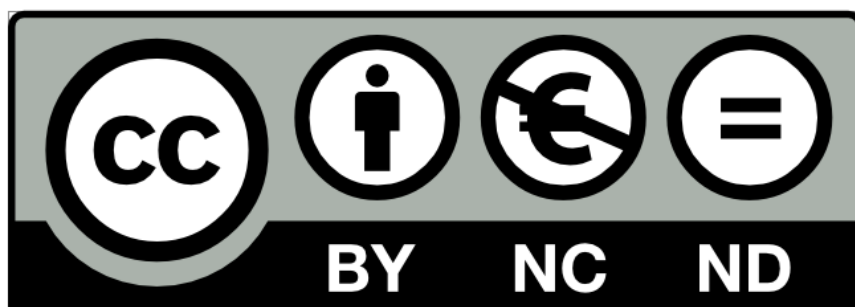


# Tietoturvan muisti- lista

[Peruskäyttäjälle.net](https://peruskayttajalle.net)

Ohjeen versio 5.4.2022



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 [Peruskayttajalle.net](http://Peruskayttajalle.net) -sivuston.

- Peruskayttajalle.netin [Creative Commons-esittely](https://peruskayttajalle.net/tietoja.php#cc) (<https://peruskayttajalle.net/tietoja.php#cc>)
- Lisätietoa [Creative Commonsista suomeksi](https://creativecommons.fi/) (<https://creativecommons.fi/>)



# Sisällysluettelo

Johdanto .....	4
1. Käytä virustorjuntaa .....	4
2. Älä kytke tuntematonta muistitikkuja tietokoneeseen .....	4
3. Käytä vahvoja salasanoja edes tärkeimmissä verkkopalveluissa yms. ....	4
4. Käytä yleisessä käytössä olevia tietokoneita harkiten .....	5
5. Suhtaudu varauksella avoimiin langattomiin verkkoihin .....	5
6. Pidä tietokoneesi päivitettyinä .....	6
7. Varo lyhytlinkkejä .....	6
8. Tarvittaessa tarkista tiedosto haittaohjelmien varalta .....	6
9. Varo sähköpostin liitetiedostoja .....	6
10. Tarkista nettisivuston luotettavuus .....	7
11. Suojaudu roskapostilta väliaikaisella sähköpostiosoitteella .....	7
12. Varmuuskopioi tärkeät tiedostot säännöllisesti .....	7
13. Käytä tavallista käyttäjätiliä päivittäisessä käytössä .....	8
14. Hävitä muistitikut, tietokoneen kiintolevy ym. muistit asianmukaisesti .....	8
15. Älä kytke Käyttäjätilien valvontaa pois päältä .....	9
16. Älä lataa ja asenna ohjelmia mistä tahansa .....	9
17. Älä tallenna salasanoja nettiselaimen .....	9
18. Peitä mikrofoni ja kamera, kun et tarvitse niitä .....	10
19. Varo sähköpostihuijauksia .....	10
20. Käytä turvakysymyksissä vastausta, jota ei voi selvittää .....	11
21. Käytä kaksivaiheista tunnistautumista .....	11
22. Kodin kyberopas .....	11
23. Varo ilmoitus- ja puhelinhuijauksia .....	12
24. Älä luovuta henkilötietojasi ulkopuolisille .....	13
25. Rajoita seuranta käyttämällä eri nettiselaimia .....	13
26. Älä käytä yleisiä USB-latauspisteitä ilman USB-kondomia .....	14





# Johdanto

---

Olen koonnut tähän ohjeeseen listan tietoturvaan liittyviä asioita, jotka peruskäyttäjän on hyvä ottaa huomioon. Asioita ei ole lueteltu tärkeysjärjestyksessä eikä tämä lista ole myöskään täydellinen. Niihin aiheisiin, joista on olemassa tekemäni ohje tai artikkeli, olen lisännyt linkin ohjeeseen tai artikkeliin.

## 1. Käytä virustorjuntaa

Vaikka mikään virustorjuntaohjelmisto ei anna sataprosenttista suojaa haittaohjelmia (esimerkiksi virukset) vastaan, kannattaa virustorjuntaohjelmistoa silti käyttää. Windows 10:n oma virustorjuntaohjelmisto Windows Defender on kehittynyt laadultaan tarpeeksi hyväksi, eikä Windows 10:ssä ole välttämätöntä käyttää muuta virustorjuntaohjelmistoa.

## 2. Älä kytke tuntematonta muistitikkuja tietokoneeseen

Muistitikut ovat yksi keino levittää haittaohjelmia, etenkin silloin, kun halutaan murtautua jonkin tietyn organisaation tietojärjestelmiin.

Erään tutkijan kokeessa hänen yliopiston alueelle jättämistään muistitikuista suurin osa kerättiin talteen ja kytkettiin tietokoneisiin. Jos kyseisillä muistitikuilla olisi ollut haittaohjelma, se olisi levinnyt hyvin laajalle.

## 3. Käytä vahvoja salasanoja edes tärkeimmissä verkkopalveluissa yms.

Vaikka käyttäisit yleisesti heikkoja salasanoja, käytä edes tärkeimmissä verkkopalveluissa (esimerkiksi Facebook, Gmail) ja Windowsin käyttäjätileillä vahvoja salasanoja. Vahvat sanat ovat riittävän pitkiä (mieluiten 20 merkkiä tai enemmän) ja niitä on vaikeaa tai mahdotonta arvata.

Lisätietoa salasanoista löytyy mm. [Kyberturvallisuuskeskuksen sivuilta \(https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan\)](https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan).



Salasanoja ei ole pakko yrittää muistaa. Salasanojen hallintaan voi käyttää salasananhallintaohjelmaa, josta olen kirjoittanut artikkelin [Salasanat haltuun salasananhallintaohjelmalla \(https://peruskayttajalle.net/artikkelit.php#salasana\)](https://peruskayttajalle.net/artikkelit.php#salasana).

## 4. Käytä yleisessä käytössä olevia tietokoneita harkiten

Yleisessä käytössä olevat tietokoneet, joihin ei tarvitse kirjautua tai joissa kaikilla käyttäjillä on sama käyttäjätunnus ja salasana, eivät ole turvallisia. Tällaisia tietokoneita löytyy esimerkiksi kirjastoista.

Näiden tietokoneiden ongelmana on, että osa käyttäjistä ei osaa ottaa huomioon edes tietoturvan perusasioita ja siten tietokoneeseen voi asentua haittaohjelmia. Lisäksi tällaisten tietokoneiden ylläpito voi olla puutteellista, jolloin mahdollisia haittaohjelmatartuntoja ei välttämättä huomata ollenkaan.

Kyseisillä tietokoneilla ei kannata kirjautua mihinkään verkkopalveluun (esimerkiksi lukea sähköposteja), koska mahdollinen haittaohjelma voi varastaa käyttäjätunnukset ja salasanat. Myöskään mitään tärkeitä tietoja sisältäviä tiedostoja (esimerkiksi työhakemukset, ansioluettelot) ei kannata käsitellä tällaisilla tietokoneilla.

## 5. Suhtaudu varauksella avoimiin langattomiin verkkoihin

Avoimet langattomat verkot (englanniksi "Wireless Local Area Network" eli "WLAN") ovat tietoturvaongelma, koska yhteyden kautta kulkeva tieto on kenen tahansa kuunneltavissa ja tallennettavissa. Ainoastaan jollain tavalla salattua tietoa ei voi seurata. Yksi mahdollisuus on käyttää langatonta verkkoa käytettäessä VPN-yhteyttä.

VPN-yhteys on aina salattu, jolloin kukaan ulkopuolinen ei pääse kuuntelemaan tai tallentamaan tietoja. Lisätietoa WLAN:sta ja VPN:stä löytyy esimerkiksi Ylen Digitreeneistä: <https://yle.fi/aihe/artikkeli/2017/06/08/digitreenit-avoin-wifi-houkuttelee-ala-unohdavaaroja> ja <https://yle.fi/aihe/artikkeli/2017/09/06/digitreenit-mika-ihmeen-vpn-se-suoja-nettiyhteyttasi-avoimessa-verkossa>.

Olen myös kirjoittanut artikkelin [VPN-palvelun valinta \(https://peruskayttajalle.net/artikkelit.php#vpn\)](https://peruskayttajalle.net/artikkelit.php#vpn), jossa käydään läpi VPN-palvelun valinnassa huomioitavia asioita.



## 6. Pidä tietokoneesi päivitettyinä

Yksi tietoturvan perusasioista on pitää Windows ja asennetut ohjelmat päivitettyinä. Tätä urakkaa helpottamaan löytyy erilaisia ohjelmia, jotka kertovat, ovatko tietokoneelle asennetut ohjelmat ajan tasalla.

Parhaimpana tällaisena ohjelmana pidän SUMoa (Software Update Monitor). Olen tehnyt ohjeen [Ohjelmat ajan tasalle SUMon avulla \(https://peruskayttajalle.net/ohjeet/sumo.php\)](https://peruskayttajalle.net/ohjeet/sumo.php).

## 7. Varo lyhytlinkkejä

Lyhytlinkki on linkki jollekin nettisivulle, jonka osoite on lyhennetty lyhytlinkkipalvelulla (esimerkiksi [Bitly](https://bitly.com), [TinyURL.com](https://tinyurl.com)). Esimerkiksi linkki <https://peruskayttajalle.net/ohjeet.php> muuttuu lyhytlinkkinä muotoon <https://goo.gl/SHGHii>.

Lyhytlinkkien todellinen osoite kannattaa selvittää aina ennen lyhytlinkin avaamista, koska lyhytlinkkejä käytetään haittaohjelmien levittämiseen. Olen tehnyt ohjeen [Tarkista lyhytlinkkien todellinen osoite \(https://peruskayttajalle.net/ohjeet/lyhytlinkki.php\)](https://peruskayttajalle.net/ohjeet/lyhytlinkki.php).

## 8. Tarvittaessa tarkista tiedosto haittaohjelmien varalta

Jos olet epävarma, onko jokin tiedosto turvallinen, kannattaa tiedosto tutkia myös netin virustarkistuspalveluilla. Virustarkistuksen voi tehdä lähes mille tahansa tiedostolle, ei ainoastaan ohjelmille. Tarkistettaville tiedostoille on yleensä määritelty enimmäiskoko, joka voi ylittyä joidenkin tiedostojen kohdalla.

Olen tehnyt ohjeen [Yksittäisten tiedostojen virustarkistukset netissä \(https://peruskayttajalle.net/ohjeet/virustarkistus.php\)](https://peruskayttajalle.net/ohjeet/virustarkistus.php).

## 9. Varo sähköpostin liitetiedostoja

Haittaohjelmien levittäminen sähköpostin liitetiedostona on ikivanha temppu, joka on varsin tehokas menetelmä vielä tänäkin päivänä. Siksi sähköpostin liitetiedostoja ei kannata avata ilman harkintaa.



Sähköpostin lähettäjän vääräntäminen on helppoa. Siksi myös tutuilta lähettäjiltä tulevien sähköpostien liitetiedostoihin tulee suhtautua varauksella. Tällaisissa tapauksissa kannattaa kysyä kyseiseltä henkilöltä muilla keinoin kuin sähköpostitse, onko hän lähettänyt kyseisen sähköpostin ja sen liitetiedoston.

## 10. Tarkista nettisivuston luotettavuus

Nettisivuston luotettavuus on hyvä tarkistaa aina, jos olet ostamassa jotain tai olet antamassa tietoja (esimerkiksi nimi, sähköpostiosoite) jollekin nettisivustolle. Nettisivustojen luotettavuuden tutkimiseen löytyy peruskäyttäjille sopivia verkkopalveluita.

Olen tehnyt ohjeen [Nettisivustojen luotettavuuden arviointi \(https://peruskayttajalle.net/ohjeet/nettisivustojen\\_luotettavuus.php\)](https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php).

## 11. Suojaudu roskapostilta väliaikaisella sähköpostiosoitteella

Jos epäilet jonkin sähköpostiosoitettasi vaativan nettisivuston mahdollisesti lähettävän sinulle myöhemmin roskapostia tai ei-toivottua mainontaa, voit käyttää tilapäistä sähköpostiosoitetta. Olen tehnyt ohjeen [Käytä tilapäistä sähköpostiosoitetta \(https://peruskayttajalle.net/ohjeet/10\\_minute\\_mail.php\)](https://peruskayttajalle.net/ohjeet/10_minute_mail.php).

## 12. Varmuuskopioi tärkeät tiedostot säännöllisesti

Varmuuskopioinnin tärkeys ei ole asia, joka kannattaa oppia kantapään kautta. Varmuuskopioinnissa on hyvä muistaa sääntö ”3-2-1”. Käytännössä tämä tarkoittaa sitä, että kaikesta tärkeästä tiedosta on olemassa kolme eri varmuuskopiota.

Sen lisäksi tiedot on tallennettu kahteen eri fyysiseen formaattiin (esimerkiksi tietokoneen kiintolevylle ja netin varmuuskopiointipalveluun) ja yksi varmuuskopio on fyysisesti eri paikassa, esimerkiksi toisessa rakennuksessa.

Viimeinen kohta voi tarkoittaa myös varmuuskopiointia esimerkiksi ulkoiselle kiintolevylle, joka kytketään tietokoneeseen vain silloin, kun tiedostoja varmuuskopioidaan. Tietyissä tapauksissa varmuuskopiointiin voivat sopia myös muistitikut, mutta yleisesti ottaen se ei ole suositeltavaa.





Olen käsitellyt muistitikujen käyttöä varmuuskopiointiin ohjeessa [Muistitikun käyttö](https://peruskayttajalle.net/ohjeet/muistitikku.php) (<https://peruskayttajalle.net/ohjeet/muistitikku.php>) ja ulkoisia kiintolevyjä ohjeessa [Ulkoisen kiintolevyn käyttö](https://peruskayttajalle.net/ohjeet/ulkoinen_kiintolevy.php) ([https://peruskayttajalle.net/ohjeet/ulkoinen kiintolevy.php](https://peruskayttajalle.net/ohjeet/ulkoinen_kiintolevy.php)).

## 13. Käytä tavallista käyttäjätiliä päivittäisessä käytössä

Tietoturvasyistä Windowsia tulee käyttää päivittäisessä käytössä rajoitetuin oikeuksin eli käyttäjänä. Ongelmana on, että Windowsin asennuksen yhteydessä luodaan vain yksi käyttäjätili, jolla on järjestelmänvalvojan oikeudet. Tämä on vakava tietoturvaongelma, koska järjestelmänvalvojalla on oikeus tehdä tietokoneelle ihan mitä haluaa.

Jos tietokonetta käytetään normaalisti käyttäjätilillä, jolla on käyttäjän oikeudet, tietokoneeseen tarttuva haittaohjelma tai mahdollinen murtautuja ei saa automaattisesti järjestelmänvalvojan oikeuksia. Ainakin osa haittaohjelmista ei pysty asentamaan itseään tietokoneelle käyttäjän oikeuksilla.

Olen tehnyt ohjeen [Käytä tietokonetta normaalikäytössä käyttäjän oikeuksilla](https://peruskayttajalle.net/ohjeet/kayttajatilit.php) (<https://peruskayttajalle.net/ohjeet/kayttajatilit.php>).

## 14. Hävitä muistitikut, tietokoneen kiintolevy ym. muistit asianmukaisesti

Muistia sisältävät laitteet on tietoturvasyistä hyvä hävittää asianmukaisesti. Esimerkiksi tietokoneen kiintolevyltä tai SSD-asemalta voi löytyä kaikenlaista tietoa mm. tietokoneella käsitellyistä tiedostoista, mikäli kiintolevyä tai SSD-asemaa ei ole pyyhitty puhtaaksi tarkoitukseen tehdyllä ohjelmalla tai levyä ei ole tuhottu fyysisesti lukukelvottomaksi.

Kiintolevyn tai SSD-aseman ohjelmallinen pyyhkiminen onnistuu vain ehjien kiintolevyjen tai SSD-asemien kohdalla ja vaatii osaamista tai yksityiskohtaiset ohjeet. Näistä syistä joutuksen peruskäyttäjän on helpointa toimittaa tietokoneensa, kännykkänsä, muistitikunsa yms. lukittuun data-SER-keräysastiaan.

Lisätietoa aiheesta löytyy artikkelista [Kierrätä muistia sisältävät laitteet tietoturvallisesti](https://peruskayttajalle.net/artikkelit.php#kierratys) (<https://peruskayttajalle.net/artikkelit.php#kierratys>).



## 15. Älä kytke Käyttäjätilien valvontaa pois päältä

Käyttäjätilien valvonta (englanniksi "User Account Control" eli "UAC") on tärkeä osa Windowsin tietoturvaan. Käyttäjätilien valvonta otetaan käyttöön automaattisesti Windowsin asennuksen yhteydessä eli se on normaalisti käytössä.

Moni käyttäjä kytkee Käyttäjätilien valvonnan pois päältä, koska se kyselee lupaa eri toimintojen suorittamiseen. Käytännössä Käyttäjätilien valvonta kyselee aika harvoin mitään lupia ja ainoastaan silloin, kun johonkin toimintoon tarvitaan järjestelmänvalvojan oikeudet. Näin käy usein esimerkiksi ohjelmien asennuksen ja päivityksen yhteydessä.

Olen tehnyt ohjeen [Windowsin Käyttäjätilien valvonta \(https://peruskayttajalle.net/ohjeet/kayttajatilien\\_valvonta.php\)](https://peruskayttajalle.net/ohjeet/kayttajatilien_valvonta.php).

## 16. Älä lataa ja asenna ohjelmia mistä tahansa

Ohjelmat on suositeltavinta ladata suoraan niiden tekijän nettisivuilta. Netti on täynnä erilaisia ohjelmien lataussivustoja, mutta niistä vain kourallista voi pitää luotettavina. Osa lataussivustoista lisää asennusohjelmiin kaikenlaista roskaa, kuten mainoksia esittäviä ohjelmia.

Pahimmassa tapauksessa asennusohjelmaan on voitu lisätä haittaohjelma. Esimerkiksi tiedonsiirtoon tarkoitettu FileZillasta on levitetty laajasti haittaohjelman sisältävää versiota.

## 17. Älä tallenna salasanoja nettiselaimen

Nettiselaimissa on mahdollisuus tallentaa nettisivustojen salasanoja, jolloin niitä ei tarvitse kirjoittaa kirjautuessa jollekin nettisivustolle. Salasanojen tallentamista nettiselaimen ei kuitenkaan pidä käyttää, koska salasanoja ei ole suojattu kunnolla.

Tietokoneelle asentunut haittaohjelma tai murtautuja pystyy varastamaan nettiselaimen tallennetut salasanat helposti.



Myös pelkkä nettiselaimen automaattinen lomakkeiden täydennystoiminto voi olla tietoturvariski. Jotkin nettiselaimet voivat täyttää automaattista lomakkeiden täydennystoimintoa käytettäessä myös piilossa olevat lomakekentät.

Lomakekentät on erittäin helppoa piilottaa nettisivulla ns. negatiivisella marginaalilla, jolloin lomakekentät ovat kyllä olemassa nettisivulla, mutta ne eivät näy käyttäjälle.

Salasanojen tallentamiseen voi käyttää salasananhallintaohjelmia, joissa salasanat ovat turvassa. Olen kirjoittanut salasananhallintaohjelmista artikkelin [Salasanat haltuun salasananhallintaohjelmalla](https://peruskayttajalle.net/artikkelit.php#salasana) (<https://peruskayttajalle.net/artikkelit.php#salasana>).

## 18. Peitä mikrofoni ja kamera, kun et tarvitse niitä

Käytännössä kaikissa kannettavissa tietokoneissa on kamera ja mikrofoni. Tietoturvasyistä ne kannattaa peittää silloin, kun niitä ei tarvitse. Näin siksi, että on hyvin helppoa vakoilla tietokoneen käyttäjää kameran ja mikrofonin avulla ja vieläpä täysin huomaamattomasti.

Vaikka joissakin kameroissa on merkkivalo, joka palaa kun kamera on toiminnassa, voi tietokoneelle asentunut haittaohjelma tai murtautuja kytkeä merkkivalon pois käytöstä. Eli merkkivaloon ei tule luottaa liikaa.

## 19. Varo sähköpostihuijauksia

Erilaiset sähköpostihuijaukset ovat valitettavan yleisiä. Huijausviesteillä voidaan yrittää saada vastaanottajaa antamaan esimerkiksi verkkopankkitunnuksensa tai ohjata vastaanottaja haittaohjelmia jakelevalle nettisivustolle.

Ennen huijausviestien erottaminen oli helpompaa, koska ne oli usein kirjoitettu huonolla suomen kielellä. Mutta nykyään huijausviestien taso on parantunut, mikä voi harhauttaa viestin vastaanottajaa.

Siksi olen tehnyt ohjeen [Varo sähköpostihuijauksia](https://peruskayttajalle.net/ohjeet/sahkopostihuijaus.php) (<https://peruskayttajalle.net/ohjeet/sahkopostihuijaus.php>), jossa mm. käydään läpi perusasiat linkkien todellisen osoitteen selvittämisestä.



## 20. Käytä turvakysymyksissä vastausta, jota ei voi selvittää

Erilaisissa verkkopalveluissa on usein mahdollisuus kirjautua turvakysymyksen avulla, jos salasana on päässyt unohtumaan. Turvakysymykset ovat kuitenkin tietoturvariski, koska vastaamalla turvakysymykseen oikein, kuka tahansa pääsee kirjautumaan kyseiseen verkkopalveluun.

Turvakysymykset ovat yleensä sellaisia, että niiden vastaukset on helppoa selvittää. Usein selvittämistä helpottaa myös se, että ihmisillä on tapana kertoa itsestään paljon tietoja sosiaalisessa mediassa, kuten Facebookissa. Siksi turvakysymyksen vastausten tulisi olla satunnaisia sanoja tai lauseita, jotka on helppo muistaa itse.

## 21. Käytä kaksivaiheista tunnistautumista

Perinteinen kirjautuminen erilaisiin verkkopalveluihin käyttäjätunnuksella ja salasanalla ei ole tietoturvan kannalta paras mahdollinen ratkaisu, koska ne eivät anna riittävästi suojaa. Siksi on syytä käyttää kaksivaiheista tunnistautumista, silloin kun se on saatavilla. Kaksivaiheisesta tunnistautumisesta käytetään myös muita nimiä, kuten kaksivaiheinen vahvistus.

Kaksivaiheisessa tunnistautumisessa verkkopalveluihin annetaan ensin normaalisti käyttäjätunnus ja salasana. Tämän jälkeen kirjautumiseen vaaditaan esimerkiksi tekstiviestillä saatava koodi. Tällöin kirjautuminen onnistuu vasta, kun verkkopalveluun on annettu oikea koodi.

Eri verkkopalveluiden käyttämät vahvistustavat vaihtelevat tekstiviestillä saatavista koodista älypuhelimeen asennettaviin ohjelmiin ja tietokoneeseen liitettäviin muistitikkuihin.

## 22. Kodin kyberopas

Puolustusministeriön yhteydessä toimiva [Turvallisuuskomitea](https://turvallisuuskomitea.fi/) (<https://turvallisuuskomitea.fi/>) on julkaissut [Kodin kyberoppaan](https://turvallisuuskomitea.fi/kodin-kyberopas-ohjeita-digitaaliseen-arkeen/) (<https://turvallisuuskomitea.fi/kodin-kyberopas-ohjeita-digitaaliseen-arkeen/>), jossa käydään läpi peruskäyttäjän kannalta olennaisia asioita mm. tietoturvasta.



Oppaan julkaisun yhteydessä Yle tiivistä oppaan sisällöstä [10 kohdan ohjeet turvallisempaan netinkäyttöön](https://yle.fi/uutiset/3-9573346) (<https://yle.fi/uutiset/3-9573346>).

## 23. Varo ilmoitus- ja puhelinhuijauksia

Tyypillisesti ilmoitushuijauksessa nettiselaimen ilmestyy ponnausikkuna, jossa väittää tietokoneella olevan haittaohjelma tai tietokoneella olevan jonkin teknisen ongelman, joka täytyy korjata.

Yhdessä huijauksessa viestissä oli puhelinnumero, johon soittaessa huijarit väittivät kyseessä olevan Microsoftin tukipalvelun ja tarjosivat maksullista tukea ongelman ratkaisemiseen.

Ongelman korjatakseen huijarit halusivat ottaa etäyhteyden uhrin tietokoneeseen. Etäyhteyden avulla huijarit voivat käyttää uhrin tietokonetta kuin omaansa. Samalla uhrin tietokoneelle voidaan asentaa haittaohjelmia ja varastaa tietoja.

Tämän jälkeen huijarit ovat uhrin avustuksella luoneet sähköpostilla laskun tukipalvelusta. Laskua varten uhrin on pitänyt antaa henkilötunnus, osoite, puhelinnumero ja luottokortin numero. Lisäksi joissakin tapauksissa huijarit ovat pyytäneet näyttämään ajokortin tietokoneen kameralle, jotta ajokortti on saatu kuvattua myöhempää käyttöä varten.

Seuraavaksi uhria on pyydetty maksamaan lasku verkkopankissa tai luottokortilla. Laskun maksamisen jälkeen tietokoneelle on mahdollisesti tehty joitain toimenpiteitä etäyhteyden avulla.

On syytä suhtautua epäillen kaikenlaisiin ilmoituksiin siitä, että tietokoneella on haittaohjelma. Käytännössä ainoastaan tietokoneelle asennetun virustorjunnan ilmoituksiin tulee reagoida, kaikki muut ilmoitukset ovat pääsääntöisesti huijausta.

Sama kaava on käytössä myös teknisen tuen huijauspuheluissa. Huijarit väittävät tietokoneessa olevan jonkin ongelman ja haluavat asentaa tietokoneelle etähallintaohjelman.

Olen kirjoittanut puhelinhuijauksista artikkelin [Varo huijauspuheluita](https://peruskayttajalle.net/artikkelit.php#huijauspuhelut) (<https://peruskayttajalle.net/artikkelit.php#huijauspuhelut>).



## 24. Älä luovuta henkilötietojasi ulkopuolisille

Omien henkilötietojensa kanssa kannattaa olla tarkkana, koska identiteettivarkauksia tapahtuu paljon. Identiteettivarkaudessa rikollinen käyttää jonkun muun henkilötietoja ja tietojen avulla esimerkiksi tilaa tavaraa tai ottaa pikavippejä uhrin nimissä. Henkilötietoja voidaan väärinkäyttää myös pelkkään kiusaamiseen.

Yle on kahdessa artikkelissaan ([Identiteettivaras vaanii verkossa, https://yle.fi/uutiset/3-9448910](https://yle.fi/uutiset/3-9448910) ja [Näin voit yrittää välttää identiteettivarkaudelta, https://yle.fi/uutiset/3-9727894](https://yle.fi/uutiset/3-9727894)) käsitellyt identiteettivarkauksia ja niiltä suojautumista.

Noiden artikkeleiden ohjeisiin lisään vielä sen neuvon, että kaikki arkaluonteiset paperit (esimerkiksi laskut, kuitit, tiliotteet) on syytä tuhota paperisilppurilla. Asianmukaisesti paperit silppuavia ristiinleikkaavia paperisilppureita saa muutamalla kymppillä, joten sellaisen hankkiminen ei ole kohtuuttoman kallista.

Olen käsitellyt tätä aihetta artikkeleissa [Rajoita identiteettivarkauden vaikutuksia omalla luottokiellolla \(https://peruskayttajalle.net/artikkelit.php#luottokielto\)](https://peruskayttajalle.net/artikkelit.php#luottokielto) ja [Mitä tehdä jos tulit huijatuksi netissä \(https://peruskayttajalle.net/artikkelit.php#toimenpiteet\)](https://peruskayttajalle.net/artikkelit.php#toimenpiteet).

## 25. Rajoita seuranta käyttämällä eri nettiselaimia

Kaikki suuret yritykset kuten Facebook, Google ja Microsoft seuraavat käyttäjien toimintaa mahdollisemman tarkasti. Yksi keino seurannan rajoittamiseen on käyttää eri nettiselaimia eri tarkoituksiin. Yleisimpiä nettiselaimia ovat Google Chrome, Microsoft Edge, Mozilla Firefox ja Applen laitteissa Safari.

Käytännössä eri nettiselaimien käyttö tapahtuu niin, että esimerkiksi Facebookia käytetään vaikka Edgellä, Googlen palveluita Chromella ja kaikkkeen muuhun käytetään Firefoxia. Tällä tavoin yritysten on vaikeampi seurata yksittäisen käyttäjän tekemisiä netissä.

Olen kirjoittanut artikkelin [vaihtoehtoisista nettiselaimista \(https://peruskayttajalle.net/artikkelit.php#selaimet\)](https://peruskayttajalle.net/artikkelit.php#selaimet) Windowsille ja älypuhelimille.



## 26. Älä käytä yleisiä USB-latauspisteitä ilman USB-kondomia

Yleisessä käytössä olevissa USB-latauspisteissä on se ongelma, että virran lisäksi USB-liitäntä siirtää myös tietoa. Tällöin esimerkiksi lataukseen USB-liitäntään laitettava puhelin voi saada haittaohjelmatartunnan latauksen ohella. Puhelimeen voidaan myös murtautua.

Mistään USB-liitännästä ei pysty päällepäin sanomaan, onko se turvallinen vai ei. Siksi puhelinta ei kannata ladata mistään vieraasta USB-liitännästä ilman USB-kondomia. USB-kondomi estää kaiken tiedonsiirron laitteen ja latauspisteen välillä, jolloin latauksessa siirtyy ainoastaan sähköä.

## 27. Rajoita Windowsin tiedonkeruuta

Windows 10 kerää tietoa tietokoneen käytöstä erittäin laajasti ja lähettää tiedot eteenpäin Microsoftille. Windows 10:n asennuksen yhteydessä tulee ehdottomasti kieltää tietojen kerääminen kaikissa kohdissa, missä se on mahdollista.

Tämän lisäksi on ehdottomasti suositeltavaa käydä läpi kaikki Windows 10:n yksityisyysasetukset, jotka löytyvät Windows 10:n asetuksista. Osa Windows 10:n yksityisyysasetuksista on kuitenkin peruskäyttäjän kannalta erittäin hankalasti muutettavia.

Onneksi on olemassa helppokäyttöisiä ohjelmia, joilla nämä ”piilotetut” yksityisyysasetukset saa helposti näkyviin kootusti yhteen paikkaan. Olen käsitellyt aiheet ohjeessa [Parempaa yksityisyysensuojaa Windows 10:ssä \(https://peruskayttajalle.net/ohjeet/w10\\_yksityisyys.php\)](https://peruskayttajalle.net/ohjeet/w10_yksityisyys.php).

Jos et ole varma, mitä Windowsin versiota käytät, Peruskäyttäjälle.netistä löytyy [linkki \(https://peruskayttajalle.net/linkkeja.php#perustiedot\)](https://peruskayttajalle.net/linkkeja.php#perustiedot) asian tarkistamiseen.

