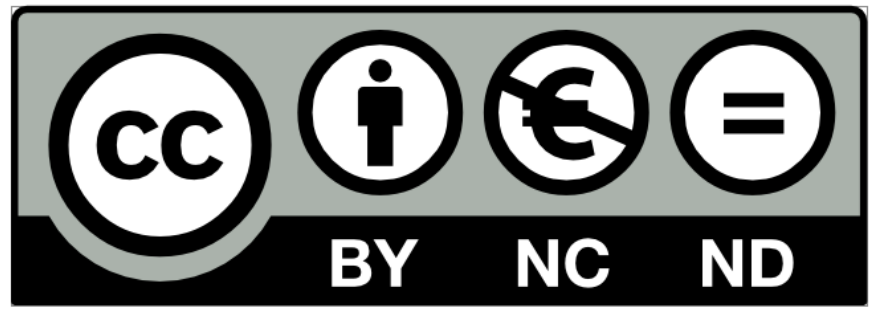
Tietoturvan muisti-lista

Peruskäyttäjälle.net

Ohjeen versio 5.3.2017



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

Tietoturvan muistilista

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, olen lisännyt linkin ohjeeseen.

1. Käytä virustorjuntaa

Vaikka mikään virustorjuntaohjelmisto ei anna sataprosenttista suojaa haittaohjelmia (esimerkiksi virukset) vastaan, kannattaa virustorjuntaohjelmistoa silti käyttää. Myös tietyt ilmaiset virustorjuntaohjelmat (esimerkiksi Avast, AVG) ovat hyviä ja toimivia.

2. Älä kytke tuntematonta muistitikkua 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.

Australiassa postilaatikkoihin on jaettu haittaohjelmia sisältäviä muistitikkuja: http://www.mikrobitti.fi/2016/09/salaperaisia-haittaohjelmilla-kyllastettyja-usb-muistitikkuja-alkoi-tipahdella-ihmisten-postilaatikoihin-poliisilta-synkka-varoitus/

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 salasanat ovat riittävän pitkiä (vähintään 16 merkkiä, mieluiten 20 tai enemmän), monimutkaisia, eivät koostu minkään kielen sanoista ja niissä on käytetty erikoismerkkejä, jos mahdollista.

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.

Yksi mahdollisuus on käyttää langatonta verkkoa käytettäessä VPN-yhteyttä. VPN-yhteys on aina salattu, jolloin kukaan ulkopuolinen ei pääse kuuntelemaan tai tallentamaan tietoja. Lisätietoa VPN:stä löytyy esimerkiksi Yksityisyydensuoja-sivustolta (https://www.yksityisyydensuoja.fi/content/virtuaalinen-erillisverkko).

Viestintävirasto on julkaissut ohjeen langattomien verkkojen tietoturvasta (https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22011langattomienverkkojentietoturvasta.html).

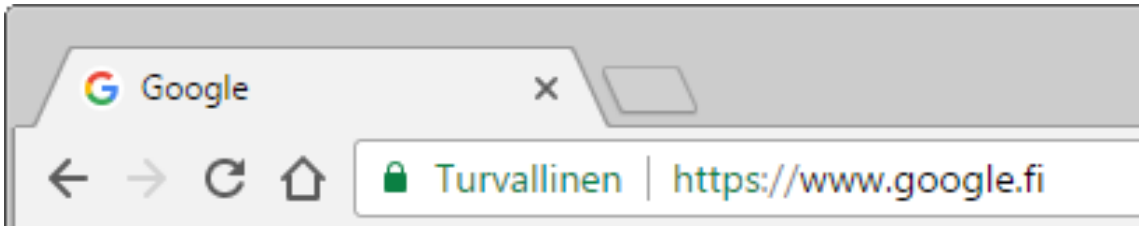
6. Pidä tietokoneesi päivitettynä

Yksi tietoturvan perusasioista on pitää Windows ja asennetut ohjelmat päivitettyinä. Tätä urakkaa helpottamaan löytyy ohjelmia kuten Personal Software Inspector. Olen tehnyt ohjeen Pidä asennetut ohjelmat päivitettyinä Personal Software Inspectorin avulla (https://peruskayttajalle.net/ohjeet/flexera_psi.php).

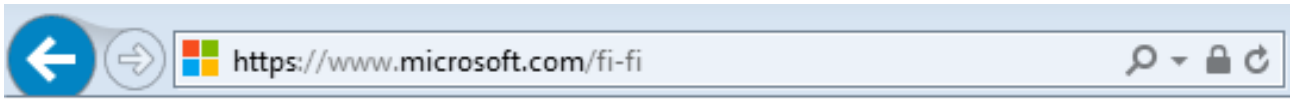
7. Käytä salattua HTTPS-yhteyttä

Nettisivuston ja käyttäjän välinen salattu HTTPS-yhteys suojaa siirrettävät tiedot niin, ettei kukaan ulkopuolinen pääse niihin käsiksi. Luonnollisesti tämä on olennaisen tärkeää esimerkiksi verkkopankkia käytettäessä.

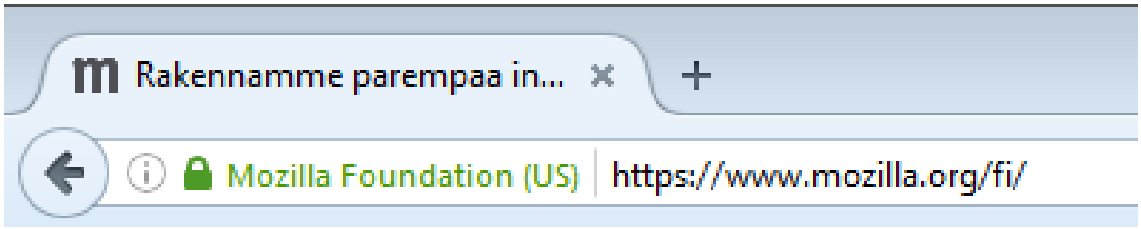
Nykyisin useat nettisivustot tarjoavat salatun HTTPS-yhteyden. Jos käytössä on salattu yhteys, lukee nettiselaimen osoiterivillä osoitteen edessä teksti *https* ja osoiterivillä on myös lukon kuva. Esimerkeissä Google Chromen osoiterivi (kuva 1), Internet Explorerin osoiterivi, jossa lukon kuva on osoiterivin lopussa (kuva 2) ja Mozilla Firefoxin osoiterivi (kuva 3).



Kuva 1



Kuva 2



Kuva 3

Tosin kaikki nettisivustot eivät tarjoa automaattisesti käyttöön salattua HTTPS-yhteyttä. Tämän ongelman voi ratkaista osittain nettiselaimeen asennettavalla HTTPS Everywhere -lisäosalla (https://www.eff.org/https-everywhere).

Olen tehnyt ohjeen Pakota salattu yhteys käyttöön HTTPS Everywherellä (https://perus-kayttajalle.net/ohjeet/https_everywhere.php).

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.

Olen käsitellyt nettisivustojen luotettavuuden arviointia tekemässäni ohjeessa Nettisivustojen luotettavuuden arviointi (https://peruskayttajalle.net/ohjeet/nettisivustojen_luotettavuus.php).

8. Varo lyhytlinkkejä

Lyhytlinkki on linkki jollekin nettisivulle, jonka osoite on lyhennetty lyhytlinkkipalvelulla (esimerkiksi Bitly, TinyURL.com). Esimerkiksi linkki *http://peruskayttajalle.net/ohjeet.php* muuttuu lyhytlinkkinä muotoon *http://bit.ly/1UVe0tk*.

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).

9. Tarvittaessa tarkista tiedosto haittaohjelmien varalta

Jos olet epävarma, onko jokin tiedosto turvallinen, kannattaa tiedosto tutkia 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).

10. Varo sähköpostin liitetiedostoja

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

Sähköpostin lähettäjän väärentäminen 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.

11. 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).

12. 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).

13. Rajoita Flash Playerin ym. nettiselaimen liitännäisten toimintaa

Nettiselaimissa (esimerkiksi Google Chrome, Internet Explorer, Mozilla Firefox) on erilaisia liitännäisiä, kuten Flash Player ja Java. Tietyt liitännäiset ovat myös tietoturvariski, koska esimerkiksi Flash Playerista löytyy jatkuvasti haavoittuvuuksia, joita hyödyntämällä voi tehdä kaikenlaista ikävää tietokoneelle.

Siksi on syytä asettaa etenkin Flash Player tilaan, jossa se ei käynnisty automaattisesti. Tällöin liitännäinen käynnistyy ainoastaan, kun annat siihen luvan (englanninkielinen termi ”Click-to-play”). Olen tehnyt ohjeen Rajoita nettiselaimen liitännäisten toimintaa (https://peruskayttajalle.net/ohjeet/nettiselaimen_liitannaiset.php).

Jos et ole varma, mitä nettiselainta käytät, Peruskäyttäjälle.netistä löytyy linkki (https://peruskayttajalle.net/linkit.php#selain) asian tarkistamiseen.

14. 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, 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. Pienempien tietomäärien varmuuskopiointiin sopivat myös muistitikut. Olen käsitellyt muistitikkujen käyttöä varmuuskopiointiin ohjeessa Muistitikun käyttö (https://peruskayttajalle.net/ohjeet/muistitikku.php) ja ulkoisia kiintolevyjä ohjeessa Ulkoisen kiintolevyn käyttö (https://peruskayttajalle.net/ohjeet/ulkoinen_kiintolevy.php).

15. Käytä normaalia käyttäjätiliä

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).

16. Hävitä muistitikut, tietokoneen kiintolevy ym. muistit asianmukaisesti

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

Kiintolevyn ohjelmallinen pyyhkiminen onnistuu vain ehjien kiintolevyjen kohdalla ja vaatii osaamista tai hyvät ohjeet. Näistä syistä johtuen peruskäyttäjän on helpointa toimittaa tietokoneensa, kännykkänsä, muistitikkunsa yms. lukittuun data-SER-keräysastiaan.

Lisätietoa aiheesta löytyy Peruskäyttäjälle.netin Linkit -sivulta (https://peruskayttajalle.net/linkit.php#elker).

17. Älä kytke Käyttäjätilien valvontaa pois päältä

Käyttäjätilien valvonta (englanniksi ”User Account Control” eli ”UAC”) on tärkeä osa Windowsin tietoturvaa. 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 Windows 7:ssä Käyttäjätilien valvonta kyselee aika harvoin mitään 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).

18. Poista käytöstä Windowsin käyttömukavuuden kehitysohjelma

Microsoftin yksi keino kerätä erilaista tietoa tietokoneen käytöstä Windows 7:ssä on Windowsin käyttömukavuuden kehitysohjelma (englanniksi ”Customer Experience Improvement Program” eli ”CEIP”).

Microsoft ei ole kertonut julkisesti, mitä kaikkia tietoja kehitysohjelma kerää. Siksi siihen on syytä suhtautua varauksella. Jos Windows 7:n asennuksen yhteydessä käytetään suositeltuja asetuksia, Windowsin käyttömukavuuden kehitysohjelma otetaan käyttöön automaattisesti.

Tekemässäni ohjeessa Vähennä Windows 7:n tiedonkeruuta (https://peruskayttajalle.net/ohjeet/ceip.php) neuvotaan, kuinka kehitysohjelman voi poistaa käytöstä helposti.

19. Poista käytöstä Microsoft Officen makrot

Niin sanotut makrovirukset ovat olleet riesana jo todella kauan. Välillä makrovirukset käytännössä hävisivät, mutta viime aikoina ne ovat tehneet paluun. Makrovirukset liittyvät lähinnä Microsoft Officeen, jossa on mahdollista automatisoida toimintoja makrojen avulla. Ikävä kyllä tämä mahdollistaa myös haittaohjelmien asentamisen.

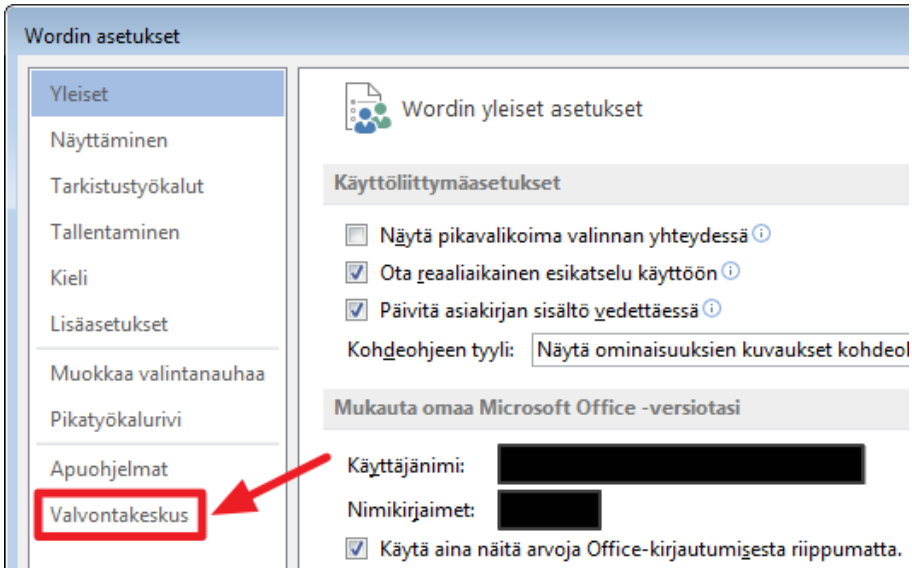
Tästä syystä makrot kannattaa poistaa käytöstä kokonaan Microsoft Officessa, koska makrot eivät ole mitenkään välttämättömiä. Asetukset vaihtelevat Officen eri versioiden välillä. Esimerkiksi Microsoft Office 2013:n Wordissa tämä tapahtuu seuraavasti:

1. Napsauta Wordissa **Tiedosto** -välilehteä.

2. Napsauta vasemmassa reunassa alimmaisena olevaa **Asetukset** -kohtaa (kuva 4).

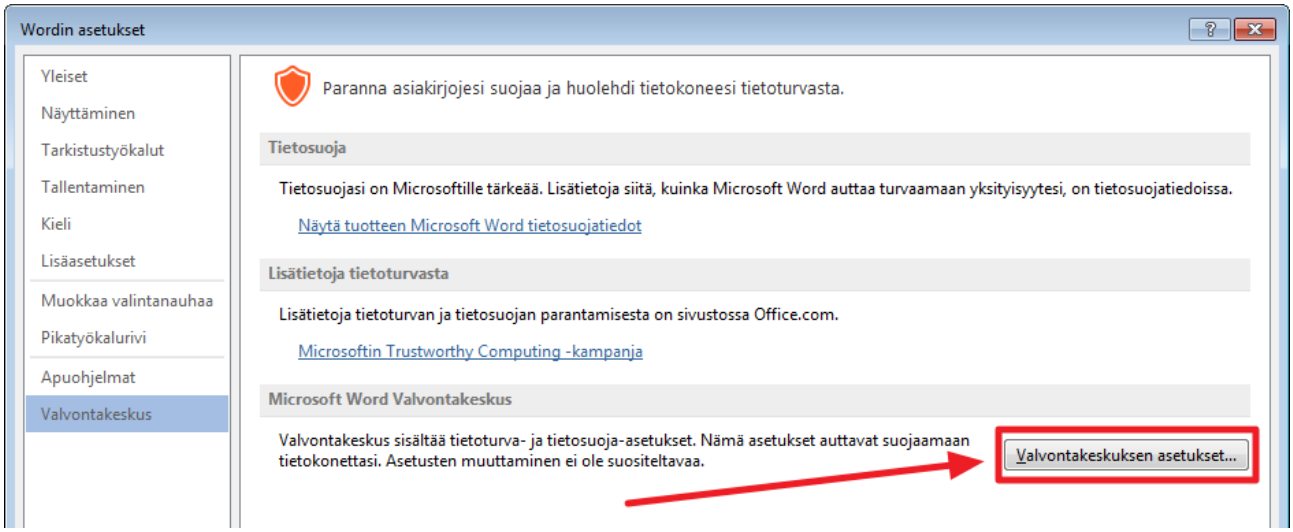
Kuva 4

3. Avautuvassa **Wordin asetukset** -ikkunassa napsauta alimmaisena olevaa **Valvontakeskus** -kohtaa (kuva 5).



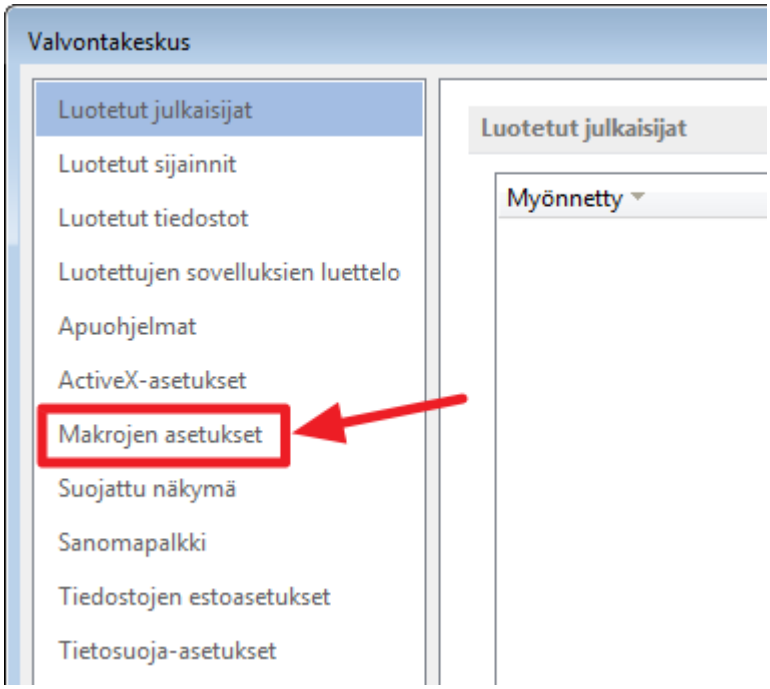
Kuva 5

4. Seuraavaksi napsauta oikeassa reunassa olevaa **Valvontakeskuksen asetukset** -painiketta (kuva 6).



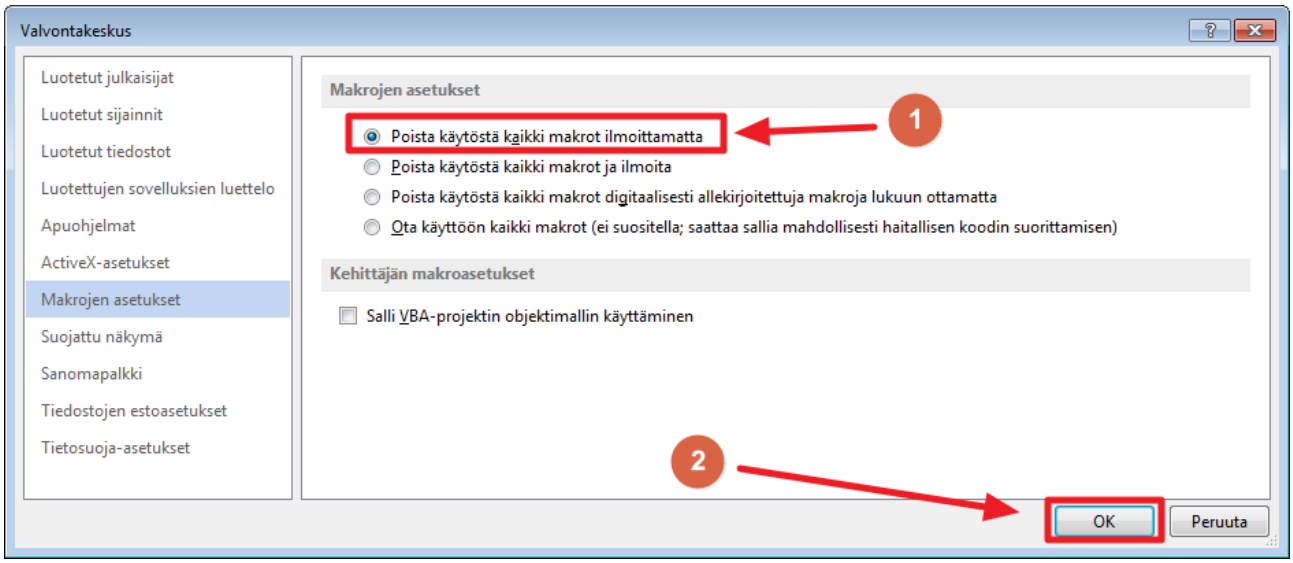
Kuva 6

5. Avautuvassa **Valvontakeskus** -ikkunassa napsauta kohtaa **Makrojen asetukset** (kuva 7).



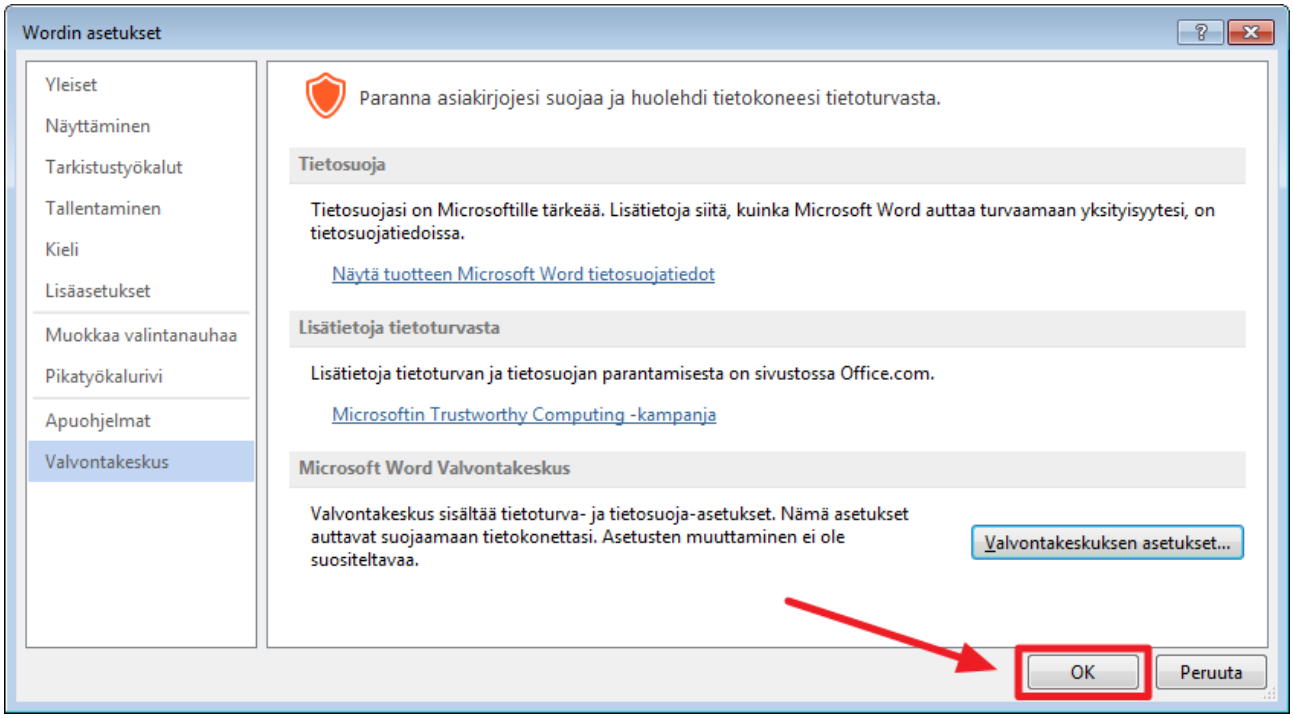
Kuva 7

6. Otsikon **Makrojen asetukset** alla valitse kohta **Poista käytöstä kaikki makrot ilmoittamatta**. Sen jälkeen napsauta ikkunan oikeassa alareunassa olevaa **OK** -painiketta (kuva 8).



Kuva 8

7. Napsauta **Wordin asetukset** -ikkunan oikeassa alareunassa olevaa **OK** -painiketta (kuva 9).



Kuva 9

8. Toista vaiheet 1–7 Wordin lisäksi myös Excelissä ja PowerPointissa.

Lisätietoa makroviruksista löytyy esimerkiksi Ilta-Sanomien artikkelista Tässä on kaksi Wordin antamaa ilmoitusta: Tiedätkö kumpi on vaarallinen? (http://www.iltasanomat.fi/digitoday/tietoturva/art-2000001913854.html).

20. Älä lataa ja asenna ohjelmia mistä tahansa

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

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

21. Älä tallenna salasanoja nettiselaimeen

Nettiselaimissa on mahdollisuus tallentaa nettisivustojen salasanoja, jolloin niitä ei tarvitse kirjoittaa kirjautuessa jollekin nettisivustolle. Salasanojen tallentamista nettiselaimeen ei kuitenkaan pidä käyttää, koska salasanoja ei ole suojattu kunnolla. Tietokoneelle asentunut haittaohjelma tai murtautuja pystyy varastamaan nettiselaimeen tallennetut salasanat helposti.

Asiasta on kirjoittanut myös Tietoviikko (http://www.tivi.fi/Kaikki_uutiset/tama-selaimen-kateva-ominaisuus-on-paha-tietoturvariski-1-7-miljoonan-kayttajan-tiedot-paljastuivat-6578634).

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 ns. negatiivisella marginaalilla, jolloin lomakekentät ovat kyllä olemassa nettisivulla, mutta ne eivät näy käyttäjälle.

Suomessa asiasta on kirjoittanut mm. Ilta-Sanomat (http://www.iltasanomat.fi/digi-today/tietoturva/art-2000005040608.html). Jos et ole varma, mitä nettiselainta käytät, Peruskäyttäjälle.netistä löytyy linkki (https://peruskayttajalle.net/linkit.php#selain) asian tarkistamiseen.

22. 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.

23. 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), jossa mm. käydään läpi perusasiat linkkien todellisen osoitteen selvittämisestä.

24. 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 turvakysymyksien vastausten tulisi olla satunnaisia sanoja tai satunnaisia kirjain- ja numerosarjoja.

25. Käytä kaksivaiheista tunnistautumista

Perinteinen kirjautuminen erilaisiin verkkopalveluihin käyttäjätunnuksella ja salasanalla ei ole tietoturvan kannalta paras mahdollinen ratkaisu, koska ne eivät anna riittävää 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 koodeista älypuhelimeen asennettaviin ohjelmiin ja tietokoneeseen liitettäviin muistitikkuihin.

Lisätietoa aiheesta löytyy esimerkiksi Googlen kaksivaiheista tunnistautumista esittelevältä nettisivulta (https://www.google.com/intl/fi/landing/2step/) ja Wikipediasta (https://fi.wikipedia.org/wiki/Kaksivaiheinen_tunnistautuminen).