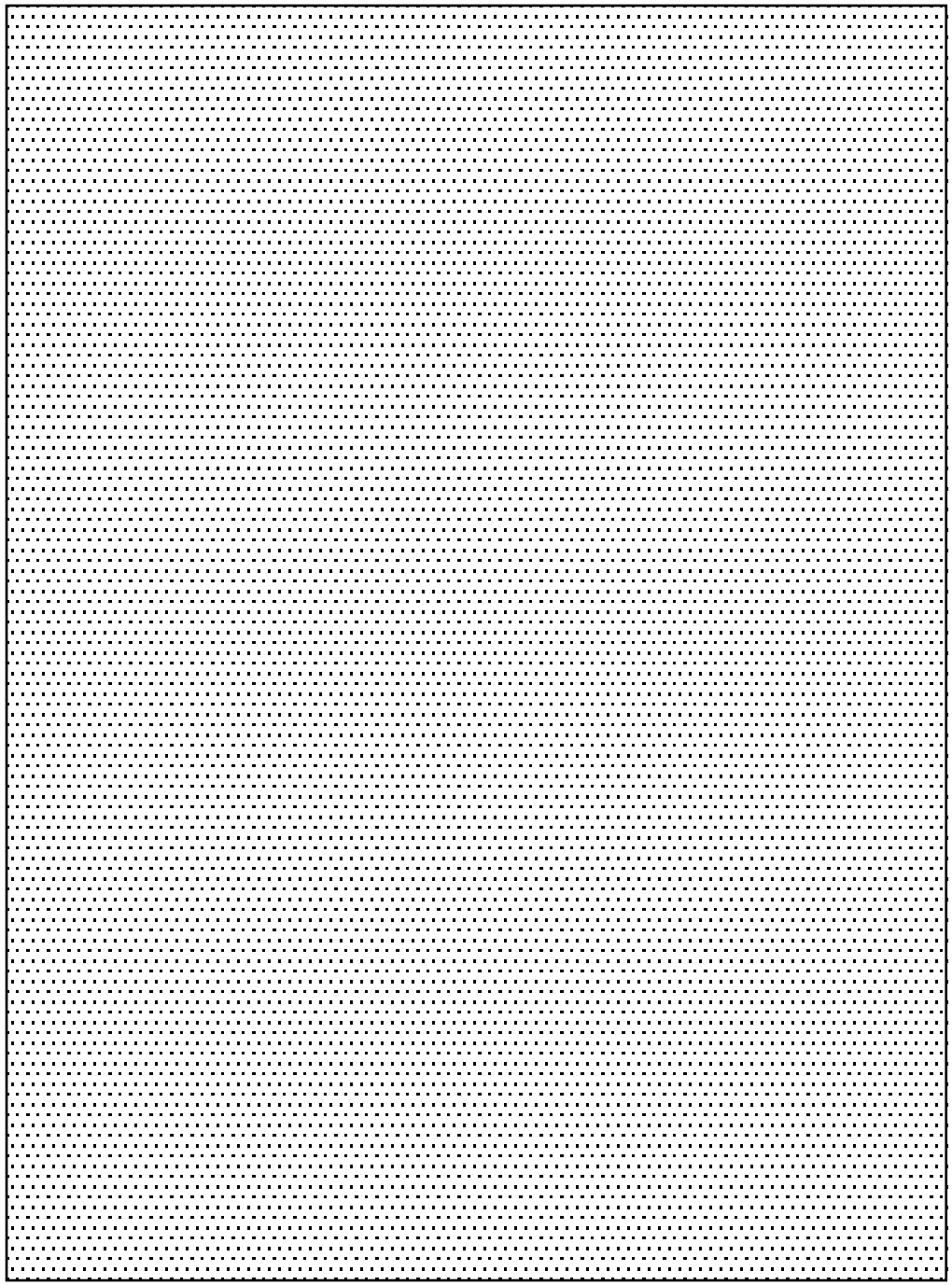
FREJA WEDENBORG

TOIMITTAJAN SALAUS-OPAS



Suomeksi toimittanut Pasi Kivioja



FREJA WEDENBORG

TOIMITTAJAN SALAUS-OPAS

Suomeksi toimittanut Pasi Kivioja



Freja Wedenborg on tanskalainen toimittaja ja kirjailija. Entinen Arbejderen-sanomalehden toimittaja työskentelee nykyisin freelancerina. Freja Wedenborg opettaa digitaalista turvallisuutta muun muassa Tanskan media-alan ja journalistiikan korkeakoulussa. Hän on Tanskan journalistiliiton hallituksen jäsen.

Twitter: @FrejaWedenborg
Internet: Cryptoguide.dk

Kirjan on toimittanut suomeksi Pasi Kivioja, Viestintäluotsi Oy.
Kivioja vastaa kappaleiden 13 ja 14 sisällöstä.
Ruutukaappaukset Pasi Kivioja, Aapo Kivioja ja Janne Pikkarainen.
Käännös tanskan kielestä Anna Mäntynen, Translato Oy.
Ulkoasu Johannes Nieminen.

© Freja Wedenborg, Pasi Kivioja ja Mediapooli, 2018

Alkuperäisteoksen *Cryptoguide for journalister – håndbog i digitalt selvforsvar*
on kustantanut Ajour (2015). Suomenkielinen versio on julkaistu alkuperäisen kustantajan luvalla.

ISBN 978-952-94-1237-2 (nid.)
ISBN 978-952-94-1238-9 (PDF)

Painettu Suomessa, Waasa Graphics Oy

Johdanto 8 1
Turvallisuustietoinen ajattelu 12 2
Faktoja valvonnasta 18 3
Uhka-arviointi 28 4
Salausvälineitä päivittäiseen käyttöön 34 5

Laitteiden suojaaminen 38 6
Massamuistin salaus puhelimessa 40 6.1
Tietokoneen massamuistin salaus 45 6.2
Vahva kirjautumissalasana 47 6.3
Salattu varmuuskopiointi 50 6.4
Ulkoisten asemien salaus 51 6.5
Tiedostojen ja kansioiden salaus 53 6.6
Hyvät turvallisuuskäytännöt 55 6.7
Tails – turvallinen käyttöjärjestelmä 57 6.8
Turvalliset laitteet 58 6.9
Tietoturva puhelimessa 60 6.10

Salasanojen suojaaminen 62 7
Vahvat salalauseet 63 7.1
Salasanojen hallintasovellukset 68 7.2

Tietoliikenteen suojaaminen 74 8
Päästä päähän -salaus 75 8.1
Signal 79 8.2
Muita viestisovelluksia 88 8.3
Sähköpostien PGP-salaus 91 8.4

Jälkien peittäminen verkossa 100 9
Tietojen kalastelun vaarat 108 10
Operaatioturvallisuutta toimittajille 114 11
Digitaalinen turvallisuus matkoilla 124 12
Mitä sanoo laki? 138 13
Väärinkäytösten paljastaminen 146 14
Mistä lisätietoja? 152 15
Sanasto 157 16

Hyvä lukija,

Tämä kirja saattaa kuulostaa paikka paikoin hurjalta agenttitarinalta, mutta jos toimittajana olet koskaan tekemisissä luottamuksellisten tietojen ja henkilöllisyydestään arkojen lähteiden kanssa, kirjassa kerrottujen taitojen hallitseminen on sinulle välttämättömyys. Suojaa edes lähteitäsi, vaikka itselläsi ei olisi mitään salattavaa.

Maailma on nykyisin sellainen paikka, jossa on koko ajan joku kalastelemassa viestejäsi, hakkeroitumassa laitteisiisi, koputtelemassa porttejasi tai kurkkimassa olkasi yli. Tämä opas selittää maallikkokielellä toimittajan tietoturvan ja suojautumisen perusteet. Kirjan kirjoittaja, toimittaja Freja Wedenborg antaa yksityiskohtaiset ohjeet tarvittavien ohjelmien hankkimiseen ja käyttöön. Kaikki tarvittavat ohjelmat ovat ilmaiseksi saatavilla, ja samalla saat hyödyllistä perustietoa myös puhelimestasi tai tietokoneestasi jo valmiiksi löytyvistä suojausmenetelmistä.

Itse järkytyin, kun kokeilin Frejan antamaa linkkiä, josta pystyy katsomaan, ovatko omat käyttäjätunnukset ja salasanat vuodettu verkkoon erilaisten tietomurtojen yhteydessä. Yksi tärkeimmistä salasanoistani oli vuodettu maailmalle jo 31 kertaa!

Kyse on digitaalisesta itsepuolustuksesta. Se ei vaadi erityisiä ninjataitoja vaan ymmärrystä digitaalisista uhkista ja hieman vaivannäköä suojautumisen eteen.

Aloita vaikka asentamalla helppokäyttöinen Signal-viestisovellus puhelimeesi, niin edes tiedustelupalvelu NSA ei pysty murtamaan viestejäsi. Ohjeet löytyvät tästä kirjasta!

Pasi Kivioja
Toimittajan salausoppaan
suomenkielisen painoksen toimittaja

1 Johdanto

Lähetämme päivittäin sähköpostia ja tekstiviestejä, soitamme puheluita, juttelemme chatissa ja surfaamme netissä. Kaikkea puhelimella ja tietokoneella tapahtuvaa viestintäämme valvotaan, ja sen lokitietoja tallennetaan.

Työnantajat, internet- ja puhelinoperaattorit, kyberrikolliset ja käyttämiämme verkkopalveluita ylläpitävät yritykset pystyvät kaikki seuraamaan toimintaamme verkossa – esimerkiksi sitä, mitä etsimme internetin hakukoneilla, kenen kanssa viestimme, missä ja milloin viestintä tapahtuu ja mistä siinä on kyse. Viranomaisilla on keinoja vaatia viestiliikennettä koskevien tietojen luovuttamista sekä valvoa laitteitamme ja viestintäämme kohdennetusti.

Viranomaisten harjoittama joukkovalvonta haastaa perustuslaillista oikeuttamme luottamukselliseen viestintään vailla valvonnan pelkoa silloin, kun meitä ei epäillä rikoksesta.

Meille toimittajille tämä tarkoittaa ratkaisevaa muutosta työntekomme perusedellytyksissä. Lehdistönvapauden keskeistä kulmakiveä, lähdesuojaa, on entistä vaikeampi turvata. Vaarassa ovat kontaktit sellaisissa maissa, joissa jo toimittajille puhuminen voi olla hengenvaarallista, tai työntekijät, joita uhkaa irtisanominen tai vankeusrangaistus työnantajaa koskevien tietojen luovuttamisesta.

Tilanteesta riippumatta toimittajien lähteiden on voitavat luottaa siihen, että se, mitä he toimittajille kertovat, pysyy salassa – myös digitaalisessa maailmassa.

Siksi meidän toimittajien on osattava suojata sekä itseämme että lähteitämme valvonnalta. On myös osattava välttää digitaalisia jälkiä, jotka voivat johtaa tietojen paljastajan jäljille. Jos emme onnistu tässä, lähteemme joutuvat vaaraan. Silloin on olemassa myös sellainen riski, etteivät lähteet uskalla lähestyä meitä, ja tärkeitä tarinoita voi jäädä kertomatta julkisuudessa.

Tässä kirjassa käsiteltävien välineiden ja menetelmien avulla digitaalisesta itsepuolustuksesta voi

tulla kaikille toimittajille tuttu ja helposti hallittava laji. Kirjan pääasiallinen kohderyhmä ovat toimittajat ja journalistiikan opiskelijat, mutta siitä on hyötyä jokaiselle, joka haluaa viestiä luottamuksellisesti ja varjella yksityisyyttään verkossa. Esimerkiksi lääkärin ja asianajajan ammateissa on niin ikään hyödyksi osata pitää potilaiden tai asiakkaiden kanssa käytävä viestintä salassa.

Kirjassa esitellään yksinkertaisia ja maksuttomia turvallisuutta parantavia työkaluja tietokoneeseen, puhelimeen ja muihin laitteisiin. Tilasyistä suurin osa välineistä esitellään yksityiskohtaisesti Mac-ympäristössä, mutta ohjeita voi soveltaa myös Windows-ympäristöön. Silloin, kun Windowsin ja Macin välillä on merkittäviä eroja, molempia käyttöjärjestelmiä varten on esitetty omat ohjeensa.

Kirjassa esiteltyä työkalupakkia käyttämällä voi suojautua yleisimmiltä hakkerihyökkäyksiltä ja kohdentamattomalta joukkovalvonnalta, jolle jokainen internet- tai televiestinnän käyttäjä altistuu jatkuvasti. Kirja sisältää perustiedot myös tietoturvasta, johon jokaisen toimittajan on nykymaailmassa kiinnitettävä huomiota.

Toimittajan salausoppaan tanskankielinen alkuteos *Cryptoguide for Journalister* julkaistiin ensimmäisen kerran vuonna 2015, kun Edward Snowdenin paljastukset globaalista joukkovalvonnasta olivat tulleet julki. Sen jälkeen yhä useammat toimittajat ovat kiinnostuneet digitaalisesta turvallisuudesta ja sen edistämisestä.

Turvallisuus on kaikkien yhteinen asia, eikä yksikään toimittaja voi kantaa siitä vastuuta yksin. Yksittäisen toimittajan tunnolliset salausrutiinit eivät auta juuri mitään, jos kaikki muut toimituksessa hutiloivat tietoturva-asioissa.

Mediapoolin päätös julkaista suomeksi toimitettu *Toimittajan salausopas* edistää merkittävästi koko media-alan mahdollisuuksia kantaa yhteisvastuuta digitaalisesta turvallisuudesta. Kiitän Mediapoolia tästä lämpimästi.

Digitaalisesta turvallisuudesta huolehtimisen ei tarvitse olla hankalaa. Olen itse kävelevä esimerkki siitä, että kuka tahansa voi oppia tarvittavat menetelmät: en ole salausasiantuntija, vaan toimittaja, joka käyttää kirjassa esiteltäviä välineitä käytännön työssä.

Siksi olenkin suuren kiitoksen velkaa niille asiantuntijoille, jotka ovat avoimesti jakaneet mittavaa tietämystään kanssani. Erityismaininnan ansaitsee tietoturvakouluttaja Aslak Ransby, mutta myös monet toimittajakollegat ovat olleet korvaamaton apu.

Ennen kaikkea haluan kuitenkin kiittää sinua, joka tätä kirjaa nyt luet joko painettuna tai sähköisenä versiona.

Mitä useampi toimittaja käyttää turvallisuutta parantavia välineitä säännöllisesti, sitä vaikeammaksi käy valvonnan kohdentaminen niihin kollegoihin, jotka kulloinkin tarvitsevat erityistä suojaa viranomaisten valokeilalta. Kun riittävän moni käyttää salattua viestintää, viranomaisten digitaalisella joukkovalvonnalla saavuttama hyöty voi kuivua kokoon, ja saatamme saada takaisin oikeutemme luottamukselliseen viestintään.

Se on tärkeä tavoite niin omien työolosuhteidemme kuin lehdistönvapauden ja demokratiankin kannalta.

Freja Wedenborg
Kööpenhaminassa lokakuussa 2018

2

Turvallisuustietoinen ajattelu

2

Sanotaan se nyt heti kärkeen aivan selvästi: mikään yksittäinen temppu ei takaa tietoturvaa.

Varsinkin Edward Snowdenin tekemien joukkovalvontapaljastusten jälkeen markkinoille on tullut liuta uusia sovelluksia, jotka lupaavat ratkaista tietoturvapulmia eri tavoin, esimerkiksi salattujen sähköpostipalveluiden tai VPN-verkon avulla.

Monet ratkaisuista toimivat toki hyvin, mutta ne edellyttävät käyttäjän luottavan palveluntarjoajaan. Tietoja vuotaa tällöin pois käyttäjän hallusta.

Tärkeää on myös ymmärtää, että eri tilanteissa tarvitaan erilaisia välineitä. Millään välineellä ei voi ratkaista kaikkia tietoturvapulmia kerralla.

Jos toimittaja vaikkapa haluaa viestiä lähteensä kanssa salatuilla sähköpostiviesteillä, mitä hyötyä siitä on, jos lähteen työnantajalla on pääsy hänen sähköposteihinsa? Silloin sähköpostien lähetyksen salaaminen ei juuri auta. Lähde saattaa myös oleskella maassa, jossa jo pelkkä salaustyökalujen asentaminen tietokoneelle herättää viranomaisten huomion. Joskus taas voi olla tarpeen salata ulkoisella kovalevyllä olevia tietoja maasta toiseen matkustettaessa tai peittää tietyllä verkkosivustolla vierailemisen jäljet.

Valvonta ja muut digitaaliseen turvallisuuteen kohdistuvat uhat ovat jatkuvassa muutoksessa – samoin välineet, joilla niiltä voi suojautua. Siksi olennaista ei ole se, mitä suojausvälineitä tai -tekniikoita käyttää, vaan se, että pystyy ymmärtämään ja analysoimaan uhkia sekä suojautumaan niiltä realistisen suunnitelman mukaisesti. Tällöin voi valita oikeanlaisia välineitä.

Laita pyöräsi lukkoon

Jos toimittaja haluaa suojata luottamuksellista viestintäänsä tai tietojaan, on ensiarvoisen tärkeää oppia kiinnittämään huomiota arkisiin turvallisuusseikkoihin.

Vaikka osa arvokkaimmasta omaisuudestamme sijaitsee nykyisin tietokoneilla ja puhelimissa, monet

eivät ajattele työasiakirjojen, yksityisten valokuvien ja vastaavien digitaalisten tietojen turvallisuutta samalla tavoin kuin fyysistä turvallisuutta. Ani harva jättää tahallaan ulko-oven lukitsematta kotoa poistuessaan, mutta moniko muistaa aina lukita tietokoneensa?

Jos ihminen liikkuu polkupyörällä, hän luultavasti laittaa sen lukkoon jättäessään sen jonnekin. Jos pyörä on yön yli taloyhtiön sisäpihalla, siinä saattaa olla pelkkä takapyörän U-lukko. Jos pyörä taas jätetään rautatieasemalle muutaman päivän matkan ajaksi, siinä voi olla lisäksi vaijerikiinnitys johonkin kiinteään rakenteeseen. Vanha, ruosteinen kulkupeli, joka joutaisi jo vaihtoon, ei välttämättä kaipaa yhtä järeitä turvatoimia kuin upouusi kilpapyörä, jota varten on säästetty kuukausikaupalla – sellaiseen kannattaa hankkia parempi ja kalliimpi lukko.

Tietoturvaa ja digitaalista turvallisuutta on opittava ajattelemaan aivan vastaavalla tavalla kuin polkupyörän lukitsemisen tarvetta.

Tässä oppaassa kerrotaan välineistä, joita digitaalisen turvallisuuden työkalupakkiin voi sisältyä. Lukija saa käsityksen myös siitä, millaisia digitaalisia hyökkäyksiä toimittajaan voi kohdistua, sekä keinoista tilanteiden analysoimiseksi. Kirjan tietojen pohjalta voi valita, mitä välineitä milloinkin kannattaa käyttää.

Neljä vinkkiä turvallisuustietoiseen ajatteluun

1. VARAUDU ENNALTA

Tietoturva on syytä ottaa huomioon tästä hetkestä alkaen. Jos alkaa miettiä turvallisuusasioita vasta kun tekeillä on erityistä suojausta edellyttävä lähde tai juttu, voi olla jo liian myöhäistä. Varautumiseen voi suhtautua kuin ensiaputaitoihin – keinojen tunteminen on tärkeää, jotta niistä on hyötyä tositilanteessa.

Toimittaja voi ajatella, ettei tarvitse salaustaitoja, koska hän ei toimi sellaisten lähteiden tai aiheiden parissa, jotka voisivat tehdä hänestä valvonnan kohteen.

Jos toimittaja salaa ainoastaan arkaluonteista viestintäänsä, salauksen käyttö on muutos käyttäytymisessä, mikä voi herättää ei-toivottua huomiota ja helpottaa juuri niiden seikkojen havaitsemista, jotka toimittaja haluaisi pitää salassa. Sen vuoksi on tärkeää salata myös muuta tietoliikennettä kuin vain sitä, jota varsinaisesti haluaa varjella. Yhtä tärkeää on tietää jo ennakolta, miten lähteitä voi suojata valvonnalta. Muutoin jo ensimmäinen yhteydenotto saattaa vaarantaa kaiken tai lähde ei uskalla puhua toimittajille. Tärkeä uutinen saattaa jäädä kertomatta.

2. ARKIRUTIINEJA VAI HÄLYTYSTILA?

On itsestään selvää, ettei kaikkea voi salata jatkuvasti. Siksi on tärkeää erottaa toisistaan arkiset rutiinit ja hälytystila.

Korkeimman valmiusasteen jatkuva ylläpitäminen ei ole tarpeellista eikä realistista. Jos siihen pyrkii, työtavoista voi tulla niin vaivalloisia itselle, kollegoille ja potentiaalisille lähteille, että turvallisuusrutiineja aletaan kiertää päivittäisessä työssä. Silloin ne eivät tietenkään toimi. Tiukimmistakaan turvallisuusrutii-

neista ei ole hyötyä, jos ne ovat liian hankalia toteuttaa käytännössä.

Arkisessa aherruksessa kannattaakin noudattaa muutamia joukkovalvonnalta suojaavia toimintatapoja ja kiristää turvallisuustasoa erityistä varovaisuutta vaativan lähteen tai jutun ilmaantuessa näköpiiriin. Tämä edellyttää turvallisuusasioiden pohtimista osana journalistisia työrutiineja.

3. TEHOKKUUS JA KÄYTETTÄVYYS PUNTARISSA

Toimittajan on usein punnittava turvatoimiensa tehokkuutta suhteessa niiden käytettävyyteen.

Viestiliikenteessä sähköpostien salaaminen on varmin keino, mutta entä jos lähde suostuu ottamaan toimittajaan yhteyttä ainoastaan Facebookin chatissa? Jos lähteeltä vaatii salatun sähköpostiviestin lähettämistä, iso juttu saattaa mennä sivu suun. Tällöin voi joutua tyytymään viestittelyn aloittamiseen Facebookissa, ja voi kenties myöhemmin taivutella lähteen turvallisempien menetelmien pariin. Turvallisuus on tärkeää, mutta se ei saa mennä merkittävän journalistisen sisällön edelle. Käytettyjen välineiden on oltava tehokkaita ja riittävän vaivattomia toimittajalle itselleen, hänen kollegoilleen ja lähteilleen.

4. YHTEINEN VASTUU

Digitaalinen turvallisuus on kaikkien vastuulla. Jos joku kollega käyttää heikkoja salasanoja tai napsauttaa viruslinkkiä ja asentaa tietämättään valvontaohjelman toimituksen sisäiseen verkkoon, on aivan sama, kuinka paljon huomiota muut kiinnittävät omaan tietoturvaansa tai millaisia rutiineja he noudattavat.

Siksi turvallisuusrutiineja kannattaa käydä yhdessä läpi toimituksissa, joissa työskentelee useita henkilöitä. Tärkeintä on varmistaa, ettei kukaan klikkaa mitä tahansa internetissä vastaan tulevaa tai asenna tietokoneelleen mitään, minkä turvallisuudesta ei ole

FAKTA: SALAUSTA SOLIDAARISUUDEN NIMISSÄ

Salauksesta huolehtiminen ei ole tärkeää pelkästään yksittäisten toimittajien edun vuoksi. Jos vain kiistanalaisia aiheita työstävät toimittajat salaavat viestiliikennettään, tiedustelu-viranomaisten ja muiden ulkopuolisten on helppo ottaa heidän toimintansa suurennuslasin alle. Kun mahdollisimman monet tavalliset toimittajat käyttävät salaustyökaluja säännöllisesti, syntyvä ”taustamelu” tuo tarpeellista suojaa sekä heille itselleen että muille journalisteille, kun käsillä on erityistä suojaamista vaativa skuuppi tai lähde. Salauksesta huolehtiminen on solidaarinen teko.

täysin varma. Jos työskennellään toimittajatiimissä tavallista korkeampaa turvallisuustasoa edellyttävän jutun parissa, on arvioitava uhat ja sovittava yhteisistä turvatoimista, joita kaikki noudattavat. Tämän oppaan luvussa 4 kerrotaan uhkien arvoinnista.

3

Faktoja valvonnasta

Jotta digitaaliselta valvonnalta voisi suojautua, on ymmärrettävä, mitä se on.

Tässä luvussa kerrotaan internetin toimintaperiaatteesta ja tarkastellaan digitaalisen valvonnan olemusta. Sivuilla 26–27 on yhteenvetokaavio internetin toiminnasta.

Internet

Internet on kiinteä osa useimpien suomalaisten arkea. Monet tietävät, että se on maailmanlaajuinen tietokoneiden muodostama verkko, jossa kaikki on verkottunut keskenään. Mutta miten se toimii?

Kun surfaa verkossa tai räplää Facebookia älypuhelimella, internet voi tuntua suurelta ”pilveltä”, joka on fyysisestä maailmasta irrallaan. Verkossa tapahtuvan toiminnan ajatellaan monesti myös sijoittuvan pelkästään pilveen. Internet on kuitenkin mitä suurimmassa määrin fyysinen verkko. Se on tärkeää muistaa, jos haluaa ymmärtää viestiliikenteen valvonnan maailmaa.

Internet muodostuu lukemattomista verkoista, jotka ovat yhteydessä toisiinsa kaapeleilla. Internetin käyttö edellyttää liittymäsopimuksen tekemistä internetpalveluntarjoajan (internet service provider, ISP) eli internetoperaattorin kanssa. Telian, DNA:n ja Elisan kaltaiset palveluntarjoajat tarjoavat yhteyden muodostamiseen erilaisia vaihtoehtoja, kuten modeemia, langatonta laajakaistaa tai valokuitua. Jos käytttää internetiä vaikkapa työpaikalla tai kahvilassa, jossa on avoin wifi-hotspot tai wlan-verkko, yhteyden tarjoajalla on jälleen oma sopimuksensa internetpalveluntarjoajan kanssa.

Kun internetiä käytetään esimerkiksi sähköpostin lähettämiseen, chat-viestin kirjoittamiseen tai verkkosivustolla käymiseen, tietokone lähettää internetpalveluntarjoajan välityksellä kaapelia pitkin tietueen, joka sisältää tehdyn pyynnön. Tietue päätyy eri verk-

kojen kautta sähköpostin vastaanottajan käyttämälle internetpalveluntarjoajalle tai sitä sivustoa pyörittävälle palvelimelle, jolla on tarkoitus vierailla.

Viestin vastaanottaja tai selattu verkkosivusto taas lähettää kaapelia pitkin verkkojen välityksellä vastaustietueen käyttäjälle.

Jotta maailman jokaisen tietokoneen ei tarvitse olla suoraan yhteydessä kaikkiin muihin tietokoneisiin, internetin muodostavat kaapelit on koottu ylätason internetpalveluntarjoajien alaisuuteen. Ne ovat erikoistuneet erityyppisten verkkojen yhdistämiseen internetiin. Osa näistä niin kutsutuista transit-palveluntarjoajista ylläpitää suuria merenalaisia kuitukaapeleita, jotka yhdistävät maapallon mantereet toisiinsa.

Internetiä käytettäessä syntyviä lähteviä ja saapuvia tietoja siis lähetetään eri yritysten palvelujen kautta eri puolilla maailmaa.

FAKTA: TIETOJA JA METATIETOJA

Elektronisessa muodossa olevaa tietoa eli dataa siirretään internetissä tietueina. Tietueisiin sisältyy kahdenlaisia tietoja:

Data eli avattavan verkkosivun tai lähetettävän viestin sisältö

Metadata eli viestiliikennettä koskeva tieto, kuten keskenään viestivät IP-osoitteet, viestiliikenteen ajankohta ja käytetyt välityskanavat.

Tiedon lähettäminen salaamattomassa muodossa vastaa kaikkien luettavissa olevan postikortin lähettämistä internetverkoston syövereihin. Kuka tahansa lähetystä käsittelevä voi periaatteessa nähdä niin viestin sisällön kuin lähettäjän ja vastaanottajan tiedotkin. Salaaminen tekee tietueista ikään kuin kirjekuoreen suljettuja kirjeitä, joista ulkopuoliset pääsevät näkemään ainoastaan viestiliikenteen metatiedot.

FAKTA: IP-OSOITTEET

Tietueiden lähettämiseksi oikeaan osoitteeseen käytetään niin sanottuja IP-osoitteita (IP = internet protocol). Jokaisella internetyhteydellä on oma ainutkertainen IP-osoitteensa, josta ilmenevät tietokoneen summittainen asema ja käytettävä internetpalveluntarjoaja. Tieto vastaanottajan ja lähettäjän IP-osoitteista on osa tietueen metatietoja.

Esimerkki: *Käyttäjä työskentelee Tampereella ja käy Helsingissä toimivan suomalaisen sanomalehden verkkosivuilla. Käyttäjän tietokone lähettää pyynnön sisältävän tietueen paikalliselle internetpalveluntarjoalle, joka välittää sen tiedonsiirtosiirtokaapelin kautta Espoossa toimivaan datakeskukseen. Sieltä tietue lähtee edelleen verkkosivutilan tarjoavan internetpalveluntarjoajan kautta kaapeliin, joka on yhteydessä lehden palvelimeen Helsingissä. Vastaava mekanismi toimii, kun selataan Yhdysvalloissa sijaitsevaa verkkosivustoa, mutta silloin tietue lähetetään datakeskuksesta Atlantin alapuolista merikaapelia pitkin edelleen Yhdysvaltoihin, missä se kulkee eri verkoissa ennen päätymistään oikeaan osoitteeseen. Tietueet eivät läheskään aina kulje maantieteellisesti lyhintä reittiä, vaan ne voivat kierrellä matkan varrella lukemattomissa maissa ja datakeskuksissa. Kaikki tämä tapahtuu sekunnin murto-osissa. Tietueen ollessa matkalla sen metatiedot ja sisältö ovat täysin sitä käsittelevien yritysten nähtävissä sekä viestiliikennettä tarkkailevien ulkopuolisten ulottuvilla.*

Puhelimet

Matkapuhelin ja eritoten älypuhelin on nykymaailmassa ehdottoman välttämätön työväline useimmille toimittajille. Puhelimet ovat kuitenkin myös hyvin turvattomia välineitä, sillä niitä ei voi suojata valvonnalta yhtä hyvin kuin tietokoneita ja ne kulkevat aina mukanamme.

Puhelimen käyttö puheluihin tai tekstiviesteihin edellyttää liittymäsopimusta teleoperaattorin kanssa. Sopimus avaa reitin tuhansiin tukiasemiin, joita on pystytetty eri puolille maata. Tavallisesti puhelin muodostaa myös internetyhteyden matkapuhelinverkon tukiaseman kautta. Matkapuhelin havainnoi jatkuvasti käyttäjän sijaintipaikkaa ja pyrkii aina luomaan yhteyden tukiasemaan, joka tarjoaa parhaan kuuluvuuden.

Teleoperaattori rekisteröi jokaisen puhelun ja tekstiviestin yhteydessä tukiaseman, johon puhelin on yhteydessä. Tukiasematiedoista saa useimmiten selville, millä paikkakunnalla tai missä kaupunginosassa käyttäjä on, mutta tarkka osoite jää pimentoon. Käyttäjän olinpaikka voidaan siis selvittää summittaisesti.

Älypuhelin tarkkailee sijaintiaan myös GPS-paikannuksen avulla esimerkiksi karttasovellusten ja sosiaalisen median paikannustoimintojen käyttöä varten. Puhelinyhtiöillä on käytettävissään tukiasema- ja sijaintitiedot, ja ne voivat luovuttaa niitä viranomaisille.

Viranomaisten harjoittama joukkovalvonta

Massa- eli joukkovalvonnasta puhui vain harva ennen kuin yhdysvaltalainen tiedusteluanalyytikko Edward Snowden paljasti tuhansia salassa pidettäviä Yhdysvaltain tiedustelupalvelun NSA:n asiakirjoja kesäkuussa 2013.

Snowdenin paljastusten jälkeen on kuitenkin ollut selvää, että NSA valvoo yhdessä monien muiden eri puolilla maailmaa toimivien tiedusteluviranomaisten kanssa internet- ja televiestintää. Valvonnan kohteina on niin ulkovaltojen valtiojohtajia kuin miljoonia tavallisia kansalaisiakin sekä Yhdysvalloissa että muualla. Tiedusteluviranomaiset kiertävät eri maiden perustuslakiin sisältyviä oman maan kansalaisten valvontakieltoja vaihtamalla tietoja keskenään.

Tietoja kerätään muun muassa sopimuksilla, joita on tehty internet- ja teleoperaattorien kanssa sekä sellaisten kolmannen osapuolen palvelujen kuin Googlen, Facebookin ja Skypen kanssa. Suurten internetyritysten kanssa tehtyjen tietojenluovutussopimusten lisäksi NSA ja muut tiedustelupalvelut nappaavat haltuunsa myös internetin kuitukaapeleissa kulkevaa raakadataa.

Molemmilla tavoilla kerätään käsittämättömän paljon tietoa. NSA on omien asiakirjojensa mukaan käsitellyt vuodesta 2012 lähtien päivittäin yli kaksikymmentä miljardia puhelin- ja verkkoviestintätapahtumaa kautta maailman. Tätä suurempiakin lukuja esiintyy – esimerkiksi Ison-Britannian tiedustelupalvelun GCHQ:n haltuun päätyy sisäisten asiakirjojen mukaan lähes viisikymmentä miljardia viestintätapahtumaa päivässä, ja määrä kasvaa kasvamistaan.

FAKTA: INTERNETIN HISTORIA

Internet sai alkunsa osana pohjoisamerikkalaista sotilaallista tutkimushanketta vuonna 1969. Se on levittänyt lonkeronsa kaikkialle maailmaan kahdenkymmenen viime vuoden kuluessa. Suurin osa maailman internetliikenteestä kulkee nykyäänkin Yhdysvaltain kautta pitkälti tämän historiallisen taustan vuoksi.

FAKTA: NSA:N VALVONTAOHJELMAT

Edward Snowdenin merkittävimpiin paljastuksiin lukeutui tieto PRISM-ohjelmasta, jonka avulla NSA saa suoraan käyttöönsä niin sanottujen kolmannen osapuolen palvelujen sisältöä – esimerkiksi Microsoftin, Googlen, Yahoon, Facebookin, YouTuben, Skypen, AOL:n ja Applen palveluissa liikkuvia sähköposteja, chat-keskusteluja, videoita, kuvia, tiedostoja, salasanoja ja paljon muuta tietoa. Muissa paljastuksissa on käynyt ilmi vastaavia tiiviitä yhteistyösuhteita suurimpien tele- ja internetoperaattorien kanssa.

Toinen Snowdenin julki tuomista NSA:n valvontaohjelmista on XKeyscore, jonka avulla tiedustelupalvelu seuloo tietoa valvonnassa käsiteltävästä valtavasta datamassasta. NSA:n omien asiakirjojen mukaan ohjelma kattaa ”lähes kaiken, mitä tyypillinen internetkäyttäjä voi tehdä verkossa”, ja sillä voi tehdä sähköpostien sisältöön, selainhistoriaan, chatteihin ja muihin verkkoaktiviteetteihin kohdistuvia hakuja esimerkiksi sähköpostiosoitteiden, Facebook-tilien ja puhelinnumeroiden perusteella.

Snowdenin muista paljastuksista on käynyt ilmi, että NSA valvoo kohdennetusti kriittisiä toimittajia ja poliittisia aktivisteja. Se myös tartuttaa tietokoneisiin viruksia eri ohjelmien kautta ja asentaa Yhdysvalloista vietäville tietokoneille itse kehittämiään vakoiluohjelmia. Ainakin sadassatuhannessa tietokoneessa eri puolilla maailmaa on haittaohjelma, joka voi valvoa koneen käyttäjiä myös muulloin kuin heidän ollessaan internetissä.

Kuka voi valvoa?

Tietojasi käsittelevien internet- ja teleoperaattorien lisäksi monet muutkin tahot voivat valvoa käyttäjän viestiliikennettä eri vaiheissa ja eri tavoin viestien kulkiessa tietokoneiden ja palvelinten välillä.

Yritykset

Monilla työnantajilla on esteetön pääsy niiden työntekijän käyttöön tarjoamiin sähköpostipalveluihin, työkoneeseen tai työpuhelimeen, ja ne saavat halutessaan tietoonsa niin työntekijän viestintäkumppanit kuin viestinnän sisällönkin. Tämä mahdollisuus voi toimittajan oman työnantajan lisäksi olla myös hänen lähteidensä työnantajilla.

Internetyhteyksiä käyttöön tarjoavat tahot, kuten työnantajat, oppilaitokset ja kahvilat, pääsevät käsiksi sekä metatietoihin että niiden verkossa tapahtuvan viestiliikenteen salaamattomaan sisältöön.

Kun käyttäjä käy jonkin yrityksen verkkosivulla, yritys saa tiedon IP-osoitteesta, josta sen sivustoon on tultu, sekä kävijän liikkumisesta sivustolla.

Hakkerit

IT-jargonissa hakkeri merkitsee periaatteessa vain huipputaitavaa alan asiantuntijaa, mutta nimitystä käytetään yleisesti ihmisistä, jotka tunkeutuvat luvatta tietojärjestelmiin. He voivat käyttää apunaan esimerkiksi haittaohjelmia, mutta heitä vaanii myös avoimissa verkoissa ja hotspoteissa. Jos esimerkiksi kahvilassa on tarjolla helpon tunkeutumisen mahdollistava maksuton wlan, on melko yleinen ilmiö, että hakkerit seurailevat muiden asiakkaiden toimia kahvilan verkossa.

Pilvipalveluyritykset

Suuri osa digitaalisesta toiminnasta tapahtuu nykyisin verkon pilvipalveluissa, joita ylläpitävät kolmannet osapuolet, kuten Google, Facebook, Dropbox, Skype, Yahoo, iCloud, Instagram, Twitter tai Hotmail. Niillä kaikilla on pääsy tietoihin, joita käyttäjä jakaa, lähettää tai tallentaa niiden palveluissa. Tyypillisiä esimerkkejä tällaisista tiedoista ovat Gmail-tilin sähköpostit, kollegojen kanssa Google Drivessa jaettavat tiedostot, chat-keskustelut ja kuvat Facebookissa, yksityisviestit Twitterissä ja tallennetut tiedostot Dropboxissa.

Juuri tämän kaltaiset yritykset ovat Snowdenin paljastusten mukaan antaneet miljoonien asiakkaidensa tiedot suoraan NSA:n ja muiden tiedusteluviranomaisten käyttöön. Edes tietojen suojaaminen salasanalla ei tällöin auta.

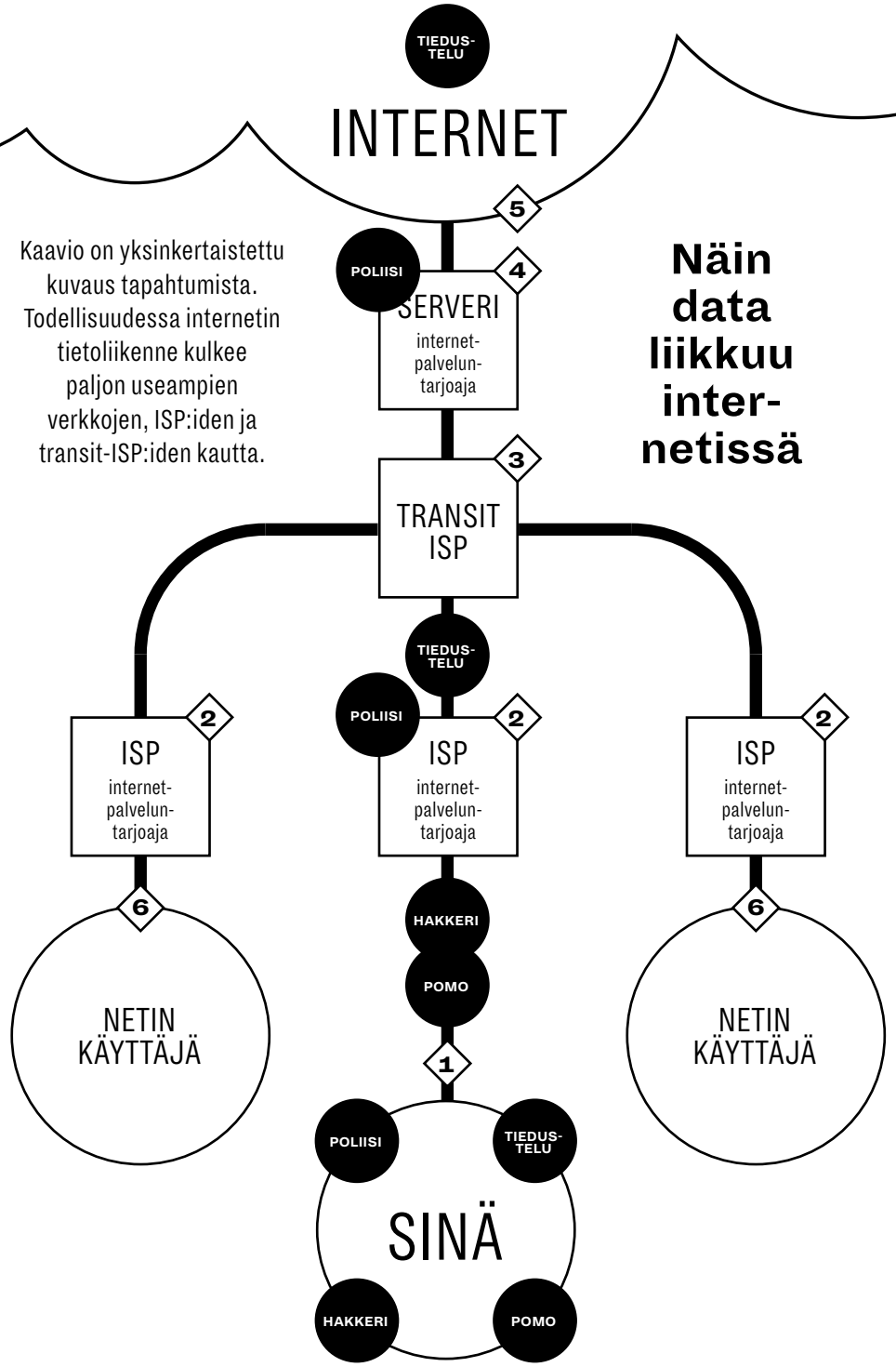
Pilvipalveluissa ei voi viestiä turvallisesti, joten niitä on tietoturvamielessä vältettävä.

1. Internetin viestiliikenne kulkee tietueina kaapeleita pitkin.
2. ISP eli internetpalveluntarjoaja on yritys, jolta käyttäjä hankkii internetyhteyden.
3. Kaikki internetin kaapelit ja verkot yhdistyvät toisiinsa transit-ISP-yritysten kautta.
4. Verkkosivut sijaitsevat palvelimilla, ja sivuilla käydään niiden kautta. Suurilla yrityksillä on yleensä omat palvelimensa.
5. Sosiaalisen median palvelut (esim. Facebook) ja webmail-sähköpostipalvelut (esim. Gmail) ovat internetsivustoja, joihin käyttäjien data tallennetaan. Jos käyttäjällä on Gmail-osoite ja hän kirjoittelee Yahoo-osoitetta käyttävän henkilön kanssa, tietoon pääsevät käsiksi Google, Yahoo, mahdolliset palvelinten ylläpitäjät sekä kaikki ISP:t ja transit-ISP:t.
6. Lähetettäessä sähköpostia muuten kuin verkkopohjaisen sähköpostipalvelun kautta viestiliikenne tapahtuu suoraan lähettäjän ja vastaanottajan ISP:iden ja transit-ISP:iden välillä.

- **Työnantajalla** voi olla suora pääsy työntekijän IT-laitteisiin, sähköposteihin ja tekstiviesteihin sekä yrityksen tietoverkkoon.
- **Hakkerit** voivat murtautua laitteille paikallisverkon kautta, suoraan laitteelta tai jossakin internetliikenteen vaiheessa.
- Kansalliset **poliisiviranomaiset** voivat vaatia ISP:ltä tietoja tai asentaa valvontaohjelmia suoraan epäiltyjen laitteille.
- NSA ja sen liittolaisten **tiedustelupalvelut** nappaavat raakadataa suoraan internetkaapeleista ja vaihtavat sitä keskenään omien kansalaisten valvontakiellon kiertämiseksi.

Näin data liikkuu internetissä

Kaavio on yksinkertaistettu kuvaus tapahtumista. Todellisuudessa internetin tietoliikenne kulkee paljon useampien verkkojen, ISP:iden ja transit-ISP:iden kautta.



4

Uhka-arviointi

Jotta käyttäjä osaisi valita oikeat välineet digitaalisen turvallisuutensa takaamiseksi, hänen on tiedettävä, miltä ja keneltä hän haluaa suojautua. Digitaalista turvallisuutta ei saavuteta välineillä vaan ymmärtämällä siihen kohdistuvia uhkia ja suojautumalla niiltä.

Toimittajan eteen voi tulla monia tilanteita, joissa on tarpeen peittää digitaaliset jäljet valvojilta.

Toimittaja haluaa ehkä estää lähteensä työnantajaa selvittämästä, kuka on antanut kriittisiä lausuntoja tiedotusvälineille, tai välttää sen, että yritys tai viranomainen kiinnittää huomiota sen verkkosivuilla tehtyyn hakuun ja osaa asettautua puolustuskannalle ennen toimittajan uutisen julkaisua. Toimittaja saattaa myös matkustaa diktatuurivaltioon ja saada haltuunsa materiaalia oppositioryhmittymältä, jonka jäsenten nimien paljastuminen sikäläisille viranomaisille tai muille tahoille voi merkitä lähteille kuolemantuomiota.

Eri tilanteissa tarvitaan erilaisia välineitä ja turvallisuustasoja. Uhka-arvioinnin avulla voi määrittää, mitkä välineet soveltuvat parhaiten kulloinkin käsillä olevan tilanteen hoitamiseen. Perusteellisessa uhka-arvioinnissa vastataan viiteen keskeiseen kysymykseen:

1. Mitä halutaan suojata?
2. Keneltä sitä halutaan suojata?
3. Millaisia hyökkäyksiä vastapuoli saattaisi tehdä?
4. Miten suuri riski on?
5. Miten voi estää riskin toteutumisen?

Tietoturvaan liittyviä oikeuksia puolustava Electronic Frontier Foundation -järjestö käyttää digitaalisessa itsepuolustusoppaassaan seuraavia käsitteitä, joita voi hyödyntää uhka-arvion kysymyksiin vastaamisessa.

Omaisuus

Digitaalisen turvallisuuden alalla suojeltavaan materiaaliin viitataan usein omaisuutena. Se on käsite, jota tarvitaan, kun vastataan ensimmäiseen kysymykseen.

Omaisuus voi olla sähköposteihin, chat-viesteihin ja tiedostoihin sisältyvää informaatiota, yhteystietoluettelo tai vaikkapa lähteen henkilöllisyys. Se voi olla tekninen väline, kuten tietokone tai puhelin, tai tieto siitä, minkä aiheen parissa toimittaja työskentelee.

Omaisuuden kartoittamiseksi voi laatia luettelon tallennetusta tiedosta, sen tallennuspaikoista, henkilöistä, joilla on pääsy tietoon, ja pääsyä rajoittavista seikoista.

On syytä ottaa huomioon yhtä lailla mahdollisten vastapuolten digitaalinen ja fyysinen pääsymahdollisuus omaisuuteen.

Vastapuolet

Toiseen kysymykseen vastaamiseen tarvitaan vastapuolten käsitettä. Vastapuoli on henkilö tai organisaatio, joka muodostaa omaisuuteen kohdistuvan uhan.

Ketä voisi kiinnostaa saada tiedot käsiinsä? Tällaisia tahoja voivat olla esimerkiksi lähteen työnantaja tai lähde itse, henkilöt, joita mainitaan jutussa tai joilla on siihen liittyvä intressi, kilpailevat tiedotusvälineet tai toimittajat, viranomaiset, poliitikot, rikollisjärjestöt tai muut haastatellut lähteet. Toimittajan tiedot voivat kiinnostaa myös tiedusteluviranomaisia ja paikallisia toimijoita muissa maissa tai paikallisia asukkaita pienissä yhteisöissä, joissa uteliaat muukalaiset pannaan varmasti merkille.

Suuri merkitys on myös sillä, haluaako suojautua sattumanvaraiselta joukkovalvonnalta vai kohdennetulta yksilölliseltä valvonnalta. Ensin mainittu kohdistuu kaikkiin – myös toimittajiin. Jälkimmäinen voi tulla kyseeseen, jos toimittaja on yhteydessä sellaiseen lähteeseen tai tutkii sellaista juttua, joka lisää kohdennetun valvonnan todennäköisyyttä.

Kapasiteetti

Kolmanteen kysymykseen vastatessa on arvioitava vastapuolen tai -puolien kapasiteettia. Vastapuolten kapasiteetti vaihtelee merkittävästi, ja ne voivat uhata omaisuutta eri tavoin.

Toimittaja voi joutua alttiiksi teknisille hyökkäyksille esimerkiksi hakkeroinnin, viestiliikenteen sähköisen valvonnan tai salasanojen murtamisen muodossa. Oikeudelliset hyökkäykset taas saattavat tulla kyseeseen, jos poliisi- tai tiedusteluviranomainen voi oikeuden päätöksellä vaatia teleoperaattoreita luovuttamaan käyttäjän viestiliikennetietoja.

Sosiaalisissa hyökkäyksissä toimittajan kollegoita tai lähteitä voidaan painostaa tai huijata luovuttamaan salasanoja tai tietoja.

Fyysiset hyökkäykset puolestaan voivat olla mitä tahansa laitteiden varastamisesta näkyvillä olevien tietojen urkkimiseen.

Hyökkäysten tyypit ja tavoitteet vaihtelevat, kuten vastapuolten kapasiteettikin. Lähteen työnantaja saattaa esimerkiksi lukea hänen työsähköpostejaan tai työpuhelimensa tekstiviestejä saadakseen selville, kuka on mustannut työpaikan mainetta julkisuudessa. Eri valtioiden tiedusteluviranomaiset taas saattavat etsiä maansa järjestelmään kriittisesti suhtautuvia ihmisiä, joilla on yhteyksiä ulkomaalaisiin toimittajiin.

Poliisi- tai tiedusteluviranomainen voi vaatia internetpalveluntarjoajaa luovuttamaan tietoja toimittajan liikkumisesta digitaalisessa maailmassa päästäkseen tietovuodon tekijän jäljille tai estääkseen paljastusjuttujen julkaisun. Muut vastapuolet saattavat haluta poistaa, muuttaa tai julkistaa tietoja, joihin ne pääsevät käsiksi murtautumalla toimittajan sähköiseen viestintään.

Luvussa 3 kerrottiin siitä, kuka digimaailmassa voi valvoa ja mitä. Ne ovat perustietoja, joiden avulla voi arvioida mahdollisia vastapuolia ja niiden kapasiteettia.

Riski

Vaikka toimittajalla olisi vastapuolia, joilla on kapasiteettia, ne eivät välttämättä käytä sitä häntä vastaan. Toimittajan on kuitenkin punnittava vastatoimien mahdollisuutta ja suojauduttava niiltä.

Digitaalisessa turvallisuudessa erotetaan toisistaan uhat ja riskit. Uhka on jotakin, mikä voi toteutua, ja riski sen toteutumisen todennäköisyys. Neljänteen kysymykseen vastaamiseksi on tehtävä riskianalyysi eli arvioitava tunnistettujen uhkien toteutumisen todennäköisyys. Analyysi helpottaa suojautumiseen käytettävien välineiden valitsemista ja keinojen laajuuden määrittämistä.

Samassa yhteydessä on arvioitava myös turvallisuuspoikkeaman mahdollisia seurauksia. Turvallisuustason nostaminen voi olla tarpeen, jos uhan toteutumisen seuraukset ovat vakavia – vaikka hyökkäyksen todennäköisyys olisi pieni. Tällaisia seurauksia voivat olla esimerkiksi lähteen vainoaminen tai vangitseminen.

Vastaavasti toimittaja voi laskea turvallisuustasoa, vaikka tietäisi, että häntä valvotaan, mutta viestinnän paljastumisella ei olisi sen suurempia seurauksia. Tiedusteluviranomainen ei tee mitään esimerkiksi sellaisella tiedolla, että on toimittajan vuoro hankkia pullat toimituspalaveriin.

Sen vuoksi viimeinen kysymys onkin, mitä tapahtuu, jos vastapuoli saa toimittajan hallussa olevaa informaatiota itselleen.

KOKEILE ITSE!

Nyt olet valmis tekemään ensimmäisen uhka-arviosi viereisen kaavion avulla.

Täytä kaavioon tiedot suojeltavasta omaisuudesta, vastapuolista, joilla voi olla pääsy yksityisiin tietoihisi, ja siitä, kuinka todennäköisesti ne pyrkivät hankkimaan pääsyn.

Kun olet täyttänyt kaavion, voit laatia tietojen perusteella turvallisuussuunnitelman, joka kaikkien jutun parissa työskentelevien on ymmärrettävä ja otettava käyttöön.

Ensimmäisiin kenttiin on täytetty mahdollisia esimerkkejä.

Omaisuus	Vastapuoli	Kapasiteetti	Riski
Viestintä työnantaja-yritystään kritisoivan työntekijän kanssa	Lähteen työnantaja	Työnantajalla on pääsy työntekijän sähköpostiin ja puhelimeen, ja se saattaa voida jäljittää vuodon työpaikan laitteita käyttäneeseen työntekijään.	Lähde saatetaan erottaa tai häntä voidaan painostaa eri tavoin.
Yrityksen kotisivuilla tehdyt haut kriittisen jutun taustoittamiseksi	Tutkimus-kohde	Yritys voi tutkia, mistä IP-osoitteista sen verkkosivustolla käydään usein ja mitä kävijät sivustolla tekevät.	Yritys voi kiinnittää huomiota taustatyöhöni liian aikaisin ja esimerkiksi piilottaa tärkeitä asiakirjoja.
Alistetun oppositioryhmittymän valokuvat konfliktialueelta	Paikalliset viranomaiset	Paikalliset viranomaiset voivat valvoa viestintää tai takavarikoida tietokoneeni esimerkiksi rajalla.	Mahdollisesti erittäin vakavia seurauksia lähteilleni, jos henkilöllisyydet paljastuvat.
Vuodettu tiedusteluviranomaisen raportti	Poliisi- ja tiedusteluviranomaiset	Poliisi voi tehdä laitteisiin ja lokitietoihin kohdistuvan etsinnän harjoittaen kohdennettua digitaalista valvontaa. Tiedustelupalvelu voi tehdä hakuja raakadatasta ja jäljittää lähteen tietoteknisten laitteiden, kuten tulostinten tai tietokoneen, käyttöä.	Lähde saattaa menettää työpaikkansa ja saada oikeudellisia seuraamuksia, ja raskauttavat asiaa koskevat tiedot voidaan tuhota.

TURVALLISUUSSUUNNITELMA

Kun olet täyttänyt kaavion, voit laatia tietojen perusteella turvallisuussuunnitelman.

Suunnitelma voi koskea yleisesti toimittajantyösi arkea tai jotakin yksittäistä projektia – esimerkiksi ulkomaanmatkaa tai tiettyä juttua.

Tärkeää on, että siinä kuvataan työtavat, jotka kaikkien jutun parissa työskentelevien on ymmärrettävä ja otettava käyttöön.

5 Salausvälineitä päivittäiseen käyttöön

FAKTA: MILTÄ SALATTU VIESTI NÄYTTÄÄ

Digitaalisen salauksen käyttö tietokoneella muuttaa ymmärrettävän viestin pitkäksi lukukelvottomien merkkien jonoksi, jonka voi lukea ainoastaan ainutkertaisen salausavaimen avulla. Seuraavassa esimerkissä on käytetty AES-salausalgoritmia.

Salaamaton viesti:
Hei äiti!

Salattu viesti:
YzJiOTBkY2FmNzk3YjM4ZTJlYmU4Y2QzYzdhZjgyOGQ=

Monet käyttävät salausta eri muodoissaan päivittäin. Sitä tarvitaan esimerkiksi verkkopankkiin kirjautumisessa. Lyhyesti selitettynä salaaminen eli kryptaus on tekstin tai muun aineiston muuntamista lukukelvottomaksi numero- ja kirjainjoukoksi, jotta sen sisältö pysyisi salassa ulkopuolisilta.

Esimerkiksi sähköposti- tai tekstiviestejä voi salata, samoin puhelimen tai tietokoneen massamuistin. Jos vastapuoli saa haltuunsa salatun viestin tai yrittää tunkeutua salatulle tietokoneelle, hänellä on edessään vain pitkä salakielinen merkkijono, josta hän ei ymmärrä mitään.

Tässä kirjassa kerrotaan kahdesta salaustyypistä: massamuistin salauksesta, jolla voidaan salata laitteille tallennettua sisältöä, sekä päästä päähän -salauksesta, jolla salataan viestintäkumppanien välistä viestintää.

On tärkeää käyttää kumpaakin salaustapaa.

Kun sähköpostiviesti lähetetään salattuna, se on turvassa matkalla lähettäjältä vastaanottajalle. Lähettäjän ja vastaanottajan tietokoneille on kuitenkin tallennettu viestin salaamiseen ja salauksen purkamiseen tarvittavat salausavaimet, ja viesti voi olla tietokoneella myös salaamattomassa muodossa. Jos tietokoneen suojaamisesta ei ole huolehdittu, mahdollinen vastapuoli voi tunkeutua tietokoneelle takaportin kautta ja hankkia viestin sisällön haltuunsa salauksesta huolimatta.

Digitaalinen turvallisuus on kunnossa vain, kun sekä viestintään käytettävät laitteet että viestiliikenne salataan.

Kirjan seuraavissa luvuissa kerrotaan välineistä, joita toimittajan kannattaa ottaa työkalupakkiinsa digitaalisen turvallisuuden varmistamiseksi. Luvuissa käsitellään laitteiden suojaamista, vahvoja salasanoja, viestiliikenteen salaamista ja digitaalisten jälkien peittämistä.

Kun työkaluja käytetään tarkoituksenmukaisesti, edes koko maailman tietokoneiden laskentateho ei riitä salausten murtamiseen.

5

FAKTA: AVOIN LÄHDEKOODI

Lähes kaikki tässä kirjassa suositeltavat välineet ovat tietokoneen tai puhelimen käyttöjärjestelmään sisältyviä ominaisuuksia tai maksuttomia avoimen lähdekoodin ohjelmia.

Avoimella lähdekoodilla (open source) tarkoitetaan sitä, että ohjelman laatija on saattanut sen lähdekoodin julkisesti saataville. Koodin avulla kuka tahansa voi nähdä ohjelman toimintaperiaatteen sekä auttaa havaitsemaan mahdollisia turvallisuuspuutteita ja osallistua ohjelman parantamiseen. Riippumattomat tietoturva-asiantuntijat testaavat useimpia yleisiä avoimen lähdekoodin ohjelmia säännöllisesti niiden laadun varmistamiseksi. Näin estetään esimerkiksi se, että ohjelmoijat voisivat piilottaa sovelluksiinsa takaportteja, joiden kautta ulkopuoliset pääsisivät sisään sovelluksiin tai laitteisiin.

Läpikotaisin testatut, jo jonkin aikaa markkinoilla olleet ja jatkuvasti päivitettävät avoimen lähdekoodin sovellukset ovat aina suositeltava ratkaisu tietoturvasta huolehtimiseen. Kannattaa ottaa tavaksi etsiä sovelluksista ja niiden julkaisijoista tietoa myös internetistä. Ovatko ne saaneet kiittäviä arvioita digitaalisen turvallisuuden tuntijoilta – vai onko sovellus kenties joutunut tietomurtojen kohteeksi tai sen julkaisija taipunut tiedusteluviranomaisten painostuksen alla?

6 Laitteiden suojaaminen

Tietoteknisten järjestelmien pääkomponentit ovat laitteisto ja ohjelmistot. Laitteet ovat fyysisiä esineitä ja ohjelmat niissä toimivia sovelluksia.

Laitteiden suojaaminen on aivan yhtä tärkeää kuin viestinnänkin suojaaminen.

Seuraava rinnastus paperimuotoiseen viestintään kuvastaa tietoturvan merkitystä. Ystävä lähettää toiselle luottamuksellisen kirjeen suljetussa kirjekuoressa, jotta postinkantaja ei voi lukea sitä. Kun kuori on avattu ja kirje luettu, ne jäävät kirjoituspöydälle. Siksi on tärkeää huolehtia talon ovien lukituksesta, jotta kukaan ei pääse livahtamaan sisään takaovesta ja lukemaan kirjettä.

Tässä luvussa kerrotaan kovalevyn salaamisesta ja muista keinoista, joilla laitteita voi suojata.

Massamuistin salaus

Massamuistin salauksella tietokoneen ja puhelimen voi lukita samaan tapaan kuin talon oven.

Vaikka tietokoneessa tai puhelimessa käytettäisiin PIN-koodilukitusta, laitteisiin voi murtautua monin eri tavoin, jos ne joutuvat pois käyttäjänsä hallusta – silloinkin, kun laitteen virta katkaistu. Tietokoneen kovalevyn voi esimerkiksi siirtää toiseen tietokoneeseen ja päästä käsiksi kaikkiin sille tallennettuihin tiedostoihin. Tämä vaara on olemassa sekä viranomaisten tekemän takavarikon yhteydessä että silloin, kun laite varastetaan tai unohtuu jonnekin.

Vaaralta voi suojautua käyttämällä laitteessa koko kovalevyn suojausta. Tällöin kaikki tietokoneella tai puhelimessa olevat tiedot salataan, kun laitteen virta on katkaistu. Jos ulkopuoliset yrittävät tunkeutua suljettuun laitteeseen, kovalevy menee lukkoon, ja tunkeutujan kouraan jää vain valtava määrä lukukelvotonta koodia.

Monissa uusissa matkapuhelinmalleissa salatun yksikön voi avata sormenjälki- tai kasvojentunnistuksella tai PIN-koodilla.

Tietokoneen koko levyn salauksen yhteydessä on käytettävä salasanasuojausta. Syöttämällä salasanan pääsee käsiksi myös salattuun levyyn. Siksi salasanan on oltava vahva ja mahdoton murtaa. Luvussa 7 kerrotaan tällaisten salasanojen luomisesta. Salasanan on *ehdottomasti* oltava helppo painaa mieleen, eikä se saa päätyä asiattomien haltuun.

Siksi on ehdottomasti syytä ottaa levyn sisällöstä varmuuskopio ennen kuin koko levyn salaus kytketään päälle. Salauksen aktivoimiseen kannattaa myös varata aikaa ja hakeutua rauhalliseen paikkaan, jossa kukaan ei pääse urkkimaan salasanaa kurkkimalla olan yli. Salasanan voi tarvittaessa kirjoittaa muistiin paperilapulle, joka säilytetään turvallisessa paikassa erillään laitteesta, kunnes käyttäjä muistaa salasanan vuorenvarmasti.

Menettely voi kuulostaa vaivalloiselta, mutta koko levyn salauksen käyttö on digitaalisen turvallisuuden A ja O.

MUISTA!

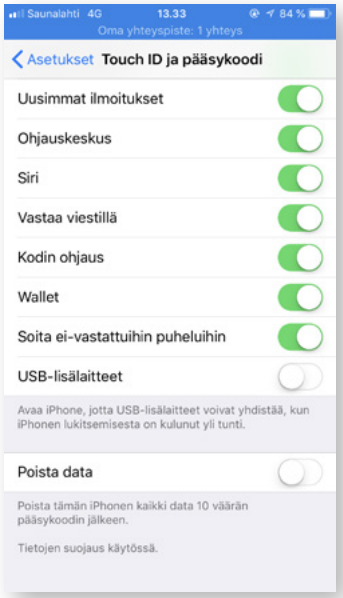
Jos salasana unohtuu, kun koko levyn salaus on käytössä, mitään levyllä olevaa aineistoa ei voi käyttää.

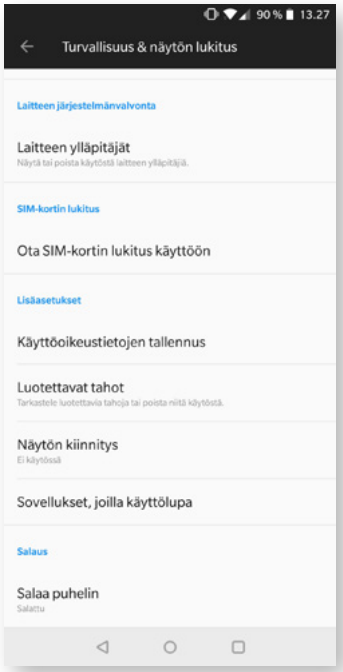
6.1 Massamuistin salaus puhelimessa

Kun puhelimessa on käytössä massamuistin salaus ja sen virta on katkaistu, puhelimen tietoihin ei pääse käsiksi ilman lukituksen avaavaa PIN-koodia tai biometristä tunnistetta. Jos joku yrittää tunkeutua puhelimeen, se lukittuu, ja tunkeutujan kouraan jää vain valtava määrä lukukelvotonta salakieltä.

Kun toimittaja matkustaa ulkomaille tai muuhun paikkaan, jossa voi olla olemassa puhelimen takavarikoimisen vaara, puhelimen voi suojata salauksella ja katkaista siitä virran sen jälkeen kokonaan.

Useimmissa uusissa älypuhelinmalleissa suojaus on käytössä oletusasetuksena.





VAIHE VAIHEELTA: IPHONE

iPhonesta salauksen päälläolon voi tarkistaa asetusvalikon kohdasta *Touch ID ja pääsykoodi*.

Avautuvan valikkosivun alareunassa näkyy teksti *Tietojen suojaus käytössä*. Tämä osoittaa, että iPhonessa käytetään massamuistin suojausta.

Heti suojauksesta kertovan tekstin yläpuolella käyttäjä voi asettaa puhelimen poistamaan kaikki tiedot, jos pääsykoodi syötetään väärin kymmenen kertaa peräkkäin. Asetuksen käyttöönottoon sisältyy riski, että tiedot häviävät silloinkin, kun käyttäjä itse esimerkiksi yrittää avata laitteen lukituksen sormenjälkitunnistuksella mutta käyttää väärää sormea.

Toiminnon voi aktivoida, jos matkustaa sellaiselle seudulle tai työstää sellaista juttua, että on syytä pelätä puhelimen takavarikointia ja pyrkimyksiä tunkeutua siihen.

VAIHE VAIHEELTA: ANDROID

Android-puhelimista salauksen voi tarkistaa asetusvalikon suojausasetuksista. Suojausasetusten tarkka sijainti vaihtelee eri puhelinmalleissa. Joissakin malleissa ne löytyvät kohdasta *Asetukset* → *Turvallisuus & näytön lukitus* → *Salaus*. Jos puhelimen ilmoitetaan olevan salattu, muistin salaus on käytössä.

Jos matkapuhelin ei ole aivan uusi, massamuistin suojaus on kytkettävä päälle erikseen. Se tehdään samassa asetusvalikossa, jossa PIN-koodi vaihdetaan.

BIOMETRINEN JA MANUAALINEN TUNNISTAUTUMINEN

Useimmissa uusissa puhelinmalleissa on mahdollisuus käyttää biometristä tunnistautumista, kuten sormenjälkeä, kasvojentunnistusta tai iiristunnistusta. Ajatus voi tuntua epämiellyttävältä, mutta useimmiten biometrinen tunnistautuminen on turvallisempaa kuin tavanomaisen PIN-koodin käyttäminen. Pääsykoodi on nimittäin mah-

dollista saada haltuun kurkkimalla käyttäjän olan yli tai arvaamalla, jos koodi on liian helppo tai ilmeinen.

Kuten digitaalisessa turvallisuudessa yleensäkin, turvallisin ratkaisu määräytyy aina tilannekohtaisesti.

Toimittaja saattaa joutua tilanteeseen, jossa vastapuoli voi pakottaa hänet avaamaan puhelimen lukituksen joko fyysisesti pakottamalla tai uhkaamalla oikeudellisilla seuraamuksilla.

Vastapuoli voi myös avata puhelimen sen käyttäjän biometrisellä tunnisteella esimerkiksi painamalla puhelimen käyttäjän peukaloa vasten tai pitämällä sitä tämän kasvojen edessä. Numeerinen pääsykoodi voi olla biometristä tunnistetta turvallisempi, jos voidaan olettaa, ettei käyttäjää pakoteta paljastamaan koodia. Tunnistautumistapaa voi muuttaa puhelimen asetuksista.

Joissakin maissa viranomaiset voivat lain nojalla pakottaa käyttäjän avaamaan puhelimensa lukituksen kasvojentunnistuksen avulla, mutta pääsykoodia ei ole pakko paljastaa.

Jos toimittaja arvioi, että voi joutua avaamaan puhelimensa lukituksen tunnistautumistavasta riippumatta, voi olla paras vaihtoehto poistaa puhelimesta kaikki arkaluonteiset tiedot ja yksinkertaisesti avata lukitus, kun sitä vaaditaan.

PÄÄSYKOODIN PITUUS

Jos turvallisin vaihtoehto vaikuttaisi olevan puhelimeen käsin syötettävä pääsykoodi biometrisen tunnistautumisen sijaan, koodin on oltava vähintään kahdeksanmerkkinen.

Useimmilla vastapuolilla on käytettävissään koodien murtamiseen tarvittava laitteisto, ja tavallinen nelinumeroinen koodi aukeaa helposti. Siksi pääsykoodin on oltava riittävän pitkä ja monimutkainen.

Tietenkin pitkän koodin syöttäminen puhelimen avaamiseksi jokaisella käyttökerralla on hieman hankalampaa kuin lyhyen koodin, joten on arvioitava vaivaa suhteessa turvallisuusriskiin. Jos pitkän pääsykoodin syöttäminen aina ennen puhelimen käyttöä tuntuu liian vaikealta, on parempi käyttää lyhyttä koodia mieluummin kuin jättää koodi kokonaan pois.

MUISTA!

Pääsykoodi on ehdottomasti pystyttävä muistamaan, sillä muuten puhelinta ei voi käyttää. Siksi puhelimen tiedot kannattaa varmuuskopioida aina ennen pääsykoodin muuttamista.

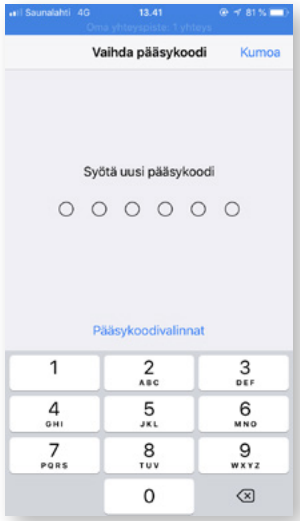
VAIHE VAIHEELTA: IPHONE

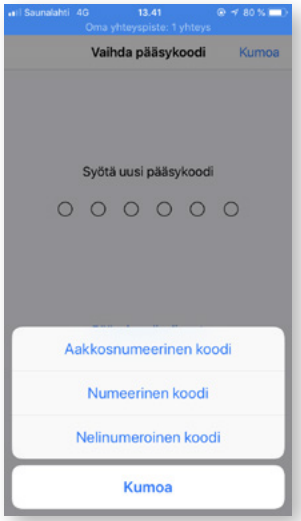
1. Pääsykoodin pituutta voi muuttaa asetusvalikon kohdassa *Touch ID ja pääsykoodi*. Valitse *Vaihda pääsykoodi*.

2. Syötä nykyinen pääsykoodisi. Näyttöön avautuu sivu, jolla sinua pyydetään syöttämään uusi koodi. Älä syötä uutta koodia vaan valitse *Pääsykoodivalinnat*.

3. Valitse *Aakkosnumeerinen koodi*. Nyt voit syöttää uuden moninumeroisen pääsykoodin. Koodissa on syytä olla vähintään kahdeksan merkkiä – niin numeroita, kirjaimia kuin erikoismerkkejäkin.

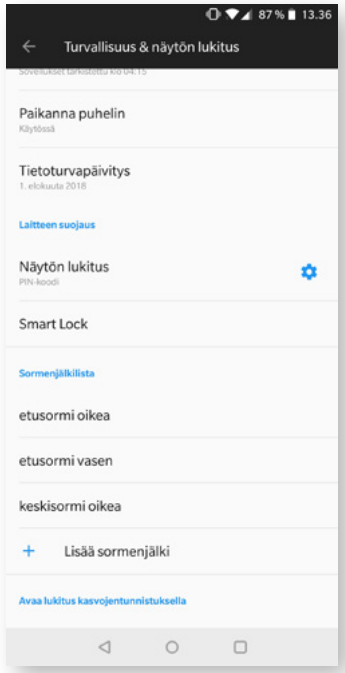


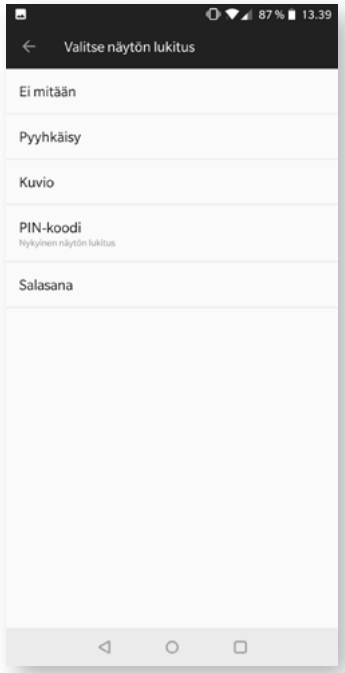




VAIHE VAIHEELTA: ANDROID

1. Näppärän nelinumeroisen PIN-koodin voi ottaa käyttöön helposti asetusvalikon kautta lukitusnäytön asetuksissa (joissakin malleissa *Asetukset* → *Turvallisuus & näytön lukitus* → *Näytön lukitus* → *PIN-koodi*).
2. Kuvion sijaan koodiksi voi valita lyhyen PIN-koodin tai pidemmän salasanan. Valitsemalla salasanan puhelimeen voi asettaa vahvan salalauseen luvun 7 ohjeiden mukaan.



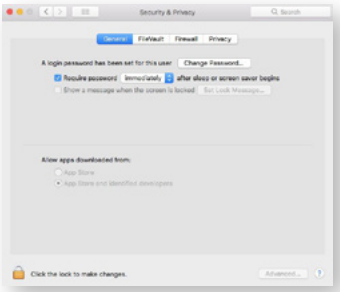


FAKTA: IPHONE VAI ANDROID?

Yleisesti iPhonen tietoturvaa pidetään huomattavasti parempana kuin Android-puhelinten. Yksi syy on se, että Android-käyttöjärjestelmää käytetään useiden eri valmistajien puhelimissa, eikä niihin aina tarjota järjestelmällisiä tietoturvapäivityksiä. Sen vuoksi Android-puhelimet ovat iPhonea alttiimpia viruksille ja haittaohjelmille.

Apple panostaa turvallisuuteen johdonmukaisesti, ja sen puhelimissa oleva turvasiru estää ulkopuolisten yritykset murtaa puhelimen pääsykoodi väsytyshyökkäyksillä. Väsytyshyökkäyksessä eli kryptoanalyysihyökkäyksessä käyttäjätiliä pommitetaan lukemattomilla pääsykoodeilla, kunnes oikea koodi löytyy.

Apple on myös ilmoittanut, että iOS 12 -käyttöjärjestelmäversioon tulee suojaus useita poliisiviranomaisten käyttämiä hakkerointikeinoja vastaan. Näin se haluaa suojella iPhone-käyttäjien yksityisyyttä.





6.2 Tietokoneen massamuistin salaus

VAIHE VAIHEELTA: MAC

1. Applen ohjelma kovalevyn salaukseen on nimeltään FileVault. Se sisältyy valmiiksi OS X -käyttöjärjestelmän uusimpiin versioihin. FileVault sijaitsee *Järjestelmäasetukset*-valikon kohdassa *Suojaus ja yksityisyys*. Asetusten muuttamiseksi napsauta lukkosymbolia ja sen jälkeen *Laita FileVault päälle* -painiketta.
2. Saat järjestelmästä palautusavaimen, jolla tietokoneen lukituksen voi avata, jos sen kirjautumissalasana unohtuu. Kirjoita avain muistiin jonnekin muualle kuin tietokoneelle ja tallenna se erittäin turvalliseen paikkaan. Kun siirryt eteenpäin *Jatka*-painikkeella, Apple tarjoutuu säilyttämään palautusavaimen puolestasi. Hylkää ehdotus, sillä Apple on aiemmin luovuttanut asiakkaiden luottamuksellisia tietoja tiedustelupalvelu NSA:lle. Jos joku ulkopuolinen saa tietoonsa tietokoneen palautusavaimen, hän pääsee käsiksi koko kovalevyn sisältöön salauksesta huolimatta.
3. Seuraavaksi tietokone on käynnistettävä uudelleen. Uudelleenkäynnistyksen jälkeen levyn salaus kytkeytyy toimintaan. Aktivoituminen kestää tovin, mutta tietokonetta voi käyttää sillä välin normaalisti.
4. Kun levyn salaus on valmis, tietokone on suojattu tehokkaasti koko kovalevyn salauksella, eivätkä ulkopuoliset pääse käsiksi sen tietoihin ilman kirjautumissalasanaa. Muista kytkeä lukitus jälleen päälle ennen kuin poistut järjestelmäasetuksista, jotta asetukset eivät voi muuttua.

MASSAMUISTIN SALAUS WINDOWS-YMPÄRISTÖSSÄ

Valitettavasti koko levyn salaaminen ei Windows-tietokoneissa onnistu yhtä helposti kuin Maceissa.

Joihinkin Windows-käyttöjärjestelmäversioihin sisältyy BitLocker-niminen salaustyökalu, ja turvallisinta onkin käyttää tällaisia versioita. Microsoftin ohjesivustolla microsoft.com/fi-fi/windows opastetaan BitLocker-salauksen käyttöönotossa.

Jos Windows-tietokoneella ei ole BitLockeria, sen turvallisuutta voi parantaa hieman vaihtamalla kirjautumissalasanaa, joka on syötettävä koneeseen sen käynnistämisen yhteydessä.

Useimpien käyttäjien salasanat ovat liian lyhyitä ja helposti murrettavissa. Vaihtamalla salasanaksi vahvan salalauseen ja huolehtimalla siitä, ettei kukaan voi käyttää tietokonetta ilman kyseistä salasanaa, koneen tiedot pysyvät suojassa perustason tietoturvahyökkäyksiltä. Luvussa 7 kerrotaan vahvojen salalauseiden luomisesta.

FAKTA: KANNETTAVA VAI PÖYTÄKONE?

Toimittajat käsittelevät työssään usein arkaluonteisia tietoja. Silloin joka paikkaan helposti mukana kulkeva kannettava tietokone on parempi vaihtoehto kuin pöytäkone, jota on mahdotonta pitää silmällä jatkuvasti niin kotona kuin työpaikallakin.

Hyvä ratkaisu voi olla erillisen tietokoneen tai puhelimen hankkiminen työkäyttöön, jotta siinä voi ylläpitää korkeampaa suojaustasoa kuin yksityiskäytössä olevassa laitteessa.

FAKTA: APPLE VAI WINDOWS?

Tietokoneiden maailmassa on mahdotonta vastata yksiselitteisesti kysymykseen siitä, onko tietoturva paremmalla tolalla Apple- vai Windows-tietokoneissa.

Applen tuotteet eivät ole niin alttiita haittaohjelmille ja muille tartunnoille kuin pc-tietokoneet, ja niissä on laajat salausominaisuudet. Haittapuolena on se, että Apple-tietokoneissa voi käyttää ainoastaan valmistajan omaa käyttöjärjestelmää. Windows-tietokoneeseen puolestaan voi halutessaan asentaa alkuperäisen käyttöjärjestelmän tilalle avoimen lähdekoodin käyttöjärjestelmän, esimerkiksi Linuxin.

6.3 Vahva kirjautumissalasana

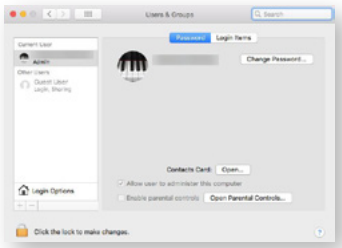
Kovalevyn salaus on toiminnassa silloin, kun tietokone on sammutettu. Usein kuitenkaan tietokonetta ei sammuteta kokonaan – esimerkiksi kesken työpäivän tai tien päällä työskenneltäessä.

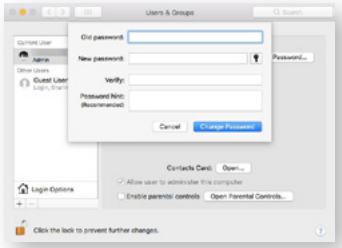
Siksi on tärkeää käyttää tietokoneessa vahvaa kirjautumissalasanaa, joka täytyy syöttää aina ennen kuin konetta voi alkaa käyttää.

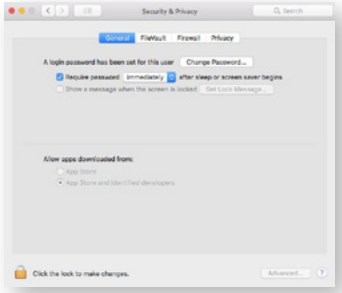
Tietokoneen asetusten on oltava sellaiset, että salasana vaaditaan aina, kun koneen kansi on ollut kiinni tai kun se on nukahtanut oltuaan tietyn aikaa käyttämättä. Tämä on perustason varotoimi vastapuolten hyökkäyksiltä suojautumiseksi siinä tapauksessa, että vastapuoli on saanut haltuunsa nukkuvan tietokoneen ja sen pääsykoodin.

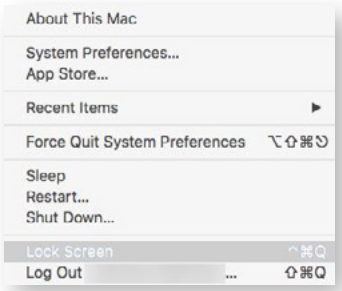
Tietokoneen kirjautumissalasana voi aivan hyvin olla sama kuin koko levyn salauksessa käytettävä salasana.

VAIHE VAIHEELTA: MAC









1. Vaihda kirjautumissalasanasi *Järjestelmäasetusten* kohdassa *Käyttäjät ja ryhmät*. Napsauta näytön vasemmassa alakulmassa olevaa lukkosymbolia ja valitse luvussa 7 kuvattujen periaatteiden mukainen vahva salasana, jonka varmasti muistat. Samaa salasanaa tarvitset myöhemmin, jos haluat muuttaa tietokoneen järjestelmäasetuksia napsauttamalla lukkosymbolia.

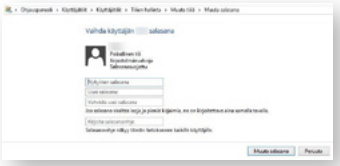
2. Näyttöön avautuneessa ikkunassa pyydetään syöttämään salasanavihje. Älä syötä sitä. Kyseessä on turvakysymyksen kaltainen elementti, jonka on tarkoitus helpottaa salasanan muistamista. Salasanavihjeen myötä Apple saisi haltuunsa keinon turvallisen salasanasi murtamiseen, ja se on aiemmin luovuttanut asiakkaidensa luottamuksellisia tietoja NSA:lle.

3. Siirry *Järjestelmäasetusten Suojaus ja yksityisyys* -valikon *Yleinen*-osioon. Valitse *Vaadi salasana herääämisen jälkeen tai näytönsäästäjän käynnistyttyä* -kentässä vaihtoehto *välittömästi*. Näin voit varmistaa, ettei tietokonetta voi käyttää ilman salasanaa, kun sen kansi on ollut kiinni tai näytönsäästäjä päällä.

4. Tietokoneen on oltava suojattu salasanalla myös silloin, kun jätät sen päälle ilman valvontaa esimerkiksi kahvitauon ajaksi. Sen voi hoitaa näytön lukitustoiminnolla, joka aktivoituu napsauttamalla omenakuvaketta päävalikkorivin vasemmassa yläkulmassa. Näin voit varmistaa, ettei tietokonetta voi käyttää ilman salasanaa, kun se jää auki ja päälle ilman valvontaa.

Vanhemmissa Apple-tietokoneissa toiminto sijaitsee eri paikassa ja edellyttää Avainnipun käyttö -sovelluksen käyttöä. Sen voi avata *Ohjelmat*-kansion *Lisäohjelmat*-kohdassa. Toinen vaihtoehto on etsiä sovellus napsauttamalla hakutoimintoa kuvastavaa suurennuslasikuvaketta näytön valikkorivillä oikeassa yläkulmassa. Kun olet avannut ohjelman, ota käyttöön *Näytä avainnipun tila valikkorivillä* -toiminto. Tämän jälkeen pysyvän valikkorivin oikeaan laitaan näytön yläreunassa ilmestyy pieni lukkosymboli. Sitä napsauttamalla voi valita valikosta *Lukitse näyttö* -vaihtoehdon.





VAIHE VAIHEELTA: WINDOWS

Windows-tietokoneen salasanan voi vaihtaa ohjauspaneelin kohdassa *Käyttäjätilit*.

Valitse *Käyttäjätilit* ja sen jälkeen *Tilien hallinta* → *Muuta tiliä* → *Muuta salasana*.

Näyttöön avautuvat käyttäjätiliasetukset. Valitse luvussa 7 kuvattujen periaatteiden mukainen vahva salasana, jonka varmasti muistat. Älä valitse *Salasanavihje*-kenttää, sillä salasanavihjeen käyttö helpottaa salasanan murtamista.

6.4 Salattu varmuuskopiointi

Tietokoneen sisällön säännöllinen varmuuskopiointi on tärkeää. Jos tietokoneessa on käytössä massamuistin salaus, Apple tai Microsoftin Windows ei pääse käsiksi hävinneelle tietokoneelle tallennettuihin tietoihin. Myös salaustyökalujen käyttö voi estää pääsyn tietoihin. Siksi varmuuskopioinnin merkitys lisääntyy entisestään.

VAIHE VAIHEELTA: MAC

Mac-tietokoneiden sisällöstä voi luoda salatun varmuuskopion järjestelmän omalla Time Machine -varmuuskopiointisovelluksella. Tiedoista on otettava säännöllisesti varmuuskopio ulkoiselle asemalle, esimerkiksi kovalevylle, ja se on säilytettävä turvallisessa paikassa.

Ulkoista asemaa ei ole saanut aikaisemmin käyttää mihinkään muuhun tarkoitukseen. Jos varmuuskopio sisältää erityisen arkaluonteista toimituksellista aineistoa, se on säilytettävä paikassa, jota ei voi välittömästi yhdistää tietokoneen omistajaan ja johon ei tehdä kotietsintää.

1. Avaa Time Machine -sovellus *Järjestelmäasetuksista*.
2. Liitä tietokoneeseen ulkoinen asema ja napsauta *Valitse varmuuskopiolevy*. Nyt asemalle luodaan automaattisesti varmuuskopio tietokoneen sisällöstä aina, kun se on liitettynä koneeseen. Huomaa, että ulkoisella asemalla olevat tiedot korvautuvat aina uusilla, kun asema liitetään koneeseen.
3. Kun varmuuskopiolevy on valittu, sen voi suojata *Salaa varmuuskopiolevy* -valinnalla. Salaukseen on tärkeää käyttää luvussa 7 kuvattavien periaatteiden mukaista vahvaa salasanaa.



VAIHE VAIHEELTA: WINDOWS

Jos käyttämässäsi Windows-versiossa on BitLocker-levynsalaustyökalu, sillä voi luoda salattuja varmuuskopioita. Bitlocker on sisällytetty Windowsin Pro-, Enterprise- ja Education-versioihin, mutta Home-versiossa sitä ei ole.
1. Hae BitLocker Manager käynnistysvalikosta ja käynnistä se.
2. Ota BitLocker käyttöön varmuuskopiointiin käytettävässä ulkoisessa asemassa valitsemalla sen kohdalla *Turn on BitLocker*.
3. Luo vahva salasana ja napsauta *Next*. Luvussa 7 kerrotaan vahvojen salasanojen luomisesta.
4. Tallenna tai tulosta palautusavain, jotta se on tallessa salasanan hukkumisen varalta.
5. Valitse haluamasi salaustapa, napsauta *Next* ja sen jälkeen *Start Encryption*.

6.5 Ulkoisten asemien salaus

Tiedostoja, kansioita ja ulkoisia asemia voi salata monin eri tavoin.

Yksi vaihtoehto on VeraCrypt-sovellus, jolla salattuja kohteita voi avata sekä Mac- että Windows-tietokoneilla. Tästä voi olla hyötyä, jos halutaan esimerkiksi salata kovalevy tai muistitikku ja luovuttaa se toiselle henkilölle salausavaimen kanssa.

Tietokoneella voi olla myös valmiiksi asennettuna erilaisia salaustyökaluja. Salaaminen on melko yksinkertaista, jos ainoastaan käyttäjän itsensä on tarkoitus pystyä avaamaan omalla tietokoneellaan sijaitsevia tiedostoja tai asemia.

Tässä osiossa kerrotaan nykyisin käytettävissä olevista salausvälineistä Mac-ympäristöissä.

VAIHE VAIHEELTA: MAC

Jos halutaan salata ulkoinen asema, sen sisältö täytyy ensin poistaa ja alustaa asema. Se tapahtuu *Levytyökalu*-lisäohjelmalla (Disk Utility).

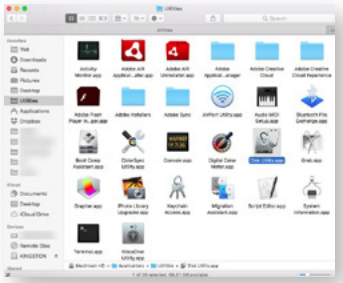
1. Sen voi avata *Ohjelmat*-kansion *Lisäohjelmat*-valikosta. Toinen vaihtoehto on etsiä sovellus napsauttamalla hakutoimintoa kuvastavaa suurennuslasikuvaketta näytön valikkorivillä oikeassa yläkulmassa.

2. Valitse ohjelmaikkunan yläreunan valikkoriviltä *Tyhjennä* ja sen jälkeen vasemman laidan valikosta ulkoinen asema, jonka haluat salata. Varmista, että napsautat varsinaista asemaa etkä jotakin sen alakansioista. Valitse pudotusvalikosta *Mac OS → laajennettu (kirjaava, salattu)*. Valitse sen jälkeen *Tyhjennä*.

3. Syötä näyttöön avautuvaan dialogi-ikkunaan vahva salasana, jonka olet luonut luvussa 7 kuvattavien periaatteiden mukaisesti. Jätä salasanavihje tyhjäksi, jotta salasanaasi ei voi arvata sen avulla. Valitse sen jälkeen *Tyhjennä*. Muista! Valitun aseman sisältö poistetaan.

4. Ulkoinen asema on nyt salattu, ja sen voi avata ainoastaan asettamallasi salasanalla. Kun haluat käyttää asemaa, syötä salasana, siirrä tarvittavat tiedostot asemaan ja poista se koneesta. Nyt asemaan tallennetun luottamuksellisen aineiston voi luovuttaa esimerkiksi kollegalle tai muulle kontaktille.

Toimita aseman vastaanottajalle salasana jollakin muulla tavoin erillään asemasta. Jos esimerkiksi lähetät muistitikun postissa tai kuriiripalvelun kautta, voit lähettää salasanan esimerkiksi salatussa sähköposti- tai tekstiviestissä. Varmin keino salasanan toimittamiseen on luovuttaa se kasvotusten.





6.6 Tiedostojen ja kansioiden salaus

Luvussa 8.4 kerrotaan PGP-avaimen luomisesta. Sen avulla voi salata myös tiedostoja ja kansioita.

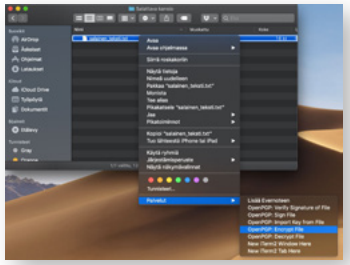
VAIHE VAIHEELTA: MAC

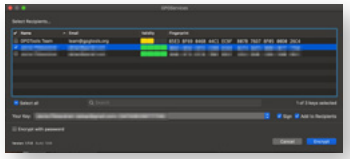
1. Napsauta kakkospainikkeella tiedostoa tai kansiota, jonka haluat salata, ja valitse *Palvelut → OpenPGP: Encrypt File.*

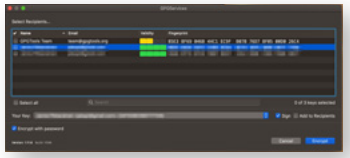
2. Nyt voit salata tiedoston toisen käyttäjän julkisella PGP-avaimella tai salasanalla. Jos esimerkiksi haluat vaihtaa asiakirjoja kollegasi kanssa, voit salata ne hänen julkisella PGP-avaimellaan napsauttamalla näyttöön avautuvaa dialogi-ikkunaa. Jos haluat pystyä avaamaan tiedoston myös itse, valitse *Add to Recipients*. Jos haluat liittää tiedostoon oman julkisen salausavaimesi, valitse *Sign*. Jos vain sinun itsesi pitää voida avata tiedosto, voit käyttää omaa PGP-avaintasi.

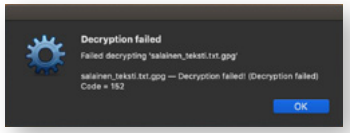
3. Tiedoston voi salata myös vahvalla salasanalla valitsemalla *Encrypt with password* sekä poistamalla kaikki vastaanottajat ja *Add to Recipients* -valinnan. Voit kertoa salasanan vastaanottajalle tavatessanne tai lähettää sen hänelle jotakin toista salattua kanavaa pitkin. Noudata luvussa 7 kuvattavia vahvojen salasanojen periaatteita.

4. Tiedosto tai kansio on nyt salattu. Jos joku yrittää avata sen ilman avainta tai salasanaa, jota on käytetty sen salaamiseen, näyttöön avautuvassa dialogi-ikkunassa ilmoitetaan, ettei avaaminen ole mahdollista.



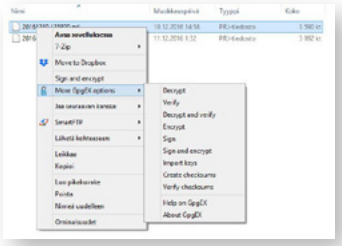


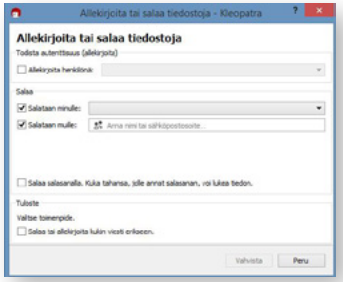




VAIHE VAIHEELTA: WINDOWS

1. Napsauta kakkospainikkeella tiedostoa tai kansiota, jonka haluat salata, ja valitse *More GpgEX options* ja sen jälkeen *Encrypt*.
2. Nyt tiedoston voi salata joko salasanalla tai PGP-avaimella edellä Mac-käyttöjärjestelmän yhteydessä esitettyjen ohjeiden mukaisesti.





VINKKI!

Salaamiseen voi käyttää myös VeraCrypt-nimistä avoimen lähdekoodin sovellusta, joka on ladattavissa osoitteesta veracrypt.fr/en/Downloads.html.

Mac-käyttäjä voi ladata sivustosta dmg-tiedoston ja Windows-käyttäjä exe-tiedoston. Jos asentaa ohjelman Mac-tietokoneelle, ensin on asennettava OSXFUSE-lisäohjelma, jonka saa samalta sivustolta.

VeraCryptiä voi käyttää ulkoisten asemien salaamiseen ja salattujen kansioiden luomiseen. Molemmat lukitaan salasanalla. Salattuja tiedostoja tai asemia voi vaihtaa kontaktien kanssa ja toimittaa niiden avaamiseen tarvittavat salasanat muuta viestintäkanavaa käyttäen. Jos esimerkiksi jaat salatun kansion kontaktin kanssa lataamalla sen pilvipalveluun, voit lähettää salasanan Signal-sovelluksen kautta. Jos taas luovutat kontaktille salatun kovalevyn tai muistitikun, voit kertoa salasanan samassa yhteydessä suullisesti.

6.7 Hyvät turvallisuuskäytännöt

Kun laitteissa käytetään koko levyn salausta, on tärkeää varmistaa, että myös arkiset turvallisuusrutiinit ovat kunnossa.

Laitteet ja ohjelmistot kehittyvät jatkuvasti, samoin tunkeutumiskeinot ja välineet hyökkäyksiltä suojautumiseen. Maailman tiedustelupalvelut kehittävät valtavilla rahasummilla ohjelmia, joilla voidaan valvoa sähköistä viestintää. Tämän tästä tehdään paljastuksia saastuneista ohjelmista ja yrityksistä, jotka tekevät yhteistyötä tiedustelupalvelujen kanssa. Toiset yritykset taas keskittyvät turvallisuusaukkojen tilkitsemiseen ja uusien keinojen kehittämiseen valvonnalta suojautumiseksi.

Hyvät turvallisuuskäytännöt auttavat varmistamaan, että laitteet ja oma osaaminen pysyvät ajan tasalla. Laitteiston suojaaminen haittaohjelmilta ja varmuuskopiointi ovat avainasemassa.

Tässä luvussa kerrotaan palomuurin käytöstä tietokoneen suojaamiseksi haittaohjelmilta. Luvussa 6.4 puolestaan käsitellään salattua varmuuskopiointia.

KÄYTTÖJÄRJESTELMÄPÄIVITYKSET

Tietokoneen ja puhelimen käyttöjärjestelmä on aina muistettava pitää ajan tasalla. Useimmat uudet laitteet ilmoittavat, kun järjestelmäpäivitys on saatavilla. Vaikka päivitysilmoitus harvoin sattuu hetkeen, jolloin mitään ei ole kesken, päivittäminen on paras keino varmistaa, että laite on mahdollisimman hyvin suojassa viruksilta ja muilta digitaalisilta hyökkäysyrityksiltä.

Siksi salaustyökaluista, ohjelmista ja käyttöjärjestelmistä on aina käytettävä viimeisintä versiota. Monet salaustyökalut eivät yksinkertaisesti toimi vanhoissa käyttäjärjestelmissä, eivätkä valmistajat tarjoa niihin myöskään tietoturvapäivityksiä.

Kannattaa seurata myös sitä, mitä verkkopalstoilla kirjoitetaan omassa käytössä olevista ohjelmista ja tietoteknisistä välineistä sekä niiden valmistajien tarjoamista päivityksistä.

PALOMUURI

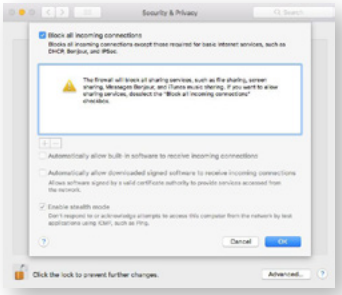
Palomuuri on ohjelma, joka estää luvattoman pääsyn tietokoneelle internetin kautta sekä estää konetta ottamasta luvatta yhteyden internetiin. Se kannattaa pitää toiminnassa. Palomuuri suojaa haittaohjelmilta, joita käyttäjä ei ole hyväksynyt. Se myös estää tietokoneen ohjelmia lähettämästä tietoja kolmansille osapuolille.

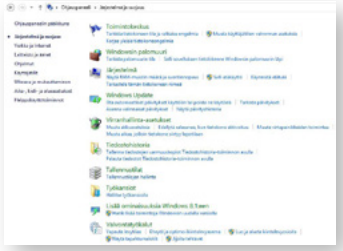
VAIHE VAIHEELTA: MAC

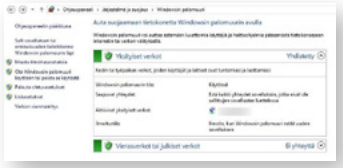
1. Siirry *Järjestelmäasetusten Suojaus ja yksityisyys* -valikkoon. Asetusten muuttamiseksi napsauta oikeassa alakulmassa näkyvää lukkosymbolia ja sen jälkeen *Laita palomuuri päälle* -painiketta.
2. Nyt palomuuri on toiminnassa. Palomuurin asetuksista voit valita, mitkä ohjelmat saavat lähettää tietoja tietokoneeltasi.
3. Turvallisinta on valita palomuurin asetuksista *Estä kaikki saapuvat yhteydet* -vaihtoehto.

Valinta voi tosin aiheuttaa harmia, jos haluat esimerkiksi yhdistää tietokoneesi tulostimeen tai jakaa yhteyksiä. Jos et halua tällöin ottaa palomuuria pois käytöstä, voit myös poistaa *Salli allekirjoitettujen ohjelmistojen saapuvat yhteydet automaattisesti* -vaihtoehdon. Näin voit varmistaa, ettei tieto liiku ilman lupaasi. Kun jokin ohjelma kysyy, sallitaanko saapuvat yhteydet, kysymykseen kannattaa miltei aina vastata kieltävästi.

Kun palomuuriasetukset ovat valmiit, napsauta OK. Muista kytkeä lukitus jälleen päälle ennen kuin poistut järjestelmäasetuksista, jotta asetukset eivät voi muuttua.







VAIHE VAIHEELTA: WINDOWS

Windowsissa palomuuri otetaan käyttöön ohjauspaneelin *Järjestelmä ja suojaus* -osiosta.

Valitse *Windowsin palomuuri* ja sen jälkeen *Käytössä*, jotta palomuuri varmasti on aina päällä. Jos palomuuri ei ole päällä, laita se päälle. Palomuuri-ikkunan pitäisi näyttää lopuksi samalta kuin viereisessä kuvassa.

6.8 Tails – turvallinen käyttöjärjestelmä

Tässä kirjassa esitellään arkisia salaustyökaluja, joita voi käyttää sellaisten tavallisten käyttöjärjestelmien kuin Mac OS:n tai Windowsin yhteydessä. On kuitenkin muistettava, että molemmat käyttöjärjestelmät ovat suljetun lähdekoodin järjestelmiä. Siksi niissä voi olla takaportteja, joiden kautta tiedusteluviranomaiset voivat päästä järjestelmiin. Sekä Microsoftin että Applen tiedetään tehneen yhteistyötä tiedustelupalvelu NSA:n kanssa.

Avoimen lähdekoodin järjestelmät ovat yleensä turvallisempi vaihtoehto. Yleisin turvallinen avoimen lähdekoodin käyttöjärjestelmä on Linux-pohjainen Ubuntu, jonka voi asentaa PC-tietokoneelle Windowsin sijaan.

Vielä turvallisempi vaihtoehto työkäyttöön on niin ikään Linux-pohjainen Tails. Se on anonyymi käyttöjärjestelmä, jota käytetään tyypillisesti ulkoiselta asemalta, kuten muistitikulta. Käyttöjärjestelmään on liitetty liuta muita avoimen lähdekoodin ohjelmia, jotka on tarkoitettu valvonnan välttämiseen. Pakettiin kuuluvat esimerkiksi Tor-pohjainen anonyymi verkkoselain sekä salatut sähköposti- ja chatsovellukset. Kun tietokone käynnistetään siten, että Tails-käyttöjärjestelmän sisältävä muistitikku on koneessa, Tails otetaan automaattisesti käyttöön. Muistitikulle voi tallentaa tiedostoja ja työasiakirjoja. Kun tieto-

kone suljetaan, työskentelyn kaikki digitaaliset jäljet poistetaan, ja työn tulokset on tallennettu ainoastaan muistitikulle.

Käyttöjärjestelmä sopii erityisesti käytettäväksi yksittäisissä projekteissa, jotka vaativat korkeaa turvallisuustasoa. Tailsin voi ladata osoitteesta tails.boum.org. Kirjan lopussa on vinkkejä osoitteista, joista käyttöjärjestelmästä sekä sen asennuksesta ja käytöstä saa lisätietoa.

6.9 Turvalliset laitteet

Edward Snowdenin paljastuksista tiedämme, että tiedustelupalvelut paitsi valvovat toimintaamme internetissä myös asentavat valvontaohjelmia suoraan ihmisten tietokoneille. Snowdenin vuotamista asiakirjoista ilmenee muun muassa, että Yhdysvaltain tiedustelupalvelu NSA on asentanut valvontavälineitä yli 100 000 reitittimelle, palvelimelle ja tietokoneelle ennen niiden viemistä Yhdysvalloista muihin maihin. Ison-Britannian tiedustelupalvelu GCHQ puolestaan on napannut miljoonien tavallisten Yahoon verkkopalvelujen käyttäjien ottamia kuvia.

Tietokoneen osia, joita voidaan käyttää valvontaan, ovat verkkokamera, mikrofoni, kovalevyn ajuri, WLAN-verkkokortti, Bluetooth-kortti ja muut verkkoyhteyden muodostamiseen käytettävät osat.

Helppo tapa välttää verkkokameran tai puhelimen kameran kautta tapahtuva valvonta on yksinkertaisesti teipata kameran linssi piiloon. Siihen kannattaa käyttää teippiä, joka on helppo irrottaa kameran käyttöä varten ja laittaa jälleen takaisin paikalleen.

Mac-tietokoneissa puolestaan mikrofonin kautta tapahtuvan perusmuotoisen salakuuntelun voi estää säätämällä lähtevän äänen tason minimiin. Sen voi tehdä *Järjestelmäasetusten Äänet*-kohdassa.

Jos käyttäjällä on syytä uskoa, että häntä valvoo kohdennetusti jokin taho, jolla on mittavat voimavarat käytettävissään, laitteisto on suojattava valvontaa vastaan tehokkaammin.

VINKKI!

Tietokoneen verkkokameran linssin päälle voi kiinnittää teipinpalan ja mikrofonin lähtevän äänen säätää minimitasolle. Se ainakin vaikeuttaa kameran tai mikrofonin kautta tapahtuvaa valvontaa.

FAKTA: AIR GAPPED -TIETOKONE

Tietokonetta, joka ei koskaan ole ollut yhteydessä internetiin, kutsutaan air gapped -koneeksi (*air gap* = ilmarako). Jos toimittaja käsittelee korkeaa turvallisuustasoa vaativaa aihetta, voi olla fiksua käyttää kahta tietokonetta, joista toisella ei pääse verkkoon lainkaan. Esimerkiksi toimittaja Glenn Greenwald käytti tällaista tietokonetta käsitellessään Snowden-asiakirjoja.

Yksi mahdollisuus on hankkia tietokone, jota ei koskaan yhdistetä verkkoon. Tällä tietokoneella voi työstää kaikkein arkaluonteisinta aineistoa – esimerkiksi kirjoittaa artikkeleita, tallentaa tiedostoja ja käyttää muistitikuille tallennettuja sisältöjä. Jos tietokoneen hankkii nimettömästi liikkeestä eikä verkon kautta, vaihtaa käyttöjärjestelmän ja poistaa koneesta kokonaan osat, jotka voivat ottaa yhteyden internetiin, se on erittäin turvallinen työkalu.

On tärkeää muistaa olla kertomatta nimeään tietokonetta hankkiessaan ja maksaa se käteisellä luotto- tai pankkikortin sijaan. Tietokoneen on oltava pc, johon on helppo vaihtaa käyttöjärjestelmä mahdollisen valmiiksi asennetun Windowsin tilalle. Lisäksi se täytyy voida avata esimerkiksi verkkokameran ja mikrofonien poistamiseksi. Mac-tietokoneissa käyttöjärjestelmän vaihtaminen on hankalaa.

Kirjan lopussa luvussa 13 annetaan vinkkejä, mistä voi saada lisätietoja, jos työskentelee tiukkoja turvatoimia vaativan aiheen tai lähteen parissa.

6.10 Tietoturva puhelimessa

Matkapuhelin on nykypäivänä ehdottoman välttämätön väline useimmille toimittajille. Sillä voi paitsi soittaa ja lähettää tekstiviestejä myös surfata netissä ja somettaa. Puhelimeen tallentuu monenlaista tietoa esimerkiksi viesteinä, sähköposteina, Messenger-keskusteluina, kuvina ja äänitiedostoina. Joukossa voi olla myös luottamuksellista viestinvaihtoa lähteiden kanssa.

Valitettavasti puhelin on välineenä yhtä haavoittuva kuin hyödyllinen. Älypuhelimia ei voi salata vastaavalla tavalla kuin kannettavia tietokoneita. Vaara saada puhelimeen haittaohjelma, joka voi imuroida siitä sisältöä, on suuri. Lisäksi voi olla vaikea pysyä kärryillä siitä, millaisia oikeuksia puhelimen sisältöihin luovuttaa kolmansille osapuolille eri sovellusten asentamisen yhteydessä.

Suurin älypuhelimiin liittyvä turvallisuusuhka on, että puhelin pitää jatkuvasti lokia tukiasematiedoista. Niiden avulla saa selville, missä puhelin sijaitsee sekä milloin sillä on käytetty internetiä, lähetetty tai saatu tekstiviestejä tai puhuttu puheluita. Älypuhelin tarkkailee sijaintiaan myös gps-paikannuksen avulla esimerkiksi karttasovellusten ja sosiaalisen median paikannustoimintoa varten. Puhelinyhtiöillä on käytettävissään tukiasema- ja sijaintitiedot, ja ne voivat luovuttaa niitä viranomaisille. Google voi paikantaa puhelimen sijainnin, vaikka käyttäjä olisi kytkenyt sijaintitietojen seurannan pois päältä.

Vaikka älypuhelimet ovat tietokoneita riskialttiimpia, niidenkin turvallisuutta voi parantaa monin tavoin.

Puhelimen sisällön voi salata edellä kuvatulla tavalla. Lisäksi puhelimeen voi asentaa turvallista viestintää edistäviä sovelluksia. Niistä kerrotaan lisää luvussa 8.

FAKTA: PÄÄLLÄ VAI POIS PÄÄLTÄ?

Puhelin ei ole suojassa valvonnalta, vaikka sen virta olisi katkaistu. Jos useita puhelimia suljetaan samassa paikassa samanaikaisesti, se voi päinvastoin kiinnittää huomiota. Salaisiin tapaamisiin lähdettäessä onkin turvallisinta jättää puhelin kotiin virta päällä.

FAKTA: KERTAKÄYTTÖPUHELIN

Kertakäyttöpuhelin eli *burner phone* on puhelin, jota ei voi jäljittää sen käyttäjään. Sellaisen hankkimista voi harkita esimerkiksi arkaluonteisen kontaktin kanssa tapahtuvaa yhteydenpitoa tai erityisen valonarkaa juttua varten. Valvonnan minimoimiseksi kannattaa hankkia käteisellä puhelin, joka on teknisesti mahdollisimman alkeellinen – ei missään nimessä älypuhelin – ja jossa on anonyymi prepaid-kortti.

Jos kaikki viestinnän osapuolet toimittajakollegoita ja lähteitä myöten hankkivat kertakäyttöpuhelimet ja käyttävät niitä viisaasti, valvonnan vaarat voi minimoida tehokkaasti. Puhelinta saa käyttää ainoastaan tietyn jutun tai kontaktin yhteydessä, eikä sillä missään nimessä saa hoitaa mitään muita työ- tai yksityisasioita. Jutun valmistuttua puhelin on hävitettävä. Kertakäyttöpuhelinta ei saa kuljettaa tai säilyttää samaan aikaan ja samassa paikassa normaalisti käytettävän puhelimen kanssa. Sen numeroa ei myöskään saa tallentaa omaan puhelimeensa tai tuttavien puhelimiin, sillä numeron avulla puhelimen saattaa pystyä jäljittämään sen käyttäjään.

7

Salasanojen suojaaminen

Vahvojen salasanojen valitseminen ja asianmukainen käyttö ovat digitaalisen itsepuolustuksen kulmakiviä.

Edellisessä luvussa kerrottiin laitteiden suojaamisesta koko levyn salauksella. Sitä voi verrata siihen, miten lukko suojaa taloa. Jos tietokoneen salasana on heikko, se on ikään kuin huono lukko, joka on olemassa vain muodon vuoksi mutta ei todellisuudessa tarjoa minkäänlaista suojaa.

Valitettavasti monet käyttävät salasanoja, jotka on erittäin helppo arvata – onhan ne valittu siten, että ne olisi helppo muistaa. Helpot salasanat ovat liian lyhyitä, yksinkertaisia ja ilmeisiä: esimerkiksi *salasana123*, käyttäjän syntymäpäivä tai lemmikkikissan nimi. Koodinmurto-ohjelmat selvittävät tällaiset salasanat muutamassa sekunnissa.

Siksi on tärkeää osata valita niin vahvoja salasanoja, että niiden murtaminen on mahdotonta.

Vahvat salasanat ovat niin pitkiä ja hankalia merkkijonoja, että ne ovat oikeastaan salalauseita. Tärkeiden tietojen suojaamista ei kannata jättää helposti murrettavien lyhyiden salasanojen varaan.

7.1 Vahvat salalauseet

Nykypäivän tietokoneet ovat niin tehokkaita, että ne voivat selvittää nopeasti sattumanvaraisetkin salasanat, jotka ovat alle neljätoista merkkiä pitkiä. Koordinmurto-ohjelmat voivat käydä läpi miljoonia salasanoja sekunneissa, ja ne voivat raksuttaa tarvittaessa päiväkausia samanaikaisesti useilla eri tietokoneilla. Ohjelmat osaavat etsiä tietoa tietokoneen omistajasta sekä hyökkäyksen kohteena olevalta tietokoneelta että julkisista verkkolähteistä.

Jos käyttäjä siis on jossain vaiheessa tallentanut salasanan tietokoneelleen tai käyttänyt salasanana jotakin henkilökohtaista tietoaan, kuten syntymäpäiväänsä, salasana murtuu tuossa tuokiossa. Ohjelmat hyödyntävät eri kielten sanakirjoja ja tuntevat yleiset

käytännöt kirjainten korvaamiseen symboleilla (a = @, s = $ ja niin edelleen).

Vahva salalause on sellainen, että se kestää tämän prosessin murtumatta. Vahvoilla salalauseilla on kolme perusominaisuutta:

Pituus: Salalauseen on oltava yli neljätoista merkkiä pitkä. Mitä pidempi se on, sitä vaikeampi sitä on selvittää. Salalauseen pituus on tärkeämpi turvaominaisuus kuin sen monimutkaisuus eli esimerkiksi sen sisältämät erikoismerkit ja numerot.

Yllättävyys: Käyttäjien on pidettävä salalauseensa vain omana tietonaan. Omien salalauseiden on oltava helppoja muistaa ja kirjoittaa oikein. Samalla niiden on oltava niin yllättäviä, ettei kukaan muu voi arvata niitä, vaikka tuntisi käyttäjän hyvin.

Ainutkertaisuus: Salalauseiden kierrättämistä eli samojen salalauseiden käyttöä eri palveluissa on vältettävä. Näin voidaan minimoida vahingot, jos salalauseita sattuu päätymään vääriin käsiin.

Jäljempänä tässä luvussa kerrotaan sovelluksista, joilla salasanoja ja -lauseita voi hallita ja pitää järjestyksessä. Jotkin salasanat on kuitenkin yksinkertaisesti muistettava – esimerkiksi tietokoneen, salasanojen hallintasovelluksen ja varmuuskopioinnissa käytettävän aseman salasanat sekä kenties myös erityisen tärkeiden salattujen muistitikkujen tai tiedostojen salasanat.

Muistettavien salasanojen luetteloon voi olla viisasta lisätä myös sen sähköpostiosoitteen salasana, johon verkkopalveluista lähetetään viesti, jos käyttäjä pyytää palauttamaan jonkin palvelun salasanan.

Tämän kaltaisten salasanojen ja -lauseiden ainoa turvallinen säilytyspaikka on käyttäjän oma pää, joten ne on pystyttävä muistamaan. Silti niiden on oltava niin hankalia, etteivät murto-ohjelmat tepsi niihin.

Tämän luvun faktalaatikoissa esitellään menetelmiä, joilla voi luoda murtamattomia mutta helposti muistettavia salalauseita. Maksimaalisen turvallista salalauseiden luominen on silloin, kun käyttäjä on yksin huoneessa, jonka verhot ovat kiinni, ja hän kirjoittaa muistiinpanonsa käsin kovan alustan päällä, jotta alustaan ei jää painaumia kynästä. Uudet salalauseet on opeteltava ulkoa ja muistilappu tuhottava tai piilotettava erittäin turvalliseen paikkaan.

FAKTA: SCHNEIERIN MENETELMÄ

Käytetyimpiä menetelmiä murtumattomien salalauseiden laatimiseen on amerikkalaisen kryptografin Bruce Schneierin kehittämä menetelmä.

Siinä valitaan jokin helposti muistettava lause ja muodostetaan salalause sen kaikkien sanojen alkukirjaimista erikoismerkeillä ja numeroilla ryydittynä. Salalauseen on sisällettävä kirjaimia, erikoismerkkejä ja numeroita ja oltava vähintään neljätoista merkkiä pitkä.

Lause kannattaa valita niin, että se on henkilökohtainen eli helposti muistettava muttei liian ilmeinen käyttäjästä julkisesti saatavilla olevien tietojen perusteella. Se voi perustua esimerkiksi johonkin henkilökohtaiseen kokemukseen tai käyttäjälle tärkeään lauluun.

Esimerkiksi lauseesta *Luettuani tietoturvaoppaan kolmeen kertaan lupaan, etten koskaan enää lähetä yhtäkään salaamatonta viestiä!* voisi muodostua salasana Lt3Xl,eKel1sv! tai *Yksi pieni elefantti* -lastenlaulun ensimmäisestä säkeistöstä 1pEmn-aTe-kMohn.

Tässäkin menetelmässä on tärkeää välttää aiemmin käytettyjen lauseiden kierrättämistä. Lisäksi on varmistettava, että muistaa, missä kohdassa on esimerkiksi käyttänyt pieniä ja suuria kirjaimia.

FAKTA: NOPPAWARE-MENETELMÄ

Noppaware perustuu amerikkalaisen tietoturva-asiantuntijan Arnold Reinholdin kehittämään Diceware-menetelmään, jonka Kai Puolamäki, Martin Vermeer ja Pauli Virtanen ovat suomalaistaneet. Sen toimintaperiaatteena on pitkä sanaluettelo, jonka jokaiselle sanalle on osoitettu viisinumeroinen, numeroista 1–6 koostuva koodi. Heittämällä noppaa ja seuraamalla sanaluetteloa on mahdollista luoda sattumanvaraisten sanojen muodostamia lauseita, joiden murtaminen on mahdotonta mutta muistaminen helppoa. Näin se käy:

1. Avaa Noppaware-sanaluettelo osoitteessa users.ics.aalto.fi/kaip/noppaware/noppaware.txt.

2. Valitse käytettävien sanojen määrä. Jos salalauseella on tarkoitus suojata salausjärjestelmiä, siinä on oltava vähintään kuusi sanaa.

3. Heitä noppaa ja kirjaa silmäluvut ylös paperille tietokoneesi viereen. Ryhmittele tulokset viiden numeron ryhmiin ja heitä noppaa niin monta kertaa, että koossa on tarvittava määrä sanoja. Voit heittää viittä noppaa kerralla tai yhtä noppaa viisi kertaa. Jos heität viittä noppaa kerralla, kirjaa silmäluvut ylös järjestyksessä vasemmalta oikealle, jotta et alitajuisesti järjestä niitä numerojärjestykseen.

4. Etsi jokaiselle viisinumeroiselle koodille vastine Noppaware-sanaluettelosta. Esimerkiksi tulos 11234 vastaa sanaa aava. Kokoa salalause sanaluettelon sanoista siinä järjestyksessä, jossa heitit numerosarjat.

5. Näistä sanoista muodostuu uusi salalauseesi. Lisätietoja menetelmän käytöstä sekä sanaluetteloita eri kielillä on saatavana osoitteesta world.std.com/~reinhold/diceware.html.

TURVAKYSYMYKSET

Osassa verkkopalveluita käytetään turvakysymyksiä, joilla pyritään varmentamaan käyttäjän henkilöllisyys salasanan hukuttua. Tyypillisiä turvakysymyksiä ovat esimerkiksi käyttäjän äidin tyttönimi ja ensimmäisen lemmikin nimi. Turvakysymyksiin vastattaessa ei kannata käyttää yleisesti saatavilla olevia tietoja, jotka vastapuoli voi löytää helposti, sillä niiden avulla voi kiertää käyttäjän salasanan.

Jos käyttäjä on esimerkiksi julkaissut Facebookissa Mirri-kissansa kuvan, on suorastaan hölmöä käyttää kissan nimeä vastauksena turvakysymykseen, jossa tiedustellaan lemmikin nimeä. Ennemmin vastauksena kannattaa käyttää salasanan tyyppistä merkkijonoa tai mielikuvitusolentoa, jota kukaan muu ei voi arvata. Vastauksen turvakysymykseen on oltava yhtä vaikea arvata kuin sillä suojattava salasanakin.

On hyvä käydä läpi palvelut, joiden turvakysymyksiin on vastannut, ja tarkistaa omat vastauksensa.

7.2 Salasanojen hallintasovellukset

Salasanoja tarvitaan päivittäin lukemattomissa eri kirjautumistilanteissa, kun käytetään esimerkiksi sähköpostia, verkkopankkia, sosiaalista mediaa, suoratoistopalveluita, verkkokauppoja ja monia muita palveluita.

Tämän tästä jossakin palvelussa tulee kehotus vaihtaa salasana. Jos internetin käyttäjä yrittää laskea, moneenko eri paikkaan on kautta aikojen luonut salasanan, hän ei luultavasti edes muista niitä kaikkia.

Koska monien salasanojen muistaminen on vaikeaa, on inhimillistä turvautua samoihin salasanoihin useammassa kuin yhdessä palvelussa. Se on kuitenkin erittäin huono ajatus, sillä silloin yhden salasanan päätyminen vääriin käsiin avaa verkossa samalla kertaa monia ovia. Salasanojen kierrättäminen on yleisimpiä syitä siihen, että käyttäjätietoja päätyy hakkerien haltuun.

Esimerkki: *Käyttäjä on luonut LinkedIn-tilin ja määrittänyt sille salasanan. Käyttäjätunnuksena toimii hänen sähköpostiosoitteensa. LinkedIn on siis saanut haltuunsa käyttäjän salasanan, jota sovellus säilyttää käyttäjätilin tietojen yhteydessä. Jotta käyttäjä muistaisi kaikki salasanansa, hän käyttää samasta salasanasta erilaisia muunnelmia ja lisää sen loppuun vaihtelevia numeroita tai muuttaa kirjoitustapaa hieman.*

LinkedIniin tehdään hakkerihyökkäys, jossa suuri osa salasanatiedoista päätyy vääriin käsiin. (Näin todella tapahtui vuonna 2016.) Käyttäjän tiedot ovat hakkeroitujen käyttäjätietojen joukossa. Nyt hakkerit tietävät hänen salasanansa ja sähköpostiosoitteensa yhdistelmän. He panevat tietokoneen testaamaan sähköpostiosoitetta ja eri salasanavariaatioita suosituissa verkkopalveluissa. Automaattisessa prosessissa tietokone pystyy kokeilemaan miljoonia muunnelmia miljoonien sähköpostiosoitteiden ja käyttäjätilien yhteydessä erittäin lyhyessä ajassa. Käyttäjän LinkedIn-salasana on harmittavan samankaltainen Twitter- ja Gmail-salasanojen kanssa. Siksi hakkerit pääsevät myös käyttäjän Twitter- ja Gmail-tileille ja kaikkiin niillä oleviin tietoihin ja keskusteluihin.

ONKO TIETOSI HAKKEROITU?

Verkko-osoitteessa haveibeenpwned.com kuka tahansa voi tarkistaa, onko oma käyttäjätunnuksena käytetty sähköpostiosoite päätynyt jostakin verkkopalvelusta ulkopuolisten käsiin. Sivustoa päivitetään sitä mukaa kuin uusia tietovuotoja tulee ilmi. Jos oma sähköpostiosoite on vuotanut, käyttäjän on välittömästi vaihdettava salasanansa vuodon kohteena olleessa verkkopalvelussa sekä muilla sivustoilla, joissa hän on käyttänyt samankaltaisia salasanoja.

Verkkosivuston Passwords-alasivulla voi tarkistaa, onko omia salasanoja käytetty muualla. Esimerkiksi salasana oli lokakuuhun 2018 mennessä esiintynyt vuodetuissa käyttäjätiedoissa salasanana 9 449 kertaa.

Samoja salasanoja ei saa kierrättää palvelusta toiseen tai käyttää eri muunnelmia samasta salasanasta.

On kuitenkin mahdotonta muistaa riittävän monta satunnaisesti muodostettua salasanaa. Silloin apuun tulee salasanojen hallintasovellus eli *password manager*.

Salasanojen hallintasovellus on ohjelma, jonka avulla voi luoda turvallisesti suuren määrän vahvoja salasanoja ja hallita niitä. Sillä on helppo saada aikaan monimutkaisia ja satunnaisia salasanoja, joiden arvaaminen on mahdotonta.

Se toimii ikään kuin salattuna kassakaappina, jossa salasanat säilyvät turvassa yksittäisen pääsalasanan takana. ”Kassakaappiin” voi tallentaa sekä itse luotuja että salasanasovelluksen luomia salasanoja.

Kun salasanaa tarvitaan, kassakaapin voi avata ja hakea sieltä tarvittavan salasanan. Tätä varten täytyy muistaa ainoastaan yksi pääsalasana. Käytännössä siis riittää, että muistaa tietokonetta käyttäessään kaksi hyvää, vahvaa salasanaa: tietokoneen ja salasanojen hallinnan salasanat. Ne onkin sitten pidettävä erittäin varmassa tallessa!

Helppokäyttöisiä pilvipohjaisia salasanojen hallintasovelluksia ovat esimerkiksi LastPass ja 1password. Niistä kumpikaan ei ole avoimen lähdekoodin ohjelma, mutta monet tietoturva-asiantuntijat suosittelevat niitä. LastPass on ilmaissovellus, ja 1passwordin käytöstä veloitetaan pieni kuukausimaksu.

KeePassX on ilmainen avoimen lähdekoodin ohjelma. Se eroaa useimmista muista salasanojen hallintasovelluksista siten, että se tallentaa salasanat paikallisesti tietokoneelle pilvipalvelun sijaan. Näin

tiedot pysyvät hivenen paremmin käyttäjän omassa hallussa. Toisaalta paikallisuus voi myös mutkistaa sovelluksen käyttöä, sillä salasanojen synkronointi esimerkiksi puhelimen ja tietokoneen välillä ei ole mahdollista. Lisäksi KeePassX:n käyttöliittymä kaipaisi ehkä hienoista modernisointia.

VAIHE VAIHEELTA: MAC

1. Avaa tavallinen verkkoselain (esimerkiksi Chrome tai Firefox) ja mene osoitteeseen keepassx.org. Valitse vasemman laidan valikosta *Downloads* (Lataukset) ja lataa uudelta alasivulta Macin *Binary bundle* -asennuspaketti napsauttamalla sitä.

2. Etsi äsken lataamasi tiedosto Lataukset-kansiosta ja kaksoisnapsauta sitä. Näyttöön avautuu KeePassX-ohjelman sisältävä kansio. Vedä ohjelman vihreä avainkuvake Ohjelmat-kansioon. Halutessasi voit kiinnittää KeePassX-pikakuvakkeen tietokoneen ohjelmapalkkiin vetämällä ohjelman kuvakkeen näytön alareunaan muiden kuvakkeiden viereen.

3. Avaa KeePassX kaksoisnapsauttamalla ohjelman kuvaketta. Vahvista toiminto napsauttamalla *Avaa*. Jos kone ei suoja-asetusten vuoksi suostu avaamaan ohjelmaa, mene *Järjestelmäasetusten Turvallisuus ja yksityisyys* -kohtaan, josta voit hyväksyä KeePassX:n käynnistämisen.

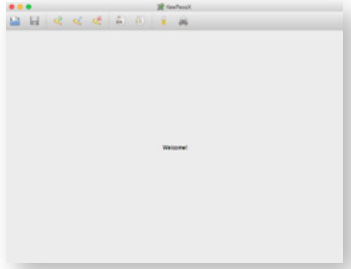
4. Näyttöön avautuu salasanatietokantojen yleisnäkymä. Ikkuna on tyhjä, koska tietokantoja ei ole vielä luotu. Napsauttamalla ylävalikon *Tietokanta → Uusi tietokanta* -kohtaa voit luoda uuden tietokannan. Useimmille käyttäjille salasanojen säilyttämiseen riittää yksi tietokanta.

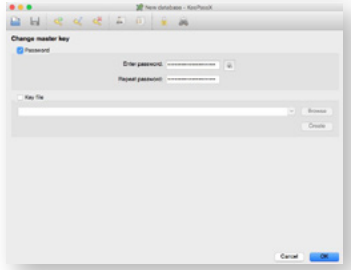
5. Seuraavaksi sinun on luotava pääsalasana tai mieluiten pääsalalause, jolla muut salasanat suojataan. Pääsalasanana on ehdottomasti käytettävä vahvaa ja vaikeasti murrettavaa salasanaa, jonka pystyt varmasti muistamaan.

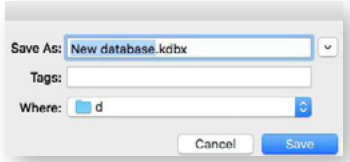


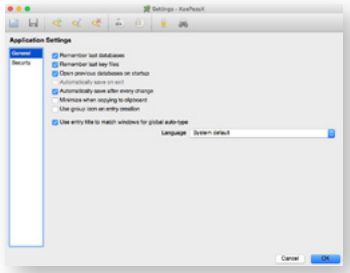


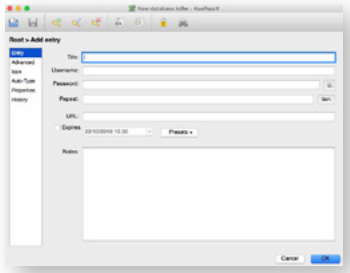


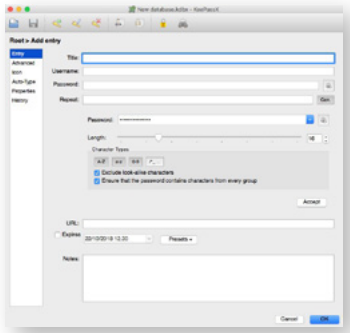












Käytä salasanan miettimiseen aikaa ja luo vahva salalause luvussa 7.1 annettujen ohjeiden mukaisesti. Voit kirjoittaa salasanan muistiin paperille, jos se on ehdottoman välttämätöntä. Paperi on säilytettävä erittäin turvallisessa paikassa. Jos KeePassX:n pääsalasana häviää, häviävät samalla myös kaikki muut salasanat.

Kun olet keksinyt sopivan pääsalasanan, syötä se *Password*-kenttään ja napsauta OK.

6. Tallenna tietokanta napsauttamalla levykekuvaketta ikkunassa vasemmassa yläkulmassa. KeePassX kysyy, minne tietokanta tallennetaan. Voit valita tallennuskohteeksi esimerkiksi Dokumentit-kansion.

7. Ennen uuden salasanatietokannan käyttöönottoa sinun on tehtävä KeePassX:n tarvittavat asetukset, jotta se tallentaa kaikki muutokset automaattisesti. Silloin sinun ei tarvitse muistaa napsauttaa levykekuvaketta joka kerta, kun olet lisännyt tietokantaan uuden salasanan.

Muuta asetuksia avaamalla *Preferences*-valikko vasemmasta yläreunasta. Valitse valikosta *General* ja sen jälkeen *Automatically save database after every change*.

8. Nyt olet valmis luomaan ensimmäisen vahvan salasanasi KeePassX:llä. Käytä näppäinyhdistelmää ⌘Y tai napsauta vihreällä nuolella varustettua avainkuvaketta KeePassX-ikkunassa, jotta voit luoda uuden salasanan (*Add New Entry*). Näyttöön avautuu ikkuna, jossa voit syöttää tarvittaviin kenttiin haluamasi käyttäjätilin tiedot.

9. Syötä *Password*-kenttään uusi vahva salasanasi kyseiselle käyttäjätilille. Voit keksiä salasanan itse edellä kuvatulla tavalla tai pyytää KeePassX:n luomaan sellaisen. Se tapahtuu napsauttamalla pientä *Gen.*-painiketta (*generate*). Ohjelman vakioasetukset kelpaavat aivan hyvin salasanojen luomiseen.

Nyt KeePassX-ohjelmaan on tallennettu yhden käyttäjätilin vahva salasana. Salasana tallentuu ohjelman salattuun ”kassakaappiin” ikään kuin muisti-

lapulle kirjoitettuna. Kaapin ovi avautuu ainoastaan pääsalasanalla.

10. Kun olet syöttänyt salasanan ja sulkenut syöttöikkunan, käyttäjätili on nähtävissä salasanatietokannan yleisnäkymässä. Voit kopioida uuden salasanasi napsauttamalla sitä hiiren kakkospainikkeella ja valitsemalla *Copy Password to Clipboard*. Sen jälkeen voit kirjautua käyttäjätilillesi ja syöttää salasanan sitä pyydettäessä aivan niin kuin tavallisestikin. Voit käyttää äsken luotua salasanaa joko luodessasi uuden käyttäjätilin johonkin palveluun tai muuttamalla salasanojasi eri palvelujen käyttäjätiliesi asetuksissa.

11. Salasanojen hallintasovellukset tallentavat tietoja salatussa muodossa internetiin tai paikallisesti tietokoneelle. Pilvipohjaiset salasanasovellukset ovat paikallisia helppokäyttöisempiä mutta samalla haavoittuvampia ulkopuolisille hyökkäyksille. KeePassX tallentaa salasanat salatussa muodossa paikallisesti käyttäjän tietokoneelle. Sen ansiosta käyttäjän hallintamahdollisuudet lisääntyvät, mutta samalla kasvaa riski, että kaikki salasanat häviävät kerralla, jos tietokone kaatuu tai varastetaan.

Sen vuoksi on erittäin tärkeää ottaa KeePassX-tietokannasta säännöllisesti varmuuskopio ja tallentaa se varmaan paikkaan. Tämän voi hoitaa luvussa 6.3 kuvattun yleisen varmuuskopioinnin yhteydessä tai kopioimalla tietokannan erikseen muistitikulle luvussa 6.4 selostetulla tavalla. Kopion tietokannasta voi tallentaa KeePassX-ikkunan yläreunan *File*-valikon kautta.

VAIHE VAIHEELTA: WINDOWS

KeePassX asennetaan Windows-ympäristöön hyvin samalla tavalla kuin Mac-ympäristöön.

1. Lataa keepassx.org-sivuston *Downloads*-osiosta *Binary bundle for Windows* -asennuspaketti napsauttamalla sitä.

2. Etsi tiedosto *Ladatut tiedostot* -kansiosta ja avaa se kaksoisnapsauttamalla tiedoston nimeä. Halutessasi voit siirtää ohjelman *Program files* -kansioon. Avaa sitten KeyPassX ja noudata edellä mainittuja ohjeita 4–11.

8 Tietoliikenteen suojaaminen

Edellisissä luvuissa on puhuttu laitteiden ja salasanojen suojaamisesta. Tässä luvussa painopiste siirtyy viestiliikenteen suojaamiseen.

Salaamaton viestintä on kuin jokaisen luettavissa olevien postikorttien lähettämistä internetissä. Viestin sisällön voi lukea kuka tahansa, joka käsittelee viestiä sen matkan varrella: viestin lähettämiseen käytettävä palvelu, lähettäjän ja vastaanottajan internetoperaattorit ja mahdolliset ulkopuoliset, jotka nappaavat viestin jossakin vaiheessa. Tästä kerrotaan lisää luvussa 3.

Salatun viestin lähettäminen taas on kuin kirjepostia suljetussa kuoressa. Viestin sisältö on turvassa ja sinetöity, ja vain vastaanottaja voi lukea sen.

Varmin keino viestinnän salaamiseen on niin sanottu päästä päähän -salaus (end-to-end crypting). Tässä luvussa esitellään välineitä älypuhelinten, chat-keskustelujen ja sähköpostiviestien päästä päähän -salaukseen. Aivan ensimmäiseksi käydään läpi salauksen toimintaperiaatteita ja sen käyttöön liittyviä erityisiä riskejä.

8.1 Päästä päähän -salaus

Useimmat käyttävät jo salausta monissa arkisissa muodoissa. Kun käyttäjä kirjautuu esimerkiksi verkkopankkiinsa digitaalisella allekirjoituksella, sivuston tiedot salataan ulkopuolisilta. Vastaava salaus on käytössä sähköpostipalveluissa ja sosiaalisen median palveluissa, joissa on mahdollisuus käyttää salattua viestintää. Yhteistä tämän kaltaisille ratkaisuille on, että salaustoiminnon tarjoaja, kuten pankki, Facebook tai Gmail, pystyy aina lukemaan viestien tiedot ja siten myös luovuttamaan niitä eteenpäin. Jos salauksesta vastaa kolmas osapuoli, käyttäjä jättää viestiensä salassa pysymisen sen varaan.

Monet verkkopalvelut ovat tarjonneet käyttäjille tietojen varmaa salausta, mutta silti ne ovat luovuttaneet tietoja eteenpäin tai niiden käyttämä salausmenetelmä on osoittautunut haavoittuvaksi.

Päästä päähän -salaus on salausmenetelmä, jolla vain viestin lähettäjä ja vastaanottaja voivat lukea salatun sanoman.

Päästä päähän -salauksen kantava periaate on, että molempien osapuolten on käytettävä samankaltaista salausohjelmaa, jotta he voivat viestiä keskenään salatusti. Ohjelmien ei tarvitse olla täsmälleen samat, mutta niiden on käytettävä samantyyppistä salausprotokollaa.

Jos esimerkiksi puhelimeen tai tietokoneelle on asennettuna Signal-sovellus, käyttäjä voi lähettää salattuja tekstiviestejä vastaanottajille, joilla on Signal omassa puhelimessaan tai tietokoneellaan.

Jos sähköpostiohjelmassa vastaavasti on käytössä PGP-salaus, siitä voi lähettää salattuja viestejä vastaanottajille, jotka niin ikään käyttävät omassa sähköpostiohjelmassaan jotakin PGP-salausta.

KAKSI AVAINTA

Päästä päähän -salauksen tärkein elementti on salausavainten vaihtaminen.

Salattu viestinvaihto edellyttää, että lähettäjällä ja vastaanottajalla on käytössään avainpari, jolla viesti lukitaan ja avataan. Avainpariin sisältyy kaksi avainta: julkinen ja yksityinen.

Avaimet ovat keskenään erilaiset, mutta niiden yhdistelmä on aina ainutkertainen. Niitä voisi verrata halkaistuun kiveen, jonka molemmat puoliskot ovat erilaiset mutta sopivat silti saumattomasti yhteen.

Julkisen avaimen voi jakaa muiden kanssa tai laittaa vapaasti saataville internetiin. Sitä käytetään viestien salaamiseen.

Yksityinen avain on pidettävä omana tietonaan. Se on tallennettava käyttäjän tietokoneelle ja pidettävä salassa. Sillä avataan salatut viestit.

Joissakin salausohjelmissa, kuten Signalissa, avaimet vaihdetaan automaattisesti käyttäjän huomaamatta. Signalin käyttö ei siis periaatteessa edellytä tässä kerrottavan taustatiedon tuntemista.

FAKTA: SALAUS TOIMII

”Salaus toimii”, totesi NSA-ilmiantaja Edward Snowden chat-keskustelussa The Guardian -lehden lukijoiden kanssa kesäkuussa 2013 pian Hongkongista pakenemisensa jälkeen. ”Asianmukaisesti toteutetut vahvat salausjärjestelmät ovat niitä harvoja asioita, joihin voi luottaa.”

Tällä Snowden tarkoitti muun muassa tässäkin kirjassa esiteltäviä Signalia, PGP:tä ja Toria.

Sähköpostiviestien PGP-salauksessa taas avaimet vaihdetaan manuaalisesti, ja se edellyttää viestintäkumppaneilta aktiivisia toimenpiteitä. Käyttäjä voi hallita manuaalista prosessia hieman paremmin kuin automaattista, mutta kumpikaan menetelmä ei ole toista turvallisempi. Kahden avaimen periaate on käytössä sekä Signalissa että PGP-salauksessa.

TODENNUS JA SORMENJÄLKI

Julkisten avainten todentamisella voidaan varmistua siitä, että viestintäkumppani todella on se, joka väittää olevansa. Samalla voidaan varmistaa myös, että salausavaimet ovat sen henkilön tai tahon hallussa, jolle ne oikeasti kuuluvat.

Avoin avain voidaan todentaa vertaamalla avaimesta toimitettua versiota viestintäkumppanin hallussa olevaan versioon.

Salausavaimet ovat pitkiä ainutkertaisia merkkijonoja, jotka koostuvat numeroista, erikoismerkeistä ja kirjaimista. Julkinen avain voi olla kymmenen- tai kaksikymmentätuhatta merkkiä pitkä ja yksityinen avain vielä pidempi.

Jotta avainten vertaaminen olisi mahdollista, julkisilla avaimilla on sormenjälki. Se on ainutkertainen mutta paljon varsinaista avainta lyhyempi merkkijono, jota voi käyttää avaimen nimenä. Sormenjälki on tavallisesti noin 40 merkin pituinen, ja se voi näyttää esimerkiksi tältä: 6FFA 14E4 C7B3 A275 BE33 3390 3BF3 E1BF 03B9 7B60.

Avaimen käyttäjä voi todentaa julkisen avaimen vertaamalla sen sormenjälkeä huolellisesti merkki merkiltä itselleen toimitetun avaimen sormenjälkeen.

Keskeistä todentamisessa on, että se ei saa tapahtua samassa viestintäkanavassa kuin vahvistettava viestintä. Näin todentaminen voidaan varmistaa, vaikka jompikumpi kanavista ei olisi enää luotettava.

Jos viestintäkumppanin julkinen avain on peräisin esimerkiksi hänen kotisivultaan, sormenjäljen vahvis-

tamiseksi kannattaa pyytää häntä esimerkiksi lähettämään se Twitterin kautta. Mahdollisen hakkerin olisi tällöin pitänyt päästä käsiksi sekä hänen kotisivuunsa että Twitter-tiliinsä, jotta pääsisi sotkeutumaan viestintään. Jos toimittaja haluaa esimerkiksi chatata kontaktinsa kanssa salatussa yhteydessä, sormenjäljet voi tarkistaa esimerkiksi salattujen sähköposti- tai tekstiviestien avulla. Tällöin mahdollisella tunkeilijalla pitäisi olla pääsy molempien osapuolten puhelimiin ja chat-viesteihin. Tätä kutsutaan myös *out-of-band*-todennukseksi.

Turvallisinta on kuitenkin huolehtia todentamisesta kasvotusten, jos mahdollista. Sen voi hoitaa tapaamisen yhteydessä siten, että molemmat tarkistavat toisen sormenjäljen omalla tietokoneellaan. Sen jälkeen viestintä voi jatkua turvallisissa merkeissä. Jos viestinnän osapuolet tuntevat toisensa ja tunnistavat toistensa äänet, todentaminen voi tapahtua myös puhelimitse lukemalla sormenjäljet ääneen merkki merkiltä.

METATIETOJEN VAARAT

Tietoa siirretään internetissä tietueina. Kuten luvussa 3 kerrotaan, tietueet sisältävät dataa eli avattavan verkkosivun tai lähetettävän chat- tai sähköpostiviestin sisältöjä sekä metatietoja eli tietoa viestinnästä.

Monet salausvälineet salaavat tietoliikenteen datan mutta eivät sen metatietoja. Jos vastapuoli saa viestin käsiinsä, hän ei voi tällöin nähdä sen sisältöä, mutta viestin metatiedot ovat näkyvissä. Metatietoja ovat esimerkiksi IP-osoitteet, joiden välillä viestinvaihto tapahtuu, viestinnän ajankohta tai mahdollisten liitetiedostojen koko. Jos kyseessä on sähköposti, vastapuoli voi nähdä myös lähettäjän ja vastaanottajan sähköpostiosoitteen sekä aiheriville kirjoitetun otsikon.

Tämä vastaa sitä, että postinkantaja voi lukea luottamuksellisen viestin sisältävästä suljetusta kirjekuoresta lähettäjän ja vastaanottajan yhteystiedot.

Metatiedoissa voi piillä monenlaista paljastavaa informaatiota.

Esimerkki: *Kuvitellaanpa, että suojelupoliisin työntekijä lähettää suurelle suomalaiselle mediakonsernille kuuluvaan IP-osoitteeseen sähköpostiviestin, jonka liitteenä on suurikokoinen tiedosto. Pian tämän jälkeen suojelupoliisin työntekijä puhuu mediakonsernin palveluksessa olevan toimittajan kanssa puoli tuntia puhelimessa. Sitten hän soittaa puhelun ammattiyhdistyksensä edustajalle ja työoikeuteen erikoistuneelle asianajajalle. Muutaman päivän kuluttua mediakonsernin tiedotusväline julkaisee paljastusjutun, joka perustuu suojelupoliisista vuodettuihin asiakirjoihin. Vaikka työntekijä on käyttänyt salausta sekä sähköposteissaan että puheluissaan, metatietojen perusteella ei ole mitenkään vaikeaa selvittää tapahtumien todennäköistä kulkua.*

Seuraavassa esiteltävä Signal on esimerkki työkalusta, joka tallentaa erittäin vähän metatietoja.

8.2 Signal

Signal on päästä päähän salattu ilmaissovellus, jolla voi soittaa puheluita, käydä videochat-keskusteluja ja lähettää viestejä päästä päähän -salauksella. Sovelluksella voi lähettää liitetiedostoja ja kuvia ja käydä monenkeskisiä puhelinkeskusteluja aivan kuten sähköpostikirjeenvaihdossakin. Se toimii iPhone- ja Android-puhelimissa sekä Mac- ja Windows-tietokoneissa.

Signalilla viestitään puhelinverkon sijaan internetissä, joten sen käyttöön puhelimessa tarvitaan internetyhteys.

Kaiken päästä päähän salatun viestinnän tavoin salauksen toimivuuden edellytyksenä on, että kaikki viestinnän osapuolet käyttävät Signalia. Tällöin tietokoneet ja puhelimet voivat viestiä keskenään.

Signalin kehittäjä on avoimen lähdekoodin ohjelmistotalo Open Whisper Systems.

Signalin suosiolle on hyvät syyt. Ensinnäkin se on avoimen lähdekoodin sovellus. Sen vuoksi riippumattomat tietoturva-asiantuntijat pystyvät helposti testaamaan sitä ja havaitsemaan mahdollisia vikoja ja turvallisuuspuutteita.

Toiseksi Signal on erittäin helppo asentaa ja käyttää. Lähteitä, kollegoja ja muita kontakteja voi siis pyytää käyttämään Signalia pelkäämättä, että salatun viestinnän monimutkaisuus houkuttelee heidät laiskottelemaan varotoimien kanssa.

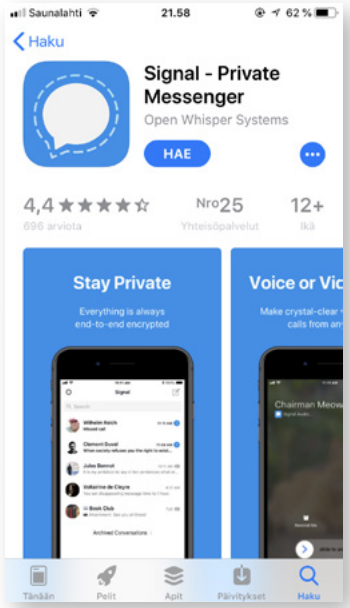
Esimerkiksi toimittajan omissa tai tiedotusvälineen yhteystiedoissa voi mainita sellaisen laitteen puhelinnumeron, jossa käytetään Signalia. Mahdollisia lähteitä on helppo opastaa sovelluksen asentamisessa ja kehottaa lähettämään arkaluonteisia tietoja ainoastaan Signalin välityksellä.

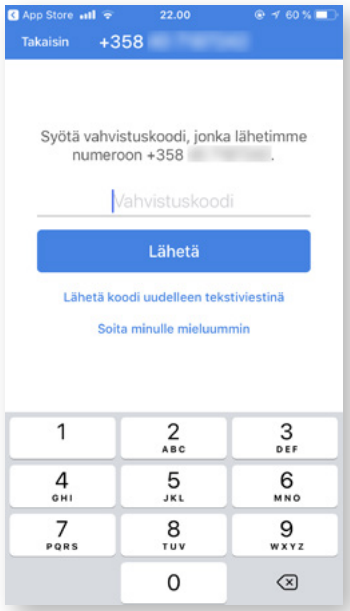
Kolmanneksi sovellus on erittäin turvallinen. Luottamuksellisten asiakirjojen vuotojen perusteella tiedetään, ettei edes Yhdysvaltain tiedustelupalvelu NSA ole pystynyt murtamaan Signalin salausta. Sen käyttöä suosittelevat Edward Snowden ja monet muut tietoturvaekspertit.

Neljänneksi Signal tallentaa erittäin vähän metatietoja, paljon vähemmän kuin muut salausvälineet. Tämä on sen hyvistä ominaisuuksista kenties jopa paras.

Vuonna 2016 Yhdysvaltain liittovaltion poliisi FBI yritti tuomioistuimen päätöksellä saada Signalin luovuttamaan tietoja joistakin sovelluksen käyttäjistä. Luovutetusta aineistosta kuitenkin ilmenee, että Signalin käyttäjistään tallentamat tiedot rajoittuvat kahteen: Signalin ensimmäisen käyttöönoton ajankohtaan ja viimeisimpään käyttökertaan. Yritys ei yksinkertaisesti tallenna käyttäjistään muita tietoja, kuten nimiä, viestintäkumppaneita, viestinnän ajankohtia tai osapuolten IP-osoitteita.

Signal-viesteissä siis kaikki sisällöstä metatietoihin ja mahdollisiin liitetiedostoihin tai kuviin on salattu päästä päähän. Kun sovellusta käytetään puhelujen soittamiseen tai videochat-keskusteluihin, sekä sisältö että metatiedot salataan.





Lisätietoja Signalista ja sen toimintaperiaatteista saa osoitteesta signal.org. Todettakoon vielä, että kirjan kirjoittaja ei omista Signalin julkaisijan osakkeita, vaan kyseessä on voittoa tavoittelematon projekti!

VAIHE VAIHEELTA

1. Etsi Signal: Private Messenger -sovellus puhelimesi App Storesta tai Play Kaupasta ja asenna se.

2. Signal pyytää lupaa käyttää puhelimen yhteystietoja. Luvan antaminen on välttämätöntä, jotta sovellus löytää muut Signalin käyttäjät, joiden kanssa voi viestiä salatusti. Valitse *OK*.

3. Tarvitsemasi salausavaimet luodaan automaattisesti sovelluksen asennuksen yhteydessä. Vanhoissa matkapuhelinmalleissa avaimet on vahvistettava erikseen. Se tapahtuu syöttämällä sovellukseen oma puhelinnumero ja valitsemalla laitteen varmentaminen. Sinulle lähetetään tekstiviestinä varmennuskoodi. Useimmissa puhelimissa varmentaminen kuitenkin tapahtuu automaattisesti.

4. Nyt olet valmis aloittamaan salatun viestimisen Signalilla. Napauttamalla pientä kuvaketta näytön oikeassa yläkulmassa näyttöön avautuu luettelo omista yhteystiedoistasi, joilla on Signal asennettuna älypuhelimeensa.

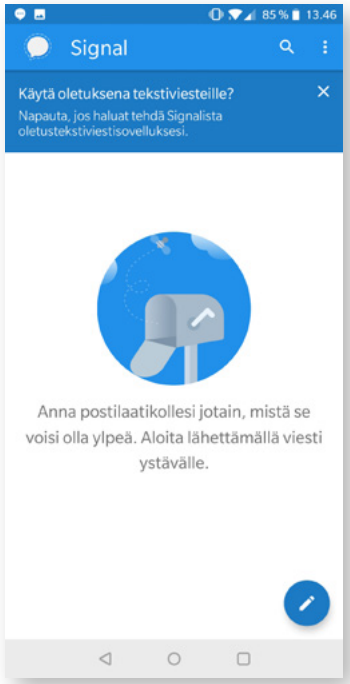
5. Valitse henkilö, jonka kanssa haluat viestiä. Jos haluat lähettää hänelle viestin, napauta yhteystiedon nimeä. Puhelinkuvakkeen valitsemalla voit soittaa henkilölle. Puhelun ollessa käynnissä voit halutessasi muuttaa sen videopuheluksi.

6. Nyt Signal on valmis käytettäväksi iPhonessasi puhelu- ja viestiliikenteen hoitamiseen.

ERITYISOHJEITA ANDROID-PUHELIMIIN

Signal asennetaan iPhoneen ja Android-puhelimiin lähes identtisesti. Erona on kuitenkin se, että Android-puhelimissa käyttäjältä kysytään, haluaako hän tehdä Signalista oletusarvoisen viestisovelluksen. Jos tähän vastataan kyllä, Signalia voi käyttää sekä salattuun viestintään muiden Signalin käyttäjien kanssa että tavallisiin salaamattomiin tekstiviesteihin niiden kanssa, joilla ei ole Signalia.

Jokaisen viestin alaosassa on pieni riippulukkosymboli, joka kertoo, onko viesti salattu. Jos lukko on kiinni, viesti on salattu. Jos lukko on auki, sitä ei ole salattu. Myös viestiketjun tekstikentän alaosassa lukee salatuissa viesteissä *Signal message* ja salaamattomissa viesteissä *Unsecured SMS*.



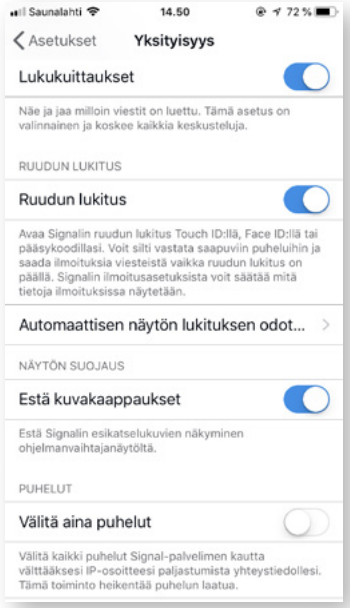
YKSITYISYYSASETUKSET

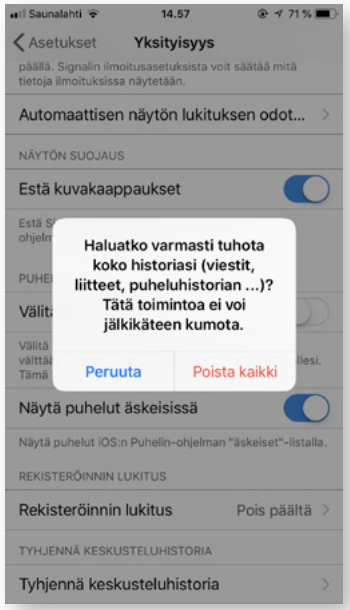
Kun Signal on asennettu puhelimeen, sen yksityisyysasetuksia voi muuttaa entistä turvallisempaan suuntaan.

Signalin asetusvalikko avautuu napauttamalla pientä hammasrataskuvaketta vasemmassa yläkulmassa (iPhone) tai kolmea pistettä oikeassa yläkulmassa (Android), kun näytössä on näkyvissä Signalin puheluluettelo. Esimerkiksi seuraavia asetuksia voi muokata:

1. Lukitusnäyttö: Yksityisyysasetuksissa voi kytkeä toimintaan Signalin lukitusnäytön turvallisuuden parantamiseksi entisestään. Signalin lukitusnäytön ollessa käytössä Signal lukittuu siten, että sen saa auki ainoastaan puhelimen pääsykoodilla tai Touch ID:llä. Toiminto voi olla kätevä esimerkiksi silloin, jos joutuu poistumaan tapaamisesta hetkeksi mutta haluaa jättää puhelimensa paikalle ja auki.

iPhonessa toiminto kytketään päälle *Yksityisyysasetusten Ruudun lukitus* -kohdan *Automaattisen näytön lukituksen odotusaika* -asetuksessa. Aika määrittää sen, kuinka kauan kestää sovelluksen sulkemisesta lukituksen päälle kytkeytymiseen.





Android-puhelimissa vastaava valinta tehdään syöttämällä koodi yksityisyysasetuksissa: *Yksityisyys → Näytön lukitus*. Käyttäjän on annettava koodi avatessaan Signalin ensimmäisen kerran sen jälkeen, kun puhelin on ollut lukittuna tai jos Signal on lukittu manuaalisesti. Signalin voi asettaa lukittumaan myös automaattisesti tietyn ajan kuluttua samoin kuin iPhonessa.

2. Ilmoitukset: Käyttäjä voi määrittää, miten Signal-viestit näytetään lukitusnäytössä. Signalin kautta tulevista viesteistä voi estää push-ilmoitusten näyttämisen puhelimen ollessa lukittuna. Tällöin muut eivät voi nähdä ilmoitusta, jos käyttäjälle saapuu kesken palaverin huippusalainen Signal-viesti, ja puhelin on pöydällä näyttö ylöspäin.

iPhonessa toimintoa voi muokata Signalin valikossa *Asetukset → Ilmoitukset → Näytä*. Siinä voi valita, näytetäänkö viestistä lähettäjä ja sisältö, pelkkä lähettäjä tai ei lähettäjää eikä sisältöä. Turvallisin valinta on viimeinen. Android-puhelimissa vastaava polku on *Asetukset → Ilmoitukset → Näytä*.

3. Puhelujen näyttäminen viimeisimmissä puheluissa: Toiminto sijaitsee iPhonessa Signalin yksityisyysasetuksissa. Valinnan *Näytä puhelut äskeisissä* on syytä olla aina *pois päältä*. Signal ei tallenna metatietoja siitä, kuka viestii kenen kanssa ja milloin. Jos näyttäminen on *päällä*, Signalilla soitetut puhelut kirjataan puhelimen puhelutietoihin. Tällöin ei ole mitään hyötyä siitä, ettei Signal tallenna puhelutietoja.

4. Puheluhistorian tyhjentäminen: Rajun kuuloinen toiminto *Tyhjennä keskusteluhistoria* pyyhkii pois kaikki puhelutiedot, viestit ja liitteet. Toimittajalle toiminnon tuntemisesta voi olla hyötyä esimerkiksi silloin, jos hän joutuu tilanteeseen, jossa häntä voidaan painostaa avaamaan Signal puhelimestaan. Tällöin puheluhistorian voi poistaa nopeasti.

Sekä Android- että iPhone-puhelimissa on myös monia muita hyödyllisiä asetuksia tilanteisiin, joissa turvallisuuteen on kiinnitettävä erityistä huomiota.

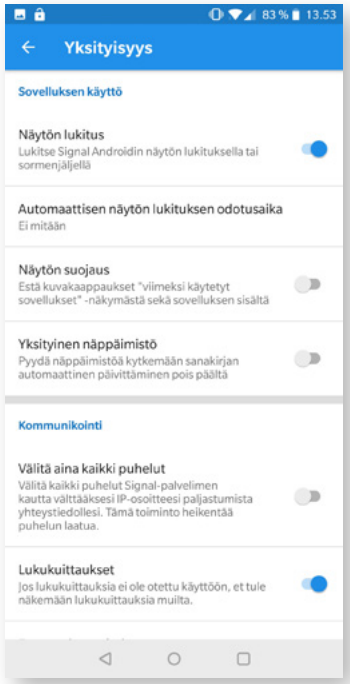
SIGNALIN KAMERAN KÄYTTÖ

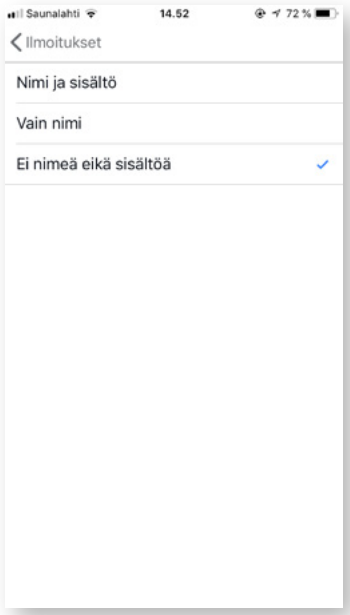
Aiemmin mainittiin, että Signal-viesteihin voi liittää tiedostoja ja kuvia, jotka sijaitsevat tietokoneen kovalevyllä tai puhelimen kuvissa.

Kun Signalia käytetään puhelimella, sen kameratoiminnolla voi myös ottaa ja lähettää kuvia. Näin voi välttää kuvan tallentumisen kameran kuviin tai muihin salaamattomiin kohteisiin. Tällöin kukaan ei voi saada kuvia käsiinsä tunkeutumalla käyttäjän puhelimeen tai pilvipalveluun, johon kuvia kenties tallennetaan.

Ominaisuudesta voi olla erityistä hyötyä, jos toimittaja odottaa saavansa lähteeltä luottamuksellista tietoa.

Esimerkki: *Toimittajan lähde on virkamies, ja lähteen työnantaja on rikkonut lakia. Lähteellä on työpaikallaan pääsy asiakirjaan, joka todistaa asian, ja hän haluaa jakaa dokumentin toimittajan kanssa. Jos lähde lähettää asiakirjan toimittajalle työkoneeltaan tai työpaikkansa tulostimelta, on olemassa suuri vaara, että hän jättää laitteelle digitaalisen sormenjälkensä. Sen avulla vuoto voidaan jäljittää häneen. Lähde asentaa yksityispuhelimeensa Signalin. Hän luo Signal-keskustelun toimittajan kanssa ja avaa kameran, kun keskustelu on käynnissä. Luottamuksellinen asiakirja on avattuna hänen edessään työkoneella. Lähde ottaa puhelimensa Signal-sovelluksen kameralla kuvan asiakirjasta tietokoneen näytöltä ja lähettää kuvan toimittajalle. Näin hän ei jätä digitaalisia sormenjälkiä työkoneelleen eikä tulostimelle tai puhelimensa kuviin.*

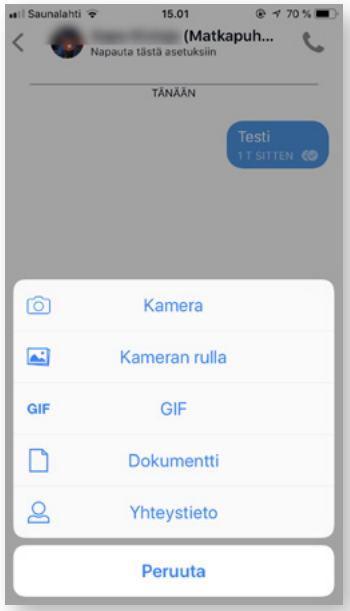




VAIHE VAIHEELTA

1. Paina Signal-keskustelun aikana pientä plussymbolia vasemmassa alakulmassa. Saman symbolin kautta pääset lähettämään myös kuvia, dokumentteja, GIF-tiedostoja ja yhteystietoja.

2. Valitse kamera ja ota kuva tai kuvaa video, jonka haluat lähettää. Kun olet valmis, valitse *Käytä kuvaa/videota* ja *Lähetä*. Kuva tai video lähetetään Signalin kautta tallentamatta sitä puhelimen kuviin.



3. Lähettäjä ja vastaanottaja voivat tallentaa kuvan puhelimeensa napauttamalla sitä ja valitsemalla latauskuvakkeen oikeasta alakulmasta. Kun kuva on tallennettu turvalliseen paikkaan, sen voi poistaa Signal-keskustelusta napauttamalla vasemman alakulman roskakorikuvaketta.

VIESTIEN HÄVITTÄMINEN

Yksi Signalin monista fiksuista ominaisuuksista on, että sovelluksen voi asettaa poistamaan keskustelun viestit aina tietyn ajan kuluttua.

Siitä voi olla hyötyä, jos toimittaja esimerkiksi viestii arkaluonteisesta jutusta chat-keskustelussa. Vaikka kaikikki keskustelun osapuolet olisivat periaatteessa luotettavia, käytännössä mitä tahansa voi aina tapahtua. Puhelin saattaa unohtua jonnekin tai tulla takavarikoiduksi tai hakkeroiduksi. Toimittaja voi olla juttumatkalla tekemisissä paikallisen fikserin tai muun avustajan kanssa, johon hän ei täysin luota, ja niin edelleen.

Mitä useampi osallistuja keskustelussa on, sitä suuremmat ovat turvallisuusriskit. Jos turvallisuuden pettämisellä voi olla vakavia seurauksia, voi olla järkevää asettaa sovellus poistamaan keskustelun viestit, kun ne on luettu.

Näin vältetään keskustelun päätyminen ulkopuolisten haltuun, vaikka puhelimiin tunkeuduttaisiin.

VAIHE VAIHEELTA

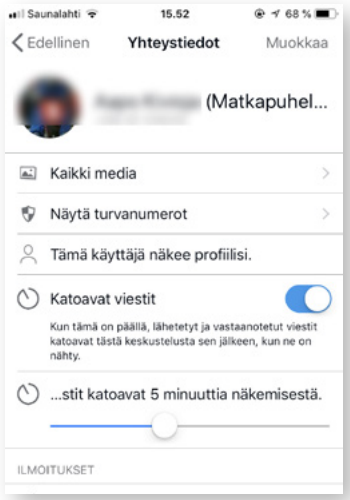
1. Signal-keskustelussa keskustelukumppanin tai -ryhmän nimi näkyy näytön yläreunassa. Napauta sitä, niin pääset keskustelun asetuksiin.
2. Kytke *Katoavat viestit* toimintaan. Voit valita, kuinka kauan viestit säilyvät keskustelussa ennen kuin ne poistetaan. Aika voi olla esimerkiksi viisi minuuttia. Pääset takaisin keskusteluun napauttamalla *Takaisin*-painiketta vasemmassa yläkulmassa.
3. Viestit on nyt asetettu häviämään automaattisesti viiden minuutin kuluttua siitä, kun kaikki keskustelun osallistujat ovat nähneet ne. Viestit häviävät keskustelusta kaikkien osallistujien puhelimissa. Asetus koskee vain viestejä, jotka lähetetään sen jälkeen, kun viestien hävittäminen on otettu käyttöön.

RYHMÄKESKUSTELUT

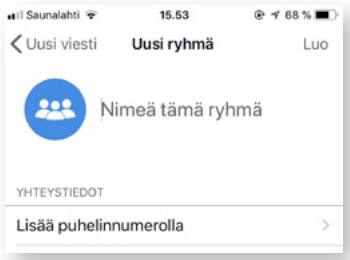
Signalia voi käyttää myös ryhmäkeskusteluihin. Toiminto voi olla hyödyksi, jos toimittaja haluaa esimerkiksi lähettää viestejä ja tiedostoja kollegoilleen, joiden kanssa hän työstää samaa juttua.

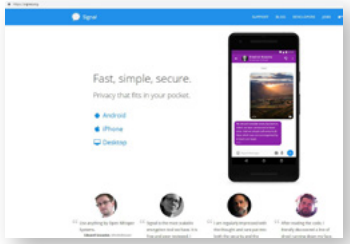
VAIHE VAIHEELTA

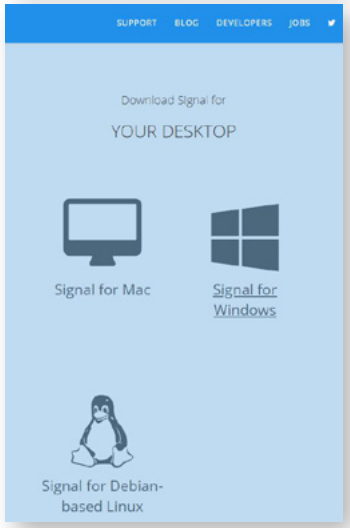
1. Avaa Signal-sovellus ja napauta oikeassa yläkulmassa olevaa viestikuvaketta uuden keskustelun aloittamiseksi. Napauta sitten ryhmäkuvaketta oikeassa yläkulmassa.
2. Voit antaa ryhmälle nimen ja lisätä keskusteluun osallistujia. Voit valita käyttäjiä omista Signal-yhteystiedoistasi tai syöttää osallistujien puhelinnumeroita. Ryhmän kuvan voi vaihtaa ja muitakin asetuksia muuttaa haluttaessa.
3. Toistaiseksi ryhmien perustaminen Signalissa on mahdollista ainoastaan puhelimella. Kun ryhmäkeskustelu on perustettu, siihen voi kuitenkin kirjoittaa viestejä myös tietokoneelta, jolle Signal on asennettu. Seuraavalla sivulla annetaan siihen ohjeet. Ominaisuudesta voi olla paljon hyötyä, jos joukko toimittajia työskentelee saman aiheen parissa.

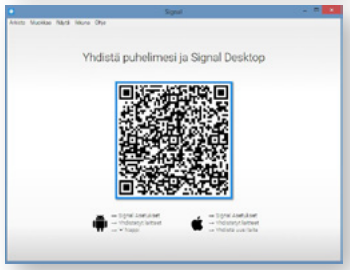


Muista!
Signal-keskustelusta voi tietenkin poistaa myös yksittäisiä viestejä tai tiedostoja. Se onnistuu painamalla viestiä niin kauan, kunnes näyttöön avautuu valikkoikkuna. Huomaa kuitenkin, että tällöin viesti tai tiedosto poistuu keskustelusta vain omalta laitteeltasi. Jos se halutaan poistaa kaikkien keskustelun osallistujien laitteilta, on käytettävä viestien hävittämistoimintoa.









CHAT JA SÄHKÖPOSTI SIGNALIN TYÖPÖYTÄSOVELLUKSESSA

Signal on saatavana myös tietokoneelle työpöytäsovelluksena. Sen asentaminen voi olla järkevää, jos toimittaja käyttää Signalia ensisijaisena viestintävälineenään journalistisessa työssä ja käy sen välityksellä paljon tai pitkiä salattuja keskusteluja. Kun Signalilla kirjoitetaan viestejä tietokoneella, se toimii samoin kuin mikä tahansa chat-keskustelu.

Signal työpöytäsovelluksella keskusteluihin voi liittää kuvia ja muita tiedostoja tietokoneelta ja lähettää suuriakin liitetiedostoja. Signalia voi siis käyttää aivan kuten sähköpostia, mutta se on helpompi ja turvallisempi vaihtoehto, koska metatietoja tallentuu vähemmän.

Keskustelu synkronoidaan automaattisesti puhelimen ja tietokoneen välillä, joten Signalia voi käyttää sujuvasti vaikka vuorotellen molemmilla laitteilla. Tietokoneen ja puhelimen välinen tiedonsiirto on salattua, joten kukaan ei pääse keskusteluihin käsiksi.

VAIHE VAIHEELTA

1. Mene osoitteeseen signal.org ja valitse *Desktop*. Valitse Signal Mac- tai Windows-tietokoneeseen.
2. Lataa asennuspaketti. Se on siirrettävä manuaalisesti ohjelmakansioon.
3. Kaksoisnapsauta Signalia ohjelman käynnistämiseksi. Ensimmäisellä kerralla käynnistyminen voi kestää jonkin aikaa, sillä aiemmat keskustelut ladataan tietokoneelle.
4. Nyt voit lähettää ja vastaanottaa viestejä Signalin kautta myös tietokoneella.

Voit luoda uuden keskustelun Signalissa hakemalla tallennetun yhteystiedon tai syöttämällä puhelinnumeron vasempaan yläkulmaan. Ryhmäkeskusteluja ei kuitenkaan tätä nykyä voi luoda Signal-työpöytäso-

velluksella, vaan ne on aloitettava puhelimella. Sen jälkeen keskustelua voi jatkaa myös tietokoneella.

8.3 Muita viestisovelluksia

Snowdenin tekemien joukkovalvontapaljastusten myötä turvallisten viestisovellusten kysyntä on kasvanut. Markkinoille on tullut useita kaupallisia salattuja viestisovelluksia.

Niillä on hyvät ja huonot puolensa verrattuna esimerkiksi Signaliin.

Suurin haittapuoli palveluissa on, että ne kaikki tallentavat paljon enemmän metatietoja kuin Signal. Signal tallentaa ainoastaan tiedon siitä, milloin käyttäjä on ottanut sovelluksen käyttöön ja käyttänyt sitä viimeksi. Useat kaupalliset sovellukset sitä vastoin tallentavat ja luovuttavat tietoja siitä, kenen kanssa käyttäjä viestii, milloin ja missä. Tällaiset tiedot voivat kertoa jopa enemmän kuin viestiliikenteen sisältö.

Toinen ongelma on se, ettei mikään kyseisistä palveluista perustu täysin avoimeen lähdekoodiin. Sen vuoksi niistä on vaikeampi havaita mahdollisia takaportteja ja muita tietoturvapuutteita kuin esimerkiksi Signalista.

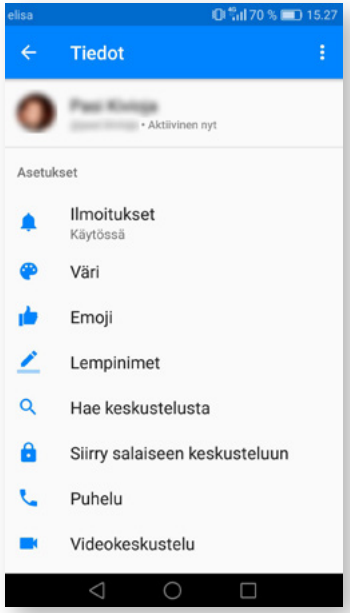
Joskus voi kuitenkin olla järkevää käyttää kaupallista viestisovellusta Signalin sijaan.

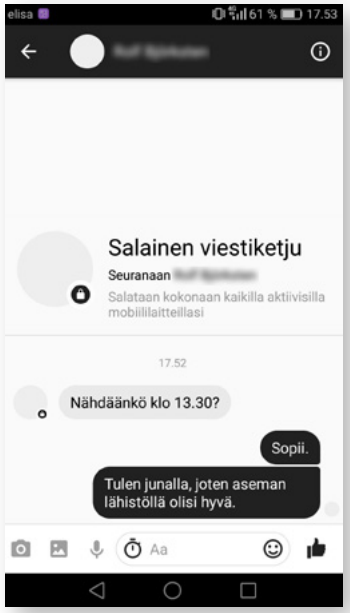
Joissakin tilanteissa tai maissa jo se voi olla raskauttavaa, että toimittajalla tai hänen kontaktillaan ylipäätään on Signalin kaltainen sovellus käytössään. Esimerkiksi WhatsApp ja Telegram ovat paljon Signalia yleisempiä sovelluksia useimmissa Afrikan ja Lähi-idän maissa.

Toimittaja saattaa myös olla tekemisissä kontaktien kanssa, joilla ei ole varaa hankkia Signalin käytön edellyttämiä uudehkoja laitteita. Kaikki lähteet eivät myöskään ole teknisesti niin valveutuneita, että suoriutuisivat asentamisesta.

Jälleen kerran turvallisimman viestintävälineen valinta määräytyy täysin sen mukaan, missä tilanteessa sitä on tarkoitus käyttää.

Seuraavassa pureudutaan kaupallisten salattujen viestisovellusten ominaisuuksiin.





FACEBOOK MESSENGER

Puhelimessa käytettävän Messenger-sovelluksen keskustelut voi muuttaa salatuiksi.

Niiden sisältö salataan päästä päähän -salauksella, joka perustuu Signalin kehittäjien luomaan protokollaan. Viestien sisältö pysyy sen vuoksi salassa yhtä hyvin kuin Signalia käytettäessä.

Facebook Messenger kuitenkin tallentaa keskusteluista paljon metatietoja. Facebook pitää kirjaa esimerkiksi siitä, kenen kanssa käyttäjä viestii ja milloin.

Keskustelut voi salata ainoastaan silloin, kun Facebook Messenger -sovellusta käytetään mobiililaitteella eli esimerkiksi puhelimella. Jos keskustelua käydään Facebookin kautta tietokoneen verkkoselaimella, viestit eivät ole salattuja. Myöskään monenkeskistä chat-keskustelua tai puheluita ja videochatteja ei salata.

VAIHE VAIHEELTA

1. Napsauta yhteystiedon nimen vieressä olevaa i-kirjainta keskustelun yläosassa Facebook Messenger -sovelluksessa.
2. Valitse *Siirry salaiseen keskusteluun*.
3. Yhteystiedon kanssa luodaan uusi salattu keskustelu. Viestit näytetään mustalla taustalla sinisen sijaan. Nyt keskustelu on salattu päästä päähän, ja sen sisältö on turvassa. Muista kuitenkin, että metatietojen tallentaminen voi aiheuttaa turvallisuusriskin.

WHATSAPP

WhatsApp-viestisovelluksen omistaa Facebook. Facebook Messengerin tavoin myös WhatsAppissa käytetään Signalin kehittämää huipputurvallista päästä päähän -salausprotokollaa.

WhatsApp-viestit salataan automaattisesti, ja sovelluksessa on paljon samoja toimintoja kuin Signalissa: viestintäkumppanin sormenjäljen todentaminen, puhelinkeskustelu, videochat, ryhmäpuhelu ja niin edelleen.

Jälleen kerran metatiedot ovat ratkaiseva erottava tekijä. Facebook osti WhatsAppin vuonna 2014, ja siitä lähtien käyttäjien metatietoja on siirtynyt WhatsAppista Facebookille.

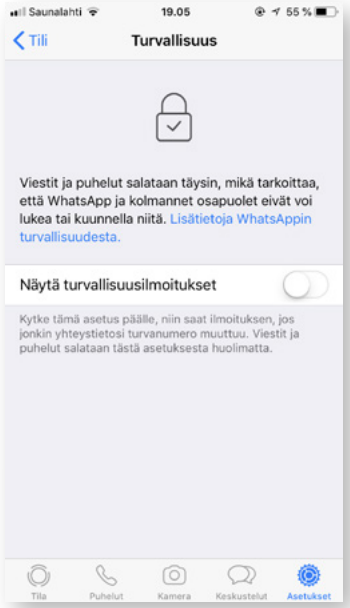
TELEGRAM

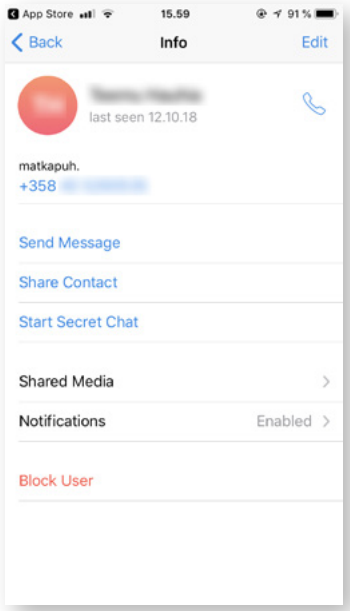
Dubailaisyrityksen markkinoima Telegram Messenger on venäläistaustaisten ohjelmoijien luoma viestisovellus. Sillä käytävät keskustelut voidaan salata päästä päähän. Niitä ei salata automaattisesti, vaan salaus on otettava käyttöön yhteystietoasetuksissa valitsemalla kontaktin kohdalla *Start Secret Chat*.

Sen jälkeen keskustelujen sisältö salataan Telegramin omalla salausprotokollalla. Jos keskustelua ei ole salattu, Telegramilla on pääsy sekä keskustelujen metatietoihin että sisältöön.

Salatuista keskusteluista sovellus saa käyttöönsä ainoastaan metatiedot.

Monet tietoturva-asiantuntijat kehottavat valitsemaan jonkin muun vaihtoehdon Telegramin sijaan muun muassa siitä syystä, että sovelluksen salausprotokollasta on löydetty paljon virheitä.

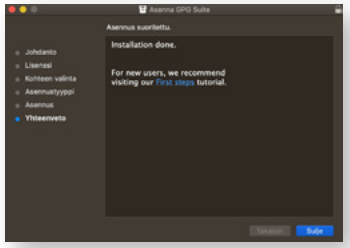




FAKTA: PGP VAI GPG?

Ohjelmoija Phil Zimmermann kehitti PGP-salauksen vuonna 1991 salatakseen muun muassa aktivistien viestintää. Lyhenne tulee sanoista *Pretty Good Privacy* eli aika hyvä tietoturva, mutta todellisuudessa se suojaa viestejä erittäin hyvin. PGP on kaupallinen sovellus, josta on sittemmin kehitetty samaan tekniikkaan perustuva maksuton avoimen lähdekoodin versio, jonka nimi on GPG. Tässä luvussa kuvataan GPG-salausta, mutta arkisessa puheessa molemmista salausmenetelmistä käytetään usein lyhennettä PGP.





8.4 Sähköpostien PGP-salaus

Salattujen sähköpostiviestien lähettämiseen ja vastaanottamiseen tarvitaan PGP-salausprotokollaa. PGP:n käyttö on melko monimutkaista, sillä siinä käyttäjän on itse luotava salausavainpari ja vaihdettava julkisia avaimia viestintäkumppaninsa kanssa. Samalla se on myös yksi turvallisimmista salaustavoista.

VAIHE VAIHEELTA: MAC

Sähköpostien PGP-salauksessa on kolme vaihetta, joihin viitataan tässä selvyyden vuoksi kirjaimilla **A**, **B** ja **C**.

A: GPG Keychain

1. Ensimmäiseksi tietokoneelle on ladattava ohjelma, jolla luodaan salausavaimia. Ohjelman voi ladata osoitteesta gpgtools.org napsauttamalla *Download GPG Suite* -latauspainiketta.

2. Etsi GPG_Suite-tiedosto kansiosta, johon se tallennettiin. Tietokoneen vakioasetuksilla tallennuskohde on Lataukset-kansio. Kansioon siirtymisen sijaan tiedoston voi avata myös tietokoneen sovelluspalkin latauksista. Avaa paketti napsauttamalla sitä.

Näyttöön avautuu ikkuna, jossa pyydetään asentamaan GPG Suite napsauttamalla ohjelmakuvaketta. Noudata ohjeita ja valitse *Asenna*.

3. Käy läpi asennusprosessi napsauttamalla aina *Seuraava*-painiketta, kunnes viereinen ikkuna (vas. alh.) tulee näkyviin.

Nyt GPG Keychain on asennettu tietokoneen ohjelma- tai lisäohjelmakansioon. Sinun ei tarvitse aktiivisesti käyttää sovellusta, vaan muut prosessiin osallistuvat ohjelmat tarvitsevat sitä salauksen toteuttamiseksi.

B: Thunderbird

1. Tarvitset sähköpostiohjelman, joka tukee viestien salausta. Voit käyttää tietokoneelle asennettua oletussovellusta, mutta helppokäyttöisempi vaihtoehto salauksen yhteydessä on ilmaisohjelma Thunderbird. Sen voi ladata osoitteesta mozilla.org/da/thunderbird napsauttamalla vihreää latauspainiketta.

2. Etsi Thunderbird-tiedosto kansiosta, johon se tallennettiin. Avaa paketti napsauttamalla sitä.

Näyttöön avautuu ikkuna, jossa pyydetään asentamaan Thunderbird vetämällä se ohjelma- tai lisäohjelmakansioon. Noudata ohjeita ja vedä Thunderbird-kuvake ohjelmakansion kuvakkeen päälle.

Nyt Thunderbird on asennettu ohjelmakansioon. Halutessasi voit kiinnittää ohjelman pikakuvakkeen tietokoneen ohjelmapalkkiin vetämällä sen näytön alareunaan muiden kuvakkeiden viereen.

3. Avaa Thunderbird napsauttamalla sen kuvaketta. Vastaa varmistuskysymykseen ohjelman avaamisesta napsauttamalla *Avaa*.

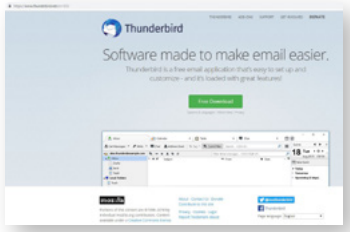
4. Tee sähkopostiohjelmaan tarvittavat asetukset, jotta se hakee viestit omalta sähköpostitililtäsi. Jos ohjelma ei käynnistä asetusten luomisprosessia automaattisesti, valitse *Hanki uusi sähköpostitili*.

5. Halutessasi voit tehdä ohjelmasta oletussovelluksen sähköpostien käsittelyyn tai luoda uuden sähköpostiosoitteen.

Tässä esimerkissä käytetään olemassa olevaa Gmail-osoitetta sen osoittamiseksi, miten salausta voidaan käyttää verkkopohjaisen webmail-sähköpostin yhteydessä. Napsauta *Ohita tämä kohta ja käytä olemassa olevaa sähköpostiosoitetta*.

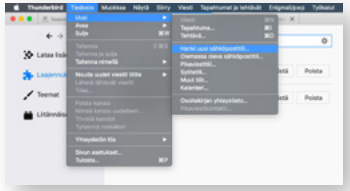
Täytä kenttiin sähköpostiosoitteesi tiedot ja salasana. Napsauta *Jatka* ja sitten *Luo tili*.

6. Sinut ohjataan omaan sähköpostiisi verkkoselaimessa – esimerkissämme Gmailin sivustoon. Siellä sinun on annettava Thunderbirdille sähköpostitilisi käyttöoikeus.

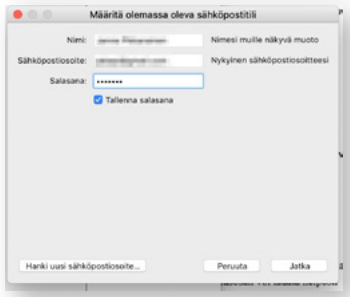


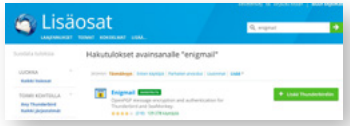


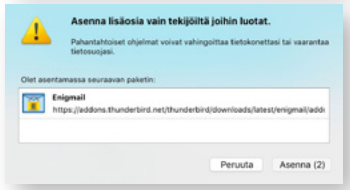


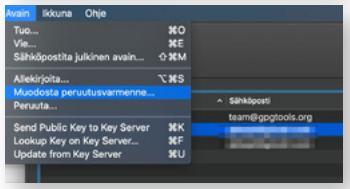


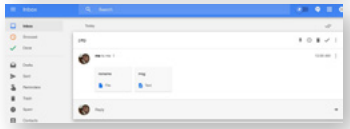












FAKTA: PGP-AVAINPARIT

Salausavain on kahden yhteensopivan avaimen pari. **Julkisella** avaimella salataan eli lukitaan viestejä. Sen voi luovuttaa toisille tai laittaa julkisesti saataville esimerkiksi omalle kotisivulleen. **Yksityisellä** avaimella avataan viestejä eli puretaan niiden salaus. Se on tallennettu ainoastaan käyttäjän tietokoneelle, eikä sitä saa koskaan luovuttaa kenellekään ulkopuoliselle.

C: Enigmail

Kun Thunderbird on asennettuna tietokoneelle, siinä on käytettävä laajennusosaa, jonka ansiosta se voi salata viestejä GPG-avaimilla. Enigmail-nimisen laajennusosan voi ladata helposti Thunderbirdin kautta.

1. Napsauta Thunderbird-ikkunan oikeassa yläkulmassa, hakukentän vieressä olevaa pientä nelikulmaista valikkokuvaketta.

2. Avaa valikosta *Lisäosat*, sitten *Laajennukset* ja kirjoita oikean yläkulman hakukenttään ”Enigmail”. Kun Enigmail on löytynyt, napsauta sen asennuspainiketta.

3. Näyttöön avautuu Enigmailin ohjattu asennus. Jos asennus ei jostain syystä ala automaattisesti, sen voi käynnistää näytön yläreunasta valikkoriviltä kohdasta *Enigmail → Setup Wizard*.

4. Siirry asennusprosessissa eteenpäin hyväksymällä Enigmailin ehdottamat vakioasetukset *Jatka*-painikkeella, kunnes näkyvissä on seuraava ikkuna:

5. Luo itsellesi PGP-avain. Valitse avaimelle vahva salasana, jonka varmasti muistat. Tarvitset sitä aina, kun purat sähköpostiviestin salauksen. Salasanan on oltava toimiva. Luvussa 7 annetaan ohjeita vahvojen salasanojen ja -lauseiden luomiseksi. Napsauta sitten *Jatka*.

Jos olet luonut hyvän, turvallisen salasanan, näyttöön ilmestyy luultavasti dialogi-ikkuna, jossa varoitetaan liian pitkästä salasanasta. Kuittaa huomautus napsauttamalla *Ohita*.

6. Ennen kuin Enigmail voi luoda salausavaimia, sinun on luotava peruutussertifikaatti. Sen avulla voit peruuttaa salausavaimesi, jos tietokoneesi varastetaan ja avaimet poistuvat hallustasi. Napsauta *Create Revocation Certificate*. Seuraavaksi sinun on syötettävä uusi salasanasi ja valittava sertifikaatille tallennuskohde, esimerkiksi Dokumentit-kansio. Kun sertifikaatti on luotu, se kannattaa varmuuden vuoksi tallentaa myös jonnekin muualle kuin tietokoneelle – esimerkiksi muistitikulle, jota säilytät varmassa tallessa.

7. Kun peruutussertifikaatti on luotu, Enigmail aloittaa salausavainten luomisen. Ikkunan on pysyttävä auki koko prosessin ajan. Kun avaimet on luotu, voit jatkaa eteenpäin.

Nyt voit aloittaa salattujen sähköpostien käytön.

PGP-AVAINTEN KÄYTTÖÖNOTTO

Kun sähköpostien salaamiseen tarvittavat sovellukset on asennettu ja PGP-avaimet luotu, on aika aloittaa niiden käyttö. Seuraavassa kerrotaan, kuinka se tapahtuu.

1. Julkinen avaimesi löytyy aina ikkunan yläreunan valikkoriviltä *Enigmail*-valikon *Key Management* -kohdasta.

2. Jotta muut käyttäjät voivat vaihtaa salattuja viestejä kanssasi, he tarvitsevat julkista salausavaintasi. Voit toimittaa sen heille eri tavoin.

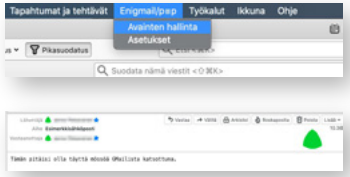
Jos haluat, että julkinen avaimesi on helposti uusien lähteiden ja muiden tuntemattomia saatavilla, se kannattaa panna näkyville julkisesti. Silloin kuka tahansa voi lähettää sinulle salattuja viestejä. Sopiva julkaisupaikka voi olla esimerkiksi kotisivu, blogiprofiili tai vastaava helposti löydettävissä oleva paikka. Yleisiä tapoja ovat myös julkisen avaimen julkaiseminen erityisillä verkkosivuilla, kuten keybase.io -sivustolla, ja niiden ilmoittaminen sosiaalisen median käyttäjäprofiileissa.

Jos napsautat julkista avaintasi hiiren kakkospainikkeella, pääset ensimmäisistä valikkokohdista kopioimaan avaimen leikepöydälle tai tallentamaan sen tiedostona. Näin tallentuva tiedosto on se, jota sinun on käytettävä julkisen avaimesi julkaisemiseen esimerkiksi kotisivullasi.

Useimmat PGP-salauksen käyttäjät lataavat julkisen avaimensa avainpalvelimelle (*key server*). Avainpalvelimet ovat ikään kuin verkossa toimivia julkisten avainten puhelinluetteloita, ja niiltä voi etsiä myös

VINKKI!

Yhä useammat toimittajat asettavat julkisen PGP-avaimensa saataville internetiin, jotta lähteet ja muut kiinnostuneet voivat lähettää heille salattuja sähköpostiviestejä helposti. Se on harkitsemisen arvoinen toimintatapa. Julkisen avaimen voi julkaista esimerkiksi omilla kotisivuillaan tai blogissaan. Sormenjäljen voi liittää sähköpostin allekirjoitukseen ja avaintunnuksen Twitter-profiiliin, jotta avaimen voi todentaa.

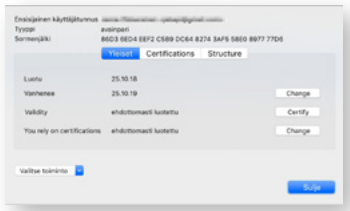


SORMENJÄLJET JA AVAIN-ID

Salausavaimet ovat pitkiä ainutkertaisia merkkijonoja, jotka koostuvat numeroista, erikoismerkeistä ja kirjaimista. Julkinen avain voi olla kymmenen- tai kaksikymmentätuhatta merkkiä pitkä ja yksityinen avain vielä pidempi.

Jokaisella julkisella avaimella on myös sormenjälki, joka on paljon lyhyempi mutta niin ikään ainutkertainen merkkijono. Sen avulla julkisen avaimen voi tunnistaa sen aitouden todentamiseksi.

Avain-ID:n pitkä muoto koostuu sormenjäljen 16 viimeisestä merkistä ja lyhyt sen kahdeksasta viimeisestä merkistä. Mitä lyhyempi avaimen todentamiseen käytettävä merkkijono on, sitä epävarmempi on todennustulos.



muiden käyttäjien julkisia avaimia. Valitettavasti järjestelmä ei toimi kovin hyvin muun muassa sen vuoksi, että avainpalvelimia on paljon, ja on vaikea tietää, miltä palvelimelta löytää etsimänsä.

Valikon kautta on mahdollista myös ladata julkinen avain avainpalvelimelle. Tätä opasta kirjoitettaessa suosituin avainpalvelin oli pgp.mit.edu.

Jos haluat saattaa julkisen avaimesi ainoastaan valikoitujen ihmisten tietoon, sitä ei tietenkään kannata julkaista yleisesti. Joissakin maissa voi aiheutua ongelmia jo siitä, että he ovat yhteydessä henkilöön, joka ilmoittaa julkisesti käyttävänsä salausta. Yksi tapa käyttää salausta on uuden julkisen avaimen luominen tiettyä arkaluonteista juttua varten.

Julkisen avaimen voi siis lähettää myös sähköpostilla viestintäkumppaneilleen ja tähdentää heille, etteivät he saa antaa avainta kenellekään muulle. Avaimen voi lähettää sähköpostiviestillä kolmannesta valikkokohdasta, joka avautuu kakkospainikkeella napsauttamalla.

3. Kun olet luovuttanut julkisen avaimesi viestintäkumppanillesi tai julkaissut sen, sinun on huolehdittava siitä, että avaimen sormenjälki on mahdollista todentaa jotakin muuta kanava käyttäen.

Voit esimerkiksi liittää sormenjälkesi sähköpostiallekirjoitukseesi, painattaa sen käyntikorttiisi tai julkaista sen sosiaalisen media profiilitiedoissasi. Jotkut toimittajat pitävät lyhennettyä sormenjälkeään eli avain-ID:tään näkyvissä Twitter-profiilissaan, toiset taas käyttävät linkkejä sivuille, joilta heidän julkisen avaimensa ja sormenjälkensä voi todentaa turvallisesti.

Julkisen avaimesi sormenjälki näkyy ikkunassa, joka avautuu, kun kaksoisnapsautat avainsymbolia *Key Management* -ikkunassa tai valitset *Key Properties* -kohdan kakkospainikkeella avautuvasta valikosta.

SALATUN SÄHKÖPOSTIN LÄHETTÄMINEN

Nyt olet valmis lähettämään ensimmäisen salatun sähköpostiviestisi. Tarvitset sitä varten viestin vastaanottajan julkisen salausavaimen. Sen voi löytää avainpalvelimelta ja todentaa luotettavasti tai noutaa sen paikasta, jossa vastaanottaja on julkaissut oman avaimensa.

Tässä esimerkissä käytetään toimittaja Glenn Greenwaldin julkista salausavainta, jonka hän on julkaissut The Intercept -julkaisun verkkosivustolla. Greenwald oli perustamassa julkaisua Snowden-paljastustensa jälkeen.

1. Glenn Greenwaldin julkinen salausavain on saatavilla hänen profiilissaan The Intercept -sivustolla.

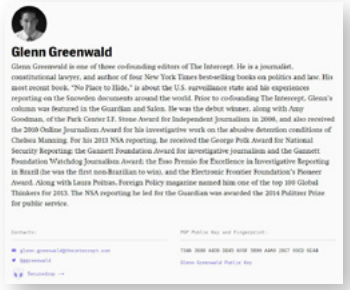
Napsauttamalla *Glenn Greenwald public key* -linkkiä avain tulee näkyviin.

2. Valitse koko teksti *Muokkaa*-valikon *Valitse kaikki* -kohdasta tai näppäinkomennolla ⌘ A. Tallenna tiedosto asc-muodossa *Tiedosto*-valikon *Tallenna sivu* -toiminnolla tai näppäinkomennolla ⌘ S. Tiedostopäätteen on ehdottomasti oltava .asc. Jos pääte on jokin muu, muuta se oikeaan muotoon.

Avaa Thunderbirdin *Enigmail*-valikosta *Key Management*. Tiedostovalinnoissa on käytettävissä avaintiedostojen tuontitoiminto eli *Import Keys from File*. Valitse Greenwaldin avain kohteesta, johon tallensit sen.

Nyt Glenn Greenwaldin julkinen salausavain on tuotu avaintenhallintaasi.

Kun aloitat uuden viestin luomisen Thunderbirdillä ja kirjoitat vastaanottajan kohdalle Greenwaldin sähköpostiosoitteen, pääset napsauttamaan mustaa aukinaista riippulukkoa sähköposti-ikkunan yläreunassa. Lukko menee kiinni ja muuttuu keltaiseksi, ja näkyviin tulee viestin salaamisesta kertova ilmoitus *This message will be encrypted*. Koko viestin sisältö ja sen mahdollisten liitetiedostojen sisältö salataan nyt





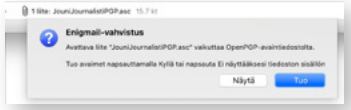
siten, että ulkopuoliset voivat nähdä ainoastaan metatiedot siitä, ketkä viestinvaihtoa käyvät ja milloin, sekä viestin aiherivin tiedot.

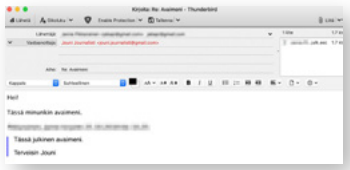
Jos napsautat *Attach My Public Key* -painiketta, julkinen salausavaimesi liitetään viestiin automaattisesti. Sen avulla Glenn Greenwald voi lähettää sinulle salatun sähköpostiviestin.

Nyt olet valmis lähettämään ensimmäisen salatun sähköpostiviestisi. Jos vastedes viestit kontaktien kanssa, joiden avain on tallennettu tietokoneellesi, heille osoitettu sähköposti salataan automaattisesti.

AVAINPYYNTÖÖN VASTAAMINEN

Jos lähde tai muu henkilö, joka haluaa viestiä kanssasi salatussa yhteydessä, ei löydä julkista avaintasi, saatat saada häneltä sähköpostiviestin, jonka liitteenä on hänen julkinen avaimensa. Hän pyytää vastaamaan viestiin lähettämällä oman avaimesi hänelle.







1. Sähköpostiviestiä ei ole salattu. Napsauta saapuneen viestin liitteenä olevaa avaintiedostoa hiiren kakkospainikkeella ja valitse *Import OpenPGP Key*. Avain tuodaan avaintenhallintaasi.

2. Nyt voit vastata saamaasi viestiin salatulla sähköpostiviestillä. Liitä viestiin oma julkinen salausavaimesi napsauttamalla valikkorivin *Attach My Public Key* -painiketta. Muista kertoa, miten viestin vastaanottaja voi todentaa avaimesi luotettavuuden.

3. Ohjelma pyytää sinua valitsemaan, miten liitetiedostot salataan. Paras vaihtoehto on aina sähköpostiviestin salaaminen kokonaisuudessaan, sillä silloin liitetiedostoista paljastuu mahdollisimman vähän metatietoja.

4. Nyt voitte viestiä salatuilla sähköpostiviesteillä. Jos sinulla on Gmail-tili ja kirjaudut sille verkkoselaimesta, näet, miltä viestit näyttävät ilman salausavaimia. Aiherivi sekä metatiedot lähettäjästä ja vastaanottajasta ja viestinvaihdon ajankohdasta ovat

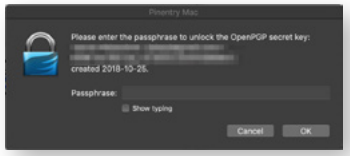
luettavissa, mutta viestin varsinainen sisältö on lukukelvotonta salattua ”merkkimössöä”.

Jos haluat piilottaa tiedon viestintäkumppanistasi ja siitä, että viestintänne on salattua, sinun on tehtävä Thunderbirdiin anonyymin sähköpostitilin asetukset. Tili on perustettava Tor-verkkoselaimella, etkä saa käyttää omaa nimeäsi tai muita tietoja, joista sinut voi tunnistaa.

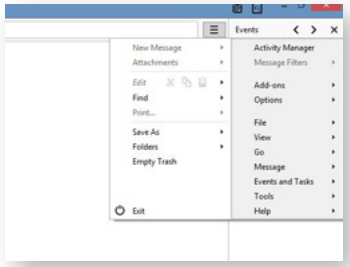
5. Kun kontaktisi lähettää sinulle salatun vastausviestin, pääset lukemaan sen syöttämällä salausavaimesi salasanan, jonka loit PGP-avaintesi yhteydessä.

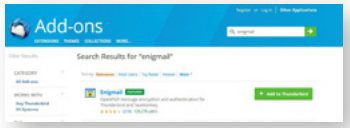
6. Salasanan syöttämisen jälkeen sähköpostiviestin ja sen liitetiedostojen salaus aukeaa – vain sinulle.

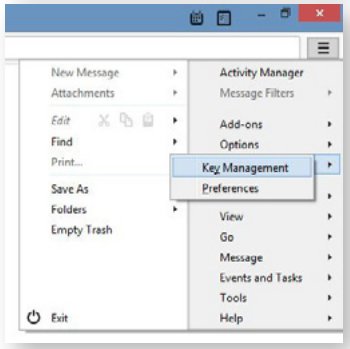
Nyt osaat käyttää monimutkaisimpia kehitettyjä salausvälineitä, joita edes NSA ei ole pystynyt murtamaan.











VAIHE VAIHEELTA: WINDOWS

Windows-ympäristössä PGP-salauksen käyttöönotto tapahtuu pitkälti samoin kuin Macissa.

1. Windowsin PGP-sovellus on nimeltään Gpg4win. Sen voi ladata osoitteesta gpg4win.org.

2. Kun olet asentanut tietokoneellesi Thunderbirdin Mac-käyttöjärjestelmää koskevan kuvauksen mukaisesti, voit avata Enigmailin Thunderbirdin oikeassa yläkulmassa olevan asetusvalikon laajennuksista.

3. Kirjoita hakukenttään ”Enigmail”, ja kun lisäosa tulee näkyviin, napsauta sen vieressä olevaa *Asenna*-painiketta.

4. Käynnistä Thunderbird uudelleen linkin kautta ja seuraa sovelluksen asennusohjeita. Enigmail on asennettu. Nyt voit luoda Thunderbirdiin toisen sähköpostitilin Mac-ympäristöä koskevien ohjeiden mukaisesti.

5. Thunderbirdin Windows-versiossa avaintenhallinnan Key Manager sijaitsee oikean laidan valikossa.

6. PGP-salaukseen tarvittavien sovellusten asentaminen ja käyttö tapahtuu samoin kuin Mac-ympäristössä.

9

Jälkien peittäminen verkossa

Suuri osa digitaalisesta toiminnastamme tapahtuu internetissä: tviittaaminen, Facebook-chat, Gmail-sähköpostin käyttö, hakukoneiden käyttö ja niin edelleen.

Sitä mukaa kun datamäärä kasvaa, yhä suurempi osa datasta säilytetään sellaisissa kolmannen osapuolen pilvipalveluissa kuin Google, Facebook tai Dropbox. Esimerkiksi Google-pohjaista sähköpostia voi käyttää sähköpostiarkistona, jossa säilytetään viestejä vuosien takaa. Kuvia tallennetaan Dropboxiin, työtiedostoja jaetaan Google Drivessä, tapaamistietoja tallennetaan verkkopohjaisiin kalentereihin ja pikaviestejä vaihdetaan Facebook Messengerissä. Monet internetin käyttäjät ovat uskoneet valtavan määrän työhön ja yksityiselämään liittyviä tietojaan verkkopalvelujen haltuun.

Tiedot ovat arvokasta omaisuutta, ja siksi kolmannen osapuolen palvelut ovatkin usein hakkerien ja hyökkäysten kohteena.

Kaksivaiheinen vahvistus

Onneksi käyttäjät voivat itsekin tehdä paljon käyttäjätiliensä suojaamiseksi digitaalisilta hyökkäyksiltä.

Ensinnäkin on käytettävä vahvoja salasanoja ja vältettävä samojen salasanojen käyttöä useissa palveluissa. Tästä kerrotaan lisää luvussa 7.

Lisäksi käyttäjätilit on syytä pitää mahdollisimman hyvässä turvassa. Siihen tarvitaan kaksivaiheista vahvistusta, josta käytetään lyhennettä 2FA.

2FA antaa verkkopalvelujen käytölle lisäsuojaa hyvän salasanan ohella ja vähentää merkittävästi hakkerointiyritysten vaaraa.

Jos hakkeri yrittää kirjautua sisään toisen käyttäjän tilille verkkopalvelussa, hän käyttää siihen tilin haltijan salasanaa. Salasana on ehkä helposti arvattava tai sitä on käytetty useassa palvelussa, ja joltakin sivustolta se on tietoturvavuodon yhteydessä pääty-

nyt ulkopuolisten käsiin. Jos kaksivaiheinen vahvistus ei ole käytössä, hakkeri pääsee kirjautumaan palveluun miltä tahansa tietokoneelta pelkällä käyttäjätunnuksella ja salasanalla.

Kaksivaiheinen vahvistus tuo kirjautumisprosessiin ylimääräisen vahvistuskierroksen silloin, kun käyttäjätilille halutaan kirjautua laitteelta, jolta sille ei aiemmin ole kirjauduttu.

Ylimääräiseen vahvistukseen käytetään toista kanavaa, johon hakkerilla ei ole pääsyä. Yksi toteutusvaihtoehto on tekstiviestin lähettäminen puhelimeen ja kirjautuminen viestissä ilmoitetulla vahvistuskoodilla. Toinen vaihtoehto on tulostettu vahvistuskoodiluettelo, jota käytetään samaan tapaan kuin esimerkiksi verkkopankin avainlukuja.

Lähes kaikki suuret verkkoalustat tarjoavat käyttäjilleen kaksiportaista vahvistusta jossakin muodossa. turnon2fa.com-sivustoon on koottu englanniksi eri verkkopalvelujen käytäntöjä ja kattavia ohjeita siitä, miten vahvistuksen voi ottaa käyttöön. *Tutorials*-sivulla listataan palvelut, joita koskevia ohjeita sivustolla on tarjolla.

SUOJAUSAVAIMET

Samaan tahtiin kaksivaiheisen vahvistuksen yleistymisen kanssa hakkerit ovat kehittäneet hyökkäystekniikkaansa siten, että he huiputtavat käyttäjiä luovuttamaan vapaaehtoisesti sekä ensimmäisen että toisen tason salasanansa. Lisäturvaa kirjautumiseen voi saada hankkimalla fyysisen suojausavaimen, joka toimii vielä yhtenä kirjautumisvarmenteena. Yleensä avain on muistitikku, joka on laitettava tietokoneeseen esimerkiksi ennen ensimmäistä kirjautumista sähköpostitilille kyseiseltä laitteelta.

Tech Solidarityn verkkosivustolla soitteessa techsolidarity.org/resources.html on englanniksi tietoa siitä, miten suojausavaimen voi hankkia Gmailiin ja suurimpiin sosiaalisen median palveluihin.



MUISTA!

Kannattaa miettiä tarkasti, mitä tallentaa verkkopalveluihin. Kaksivaiheinen vahvistus ja vahvat salasanat auttavat suojaamaan käyttäjätiliä ulkopuolisilta hyökkäyksiltä. On kuitenkin muistettava, että palveluihin tallennetut tiedot eivät ole turvassa palveluiden ylläpitäjiltä. Esimerkiksi Facebook ja Google pääsevät käsiksi käyttäjiensä tietoihin ja luovuttavat niitä säännönmukaisesti viranomaisille oikeuden päätöksellä. Siksi pilvi ei ole oikea paikka arkaluonteisten tietojen säilyttämiseen, jos ne halutaan pitää suojassa. Ne ovat turvassa ainoastaan käyttäjän omilla laitteilla, joissa on käytössä massamuistin salaus ja silloin, kun niitä lähetetään päästä päähän salatulla yhteydellä.

Tor-verkko

Tavallisia verkkoselaimia ovat esimerkiksi Chrome, Safari, Firefox ja Explorer. Kun internetiä käytetään niillä, selain pitää lokia siitä, millä sivustoilla käyttäjä käy ja mitä tietoja hän hakee. IP-osoitteen avulla käyttäjän reitti internetissä voidaan jäljittää siihen toimistoon tai kahvilaan asti, jonka verkon välityksellä yhteys on luotu.

Esimerkiksi internetpalveluntarjoajat pystyvät näkemään, millä kotisivuilla niiden asiakkaat vierailevat. Myös sivustojen ylläpitäjät voivat nähdä, mistä IP-osoitteesta heidän sivuillaan on käyty. Tämä voi olla ongelmallista esimerkiksi silloin, jos toimittaja hankkii tietoja yrityksistä tai muista organisaatioista, muttei halua kohdeorganisaation tai muidenkaan tietävän, että sivuilla on käyty hänen työpaikkansa IP-osoitteesta.

Tällaisia jälkiä voi peittää asentamalla tietokoneelleen anonyymin avoimen lähdekoodin verkkoselaimen nimeltä Tor.

Tor toimii periaatteessa samoin kuin muutkin verkkoselaimet, mutta tietoliikenne kulkee salatussa yhteydessä lukuisten Tor-palvelinten kautta eri puolilla maailmaa. Suoraa yhteyttä käyttäjän ja verkkosivuston välille ei siis synny, joten liikennettä ei myöskään voida jäljittä takaisin käyttäjän IP-osoitteeseen. Tor-selainta käytettäessä edes selaimen ylläpitäjä ei pysty seuraamaan käyttäjän liikkeitä tai hakuja verkossa.

On tärkeää muistaa, että vain internetissä tapahtuva tietoliikenne anonymisoidaan Tor-selainta käytettäessä. Jos selaimelta kirjaudutaan Facebookiin, Gmailiin tai muihin palveluihin, palvelujen ylläpitäjät tietenkin näkevät, mitä sisään kirjautunut käyttäjä tekee. Ainoastaan käyttäjän sijainti pysyy pimennossa.

MUISTA!

Tor on anonymisoiva verkkoselain, mutta se ei huolehdi tietojen salauksesta. Tor-selaimen kautta lähetetyt sähköpostit ja chat-viestit ovat salaamattomia, jos niitä ei erikseen salata.

MILLOIN TOR ON TARPEELLINEN?

Toimittaja voi käyttää Tor-selainta esimerkiksi silloin, kun hän haluaa pitää salassa kertaluonteiset tai toistuvat käyntinsä tietyllä verkkosivustolla tai tiettyä aihetta koskevat hakunsa. Journalistisessa työssä se voi olla tarkoituksenmukaista, jos haluaa olla kiinnittämättä taustatutkimuksen kohteen huomiota. Tor soveltuu käytettäväksi myös joidenkin tässä kirjassa esiteltävien salausvälineiden kanssa, jos toimittaja haluaa vaikkapa käydä salattua chat-keskustelua ja pitää salauksen käytön omana tietonaan.

Tor-selainta kannattaa käyttää anonyymiin verkossa liikkumiseen ja aika ajoin myös muihin puuhiin. Jos Toria käyttää vain yhdellä verkkosivulla vierailemiseen, voi käyttäjä paljastua, kun tuntematto-masta IP-osoitteesta sivustoon suuntautuva liikenne ja hänen Tor-selaimen käyttönsä osuvat aina samaan aikaan. Ei kuitenkaan ole mitään syytä käyttää Tor-selainta koko ajan – varsinkaan, jos selaimella kirjautuu Facebookin tai Gmailin kaltaisiin verkkopalveluihin.

FAKTA: IP-OSOITE

IP-osoite *(Internet Protocol)* on ainutkertainen osoite, jota tietokone, puhelin tai muu päätelaite käyttää internetyhteyden muodostamiseen. IP-osoite kertoo käyttäjän summittaisen sijaintitiedon ja internetpalveluntarjoajan nimen. Tavallisesti verkkosivustolla kävijän tai palvelimen käyttäjän IP-osoite ilmoitetaan aina sivuston tai palvelimen ylläpitäjälle. Tor-selain ja muut vastaavat palvelut piilottavat IP-osoitteen, jolloin verkossa voi liikkua anonyymisti.

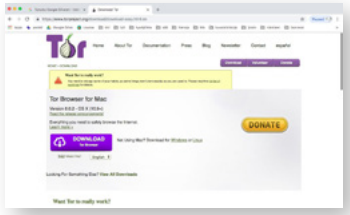
VAIHE VAIHEELTA: MAC

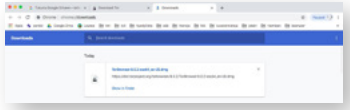
1. Avaa tavallinen verkkoselain (esimerkiksi Chrome tai Firefox) ja mene osoitteeseen torproject.org. Napsauta latauspainiketta.

2. Sinut siirretään lataussivulle, jolla sinulle ehdotetaan automaattisesti tietokoneesi käyttöjärjestelmään sopivaa Tor-selaimen asennustiedostoa. Napsauta latauspainiketta uudelleen. Jos haluat ladata jonkin muun version kuin automaattisesti tarjotun, pääset vaihtamaan asennustiedostoa painikkeen vieressä olevan linkin kautta.

3. Etsi Tor Browser -asennustiedosto kansiosta, johon se tallennettiin. Tietokoneen vakioasetuksilla tallennuskohde on Lataukset-kansio. Kansioon siirtymisen sijaan tiedoston voi avata myös tietokoneen sovelluspalkin latauksista. Avaa paketti napsauttamalla sitä.

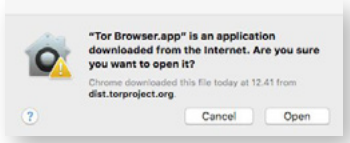


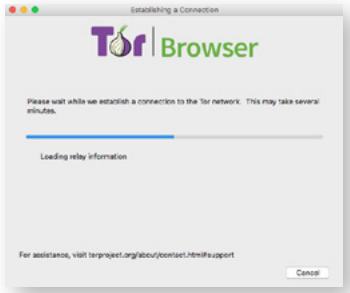


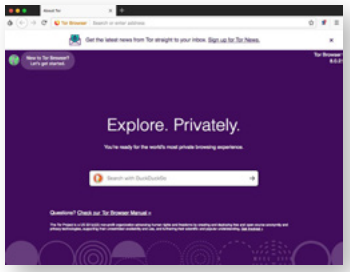












4. Näyttöön avautuu ikkuna, jossa pyydetään asentamaan Tor Browser vetämällä se ohjelma- tai lisäohjelmakansioon. Noudata ohjeita ja vedä Tor-kuvake kansion kuvakkeen päälle. Nyt Tor on asennettu kyseiseen kansioon.

5. Nyt voit avata Tor-selaimen ohjelma- tai lisäohjelmakansiosta kaksoisnapsauttamalla sen kuvaketta. Halutessasi voit kiinnittää Torin myös tietokoneen ohjelmapalkkiin vetämällä sen kuvakkeen näytön alareunaan muiden kuvakkeiden viereen. Ensimmäisellä käyttökerralla Tor saattaa käynnistyä hieman jähmeästi.

Kun avaat Tor-selaimen ensimmäistä kertaa, näyttöön avautuu ohjelman alkuperästä varoittava ikkuna. Vaikka tällaiset varoitukset on yleensä syytä ottaa vakavasti, napsauta Avaa, sillä tiedät sovelluksen luotettavaksi.

Näyttöön avautuu ikkuna, jossa voit muuttaa sovelluksen asetuksia. Tor-selaimen peruskäytössä se ei ole välttämätöntä, joten voit jatkaa eteenpäin napsauttamalla *Connect*. Nyt näyttöön avautuu ikkuna, jossa näkyy sininen palkki, kun tietokone luo yhteyttä Tor-verkkoon.

6. Lopuksi näkyviin tulee violetti ruutu, ja Tor-selain on valmis anonyymiin surfaamiseen verkossa. Selain toimii pääpiirteissään samoin kuin muutkin verkkoselaimet, mutta se voi olla hieman totuttua hitaampi, koska liikenne kulkee monen eri palvelimen kautta. Huomaa, että Torissa ei ole valmiina asetusta, joka käyttäisi Googlea hakukoneena.

Jos haluat varmistaa, että käytät internetiä Tor-verkon kautta, voit mennä Tor-selaimella osoitteeseen check.torproject.org. Jos olet Tor-verkossa, näytölle avautuu selainikkuna, jossa lukee: *"Congratulations. This browser is configured to use Tor."*

VPN

IP-osoitteen piilottamiseen voi käyttää myös VPN-yhteyttä. VPN-palvelun kautta voi luoda salatun internetyhteyden, jossa IP-osoitetta ei paljasteta. Sen avulla käyttäjä voi ohjata tietoliikenteensä uudelleen ja esimerkiksi kiertää maakohtaiset estot, joita erilaisilla sisällöillä voi olla. Hyvä kaupallinen VPN-yhteyspalvelu on suomalaisen F-Securen Freedome VPN, joka on ladattavissa internetistä. Suuri ero Tor-verkkoon nähden on kuitenkin se, että VPN-palveluntarjoaja voi tarkkailla palvelun kautta kulkevaa tietoliikennettä. Jos esimerkiksi Freedomen käyttäjä vierailee tietyllä verkkosivulla, muut verkon käyttäjät tai verkkosivun ylläpitäjä eivät saa siitä tietoa, mutta F-Secure kylläkin. Ominaisuus voi olla ongelmallinen, jos jos olet valinnut jonkin epäilyttävän palveluntarjoajan VPN-yhteyden.

VINKKI!

Huolehdi päivityksistä. Kun olet asentanut Tor-selaimen koneellesi, siihen tulee melko usein tarjolle uusia versiopäivityksiä. Päivitykset kannattaa tehdä, kun avaa selaimen. Näin yhteys on aina mahdollisimman turvallinen. Uusin versio on aina saatavana Tor-selaimen vasemman laidan valikkopalkissa olevan sipulikuvakkeen kautta.

9

10
Tietojen kalastelun vaarat

Edellisissä luvuissa kerrottiin mahdollisuuksista suojautua tietoihinsa kohdistuvilta väsytyshyökkäyksiltä, joissa yritetään esimerkiksi murtaa salasanoja tai saada kolmannen osapuolen palveluntarjoajat luovuttamaan tietoja.

Usein digitaaliset hyökkäykset on toteutettu varsin ovelasti. Pahaa aavistamaton uhri pyritään saamaan asentamaan haittaohjelma omalle laitteelleen itse tai luovuttamaan salasanansa vapaaehtoisesti. Tätä kutsutaan tietojen kalasteluksi eli verkkourkinnaksi (*phishing*). Kalasteluyritykset voivat olla laaja-alaisia tai kohdennettuja.

Laaja-alaisessa tietojen kalastelussa hakkeri lähettää samankaltaisen viestin suurelle ihmisjoukolle ja toivoo, että edes muutama käyttäjä nappaa syötin.

Microsoftin työntekijäksi tekeytyvä henkilö voi esimerkiksi väittää puhelimessa, että käyttäjän tietokone on saanut virustartunnan. Sähköpostilaatikkoon saattaa tupsahtaa ”verovirastolta” ilmoitus veronpalautuksesta, tai ”kuriiripalvelu” voi ilmoittaa tekstiviestillä lähetyksen saapumisesta vastaanottajalle. Messenger-yhteystiedolta voi tulla varoitusviesti, jonka mukaan vastaanottajasta kiertää verkossa jo tuhansia katsojia kerännyt video – ja niin edelleen.

Kohdennettu kalastelu voi olla paljon hienostuneempaa ja jopa yksittäiselle toimittajalle räätälöityä.

Hakkerit ovat onnistuneet esimerkiksi soluttautumaan internetin valeprofiilien avulla Qatarin ihmisoikeusloukkauksia tutkineiden toimittajien lähipiiriin tai kansalaisjärjestöjen toimintaan. Valeprofiilien taustalla olevat hakkerit pitävät yhteyttä uhriinsa pitkään ennen kuin lähettävät linkin esimerkiksi Google Docs -asiakirjaan, johon uhri pääsee tutustumaan kirjautumalla sisään Google-tililleen. Asiakirjan jakolinkki johtaa verkkosivulle, joka muistuttaa erehdyttävän

paljon Googlen kirjautumissivua, ja uhri syöttää sivulle pahaa aavistamatta sähköpostiosoitteensa ja salasanansa.

Vuoden 2016 Yhdysvaltain presidentinvaalien iltana, kun Trumpin valinta näytti todennäköiseltä, (tiettävästi venäläinen) hakkerijoukko lähetti lukemattomille amerikkalaistoimittajille sähköpostilla asiakirjan. Sen väitettiin sisältävän todistusaineistoa vaalien peukaloinnista. Hakkerit tekeytyivät arvostetun Harvardin yliopiston professoriksi, ja sähköposti näytti tulevan yliopiston palvelimelta.

Tietojen kalasteluyrityksissä uhria johdatellaan yleensä verkkosivulle, jolla hän voi luovuttaa salasanansa hakkereille itse, tai yritetään saada hänet lataamaan vakoiluohjelman saastuttama tiedosto.

Klassisten kalasteluyritysten kolme arkkityyppiä ovat tekaistut viestit, kehotus toimenpiteeseen ja salasanojen metsästys.

Yhteistä kaikille yrityksille on, että niissä käytetään hyväksi pelon, hämmennyksen ja odotuksen kaltaisia tunteita, jotta uhri saataisiin toimimaan toivotulla tavalla.

Hyökkäysten havaitseminen on joskus hyvin hankalaa. Toimittaja ei voi aina sivuuttaa hänelle lähetettyjä viestejä, vaikka ne vaikuttaisivatkin epäilyttäviltä, sillä niissä saattaa piillä varsinaisen jymyjutun siemen.

Onneksi tietojen kalastelua voi torjua parin nyrkkisäännön avulla.

1. TYYPILLISET EPÄILYTTÄVÄT MERKIT

Vaikka kalasteluyritys olisi taidokkaasti toteutettu, jokin yksityiskohta yleensä paljastaa, että jotain on pielessä. Se voi olla esimerkiksi virheellinen internetosoite. Jos kalasteluyrityksen tarkoitus on houkuttaa käyttäjä verkkosivulle, joka muistuttaa erehdyttävästi esimerkiksi Google-tilin, Facebookin tai vastaavan palvelun kirjautumissivua, valesivu on yleensä ulkonäöltään tarkka kopio aidosta sivusta. Yksi asia

kuitenkin on toisin: URL eli verkkoselaimen osoitepalkissa näkyvä verkkosivun osoite. kun esimerkiksi oikean Google-sivun osoite on muotoa google.user.com, valesivun osoite voi olla siitä hieman poiketen vaikkapa user.google.com.

Jos linkin aitous epäilyttää, turvallisinta on aina etsiytyä muuta kautta siihen palveluun, johon viestin vastaanottajan halutaan kirjautuvan.

Jos toimittaja esimerkiksi saa sähköpostiinsa linkin Google Docs -asiakirjaan, hänen ei kannata napsauttaa linkkiä vaan avata verkkoselain erikseen ja kirjautua omalle Google Docs -tililleen Gmailin tai Googlen tavanomaisen kirjautumissivun kautta. Jos lähettäjä todella on jakanut toimittajan kanssa tiedoston Google Docsissa, se avautuu tätä kautta.

Vastaavasti kannattaa toimia silloinkin, jos saa sähköpostitse tai tekstiviestinä esimerkiksi kehotuksen muuttaa Facebook-tilin salasana. Viestiin sisältyvän linkin napsauttamisen sijaan kannattaa kirjautua Facebookiin verkkoselaimen kautta tavalliseen tapaan ja muuttaa salasana palvelussa.

Huijausyrityksestä voi kieliä myös pyyntö ladata jokin ohjelma, jolla voi avata liitetiedoston, ja kielellisten kummallisuuksienkien pitäisi soittaa hälytyskelloja.

2. TIEDOSTOJEN AVAAMINEN PILVESSÄ

Tietojen kalasteluyrityksessä uhrille voidaan lähettää tiedosto, joka kehotetaan avaamaan, ja sen jälkeen tiedosto voi tartuttaa tietokoneelle tai puhelimeen haittaohjelman. Tiedoston avaamisen omalla laitteellaan voi kiertää esimerkiksi pilvipalvelun avulla.

Sähköpostiviestin liitetiedoston voi tallentaa laitteelleen ja ladata edelleen esimerkiksi Google Driveen. Saastuneen tiedoston lataaminen ei sinänsä ole vaarallista, vaan vasta sen avaaminen. Jos tiedosto ladataan Google Driven kaltaiseen pilvipalveluun ja avataan vasta siellä, se avautuu Googlen tietokoneella. Googlella puolestaan on kapasiteettia torjua viruksia ja

haittaohjelmia. Tämän vuoksi esimerkiksi Google Driven avulla voi tarkistaa, onko tiedosto todella se, mikä sen väitetään olevan. Tarkistamisen jälkeen tiedostoa voi halutessaan käyttää omalla tietokoneellaan.

On tietenkin muistettava, että Google saa haltuunsa tiedoston, joka sen pilvipalveluun ladataan.

VINKKI!

Käytä luvussa 9 kuvattua kaksivaiheista vahvistusta aina kun mahdollista. Se suojaa käyttäjätilejä, jos niiden salasanoja päätyy ulkopuolisten haltuun ja tietojen urkkija yrittää kirjautua tileille.

10

11

Operaatioturvallisuutta toimittajille

VINKKI!

Turvallinen viestintä lähteiden kanssa on muutakin kuin digitaalista turvallisuutta. Ennen ryhtymistä yhteistyöhön väärinkäytösten paljastajan kanssa toimittajan on paneuduttava myös mahdollisiin oikeudellisiin seuraamuksiin, joita yhteistyöstä voi seurata lähteelle tai hänelle itselleen. Salassa pidettävän tiedon vuotaminen tiedotusvälineille voi saattaa lähteen tukalaan tilanteeseen. Hän voi joutua irtisanomisen tai oikeustoimien kohteeksi, häntä voidaan painostaa esimerkiksi sulkemalla ulos porukasta tai levittämällä hänestä tietoja julkisuudessa. Toimittajan on varmistettava, että lähde on tietoinen tällaisten seurausten mahdollisuudesta. Toimittajan on myös syytä arvioida kriittisesti lähteen motiiveja – kuten journalistisessa työssä yleensäkin. Kannattaa pohtia, mitä etua lähteelle voi olla jutun julkaisemisesta, ja tarkastaa kaikkien tietojen paikkansapitävyys perin pohjin.

Aiemmissa luvuissa on esitelty monia työkaluja, jotka auttavat suojautumaan meihin kaikkiin kohdistuvalta digitaaliselta joukkovalvonnalta. Jos toimittaja on erikoisalueensa tai jonkin tietyn lähteen tai jutun vuoksi joutunut kohdennetun valvonnan kohteeksi, työn ja lähteiden suojaamiseen tarvitaan perusvälineitä kehittyneempiä välineitä.

Operaatioturvallisuus eli OPTU (englanniksi operational security, OPSEC) on sotilaskielestä lainattu käsite, jolla tarkoitetaan menetelmiä tiedon suojaamiseen viholliselta tietyn operaation yhteydessä.

Ensimmäinen askel journalistisen työn operaatioturvallisuudessa on turvallisuustietoinen ajattelu jo ennen kuin näköpiirissä on erityistä suojautumista vaativa juttu. Muuten turvatoimet muuttavat toimittajan normaalia käyttäytymistä epäilyksiä herättävästi, ja hänen salattu viestintänsä on helppo erottaa muusta viestinnästä.

Seuraavassa annetaan vinkkejä operaatioturvallisuuden varmistamiseen toimittajan työprosessissa.

Yhteydenpito lähteen kanssa

Julkisella GPG-avaimella ja älypuhelimen salauksella pääsee jo pitkälle, sillä silloin lähteet voivat lähettää toimittajalle salattuja sähköposteja ja muita viestejä sekä soittaa hänelle. Toimittajaan yhteyttä ottavat lähteet eivät kuitenkaan usein tiedä mitään salauskeinojen käytöstä.

Taso 1: Työpaikan ulkopuolella

Jos lähteeseen kohdistuvan ensisijaisen uhan muodostaa hänen työnantajansa, riittävä varotoimi voi olla, ettei kontakti päädy työnantajan tietoon. Työnantajalla voi olla pääsy lähteen sähköposteihin, työkoneeseen tai työpuhelimeen, joten hänen on vältettävä niiden käyttöä ja hoidettava yhteydenpitoa toimittajaan työpaikkansa ulkopuolella.

Taso 2: Nimettömyys

Kun on kyse hyvin arkaluonteisista tiedoista, kontaktia ei saa olla mahdollista jäljittää lähteen omaan tietokoneeseen, sähköpostiin tai puhelimeen. Jos lähde haluaa keskustella toimittajan kanssa, häntä voi kehottaa hankkimaan halvan matkapuhelimen, jossa ei ole internetyhteyttä, ja siihen prepaid-SIM-kortin. Jos lähde haluaa lähettää toimittajalle sähköpostia, häntä voi pyytää luomaan anonyymin sähköpostitilin väärällä nimellä ja mielellään sellaiselta tietokoneelta, jota ei voida liittää häneen – esimerkiksi nettikahvilassa tai kirjastossa. On varmistettava, ettei hänen käyttämässään tilassa ole valvontakameroita. Varminta on luoda uusi sähköpostitili jokaista yhteydenpitokertaa varten.

Taso 3: Kirjeposti

Yksi turvallisimmista menetelmistä on pyytää lähdettä lähettämään toimittajalle perinteinen paperikirje. Kirjeen voi osoittaa toimittajan työosoitteeseen tai vielä varmemmin kotiin tai sellaisen luotettavan henkilön osoitteeseen, josta viranomaiset eivät sitä todennäköisesti etsi. Kirje ei saa herättää minkäänlaista erityistä huomiota postissa, joten lähteen on huolehdittava, että tarvittava postimaksu on maksettu, vastaanottajan osoite oikea ja merkitty oikeaan kohtaan selvästi sekä kirjekuori sopivan koruton. Kirjeeseen ei tietenkään saa merkitä lähettäjän tietoja.

Taso 4: Lähteen kanssa kasvotusten

Kasvokkain tapaaminen on aina turvallisin viestintäkeino – silloin digitaalisen valvonnan vaaraa ei ole. Jos lähteellä on toimittajalle tärkeää kerrottavaa, tapaaminen on sovittava paikkaan, jossa voi varmasti puhua rauhassa. Tapaamisesta sopimiseen ei saa käyttää toimittajan tai lähteen työsähköpostia tai -puhelinta, Facebookia tai vastaavaa kanavaa. On ehdottoman välttämätöntä, ettei kenelläkään tapaamisen

FAKTA: FIKSU PYYTÄÄ APUA!

Jos toimittajalla on hallussaan erityistä suojaamista vaativaa arkaluonteista aineistoa, turvallisuusvinkkien opiskelu kirjoista tai nettioppaista ei riitä. Silloin tarvitaan apua todelliselta asiantuntijalta, johon voi luottaa ehdoitta. Tämän kirjan lopussa annetaan vinkkejä siitä, mistä salausasiantuntijoita voi etsiä.

osallistujalla ole mukanaan älypuhelinta tai muita digitaalisia laitteita. Ne on jätettävä kotiin tai työpaikalle virta päällä tai annettava luotettavan henkilön haltuun ja pyydettävä häntä kulkemaan niiden kanssa jonnekin aivan toisaalle. Näin laitteiden käyttäjien todellisia liikkeitä ei voida jäljittää tukiasematietojen avulla. Matkaliput, taksit ynnä muut on maksettava käteisellä, eikä pankki- tai matkakortteja saa käyttää tapaamisen aikana eikä meno- tai paluumatkoilla. Tapaamispaikkaan on kuljettava pysähtelemättä, jotta tapaamisen osanottajien seuraaminen olisi mahdollisimman hankalaa. Lisäksi tapaaminen on sovittava paikkaan, jossa ei ole valvontakameroita, jotta varsinaista tapaamista ei voi seurata. Tapaamisessa on syytä sopia siitä, miten viestinnän turvallisuus vastedes varmistetaan – esimerkiksi luvussa 8 kuvattavia salausvälineitä käyttämällä. Luvussa 4 kuvattavaa uhka-arviointia voi käyttää tarkoituksenmukaisimpien välineiden määrittämiseen, ja tietojen perusteella voi laatia toimittajantyötä koskevan turvallisuussuunnitelman.

Aineiston kerääminen

Lähteen työpaikalta peräisin oleva materiaali voi olla ratkaisevaa jutun uskottavuuden kannalta. Suomen lain mukaan toimittaja ei voi vaatia viranomaislähdettä vuotamaan luottamuksellista aineistoa, koska tällöin toimittaja itsekin voisi syyllistyä salassapitorikoksen yllytykseen. Ilman yllyttämistä toimittaja voi kuitenkin vastaanottaa luottamuksellista aineistoa syyllistymättä rikokseen. Toimittaja voi neuvoa lähdettä suojausasioissa ja aineiston keräämisessä ennen toimittajan juttusille tuloa. Lähteelle on tähdennettävä, että useimmista asioista jää digitaalisia jälkiä. Asiakirjat on kopioitava tai koottava ulkoiselle välineelle, kuten muistitikulle, ilman että tapahtumaa voi jäljittää lähteeseen. Lähde ei esimerkiksi saa olla kirjautuneena sisään tulostimelle tai tietokoneelle,

jolla hän käsittelee aineistoa. Jos lähde ei ole varma siitä, miten voisi välttää jäljittämisen, hän voi ottaa tietokoneensa näytöltä tai asiakirjoista kuvia kameralla, jossa ei ole internetyhteyttä tai joka ei muulla tavoin ole yhdistettynä verkkoon.

Toimitustyön aikana

Työn alkajaisiksi on tehtävä uhka-arviointi ja laadittava turvallisuussuunnitelma luvun 4 mukaisesti.

AINEISTON SÄILYTTÄMINEN

Kun toimittajalle on luovutettu luottamuksellista aineistoa, se on ehdottomasti säilytettävä varmassa tallessa.

Huolimattomuus on yksi suurimmista turvallisuusriskeistä. Toimittaja saattaa esimerkiksi unohtaa junaan puhelimensa, jossa ei ole näppäinlukitus käytössä, jättää tietokoneensa vartioimatta kahvilan pöytään tai antaa asiattomille henkilöille työtehtävien hoitamiseen käyttämänsä tiedostonjakopalvelun käyttöoikeuden.

Tiukimmatkin turvatoimet ovat voimattomia hajamielisyyden, ajattelemattomuuden tai hetkellisen huolimattomuuden edessä. Toimittaja ei koskaan saa jättää tietokonettaan tai puhelintaan hetkeksikään pois silmistään.

Tietokone, puhelin ja ulkoiset levyasemat on syytä salata, jotta muut eivät voi lukea niitä, vaikka laite unohtuisi junaan, tulisi varastetuksi, takavarikoiduksi tai joutuisi muutoin hukkaan. Salauskeinoista kerrotaan luvuissa 6 ja 7.

Yleisimmin hukkaan joutuu puhelin, johon on vieläpä kaikkein helpointa tunkeutua. Siksi älypuhelimesta on muistettava säännöllisesti poistaa tekstiviestejä ja muuta tietoa, jonka paljastuminen voisi vaarantaa lähteen tai jutun. Raskauttavaa tietoa voi olla jo se, että toimittaja on yhteydessä lähteeseen.

Toimittajan on harkittava työtiedostojensa säilyttämistä salatulla ulkoisella kovalevyllä tai muistitikulla tietokoneen sijaan, jos tällaista ulkoista välinettä on helpompi kuljettaa jatkuvasti mukana kuin tietokonetta.

FAKTA: OLAN YLI KURKKIMINEN

Yleinen tapa vaarantaa oma digitaalinen turvallisuutensa on varomattomuus sisäänkirjautumisissa. Olan yli kurkkiminen tarkoittaa sitä, että vastapuoli yksinkertaisesti seuraa, kun käyttäjä kirjautuu salasanallaan tietokoneeseensa, sähköpostiinsa tai puhelimeensa julkisella paikalla. Usein tämä tapahtuu väenpaljouden keskellä vaikkapa kahvilassa tai julkisessa liikennevälineessä. Olan yli voi kurkkia myös etäältä kiikarin avulla. Toimittaja voi suojautua kurkkimiselta varmistamalla, ettei yksikään valvontakamera tai ihminen tarkkaile häntä, kun hän syöttää laitteisiinsa salasanoja tai muuta arkaluonteista tietoa.

Aineistoista on tehtävä salattuja varmuuskopioita, jotka on säilytettävä turvallisessa paikassa. Paikka voi olla esimerkiksi sataprosenttisen luotettavaksi tiedetyn ystävän tai perheenjäsenen koti. Parasta on, jos henkilö suostuu säilyttämään aineistoa tietämättä, mitä se koskee. On tärkeää, ettei säilytyspaikkaa voi heti yhdistää toimittajaan tai hänen työpaikkaansa ja ettei poliisi todennäköisesti tee kyseiseen paikkaan etsintää. Jos aineisto on paperitulosteita tai muuta fyysistä materiaalia, sen voi skannata salatun varmuuskopion tekemistä varten ja pitää alkuperäiskappaleet itsellään.

Jos on olemassa vaara, että aineisto takavarikoidaan tai jutuntekoa muulla tavoin pyritään estämään, aineistosta kannattaa kaiken varalta luonnostella juttu, joka on tarvittaessa nopeasti julkaistavissa.

On muistettava, että lentokenttien turvatarkastuksiin liittyy tavallista suurempi tietokoneiden ja puhelinten tutkimisen riski. Riski on olemassa myös läpikulkumatkoilla ja erityisesti matkustettaessa sellaisten maiden kautta, joiden viranomaiset voivat vaatia toimittajia paljastamaan laitteidensa salasanoja.

Jos toimittajalla on hallussaan erittäin tulenarkaa aineistoa, voi olla hyvä ajatus jakaa sen salattuja varmuuskopioita luotetuille kontakteille eri maissa. Kopiot voi kenties toimittaa perille sellaisen luotettavan kuriirin matkassa, joka matkustaa kyseisellä reitillä säännöllisesti.

TAUSTATYÖ

Toimittajan vastapuoli saattaa saada jutusta vihiä jo sen taustoittamisen yhteydessä. Näin voi käydä esimerkiksi silloin, jos toimittaja pyytää tiedustelupalvelulta kommenttia salaiseen raporttiin, jonka aikoo julkistaa, tai jos hän tutkii yrityksen verkkosivustoa yrityksen toimintaa kritisoivaa skuuppiaan varten. In-

ternethakujen anonymisoinnista on huolehdittava luvussa 8.2 kuvatulla tavalla. Paljastumisriskiä lisääviä yhteydenottoja lähteisiin on viivytettävä, kunnes toimittaja voi olla varma, että kasassa on jotakin, minkä voi julkaista heti yhteydenoton jälkeen.

JULKAISEMINEN

Toimittajan on tietenkin tutkittava tarkoin, sisältyykö julkaistaviin tietoihin lähteiden kannalta raskauttavia seikkoja. Luotettavan juristin on syytä käydä aineisto läpi lähdesuojan kannalta ennen julkaisemista.

Digitaalisen viestinnän tavoin myös tallennettuihin asiakirjoihin ja tiedostoihin liittyy metatietoja. Jos toimittaja vaikkapa julkaisee lähteensä kameralla otetun kuvan tai tämän tietokoneelta peräisin olevan tiedoston digitaalisessa muodossa, lähde voi paljastua. Varmin keino sen välttämiseksi on ottaa kuvakaappauksia sellaisen tietokoneen näytöltä, joka ei ole ollut lähteen käytettävissä.

YHTEYDET KOLLEGOIHIN

Jossakin vaiheessa toimittajan on kerrottava jutustaan kollegoilleen tai päätoimittajalle. On myös tavallista, että juttuja tehdään useiden toimittajien yhteistyönä. Tällöin on tärkeää varmistaa, että jutusta tietää mahdollisimman harva ja että kukin saa vain omalta kannaltaan välttämättömät tiedot.

Toimittajan on yleisestikin vältettävä puhumasta jutuistaan muiden kanssa – myös vapaa-ajalla – ja puhuttava niistä vain, kun se todella on välttämätöntä. Mitä useampi tietää lähteestä ja aiheesta, sitä suurempi on turvallisuusriski. Turvallisuus on juuri niin vahva kuin ketjun heikoin lenkki.

Toimittajan on laadittava turvallisuussuunnitelma luvun 4 mukaisesti. Yhteistyökumppanien tapaamisessa on suosittava kasvokkaisia tapaamisia tai käytettävä luvussa 8 kuvattuja salausvälineitä.

Jos aineistoa on vaihdettava kollegojen kesken eikä tapaamista voida järjestää, aineisto on lähetettävä salatuissa sähköpostiviesteissä tai luovutettava salatuilla muistitikuilla luotettavia välikäsiä käyttäen.

Kolmansien osapuolten tiedostonjakopalvelujen, kuten Dropboxin tai Google Driven, ja verkkoasemien käyttöä on ehdottomasti vältettävä.

VINKKI

Hyvin harvoilla media-alan työpaikoilla on olemassa vakiomenettely arkaluonteisen viestinnän hoitamiseksi tai turvallinen yhteydenottomahdollisuus potentiaalisille lähteille. Toimittajat voivat päinvastoin jopa törmätä työpaikan IT-osaston vastarintaan, jos he haluavat asentaa salausohjelmia tietokoneilleen.

On tärkeää levittää ymmärrystä siitä, että digitaalinen turvallisuus on välttämättömyys kaikissa toimittajien työyhteisöissä. Päätoimittajalle kannattaa ehdottaa yhteisten ohjeistusten laatimista luottamuksellisen tiedon käsittelyä varten ja sen varmistamiseksi, että toimittajat voivat asentaa tarvittavat turvallisuutta edistävät ohjelmat työkoneilleen ja -puhelimiinsa. Tiedotusvälineen verkkosivuilla voidaan myös saattaa tarjolle salattu yhteydenottomahdollisuus. Sivuilla voidaan ilmoittaa esimerkiksi Signal-puhelinnumeroita, tiedotusvälineen tai tiettyjen toimittajien julkiset PGP-avaimet tai avoimen lähdekoodin Secure Drop -järjestelmä, joka on suunniteltu erityisesti ulkopuolelta tulevia yhteydenottoja varten. Siitä on lisätietoja osoitteessa securedrop.org.

KUN JUTTU ON VALMIS

Vaikka juttu on saatu turvallisesti valmiiksi ja julkaistu, asiasta voi edelleen aiheutua merkittävää uhkaa toimittajan lähteelle.

Siksi on tärkeää pyyhkiä pois kaikki jäljet, jotka voisivat johtaa lähteen paljastumiseen. Pelkkä tiedostojen siirtäminen tietokoneen roskakoriin ei poista niitä. Macilla tiedostot on poistettava roskakorista tyhjentämällä se esimerkiksi Finder-valikon kautta. Tällä tavalla poistettujakin tiedostoja on mahdollista palauttaa, ellei tietokone ole kirjoittanut niiden päälle.

Jos aineisto on erittäin tulenarkaa, yksi vaihtoehto siitä eroon hankkiutumiseksi on kovalevyn ja ulkoisten levyjen luotettava tuhoaminen. Esimerkiksi veteen upottaminen tai kovalevyn alustaminen eivät tuhoa dataa. Kovalevyn fyysinen tuhoaminen vasaralla, voimakkaaseen magneettikenttään vieminen ja tietojen päällekirjoittaminen ovat varmimpia keinoja tietojen hävittämiseen.

Raskauttava fyysinen materiaali, kuten paperiasiakirjat, on niin ikään tuhottava sen sijaan, että heittää ne paperinkeräykseen. Paperit voi tuhota esimerkiksi paperisilppurilla tai polttamalla.

Aineisto kannattaa kuitenkin tuhota vasta siinä vaiheessa, kun toimitustyö on päättynyt, juttu julkaistu ja lähde varmasti turvassa.

MUISTISÄÄNTÖ 1: YKSINKERTAINEN ON KAUNISTA

Olipa kyse sitten aineiston kopioinnista, yhteydenpidosta lähteeseen tai yhteistyöstä kollegojen kanssa, helpoin tapa välttää digitaalisen valvonnan riski on tavata kasvotusten tai kopioida aineisto digitaalisia apuvälineitä käyttämättä. Toimittajan haltuunsa saamien fyysisten asiakirjojen turvalliselle säilyttämiselle on tietenkin omat vaatimuksensa.

MUISTISÄÄNTÖ 2: NEED TO KNOW -PERIAATE

Mitä harvempi tietää jutusta, sitä pienempi turvallisuusriski on. Toimittajan on pidettävä tietonsa visusti piilossa, ja tietoa on syytä jakaa vain silloin, kun se on ehdottoman välttämätöntä – ja silloinkin mahdollisimman vähän.

MUISTISÄÄNTÖ 3: JOKAINEN ON OMAN TURVALLISUUTENSA PAHIN UHKA

Useimmat turvallisuuspoikkeamat johtuvat ihmisten huolimattomuudesta eivätkä niinkään siitä, että vastapuoli onnistuisi murtamaan digitaalisen puolustusmuurin. Arkaluonteista juttua työstävä toimittaja ei missään vaiheessa saa löysätä ohjaksia esimerkiksi jättämällä juttuun liittyviä tietoja sisältävää laitettaan vartioimatta tai unohtamalla asiakirjoja jonnekin. Kontrollin on säilyttävä myös sosiaalisessa kanssakäymisessä. Huolestuttavan usein arkaluonteisia tietoja paljastuu huolettoman small talkin tai huonosti peiteltyjen humalaisten vihjausten vuoksi.

11

12

Digitaalinen turvallisuus matkoilla

MUISTA!

Digitaalinen turvallisuus on osa matkan kokonaisturvallisuutta. Laitteiden salaaminen voi estää tietojen paljastumisen tarkastuspisteissä, mutta se ei riitä kovakouraisessa kuulustelutilanteessa, jossa toimittaja pakotetaan luovuttamaan salasanoja ja kontaktien henkilötietoja. Digitaalisesta turvallisuudesta huolehtimalla voidaan minimoida raskauttavan aineiston kuljettaminen mukana tilanteissa, joihin liittyy vakavia uhkia fyysiselle terveydelle. Siksi digitaalinen turvallisuus on otettava osaksi yleistä turvallisuussuunnitelmaa.

Ulkomaille suuntautuvilla juttumatkoilla monet digitaalista turvallisuutta koskevat asiat ovat samoja kuin yleensäkin. Yleisen turvallisuuden lisäksi matkustamiseen liittyy kuitenkin myös erityispiirteitä, jotka on otettava erikseen huomioon. Yksi tärkeimmistä on se, että ulkomailla huolimattomuus voi saattaa toimittajan paikalliset lähteet ja kontaktit erityisen suureen vaaraan.

Tämän luvun ohjeet soveltuvat tarkistuslistaksi digitaalisen turvallisuuden maksimoimiseksi myös ulkomailla.

Uhka-arviointi

Turvallisuussuunnitelman laatiminen matkaa varten edellyttää uhka-arvioinnin tekemistä luvun 4 mukaisesti. Minne matka suuntautuu, mitä halutaan suojata ja keneltä? Digitaalinen turvallisuus tarkoittaa teknisten välineiden lisäksi mahdollisten uhkien arviointia tilannekohtaisesti ja suunnitelman laatimista niiden torjumiseksi.

Toimittajan on mietittävä, mitä uhkia voi kohdistua suojeltavaan omaisuuteen. Keitä voisi kiinnostaa saada tietoja haltuunsa pakottamalla? Millaiset voimavarat näillä toimijoilla on käytettävissään?

Jos toimittajan lähde tai juttu kritisoi matkan kohdemaan valtaapitäviä, uhka on ilmeinen. Hyökkäyksiä voivat kuitenkin tehdä muutkin kuin hyvin resursoidut hallintokoneistot. Vastapuolia kohdemaassa voivat olla myös hakkerit, kilpailevat tiedotusvälineet sekä kritiikin kohteeksi joutuvat yritykset tai poliittiset ryhmittymät, jotka vastustavat toimittajan näkökulmaa. Eri vastapuolilla on erilaisia toimintamahdollisuuksia ja hyökkäysmenetelmiä. Hallintoviranomainen saattaa asettaa toimittajan laitteen huipputekniseen valvontaan, kun taas vihamielinen poliittinen ryhmittymä ehkä ennemmin murtautuu hänen hotellihuoneeseensa ja varastaa tietokoneen. On arvioitava tarkkaan, mistä kaikkialta uhkia voi olla odotettavissa ja millaisia keinoja hyökkääjillä voi olla käytettävissään.

Turvallisuussuunnitelman on aina perustuttava matkan kohdemaan tilanteeseen. Joidenkin maiden lainsäädäntö antaa viranomaisille oikeuden vaatia pääsyä salattuihin laitteisiin jopa usean vuoden vankeusrangaistuksen uhalla. Joissakin maissa puolestaan on tapana hyökätä kriittisten toimittajien kimppuun. Tämän kaltaisia asioita on syytä pohtia osana matkustusturvallisuutta.

Joskus paras ratkaisu voi olla antaa vastustelematta paikallisten viranomaisten tutkia laitteet. Tämä on turvallisinta, kun laitteilla ei ole raskauttavaa aineistoa tai epäilyttäviä salausohjelmia. Toisinaan taas on pyrittävä suojelemaan laitteita kaikin mahdollisin keinoin, jotta ne eivät päädy muiden käsiin.

Seuraavat seikat on selvitettävä ennen matkalle lähtöä:

- Miten kohdemaassa kohdellaan toimittajia ja lähteitä?
- Estetäänkö siellä verkkosivustojen, sovellusten tai muun sellaisen tekniikan käyttöä, jota on tarkoitus hyödyntää matkalla? Onko toimittajan laitteilla ohjelmia tai sovelluksia, jotka voivat kiinnittää epätoivottua huomiota, jos paikallisviranomaiset havaitsevat ne?
- Millaiset oikeudelliset olot maassa vallitsevat? Onko viranomaisilla esimerkiksi oikeus vaatia toimittajaa paljastamaan salattujen tiedostojensa salasanoja? Eri maiden digitaalisesta turvallisuudesta saa luotettavaa tietoa esimerkiksi kansalaisoikeusjärjestö Freedom Housen vuotuisista maaraporteista tai Committee to Protect Journalists -järjestön maakatsauksista.

Ennen matkaa

Digitaalisesta turvallisuudesta on laadittava suunnitelma jo taustoitusvaiheessa. Niin voidaan välttää viime hetken improvisointi, joka saattaa vaarantaa toimittajan työn ja kontaktit. Suunnitelman täytyy sisältää kerätyn aineiston turvallisen säilyttämisen menetelmät matkalla sekä viestintätavat kontaktien kanssa

niin kohdemaassa kuin kotimaassakin. Säilytysmenetelmät ja viestintätavat on testattava ennen matkalle lähtöä niiden toimivuuden varmistamiseksi.

Turvallisuussuunnitelman on oltava kaikkien osapuolten kannalta toteuttamiskelpoinen, jotta kukaan ei mukavuudenhalusta laiminlyö määriteltyjä toimintatapoja. Toimittajan turvallisuus on vain yhtä hyvä kuin ketjun heikoin lenkki. Jos matkaseurana on free-kuvaajia tai kollegoja muista tiedotusvälineistä, on varmistettava, että kaikki tuntevat riskit ja toimintatavat ja ovat yhtä mieltä siitä, miten digitaalisesta turvallisuudesta huolehditaan.

Laitteiden valmisteleminen matkaa varten

Kannettavalla tietokoneella, älypuhelimessa, kamerassa, nauhurissa ja toimittajan muiden työvälineiden muistissa on valtavasti tietoa, johon mahdolliset vastapuolet voivat pyrkiä pääsemään käsiksi. Olennainen osa matkan turvallisuuden suunnittelua on näiden laitteiden valmisteleminen matkustuskuntoon.

LAITTEIDEN VALITSEMINEN

Ensin on valittava matkalle mukaan otettavat laitteet. Mukanaan ei kannata kuljettaa muita kuin tehtävän hoitamisen kannalta välttämättömiä laitteita ja aineistoja. Mahdollisuuksien mukaan matkalla on syytä käyttää eri tietokonetta ja puhelinta kuin muulloin. Niin voi välttää henkilökohtaisten ja muihin työtehtäviin liittyvien tietojen menettämisen matkalla.

LAITTEIDEN SALAAMINEN

Ratkaisevan tärkeä digitaalisen turvallisuuden osa on laitteiden massamuistin salaaminen ennen matkalle lähtemistä. Salata voi myös ulkoiset asemat, kuten muistitikut ja ulkoiset kovalevyt, sekä erityisen arkaluonteiset tiedostot ja kansiot, jotta ne ovat turvassa.

Laitteiden, tiedostojen ja kansioiden salaamisesta kerrotaan luvussa 6.

Valitettavasti kamerassa tai nauhurissa käytettäviä muistikortteja ei voi salata. Siksi tiedostot on kuvaamisen tai nauhoittamisen jälkeen aina siirrettävä muistikortilta salattuun tallennuskohteeseen ja alustettava muistikortti.

HYVÄT TURVALLISUUSKÄYTÄNNÖT

Puhelimeen ja tietokoneelle on oltava asennettuna kaikki saatavilla olevat päivitykset niiden suojaamiseksi viruksilta ja haittaohjelmilta. Tästä kerrotaan luvussa 6.7.

VARMUUSKOPIOINTI

Ennen matkaa on kopioitava kaikkien laitteiden sisältämät tiedot ja sijoitettava kopiot varmaan talteen. Turvallisin säilytyspaikka on salattu ulkoinen kovalevy. Näin voidaan estää tietojen häviäminen, jos laite katoaa tai siihen tunkeudutaan matkalla. Salatun varmuuskopion tekemisestä kerrotaan luvussa 6.

YLIMÄÄRÄISEN TIEDON SIIVOAMINEN

Matkalla saattaa menettää kaiken, mitä kuljettaa mukanaan. Sitä varten on käytävä läpi kaikki tietokoneella olevat tiedostot, sähköpostitilillä olevat viestit, puhelimen kuvat ja yhteystiedot ja niin edelleen.

Osa tiedoista on työtiedostoja, yhteystietoluetteloja, kuvia, haastattelumuistiinpanoja ja vastaavia, osa taas vähemmän selkeitä tietoja, kuten paikannustietoja laitteen käyttäjän eri sijaintipaikoista, verkkoselaimen hakuhistoriatietoja ja laitteille tallennettuja sähköpostien ja sosiaalisen median palvelujen kirjautumistietoja. Jos joukossa on tietoja, joita ei voi päästää viranomaisten ja muiden vastapuolten haltuun, niistä on otettava kotiin jäävä varmuuskopio ja poistettava ne tietokoneelta tai puhelimesta.

Erityisen tärkeää on toimia näin, jos laitteilla oleva

tieto voi vääriin käsiin joutuessaan saattaa toimittajan lähteitä tai kontakteja vaaraan. Tällaisia tietoja voivat olla esimerkiksi yhteystiedot, toimittajan kanssa jaetut tiedot, lähteiltä saadut kuvat ja heidän kanssaan sähköpostitse, tekstiviestinä tai chatissa käyty viestinvaihto sekä puheluhistoria.

Kotimaassa täysin mielenkiinnottomilta vaikuttavat asiat voivat jossakin muualla olla hyvinkin arvokkaita. Jos toimittajalla on hallussaan vaikkapa luettelo palestiinalaisista kontakteista, siitä voi Israeliin matkustettaessa tulla varsin arkaluonteinen – ja päinvastoin.

OHJELMIEN ASENTAMINEN

Matkalla käytettävät ohjelmat ja sovellukset on saatettava käyttökuntoon ennen lähtöä.

Käyttäjätilien valmisteleminen matkaa varten

Sähköpostiosoite toimii avaimena moniin verkkopalveluihin. Jos vastapuoli saa käsiinsä toimittajan sähköpostitilin, sen avulla on mahdollista palauttaa salasanoja ja saada pääsy muihin toimittajan käyttämiin palveluihin. Sen vuoksi on huolehdittava sähköpostitilin suojaamisesta vahvalla salasanalla luvussa 7 kuvatun mukaisesti.

KAKSIVAIHEINEN VAHVISTUS

Matkan aikana tarvittavilla käyttäjätileillä on syytä käyttää kaksivaiheista vahvistusta tärkeän lisäturvan saamiseksi. Siitä kerrotaan luvussa 9.

Jos laitteita häviää matkalla, sisältöä voi hävitä myös niistä palveluista, joihin toimittaja on kirjautuneena sisään. Sen vuoksi kannattaa harkita uloskirjautumista sähköpostitililtä, Facebookista ja muista verkkopalveluista ennen matkaa.

MATKATILIT

Voi olla hyvä idea perustaa matkakohtainen sähköpostitili, jotta matkalla tapahtuva viestintä pysyy täysin erillään muusta päivittäisestä viestinnästä. Sähköpostipalvelua on voitava käyttää verkkoselaimella salatussa https-yhteydessä. Esimerkiksi Googlen Gmail toimii näin. Turvallisen https-yhteyden tunnistaa vihreästä riippulukosta selaimen osoiterivillä. Tarpeen mukaan kannattaa luoda myös uudet ”matkatilit” sellaisiin palveluihin kuin AppleID ja Google Drive, jos haluaa käyttää näitä palveluita. Näin voi matkalla välttää ulkopuolisten pääsyn vanhoihin sähköposteihinsa, kuviinsa, yksityisiin tiedostoihinsa tai asetuksiinsa.

JULKISET TIEDOT

Ennen matkaa toimittajan on käytävä läpi tiedot, joita hänestä itsestään on avoimesti saatavana verkossa. Aiemmat työpaikat, julkiset asuinpaikkatiedot ja sosiaalisen median rajapinnat voivat kohdistaa toimittajaan epätoivottua huomiota, jos paikalliset viranomaiset tarkastavat hänen taustojaan. Näin voi käydä esimerkiksi viisumia haettaessa, rajatarkastuksessa tai jossakin muussa yhteydessä.

Jos toimittajan työstämä aihe on arkaluonteinen, siitä ei saa sanoa mitään sosiaalisessa mediassa. Henkilöitä, paikkoja ja aiheita koskevia tietoja voidaan kaivaa esiin ja käyttää toimittajaa ja muita henkilöitä vastaan. Maahantulon yhteydessä viranomaiset voivat etsiä toimittajan somesta, lähteelle voi aiheutua ongelmia suomalaisen toimittajan tapaamisesta paikallisessa kahvilassa, matkan jälkeen vastapuoli voi yrittää selvittää toimittajan lähteitä ja niin edelleen.

Matkan aikana

LAITTEIDEN VARTIOIMINEN

Varkausriskin lisäksi on olemassa tietojen kopioimisen vaara tietokoneelta tai puhelimesta, jos toimittaja ei ole jatkuvasti varuillaan. Laitteelle voidaan myös asentaa valvontaohjelmia ja sovelluksia tai muuttaa laitetta niin, että sen jäljittäminen helpottuu tai sillä annettuja näppäinkomentoja voidaan seurata.

Sen vuoksi tietokone, puhelin ja vastaavat laitteet on pidettävä aina mukana. On vältettävä niiden säilyttämistä hotellien kassakaapeissa, sillä ne saa yleensä avattua yleisavaimella. Jos laitteesta on luovuttava hetkeksi, se on ehdottomasti suljettava kokonaan, jotta massamuistin suojaus tuo sille suojaa.

Julkisilla paikoilla on varmistettava, ettei kukaan kurki olan yli, kun laitteeseen syötetään salasanoja tai PIN-koodeja. Laitteen näppäimistö tai puhelimen näyttö on peitettävä lukituksen avaamisen ajaksi.

VIERAIDEN LAITTEIDEN VAARAT

Kun käytetään muiden hallitsemia laitteita ja verkkoja, on noudatettava erityisen suurta varovaisuutta. Hotellien ja nettikahviloiden USB-latauspisteissä saattaa olla laite, joka lukee tietoja kaapelin kautta lataamisen aikana. Sen vuoksi matkoilla saa käyttää ainoastaan omia latureita, johtoja ja kaapeleita.

Lahjaksi saatuja muistitikkuja tai -kortteja ei pidä käyttää, sillä niistä voi saada kaupan päälle viruksen tai haittaohjelman. Jos matkalla tarvitaan lisää tallennustilaa, on ostettava uusia, käyttämättömiä tallennusvälineitä.

Käyttäjätileille ei koskaan saa kirjautua kahvilan tai hotellin tietokoneelta, sillä niissä saattaa olla vakoiluohjelmistoja, jotka tallentavat syötetyt käyttäjätunnukset.

VIERAIDEN VERKKOJEN VAARAT

Kun laite yhdistetään langattoman verkon hotspotiin, verkon järjestelmänhaltija voi tallentaa ja valvoa verkossa tapahtuvaa toimintaa. Perusoletuksena kannattaa varautua siihen, että langatonta verkkoa valvotaan jotenkin. Erityisen riskialttiita ovat lentokenttien langattomat verkot ja julkiset hotspotit, joissa vaaditaan erillistä salasanasuojattua kirjautumista. Tietoliikenteen valvomisen langattomassa verkkoyhteydessä voi estää käyttämällä VPN-yhteyttä.

Puhelimen langattomien yhteyksien eli GPS:n, WiFin ja Bluetoothin kanssa on oltava varovainen, sillä langattomien yhteyksien ollessa käytössä puhelin pyrkii luomaan yhteyden muihin puhelimiin. Tämä voi jättää jälkiä siitä, mitä toimittaja on tehnyt verkossa. GPS, WiFi ja Bluetooth onkin järkevää kytkeä pois päältä, kun niitä ei tarvita. Puhelimen voi myös kytkeä lentotilaan, jos haluaa estää paikallista teleoperaattoria seuraamasta sen sijaintia.

RAJALLA

Kun toimittaja matkustaa maasta toiseen tai kulkee tarkastuspisteen läpi, hänen on oltava varautunut siihen, että kaikki laitteet ja niillä olevat tiedot voidaan tutkia tai takavarikoida tai niihin voidaan asentaa seuranta- tai haittaohjelmia.

Lentokenttien turvatarkastuksiin liittyy tavallista suurempi tietokoneiden ja puhelinten tutkimisen riski myös läpikulkumatkoilla.

Jos poliisi saa matkakohteessa vaatia toimittajaa paljastamaan salasanojaan, kyseistä lainsäädäntöä on noudatettava. The Guardian -lehdelle paljastuksia tehneen Snowden-toimittaja Glenn Greenwaldin brasilialainen kumppani David Miranda sai kokea tämän, kun brittiviranomaiset pitivät häntä tuntikausia kiinniotettuna Heathrow'n lentokentällä ja puristivat hänestä ulos lukuisia salasanoja.

Paras tapa suojata tietoja tämän tyyppisessä tilanteessa on olla pitämättä niitä mukanaan. Matkalle ei pidä ottaa mukaan tarpeetonta tietoa. Jos mahdollista, matkalla kerättyjä tietoja on hyvä lähettää säännöllisesti kotimaahan ennen kotiinpaluuta.

ETSINNÄT JA TARKASTUKSET

Toimittajan on pidettävä mukanaan olevia laitteita jatkuvasti silmällä. Niitä kannattaa kuljettaa ennemmin käsimatkatavaroissa kuin ruumaan menevässä matkalaukussa. Jos laite tutkitaan rajatarkastuksessa, siihen saatetaan asentaa haittaohjelmia, jos se on hetkenkin näkymättömissä. Jo muutama minuutti poissa omistajan silmistä riittää siihen, että rajavartija siirtää muistitikulta tietokoneeseen tai puhelimeen haittaohjelman.

Koko levyn suojaus suojaa laitteiden ja tallennusvälineiden tietoja kopioinnilta ja muuttamiselta silloin, kun ne ovat kokonaan pois päältä. Tämä on vahva tekninen keino tietojen suojaamiseen.

Viranomaiset voivat kuitenkin vaatia toimittajaa avaamaan laitteiden lukituksen. Vaatimuksen vastustaminen ei aina ole turvallista. Maan ja tilanteen mukaan tietojen luovuttamisesta kieltäytyminen voi johtaa erilaisiin rangaistuksiin.

Toimittajilta on esimerkiksi evätty maahanpääsy tai takavarikoitu tietokoneita ja kovalevyjä, jos he ovat kieltäytyneet luovuttamasta pääsyä salattuun aineistoon.

Kaikki tietokoneella, puhelimella ja tallennusvälineillä olevat salaamattomat tiedot voidaan kopioida, kun fyysinen pääsy laitteeseen on saatu. Laitteilla olevia tietoja on myös mahdollista muuttaa tai poistaa, ja tietokoneelle tai puhelimeen voidaan asentaa valvonta- ja haittaohjelmia.

Vaikka puhelimen sisältö olisi suojattu koko levyn salauksella, puhelimelta ja sim-kortilta voi yhä lukea tietoja, joiden avulla esimerkiksi televerkon käyttöä

matkalla voidaan tarkkailla. Tämä riski on olemassa, jos puhelin tutkitaan vaikkapa maahantulon yhteydessä. Ylimääräisten ohjelmien aiheuttamien haittojen välttämiseksi toimittaja voi kohdemaahan saavuttuaan ostaa uuden puhelimen, jossa on prepaid-liittymä.

TAPAAMISET LÄHTEIDEN KANSSA

Toimittajan ei koskaan pidä kertoa lähteistään tai tapaamisistaan heidän kanssaan kenellekään, jonka ei tarvitse tietää asiasta. Ainoastaan välttämättömät tiedot kannattaa jakaa ja nekin pelkästään ihmisten kanssa, joihin voi vuorenvarmasti luottaa.

On muistettava, että toimittajan, lähteen ja muiden läsnäolijoiden puhelinten telepaikannustiedoista voi käydä ilmi, että he ovat tai ovat olleet samassa paikassa. Tämä voi olla riskialtista esimerkiksi lähteille, joita paikallinen hallinto saattaa pyrkiä painostamaan, sillä viranomaisilla voi olla pääsy teleyhtiöiden lokitietoihin.

Jos tällainen riski on mahdollinen, toimittajan on kytkettävä puhelimensa lentotilaan tai mieluiten kokonaan pois päältä ennen ovesta ulos astumista. Lähteen ja muiden paikalle tulijoiden on toimittava samoin. Tämä suojaa tukiasematietoihin perustuvalta paikannukselta. Jos yhteenkin puhelimeen on asennettu liikkeitä valvova haittaohjelma, puhelimen sulkeminen ei riitä. Tällöin valvonnan voi välttää ainoastaan jättämällä puhelimet luotettavan henkilön haltuun ennen tapaamista. Tapaamisen valvonnan riski on asetettava vaakakuppiin sen riskin kanssa, että kukin luopuu laitteistaan pystymättä pitämään niitä koko ajan silmällä.

Viestintä matkan aikana

Ennen matkaa toimittajan on suunniteltava, miten viestii matkakohteessa ja kotimaassa olevien kontaktiensa kanssa. On muistettava, että tele- ja internetoperaattorit rekisteröivät digitaalisia jälkiä, jotka viranomaiset voivat saada käyttöönsä. Erityisesti tämä

pätee puhelinten sijaintipaikasta kertoviin tukiasematietoihin sekä toimittajan viestintäkumppaneita ja verkkosivuvierailuja koskeviin tietoihin.

Kontaktien kanssa viestimiseen voi käyttää salaussovelluksia. Esimerkiksi WhatsApp- ja Signal-sovelluksilla välitettävät viestit ja puhelut ovat salattuja. Joka tilanteeseen on valittava tarkoituksenmukaisin sovellus.

Signal on turvallisempi kuin WhatsApp, sillä se tallentaa vähemmän metatietoja. Joissakin maissa kuitenkin jo pelkästään Signalin asentaminen puhelimeen voi olla riittävä syy joutua viranomaisten huomion kohteeksi, kun taas melko yleisesti käytetty WhatsApp ei juuri herätä huomiota.

Luvussa 8 kerrotaan lisää Signalin ja muiden salatun viestimisen apuvälineiden eduista ja haitoista.

TIETOJEN LÄHETTÄMINEN KOTIIN

Arkaluonteisen aineiston kuljettaminen mukana matkalla voi olla kuormittavaa varsinkin, jos kiinniotetuksi ja kuulustelluksi joutumisen uhka on olemassa. Toimittajan kannattaa lähettää materiaalia kotiin aina, kun käytössä on internetyhteys, ja poistaa materiaali sen jälkeen laitteiltaan. Tietojen salaamisesta voi huolehtia esimerkiksi käyttämällä salattua sähköpostia tai salaamalla lähetettävät tiedostot.

Tietoja voi myös ladata Dropboxin tai Google Driven kaltaisiin pilvipalveluihin. Jos tietoja tallennetaan pilveen, ne on muistettava salata ensin. On hyvä sopia jonkun kotimaassa olevan kanssa, että hän lataa tiedostot pilvestä saman tien itselleen. Näin ne eivät häviä, jos joku ulkopuolinen pääsee käsiksi käyttäjätiliin ja poistaa tiedostot.

PAIKALLISEN SENSUURIN KIERTÄMINEN

Joissakin maissa estetään pääsy tietyille verkkosivustoille tai sosiaalisen median palveluihin. Eston voi kiertää VPN-yhteyden avulla, kunhan sen tarjoaja on luotettava toimija. Jos toimittajan työnantaja tarjoaa käyttöön VPN-yhteyden, sitä ei välttämättä voi käyttää. Yksi vaihtoehto kaupallisten VPN-palvelujen joukossa on Freedome. Kaupallisia VPN-palveluja turvallisempi vaihtoehto on anonyymi verkkoselain Tor. VPN:stä ja Torista kerrotaan luvussa 9.

Matkan jälkeen

SALASANOJEN VAIHTAMINEN

Kotiin palattua kannattaa varmuuden vuoksi vaihtaa kaikkien laitteiden ja palvelujen salasanat sähköpostista ja sosiaalisen median palveluista Apple ID:hen ja vastaaviin.

TURVALLISUUDEN YLLÄPITÄMINEN

Lähteet voivat olla vaarassa myös sen jälkeen, kun toimittaja on palannut turvallisesti kotiin. He jatkavat elämäänsä sortohallinnon alaisuudessa. Toimittajaan voi kohdistua hakkeroimisen vaara myös kotiinpaluun jälkeen. Sen vuoksi on jatkettava turvatoimia, jotka suojaavat lähteiden henkilöllisyyttä ja kuvamateriaalia. Aineistoa ei saa säilyttää salaamattomana, ja tietojen julkistamista verkossa ja sosiaalisessa mediassa on harkittava tarkoin. On muistettava, että kuviin ja asiakirjoihin voi sisältyä myös paljastavia metatietoja. Minkä tahansa maan hallinto voi seurata myös Suomessa julkaistavia juttuja.

”SAASTUNEET” LAITTEET

Jos tietokone tai puhelin on ollut poissa toimittajan silmistä matkan aikana, sen turvallisuudesta ei enää ole varmuutta. Siihen saattaa olla asennettu haittaohjelma, jolla voi valvoa toimittajaa tai napata salasanoja ja käyttäjätilien tietoja, kun hän kirjautuu sähköpostiin tai sosiaalisen median palveluihin.

Sen vuoksi laitetta ei saa käyttää ennen sen uudelleen asentamista. Laite on avattava yhdistämättä sitä internetiin ja kopioitava tarpeelliset tiedostot ulkoiselle välineelle. Sitten tietokone on asennettava uudelleen tai puhelimen tehdasasetukset palautettava. Sen jälkeen tärkeät tiedostot voi siirtää takaisin laitteelle, mutta on huomattava, että niissä voi pahimmassa tapauksessa piillä haittaohjelma.

Jos toimittajan vastapuoli on tiedustelupalvelu tai muu hyvin toimintakykyinen koneisto, edellä kuvattu menettely ei välttämättä riitä haittaohjelmien poistamiseen. Tällöin ainoa mahdollisuus on tietokoneen tai puhelimen hävittäminen.

MUISTA!

Toimittajan laitteilla olevat ohjelmat ja sovellukset voivat kiinnittää häneen epätoivottua huomiota, jos paikalliset viranomaiset havaitsevat ne. Näin voi käydä esimerkiksi silloin, jos käytössä ei ole massamuistin suojausta tai jos toimittaja pakotetaan avaamaan laitteidensa lukitus ja salaus.

Varsinkin Tor-sovellus voi herättää kielteistä huomiota, sillä tämä toisinajattelijoidenkin suosima selain on viranomaisten erityisen mielenkiinnon kohteena monissa maissa. Paras vaihtoehto voi olla poistaa Tor tietokoneelta ennen matkaa ja turvautua sen sijaan VPN-yhteyteen, jonka käyttötarkoituksiin lukeutuu myös sellainen harmiton toiminta kuin Netflixin ja Spotifyn käyttö.

Joidenkin ohjelmien käyttö on kokonaan estetty tietyissä maissa, ja silloin takataskussa on hyvä olla toimivia vaihtoehtoja.

13

Mitä sanoo laki?

Juridisessa mielessä valvonnasta ja lähdesuojasta käytävä keskustelu sijoittuu yksilönvapauksien ja turvallisuuden väliseen jännitteiseen kenttään.

Jokaisella Suomen kansalaisella on perustuslain turvaama sananvapaus ja oikeus yksityiselämän suojaan. Perustuslain 10. pykälässä ja Euroopan ihmisoikeussopimuksen 8 artiklassa todetaan, että kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Viranomaiset eivät voi ilman laillista perustetta tai rikosepäilyä valvoa kansalaisten posti-, tele- tai muuta viestintää.

Euroopan ihmisoikeussopimuksen 8 artikla toteaa näin:
Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta
1. *Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.*
2. *Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.*

Tämän vuoksi viestinnän valvontaan tai kuunteluun tarvitaan yleensä tuomioistuimen lupa.

Kansalaisten vapauksia on kuitenkin rajoitettu vuonna 2001 tehtyjen terrori-iskujen jälkeen. Lisätietoja aiheesta on luvussa 3.

Laki ei anna toimittajille tai tiedotusvälineille lähdesuojaa lukuun ottamatta erityistä suojaa puhelinten, sähköisen viestinnän tai muun viestiliikenteen valvonnalta, jota poliisi- ja tiedusteluviranomaiset voivat harjoittaa. Siksi toimittajien on tiedettävä, miten suojata itseään ja lähteitään valvonnalta.

UUSI TIEDUSTELULAKI LISÄÄ VIRANOMAISTEN OIKEUKSIA

Kiireellisesti säädettävä Suomen tiedustelulaki rajoittaa kansalaisten oikeuksia kansallisen turvallisuuden nimissä. Lain myötä suojelupoliisi ja puolustusvoimat voivat seuloa Suomesta lähteviä ja Suomeen saapuvia sähköpostiviestejä, jos kansallinen turvallisuus on uhattuna. Tällaisen uhkan voisi muodostaa esimerkiksi terrorismi, väkivaltainen radikalisoituminen tai joukkotuhoaseisiin tai kansainvälisen rauhan ja turvallisuuden vaarantamiseen liittyvä muu toiminta. Siviilitiedustelua voidaan tehdä myös, jos yhteiskuntajärjestystä uhkaa kansainvälinen rikollisuus.

Keinovalikoimaan kuuluvat muun muassa puheluiden kuuntelu, ja matkapuhelinten sijaintitietojen tarkkailu, peitetoimet ja valeostot. Viranomaiset voivat pysäyttää kirjeen tai muun lähetyksen postiin ja jäljentää sen esimerkiksi valokuvaamalla. Uusien lakien mukaan tiedustelumenetelmiä voidaan käyttää myös silloin, kun taustahenkilö tai -taho ei vielä varsinaisesti ole tiedossa.

Tiedustelulakipaketin säätäminen edellytti perustuslain 10. pykälän muuttamista. Eduskunta äänesti lokakuussa 2018, että perustuslakia voidaan muuttaa kiireellisesti. Näin ollen perustuslain muutokseen ei tarvita vuoden 2019 eduskuntavaalien jälkeisen eduskunnan hyväksyntää vaan muutos katsottiin äänestyksen jälkeen hyväksytyksi.

Hallitus esitti perustuslain 10. pykälään kahdentoista sanan lisäystä. Laissa luki aiemmin, että lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Muutosesitys lisäsi tämän jatkoksi: ”... sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”. Lisäksi

rikosten tutkinta muutettiin säännöksessä rikosten torjunnaksi.

Perustuslain muutos mahdollistaa koko muun tiedustelulakipaketin täysimittaisen säätämisen ja voimaansaattamisen ennen seuraavia vaaleja.

ONKO SALAAMINEN LAILLISTA?

Suomessa viestinnän salaaminen on sallittua, ja kaikki tässä kirjassa esitellyt välineet ovat täysin laillisia. Esimerkiksi Isosta-Britanniasta ja Ranskasta poiketen Suomen viranomaiset eivät myöskään voi vaatia salatun materiaalin salasanojen luovuttamista.

Salatun tiedon luovuttaminen tai välittäminen edelleen voi toki silti olla laitonta.

Lähdesuojan takaaminen on erityisen tärkeää silloin, kun viestitään lakisääteistä salassapitovelvollisuuttaan rikkovien työntekijöiden kanssa, jotka luovuttavat tiedotusvälineille yhteiskunnallisesti merkittäviä tietoja.

Siksi väärinkäytösten paljastajien ja heidän luovuttamiaan tietoja julkaisevien toimittajien on syytä tuntea seuraavat oikeudelliset perusasiat.

SANANVAPAUS VASTAAN SALASSAPITOVELVOLLISUUS

Sananvapaus on kirjattu Suomen perustuslain 12. pykälään ja Euroopan ihmisoikeussopimuksen 10 artiklaan.

Ilmaisunvapautta voidaan rajoittaa salassapitovelvollisuudella työsuhteen tai viran perusteella. Yleensä rajoitukset koskevat työn kautta tietoon tulleita seikkoja, jotka eivät kuulu ulkopuolisille. Tällaiset tiedot ovat salassapidettäviä.

Virkamiehet ja julkisyhteisön työntekijät voivat saada salassapitovelvollisuutensa rikkomisesta ankaramman vankeusrangaistuksen kuin muut henkilöt. Heidät voidaan myös rikoslain nojalla panna viralta.

Virkamiehelläkin on sananvapaus, jonka turvin hänellä on oikeus ilmaista toimialaansa liittyviä kanto-

jaan ja mielipiteitään melko laajasti. Vastaan tulee kuitenkin helposti salassapitovelvollisuuden lisäksi lakisääteinen lojaliteettivelvollisuus työnantajaa kohtaan.

Tämä korostaa sen välttämättömyyttä, että toimittajien on pyrittävä suojaamaan lähteitään paljastumiselta, jos nämä eivät halua tulla julkisuuteen omalla nimellään.

Salassapitovelvollisuus koskee erityisesti seuraavia osa-alueita:

Yksityishenkilöiden yksityiselämä. Arkaluonteisia henkilötietoja ovat muun muassa ihmisen terveyteen, seksuaaliseen suuntautumiseen, sosiaalisiin ongelmiin ja henkilökohtaiseen taloustilanteeseen liittyvät tiedot sekä henkilötunnus. Henkilötietojen luovuttamiseen tarvitaan suostumus henkilöltä itseltään.

Valtion turvallisuus. Salassapitovelvollisuus koskee tietoja, joiden suojelun perusteena on valtion turvallisuus tai valtakunnan puolustus. Sotasalaisuudet ovat tietoja, joiden katsotaan voivan aiheuttaa haittaa valtion puolustukselle, jos niitä luovutetaan ulkovallalle tai muussa vihamielisessä tarkoituksessa. Kyseeseen tulevat tiedot esimerkiksi pian alkavista, käynnissä olevista ja tulevista operaatioista.

Ulkopoliittiset olot. Salassapitovelvollisuus koskee tietoja, jotka on pidettävä salassa EU:n oikeussääntöjen tai muiden kansainvälisestä oikeudesta johtuvien velvoitteiden perusteella. Se pätee myös tilanteisiin, joissa arvioidaan, että luottamuksellisuus on välttämätöntä olennaisten ulkopoliittisten intressien suojelemiseksi suhteessa muihin maihin tai YK:n, NATO:n ja EU:n kaltaisiin kansainvälisiin organisaatioihin.

MILLOIN SALASSAPITOVELVOLLISUUDEN VOI RIKKOA?

Joskus salassapitovelvollisuutta käytetään yleisen edun kannalta merkittävien tietojen pimittämiseen.

Salassapitovelvollisuuden rikkominen voi olla moraalisesti oikeutettua, kun kyseessä ovat tiedot,

joilla on suurta yhteiskunnallista merkitystä. Usein lähteelle on eduksi, jos hän on pyrkinyt ilmoittamaan ongelmasta jo sisäisesti ennen salassapitovelvollisuutensa rikkomista.

Julkisen sanan neuvosto otti elokuussa 2018 kantaa siihen, voiko journalisti rikkoa lakia sananvapauden nimissä tai julkaista tietoja salaisiksi määritellyistä asiakirjoista. JSN totesi, että journalistin tulee työssään noudattaa Journalistin ohjeita ja lakeja.

Kannanotossa kuitenkin todettiin myös, että poikkeustapauksissa yleisön tiedonsaantioikeuden varmistaminen saattaa edellyttää journalistilta toimintaa, joka voi olla tulkittavissa lainvastaiseksi. Tämä voi tulla kyseeseen erityisesti kahdessa tilanteessa: joko lähdesuojan turvaamiseksi poikkeustilanteissa tai kun kyse on yhteiskunnallisesti merkittävän tiedon julkaisemisesta. JSN:n mukaan historiassamme on paljon esimerkkejä tilanteista, joissa sananvapautta on käytetty vallitsevien lakien vastaisesti mutta niin, että sitä on jälkikäteen pidetty oikeutettuna.

MITÄ TIEDOTUSVÄLINEISSÄ SAA KERTOA?

Suomessa tiedotusvälineet saavat yleensä vapaasti julkaista tietoja riippumatta siitä, ovatko ne peräisin omalla nimellään vai nimettömänä esiintyvältä lähteeltä. Julkaistavien tietojen sisältöä rajoittavat Journalistin ohjeiden säännökset muun muassa onnettomuuden ja rikosten uhrien hienovaraisesta kohtelusta sekä lain kohdat esimerkiksi yksityiselämän suojasta, salakatselusta ja kunnianloukkauksesta.

On eri asia, hankkiiko toimittaja salassapidettäviä tietoja aktiivisesti itse vai julkaiseeko hän hänelle luovutettuja tietoja. Aktiivinen tietojen hankkiminen voi olla rangaistavaa, jos se katsotaan yllyttämiseksi salassapitorikokseen.

MILLOIN LÄHDESUOJA ON VOIMASSA?

Tiedotusvälineiden lähdesuojan merkitys korostuu aikoina, joina ilmaisunvapautta pyritään kaventamaan. Lähdesuojaa koskeva lainsäädäntö sisältyy sananvapauslakiin ja pakkokeinolakiin. Lähdesuojalla tarkoitetaan Suomessa oikeutta kieltäytyä ilmaisemasta, kuka on antanut viestin sisältämät tiedot ja kuka on laatinut viestin. Lisäksi viestin laatija tai julkaisija saa todistajana kuultaessa kieltäytyä vastaamasta kysymyksiin, jotka paljastaisivat tietojen antajan henkilöllisyyden.

Oikeus kieltäytyä todistamasta merkitsee siis sitä, ettei toimittajia ja muita toimituksellisen työn tekijöitä voida velvoittaa kertomaan tietojaan lähteen henkilöllisyydestä. Tämä voi olla merkittävä oikeus, jos lähde esimerkiksi joutuu pelkäämään vastatoimia tärkeiden tietojen luovuttamisen vuoksi. Mahdollisesta nimettömyydestä on sovittava selvästi lähteen kanssa.

Sananvapauslain mukaan lähdesuoja on toimittajan *oikeus* olla ilmaisematta tietojen antajaa, mutta Journalistin ohjeiden kohdan 14 mukaan journalistilla on sekä *oikeus* että *velvollisuus* pitää tietoja luottamuksellisesti antaneen henkilöllisyys salassa siten kuin lähteen kanssa on sovittu.

JSN linjasi MTV:lle antamassaan vapauttavassa päätöksessä 5660/TV/14 vuonna 2014, että lähdesuojasta pitää tehdä selkeä sopimus lähteen kanssa, eikä suoja ole automaattisesti voimassa jokaisen tietoja anonyymisti kertovan kanssa. Jos lähdesuoja myönnetään, lähteen henkilöllisyyden pitää olla toimituksen tiedossa.

14

Väärinkäytösten paljastaminen

Toisinaan työntekijöiden tietoon tulee salassa pidettäviä asioita, joilla on suurta yhteiskunnallista merkitystä. Tyypillisesti niissä on kyse työpaikalla tapahtuvista laittomuuksista tai erittäin arveluttavasta toiminnasta.

Jos työntekijä ei pidä hyödyllisenä asioista kertomista yrityksen sisällä tai toimivaltaisille viranomaisille, hän saattaa pyrkiä tuomaan ongelman julkisuuteen jotenkin muuten – usein jonkin tiedotusvälineen puoleen kääntymällä. Tällöin henkilöstä tulee väärinkäytösten paljastaja (englanniksi whistleblower eli pilliinpuhaltaja), joka tuo ilmi salaisia tietoja yhteiskunnallisesti merkittävistä laittomuuksista tai arveluttavasta toiminnasta.

Valinnalla voi olla hänelle tuntuvia henkilökohtaisia seurauksia aina kollegojen ja lähipiirin harjoittamasta painostuksesta sakko- tai vankeusrangaistukseen asti. Monet pilliinpuhaltajat murtavat vaikenemisen muurin yhteisössä, jossa ei ole sopivaa ottaa ongelmia esille. Usein heidät leimataan vastuunpakoilijoiksi tai pettureiksi, ja heidän työnantajansa, kollegansa, ystävänsä ja perheenjäsenensä voivat reagoida tapahtumaan rajusti. Reaktiot voivat johtaa muodollisiin seuraamuksiin, kuten irtisanomiseen tai työtehtävien vaihtoon, tai epämuodollisiin ilmiöihin, kuten kiusaamiseen, yhteisön ulkopuolelle sulkemiseen tai uhkailuun.

Usein on käynyt niin, että väärinkäytösten paljastaja on ainoana joutunut oikeuden eteen ja saanut rangaistuksen, ja hänen paljastamansa laittomuudet on jätetty tutkimatta.

Oikeustieteen tohtori, viestintäoikeuden dosentti Riku Neuvonen kirjoittaa Edilex-lakikirjaston artikkelissaan *Pilliinpuhaltajien asema Suomessa*, että Euroopan ihmisoikeustuomioistuimen ratkaisussa on asetettu pilliinpuhaltajan saamalle sananvapauden suojalle kuusi kriteeriä:

1. Onko pilliinpuhaltajalla muita vaihtoehtoja kuin vuotaa tieto suurelle yleisölle?
2. Mikä on tietoihin liittyvä yleinen etu?
3. Kuinka luotettavaa ja autenttista vuodettu tieto on?
4. Mikä on työnantajalle aiheutuneen haitan laajuus?
5. Toimiko pilliinpuhaltaja hyväntahtoisesti vai oliko taustalla muita motiiveita vai jopa vahingoittamistarkoitus?
6. Millainen seuraamus tai rangaistus pilliinpuhaltajalle on toiminnastaan koitunut?

Neuvonen mainitsee esimerkkinä, että tiedevilppi ja sen paljastamiseen liittyvät menetelmät ovat monissa maissa kehittyneimpiä pilliinpuhaltajamenettelyjä organisaatioiden sisällä. Suomessa tiedevilpin tutkinta alkaa tutkimuslaitoksen rehtorille kirjallisesti ja omalla nimellä tehdystä epäilyilmoituksesta. Jos esiselvitys havaitsee vilppiä tapahtuneen, rehtori perustaa erillisen tutkintaryhmän. Hän myös päättää, onko hyvää tieteellistä käytäntöä rikottu.

Sinänsä avoimeen menettelyyn liittyy kuitenkin monia ongelmia, joiden vuoksi pilliinpuhaltajat saattavat hakea hyvitystä julkisuuden kautta, mikä sekin voi tapahtua nimettömästi lähdesuojan turvin. Yksi tällainen huomiota herättänyt tiedevilppiepäily paljastui oman organisaationsa käytäntöihin turhautuneiden nimettömien pilliinpuhaltajien ansiosta VTT:llä vuonna 2016. Tapauksen toi esiin laajassa artikkelissaan Helsingin Sanomat. Julkisen sanan neuvosto jakoi lehdelle myöhemmin sekä langettavia että vapauttavia päätöksiä asian uutisoinnista ja jatkohoidosta.

FAKTA: TUNNETTUJA VÄÄRINKÄYTÖSTEN PALJASTAJIA

Kansainvälisellä näyttämöllä huomiota herättävimpiä paljastuksia ollut amerikkalaissotilas Chelsea Manningin tapaus. Manning sai 35 vuoden vankeustuomion yli 700 000 salassa pidettävän asiakirjan vuotamisesta WikiLeaks-vuotosivustolle. Esimerkiksi Yhdysvaltain sotatoimia Irakissa ja Afganistanissa koskevat paperit johtivat WikiLeaks-paljastuksiin hyökkäyksistä siviilejä kohtaan, heidän tappamisestaan ja muiden sodankäynnin sääntöjen rikkomisesta. Presidentti Barack Obama lievensi Manningin tuomiota, ja hän vapautui toukokuussa 2017.

Jos mennään ajassa hieman taaksepäin, yksi ensimmäisistä suurista ilmiannoista tapahtui vuonna 1971, kun sotilasanalyytikko Daniel Ellsberg vuoti niin kutsutut Pentagon-paperit The New York Timesille ja muille amerikkalaislehdille. Asiakirjoista ilmeni, että Yhdysvaltain hallinto oli johdonmukaisesti valehdellut maan sotatoimista Vietnamissa. Ellsberg joutui oikeuden eteen, mutta sai yhtenä harvoista tunnetuista väärinkäytösten paljastajista vapauttavan tuomion.

Kaikkein tunnetuin paljastustapaus sattui vuonna 2013, kun tiedusteluanalyytikko Edward Snowden vuoti valtavan määrän asiakirjoja, joiden mukaan Yhdysvaltain ja muiden maiden tiedustelupalvelut valvovat laittomasti miljoonien ihmisten verkkoviestintää ja pitävät siitä kirjaa.

Edward Snowden elää nykyisin maanpaossa Venäjällä, ja häntä saattaa odottaa jopa 30 vuoden vankeusrangaistus, jos hän palaa kotimaahansa Yhdysvaltoihin. Snowde nin tekemät paljastukset ovat nostattaneet maailmanlaajuisen keskustelun globaalista joukkovalvonnasta. Vuodon ansiosta toimittajat ovat ymmärtäneet lähteidensä ja juttujensa suojelemisen välttämättömyyden.

Väärinkäytösten paljastajat tiedotusvälineissä

Monille pilliinpuhaltajille tiedotusvälineet ovat viimeinen vaihtoehto sen jälkeen, kun he ovat yrittäneet kertoa laittomuuksista tai muista vakavista ongelmista sisäisesti organisaatiossaan. Hyvin harvat väärinkäytösten paljastajat ovat tottuneet toimimaan julkisuudessa.

Siksi on tärkeää, että toimittaja osaa varjella ilmiantajan henkilöllisyyttä ja kertoa hänelle siitä, mitä edessä voi olla. Toimittajan on myös ehdottomasti sovittava väärinkäytösten paljastajan kanssa selvästi, mitä julkaistaan ja milloin, jotta tämä voi valmistautua asian saamaan julkisuuteen. Jos toimittaja on luvannut paljastajalle lähdesuojan, nimettömyydestä on sovittava selvästi myös päätoimittajan kanssa.

Jos asia on sellainen, että väärinkäytösten paljastaja voi luottamuksellisuutta liiaksi vaarantamatta pyytää neuvoja esimerkiksi ammattiyhdistykseltä tai luotettavalta asianajajalta, häntä on kehotettava tekemään niin.

Suomessa Journalistin ohjeisiin sisältyy velvollisuus suhtautua lähteisiin kriittisesti etenkin, jos lähde saattaa tavoitella omaa etuaan. Sama perussääntö pätee myös väärinkäytösten paljastajiin. Heidän tietoihinsa on suhtauduttava kriittisesti ja varmistettava, että syytöksille löytyy totuuspohjaa.

Joskus väärinkäytösten paljastajan työyhteisö pyrkii saattamaan hänen uskottavuutensa tai motiivit kyseenalaisiksi. Jos kyseessä on erityisen vaikutusvaltainen organisaatio, jolla on oma tiedotusyksikkönsä tai hyvät kontaktit mediaan, julkisuuden valokeila saattaa kääntyä ilmiantajan persoonaan hänen paljastamiensa laittomuuksien tai muiden ongelmien sijaan.

Tällöin on tärkeää keskittyä asian substanssiin ja seikkoihin, joita ilmiantaja on tuonut julki. Vain niin voidaan saattaa usein hyvin vakavat laittomuudet tai muut väärinteot julkisen valvonnan alaisuuteen.

FAKTA: MITÄ VÄÄRINKÄYTÖSTEN PALJASTAMINEN ON?

Väärinkäytösten paljastaja tuo ilmi salaisia tietoja yhteiskunnallisesti merkittävistä laittomuuksista tai arveluttavasta toiminnasta työyhteisössään.

Usein henkilöllä on jonkinasteinen salassapitovelvollisuus työsuhteen perusteella. Hän asettaa kuitenkin ilmaisunvapautensa etusijalle salassapitoon nähden silloin, kun hän päättää puhaltaa pelin poikki ja ilmoittaa havaitsemistaan epäkohdista.

Useimmissa paljastuksissa työntekijä on ensin yrittänyt ottaa ongelman esiin organisaation sisällä. Jos se ei ole tuottanut tulosta, hän pyrkii viimeisenä keinonaan korjaamaan asiaa hakemalla sille julkisuutta tiedotusvälineissä.

14

15
Mistä lisätietoja?

Tässä kirjassa on esitelty paljon välineitä viestiliikenteen ja internethakujen turvallisuuden parantamiseen päivittäisessä elämässä. Jos toimittajalla on näpeissään seuraava Snowden-tapaus tai muu erityisen korkeaa turvallisuustasoa edellyttävä lähde tai aihe, hän tarvitsee työkalupakkiinsa välineitä, jotka ovat edistyneempiä kuin tässä kirjassa kuvatut perusvälineet. Seuraavista vinkeistä voi olla hyötyä lisätietoa etsittäessä.

Hyödyllisiä verkkosivustoja

ssd.eff.org
Electronic Frontier Foundation on kansalaisjärjestö, joka puolustaa kansalaisoikeuksia internetissä. Järjestö on julkaissut valvonnalta suojautumista koskevan laajan, maksuttoman verkko-oppaan nimeltä *Surveillance Self-Defense*. Verkkosivustolla on salausvälineiden asennusoppaita, toimittajille ja journalistiikan opiskelijoille suunnattuja infopaketteja ja paljon muuta hyödyllistä aineistoa.

cpj.org
Lehdistönvapautta puolustava järjestö The Committee to Protect Journalists on koonnut toimittajille tarkoitetun ”ensiapupakkauksen”, jossa käsitellään myös digitaalista turvallisuutta. Lisäksi sivusto sisältää yleiskatsauksen turvallisuustilanteesta eri maissa. Siitä on hyötyä eritoten riskialueilla matkustaville tai työskenteleville toimittajille.

freedomhouse.org
Kansalaisjärjestö Freedom House julkaisee maakohtaisia vuosiraportteja digitaalisesta turvallisuudesta eri puolilla maailmaa. Niihin kannattaa tutustua ennen ulkomaille suuntautuvalle juttumatkalle lähtöä. Järjestö saa osan rahoituksestaan Yhdysvaltain liittovaltion budjetista.

securityplanner.org
Kanadalainen kansalaisjärjestö Citizen Lab on laatinut vuorovaikutteisen turvallisuusoppaan. Sitä ei ole suunnattu erityisesti toimittajille, mutta se sisältää paljon hyödyllisiä ja yleistajuisia vinkkejä, joita myös toimittajat voivat hyödyntää.

cryptoguide.dk
Toimittajien salausoppaan alkuteos, *Cryptoguide for journalister*, on kirjoitettu tanskaksi, ja teoksella on oma verkkosivustonsa. Sivustolla on tanskankielisen sisällön lisäksi tietoja ja vinkkejä myös englanniksi sekä päivittyvä linkkikokoelma monien kirjassa kuvattujen työkalujen verkkosivuista. Sivuilta löytyvät myös kirjan kirjoittajan yhteystiedot – ota yhteyttä, jos haluat kysyä jotakin tai antaa palautetta!

16
Sanastoa

Salauksesta ei voi puhua käyttämättä teknisiä käsitteitä. Niitä vilisee myös tässä kirjassa, ja monet käsitteet esiintyvät toistamiseen eri luvuissa. Jos kaipaat jollekin käsitteelle selitystä, katso tästä hakemistosta, millä sivulla se esiintyy ensimmäistä kertaa.

Solidaarisuussalaus **17**

Tietue **19**

IP-osoite **20**

Metatiedot **20**

Haittaohjelma **24**

Päästä päähän -salaus [end-to-end crypting] **35**

Salausavaimet **35**

Avoin lähdekoodi [open source] **36**

Sormenjälki **39**

Massamuistin salaus **39**

Air gapped -tietokone **51**

PGP **53**

Kertakäyttöpuhelin [burner phone] **61**

Avain-ID **95**

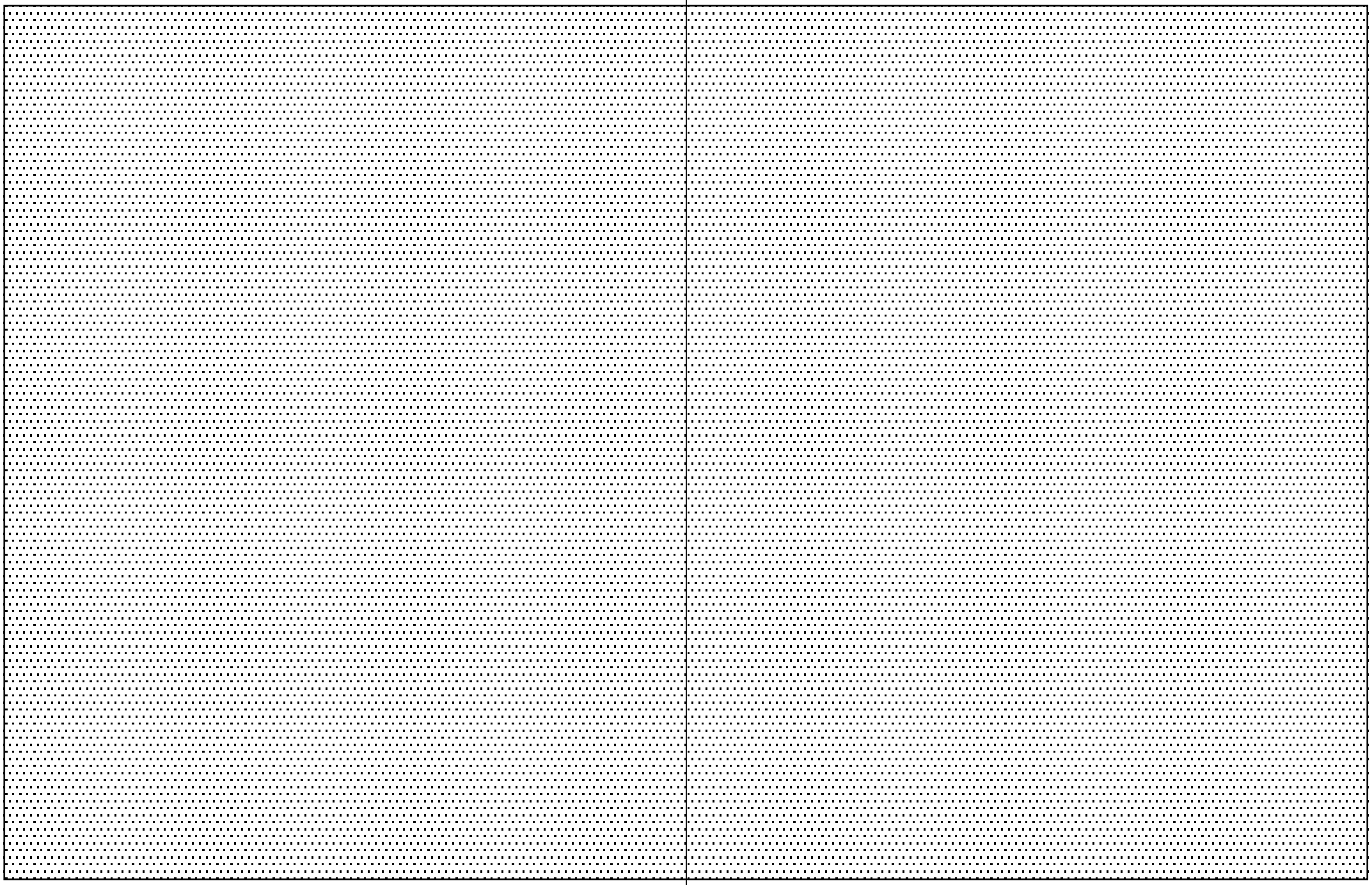
GPG **91**

Kaksivaiheinen vahvistus [2FA] **101**

VPN **106**

Tietojen kalastelu [phishing] **109**

Olan yli kurkkiminen [shoulder surfing] **118**





HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI





(*Toimittajan salausopas* 256-bittisellä salauksella kirjoitettuna)

johdattaa digitaalisen itsepuolustuksen maailmaan. Kirja sisältää ohjeita luottamuksellisten tietojen ja lähteiden suojaamiseen.

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI