TIETOTURVA

Enterin suositukset eri laiteympäristöille

Suositukset ovat laatineet ENTER ry:n vertaisopastajat

Esa Martonen, Veli Kahrala, Jukka Hanhinen, René Tigerstedt

Maaliskuu 2020

Lähteenä on käytetty mm. Kyberturvallisuuskeskuksen oppaita.

enter
Ikäihmisten
tietotekniikkayhdistys

TUETTU VEIKKAUKSEN TUOTOILLA

Sisällysluettelo

1. Yksityishenkilöiden tietoturvauhat

Viestintäviraston mukaan yksityishenkilöiden suurimmat uhat ovat herkkäuskoisuus, kiristyshaittaohjelmat, heikot salasanat, älylaitteiden ailahteleva tietoturva ja yksityisyys. Suojautumisessakin tutut kotikonstit ovat paikallaan: hillitse klikkailuja, päivitä, varmuuskopioi, käytä laadukkaita salasanoja ja tietoturvaohjelmistoja.

Kuva 1. Viestintävirasto: Yksityishenkilöiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017

Nettiyhteydellä varustettu älypuhelin (ja tabletti) on tietokone, johon tallennetaan paljon henkilökohtaista tietoa ja siten siihen kohdistuu samat uhat kuin tietokoneisiin. Puhelin vielä kulkee aina käyttäjänsä mukana. Tyypillisesti puhelin ja tabletti ovat kirjautuneena aina kaikkiin käytössä oleviin palveluihin (Gmail, WhatsApp jne). Sillä toimitetaan myös pankkiasioita, käytetään viestintään ja selataan terveystietoja. Tämän vuoksi laitteen suojaaminen on erittäin tärkeää. Puhelin kulkee aina omistajan mukana ja voi helposti kadota.

Kyberturvallisuuskeskuksen sivustolta (https://kyberturvallisuuskeskus.fi) löytyy ajankohtaista tieto turvallisesta verkkokäyttäytymisestä.

Seuraavaksi hieman tarkemmin alusta kerrallaan miten ratkaisut otetaan käyttöön.

2. Älypuhelinten ja tablettien tietoturva

Nettiyhteydellä varustettu älypuhelin (ja tabletti) on tietokone, johon tallennetaan paljon henkilökohtaista tietoa. Tyypillisesti puhelin ja tabletti on kirjautuneena aina kaikkiin käytössä oleviin palveluihin (Gmail, WhatsApp jne). Sillä toimitetaan myös pankkiasioita, käytetään viestintään ja selataan terveystietoja. Tämän vuoksi laitteen suojaaminen on erittäin tärkeää. Puhelin kulkee aina omistajan mukana ja voi helposti kadota.

2.1. Vaihda SIM-kortin PIN-koodi

Operaattorien SIM-korttien oletusarvoiset PIN-koodit ovat joko 0000 tai 1234. Eri laitteissa PIN-koodin vaihto löytyy yleensä tietoturva-asetuksista. Suositus on, että SIM-kortille annetaan sama PIN-koodi kuin näytön lukitukseen. Tällöin ei synny sekaannusta puhelimen käynnistyksen yhteydessä. Virtahan katkaistaan laitteesta todella harvoin ja on aika ikävää kun SIM-kortin PIN-koodia ei muista esim. matkoilla - kolme väärää yritystä ja puhelin on lukossa.

2.2. Ota käyttöön näytön lukituskoodi

Näytön lukitus on erittäin tärkeä asia - jopa tärkeämpi kuin SIM-kortin PIN-koodi. Näyttöasetuksista säädetään minuuttimäärä, jonka jälkeen näyttö menee lukkoon. Aika lasketaan näytön viimeisimmästä kosketuksesta. Suositus on 2 minuuttia, enintään 5 minuuttia. Tällöin mahdollisessa puhelimen katoamistilanteessa laitteen löytäjällä on keskimäärin 1 minuutti aikaa aloittaa laitteen käyttö. Mitä lyhyemmäksi näytön lukitusaika säädetään sitä turvallisempi puhelin on, mutta vastaavasti sitä ikävämpi käyttää. Monissa puhelimissa oletusarvo on 30 sekuntia.

Lukitus voidaan laitteesta riippuen tehdä numerokoodilla, (salasanalla), numeronäppäimistölle piirrettävällä kuviolla tai sormenjäljellä. Jos laitteessa on mahdollisuus käyttää sormenjälkitunnistusta, niin se erittäin suositeltava, kätevä ja turvallinen tapa. Numerokoodia käytettäessä kannattaa käyttää samaa koodia kuin mikä on asetettu SIM-kortin PIN-koodiksi.

2.3. Lataa ja asenna kaikki tarjotut järjestelmäpäivitykset

Tarkasta laitteen asetuksista, että automaattiset päivitykset ovat päällä. Monissa puhelimissa on oletusarvoisesti asetus, että päivitykset tapahtuvat vain Wifi-verkossa (tämä asetus on päällä käytännössä kaikissa puhelimissa). Jos henkilöllä ei ole kotona Wifi-verkkoa, järjestelmä ei päivity mahdollisesti koskaan. Suomessa käytössä olevat mobiililiittymät sisältävät yleensä rajattoman data, joten asetus on syytä muuttaa sellaiseksi, että päivitykset tapahtuvat myös mobiiliverkossa.

2.4. Käytä vain tuettuja Android- tai iOS-versioita

Vanhin tuettu Android-versio on tällä hetkellä (3/2020) 7.0 Nougat. Kaikki 6-alkuiset tai sitä vanhemmat versiot ovat tukemattomia ja sisältävät siten tietoturvariskejä. Apple tukee vain laitteita, joihin saa viimeisimmän iOS version asennettua. Vanhimmat tuetut laitteet ovat tällä hetkellä mm. iPhone 7, iPad (5gen.) ja iPad Air 2.

2.5. Sovellukset turvallisesti sovelluskaupasta

Lataamalla sovelluksia ainoastaan Googlen Play-kaupasta tai Applen AppStoresta, voit olla varma, että et sovelluksen mukana saa haittaohjelmia. Sekä Google että Apple tarkistavat sovellukset ennen hyväksymistä kauppoihinsa. Monet älylaitteelle ladattavat sovellukset ovat maksuttomia.

Maksulliset sovellukset voi maksaa luottokortilla, jonka voi halutessaan tallentaa Google- tai Apple-tilille tai voit käyttää siihen esim. ruokakaupoista tai R-Kioskeista ostettavia lahjakortteja. Kaupoista haetut sovellukset myös päivittyvät automaattisesti.

2.6. Suojaa Android-puhelimesi haittaohjelmilta

Suosittelemme maksuttoman tietoturvaohjelman asentamista (esim. Avast, AVG ja Avira). Maksuttomat ohjelmat sisältävät yleensä myös enemmän tai vähemmän

aggressiivisia mainoksia maksullisesta versiosta. Maksamalla pääsee mainoksista eroon, mutta lisäturvaa ei maksullisella tuotteella Androidiin saa.

2.7. Huolehdi varmuuskopioinnista

Helpoimmin puhelimen varmuuskopiointi tapahtuu synkronointiasetusten avulla. Asetuksista laitetaan laitteen varmuuskopiointi päälle seuraavasti:

Android laitteet Google tilille

Laitteen asetukset - Pilvi ja tilit - Varmuuskopioi ja palauta - Google-tili: Varmuuskopioi omat tiedot (päällä)

Kuvien varmuuskopiointi

Google kuvat -sovellus: Asetukset - Varmuuskopiointi ja synkronointi (päällä)

Apple laitteet iCloud tilille

Asetukset - iCloud - Varmuuskopiointi

Varmuuskopioinnissa tallennetaan pilveen kaikki tarvittavat tiedot, kuten asetukset, yhteystiedot ja ladatut sovellukset laitteen täydelliseen palauttamiseen vaikkapa uuteen laitteeseen vanhan laitteen rikkoutuessa tai kadotessa. Varmuuskopioinnin lisäksi asetetaan kuvat ja dokumentit synkronoitavaksi pilveen, joten nekin tulevat talteen.

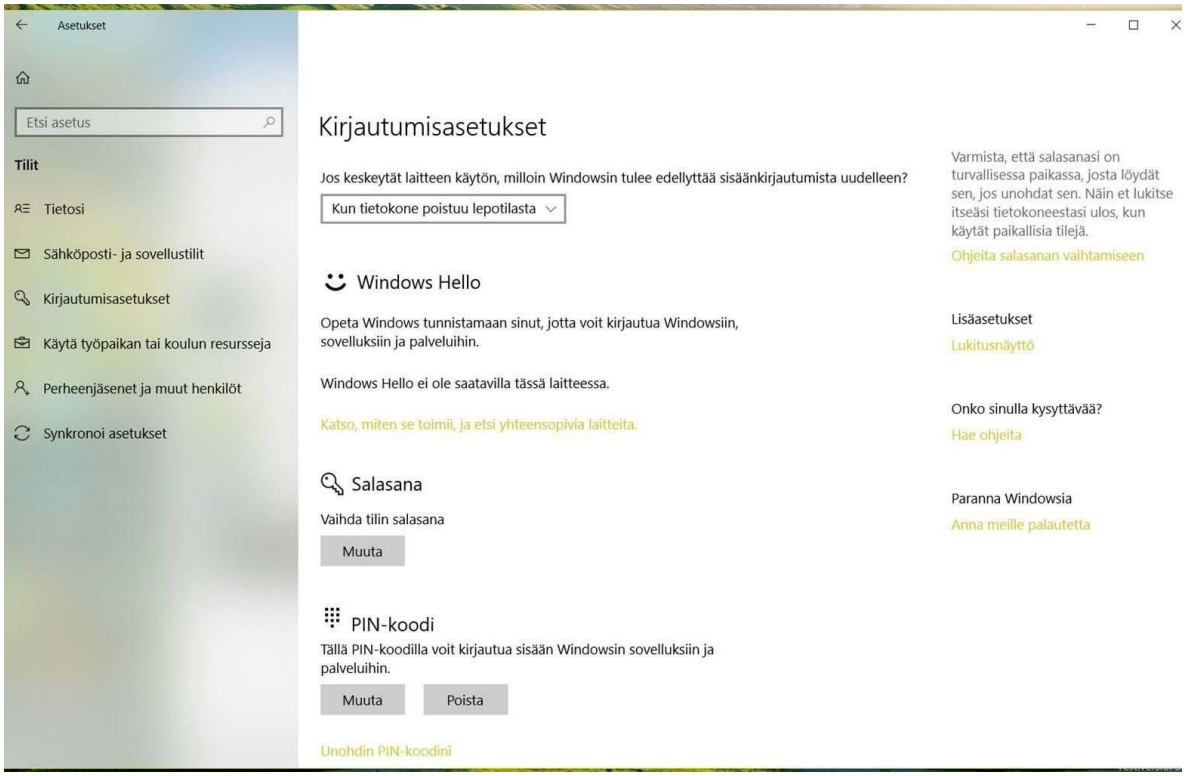
HUOM! Synkronointi tarkoittaa, että kun poistat kuvan tai dokumentit yhdeltä laitteelta tai pilvestä, se poistuu myös kaikilta muilta laitteilta. Tähän voi asetuksilla kuitenkin vaikuttaa
Sen takia valokuvat kannattaa varmuuskopioida säännöllisesti myös tietokoneelle tai ulkoiselle kovalevylle.

3. Tietokoneiden tietoturva: Windows ja Mac

3.1. Windows tietoturva

3.1.1. Kirjaudu aina salasanalla tai PIN-koodilla

Windows kirjautumiseen tulee aina käyttää salasanaa tai PIN-koodia. Windowsin tulisi aina liittää Microsoft-tiliin. Paikallisen tunnuksen salasanat voidaan ohjelmallisesti nollata, ja siten tiedot ovat ulkopuolisten käytettävissä. Salasanan lisäksi voit antaa PIN-koodin, joka helpottaa kirjautumista. PIN-koodi luodaan Asetukset / Tilit / Kirjautumisasetukset -sivulla (ks. Kuva 2). Jos PIN-koodi annetaan väärin monta kertaa tai unohtuu, kirjautuminen tehdään käyttäjätunnuksella ja salasanalla.



Kuva 2. Microsoft-tilin kirjautumisasetukset, PIN-koodin luominen

Microsoft tilin käyttö helpottaa avaamista, jos salasana pääsee unohtumaan. Windows 10 voidaan myös tarvittaessa asentaa uudelleen ilman avainkoodeja (lisenssitietoja), jos

käytetään Microsoft tiliä. Ainakin yhdellä käyttäjätunnuksella on oltava järjestelmänvalvojan oikeudet. Muuten päivittäminen voi tuottaa ongelmia.

3.1.2. Käytä aina vähintään Windows virusten ja uhkien torjuntaa (Defender)

Windowsin mukana tuleva Defender, joka on osa Windows 10 ja Windows 8.1 käyttöjärjestelmiä, tarjoaa riittävän hyvän suojan peruskäyttäjälle. Defender otetaan käyttöön Asetuksista *Päivittäminen ja suojaus* osiosta Windows Defender välilehden alta (ks. Kuva 3). Jos koneeseen ei ole asennettu muuta virusturvaa, niin Defender on käytössä automaattisesti.

Kuva 3. Kuinka ottaa Windows Defender käyttöön

Viimeisimpien testien mukaan Windows Defender tarjoa lähes yhtä hyvän turvan erilaisia viruksia vastaan kuin parhaat ilmaiset (Avast, Avira ja AVG) virusturvaohjelmat. Vaikka mainitut ilmaisversiot tarjoavat jonkin verran paremman suojan, käyttäjää saattaa häiritä niiden jatkuvasti mainostamat maksulliset versiot. Windows 7 käyttöjärjestelmään tulisi asentaa jokin ilmainen tai maksullinen virusturva.

Maksulliset tietoturvaohjelmat (Avast, AVG, Avira, F-Secure, jne) tarjoavat yleensä joitakin lisäominaisuuksia, kuten

- verkkoliikenteen rajoittaminen pankki- ja verkko-ostoksissa

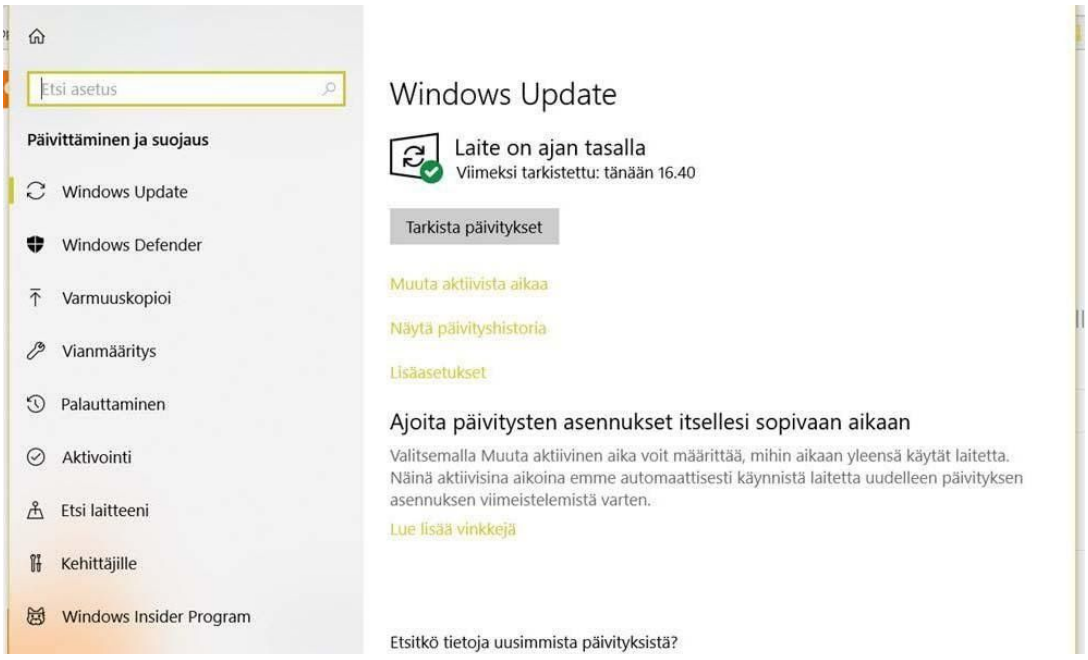
- vaarallisten internet-sivujen esto
- sovellusohjelmien päivityksistä huolehtiminen
- uusien ohjelmien käyttö eristettynä muusta ympäristöstä.

Pankkiyhteyksiin kannattaa käyttää mobiililaitteiden pankkisovelluksia, jotka ovat turvallisempia kuin selaimella käytetty pankkiyhteys.

Window Defender sisältää virustorjunnan lisäksi palomuurin. Se tulee automaattisesti päälle ja sen asetukset riittävät normaalikäyttöön. Mikäli olet ottanut muun virustarkistuksen käyttöön, sisältää se joskus oman palomuuriohjelmiston. Se korvaa Windows 10:n oman palomuurin.

3.1.3. Huolehdi järjestelmäpäivityksistä

Windows päivitykset tulevat automaattisesti, mutta se edellyttää että kone on vähintään kerran kuukaudessa päällä vähintään 2-3 tuntia. Tietyt päivitykset vaativat uudelleenkäynnistyksen, joka tehdään automaattisesti koneen ollessa päällä aktiivisen ajan ulkopuolella. Uudelleenkäynnistäminen tulee myös ilmoituksena ja virran katkaisu-ikonista.



Kuva 4. Tarkista Windows päivityksen tila: Asetukset, Päivittäminen ja suojaus.

Eräissä laitteissa (HP, Lenovo, Dell) on Support Assistant, johon tulee ilmoitus laiteohjelmistojen päivityksistä. Päivitykset on syytä asentaa. Myös sovellusohjelmien päivitykset tulee asentaa. Esim Adobe Flash, jota useat verkkosivustot käyttävät tulee päivittää säännöllisesti.

3.1.4. Muuta huomioitavaa

Huolehdi ohjelmistojen lisenssitietojen ja muiden yksilöllisten tietojen talteenottamisesta.

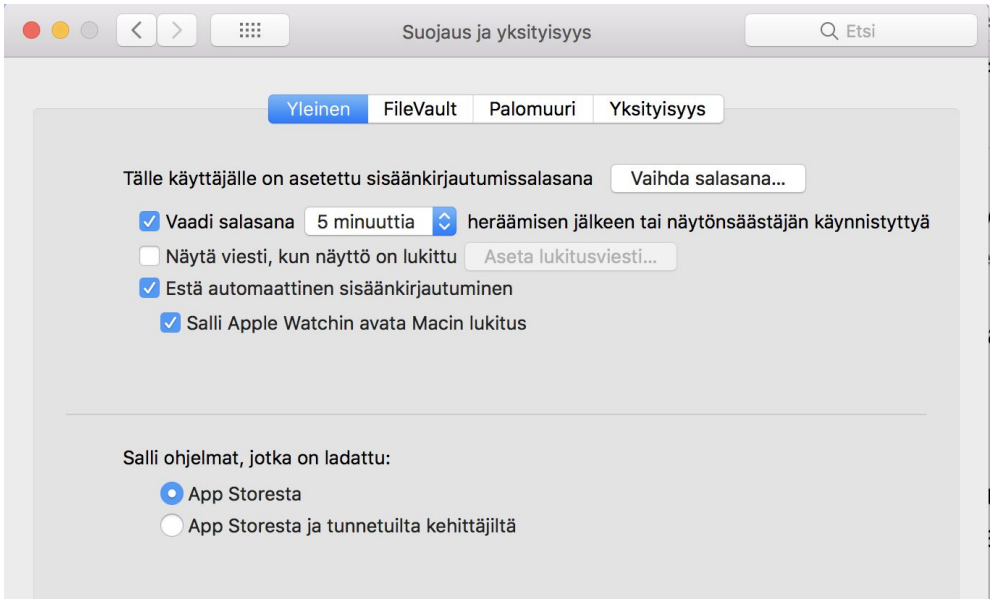
Windows 10 on yksilöity kullekin laitteelle *product key*:llä eli *tuoteavaimella*. Vastaavasti lähes kaikki ostetut ohjelmistot käyttävät samaa menettelyä, termit vain vaihtelevat (serial number yms.). Talleta nämä lisenssitiedot mahdollista tarvetta varten.

Windows 10 on aktivoituessaan tallettanut tuoteavaimen sekä koneelle että Microsoft-tilille. Yleensä uudelleenasennuksen yhteydessä tuoteavain löydetään automaattisesti. Jos tietokoneen emolevy on jouduttu vaihtamaan, niin silloin joudutaan antamaan tuoteavain manuaalisesti. Vanhoissa laitteista tuoteavain löytyy koneen alla olevasta tarrasta. Uusissa laitteissa ei ole tarraa.

3.2. Mac Virusturva

3.2.1. Suositeltava virusturva

Myös Mac tarvitsee nykyään virusturvan. Suosittelemme maksuttoman virustorjuntaohjelman asentamista. Sophos on kotikäyttäjille ilmainen ja mainokseton. Muita ilmaisia tarjoavat Avast, Avira ja AVG.



Kuva 5. Turvalliset Macin kirjautumisasetukset: Järjestelmäasetukset, Suojaus ja yksityisyys

3.2.2. Huolehdi järjestelmäpäivityksistä

Mac-laitteille järjestelmäpäivitykset tarjotaan AppStoren kautta automaattisesti. Oheiset asetukset varmistavat, että päivitykset haetaan ja asennetaan automaattisesti.

Kuva 6. Asetukset, joilla saat automaattiset järjestelmäpäivitykset

3.3. Käytä vain tuettuja Windows ja MacOS versioita

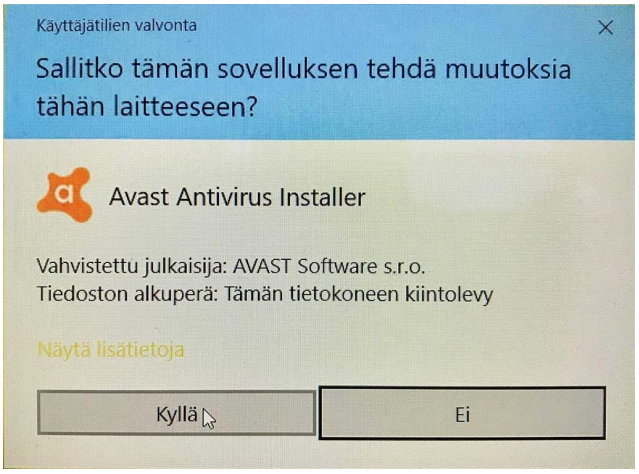
Vanhin tuettu versio Windows 8.1 tuki jatkuu 1/2023 saakka. Tukemattomia Windows versioita ei ole syytä käyttää verkkoon yhdistettynä. Suositellaan laitteen vaihtamista uudempaan.

3.4. Ole huolellinen mistä lataat ohjelmia

Windows Kauppa ja Mac Appstore ovat turvallisia paikkoja ladata uusia ohjelmistoja laitteelle. Windowsiin ja Maciin joutuu kuitenkin usein asentamaan ohjelmia muualtakin kuin sovelluskaupoista. Tällaisia ovat esim. CCleaner ja Adobe Flash, jotka ovat joko hyödyllisiä tai tarpeellisia nettiselailussa. Varsinkin Flash videoiden mukana levitetään usein haittaohjelmia hyödyntäen Flash-ohjelman haavoittuvuuksia. Siksi näiden ohjelmien päivittämisestä tulee myös huolehtia.

Jos asennat ohjelman sovelluskaupan ulkopuolelta, lataa se sovelluksen tekijän omalta sivustolta. Lue myös huolellisesti mitä kaikkea oletkaan asentamassa, sillä useat ohjelmat, varsinkin ilmaiset, asentavat oletuksena myös muita tarpeettomia lisukkeita, jotka tulee ruksata pois. Sovelluskaupoista ladatut sovellukset päivittyvät automaattisesti, joten niitä voi tässäkin mielessä suositella.

Katso aina mitä hyväksyt, kun vaaditaan järjestelmävalvojan hyväksyntä. Jos tiedät, että olet asentamassa kyseistä ohjelmaa, hyväksy ilmoitus (Kuva 7). **Jos tämä ilmoitus tulee nettiselailun aikana tai avatessasi sähköpostin liitettä, älä missään tapauksessa hyväksy pyyntöä.**



Kuva 7. Useat asennukset Windows- ja Mac-laitteissa vaativat järjestelmävalvojan hyväksynnän

3.5. Huolehdi varmuuskopioinnista

Tee varmuuskopiot kaikesta sinulle tärkeästä materiaalista kuten valokuvista ja dokumenteista. Ohjelmista on syytä säilyttää lisenssitiedot pienessä vihkossa salasanojen kanssa.

Varmuuskopioinnin voi tehdä ulkoiselle kovalevylle tai pilveen. Jos käytät koneen ja pilven synkronointia, niin muista, että tiedoston (teksti tai kuva) poisto koneelta poistaa myös pilvestä.

Windows sisältää sovelluksen, jonka voi säätää hoitamaan haluttujen kansioiden varmuuskopioinnin automaattisesti, säännöllisin väliajoin. Sovellus on toimiva, mutta vie melko paljon tallennusmuistitilaa.

4. Käyttäjätunnukset ja salasanat

4.1. Tarvitset käyttäjätunnuksia

Kun uusi laite otetaan käyttöön luodaan aina käyttäjätunnus käyttäjätiliin seuraavasti:

- Windows: Microsoft-tili
- Mac: Apple ID
- Android: Google-tili
- iOS (iPhone/iPad): Apple ID

Käyttäjätiliä luodessa on tärkeää valita hyvä salasana, joka kirjoitetaan muistiin vihkoon tai muualle, mistä se tarvittaessa löytyy. Samalla käyttäjätilin tietoihin on syytä antaa puhelinnumero, jonka avulla käyttäjätili voidaan palauttaa, mikäli salasana unohtuu. Käyttäjätiliin voidaan kytkeä myös muita palveluita, kuten varmuuskopiointi ja laitteen löytäminen sekä mahdollinen sulkeminen etänä.

Käyttäjätunnuksena käytetään yleisimmin sähköpostiosoitetta, koska se on samalla sekä yksilöivä tunnus että yhteystieto. Kun rekisteröidyt uuteen palveluun, niin on suositeltavaa luoda palveluun oma tunnus tai kirjautua Google-tunnuksilla. Sen sijaan Facebook-tunnuksilla kirjautumista ei suositella.

4.2. Käytä hyviä salasanoja

Huomaa, että kaikki salasanat eivät ole yhtä tärkeitä. Sähköpostin salasana on ehkä kaikkein tärkein, sillä sähköpostiosoite on usein avain muihin käyttämiisi palveluihin. Ulkopuolinen, joka saa sähköpostisi salasanan tietoonsa, voi yrittää kirjautua esim. tori.fi -palveluun tunnuksellasi. Siellä hän kertoo unohtaneensa palvelun salasanan, jonka jälkeen hän voi sähköpostistasi kalastaa salasanan palautuslinkin.
Muita tärkeitä salasanoja ovat esim. Googlen, Apple ID:n, Microsoft tilin, maksupalveluiden, nettikauppojen ja sosiaalisen median salasanat.

Tee tärkeistä salasanoistasi vahvoja ja käytä eri salasanoja tärkeissä palveluissa. Vahva salasana on riittävän pitkä (mielellään ainakin 15 merkkiä), voi sisältää vaikkapa kolme sanaa käyttäen isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä. Huonoja salasanoja ovat numerosarjat ja selväkieliset sanat. Älä myöskään käytä salasanana esim. auton rekisterinumeroa tai lemmikin nimeä.

Lisää salasanoista ja kirjautumisesta Enterin dokumentissa *Kirjautuminen ja tunnistautuminen sähköisissä palveluissa (4/2018)*.

4.3. Salasanojen muistaminen

Kirjoita salasanat muistiin esim. pieneen vihkoon ja säilytä vihko turvallisessa paikassa. Käytön helpottamiseksi voit tallentaa salasanat selaimen muistiin. Selain kysyy yleensä lupaa tallentaa salasanan, kun kirjaudut palveluun ensimmäistä kertaa.

4.4. Älä pelästy tietoturvailmoituksia

Saatat todennäköisesti saada tietoturvailmoituksia ainakin Googlelta, Applelta, Microsoftilta ja Facebookilta, jos sinulla on käytössä jotain näiden palveluita. Esimerkiksi Google varoittaa, jos olet avannut Gmail-sähköpostisi uudelta tai vieraalta (esim. kirjaston) laitteelta. Jos tiedät, että olet itse näin toiminut, niin voit unohtaa viestin. Jos olet varma, että et ole käyttänyt muuta laitetta, **kannattaa ensimmäisenä vaihtaa salasanat** tai tulla Enterin opastukseen.

Muutenkaan ei kannata panikoitua erilaisista tietoturvailmoituksista. Useimmiten niille on täysin järkevä, vaaraton selitys. Jos et ymmärrä viestin sisältöä, kannattaa tulla opastukseen ja selvittää asiantuntijan kanssa, mistä on kyse.

5. Sähköposti ja vaaralliset verkkosivut

Ole tarkkana sähköpostien kanssa. Katso todellinen sähköpostiosoite, älä luota pelkästään näkyvään lähettäjän nimeen.

Jos saat sähköpostia tuntemattomasta osoitteesta, tai tutultakin toimijalta, kannattaa aina käyttää harkintaa, kun sähköpostin avaa. Lähettäjän sähköpostiosoite on helppo väärentää ja siten lähettää huijausviestejä. Varmista, että ainakin sähköpostin lähettäjän nimi ja varsinainen sähköpostiosoite täsmäävät. Ohessa esimerkkejä huijausviestien lähettäjästä ja sähköpostiosoitteista (... on turvallisuussyistä piilotettua tekstiä)

Läh: S-marketin paketit Osoite: <...@www36.rantassticaffars.eu>

Läh: "Elisa" Osoite: <...@gmx.de>

Läh: "Google Inc™" Osoite: <...@bici24.eu>

Läh: "Google Inc™" Osoite: <...@jami.re.kr>

Jätä liitteet avaamatta, jos on pienikin epäilys huijausviestistä. Viesteissä olevat painikkeet pitää ehdottomasti jättää painamatta, koska ne voivat viedä vaaralliselle

verkkosivustolle. **Sähköpostin välityksellä tulevat haittaohjelmat sijaitsevat useimmiten linkeissä, painikkeissa tai liitteissä.**

Älä lähetä tärkeitä henkilökohtaisia tietoja kuten henkilötunnusta, tunnuksia tai salasanoja sähköpostilla. Pankki tai poliisi ei koskaan kysy henkilötietoja sähköpostin välityksellä, ei myöskään pankkitunnuksia.

5.1. Miten tunnistat huijausviestin?

Huijausviestillä tarkoitetaan esim. sähköpostiviestiä, missä pyydetään käyttäjätunnuksia, salasanoja tai muita henkilökohtaisia tietoja. Huijausviesteillä toimitetaan myös haittaohjelmia. Alla olevat havainnot helpottavat tällaisen viestin tunnistamisen.

- Saat sähköpostiviestin, jota et ole odottanut.
- Et tunnista viestin lähettäjää tai lähettäjän sähköpostiosoitetta.
- Lähettäjä saattaa vaikuttaa todelliselta (esim. joku tunnettu taho), mutta lähetysosoite paljastaa huijauksen.
- Lähettäjäksi kerrotaan esimerkiksi pankki tai luottokorttiyhtiö.
- Viestiä ei välttämättä ole osoitettu sinulle henkilökohtaisesti.
- Viesti on kirjoitettu huonolla suomen kielellä tai englanniksi.
- Viestissä varoitetaan turvallisuusuhkasta tai kerrotaan teknisestä viasta, joka edellyttää kiireellisiä toimia.
- Viestissä voidaan luvata rahaa tai uhata sulkea tilisi.
- Viestissä oleva linkki tai verkko-osoite ohjaa sivulle, jossa sinulta kysytään luottamuksellisia tietoja.

Jos viesti kuulostaa uskomattoman hyvältä tarjoukselta tai voitolta, niin se on todennäköisesti huijaus, joka yrittää asentaa haittaohjelman tai muuten huijata tärkeitä henkilökohtaisia tietoja.

5.2. Huijausverkkosivut

Verkkosivut on helppo väärentää näyttämään vaikkapa verkkopankilta. Tunnistat oikean turvallisen sivun tarkistamalla sivun verkko-osoitteen edessä olevasta lukitusta lukosta (esim. Chrome-selaimella)

5.3. Voinko ostaa verkosta?

Verkko-ostokset lisääntyvät jatkuvasti ostamisen helppouden, valikoiman laajuuden jne takia. Maksaminen vaatii useimmin luottokorttitietojen antamista, pankkitunnusten käyttämistä tai vaikkapa PayPal-maksupalvelua. Verkko-ostoksiin on vaikea antaa tarkkoja ohjeita, mutta järjen ja varovaisuuden käyttäminen on sallittua. Kaikki em. maksutavat ovat turvallisia oikein käytettynä ja turvallisten kauppiaiden kanssa.

Ennen ostoksia kannattaa googlettaa muiden asiakkaiden kokemuksia kauppiaasta. Jos löytää negatiivisia kommentteja kannattaa ostokset unohtaa. Ja jos tarjous on uskomattoman hyvä, saattaa käydä, että maksu kyllä menee perille, mutta ostosta ei koskaan tulekaan.

Huutokauppaostoksissa (esim. tori.fi) erityinen varovaisuus on paikallaan.

5.4. Facebook ja mitä oikein jaan verkossa

Facebookissa voi keskustella ja löytää ryhmiä, jonka jäseniä yhdistää esimerkiksi harrastus tai asuinalue. Suljetuista ryhmistä keskusteluja ei voi jakaa ulospäin. Myös omat yksityisyysasetukset kannattaa asettaa niin, etteivät julkaisemasi tekstit ole julkisia vaan näkyvät vain heille, jotka olet hyväksynyt ystäviksesi.

Facebookissa on myös paljon mainoksia, pelejä ja kilpailuja. Näitä avaamalla jaat omat Facebook-tietosi kyseisen mainostajan tai pahimmassa tapauksessa huijarin kanssa. Omat tietosi sisältävät myös ystäviesi yhteystiedot, joten huijareiden tapauksessa he

pystyvät nimissäsi lähettämään vaikkapa viruksia sisältäviä viestejä ystävillesi. Suhtaudu siis epäillen kaikkeen ylimääräiseen Facebookissa äläkä osallistu esim. nimitesteihin.

Verkossa on paljon sivuja, jotka vaativat rekisteröitymisen. Usein rekisteröitymisen tarkoitus on kerätä yhteystietoja esim. mainosviestien lähettämiseksi tai myyntitarkoituksiin. Kannattaa siis olla tarkkana mitä tietoja jakaa ja minne.

6. Liittyminen ulkomaailmaan

6.1. Käytä mobiililaitetta pankkiyhteyksiin

Pankkiasioissa turvallisinta on käyttää palveluntarjoajan omaa mobiilisovellusta eli appsia. Rikollisilla on mahdollista huijata pankkisivustoja kytkeytymällä selaimen ja pankin väliin ja siirtää maksut vaikkapa omalle tililleen. Sen sijaan mobiilisovellusta ei rikollisilla ole mahdollista huijata.

6.2. Wi-Fi ja Bluetooth

Tietoturvan sekä akun kestävyyden kannalta on suositeltavaa kytkeä Wi-Fi ja Bluetooth pois päältä, aina kun et käytä niitä. Älä hyväksy vieraita bluetooth-yhdistämispyyntöjä.

Suosittelemme, että et tee selaimella herkkiä (terveys, verkkokauppa jne) asioita avoimessa wifi-verkossa.

6.3. Ole varovainen USB-muistien kanssa

Jos saat toiselta henkilöltä USB-muistilla kuvia tai muita tiedostoja, kannattaa varmistaa, että virusturva on käytössä, kun liität USB-muistin laitteeseesi. USB-muistit ovat tunnettu tapa levittää haittaohjelmia.

Lisäksi on muistettava, että ennen muistilaitteen irroittamista koneesta USB-muisti on ensin ohjelmallisesti katkaistava. Pahimmassa tapauksessa voit menettää USB-muistissa olevaa tietoa.

6.4. Tietoliikennelaitteet (admin/admin)

Meillä on kodeissamme yhä enemmän laitteita kytkettynä kodin lähiverkkoon. Turvallisuuden kannalta kaikkein tärkein laite niistä on reititin, johon kaikki langattoman verkon laitteet kytketään. Reitittimen kautta me sitten kytkeydymme yleiseen tietoverkkoon (Internet).

Tämän laitteen hallintaan käytettävä salasana saattaa olla useinkin seuraava:

Käyttäjä: Admin
Salasana: Admin

Tämä reitittimen salasana on syytä muuttaa heti käyttöönotossa ja kirjoittaa se itselleen muistiin. Joissain tapauksissa, jos reititin on operaattorin kautta hankittu, hoidetaan salasanan vaihto operaattorin toimesta. Siitä sitten informoidaan käyttäjää, jotta hän on tietoinen muutoksesta.

Huomio!

Tämä salasana ei siis ole se salasana, joka tarvitaan WIFI/WLAN-verkkoon kytkeytymiseen! (Löytyy usein reitittimen pohjasta tai näytön valikosta)

Tulevaisuudessa myös kodinkoneet, ovien lukot, lämmityslaitteet, valvontakamerat ja valaistus kytketään kodin lähiverkkoon omilla Gateway-tuotteillaan. Niiden laitteiden hallinnointiin käytettävästä salasanasta on myös syytä pitää hyvää huolta ja on hyvä muuttaa oletussalasana mikäli vain mahdollista.

Lähteenä on käytetty mm. Kyberturvallisuuskeskuksen oppaita.