[Yleistä tietokoneviruksista 1](#_Toc304279539)

[Erilaisia viruksia ja tuholaisia 1](#_Toc304279540)

[Suojautuminen viruksia vastaan 2](#_Toc304279541)

[Virustartunnan vältteleminen 2](#_Toc304279542)

# Yleistä tietokoneviruksista

Tietokonevirukseksi kutsutaan tietokoneohjelmaa, joka monistaa itseään ja pyrkii tartuttamaan itsensä tietokoneeseen. Leviämisen jälkeen virus ennemmin tai myöhemmin aktivoituu ja suorittaa toimenpiteet, joita viruksen tekijä on halunnut sen tekevän. Toimenpiteet voivat vaihdella aina piloista hyvinkin vakaviin vahinkoihin, kuten esimerkiksi arkaluontoisten tiedostojen lähettämiseen sähköpostitse keskusteluryhmiin.

Viruksen määrittelyn ulkopuolelle jää muutamia nykyaikaisia tuholaisia ja riesoja, joista kannattaa olla tietoinen. Seuraavissa luvuissa esitellään erilaisia tietokoneviruksia ja muita tuholaisia, joista on tullut yhä jokapäiväisempi riesa tietokoneiden käyttäjille.

# Erilaisia viruksia ja tuholaisia

Perinteisesti virukset luokiteltu esimerkiksi niiden leviämistavan mukaan.

* Sovellusohjelmavirukset eli makrovirukset leviävät sovellusohjelmatiedostojen, kuten esimerkiksi Word-dokumentit, mukana. Makrovirukset on tehty kyseisen sovellusohjelman makrokielellä. Nykyisin varsinkin Microsoftin tuotteissa on niin kehittynyt makrokieli, että makrovirukset ovat erittäin tehokkaita.
* Tiedostovirukset leviävät ohjelmatiedostojen, kuten esimerkiksi .exe- ja .com-tiedostojen, mukana. Nykyiset virukset leviävät kohtuullisen harvoin ohjelmatiedostojen mukana, mutta toki poikkeuksiakin löytyy.
* Levykevirukset eli käynnistyslohkovirukset leviävät yleensä koneista toiseen levykkeiden välityksellä. Nykyisin levykkeiden käyttö on niin vähäistä, että käynnistyslohkoviruksia ei enää juuri tapaa.

Maailmalla liikkuu myös muita tuholaisia, joita ei luokitella varsinaisiksi viruksiksi, mutta jotka voivat aiheuttaa yhtä korvaamatonta tuhoa kuin viruksetkin.

\* Mato on ohjelma, joka leviää itsekseen tietokoneisiin käyttäen hyväksi järjestelmistä löytyviä tietoturva-aukkoja. Matoa ei perinteisesti käsitetä virukseksi, mutta nykyään esiintyvistä viruksista on suurin osa matomaisesti itseään levittäviä. Tämän vuoksi madoiksi käsitetään tässä yhteydessä kaikki nykyaikaiset skriptivirukset.

\* Troijan hevonen on ohjelma, joka sisältää jotakin muuta kuin käyttäjä uskoo sen sisältävän. Troijan hevosta ei pidetä viruksena, koska ne eivät tartuta itseään koneeseen viruksen tavalla. Troijan hevosia käytetään yleensä järjestelmän salasanojen urkkimiseen. Nykyisten virusten mukana voi tulla myös Troijan hevonen, joka kerää salasanatietoja ja lähettää ne sitten viruksen tekijälle.

\* Ohjelmien odottamaton toiminta tai käyttäjä ovat edelleenkin usein esiintyvä vitsaus, joiden seurauksena häviää tietoja. Aina ei tosiaankaan ole kyse viruksista, jos tapahtuu jotakin odottamatonta.

Sähköpostin käytön lisääntyminen on tuonut mukanaan muutamia lisäharmeja, jotka eivät sellaisenaan ole vaarallisia, mutta joista aiheutuu riesaa koko ajan.

\* Hoaxit ovat sähköpostihuhuja ja -huijausvaroituksia, jotka eivät ole totta, mutta joita ihmiset lähettävät helposti edelleen.

\* Spam on roskapostia, jota sähköpostilaatikko tulee pullolleen koko ajan.

Nykyaikaisissa viruksissa on hyvin monenlaisen tuholaisen tai harmin piirteitä, joka tekee viruksista entistä vaarallisempia. Nykyään virukset voivat levitä madon tavoin koneesta toiseen ja samalla ne voivat saastuttaa ohjelma- tai sovellusohjelmatiedostoja. Virukset voivat levitä myös sähköpostin liitetiedostona tai viruksen voi saada WWW:stä ladatun tiedoston mukana. Viruksissa voi olla mukana Troijan hevonen, jolla saadaan halutut salasanat tietoonsa. Lisäksi monet nykyisistä viruksista yrittävät levittää itseään sähköpostin välityksellä.

## Suojautuminen viruksia vastaan

Viruksentorjunta ja niiden leviämisen estäminen on jokaisen tietokoneen käyttäjän velvollisuus. Jokainen sähköpostin käyttäjä on velvollinen tarkistamaan sähköpostitse saamansa ja lähettämänsä dokumentit. Koskaan ei tiedä mitä ne sisältävät, vaikka ne tulisivat luotettavaltakin taholta. Aina kannattaa olla varovainen, mutta ei kuitenkaan vainoharhainen. Seuraavaan on koottu sekä yleisiä että viruskohtaisia ohjeita virustorjuntaan:

\* Hanki virustorjuntaohjelma ja huolehdi sen päivityksestä

\* Huolehdi ohjelmistojen ja käyttöjärjestelmän päivityksestä

\* Tarkista aina saamasi dokumentit ennen niiden aukaisemista

\* Älä lähetä sovellusohjelmatiedostoja sähköpostitse

\* Tarkista dokumentit ennen niiden lähettämistä

\* Poista sähköpostiohjelmista liitetiedostojen automaattinen aukaisu

\* Makrovirusvaroitukset kannattaa kytkeä päälle

\* Pidä torjuntaohjelma aktiivisena

## Virustartunnan vältteleminen

Nykyisille matoviruksille on tunnusomaista riippuvuus sopivista ohjelmistoista ja olosuhteista. Esimerkiksi useimmat matovirukset tarvitsevat tiettyä sähköpostiohjelmaa tai tietyn ohjelman tietoturva-aukkoja levitäkseen.

Matoviruksille ovat tällä hetkellä erityisen alttiina sellaiset ihmiset, jotka käyttävät MS Office-tuoteperheen tuotteita. Tarttuessaan jotkin matovirukset voivat lähettää itseään eteenpäin, mutta se vaatii otollisen ympäristön. Esimerkiksi joidenkin virusten leviäminen on mahdollista, jos tietokoneessa on tietty Outlook-sähköpostiohjelman versio sekä osoitteisto ja Internet Explorerin tietty versio tietyillä tietoturva-aukoilla.

Jos luet kaiken sähköpostisi Unix- tai Linux-ympäristössä, ei sinulla ole välitöntä matoviruksen tartuntavaaraa. Saamasi liitetiedostot voivat kuitenkin sisältää viruksia, joten niitä ei kannata lähettää eteenpäin ennen tiedostojen tarkistamista. Kun liitetiedosto siirretään Windows-koneelle ja aukaistaan ilman tarkistamista, niin silloin liitteessä ollut virus voi tarttua. Liitetiedostojen kanssa täytyy siis olla tarkkana!

Välttelyssä kannattaa kuitenkin pitää järki mukana. Vaikka virukset kiusaavat tällä hetkellä Microsoftin ohjelmien käyttäjiä, niin viruksia kirjoitetaan myös muidenkin ohjelmistotalojen ohjelmistoille. Viruksia aletaan kirjoittaa enemmän muillekin ohjelmistoille, kun niiden käyttö on riittävän laajaa!

Virusten tulevaisuutta käsittelevissä artikkeleissa visioidaan nykyistäkin nopeammin leviäviä viruksia, jotka olisivat entistä riippumattomampia käytetystä alustasta. Tällaisten virusten varalta ei siis kannata perustaa virussuojaansa pelkän välttelyn varaan!