Näin meitä huijataan!

Verkossa yleisesti tavattuja huijausmenetelmiä

Päivitetty 30.3.2017

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Taustaa

Suomalaisiin käyttäjiin kohdistuvat tietojenkalastelukampanjat ja erilaiset huijaussivut jatkavat yleistymistään. Myös huijausviestien ja -sivustojen kieliasu ja ulkonäkö ovat parantuneet merkittävästi. Viestien lähettäjät ovat myös aiempaa organisoidumpia ja pitkäjänteisempiä.

Aiemmin huijausviestin pystyi erottamaan tökeröstä suomenkielestä tai epämääräisestä ulkoasusta, mutta nyt käyttäjältä vaaditaan enemmän tarkkaavaisuutta.

Tässä raportissa tarkastellaan yleisimpiä huijausmenetelmiä, joita Viestintäviraston Kyberturvallisuuskeskus on saanut tietoonsa. Raportissa esitetyt menetelmät ovat esimerkinluontoisia, eivätkä kata kaikki mahdollisia huijauksia. Raportissa käydään myös läpi yksinkertaisia ohjeita, joilla huijauksia vastaan voi suojautua.

Erilaisia huijauksia

1 Älä usko liian houkuttelevia tarjouksia

Verkossa valtaosa käyttäjistä on ihan samanlaisia tavallisia ihmisiä kuten me kaikki muutkin. Mukana on kuitenkin huijareita, jotka haluavat rahasi. Valitettavasti juuri nämä huijarit näkevät eniten vaivaa saadakseen syöttinsä juuri sinun nähtäväksesi, joten huijauksiin on helppo törmätä.

Huijauksia tulee vastaan sähköpostissa, keskustelu- ja seuranhakupalstoilla, osto- ja myyntipalstoilla, tekstiviesteissä, nettimainoksissa, puhelimessa, televisiossa, melkein missä vain. Opi tunnistamaan tavallisimmat huijarit ja huijauskeinot, niin vältyt monelta harmilta.

1.1 Romanssihuijaukset: Hän haluaa juuri sinut!

Huijauksen voi rakentaa myös lupaavaksi naamioidun ihmissuhteen varaan. Etenkin toiveikasta ihmistä on valitettavan helppo johtaa harhaan. Jos tarjolla on esimerkiksi eksoottista kaukorakkautta, moni on valmis auttamaan rakastaan myös rahallisesti. Kontakti uhriin saadaan usein väärennetyllä profiililla seuranhakupalvelun kautta sopivaa kohdetta hakemalla.

Kun uhri löytyy, huijari haluaa rakentaa tähän luottamuksellisen ja syvän suhteen. Alkuhuuman jälkeen huijari kehittää esimerkiksi tarinan, jossa hänen vaikea avioeronsa uhkaa suhteen jatkoa. Uhka poistuu ja ongelmat ratkeavat, jos uhri vain lainaa kaukorakkaalleen rahaa.

1.2 Rahanpesuun houkuttelu

Nettimainoksilla houkutellaan ansaitsemaan helppoa rahaa vain netissä istumalla ja klikkailemalla. Kohteena ovat myös suomalaiset. Helppo rahantulo kuulostaa houkuttelevalta, mutta ilmaisia lounaita ei tässäkään ole. Mainokset sisältävät erilaisia todistuksia siitä, miten loistava mahdollisuus on kyseessä. Tämä ei kuitenkaan ole totta. Rikolliset tarjoavat rahaa tilisiirroista, joita tehdään erisuuruisille rahasummille. Todellisuudessa uhri huijataan osaksi laitonta kansainvälistä rahanpesua.

Rahanpesuhuijauksessa uhrille kerrotaan jokin peitetarina. Tarina kertoo vaikkapa sukulaisesta, joka ei jostain syystä voi siirtää rahaa suoraan, vaan uhrin täytyy toimia välikätenä. Siirtoihin käytetään pankkien lisäksi muitakin maksulaitoksia ja maksuvälineitä.

Rahanpesu voidaan naamioida myös valuuttakaupaksi, järjestetyksi vedonlyönniksi, arpajaisiksi tai muuksi "erinomaiseksi" mahdollisuudeksi liike- tai sijoitustoimintaan.

1.3 Pyramidihuijaukset

Kaupankäyntimenetelmiä, joissa ansaintamalli perustuu uusien jäsenten rekrytointiin, kutsutaan yleensä pyramidihuijauksiksi. Menetelmä yritetään naamioida liike- tai sijoitustoiminnaksi, koska Rahankeräyslaki 255/2006 kieltää niin kutsutun *pyramidipelin*.

Pyramidipelin tunnistaa selvimmin siitä, että järjestelmään sisään tuleva kassavirta muodostuu pääasiassa uusien jäsenten maksamista maksuista. Maksut yritetään monesti verhota erilaisiksi rekrytointimaksuiksi, koulutus- tai kurssimaksuiksi, aloituspaketin hinnaksi tai suoraan jäsenmaksuiksi.

Hälytyskellojen pitäisi soida, kun pyramidihuijari lupaa uusille jäsenille merkittävää voittoa tai tulevaisuuden arvonnousua nyt sijoitetulle rahalle. Jopa satojen prosenttien tuoton väitetään syntyvän valuuttakaupasta tai virtuaalikolikoista tai muusta keksinnöstä, jota muut eivät tiedä. Älä usko!

1.4 Nigerialaishuijaus

Tämäkin huijaus perustuu uhrin hyväuskoisuuden väärinkäyttöön. Tyypillistä on, että uhrille uskotellaan että hän on voittanut lotossa tai että hänen kaukainen sukulaisensa on jättänyt suuren perinnön. Uhrille uskotellaan, että potin voi lunastaa antamalla pankkitiedot ja siirtämällä tietyn rahasumman perinnön käsittelystä aiheutuvia kuluja varten. Rahat siirrettyään huijarit saattavat pyytää uhrilta vielä uusia rahasiirtoja "ennakoimattomien ylimääräisten kulujen kattamiseksi". Kirjeessä luvattua lottopottia tai perintöä ei kuitenkaan koskaan kuulu.

Uhria saatetaan lähestyä sähköpostilla, tekstiviestillä tai perinteisellä postilla. Nigerialaiskirjeistä voi lukea lisää esim. Wikipediasta:

http://fi.wikipedia.org/wiki/Nigerialaiskirjeet

---------- Forwarded message ----------
From: INFO PRIZE DETAILS <wolgangan.dom8@gmail.com>
Date: 2010-04-21 2:57 GMT+03:00
Subject: Netherlands Lucky Day
To:

Ref:GNP501/731KW

We are delighted to inform you of our Lucky Day Lotto prize award held on the 16th of February 2010 in Netherland. This lotto awards is fully based on an electronic selection, Winners were picked by computerized system, drawn from over 43,000,00 companies and individuals e-mail addresses worldwide.This award is officially announced to day in Amsterdam The Netherland,Your email ID has hereby been approved a lump sum pay out of Ђ1,319,025 Cent in cash credit file Ref: GNP501/731KW,
Batch: AM72/PGS27/09FC, Winning No: DC61/PDN32/01NL

Simply contact Our Office of Foreign Financial Security Vsb Netherland on phone and email for your prize claim immediately.

Mr. Rob Van Dirk.
Tel +31-684-874-123,
e-mail: nl.luckydays@aol.nl

Congratulations! once again.

Yours in service,
Mrs. Marrith Driker
Dpt Sec
Nl. Lucky Day Loto

Kuva 1: Esimerkki ns. nigerialaiskirjeestä, jossa uhrin hyväuskoisuutta pyritään väärinkäyttämään.

1.5 Liian hyvät tarjoukset voivat olla tilausansoja

"Onneksi olkoon - saat uuden iPhone 6s (sisältää 3 päivän kokeilun)"

"Hanki iPhone 6s -puhelin, hinta 1 euro"

Viimeaikoina on yleistynyt huijaus, jossa käyttäjälle luvataan esimerkiksi uusi älypuhelin tai jokin muu houkutteleva tuote eurolla. Taustalla saattaa olla joko luottokortti- tai pankkitietojen kalasteluyritys tai niin sanottu tilausansa.

Tilausansalla tarkoitetaan yritystä, joka saa kuluttajan tilaamaan mainoksen tai viestin pohjalta jotain, mitä ei ymmärtänyt tilaavansa. Erehdyttäminen voi olla joko tahatonta tai tahallista. Olennaista kuitenkin on, että viestin tai tarjouksen vastaanottaja ei saa viestin sisällöstä todenmukaista kuvaa ja tämä vaikuttaa hänen ostopäätökseensä.[1]

1 http://www.ecc.fi/Ajankohtaista/Tiedotteet/2015/6.5.2015-tunnistatko-tilausansan-esimerkkeja-ja-ohjeet-ansojen-valttamiseen/

Esimerkiksi uutta älypuhelinta tarjoavissa huijauksissa käyttäjä saattaa huomaamattaan sitoutua suoratoistopalvelun asiakkaaksi kalliilla kuukausimaksulla. Sopimuksesta voi olla vaikea päästä irti. Tilausansan houkuttimena toimivaa älypuhelinta ei koskaan lähetetä, vaan se saatetaan esimerkiksi arpoa yhdelle asiakkaalle tai korvata jollain toisella tuotteella.

Kuva 2: Tilausansa saa kuluttajan tilaamaan jotakin, mitä hän ei ole ymmärtänyt tilaavansa. Kuvan sivustolle tietonsa syöttämällä ei saa uutta iPhonea eurolla, vaan sitoutuu 79 euroa kuussa maksavan suoratoistopalvelun asiakkaaksi.

Kyberturvallisuuskeskus, suomalaiset teleyritykset ja Kilpailu- ja kuluttajavirasto ovat saaneet lukuisia yhteydenottoja halpaa älypuhelinta mainostaviin tilausansoihin liittyen.

Kuluttajan täytyy olla valppaana verkossa eikä uskoa kaikkea mitä verkkosivu lupaa. Lisätietoa tilausansoista löytyy Euroopan kuluttajakeskuksen sivuilta:

http://www.ecc.fi/Ajankohtaista/Tiedotteet/2015/6.5.2015-tunnistatko-tilausansan-esimerkkeja-ja-ohjeet-ansojen-valttamiseen/

2 Tietojenkalastelu

Tietojenkalastelua tehdään mm. pankkitunnusten, luottokorttinumeroiden, sähköpostitunnusten ja sosiaalisen median tunnusten saamiseksi. Tietojenkalastelu alkaa tyypillisesti sähköpostilla, jonka avulla käyttäjä ohjataan tietojenkalastelusivulle.

Tietojenkalastelusivujen ulkoasu ja teema vaihtelee melkoisesti, mutta parhaimmillaan ne on toteutettu hyvällä suomen kielellä. Lisäksi niiden erottaminen alkuperäisestä sivusta, johon huijaussivusto perustuu, voi olla vaikeaa.

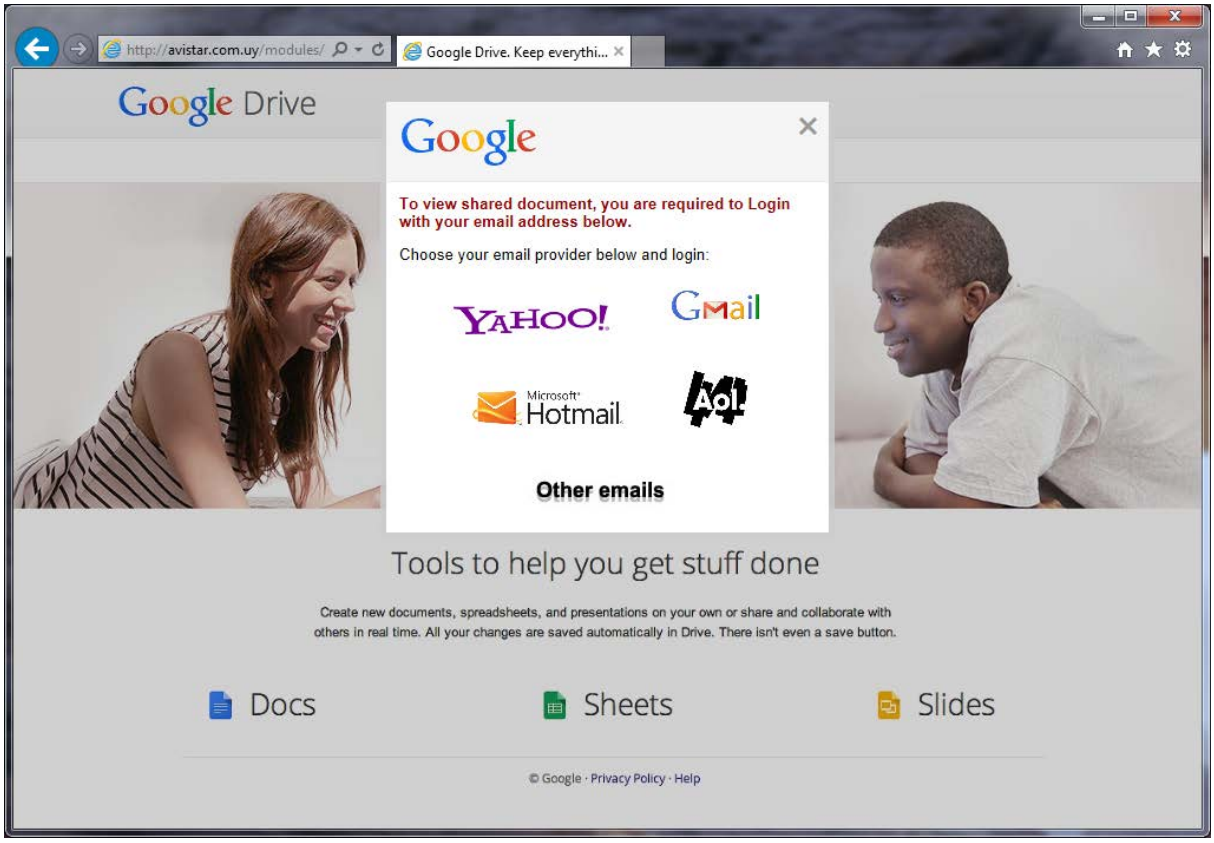
2.1 Sähköpostin ja sosiaalisen median tunnusten kalastelu

Sähköpostin ja sosiaalisen median käyttäjätunnusten kalastelu on lisääntynyt. Mitä luultavimmin taustalla on näiden käyttäjätietojen kasvanut merkitys. Suuri osa ihmisen viestinnästä välittyy nykyisin sosiaalisen median tai sähköpostin kautta.

Samoja sähköpostin ja sosiaalisen median tunnuksia käytetään useisiin eri palveluihin kirjautumisissa. Ominaisuus helpottaa elämää, koska näin jokaiseen palveluun ei tarvitse keksiä uutta käyttäjätunnusta ja salasanaa. Haittapuolena on kuitenkin, että jos tunnukset joutuvat vääriin käsiin, esimerkiksi huijari voi kaapata uhrinsa muidenkin palvelujen tilejä.

Vaikka samaa sähköpostiosoitetta ei käytettäisi muihin palveluihin kirjautumisessa, henkilö on saattanut hyödyntää sähköpostiosoitettaan muiden palvelujen käyttäjätilien rekisteröinnissä. Useiden palvelujen sinänsä hyödyllinen "unohdin salasanani" -toiminto lähettää yleensä uuden salasanan luontilinkin henkilön sähköpostiosoitteeseen. Jos esimerkiksi huijari pääsee hallitsemaan juuri tätä sähköpostitiliä, hänen on mahdollista ottaa haltuun muutkin uhrinsa käyttäjätilit.

Sosiaalisen median tunnusten avulla voi myös turmella henkilön tai yrityksen imagoa luvattomien tilapäivitysten tai tviittien avulla. Lisäksi rikolliset voivat kiristää kohdettaan pyytämällä lunnaita tunnusten palauttamiseksi.



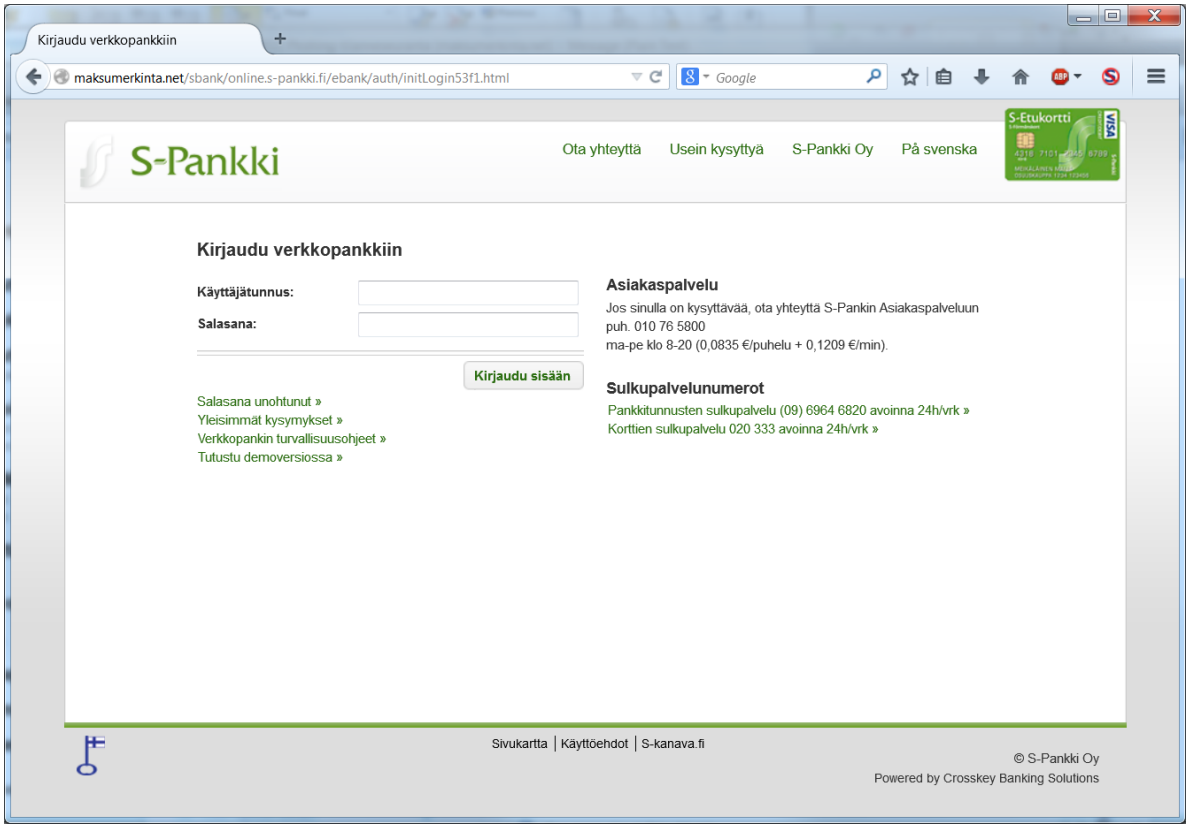
Kuva 3: Esimerkki sähköpostitunnusten kalastelusivusta. Tietojenkalastelusivustoa saattaa olla pelkän sisällön perusteella vaikea erottaa aidoista sivuista. Selaimen osoitekentän verkkotunnus kuitenkin yleensä paljastaa huijauksen.

2.2 Pankkitunnusten kalastelu

Verkkopankkitunnusten kalastelu alkoi lisääntyä keväällä 2014 huijauskampanjan seurauksena. Kampanjan avulla nostettiin 400 000 eurolla pikaluottoja ja tehtiin 50 000 euron edestä rahasiirtoja heinäkuun 2014 puoliväliin mennessä. Rikolliset kirjautuivat kalastettujen tunnusten avulla käyttäjien pankkitileille, joista rahoja siirrettiin ulkomaisille tileille. Verkkopankkitunnusten avulla myös tunnistauduttiin pikalainoja tarjoavien yritysten verkkosivuille, josta lainoja nostettiin uhrin nimissä.

Sähköpostiviestien lisäksi pankkitietojen kalastelussa käytetään tekstiviestejä ja verkkopankkien sisäänkirjautumissivuja muistuttavia www-sivustoja. Tekstiviestejä on hyödynnetty erityisesti kertakäyttöisten tunnuslukujen kalasteluun, laadukkaasti toteutetut www-sivustot puolestaan vakuuttavat uhrin uskomaan, että kyseessä ovat luotettavat verkkopankkisivut, vaikka kyseessä on puhdas huijaus.

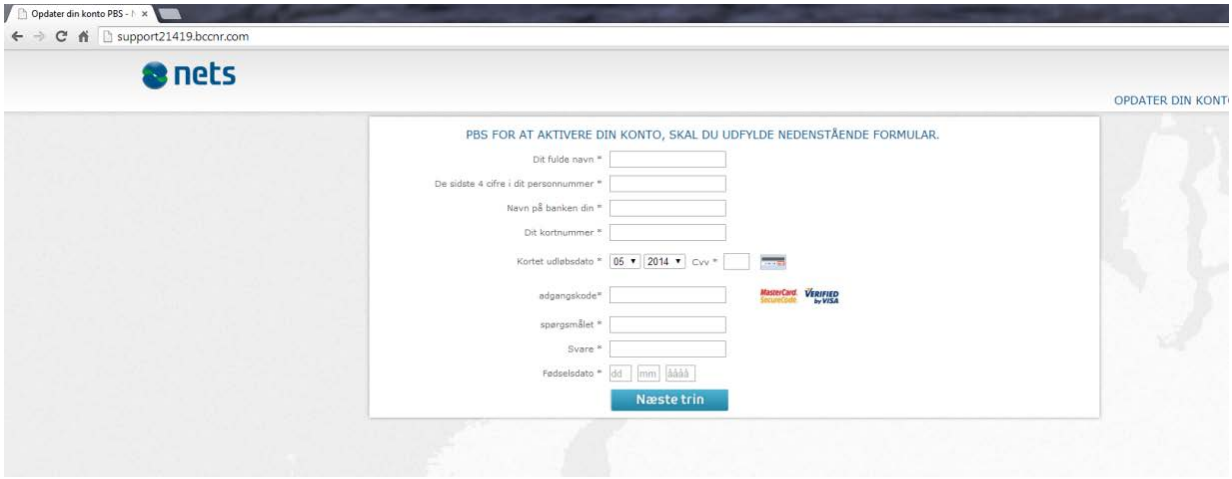
Verkkopankkitunnuksia on kalasteltu esimerkiksi tekaistujen myöhästyneiden maksujen varjolla. Myös uhrille saapuneiksi väitettyjä tavaralähetyksiä käytetään usein peitetarinana. Yhteistä kaikille peitetarinoille on, että uhri uskotellaan luulemaan, että hänelle seuraa vaikeuksia tai häneltä jää jotakin hyvää saamatta, jos hän ei toimi nopeasti. Hyvin tyypillisesti eräpäivän uskotellaan, olevan aivan kohta ovella. Huijarit uskottelevat uhrin pääsevän tarkastelemaan tai korjaamaan häntä koskevia tietoja verkkopankkitunnuksillaan. Huijarit käyttävät tätä taktiikkaa myös muiden tietojen kalasteluun.



Kuva 4: Esimerkki pankkitunnusten kalastelusivusta. Sivusto on laadukkaasti toteutettu, mutta osoiterivin väärä osoite paljastaa huijauksen. Myös tietoliikenneyhteyden salausta kuvaava lukittu lukkoikoni puuttuu osoiteriviltä. Kuvan tietojenkalastelusivu on irtikytketty verkosta 10.7.2014.

2.3 Luottokorttitietojen kalastelu

Myös luottokorttitietojen huijaaminen on rikollisten suosima keino päästä käsiksi ihmisten varoihin on. Tyypillisesti luottokorttitietojen kalastelu alkaa väärennetyllä sähköpostiviestillä, joka ensisilmäyksellä vaikuttaa tulevan luottokorttiyhtiöltä. Viestissä pyydetään päivittämään tai tarkistamaan luottokortin tiedot. Tiedot pyydetään syöttämään tarkastusta tai aktivointia varten verkkosivustolla, johon on linkki sähköpostiviestissä. Linkin teksti ei silmämääräisesti paljasta sivuston todellista osoitetta. Kalastelusivustolla olevaan lomakkeeseen pyydetään syöttämään luottokortin numeron ja voimassaoloajan lisäksi myös suojakoodi. Usein Lomakkeessa kysytään myös verkkomaksamiseen liittyviä "Verified by Visa" tai "Mastercard Securecode" todentamistunnuksia.



Kuva 5: Esimerkki luottokorttitietojen kalastelusivusta.

3 Mobiilimaksu-ominaisuutta on käytetty väärin

Monet teleyritykset tarjoavat verkkosivujen ylläpitäjille ratkaisua, jossa verkkosivu voi laskuttaa tarjoamansa palvelun sivulla vierailevan käyttäjän normaalin matkapuhelinlaskun yhteydessä. Tämä palveluiden tilaamista ja maksavista sujuvoittava toiminto on valitettavasti aiheuttanut myös vahingossa klikattuja maksuja.

Joissain tapauksissa sivusto ei ole selkeästi viestinyt, että mobiilimaksunappia painamalla syntyy maksutapahtuma, joka veloitetaan käyttäjän normaalin matkapuhelinlaskun yhteydessä. Palveluntarjoajasta riippuen mobiilimaksunapin toiminnallisuus saattaa johtua tahattomasta heikosta sivustojen suunnittelusta, mutta sen taustalla voi olla myös tahallista kuluttajan erehdyttämistä.

Langattomalla laajakaistalla tai älypuhelimella nettiä surffatessa tulee olla tietoinen, että tietyt sivustot voivat laskuttaa palveluistaan myös matkapuhelinlaskulla. Jos jokin sivusto ei selkeästi viesti, että palvelusta aiheutuva maksu veloitetaan matkapuhelinlaskulta, kannattaa tällainen sivusto ilmoittaa omalle teleyritykselle.

4 Nettikauppapetokset

Netin osto- ja myyntipalstat ovat mainioita paikkoja löytää käytettyjä hyödykkeitä, mutta ne ovat myös huijareiden suosiossa. Sielläkin kannattaa varoa epäilyttävän hyviä tarjouksia.

Huijari voi myydä tuotetta, jota ei ole olemassa. Rahat menevät, mutta tuotetta ei näy tai ostos on jotakin ihan muuta kuin sovittiin. Jos kauppa ei onnistu kasvotusten, pyydä myyjältä havainnolliset kuvat myytävästä tuotteesta. Kysy, kuka nimimerkin takana on ja voisitko saada tuotteen samaan kuvaan päivän lehden kanssa ennen kuin maksat tuntemattoman tilille rahaa.

Kuvien aitoutta voi yrittää tarkastaa esimerkiksi Googlen kuvahaulla, jonka löytää esimerkiksi Chrome-selaimesta hiiren oikean napin valikosta. Jos identtinen kuva löytyykin netistä, todennäköisesti se ei ole myyjän itsensä ottama kuva. Tällaisessa tilanteessa on syytä epäillä, onko myyjällä koko tuotetta ollenkaan.

Myyjän hyvä mainekaan ei aina takaa luotettavuutta, sillä myyjän käyttäjätili on voitu kaapata. Huijarit seuraavat

ahkerasti salasanavuotoja, joiden avulla kaappauksia toteutetaan. Luotettavalta näyttävä myyjä tai ostaja ei ehkä edes tiedä, että huijari on kaapannut hänen tilinsä ja lokaa hänen maineensa tehtailemalla petoksia toisensa perään. Yritä aina varmistaa myyjän henkilöys ennen kauppaa.

Käytä postiennakkoa, jos et voi olla varma myytävästä tuotteesta. Yksityishenkilöiden välisissä postilähetyksissä lähettäjä saa antaa luvan postipaketin sisällön tarkastamiseen ennen kuittaamista ja maksamista.

Kun tehdään kauppaa kasvotusten, käteisellä rahalla maksaminen on helppo todentaa omin silmin. Jos summa on liian suuri käteisellä kuljetettavaksi tai se tuntuu muuten turvallisemmalta maksaa sähköisesti, kannattaa varmistaa maksun perille meno aina omalla päätelaitteella. Älypuhelimessa toimivalla pikamaksusovelluksella voi varmistaa itselleen kuittauksen heti, kun maksu on varmennettu.

5 Huijariroskapostia tekstiviestein

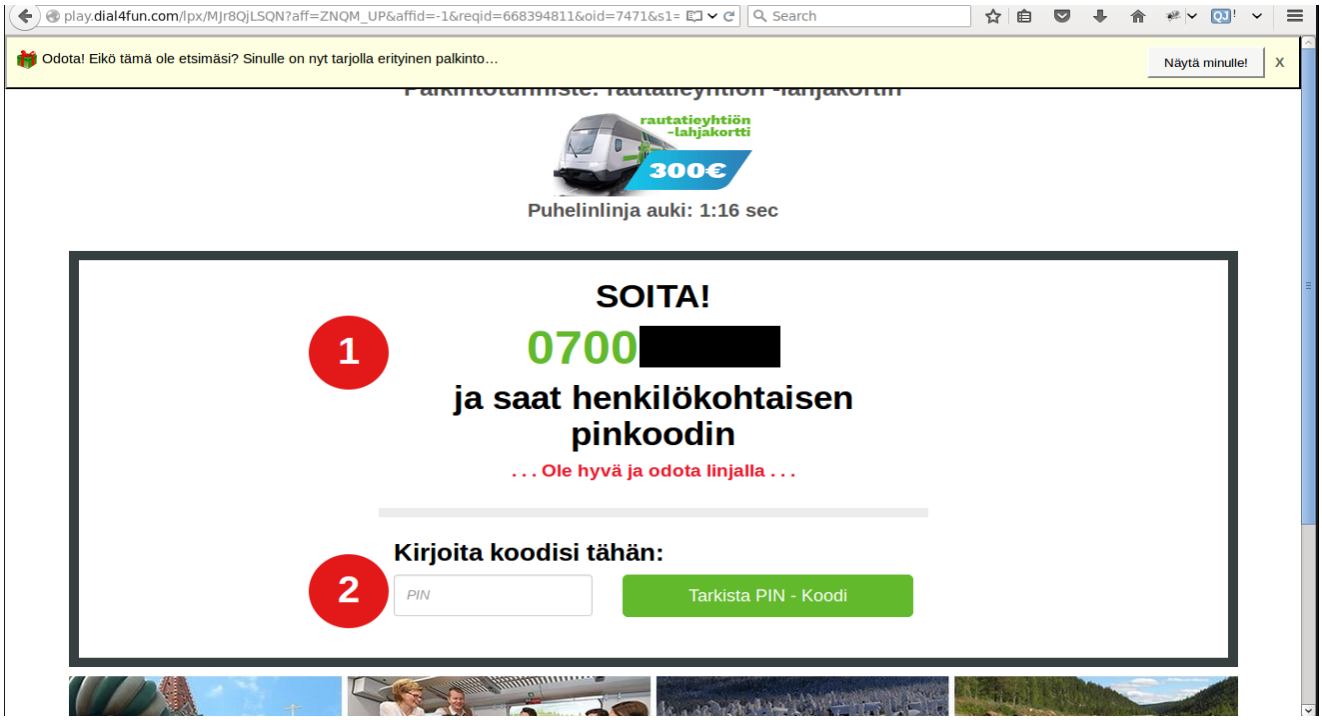
Moni on jo tottunut ohittamaan sähköpostitse tulevat roskapostit ja huijaukset. Tekstiviestit ovat Suomessa vielä vähän käytetty mainoskanava, jota ei osata varoa yhtä hyvin. Tekstiviestinkin lähettäjätiedot on helppo väärentää ja uskotella, että viesti tulee pankista, pikavippiyritykseltä tai viranomaiselta. Nykyälypuhelimissa tekstiviestistä voi suoraan klikata linkkiä, joka ohjaa nettisivulle, jossa odottaa joko huijaus tai haittaohjelma.

Suomessa tekstiviestihuijaukset (smishing) ovat vielä harvinaisia. Muualla Euroopassa ja Yhdysvalloissa ne ovat yleistyneet viime vuosina. Viranomaiset odottavat ilmiön rantautuvan Suomeenkin ennemmin tai myöhemmin.

6 Lahjakortti edellyttää soittoa maksulliseen numeroon

"Voita lahjakortti Suomen suurimpaan huonekaluliikkeeseen! Vastaa seuraaviin 3 kysymykseen selvittääksesi, voimmeko lähettää 700€ lahjakortin sinulle."

"Voita VR- lahjakortti arvoltaan 300 euroa! "



Kuva 3: Sivuston lupaama 300 euron lahjakortti edellyttää soittoa maksulliseen puhelinnumeroon.

Rikolliset mainostavat houkuttelevaa lahjakorttia esimerkiksi huonekaluliikkeeseen tai VR:lle, kunhan vain vastaa muutamaan kysymykseen, kuten kuinka usein matkustaa junalla. Kysymysten jälkeen uhria pyydetään soittamaan maksulliseen numeroon, jotta hän saa PIN-koodin. Lahjakorttia ei soitosta huolimatta kuitenkaan koskaan tule.

7 Toimitusjohtajahuijaus koskee etenkin yrityksiä

Toimitusjohtajahuijauksessa rikolliset lähestyvät yrityksen taloushallintoa tai henkilöä, jolla on laskunmaksuoikeudet, esimerkiksi yrityksen toimitusjohtajan tai talousjohtajan identiteetillä.

Huijauksessa valejohtaja pyytää maksamaan laskun tietylle tilille. Usein tilanteeseen liittyy painostuskeino, kuten myöhässä olevasta maksusta johtuva kiire. Usein kiireelliset maksupyynnöt lähetetään myöhään perjantai-iltapäivällä, ennen viikonloppua.

Suomalaisetkin yritykset ovat joutuneet toimitusjohtajahuijausten kohteiksi. Esimerkiksi vuonna 2015 menetykset ovat olleet julkisuuteen tulleissa tapauksissa yhteensä yli 18 miljoonaa euroa.

Tässä huijaustyypissä on sekä Suomessa että maailmalla havaittu selkeää perehtyneisyyttä kohteena olevaan organisaatioon. Hyökkääjä saattaa rekisteröidä huijausviestien lähettämistä varten verkkotunnuksen, joka muistuttaa hyvin paljon alkuperäistä kohdeorganisaation verkkotunnusta. Esimerkiksi jos talousjohtajan oikea osoite on matti@yritys.fi, saattavat rikolliset lähettää huijausviestejä osoitteesta matti@yyritys.fi. Eroa oikean ja väärän osoitteen välillä ei välttämättä kiireessä aina huomaa.

Laskuhuijauksia voidaan yrittää tehdä myös johtajan omasta sähköpostilaatikosta, jos siihen onnistutaan murtautumaan esimerkiksi arvaamalla heikko

salasana tai ujuttamalla tietokoneeseen haittaohjelma.

Yritysten on syytä varautua toimitusjohtajahuijauksiin kouluttamalla taloushallinnon henkilöstöä sekä luomalla työilmapiirin, jossa kynnys varmistaa jonkin laskun oikeellisuus on mahdollisimman matala. Yrityksissä on myös oltava selkeä prosessi, miten laskut vastaanotetaan ja pannaan maksuun.

8 Hybridihuijaukset

8.1 Tekniikkahuijaukset

Huijarit yrittävät myös pelotella väittämällä, että laitteessasi on jotakin vikaa ja hän auttaa korjaamaan sen. Hän voi ottaa yhteyttä sähköpostitse, puhelimella, tekstiviestitse tai nettimainoksen välityksellä.

Huijari voi väittää, että koneessasi on virus ja sinun täytyy asentaa torjuntaohjelma esimerkiksi hänen www-sivustonsa kautta, jotta ongelma poistuu. Todellisuudessa mitään virusta ei ole ja huijarin tarjoama torjuntaohjelmakin olisi itse asiassa haitallinen.

Huijarin väittämä vika voi olla video, joka ei näy, tai muu nettisisältö, joka ei aukea, ellet asenna huijarin tarjoamaan apuohjelmaa, videokoodekkia tai katselusovellusta. Huijarin apuohjelman mukana koneelle kuitenkin livahtaa myös haittaohjelma, joka voi lukita koneesi, varastaa käyttäjätietosi, pankkitunnuksesi tai luottokorttiesi numerot.

8.2 Muut hybridihuijaukset

Monenlaisten verkon vaarojen ja haittojen yhdistelmää kutsutaan hybridihuijaukseksi.

Keinoina käytetään kaikkea mahdollista sähköpostista monimutkaiseen haittaohjelma-verkkomurto-hyökkäyskuvioon. Vain mielikuvitus on vedätyskeinojen rajana.

Perinteisen yritys- tai toimitusjohtajahuijauksen kohteelle lähetetään perusteeton lasku. Huijaus muuttuu hybridiksi, kun huijauslaskun sisään piilotetaan haittaohjelma, joka varastaa työasemalta luottokorttitietoja, salasanoja ja pankkitunnuksia.

Yhdistelmävedätyksen loppusilaukseksi uhrin kone voidaan lukita ja sen kaikki tiedostot salata, ellei hän suostu huijarin lasku- tai lunnasvaatimuksiin. Mahdollista on myös, että kohteena olevan yrityksen työasemaverkkoon piiloutuu vakoiluohjelma, joka jää tarkkailemaan tilannetta ja odottamaan huijarin etäkomentoja.

Suojautuminen

Huijauksilta suojautuminen edellyttää tarkkaavaisuutta. Huijauksiin ei yleensä liity haittaohjelmaa tai muuta teknistä apuvälinettä, vaan huijaus tehdään käyttäjän hyväuskoisuutta hyväksikäyttäen.

Alle on koottu lista yksinkertaisista varotoimenpiteistä, joita noudattamalla suurimman osan huijauksista voi välttää.

9 Älä luota sokeasti sähköpostin lähettäjätietoihin

Sähköpostien lähettäjätiedot on kohtuullisen helppo väärentää. Vaikka sähköposti näyttäisi tulevan esimerkiksi omalta pankilta tai toimitusjohtajalta, saattaa se silti olla väärennetty. Voi myös olla, että sähköpostin lähettäjän tietokoneeseen on murtauduttu tai hänen sähköpostisalasana on arvattu.

Tulisikin pohtia

- miksi sain kyseisen viestin
- onko lähettäjä minulle entuudestaan tuttu
- olenko viestissä mainitun palvelun käyttäjä
- eroaako viestin sisältö tuntemani palvelun tarjoajan tyypillisestä viestinnästä tai viestien ulkoasusta
- onko viestin kirjoitusasu ja kielioppi asiallinen
- onko viestin sisältö jotenkin muuten epäilyttävä?

Muistathan, että esimerkiksi pankit tai perintätoimistot eivät lähetä sähköposteja, jotka ohjaavat asiakkaat verkkosivulle kirjautumaan.

Jos sähköpostiviestissä on linkki, tarkasta, mihin internetosoitteeseen linkki viittaa. Jos linkin takana oleva verkkotunnus ei liity viestin lähettäjään, kyseessä on luultavasti tietojenkalastelutarkoituksessa lähetetty huijausviesti.

10 Älä luota kaikkiin verkkosivustoihin

Liian hyvät tarjoukset useimmiten ovat liian hyviä ollakseen totta. Jos tarjous vaikuttaa epäilyttävän hyvältä, kannattaa käyttää hetki tarjouksen ehtoihin ja tarjouksen tekijän sivustoon tutustumiseen. Hyvä keino on myös etsiä halpaa tuotetta tarjoavaa yritystä hakukoneella ja katsoa, minkälaista keskustelua yrityksestä käydään internetissä.

Ole erityisen tarkkana, jos epäilyttävän oloiselta verkkosivustolta ohjataan esimerkiksi verkkopankin sisäänkirjautumissivulle, pyydetään luottokorttitietoja tai pyydetään soittamaan maksulliseen numeroon.

11 Tarkasta selaimen kohdeosoite

Miltä tahansa sivustolta verkkopankin tai muun palvelun sisäänkirjautumissivulle siirryttäessä tulee aina tarkastaa selaimen kohdeosoite. Sivustojen väliset linkit on helppo saada näyttämän aidoilta, vaikka todellisuudessa henkilö onkin ohjattu tietojenkalastelusivulle aidon verkkopankin sijaan.

Esimerkiksi keväällä 2014 toimineessa pankkitunnusten kalastelukampanjassa tietojenkalastelusivut ovat olleet verkkotunnusten kuten maksumyohassa.info tai lindorffonline.net alaisuudessa. Ensimmäinen osoite on melko lähellä perintätoimisto Lindorff Oy:n ylläpitämää maksumyohassa.fi -sivustoa ja jälkimmäinen muistuttaa ulkoasultaan Lindorffin omaa osoitetta lindorff.fi. Ri-

kolliset pyrkivät siis harhauttamaan käyttäjiä rekisteröimällä tietojenkalastelusivuiksi verkkotunnuksia, jotka ovat lähes saman muotoisia ja nimisiä kuin alkuperäisetkin verkkotunnukset.

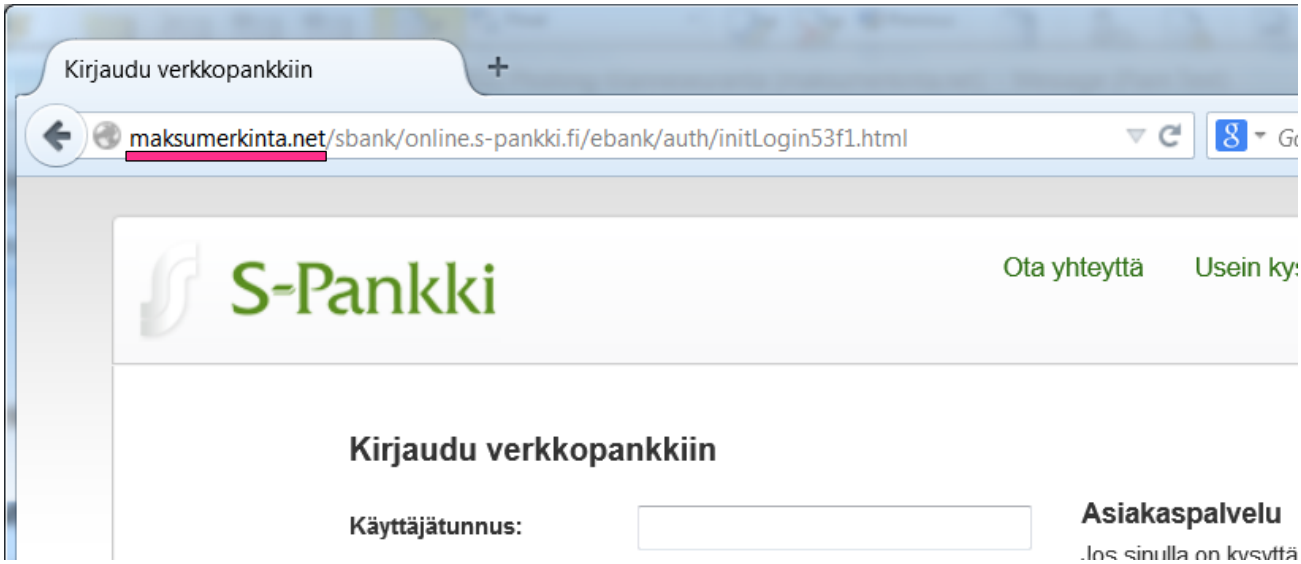
Opettele erottamaan tietojenkalastelusivut tarkkailemalla, esimerkiksi verkkopankissa tai sosiaalisessa mediassa asioidessasi, miltä oikea verkkotunnus näyttää. Jos olet epävarma verkkotunnuksen aitoudesta, etsi kyseisestä organisaatiosta tietoa hakukoneella ja katso, mitä verkkotunnusta hakukone ehdottaa kyseiselle yritykselle.

Myös verkkotunnusten rakenteesta on hyvä tietää perusteet. Verkkotunnukset koostuvat pistein erotelluista osista. Jokaisessa verkkotunnuksessa on vähintään kaksi osaa. Osia luetaan oikeanpuolimmaisesta vasemmanpuolimmaiseen päin.

Esimerkiksi verkkotunnukset suomi.fi ja asiointitili.suomi.fi kuuluu paitsi päätason fi-alueeseen myös toisen tason suomi.fi-alueeseen. Molemmista tunnuksista ja niissä tapahtuvasta toiminnasta vastaa sama taho, eli suomi.fi-verkkotunnuksen haltija. Sen sijaan esimerkiksi verkkotunnuksella asiointitili.example.com ei ole mitään tekemistä verkkotunnuksen asiointitili.suomi.fi:n kanssa.

Joskus rikolliset hyödyntävät tätä verkkotunnusten oikealta vasemmalle kulkevaa luentajärjestystä rekisteröimällä aidon kuuloisia aliverkkotunnuksia. Esimerkiksi verkko-osoitteella www.nordea.fi.example.com ei ole mitään tekemistä Nordean www.nordea.fi -sivuston kanssa, vaan sitä ylläpitää example.com-verkkotunnuksen haltija.

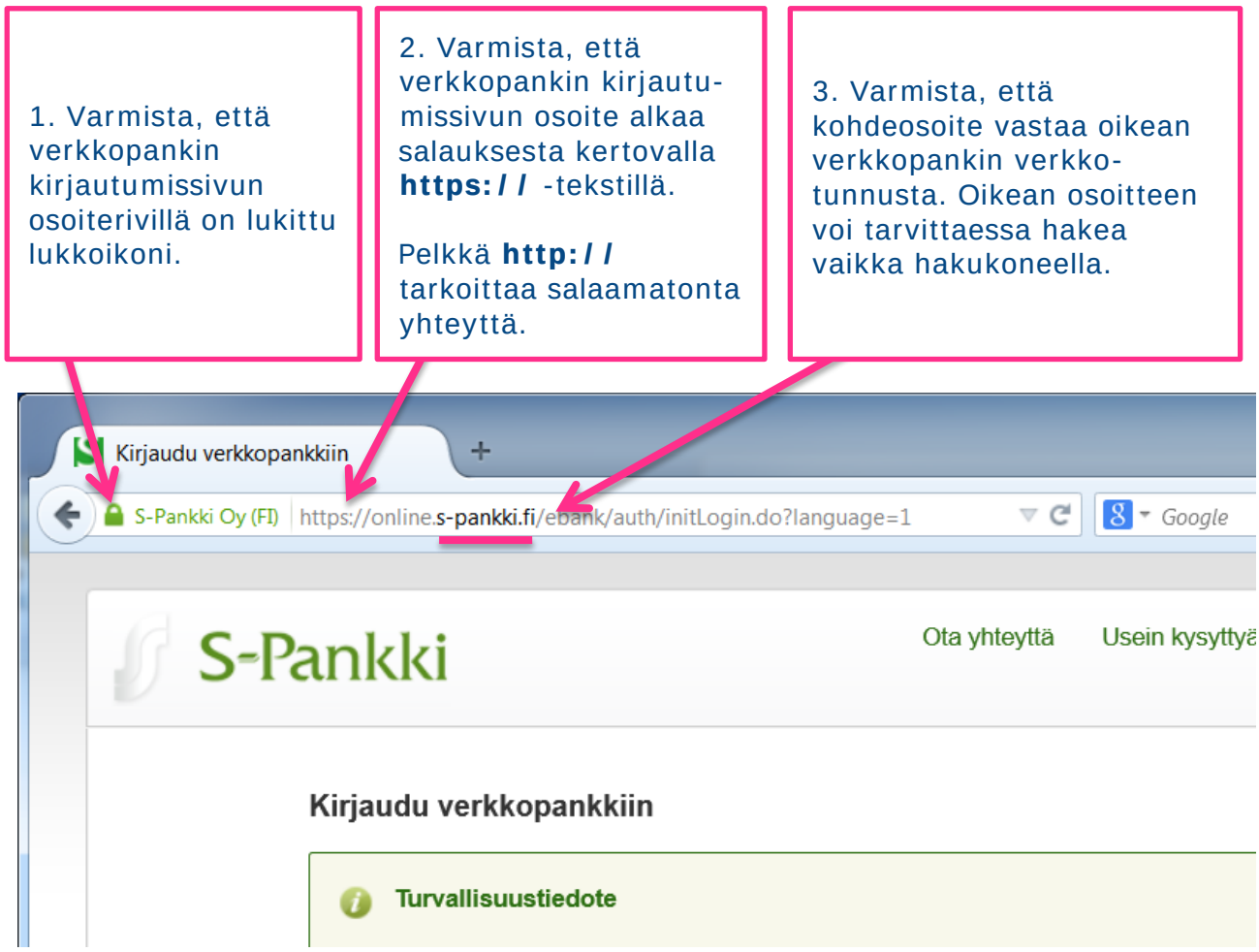
Kuva 4: Kuvassa on sisällön puolesta laadukkaasti toteutettu tietojenkalastelusivu. Huijauksen voi kuitenkin päätellä osoitekentän väärästä verkkotunnuksesta. Myös tietoliikenneyhteyden salausta kuvaava lukittu lukkoikoni puuttuu osoiteriviltä. Kuvan tietojenkalastelusivu on irtikytketty verkosta 10.7.2014.



12 Tarkasta, onko selaimen tietoliikenteen salaus päällä

Verkkopankkien selainliikenne on aina salattu. Selaimen tietoliikenneyhteyden salauksen voi varmistaa selaimen osoiterivin lukkoikonista ja **https://** -alkuisesta verkko-osoitteesta. Jos osoiterivillä ei ole lukkoikonia, voi olla varma, ettei kyseessä ole oikea verkkopankki.

Pelkkä lukkoikoni ei kuitenkaan ole takuu aidosta verkkopankista, siksi myös kohdeosoite tulee tarkistaa selaimen osoiteriviltä. Jos on epävarma oman pankin aidosta verkkotunnuksesta, kannattaa etsiä pankkia hakukoneella.



Kuva 5: Kuvassa on oikea S-Pankin sisäänkirjautumissivu. Oikea verkkotunnus S-Pankille on tällä hetkellä s-pankki.fi. Kuvakaappaus on otettu 22.7.2014.

13 Ilmoita huijaussivustosta

Epäilyttävistä viesteistä tai sivustoista kannattaa ilmoittaa Viestintävirastolle. Viraston Kyberturvallisuuskeskus voi välittää tiedon toimivaltaisille tahoille, jotta huijaussivustot saataisiin kytkettyä pois internetistä.

Viestintäviraston Kyberturvallisuuskeskukseen voi lähettää vinkkejä huijausviesteistä tai -sivustoista sähköpostiosoitteeseen: cert@viestintavirasto.fi

Yhteystiedot:
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi