Arkipäivän tietoturvaa

– Selkeä tietoturvaopas

Tämän oppaan löydät verkosta: www.selko-e.fi/tietoturva

Kehitysvammaisten Tukiliitto ry
Selko-e
(tietoja päivitetty osittain 13.10.2014)
veijo.nikkanen@kvtl.fi

1. Miksi tieto on arvokasta?

Tietoyhteiskunnasta puhutaan, kun halutaan korostaa tiedon ja osaamisen merkitystä ihmisten elämässä ja yhteiskunnan toiminnassa. Asiat ovat monimutkaisia ja niiden suunnitteluun, tekemiseen ja käyttämiseen tarvitaan paljon tietoa. Tiedosta on tullut arvokasta ja arvokkaista asioita pidetään yleensä huolta. Tiedosta pidetään siis huolta ja sitä suojellaan. Esimerkiksi kännykkä edustaa tietoa, kuten myös kaivurin käyttö. Arvokasta tietoa on myös kaikki sellainen tieto jolla on ainutlaatuisuutensa vuoksi merkitystä käyttäjälle, vaikka ei rahallisesti olisikaan arvokasta.

Mikä on arvokasta tietoa?
Pohdi mikä on arvokasta tietoa. Minkä tietojen häviämisestä tai leviämisestä olisi sinulle harmia.

Esimerkkejä arvokkaista tiedoista
- salasanat ja käyttäjätunnukset
- valokuvat
- terveys/ihmissuhde/talous ja muut yksityiset tiedot
- tilitiedot
- tiedostot ja ohjelmat joita ei ole oikeutta levittää
- tiedostot tai esineet jotka sisältävät paljon tieto tai työtä
- ainutlaatuiset asiat, jotka eivät ole korvattavissa

Pohdi mitkä tiedot ovat muille arvokkaita?

Mitä tietoturva on?
Mitä tietoturva on? Mitä tietoturva tarkoittaa tavallisen ihmisen eli peruskäyttäjän kannalta. Tässä oppaassa selvitetään mitä tietoturva tarkoittaa ja miten voin parantaa omaa tietoturvaani.

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.

Tietoturvan ehdot tai milloin tieto on turvassa
1. Tiedot eivät tuhoudu (saatavuus)
- tietoa sisältävä esine ei esim. pala tai rikkoonnu
2. Tiedot ovat käytettävissä järkevästi (eheys)
- tietojen viite-eheys ei muutu eli ne pitävät paikkansa
- esim. kirjastossa kirjat eivät joudu väärään paikkaan - esim. tietokannassa olevat tiedot eivät ole sekaisin
3. Tiedot eivät joudu vääriin käsiin (luottamuksellisuus)
- vain ihmiset jotka on tarkoitettu käyttämään tietoja voivat niitä käyttää

Hyvä tietoturva on
1. Asennetta - tietoa pidetään tärkeänä
2. Osaamista - osataan itse tai osataan kysyä apua tietoturva-asioissa
3. Tekniikkaa - huolehditaan laitteista ja välineistä joilla tietoa käsitellään

Mikä on suurin riski ja haitta?
Ihminen (käyttäjä itse) on tietoturvan suurin yksittäinen riski. Myös lapset, vaikka osaavatkin teknisesti hyvin käyttää laitteita ja ohjelmia voivat olla riski. Tutkimuksien mukaan 80-90 %:ia tiedon häviämisen syistä muodostavat, inhimilliset erehdykset, ohjelmisto-ongelmat ja laitteisto vauriot. Kun taas vain 10-20 % hävikistä johtuu viruksista, ilkivallasta tai tulipalojen kaltaisista onnettomuuksista. Inhimillisten erehdysten osuus vaihtelee lähteistä riippuen 30-40 %: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 suurempi. Omalla käyttäytymisellään voi siis vaikuttaa paljon tietoturvaansa.

Tietoturva merkitsee eri käyttäjäryhmille erilaisia asioita
1. Satunnaiselle surffaajalle eli kotikäyttäjälle
- jolle tietoturvariskit ovat joko tiedostamattomia tai hämäriä.
Vakavinta, hallinnan menettäminen, suurin ei tieto eikä oma työ, vaan taloudellinen, kone ei toimi tai jumittaa. Rikki meneminen ja toimimattomuus ovat peruskäyttäjälle sama asia - osaaminen maksaa. Ei mikrotukea 24 h/vrk.

2. Palveluammattilaiselle
- joka käyttää tietotekniikkaa apuvälineenä työn suorittamisessa.
Vakavinta on muiden tietojen joutuminen vieraisiin käsiin, työtä ja työaikaa hukkuu. Mikrotuki 24 h/vrk, joku jolle voi soittaa (virallisesti).

3. Tietoturva-ammattilaiselle
- joka tiedostaa riskit ja mahdollisuudet niiden ehkäisyyn.
Vakavinta on se että tieto häviää kokonaan. Tietokannat yms. Toiminta pysähtyy. Ihmiset kärsivät.

Erilaiset käyttäjät - Yhteinen vastuu
Tietoturva-asioista tulisi aina saada tietoa sellaisella kielellä jota ymmärtää. Kuuntelijan kokemusmaailma on selitettäessä otettava huomioon. Kielen jolla tietoturva-asioita käsitellään, tulee olla ymmärrettävää ihmiselle jonka asioista on kysymys. Helpointa on ymmärtää seuraukset, joita huonosta tietoturvasta seuraa. Omaa arkea lähellä olevia asioita on helpompi ymmärtää kuin vaikeita käsitteellisiä juttuja.
Tietoturvan merkityksen ymmärtäminen johtaa ilmiön hallintaan tai ainakin toimeen tulemiseen.
Nyrkkisäännöt ja tarkistuslistat auttavat tottumatonta parantamaan tietoturvaansa.

1.1. Missä on arvokasta tietoa?

Käytämme monia erilaisia paikkoja tiedon säilyttämiseen ja käsittelyyn. Unohdamme usein, missä olemme tietoa käsitelleet.

Paikkoja joissa säilytämme tai käsittelemme tärkeää tietoa:

1. Laitteet
- tietokone
- kannettava tietokone
- tabletti tietokone
- CD/DVD/bluray

- USB tikku
- kamera ja muistikortit
- puhelin
- ulkoinen kiintolevy

2. Palvelut
- sähköposti
- facebook
- keskusteluryhmät
- chat ja muut pikaviestipalvelut
- kotisivut
- kuvapalvelut
- varmuuskopiontipalvelut

3. Paperit
- palvelusopimukset
- salasanat
- lääkärintodistukset
- takuupaperit, kuitit
- valokuvat
- omat muistiinpanot

4. Puhe
- seinilläkin korvat on

2. Ennakolta ja etukäteen

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

Suunnittelu ja valmistelu (ohjelmat):
Valitaan käyttöön tietoturvalliset ohjelmat ja palvelut.
Varmistetaan niiden toiminta ja asetukset.
Huolehditaan päivityksistä (sekä ohjelmat, että tunnistekuvaukset).
Asennetaanko kaikki, vai vain ohjelman käytettävät ominaisuudet.

Varmuuskopiointi:
Varmuuskopiointi tarkoittaa sitä, että käytettävistä tiedoista otetaan kopio jota säilytetään eri paikassa kuin käytettäviä tietoja. Varmuuskopio on otettava riittävän usein ja sen on oltava helposti käyttöön palautettava, mutta turvallisesti säilytetty.

Varmuuskopiointi tapoja:
1. Ulkoinen kiintolevy
2. CD/DVD/BLUray
3. USB-tikku
4. Sähköposti
- voit lähettää itsellesi muutaman tärkeän tiedoston
5. Sivutila/verkkopalvelu
- ilmaiset verkkolevyt ja palvelut voivat olla hyvä ratkaisu
6. Paperinen tuloste
Pidä huolta myös varmuuskopioista ja opettele palauttamaan tiedot varmuuskopiolta.

Salaaminen:
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:
Salasanat eivät ole vain välttämätön kiusa. Kannattaa miettiä miksi salasanoja yleensä käytetään. Useimpien palveluiden käyttö edellyttää käyttäjätunnuksen ja salasanan keksimistä. Tarvitset usein myös toimivan sähköpostiosoitteen jotta palvelu voi varmistaa sinut aidoksi käyttäjäksi. Käyttäjätunnus ja salasana muodostavat avainparin joilla palvelu tunnistaa sinut ja joilla pääset käyttämään omia tietojasi.

Älä anna ihmisten kurkkia salasanojasi, edes keltaisesta näyttöön kiinnitetystä lapusta. Tämän takia useimmissa palveluissa joita käytetään salasanaa, se ei näy selvänä, vaan sen tilalla on tähtiä. Oma nimi ei ole paras salasana, eikä samaa salasanaa kannata käyttää joka paikassa.
Ihmisen muisti ei riitä yleensä hallitsemaan kaikkia salasanoja. Salasanoista on siis oltava kopiot jossakin. Säilytä salasanat ja salasanoja sisältävät paperit erillään tietokoneesta ja paikassa josta löydät ne.

Käyttäjätunnusten lisäksi jotkut Internetin palvelut käyttävät tunnistautumisessa hassunmuotoisiin kirjaimiin tai kuviin perustuvia pieniä kuvia. Tällöin käyttäjän tulee tunnistaa kuvassa esiintyvät kirjaimet ja kirjoittaa ne oikein niille varattuun kohtaa. Tällaista tunnistusta voidaan käyttää esimerkiksi silloin kun on unohtanut salasanansa ja kirjoittanut sen monta kertaa väärin.

Käyttäessäsi luotto-, maksu-, tai pankkikorttia, ole erityisen huolellinen salasanojen suhteen. Oman tilipankin palveluiden käyttö verkossa on Suomessa turvallista, koska meillä on käyttäjätunnuksen ja salasanan lisäksi käytössä henkilökohtaiset avainlukulistat. Älä kuitenkaan säilytä näitä samassa paikassa jossa ne ovat alttiina hukkumiselle.

Turvalliset toimintatavat:
Tietoturva vaatii seurantaa, ja ennen kaikkea omien tapojen seurantaa.
Jätänkö läppärin autoon penkille vai laitanko sen piiloon?
Avainlukulista, käyttäjätunnus ja salasana ovat samassa lompakossa?
Juttelenko kovaan ääneen tietoturva-asioista?
Kun vanha kone lähtee, sen levyä ei tyhjennetä?
Laitanko paperit silppuriin tai uuniin vai roskikseen?
Kuka käsittelee papereitani?
Käytänkö samaa salasanaa 10 vuotta?

Hyvä toimintapa palveluiden käytössä:
1. Kirjaudu sisälle oikeasta kirjautumispaikasta.
2. Kirjaudu ulos ja sulje ohjelma tai palvelu oikein.
3. Tyhjennä tarvittaessa välimuisti.
4. Katso ettei kukaan tirkistele, mikäli käytät julkista konetta.
5. Tee rauhassa.

Arkaluontoiset asiat talteen
Arvokkaita asioita, kuten rahat pannaan lukkojen taakse. Raha ja muut arvokkaat asiat voivat nykyään olla virtuaalisia. Asia tiedetään, mutta sitä ei tiedosteta. Ihmiset eivät välttämättä ymmärrä että joku voi tulla katselemaan.

Kaksi suuntaisuus - Internetissä et ole koskaan yksin ja sinut huomataan!
Me katselemme - meitä katsellaan. Internet ei ole yksisuuntainen kuten televisio.
Kun vierailen verkkosivulla katselemassa sitä, niin myös minun toimintaani ja vierailuani sivulla seurataan.. Myös kaikkea netissä liikkumistamme voidaan seurata (vrt. matkakortti).
Verkossa seuranta on automatisoitua ja perustuu useimmiten kekseihin eli Cookieisiin sekä Internet-sivujen käytöstä kertyviin tiedostoihin eli lokeihin. Useimmiten Internet-palveluiden tuottajat käyttävät keräämiään tietoja omien palvelujensa kehittämiseen. Osa sivustojen ylläpitäjistä käyttää itse, sekä myy tietoja myös aktiiviseen mainontaan.

3. Riskit

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

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

Automatiikka
Laitteessa tai käytettävissä ohjelmistoissa voi olla toiminnassa automatiikka, joka esimerkiksi julkaisee sisällön Internetissä tai tallettaa sen verkkokansioon. Automatiikka voi olla esimerkiksi liiankin helposti, yhden napinpainalluksen takana.

Internet huijaukset
Phishing eli luotto- ja henkilötietojen kalastus tarkoittaa huijausta. Ihmisille lähetetään sähköpostiviestejä, jotka on naamioitu esimerkiksi oman pankin lähettämiksi. Viesteissä kehotetaan vaihtamaan verkkopankin tunnuslukuja Internet-sivulla, joka taas on naamioitu näyttämään pankin sivustolta.

Internet sivut
www-tiedostot ja laajennukset kuten Plug-Init, Active-x-komponentit, Flash, Java ja JavaScript-viritelmät tekevät Internet-palveluista vuorovaikutteisempia, mutta samalla avaavat useita tietoturva-aukkoja. Kun jonkun sivun käyttäminen vaatii hyväksymään uuden ominaisuuden käyttöönoton selaimessa ja tietokoneella olisi hyvä tietää myös uudet, mahdolliset tietoturvaongelmat.
Käytetyn teknologian lisäksi Internet sivuilta voi vahingossa ladata viruksia tai muuta haittaavaa sisältöä. Eniten haittaohjelmia levittävätkin lataussivut, jotka lupaavat tarjota ilmaiseksi muualla maksullista sisältöä kuten musiikin ja elokuvien suoratoistopalvelut.

Tiedostonjako
Lähiverkossa (esim. taloyhtiön verkko) tapahtuva tarkoituksellinen tai tahaton tiedostojen jako on riski-altista. Vertaisverkoissa toimivat P2P- eli tiedostonjako-ohjelmat ovat tuoneet mukanaan tietoturva riskejä ja ylläpidollisia ongelmia. Laitteiden tiedostonjako asetuksiin on hyvä myös perehtyä, ettet vahingossa jätä tiedostonjakoa päälle.

Mobiililaitteet
Kaikki kannettavat viestintään käytettävät laitteet; tietokoneet, tabletit 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 vääriin 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 tai lähettää saastuneista tiedostoja.

Sähköposti
Varo näppivirheitä! Mihin menevät viestit jotka eivät koskaan saavu perille?
Mitä niillä tehdään?
Myös sähköpostiohjelman tai palvelun asetukset tulee laittaa kuntoon. Poista käytöstä automaattinen kuvien lataaminen ja viestien avaaminen.
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, toimi seuraavasti:
1. päivitä virustietokannat. 2. kopioi liitetiedosto koneelle. 3.tarkista tiedosto virustorjuntaohjelmalla. 4. avaa tiedosto sille tarkoitetulla ohjelmalla.
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. Säädettäviä 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. Useimmiten viruksia saadaan nykyään verkkosivuilta tai sähköpostin välityksellä.

Virustorjuntaohjelma
Virustorjuntaohjelma on sovellus joka suojaa 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.

Virustorjuntaohjelma netissä - Online scannerit
Mikäli laitteesi on jo saanut tietokoneviruksen, eikä toimivaa virustorjuntaohjelmaa ole, voi viruksen yrittää poistaa verkossa olevasta palvelusta käsin. Nämä palvelut ovat vain hätävara, eikä niillä voi korvata jatkuvasti päällä olevaa virustorjuntaohjelmaa. Kaikilla suurimmilla virustorjuntaohjelmistojen valmistajilla on omat verkossa olevat palvelunsa. Suurimmalla osalla ne ovat maksuttomia. Esimerkiksi F-securella on suomenkielinen verkossa oleva virustorjuntaohjelma.
- www.f-secure.com/fi_FI/web/home_fi/online-scanner

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. Uudemmat virustyypit pystyvät myös muuttamaan itseään välttääkseen virustorjuntaohjelman.

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 - liikkuvat itsenäisesti etsien saastutettavaksi kelpaavaa tietojärjestelmää.
Tiedostovirukset - tarttuvat ohjelmiin ja suorittavat jonkin toiminnon koneella.
Levykevirukset - Koneen käynnistäminen eli buuttaaminen viruksen sisältämältä levykkeeltä tai muistitikulta aikaansaa virustartunnan.
Makrovirukset - on ohjelmoitu jonkin ohjelman, kuten esimerkiksi Wordin käyttämällä makrokielellä.

Virustorjuntaohjelmia (ilmaisia kotikäytössä):

Avira AntiVir Personal
- www.free-av.com/en/download/index.html

Avast! Free Antivirus
- www.avast.com/eng/download-avast-home.html (suomeksi)

AVG Free Edition
- free.avg.com/ww-en/download-avg-anti-virus-free

Virustorjuntaohjelma (esimerkki maksullisesta)
(laajempia, sisältävät palomuurin ja vakoiluohjelmien poiston):
F-secure - www.f-secure.fi

4.2. Palomuuri

Palomuuri 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.

Windows-käyttöjärjestelmien mukana tulee palomuuri, joka ei rajoita ulos menevää liikennettä (ts. mitkä ohjelmat käyttävät Internet yhteyttä). Parempi ratkaisu on käyttää oikeaa palomuuria, joka valvoo kaikkea liikennettä ja antaa käyttäjän valita käytettävät ohjelmat (tai alussa olevat oletusasetukset ovat riittävät eikä tarvitse tehdä liian vaikeita valintoja).

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

Porttiskannaus
Suurin osa palomuuriin 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/palomuuriohjelmaa niin paljon ulkoa päin tulevalla liikenteellä että se ei pysty hoitamaan tehtäviään. Useimmiten tämä johtaa koko tietokoneen toimimattomuuteen.

Ongelmia palomuurin kanssa?
Palomuuri 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 muuttumaan. 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

modeemissa palomuuri, että koneessa palomuuri-ohjelmisto kannattaa käyttää vain toista. Samoin kaksi ohjelmisto-palomuuria voi häiritä toisiaan. (Esimerkiksi Windowsin palomuuri ja ZoneAlarm). Ohjelmistopalomuurejakaan ei kannata pitää kahta päällä yhtä aikaa. Myös eri valmistajien palomuuri ja virustorjunta-ohjelmat voivat myös häiritä toisiaan.

Palomuuri ohjelmia (ilmaisia kotikäytössä):
ZoneAlarm Free -
www.zonealarm.com/#firewall

Comodo Personal Firewall -
www.comodo.com/home/internet-security/firewall.php

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 ennakolta
Roskaposti kannattaa ehkäistä mieluummin jo ennakolta. Mainospostissa käytettäviä osoitteita kerätään kotisivuilta, keskustelupalstoilta ja yleisesti kaikin keinoin. Muutamalla yksinkertaisella keinolla vähennät roskapostitulvaa. Muista kuitenkin että roskaposti vähenee hiljalleen ja keinot purevat vasta ajan kanssa.

1. Katso minne kirjoitat sähköpostiosoitteesi. Vältä kirjoittamasta osoitettasi oikeassa muodossa julkisille verkkosivuille. Tarkista osoitteesi myös muiden sivuilta.
2. Vältä osallistumista epämääräisiin tai mitättömiin arvontoihin.
3. Älä koskaan vastaa roskapostiviesteihin, sillä silloin saat entistä enemmän mainoksia ja osoitteesi päätyy toimivien osoitteiden listalle.
4. Älä pyydä roskapostin lähettäjää poistamaan sähköpostiosoitettasi postituslistalta.
5. 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.
6. Tee sähköpostiosoitteita käyttötarpeen mukaan. Jos joudut rekisteröitymään johonkin palveluun josta epäilet tulevan roska- tai mainospostia, tee tätä varten oma sähköpostiosoite, jota käytät vain tähän tarkoitukseen. Tällaisen osoitteen voit tehdä esimerkiksi johonkin ilmaiseen palveluun.

Suodatus
Roskaposti-viestit voidaan suodattaa erilleen 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 roskat 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.

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. Joskus vakoiluohjelmat toimivat yhteistyössä virusten levittäjien kanssa. Vakoiluohjelman poisto saattaa lopettaa joidenkin ohjelmien toiminnan, mikäli näillä on mainostussopimus.

Pop-uppien esto
Sivuilta esiin aukeavien ponnahdusikkunat eli pop-upit häiritsevät usein käyttäjää. Selaimissa on mahdollisuus estää näitä mainosikkunoita 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 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
- www.lavasoft.com/products/ad_aware.php

AVG Anti-Spyware&Anti-Virus
- free.avg.com/ww-en/homepage

HijackThis
- sourceforge.net/projects/hjt

5. Tietokoneen käyttäjän tietoturvan muistilista:

Seuraavia ohjeita noudattamalla voit parantaa koneesi ja tietojesi turvallisuutta. Ohjeet koskevat laitteita, 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 tai valitse mitään sellaista Ok-nappia minkä tarkoitusta et tiedä.
Mieti ennen kuin klikkaat myös sähköpostia lähettäessäsi. Väärin kirjoitettu sähköpostiosoite, ja viestisi päätyy väärälle vastaanottajalle.

3. Tuhoa 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 päätyy.

6. Päivitä tietokoneesi ja puhelimesi käyttöjärjestelmä säännöllisesti.
Vaikka suosituimmille käyttöjärjestelmille tehdään eniten viruksia, tietoturvauhat koskevat myös muita käyttöjärjestelmiä, joita täytyy myös päivittää.

7. Hanki tietokoneeseen tai laitteeseesi 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.

8. Asenna palomuuriohjelma.
Palomuuri-ohjelma tai -laite suojaa tietokoneesi Internet-yhteyden kautta tulevilta hyökkäyksiltä. Palomuuri pitää tietosi piilossa luvattomilta katselijoilta.

9. Säädä tietoturva-asetukset kuntoon!
Ohjelmien tietoturvaominaisuudet ovat hyödyttömiä, mikäli ne eivät ole päällä tai säädetty oikein. Säädettäviä tietoturvaominaisuuksia löytyy mm. käyttöjärjestelmästä, selaimesta, virustorjuntaohjelmasta, pikaviestiohjelmista, palomuurista ja sähköpostiohjelmasta.

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

5.2. Facebookin tietoturva

10 ohjetta jotka auttavat sinua hallitsemaan tietojasi Facebook-palvelussa.

1. Rekisteröityminen
- Käytä toista salasanaa kuin sähköpostissasi.
- Kirjoita salasana tarvittaessa talteen.

2. Tutustu yksityisyys- ja julkisuusasetuksiin
- Omat julkisuusasetukset määrittelevät mitä tietoja näkyy ja kenelle
- Omat tiedot voivat näkyä väärille ihmisille
- Kaverien tiedot voivat näkyä väärille ihmisille

3. Seuraa - Facebook muuttuu jatkuvasti
- Omien tietojen näkymistä täytyy seurata säännöllisesti
- Yksityisyysasetuksissa saattaa tapahtua suuria muutoksia nopeasti

4. Jäsenyydet ryhmissä ja Facebook -sivuista tykkääminen
- Mieti haluatko sinun tietojasi käytettävän mainontaan
- Et välttämättä tiedä missä ja miten tietosi näkyvät

5. Vastuu - Mieti ennen kuin jaat
- Omia juttuja
- Liian paljastavia päivityksiä
- Kaverien tietoja
- Valokuvia ei saa jakaa toisista ihmisistä ilman lupaa
- Jaon jälkeen vahinko on jo tapahtunut, vaikka poistaisitkin postauksen saman tien

6. Vältä virheklikkauksia
- Facebook latautuu hitaasti, Virheklikkausten mahdollisuus on suuri
- Kaikkea ei pidä klikata

7. Valitse ystäväsi Facebookissa
- Kaikkia kaveripyyntöjä ei tarvitse hyväksyä. Sinulla on oikeus valita itse kaverisi.

8. Valitse ryhmät, asiat ja sivut joissa toimit

9. Pelit ja sovellukset jakavat tietoja
- Älä asenna pelejä ja sovelluksia ennen kuin tiedät mitä ne tekevät
- Älä asenna pelejä ja sovelluksia ennen kuin tiedät miten ne jakavat tietoja
- Muiden ulkoisten palveluiden käyttäminen Facebook-kirjautumisen avulla

10. Vältä ketjupostauksia, jos et tunne asiaa
- Huijaus ja häirintäviestejä voi levitä Facebookin kautta kavereille

Selko-e:n Facebook sivu: www.facebook.com/pages/Selko-e/81352074380

6. Linkkejä ja lisätietoa

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

Linkkejä:
www.viestintavirasto.fi/tietoturva.html
- Viestintäviraston tietoturvasivut.
linux.fi/wiki/Tietoturva
- Linux-käyttäjän tietoturva
www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf
- Tiivis tietoturvasanasto (pdf-tiedosto).
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.