

## ASIAKASLIITTYMIEN TIETOTURVA

### Yleiset tietoturvariskit

#### Haittaohjelmat

Tietoturvan kannalta tunnetuimpia haittaohjelmia ovat virukset, madot ja vakoiluohjelmat. Tyypillisesti haittaohjelmat tulevat tietokoneelle vertaisverkon, sähköpostin, pikaviestiohjelmien, muistitikujen, cd- ja dvd-levyjen kautta tai ladattaessa tiedostoja internetistä.

#### Saastuneen tietokoneen oireet

- tietokoneen, Internet-selailun ja sähköpostin toiminta hidastuu
- ohjelmistojen toiminta häiriintyy
- tietokone käynnistyy itsestään
- tietokoneelta häviää tietoja tai ne muuttuvat
- Internet-selain ohjaa kaupallisille sivuille ja aukaisee useita ikkunoita mainossivuille

Pahimmassa tapauksessa sähköpostivirukset voivat lähettää itsensä automaattisesti kaikkiin käyttäjän osoitekirjan sähköpostiosoitteisiin ja saattavat liittää viestiin tietokoneella olevia tietoja. Virukset voivat muuttaa tietokoneen roskapostin välitystoimistoksi. Tällainen tietokone lähettää automaattisesti käyttäjän tietämättä suuria määriä sähköpostiviestejä. Verkkomadot etsivät verkosta päivittämättömiä tietokoneita. Verkkomadot leviävät viruksia nopeammin koneelta toiselle. Erilaisia haittaohjelmatyyppejä perinteisten viruksien ja matojen lisäksi ovat botit ja troijan hevokset. Botit ovat haittaohjelmia, joilla tietokoneita hallitaan käyttäjän tietämättä verkon välityksellä. Botilla varustettua konetta käytetään yleensä laittomiin tiedosto- tai verkkopalveluihin ja roskapostin välitykseen. Troijan hevoseksi kutsutaan haittaohjelmaa, joka naamioidaan esimerkiksi viattoman näköiseksi peliksi tai muuksi hyötyohjelmaksi. Troijan hevonen voi sisältää mitä hyvänsä toimintoja. Pahimmillaan se voi tuhota tietokoneen kovalevyn sisällön.

Takaportti on ohjelma, joka avaa ulkoisen tietoliikenneyhteyden suojaamattomaan tietokoneeseen. Takaportin kautta tietokoneesta voidaan varastaa käyttäjän henkilökohtaisia tietoja. Vakoiluohjelmia ovat ohjelmat, jotka keräävät tietoa tietokoneen tai ohjelmistojen käyttötavoista, käyttäjän tallentamista tiedoista tai näppäinpainalluksista. Vakoiluohjelma voi lähettää tiedon automaattisesti eteenpäin tai vakoiluohjelma voi avata pääsyn tietokoneeseen verkon kautta asentamalla tietokoneeseen takaportin. Mainosohjelmat luokitellaan haittaohjelmiksi, ne ovat monesti osana ns. ilmaisjakeluohjelmia. Mainosohjelman tavoitteena on saada käyttäjä menemään halutulle internetsivustolle. Rootkit eli piilohaittaohjelma on ohjelma, joka piilottaa oman toimintansa näkymättömiin käyttäjältä ja tavalliselta virustentorjuntaohjelmalta.

#### Asiakkaan lähiverkko ja liityntä Internetiin

Langatonta verkkoa käytettäessä on muistettava, että kaikkia yhteyksiä voidaan salakuunnella, ellei niitä ole salattu. Avoin verkko mahdollistaa laajakaistayhteyden luvattoman käytön. Lähiverkon ollessa kaape-loitu, ulkopuoliset eivät voi käyttää laajakaistayhteyttä luvatta.

#### Toimenpiteet tietoturvasta huolehtimiseksi

##### Päivitä käyttöjärjestelmäsi ja siihen asennetut ohjelmistot

Windows-käyttöjärjestelmille julkaistaan jatkuvasti uusia päivityksiä, jotka parantavat käyttöjärjestelmän toimivuutta ja tietoturvaa. Automaattisilla päivityksillä käyttöjärjestelmä pysyy ajan tasalla. Uudet päivitykset löytyvät osoitteesta <http://update.microsoft.com>. Osoitteesta saa päivitykset myös Microsoftin muille tuotteille, kuten Office. XP ja Vista sisältävät tietoturvakeskuksen, joka valvoo koneen tilaa. Windowsin tietoturvakeskus löytyy ohjauspaneelistä, sieltä voi tarkistaa virustorjunnan ja palomuurin tilan ja käyttöjärjestelmän ajantasaisuuden. Huomioitavaa on, että Windows ei välttämättä tunnista toisen valmistajan palomuuria. On suositeltavaa käyttää automaattisia päivityksiä.

Linux-jakeluiden päivitykset on hyvä tarkistaa tasaisin väliajoin. Puhtaan asennuksen jälkeen käyttöjärjestelmän päivitys on erityisen tärkeää, koska uusia ja tietoturvan kannalta tärkeitä päivityksiä ilmestyy päivittäin. Puoli vuotta vanha asennuslevy on vanhentunut. Mac-käyttäjien kannattaa pitää käyttöjärjestel-

mänsä ajan tasalla ja huolehtia erityisesti toisen osapuolen ohjelmistojen ajantasaisuudesta ja päivityksistä. Mikäli asennat Applen tietokoneeseen Windows-käyttäjärjestelmän, tulee tietoturvaan suhtautua samalla vakavuudella kuin "tavallisen" Windows-PC:n käyttäjän.

Käytettävien ohjelmien ajantasaisuudesta on huolehdittava käyttöjärjestelmästä riippumatta. Suurin osa ohjelmista ilmoittaa automaattisesti saatavilla olevista päivityksistä. Käyttäjän on hyvä olla aktiivinen ja tarkistaa muutaman kuukauden välein saatavilla olevat päivitykset käyttöjärjestelmään asennetuille ohjelmille. Päivittäminen on tärkeää, koska päivitykset korjaavat ohjelmistojen tietoturva-aukkoja.

### Käy läpi verkkolaitteesi

- Tarkista asetukset ja aseta vahvat salasanat
  - Käytä pieniä ja isoja kirjaimia sekä numeroita
  - Älä käytä erisnimiä tai sanakirjasta löytyviä sanoja
  - Pituus vähintään 8 merkkiä
- Sulje tarpeettomat käyttäjätilit
- Estä hallinta internetistä käsin, mikäli tarvetta etähallintaan ei ole
- Pyri hyödyntämään laitteiden tietoturvaominaisuuksia, kuten palomuri ja osoitteenmuunnos (NAT)
  - Nämä ominaisuudet on otettavissa käyttöön useimmissa laajakaistamodeemeissa
  - Käyttöönotto modeemissa www-selaimella hallittavan graafisen käyttöliittymän kautta
- Telekarelia Oy:n suosittelema ja testaama Zyxel -modeemin hallintaosoite on <http://192.168.0.254/>, oletuksena käyttäjätunnus admin, salasana 1234
- Lisäohjeita Telekarelian laajakaistaohjeistuksessa ja modeemin ohjekirjassa
- Jos käytössä on langaton lähiverkko (WLAN), käytä salausta (WPA/WPA2) ja vahvaa salasanaa
  - Ohjeita on Telekarelian laajakaistaohjeistuksessa ja modeemin ohjekirjassa

### Torju haittaohjelmat

Jos käyttöjärjestelmäsi on Windows (2000/XP/Vista), helpoin tapa huolehtia koneen tietoturvasta on varustaa se tietoturvakäytöllä, joka sisältää virustorjunnan, palomuurisovelluksen, haittaohjelmatyökalan, sähköpostisuodatuksen ja Rootkit-suojauksen. On tärkeää, että ohjelmisto päivittää virustunnisteet automaattisesti vähintään kerran päivässä ja muut ohjelmiston komponentit tarpeen mukaan. Ota yhteyttä Telekarelian asiakaspalveluun ja tilaa Telekarelia Tietoturvapalvelu puhelimitse 013 743 743 tai osoitteesta <http://www.telekarelia.fi/tilaa+palveluita/>. Palvelu on kuukausimaksullinen ja se on voimassa, kunnes tilaus irtisanotaan. Telekarelia Tietoturvapalvelu tarjoaa kattavan suojan viruksia, haitta- ja vakoiluohjelmia vastaan.

Sähköpostin käyttäjä voi vähentää roskapostia seuraavilla keinoilla

- sähköpostiosoitteita ei pidä kirjoittaa Web-sivustoille, uutisryhmäviesteihin tai mihinkään, mistä ne voi helposti löytää
- jos roskapostia tai muuta tuntemattomista osoitteista lähetettyä postia tulee sähköpostilaatikkoon, viesteihin ei tule vastata eikä niissä mainituissa Web-osoitteissa kannata vieraila
- tietokoneessa tulee olla aina käytössä virustorjuntaohjelma ja henkilökohtainen palomuri. Näin tietokone ei saa tartuntaa eikä ala lähettää roskapostia eteenpäin

### Ajankohtaiset tietoturvariskit

- roskaposti
- yhteisöpalveluissa (esim. Facebook ja MySpace) leviävät haittaohjelmat
- phishing eli tietojen kalastelu
- luotettavien brändien hyväksikäyttö
- botti- eli orjakoneverkostot
- verkko-ohjelmien lisäosat
- scareware eli pelotteluohjelmistot

Lisätietoa: [www.virustorjunta.net](http://www.virustorjunta.net), [www.f-secure.com/weblog/](http://www.f-secure.com/weblog/), [www.cert.fi/tietoturvanyt.html](http://www.cert.fi/tietoturvanyt.html) ja [www.tietoturvakoulu.fi](http://www.tietoturvakoulu.fi)