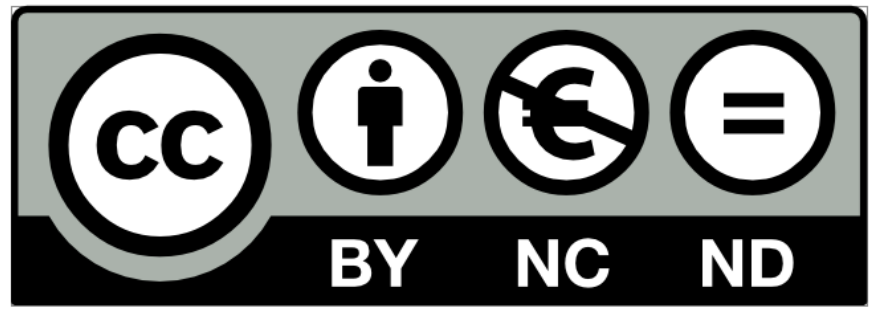
Varo sähköpostihui-jauksia

Peruskäyttäjälle.net

Ohjeen versio 14.10.2018



Sisällysluettelo

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.

Vuodesta 2016 lähtien on ollut meneillään laaja Applen käyttäjätunnuksiin kohdistuva tietojenkalastelukampanja, johon on liittynyt myös verkkopankkitunnusten huijaamista. Koska kyse on varsin hyvin toteutetusta huijauksesta, Viestintävirasto antoi varoituksen huijauksesta jo vuonna 2016 (https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2016/varoitus-2016-03.html).

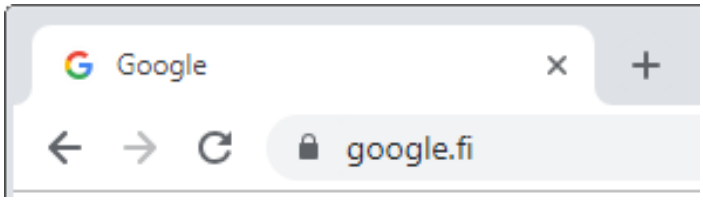
Tässä ohjeessa käydään läpi huijauksen tunnistaminen ja sähköpostiviestin sisältämän linkin osoitteen tarkistaminen webmailissa eli nettiselaimella luettavassa sähköpostissa.

2 Huijauksen tunnistaminen

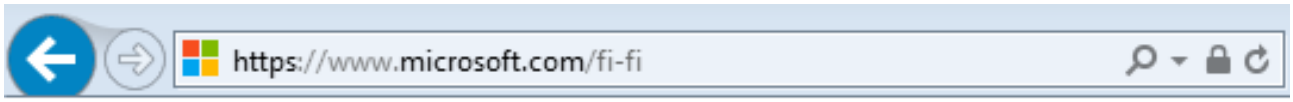
Nettisivun ulkoasua ei voi koskaan pitää merkkinä luotettavuudesta, koska minkä tahansa nettisivun ulkoasu on kopioitavissa. Yleensä erilaisten tietojenkalastelu- ja huijaussivustojen ulkoasu on kopioitu oikeasta verkkopalvelusta.

Siksi on ehdottoman tärkeää tarkistaa linkin todellinen osoite ennen linkin napsauttamista. Jos linkki on jo avattu, ensimmäiseksi tulee tarkistaa, mitä nettiselaimen osoiterivin alussa lukee. Osoiterivin alussa on yleensä vihreä lukon kuva ja sen jälkeen ainoastaan teksti *https*.

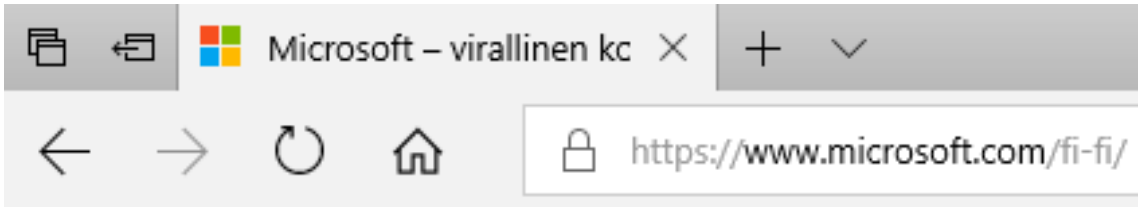
Esimerkeissä Google Chromen osoiterivi (kuva 1), Internet Explorerin osoiterivi, jossa lukon kuva on osoiterivin lopussa (kuva 2), Microsoft Edgen osoiterivi (kuva 3) ja Mozilla Firefoxin osoiterivi (kuva 4).



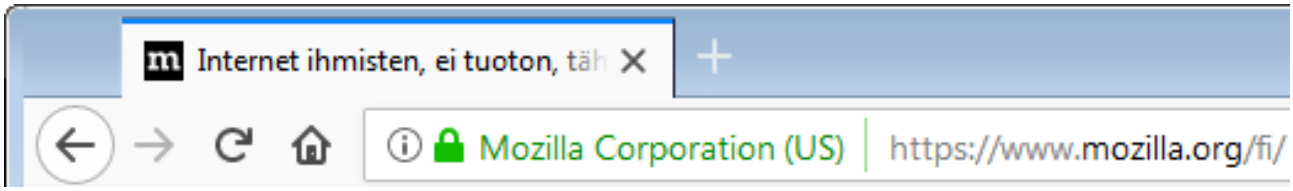
Kuva 1



Kuva 2



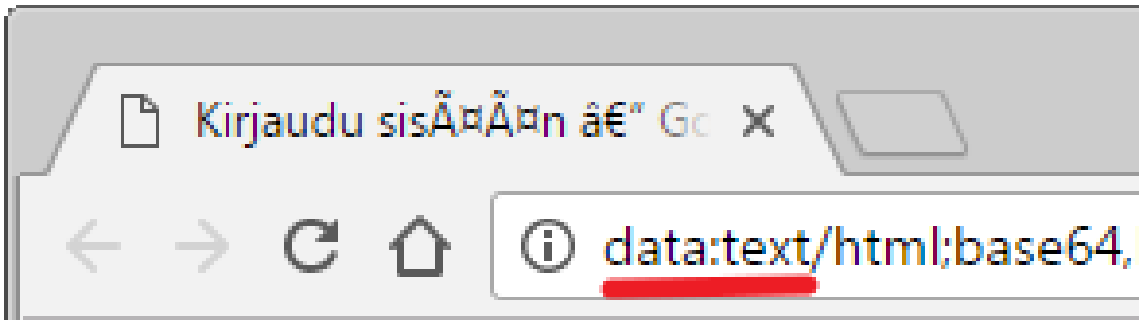
Kuva 3



Kuva 4

Uutena keinona harhauttaa käyttäjiä voidaan käyttää tekniikkaa, jossa osoiterivin alussa lukeekin teksti *data:text* ja vasta tämän jälkeen teksti *https*. Tällöin kyseessä ei ole oikea nettisivu eikä tällaiselle ”sivulle” tule antaa mitään tietoja tai napsauttaa mitään linkkejä.

Esimerkkikuva ei ole aivan samanlainen, mutta samantapainen (kuva 5).



Kuva 5

Uudesta tavasta huijata käyttäjiä ovat kirjoittaneet mm. MTV (https://www.mtv.fi/lifestyle/digi/artikkeli/ala-klikkaa-auki-naita-ystaviesi-lahettamia-viesteja-gmail-kayttajien-tietoja-yritetaan-kalastella/6265966) ja tietoturvayhtiö Wordfence (https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri/).

> **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.

Toiseksi tulee ehdottomasti 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.

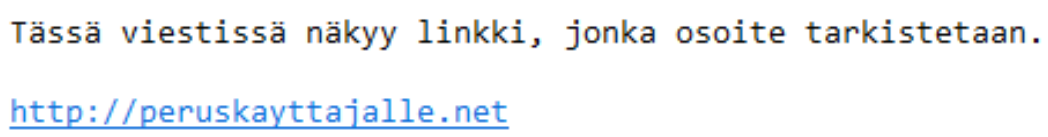
Jos on pieninkin epäilys siitä, onko nettisivusto luotettava, kannattaa asia tarkistaa. Olen tehnyt ohjeen Nettisivustojen luotettavuuden arviointi (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php).

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.

3 Sähköpostiviestien tyypit

Sähköpostiviestejä on olemassa kahta tyyppiä: teksti- ja HTML-muotoisia. Tekstimuotoisissa viesteissä tekstiä ei ole muotoiltu (esimerkiksi muutettu fonttia ja tekstin kokoa) ja linkin todellinen osoite on aina näkyvissä (kuva 6).



Kuva 6

HTML-muotoisissa viesteissä tekstiä on mahdollista muotoilla (esimerkiksi muuttaa fonttia ja tekstin kokoa) ja piilottaa linkin osoite (kuva 7).

Kuva 7

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.

Nettiselaimista ainakin Google Chromessa, Internet Explorerissa, Microsoft Edgessä ja Mozilla Firefoxissa 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://www.mywot.com/en/download* (kuva 8).

Kuva 8

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/linkit.php#selain) asian tarkistamiseen.

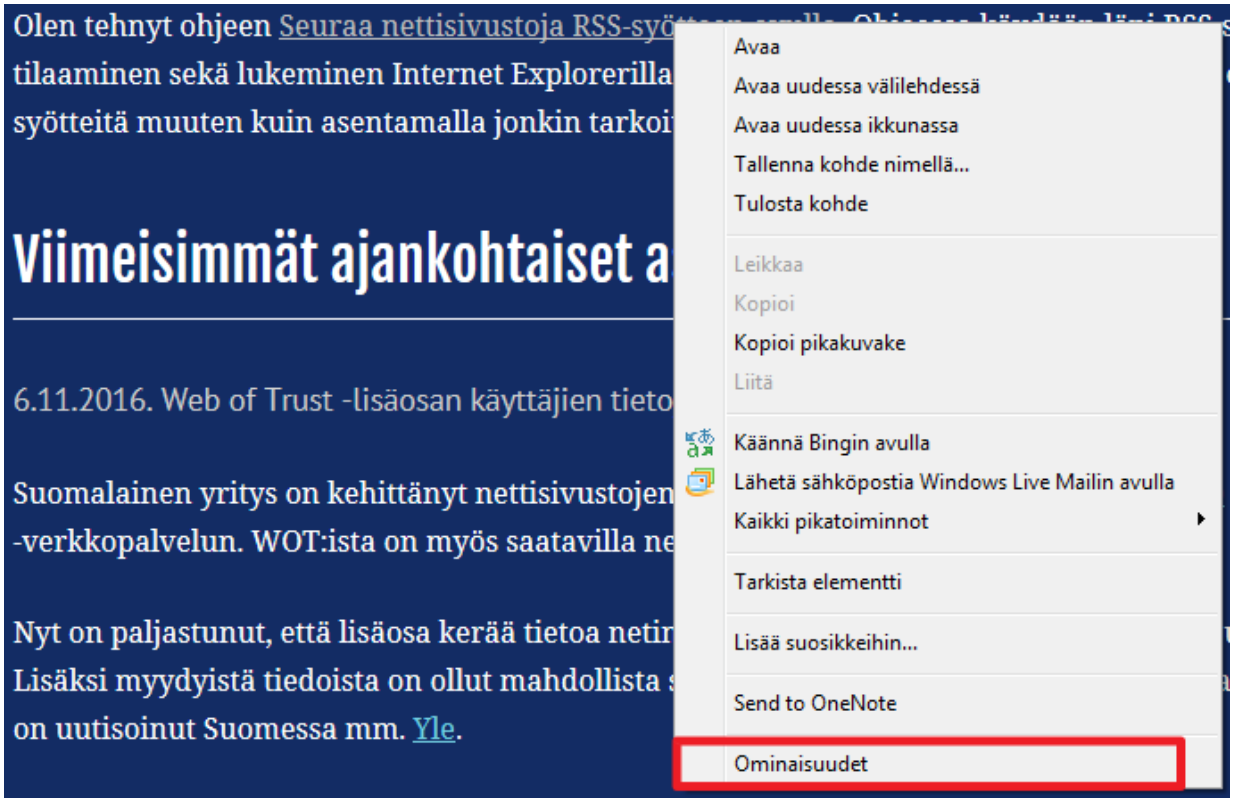
Voit kopioida linkin osoitteen eri nettiselaimissa seuraavasti:

Google Chromessa napsauta linkkiä hiiren oikealla painikkeella ja avautuvassa valikossa valitse kohta **Kopioi linkin osoite** (kuva 9).

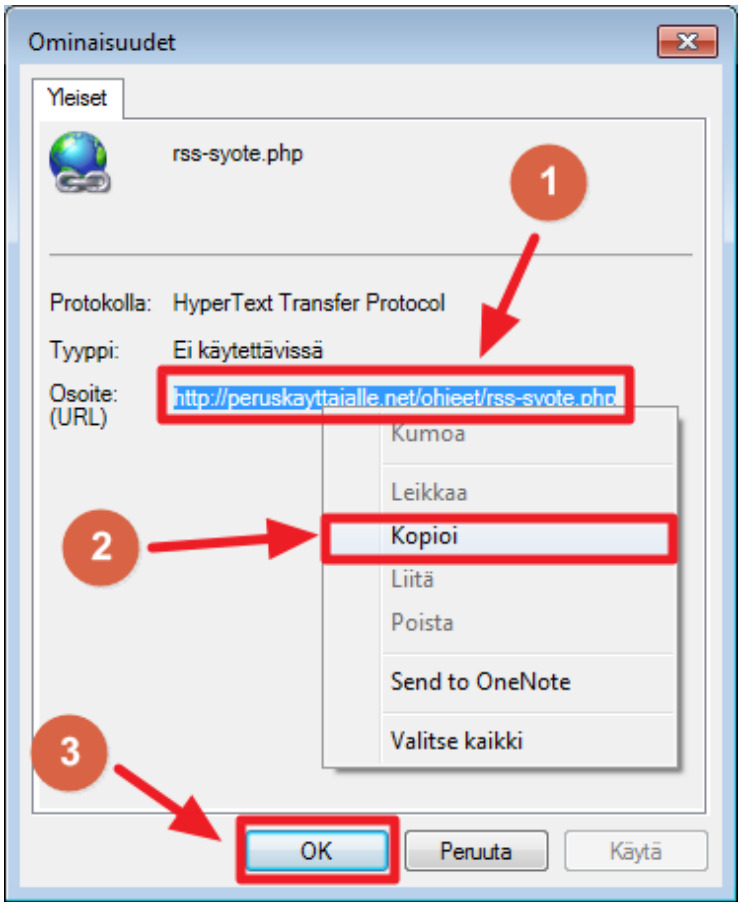
Kuva 9

Internet Explorerissa linkin kopioiminen on hankalampaa. Ensimmäiseksi napsauta linkkiä hiiren oikealla painikkeella ja avautuvassa valikossa valitse kohta **Ominaisuudet** (kuva 10).

Avautuvassa **Ominaisuudet** -ikkunassa ”maalaa” kohdassa **Osoite** oleva linkin osoite pitämällä hiiren vasenta painiketta pohjassa, jolloin osoite muuttuu sinivalkoiseksi. Seuraavaksi napsauta ”maalattua” osoitetta hiiren oikealla painikkeella ja avautuvasta valikosta valitse kohta **Kopioi**. Lopuksi sulje **Ominaisuudet** -ikkuna napsauttamalla alareunan **OK** -painiketta (kuva 11).

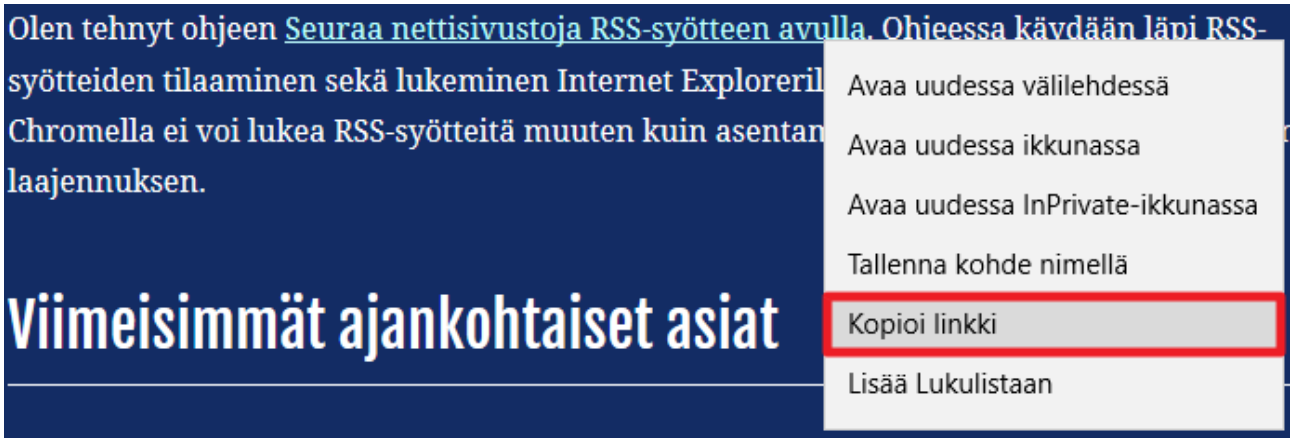


Kuva 10



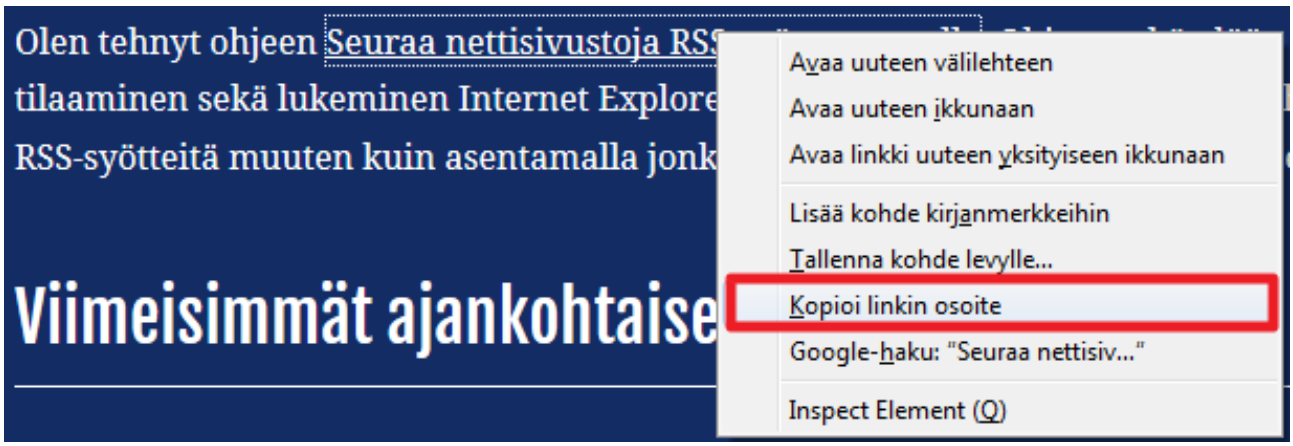
Kuva 11

Microsoft Edgessä napsauta linkkiä hiiren oikealla painikkeella ja avautuvassa valikossa valitse kohta **Kopioi linkki** (kuva 12).



Kuva 12

Mozilla Firefoxissa napsauta linkkiä hiiren oikealla painikkeella ja avautuvassa valikossa valitse kohta **Kopioi linkin osoite** (kuva 13).

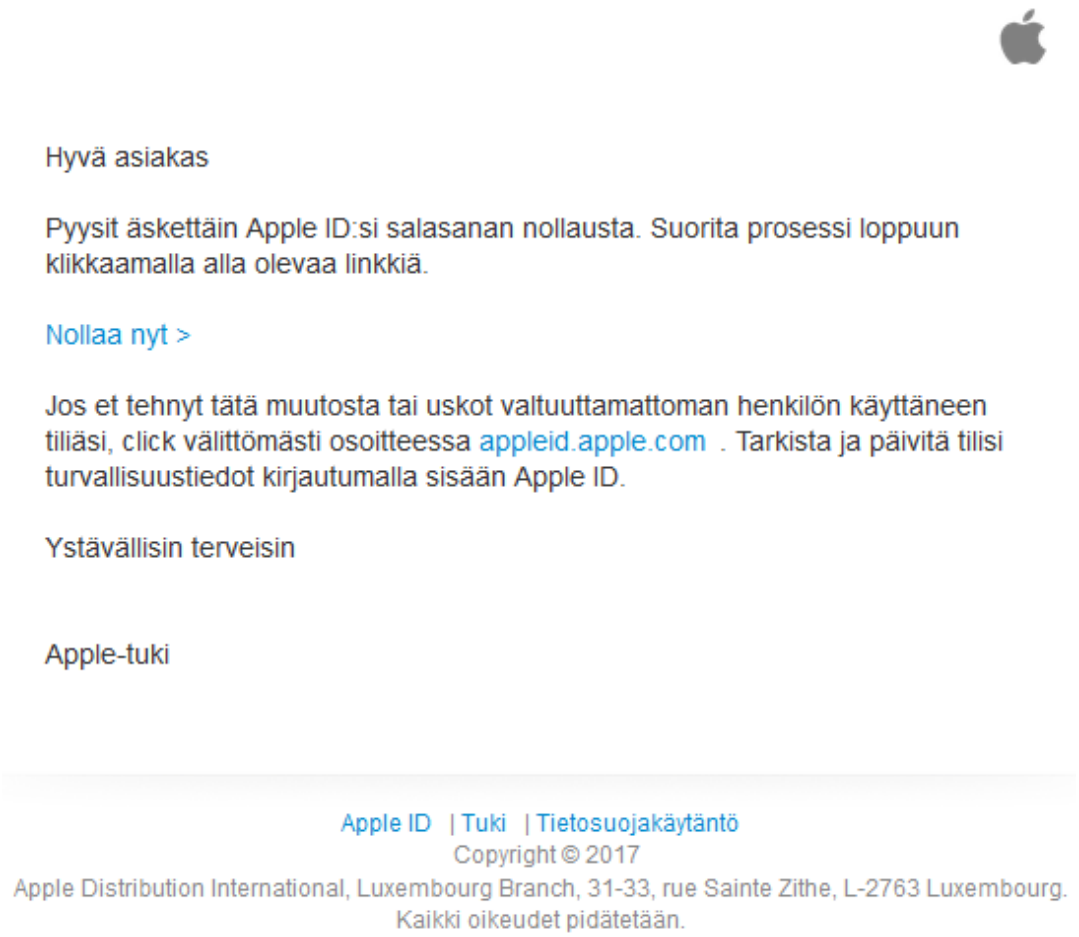


Kuva 13

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) (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php).

5 Esimerkkejä huijausviesteistä

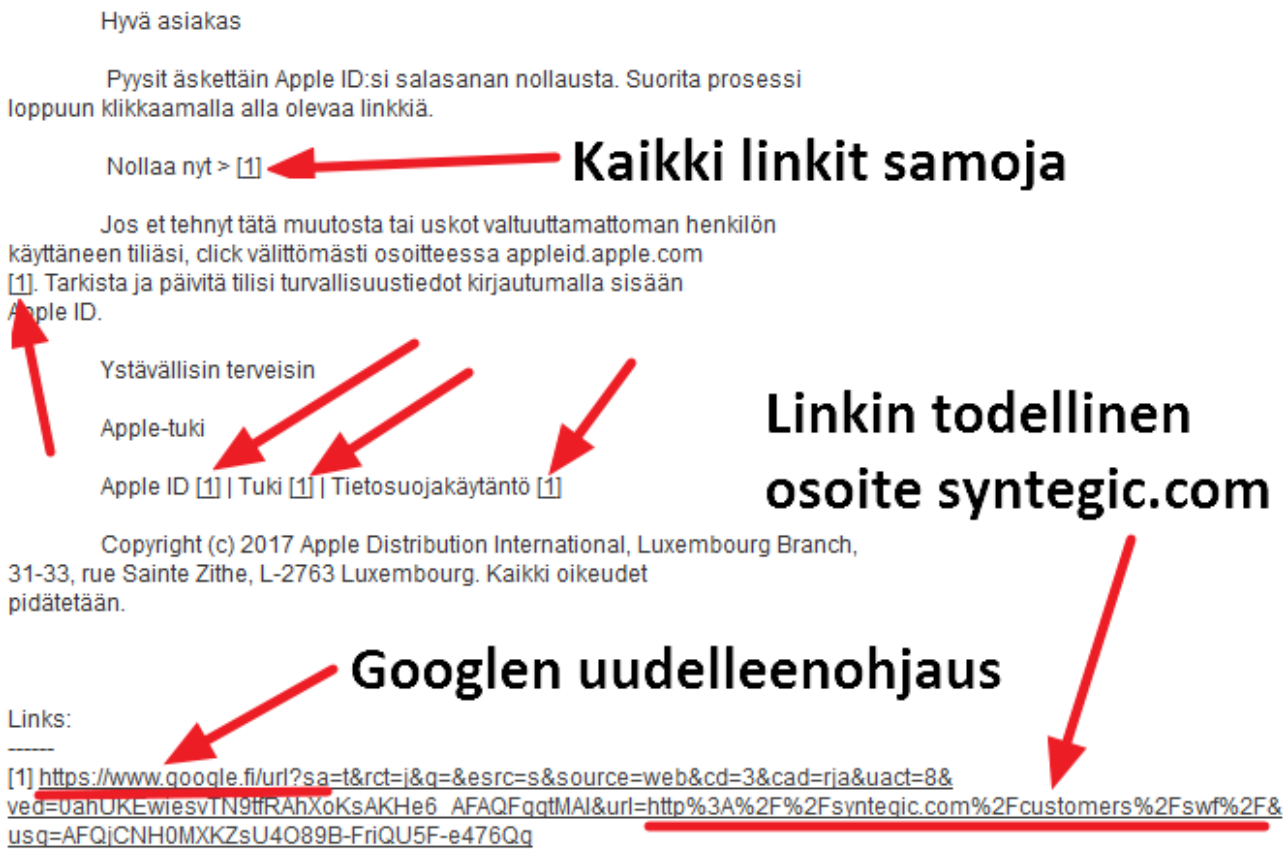
Esimerkeissä on erilaisia huijausviestejä. Esimerkissä 1 huijausviestillä yritetään kalastella Applen käyttäjätunnuksia. Kuvassa 14 on huijausviesti HTML-muodossa, jolloin linkkien todellisia osoitteita ei näe suoraan ja muutoinkin viesti näyttää melko uskottavalta.



Kuva 14

Kuvassa 15 on sama huijausviesti tekstimuodossa. Tällöin paljastuu, että kaikki viestin linkit ohjaavat samaan osoitteeseen. Huijarit myös yrittävät hämätä viestin vastaanottajia käyttämällä Googlen uudelleenohjaustoimintoa, jolloin linkin osoitteen alussa lukee *https://www.google.fi*.

Todellisuudessa Googlella ei ole mitään tekemistä asian kanssa. Linkin todellinen osoite on *http://syntegic.com/customers/swf/*. Lisätietoa Googlen uudelleenohjauksesta löytyy luvusta 6.



Kuva 15

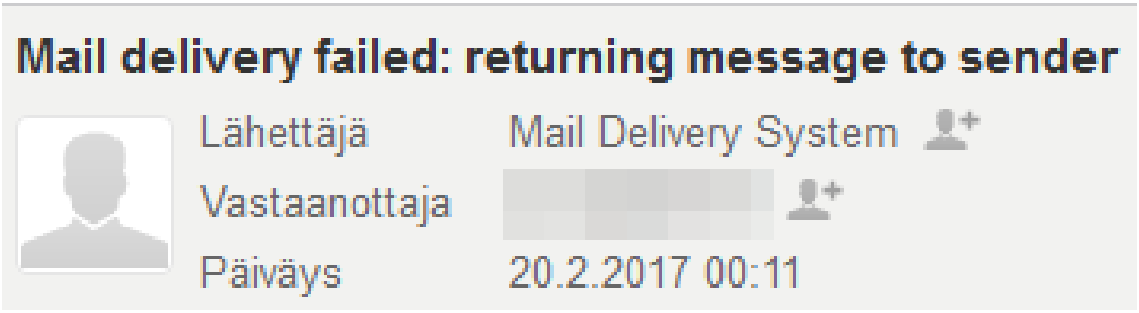
Esimerkissä 2 on kyse rahansiirtopalvelu Western Unioniin liittyvästä tietojenkalastelusta. Kuvassa 16 on huijausviesti HTML-muodossa. Tekstin *http://ocmnet.net* kohdalla pitäisi olla Western Unionin logo, joka ladataan kyseisestä osoitteesta. Itselläni kuva ei latautunut. Tässä huijausviestissä oleva teksti on todennäköisesti käännetty jollain käännösohjelmalla.

Kuva 16

Kuvassa 17 on sama huijausviesti tekstimuodossa. Tällöin paljastuu, että todellisuudessa linkki ohjaa *https://www.westernunion.fin* sijaan osoitteeseen *http://sekolahprogresif.net*. Myös tässä huijausviestissä on käytetty Googlen uudelleenohjaustoimintoa.

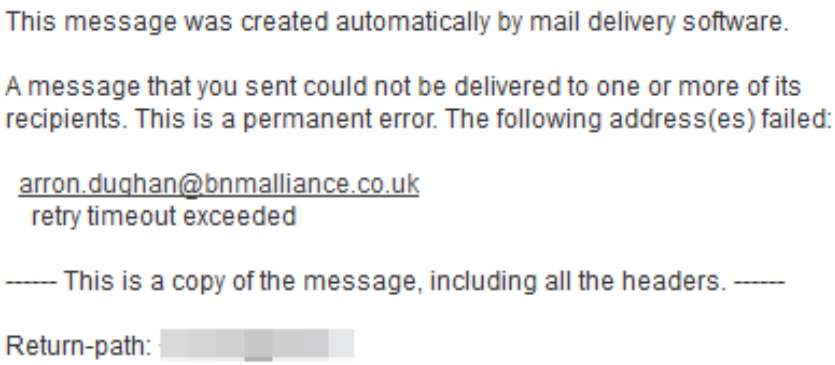
Kuva 17

Esimerkissä 3 huijausviesti on naamioitu ilmoitukseksi lähetetystä sähköpostiviestistä, joka ei ole mennyt perille. Tästä syystä viestin otsikkona on englanniksi **Mail delivery failed: returning message to sender**, joka muistuttaa oikeaa ilmoitusta asiasta. Myös viestin lähettäjäksi on merkitty uskottavalta kuulostava *Mail Delivery System* (kuva 18).



Kuva 18

Itse viestikin on luotu mahdollisimman aidolta ilmoitukselta vaikuttavaksi. Viestin alku on samankaltainen kuin oikeassakin ilmoituksessa (kuvat 19 ja 20).



Kuva 19

Received: from 189.202.44.148.cable.dyn.cableonline.com.mx ([189.202.44.148])
by mailrelaym1.core.cw.net with esmtp (Exim 4.72)
(envelope-from)
id 1cfZgK-0005y7-TJ
for arron.dughan@bnmalliance.co.uk; Sun, 19 Feb 2017 22:10:13 +0000
Message-ID:
Date: Sun, 19 Feb 2017 07:09:45 -0800
From:
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.4) Gecko/20100608 Thunderbird/3.1
MIME-Version: 1.0
To: <arron.dughan@bnmalliance.co.uk>
Subject: Welcoming speech
Content-Type: multipart/alternative;
boundary="------------020206040905040208000101"

This is a multi-part message in MIME format.
--------------020206040905040208000101
Content-Type: text/plain; charset=CP-850; format=flowed
Content-Transfer-Encoding: quoted-printable

Kuva 20

Viestin lopussa on linkki, jonka todellista osoitetta ei ole vaivauduttu piilottamaan (kuva 21).

If you are interested in this offer, please visit <a =
href=3D"http://demo9.zhunong365.com/zu5vqcj/fafqeqkens/">Our =
Site

Kuva 21

Esimerkissä 4 (kuva 22) on sama idea kuin esimerkissä 3, mutta tässä tapauksessa viestissä on kaksi liitetiedostoa. Kuvassa 23 näkyvissä liitetiedostoista toinen näyttäisi olevan tiedostomuodoltaan .eml eli sähköpostiviesti ja toisen liitetiedoston tyyppiä ei ole tunnistettu (tiedostomuoto .???).

Undelivered Mail Returned to Sender

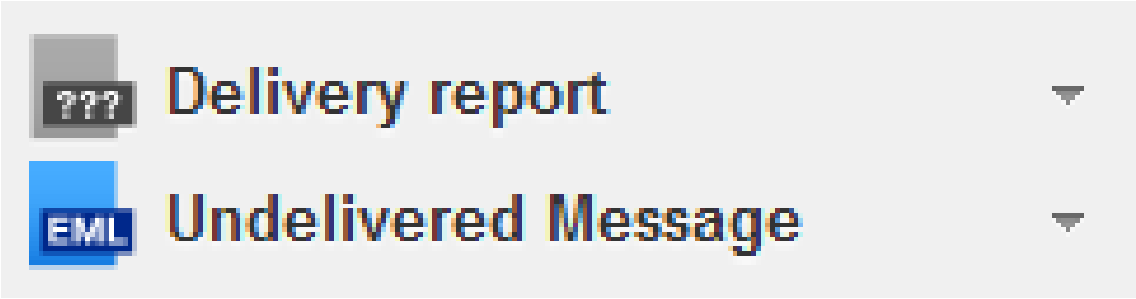
Lähettäjä MAILER-DAEMON@maili2.kaapeli.fi
Vastaanottaja
Päiväys 20.2.2017 00:16

This is the mail system at host maili2.kaapeli.fi.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

Kuva 22



Kuva 23

Huom! Liitetiedostoja ei tule avata, jos et ole ehdottoman varma siitä, että liitetiedostot on lähettänyt sama henkilö kuin sähköpostiviestissä väitetään ja että liitetiedostot ovat varmasti turvallisia avata.

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).

Esimerkissä 5 on tavanomainen lääkkeitä kaupitteleva huijausviesti, johon on lisätty muka mahdollisuus poistua postituslistalta (kuva 24). Luonnollisesti linkkiä ei kannata napsauttaa, koska nettisivustolla voi olla haittaohjelmia.

PharMarkt

Cheapest store:

http://hotwebmaster.su

Avg price -17% lower
172 stores in database now

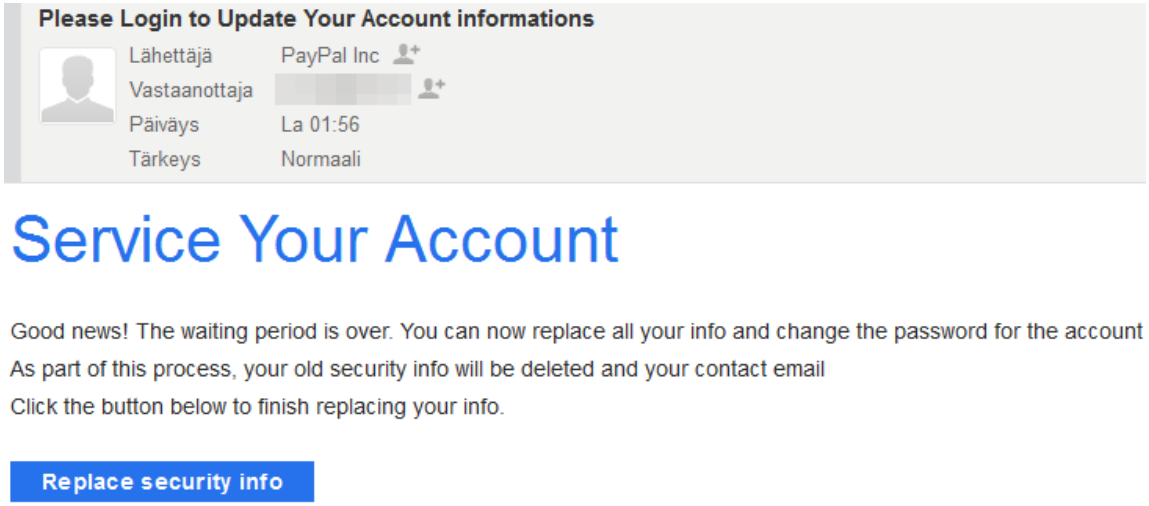
This message was sent to [redacted] If you don't want to receive these emails from PharMarkt in the future, please follow the link below to unsubscribe.

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

Kuva 24

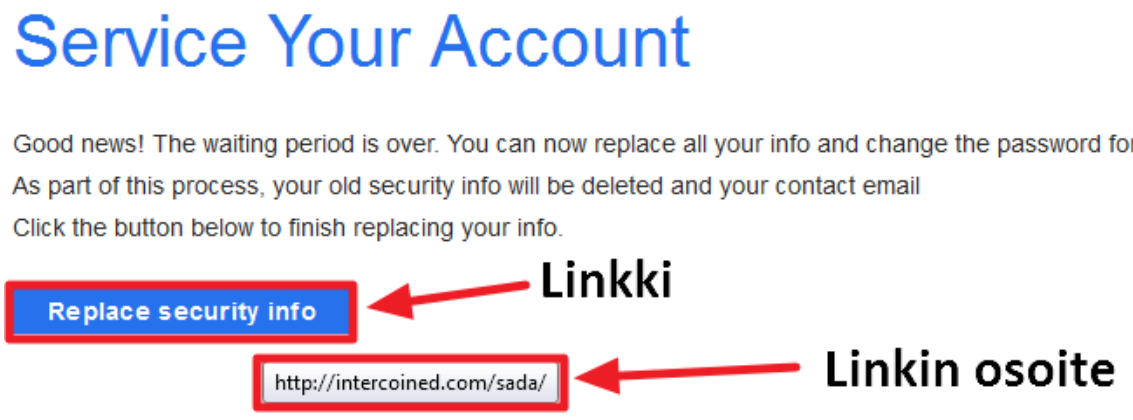
Huom! Huijausviesteihin tai muuhun roskapostiin ei pidä koskaan vastata. Vastaaminen kertoo ainoastaan huijareille ja roskapostittajille, että kyseinen sähköpostiosoite on käytössä. Tämä johtaa vain entistä suurempaan määrään roskapostia.

Esimerkissä 6 huijausviestillä yritetään kalastella PayPalin käyttäjätunnuksia. Kuvassa 25 on huijausviesti HTML-muodossa, jolloin kohdan **Replace security info** linkin todellista osoitetta ei näe suoraan ja viestiä voi pitää kohtalaisen uskottavana.



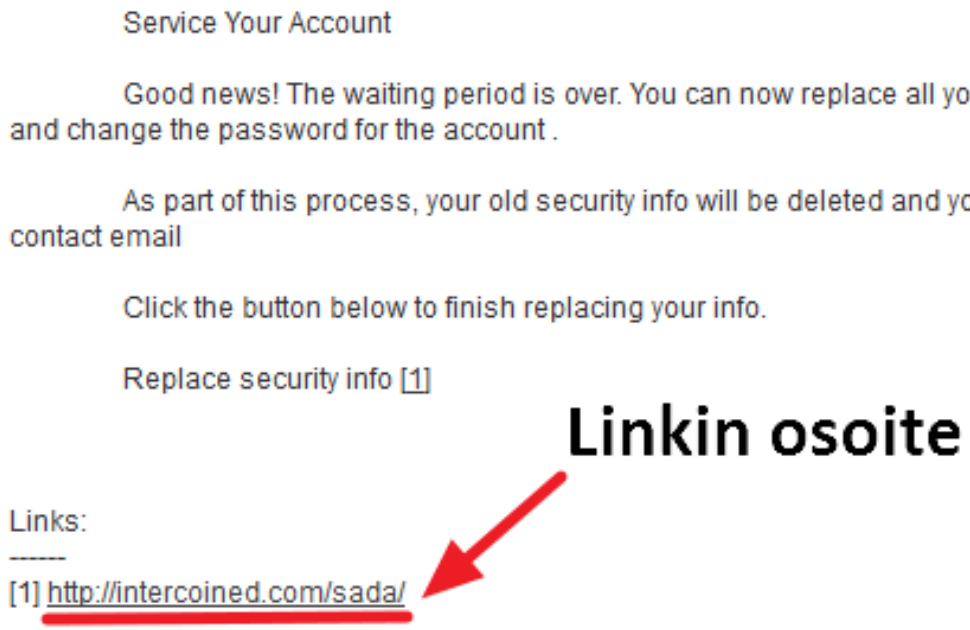
Kuva 25

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 *http://intercoined.com/sada/* (kuva 26).



Kuva 26

Kuvassa 27 on sama huijausviesti tekstimuodossa. Myös kuvassa 27 näkyy, että linkin osoite on *http://intercoined.com/sada/*.



Kuva 27

Esimerkissä 7 on perinteisempi huijausviesti, jossa ei ole linkkejä. Kuvassa 28 näkyy osa viestistä. Kyseisessä viestissä mainostetaan virtuaali- eli kryptovaluutta Swisscoinia.

Kuva 28

Virtuaalivaluutoista löytyy tietoa mm. Wikipediasta (https://fi.wikipedia.org/wiki/Krypto-valuutta 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. Tätä kirjoittaessa Bitcoinin arvo on laskenut reilusti huippulukemista.

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)

6 Googlen uudelleenohjaus

Luvun 6 esimerkeissä sähköpostihuijauksista on osassa huijausviestejä käytetty Googlen uudelleenohjausta hämäämään viestin vastaanottajia. Google käyttää 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*.

7 Skrollin artikkeli tietojenkalastelusta

Tietokonekulttuurin erikoislehti Skrollissa (https://skrolli.fi/) julkaistiin numerossa 2017.1 tietojenkalastelusta artikkeli *Aikainen rosmo tunnarit nappaa*. Tietojenkalastelu on yksi sähköpostihuijauksien alalajeista, jossa pyritään hankkimaan ihmisiltä esimerkiksi verkkopankkitunnukset tai eri verkkopalveluiden käyttäjätunnukset ja salasanat.

Artikkeli perustuu todelliseen huijausviestiin ja siinä käsitellään ennen kaikkea huijauksen teknistä toteutusta. Siitä huolimatta artikkeli on hyödyllistä luettavaa myös peruskäyttäjälle.

Kuten muutkin Skrollin vanhemmat numerot, myös Skrollin numero 2017.1 on ladattavissa ilmaiseksi PDF-muodossa (https://skrolli.fi/2017.1.lukko.pdf). Artikkeli *Aikainen rosmo tunnarit nappaa* löytyy sivuilta 10–13.