SUOMEN
DIAKONIA
OPISTO

Digilaitteiden tietoturvaopas

Aarno Hyvönen

verkkopedagogi, lehtori
Suomen Diakoniaopisto,
Lahden kampus
Etelä-Suomen aluehallintovirasto

Digitaalisen, kannustavan, virikkeellisen ja tukevan oppimisympäristön kehittäminen (DIGI-KAVIOT) –hanke

Osaava-ohjelma
Programmet Kunnig

www.sdo.fi

Digilaitteet eivät koskaan ole täydellisen turvallisia, vaikka kaikki tiedossa olevat asiat olisi huomioitu ja riskit ennakoitu. Laitteissa ja ohjelmissa on aina tietoturvaongelmia, joita ei vielä ole yleisessä tiedossa. Paraskaan tietoturva välttämättä takaa sitä, etteivät esim. omat yksityiset tiedot voisi jossain tilanteessa joutua vääriin käsiin tai tulla tuhotuiksi. Kannattaa koko ajan seurata tietoturvaan liittyvää julkista keskustelua ja tehdä voitavansa riskien minimoimiseksi. Päivittämätön digilaite on aina suuri riski, samoin liian helpot salasanat. Myös harkitsematon ohjelmien lataaminen tai linkkien seuraaminen voi laitteen saastumiseen tai yksityisten tietojen menetykseen. Seuraamalla julkista aiheeseen liittyvää keskustelua aktiivisesti voi välttää monia sudenkuoppia. Viestintäviraston ja tietokonelehtien sivuilta löytyy aina ajankohtaista keskustelua tietoturvaongelmista ja niihin liittyvistä ratkaisuista.

Suojautuminen tietomurroilta

Kaikki digitaaliset laitteet ovat haavoittuvaisia ja niihin voi kohdistua hyökkäyksiä. Ongelmat koskevat näin ollen yhtälailla kaikkia laiteita:

- tietokoneet ja tabletit
- älypuhelimet
- TV- ja digiboksi
- puettavat älylaitteet (kellot, sormukset jne.)
- kodinkoneita (jääkaapit, pesukoneet yms. siirtyvät pikkuhiljaa verkkoon),
- valvontakameroita, hälytyslaitteet
- autot

Krakkerit etsivät heikkoja kohtia kohdekoneiden tietoturvassa ja pyrkivät saamaan tietokoneita hallintaansa.

> *Krakkeri.* ***Krakkeri*** *tai* ***kräkkeri*** *(cracker; alkujaan englannin sanasta crack, murtaa) on henkilö, joka murtautuu tietojärjestelmään ilman järjestelmästä vastaavan tahon*

> *lupaa. Myös tietokoneohjelmien kopiosuojausten murtajaa kutsutaan krakkeriksi. Sanaa hakkeri käytetään usein mediassa sanan krakkeri tilalla.*
> *Vrt. Hakkeri. Sana hakkeri tarkoitti tietotekniikassa alun perin sellaista henkilöä, joka kykeni saavuttamaan tavoitteensa olemassa olevien järjestelmien rajoituksista huolimatta. Ratkaisut olivat toisinaan nopeasti tehtyjä ja hieman arveluttavia, mutta joskus myös nerokkaita. Näitä ratkaisuja kutsuttiin englanniksi termillä hack (puhekielessä purkkaratkaisu) ja niiden tekijöitä hakkereiksi (hacker). (Wikipedia)*

Eräässä tapauksessa krakkerit onnistuivat ohjaamaan etäältä auton ilmastointia, radiota ja tuulilasinpyyhkijöitä, toisessa tapauksessa internetyhteydessä olevaa autoa onnistuttiin ohjaamaan verkon kautta. Ongelma korjattiin autovalmistajan toimesta. Itsestään kulkevat autot tulevat olemaan varmasti erittäin haluttu kohde krakkereille. Valitettavasti krakkerit ovat usein laitevalmistajia askeleen edellä.

Valvontakamerat ovat krakkereiden suosiossa. Laitteissa ei aina jakseta muuttaa oletussalasanoja ja paneutua kunnolla muihin tietoturva-asetuksiin. Netissä on sivuja jonne on koottu näitä vapaasti katsottavia valvontakameroita. Laitteiden luonne muuttuu kun niitä voi katsoa kuka tahansa: laitteiden avulla varkaat voivat seurata onko omistajat paikalla ja onko mitään varastettavaa.

LG jäi kiinni luvattomasta tiedon tallentamisesta TV:n mikrofonin kautta. Puheohjattu laite kuuntelee käynnissä ollessaan ympäristön ääniä. Laite lähetti tietoja LG:n palvelimelle. TV:seen voidaan myös murtautua ja saada kuunteluyhteys kohteeseen.

Vuonna 2015 lasten itkuhälyttimiä tutkinut amerikkalainen tietoturvayhtiö osoitti, että niissä on vakavia tietoturvaongelmia, joiden hyväksikäyttämällä krakkeri voi kuunnella tai jopa katsella mitä kodissasi tapahtuu. Itkuhälyttimen kautta krakkeri voi päästä käsiksi jopa kodin tietoverkkoon ja siellä oleviin asiakirjoihin ja kuviin. Tämä tyyppiset ongelmat tulevat yleistymään kun esineiden internet laajenee ja yleistyy päivä päivältä.

> ***Esineiden internet.*** *Gartnerin määritelmän mukaan teollisessa internetissä on kyse fyysisistä laitteista, jotka pystyvät aistimaan ympäristöään ja viestimään tai toimimaan aistimansa perusteella älykkäästi.(Wikipedia)*

Tietokoneisiin (ja muihin digilaitteisiin) voidaan tunkeutua ja etäkäyttää sitä haluamallaan tavalla. Tietokoneen tai puhelimen kameraa voidaan katsoa, tiedostoja voidaan kopioida tai jopa levittää internetissä. Laitteita voidaan käyttää myös muihin rikollisiin tarkoituksiin, kuten valjastaa ne jonkun palvelun estohyökkäyksiin. Palvelunestohyökkäyksissä käytetään usein hyväksi jotakin haittaohjelmaa, joka automatisoi laitteiden kytkemisen. Eli hyökkääjän ei tarvitse tehdä mitään, riittää kun uhri käy väärällä sivulla suojaamattomalla koneella. Krakkereilla on käytössään taitavampien krakkereiden tekemiä valmiita ohjelmia, joilla suojaamattoman tietokoneen käyttöönotto onnistuu ilman suurempaa osaamista. Ohjelmia voi ladata ilmaiseksi tai pientä maksua vastaan internetistä.

Ohjelmistopäivitykset

Ensimmäinen asia suojautumisessa tietomurtoja vastaan on koneiden ja laitteiden päivitykset. Kaikkiin digilaitteisiin tulee yleensä tietoturvapäivityksiä. Nämä päivitykset kannattaa ladata viipymättä, sillä niissä on usein korjattu tietoturva-aukkoja. Krakkereiden ohjelmat toimivat vain suojaamattomissa koneissa. Valitettavasti ihmiset eivätkä tee tietoturvapäivityksiä heti vaan siirtävät päivitystä tuonnemmaksi, toisinaan ikävin seurauksin. On mahdollista, että tulee osallistuneeksi palvelunestohyökkäykseen täysin tietämättään ja vain siksi ettei ole päivittänyt konettaan ajoissa.

Tietokoneessa (Pc, Apple, Linux) *varusohjelmien* järjestelmäpäivitykset tulevat yleensä automaattisesti, mutta käyttäjän on yleensä hyväksyttävä päivityksen vastaanotto. Järjestelmään asennut työvälineohjelmat eivät kuitenkaan päivity automaatteisesti kuten, selaimet (Firefox, Chrome…), selaimien lisäosat (Flash, Java, Pdf-lukija), siksi krakkereiden ohjelmat hyödyntävät useimmiten juuri lisäosien aukkoja. Monissa ohjelmissa päivitykset tarkistetaan ohje-valikon kautta (Firefox, Adobe Reader). Javan voi tarkistaa esim. ohjauspaneelin kautta. Myös jotkut virustorjuntaohjelmat varottavat vanhentuneista ohjelmista (mm. Avast ja Norton). Java kannattaa poistaa jos sitä ei tarvita, koska se on usein haavoittuva. Aina siihen aina ole olemaakaan päivitystä, vaikka virhe on jo tiedossa ja hyväksikäyttömenetelmä on jo kehitetty. Tätä kutsutaan nollapäivähaavoittuvuudeksi.

Varusohjelma *on tietokoneohjelma, joka mahdollistaa laitteen käytön ja on usein asennettu siihen valmiiksi. Varusohjelmia ovat laitteen alkulatausohjelmat (esimerkiksi bios) ja käyttöjärjestelmä.*

Työvälineohjelmat *ovat taas vapaamuotoisempia ohjelmia, joilla työtehtävä ei ole ennalta määrätty. Tällaisia ohjelmia ovat mm. tekstinkäsittely, taulukkolaskenta, julkaisuohjelmat, grafiikkaohjelmat, CAD-suunnitteluohjelmat, kortisto-ohjelmat, tietokantaohjelmat ja internet selainohjelmat. Lisätietoa.*

Nollapäivähaavoittuvuus *(engl. zero-day vulnerability/attack/threat, 0-day) tarkoittaa tietoturva-aukkoa, jolle ei ole olemassa korjausta, mutta haavoittuvuudelle on olemassa hyväksikäyttömenetelmä. Nollapäivän aukko syntyy, kun joko tietoturva-aukon löytäjä julkaisee tiedot samalla kun ilmoittaa aukosta ohjelman kehittäjille, ei ilmoita siitä ollenkaan, tai kun tietoturva-aukkoa ei paikata ilmoituksesta huolimatta. (Wikipedia)*

Asiallinen virustorjunta

Virustorjuntaohjelma on tietokoneissa välttämätön, tableteissa ja puhelimissa suositeltava varuste. Windows käyttöjärjestelmässä on Windows 8 versiosta alkaen ollut mukana sisäänrakennettu virustorjuntaohjelma. Sen antama turva on kuitenkin verraten huono. Esim. vuonna 2015 AV-TESTin suorittamassa tietoturvatestissä se sai 0 pistettä. Maksulliset virustorjuntaohjelmat tunnistavat hyvin myös haittaohjelmat. Parhaita maksullisia virustorjujia ovat mm.: Norton, Bitdefenderr, McAfee, Kaspersky ja F-secure. Mac-käyttöjärjestelmässä on vähemmän haittaohjelmia kuin Windowsissa, silti siinäkin on nykyisin syytä olla virustorjuntaohjelma. Suosion noustua myös haittaohjelmia on ilmaantunut. Linux-järjestelmissä on mahdollista toimia ilman reaaliaikaista virustorjuntaa. Haittaohjelmia on vähän ja järjestelmä on luonnostaan turvallisempi. Puhelimissa ja tableteissa on tietokoneita hieman pienempi riski saada haittaohjelmia, varsinkaan jos ei itse asenna siihen ohjelmia. Android-järjestelmissä on suurempi riski saada haittaohjelmia, koska GooglePlay-kauppan sovelluksia ei testata ennakkoon ja siellä on aika ajoin ollut kaikkien ladattavissa haittaohjelmia sisältäviä ohjelmia. Ohjelmia mobiililaitteisiin ei pidä ladata muualta kuin virallisista lähteistä. Myös mo-

biililaitteissa olisi hyvä olla vähintään ilmainen virustorjunta asennettuna. Andoid puhelimiin saattaa ilmestyä myös mainoksia, jotka ilmoittavat koneen olevan saastunut ja pyytää asentamaan virustorjuntaohjelman. Eräs kiinalainen virustorjuntayritys markkinoi tuotteitaan tällaisella kyseenalaisella tavalla. Eli ei kannata heti uskoa, jos tällainen ilmoitus ruudulle ilmestyy. Vastaavia löytyy myös Windows-tietokoneisiin.

Palomuuri

Palomuurit ovat joko ohjelmistolla tai laitteistolla toteutettuja järjestelmiä, jotka suojaavat esimerkiksi yrityksen sisäverkkoa ulkoverkosta tulevilta hyökkäyksiltä. Palomuurin toiminnan perusedellytyksenä on, että kaikki verkkoliikenne sisä- ja ulkoverkon välillä kulkee sen läpi ja että palomuuri päästää lävitseen vain halutun kaltaisen verkkoliikenteen. Nykyisissä tietokoneissa on sisäänrakennettu ohjelmapalomuuri. Myös laajakaistamodeemeissa on sisäänrakennettu palomuuri, joka suojaa verkkoyhteyttä.

Windows-tietokoneiden erilaiset tilit ja oikeudet

Monet käyttävät Windows-tietokoneita pääkäyttäjäoikeuksilla ja jopa ilman salasanaa. Tällöin käyttäjä antaa haittaohjelmille ja krakkereille melko vapaat kädet toimia. Käyttöjärjestelmään tehtävä suuretkaan muutokset eivät silloin vaadi salasanan antamista. Windows-tietokoneissa kannattaa käyttää järjestelmää tavallisen käyttäjän oikeuksilla. Koneeseen luodaan vähintään kaksi tiliä, joista toinen on tavallinen käyttäjä ja toinen järjestelmän valvoja. Konetta käytetään tavallisen käyttäjän tilillä, jolloin ei voida vahingossa tai haittaohjelman toimesta asentaa koneeseen mitään tarpeetonta. Kun koneeseen asennetaan jotakin, kysyy ohjelma aina pääkäyttäjän salasanaa. Tavalliselle käyttäjälle ei tällöin ole pakko laittaa salasanaa lainkaan. Järjestelmän valvojalle salasana kannattaa sen si-jaan aina asettaa. Macissa, Androissa ja Linuxissa ei normaalisti käyttäjällä ole täysiä oikeuksia levylle

kirjoittamiseen ja lukemiseen. Oikeuksia on rajoitettu ja siksi järjestelmät ovat turvallisempia. Erityisillä toimilla erikoisoikeudet (root-oikeudet) on kuitenkin otettavissa käyttöön. Esim. Android-puhelimissa puhutaan ”roottaamisesta”, kun puhelimen oikeudet otetaan käyttöön. Tällöin puhelimeen voidaan asentaa toinen käyttöjärjestelmä ja ohjelmia jotka eivät toimi normaalioikeuksilla toimivassa puhelimessa. Puhelimen käyttöehdot kieltävät ”roottaamisen” ja se ”roottauksen” jälkeen puhelimen takuu ei ole enää voimassa. Puhelimen turvallinen käyttö tämän jälkeen vaatii paljon normaalia enemmän tietoa ja osaamista.

Riittävän vaikeat salasanat Salasanoihin täytyisi jokaisen kiinnittää erityistä huomiota. Mukavuuden halu ja ajanpuute johtavat helposti liian helppoihin salasanoihin. Ongelmallista on käyttää samoja salasanoja useissa palveluissa. ”Ei minulla ole mitään salaisuuksia – siksi asia ei koske minua. Ihan sama vaikka joku kävisi katsomassa tiliäni”. Näin moni perustelee helppoa salasanaansa. Miksi tämä väite on ongelmallinen:

- monet sähköpostitilit sisältävät sähköpostin ohella muista pilvipalveluja, joten samalla salasanalla voi päästä käsiksi myös pilvessä oleviin kuviin ja tiedostoihin
- identiteettivarkaudet ovat tätä päivää– esiinnytään toisen henkilön nimellä ja tilataan tuotteita toisen laskuun tai vaikkapa kirjoitetaan tai julkaistaan jotakin toisen nimissä
- sähköpostitunnuksen avulla toinen henkilö voi vaikkapa siirtää virustorjuntaohjelmasi omaan koneeseensa tai vaikkapa peruuttaa tekemäsi tuotetilauksen
- joku voi vaikkapa julkaista sosiaalisessa mediassa asiattomuuksia sinun nimissäsi. Mahdollisuuksia on todella paljon, mihin toisen sähköpostitiliä voi käyttää. Mustassa pörssissä sähköpostitileillä tehdään kauppaa ja jossain vaiheessa esim.Gmail-tilin hinta oli 6€/kpl. Krakkerit murtavat jatkuvasti palveluja ja käyttäjien salasanat valuvat vääriin käsiin. Jos käyttäjällä on sama salasana kaikissa palveluissa, tilanne pahenee entisestään. Salasana pitää siis olla riittävän vaikea ja se pitää olla erilainen eri palveluissa ja lisäksi sitä pitäisi vaihtaa säännöllisesti, mutta vielä tärkeämpää on pitää jokaiselle palvelulle erilaiset salasanat. Joillakin palvelimilla on päällä pakotettu salasanan vaihto määräajoin. Ihmisen mukavuudenhalusta, kiireestä yms. johtuen salasanoja ei uusimistilanteissa harkita riittävän huolellisesti ja seurauksena voi olla entistä huonompi tietoturva. Palveluissa, joissa voidaan käyttää kaksivaiheista tunnistautumista, kannattaa tämä mahdollisuus hyödyntää. Tällöin palveluun pääsee kirjatumaan vieraalla koneella vasta kun on kirjoittanut puhelimeen tekstiviestinä tulleen koodin. Tutulla koneella koodia ei vaadita. Kaksivaiheisen tunnistautumisen käyttöönotto:

- **Google-tili:** https://support.google.com/accounts/answer/185839?hl=fi
- **Microsoft-tili:** https://support.microsoft.com/fi-fi/instantanswers/80aef08c-0574-46be-92a3-31f3b04060fd/turning-two-step-verification-on-or-off-for-your-microsoft-account
- **Facebook:** Klikkaa kolmiota yläpalkissa-käyttäjätilin asetukset-Turvallisuus-Vaadi turvakoodia käyttäjätilini käyttämiseen tuntemattomasta selaimesta.

Keinoaja vaikean salasanan tekemiseen

- Laulunsanat, ”Maan korvessa kulkevi lapsosen tie …. ”MkKLst”)8
- Lisäksi on hyvä lisätä salasanaan erikoismerkkejä, kuten tässä 8 ja sulku ja isoja ja pieniä kirjaimia.
- Kirjaimet muodostavat kuvioita tai hahmoja.
- ”(*--o@ö-*)” ”Possu”
- !([*]—U—[*])! ”Naisella tähtisilmät ja korvakorut”
- Näitä kuvioita voi vaikka lisätä oman helpon salasan perään tai loppuun.
- PIN-koodi-salasanat. Muodostetaan yksi vaikea vaikkapa viiden merkin salasana, jota käytetään runkona muille salasanoille.
- Esim. runko=PIN: 5aA@)
  - Gmail: G5**5aA@)**7776Yy
  - Outlook: 08**5aA**@)836Vi
- PIN-koodiin lisätyt merkit voidaan kirjoittaa paperille tai vaikkapa puhelimeen muistiin. Huom! koko salasanaa ei pidä kirjoittaa sähköisesti muistiin minnekään.
- Käytä salasanalauseita. Edut: salasanoista tulee riittävän pitkiä ja helposti muistettavia.
- Lehmä@ammui(*-*)Ja_aivasti2* (Lehmä ammui ja aivasti kaksi kertaa)
- Ki@@a_söi~hiiren&katui-sitä (Kissa söi hiren ja katui sitä)
- Näissä olisi hyvä käyttää lisäksi vaikka kertomukseen sopivia kuvia.

Kodin internet-yhteyden turvallisuus

Kotikoneissa ongelmana ovat laajakaistamodeemit, joiden kautta tietokoneet muodostavat yhteyden internettiin joko langattomasti (WLAN) tai Ethernet-kaapelilla. Modeemi kytketään verkkoon sen enempää tietoturva-kysymyksiä pohtimatta. Oletusasetuksilla yhteyden muodostaminen ei välttämättä ole turvallinen. Laajakaistamodeemissa tulisikin huomioida ainakin seuraavat asiat:

- modeemien ohjelmistopäivitykset. Operaattori saattaa hoitaa modeemien päivitykset myös automaattisesti. Asia kannattaa varmistaa operaattorilta.
- modeemien päähallintaohjelmien salasanat, jotka pitäisi aina vaihtaa ennen modeemin käyttöönottoa.
- modeemissa voi olla päällä asetus, joka mahdollistaa modeemin hallintapaneelin asetusten säädön etäyhteydellä. Se kannattaa kytkeä pois päältä.
- Modeemin WLAN-tukiaseman langattoman verkon salasana kannattaa vaihtaa ennen modeemin käyttöönottoa. Nykyaikaiset modeemit käyttävät WLAN-salaukseen WPA2-protokollaa, joka on kohtuullisen turvallinen. Joissakin vanhemmissa modeemeissa saattaa vielä olla turvaton WEP-salaus. Yleensä modeemeissa on valmiiksi laitettu salaus päälle ja salasana on kirjoitettuna laitteen pohjaan. Joissakin vanhemmissa laitteissa voi kuitenkin olla, ettei suojausta ole lainkaan päällä. Silloin kuka vain voi kytkeytyä kotiverkkoosi.
- Tätä ohjetta kirjoitettaessa on parhaillaan menossa (29.11.2016) palveluestohyökkäys joka perustuu modeemeissa oleviin haavoittuvuuksiin. Mirai-haittaohjelma on erikoistunut verkkoon kytkettyjen laitteiden saastuttamiseen. Ennen viikonloppua saastuneita koneita tiedettiin olevan satoja ja viikonlopun jälkeen niitä oli jo 16000. Viestintävirasto suosittelee, että operaattorit suodattaisivat portin 7547 portin liikennettä, koska tämän portin haavoittuvuuden hyödyntämisestä on kyse. Tavallista internetin käyttäjää suositellaan päivittämään modeeminsa ohjelmat ja vaihtamaan hallintapaneelin salasana. Hallintapaneelin kautta voi myös kytkeä pois palveluja, joita ei tarvita. Esim. hallintapaneelin asetuksiin tulee päästä vain sisäverkon kautta, ei suoraan internetistä. Lisätietoa viestintäviraston sivuilla: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2016/11/ttn201611291741.html

Hotellien, lentokenttien yms. tietoturvakysymykset

Hotelleissa ja julkisissa tiloissa on usein tarjolla ilmaiseksi tai maksua vastaan langattomia Wlan-yhteyksiä. Yhteydet eivät aina ole mitenkään suojattuja, jolloin kuka tahansa voi kytkeytyä verkkoon. Tällöin sivulliset voivat helposti kuunnella ja tallentaa kaiken mitä verkossa tapahtuu. Vältä siis yhteyksiä, joita ei ole salattu. Avoimen yhteyden voi helposti pystyttää kuka tahansa, mikä mahdollistaa myös huijaukset. Huijari-verkossa saatetaan vaatia luottokorttitietojen esittämistä ennen verkon käyttöä, jolloin tiedot luottotiedot menetetään. Hotelleissa ja muissa julkisissa paikoissa huijariverkkojen nimet saattavat olla hyvin oikealta kuulostavia eli niissä voi esiintyä esim. hotellin nimi tms. Vaikka yhteys olisi suojattu, ei yhteys tukiasemasta eteenpäin aina ole suojattua. Eli riippuen siitä käyttääkö sivusto SSL-salausta vai ei, esim. pankkipalvelut ja monet sähköpostipalvelut ovat SSL-suojattuja, mutta kaikki palvelut eivät sitä ole. Silloin liikennettä voidaan seurata ja krakkerit voivat esim. urkkia käyttäjien salasanoja ja käyttäjätunnuksia. Tunnistat SSL-suojatun palvelun lukon kuvasta osoiterivillä. VPN-yhteyden avulla voidaan suojata yhteys tehokkaasti. Tätä tekniikkaa käytetään mm. yritysten työntekijöiden etäyhteyksiin. VPN-yhteyden voi hankkia voi hankkia tietokoneeseen tai mobiililaiteeseen, jolloin kaikki liikenne salataan koko istunnon ajalta. Yhteys hidastuu tästä jonkin verran. Esim. suomalainen tietoturvatoimittaja F-secure myy Freedom-ohjelmaa tähän tarkoitukseen. Myös ilmaisia ohjelmia on tarjolla, mutta niiden turva ei ole aivan yhtä hyvä. Esim. Opera tarjoaa ilmaista VPN-yhteyttä Android ja Iphone –laitteille. Googlen Nexus –puhelimissa VPN on valmiina asennettuna. Ongelmana ilmaisissa palveluissa on se, että ne luultavasti keräävät omiin tarkoituksiinsa tietoa. VPN-yhteyksiä on käytetty myös hyväksi myös kun on haluttu kiertää palvelutarjoajien alueellisia rajoituksia. Eräät sivustot toimivat ainoastaan oman maan sisällä. Kun liikenne kierrätetään tietyn palvelimen kautta ja peitetään käyttäjän todellinen sijainti, on voitu käyttää palvelua, joka muuten olisi estetty ulkomailta käsin. Esim. Netflix:n Yhdysvaltojen tarjoama videovalikoima on houkutellut väärinkäytöksiin. Netflix on kuitenkin omilla toimillaan vaikeuttanut tätä toimintaa. Myös toisinajattelijat ovat käyttäneet tekniik-

kaa kotimaansa sen-suurin kiertämiseen. Toinen tekniikka, jota käytetään henkilöiden anonymiteetin suojelemiseen VPN:n rinnalla on Tor (The Onion Router). Lisätietoa: https://fi.wikipedia.org/wiki/Tor_(verkko). Verkkoa käytettään sekä laillisiin, että laittomiin tarkoitusperiin. Osa käyttäjistä haluaa vain suojat internettoimintansa mainostajilta ja verkkovakoojilta; toisaalta tekniikkaa käytetään myös rikollisiin tarkoitusperiin, kuten lapsipornon levitykseen ja huumeiden välitykseen. Tekniikkaa hyödyntää mm. Mozilla Firefox ESR-selain.

Ponnahdusikkuna ja ilmaisohjelmat

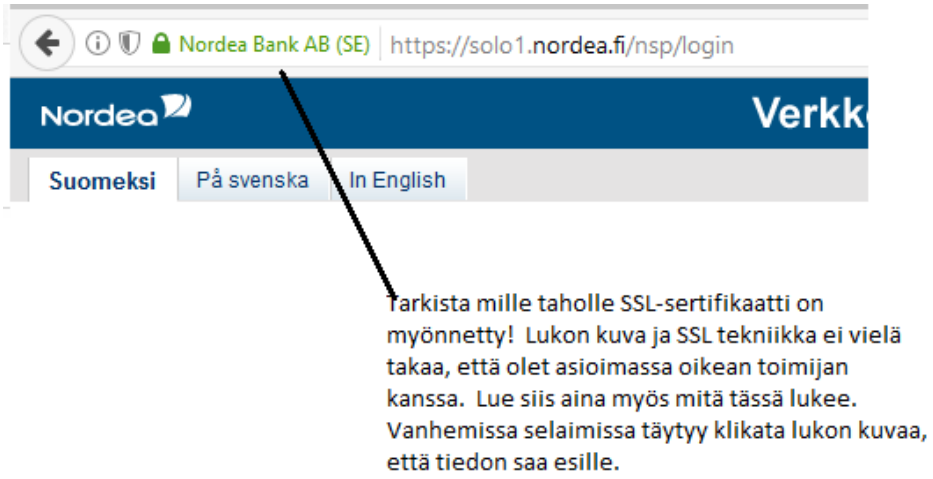
Vältä ilmaisohjelmia ja ponnahdusikkunoiden klikkailua monien ilmaisohjelmien kylkiäisisinä tulee usein monenlaisia haittaohjelmia. Asennettaessa ilmaisohjelmia, lue asennuksen yhteydessä tulee lukea huolellisesti kaikki asennusvaiheet läpi ja ruksaa pois mahdolliset ”lisukkeet”. Joskus täytyy myös edetä ”kustomoitu/edistystynyt” asennusta myöten, jotta voi estää epätoivotut ohjelmistot. Monet haittaohjelmat leviävät ponnahdusikkunoiden kautta, joissa varoitetaan koneen suorituskyky ja tietoturva-ongelmista ja joihin luvataan ratkaisua. Näitä linkkejä ei kannata mennä klikkaamaan. Ilmaisohjelmia voi ladata hieman turvallisemmin Ninite-sivuilta. He lupaavat sivuillaan, että ovat poistaneet ladattavista ohjelmista ylimääräiset lisäkkeet. Lisäksi ohjelmien lataus on sivustolta äärimmäisen helppoa: ruksaat mitä haluat ja asennat kaikki ohjelmat samalla kertaa. Palvelu löytyy osoitteesta: www.ninite.com. Pop-up -ikkunoiden ilmestymistä voi vähentää mainosohjelmien esto -ohjelmilla, joita voi asentaa selaimen lisäosina. Mm.Adblockplus-ohjelma estää melko tehokkaasti mainosikkunoiden avautumista. https://ad-blockplus.org/ Toisaalta nämä ohjelmat päästävät rahasta läpi valikoiden tahojen mainoksia. Täytyyhän heidänkin jotain hyötyä kehittämästään ilmaisohjelmasta!

Internet-selaimen välimuistin tyhjennys ja inconitotilan käyttö

Internet-selaimen välimuistin tyhjennys vaikeuttaa tiedonurkkijoiden työtä jossain määrin. Siksi olisi hyvä tyhjentää säännöllisesti selaimen välimuisti. Tietokoneen kiintolevyille tallentuvat automaattisesti tekstit, kuvat ja sivut joilla olla käyty. Tallentaminen on perusteltua, koska se sujuvoittaa sivujen latautumista ja mm. kaikkea sisältöä ei aina tarvitse hake palvelimelta asti vaan osa voidaan ladata vanhasta muistista omalta koneelta. Jotkut verkkokaupat lukevat välimuistissa olevia tietoja ja jopa nostavat hintaa, jos käyttäjä on käynyt lähiaikoina samalla sivulla. Logiikkana on se, että käyttäjä joka palaa sivulle on mahdollisesti jo tehnyt ostopäätöksen eikä ehkä huomaa pientä muutosta hinnassa. Kaikissa selaimissa voit käynnistää välimuistin tyhjennyksen näppäinyhdistelmällä ctrl+vaihto (shitf)+ del. Välimuistin tallentamisen voi myös estää lukemalla internet-sivuja privat-tilassa. Edge-selaimessa sitä kutsutaan inPrivate-ikkunaksi, Chromessa incognito ja Firefoxissa yksityiseksi ikkunaksi. Täydellisesti ei urkinnalta kuitenkaan voida suojautua, koska uusia tekniikoita tiedon keräämiseen kehitetään jatkuvasti eivätkä kaikki haavoittuvuudet ole koskaan yleisessä tiedossa.

Turvalliset nettiostokset

Nettiostoksissa kannattaa hyödyntää hintavertailua suorittavia sivustoja, mutta ennen kaupankäyntiä kannattaa huolellisesti tutustua liikkeen toimintaperiaatteisiin ja saamiin asiakaspalautteisiin. Hintojen lisäksi kannattaa vertailla myös asiakaspalvelun laatua, toimitusaikaa ja luotettavuutta. Ennen kaupankäyntiä kanttaa selvittää ainakin seuraavat asiat:



Kuva 1. SSL-salaus

- Tarkista että yhteys on suojattu, lukon kuva osoiterivillä. Tarkista myös, että SSL on myönnetty kyseessä olevalle yritykselle (kuva 1. SSL-salaus)
- Selvitä ennen kaupankäyntiä kauppiaan yhteystiedot, tilaus- ja toimitusehdot ja tiedot tullimaksuista.
- Tee hakuja kauppiaasta hakukoneella esim. kauppiaan nimi ja ongelmat (problems)
- Luottokortilla maksaminen turvallisempaa, koska luottokunta yleensä korvaa jos tuotetta jos tuote ei syystä tai toisesta toimitetakaan
- Jos et halua antaa luottokorttitietoja monille kauppiaalle, harkitse PayPal-tilin avaamista.

Turvallinen puhelimen käyttö

Puhelimeen säilötään tänä päivänä paljon henkilökohtaista tietoa ja sitä käytetään myös maksuvälineenä. Siksi laitteen tietoturvaan tulee kiinnittää erityistä huomiota.

- Käytä puhelimen suojakoodia (numero, kuvio, sormenjälkitunnistus)

- Suojaa PIN-kortti turvallisella suojakoodilla
- Käytä automaattista lukitusta
- Päivitä ohjelmat säännöllisesti
- Lataa ohjelmia vain virallisesta sovelluskaupasta, älä esim. suoraan nettisivuilta.
- Harkitse tarkkaan mitä oikeuksia annat sovelluksen käyttää. Ohjelma kysyy asennuksen aikana tätä. Jos esim. uutisten katseluohjelma haluaa oikeuden päästä käsiksi osoitekirjaasi, voi miettiä kuinka turvallinen ohjelma on. Kaikkia oikeuksia ohjelmille ei tarvitse antaa. Toisaalta voi olla, ettei ohjelma toimi oikein, jos oikeuksia rajataan liikaa
- Jos puhelin katoaa, muista vaihtaa salasana kaikkiin palveluihin. Joissakin puhelimissa voit etähallinta puhelinta esim. tyhjentää sen muistin ja estää sen käytön. Kadonnut laite kannattaa myös poistaa pilvipalvelun laitelistalta, jottei pilvipalvelun tietoihin päästä käsiksi. Puhelimissa voi olla myös automaattisia suojauksia, jotka huomaavat epäilyttävän käytön ja vaativat tunnistautumista jos puhelin siirtyy maasta toiseen. Puhelimen tietosuoja ominaisuuksiin kannatta tutustua hyvin jo ennakolta ja ottaa haluamansa suojaukset käyttöön.
- Jos myyt puhelimen:
    - poista laite pilvipalvelun laitelistalta
    - tyhjennä puhelimen muisti ja muistikortti. Poiston jälkeen tiedot eivät poistu vielä pysyvästi ja ne on vielä palautettavissa erityisillä ohjelmilla. Esim. CCleanerin tyhjennä vapaa levytila -toimintoa voi käyttää myös puhelimen tallennusvälineen tietojen lopulliseen poistoon.
    - Erillinen muistikortti kannattaa ottaa puhelimesta talteen
    - Palauta lopuksi puhelin tehdasasetuksiin.
    - Jos ostat käytetyn puhelimen, tee aina tehdasasetuspalautus ennen käyttöönottoa ja varmista ettei puhelin ole liitetty mihinkään pilvipalveluun.
    - Myös mobiililitteisiin voi tulla haittaohjelmia. Haittaohjelma voi ilmetä hidasteluna, akun nopeampana kulumisena, laitteen jumiutumisena, epätavallisen runsaana nettiliikenteenä ja ylimääräisinä mainoksina. Puhelin saattaa alkaa

lähetellä myös viestejä osoitekirjassa oleville henkilöille tai maksullisiin palvelunumeroihin. Tarkkaile nettiliikennettä puhelimen asetuksista ja seuraa myös puhelinlaskusi erittelyjä

  - Palauta puhelin tehdasasetuksiin. Ohjeita löydät puhelimen valmistajan tukisivuilta ja internetistä miten tämä tehdään
  - Vaihda kaikkien palvelujen salasanat.

- Poista ylimääräiset langattomat yhteydet
  - Käytä vain niitä langattomia yhteyksiä joita oikeasti tarvitset. Esim. jos et käytä Bluetooth tai Wlania, kytke ne pois päältä. Säästä sähköä ja lisäksi vähennät riskiä tietomurtojen osalta.
- Puhelimen päivitysten lakkaaminen: Laitevalmistaja lopettaa uusien järjestelmäpäivitysten jakamisen laitteille jossain vaiheessa. Silloin kannattaa harkita puhelimen vaihtoa. Halvemmissa puhelimissa tämä voi tapahtua aika nopeastikin. Uusissa järjestelmäversioissa korjattuja tietoturva-aukkoja ei välttämättä korjata enää lainkaan vanhempiin puhelimiin. (Viestintäviraston www-sivut)

Lähteet

Mikrobitti lehti: http://www.mikrobitti.fi/

Tivi: http://www.tivi.fi/

Viestintävirasto: https://www.viestintavirasto.fi/

Wikipedia: https://fi/wikipedia.org/

Lisätietolinkkejä

https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Tietoturvavinkkeja_matkapu-heli-men_turvalliseen_kayttoon.pdf

http://yle.fi/uutiset/3-8277513_(itkuhälyyttimet)

https://www.viestintavirasto.fi/kyberturvallisuus/laitteenturvallinen-kaytto/adsl-mo-deemi.html