Mitä tehdä, jos ex-kumppanisi vainoaa sinua teknologian avulla

Miten ex-kumppanisi voi vainota sinua, päästä käsiksi tietoihin sinusta tai vain häiritä sinua – ja mitä voit tehdä asialle!

Linus Nyman & Laura Kankaala
Disobey Outreach

Käännös: Arno Seiro

Disobey Outreach on voittoa tavoittelematon organisaatio, joka keskittyy auttamaan uhan alla olevia ihmisiä ja ryhmiä heidän tietoturva- ja tietosuoja-asioissaan. Yksi pääasiallinen kohteemme on auttaa digivainon tai digihyväksikäytön uhreja, jota he joutuvat kokemaan kumppaninsa tai ex-kumppaninsa toimesta.

Disobey Outreach on lähtenyt liikkeelle vuosittaisesta Pohjoismaiden Disobey-tietoturvatapahtumasta. Sekä yhteisönä että tapahtumana Disobey haluaa vaalia energistä yhteisöä, johon kuuluvat työnluojat, -tekijät ja -sankarit. Disobey järjestetään vuosittain Suomessa.

Linus Nyman (PhD) on tutkija, joka on erityisen kiinnostunut tietosuojasta ja -turvasta sekä liki pitäen kaikista muista IT-asioista. Hän on viettänyt vuosia yliopistolla, sekä tutkijana että kehittäjänä. Linus on myös opettanut yliopistolla. Hän nauttii siitä, että pyrkii tekemään teknologian oppimisen hauskaksi (tai ainakin ei pelkästään kivuliaaksi).

Laura Kankaala on tietoturva-ammattilainen, jonka tausta on käytännön turva-asioissa. Hän on työskennellyt useissa ammateissa ja aloilla, jotka liittyvät tietoturvaan, sekä hyökkäyksen että puolustuksen puolella. Hänen missionsa on tehdä tietoturva-asioista kaikille ymmärrettäviä ja saatavilla olevia.

Tämä opas on kirjoitettu käyttäen avoimen lähdekoodin ohjelmaa LibreOffice,
jonka on tehnyt The Document Foundation.

Sisällysluettelo

1. Kenelle tämä opas on?

Jos uskot, että ex-kumppanisi (tai pian ex-kumppaniksi muuttuva) saattaisi vainota eli puhekielisesti stalkata sinua, yrittää päästä käsiksi tietoihin sinusta tai jollain muulla tavalla käyttää teknologiaa sinun ahdistelemiseksesi, niin siinä tapauksessa tämä opas on sinua varten.

On olemassa lukuisia tapoja, joilla entinen kumppanisi voi teknologian avulla häiritä elämääsi tai seurata tekemisiäsi ilman, että huomaat mitään. Ja riskit ovat suuremmat, jos ex-kumppanisi pääsee tai on päässyt fyysisesti käyttämään puhelintasi, tietokonettasi, autoasi tai käymään kotonasi. Sama pätee, jos olet jossain vaiheessa jakanut jonkun kanssa internet-tiliesi salasanoja. Tai jos käytät sellaisia salasanoja tai vastauksia turvallisuuskysymyksiin, jotka voivat olla helppoja arvata. Lista jatkuu lähes loputtomiin, mutta ymmärrät jo missä mennään. Riskejä on melkoinen määrä. Käymme läpi monia tapoja, joilla teknologiaa voidaan käyttää vainoamiseesi tai häiritsemiseesi, ja mitä voit tehdä asian hyväksi.

Jos et ole teknologiasta hyvin perillä oleva ihminen, nämä aihealueet voivat kuulostaa aluksi hieman hankalilta tai jopa pelottavilta. Voi tuntua siltä, että opittavaa on liikaa ja ettet voi kuitenkaan vaikuttaa asioiden kulkuun. Kuten yksi kotiväkivallan uhrien tukiryhmän jäsen sanoi: “Jos ex-kumppanini haluaa murtautua Facebook-tililleni, hän myös tekee sen.” Mutta tilanne ei ole niin synkkä. Pitkälti sen takia kirjoitimme tämän oppaan – haluamme kertoa, että on olemassa yksinkertaisia asioita, joita voi tehdä vainoamisen riskin vähentämiseksi. Sinun ei tarvitse olla tekniikkaguru, eikä perusasioiden oppiminen ole kovin vaikeaa.

Käymme tässä oppaassa läpi niitä asioita, joilla joku voisi vainota entistä kumppaniaan teknologian avulla. Oletamme myös, että tämä ihminen on kohtalaisen taitava teknologian saralla ja ettei hän käytä hyväkseen mitään laitteita tai jos käyttää, niin vain sellaisia, joita on helposti saatavilla. Mutta meillä on lopussa osio, joka käsittelee tilannetta, jossa ex-kumppani on erityisen taitava teknisesti.

Emme käsittele tilannetta, jossa ex-kumppani pystyy käyttämään valtion, armeijan tai poliisin laitteita tai tietokantoja tai muita vastaavia korkean teknologian asioita. Emme myöskään käsittele asioita, joita ei voida ratkaista lisäämällä tietoturvatasoasi. Esimerkkejä tällaisesta olisi kostoporno tai jos exäsi levittää sinusta ikäviä asioita internetissä. Tuonkaltaisissa asioissa suosittelemme, että haet apua muualta.

Tämä opas ei kata mitä tehdä, jos on olemassa riski fyysisestä väkivallasta. Emme ole psykologeja tai poliiseja – voimme tarjota vain tekniikkaan liittyviä neuvoja. Ota yhteyttä johonkin tukiryhmään tai poliisiin, jos pelkäät väkivaltaa. On myös turvakoteja, joihin voit mennä paetaksesi vaikeaa tilannetta kotona. Emme käsittele näitä aiheita, mutta alueesi tukiryhmien, suojakotien ja poliisin verkkosivustot ja puhelinnumerot löytyvät verkosta.

Tämä opas ei kata mitä tehdä, jos on olemassa riski fyysisestä väkivallasta. Emme ole psykologeja tai poliiseja – voimme tarjota vain tekniikkaan liittyviä neuvoja. Mikäli koet fyysisen väkivallan uhkaa, otathan yhteyttä sosiaali- ja terveydenhuollon toimijoihin tai poliisiin. Lähisuhdeväkivaltaan liittyvissä asioissa Suomessa voit olla yhteydessä myös Nollalinjaan, p. 080 005 005 (24/7), https://www.nollalinja.fi/. Nollalinjan sivuilta löydät myös tiedot Suomessa toimivista turvakodeista. Turvakodit tarjoavat suojaa ja turvaa lähisuhdeväkivaltatilanteissa. Emme käsittele näitä aiheita, mutta alueesi viranomaisten, turvakotien ja poliisin verkkosivustot ja puhelinnumerot löytyvät verkosta.

Huom: Käytä internetiä *turvallisesti* etsiessäsi turvakoteja, tukiryhmiä tai muita vastaavia aiheita verkossa. Kerromme oppaan luvussa 7, kuinka voit käyttää internetiä nimettömästi.

Missä kohdin digitaalinen elämäsi on haavoittuvainen?

Jotta entinen kumppanisi voisi käyttää esimerkiksi jotakin sosiaalisen median tiliäsi, hän ei voi vain ladata paholaisen taikapölyä internetiin ja taianomaisesti kirjautua tilillesi. Hänen on löydettävä tilisi turvallisuudessa haavoittuvuus – keino kirjautua sisään.

Tilin turvallisuutta voidaan verrata kodin turvallisuuteen: jos ovi tai ikkuna on jäänyt auki, silloin kodin turvallisuuspuolella on haavoittuvuus. Samoin sosiaalisen median tileillä täytyy olla joku haavoittuvuus, jota ex-kumppani voi käyttää hyväkseen – virtuaalinen vastine sille, että talon ovi on lukitsematta tai kynnysmaton alla on avain.

Yleisesti ottaen haavoittuvuudet voidaan jakaa kahteen ryhmään: käyttämiemme ohjelmien haavoittuvuuksiin ja ihmisten haavoittuvuuksiin. Haavoittuvuus ohjelmassa olisi sama kuin kodin ovessa olisi huono lukko. Ja aivan kuten jotakuta voitaisiin huijata päästämään joku taloon sisään, me käyttäjät luomme haavoittuvuuksia oman toimintamme takia.

Tässä oppaassa keskitymme tuohon jälkimmäiseen haavoittuvuuteen eli turvallisuutemme aukkokohtiin, jotka johtuvat valinnoistamme ja tekemisis-

tämme. Ja hyvä uutinen on se, että nämä haavoittuvuudet ovat yleensä varsin helppoja korjata. Esimerkiksi se, että ex-kumppanisi hakkeroi eli pääsee käsiksi jonkin sosiaalisen median tilisi tietoihin, on todennäköisesti yhtä helppoa kuin että hän arvaa salasanasi. Ja heikot salasanat ovat haavoittuvuus, jonka voit hoitaa kuntoon minuuteissa! Sen tempun me näytämme toisessa luvussa.

Kun jonkin asian tekee turvallisemmaksi, usein valitettavana sivutuotteena seuraa se, että asian käyttö muuttuu hankalammaksi. Se kannattaa pitää mielessä, kun puntaroi eri vaihtoehtoja digitaalisessa elämässään. Tavoite on löytää sopiva tasapaino turvallisuuden ja mukavuuden välillä. Tässä oppaassa menemme hieman pidemmälle turvallisuuden puolelle kuin mitä ihmiset yleensä tekevät, mutta olemme silti yrittäneet löytää hyvän tasapainon mukavuuden kanssa. Ja autamme sinua tekemään oikeita valintoja sellaisissa asioissa, joissa vähäinenkin määrä enemmän turvallisuutta voi tehdä ison eron lopputulokseen.

Tavalliset tavat, joilla ex-kumppanisi voi häiritä digitaalista elämääsi

Tämä opas kattaa tavalliset tavat, joilla exäsi voi häiritä digitaalista elämääsi keskittyen neljään pääkategoriaan: internet-tilisi, älylaitteesi, vakoiluun tarkoitetut sovellukset ja vakoiluun tarkoitetut laitteet. Kullakin kategorialla on oppaassa oma lukunsa, mutta ensiksi käymme nuo kohdat lyhyesti läpi.

Internet-tilit

Jos joku haluaa vainota sinua ilman että laittaa senttiäkään vakoilutarvikkeisiin, hän voi yrittää päästä kirjautumaan jollekin internet-tilillesi. Sellainen on mikä tahansa tili, jolle kirjaudut verkossa, kuten sähköpostisi, verkkopankkisi ja sosiaalisen median tilisi, mutta myös erilaiset palvelut kuten kalenterit, Etsi puhelimeni -tyyppiset sovellukset, pilvipalvelut ja myös esimerkiksi Google Hallintapaneeli (engl. Dashboard), joka voi muun muassa seurata sinua ja pitää kirjaa sijaintitiedoistasi eri ajankohtina.

Enemmän tai vähemmän noita kaikkia tilejä ja palveluita voi käyttää epämiellyttäviin tarkoituksiin, jos ex-kumppanisi onnistuu saamaan sisäänkirjautumiseen tarvittavat tiedot. Hän voi esimerkiksi lukea ja tuhota sähköpostejasi, nähdä ketä tapaat ja milloin, katsoa ja tuhota kuviasi, nähdä missä paikoissa olet liikkunut tai keihin ihmisiin olet ollut yhteydessä, mitä hakusanoja olet käyttänyt Googlessa ja mitä videoita olet katsonut YouTubessa.

Internet-tilit ja se miten niistä tehdään turvallisia, käsitellään luvussa 2.

Älylaitteet

Älylaitteilla tarkoitetaan laitteita, jotka on liitetty internetiin (tästä tulee termi Internet of Things eli lyhennettynä IoT). Se tarkoittaa sitä, että tuote on internetiin yhteydessä tietokoneen avulla. On vaikea löytää tuotetta, josta joku yritys ei ole tehnyt älyversiota. Löytyy älyvessoja, älypesukoneita, älyvalvontakameroita, älylastenvahteja, älyvesipulloja, älyalusvaatteita, älyhiirenloukkuja ja vaikka mitä.

Joitakin noista laitteista voidaan käyttää vainoamiseen, erityisesti valvontakameraa. Ja myös niitä laitteita, joita ei voida helposti käyttää sinun jäljittämiseksesi, voidaan käyttää erilaisiin ilkeämielisiin tarkoituksiin ja ylipäätään tehdä elämästäsi kurjaa. Joku voisi esimerkiksi säätää valojesi himmennystä tai talosi lämpötilaa tai kontrolloisi jollain tavalla kotisi muita älylaitteita.

Luvussa 3 käsitellään internetiin liitettyjä laitteita ja kuinka tehdä niiden käytöstä turvallista.

Vakoiluohjelmat

Softa tarkoittaa periaatteessa niitä ohjelmia, joita käytät puhelimessasi, tabletissasi tai tietokoneessasi. Tässä oppaassa keskitymme vakoiluohjelmien ryhmään, joita kutsutaan yleensä vainoamisohjelmiksi (engl. stalkerware), vakoiluohjelmiksi (engl. spyware) tai englanniksi käytetään myös termiä spouseware (spouse = puoliso). Tämänkaltainen softa antaa vainoajalle etäyhteyden puhelimeesi, tablettiisi tai tietokoneeseesi, jolloin hän voi nähdä paljon erilaisia asioita. Hän voi nähdä esimerkiksi kehen olet yhteydessä ja missä olet fyysisesti kunakin hetkenä. Tällaiset sovellukset saattavat näyttää päällepäin sellaisilta, joilla vanhemmat seuraavat lastensa tekemisiä, mutta niitä voidaan käyttää myös muihin tarkoituksiin.

Luvussa neljä käymme läpi erilaisia vaarallisia sovelluksia ja appeja (mobiilisovelluksia), joilla sinua voidaan vainota. Samoin luvussa kerrotaan, miten voit suojata laitteesi.

Vakoilulaitteet

Laite viittaa johonkin fyysiseen esineeseen. Esimerkiksi puhelin on laite, ja siinä olevat appit eli mobiilisovellukset ovat softaa. Keskitymme sellaisiin vakoilulaitteisiin kuin GPS-paikantimet, piilovideokamerat ja salakuuntelulaitteet. Käymme läpi esimerkkejä näistä laitteista, mitä ne pystyvät tekemään, ja mitä sinä voit tehdä havaitaksesi niitä.

Luvussa 5 käsitellään vakoilulaitteita ja miten havaita niitä.

Joitain erityistapauksia

Tähän asti käsitellyt aihepiirit kattavat kasan perusuhkia. Mutta on joitakin tilanteita, jotka ansaitsevat erityismaininnan.

Jos ex-kumppanisi on erityisen etevä teknisissä asioissa, se ei kuitenkaan tee tilanteestasi toivotonta. Sinun täytyy vain olla tietoinen lisääntyneistä riskeistä. Tuota asiaa käsitellään luvussa 6.

Jos edelleen asut hankalan kumppanisi kanssa, silloin sinun täytyy olla tietoinen muutamista lisätavoista, joilla hän voi vakoilla sinua. Tuollaisessa tilanteessa sinun täytyy osata peitellä jälkesi verkossa ja käyttää tietokonetta siten, että siitä ei jää mitään jälkiä. Näitä asioita käsitellään luvussa 7.

2. Internet-tilit

Verkossa olevat tilisi ovat todennäköisesti helpoimmat ja haavoittuvimmat kohteet digitaalisessa elämässäsi. Siinä oli huonot uutiset. Hyvät uutiset on se, että on mahdollista (ja itse asiassa aika helppoa) tehdä internet-tileistäsi hyvin turvallisia.

Jotta voit tehdä niin, käymme läpi tärkeimmät tietoturvallisuutta koskevat asiat: salasanat, turvakysymykset ja kaksivaiheisen tunnistautumisen. Käsittelemme myös hieman tilien yksityisyysasetuksia ja sitä, miten välttää vahingossa tapahtuvaa tietojen liiallista jakamista.

Salasanat

Olet saattanut kuulla puhuttavan vahvasta salasanasta, mutta mitä ihmettä se oikein tarkoittaa? Vahvaa salasanaa on liki mahdotonta kenenkään arvata.

Tässä on muutamia yleisesti käytettyjä tapoja arvata salasana:

- ***Usein käytettyjen salasanojan kokeilu***

  Valitettavasti olemme joskus hiukan laiskoja, kun keksimme salasanoja. Valitsemme sellaisia kuin “salasana” tai joitakin helposti muistettavien numeroiden tai kirjaimien yhdistelmiä, kuten “123456”. Mutta nämä salasanat ovat liian yksinkertaisia ja tunnettuja. Verkossa on luettelo yleisimmin käytetyistä salasanoista, joita entinen kumppanisi voi kokeilla. Joten salasanat, kuten “letmein” ja “qwerty123”, ovat ehdottomasti heikkoja salasanoja, ja ne ovat todella hyödyllisiä vain, jos haluat estää lemmikkieläintesi pääsyn tileillesi, kun olet itse ulkona talostasi.

  Joten haluat *välttää yleisimmin käytettyjä salasanoja.*

- ***Henkilökohtaiset tietosi, jotka hän tietää***

  Toinen tapa, jolla joku voi yrittää arvata salasanasi, on kokeilla sinuun liittyviä henkilökohtaisia, tärkeitä asioita. Tämä kohta on erityisen tärkeä silloin, kun vainoaja tuntee sinut. Mutta olet myös mahdollisesti jakanut tietoa itsestäsi sosiaalisessa mediassa.

  Sellaisia asioita voivat olla esimerkiksi kissasi nimi, oma nimesi ja syntymäaikasi, lempikirjailijasi tai elokuvasi ja niin edelleen. Näistä muodostuu heikkoja salasanoja, koska ne voidaan arvata helposti– tai ainakin melko helposti.

Joten *älä käytä henkilökohtaisia tietojasi* salasanoissasi.

- ***Kaikkien salasanojen kokeilu***

  Pelottavin vaikkakin harvinainen tapa, jota voidaan käyttää salasanasi murtamiseksi, on niin sanottu väsytysmenetelmä (engl. brute force). Se tarkoittaa käytännössä sitä, että kokeillaan vain kaikkia mahdollisia salasanoja, kunnes oikea löytyy. Eli ensin yritetään kirjainta a, ja jos se ei toimi, niin sitten kirjainta b ja niin edelleen, kunnes kaikkien kirjainten ja merkkien kaikki yhdistelmät on käyty läpi.

  Se veisi käsityönä valtavasti aikaa, vaikka salasana olisi kohtalaisen lyhyt. On olemassa tietokoneohjelmia, jotka etsivät salasanaa automatisoidusti, mutta niilläkin on rajoitteita. Palveluntarjoajat ovat lisänneet suojauksia automatisoituja ohjelmia vastaan. Esimerkiksi tilisi jäädytetään useiden minuuttien ajaksi, jos salasanaasi on yritetty arvata väärin tietyn määrän kertoja. Ja olet nähnyt ne “todista, että olet ihminen” -haasteet, joissa sinun on kirjoitettava, mitä näet sumeiden tai epäselvien kirjainten ja numeroiden laatikossa.

  Väsytysmenetelmä on toteutettavissa, jos entinen kumppanisi on onnistunut saamaan haltuunsa salasanojen tietokannan tietovuodon seurauksena. Internet-palveluiden ei pitäisi tallentaa salasanoja selkotekstimuodossa, joten ne tallennetaan salatussa muodossa. Automatisoituja ohjelmia voidaan kylläkin käyttää salasanojen salauksen purkamiseen, mutta tässä salasanan pituudella ja monimutkaisuudella on todella suuri merkitys.

  Jos salasanasi on tullut julkiseksi tietokantamurron yhteydessä, ei ole mitään tapaa suojautua automatisoidulta ohjelmalta, joka lopulta purkaa salauksen, ja salasanallasi voidaan kirjautua tilillesi. Hyvä puoli on taas se, että jos teet salasanastasi pitkän, silloin tietokoneella menee todeeeeella pitkä aika sen selvittämiseen. Kuten esimerkiksi miljardeja vuosia. Kyllä, miljardi on luku, jossa on yhdeksän nollaa. Joten vaikka ex-kumppanisi lopulta onnistuu selvittämään salasanasi, voit lohduttautua sillä, että siinä vaiheessa aurinko on jo luhistunut, ja maapallo on ollut asumiseen kelpaamaton jo pitkän aikaa.

  Joten *paras tapa puolustautua on edelleen vahva salasana*, sellainen, joka on yksilöllinen ja vähintään 12 merkkiä pitkä.

Vahvan salasanan luominen

Miten vahva salasana sitten luodaan? Lyhyt vastaus: ajattele salasanaa sala*lauseena*, ei sala*sanana*. Älä käytä yhtä sanaa niin, että lisäät siihen joitain

kikkoja, kuten isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Sen sijaan keksi jokin lause tai sanojen yhdistelmä, josta lähdet kehittämään salasanaasi.

Lyhyitäkin salasanoja voi olla vaikea muistaa, jos niissä on yksi sana, mutta monta erikoismerkkiä. Ne ovat myös turvattomampia kuin pitkät salasanat. Joten muista, että salasanojen kohdalla pituus on tärkeämpää kuin monimutkaisuus. “PiiiitkätSalasanatOvatVaikeastiArvattavissa” on esimerkki salasanasta, johon väsytysmenetelmällä menisi miljoonia vuosia pitempään selvittää kuin “S@la5ana”, vaikka jälkimmäinen vaikuttaa ensi alkuun varmemmalta, onhan siinä käytetty erikoismerkkiä @ ja ovelasti lukua 5.

Se ei tarkoita sitä, että monimutkaisuuden eli isojen ja pienten kirjaimien, erikoismerkkien ja numeroiden lisääminen olisi huono asia, päinvastoin, mutta tärkeintä on pituus. Kun olet tehnyt itsellesi pitkän salasanan, voit lisätä siihen monimutkaisia asioita, jotta se olisi vielä turvallisempi. Otetaan esimerkki: Yksi tapa tehdä salalauseista helpommin muistettavia, on ajatella omaa elämää tai mielipiteitä. Luomme vaikkapa salasanan “EkaFillariniOliSininen”. Sitten lisäämme siihen jotain monimutkaisuutta ilman, että siitä tulisi vaikeammin muistettava: “EkaFillariniOli#Sininen!”.

Yksi asia kannattaa pitää mielessä, kun miettii salasanan muodostamista lauseesta. On olemassa tietokoneohjelmia, jotka osaavat etsiä laulujen sanoituksia, erilaisten sanojen yhdistelmiä jne. Joten älä käytä jonkin suosikki-laulusi sanoja suoraan. Voit vaikkapa kirjoittaa englanninkielisiä sanoja niin kuin ne lausuttuna kuulostavat, käyttää jotain harvinaista kieltä kuten suomea(!), lisätä erikoismerkkejä ym. Eli jos käytetään tätä menetelmää kuuluisan laulun sanoihin, se voisi näyttää tältä: “SaundOf#Sailens!”. Foneettinen kirjoituasu on hyvä idea, vaikka salasanasi ei tulisi laulun sanoista.

Lyhyesti: käytä salasananasi lausetta ja lisää siihen erikoismerkkejä sinne tänne.

Älä käytä samaa salasanaa uudestaan

Salasanojen muistaminen on hankalaa, joten monet ihmiset käyttävät samaa salasanaa monella eri tilillä (käymme kohta läpi, miten muistaa pitkiä salasanoja). Salasanojen kierrättäminen on (erittäin) huono idea, koska jos joku saa käsiinsä yhden salasanasi, hän voi kirjautua sillä monille eri tileillesi. Muistatko sen jutun haavoittuvuuksista? Salasanan uudelleen käyttäminen toisilla tileillä on kuin sinulla olisi vain yksi avain, joka kävisi kaikkiin lukkoihisi: kotisi, autosi, polkupyöräsi jne.

On monia tapoja, joilla joku ilkeämielinen ihminen voi yrittää saada tietoonsa salasanasi: joku voi vain yrittää katsoa olkasi yli, kun kirjoitat salasanasi tai lähettää sähköpostiviestin, joka huijaa sinut paljastamaan salasanasi ja löytyy

muitakin tapoja. Mutta sitten on vielä yksi tapa, jonka takia joka vuosi valtavia määriä salasanoja päätyy vääriin käsiin. Olet saattanut kuulla sanan “tietomurto”. Periaatteessa se tarkoittaa sitä, että kasa informaatiota päätyi internetiin, vaikka niin ei olisi saanut käydä. Kyseessä voi olla inhimillinen virhe tai huono tietoturvataso. Informaatio voi olla vaikkapa ihmisten nimiä, henkilötunnuksia, luottokorttien numeroita jne. Mutta kyseessä voi olla myös sähköpostiosoitteita ja salasanoja. Joten on olemassa vaara, että salasanasi paljastuu johonkin organisaatioon tehdyn tietomurron seurauksena, jos sinulla oli tili siellä. Mutta onko tämä ainut paikka, jossa olit käyttänyt tätä salasanaa? Yksi helppo, mutta tärkeä tapa rajoittaa tietomurron aiheuttama haittaa on se, että käyttää eri salasanoja eri tileillä.

Sinulla pitäisi ihannetilanteessa olla vahva ja yksilöllinen salasana jokaiselle internetissä olevalle tilillesi. Mutta jos on olemassa riski, että et jaksa niin tehdä (se on vähän vaivalloista, mutta suosittelemme sitä joka tapauksessa), niin sitten sinulla pitäisi ainakin olla vahvat ja erilaiset salasanat kaikille tärkeille tileillesi.

Sähköpostitilisi on hyvä esimerkki sellaisesta tilistä. Syy on se, että jos exäsi saa haltuunsa sähköpostisi salasanan, hän voi hallita kaikkia tilejäsi, jotka on liitetty tuohon sähköpostiisi. Olet todennäköisesti huomannut sisäänkirjautumissivuilla tekstin, jossa lukee “Unohditko salasanasi?”. Siitä linkistä pääset yleensä muuttamaan salasanasi. Ja mihin tuo linkki lähetetään? Sinun sähköpostiisi. Eli jos joku saa haltuunsa sähköpostisi sisäänkirjautumistiedot, hän voi ensitöikseen vaihtaa siihen salasanan, jolloin et enää itse pääse sähköposteihisi käsiksi. Sen jälkeen hän voi alkaa käydä läpi eri sosiaalisen median ja muita tilejä, jotka on liitetty tuohon sähköpostiin ja hän voi muuttaa niiden tilien kaikki salasanat. Sähköpostisi pitäminen turvassa on oleellisen tärkeää. Heikko salasana tekee kaikista siihen sähköpostiin linkitetyistä tileistä haavoittuvaisia.

Turvakysymykset

Turvakysymysten idea menee ajassa taaksepäin niin kauas, että sosiaalista mediaa ei edes ollut olemassa (usko pois, sellainenkin aika on ollut). Se oli aikakausi, jolloin koko maailma ei tiennyt, mitä koulua joku oli käynyt tai mitä hän oli syönyt aamiaiseksi kolme vuotta sitten. Kuka tahansa voi hyvinkin päästä käsiksi sellaisiin turvakysymystesi vastauksiin kuin mikä oli äitisi tyttönimi, minkä nimisellä kadulla asuit lapsena tai mikä oli ensimmäisen lemmikkisi nimi. Mutta vielä paremmat mahdollisuudet heillä on tähän, jos he tuntevat sinut hyvin tai jos olet aktiivinen sosiaalisessa mediassa.

Ratkaisu parempiin turvakysymysten vastauksiin on helppo: valehtele! Kohtele turvakysymyksiä kuin salasanoja. Tee niistä yksilöllisiä. Eli älä koskaan anna samaa vastausta samaan turvakysymykseen eri sivustoilla, koska vastauksesi

saattaa vuotaa tietomurron seurauksena vääriin käsiin. Ja muista myös yhtä tärkeänä asiana, että vastauksellasi ei saa olla mitään tekemistä kysymyksen kanssa. (Mikä oli äitini tyttönimi? No se oli tietysti KoiratPomppivat-KorkeammalleKuinKissat#boingboing!).

Kaksivaiheinen tunnistautuminen

Kuten olemme puhuneet, jos joku saa käsiinsä yhden salasanasi, sillä voi olla todella ikäviä seurauksia. Tämä seuraava aihe, kaksivaiheinen tunnistautuminen (joskus käytetään myös termiä kaksivaiheinen todentamismenetelmä), on luotu, jotta internet-tilisi pysyisi turvallisena. Se toimii siten, että vaikka joku arvaisi tai saisi salasanasi haltuunsa, hän ei silti pystyisi kirjautumaan tilillesi.

Kaksivaiheinen tunnistautuminen viittaa siihen, että sinun täytyy todistaa kaksi kertaa olevasi sinä itse. Tyypillinen esimerkki olisi pankkikortti, jolla on oma tunnusluku. Jotta tiliä pääsee käyttämään, sinulla täytyy olla sekä itse kortti että tunnusluku.

On eri tapoja toteuttaa kaksivaiheinen tunnistautuminen internet-tileille. Yleinen tapa on sellainen, jossa sen jälkeen, kun olet kirjoittanut käyttäjänimesi ja salasanasi, sinulle lähetetään puhelimeesi viesti, joka pitää sisällään sarjan kirjaimia ja numeroita. Verkkopalvelu pyytää sinua sen jälkeen syöttämään vastaanottamasi tekstiviestin. Jos et tee niin tai kirjoitat väärän vastauksen, et pääse kirjautumaan tilille.

Tämä varmistaa sen, että vaikka tietäisi jonkun käyttäjänimen ja salasana, hänen tililleen ei kuitenkaan pääse kirjautumaan. Hyökkääjän täytyy myös päästä käsiksi toiseen tunnistautumistapaan. Äskeisessä esimerkissä se oli puhelimeen lähetetty viesti. Silloin hyökkääjän pitäisi myös päästä käsiksi puhelimeesi (ja avata sen lukitus), ja vasta sitten he pääsisivät tiliisi käsiksi.

Jotkut kaksivaiheisen tunnistautumisen tavat ovat turvallisempia kuin toiset. Tekstiviesti ei ole turvallisin tapa. Mutta on tärkeää, että käyttää edes *jotain* kaksivaiheisen tunnistautumisen tapaa, jos sellainen on tarjolla.

Apua salasanojen muistamiseen

Näinä päivinä monilla meistä on tusinoittain internet-tilejä. Eli meillä on PALJON salasanoja muistettavaksi. Tässä oppaassa suosittelemme, ettet käytä mitään noista salasanoista kahteen kertaan *ja* että muodostat jokaisesta salasanasta niin pitkän ja monimutkaisen kuin mahdollista. Miten ihmeessä voit muistaa ne kaikki? Pelko pois – on olemassa muutamakin eri tapa, jolla pystyy ratkaisemaan tämän ongelman.

- **Salasanamanageri:** On olemassa ohjelmia, joiden tehtävänä on hallita salasanojasi. Niissä on usein toiminto, joka luo pitkiä, yksilöllisiä salasanoja. Silloin kirjautuminen tilille voi olla niin yksinkertaista, että salasanamanageri automaattisesti kirjoittaa tarvittavan salasanan. Tai sitten kopioit salasanan salasanamanagerista ja liität sen kirjautumissivulle. Jotkut salasanamanagerit tallentavat salasanasi (salattuna) pilveen, jotkut ohjelmat tallentavat ne sille tietokoneellesi tai puhelimellesi, jolle olet asentanut salasanamanagerin. Molemmissa vaihtoehdoissa on sama periaate: sinun täytyy muistaa vain yksi salasana – se, jota tarvitset salasanamanagerisi käyttöön. Ja sitten salasana-manageri muistaa puolestasi kaikki muut salasanat.
- **Paperille tehty lista:** Kuulostaa huonolta idealta, että kirjoitat kaikki salasanasi yhdelle paperiliuskalle, mutta se riippuu tilanteestasi. Jos asut yksin tai asut ihmisten kanssa, joihin luotat, silloin kodissasi oleva muistilista salasanoistasi on täysin hyväksyttävissä oleva vaihtoehto. Voit hieman lisätä turvallisuutta sillä, että pidät salasanalistasi esimerkiksi lukitussa pöytälaatikossa ja pitämällä avaimen avainnipussasi. Voit tehdä asiat vielä hieman turvallisemmiksi, jos et kirjoita muistiin kaikkein tärkeimpien tiliesi salasanoja, esimerkiksi sellaisen sähköpostitilin salasanaa, jota käytät muiden tilien palauttamiseen.
- **Muistilista tiedostona tietokoneellasi tai puhelimellasi:** Tällainen lista pitäisi olla salattu pitkällä yksilöllisellä salasanalla. Ja pidä varmuuskopio tiedostosta jollain toisella tietokoneella tai USB-tikulla ja mieluiten vielä niin, että varmuuskopio sijaitsee jossain muualla kuin kodissasi. Näin suojaat listasi sitä vastaan, että sattuisit kadottamaan laitteesi tai kodissasi olisi vaikkapa tulipalo.

Tilin suojaus- ja yksityisyysasetukset

Yleisesti ottaen tietoturva tarkoittaa itsesi suojelemista hakkeroinnilta tai huijaukselta, ja yksityisyys on asioita, joita jaamme – joskus tietoisesti, joskus tahattomasti.

Yksi asia, joka sijaitsee tietoturva- ja yksityisyysasioiden välimaastossa, on oletusasetuksesi tiedostojen taltioimiselle. Esimerkiksi mihin puhelimesi tallentaa sillä ottamasi kuvat tai videot? Tallentuvatko ne pelkästään puhelimen omaan muistiin vai saman tien myös pilveen? Jos sinulla on pilveen tallennettuja asioita, sinun pitää olla erityisen huolellinen sen sivuston suhteen, joka kontrolloi pilveäsi. Toisin sanoen käytä vahvaa salasanaa, kaksivaiheista tunnistautumista jne.

Sinun tulisi myös miettiä tilannetta, jossa appi tai palvelu kerää tai jakaa sijaintitietojasi. Jos lähetät kuvan sosiaaliseen mediaan, etkä halua, että muut tietävät missä olet, varmista, että sivusto ei lisää tai merkitse sijaintia kuvaan.

Voit yleensä muuttaa ainakin joitain asetuksia sen suhteen, mitä haluat jakaa muiden kanssa (tai tilin tai palvelun takana olevan yrityksen kanssa). Tarkista internet-tiliesi yksityisyysasetukset varmistaaksesi, ettet jaa itsestäsi enemmän kuin sinulle sopii ja minimoi riski, että jaat tai jopa tallennat tarpeettomia tietoja, joita entinen kumppanisi voi väärinkäyttää.

Kirjautumistietojen avulla voi havaita väärän käyttäjän

Jotkut internetin palveluntarjoajat tarjoavat mahdollisuuden nähdä lokikirjan, josta voit saada selville, jos joku on yrittänyt kirjautua tileillesi. Jotkut palvelut näyttävät, milloin ja missä tiliäsi on käytetty. Voit nähdä vaikkapa missä sinä (tai joku, joka on tekeytynyt sinuksi) kirjauduit sisään aiemmin, ja milloin se tapahtui. Joten voit nähdä, jos tililläsi on vierailtu sellaisesta paikasta, esimerkiksi kaupungista käsin, jossa et silloin ollut tai jos tilillä on vierailtu silloin, kun et itse käyttänyt sitä palvelua.

Tarkistaaksesi nämä asetukset Googlen osalta, kirjaudu ensin selaimella Gmail- tai Google-tilillesi. Mene sen jälkeen kohtaan Google-sovellukset (selaimessa se kuvake, jossa on yhdeksän pistettä). Sieltä valitse Tili -> Tietoturva -> Viimeisimmät tietoturva-tapahtumat. Se näyttää, jos tilillä on ollut hämärä-peräisiä sisäänkirjautumisia.

- Tietoturva-kohdasta löytyy myös “Laitteesi”. Siitä näet, jos Google-tilillesi on kirjautunut tuntematon laite.
- Kohdasta “Kolmannen osapuolen sovellukset” näkee se sovellukset, joilla on pääsy Google-tilille. Käy läpi luettelo ohjelmistoista, esimerkiksi tunnista-mattomista selaimista, joilla on käyttöoikeus Google-tilin tietoihin.

Voit poistaa kaikki epäilyttävät laitteet ja selaimet, jotka on liitetty tiliisi. Ennen kuin teet niin, ota sivusta kuvakaappaus tai kirjoita muistiin kaikki laitteet, jotta voit tulevaisuudessa käyttää sitä todisteena.

Mene sen jälkeen kohtaan Google-sovellukset -> Tili -> Ihmiset ja jakaminen. Jos siinä kohtaa “Sijainnin jakaminen” on päällä, ota se pois päältä.

Google hallintapaneeli

Jos sinulla on Google- tai Gmail-tili, sinun on hyvä tietää, että oletusarvoisesti Google seuraa tekemisiäsi varsin paljon. Esimerkiksi sellaisia asioita kuin mitä

etsit internetistä (jos käytät Googlea kun googletat), mitä YouTube-videoita olet katsonut, missä olet ollut (jos sinulla on Android-puhelin tai Google Maps -ohjelma), jne. Voit nähdä ainakin osan siitä, miten Google seuraa sinua Googlen hallintapaneelista (engl. Google Dashboard). Jos sinulla on Googlen tili, voit kirjautua sisään hallintapaneeliin osoitteessa: myaccount.google.com/dashboard

Kannattaa miettiä sen etuja ja riskejä, että Google pitää kirjaa kaikesta tästä. Tarvitsetko tuota tietoa, joka on sinusta tallennettu? Mieti niitä seurauksia, jos ex-kumppanisi pääsisi käsiksi sinun Google hallintapaneelin tietoihin. Huomaa, että voit poistaa erilaiset lokitiedot sieltä. Voit myös keskeyttää suurelta osin tietojen kirjaamisen lokiin verkkopalvelussa. Ja kuten jo aiemmin mainittu, tämä on esimerkki sivustosta, joka kannattaa suojata erityisen hyvin, koska jos exäsi pääsee tietoihin käsiksi, hän voi nähdä *hyvin paljon* tietoja sinusta.

iCloud

Jos entinen kumppanisi saa käsiinsä iCloud-tilisi käyttäjätunnuksen ja salasanan, hän voi katsoa kaikkea sitä, mitä olet tallentanut iCloudiin. Tarkista, mitkä laitteet on liitetty iCloud-tiliin. Tämän voi nähdä iOS-laitteen asetuksista ja menemällä “Apple ID, iCloud, iTunes & App Store”. Laitteiden lista näyttää laitteen nimen ja minkälainen laite on kirjautunut sisään iCloud-tilille. Jos näet mitään tuntemattomia tai outoja laitteita, ota siitä ruutukaappaus, jotta sinulla on todiste oudosta laitteesta. Sen jälkeen poista se laite ja vaihda iCloud-tilisi salasana. Parannat vielä turvallisuutta, kun otat iCloud-tilillesi käyttöön kaksivaiheisen tunnistautumisen, josta oli puhetta aiemmin tässä luvussa.

Seuraavaksi käy läpi loput tilisi ja lisää samalla lailla turva-asetuksia, jos se on mahdollista.

3. Älylaitteet

Internetiin yhteydessä olevat laitteet tulevat koko ajan yleisimmiksi. Olipa kyseessä melkein mikä tahansa tuote, yritykset pyrkivät väen väkisin olemaan ensimmäinen, joka pystyy tarjoamaan "älyversion" tuotteesta. Ja näyttää siltä, että jatkossa on entistä vaikeampaa edes *löytää* sellaista versiota tuotteesta, joka ei ole internetiin yhteydessä.

Jos kaikki yritykset olisivat hyviä tietoturvan saralla ja todella huolehtisivat sinun yksityisyydestäsi, tämä trendi ei olisi niin huolestuttava. Mutta yritykset eivät ole siinä hyviä. Eivätkä ne huolehdi yksityisyydestäsi. Näin se vain menee. Sen takia sinun on pakko oppia joitain perusasioita liittyen älytuotteiden tietoturva-ongelmiin ja kuinka tehdä niistä turvallisia.

Älylaitteisiin liittyvät tietoturvahuolet pitävät sisällään yleiset turvaongelmat, joista jokaisen pitäisi olla huolissaan ja lisähuolenaiheet, joista pitää olla huolissaan, jos epäilet, että exäsi vainoaa sinua. Jaamme nämä aiheet neljään osaan: tietoturvaan liittyvät haavoittuvuudet, oletussalasanat, tietosuoja-asetukset ja tietojen jakaminen sekä tilanne, jossa joku voi päästä kirjautumaan laitteellesi tai hallitsemaan sitä. Sitten luvun lopussa esitämme yhteenvedon asioista, joita kannattaa miettiä, kun on ostamassa älylaitteita.

Tietoturvaa koskevat haavoittuvuudet

Älytuotteiden tietoturva voidaan tiivistää yhteen (ja melko masentavaan) lauseeseen: monet – elleivät useimmat – älytuotteet eivät ole kovin tietoturvallisia, ja niiden tietoturva voi heikentyä ajan myötä. Tämä johtuu kahdesta asiasta: ohjelmistokehityksestä ja päivityksistä. On erittäin vaikea kehittää ohjelmistoja, jotka eivät vain toimisi, mutta joissa olisi myös tietoturva kunnossa. Jos valmistajalla ei ole tietämystä tietoturvasta tai hänen täytyy säästää kustannuksissa, yrityksen tuotteissa on todennäköisesti tietoturvaongelmia. Turvallisuus on koko ajan taistelua kahden osapuolen välillä. Toisella puolella yritetään löytää haavoittuvuuksia, jotta niitä voitaisiin käyttää hyväksi ja sitä kautta saavuttaa jotain hyötyä. Toisella puolella taas yritetään löytää haavoittuvuuksia, jotta ne voidaan "paikata", joka tarkoittaa korjata tai poistaa haavoittuvuudet.

Älylaitteet ovat huonomaineisia siinä suhteessa, että niihin ei juurikaan saa turvapäivityksiä. Ja silloin kun niihin saa turvapäivityksen, me käyttäjät olemme tunnetusti huonoja päivittämään laitteitamme. Tiedätkö esimerkiksi ketään, joka olisi päivittänyt ohjelmiston internetiin liitettyyn leivänpaahtimeensa? Jos päivityksiä ei tehdä, kaikki älylaitteet tulevat lopulta haavoittuvaisiksi. Joten juuri ostamassasi älylaitteessa voi olla jo alkaa päälle haavoittuvuus tai turvaongelma,

ja ajan kuluessa kaikkiin älylaitteisiin sellainen joka tapauksessa tulee, jos tuote ei saa päivityksiä.

Oletussalasanat

Edellisessä luvussa puhuimme vahvojen salasanojen tärkeydestä. Nyt puhumme täysin päinvastaisesta asiasta: oletussalasanoista. Se tarkoittaa sitä salasanaa, joka laitteessa on valmiina, kun ostit sen. Esimerkiksi yleinen oletussalasana, jolla voi avata monet SIM-kortit on 0000 ja 1234.

Oletussalasanat eri laitteille on melko helppo jokaisen löytää, kunhan etsii asiaa internetistä. Ja jos et vaihda oletussalasanojasi, laitteessasi on todella jätti-kokoinen haavoittuvuus – erittäin heikko salasana. Jotkut älylaitteet on tehty siten, että niiden oletussalasanan vaihtaminen ei käy päinsä. Ja se on täysin järjetön tapa suunnitella laite. Valitettavasti et juurikaan voi asialle mitään, paitsi ettet osta kyseisiä tuotteita. Valitettavasti ei ole täysin helppoa saada selville, mitä tuotteita välttää. Se vaatii työtä. Pitää etsiä internetistä, josko edes jotain olisi sanottu laitteen tietoturva-asioista ennen kuin ostaa sen.

Etäkäyttö tai -hallinta

Laitteen hallinta internetin kautta voi olla kätevää. Mutta kun avaat laitteelle pääsyn internetiin, samalla kenelle tahansa internet-yhteyden omaavalle avautuu mahdollisuus hallita laitettasi. Vaikka älytalot ovat kohtalaisen uusi asia, jo nyt on tapauksia, joissa talon älylaitteita on käytetty kotiväkivallan välineinä. Nellie Bowlesin New York Timesiin kirjoittama artikkeli vuonna 2018 esitteli useita ongelmia ja huolenaiheita, jotka liittyvät älylaitteiden käyttöön kotiväkivallassa. Bowles kertoi, kuinka uhrit olivat tulla hulluiksi, kun heidän laitteensa menivät päälle ja pois itsestään, heidän älylukkonsa lakkasivat toimimasta, heidän termostaattinsa vaihtoivat lämpötilaa ja muita epämiellyttäviä asioita tapahtui.

Jos kodin älylaitteet käyttäytyvät oudosti, ensimmäinen temppu on yksin-kertaisesti sammuttaa se ja sitten käynnistää laite uudelleen. Tätä tapaa kannattaa käyttää ensiksi, koska se on usein ainut mitä tarvitsee tehdä silloin, kun tekninen laite temppuilee.

Kannattaa myös miettiä, ettei vain ollut niin, että ex-kumppanisi asensi laitteen sinun käyttöösi. Jos heillä on mahdollisuus kirjautua yhteenkään kotisi älylaitteeseen, jos heillä on siihen vaadittava salasana, silloin on mahdollista, että heidän takiaan laitteesi käyttäytyvät oudosti. Sellaisessa tapauksessa käynnistä laite uudelleen ja sitten vaihda siihen salasana. Jos et pysty vaihtamaan salasanaa laitteeseen, koska sinulla ei ole nykyistä tiedossa ja joudut sen takia kysymään sitä sähköpostitse, joka menee automaattisesti ex-kumppanillesi, silloin voit joko

olla suoraan yhteydessä valmistajaan tai ottaa laitteen irti verkosta. Yksi varokeino on myös se, että vaihdat salasanan reitittimeesi eli siihen laatikkoon, jonka kautta internet tulee kotiisi.

Tietosuoja-asetukset ja tietojen jakaminen

Älylaitteiden ongelmat eivät helpolla lopu. Niitä vaivaa sama asia kuin sosiaalisen median tilejäkin. Älylaitteet lähettävät oletusasetuksilla ulos tietoa enemmän kuin ehkä haluat jakaa. Tarkista älylaitteesi asetuksista tai käyttöohjeista, mitä tietoa laite jakaa oletuksena ja mitä voit muuttaa niissä asetuksissa.

Jos tiedät mistä etsiä, internetistä löytyy hämmentävän paljon tietoa, joka pitäisi olla salasanan suojaamana, mutta ei ole sitä: metallinpolttouunien hallintalaitteet, valvontakamerat, uima-altaat ja koko joukko muita asioita. Joten ainakin varmista, että älylaitteesi vaatii salasanan ennen kuin sitä voi käyttää. Ja pidä huolta, että se salasana ei ole oletussalasana.

Älylaitteiden ostaminen

Tämä saattaa kuulostaa hieman oudolta, mutta kun olet ostamassa älytuotetta, harkitse, tarvitseeko sen olla lainkaan yhteydessä internetiin. Esimerkiksi valvontakameran on varmaan hyvä olla internetiin yhteydessä. Muiden laitteiden, kuten leivänpaahtimien, pesukoneiden ja sen sellaisten, ei välttämättä tarvitse olla lainkaan internetiin yhteydessä. Jos pystyt löytämään tuotteen, jossa ei ole internet-yhteyttä, valitse se.

Tässä tilanteessa kannattaa vertailla hyötyjä ja haittoja: kuinka paljon siitä on hyötyä, että pystyt käyttämään kotona olevaa laitetta myös ollessasi kodin ulkopuolella ja toisaalta, kuinka paljon haittaa siitä voi olla, jos joku pystyy kirjautumaan laitteellesi joko arvaamalla salasanasi tai löytämällä laitteesta jonkun muun haavoittuvuuden.

On tärkeää myös miettiä sitä, kuinka tietoturvallinen laite on, kuinka paljon valmistaja on uhrannut aikaa sen puolen kehittämiseen. Voit etsiä internetistä laitteen tietoturvaan liittyviä arvioita. Ja kun ostat älylaitetta, kysy myyjältä sen tietoturvasta. Kaksi tärkeää kysymystä ovat:

1. Voitko vaihtaa laitteen oletussalasanan?
2. Saako laite suojauspäivityksiä?

Ja kun sinulla on uusi älylaite, *aloita sen käyttö vaihtamalla oletussalasana.*

Sen lisäksi että olet huolellinen, kun ostat älytuotteita, voi lisätä tietoturvaa entisestään käyttämällä kaupoista saatavia tuotteita. Esimerkiksi on olemassa

reitittimiä, jotka tuovat taloosi internet-yhteyden (kuten niiden kuuluukin tehdä), mutta sen lisäksi ne tekevät älylaitteista aiempaa turvallisempia tutkimalla laitteesta lähtevää ja siihen tulevaa internet-liikennettä ja päättelemällä, mikä liikenne saa liikkua ja mikä ei.

4. Vakoiluohjelmat

Vakoiluohjelmien tarkoituksena on päästää joku etäkäyttämään laitettasi ilman, että huomaat sitä. Yleisnimi tällaisille ohjelmille on etäältä ohjattava troijalainen, ja siitä käytetään usein lyhennystä RAT (engl. Remote Access Trojan). Mutta tässä oppaassa käsittelemme erityisesti ohjelmia, joita kutsutaan vainoamisohjelmiksi (engl. stalkerware), vakoiluohjelmiksi (engl. spyware) ja englannkinkielellä spouseware (spouse = puoliso). Me käytämme termiä vainoamisohjelma.

Jotkut vainoamisohjelmat on tehty nimenomaan vainoamista varten ja pitämään jotakuta ihmistä silmällä ilman, että hän huomaa sitä. Mutta on olemassa myös joukko samankaltaisia ohjelmia, joiden tarkoitus (ainakin periaatteessa) on auttaa ihmisiä seuraamaan omia lapsiaan, rakkaitaan tai työntekijöitään.

Näiden kahden ero ei ole niin selkeä kuin mitä sitä ajattelisi tai haluaisi. Ohjelmia, joita markkinoidaan huolestuneille vanhemmille, voidaan myös käyttää partnerin seuraamiseen. Lisäksi olemme löytäneet ohjelmia, joiden kotisivuilta löytyy ohjeet siitä, miten ohjelman voi piilottaa puhelimeen siten, että puhelimen omistaja ei huomaa sitä ollenkaan asennetun.

Mitä vainoamisohjelma voi tehdä?

Jos ex-kumppanisi pääsee asentamaan tällaisen ohjelman tietokoneellesi, hän voi päästä käsiksi tiedostoihin ja dokumentteihin, nähdä millä sivuilla olet käynyt internetissä, nähdä tallennetut salasanasi kuin myös muuttaa laitteesi asetuksia, jos niitä ei suojaa salasana tai salasana on helposti arvattavissa.

Jos vainoamisohjelma on asennettu puhelimeesi, exäsi voi päästä käsiksi valokuviisi, tekstiviesteihisi, sähköpostiisi, soittohistoriaasi, yhteystietoihisi, puhelimesi kameraan ja äänitallennuksiin sekä paikannukseen, joka kertoo, missä puhelimesi eli sinä olet.

Mistä ex-kumppanisi ostaisi vainoamis-ohjelman, ja kuinka sellainen asennetaan puhelimeen?

Suurin osa kovan luokan vainoamisohjelmista myydään näiden ohjelman-tekijöiden omilta sivustoilta. Tuollaiset ohjelmat kykenevät piiloutumaan laitteessa ja nuuskimaan monia asioita. Niitä ei pitäisi pystyä ostamaan virallisista kaupoista kuten App Store -kauppa (iOS) tai Google Play Kauppa

(Android). Joskus sellaisia ohjelmia noistakin paikoista löytää, ennen kuin joku raportoi niistä ja ne poistetaan kaupasta.

Joka tapauksessa iOS- ja Android-kaupoissa on paljon sellaisia appeja, joissa on joitakin samoja ominaisuuksia kuin vainoamisohjelmissa. Esimerkiksi ne voivat nähdä puhelimen sijainnin, mutta ne mainostavat itseään ohjelmina, joita käytetään sallittuihin tarkoituksiin, kuten iäkkään, muistisairaan vanhemman seuraamiseen. Tällaisia ohjelmia voi ladata virallisesta App Store -kaupasta (iOS) ja Google Play Kaupasta (Android).

Teknisesti on mahdollista tehdä vainoamisohjelma, jonka voi asentaa ilman että pääsee fyysisesti puhelimeen käsiksi. Näin voi tehdä esimerkiksi siten, että lähettää käyttäjälle linkin ladattavaan tiedostoon ja huijaa häntä luulemaan, että lataus on harmiton. Tällaiset tapaukset ovat ilmeisesti kuitenkin vähemmistössä. Yleensä vainoamisohjelma ladataan suoraan käyttäjän puhelimeen silloin, kun hyökkääjä pääsee siihen käsiksi. Eli todennäköisin vaihtoehto on, että exäsi pyrkii asentamaan vainoamisohjelman puhelimeesi silloin, kun hän pääsee siihen fyysisesti käsiksi.

Vainoamisohjelman löytäminen puhelimesta

On laitonta asentaa vainoamissovelluksia puhelimeesi ilman lupaasi. Jos sinulla on syytä uskoa entisen kumppanisi asentaneen tällaisen ohjelman puhelimeesi, ja jos se on turvallista tehdä, niin vie puhelin poliisille. Ennen kuin viet sen poliisille, aseta puhelin lentokonetilaan, jotta se ei ole liitetty internetiin. Lisäturvallisuuden vuoksi voit myös sammuttaa puhelimen tai asettaa sen radiosignaaleja täydellisesti vaimentavaan Faradayn pussiin, jos sinulla on sellainen. Tällä tavoin entinen kumppanisi ei näe sinun menevän poliisin pakeille. Ja jos vainoamisohjelmassa on jonkinlainen etäyhteyden kautta käytettävä poistotoiminto, silloin entisen kumppanisi tulisi myös olla mahdotonta käyttää sitä, jos puhelimesi ei pysty muodostamaan yhteyttä internetiin.

Mutta kuinka edes tiedät, että puhelimeesi on asennettu vainoamisohjelma? Valitettavasti virustentorjuntaohjelmat eivät aina löydä vainoamisohjelmia. Ja vaikka löytäisivätkin, ne eivät aina pidä niitä vaarallisina. Eva Gaupin, joka edustaa Electronic Freedom Foundation -nimistä säätiötä, on yksi niistä, jotka pyrkivät muuttamaan tätä tilannetta. Hän haluaa, että useammat virustentorjuntaohjelmat löytäisivät vainoamisohjelmat ja varoittaisivat niistä. Koska näin ei kuitenkaan nyt ole asianlaita, käyttäjien pitää olla erityisen varuillaan.

Vaikka virustentorjuntaohjelmat eivät ole täydellisiä, on kuitenkin hyvä idea skannata niillä puhelimesi, jos sellainen on käytössäsi. Katso tarkkaan kaikki

löydökset, jos niissä on mitään yllätyksiä tai edes hiukan kyseenalaisia löytöjä. Kuten todettua, vaikka virustentorjuntaohjelma löytää vainoamisohjelman, se ei välttämättä pidä sitä vaarallisena. Jos virustentorjuntaohjelma löytää ohjelman, jota et tunne, tarkista internetistä, mikä tuo ohjelma on ja mitä se tekee.

Voit löytää vainoamisohjelman puhelimestasi seuraavalla tavalla:

- Asennetut ohjelmat löytyvät puhelimesi asetuksista. Android-laitteissa kaikki appit on listattu allekkain. Sen sijaan iOS-laitteissa vieritä sivun alalaitaan: viimeinen listaus on kolmannen osapuolen ohjelmat, jotka eivät kuulu iOS:ään oletusasennuksena.

- Käy appit läpi yksi kerrallaan. Jos löydät jonkun tuntemattoman appin, se ei välttämättä ole vainoamisohjelma, mutta voi olla sellainen. Tarkista internetistä, mikä appi on kyseessä ja mihin sitä käytetään.

- Jos löydät appin, joka vaikuttaa vainoamisohjelmalta, ota siitä kuvakaappaus tai kirjoita sen nimi muistiin. Kuten sanottua, suosittelemme, että viet puhelimen poliisille. Mutta jos se ei ole mahdollista tai et halua poliisia tilanteeseen mukaan, voit poistaa appin, jos sinun ei tarvitse pelätä exäsi suuttuvan asiasta, jos hän huomaa sinun poistaneen appin. Sen jälkeen kun olet poistanut vainoamisohjelman, päivitä laitteesi. Jos haluat olla erityisen huolellinen, palauta puhelimeen tehdasasetukset.

Muita neuvoja:

- Tehdasasetusten palautus poistaa kaikki tiedostot, myös kuvat. Kopioi ensin kaikki se, minkä haluat säilyttää toiselle laitteelle tai tallennus-paikkaan ennen kuin palautat tehdasasetukset.

- Useimmat vainoamisohjelmat kuluttavat paljon akkua, koska ne ovat taustalla jatkuvasti toiminnassa, esimerkiksi paikallistavat puhelinta. Joten tarkkaile akkusi kestoa, se voi antaa sinulle vihjeen, että jotain epäilyttävää on käynnissä.

- Katso, onko Android-laitteessasi ruksattu käyttöön “Tuntemattomat lähteet” tai “Tuntemattomien sovellusten asentaminen” (Esimerkiksi: Asetukset -> Sovellukset ja ilmoitukset -> Lisätiedot -> Sovellusten erikoiskäyttö -> Tuntemattomien sovellusten asentaminen). Tämä asetus sallii appien lataamisen Googlen virallisen kaupan ulkopuolelta, joka tarkoittaa, että ne *ohiladataan* laitteelle. Vainoamisohjelma on todennäköisimmin ohiladattu suoraan internetistä apk-tiedostoina ja asennettu suoraan laitteelle. Tämä asetus on yleensä Android-laitteissa “Ei käytössä” ja voit ottaa sen pois käytöstä, jos se on käytössä.

Jailbreikkaaminen (iOS) ja roottaaminen (Android)

Puhelimen jailbreikkaaminen tai roottaamnen tarkoittaa sitä, että puhelinta on muutettu antamaan käyttäjälle lisää valtuuksia – hän voi tehdä puhelimellaan enemmän – kun hän pystyisi normaalilla puhelimella. Puhelimen jailbreikkaaminen tai roottaaminen antaa ex-kumppanillesi mahdollisuuden asentaa vainoamisohjelmia tai tehdä vainoamisohjelmasta vaikeammin löydettävän ja poistettavan.

Nämä kaksi termiä tarkoittavat samaa asiaa. Jailbreikkaaminen koskee iOS-laitteita (iPhonet ja iPadit), kun taas roottaaminen koskee Andoideja. Tutustutaan näihin kahteen erikseen.

Jailbreikattu iOS

A Jailbreikatussa laitteessa sitä on käsitelty siten, että käyttäjällä on laajemmat käyttöoikeudet laitteeseen kuin normaaliin iOS-laitteeseen. Sen takia on mahdollista tehdä asioita, joita ei normaalisti voisi tehdä, kuten nähdä dataa siitä, missä paikoissa laite on ollut. On myös mahdollista piilottaa appien ikoneita, kuten esimerkiksi vainoamisohjelman ikoni. Ja jailbreikattuun puhelimeen voi olla mahdollista asentaa vainoamisohjelmia, joita on erityisen vaikeaa poistaa.

Useimmat iOS-vainoamisohjelmat tarvitsevat jailbreikatun laitteen, jotta ne voidaan asentaa. Ja kun ohjelma on laitteessa, se voidaan piilottaa hyvin. Voi olla, ettet löytäisi sitä, kun tutkisit laitetta käyttöliittymän kautta.

Vaikka et ole itse jailbreikannut laitettasi, joku muu on saattanut tehdä sen, jos hän on päässyt puhelimeesi käsiksi. On hankalaa varmistaa, onko iOS-laite jailbreikattu. On olemassa kuitenkin ilmeisiä merkkejä siitä, kuten tiettyjen ohjelmien esiintyminen laitteessa.

- Etsi Cydia-nimistä appia. Tämä ohjelma on appikauppa, josta löytyy jailbreikatulle laitteelle asennettavia ulkoisia appeja. Cydian löytyminen on varma merkki jailbreikatusta laitteesta.
- Koita päivittää iPhone-puhelimesi. Jos päivitys ei onnistu tai se jumittaa, puhelin saattaa olla jailbreikattu, koska iPhone-puhelinten päivitykset eivät aina asennu puhelimissa, joita on peukaloitu.
- Käytä iTunesia tai iPhonea palauttaaksesi puhelimen tehdasasetukset. Tämän poistaa useimmissa tapauksissa vainoamisohjelmat puhelimestasi.

Huom! Jos laitteesi on jailbreikattu, huonoja uutisia tulee lisää, koska silloin yleensä iPhonesi takuu ei ole enää voimassa.

Rootattu Android

Rootattu Android-laite antaa sovelluksille pääsyn laitteen rajoitettuihin ominaisuuksiin ja yksityisiin tietoalueisiin. Tämä tarkoittaa sitä, että ex-kumppanisi saattaa päästä käsiksi wifin salasanaan, laitteen toimintoihin kuten kameraan ja mikrofoniin sekä puhelimeesi tallennettuihin tietoihin. Rootatusta laitteesta voi myös olla vaikeampaa poistaa syvälle piilotettuja vainoamis-ohjelmia.

Monet kaikista pahimmista vainoamisohjelmista vaativat rootatun Android-laitteen. Laitteen käyttöliittymän silmämääräinen tarkistaminen ei sellaisenaan välttämättä paljasta vainoamisohjelmien olemassaoloa.

- Tarkista, onko Kinguser- tai Superuser-nimisiä sovelluksia puhelimessasi. Nämä sovellukset asennetaan, kun laite rootataan, ja ne ovat varma merkki siitä, että Android-laite on rootattu.
- Yritä päivittää Android-laitetta, jos epäilet sen olevan rootatun. Jos lataaminen epäonnistuu, laite saattaa olla rootattu.
- On suositeltavaa suorittaa tehdasasetusten palauttaminen puhelimen sovellusten ja tietojen nollaamiseksi. Joidenkin vainoamisohjelmien on aiemmin ilmoitettu selviävän jopa tehdasasetusten palauttamisesta. Tarkkaile, jos vainoamisohjelmista löytyisi edelleen merkkejä.

Huom! Kuten iOS-laitteissa, useimmissa tapauksissa rootatun Android-laitteen takuu raukeaa.

5. Vakoilulaitteet

Termi “ohjelmisto” viittaa sovelluksiin tai appeihin. “Laitteisto” tarkoittaa fyysistä asiaa. Puhelimesi on laitteisto, puhelimesi appit ovat ohjelmistoja. Joten vakoilulaitteisto tarkoittaa käytännössä vain laitteita, jotka on suunniteltu vakoilemaan henkilöitä.

Jos olet koskaan nähnyt Bond-elokuvan, tiedät, että on olemassa paljon sellaisia laitteita, joita voitaisiin käyttää jonkun vakoilemiseen. Mutta James Bond on mielikuvituksen tuote. Oikeassa elämässä sellaisten vakoilulaitteiden, jotka ovat helposti saatavissa verkosta, luettelo on onneksi paljon rajoitetumpi. Ja juuri sellaisiin helposti verkosta hankittaviin laitteisiin keskitymme tässä osiossa. Tarkemmin sanoen katamme GPS-paikantimet sekä piilotetut videokamerat ja salakuuntelulaitteet. Keskustelemme lyhyesti myös drooneista, mutta lähinnä sen takia, että kerromme, miksi droonit eivät todennäköisesti ole suuri riski useimmille ihmisille.

Yksi tärkeä asia vakoilulaitteiden ymmärtämisessä on ero aktiivisten ja passiivisten laitteiden välillä. Aloitetaan siitä ja siirrytään sitten keskustelemaan erilaisista laitteista.

Aktiiviset ja passiiviset vakoilulaitteet

Vakoilua varten suunnitellut laitteet voivat olla joko aktiivisia tai passiivisia. Aktiivinen tarkoittaa, että se voi välittää keräämäänsä tietoa. Passiivinen tarkoittaa, että se ei voi tehdä niin. Esimerkiksi internetiin kytketty videokamera on aktiivinen laite. Se pystyy lähettämään tallentamaansa videokuvaa internetin välityksellä laitetta hallitsevalle henkilölle. Videokamera, jota ei ole kytketty internetiin (ja jolla ei ole muuta tapaa siirtää tietoja), on passiivinen laite. Sen sijaan että se lähettää videostriimiä internetin kautta, se vain tallentaa kerätyt tiedot paikallisesti omaan muistiin.

Tämä ero aktiivisen ja passiivisen välillä on merkittävä. Se vaikuttaa sekä laitteen käyttäjän vaihtoehtoihin että meidän vaihtoehtoihimme, miten voimme yrittää löytää tällaisen laitteen.

- **Mitä tulee vaihtoehtoihin ja rajoituksiin, jotka koskevat vainoajaa:** jos joku on asentanut passiivisen laitteen, esimerkiksi GPS-paikantimen autoosi, hänen on päästävä fyysisesti käsiksi autoosi, jotta hän pääsee näkemään kerätyt tiedot. Jos hän on asentanut aktiivisen GPS-paikantimen autoosi, hänellä on pääsy tietoihin internetin välityksellä ilman, että hän joutuu käymään laitteella fyysisesti.

- **Mitä tulee vaihtoehtoihisi löytää laite:** Jotta voit löytää passiivisen laitteen, sinun täytyy löytää itse fyysinen laite. Myös aktiivinen laite voidaan löytää etsimällä itse laite. Fyysisen laitteen etsimisen lisäksi voidaan kuitenkin etsiä myös merkkejä siitä, että dataa siirtyy. Tämä ei kerro sinulle tarkalleen, missä laite on (tai edes millainen laite se on), mutta se voi antaa meille varoituksen siitä, että joku piilotettu laite lähettää tietoja.

  Se että etsitään merkkejä datan siirtymisestä, saattaa kuulostaa hiukan tekniseltä. Ja se on – ainakin vähän. Se vaatii myös jonkin verran lisälaitteita. Emme kata sitä tässä oppaassa, vaan käsittelemme sen sijaan joitain tapoja etsiä vakoilulaitteistoja. Ne tavat eivät vaadi erityisiä laitteita tai taustatietoja. Mutta nyt on aika siirtyä keskustelemaan itse laitteista. Ne voivat kaikki olla joko aktiivisia tai passiivisia.

GPS-paikantimet

Ei ole olemassa tarkkaa tietoa siitä, kuinka yleistä on, että joku käyttää GPS-paikanninta ex-kumppaninsa seuraamiseen. Suomessa kerrottiin tammikuussa 2020 eräästä kaverista, joka oli piilottanut GPS-paikantimen ex-kumppaninsa autoon, mutta sellaiset uutiset ovat harvinaisia ainakin Suomessa. Ei kuitenkaan voida tietää, kuinka paljon tai vähän GPS-paikantimia *jää löytymättä*. Yhden asian kuitenkin tiedämme. Lähes joka kerta kun puhumme digitaalisen vainon tai väärinkäytön uhrien kanssa, he kysyvät GPS-paikantimista. Jollei muuta niin toivottavasti paikantimista kertominen tässä kaikottaa kaikki pelot, jotka voivat johtua siitä, ettei paikantimien vahvuuksia eikä ennen kaikkea niiden rajoituksia ymmärretä.

Ennen kuin tutustumme paikantimien yksityiskohtiin, puhutaanpa hyvin lyhyesti siitä, mitä hemmettiä GPS tarkoittaa, ja mitä se tekee. GPS tarkoittaa maailmanlaajuista paikallistamisjärjestelmää (Global Positioning System). Periaatteessa GPS kertoo sinulle, missä olet. Se tekee tämän ottamalla yhteyden satelliitteihin, jotka kiertävät maapalloa. GPS:ää käytetään melko laajasti. Älypuhelimet ovat usein käytetty esimerkki laitteesta, josta saatat löytää GPS:n toiminnassa. Puhelimesi käyttää sisäänrakennettua GPS:ää, kun se esimerkiksi osoittaa sijaintisi kartalla.

On olemassa tapoja, joilla ex-kumppanisi voi käyttää puhelimesi GPS:ää sinun seuraamiseesi. Hän voi esimerkiksi asentaa puhelimeesi vainoamisohjelman tai päästä Google hallintapaneeliisi käsiksi, jos sinulla on se asetettuna niin, että se tallentaa sijaintisi. Exäsi voisi myös käyttää autoosi piilotettua puhelinta, jolla seurata sinua. Tässä osiossa keskitymme kuitenkin GPS-paikantimiin – laitteisiin, jotka ovat nimenomaan suunniteltu seuraamiseen.

Tuossa oli GPS:n perusteet. Seuraavaksi tarkastellaanpa lähemmin joitain GPS-paikantimien ominaisuuksia ja rajoituksia.

Mitä GPS-paikannin voi tallentaa?

GPS-paikantimia on saatavana monia erilaisia. Vaikka ne kaikki voivat tallentaa sijaintitietoja, useat niistä voivat tehdä myös paljon enemmän. Esimerkiksi autoon suunniteltu GPS-paikannin voisi tarjota täydellisen kartan kaikista käymistäsi paikoista, mitä reittejä käytit niihin paikkoihin päästäksesi, mihin aikaan ajoit ja jopa kuinka nopeasti ajoit.

Aktiiviset GPS-paikantimet, ne, jotka voivat välittää tietoja laitteen asentaneelle henkilölle, voidaan myös asettaa lähettämään hälytyksiä. Yksi erityinen hälytyslaji, josta on oltava tietoinen, on nimeltään geoaitaaminen. Tämän avulla henkilö voi asettaa kartalla “aidan” maantieteellisen alueen ympärille, ja pyytää sitten GPS-paikanninta lähettämään hälytys, jos auto poistuu kyseiseltä alueelta. Joten jos entinen kumppanisi olisi tietoinen tavanomaisista ajoreiteistäsi (kauppaan, töihin, harrastuksiin), niin hän voisi perustaa geoaidan aloittaen tuon alueen ulkopuolelta. Sitten entinen kumppanisi saisi hälytyksen aina, kun ajat minne tahansa normaalin reittisi ulkopuolelle.

Kuinka pitkään GPS-paikannin voi tallentaa?

Periaatteessa GPS-paikannin voi tallentaa niin pitkään kuin siinä riittää tallennustilaa ja akussa virtaa. Tallennetun datan määrä (data siitä, mihin olet ajanut, milloin, kuinka kovaa jne.) riippuu siitä, millainen laite on kyseessä. Passiiviset laitteet, jotka tallentavat tietoja vain omalle kiintolevylleen, voivat tallentaa vain niin paljon kuin laitteen sisäiseen tallennustilaan mahtuu. Nykyään kuitenkin jopa pieni USB-tikku, kuten sellainen, jonka voit kiinnittää avainketjuusi, voi tallentaa valtavia määriä tietoja. Joten käytännössä todellinen rajoitus on todennäköisesti virransaanti.

Jos GPS saa virtaa autostasi, se toimii niin kauan kuin se pystyy lataamaan itsensä autostasi. Jos sitä ei ole kytketty auton virtalähteeseen, se tarvitsee oman akun. Ja tämä akku, kuten älypuhelimen akku, on ladattava aina silloin tällöin. Se tarkoittaa, että ex-kumppanisi on fyysisesti käytävä autossasi, jotta hän pääsee lataamaan GPS:ää. Yleisimpien GPS-paikantimien akkukestot vaihtelevat kahdesta päivästä hiukan yli kahteen viikkoon. Mutta GPS-paikantimet, joissa on suuret ulkoiset akut, toimivat jopa kuusi kuukautta lataamatta.

Kuinka joku voi käyttää GPS-paikantimen tietoja?

Vastaus juontaa juurensa keskusteluun aktiivisista tai passiivisista laitteista. Jos joku piilottaa passiivisen GPS-paikantimen autoosi, hänen on päästävä laittee-

seen käsiksi, jotta voi nähdä siihen tallennetut tiedot. Jos joku piilottaa aktiivisen GPS-paikantimen autoosi, hän voi käyttää sen tietoja etänä. Tämä tapahtuu yleensä sovelluksen tai verkkosivuston kautta.

Mihin kohtaan autoa GPS-paikannin piilotetaan?

GPS-paikannin voidaan piilottaa autoon eri tavoin. Avaintekijä on se, pääseekö kyseinen henkilö auton sisäpuolelle.

- **Auton ulkopuolelle:** Jos hän ei pääse autoon, yksinkertaisin vaihtoehto on, että GPS-paikannin asetetaan magneettikoteloon. Tämä magneettikotelo voidaan sitten kiinnittää mihin tahansa auton magneettiseen pintaan. Jotta sen löytäminen olisi vaikeampaa, se piilotetaan todennäköisesti jonnekin auton alle eikä mihinkään näkyvään paikkaan.
- **Auton sisäpuolelle:** Jos ex-kumppanillasi on pääsy autoosi, hänellä on joitain vaihtoehtoja. Yksi vaihtoehto on piilottaa GPS-paikannin (tai matkapuhelin) mihin tahansa sopivaan paikkaan: istuimen alle, hansikaslokeroon tai käyttämällä magneettirasiaa, kuten edellä kuvattiin. Jos hän haluaa kuitenkin jatkuvan virransyötön GPS-laitteelle, hänen on kytkettävä se autosi virtalähteeseen.

Jotkut GPS-paikantimet on suunniteltu kytkettäviksi autoosi sisäänrakennettuun itsediagnostiikan (OBD) liittimeen. Vanhempien mallien autoissa OBD-liitin saattaa sijaita auton konepellin alla. Vuoden 2000 tienoilta autoissa on käytetty OBD-II-diagnostiikkaliittimiä. Niiden on oltava kuljettajan ulottuvilla, ja ne sijaitsevat yleensä kojelaudan alla.

Toinen vaihtoehto on kytkeä paikannin auton akkuun. Joka tapauksessa mikä tahansa paikka, josta laite saa virtaa, kelpaa – aiemmin mainitsemassamme tapauksessa Suomessa GPS-paikannin oli piilotettu ajovaloumpioon.

Löytääksesi GPS-paikantimen autosta, etsi mitä tahansa autoon kuulumatonta. Jos tunnet autot hyvin, voit etsiä myös auton johtoihin kytkettyjä asioita, joiden ei ole tarkoitus olla siellä. Jos et tunne autoja hyvin, kysy ystävältäsi tai korjaamolta apua. Korjaamot pystyvät nostamaan auton ylös ja katsomaan auton alle. Jos löydät GPS-paikantimen tai minkä tahansa vakoilulaitteen autostasi tai kodistasi, ilmoita siitä poliisille.

Jos olet huolissasi GPS-seurannan mahdollisuudesta – ja tarkemmin sanottuna *aktiivisesta* GPS-paikantimesta – voit myös etsiä paikantimen lähettämää signaalia. Tämä on kuitenkin teknisempi menetelmä, joka ei kuulu tähän oppaaseen.

Miltä GPS-paikantimet näyttävät?

GPS-paikantimet ovat yleensä varsin pieniä, sellaisia puhelimen latauslaitteen kokoisia (johdolla tai ilman). Jos kirjoitat Amazonin, eBayn tai vastaavan verkkosivuston hakukenttään “GPS tracker”, löydät useita eri laitteita. Joissakin on magneetti, jotta ne voidaan kiinnittää auton alle. Joissakin on liitin tai johto, jotta ne voivat ottaa auton OBD-liittimestä tai akusta virtaa.

Joitakin muita tapoja seurata autoa

Uudemmissa autoissa on yleensä navigointijärjestelmä, joka voi tallentaa sen, missä auto on ollut. Jos sinulla on tällainen auto, tarkista sen asetukset nähdäksesi, mitä se tallentaa ja miten tietoihin pääsee käsiksi sekä tee tarvittavat muutokset.

Autoissa voi olla kojelautakameroita, jotka kuvaavat videota auton ollessa liikkeessä. Kojelautakamera seuraa myös yleensä, missä auto on ollut. Jotkut kojelautakamerat voivat myös siirtää nämä tiedot suoraan pilveen. Jos sinulla on kojelautakamera, tarkista sen asetukset nähdäksesi, mitä tietoja se kerää, kuinka se tallentaa sen ja kuinka joku voi päästä siihen käsiksi. Jos esimerkiksi haluat tallentaa kojelautakameran tiedot pilveen, varmista, että siihen käytetty tili on suojattu salasanalla ja vahvalla sellaisella tietenkin.

Voi olla myös muita tapoja, joilla autoasi voidaan seurata. Esimerkiksi ostoskeskusten tai tapahtumapaikkojen pysäköintihalleissa voi olla kamera, joka lukee saapuvien autojen rekisterikilpiä. Näiden paikkojen appit voivat ilmoittaa sinulle – tai kenelle tahansa, jolla on rekisterinumerosi heidän sovelluksessaan – kun saavut ja lähdet pois tuosta pysäköintihallista.

Piilokamerat

Piilokameroita asennetaan erilaisiin jokapäiväisiin laitteisiin. Jotkut kaupat myyvät videokameroita, joita ovat piilotettu muun muassa herätyskelloihin, puhelinlatureihin, DVD-soittimiin, täytettyihin leluihin ja jopa pistorasioihin.

Jotkut kamerat pystyvät tunnistamaan liikettä. Silloin ne tallentavat vain, kun alueella tapahtuu liikettä, ja se säästää tallennustilaa. Riippuu mukana tulevan tallennustilan koosta, kuinka paljon videota ne voivat tallentaa. Esimerkiksi yksi valmistaja kertoo, että heidän tuotteellaan on 32 Gt tallennustilaa, mikä mahdollistaa yhteensä noin 200 tuntia tallennettua videota.

Kuten GPS-paikantimissa, piilokamerat voivat olla joko aktiivisia tai passiivisia. Aktiivinen kamera tarvitsee internet-yhteyden. Yleensä ne yhdistyvät langattomaan verkkoon sen sijaan, että niillä olisi omaa internet-yhteyttä sisäänraken-

netun SIM-kortin kautta. Tämä tarkoittaa, että kameran on päästävä yhdistymään lähellä sijaitsevaan langattomaan verkkoon.

Jos asut kotona, jonka olet aiemmin jakanut entisen kumppanisi kanssa, niin voi olla, että aktiivinen piilotettu laite on kytketty kotisi internet-yhteyteen. Yksinkertainen tapa poistaa aktiiviset vakoilulaitteet (joko kamera tai mikrofoni) on vaihtaa kodin internet-yhteyden salasana. Tällä tavoin kaikkien internet-yhteyden tarvitsevien laitteiden on annettava salasana uudestaan, jotta internetin käyttö olisi taas mahdollista.

Sivuhuomautuksena voidaan sanoa, että sekä videota että ääntä tallentavia valvontalaitteita ei yleensä saa lain mukaan myydä. Valitettavasti niitä ei kuitenkaan ole kovinkaan vaikeaa löytää.

Piilokameran löytäminen

Yksi yhteinen asia kaikissa piilokameroissa on se, että ne tarvitsevat objektiivin, jonka kautta kamera voi kuvata. Joten helpoin tapa etsiä piilokameraa on etsiä objektiivia. Tarkemmin sanottuna etsiä objektiivista heijastuvaa valoa. Perusajatus on sama kuin jos osoittaisit valolla peiliin tai ikkunaan: näet siitä takaisin heijastuvan valon.

Tätä tarkoitusta varten on saatavana erityisiä laitteita (tai taskulamppuja), samoin kuin sovelluksia, joita voit ladata tätä tarkoitusta varten. Voit kuitenkin kokeilla sitä myös tavallisella taskulampulla tai muulla käytettävissä olevalla valonlähteellä. Sammuta kodin valot ja kohdista sitten valoa ympäriinsä ja koita nähdä, jos jostain yllättävästä paikasta heijastuu valoa. Objektiivit ovat todella pieniä, yhtä pieniä kuin kännykkäsi objektiivi, joten etsi varsin pientä heijastusta.

Kuten muissa aktiivisissa laitteissa, voit myös etsiä sen lähettämiä signaaleja. Jos kyseessä on aktiivinen kamera, joka on kytketty wifi-verkkoosi, voit tutkia verkkoon kytkettyjä laitteita nähdäksesi, löytyykö laitteita, joita et tunnista. Saatavilla on ohjelmia, joiden avulla voit nähdä, mitkä laitteet on kytketty wifi-verkkoosi. Tämä voidaan yleensä tehdä myös reitittimen web-käyttöliittymän kautta (katso lisätietoja reitittimen mukana toimitetuista ohjeista).

Jos haluat vain heti päästä eroon verkossasi olevista epäilyttävistä laitteista, voit tehdä sen nopeasti ja helposti vaihtamalla internetin eli reitittimesi salasanan. Mutta jos haluat tutkia reititintäsi, löytyykö sieltä joitain ei-toivottuja laitteita, sinun pitää tehdä se ennen kuin vaihdat salasanan, koska muuten ne laitteet poistetaan heti verkostasi. Reitittimen ei-toivotut laitteet voi tarkistaa sen verkkosivustolta, katso reitittimen ohjeista laitteen verkko-osoite.

Jos todella löydät piilokameran tai minkä tahansa muun vakoilulaitteen, niin ole yhteydessä poliisiin.

Salakuuntelulaitteet

Aivan kuten kamerat, mikrofonit voidaan piilottaa arkipäiväisiin tuotteisiin, kuten kyniin, pinsseihin ja nappeihin. Kuten kameroissa ja GPS-paikantimissa, on olemassa sekä aktiivisia että passiivisia salakuuntelulaitteita sekä näiden sekoituksia. Toisin sanoen on olemassa mikrofoneja, jotka siirtävät ääntä internetin yli, tallentavat ääntä laitteelle tai tekevät noita molempia. Ääni vaatii vähemmän tallennustilaa kuin video, joten passiivinen mikrofoni voi tallentaa yleensä pidempään kuin kamera.

Salakuuntelulaitteen löytäminen

Kuten GPS-paikantimissa ja kameroissa, passiivinen mikrofoni vaatii itse laitteen löytämistä. Aktiivinen mikrofoni voidaan havaita, kun se lähettää dataa. Se antaa sinulle kuitenkin vain vihjeen laitteen olemassaolosta, eikä kerro tarkalleen missä se on.

Aktiivinen mikrofoni käyttää todennäköisesti lähellä olevaa wifiä internet-yhteyden muodostamiseen. Helppo tapa poistaa piilotettujen salakuuntelu-laitteiden pelkoa on vaihtaa internetin eli reitittimesi salasana. Voit myös tutkia, mitä laitteita on kytketty kotisi internetiin (reitittimeesi) nähdäksesi, onko laitteita, joita et tunnista. Jos löydät piilotetun mikrofonin (tai minkä tahansa vakoilulaitteiston), ota yhteyttä poliisiin.

Kokemuksemme perusteella piilotetut salakuuntelulaitteet ja kamerat eivät ole yhtä yleisiä kuin GPS-paikantimet. Jos kuitenkin olet huolissasi siitä, että joku tallentaa keskustelujasi, yleisesti suositeltu temppu potentiaalisten sala-kuuntelijoiden elämän vaikeuttamiseksi on käyttää taustamelua. Joskus tätä taustamelua kutsutaan “valkoiseksi” kohinaksi. Tämä viittaa sellaiseen taustameluun, jonka tarkoituksena on tehdä salakuuntelu erityisen vaikeaksi. Se tarkoittaa käytännössä sitä, että soitat jotain muuta taustalla – se voi olla musiikkia, aaltojen kohinaa jne. Tämä tekee salakuuntelijalle vaikeammaksi kuulla, mitä sanot.

Lyhyt huomautus droonien käytöstä sinun seuraamiseksesi

Joskus ihmiset kysyvät, voiko entinen kumppani käyttää droonia seuratakseen liikkuvaa pakettiautoa, jotta hän näkee, mihin ihminen on muuttamassa. Teoriassa droonia voitaisiin käyttää seuraamaan sinua tai autoasi. Mutta on olemassa teknisiä rajoituksia, joiden takia seuraaminen on erittäin vaikeaa. Niistä tärkein on akun käyttöikä – kuinka kauan drooni voi lentää ennen kuin sitä tarvitsee ladata.

Pienissä droneissa on akkuja, joita täytyy ladata muutamien minuuttien käytön jälkeen. Mitä isompi akku, sitä suurempi droonin pitää oltava, jotta se jaksaa kantaa isoa akkua. Mutta jopa markkinoiden kalleimpien droonien lentoaika on paljon alle tunnin. On drooneja, jotka voivat lentää useita tunteja, mutta ne ovat armeijan drooneja, ja niiden siipien kärkiväli on vähintään auton kokoluokkaa.

Jos joku haluaa seurata sinua droonilla, hänellä on toinenkin huolenaihe, nimittäin etäisyys, jolta hän voi hallita droonia. Jotta droonia voi ohjata, hänen on oltava sen käyttöetäisyydellä. Akun käyttöiän tavoin droonien käyttöetäisyys vaihtelee. Halpoja malleja ei voi käyttää kuin enintään muutaman sadan metrin päästä. Kalliimpien mallien käyttöetäisyys voi olla yli 15 kilometriä. Mutta ellet liiku kuin vain lyhyen matkaa, droonia hallitsevan henkilön on silti oltava omassa autossaan varsin lähellä sinua, jotta hän voi ohjata droonia.

6. Jos ex-kumppanisi on epätavallisen taitava teknisesti

On olemassa joitain lisätapoja, joilla exäsi voi vainota sinua, hakkeroida tilisi tai yleensä sotkea elämääsi, jos he ovat vähän enemmän tekniikkaa taitavia. Tilanne ei kuitenkaan ole niin pelottava tai musertava kuin termi “teknisesti taitava” aluksi saattaisi antaa ymmärtää. Puhumme ensisijaisesti asiasta, jonka olet jo kokenut useita kertoja aiemmin: joku yrittää saada sinut luulemaan olevansa joku muu. Tämä tehdään yleensä sen takia, että sinua huijataan napsauttamaan linkkiä tai antamaan kirjautumistietosi jollekin verkkosivustolle. Tällainen ihmisten huijaaminen verkossa on ilmiö, jota kutsutaan yleisesti tietojenkalasteluksi, mutta laajemmin se tunnetaan nimellä sosiaalinen manipulointi.

Joidenkin tietojenkalasteluhyökkäysten lisäksi käsittelemme myös yhtä toista asiaa, jota teknisesti taitava ex-kumppani voisi mahdollisesti yrittää: vakoilla sinua vakoilemalla internet-liikennettäsi. Tätä varten heidän on oltava samassa verkossa kuin sinä. Se tarkoittaa, että heillä on oltava pääsy sinun kanssasi samaan internet-yhteyteen. Tämä on todennäköisempää tilanteessa, jossa asut vielä hänen kanssaan (tilannetta käsitellään tarkemmin luvussa 7), mutta teknisesti se on myös mahdollista, jos käytät julkista wifi-yhteyttä.

Tietojenkalastelu – ja kuinka havaita huijaus-verkkosivusto

Tietojenkalastelu tarkoittaa yritystä huijata sinua antamaan arvokasta tietoa. Perinteisessä tietojenkalastelussa tämä tarkoittaa usein esimerkiksi sitä, että sinua yritetään huijata antamaan varkaille internet-tilisi sisäänkirjautumis-tiedot.

Ihmiset, jotka yrittävät huijata sinua antamaan heille arvokasta tietoa, yrittävät saada sinut ajattelemaan, että annat tiedot lailliselle henkilölle tai sivustolle. Yksi tapa on tehdä sivustosta luotettavan näköinen. Tämä tehdään yleensä luomalla sivusto, joka näyttää aidolta sisäänkirjautumissivulta. Se näyttää aivan tililtäsi, jolta he yrittävät huijata sinua antamaan sisäänkirjautumistietosi. Ja sitten he pyrkivät saamaan sinut kirjautumaan sisään sille sivustolle. Koska sivu ainoastaan näyttää todelliselta, mutta oikeasti ei ole, sisäänkirjautuessasi kirjautumistietosi lähetetään huijareille.

Miksi ex-kumppanisi tekisi näin? Kuten aiemmin mainittiin, yksi tavoite voisi olla saada sisäänkirjautumistietojasi joihinkin verkkosivustoihin. Hän voi myös

yrittää huijata sinua lataamaan haittaohjelma tietokoneellesi tai puhelimeesi. Tai huijata sinua antamaan nykyinen osoitteesi tai puhelinnumerosi.

Tietojenkalastelulta suojautumisen perusteet ovat samat kuin mitä pitää muistaa yleensäkin tällaisissa tilanteissa.

- **Tarkista verkkosivuston osoite eli URL**
  URL (Uniform Resource Locator) on verkkosivuston osoite. Tietojenkalastelusivusto voi sisältönsä puolesta näyttää täsmälleen samalta kuin oikea sivusto. Kun tarkastellaan vain sivuston sisältöä, ei ole mitään keinoa tietää, onko kyse oikeasta vai tietojenkalastelusivustosta. Tietojenkalastelusivustot eivät kuitenkaan voi väärentää verkkosivuston osoitetta eli URL-osoitetta.

  Huijarit yrittävät usein saada verkkosivuston osoitteen näyttämään viralliselta sivustolta. Tämä voidaan tehdä esimerkiksi kirjoittamalla hiukan väärin sen sivuston nimi, jota he yrittävät matkia, tai lisäämällä suositun sivuston nimen, kuten google, huijaussivuston verkko-osoitteeseen.

  Onneksi tällaiset huijaukset on helppo havaita, jos osaa etsiä niitä. Kun tarkistat verkko-osoitetta, aloita siitä, jota kutsutaan “Ylätason verkko-tunnukseksi": .com, .org ja niin edelleen. Ja siirry sitten vasemmalle. Nimi tai sana, joka on välittömästi pisteen vasemmalla puolella, on sivusto, jolla vierailet.

  Joten jos olet sivulla, jonka osoite on google.huijaussivu.com, niin – vaikka URL-osoitteessa sanotaan google, olet sivulla, joka kuuluu sivustolle huijaussivu.com. Ja vastaavasti, jos olet osoitteessa huijaussivu.google.com, niin olet Googlelle kuuluvalla sivulla.

- **Vältä klikkaamasta linkkejä**
  Yleinen tapa huijata ihmisiä on lähettää sähköposti, jossa sanotaan jotain seuraavan tapaan: “Tilisi on murrettu. Tilisi suojaamiseksi sinun on vaihdettava salasanasi.” Ja sitten on linkki, joka näyttää olevan sisäänkirjautumissivu. Kuten aiemmin todettiin, kyseessä on todennäköisesti huijaus. Jos kuitenkin mielestäsi on syytä uskoa, että kyseessä voi olla oikea sähköposti, voit välttää riskin, että kyseessä on tietojenkalasteluyritys sillä, että menet verkkosivulle suoraan eli kirjoitat osoiteriville sivun osoitteen sen sijaan, että klikkaisit linkkiä.

  Joten sanotaan vaikka, että Mikähyvänsä Oy lähettää sinulle sähköpostin, jossa sanotaan, että sinun on vaihdettava salasanasi, ja viestissä on mukana linkki sitä varten. Jos uskot, että kyseessä voi olla luotettava

sähköposti, kirjoita linkin napsauttamisen asemesta Mikähyvänsä Oy:n verkkosivuston osoite selaimeesi.

Linkit voidaan myös saada näyttämään siltä, että ne johtavat eri sivustoon kuin mihin ne tosiasiallisesti johtavat. Joten et voi luottaa siihen, että linkki vie sinut sille sivustolle, jolle se näyttäisi vievän. Jos käytät tietokonetta, voit tarkistaa, mihin linkki todella johtaa viemällä hiiren sen päälle.

Saatat haluta ehkä napsauttaa linkkiä tilanteessa, jossa odotat sellaista saapuvaksi. Kuten esimerkiksi jos olet unohtanut salasanan ja pyytänyt salasanan palauttamista. Silloin tiedät odottaa linkkiä salasanan palautus-sivustolle.

- **Älä lataa asioita, jos et ole täysin varma, mitä ne ovat**
  Huoleton lataaminen on uskomattoman tehokas tapa täyttää tietokoneesi tai puhelimesi haitallisilla sovelluksilla, kuten vakoiluohjelmilla tai kiristyshaittaohjelmilla. Aivan kuten linkkien klikkaamisessa: Jos tiedät, mitä olet lataamassa ja uskot, että sivusto on luotettava, anna mennä vaan.

  Ole erityisen varovainen sellaisesta ladattavasta sisällöstä, joka lähetetään sinulle sähköpostitse tai viestisovelluksen kautta. Jos joku, jonka henkilöllisyyttä et voi todistaa (esimerkiksi soittamalla hänelle), pyytää sinua lataamaan jotain Facebookin Messengerin kautta, on parempi jättää viesti huomiotta kuin ladata.

- **Älä klikkaa kohtia "Ota sisältö käyttöön" tai "Ota makrot käyttöön"**
  Jos saat tiedoston, joka ei näytä oikealta – esimerkiksi sellaisen, jossa on tekstiä, jota on mahdoton lukea – ja saat ilmoituksen, että sinun on "otettava sisältö käyttöön" tai "otettava makro käyttöön" tiedoston lukemiseksi, älä tee sitä. Makrojen (joskus kutsutaan vain sisällöksi) ottaminen käyttöön tyypillisesti Microsoft Office-tiedostossa (Word, Excel) antaa tietokoneelle mahdollisuuden ajaa ohjelmaa, joka on piilotettu vastaanottamaasi tiedostoon. Voidaan pitää varmana, että tämä ohjelma on haitallinen.

  Jos et tiedä, mitä makrot ovat, etkä ole täysin varma, että tiedosto on aito, älä klikkaa Ota käyttöön -kohtaa.

Sähköpostin ja puhelinnumeron väärentäminen

Sivustot voidaan tehdä huijaamaan sinua uskomaan, että ne kuuluvat jollekin tietylle yritykselle, vaikka näin ei ole, mutta myös sähköpostiosoitteita ja puhelin-numeroita voidaan muuttaa.

On olemassa verkkosivustoja, joiden avulla ihmiset voivat lähettää sähköpostia niin, että ne näyttävät tulevan siitä sähköpostiosoitteesta, josta lähettäjä haluaa näyttää sen tulevan. Voit lähettää sähköpostia, joka näyttää tulevan mistä tahansa keksimästäsi osoitteesta. Joten jos saat sähköpostin, joka näyttää siltä, että se on ystävältäsi (tai poliisilta, presidentiltä tai keneltä tahansa), niin se voi olla heiltä – mutta kyseessä voi olla myös jotain, jota kutsutaan sähköpostin väärentämiseksi: lähettäjän sähköpostiosoitteen muuttaminen niin, että vastaanottaja erehtyy sen lähettäjästä. Vakiintuneet sähköpostipalveluntarjoajat, kuten Gmail, voivat ehkä varoittaa sinua epäilyttävistä sähköposteista.

Jos saat sähköpostiviestin, joka näyttää siltä, että se on ystävältäsi tai joltakin luotettavalta taholta, mutta sähköposti tuntuu jollain tavalla epäilyttävältä tai siinä pyydetään sinulta henkilökohtaisia tietoja, muista sähköpostien väärentäminen. Soita tai lähetä sähköpostia ystävällesi ja tarkista, että alkuperäinen sähköposti todella tuli häneltä.

Sama pätee puhelimiin. Puhelinnumero on mahdollista väärentää, niin että puhelu tai tekstiviesti näyttää tulevan eri numerosta kuin mistä se oikeasti tulee. Mitä teknisesti taitavampi ex-kumppanisi on, sitä epäilevämpi sinun täytyy olla sähköpostien ja tekstiviestien suhteen. Jos ystäväsi lähettää sinulle sähköpostin tai tekstiviestin, joka vaikuttaa oudolta, soita hänelle suoraan varmistaaksesi, että se tuli häneltä.

Julkiset langattomat valetukiasemat keinona vakoilla tietoliikennettä

Voi tuntua siltä kuin internetissä surffaaminen ja sähköpostien lähettäminen tapahtuu näkymättömästi. Kirjoitat jotain selaimeesi ja siinä se on, haluamasi verkkosivu. Tämä kaikki ei kuitenkaan tapahdu niin näkymättömästi kuin miltä se vaikuttaa. Oli kyseessä sitten internetissä surffaaminen, sähköpostien lähettäminen, suoratoiston katsominen tai mikä tahansa muu juttu verkossa, todella paljon dataa lähetetään ja vastaanotetaan. Tätä dataa lähetetään pienissä informaatioerissä, joita kutsutaan paketeiksi.

Jos haluan katsoa kissavideoita, minun tietokoneeni täytyy ensin puhua sellaiselle tietokoneelle, jolla on kissavideoita ja kertoa sille koneelle, että haluan nähdä niitä. Tämä liikenne meidän tietokoneemme ja vierailemiemme sivustojen ja palveluiden välillä kulkee useiden eri paikkojen kautta. Tässä oppaassa olemme huolissamme siitä, että ex-kumppanisi voi pystyä kyyläämään tuota liikennettä. Sitä kutsutaan “pakettien nuuskimiseksi”.

Tarkasti ottaen kuinka paljon exäsi voi nähdä riippuu paljolti siitä, kuinka iso osa internet-liikenteestäsi on salattua. Se taas riippuu siitä, millä sivuilla vierailet ja

mitä appeja käytät. Perusesimerkkki olisi se, että hän voisi nähdä, millä sivustoilla vierailet. Pahin vaihtoehto on se, jos mitään ei ole salattu, että hän näkee kaiken ja pystyy myös lukemaan lähettämäsi ja vastaanottamasi sähköpostit. Sellainen vaihtoehto ei ole todennäköinen, sillä yhä enenevässä määrin webbisivut, sähköpostipalvelun tarjoajat ynnä muut ovat alkaneet salata liikennettä. Joka tapauksessa haluat silti estää sen, että ex-kumppanisi pystyy nuuskimaan internetin käyttöäsi.

Jos et elä sen ihmisen kanssa, josta olet huolissasi, niin silloin isoin riski, että hän pääsee nuuskimaan internetin käyttöäsi, on silloin, kun käytät julkista langatonta tukiasemaa eli wifi- tai wlan-tukiasemaa. On turvallisempaa olla käyttämättä sellaista ja sen sijaan käyttää puhelimesi omaa internet-yhteyttä. Jos tämä ei jotain syystä ole mahdollista, silloin sinun tulee olla tietoinen riskeistä ja haavoittuvuuksista julkisten wifien kanssa. Myös langattomien tukiasemien nimiä voidaan väärentää.

Suosikkikahvilallasi saattaisi olla julkinen wifi, nimeltään vaikkapa Kahvilawifi. Ja jos kirjaudut siihen, käytät kahvilan wifiä. Tai sitten et. Ongelma on se, että mikään ei estä ketään perustamasta julkista wifi-tukiasemaa ja nimeämästä sitä miksi haluaa. Ex-kumpppanisi voi luoda wifi-yhteyden ja nimetä sen Kahvilawifiksi. Teknisesti se on helppoa: heillä täytyy vain olla laite, joka voi jakaa wifinsä, esimerkiksi reititin, puhelin, kannettava jne. Tämän laitteen täytyy kuitenkin olla varsin lähellä sitä laitetta, joka ottaa tukiasemaan yhteyden ja wifillä on kuitenkin varsin lyhyt toimintamatka.

Huijaus-wifin tukiaseman toimintasäteeseen vaikuttaa muutama seikka, mutta joka tapauksessa se on lyhyt. Ex-kumppanisi pitäisi olla samassa huoneessa kanssasi tai ainakin jossain hyvin lähellä. He eivät voi perustaa huijaus-wifi-asemaa kotiinsa, koska wifin toimintamatka ei ulottuisi kahvilaan.

On muutama seikka, jotka kannattaa pitää mielessä liittyen wifi-huijauksiin. Jos suosikkikahvilallasi on salasanalla suojattu wifi, heidän salasanansa on jossain listattuna. Ja exäsi voi laittaa täsmälleen saman salsasanan omaan huijaus-wifi-yhteyteen. Tällöin olettaisit vielä varmemmin, että olet yhteydessä kahvilasi wifiin, vaikka näin ei olekaan asia.

Tämä huijaus on vielä vaikeampaa havaita, jos annat puhelimesi muodostaa yhteyden automaattisesti julkisiin wifi-verkkoihin. Ja silloin vaikka et ole lähelläkään suosikkikahvilaasi, jos puhelimesi huomaa kahvilasi wifiltä vaikuttavan verkon, se muodostaa yhteyden tähän verkkoon.

Joten jos mahdollista, käytä puhelimesi omaa internet-yhteyttä. Ja jos olet kaupungilla ja sinun pitää yhdistää kannettavasi tai tablettisi internetiin, silloin voit jakaa puhelimesi internet-yhteyden noille laitteille. Tätä kutsutaan wifi-

hotspotin eli langattoman mobiilitukiaseman luomiseksi. Huomioi, että tällaisessa tapauksessa puhelimesi dataa kuluu, kun joku muu laitteesi käyttää sen internet-yhteyttä.

- Riippuu puhelimestasi, mistä siitä löytyy mahdollisuus käyttää hotspotia. Mutta se löytyy jostain asetuksista, sieltä esimerkiksi “verkko ja internet” ja sitten “hotspot ja yhteyden jako”.
- Kun sallit puhelimesi jakavan internet-yhteyden, niin se saattaa oletuksena sallia kaikkien käyttää tuota yhteyttä. Jos näin on, niin aseta hotspottiisi salasana. Sen voit tehdä kohdasta, jossa lukee jotakin sen tapaista kuin “Luo wifi-hotspot”.

Kun se on tehty, etsi kannettavallasi tai tabletillasi puhelimesi wifi-verkko ja anna salasana, jotta voit yhdistää siihen. Nyt sinun ei tarvitse huolehtia siitä, että ex-kumppanisi seuraa internet-liikennettäsi!

On vielä muutamia muita varokeinoja, joita kannattaa käyttää, kuten internet-liikenteesi salaaminen käyttäen HTTPS:ää ja jos mahdollista, käyttäen VPN:ää. Näistä varokeinoista puhumme seuraavassa luvussa.

7. Jos asut yhä hänen kanssaan

Tämä luku on ihmisille, jotka yhä asuvat henkilön kanssa, jota he pelkäävät. Käymme läpi minkälaisten asioiden tekeminen jättää jälkiä, joita tämä henkilö voi löytää. Kerromme myös, miten käyttää tietokonetta ja surffata netissä ilman, että siitä jää jälkiä.

Tämä luku ei käsittele tilannetta, jossa on fyysisen väkivallan riski. Emme ole psykologeja tai poliiseja, voimme vain antaa teknologiaan liittyviä neuvoja. On olemassa erilaisia tukiryhmiä kuten myös poliisi, joihin voit olla yhteydessä, jos pelkäät väkivaltaa. Voit paeta myös erilaisiin turvakoteihin, jos tilanne kotona äityy pahaksi kotona. Emme käsittele näitä tilanteita, mutta tukiryhmien, turvakotien ja poliisin internet-sivustot ja puhelinnumerot löytyvät internetistä.

Huom! Käytä internetiä *turvallisesti*, kun etsit sieltä turvakoteja, tukiryhmiä tai mitä tahansa aiheeseen liittyvää. Käymme tässä luvussa läpi sen, miten käyttää internetiä nimettömänä.

Internet-liikenteen vakoilu kodin internet-yhteyden kautta

Edellisessä luvussa käsittelimme riskejä, jotka liittyvät julkiseen wifiin ja pakettien nuuskintaan. Jos asut edelleen henkilön kanssa, jota pelkäät, silloin on myös olemassa riski, että hän vakoilee kotisi internet-yhteyden kautta tapahtuvaa internet-liikennettäsi. Koska hän voi käyttää samaa internet-yhteyttä kuin sinä, hän käyttää samaa verkkoa ja hän voi (jos on teknisesti riittävän kyvykäs) seurata kaikkea internet-liikennettä, joka kulkee kotisi wifi-yhteyden kautta.

Kuten julkisten wifi-tukiasemien kohdalla, helppo ratkaisu on käyttää puhelintasi tukiasemana internetiin silloin, kun et halua kumppanisi näkevän millä sivuilla liikut. Mutta on myös muita varokeinoja, joita kannattaa harkita. Niitä suosittelemme kaikille riippumatta siitä, uhkaako joku ihminen heitä vai ei.

Internet-liikenteesi salaaminen: HTTP, HTTPS ja selaimen lisäosa "HTTPS kaikkialla"

Tietokoneesi keskustelee internetin kanssa tietokonekielellä (eli protokollalla), jota kutsutaan HTTP:ksi (engl. Hypertext Transfer Protocol). Tai tarkemmin sanottuna tietokoneesi keskustelee toisen tietokoneen kanssa, jota kutsutaan palvelimeksi, josta puolestaan löytyy haluamasi sivu. Sinun ei tarvitse muistaa tai edes ymmärtää mitään tuosta. Tärkeää on muistaa, että HTTP ei ole salattua. Se

tarkoittaa, että jos partnerisi pääsee näkemään sen salaamattoman liikenteen, hän tietää paljon siitä, mitä teet internetissä.

Onneksi yhä useampi sivusto tarjoaa salatun yhteyden. Se tapahtuu käyttämällä jotain, jota kutsutaan HTTPS (huomaa lopun kirjain “S”. Voit ajatella sitä S-kirjainta kuten Salattua). HTTPS salaa liikenteen sinun ja vierailemasi sivuston välillä. Silloin partnerisi ei pysty sitä lukemaan eikä ymmärtämään.

On olemassa ilmainen selaimen lisäosa, joka varmistaa, että käytät joka kerta salattua yhteyttä, kun se vain on mahdollista. Tämä lisäosa on nimeltään “HTTPS Everywhere”. Sitä kehittää ja pitää yllä voittoa tavoittelematon Electronic Frontier Foundation. HTTPS Everywhere on tarjolla seuraaville selaimille: Chrome, Firefox ja Opera. Voit lukea HTTPS Everywhere -lisäosasta enemmän ja ladata sen ilmaiseksi osoitteesta https://www.eff.org/https-everywhere

Huom! On tärkeää muistaa, että HTTPS ei piilota sitä, että olet vieraillut jollain sivustolla. Vielä kerran, koska asia on tärkeä: HTTPS salaa sinun liikenteesi selaimen ja verkkosivuston välillä, mutta se ei piilota tietoa, millä sivustoilla vierailet. Joten vaikka käytät HTTPS:ää ja asut henkilön kanssa, joka seuraa internetin käyttöäsi, ei ole edelleenkään vaaratonta vierailla sellaisilla sivustoilla, joista hän saattaisi suuttua, kuten sivusto kotiväkivallasta tai vainoamisesta.

Näennäinen yksityisverkko eli VPN

HTTPS suojaa sitä, ettei kukaan näe mitä olet katsonut jollakin verkkosivustolla, mutta se ei piilota verkko-osoitetta keneltäkään, joka käyttää samaa verkkoyhteyttä. Toisin sanoen hän näkee, että vierailet sivustolla *esimerkki.com*, mutta hän ei näe, mitä katsot *esimerkki.com*-sivustolla eikä hän näe luottokorttisi numeroa, jos käytät sitä tuolla verkkosivustolla.

Lisäturvaksi voit käyttää näennäistä yksityisverkkoa eli VPN:ää (engl. Virtual Private Network). VPN tekee kahta asiaa, jotka parantavat sekä tietoturvaasi että yksityisyyttäsi.

1. VPN salaa liikenteesi. Tämä tarkoittaa sitä, että joku samaa verkkoyhteyttä käyttävä näkee internet-liikennettä, mutta hän ei näe, mitä se on.

2. VPN lähettää kaiken internet-liikenteesi VPN:n tarjoajan oman palvelimen (tai tietokoneen) kautta ja sitten sille sivustolle, jolle haluat mennä. Käytännössä tämä tarkoittaa, että vierailemasi sivusto ei tiedä, että sen havaitsema liikenne tulee sinun tietokoneeltasi.

Yleensä verkkosivusto saa paljon tietoa vierailijoista, mukaan lukien mitä selainta ja käyttöjärjestelmää vierailija käyttää, se näkee vierailijan IP-osoitteen, joka antaa verkkosivustolle melko tarkan arvion siitä, missä vierailija on

fyysisesti ja muutakin tietoa jää vierailijasta verkkosivustolle. Nämä huolet eivät ole erityisen oleellisia tässä oppaassa, ellet vieraile verkkosivustolla, jota ylläpitää ex-kumppanisi tai ihminen, jota pelkäät. Mutta jos sinulla on varaa, niin luotettava VPN on aina hyvä investointi, jos on kiinnostunut tietosuojasta. VPN:iä on tarjolla älykännyköihin, tietokoneille ja tableteille.

Huomio! Kaikki liikenteesi kulkee VPN:n palveluntarjoajan kautta. Joten älä hae internetistä sanoilla “ilmainen VPN”, ja sitten summamutikassa valitse yhtä. Valitse VPN, johon voit luottaa, sellainen, jonka takana on hyvämaineinen yritys.

Verkossa surffaaminen nimettömänä

Neuvomme nimettömänä surffaamisesta riippuu siitä, kenen et halua näkevän internet-liikennettäsi. Käymme läpi muutaman vaihtoehdon, helposta vaikeaan.

Olet ainoastaan huolissasi ex-kumppanistasi, et enää asu hänen kanssaan eikä hänellä ole pääsyä tietokoneellesi eikä puhelimellesi

Tällaisessa tapauksessa ex-kumppanillesi on hyvin vaikeaa vakoilla lainkaan internet-liikennettäsi. (Ainoita poikkeuksia saattavat olla harvinaiset tilanteet, jolloin hän on esimerkiksi töissä sinun internetin palveluntarjoajallasi, tai hän tekee töitä poliisille, valtiolle tai jotain vastaavaa.) Tällaisessa tapauksessa pääasiat, joita pohtia:

- Internet-tiliesi turvaaminen. Jos exälläsi on pääsy tai hän pystyy hakkeroimaan esimerkiksi Googlen tilisi, silloin hän pääsee käsiksi sinun Googlen hakuhistoriaan, katsomiisi YouTube-videoihin, paikkoihin, joissa olet ollut yms. (Katso lukua 2, jossa kerrotaan, kuinka suojata internet-tilisi.)
- Muista keskustelu julkisten wifien tukiasemista. On turvallisempaa surffata internetissä käyttämällä kotisi internet-yhteyttä tai puhelimesi wifiä. Ja harkitse, josko asentaisit HTTPS Everywhere -lisäosan selaimeesi ja hankkisit VPN:n.

Ainut huolesi on ihminen, jonka kanssa asut ja hänellä on pääsy tietokoneellesi tai puhelimeesi

Kuten oli puhetta tämän luvun alussa, teknologian hyvin tunteva ihminen voi seurata verkkoliikennettä, joka kulkee kotisi internet-yhteyden kautta. Joten tällaisessa tilanteessa pääasiat, joita on hyvä pohtia:

- Voit käyttää VPN:ää salataksesi internet-liikenteesi. Mutta jos käytät kotisi internet-liikennettä, esimerkiksi surffaat tietokoneellasi tai tabletillasi,

niin vaikka sinulla olisi käytössä VPN, tämä henkilö pystyy edelleen näkemään, että olet käynyt verkossa. Tämän voit välttää käyttämällä puhelintasi.

- Aseta selaimesi (ohjelma, jolla surffaat internetissä) toimimaan yksityisessä selaustilassa. Tämä ominaisuus on käytössä useimmissa selaimissa, hieman eri nimisinä. Tässä tilassa tietokoneesi ei tallenna selaushistoriaasi eikä evästeitä niiltä sivustoilta, joilla vierailit. Ne sivustot kyllä tietävät, että vierailit siellä, mutta kukaan, joka tutkii puhelintasi myöhemmin ei tiedä, kunhan olet sulkenut sivuston. Huomaathan, että yksityisessä selaustilassa lataamasi tiedostot eivät häviä koneeltasi, kun suljet selaimen. Tiedostojen turvallista poistamista käsitellään myöhemmin tässä oppaassa.
- Jos tällä henkilöllä on pääsy sinun internet-tileillesi tai hän pystyy murtautumaan niihin, hän voi yhä saada selville paljon tekemisistäsi. Katso lukua 2, siellä kerrotaan lisää, kuinka turvata internet-tilisi.
- Sen sijaan että käyttäisit omaa tietokonettasi, voit käyttää ystäväsi, kirjastosi, turvakodin, tukiryhmän yms. Tietokonetta.
- Yksi lisävaihtoehto käyttää internetiä salaa, on käyttää jotain mitä kutsutaan nimellä TAILS. Siitä kerromme seuraavassa osassa.

Et halua kenenkään näkevän internet-liikennettäsi

Jos et halua riskeerata mitään liittyen internet-liikenteeseesi, silloin Tor-selain on vaihtoehtosi. Olet saattanut kuulla Torista, kun on puhuttu rikollisesta toiminnasta. Aloitetaan keskustelu Torista selventämällä muutama mahdollinen väärinkäsitys.

Tor-hanke on voittoa tavoittelematon organisaatio Tor-selaimen takana. Tor-hanke koostuu muutamista eri tuotteista ja työkaluista. Noiden työkalujen joukossa on sellaisia, jotka mahdollistavat ihmisille pitää sivustoja nimettömänä. Olet saattanut kuulla termin pimeä verkko (engl. dark web). Rikolliset ovat yksi sellainen joukko ihmisiä, jotka haluavat liikkua internetissä piilossa ja ylläpitää nimettömiä verkkosivustoja, joten he ovat yksi Torin tuotteiden monista käyttäjistä.

Mutta tällainen sensationaalinen kuva Torista jättää ulkopuolelleen monet muun Torin käyttötavat ja käyttäjät, jotka hyötyvät siitä. Tällaisia ryhmiä ovat esimerkiksi toimittajat, ilmiantajat, toisinajattelijat diktatuureissa ja kotiväkivallan tai vainoavan ex-kumppanin uhrit. Kaikilla näillä ihmisillä on hyvät syyt olla erityisen huolellisia nimettömyydestään verkossa.

Tor-selaimen keskittyy nimettömänä toimimiseen ja nimettömään kommunikaatioon varmistaen, että kukaan ei saa selville, millä sivustoilla vierailet. Tämä on se työkalu, jota suosittelemme tähän tilanteeseen. Huomaa kuitenkin, että Tor-selain itsessään näkyy puhelimessasi tai tietokoneessasi. Voit piilottaa ne sivustot, joilla käyt, mutta et sitä, että olet asentanut Torin. Jos et voi ottaa sitä riskiä, niin lue seuraava osio, jossa puhutaan TAILSista.

Huom! Pimeän verkon sivustot eivät löydy normaaleilla hauilla, jotka tehdään Tor-selaimella. Et voi vahingossa törmätä laittomaan sivustoon, et ainakaan mihinkään sellaiseen laittomaan sivustoon, mihin et voisi törmätä millä tahansa selaimella. Tor-selain toimii aivan kuin hakukoneet ja selaimet, joita normaalisti käytät. Saat samanlaiset hakutulokset ja voit vierailla täsmälleen samoilla sivustoilla Tor-selaimella kuin millä tahansa selaimella, jota nyt käytät. Jotta pääsisit salatuille sivustoille, joista olet saattanut kuulla, sinun täytyy tietää täsmälleen oikea osoite. Ja ne ovat pitkiä, eikä niissä ole mitään tolkkua.

Käytä tietokonetta *ja* surffaa verkossa nimettömänä käyttäen TAILSia

TAILS (engl. The Amnesic Incognito Live System) on käyttöjärjestelmä, jonka on kehittänyt tietoturva- ja tietosuoja-asiantuntijat. Tavoitteena on turvata käyttäjän yksityisyys ja nimettömyys. Oletuksena TAILS ei tallenna mitään informaatiota sessiostasi. Se tarkoittaa sitä, että kun suljet tietokoneesi, kaikki mitä teit koneellasi, hävitetään. Oletuksena TAILS myös lähettää internet-liikenteen Torin kautta.

Voit asentaa TAILSin tietokoneelle siten, että sitä käytetään aina. Voit myös käyttää TAILSia USB-tikun avulla. Silloin jää piiloon jopa se, että sinulla on pääsy TAILSiin. Ainut keino jollakulla havaita, että olet käyttänyt TAILSia, on löytää USB-tikku, jolla TAILS on.

- Käyttääksesi TAILSia USB-tikulta, asenna ensin TAILS USB:lle.
- Sitten laita TAILS USB kiinni tietokoneeseesi. Laita tietokone päälle tai jos se on päällä, uudelleenkäynnistä se.
- Ennen kuin normaali käyttöjärjestelmä tietokoneessasi varsinaisesti käynnistyy, sinulle annetaan mahdollisuus avata sellainen kuin käynnistysvalikko (engl. boot menu). Sieltä käsin voit kertoa tietokoneellesi käyttää TAILSia normaalin käyttöjärjestelmän asemesta.
- Valitettavasti tämä osa on vähän hankala, koska se mitä näppäintä pitää painaa, riippuu käyttöjärjestelmästäsi ja tietokoneestasi. Tietokoneesi näyttää, mitä näppäintä painaa, niin sanottua “Boot menu -näppäintä”, mutta se saattaa näkyä ruudulla vain hetken.

    - PC:ssä yleensä esiintyvät Boot menu -näppäimet ovat: Esc, F7, F8, F9, F10, F11 ja F12 (voi olla myös Novo-näppäin Lenovo-merkkisessä tietokoneessa)

      Löydät yksityiskohtaisemman listan ja aloitusoppaan TAILSin sivustolta: https://tails.boum.org/install/win/usb/index.en.html#start-tails

    - Macissa, paina ja pidä alhaalla Alt-näppäin. TAILSin sivustolla lisää infoa: https://tails.boum.org/install/mac/usb/index.en.html#start-tails

- Boot menusta voit sitten valita, että käynnistät TAILSin USB-tikulta.

Kun TAILS on käytössä tietokoneessasi, se käyttää tietokoneesi laitteistoa jättämättä toiminnastasi jälkiä "normaalin" tietokoneesi kovalevylle. Voit lukea lisää TAILSista ja ladata sen tältä sivustolta: https://tails.boum.org/

Tiedostojen turvallinen poistaminen

Kun poistat tiedoston puhelimeltasi tai tietokoneeltasi, itse asiassa se tiedosto ei tuhoudu. Annat vain tietokoneellesi luvan käyttää sitä tilaa muistista muuhun tarkoitukseen sitten, kun tietokoneesi tarvitsee lisää tilaa. Jos etsit poistamaasi tiedostoa, sitä ei enää löydy, mutta se on silti vielä siellä. Ja on olemassa ohjelmia, joita voidaan käyttää tällaisten tiedostojen löytämiseen.

Jos haluat kokonaan poistaa kaiken todisteen jonkin tiedoston olemassa olosta, silloin ainut turvallinen tapa on kokonaan kirjoittaa sen päälle. Eli pitää täyttää jollain muulla se kohta tietokoneesi kovalevyllä, jossa tiedosto oli. Ja varmuuden vuoksi täytyy kirjoittaa sen kohdan päälle tietokoneesi muistissa useita kertoja.

Jos tiedät, minkä tiedoston haluat poistaa, on olemassa ohjelmia, jotka kirjoittavat siihen päälle useita kertoja muuta tietoa. Esimerkiksi TAILSilla on sellainen ohjelma. Jos olet sen sijaan poistanut tiedoston etkä tiedä, missä se on kovalevylläsi ja haluat ylikirjoittaa sen, sinun täytyy kenties täyttää kaikki vapaana oleva muisti tietokoneellasi useaan kertaan. Täyttää millä, saatat kysyä. Sushi-resepteillä, yksisarvisen kuvilla, Rick Ashleyn videoilla – millä tahansa, jolla ei ole mitään merkitystä, jos se löydetään. Kokonaisen kovalevyn täyttäminen useaan kertaan kestää hyvän tovin. Onneksi on olemassa ohjelmia, jotka auttavat sinua tekemään sen. Huomaa kuitenkin, että jos henkilö, jota pelkäät, on riittävän taitava teknisesti löytämään hävitetyt tiedostot, he todennäköisesti huomaavat, että olet ylikirjoittanut jotakin. Hän ei vain tiedä mitä.

Jos sinun ei tarvitse poistaa tiedostoa, vaan vain varmistaa se, että muut eivät pysty avaamaan sitä, voit salata tiedoston. Se ei ole alkuunkaan niin vaikeaa kuin

miltä se kuulostaa. Löytyy ohjelmia, jotka tekevät sen puolestasi. Sinun täytyy antaa avain, salasana, jota voit käyttää tiedoston avaamiseen eli salauksen purkuun. Mutta tiedosto on koko ajan näkyvillä, sitä ei vain voi avata, jos ei ole oikeaa avainta. Jos haluat olla erityisen varovainen, voit ensin salata tiedoston ja sitten poistaa sen

Laitteittesi ja internet-tiliesi turvaaminen, kun asut jonkun kanssa, johon et luota

Tällaisessa tilanteessa on kaksi lähestymistapaa, riippuen siitä, miten uskot ex-kumppanisi reagoivan siihen, että olet lisännyt tietoturvaasi. Lyhyt versio on tämä:

- Jos sinun ei tarvitse pelätä mitään aggressiivista reaktiota, voit käyttää tämän oppaan kaikkia vinkkejä ja suojata laitteesi viimeisen päälle.
- Jos sen sijaan hänen reaktionsa saattaa olla aggressiivinen, älä tee mitään, mikä voisi herättää epäilyksiä tai nostattaa vihaa. Sen sijaan kehitä uusia, salaisia viestintätapoja.

Katsotaanpa tarkemmin kutakin skenaariota ja sitä, mitä sinä voit tehdä asian hyväksi.

Vaikka suojaat tilisi ja laitteesi, ei ole syytä pelätä, että kukaan reagoisi mitenkään

Älä käytä kasvojen- tai sormenjälkitunnistusta puhelimesi ainoana näytön lukituksen avaajana. Kasvojentunnistusta voidaan käyttää, kun nukut ja puhelintasi pidetään kasvojesi edessä. Ja sormesi voidaan asettaa puhelimen päälle. Käytä sen sijaan PIN-koodia tai salasanaa, mieluiten kuutta merkkiä tai pidempää. Kuten internet-tilien salasanoissa, älä tee salasanastasi tai PIN-koodistasi helppoa arvata. Joten älä esimerkiksi käytä syntymäpäivääsi tai lapsesi syntymäpäivää puhelimen lukituksen avaamiseen.

Vaihda SIM-kortin PIN-koodi, jotta se ei olisi oletussalasana, joka sillä oli ostaessasi SIM-kortin (SIM-korttien oletus-PIN-koodit löytyvät yleensä verkosta, jos tietää, mikä puhelinoperaattori jollakin on).

Lukitse tietokone salasanalla. Jälleen käytä salasanaa, jota kumppanisi ei todennäköisesti arvaa. Sammuta tietokone tai aseta se nukkumaan tai lepotilaan, kun lähdet sen luota pois, jopa vain mennäksesi kylpyhuoneeseen. Ja aseta tietokone vaatimaan salasana, kun herätät sen lepotilasta.

Aseta tietokone nukkumaan, kun se ei ole aktiivisessa käytössä. Näin se menee nukkumaan automaattisesti, jos unohdit laittaa sen nukkumaan, kun lähdit koneen luota pois.

Tietokoneen lukitsemisen lisäksi voit lisätä ylimääräisen suojaustason salaamalla tietokoneesi kiintolevyn. Tämä kiintolevyn salausprosessi voidaan asettaa suoritettavaksi automaattisesti. Kun avaat tietokoneen, sinulta kysytään ensin kovalevyn salauksen salasanaa ja sitten salasanaa tietokoneen lukituksen avaamiseksi. (Älä käytä samaa salasanaa molemmille.) Useimmissa tilanteissa tämä tuo todennäköisesti enemmän turvallisuutta kuin tarvitset. Mutta jos henkilö, jonka kanssa asut, on taitava tietokoneen käyttäjä, hän voi esimerkiksi päästä käsiksi tiedostoihisi kytkemällä kiintolevyn toiseen tietokoneeseen (eri käyttöjärjestelmää käyttävälle) ja siten pystyä ohittamaan tietokoneesi salasanatarkistuksen. Mutta jos kiintolevysi on salattu, hän ei pääse käsiksi tiedostoihisi.

Ole varovainen, kun surffaat puhelimellasi ja tietokoneellasi. Kumppanisi saattaa katsoa olkapääsi yli, kun avaat laitteen lukituksen ja siten nähdä salasanasi tai PIN-koodisi.

Viimeisenä, jokseenkin itsestään selvänä huomautuksena: Näiden vinkkien lisäksi kaikki, mitä olemme aiemmin käsitellyt tässä oppaassa internet-tilien, tietokoneiden jne. turvaamisesta, on tietysti myös hyvin tärkeää.

Jos pelkäät vihamielistä reaktiota, kun suojaat tilejäsi ja laitteitasi

Jos on mitään syytä epäillä, että kanssasi asuva henkilö voi tulla väkivaltaiseksi tai muulla lailla käyttäytyä huonosti, silloin sinun täytyy olla varovainen, ettei hän huomaa sinun etsivän merkkejä vainoamisesta, olevan kiinnostunut parantamaan turvallisuuttasi tai yrittävän tehdä asioita hänen huomaamattaan.

Voit pitää olemassa olevat tilisi, mutta luoda uudet, salaiset tilit viestintää varten. Pidä yllä normaalia tilannetta tietokoneellasi ja puhelimellasi, tee niitä asioita, joita normaalistikin teet. Ja käytä uusia tilejäsi salaiseen viestimiseen.

Jos kanssasi elävällä henkilöllä on pääsy puhelimeesi, sinun täytyy miettiä, josko siihen on asennettu vainoamisohjelma tai jokin muu tapa seurata sinua. Sama koskee tietokonettasi. Jos laitteesi on saastutettu sellaisella ohjelmalla, silloin hän voi tietää, mitä olet tehnyt sillä tietokoneella. Käytä sellaista tietokonetta, jota hän ei voi tarkkailla, esimerkiksi ystävän tai kirjaston konetta, ja luo sillä uusi sähköpostitili, sosiaalisen median tili tai mikä tahansa tili, jota haluat käyttää salaiseen viestimiseen. Jos tietokoneellasi tai puhelimellasi on vakoiluohjelma, silloin kanssasi asuva henkilö saattaa voida nähdä sekä sen, että olet luonut uuden tilin että nähdä salasanasi.

Jos sinulla on mahdollisuus piilottaa ylimääräinen kännykkä, jossa on prepaid-liittymä (eli voit käyttää liittymää nimettömänä), se on yksi hyvä vaihtoehto. Jos piilotat puhelimen taloosi, muista laittaa se äänettömälle ja estä ilmoitusten näkyminen, jotta puhelinta ei voi havaita. Sinun täytyy myös olla huolellinen, jotta puhelimesta ei tule kotiisi tai sähköpostiisi mitään laskua, jonka tämä henkilö saattaisi löytää. Jos hän pääsee käsiksi pankkitiliisi tai lukemaan tiliotteitasi, et halua, että kännykkäsi näkyy pankkitililläsi tai tiliotteellasi. Sen estämiseksi voit ostaa ylimääräisen puhelimen ja SIM-kortin käteisellä. Voi olla vaarallista vain ostaa erillinen SIM-kortti, jonka vaihtaa omaan peruspuhelimeen, kun haluat keskustella salaisesti, koska puhelimesi voi tallentaa muistiin tätä salaista viestintää, kuten tekstiviestejä tai yhteystietoja.

Yksi vaihtoehto on TAILS, josta oli puhetta aikaisemmin. TAILSin avulla voit käyttää mitä tahansa tietokonetta, jopa kotikonettasi, ilman että siitä jää jälkiä itse tietokoneeseen. Ainut merkki TAILSin käytöstä on se USB-tikku, jolla TAILS on.

Muista: Ole varovainen, ettet vahingossa jatka jollain vanhalla viestintäkanavalla keskustelua, jonka aloitit uudella sähköpostilla, sosiaalisen median tilillä tai jollain muulla viestintäkanavalla, koska kanssasi asuva henkilö saattaa seurata vanhoja tilejäsi. Esimerkiksi vastaisit vahingossa vanhalla sähköpostiosoitteellasi ystäväsi viestiin, joka oli lähetetty salaiseen sähköpostiisi.

Kiitokset

Ennen kaikkea haluamme kiittää sydämestämme kaikkia niitä ihmisiä, jotka ovat kertoneet meille tarinansa. Teidän kysymyksenne ja huolenne auttoivat tämän oppaan syntymisessä. Oli mieluisaa puhua jokaisen teistä kanssa. Se on aika hämmästyttävää, kun ajatellaan, kuinka epämiellyttäviä aihepiirejä käsittelimme.

Olemme myös kiitollisuudenvelassa monille sosiaalityöntekijöille ja vapaa-ehtoisille, jotka ovat käyttäneet aikaansa meidän kanssa keskustelemiseen. Erityisesti kiitos Jonna Brandtille Tukikeskus Varjosta (Viola ry). Hän on ollut tämän oppaan tietolähde sekä väsymätön kannustaja monien versioiden ajan, siitä lähtien kun olimme kirjoittamassa muutamia vinkkejä, jotka olisivat mahtuneet käyntikortin kokoiseen tilaan. Kiitokset myös Tukikeskus Varjon sekä Violan muille työntekijöille ja asiakkaille, kuten myös Naisten Linjalle sekä Avopalvelu Pesälle.

Kiitokset Antti Kuritulle siitä, että hän luki alkuluonnoksen ja korjasi joitakin virheitä. Kiitokset myös tekstintarkastaja Chris McPheelle, joka teki taas loistotyötä, kuten hän aina tekee. Ja Jari Perkiömäki kunnostautui suomen-kielisen käännöksen terminologiataiturina. Kiitokset myös Tukikeskus Varjolle ja Viola ry:lle käännöstyön mahdollistamisesta.

Toivomme vilpittömästi, että tästä oppaasta on apua niille ihmisille, jotka sitä tarvitsevat.

Linus Nyman & Laura Kankaala