

Joka kodin tietoturvaopas

www.tietoturvaopas.fi



turvallisesti @ nettiin
kansalliset tietoturvatalkoot

Joka kodin tietoturvaopas

Suojaamaton tietokoneesi on internetissä turvassa noin minuutin. Sitten alkaa tapahtua.

Internetin ja sähköpostin välityksellä leviävät virukset, madot ja muut lierot varastavat tiedostojasi ja salasanojasi, käyttävät väärin henkilöllisyyttäsi ja tuhoavat ohjelmistojasi.

Verkkomato orjuuttaa käden käänteessä suojaamattoman tietokoneesi miljoonien roskapostiviestien lähetystoimistoksi ilman, että Sinulla on aavistustakaan asiasta. Muuttaman päivän jälkeen operaattorisi ottaa Si-

nuun yhteyttä ja pian häirikkökone suljetaan verkon ulkopuolelle.

Tietokoneesi on tässä vaiheessa jo siivottomassa kunnossa.

Tietokonevirukset ja verkkomadot ovat viimeisen vuoden aikana lisääntyneet ja saaneet maailmalla aikaan vakavia tuhoja. Nämä haittaohjelmat uhkaavat pahimmillaan koko tietoyhteiskunnan kehitystä.

Onneksi tietokoneen voi suojata hyökkäyksiltä. Tämä opas kertoo, miten.

Lisää tietoa löydät osoitteesta <http://www.tietoturvaopas.fi>

Sisältö

- Miten internetiä käytetään? **3**
- Nettikäytön uhat **3**
- Kolme askelta tietoturvaan **4**
- Sähköpostin turvallinen käyttö **5**
- Miten virus poistetaan? **5**
- Roskaposti jätekuljetukseen **6**
- Kun otat uuden koneen käyttöön **6**
- Windows-käyttöjärjestelmien päivitysohjeet **7**
- Mistä apua? **8**

SÄILYTÄ TAMÄ OPAS!



Tämän oppaan tuottivat:

- Computer Associates Finland
- Eduskunnan Liikenne- ja viestintävaliokunta
- Elisa Oyj
- Finnet-ryhmä
- F-Secure Oyj
- Liikenne- ja viestintäministeriö
- Microsoft Oy
- Nordea Pankki Suomi Oyj
- Nokia Oyj
- Pelastakaa Lapset ry
- TeliaSonera Finland Oyj
- Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry
- Tietosuojavaltuutetun toimisto
- Tietoturva ry
- Viestintävirasto

Miten internetiä käytetään?

Internetin käyttämiseen tarvitaan tietokone ja internetyhteys. Yleisimmin käytettyjä internetpalveluja ovat www-sivujen selailu ja sähköposti, joiden käyttämiseen tarvitaan selainohjelma (yleisimmin Internet Explorer tai Netscape) ja sähköpostiohjelma. Internetliit-

tymät ovat erilaisia: puhelinmodeemi- ja ISDN-liittymät ovat auki vain silloin, kun käyttäjä ne avaa, laajakaistaliittymät eli yleensä ADSL-liittymät taas ovat aina auki, kun tietokonekin on päällä.

Nettikäytön uhat

Internetiin kytketty suojaamaton tietokone on jatkuvasti alttiina verkkohyökkäyksille, kuten viruksille ja tietomurroille.

Virukset ja madot

Virukset ja madot ovat haittaohjelmia. Niitä tulee tietokoneelle sähköpostista, internetistä ja erilaisten tiedostojen mukana. Uusia levitystapoja keksitään lisää jatkuvasti.

Virus on pieni ohjelma, joka leviää yleensä itsestään ja aiheuttaa lähes aina haittaa tietokoneelle, siinä käytettäville ohjelmille sekä tietokoneen käyttäjälle.

Sähköpostimato, kuten Sobig.F tai Mydoom, voi lähettää itsensä kaikkiin käyttäjän osoitekirjassa oleviin osoitteisiin ja saattaa vielä liittää viestin mukaan tietokoneella olevia tietoja.

Virukset voivat myös muuttaa tietokoneen roskapostin lähetystoimistoksi. Tällainen kone lähettää automaattisesti suuria määriä viestejä ilman, että käyttäjä sitä edes huomaa.

Verkkomadot, kuten Slammer ja Lovsan, etsivät internetiin kytkettyjä koneita, joihin ei ole asennettu viimeisimpiä korjauspäivityksiä. Madot leviävät viruksia huomattavasti nopeammin suoraan koneelta toiselle.

Troijan hevoseksi kutsutaan haittaohjelmaa, joka naamioidaan vaikkapa viattoman näköiseksi peliksi, mutta joka voi esimerkiksi tuhota tiedostoja tietämättäsi.

Tietomurrot ja -varkaudet

Tietomurtautujia kutsutaan hakkereiksi tai krakkereiksi. He voivat esimerkiksi murtautua suojaamattomalle tietokoneelle ja käyttää sitä kuten omaansa. He voivat myös varastaa tiedostojasi tai henkilökohtaisia tietojasi (esimerkiksi salasanoja tai luotokorttinumeron) ja käyttää niitä väärin tarkoituksiin.

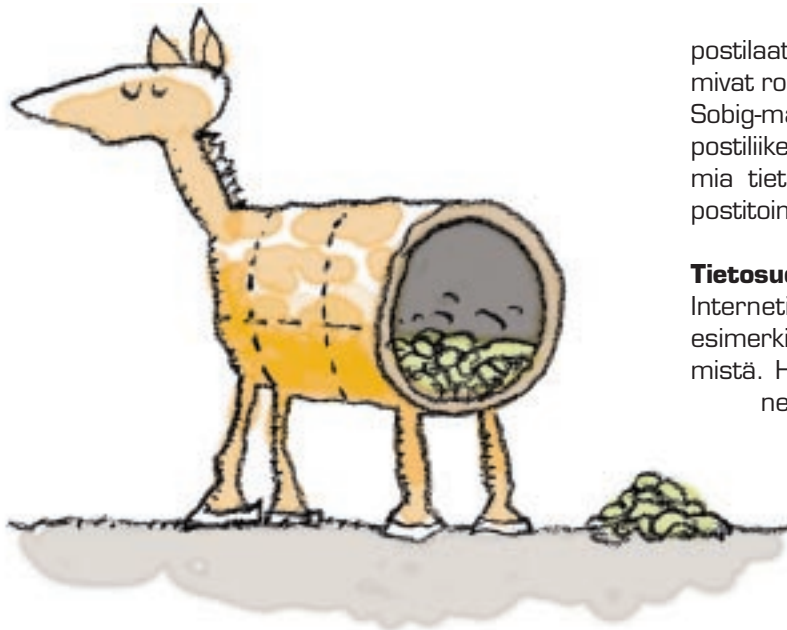
Tietomurtautuja tai haittaohjelma voi tunkeutua suojaamattomalle tietokoneelle ja asentaa sinne takaporttiohjelman. Se avaa reitin tietokoneelle, jota voidaan käyttää toiselta koneelta ilman, että koneen omistaja huomaa mitään.

Huijaukset ja ketjukirjeet

Sähköpostia käytetään monenlaisiin huijausyrityksiin. Rahaa anelevat "nigerialaiskirjeet" ovat niistä hyvä esimerkki.

Rahananeluviesteihin ja vaikkapa ketjukirjeisiin kannattaa suhtautua suurella varauksella, eikä niihin kannata vastata tai lähettää niitä eteenpäin.





Roskaposti eli spämmi

Roskapostiksi kutsutaan ei-toivottua, suurina massoina lähetettyä, ei kenellekään erityisesti kohdistettua sähköpostiviestintää, josta on tullut kasvava ongelma. Se ruuhkauttaa sähköpostijärjestelmiä ja tukkii ihmisten sähkö-

postilaatikoita. Jotkut sähköpostimadot toimivat roskapostittajien työkaluna. Esimerkiksi Sobig-mato aiheutti valtavan määrän roskapostiliikennettä kaappaamalla suojaamattomia tietokoneita ja käyttämällä niitä roskapostitoimistoina.

Tietosuojaja

Internetistä kerätään sähköpostiosoitteita esimerkiksi web-sivustoista tai keskusteluryhmistä. Harkitse tarkkaan, mihin annat internetissä henkilökohtaisia tietojasi kuten nimeä tai sähköpostiosoitetta. Jos jollakin sivustolla kysytään tietojasi, tarkista, että sivuston ylläpitäjä kertoo rekisteriselosteessa, mihin ja miten tietoja käytetään ja luovutetaanko niitä edelleen.

Kaikki ei sovi lasten silmille

Internetissä on paljon materiaalia, joka ei sovi lapsille tai alaikäisille. Keskustele lastesi kanssa surffailusta ja internetin turvallisesta käytöstä. Ideoita ja neuvoja saat Pelastakaa lapset ry:n nettisivuilta osoitteesta <http://www.pela.fi/nettivihje/ohjeita.htm>

Kolme askelta tietoturvaan

Internetin häiriöiltä ja haitoilta voi suojautua, kun muistaa huolehtia oman tietokoneen tietoturvasta. Myös puhelinmodeemiliittymää käyttävä tietokone tulee suojata.

1 Pidä tietokoneen käyttöjärjestelmä ajan tasalla

Tietoturvan kannalta on tärkeää, että käyttöjärjestelmä ja ohjelmat pidetään ajan tasalla. Ajan tasalla pitäminen tarkoittaa sitä, että säännöllisin väliajoin tarkistetaan, onko käyttöjärjestelmään tullut uusia korjauksia tai päivityksiä, ja tarvittaessa asennetaan ne. Ohjeita Windows-käyttöjärjestelmien päivittämiseen löytyy tämän oppaan lopusta.

2 Asenna virustorjunta ja pidä se ajan tasalla

Viruksilta ja madoilta suojaudutaan virustorjuntaohjelmalla tai -palvelulla. Niitä saa muun muassa internetoperaattoreilta, tietokone-myymälöistä tai internetistä. Jos lataat virustorjuntaohjelman internetistä, käytä vain luotettavan ohjelmistotarjoajan palveluja.

Virustorjuntaohjelma tutkii koneessasi olevia ja siinä käsiteltäviä tiedostoja, sähköpostiviestejä sekä internetistä selaimen kaut-

ta lataamiasi tiedostoja ja pyrkii poistamaan haitalliset tiedostot.

Huolehdi, että virustorjuntaohjelmasi on jatkuvasti ajan tasalla. Jos ohjelmistossasi ei ole automaattista päivitystä, joudut tekemään sen itse.

Internetoperaattorien tarjoama suodatuspalvelu poistaa virukset sähköposteistasi jo ennen kuin ne saapuvat koneellesi.

3 Asenna palomuuuri ja huolehdi sen päivityksestä

Virustorjuntaohjelma ei estä koneelle tulevia murtoyriytyksiä. Tietomurtojen ja verkkohyökkäysten estämiseen tarvitaan palomuuuri. Palomuuuri on yleensä tietokoneelle asennettava ohjelma, joka valvoo koneen tietoliikennettä.

Monet tietoturvayhtiöt tarjoavat ohjelmistopaketteja, joihin kuuluu sekä palomuuuri että virustorjuntaohjelmisto. Ne sisältyvät myös operaattoreiden tarjoamaan kuukausi-veloitteiseen tietoturvapalveluun.

Palomuuuri asennetaan tietokoneelle samalla tavoin, kuin muutkin tietokoneohjelmat, ohjeita seuraten. Palomuuriohjelma tulee päivittää aina, kun ohjelmatoimittaja ilmoittaa päivityksen tarpeesta.

- Microsoft ei koskaan lähetä korjauksia sähköpostin välityksellä, vaan käyttäjiä kehoitetaan aina menemään Microsoftin sivuille (esimerkiksi osoitteeseen <http://windowsupdate.microsoft.com>) asentamaan korjaus. Jos saat sähköpostin, jonka lähettäjä näyttäisi olevan Microsoft ja jossa kehoitetaan asentamaan liitteenä oleva korjaus, sähköposti ei ole todellisuudessa Microsoftilta, vaan kyseessä on todennäköisimmin sähköpostimato tai -virus.

- Virustorjuntaohjelmia tekevät yritykset eivät lähetä päivityksiä sähköpostiin. Päivitystiedot tulisi aina hakea virustorjuntayrityksen kotisivulta tai käyttämällä virustorjuntaohjelmiston päivitystoimintoa.

Sähköpostin turvallinen käyttö

1 Älä avaa epäilyttäviä sähköpostin liitetiedostoja. Varo erityisesti sellaisia liitetiedostoja, joiden pääte on .COM, .EXE, .SHS, .PIF tai .VBS. Suhtaudu erityisen epäluuloisesti tiedostoihin, joissa on kaksiosainen tiedostopääte, esim. TIEDOSTO.JPG.VBS tai TEKSTI.DOC.EXE. Poista viestit liitetiedostoihin.

2 Jos sähköpostiviesti näyttää epäilyttävältä, poista se avaamatta sitä. Suhtaudu varauksella viesteihin, jotka on kirjoitettu kielellä, jota lähettäjä ei yleensä käyttäisi. Muista, että viruksen tai madon sisältämä viesti voi tulla myös liiketuttavaltasi tai ystävältäsi.

3 Jos sähköpostiohjelmassasi on esikatselutoiminto, käytä sitä varoen.

Lisätietoja sähköpostin turvallisesta käytöstä löydät osoitteesta www.tietoturvaopas.fi



Miten virus poistetaan?

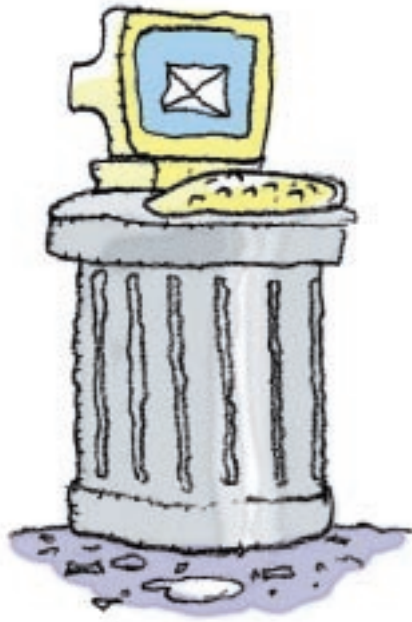
Kun käytössäsi on ajan tasalla oleva virustorjuntaohjelma, se poistaa automaattisesti kaikki tunnetut virukset. Jos löydät viruksen sähköpostilaatikosta, poista saastunut viesti avaamatta tai esikatsellematta sitä.

Jos epäilet, että koneessasi on virus ja käytössäsi ei ole viruksentorjuntaohjelmaa, hanki ja asenna sellainen. Asentamisen jäl-

keen ohjelma tarkistaa ja siivoaa koneen. Joissakin tapauksissa viruksen tai madon poistamiseen tarvitaan erillinen korjausohjelma tai ohjeistus, jonka saa esimerkiksi tietoturvayhtiöiden web-sivustolta.

Joskus koneen puhdistaminen vaatii asiantuntijan apua.

Roskaposti jätekuljetukseen



- 1** Älä koskaan avaa epäilyttäviä viestejä, vaan poista ne suoraan viestivalikosta.
- 2** Älä koskaan vastaa roskaposti-viestiin.
- 3** Ota käyttöön operaattorin ja sähköpostiohjelman mahdollinen roskapostin suodatusominaisuus.
- 4** Luovuta harkiten sähköposti-osoitteesi esimerkiksi internet-sivujen kyselyihin ja keskustelupalstoille.
- 5** Älä lähetä ketjuviestejä tai kierto-kirjeitä edelleen.

Kun otat uuden tietokoneen käyttöön

1 Tarkista ennen internetyhteyden kyt-kemistä, että tietokoneeseen on asennettu palomuri. Jos uuden koneesi käyttöjärjestelmä on Windows XP, kytke siihen kuuluva palomuri päälle ja käytä sitä, kunnes olet asentanut erillisen palomuriohjelmiston sekä virustorjuntaohjelman. Useimmat tietoturvaohjelmistot vaativat asennetta-essa internetyhteyden.

2 Nyt voit laittaa verkkokaapelin paikalleen ja avata internetyhteyden.

3 Asenna koneeseen virustorjuntaohjelma ja palomuri.

4 Jos käytössäsi on Windows-käyttöjärjestelmä, hae osoitteesta <http://windowsupdate.microsoft.com> viimeisimmät suojauspäivitykset käyttöjärjestelmäsi.

5 Ota käyttöjärjestelmän automaattisen päivitystoiminto käyttöön. Näin Windows hakee automaattisesti kriittiset turvapäivitykset koneellesi aina kun koneesi on kytketty internetiin.



Useimmissa uusissa kotitietokoneissa on Windows XP -käyttöjärjestelmä, jossa on helppokäyttöinen palomuri. Palomuri kytketään päälle näin: avaa **Käynnistä**-valikko ja valitse sieltä **Ohjauspaneeli**. Valitse Ohjauspaneelistä vaihtoehto **Verkkoyhteydet**. Napsauta internetyhteyden kuvaketta hiiren kakkospainikkeella (yleensä hiiren oikea painike), valitse **Ominaisuudet**, sen jälkeen **Lisäasetukset**-välilehti ja sieltä kohta **Internetyhteyden palomuri: Suojaa tätä tietokonetta ja verkkoa rajoittamalla tietokoneen käyttämistä internetin välityksellä**. Kun vaihtoehto on valittu, poistut ikkunasta napsauttamalla **OK**-painiketta. Windows XP:n palomuri on käytössä.

Windows-käyttöjärjestelmien päivitysohjeet

Windows-käyttöjärjestelmään tarjolla olevien korjausten tarkistamiseen ja niiden asentamiseen on olemassa kaksi eri tapaa:

A) Windows Update -sivusto

on Microsoftin verkkopalvelu, josta voit itse tarkistaa, mitä korjauksia ja päivityksiä tietokoneeseesi asennettuun käyttöjärjestelmään on tarjolla. Voit valita ne korjaukset ja päivitykset, jotka haluat asentaa. Tämä palvelu toimii myös suomeksi ja löytyy osoitteesta <http://windowsupdate.microsoft.com>. Lisätietoja Windows Update -sivuston käyttämisestä löytyy edellä mainitusta osoitteesta sekä tietoturvaoppaasta osoitteesta <http://www.tietoturvaopas.fi>

Huomautus: Windows Update -sivustolla voit päivittää seuraavat käyttöjärjestelmät: Windows 98 ja Windows 98 SE, Windows ME, Windows 2000, Windows XP ja Windows Server 2003. Mikäli käytössäsi on Windows 95 tai Windows NT, saat päivitykset osoitteesta <http://www.microsoft.com/downloads>

B) Automaattinen päivitys

on käyttöjärjestelmään kuuluva toiminto, joka hakee automaattisesti kriittiset turvapäivitykset koneellesi aina, kun koneesi on kytketty internetiin.

Automaattinen päivitystoiminto on käytettävissä koneissa, joissa on Windows ME, Windows 2000, Windows XP tai Windows Server 2003.

Alla olevat ohjeet automaattisen päivitystoiminnon käyttämisestä on tarkoitettu koneisiin, joiden käyttöjärjestelmä on Windows XP. Muiden Windows-käyttöjärjestelmien automaattisen päivitystoiminnon käyttöönotosta löydät lisätietoja osoitteesta <http://www.tietoturvaopas.fi>

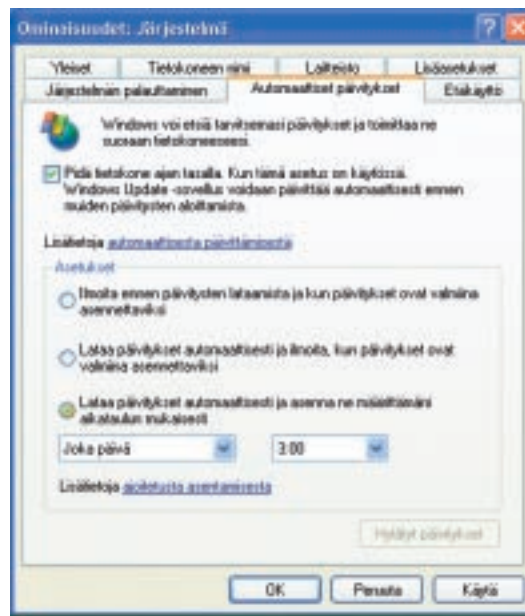
Automaattisen päivitystoiminnon käyttöönotto

Voit ottaa automaattisen päivitystoiminnon käyttöön seuraavasti:

1 Avaa **Käynnistä**-valikko ja napsauta hiiren kakkospainiketta (yleensä oikea painike) vaihtoehdon **Oma tietokone** kohdalla. Näyttöön tulee seuraavan kuvan kaltainen valikko:



2 Valitse valikosta vaihtoehto **Ominaisuudet**. Näyttöön tulee **Ominaisuudet: Järjestelmä** -ikkuna. Valitse ikkunassa **Automaattiset päivitykset** -välilehti, jonka jälkeen näytössä on seuraavan kuvan esittämä ikkuna:



3 Jos haluat, että käyttöjärjestelmään ladataan Windows Update -sivustolle tulevat tietoturvapäivitykset automaattisesti, valitse kohta **Lataa päivitykset automaattisesti ja asenna ne määrittämällä aikataulun mukaisesti** ja valitse sen jälkeen ajankohta, jolloin päivitykset ladataan ja asennetaan, esim. "Joka päivä" ja "10.00". Tämän jälkeen käyttöjärjestelmä lataa päivitykset määrittämänäsi ajankohtana ja asentaa ne.

Mistä apua?

Jos tietokoneesi ei toimi

- Ota yhteys laitemyyjään tai valtuutettuun huoltoliikkeeseen

Jos epäilet virusta

- [www://support.f-secure.fi](http://support.f-secure.fi)
- <http://www3.ca.com/virusinfo/>

Jos haluat tietoa

käyttöjärjestelmäsi, ohjelmiesi ja selaimesi turvapäivityksistä

- <http://windowsupdate.microsoft.com>
- <http://www.microsoft.fi/tietoturva>

Jos haluat vähentää roskapostia

- Ota käyttöön sähköpostiohjelmiasi roskapostin suodatusominaisuus
- Ota yhteys operaattoriisi

Jos internetyhteys ei toimi

Ota yhteys operaattoriisi

- Elisa: Vikailmoitukset, 24 h, puh. 10 019
- Sonera: Tekninen asiakaspalvelu, vikailmoitukset (24 h) 0800 19 101
- Paikalliset puhelinyhtiöt: 0800 30109
- DNA: Tekninen tuki, puh. 0600 390 907 (arkisin 9–22, lauantaina 10–16), puhelun hinta on pvm/mpm + 0,37 €/min. (sis. alv. 22 %)

Tietoturvasta ja -suojusta lisätietoja saat

- <http://www.tietoturvaopas.fi>
- <http://www.f-secure.fi>
- Liikenne- ja viestintäministeriö <http://www.mintc.fi>

- Viestintävirasto

<http://www.ficora.fi>,

<http://www.cert.fi>

- Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry

<http://www.ficom.fi>

- Tietosuojavaltuutetun toimisto

<http://www.tietosuoja.fi>

- Tietoturva ry

<http://www.tietoturva.fi>

- Pelastakaa lapset ry

<http://www.pela.fi/nettivihje>

Microsoftin tekninen tuki

palvelee veloituksetta tietoturvaan liittyvissä kysymyksissä. Microsoftin tuotetuen asiantuntijat antavat ilmaista apua viruksia koskevissa asioissa riippumatta siitä, millainen käyttöoikeus- tai tuotetukisopimus käyttäjällä on tai onko käyttäjällä tukisopimusta.

- Puh. (09) 525 502 500

Palvelu on avoinna klo 9.00–17.00 maanantaista perjantaihin.

Tietoturvaa kuukausihintaan

Osan tietoturvahuolistasi voit antaa kuukausiveloitusta vastaan operaattoriisi hoidettavaksi.

- Elisa Tietoturvapalvelu: <http://www.elisa.fi/tietoturva>

- Sonera Internet Tietoturva: <http://www.soneraplaza.fi/internet/tietoturva>

- dna Nettiturva: www.dnainternet.fi/tuotetuki

SÄILYTÄ TÄMÄ OPAS!



Tutustu oppaan laajempaan versioon osoitteessa www.tietoturvaopas.fi. Sivustoa päivitetään jatkuvasti. Siellä julkaistaan tuoreimmat virusvaroitukset ja ajankohtaiset tiedot tietoturva-asioista.