyttöohje.
Saatavilla osoitteesta
https://ebank.www.aktia.net/VerkkopalvelutWeb/sisalto/opaste.jsp?id=10000&kielip=fi&B=4055
Luettu 30.1.2010

FK 2010. Pankkiturvallisuus. Finanssialan keskusliitto.
Saatavilla osoitteesta
http://www.pankkiturvallisuus.fi/modules/system/stdreq.aspx?P=4105&VID=default&SID=6436482486902 53&S=0&C=25900
Luettu 13.4.2010

Kuluttajavirasto 2010. Huijaukset.
Saatavilla osoitteesta
http://www.kuluttajavirasto.fi/fi-FI/huijaukset/
Luettu 13.4.2010.

Nordea 2010a. Huijausviestejä liikkeellä 10.3.2010 alkaen.
Saatavilla osoitteesta
http://www.nordea.fi/Henkil%C3%B6asiakkaat/Internet+ja+puhelin/Neuvoja+Internet+ja+puhelinpalveluista/Huijausviestej%C3%A4+liikkeell%C3%A4+1032010+alkaen/1336112.html
Luettu 15.3.2010.

Nordea 2010b. Maksun lisävahvistus käyttöön verkkopankissa.
Saatavilla osoitteesta
https://www.nordea.fi/Tietoa+Nordeasta/Maksun+lis%C3%A4vahvistus+k%C3%A4ytt%C3%B6%C3%B6n+verkkopankissa/1282952.html
Luettu 15.3.2010.

Nordea 2010c. Tietoturva.
Saatavilla osoitteesta
http://www.nordea.fi/Henkil%C3%B6asiakkaat/Internet+ja+puhelin/Neuvoja+Internet-+ja+puhelinpalveluista/Tietoturva/700824.html
Luettu 30.1.2010.

Nordea 2010d. Pankkitunnuksilla käytettävien palvelujen yleiset ehdot.
Saatavilla osoitteesta
http://www.nordea.fi/Henkil%C3%B6asiakkaat/Internet%2bja%2bpuhelin/Internet-palvelut/Ehdot/903592.html
Luettu 3.5.2010.

OP 2010a. Osuuspankin asiakkaiden verkkotunnuksia yritetty kalastella.
Saatavilla osoitteesta
https://www.op.fi/op?cid=151245758&srcpl=4
Luettu 15.3.2010.

OP 2010b. Tietoturvaopas.
Saatavilla osoitteesta
https://www.op.fi/op?id=940&srcpl=6

Luettu 30.1.2010.

S-Pankki 2010a. Verkkopankin turvallisuusohjeet.
Saatavilla osoitteesta
https://online.s-pankki.fi/help/general/securityInfo_fi.html
Luettu 30.1.2010.

S-Pankki 2010b. Maksupalvelulaki.
Saatavilla osoitteesta
http://www.s-pankki.fi/henkiloasiakkaat/maksut/fi_FI/maksupalvelulaki/
Luettu 6.5.2010.

Säästöpankki 2010. Turvallisuus.
Saatavilla osoitteesta
https://www.saastopankki.fi/VerkkopalvelutWeb/portaali/index.jsp?sivu=po_tiedotteet
Luettu 30.1.2010

Viestintävirasto 2009. Viestintävirasto kehottaa teleyrityksiä suodatustoimiin maksuvälinepetosten hillitsemiseksi. Lehdistötiedote.
Saatavilla osoitteesta
http://www.ficora.fi/index/viestintavirasto/lehdistotiedotteet/2009/P_37.html
Luettu 26.11.2009.

Viestintävirasto 2010. Tietoturvaopas.
Saatavilla osoitteesta
http://www.tietoturvaopas.fi/index.html
Luettu 13.4.2010.

Liitteet:

Liite 1: Kuluttajahaastateltavien taustatiedot

Ikä? ____

Sukupuoli? _____

Koulutus? _____

Kuinka kauan käyttänyt verkkopankkia, vuosia? _____

Kuinka usein käyttää verkkopankkia? _____

Liite 2: Haastattelurunko kuluttajahaastateltaville

- Verkkopankin käyttö
    - Käyttääkö useita palvelukanavia? Mikä yleisin?
    - Onko monen pankin asiakas? Käyttääkö monen pankin verkkopankkia?
    - Mihin tarkoituksiin käyttää verkkopankkia?
    - Verkkopankin hyödyt?

- Turvallisuus
    - Kokeeko verkkopankin turvalliseksi?
    - Onko tietoinen turvallisuusuhista? Millaisista on kuullut?
    - Onko itse kokenut tilanteita, joissa turvallisuus vaaraantuu?
    - Onko tunnistautuminen riittävän turvallinen? Miten suhtautuisi ulkoisiin laitteisiin kirjautumisessa?
    - Onko omia käytäntöjä parantaa turvallisuutta? Millaisia?

- Tiedotus
    - Onko pankki varoittanut turvallisuusuhista?
    - Onko pankki antanut turvallisuusohjeita?
    - Mistä on kuullut turvallisuusuhista?
    - Onko tiedotus riittävällä tasolla vai pitäisikö sitä lisätä?
    - Mikä olisi paras kanava tiedotukseen?

- Vastuunjako

- Kenellä on vastuu taloudellisista menetyksistä?
- Missä tilanteissa pankin pitäisi korvata menetykset?
- Missä tilanteissa asiakas olisi itse vastuussa?

Liite 3: Haastattelurunko asiantuntijoille

- Turvallisuus
  - Millaisia turvallisuusuhkia verkkopankkiin liittyy?
    - Miten ne ovat kehittyneet viime aikoina?
  - Kohdistuuko suomalaispankkeihin paljon hyökkäyksiä?
    - Jos ei niin miksi? Oltaisiinko niihin varauduttu?
  - Miten näihin uhkiin voidaan varautua?
    - Voivatko pankit estää?
  - Ovatko suomalaispankkien järjestelmät ajan tasalla?
    - Onko muualla paremmin?
    - Onko kehitettävää?
  - Onko tunnistautuminen suomalaispankeissa turvallinen?
    - Onko muualla paremmin?
    - Onko kehitettävää?
  - Mikä on teleyritysten rooli?

- Tiedotus
  - Tiedottavatko pankit riittävästi turvallisuusuhista?
  - Kenen vastuulla olisi turvallisuudesta tiedottaminen?

- Vastuunjako
  - Kenen vastuulla korvata taloudelliset menetykset?
  - Voivatko pankit edellyttää asiakkailtaan tietynlaista käyttäytymistä?