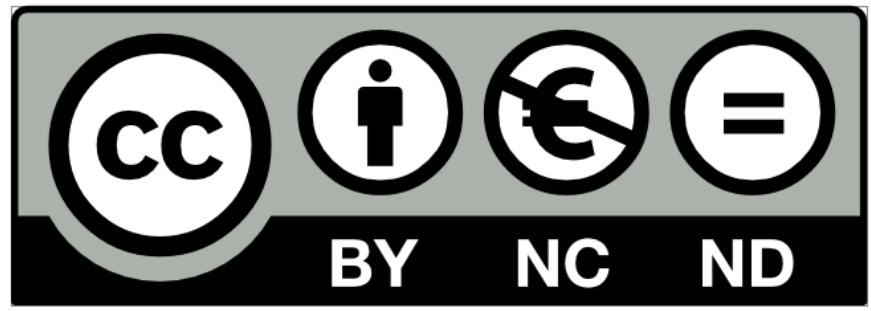
Varo sähköpostihui-jauksia

Peruskäyttäjälle.net

Ohjeen versio 1.4.2021



Tämä teos on lisensoitu **Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen** -lisenssillä. Tarkastele lisenssiä osoitteessa https://creativecommons.org/licenses/by-nc-nd/4.0/deed.fi

Voit jakaa tätä teosta, kunhan mainitset selkeästi sen alkuperäksi ja tekijäksi Peruskäyttäjälle.net -sivuston.

- ➔ Peruskäyttäjälle.netin Creative Commons-esittely (https://peruskayttajalle.net/tietoja.php#cc)
- ➔ Lisätietoa Creative Commonsista suomeksi (https://creativecommons.fi/)

Sisällysluettelo

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

1 Johdanto

Erilaiset tietojenkalastelu- ja huijausviestit ovat useille sähköpostin käyttäjille arkipäivää. Näiden viestien taso vaihtelee ja pitkään suomenkieliset viestit olivat epäuskottavia, koska ne oli usein kirjoitettu huonolla suomen kielellä. Nykyään suomenkieliset huijausviestit voivat olla kieliasultaan lähes moitteettomia, mikä voi harhauttaa viestin vastaanottajaa.

Tässä ohjeessa käydään läpi mm. huijauksen tunnistaminen, hakukoneiden uudelleenohjauksen väärinkäyttäminen ja nettisivuston osoitteen väärentäminen käyttäjien hämäämiseksi.

2 Huijauksen tunnistaminen

Kaikki huijaukset perustuvat psykologiaan. Käytännössä huijauksissa pyritään aikaansaamaan jokin tunnereaktio, esimerkiksi innostus tai säikähdys. Tällä pyritään siihen, että uhri ei ala miettimään asiaa sen tarkemmin, vaan toimii huijareiden haluamalla tavalla.

Huijauksissa käytetään tyypillisesti kolmea keinoa. Ensimmäinen keino on tarjota uhrille jotain tuotetta ilmaiseksi tai poikkeuksellisen halvalla. Tähän pätee se vanha sääntö, että jos jokin vaikuttaa liian hyvältä ollakseen totta, se ei ole totta.

Toinen keino on painostaa uhria toimimaan nopeasti jollakin verukkeella. Yksi esimerkki tällaisesta ovat huijausviestit, joissa uhataan esimerkiksi jonkin verkkopalvelun tilin sulkemisella, ellei uhri ota nopeasti yhteyttä napsauttamalla viestissä olevaa linkkiä. Myös jonkin tarjouksen voidaan väittää olevan voimassa vain hyvin lyhyen aikaa.

Tällaisissa tapauksissa pitää ehdottomasti pitää pää kylmänä. Painostaminen ja kiireen luominen ovat erittäin yleisiä huijauksissa käytettyjä keinoja.

Kolmas keino on auktoriteetin käyttäminen huijauksessa. Huijauksissa voidaan käyttää niin viranomaisia kuin julkisuuden henkilöitä. Auktoriteetteja käyttämällä huijarit pyrkivät hankkimaan luottamusta.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Esimerkiksi useissa virtuaalivaluuttahuijauksissa on hyödynnetty julkisuuden henkilöitä. Näissä huijauksissa jonkun julkisuuden henkilön on väitetty rikastuneen sijoittamalla johonkin virtuaalivaluuttaan, tyypillisesti Bitcoiniin.

Näissä huijauksissa on käytetty eri medioiden, kuten Iltalehden, väärennettyä nettisivustoa, jossa on julkaistu tekaistu juttu julkisuuden henkilön äkkirikastumisesta virtuaalivaluuttaan sijoittamalla.

Nettisivun ulkoasua ei voi koskaan pitää merkkinä luotettavuudesta, koska minkä tahansa nettisivun ulkoasu on kopioitavissa. Yleensä erilaisten tietojenkalastelu- ja huijaussivustojen ulkoasu on kopioitu oikeasta verkkopalvelusta.

Siksi on ehdottoman tärkeää tarkistaa linkin todellinen osoite ennen linkin napsauttamista. Jos linkki on jo avattu, ensimmäiseksi tulee tarkistaa nettiselaimen osoiteriviltä nettisivun verkkotunnus eli osoite (esimerkiksi *peruskayttajalle.net*).

Joissakin tapauksissa tietojenkalastelusivuston verkkotunnus on samantapainen kuin oikean nettisivuston verkkotunnus tai se voi sisältää asiaan liittyviä sopivia sanoja. Myös vanhentuneiden verkkotunnusten kaappaaminen on vanha keino harhauttaa käyttäjiä.

Kaikki verkkotunnusten varaukset ovat voimassa määräaikaisesti. Jos verkkotunnuksen senhetkinen omistaja ei uusi verkkotunnuksen varausta ajoissa, verkkotunnus vapautuu ja sen voi hankkia kuka tahansa.

Nykyään huijauksissa hyödynnetään myös luotettavien toimijoiden palveluita. Huijarit ovat keksineet hyödyntää esimerkiksi Microsoftin Office.com -verkkopalvelua kaapatakseen käyttäjien salasanoja. Käytännössä tämä tapahtuu luomalla uskottavan näköinen ”kirjautumissivu”. Myös Google Forms -lomakepalvelua on hyödynnetty samaan tarkoitukseen.

Tämän kaltaisilta huijauksilta välttymiseen auttaa ainoastaan se, että varoo napsauttamasta mitään vähänkään epäilyttäviä linkkejä. Tarvittaessa mihin tahansa verkkopalveluun kannattaa kirjautua menemällä varmasti aidoiksi tiedetyille palvelun nettisivuille ja hoitamalla kirjautuminen sitä kautta.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Esimerkiksi Gmailiin voi kirjautua kirjoittamalla nettiselaimen osoiteriville osoitteen *gmail.com* ja Outlookiin osoitteella *outlook.com*.

Jos on pieninkin epäilys siitä, onko nettisivusto luotettava, kannattaa asia tarkistaa. Olen tehnyt ohjeen Nettisivustojen luotettavuuden arviointi (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php).

Jos kyse on lyhytlinkistä, tarkista lyhytlinkin todellinen osoite aina ennen linkin napsauttamista. Lyhytlinkki on linkki jollekin nettisivulle, jonka osoite on lyhennetty lyhytlinkkipalvelulla (esimerkiksi Google URL Shortener, Bitly, TinyURL.com). Olen tehnyt ohjeen Tarkista lyhytlinkkien todellinen osoite (https://peruskayttajalle.net/ohjeet/lyhytlinkki.php).

Myöskään viestin lähettäjän sähköpostiosoitteeseen ei voi luottaa, koska lähettäjän osoite on mahdollista väärentää. Erääseen sähköpostiosoitteeseeni tulee säännöllisesti tietojenkalastelu- ja huijausviestejä, joiden lähettäjän sähköpostiosoite on väärennetty.

Huom! Se, että jollakin nettisivustolla on käytössä salattu HTTPS-yhteys, ei tee nettisivustosta itsessään luotettavaa. Koska varsin moni käyttäjä yhdistää HTTPS-yhteyden turvalliseen ja luotettavaan nettisivustoon, ovat monet tietojenkalastelu- ja huijaussivustot ottaneet HTTPS-yhteyden käyttöön.

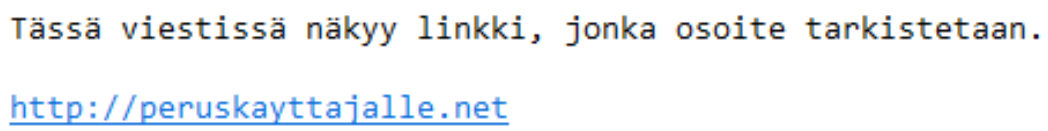
HTTPS-yhteyden käyttöön vaadittavan sertifikaatin voi hankkia käytännössä kuka tahansa. Sertifikaatteja on eritasoisia niiden turvallisuuden mukaan ja alimman tason sertifikaattien hankintaa ei rajoiteta tai valvota mitenkään.

3 Sähköpostiviestien ulkoasu

Sähköpostiviestien ulkoasu vaihtelee sen mukaan, missä muodossa viesti näytetään. Sähköpostiviesteissä on olemassa kaksi muotoa: teksti- ja HTML-muoto.

Tekstimuotoisissa viesteissä tekstiä ei ole muotoiltu (esimerkiksi muutettu fonttia ja tekstin kokoa) ja linkin todellinen osoite on aina näkyvissä (kuva 1).

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä



Kuva 1

HTML-muotoisissa viesteissä tekstiä on mahdollista muotoilla (esimerkiksi muuttaa fonttia ja tekstin kokoa) ja piilottaa linkin osoite (kuva 2).

Kuva 2

Tekstimuotoisissa viesteissä huijaaminen on luonnollisesti vaikeampaa, koska linkin todellinen osoite on aina näkyvissä, toisin kuin HTML-muotoisissa viesteissä.

4 Linkkien todellisen osoitteen tarkistaminen

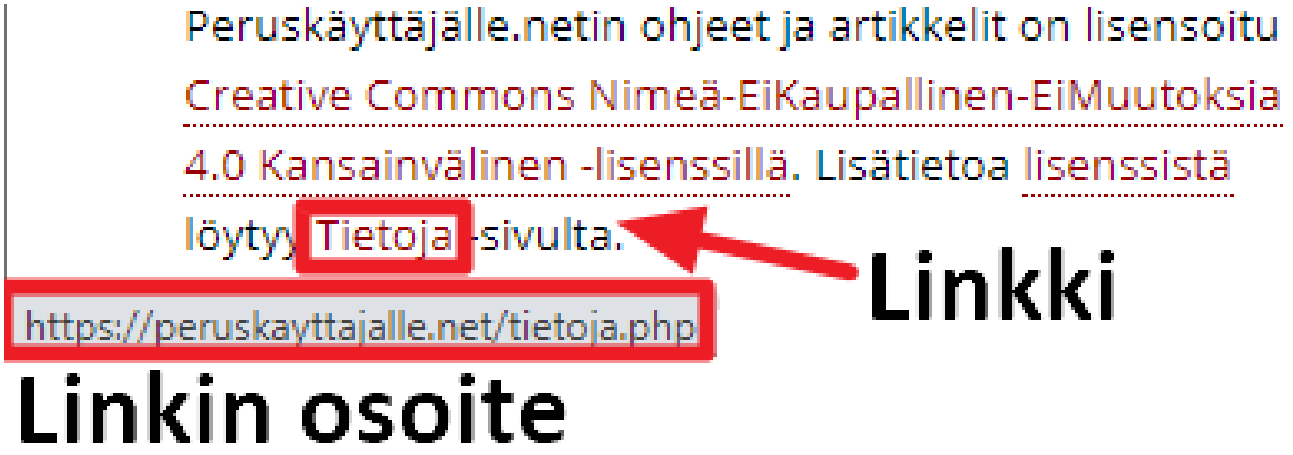
Sähköpostiohjelmissa (esimerkiksi Outlook, Mozilla Thunderbird) on yleensä helppoa selvittää linkin todellinen osoite viemällä hiiren osoitin linkin päälle, jolloin ikkunaan ilmestyy näkyviin linkin osoite.

Webmailissa eli nettiselaimella luettavassa sähköpostissa (esimerkiksi Gmail, Outlook.com) linkkien todellisen osoitteen tarkistaminen on myös yhtä helppoa. Tarvittaessa voit myös kopioida linkin osoitteen, jos haluat tarkistaa linkistä löytyvän nettisivuston luotettavuuden.

Yleensä nettiselaimissa minkä tahansa linkin todellisen osoitteen voi tarkistaa viemällä hiiren osoittimen linkin päälle, jolloin nettiselaimen ikkunan alalaitaan ilmestyy näkyviin linkin osoite. Esimerkissä linkin osoite on *https://peruskayttajalle.net/tietoja.php* (kuva 3).

Älypuhelimien nettiselaimissa tilanne vaihtelee. Linkin osoitteen voi saada näkyviin painamalla linkkiä pitkään. Tämä kuitenkin vaihtelee eri älypuhelimissa niin valmistajan kuin älypuhelimen käyttöjärjestelmän ja nettiselaimen version mukaan.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

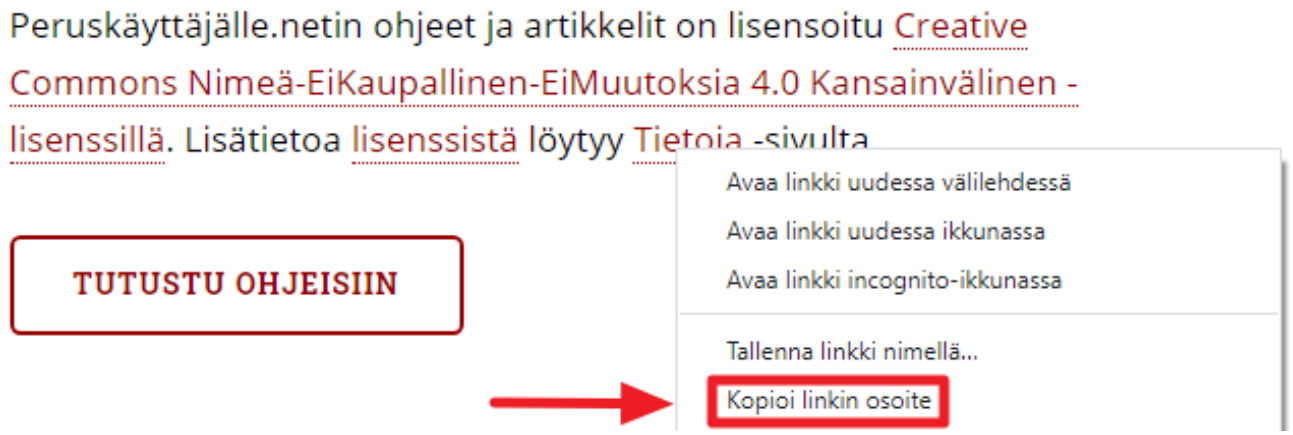


Kuva 3

Tarvittaessa linkin osoite on mahdollista kopioida. Linkin osoitteen kopioiminen vaihtelee nettiselaimittain. Jos et ole varma, mitä nettiselainta käytät, Peruskäyttäjälle.netistä löytyy linkki (https://peruskayttajalle.net/linkkeja.php#selain) asian tarkistamiseen.

Taaskin älypuhelimien nettiselaimissa tilanne vaihtelee. Linkin osoite voi olla mahdollista kopioida painamalla linkkiä pitkään ja avautuvasta valikosta pitäisi löytyä sopiva vaihtoehto linkin kopioimiselle.

Tietokoneella useimmissa nettiselaimissa linkin voi kopioida napsauttamalla linkkiä hiiren oikealla ja avautuvasta valikosta valitse kohta **Kopioi linkki** tai **Kopioi linkin osoite** (kuva 4).



Kuva 4

Tarvittaessa voit tarkistaa linkin takaa löytyvän nettisivuston luotettavuuden helposti erilaisten verkkopalveluiden avulla. Olen tehnyt ohjeen Nettisivustojen luotettavuuden arviointi (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php).

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

5 Hakukoneiden uudelleenohjaukset

Google ja myös muut hakukoneet käyttävät uudelleenohjausta mm. linkkien napsautusten seurantaan. Valitettavasti tätä uudelleenohjaustoimintoa voi myös käyttää väärin.

Uudelleenohjauksessa linkin todellinen osoite löytyy linkin loppupuolelta. Esimerkiksi Google-haku *peruskayttajalle.net* antaa ensimmäiseksi tulokseksi Peruskäyttäjälle.netin etusivun. Tällöin uudelleenohjauksen linkin osoite on:

https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjg-xZvlpJrWAhXnDpoKHWNACSwQFggrMAA&url=https%3A%2F%2Fperuskaytta-jalle.net%2F&usg=AFQjCNHtmNsESLu8OjYgEDsqi2AR1ewLLQ

Linkin todellinen osoite eli *https://peruskayttajalle.net* löytyy merkinnän *&url=* jälkeen. Linkin osoitteessa oleva merkintä *%3A* tarkoittaa kaksoispistettä (:) ja merkintä *%2F* kauttaviivaa (/). Koska kauttaviivoja on kaksi peräkkäin, myös merkintöjä *%2F* on kaksi peräkkäin.

Vastaavasti Peruskäyttäjälle.netin Ohjeet -sivun linkin osoite on Googlen uudelleenohjauksessa seuraava:

https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0ahUKEwjg-xZvlpJrWAhXnDpoKHWNACSwQFghIMAU&url=https%3A%2F%2Fperuskaytta-jalle.net%2Fohjeet.php&usg=AFQjCNEH2sspsSO58m1SxRnGaV3BuonuBw

Tällöin *https://peruskayttajalle.netin* perässä on kauttaviiva (merkintä *%2F*), jonka perässä on Ohjeet -sivun osoite eli *ohjeet.php*. Koko osoite on siis *https://peruskayttajalle.net/ohjeet.php*.

Muiden hakukoneiden uudelleenohjaukset ovat samankaltaisia. Esimerkiksi Yahoon uudelleenohjauksen linkin alussa lukee *search.yahoo.com* ja todellinen osoite on vasta linkin loppupuolella.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

6 Osoitteen väärentäminen

Yksi hyvin yleinen keino väärentää osoite näyttämään aidolta on vaihtaa kirjaimia numeroihin. Esimerkiksi kirjain O voidaan vaihtaa numeroksi 0 ja kirjain L numeroksi 1. Toinen mahdollisuus on hyödyntää *internationalized domain name* -verkkotunnuksia (lyhenne *IDN*).

IDN-verkkotunnuksissa verkkotunnus sisältää vähintään yhden ns. kansallisen merkin, kuten Å, Ä tai Ö. Koska ns. kansallisia merkkejä on hyvin paljon, löytyy niistä useita latinalaisia aakkosia muistuttavia merkkejä. Tällaisia ovat esimerkiksi kyrillisten kirjainten A ja E.

Tällaiset huijaukset voivat olla hyvin vaikeita havaita, koska kaikki nettiselaimet eivät muuta ns. kansallisia merkkejä verkkotunnuksessa punycode-muotoon. Tällöin esimerkiksi verkkotunnus *ää.fi* näkyy nettiselaimen osoiterivillä punycode-muodossa *xn--4ca0b.fi*.

7 Esimerkkejä huijausviesteistä

Huijausviestejä voi nähdä mistä tahansa aiheesta. Huijarit yrittävät saada itselleen rahan lisäksi käyttäjätunnuksia ja salasanoja, verkkopankkitunnuksia, luottokorttien tietoja ja myös henkilötietoja. Käytännössä huijareille kelpaa rahan lisäksi kaikki tieto, minkä voi muuttaa rahaksi jollakin tavalla.

Henkilötiedot ovat rikollisille rahanarvoista tavaraa, koska henkilötietoja voi esimerkiksi hyödyntää identiteettivarkauksissa tai muiden rikosten yhteydessä. Rikolliset myös myyvät hankkimiaan tietoja muille rikollisille.

Usein identiteettivarkaudessa uhrin henkilötietoja hyödynnetään ostamalla luotolla tavaraa, joka sitten myydään eteenpäin. Tällöin uhri joutuu kärsimään seurauksista, kun maksamattomia maksuja aletaan perimään.

Myös tietojenkalastelu on hyvin yleistä. Tietojenkalastelussa yritetään saada uhri luovuttamaan esimerkiksi käyttäjätunnuksensa ja salasanansa huijaussivulle, joka matkii oikeaa verkkopalvelun kirjautumissivua. Myös verkkopankkitunnuksia kalastellaan.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Huom! Esimerkkien linkkien alkuosa on muutettu tietoturvasyistä muotoon *hxxp* tai *hxxps*. Tämä johtuu siitä, ettei linkkejä voi avata vahingossa. Oikeasti linkkien alkuosa on muodossa *http* tai *https*.

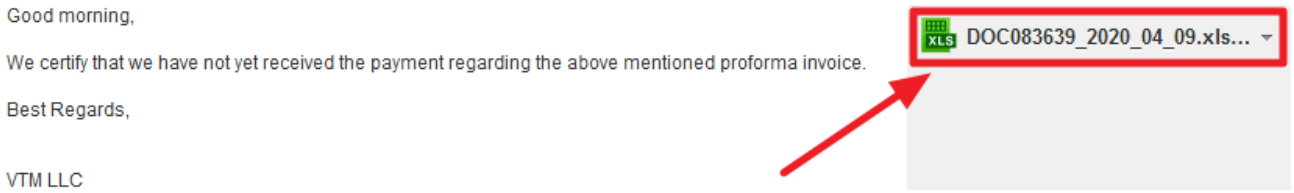
7.1 Ole varovainen sähköpostin liitetiedostojen kanssa

Esimerkissä kuvassa 5 viestin liitteenä on Excel-taulukko, joka on tosiasiassa haittaohjelma. Tällaisia viestejä lähetetään millä tahansa aiheilla. Liitetiedostojen kanssa tulee aina olla hyvin varovainen.

Se että viesti näyttää tulevan tutulta tai muutoin luotettavalta lähettäjältä, ei tee viestistä tai liitetiedostosta luotettavaa. Sähköpostin lähettäjä on helppo väärentää. Myös lähettäjän sähköpostitili on voinut joutua vääriin käsiin.

Liitetiedostoissa ei voi luottaa siihen, mikä niiden tiedostomuoto näyttäisi olevan, koska liitetiedostojen tiedostomuoto on helppo väärentää. Todellisuudessa harmittomalta näyttävä liitetiedosto voi sisältää haittaohjelmia (esimerkiksi virukset ja troijalaiset).

Liitetiedostojen kohdalla kannattaa tarvittaessa kysyä lähettäjältä, onko hän lähettänyt kyseisen viestin ja liitetiedoston. Yhteyttä lähettäjään ei pidä ottaa sähköpostitse, vaan esimerkiksi soittamalla lähettäjälle.



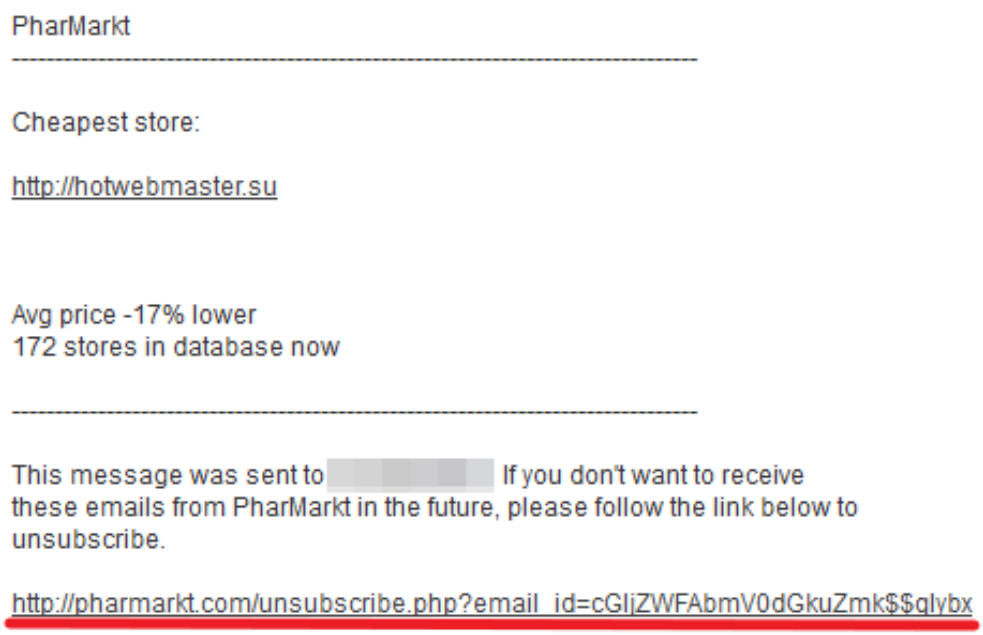
Kuva 5

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

7.2 Älä vastaa huijausviesteihin

Esimerkissä kuvassa 6 on tavanomainen lääkkeitä kaupitteleva huijausviesti, johon on lisätty muka mahdollisuus poistua postituslistalta. Huijausviesteihin tai muuhun roskapostiin ei pidä koskaan vastata.

Vastaaminen kertoo huijareille ja roskapostittajille, että kyseinen sähköpostiosoite on käytössä. Tämä johtaa vain entistä suurempaan määrään roskapostia.


PharMarkt

Cheapest store:

http://hotwebmaster.su

Avg price -17% lower
172 stores in database now

This message was sent to [redacted] If you don't want to receive these emails from PharMarkt in the future, please follow the link below to unsubscribe.

http://pharmarkt.com/unsubscribe.php?email_id=cGljZWFAbmV0dGkuZmk$$qlybx

Kuva 6

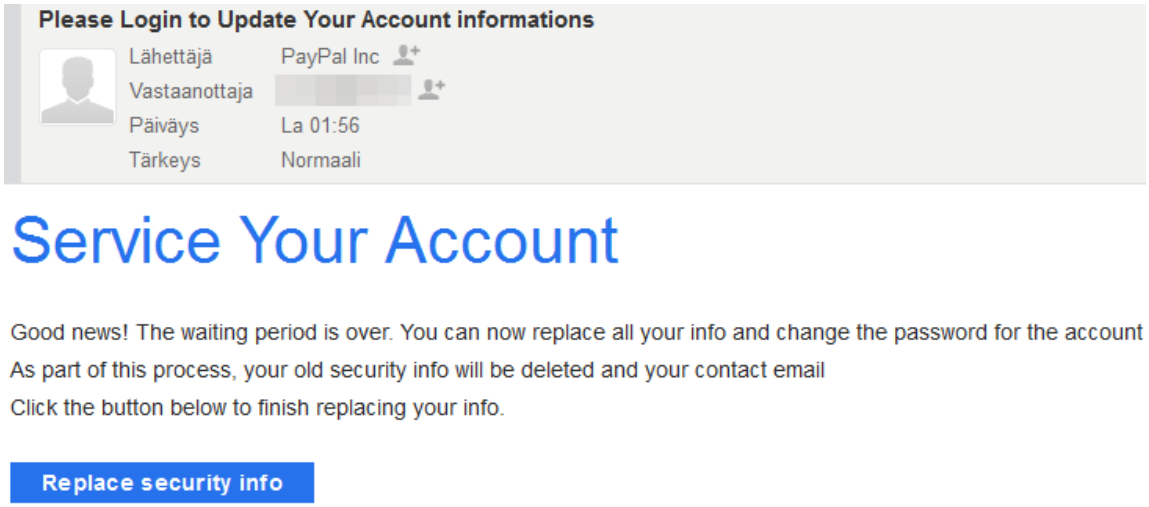
7.3 Käyttäjätunnusten kalastelu

Esimerkissä huijausviestillä yritetään kalastella PayPalin käyttäjätunnuksia. Kuvassa 7 on huijausviesti HTML-muodossa, jolloin kohdan **Replace security info** linkin todellista osoitetta ei näe suoraan ja viestiä voi pitää kohtalaisen uskottavana.

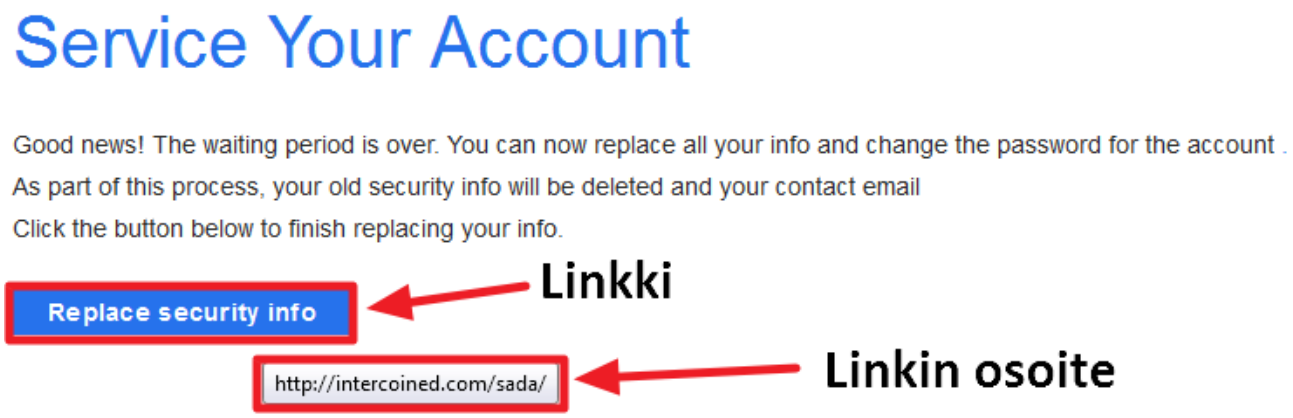
Koska kyseinen viesti on tullut webmailiin eli nettiselaimella luettavaan sähköpostiin, onnistuu linkin todellisen osoitteen tarkistaminen helposti. Tällöin tarvitsee ainoastaan viedä hiiren osoitin kohdan **Replace security info** päälle, jolloin nettiselaimen ikkunan alalaitaan ilmestyy näkyviin linkin osoite.

Esimerkissä linkin osoite on *hxxp://intercoined.com/sada/* (kuva 8).

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä



Kuva 7



Kuva 8

Minkä tahansa palvelun käyttäjätunnuksia voidaan kalastella. Yleisesti ottaen suosiossa ovat suuret verkkopalvelut ja yritykset. Tämän kaltaisiin viesteihin pitää aina suhtautua suurella varovaisuudella.

Suurin osa tämän kaltaisista viesteistä on huijausta. Jos epäilet vähänkään viestin aitoutta, kirjaudu kyseiseen palveluun nettiselaimen kautta. Jos kuitenkin napsautat linkkiä, tarkista sivun osoite huolellisesti nettiselaimen osoiteriviltä.

Tietojenkalastelussa osoite voi olla pikaisella vilkaisulla samanlainen kuin oikean palvelun osoite. Lisäksi huijaussivuston osoite voi olla hämäyksen takia aliverkkotunnus, esimerkiksi *kirjaudu.tästä.palveluun.huijaussivusto.com*.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

7.4 Virtuaalivaluuttahuijaus

Esimerkissä on perinteisempi huijausviesti, jossa ei ole linkkejä. Kuvassa 9 näkyy osa viestistä. Kyseisessä viestissä mainostetaan virtuaali- eli kryptovaluutta Swisscoinia.

This crypto coin could go up fifty thousand percent this year

Lähettäjä Nora Udall
Vastaanottaja
Päiväys 14.1.2018 07:16

Dear

If you don't already own a few coins of something, then surely at the very least, you must have heard about cryptocurrencies.

Bitcoin, the most famous one, minted countless multimillionaires but did you know that altcoins (bitcoin alternatives) are responsible for even more riches?

Among the "big" ones, NEM went up almost 10,000 percent and Ethereum, more than 4,000 percent

Among the small and unknown ones several gained more than 50,000 percent.

To put this in perspective, a small 1,000-dollar coin purchase in one of these small ones could have turned into more than 50 million bucks.

It seems crazy, doesn't it? Well, it's the reality of the cryptocurrency market today.

Raiblocks, a relatively obscure coin at the time, went from 0.20 on December first to $20 by New Year's Eve. It is now in the top 20 largest coins in the world.

All that to say, the next big winner could be found anywhere, and today I believe I've identified the next one.

After spending hundreds of hours looking at hundreds of different coins, I locked down on one specific target.

Swisscoin.

Kuva 9

Virtuaalivaluutoista löytyy tietoa mm. Wikipediasta (https://fi.wikipedia.org/wiki/Kryptovaluutta ja https://fi.wikipedia.org/wiki/Bitcoin). Esimerkin huijauksessa on klassisen huijauksen tunnusmerkit. Sijoitukselle luvataan täysin epärealistista tuottoa (Swisscoinin mahdollinen arvonnousu yli 50000 prosenttia vuoden loppuun mennessä) ja luodaan mielikuva mahdollisuudesta äkkirikastua.

Tämän kaltainen huijaus perustuu siihen, että huijarit ovat ostaneet itselleen virtuaalivaluuttaa jo aiemmin ja yrittävät saada mahdollisimman monen ihmisen ostamaan samaista virtuaalivaluuttaa, jolloin sen arvo nousee. Kun arvo on noussut tarpeeksi, huijarit myyvät omistamansa virtuaalivaluutan.

Huijarit ovat kiinnostuneet virtuaalivaluutoista, koska kaikkien aikojen ensimmäisen virtuaalivaluutan eli Bitcoinin arvo nousi räjähdysmäisesti vuonna 2017. On esitetty epäilyksiä siitä, että Bitcoinin arvo nousi manipulaation seurauksena.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Tällä hetkellä virtuaalivaluuttoja ei säädellä tai valvota mitenkään eivätkä ne ole myöskään virallisia valuuttoja tai maksuvälineitä. Siksi niihin kannattaa suhtautua varauksella.
Mm. Yle on uutisoinut virtuaalivaluutoista ahkerasti:

- Maailman kryptovaluuttojen arvo on jo liki 700 miljardia dollaria – asiantuntijat kertovat, mitä kryptohuuma tuo tullessaan (https://yle.fi/uutiset/3-10012902)
- Kryptokriittisyys leviää – Facebook kieltää kryptovaluuttojen mainostamisen (https://yle.fi/uutiset/3-10050666)
- Kryptovaluutta BitConnectia epäillään pyramidihuijaukseksi – markkinointimiehen maanisesta esiintymisestä tuli meemi (https://yle.fi/uutiset/3-10050772)

7.5 Kiristyshuijaus

Esimerkissä on ns. pornokiristysviesti. Viestissä väitetään kiristäjän murtautuneen uhrin tietokoneelle ja tallentaneen tietokoneen kameralla uhrin vierailut pornosivustoilla. Kiristäjä haluaa rahaa vastineeksi siitä, ettei julkaise keräämiään tietoja.

Viestistä on eri versioita, joita lähetetään suomen- ja englanninkielisinä. Yhdessä versiossa esimerkiksi väitetään murtautujan lisäksi asentaneen tietokoneeseen troijalaisen, joka on yksi haittaohjelmatyypeistä. Kuvassa 10 näkyy osa esimerkkiviestistä.

Hei!

Tämä on sinulle tärkeää tietoa!

Muutama kuukausi sitten hakkasin käyttöjärjestelmäsi ja sain täydellisen hallinnan tilistäsi [ ]

Voit siis vaihtaa salasanan, kyllä .. Tai jo muuttunut ...
Haittaohjelmani kuitenkin kirjoittaa sen uudelleen.

Miten tein sen:
Reitittimen ohjelmistossa, jonka kautta menit verkossa, oli haavoittuvuus. Käytin sitä ...
Jos olet kiinnostunut, voit lukea siitä: CVE-2019-1663 - haavoittuvuus Cisco-reitittimien web-pohjaisessa hallintaliittymässä.
Ensinnäkin, löysin reitittimen etäyhteyden ja laitoin koodin siihen.
Kun menit verkkoon, troijalainen asennettiin laitteen käyttöjärjestelmään.

Tämän jälkeen tein levyn täydellisen varmuuskopion (minulla on kaikki osoitekirjasi, sivustojesi katseluhistoria, kaikki tiedostot, puhelinnumerot ja kaikkien yhteystietojen osoitteet)

Kuukausi sitten halusin lukita laitteen. Pyydä sitten BTC (bitcoin) antamaan sinulle lukituksen.
Mutta katsoin sivustoja, joita käyt säännöllisesti, ja olin järkyttynyt siitä, mitä näin!
Puhun sinulle aikuisten sivustoista.

Haluan sanoa - olet BIG perverssi. Fantaasiasi on siirretty kaukana normaalista kurssista!

Ja minulla on idea.
Tein kuvakaappauksen aikuisten sivustoista, joita olet katsonut.
Sen jälkeen tein kuvakaappauksen iloistasi/itsetyydytys (käyttämällä laitteen kameraa) ja liimattu ne yhteen.
Osoittautui hämmästyttäväksi! Olet niin mahtava!

Kuva 10

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Todellisuudessa kiristäjä ei ole murtautunut tietokoneelle, asentanut haittaohjelmaa tai tallentanut mitään tietoja. Kyseessä on puhdas roskaposti, jota on lähetetty maailmanlaajuisesti suurelle joukolle ihmisiä. Viestiin ei kannata reagoida mitenkään vaan poistaa se.

7.6 Nettikasinohuijaus

Esimerkissä on pitkään jatkuneen suomenkielisen roskapostikampanjan viesti. Viesteissä on mainostettu mm. nettikasinoita ja lainoja. Joissakin viesteissä on myös väitetty Vesa-Matti Loirin tarjoavan ilmaiseksi pelikierroksia nettikasinoilla.

Viesteissä on aina linkkejä, jotka ohjaavat kaikki samaan verkkotunnukseen. Kyseessä on tyypillinen roskaposti- ja huijauskampanja, sillä käytettävät verkkotunnukset ovat vaihtuneet usein. Esimerkissä kuvassa 11 käytetään verkkotunnusta *hxxp://olet-voittaja.com*.

Sinä olet Voittaja - Siksi palkitsemme sinut tällä edulla:

Saat 11 kierrosta ilman talletusta ja 275 euroa uuteen nettikasinoon

El Jefe

CasinoJEFEllä on sinulle lahja, joka sisältää 11 ilmaiskierrosta. Avaa ilmainen pelitili ja kierrokset ovat sinun!

Saat myös mainion tervetuliaispaketin, josta saat pelirahaa jopa 275 euron edestä. Toimi näin:

1. Tee ensimmäinen talletuksesi ja saat 100 % bonuksen 100 € asti
2. Tee toinen talletuksesi ja saat 50 % bonuksen 100 € asti
3. Tee kolmas talletuksesi ja saat 75 % bonuksen 75 € asti

Klikkaa tästä ja lunasta tervetuliaislahjasi CasinoJEFEllä tänään!

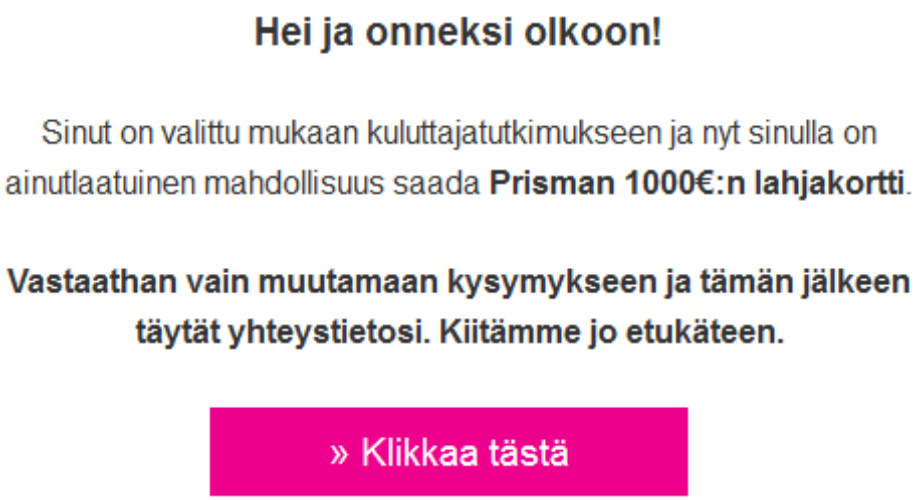
Kuva 11

7.7 Arvonta- ja lahjakorttihuijaukset

Esimerkissä kuvassa 12 on Prisman lahjakorttihuijausviesti. Huijausviestejä arvonnasta tai lahjakortista lähetetään minkä tahansa yrityksen nimissä. Kyseessä voi olla tilausansa tai tietojenkalastelu. Tilausansassa tarjotaan jotakin tyypillisesti arvokasta tuotetta ilmaiseksi tai poikkeuksellisen halvalla.

Tuotteen saadakseen huijarit haluavat uhrin luottokortin tiedot. Tietojen antaminen johtaa kuukausittaisiin veloituksiin uhrin luottokortilta. Tilausansasta ei ole myöskään helppoa päästä eroon.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

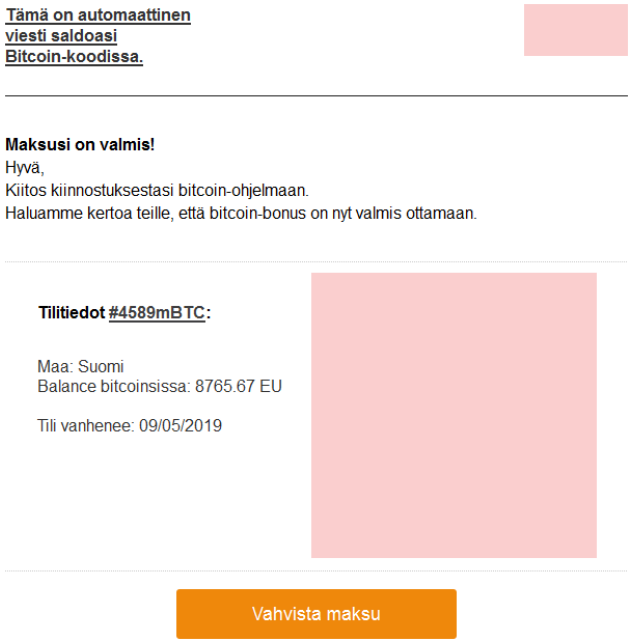


Kuva 12

7.8 Toisenlainen Bitcoin-huijaus

Esimerkissä on Bitcoin-huijausviesti. Viestin mukaan vastaanottajalla on Bitcoineja useamman tuhannen euron edestä. Todennäköisesti näissä viesteissä on kyse tietojenkalastelusta. On mahdollista, että tällaisessa huijauksessa yritetään saada kalasteltua henkilötietojen lisäksi myös tilinumero, jonka joutuminen vääriin käsiin on paha asia.

Kuvassa 13 on esimerkki huijausviestistä. Itselleni tulleet huijausviestit ovat olleet ulkoasultaan lähes samanlaisia. Esimerkkikuvassa viestissä olevia kuvia ei ole tietoturvasyistä ladattu, vaan ne näkyvät vaaleanpunaisina.

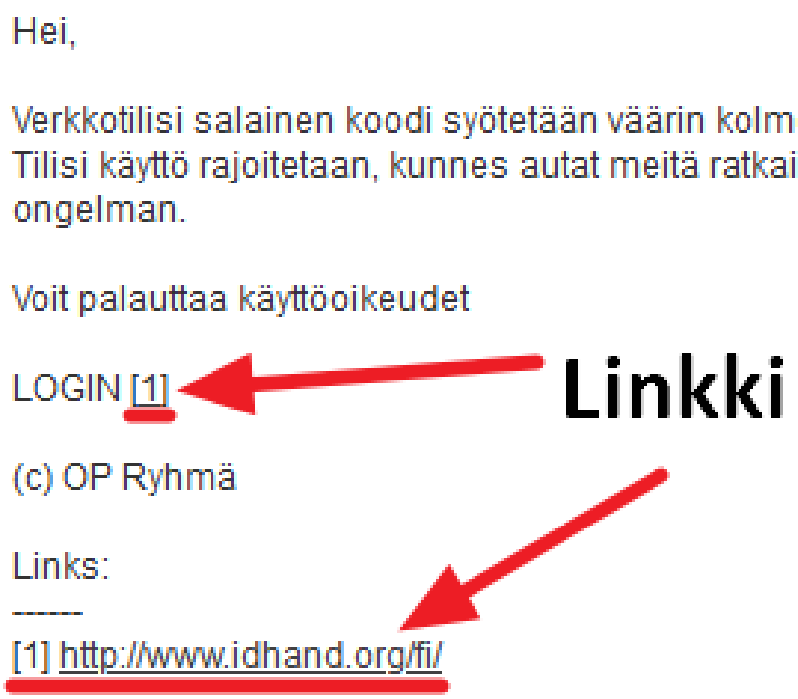


Kuva 13

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

7.9 Verkkopankkitunnusten kalastelu

Esimerkissä yritetään kalastella Osuuspankin pankkitunnuksia väittämällä, että verkkopankki on lukittu. Tässäkin viestissä näkyy, että linkin todellinen osoite on aivan eri kuin Osuuspankin oikea osoite *op.fi*. Kuvassa 14 on viesti tekstimuodossa. Linkin todellinen osoite on *hxxp://www.idhand.org/fi/*.



Kuva 14

Verkkopankkitunnuksia kalastellaan kaikkien pankkien nimissä ja millä tahansa verukkeella. Todellisuudessa pankkien lähettämissä viesteissä ei ole linkkejä. Lisäksi verkkopankkiin ei pidä koskaan kirjautua napsauttamalla mitään linkkiä.

7.10 Äkkirikastuminen tai suuret tulot

Esimerkissä on perinteinen huijausviesti, jossa luvataan suuria tuloja käytännössä ilman mitään vaivannäköä. Tämän kaltaisia viestejä on lähetetty varmaan roskapostituksen alkuajoista lähtien. Edelleenkään äkkirikastuminen tai suurien tulojen saaminen ilman vaivannäköä ei ole mahdollista (kuva 15).

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Hei,

Olen ansainnut vuosien varrella mukavan passiivisen tulon erittäin yksinkertaisella menetelmällä, jonka avulla jokainen aloittelija voi menestyä.

Kun kehitin sen, minulla ei ollut lainkaan kokemusta,
mutta näin tulokset heti...

Ennen pitkää ansaitsin tasaista palkkaa
ilman ponnisteluja.

Nyt jaan menetelmän kanssasi.

Klikkaa tästä aloittaaksesi!!!

Jos et ole kiinnostunut yksinkertaisesta
menetelmästä, joka ansaitsee rahaa nukkuessasi,
jätä tämä sähköposti ystävällisesti huomiotta.

Vain muutama paikka on vapaana, ja
haluan varmistaa, että vain tosissaan olevat,
motivoituneet ihmiset pääsevät mukaan.

Klikkaa Tästä, jos olet motivoitunut

Parhain terveisin,
Jan Beckers

Kuva 15

7.11 Pakettihuijaukset

Pakettihuijausviestejä lähetetään niin Postin kuin kaikkien kuljetusyritysten nimissä. Viestissä väitetään, että vastaanottajalle tulossa olevasta paketista puuttuu toimituskuluja ja että puuttuvat toimituskulut pitää maksaa, ennen kuin paketti voidaan toimittaa.

Yleensä muka puuttuva toimituskulu on summaltaan pieni, muutamia euroja. Näin pieni summa ei herätä niin paljon huomiota kuin jos kyseessä olisi suurempi summa. Siksi suurempi määrä viestin vastaanottajista maksaa summan ajattelematta asiaa enempää.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

Pakettihuijaukset voivat johtaa tilausansaan. Osassa pakettihuijauksia huijarit tyytyvät siihen muutamaan euroon, jonka saavat uhrilta huijattua. Myös pakettihuijauksien kohdalla riskinä ovat huijareille päätyvät tiedot.

Yleensä pakettihuijauksissa maksu pitää maksaa luottokortilla. Huijauksessa voidaan myös yrittää saada haltuun henkilötietoja.

Esimerkissä kuvassa 16 on huijausviesti Postin nimissä.

Kuva 16

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä

8 Toimenpiteet huijatuksi tullessa

Jos kaikesta huolimatta tulit huijatuksi, on tärkeää toimia nopeasti vahinkojen vähentämiseksi. Olen käynyt läpi toimenpiteitä artikkelissa Mitä tehdä jos tulit huijatuksi netissä (https://peruskayttajalle.net/artikkelit.php#toimenpiteet).

Artikkelin toimenpiteiden lisäksi tietokonetta käytettäessä on hyvä suorittaa virustarkistus kaiken varalta. Tämä on tärkeää etenkin, jos huijareilla on ollut pääsy tietokoneelle tai olet ladannut tietokoneelle esimerkiksi sähköpostin liitetiedoston.

Virustorjuntaohjelmat eivät voi millään tunnistaa kaikkia mahdollisia haittaohjelmia, mutta siitä huolimatta virustarkistus on hyvä tehdä. Tarvittaessa tietokone kannattaa viedä ammattilaisen tarkistettavaksi.

© Peruskäyttäjälle.net. Tämä ohje on lisensoitu Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen -lisenssillä