

Arkipäivän tietoturvaa

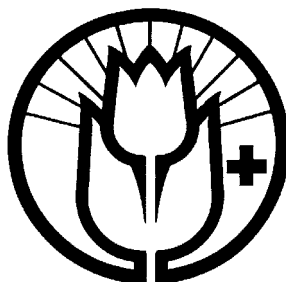
www.selko-e.fi/tietoturva

Mitä tietoturva on? Miten kerron tietoturvasta? Miten lähestyn tietokoneiden tietoturvaa? Tarkastelussa tietoturva ensisijaisesti tavallisen ihmisen eli peruskäyttäjän kannalta.

Ihmisiä pelottavat asiat, joita ei ymmärretä. Ja tietoturva on asia ja ilmiö, jota ei ymmärretä. Kuten ihmisiä pelottaa oman kehon tai elämän hallinnan menettäminen, niin yhtä paljon pelottaa oman koneen ja henkilökohtaisten tietojen hallinnan menettäminen.

Tietoturva-asioista puhuttaessa tulee kuitenkin muistaa, että usein puhutaan uhkakuvista. Mitä voi pahimmillaan mennä pieleen, eikä siitä mitä käytännössä tai tavallisesti tapahtuu. Tietoturva-asioissa kannattaa säilyttää kohtuus ja maalaisjärki.

1. Mitä tietoturva on?
2. Ennakolta ja etukäteen
3. Riskit
4. Ongelmat ja ohjelmat
 - 4.1. Virustorjunta
 - 4.2. Palomuurit
 - 4.3. Roskaposti
 - 4.4. Vakoiluohjelmat
5. Tietoturvan muistilista
6. Linkkejä ja kirjallisuutta



Kehitysvammaisten Tukiliitto ry

Selko-e

2007

(versio 14.11.2007)

veijo.nikkanen@kvtl.fi

1. Mitä tietoturva on?

Mitä tietoturva on? Tiedot turvassa?

1. Tiedot eivät tuhoudu (saatavuus)
2. Tiedot eivät joudu väärin käsiin (luottamuksellisuus)
3. Tietojen viite-eheys ei muutu -pitävät paikkansa (eheys)

Hyvä tietoturva on

1. Asennetta
2. Osaamista
3. Tekniikkaa

Mikä on suurin riski ja haitta?

Ihminen (käyttäjä itse) on tietoturvan suurin yksittäinen riski. Myös nörttilapsi. Yhdysvaltalaisen tutkimuksen mukaan 80-90%:ia tiedon häviämisen syistä (data loss) muodostavat, inhimilliset erehdykset, ohjelmisto-ongelmat ja laitteisto vauriot. Kun taas 10-20% hävikistä johtuu viruksista, ilkeistä tai tulipalojen kaltaisista onnettomuuksista. Inhimillisten erehdysten osuus vaihtelee lähteistä riippuen 32-55%:iin. Vaikka tutkimukset ovat kohdistuneet yritysmaailmaan, ovat tulokset suuntaa-antavia. Kotona, ympäristössä jossa tietotekniikan käyttö on vähemmän hallittua kuin työpaikoilla, on inhimillisten erehdysten merkitys hävikissä tuntuvasti suurempi (Oma näkemys.)

Tietoturvan merkitys eri ihmisryhmille

1. Satunnaiselle surffaajalle (tietoturvariskit tiedostamattomia tai hämääriä)
Vakavinta, hallinnan menettäminen, suurin ei tieto eikä oma työ, vaan taloudellinen, kone ei toimi tai jumittaa. Rikki meneminen - toimimattomuus on peruskäyttäjälle sama asia - osaaminen maksaa. Ei mikrotukea 24 h/vrk.
2. Palveluammattilaiselle (käyttää tietotekniikkaa apuvälineenä työn suorittamisessa)
Muiden tietojen joutuminen vieraisiin käsiin, työtä ja työaika hukkuu. Mikrotuki 24 h/vrk, joku jolle voi soittaa (virallisesti).
3. Tietoturva-ammattilaiselle (tiedostaa riskit ja mahdollisuudet niiden ehkäisyyn)
Tieto häviää kokonaan. Tietokannat yms. Toiminta pysähtyy. Ihmiset kärsivät.

Käyttäjiä erilaisia? Yhteinen vastuu? -seuraukset

Selittäminen - ymmärtäminen - ilmiön hallinta (toimeen tuleminen): Mitä merkitsee Konkretiaa, ei abstrakteja asioita
Nyrkkisäännöt ja tarkistuslistat auttavat tottumaton.
Kuuntelijan kokemusmaailma (Työasema ja sovellukset vs. kone)
Mitä ymmärretään: Kielen jolla tietoturva-asioita käsitellään tulee olla ymmärrettävissä ihmiselle jonka asioista on kysymys

2. Ennakolta ja etukäteen

Paras, halvin ja varmin tietoturva syntyy etukäteen suunnittelemalla ja varautumalla.

Suunnittelu ja valmistelu (ohjelmat):

Valitaan käyttöön tietoturvalliset ohjelmat.
Varmistetaan niiden toiminta ja asetukset.

Huolehditaan päivityksistä (sekä ohjelmat, että tunnistekuvaukset).
Asennetaanko kaikki, vai vain käytettävät ominaisuudet.

Varmuuskopiointi:

Riittävän usein ja helposti käyttöön palautettava, mutta turvallisesti säilytetty.

Salaaminen ja salasana:

Varsinainen ohjelmallisesti tapahtuva salaaminen on tehokasta, mutta kannattaa laskea tarkkaan hyötyjä. Joskus salaamisesta saattaa olla enemmän työtä ja kustannuksia, kuin saavutettuja etuja.

Salasanojen ja käyttäjätunnusten käyttö: Ei vain välttämätön kiusa. Kannattaa miettiä miksi salasanoja yleensä käytetään. Älä anna ihmisten kurkkia salasanojasi, edes keltaisesta näyttöön kiinnitetystä lapusta. Oma nimi ei ole paras salasana, eikä samaa salasanaa kannata käyttää joka paikassa.

Toimintatavat:

Tietoturva vaatii seurantaa, ja ennen kaikkea omien tapojen seurantaa.

Jätänkö läppiksen autoon penkille vai piiloon?

Juttelenko kovaan ääneen tietoturva-asioista?

Kun vanha kone lähtee, sen levyä ei tyhjennetä?

Paperit silppuriin tai uuniin vai roskikseen? Kuka käsittelee?

Arkaluontoiset asiat kaappiin, arvokkaita asioita, kuten rahat pannaan lukkojen taakse.

Raha ja muut arvokkaat asiat voivat nykyään olla virtuaalisia. Asia tiedetään, mutta sitä ei tiedosteta. Joo joo. Ei ymmärretä että joku voi tulla katselemaan.

Kaksi suuntaisuus -Internetissä et ole koskaan yksin ja sinut huomataan!

Me katselemme - meitä katsellaan (Internet ei ole televisio)

Vertaus: Minua on tultu katselemaan, entäpä jos minä katson takaisin, tai joku muu seuraa sivusta. Myös netissä voidaan liikkumistamme seurata (vrt. matkakortti), vaikka matkan varrella. Jätämmekö oven auki? Aina kun liikumme meidät huomataan, olemassaolomme huomataan myös verkossa. Verkossa vakoilu voidaan automatisoida.

Kiinni verkossa - joku käyttää konettani?

3. Riskit

Ennakointiin ja suunnitteluun kuuluu myös mahdollisten riskikohtien tiedostaminen ja löytäminen. Kaikki kohteet joissa tietoa voi joutua väärin ihmisten käsiin tai hukkaan ovat tietoturvariskejä. Seuraavassa esitellään muutamia tavanomaisimpia tilanteita.

Kone

Tietokoneen sisältö voi joutua väärin käsiin esimerkiksi varkauden, myynnin, lainaamisen tai huollon yhteydessä. Tietokoneen sisältämät tiedot voivat kadota myös laitevian, vesivahingon tai tulipalon seurauksena.

Internet

Phishing, luotto- ja henkilötietojen kalastus eli huijaus. Ihmisille lähetetään sähköpostiviestejä, jotka on naamioitu esimerkiksi tilipankin lähettämiksi. Viesteissä kehoitetaan vaihtamaan verkkopankin tunnuslukuja Internet-sivulla, joka taas on naamioitu näyttämään pankin sivustolta.

WWW-tiedostot

www-tiedostot ja laajennukset kuten Plug-Init, Active-x-komponentit, Java ja JavaScript-viritelmät tekevät Internet-palveluista vuorovaikutteisempia, mutta samalla avaavat useita tietoturva-aukkoja. Kun jonkun sivun käyttäminen vaatii hyväksymään uuden ominaisuuden käyttöönotton selaimessa ja tietokoneella olisi hyvä tietää myös uudet, mahdolliset tietoturvaongelmat.

Tiedostonjako

Lähiverkossa (esim. taloyhtiön verkko) tapahtuva tarkoituksellinen tai tahaton tiedostojen jako Windowsissa on riski-altista. Vertaisverkoissa toimivat P2P- eli tiedostonjako-ohjelmat ovat tuoneet mukanaan tietoturva riskejä ja ylläpidollisia ongelmia.

Mobiililaitteet

Kaikki kannettavat viestintään käytettävät laitteet; tietokoneet, PDA-laitteet, kommunikaattorit ja kännykät muodostavat riskitekijöitä tietoturvan kannalta. Mikäli laitteessa on päivitettäviä ohjelmia, niitä voidaan yrittää käyttää väärin. Älä päivitä laitettasi tuntemattomista tai epäilyttävistä palveluista, äläkä lähetä hauskoja "juttuja" kaverille.

USB-muistit ja muut mukana kuljetettavat tietojen tallennusvälineet

Tietoa täytyy kuljettaa välillä paikasta toiseen. Matkan aikana tallennusväline saattaa hukkua ja joutua väärin käsiin. Muistitikut, levykkeet ja levyt ovat myös erittäin herkkiä vikaantumiselle. Älä käytä tällaisia muistivälineitä tietovarastoina eikä varmuuskopioina vaan ainoastaan tietojen kuljettamiseen paikasta toiseen. Käytön jälkeen tyhjennä muisti. Hävitä vikaantunut muisti asiallisesti.

CHAT-ohjelmat

Reaaliaikaisten keskusteluyhteyksien yli voidaan suorittaa ohjelmia.

Sähköposti

Varo näppivirheitä! Mihin menevät viestit jotka eivät koskaan saavu perille? Mitä niillä tehdään?

Asetukset kuntoon. Ei automaattista kuvien lataamista eikä viestien avaamista.

Tuhoa tuntemattomat vieraskieliset sähköpostiviestit heti.

Älä koskaan vastaa mainos- ja roskaposteihin, sillä vastaamalla osoitat lähettäjälle, että sähköpostisi on käytössä ja saat entistä enemmän roskapostia. Älä avaa epämääräisiä sähköposteja ja liitetiedostoja, sillä ne saattavat sisältää viruksia, jotka vahingoittavat tietokonettasi. Vältetään liitetiedostojen käyttöä, ei lähetetä niitä ilman vastaanottajan suostumusta. Jos on pakko avata tuntematon liitetiedosto (1. päivitetään virustietokannat. 2. kopioidaan liitetiedosto koneelle. 3.tarkistetaan tiedostot virustorjuntaohjelmalla. 4. avataan tiedosto)

Tuttujen ihmisten lähettämiä outoja viestejä tulee epäillä. Miksi 79-vuotias mummu kirjoittaisi yhtäkkiä englanniksi?

Älä myöskään klikkaa mainosposteissa olevia linkkejä.

4. Ohjelmat ja ongelmat

Useimpia Internetin ja tietokoneen käyttöön liittyvistä tietoturva-riskeistä voidaan merkittävästi pienentää tietoturvaohjelmien asianmukaisella käytöllä. Vaikka kaupallisten tietoturvaohjelmien hinta onkin varsin edullinen verrattuna muihin tietokoneen käytöstä ja hankinnasta syntyviin kustannuksiin, on tavalliselle kotikäyttäjälle tarjolla myös ilmaisia vaihtoehtoja.

Valheellinen turvallisuus ohjelmistojen avulla

Ohjelmat itsessään eivät takaa turvallista tietokoneen käyttöä.

Ohjelmien tietoturvaominaisuudet ovat hyödyttömiä, mikäli ne eivät ole päällä, päivitetty tai säädetty oikein. Säädetäviä tietoturvaominaisuuksia löytyy käyttöjärjestelmästä, selaimesta, virustorjuntaohjelmasta, palomuurista ja sähköpostiohjelmasta.

Haavoittuvuus

Koska tietokoneohjelmat ovat ihmisten tekemiä, niistä löytyy virheitä ja puutteita. Näitä haavoittuvuuksiksi kutsuttuja ohjelmointivirheitä hyväksikäyttämällä toiset ihmiset voivat tuottaa harmia ohjelmien käyttäjille. Ohjelmien valmistajat korjaavatkin jatkuvasti ohjelmiin jääneitä virheitä ja julkaisevat korjaukset eli päivitykset Internetsivuillaan. Internetiin kytkettynä olevan koneen ohjelmat kannattaa siis säännöllisesti päivittää itse, tai antaa ohjelmien oman automatiikan hoitaa päivitysten hakeminen ja asentaminen.

Pyydä apua!

Jos et tiedä, kuinka hoitaa oman koneesi asennukset, päivitykset ja säädöt, kysy apua asiantuntijalta esimerkiksi liikkeestä, josta olet tietokoneesi ostanut. Pyydä neuvoa kaverilta, mikäli omat taidot eivät riitä koneen tietoturvan parantamisessa. Osaamattomuus ei ole häpeä, vaan kysymättömyys.

4.1. Virustorjunta

Tietokonevirukset ovat haittaohjelmia jotka haittaavat tai estävät tietokoneen käyttöä toivotulla tavalla. Virukset voivat myös lähettää käyttäjän tietoja Internetiin sekä tuhota tiedostoja.

Virustorjuntaohjelma

Virustorjuntaohjelma on sovellus joka suojaaa konetta haittaohjelmilta. Virustorjuntaohjelma toimii koneessa taustalla, ja puuttuu asiaan mikäli jokin ohjelma yrittää suorittaa ei toivottuja toimintoja. Virustorjuntaohjelma tunnistaa virukset viruskuvaustietokantojen avulla, jotka ovat kuin etsintäkuulutuslistoja tai sormenjälkiä. Mikäli viruskuvaustietokantoja ei päivitetä, ohjelman suojausteho vähenee nopeasti. Mikäli asetukset eivät ole kohdallaan, eivätkä toiminnot kuten päivitykset toimi, ohjelma ei pysty suojelemaan konetta. Tietokone voi saada virustartunnan mm. sähköpostista, Internet-sivuilta tai tiedostonjaon kautta.

Virustyyppejä (haittaohjelmatyyppejä)

Tietokoneviruksia luokitellaan toimintatapojensa mukaan. Tietokonevirukset toimivat monin eri tavoin ja yksittäiset virukset voivat sisältää monia ominaisuuksia tai toimintatapoja joiden avulla ne saastuttavat tietokoneita. Jonkin tietyn käsitteen käytöllä yksittäisten virusten yhteydessä halutaan korostaa jotakin tiettyä ominaisuutta.

Troijan hevonen -ohjelma sisältää käyttäjälle haitallisia ominaisuuksia, joista käyttäjä ei ole tietoinen. esim. etähallintaominaisuuksia. Troijan hevoset leviävät usein muiden virusten mukana tai ovat osa viruksen toiminnallisuutta.

Madot - Madot liikkuvat itsenäisesti etsien saastutettavaksi kelpaavaa tietojärjestelmää.

Tiedostovirukset - tarttuvat ohjelmiin ja suorittavat jonkin toiminnon koneella.

Levykevirukset - Koneen käynnistäminen eli buuttaaminen viruksen sisältämältä levykkeeltä aikaansaa virustartunnan.

Makrovirukset - on ohjelmoitu jonkin ohjelman, kuten esimerkiksi Wordin käyttämällä makrokielellä.

Virustorjuntaohjelmia (ilmaisia kotikäytössä):

AntiVir Personal Edition Classic

- www.free-av.com

Avast! Home Edition

- www.avast.com/eng/download-avast-home.html (suomeksi)

AVG Free Edition

- free.grisoft.com/freeweb.php/doc/2

Virustorjuntaohjelmia

(kaupallisia, sisältävät palomuurin ja vakoiluohjelmien poiston):

F-secure - www.f-secure.fi

Panda - www.pandasoftware.fi

4.2. Palomuri

Palomuri on laite tai ohjelmisto, jolla rajoitetaan tietokoneelta tapahtuvaa liikennettä ennalta määrättyjen sääntöjen mukaisesti. Palomuurilla voidaan rajoittaa liikennettä ulos tai sisään sekä määrittää, mitkä ohjelmat saavat käyttää Internet-yhteyttä. Palomuurin tehtävänä on ehkäistä kutsumattomat kurkistelut koneellesi.

Vanhempien Windows-käyttöjärjestelmien mukana ei tule palomuuria, vaan se täytyy hankkia erikseen. Windows XP:n mukana tuli palomuri, joka ei ollut oletuksena päällä, vaan käyttäjän tuli laittaa se itse päälle, mikäli osasi. SP2 päivityksen jälkeen palomuri on oletuksena päällä, mutta vieläkin se ei rajoita ulos menevää liikennettä (ts. mitkä ohjelmat käyttävät Internet yhteyttä). Oikea palomuri valvoo kaikkea liikennettä ja antaa käyttäjän valita käytettävät ohjelmat (tai alussa olevat oletusasetukset ovat riittävät eikä tarvitse tehdä liian vaikeita valintoja)

Henkilökohtaisista palomureista puhutaan, kun halutaan korostaa yhden koneen suojausta. Isoissa laitoksissa usein yksi palomuri suojaa montaa konetta kerrallaan, jolloin voi jäädä tarvetta suojata yksittäisiä koneita muilta käyttäjiltä. Nykyään palomuri on usein mukana myös ADSL-reitittimissä. Kotikäytössä riittää kuitenkin yleensä ohjelmallinen palomuri. Palomuuriohjelmat löytyvät nykyisin osana suurempia tietoturvaketteja, joissa löytyvät useimmat muutkin tietoturvaan liittyvät ohjelmistot.

Porttiskannaus

Suurin osa palomuriin ulkoapäin tulevasta liikenteestä on tavanomaista Internet-liikennettä. Porttiskannauksessa palomuurin ja tietokoneen asetuksia tutkitaan tarkoituksellisesti ulkoapäin tavoitteena selvittää löytyykö koneen suojauksesta aukkoja, joita hyväksikäyttämällä koneeseen voi päästä sisälle. Useimmiten näitä tietokoneen tietoliikenneportteja käyvät kolkuttelemassa ohjelmat jotka automaattisesti etsivät verkosta suojaamattomia koneita.

Palomuurin pommitus

Palomuurin pommituksesta voidaan puhua silloin, kun tarkoituksena on kuormittaa palomuuria/palomuuriohjelmia niin paljon ulkoa päin tulevalla liikenteellä että se ei pysty hoitamaan tehtäviään. Useimmiten tämä johtaa koko tietokoneen toimimattomuuteen.

Ongelmia palomuurin kanssa?

Palomuuuri voi estää joidenkin ohjelmien toiminnan. Yleensä palomuurille pitää opettaa, toisin sanoen luoda säännöt, mitkä ohjelmat saavat ottaa yhteyden Internetiin. Joskus suojaus-asetukset voivat olla jo etukäteen tehtyjä, mutta jos käytät erikoisia ohjelmia voit joutua niitä muuttamaan. Jos et tunne ohjelmaa jonka vapaata pääsyä Internetiin palomuurisi sinulle ehdottaa, älä hyväksy sitä heti, vaan selvitä ensin asia.

Kaksi toiminnassa olevaa palomuuria voi haitata toistensa toimintaa. Jos sinulla on sekä ADSL-modeemissa palomuuuri, että koneessa palomuuuri-ohjelmisto kannattaa käyttää vain toista. Samoin kaksi ohjelmisto-palomuuria voi häiritä toisiaan. (Esimerkiksi Windows XP:n palomuuuri ja ZoneAlarm). Ohjelmistopalomuuurejakaan ei kannata pitää kahta päällä yhtä aikaa. Myös eri valmistajien palomuuuri ja virustorjunta-ohjelmat voivat myös häiritä toisiaan.

Palomuuuri ohjelmia (ilmaisia kotikäytössä):

ZoneAlarm -

www.zonelabs.com/store/content/catalog/products/sku_list_zal.jsp

Outpost Firewall Free -

www.agnitum.com/products/outpostfree/index.php

Comodo Personal Firewall -

www.personalfirewall.comodo.com

4.3. Roskaposti

Roskaposti eli spammi on sähköpostilaatikkoosi pyytämättä tulevaa mainospostia ja useimmiten englanninkielistä. Suurin osa roskapostista tulee Yhdysvalloista jossa roskaposti mainontaa ei ole haluttu rajoittaa. Roskaposti mainonnan suosion syy on tehokkuus ja halpuus. Nykyään roskapostia tulee myös suomalaisilta mainostajilta. Roskaposti voi olla tavallista mainontaa, mutta usein sen avulla yritetään myös huijata hyväuskoisia käyttäjiä. Mainospostin mukana kulkee usein vakoilu- ja virusohjelmia.

Ehkäise roskaposti ennakoita

Roskaposti kannattaa ehkäistä mieluummin jo ennakoita. Katso minne kirjoitat sähköpostiosoitteesi. Älä myöskään koskaan vastaa roskapostiviesteihin, sillä silloin saat entistä enemmän mainoksia ja osoitteesi päätyy toimivien osoitteiden listalle. Älä myöskään pyydä lähettäjiä poistamaan sähköpostiosoitettasi postituslistalta. Mainospostissa käytettäviä osoitteita kerätään kotisivuilta, keskustelupalstoilta ja yleisesti kaikin keinoin. Roskapostin välttämiseksi kannattaa ottaa omasta sähköpostiohjelmasta kuvien automaattinen näyttäminen pois päältä. Kun ohjelma hakee kuvat mainostajan palvelimelta, käynnistä jää tieto mainostajalle ja roskaposti lisääntyy entisestään.

Suodatus eli filterointi

Roskaposti-viestit voidaan suodattaa tärkeistä viesteistä, joko erillisillä ohjelmilla, tai itse

sähköpostiohjelmassa olevalla suodatin-toiminnolla. Suodatus voi tapahtua sähköpostipalvelimella tai omalla koneella. Sähköpostissa oleva suodatin täytyy myös opettaa suodattamaan roska tärkeistä viesteistä. Kun kerran merkitset viestin roskaksi, silloin ohjelma tunnistaa paremmin samantapaiset viestit seuraavan kerran ja laittaa ne roskaposti-kansioon. Roskaposti-kansio kannattaa aina silloin tällöin tarkistaa, jottei mukaan olisi vahingossa joutunut tärkeitä viestejä.

Ohjelmia ja linkkejä:

Thunderbird (www.mozilla.fi/wiki/Thunderbird) on ilmainen suomenkielinen sähköpostiohjelma jossa on roskapostisuodatin. Suodattimen käyttöohjeet löydät [täältä](#).

Eudorassa (www.eudora.com) on jo pidempään ollut suodatin joka täytyy myös opettaa tunnistamaan roskaposti.

Viestintäministeriön roskapostipaketti (www.roskapostipaketti.fi) kertoo roskapostista yleisesti.

4.4. Mainos ja vakoiluohjelmat

Vakoiluohjelmat ovat pieniä ohjelmia, jotka asentuvat koneelle joiltakin Internet-sivuilta. Vakoiluohjelmat eivät tee tuhoja, mutta keräävät tietoja esimerkiksi mainontaa varten. Vakoiluohjelmat voivat kerätä myös salasanoja ja käyttäjätunnuksia tallentamalla esim. näppäimistösi painallukset. Vakoiluohjelmat tulevat usein myös jonkin näennäisesti hyödyllisen ohjelman mukana. Älä kuitenkaan hyväksy (klikkaa) mitään Internet-sivuilta esiin aukeavia sivuja, jotka pyytävät asentamaan ohjelmia tai päivityksiä. Toimiessaan koneellasi nämä vakoojat voivat häiritä muiden ohjelmien toimintaa ja hidastaa huomattavasti koneen toimintaa.

Mainos ja vakoiluohjelmien poisto

Virustorjuntaohjelmat eivät havaitse vakoiluohjelmia. Vakoilu- eli Spyware-ohjelmat voit poistaa ilmaiseksi saatavilla olevilla ohjelmilla kuten AdAware tai Spybot. Joskus vakoiluohjelmat toimivat yhteistyössä virusten levittäjien kanssa. Vakoiluohjelman poisto saattaa lopettaa joidenkin ohjelmien toiminnan. Erityisesti vakoiluohjelmien poistaminen on haitannut tiedostonjako-ohjelmia.

Pop-uppien esto

Sivuilta esiin aukeavien ponnahdusikkunat eli pop-upit häiritsevät usein käyttäjää. Edistyneemmissä selaimissa kuten Mozillassa ja Mozilla Firefoxissa on jo pidempään ollut mahdollisuus estää näitä mainosikkunoita avautumasta. Microsoft Internet Exploreriin löytyy myös lisäohjelmia, joilla pop-uppeja voidaan estää avautumasta.

Selaimen kaappaus = Selaimen kaappauksella tarkoitetaan tilannetta jossa Internet - selaimen käynnistyssivu muutetaan ohjautumaan johonkin muualle kuin käyttäjä haluaisi sen avautuvan. Ongelmia syntyy mikäli sivusto, jolle selain ohjataan, haluaa asentaa koneelle virus/vakoilu -ohjelmia.

Vakoiluohjelmien poisto-ohjelmia (ilmaisia kotikäytössä):

Mikäli koneesi toimii jotenkin oudosti tai erityisen hitaasti, kannattaa vakoilijoiden poisto-ohjelma asentaa ja käyttää. Häiritsevät vakoiluohjelmat ja mainokset eivät välttämättä poistu yhdellä ohjelmalla, vaan parhaan tuloksen aikaansaamiseksi kannattaa käyttää useita ohjelmia.

Alapuolella on joitakin vakoiluohjelmien poistoon erikoistuneita ohjelmia. Jos sinulla on maksullinen tietoturva -ohjelma tai -palvelu, siihen useimmiten kuuluu myös vakoiluohjelmien poistoon liittyvä toiminto. Vaikka käyttäisitkin useita vakoiluohjelmien poistoon liittyviä ohjelmia, älä pidä niitä kuitenkaan yhtä aikaa päällä, sillä ne saattavat häiritä toisiaan.

Ad-Aware 2007 Free

- www.lavasoft.de/products/ad_aware_free.php

AVG Anti-Spyware Free Edition

- free.grisoft.com/doc/5390/us/frt/0?prd=asf

Spybot, Search & Destroy

- www.safer-networking.org/fi/download/index.html

HijackThis

- www.spychecker.com/program/hijackthis.html

5. Tietokoneen käyttäjän muistilista:

Seuraavia ohjeita noudattamalla voit parantaa tietokoneesi ja tietojesi turvallisuutta. Ohjeet koskevat tietokoneita, joista on yhteys Internetiin.

1. Varmuuskopioi tietosi talteen ennen kuin vahinko sattuu.

Suurin osa tietojen häviämisestä johtuu ihmisestä. Olet itse suurin tietoturvariski.

2. Älä klikkaa hiirellä mitään sellaista Ok-nappia minkä tarkoitusta et tiedä.

Mieti ennen kuin klikkaat myös sähköpostia lähettäessäsi. Väärin kirjoitettu sähköpostiosoite, ja viestisi päättyy väärälle vastaanottajalle.

3. Tuoja tuntemattomat vieraskieliset sähköpostiviestit heti.

Älä myöskään klikkaa näissä viesteissä olevia linkkejä.

4. Älä avaa (klikkaa) hiirellä tuntemattomia tai vieraskielisiä sähköpostin liitetiedostoja.

5. Älä lähetä turhia liitetiedostoja.

Vältä turhaa liikennettä ja mieti missä liitteesi avataan, ja minne se lopulta päättyy.

6. Hanki tietokoneeseen virustorjuntaohjelma.

Virustorjuntaohjelma valvoo ja estää virusten toiminnan. Virustorjuntaohjelman tiedot pitää päivittää säännöllisesti. Virustorjuntaohjelman päivityksessä koneeseen siirretään tiedot uusista tietokoneviruksista, joiden toiminta koneessa täytyy estää. Tarkista että virustorjuntaohjelmassasi on automaattinen päivitys käytössä, jolloin ohjelma hoitaa itse päivityksen aina, kun Internet-yhteys avataan.

7. Päivitä tietokoneesi käyttöjärjestelmä säännöllisesti.

Varsinkin Windows-käyttöjärjestelmä on päivitettävä säännöllisesti, sillä useimmat tietokoneita saastuttavat virukset on tehty hyökkäämään juuri Windows-koneisiin. Vaikka Windows on yleisin käyttöjärjestelmä koko maailmassa, tietoturvaohjeet koskevat myös

muita käyttöjärjestelmiä, joita täytyy myös päivittää.

8. Asenna palomuuriohjelma.

Palomuuuri-ohjelma tai -laite suojaa tietokoneesi Internet-yhteyden kautta tulevilta hyökkäyksiltä. Palomuuuri pitää tietosi piilossa luvattomilta katselijoilta.

9. Sääda tietoturva-asetukset kuntoon!

Ohjelmien tietoturvaominaisuudet ovat hyödyttömiä, mikäli ne eivät ole päällä tai säädetty oikein. Säädetäviä tietoturvaominaisuuksia löytyy käyttöjärjestelmästä, selaimesta, virustorjuntaohjelmasta, palomuurista ja sähköpostiohjelmasta.

10. Älä hätäänny! Jos et tiedä mitä pitäisi tehdä, kysy kaverilta tai liikkeestä, josta koneesi hankit.

6. Linkkejä ja kirjallisuutta

Tietoturvakysymyksissä paras tiedonlähde on Internet. Samat ongelmat vaivaavat tuhansia käyttäjiä, ja aina joku löytää myös vastauksen ongelmaan ja haluaa auttaa muitakin.

Linkkejä:

www.tietoturvaopas.fi/fi/index.html

- Tietoturvaopas Microsoft-mallin mukaan.

www.linux.fi/index.php/Tietoturva

- Linux-käyttäjän tietoturvaopas

www.cis.hut.fi/kaip/tietoturvaopas.html

- Vaihtoehtoinen tietoturvaopas.

www.tieke.fi/julkaisut/oppaat_yrityksille/tietoturvaopas

- Tieken tietoturvaopas

www.yliopistojentt.uta.fi/VAHTI-CD

- VAHTI-tietoturva CD, julkisten organisaatioiden tietoturva ohjeita

www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

- Tiivis tietoturvasanasto (pdf-tiedosto).

www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

- Viestintäviraston tietoturvasivut

www.tietoturva.org

- Tietoturva RY, Ammatikseen tietoturvakysymysten kanssa toimiville.

www.tietosuoja.fi

- Tietosuojavaltuutetun toimisto, neuvoja ja ohjeita siitä, miten tietoja pitäisi käsitellä.

www.virustorjunta.net

- Virustorjuntaan keskittyvä sivusto.

Kirjallisuutta (Windows/Microsoft):

Jukka Korpela :Turvallisesti netissä - kodin tietoturvaopas

Petteri Järvinen: Tietoturva & yksityisyys