Tampereen
ammattikorkeakoulu

Opinnäytetyö

Tietoturvakoulutus kotikäyttäjille

Annika Minkkinen

Tietojenkäsittelyn koulutusohjelma
kesäkuu 2007
Työn ohjaaja: Petri Heliniemi

Tampere 2007

TAMPEREEN AMMATTIKORKEAKOULU

Tekijä(t):	Annika Minkkinen
Koulutusohjelma(t):	Tietojenkäsittely
Opinnäytetyön nimi:	Tietoturvaa kotikäyttäjille
Työn valmistumis-kuukausi ja -vuosi:	kesäkuu 2007
Työnohjaaja:	Petri Heliniemi
Sivumäärä:	28+14

Tiivistelmä

Tietoturvakoulutuksen idea oli oma. Olin huomannut ympärilläni tavallisten ihmisten tietämättömyyden aiheesta ja varsinkin sen tietyistä osa-alueista. Aiheella ei siis ole toimeksiantajaa. Kuitenkin vanha harjoittelupaikkani Tampereen kesäyliopisto lähti projektiin mukaan. He tarjosivat tilat koulutukselle ja hankkivat koulutettavat ihmiset paikalle.

Työn tavoitteena oli levittää tietoturvatietoutta tavallisille tietokoneen käyttäjille. Valistaa heitä sen eri osa-alueista sekä antaa vinkkejä ilmaiseen tietokoneen suojaamiseen.

Oman osaamisen perustana oli Tietoturvan peruskurssi ja oma kokemus näistä asioista. Materiaalin kanssa apuna toimivat taiton ja graafisen suunnittelun kurssit. Itse koulutukseen pohjalta löytyi Kouluttajakoulutus.

Työn hyödyllisyyden arviointiin käytettiin ennen ja jälkeen -lomakkeita, joissa kyseltiin kurssilaisilta heidän taustatietämystään ja käsitystä koulutuksen onnistumisesta.

Kurssille osallistui viisi henkilöä. Kaikilla heillä oli jo melko hyvä tietotekninen ymmärrys pohjalla, mutta myös he saivat kurssista jotain uutta. Kaikki aikoivat jakaa saamaansa tietoa myös tuttavilleen. Näin ollen kurssin pienestä osallistujamäärästä huolimatta koulutuksesta on hyötyä useammille.

Vastaavia kursseja tulisi järjestää enemmänkin. Aihe on kuitenkin vielä niin outo niin monelle. Ongelmana onkin saada kansalaisia lähtemään mukaan vastaavanlaisille kursseille.

Avainsanat: Palomuuri Päivitys Tietoturva Virus Spyware

TAMPERE
POLYTECHNIC

Author(s) Annika Minkkinen

Degree Programme(s) Business Information Systems

Title Data Security for Regular Users

Month and year June 2007

Supervisor Petri Heliniemi **Pages:** 28+14

Abstract

The idea for this course came from me. I had noticed how little normal people knew about data security and its areas. I introduced the idea to Tampere Summer University and they agreed to take the course in their course selection.

The goal of this thesis is to spread knowledge in the field of data security. Information is targeted to regular internet and computer users. Beside information, I chose to give them tips on how to protect the computer free of charge.

I have gained my knowledge in the field mainly from own experience. The material was created with the help of DTP courses.

I used questionnaires to gather information on how useful the course was and how much they knew in advance. Those were answered by the five participants in my course.

I was able to help five to understand and know more about data security. All of them mentioned they are going to talk about these things with their friends. Through that the course was useful to more people than just the five.

It is an indisputable fact that such courses are necessary. The problem is IT courses do not attract people, not even when they are free.

Keywords Firewall Update Data security Virus Spyware

Sisällysluettelo

1 Johdanto

Olen monta kertaa huomannut, kuinka vähän tavalliset ihmiset tietoturvasta loppujen lopuksi tietävät. Mielestäni on tärkeää tietää enemmän taustaa, koska silloin annetaan peruskäyttäjille mahdollisuus omaan harkintaan ja lievennetään paniikkia, jos sellaista tulee vastaan näiden asioiden suhteen.

Useimmat ihmiset tietävät viruksista ja ymmärtävät koneensa niiltä suojata. Palomuurin käyttökin alkaa olla, hallussa. Useimmille ihmisille on kerrottu, että tällaiset tulee koneessa olla kun netissä asioidaan. Toinen asia sitten on, kerrotaanko heille, miksi palomuuri ja anti-virus-ohjelmisto on tarpeen.

Entäpä sitten mainos- ja vakoiluohjelmat? Olen huomannut, että tietämys näihin liittyen on monesti lähes olematonta. Ihmiset ajattelevat, ettei heidän koneissaan sellaisia ole, kun mitään ei näy päällepäin. Eipä sillä, harvat ovat koskaan kuulleetkaan niistä. Tunnustan olleeni yksi näistä ihmisistä vielä kolme vuotta sitten. En ollut ikinä kuullutkaan mainosohjelmista.

Tietoturvahan on paljon muutakin kuin tietokoneen suojaamista haitallisuuksia vastaan. Se ulottuu paljon laajemmalle. Näitä asioita on tarkoitukseni myös pohtia ja kertoa eteenpäin.

Opinnäytetyöni päätavoitteena on levittää tietämystä tietoturvasta halukkaille. Tätä varten suunnittelen ja pidän pienen koulutuksen halukkaille. Tavoitteena on myös suunnitella pieni ohjevihkonen siihen avuksi ja toteuttaa se. Myös opetuspäivän arviointi voidaan laskea tavoitteeksi tämän opinnäytetyön osalta.

Materiaaliksi olen ajatellut kehittää pienimuotoisen vihkosen, jossa on kätevästi löydettävissä avaintieto. Erillisten papereiden säilyttäminen ja käsittely voi olla turhauttavaa. Vihkonen säilyy helpommin.

Oppitunnin lopussa pyydän kirjallista palautetta, josta selviää, miten koulutus onnistui. Käsittelen palautetta ja mietin kehitysideoita mahdollisia muita vastaavia kursseja varten.

Opinnäytetyössäni en käsittele tietoturvaa yrityksen näkökulmasta, koska koulutukseni on suunnattu tavallisille kotikäyttäjille.

Opinnäytetyössä ei ole varsinaista toimeksiantajaa. Kurssi järjestetään kuitenkin harjoittelupaikkani, Tampereen kesäyliopiston, kurssina.

2 Teoria

Tässä luvussa käsitellään tietoturvan teoria ja kurssin suunnitteluun liittyviä asioita.

2.1 Tietoturvan osa-alueet

Tietoturva on hyvin laaja käsite. Sen sisään mahtuu monenmoista erilaista sisältöä. Tässä ei kuitenkaan kaikkea sitä käsitellä, koska aihe on rajattu kotikäyttäjiin. Huomioon otetaan ainoastaan tärkeimpiä asioita, joita tavallisen käyttäjän olisi hyvä tietää.

2.1.1 Päivittäminen

Pahimpien uhkien torjuntaan riittää päivittäminen ja palomuuri. Tietokoneen turvallisena pitäminen on erittäin hankalaa ja työlästä, jos koneen päivitykset eivät ole ajan tasalla.

Miksi päivitetään?

Päivittäminen korjaa käyttöjärjestelmässä tai ohjelmistossa esiintyviä virheitä. Kun uusia käyttöjärjestelmiä ja ohjelmia kehitetään, niistä ei saada julkaisuvaiheessa virheettömiä. Sitä mukaa kun virheitä huomataan käytössä, niihin kehitetään korjauspäivitys. Office 2003 Excelissä oli virheitä, jotka aiheuttivat laskuvirheitä (Järvinen 2006: 18). Tällaiset suoranaiset ohjelmointivirheet voivat aiheuttaa paljon ongelmia esim. yrityksen taloushallinnossa.

Selaimissa tai ohjelmissa voi olla sellaisia virheitä, jotka saattavat jopa itsestään ladata haittaohjelmia koneelle tai jakaa tiedostoja muiden kanssa lupaa kysymättä. Näistä voi koitua vakaviakin tietoturvauhkia.

Päivityksiä on myös sellaisia, jotka eivät varsinaisesti korjaa virheitä, vaan tuovat jotain ihan uutta. Esim. yhteensopivuuden sellaisen tekniikan kanssa, jota ei ollut vielä koneen valmistuessa. Valmistajan kannalta jatkuva päivittäminen ei ole kannattavaa. Tästä syystä uusien päivityspakettien ilmestyminen lakkaa aina jossain vaiheessa. Näin ollen käyttäjän halutaan ostavan uusi versio. Vuonna 2006 Microsoft ilmoitti, ettei Windows XP:n Service Pack 1:een enää tule päivityksiä. Service Pack 2 on tietoturvallisempi kuin edeltäjänsä, sen lisäksi uusi Windows Vista

oli ilmestymässä piakkoin. On tietysti mahdollista pärjätä vanhalla versiolla ongelmitta, mutta tietoturvallinen ratkaisu vaatii uusimman version/päivityksen.

Virheitä voidaan käyttää väärin, jos suojaavaa päivitystä ei ole asennettu/julkaistu. Aina on joku, joka keksii keinon hyväksikäyttää näitä bugeja (nimitys virheille). On hyvin mahdollista, ettei pahaa aavistamaton käyttäjä edes huomaa, mitä on tapahtunut, kun esim. Word-tiedoston mukana on lähtenyt tärkeää tietoa omalta koneelta vääriin käsiin.

Windows- ja Macintosh-käyttöjärjestelmissä päivitys on nykyään automaattista. Windows asentaa päivitykset automaattisesti ja ilmoittaa asennuksen jälkeen, jos kone tulee käynnistää uudelleen. Windows XP:n SP2 päivittää automaattisesti ja osaa jopa tarvittaessa käynnistää koneen automaattisesti uudestaan. SP2 hakee päivityksiä keskellä yötä, jolloin uudelleenkäynnistys ei normaalisti häiritse käyttäjää, ellei tallentamattomia tiedostoja ole jäänyt auki. Macintosh kysyy päivityksiä löytäessään asennukseen lupaa, koska se vaatii pääkäyttäjän salasanan.

Jos koneessa on laiton käyttöjärjestelmäkopio, päivittäminen ei välttämättä onnistu. Useimmat päivitykset testaavat käyttöjärjestelmän aitouden. Tällä valmistajat pyrkivät vähentämään laitonta käyttöä. Toisin kuin päivitykset, erilaiset haittaohjelmat eivät tarkista ohjelman laillisuutta, jolloin uhka saattaa olla jopa pahempi kuin laillisessa, päivitetyssä versiossa.

Ei ole olemassa virheetöntä ohjelmaa. Arvioiden mukaan ohjelmissa on yhdestä seitsemään virhettä tuhatta koodiriviä kohden (Järvinen, 2006: 23). Käyttöjärjestelmissä on useita kymmeniä miljoonia rivejä koodia. Siitä voidaan päätellä virheiden määrän olevan valtavan suuri. Kaikkia virheitä ei aina huomata, koska on virheitä, joiden haittavaikutus on olematon. Monista ohjelmista julkaistaan puolivalmiita beta-versioita, joiden tarkoituksena on selvittää olemassa olevia virheitä ennen virallista julkaisua. Beta-versiot ovat usein ilmaisia, kun täysiversio on maksullinen. Yahoo Messengerin Mac -versio 3.0 on toistaiseksi vasta beta-vaiheessa ja siinä on vielä useita bugeja, jotka pitää saada korjatuksi ennen varsinaista versiota. Yahoo messenger on kuitenkin ilmainen myös täysversiona.

2.1.2 Palomuuri

Palomuuri voi olla joko fyysinen laite tai ohjelmisto. Windows XP:stä, Mac OS X:stä ja Linuxista ohjelmistopalomuuri löytyy valmiiksi, jolloin erillistä palomuuria ei tarvita.

Palomuuri suojaa ulkoisen ja sisäisen verkon välistä liikennettä. Se pitää luvattomat ulkoapäin tulevat hyökkäykset kurissa. Palomuuri on ainoa tapa suojautua käyttäjästä riippumattomia hyökkäyksiä vastaan. Palomuurin tärkeydestä kertoo jo sekin, että vaikkei Linuxille ja Mac OS X:lle ole toistaiseksi levikissä kovinkaan paljon haittaohjelmia, niissä molemmissa on kuitenkin palomuuri omasta takaa.

Useimmilla palomuureilla voidaan myös määritellä, mille ohjelmille sallitaan internetin käyttö. Esim. ZoneAlarm-palomuuriohjelma kysyy aina lupaa käyttäjältä, kun ohjelma yrittää päästä internetiin. Selaimien ja muiden internetiä tunnetusti käyttävien ohjelmien kohdalla kannattaa laittaa ruksi kohtaan, joka kysyy, toimitaanko näin joka kerta. Jos jokin vieras ohjelma yrittää päästä internetiin, sen pääsy voidaan estää. Jos haluaa tietää, mitä se ohjelma tekee, kannattaa sen nimi ”googlata”.

Ulkopuoliset hyökkäykset eivät aina tarkoita tietomurtoa. Aivan yhtälailla ulkoapäin saatetaan yrittää palvelujen kaatamista ja ylikuormittamista. Tässä palomuuri auttaa. Ennen kuin yhteyspyynnöt ulkoapäin päästetään koneelle, ne joutuvat palomuurille. Palomuuri päättää, onko kyseessä sallittu yhteys vai ei. Näin ollen prosessori ja muistitehoja ei viedä turhan päiten kaikkien yhteyspyyntöjen käsittelyyn, vaan kone saa toimia rauhassa.

Palomuuri tietää, milloin jokin ohjelma yrittää ulospäin suuntautuvaa liikennettä ja voi estää sen tarvittaessa. Useimmiten haittaohjelmat yrittävät lähettää tietoja ulospäin. Se ei kuitenkaan tarkoita, että kaikki ulospäin yrittävä liikenne olisi peräisin haittaohjelmista. Luotettavatkin ohjelmat tarkistavat ajoittain onko niille olemassa tuoreempia päivityksiä.

Erillinen palomuurilaite (rautapalomuuri) on toimiva vaihtoehto myös kotikäytössä, joskaan ei ihan niin tavallinen. Etuina siinä on luotettavuus, eikä se häiriinny tietokoneessa mahdollisesti tapahtuvista ongelmista.

Jos kotona on useampi kuin yksi kone, voidaan yhdellä laitteella suojata kaikki koneet. Se on aina käynnissä ja siihen ei voi murtautua.

Huonoina puolina on ylläpito. Rautapalomuuri vaatii osaavan käyttäjän, joka tarvittaessa päivittää ja tarkkailee lokeja. Ne eivät myöskään ole halpoja. Kuitenkin, jos kotona on ADSL, WLAN tai muu pääte, saattaa siinä olla jonkinlaisia palomuuritoimintoja. Toiminto pitää muistaa itse ottaa käyttöön. Rautapalomuuri ei kerro suoraan käyttäjälle, jos jokin ohjelma tahtoo käyttää liikennettä ulospäin. Se kirjaa kaiken liikenteen kuitenkin lokiin, josta voi tarkastella palomuurin tapahtumia.

Palomuuriohjelmien hyvinä puolina voidaan pitää helppoa käyttöönottoa sekä ilmoituksia lähtevästä liikenteestä, jolloin käyttäjä voi joko estää tai sallia liikenteen.

Huonoja puoliakin löytyy. Käyttäjä, jolla ei ole tarvittavaa teknistä tietämystä, voi helposti estää tarpeellista ja sallia haitallista liikennettä. Ne ovat myös vain tietokoneohjelmia, jolloin ne sisältävät virheitä, ja jotkin haittaohjelmat voivat hyväksikäyttää näitä virheitä. Ohjelmistopalomuuri käynnistyy vasta käyttöjärjestelmän käynnistymisen jälkeen. Se ei siis ole koko ajan käynnissä ja kone saattaa päästä verkkoon ennen ohjelman käynnistymistä. Se voi myös hidastaa koneen toimintaa kuluttamalla prosessorin ja muistin tehoja, ihan kuin muutkin ohjelmat.

Jos mahdollista, voi käyttää molempia. Ei kuitenkaan kahta ohjelmistopalomuuria samaan koneeseen. Niiden päällekkäiset asetukset saattavat sekoittaa toimintaa ja estää verkon toiminnan.

Järvinen(2006) kertoo kirjassaan testistään, jossa hän laittoi Windows XP SP1 -koneen käyttöön ilman palomuuria suoraan internetiin. Konetta ei käytetty surffailuun, eikä edes sähköpostin lukemiseen. Kone saastui itsestään ja ensimmäinen näkyvä merkki haittaohjelmasta tuli jo 19 minuuttia kokeen aloittamisen jälkeen. Iltapäivällä koneen työpöydälle oli asentunut pikakuvakkeita mm. online-pelipaikkoihin ja Ad-aware löysi yli 300 epäilyttävää kohdetta.

2.1.3 Selaimen valinta

Suurin osa maailman tietokoneista on varustettu Windows-käyttöjärjestelmällä ja Internet Explorerilla internetin selaamiseen. Tästä syystä suurin osa haittaohjelmista on kehitetty juuri näitä varten. Uhkien kehittäjät haluavat saada mahdollisimman paljon haittaa aikaiseksi.

Suosittelen selaimeksi Mozillan Firefoxia tai Operaa. Firefox alkaa olla jo sen verran suosittu, että on vaikea sanoa, kuinka kauan sen turvallisuus on tarpeeksi hyvä (Liite 2.). Selainta toki päivitetään jatkuvasti, jotta turvallisuusriskejä ei ehtisi tulla. Firefox on erinomainen valinta kotikoneen selaimeksi. Opera on harvinaisempi, tästä syystä vielä hieman turvallisempi. Molemmat ovat ilmaisia.

Turvallisin tilanne olisi käyttöjärjestelmän vaihto Linuxiin tai Macin OS X:ään. Tottumattomallekin tietokoneen käyttäjälle Mac on erinomainen vaihtoehto helppokäyttöisyytensä ansiosta.

2.1.4 Virukset

Virus on haitallinen ohjelma, joka pyrkii kopioimaan itseään käyttöjärjestelmästä toiseen ja tekemään tuhojaan. Virukset voivat sekoittaa kovalevyn niin pahasti, että vain formatointi auttaa. Ne saattavat muokata vain jotain tiettyä tiedostoa tai kansiota, jolloin ongelmasta voidaan selvitä ilman kovalevyn formatointia. Anti-virusohjelma on tässä apuna, sillä voi yrittää poistaa virusta.

Ensimmäinen virus havaittiin vuonna 1982 Apple II -koneissa ja ensimmäinen PC-virus neljä vuotta myöhemmin.

Kirves (2007) kirjoittaa tarkempia lukuja tämän hetkisistä haittaohjelmista. Numerot perustuvat McAfeen Marius van Oersin tietoihin. Haittaohjelmia tunnetaan yli 236 000. Näistä 69 on suunnattu Mac OS-käyttöjärjestelmien vanhempiin versioihin. Seitsemän sen sijaan uusimpaan Mac OS X -käyttöjärjestelmään. Unixin ja Linuxin eri versioihin niitä löytyy noin 700. Näiden lukujen jälkeenkin yli 235 000 on jää Windows-järjestelmille.

Anti-virus-ohjelma täytyy aina pitää ajan tasalla. Paras keino suojautua uusimpia viruksia on asentaa ohjelmiston tarjoamat päivitykset. Laajakaistayhteyksiä käytettäessä nämä ohjelmistot päivittyvät automaattisesti aina uusien päivitysten tullessa tarjolle. Dial-up-liittymien kanssa pitää itse muistaa hoitaa päivitysten asentaminen.

Virustorjuntaohjelmat ovat yleensä aina päällä käynnistyksen jälkeen, mutta monet haitat jäävät silti huomaamatta. Kuten ohjelmistopalomuuri, on virustorjuntaohjelmakin vain ohjelma. Sillä menee hetki käynnistymiseen käyttöjärjestelmän käynnistymisen jälkeen. Siinä se pieni hetki ennen käynnistystä antaa mahdollisuuden virusten leviämiselle. Tästä syystä kannattaa aika

ajoin ajaa oma anti-virus-ohjelma ja näin tarkistaa kone. Tarkistusta voidaan tehostaa myös Ad-Aware tai muilla mainosohjelmien poisto-ohjelmilla. Omasta kokemuksesta koti-PC:n virustorjuntaohjelma tarkistaessaan konetta saattaa olla huomaamatta joitain matoja tai troijalaisia, mutta taustatarkastaja huomaa nuo sitten kun Ad-Aware tekee omaa tarkistustaan.

2.1.5 Muut haittaohjelmat

Mainos- ja vakoiluohjelmat ovat yleisin tietokonetta haittaava ongelma. Jos tietokone vaikuttaa normaalia hitaammalta, se voi olla oire tällaisten ohjelmien olemassaolosta.

Vakoiluohjelmien tarkoituksena on tarkkailla koneen käyttöä, esim. näppäilyjä tai jopa käyttäjän tallentamia tietoja. Sitten se lähettää tietoa automaattisesti eteenpäin.

Mainosohjelmat luovat usein esim. pikakuvakkeita työpöydälle. Niissä usein mainostetaan online-pelejä tai muita viihdesivuja. Tällaiset eivät häivy vain roskakoriin siirtämällä. Viimeistään seuraavalla käynnistyskerralla ne ilmestyvät takaisin. Ongelma vaatii Ad-Awaren tai muun tarkoitukseen luodun ohjelman.

Troijan hevoset, kuten nimestäkin voidaan jo päätellä, ovat naamioituja haittaohjelmia. Käyttäjä voi ladata pahaa aavistamatta vaikka pelin koneellensa eikä tiedä, että se sisältääkin haittaohjelman. Troijalainen voi aiheuttaa eritasoista vahinkoa. Voi olla, ettei käyttäjä tiedä koneensa saastuneen. Troijalaiset ovat nykyään kaikkein yleisimpiä haittaohjelmia (Karvonen, 2007).

Madot ovat viruksen tyyppisiä ongelmia. Ne pyrkivät kopioitumaan toisiin laitteisiin käyttäen takaportteja ja koodivirheitä hyväkseen. Mato saattaa mukanaan asentaa esim. vakoiluohjelman koneelle.

Internet huijaukset

Internetin suosio on lisännyt myös internet-mainonnan suosiota. Nykyään on vaikea löytää nettisivua, jolla ei olisi ollenkaan mainoksia. Suurin osa mainoksista on ihan kunnollisia, mutta mukaan mahtuu monia huijauksia.

Olen törmännyt monilla sivuilla mainokseen, jossa kerrotaan minun olevan 999,999,999 vierailija sivuilla. Sitten pyydetään

klikkaamaan mainosta, jotta saisin palkintoni. Miksi yksikään sivusto huomioisi kävijää, joka ei ole tasaluku; miljoonas, kymmenesmiljoonas jne. Sen lisäksi tuo tismalleen sama mainos esiintyy muillakin sivustoilla. Jos kerrotaan, että olet yli sadasmiljoonas asiakas, kannattaa muistaa järkevä ote asiaan. Sivustojen on melko mahdotonta seurata tarkkaa kävijämäärää, joten ei kannata innostua tuollaisista.

Kaikenlaisia ”nyt olet voittanut jotain todella hienoa” yms. mainoksia hyppii silmille lähes miltä tahansa sivustolta. Niitä ei kannata uskoa. Hyvä keino tunnistaa huijaus on puutteelliset yhteystiedot. Yksikään rehellinen yritys ei ilmoita yhteystiedoikseen pelkkää sähköpostiosoitetta.

Useimmat ilmaiset matkat, tuotteet tai muut mahdolliset hyvät palkinnot internetin pop-up-mainoksissa ovatkin itse asiassa kalliita. Niitä kuvataan ilmaisina, mutta pienellä printillä tai yhteydenotolla selviää, mitä kaikkea sitten itse joutuukaan maksamaan. Poetry.com lähettää silloin tällöin sivuilla runon julkaisseille sähköpostia ”Annual Poetry Awards”. Olet voittanut palkintoja, olet yksi maailman lahjakkaimmista runoilijoista. Palkinnoksi saat pokaalin ja todistuksen. All you have to do is. lähetä uusi runo. Jos et itse pääse tulemaan paikalle maksa ammattilaiselle korvausta runosi lukemisesta, sen lisäksi palkinnoista veloitamme niin ja niin monta kymmentä dollaria.

Hyvä nyrkkisääntö on; ”jos se kuulostaa lian hyvältä ollakseen totta, se todennäköisesti ei siis ole totta”. Omaa järkeä saa aina käyttää reagoidessaan internet-mainontaan ja sivuistohin, joihin ne johtavat.

Sähköposteihin pätee myös maalaisjärjen käytön kultainen sääntö. Jos viesti näyttää oudolta, ei sitä kannata avata, ainakaan siinä olevia linkkejä/liitetiedostoja.

Ebay ja PayPal ovat olleet huijareiden suosiossa viime aikoina. Virallisen näköinen sähköpostiviesti pyytää esim. päivittämään tunnuksia. Viestissä on linkki sivulle, josta sen voi tehdä. On hyvin mahdollista, että kyseinen sivu on huijareiden kasaama näköissivu alkuperäisestä. Yksi tapa tunnistaa huijaussivu on katsoa osoiteriviä. Joskus siinä voi olla osoitteen sijaan pelkkä IP-osoite. Tällöin ei missään nimessä ole kyseessä aito sivu. Toinen keino välttää omien tunnusten joutumista vääriin käsiin, on jättää se linkki rauhaan. Osoitteen voi itse kirjoittaa osoiteriville. Silloin voi olla varma, että päätyy oikeaan paikkaan.

Yksikään virallinen taho tai yritys ei pyydä asiakkailtaan tunnuksia yms. ainakaan sähköpostitse. Jos asia epäilyttää, voi ottaa yhteyttä viestin lähettäjään ja kysyä onko viesti aito. Kuitenkaan yhteystietoja ei kannata viestistä ottaa, sitä ei koskaan tiedä, ovatko nekin huijausta. Tällaisia huijauksia kutsutaan Phishing-nimellä. Suomeksi se olisi khalastelua.

2.1.6 Salasanat

Salasanoja tarvitaan nykyään joka paikkaan. Siihen on myös hyvä syy. Salasana on ainoa keino välttyä ulkopuolisten pääsyltä omiin tiedostoihin, sähköpostiin, koneelle yms.

Salasanojen tulee olla vaikeita arvata. Niissä kannattaa käyttää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Niiden tulee kuitenkin olla sellaisia, jotka itse pystyy muistamaan. Salasana nimestään huolimatta ei saisi olla sana millään kielellä. Se ei myöskään saa olla oma, puolison, lasten syntymäpäivä tai muu itselle merkittävä päivä, auton rekisterinumero tai lemmikin nimi muutamia mainitakseni.

Paras tilanne on sellainen, jossa jokaiseen paikkaan on eri salasana. Salasanasta ei ole mitään hyötyä, jos joku ulkopuolinen onnistuu keksimään yhden ja se käykin kaikkiin kohteisiin. Käyttäjätunnusta ja salasanaa ei missään nimessä saa säilyttää samassa paikassa, ellei se paikka ole oma pää. Oma pää onkin ehdottomasti paras tunnusten säilytyspaikka, koska sieltä kukaan ei voi vahingossa niitä tietoja löytää.

Kun kirjaudutaan omilla tunnuksilla eri paikkoihin, pitää muistaa myös kirjautua ulos. Salasanasta ei ole hyötyä, jos jättää keinon tunkeutujille päästä sisään ja mahdollisesti vahingoittamaan itselle tärkeitä juttuja. Kohtele salasanojasi kuin kohtelet pankkikortin tunnuslukua. Ethän sitäkään muille näytä.

Myöskään selainten tarjoamia salasanan tallennustoimintoja ei tietoturvasyistä kannata käyttää, vaikka olisikin kyseessä oma tietokone. Ainakin niiden kanssa pitää käyttää omaa järkeä. Sähköpostin ja esim. huuto.netin salasanoja ei kannata tallentaa. Joku voi muuten sinun nimissäsi tehdä tuhoja. On paikkoja, esim. jotkin verkkolehdet vaativat kirjautumisen, joissa tunnusten tietäminen ei aiheuta pahoja tilanteita, koska käyttäjille ei anneta sellaisia toimintoja, joita voisi väärinkäyttää. Ja monissa paikoissa tietojen muuttaminen vaatii salasanaa. Kun ulkopuoliset pääsevät kirjautumaan tallennetuilla tunnuksilla, eivät he

saa tietoonsa salasanoja, eivätkä siis pysty sen perusteella tekemään muutoksia.

Salasanan turvallisuuden kannalta on tärkeä vaihtaa sitä säännöllisesti. Hotmail-sähköposti tarjoaa mahdollisuuden vaihtaa salasanaa automaattisesti 72 päivän välein. Siitä tulee muistutus ajan kuluttua umpeen tai sisäänkirjautuessa vaaditaan salasanan vaihtoa edellisen vanhentuessa.

Salasanan tulee olla vähintään kahdeksan merkkiä pitkä ja koostua isoista ja pienistä kirjaimista, sekä numeroista ja erikoismerkeistä. Sen ei tarvitse sinällään olla vaikea sana, mutta se pitää naamioida vaikeasti keksittävän muotoon.

Marylandin yliopiston tutkimuksen mukaan (Kirves, 2007) tunkeutujien neljä yleisintä salasanakokeilua olivat root, admin, test ja guest. Tämä tarkoittaa sitä, että nämä salasanat päästävät usein hyökkääjät sisään järjestelmiin. Salasanojen merkityksen pitäisi olla jo itsestään selvää, mutta ilmeisesti monet eivät silti kään vielä osaa valita vaikeaa salasanaa.

Salasanan tärkeys ei koske vain tietokoneita ja internetiä, vaan myös matkapuhelimia. Se pin-koodi pitää muistaa vaihtaa joksikin muuksi siitä 0000:sta. Myös puhelinvastaajan koodi tulee olla jotain muuta kuin se vakio. Olen kuullut ihmisestä, joka tunkeutuu vastaajaan, johon ei ole koodia vaihdettu ja tekee tuhojaan siellä.

2.1.7 Varmuuskopiointi

Tietokoneelle kerääntyy kaikenlaista tärkeää: valokuvia, tärkeitä työtiedostoja yms. Tietokone on haavoittuvainen laite. Tärkeät tiedostot tulee siis varmuuskopioida. Hyvä tapa on esimerkiksi polttaa ne CD- tai DVD-levylle. Jos tietokoneelle käy huonosti ja se joudutaan formatoimaan tai jos sieltä katoaa tietoa, on tärkeimmät tallessa. Tämä ei tietenkään toimi, ellei varmuuskopioita säilytetä hyvin. Suojassa varkauksilta ja pilaantumisilta.

2.1.8 Papereiden hävittäminen

Kotiin kertyy aina kaikenlaista paperia, josta pitää jossain vaiheessa päästä eroon. Osassa näistä on tärkeitä tietoja: tilinumeroita, asiakasnumeroita yms. Tietoja, jotka vääriin käsiin joutuessaan voivat aiheuttaa ongelmia. Pahimmillaan tämä on on-

gelma yritysmaailmassa, mutta myös kotona liikkuu arkaluonteista informaatiota, jota ei soisi muiden silmille.

Kaikenlaiseen paperien hävittämiseen on olemassa monenlaista paperisilppuria. Kotikäyttöön kätevä on esimerkiksi sellainen roskakorin päälle laitettava, joka aktivoituu kun siihen laittaa paperin.

2.1.9 Roskaposti

Sähköpostin seassa on usein paljon erilaista roskapostia. Joskus saattaa olla jopa niin, että suurin osa postista on roskaa.

Roskapostit sisältävät usein lääkemainoksia ja muita enemmän tai vähemmän arveluttavia viestejä.

Useimmat sähköpostit osaavat erotella arveluttavan materiaalin tärkeistä sähköposteista ja siirtää ne suoraan erilliseen roskapostikansioon. Ne myös tyhjentyvät automaattisesti 5 – 30 päivän välein. Kannattaa siis aika ajoin vilkaista, ettei mitään tärkeää ole eksynyt sinne.

Roskapostin lähettäjät yrittävät kiertää roskapostisuodattimia kirjoittamalla viestin otsikon käyttämällä paljon erikoismerkkejä. Suodattimet tarkkailevat viestien otsikoista yleisiä roskapostien sisältöjä. Kun viestin otsikossa lukee esim. v:ia:g:ra, se saattaa päästä suodattimen läpi asiallisen postin kansioon.

Roskaposti on hyvä jättää avaamatta ja poistaa samantien. Oman järjen käyttö on aina sallittua.

2.2 Materiaalin ideointi

Tässä ensimmäinen havaintoni oli, kuinka en ollut osannut etukäteen ottaa huomioon kaikkia tärkeitä aiheen osa-alueita. Päivittämisen tärkeys tietoturvan kannalta oli unohtunut täysin. Olen päässyt tutustumaan siihen tarkemmin tässä lukiessani ja aioinkin aloittaa koulutukseni kysymällä oppilailtani heidän tietokoneistaan ja ohjelmistaan. Tällainen taustatieto helpottaisi kovasti luennon materiaalin kanssa. Voisin ottaa mallia Mikael Daviesin viime kesän Teacher Talk For English Teachers -kurssista, jonka kurssisihteerinä olin viime kesänä, ja pyytää osallistujilta etukäteen tiedon heidän kotikoneistaan. Tuo ei käytännössä kyllä ole paras ratkaisu, joten täytynee päätyä ratkaisuun, jossa taustatiedot otetaan vasta koulutuksen yhteydessä.

On olemassa todella vähän sopivaa kirjallisuutta aiheesta. Useimmat kirjat olivat lähinnä yrityksen näkökulmasta ajatellen. Onneksi on internet. Kuitenkin perusajatuksen sain kiinni materiaaleista.

Teoria saattaa vaikuttaa hieman yksipuoliselta, mutta siihen on hyvä syy. Koulutukseni on tarkoitettu tavallisille ihmisille, joten tästä syystä teoriani on lähinnä ajateltu kotikäyttöä varten. Materiaali tulee olemaan pienenä vihkosena siinä vaiheessa kun se opiskelijoille jaetaan tunnilla.

Aloitin materiaalin suunnittelun paperilla. Kynällä ja paperilla hahmottelin hieman alkuun sisältöä ja ulkonäköä. Tekstisisältöä voisin tietysti tehdä myös omalla koneella, mutta varsinainen materiaalin luominen tulee jättää kouluun, koska en omista tarpeellisia ohjelmistoja.

Kanteen ajattelin nimeä ”Pieni kodin tietoturvaopas” ja kuvaa, jossa tietokoneeseen mönkii matoja ja troijan hevonen.

Seuraavalle sivulle tulee pieni esittelyteksti kurssista ja ehkä myös itsestäni ja copyright merkintä. Sen jälkeen osa-alueet esitellään loogisessa järjestyksessä, samassa, jossa ne esitellään kuulijoille.

Arvelin parhaaksi laittaa vinkit ilmaisohjelmista jokaisen sopivan aiheen perään. Aluksi aioin koota kaikki ilmaisvihjeet samaan paikkaan, mutta luovuin ajatuksesta. SiteAdvisorin kanssa tulee ongelma, koska sille ei ole varsinaista omaa aihetta. Ehkä se sopii huijausten ja roskapostin perään tai mainos ja vakoiluohjelmien yhteyteen.

2.3 Materiaalin teko

Materiaalista valmistui ensimmäisenä tekstit. Ne sain näppärästi tehtyä omalla koneella tekstinkäsittelyohjelmalla. Taisin kuitenkin tehdä ne melko kiireessä, koska sinne jäi ensimmäisen version jälkeen joitain kirjoitusvirheitä. Myös puutteita jäi melko runsaasti. Vahinko oli siinä, että huomasin asian vasta liian myöhään, illalla, päivää ennen koulutusta.

Materiaalista tuli kahdeksansivuinen. Sen suunnittelu käyttäen Adoben InDesignia ei ollut paras ratkaisu tähän tarkoitukseen. Materiaalista olisi tullut erittäin hieno, jos se olisi painettu painotalossa. Tulostettuna sivuihin jäi ylimääräistä valkoista, joka

osaltaan pilaa hienosti ajateltua suunnitelmaa. Materiaalista tehdään kopiokoneella A5-kokoinen vihkonen. (Liite 6).

Se on alusta loppuun omaa tuotosta kuvineen kaikkineen. Sisältö koostuu lyhennelmistä niistä asioista, jotka tässä opinnäytetyössä mainitaan.

Materiaali jäi kuitenkin hieman puutteelliseksi. Tärkeitä asioita ei kaikkia mainittu. Esim. salasanoista olisi voinut olla myös materiaalissa.

2.4 Ilmaisia ohjelmia tietoturvaan

McAfee SiteAdvisor on hyvin pieni paketti, jonka voi asentaa IE- tai MF-selaimiin, ja se toimii yleisimmillä käyttöjärjestelmillä. Asennuksen jälkeen selaimen oikeassa alareunassa näkyy McAfee SiteAdvisor-ruutu, joka vaihtaa väriä sen mukaan, kuinka turvallinen sivusto on. Väreinä käytetään liikennevalojen värejä. Tekijät ovat testanneet ja testaavat edelleen erilaisia sivustoja määrittääkseen niiden turvallisuuden. Analyysissä Järvisen (2006: 56) mukaan tutkitaan mm. seuraavia asioita:

- sivulta mahdollisesti latautuvat ohjelmat
- liialliset pop-up-ikkunat
- sivulla olevat linkit epäilyttäviin palveluihin
- sähköpostien määrä, jos surffaaja ilmoittaa oman osoitteensa palveluun.

Halutessaan SiteAdvisorin asetuksista voi asettaa hakukoneiden haun tulosten tarkistuksen. Tämä tekee jokaisen hakutuloksen otsikon perään merkinnän sivun turvallisuudesta. Tämä helpottaa paljon, kun hakee esim. laulujen sanoja tai muita asioita, joiden sivuilla on usein paljon häiritseviä pop-uppeja tai muita uhkia.

ZoneAlarm on hyvä ilmainen palomuuriohjelma. Erikseen asennettavana palomuurina siinä on toiminto, joka kysyy käyttäjältä aina jonkin ohjelman yrittäessä internetiin. Se myös ilmoittaa aina, kun sisäänpääsy-yritys on tapahtumassa, ellei valita, ettei niin tapahdu.

Viime aikoina on ollut keskustelua palomuurien ja Skypen yhteensopivuudesta. ZoneAlarm ei estä Skypen toimintaa, kun taas monet muut palomuuriohjelmat sen tekevät. Jansson (2007) mainitsee nettisivuillaan, etteivät F-Securen tuotteet sovi yhteen ZoneAlarmin kanssa. Jos koneessa on F-securea, kan-

nattaa käyttää jotain muuta palomuuria, jos F-Securen paketissa sellaista ei ole.

Avast!-antivirus on ilmainen kotikäytön antivirusohjelma. Se on myös suomenkielinen, joten sitä on melko helppo käyttää. Ohjelma vaatii kuitenkin rekisteröitymisen. Ilman sitä ainoastaan taustatarkistus toimii. Netistä tilattava sähköpostiin saapuva rekisteröintikoodi lisätään käynnistyksessä koodikenttään ja se on voimassa 14 kuukautta. Tämän jälkeen koodi täytyy uusia.

Avast! päivittää uudet virustunnisteet päivittäin, joten se on hyvin ajan tasalla. Uhan havaitessaan se päästää kovan hälytysäänen. Ääni on sellainen, että siitä jo huomaa, ettei kaikki ole kohdallaan.

Ohjelma tekee uhkien hävittämisestä helppoa. Aina sellaisen löytäessään, se kysyy, mitä sille tehdään ja antaa suositustoimenpiteen.

Avast! toimii parhaiten yhdessä Ad-Awaren kanssa. Ad-Aware on mainos- ja vakoiluohjelmien tunnistamiseen ja poistoon suunniteltu ilmaisohjelma. Vaikka olisitkin ensin ajanut avastin läpi ilman mainintaa uhista, saattaa Ad-Awaren ajo sen perään herättää Avasti!:n huomaamaan uhkia, joita se ei itse aiemmin löytänyt. Toisin sanoen se ei ole kuitenkaan Ad-Aware, joka ongelmat löytää, vaan se auttaa Avastia huomaamaan ne itse.

Ad-Awaren ilmaisversio ei sisällä taustatarkistusta. Se ei siis ole koko ajan käynnissä. Ohjelma pitää itse muistaa ajaa läpi säännöllisin väliajoin. Varsinkin, jos koneessa on havaittu hidastumista. Monet ihmiset valittelevat tietokoneensa hidastuneen kovasti, ihmettelevät jo, onko vakava ongelma kyseessä. Varmasti suurimmassa osassa näistä tapauksista ongelma ratkeaa Ad-Awaren avulla.

Itse olen huomannut, kuinka helposti ihmiset unohtavat Ad-Awareansa käyttää. Monille se on ladattu, mutta he eivät saa aikaiseksi sen käyttämistä. Ehkä joillain on se väärä luulo, että sen läsnäolo riittää. Tai sitten kyseessä on vain laiskuus.

2.5 Tuntisuunnittelu

Koulutuspäivä on nyt sovittu Tampereen kesäyliopiston kanssa ja se on 28.4.2007 kello 10 – 13. Opiskelijoita on ilmoittautunut kuusi kappaletta. He kaikki ovat tulleet Mukanetin kautta, eli ovat todennäköisimmin senioreita.

Tunnin alussa pitää kysyä opiskelijoilta heidän koneistaan, nettiyhteyksistä ja aikaisemmasta tietämyksestään aiheeseen liittyen.

Tätä varten olen tehnyt kyselylomakkeen tunnin alkua varten. Siinä on muutama kysymys, joihin vastataan ympyröimällä sopivin vaihtoehto ja muutama avoin kysymys.

Tahdon myös koulutuksen jälkeen tietää heidän ajatuksiaan koulutuksesta; sen hyödyllisyydestä ja onnistumisesta. Myöskin utelen hieman kehitysehdotuksia. Lomake löytyy liitteestä 4.

Varsinaisen tunnin suunnittelu jäi viime tippaan. Oppilaani ovat varmasti kovia puhumaan ja kysymään, joten ei tarvitse liikaa huolehtia ajankäyttöä.

Uskon, että aiheista saadaan keskustelua syntymään, koska kyseessä on porukka, joka on tottunut istumaan erilaisilla tietoteknisillä luennoilla. He ovat kaikki tulleet Mukanetin kautta. Mukanet tarjoaa tietotekniikkakoulutusta yli 50-vuotiaille ihmisille.

3 Oppitunti

Kymmeneltä lauantaiaamuna viisi ihmistä oli saapunut paikalle kuudesta ilmoittautuneesta. Tosin heistä taisi vain neljä olla listassa, jonka sain Kesäyliopistolta edellisenä päivänä. Yksi oli ylimääräinen tulokas.

Luokkaan oli järjestetty pöydät niin, että kuusi paikkaa oli yhden ympärillä. Siinä oli sopivasti tilaa kaikille, myös minulle.

Materiaalit löytyivät tietokonepuolen opettajan pöydältä. En ollut suunnitellut kuitenkaan mitään koneella tehtäväksi. Olin kyllä miettinyt asiaa, mutta päädyin puhtaaseen teoriaan.

3.1 Miten onnistui, mitä tapahtui

Alussa olin kovasti jännittynyt. Ensimmäisenä ohjelmassa oli alkulomakkeen täyttö.

Kyselylomakkeen täytön jälkeen opiskelijat hieman jutustelivat keskenään. Siihen väliin aloitin kysymällä, tietävätkö he, miksi päivityksiä tehdään.

Tästä eteenpäin asiat lähtivät luistamaan paremmin. Opiskelijani olivat hyvin aktiivisia ja kyselivät paljon. Keskustelua saatiin hyvin aikaiseksi ja kouluttajakin alkoi pikku hiljaa rentoutua.

Aikaisempi epävarmuus hävisi onneksi koulutuksen kuluessa. Puhe oli melko järkevää, eikä takerrellut.

Olin melko kiireessä valmistellut tukisanakortteja avuksi. Asioiden järjestys ei ehkä siksi ollut ihan täysin looginen, mutta asiat tulivat esitettyä. Kukaan ei myöskään moittinut sitä.

Pian tukisanakortit jäivät yksinään pöydälle huomiotta. Kun ei jännitä, ajatukset kulkevat, eikä tarvitse avitusta.

Yhdessä vaiheessa oppilaat tahtoivat esittelyn Mac-koneista ja perusteluita sen valintaan. Hain oman koneeni siihen ja esittelin sitä hieman. Olin kovasti yllättynyt heidän avomielisyydestään uutta konetta kohtaan. Kaikki ovat käyneet lukuisilla tietotekniikkakursseilla, joissa varmasti aina käytetään Windows-koneita. Monet heistä jopa sanoivat harkitsevansa Maccia seuraavaa konetta hankkiessaan. Yhden kurssilaisen oma tietokone oli vastikään hajonnut, joten hänelle se on jopa ajankohtaista nyt.

Uskoisin saaneeni käsiteltyä kaikki asiat, jotka tarkoitus oli. Aikaa koulutukseen meni noin kaksi tuntia. Jännitin hieman kestoa, koska en ollut harjoitellut koulutusta etukäteen.

3.2 Oppitunnilla esille tulleet asiat

Ensimmäinen huomionarvoinen asia on se, että oppilaani, vaikkakin eläkeläisiä, olivat kaikki melko hyvin perillä tietotekniikasta ja myös monista tietoturvan osa-alueista.

Oli itsekin mukava keskustella asioista ihmisten kanssa, joille kaikki asiat eivät olleet outoja. Hyvin kiitettävä lähtötaso. Helpottaa omaakin puhetta, kun ei tarvitse miettiä, kuinka tarkkaan asioita pitää kertoa.

Seuraavassa ensimmäisen lomakkeen vastaukset.

He olivat kaikki toistaiseksi vielä Windows XP:n käyttäjiä, paitsi henkilö, jonka kone oli hajonnut. Hänellä oli aiemmin Windows 98 käytössään. Kaikilla on käytössään palomuuri. Useimmilla erillisenä ohjelmana. Yksi käyttää laitteistomuuria ja XP:n omaa yhdessä. Hän utelikin, onko se tarpeeksi hyvä suoja.

Laajakaista oli lähes kaikilla. Koneensa hajottaneella sekä yhdellä toisella osanottajalla oli modeemiyhteys.

Myös anti-virus- ja mainos- ja vakoiluohjelmien poistoon tarkoitetut ohjelmat olivat useimmilla käytössä. Olin positiivisesti yllättynyt varsinkin Ad-Awaren ja samantyyppisten ohjelmien käytöstä. Parilla oli jopa useampia eri valmistajien tuotteita käytössään.

Avoimissa kysymyksissä ”mitä ymmärrät sanalla tietoturva” ja ”mitä odotat kurssilta” vastaukset olivat melko samanlaisia kaikilla.

Kurssilta odotettiin uusinta uutta, lisää tietoa tietoturvasta, ja kuinka koneen saa pysymään puhtaana viruksista.

Sana tietoturva toi heille mieleen kaikille tietokoneen suojaamisen viruksilta ja muilta hyökkäyksiltä. Se oli siis kaikille nimenomaan tietokoneeseen liittyvä termi.

Porukan ainoa miespuoleinen jäsen kertoi käyttäneensä Internet Exploreria ilman mitään ongelmia koskaan. Häntä epäilytti

vaihtamisessa joidenkin nettisivustojen toiminta. Suosittelimme hänelle kuitenkin Firefoxia. Jos vastaan tulee sivu, joka ei toimi kyseisellä selaimella, silloin vasta vaihtaa IE:iin.

4 Opetuksen jälkeen

Koulutuksesta sujui yli odotusten. Oppilaat viihtyivät. Heidän aktiivisuutensa toi tarvittavan lisän koulutukseen. Ilman sitä, lopputulos olisi ollut kuiva ja yksipuolinen.

4.1 Opiskelijoiden palaute

Opiskelijat täyttivät kaksi palautelomaketta. Toisen minulle ja toisen kesäyliopistolle. Luin kesäyliopiston lomakkeet läpi ennen lähtöä ja olin melko tyytyväinen annettuun palautteeseen. Se oli kuitenkin lähinnä numeroita, joista valittiin sopiva jokaiseen väitteeseen. Yleisin arvosana kurssille oli 4, asteikolla 1 - 5. Olen enemmän kuin tyytyväinen siihen.

Kotona pääsin lukemaan rauhassa myös oman lomakkeeni vastauksia. Pyysin heitä olemaan rehellisiä vastauksissaan, koska ne ovat tärkeitä tämän työn kannalta. Siltikin palaute oli parempaa kuin uskalsin toivoa.

Ensimmäisenä kysymyksenä oli heidän oma mielipiteensä kurssin hyödyllisyydestä.

Yksi kertoi asioiden olleen lähinnä kertausta, mutta pitää kuitenkin kertausta hyvänä asiana.

Muut saivat jotain uutta koulutuksesta. Ilmaiset ohjelmat olivat hyvä osa. Tieto, jota voi jatkossa soveltaa auttoi. Yksi jopa mainitsi, kuinka antoisaa oli saada puhua asioista ja tarkempaa tietoa asioista, jotka eivät itselle valmiiksi olleet täysin selviä.

Seuraavassa kysyttiin ohjaajan suoriutumista. Tiivistettynä kaikki sanoivat, että suoriuduin hyvin tehtävästäni. Tarkemmin kerrottuna yhden mielestä rauhallinen ja asiallinen esitystapa, toisen mielestä alkujännityksen jälkeen leppoisasti. Kolmas sanoi, että näppärästi vedetty kurssi.

Materiaalin kritiikki oli melko myönteistä. Varsinaista materiaalia sanottiin tarpeelliseksi ja kattavaksi. Kuitenkin yksi oli sitä mieltä, ettei sitä ollut ihan tarpeeksi.

Materiaalin kohdalla oli mainintaa myös muista asioista varsinaisen ohjevihkosen lisäksi. Runsas keskustelu oli heidän mieleensä. Vaikka unohdin materiaalista muutaman oleellisen nettisivun ja jouduin ne kirjoittamaan taululle, ei siitä tullut ollen-

kaan sanomista. Muutama olisi kaivannut tietokoneella näyttöä tai tekemistä.

Jokainen aikoo soveltaa oppimaansa kotona ja sen lisäksi aikoo vielä puhua asioista tuttaviensa kanssa.

Kaipaamaan jäätiin enemmän tietoa palomuureista. Myös eheyttäminen ja puhdistus mainittiin. He olivat myös uteliaita uuden Vistan suhteen. Yksi olisi kaivannut enemmän tietoa siitä.

4.2 Oma arviointi sujuvuudesta

Mielestäni koulutus ei olisi paljon paremmin voinut mennä. Yksi asia kuitenkin on sellainen, joka olisi voinut olla paremmin. Se on asiasta toiseen siirtyminen. Mielestäni se oli jotenkin epäluontevaa. Ei ollut sopivia aasin siltoja, joilla sulavasti vaihtaa seuraavaan aiheeseen.

Meneillään olevasta aiheesta keskusteltiin niin kauan kuin juttua riitti. Kun katsoin aiheen tulleen suunnilleen valmiiksi, vaihdoin sitä. Alkuun taisi tulla aina hieman teoriaa aiheesta ja sen jälkeen keskusteltiin ja kyseltiin lisää.

Oli mukavaa, kuinka kaikki ottivat osaa keskusteluun, eikä kukaan jäänyt ulkopuoliseksi. Kaikilla oli omia kokemuksia ja kysymyksiä.

Keskustelun kautta mieleen muistui asioita, joista halusin mainita. Asioita, joita en muistanut kirjata ylös apulappuihin. Heidän osallistumisensa auttoi minua.

4.3 Kurssin hyödyllisyys?

Kurssin hyödyllisyys tuli vastaan loppukyselyn vastauksista. Hekin jo, melko hyvin alaan perehtyneinä, saivat kurssista uutta ja lisää tietoa.

Joku kaipailikin enemmän vastaavia kursseja.

Kaikki omat sukulaiset ja ystävätkin tarvitsisivat kyseistä kurssia. Olenkin parhaani mukaan sopivissa väleissä yrittänyt heitä opastaa.

Windows julkaisi juuri uuden käyttöjärjestelmän, Vistan. Sen sisällyttäminen koulutussisältöön voisi olla paikallaan. Aiheena se on ajankohtainen ja kiinnostaa ihmisiä.

Kurssia voitaisiin hyödyntää helpolla tavalla materiaalin muodossa. Jos materiaaliin tekisi lisäyksiä aiheista, jotka sieltä vielä puuttuvat, sekä vaihtaisi kuvat, siitä tulisi mainio tietoisku jaettavaksi. Jos ei muuten, niin ainakin omaan lähipiiriin.

Eräs tuotantotekniikan opiskelija totesi samaa, jota tässä on tullut esiin selkeästi. Tarvetta olisi osata asiaa enemmän. Tietoa ei löydy, jollei siihen perehdy. Harvemmat oma-aloitteisesti näin tekevät.

5 Loppuyhteenveto

Työtä tehdessäni opin itsekin paljon uutta. Sain myös syvennettyä aikaisempaa tietämystä.

Opinnäytetyön lähtökohtana oli ajatus, että tavalliset tietokoneen käyttäjät eivät tiedä tarpeeksi tietoturvasta. Sen verran tietoa löytyy, että he ymmärtävät tietokoneen tarvitsevan suojaa.

Koulutuksen jälkeen ei ole mieli muuttunut. Nyt on enemmän todisteita väitteen paikkaansa pitävyydestä.

Tietoturva on tärkeä osa nykyajan tietoyhteiskuntaa. Sen pitäisi kuulua perusopetukseen jokaisella alalla.

Ihmisiä on todella vaikea saada osallistumaan erillisille tietoturvakursseille. Harvemmat tutustuvat aiheeseen omaaloitteisesti.

Materiaalin suhteen olisi pitänyt olla enemmän hiomista. Idea ei toteutunut ihan sellaisena, kuin olin ajatellut, eikä sitten jäänyt aikaa uuteen toteutukseen. Sisällöllisestikin se olisi kaivannut enemmän ajatusta. Kuitenkin se sai ihan hyvää palautetta koulukseen osallistuneilta.

Koska koulutukseen on todella vaikea saada osallistujia, voitaisiin tietoturvatietoutta lisätä esimerkiksi tietovihkosella. Jos olisi sopivat yhteistyötahot, voisi asiaa viedä eteenpäin.

Opinnäytetyön yhtenä tavoitteena oli suunnitella ja toteuttaa tietoturvakoulutus. Tämä tavoite saavutettiin varsin onnistuneesti.

Toisena tavoitteena oli suunnitella ja toteuttaa koulutukseen materiaalivihkonen. Tällainen valmistui myös. Siihen jäi kuitenkin hieman puutteita. Suunnitteluvaiheeseen olisi pitänyt panostaa hieman enemmän.

Kolmantena tavoitteena oli levittää tietoturvatietämystä tavallisten tietokoneen käyttäjien keskuuteen. Suoraan se onnistui viidelle hengelle. Heidän kauttaan tieto leviää ainakin muutamille muillekin.

Kaiken kaikkiaan tavoitteet saavutettiin. Pysyin aikataulussa, eikä mitään yllätyksiä tullut matkan varrella.

Lähteet ja liitteet:

- Järvinen, Petteri 2006. Paranna tietoturvaasi. Jyväskylä: WS Bookwell

- Jansson, Markus, Palomuureista ja ZoneAlarmista [online] [26.2.2007] http://www.markusjansson.net/fza.html

- Karvonen, Tuomas, Troijalaiset ryntäsivät haittaohjelmien ykköspaikalle [online][27.4.2007 10:48] http://www.digitoday.fi/page.php?page_id=14&news_id=200710315 Liite 4.

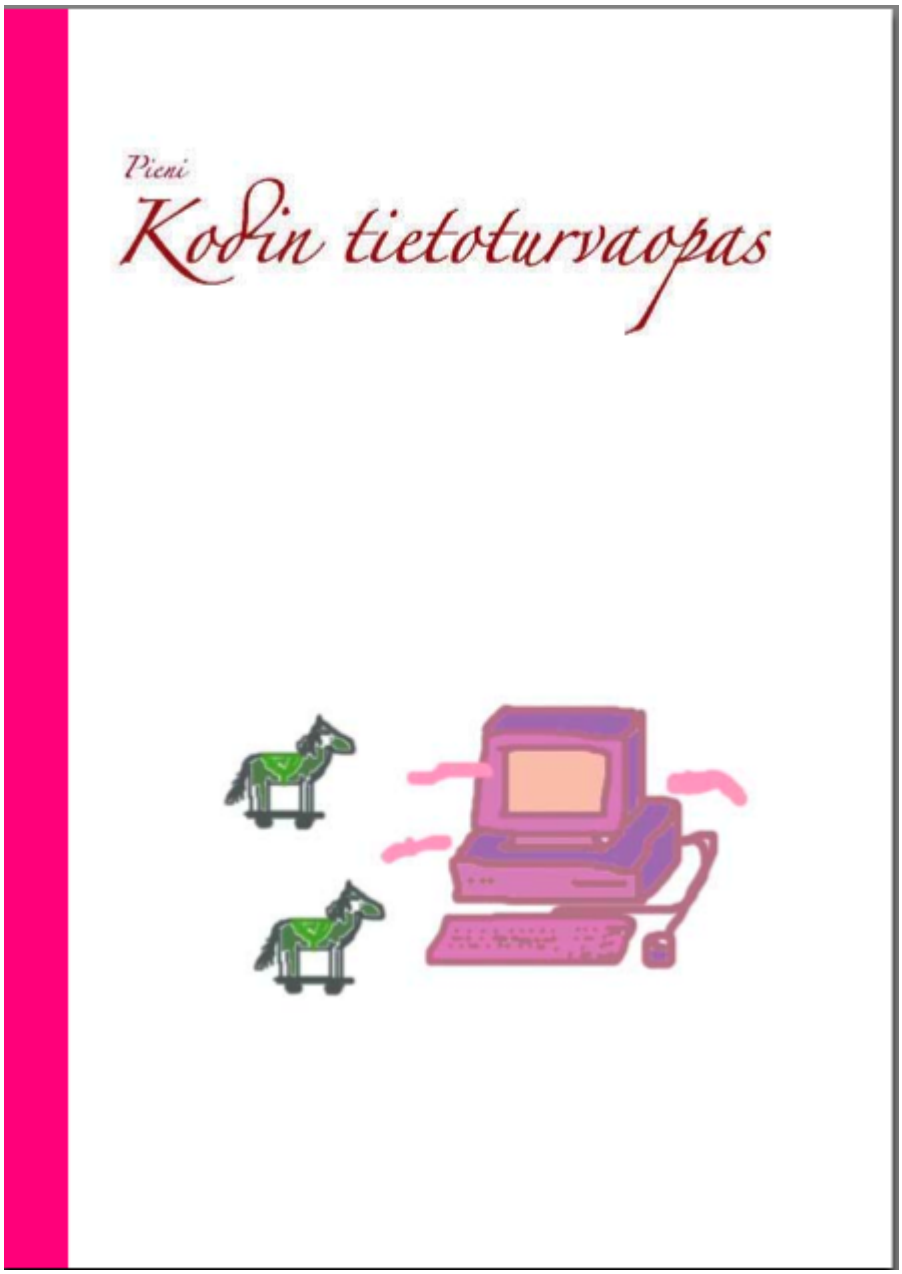
- Kirves, Antti 2007, Tutkimuskin osoittaa heikkojen salasanojen vaaran [online][12.02.2007 08:07] http://www.digitoday.fi/page.php?page_id=14&news_id=20073583. Liite 6

- Kirves, Antti 2007, Mac OS X:lle on vasta 7 haittaohjelmaa [online][21.3.2007 14:31] http://www.itviikko.fi/page.php?page_id=46&news_id=20077171 Liite 5

ilmaisohjelmalinkit

http://www.siteadvisor.com
http://www.zonelabs.com
http://www.avast.com/
http://www.lavasoft.com/products/ad-aware_se_personal.php

Liite 1.



Tervetuloa tietoturvakurssille!

Kurssin tarkoituksena on perehtyä tietoturvaan ja sen käsitteisiin.
Tämä vihkonen on suunniteltu pieneksi oppaaksi tietoturvan monipuoliseen maailmaan.

Kurssi järjestetään opinnäytetyönäni.

Toivottavasti tästä on oikeasti hyötyä!

Terveisin

Annika Minkkinen
Kurssin ohjaaja

Päivitykset

Päivityksen tärkeyttä voi olla hankala hahmottaa, jos ei tiedä syitä niihin. Päivitykset saattavat olla melko ärsyttäviä. Kone hidastuu entisestään ja usein ne vielä tahtovat käynnistää koneen uudestaan.

Kaikki tietokoneohjelmat julkaistaan viallisina. Ei sitä tahallaan tehdä. On vain kovin vaikeaa testata tuhansien koodirivien virheettömyyttä ilman laajaa käyttöä. Päivitykset korjaavat näitä virheitä. Osa virheistä saattaa aiheuttaa tietoturvauhkia.
On myös päivityksiä, jotka tuovat jotain uutta, esim. tuen tekniikalle, jota ei ollut vielä koodausvaiheessa.

Jos koneesi tahtoo asentaa päivityksiä, anna sen. Jos et heti, niin vaikka seuraavana päivänä. Silloin jo tiedetään, jos päivityksen kanssa on ollut jotain ongelmia.

PÄIVITTÄMINEN ON TIETOTURVAN KANNALTA ENSIARVOISEN TÄRKEÄÄ

Palomuuri:

Kun päivitykset on kunnossa ja palomuuri toiminnassa ollaan tietoturvan suhteen jo todella pitkällä. Ne eivät kuitenkaan riitä, mutta antavat tukevan pohjan.

Palomuureja on kahdenlaisia. Laitteistopalomuurin voi löytää kotoa esim. ADSL-modeemista. Se on siis erillinen laite, joka vahtii sisään ja ulos kulkevaa tietoliikennettä. Jos kotoasi tällainen löytyy, siitä on apua vasta, kun palomuuritoiminnon laittaa päälle. Kannattaa siis tarkistaa onko omassa modeemissa/reitittimessä/muussa verkkolaitteessa palomuuria.

Ohjelmistopalomuuri on toinen vaihtoehto. Sitä voidaan käyttää myös laitteistopalomuurin kanssa tehostamassa suojaa. Se on siis ihan kuin mikä tahansa ohjelmisto, joka asennetaan koneeseen. Siinä on myös samat uhat. Koneen kaatuessa myös palomuuri menee pois päältä, eikä välttämättä käynnisty tarpeeksi nopeasti.

Ohjelmistopalomuuri on siitä kätevä, että sillä voidaan helposti määrittää mitkä ohjelmat saavat yhdistää internettiin ja mitkä yhteydet sallitaan internetistä.

Nykyään jo tietokoneissa saattaa olla valmiina oma ohjelmistopalomuuri. Windows XP:stä ja Mac OS X:stä sellaiset ainakin löytyy. Sen saa päälle koneen omista asetuksista eikä toista palomuuria tarvita.

Vaikka ohjelmisto- ja laitteistopalomuureja voi käyttää yhtä aikaa, ei kahta ohjelmistopalomuuria kannata pitää. Ne voivat sekoittaa kaiken ja internetin käyttö ei onnistu.

ZoneAlarm:

ZoneAlarm on kotikäyttöön ilmainen ohjelmistopalomuuri. Se on melko helppokäyttöinen, eikä estä skypen käyttöä.
www.zonealarm.com

Virukset:

Virukset ovat ehkä kaikkein tunnetuin tietoturvauhka. Virus-nimitystä käytetään usein yleisnimityksenä myös madoille ja troijalaisille.
Anti-virusohjelmat etsivät ja poistavat näitä pahiksia.
Virukset yms. usein aiheuttavat tuhoja koneessa. Pahimmassa tapauksessa ne saattavat tuhota kovalevyn tai ainakin tärkeitä tiedostoja.

Anti-virus -ohjelmat ovat sellaisia, joiden taustatarkistusta ei kannata lopettaa. Sen lisäksi on hyvä aika ajoin ajaa ohjelma nähdäkseen onko jokin tuholainen onnistunut taustatarkistuksesta huolimatta ujuttautumaan koneelle.

Avast! Anti-virus:

Avast on helppokäyttöinen, ilmainen ja suomenkielinen ohjelma.
Ohjelma vaatii rekisteröitymisen, joka on voimassa 14 kuukautta.
Ilman rekisteröitymistä ohjelma ei anna suorittaa koneen tarkistusta.

www.avast.com

Mainos- ja vakoiluohjelmat ovat melkolailla yleisin haitta. Tietokoneessa, josta ei ole koskaan näitä etsitty, voi löytyä satoja, ellei tuhansia tällaisia haittaohjelmia.
Yleinen oire on koneen hidastuminen.

Mainosohjelmat voivat olla hyvinkin näkyvissä käyttäjälle. Työpöydälle voi ilmestyä kuvakkeita peleihin tai muuhun viihteeseen. Niitä voi joutua laittamaan roskakoriin jatkuvasti, kun aina ne vain ilmestyvät uudestaan.

Vakoiluohjelmien tarkoituksena on vakoilla tietokoneen käyttöä. Sellainen saattaa esim. tallentaa näppäinten paineluita ja lähettää niitä sitten eteenpäin. Jos palomuuri kysyy päästetäänkö internettiin jokin sellainen ohjelma, joka on itselle outo, kannattaa sen nimi googlata. Hakutuloksista selviää onko kyseessä haittaohjelma vai ei.

Ad-Aware SE Personal

Ad-Aware on kotikäyttöön ilmainen ohjelma, joka etsii ja tuhoaa mainos- ja vakoiluohjelmia. Ad-Aware ei suorita taustatarkistusta, vaan ohjelman käyttö jää käyttäjän vastuulle. Ad-Aware usein auttaa Avastia huomaamaan pahiksia, jotka ovat saattaneet sen omassa tarkistuksessa jäädä huomaamatta.

www.lavasoft.com

Paperien turvallinen hävittäminen:

Kotiin kertyy aina papereita, joissa on tilinumeroita tai asiakasnumeroita tai muita sellaisia tietoja, jotka voivat vääriin käsiin joutuessaan aiheuttaa vahinkoa itselle. Näiden turvallinen hävittäminen on usein ongelma. Paras ratkaisu on paperintuhoajan hankinta kotiin. Niitä on tarjolla monia erilaisia. Kotikäytössä kätevin vaihtoehto on roskakorin päälle laitettava pieni silppuri, joka aktivoituu kun siihen laittaa paperin. Silppu menee suoraan roskakoriin.

Esimerkkejä edullisista tuhoajista:

Säiliöllinen, 25€
http://www.pulju.net/shop/product_details.php?p=1106

Paperikoriin sopiva, 24,90€
http://www.salashop.fi/default.asp?l=&k=ss&o=tuoteinfo&tr=1384&t=2430

Internetistä löytyy monenlaista ja paljon erihintaisia silppureita

Bluetooth:

Bluetooth on kovasti yleistyvä ominaisuus niin tietokoneissa kuin kännylöissäkin. Se on siis langaton tiedonsiirtomenetelmä. Vaikka laite kysyy käyttäjältä sallitaanko toisella laitteella selailu, on kuitenkin turvallisinta pitää Bluetooth poissa päältä silloin kun sitä ei itse käytä. Silloin ei vahingossakaan naapuri pääse omiin tiedostoihin käsiksi.

Kännyköistä muuta:
Muista aina vaihtaa PIN-koodit ja myös vastaajan tunnusluku! Oletuskoodit on kaikkien tiedossa.

Annika Minkkinen
Tampereen ammattikorkeakoulu
Tietojenkäsittely
2007

Liite 2.

Mitä ymmärrät sanalla tietoturva?
_____
_____

Mitä odotat kurssilta?

_____

Mitä käyttöjärjestelmää käytät kotonasi?
Windows
98
XP
Vista
MUU
MAC
Linux

Mitä selainta käytät internetin selaamiseen?
Internet Explorer
Mozilla Firefox
Opera
Safari
Joku muu

Millainen internet-yhteys käytettävissäsi on?
Laajakaista
ISDN
Muu mikä?

Käytätkö palomuuria? Kyllä ei
erillinen ohjelma
Laite
käyttöjärjestelmän oma

Käytätkö anti-virusohjelmaa? Kyllä ei
Mi-
tä?_____
Miksi et?
_____

Käytätkö mainos- ja vakoiluohjelmien etsimiseen ja poistoon tarkoitettu(j)a ohjelmia? Kyllä ei

Mitä?

_____

Miksi

et?_____

Liite 3.

Mitä mieltä olet kurssin hyödyllisyydestä jälkikäteen katsottuna?
_____
_____
_____
_____

Kuinka ohjaaja onnistui tehtävässään?
_____
_____
_____
_____

Ruusuja & risuja materiaalista?
_____
_____
_____
_____

Aiotko soveltaa oppimaasi kotona?
_____

Kerrotko tuttavillesi oppimiasi asioita?
_____

Jäitkö kaipaamaan jotain?

Liite 4.

Troijalaiset ryntäsivät haittaohjelmien ykköspaikalle

Tuomas Karvonen
Julkaistu 27.04.2007 kello: 10:48

Panda Softwaren online-tarkistusohjelma Panda ActiveScanin keräämien tietojen mukaan troijalaiset olivat vuoden alussa yleisimmin havaittuja haittaohjelmia.

- Havaintojemme mukaan vuonna 2006 vakoiluohjelmat olivat yleisimpiä haittaohjelmia. Loppuvuodesta troijalaisten osuus alkoi kasvaa huomattavasti ja tämän vuoden alussa ne ovat olleet yleisimpiä liikkeessä olevia haittaohjelmia, katsastaa Pandan viruslaboratorion johtaja Luis Corrons.

- Ei ole ihme, että troijalaiset ja niiden jälkeen seuraavaksi yleisimmät mainosohjelmat ovat niin yleisiä, sillä molempia haittaohjelmatyyppejä käytetään paljon internetrikollisuudessa. Näillä haittaohjelmatyypeillä esimerkiksi kerätään käyttäjien tietoja, joita rikolliset myyvät edelleen. Muita haittaohjelmatyyppejä, kuten matoja, dialereita ja vakoiluohjelmia, havaittiin huomattavasti vähemmän.

Panda ActiveScanin keräämien tietojen mukaan yleisimpiä olivat (prosenttiluku kertoo osuuden kaikista löydetyistä haittaohjelmista):

Mato Sdbot.ftp 1,95%
Mato Puce.E 1,3%
Troijalainen Torpig.A 1,23%
Mato Brontok.H 1,21%
Troijalainen Abwiz.A 1,14%
Mato Bagle.HX 1,13%
Takaoviohjelma PcClient.DU 1,01%
Mato Netsky.P 0,95%
Troijalainen QQPass.JZ 0,94%
Troijalainen KillAV.FG 0,74%
Kansainvälinen virustilasto, vuoden 2007 ensimmäinen neljännes

Liite 5:

21.3.2007 14:31
OS X:lle on vasta 7 haittaohjelmaa
McAfee: Mac-käyttäjät ovat päässeet vähällä

Mac on toistaiseksi päässyt haittaohjelmissa paljon Windowsia vähemmällä.
Tällä hetkellä tunnetaan vain seitsemän haittaohjelmaa, jotka on tarkoitettu Applen Mac OS X -käyttöjärjestelmään, sanoo McAfeen Marius van Oers yhtiön blogissa.
Windows peittoaa Macin ainakin haittaohjelmien määrässä. Kaikkiaan haittaohjelmia tunnetaan Oersin mukaan yli 236 000, ja suurin osa niistä toimii Windows-ympäristössä

Vanhempiin Mac OS-versioihin tehtyjä haittaohjelmia McAfee tuntee vain 69.
Oers sanoo, että vaikka Mac OS X on toistaiseksi välttynyt haittaohjelmilta, tilanne saattaa muuttua, jos Applen käyttöjärjestelmä saavuttaa sille povatun viiden prosentin markkinaosuuden pöytäkoneista.

Haittaohjelmia tehdään yleensä kaikkein käytetyimpiin käyttöjärjestelmäympäristöihin, koska suuri käyttäjämäärä tarkoittaa laajempaa levitysalustaa.
Suuressa käyttäjäjoukossa on myös enemmän huonosti suojattuja tietokoneita ja tietämättömiä tai varomattomia käyttäjiä, joita haittaohjelma levittäjä voi käyttää hyväkseen.

Niinpä suurin osa haittaohjelmista on tarkoitettu Windowsiin, joka on edelleen käyttöjärjestelmistä ylivoimaisesti käytetyin.
Unixin ja Linuxin eri versioihin on Oersin mukaan tehty noin 700 haittaohjelmaa.

Antti Kirves

Liite 6.
Tutkimuskin osoittaa heikkojen salasanojen vaaran

Antti Kirves
Julkaistu 12.02.2007 kello: 08:07

Itsestään selvänä pidetty käsitys huonojen salasanojen vaarallisuudesta on saanut tuekseen tutkimustuloksia. Heikko salasana on helppo arvata.
Marylandin yliopiston tutkijat jättivät neljä heikoilla salasanoilla suojattua Linux-tietokonetta 24 vuorokaudeksi verkkoon.

Koneisiin yritettiin tunkeutua 270 000 kertaa eli kerran joka 39. sekunti. Hyökkääjät onnistuivat tunkeutumaan järjestelmiin heikkojen salasanojen turvin 825 kertaa.
Tutkijat keräsivät talteen salasanat, joilla hyökkääjät useimmin yrittivät päästä koneisiin.

Ylivoimaisesti yleisimmin käytetty sana oli "root", jota käytettiin runsaassa 12 prosentissa hyökkäyksistä. "Admin" oli seuraavaksi suosituin salasanatarjokas. Kolmanneksi useimmin hyökkääjät yrittivät sanaa "test" ja neljänneksi useimmin sanaa "guest".
Järjestelmiin päästyään hyökkääjät muun muassa selvittivät koneiden ohjelmistokokoonpanoja, latasivat tiedostoja ja muuttivat salasanoja.

Tutkimus osoitti heikkojen salasanojen helpottavan olennaisesti tietomurtojen tekemistä. Salasanoja parantamalla voidaan tutkijoiden mukaan olennaisesti parantaa tietoturvan tasoa.
Marylandin yliopisto suosittelee omissa ohjeissaan käyttämään vähintään kahdeksanmerkkisiä salasanoja, joissa on ainakin yksi iso ja yksi pieni kirjain mukana. Salasanat kehotetaan vaihtamaan puolen vuoden välein.