Opinnäytetyö (AMK)

Tietojenkäsittely

2018

Henna Nousiainen

KÄYTTÄJÄN TURVA SOSIAALISESSA MEDIASSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2018 | 34 sivua

Henna Nousiainen

KÄYTTÄJÄN TURVA SOSIAALISESSA MEDIASSA

Sosiaalinen media on kiteytynyt olennaiseksi osaksi nyky-yhteiskuntaa ja erilaisia palveluita on tarjolla lukuisia. Kommunikaatio ja sisällön jakaminen onnistuu hetkessä maailman ollessa koko ajan yhteystilassa. Yksittäisten käyttäjien lisäksi myös yritykset ja eri työympäristöt ovat ottaneet sosiaalisen median osaksi toimintaansa. Kaiken positiivisuuden kääntöpuolena on kuitenkin yksityisyyden heikkeneminen. Opinnäytetyön tavoitteena oli esitellä yleisimpiä käyttäjään kohdistuvia riskitekijöitä sosiaalisessa mediassa ja oman vastuun merkitystä uhkien ennakoimisessa.

Informaatiota koottiin aihekohtaisesta kirjallisuudesta ja internetaineistoista. Työssä käytetyissä esimerkkitapauksissa hyödynnettiin tapauskohtaisia uutisia, joiden tarkoituksena oli havainnollistaa tarkasteltavaa aihealuetta. Tietosuojan määrittelyssä hyödynnettiin Suomen lakia sekä keväällä 2018 voimaan tullutta GDPR-lakia. Lähempään tarkasteluun valittiin Facebookin tietosuojan sisältö ja tutkittiin sen käyttäjän yksityisyyttä koskevia asetuksia. Työn tutkimusmenetelmänä oli käytössä kirjallisuuskatsaus.

Voidaan väittää, että kokonaisvaltaista anonyymiyttä on lähestulkoon mahdotonta saavuttaa verkossa. Käyttäjän on kuitenkin mahdollista omilla valinnoillaan edesauttaa yksityisyytensä turvaamista sekä ennakoimaan potentiaalisia riskejä. Opinnäytetyöhön kootun informaation pohjalta tarkoituksena on ymmärtää tietoturvan merkitys perusteista alkaen sekä löytämään ratkaisuja käyttäjän identiteetin suojelemiseksi sosiaalisessa mediassa.

ASIASANAT:

sosiaalinen media, tietoturva, tietosuoja, digitaalinen jalanjälki, yksityisyys, Facebook

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2018 | 34

Henna Nousiainen

USER SECURITY ON SOCIAL MEDIA

Social media has become an integral part of society in the past years. New social media services are released continuously and it is effortless for users to communicate and create new content when the whole world is connected. Businesses and other work environments have also found ways to utilize its impact on their own platforms. However, the major risk is the lack of privacy. The aim of this thesis is to introduce the most common threats on social media and the significance of the user's responsibility.

This thesis is a literature review and the Information was collected utilizing books, Finnish law and internet articles on user security on social media. In some example cases news articles about real life scenarios were used. Facebook's privacy policy and settings were examined in detail to provide insight about its data collection.

On the basis of the literature review undertaken in this thesis, it has become clear that it may be practically impossible to remain anonymous in an online world. However, this thesis hopes to enable its readers to understand the fundamentals of information security and provide solutions to mitigate potential privacy risks on social media.

.

KEYWORDS:

social media, data security, data protection, online visibility, privacy, Facebook

SISÄLTÖ

KUVAT

1 JOHDANTO

Opinnäytetyön päätavoitteena on tutkia käyttäjän tietosuojaa -ja turvaa sosiaalisessa mediassa, joka koskettaa useiden käyttäjien päivittäistä elämää. Nykyaikana henkilökohtaisen tietoturvan merkitys on entistä suurempi digitalisoinnin roolin kasvaessa yhä olennaisemmaksi osaksi yhteiskuntaa.

Sosiaalinen media pitää sisällään paljon positiivisia asioita. Maailman menossa pysyy mukana eri uutiskanavien kautta, ihmissuhteita pystyy muodostamaan niin työmaailmassa kuin henkilökohtaisessa elämässä ja oman sisällön tuottaminen onnistuu vaivattomasti. Viestintävälineenä sosiaalista mediaa on mahdollista hyödyntää niin työelämässä, kuin vaikka myös politiikassa sen laajan saavuttavuuden vuoksi. Käyttäjän turvan uhkana on kuitenkin yksityisyyden väistämätön hälveneminen palveluiden kerätessä dataa käyttäjien toiminnasta.

Tietoturvauhkia esiintyy lukuisissa eri muodoissa, joiden takia yksittäistä kriteeriä niiden tunnistamiseksi ei ole olemassa. Tässä työssä kuvailtuja uhkia on rajattu yleisimpiin tapauksiin, joihin käyttäjä pystyy omilla valinnoillaan vaikuttamaan sekä mahdollisesti myös ennaltaehkäisemään. Työn ensimmäiset luvut on omistettu tietoturvan -ja suojan peruskäsitteiden määrittelemiselle, jotka toimivat informaation pohjustuksena.

Inspiraatio työlle lähti puhtaasta mielenkiinnosta perehtyä sosiaalisen median riskeihin käyttäjän näkökulmasta. Tavoitteena oli kerryttää aikaisempaa tietämystä ja löytää uusia ratkaisumalleja, joita voisi soveltaa myös omaan arkielämään.

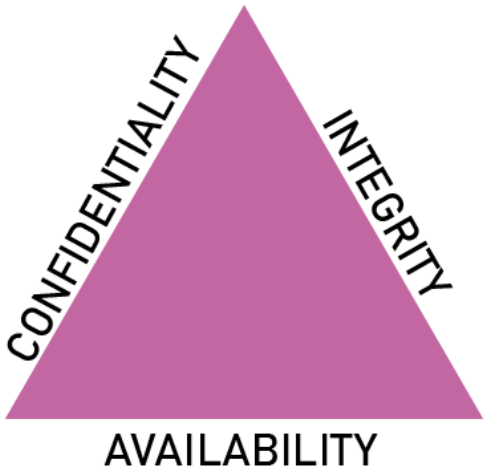
Opinnäytetyön tutkimusmenetelmänä on kirjallisuuskatsaus. Tiedon keräämisessä on käytetty aihekohtaista kirjallisuutta ja internetlähteitä. Tietosuojan määrittelyssä on hyödynnetty Suomen lakia sekä vuonna 2018 voimaan tullutta GDPR-asetusta.

2 TIETOTURVA

Tässä luvussa perehdytään tietoturvan yleismääritelmään ja sen kolmeen jaettuun alaluokkaan. Tarkoituksena on, että lukija saa kuvan tietoturvan merkityksestä ja sen muodostavista pääpilareista.

2.1 Määritelmä ja merkitys

Tietoturva pitää sisällään paljon, mutta yleisesti kuvailtuna sen voidaan sanoa kattavan tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen. (Rousku, 2013, 47.) Kyseiset käsitteet muodostavat yhdessä CIA-kolmion (Kuva 1.), joka koostuu edellä mainittujen käsitteiden englanninkielisistä vastineista: confidentiality, integrity ja availability.



Kuva 1. CIA-kolmio.

Tietoturva käsittää niin järjestelmien, tietoaineistojen, ohjelmistojen, kuin myös tietoliikenteen turvallisuuden. (Viestintävirasto 2017.) Tieto itsessään voi myös esiintyä monessa eri muodossa, eli se ei pelkästään tarkoita vain laitteisiin tallennettua dataa. Näin ollen tieto voi myöskin merkitä esimerkiksi puhuttua tai paperille kirjoitettua informaatiota.

Tietoturvauhkia on olemassa lukuisia eri huijausyrityksistä ja viruksista tietojenkalasteluun. Seuraavissa luvuissa kuvailtuja uhkia on rajattu yleisimpiin tapauksiin, joita sosiaalisen median palveluissa voi todennäköisesti kohdata.

Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan tiedon rajattua käyttöoikeutta ottaen huomioon miten salassa pidettävää sisältö on. (Taylor, Alexander, Finch & Sutton, 2013.)

Salassa pidettäviin tietoihin voidaan lukea mitkä tahansa henkilökohtaiset tiedot, kuten esimerkiksi sähköposti ja pankkitiedot. Tietojen vuodon estämistä ulkopuolisille voidaan rajoittaa esimerkiksi salasanoilla, salausalgoritmeilla tai käyttöoikeuksia hallitsemalla. (Järvinen, 2012, 10.)

Eheys

Eheys merkitsee tiedon pysymistä muuttumattomana koko sen olemassaolon ajan. Tiedon muokkaaminen tai poistaminen on sallittua vain sen käyttöoikeuden omaavien toimesta. (Taylor ym. 2013.)

Jos mietitään esimerkiksi eri sosiaalisen median palveluita: omaa profiilia ja sen sisältöä tulisi pystyä päivittämään vain käyttäjä itse. Tilille murtautuminen ulkopuolisen toimesta voi olla uhkana tiedon eheänä pysymiselle.

Saatavuus

Saatavuus merkitsee tiedon käytettävissä oloa aina tarvittaessa. Tiedon saatavuuteen voi vaikuttaa negatiivisesti esimerkiksi sivustojen kaatuminen ja luonnonkatastrofit. (Järvinen, 2012, 10.)

2.1.1 Fyysinen turva

Käsitteellä tarkoitetaan laitteistojen sekä ympäröivien toimitilojen suojaamista. Fyysistä turvaa voi uhata lukuisat riskitekijät, mitkä saattavat aiheutua ihan huomaamatta ilman, että takana olisi pahantahtoisuutta toisen henkilön toimesta.

Riskit voidaan jakaa kolmeen luokkaan: ympäristön -, teknilliset -ja ihmisten aiheuttamat uhat.

Ympäristön uhkiin voidaan lukea esimerkiksi eri luonnonkatastrofit, kuten tulvat, maanjäristykset sekä hurrikaanit. Laitteiston ja sen komponenttien toimivuuteen voi vaikuttaa myös liian matala tai korkea lämpötila sekä ilman kosteus. Huomioitavaa on myös esimerkiksi tulipalon ja vesivahinkojen mahdollisuus, jotka voivat aiheuttaa paljon fyysistä tuhoa koneille.

Teknillisiin uhkiin lasketaan esimerkiksi sähkökatkokset, jotka saattavat keskeyttää palveluiden toimivuuden. Myös ukkonen ja sen aiheuttama ylijännite on mahdollinen uhka järjestelmille.

Viimeiseen kategoriaan eli ihmisten aiheuttamiin uhkiin luetaan esimerkiksi luvaton läpikulku toimitiloissa, varkaudet ja vandalismi. (Vacca, 2012.)

2.1.2 Tekninen turva

Tekniseen turvaan kuuluu laitteiston ja ohjelmien turvaaminen mahdollisilta haavoittuvuuksilta. Esimerkiksi salausalgoritmien käyttö henkilökohtaisten dokumenttien suojaamiseksi ja ohjelmiston säännöllinen päivittäminen voivat olla turvautumiskeinoja.

Olennaista on myös käyttöoikeuksien hallinta ja rajaaminen, jotta tietoihin ei pääse käsiksi muut kuin asianomaiset henkilöt. (Viestintävirasto 2017.) Käyttäjillä on omat roolinsa ja tehtävänsä, jonka mukaan myös käyttöoikeudet jaetaan. Oikeuksien muuttamista ja poistamista hallitsee yleensä järjestelmävastaava.

2.1.3 Hallinnollinen turva

Hallinnollinen turva kattaa esimerkiksi yritysten tietoturvapolitiikan kehittämisen, josta käy ilmi pääperiaatteet ja menettelytavat tietoturva-asioissa, joihin yritys on sitoutunut. Riskien hallinta ja monitorointi ovat myös osana hallinnollista turvaa. Säännöllisten tietoturvakatsausten kautta voidaan tunnistaa olennaisimmat riskit,

joihin yrityksen kannattaa erityisesti kiinnittää huomiota. Hallinnolliseen turvaan lasketaan myös henkilöstön ohjaaminen tietoturva-asioissa. (Viestintävirasto 2017.)

3 TIETOSUOJA

Tässä luvussa käsitellään tietosuojan määritelmää sekä sen merkitystä Suomessa. Lisäksi tarkasteluun otetaan myös vastikään voimaan tullut GDPR-laki.

3.1 Määritelmä ja merkitys

Tietosuoja käsittää ihmisen henkilökohtaisten tietojen turvallisen käsittelyn. Näihin voidaan lukea mitkä tahansa tiedot, joilla henkilö voidaan tunnistaa. Kyseisiä tietoja voivat olla esimerkiksi nimi, puhelinnumero ja henkilötunnus. Jokaisella on oikeus omaan yksityisyyteen, minkä vuoksi tietojen käsittelyä varten on omat lakipykälänsä osoittamaan, milloin tietoja on lupa tarkastella ja kenen toimesta. (Tietosuojavaltuutetun toimisto n.d.)

3.2 Tietosuojalaki Suomessa

Suomessa henkilön yksityisyyttä ja tietojen käsittelyä suojaa henkilötietolaki. Sitä sovelletaan tietojen automaattiseen käsittelyyn tai tapauksissa, jossa ne muodostavat henkilörekisterin tai sen osan. Tietojen käsittely kattaa kaiken tietoihin kohdistuvan toiminnan keräämisestä poistamiseen.

Tietojen laatua koskee tarpeellisuus -ja virheettömyysvaatimus. Henkilötietojen käsittelyn tulee olla aiheellista ja tilanteen kannalta tarpeellista. Virheellisiä tai vanhentuneita tietoja ei saa käsitellä. Ennen henkilötietojen keräämistä kehitetään yleensä suunnitelma, jossa määritellään prosessin tarkoitus ja toteutusmenetelmät sekä mihin tietoja mahdollisesti luovutetaan.

Arkaluonteisia tietoja, joihin voidaan laskea henkilön

- etninen alkuperä
- poliittinen tai uskonnollinen vakaumus
- rikosseuraamukset
- terveyttä koskevat tiedot

- seksuaalinen suuntautuminen
- sosiaalihuoltoa koskevat tiedot

ei ole lupa käsitellä. Poikkeustapauksessa henkilö on antanut itse suostumuksensa. (Henkilötietolaki 22.4.1999/523, 2-11 §.)

3.3 GDPR-laki

GDPR-laki eli yleinen tietosuoja-asetus astui voimaan Euroopassa 25.5.2018. Sen perimmäisenä tarkoituksena on antaa käyttäjille enemmän hallintaoikeuksia omien tietojen käsittelyssä ja näin ollen myös suojata henkilötietoja paremmin. Lisäksi tavoitteena on, että tietosuojasääntely yhtenäistyy Euroopan sisällä asetuksen myötä.

Lain tultua voimaan jokaisella on oikeutena tietää missä ja miten omia henkilötietoja käsitellään, sekä pyytää mahdollisten puutteiden korjaamista tai jopa lopullista poistamista.

Jos yrityksellä on hallussa käyttäjään kohdistuvia tietoja, on käyttäjällä lupa pyytää pääsyä niihin ja saada vahvistus niiden käsittelytarkoituksesta. Yrityksellä on vastuu vastata pyyntöön ja toimittaa tarvittavat tiedot. (Tietosuojavaltuutetun toimisto n.d.)

4 SOSIAALINEN MEDIA

Tässä luvussa määritellään sosiaalinen media käsitteenä sekä sen tuoma vastuu ja mahdolliset riskit.

4.1 Määritelmä

Sosiaalinen media tai lyhennettynä ”some” pohjautuu ihmisten yhdistämiseen ympäri maailmaa teknologian avulla. Vuonna 2018 sosiaalisen median käyttäjiä on tilastojen mukaan jo 3,196 biljoonaa ja luku kasvaa vuosittain noin 13 %. (Chaffey, 2018.)

Sosiaalisen median olennaisimmat osat ovat sisällön jakaminen ja luominen. Eri palvelualustojen myötä käyttäjät pystyvät helposti kommunikoimaan keskenään sijainnista riippumatta. Yritykset ovat myös huomanneet sosiaalisen median tehokkaan vaikutuksen ja ottaneet sen osaksi brändinsä markkinointia.

Kaiken kaikkiaan sosiaalista mediaa voisi tiivistettynä kuvailla virtuaalisena viestintätyökaluna.

4.2 Palvelut

Sosiaalisen median palveluiden määrä on runsas ja tarjonta kasvaa jatkuvasti. Kolme suosituinta palvelua maailmanlaajuisesti käyttäjämäärään nähden ovat tällä hetkellä Facebook, Youtube ja Whatsapp. (Chaffey, 2018.)

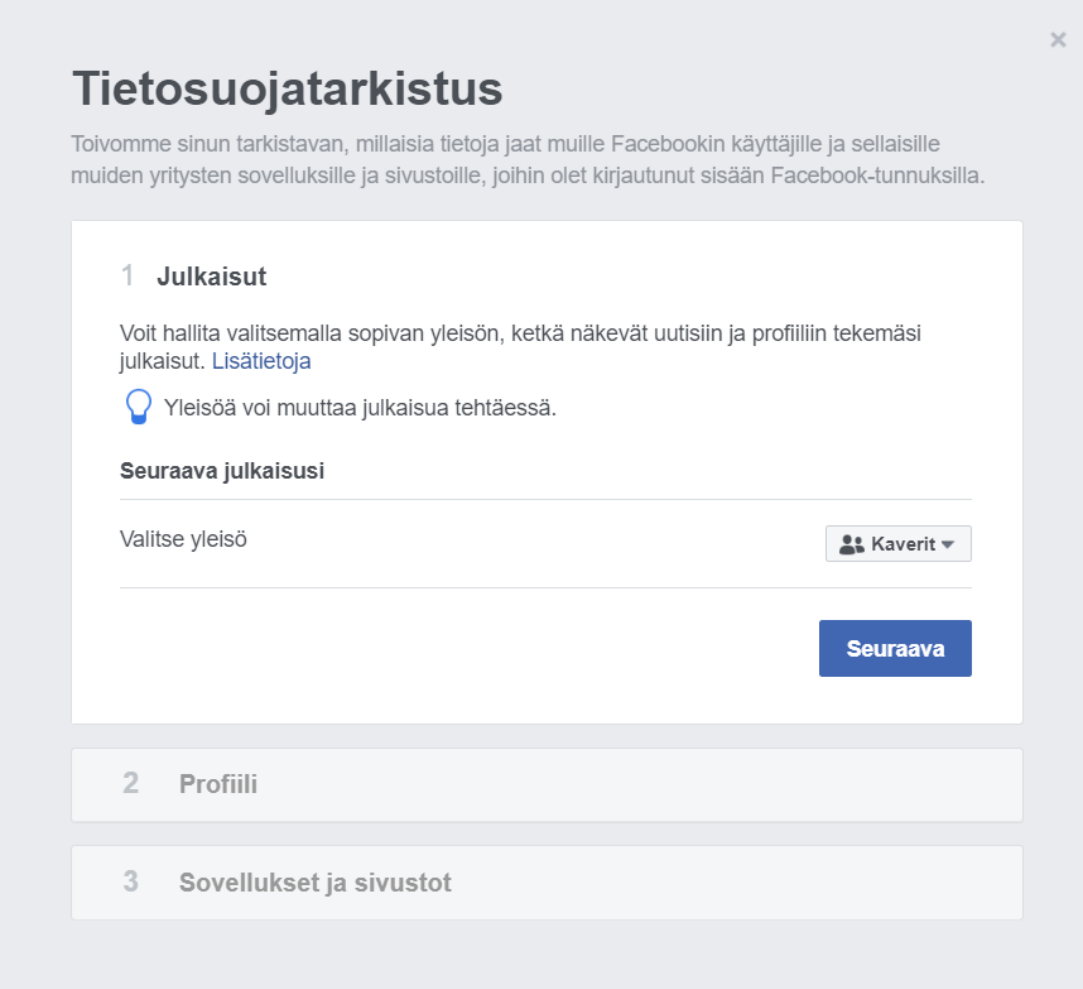
Palveluiden tietosuojakäytäntöihin on hyödyllistä tutustua aina ennen uuden käyttäjätilin luomista. Olennaisinta on erityisesti selvittää käytännöt käyttäjän tietojen keräämisen suhteen. Mitä tietoja käyttäjästä kerätään? Mihin tietoja käytetään? Mitä tiedoille tehdään, jos tilin poistaa?

Facebook

Facebookin tietosuojakäytäntö ja datan kerääminen sisältävät

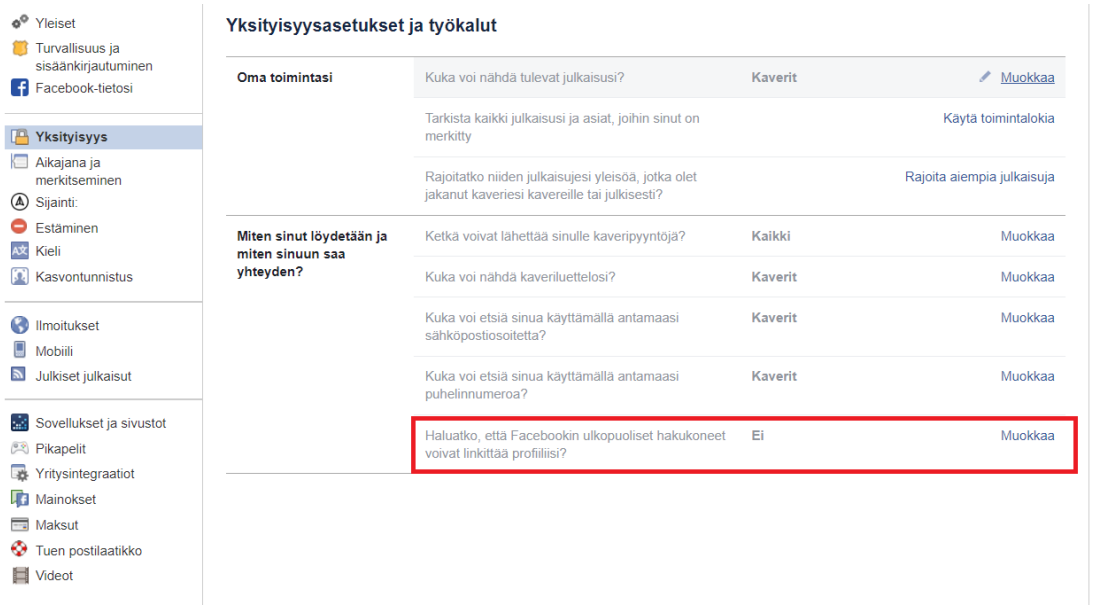
- tilille kirjautumisen ja julkaistun sisällön
- yhteydenpidon muihin ihmisiin ja ryhmiin
- toimintojen ja ominaisuuksien käytön
- maksutapahtumat
- muiden jakamat tiedot käyttäjästä
- laitetiedot, kuten esimerkiksi ominaisuudet, toiminta, yhteydet ja eväs-tetiedot
- kolmansien osapuolien keräämät tiedot käyttäjästä.

Facebook perustelee tietojen keräämisen kehittävän käyttäjän henkilökohtaista käyttökokemusta sekä palvelujen toimivuutta. Esimerkiksi mainokset voivat perustua henkilön kiinnostuksenkohteisiin ja sijaintiin. (Facebook 2018.)



Kuva 2. Facebookin tietosuojatarkistus-toiminto (Facebook).

Profiilin sisällön näkyvyyttä on mahdollista rajata käyttäjäasetuksista sekä julkaisuvaiheessa. Pikaohje-kohdasta löytyy ”Tietosuojatarkistus” toiminto (Kuva 2.), jolla käyttäjä pystyy nopeasti tarkistamaan kenelle julkaisut ja profiilin tiedot näkyvät. Lisäksi myös sovellukset, joihin kirjautuminen tapahtuu Facebook-tunnuksella, voidaan piilottaa muiden näkyvistä.



Kuva 3. Facebookin yksityisasetukset ja työkalut (Facebook).

Jokaisella käyttäjällä on yksilöllinen id-tunnus, jonka avulla hakukone voi esimerkiksi löytää Facebook-profiilin nimen perusteella. Asetuksia muokkaamalla automaattisen toiminnon pystyy ottamaan pois käytöstä ja estämään profiilin ilmestymisen hakukoneiden tuloksissa (Kuva 3.).

4.3 Oma vastuu

Sosiaalinen media ja yksityisyys eivät kulje käsi kädessä. Käyttäjällä on suurin vastuu, mitä tulee tiedon jakamiseen ja julkaisemiseen. Riski on aina olemassa, että mikä tahansa jaettu tieto leviää tahoille, joille se ei välttämättä kuulu. Sen vuoksi voidaan ajatella, että virtuaalinen maailma on yhtä lailla rinnastettavissa muuhun elämään. Jos jotain asiaa ei ole valmis jakamaan vastaan kävelevälle henkilölle, niin miksi sitten kymmenkertaiselle määrälle ihmisiä verkossa?

Suuri osa ihmisistä on valmiita jakamaan elämäänsä tekstin, kuvien ja videoiden muodossa. Totta on kuitenkin se, että netti ei unohda. Vaikka vanha kuva poistettaisiin Facebookista, ei ole varmuutta siitä, etteikö joku olisi voinut tallentaa sitä omalle koneelleen. Sama pätee myös kommentointiin ja omien mielipiteidensä esittämiseen. Julkaisut, jotka voidaan nähdä uhkaavina tai kunniaa loukkaavina voivat johtaa vakaviin seurauksiin, mikä saattaa vaikuttaa esimerkiksi työnsaantiin.

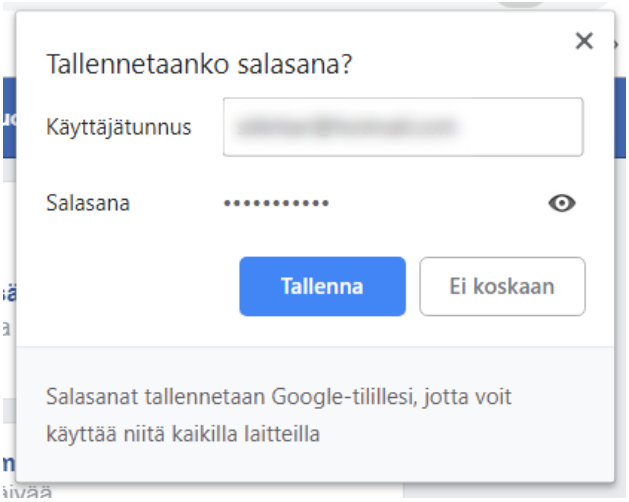
4.4 Riskit

Tietoturvariskejä on olemassa useita erityyppisiä ja niitä voi kohdata monissa eri tilanteissa. Riskien ehkäisyn perustana ovat toiminnassa oleva virustorjunta ja palomuuri, joiden päivitykset on olennaista pitää ajan tasalla. Päivittämättömissä ohjelmistoissa voi olla tietoturva-aukkoja, eikä viimeisimpien haittaohjelmien havaitseminen välttämättä onnistu yhtä tehokkaasti.

Salasanat

Heikot ja useissa paikoissa käytetyt samat salasanat ovat yleinen tietoturvariski. Vahvan salasanan suositellaan sisältävän numeroita, symboleita ja erikokoisia kirjaimia. Sen ei tulisi sisältää mitään arvattavissa olevaa informaatiota, kuten puhelinnumeroa tai lemmikin nimeä. Pituuden suositellaan olevan vähintään 10 merkkiä, jos vain mahdollista.

Uniikin salasanan luominen useisiin eri paikkoihin ja ulkoa muistaminen saattaa tuottaa päänvaivaa. Yhtenä ratkaisuna voivat olla salasananhallintaohjelmat, kuten esimerkiksi KeePass ja LastPass. Ohjelmien tarkoituksena on tallentaa salasanat salausalgoritmin turvin tietokantaan, joka suojataan yhdellä muistettavalla pääsalasanalla.



Kuva 4. Googlen salasanantallennus (Google Chrome).

Usein selaimet saattavat pyytää salasanan tallentamista muistiin (Kuva 4.), jolloin palveluun kirjautuminen onnistuu nopeammin. Vaikka se voi itsessään kuulostaa hyödylliseltä toiminnolta, on se myös olemassa oleva uhka, jos ulkopuolinen pääsee käsiksi tietokoneeseen ja sitä myöten suoraan käyttäjätileille.

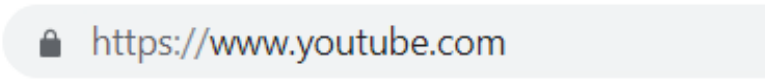
Osa palveluista tarjoaa kaksivaiheista tunnistautumista, mikä tarkoittaa kahta tai useampaa todentamistapaa käyttäjänimen ja salasanan lisäksi. Tapoja voivat olla esimerkiksi mobiilivarmenne tai tekstiviestinä tuleva kertakäyttökoodi. Kyseinen metodi lisää turvaa tilille kirjautumisessa ja käyttäjän identiteetin varmistamisessa. (Viestintävirasto 2017.)

4.4.1 Identiteettivarkaudet

Identiteettivarkaus merkitsee toisena henkilönä esiintymistä. Henkilön tietoja voidaan esimerkiksi käyttää nettiostoksiin, tekaistun profiilin luomiseen tai muuhun sopimattomaan toimintaan. (Järvinen, 2012, 276.) Tietoja voidaan urkkia käyttäjästä riippumattomasta syystä, kuten tietovuodon seurauksena. Toisinaan henkilötietoja on mahdollista saada selville vilkaisemalla pelkästään käyttäjän profiileja eri sosiaalisen median palveluissa (LifeLock n.d.)

Facebookissa pystyy esimerkiksi selvittämään yllättävän paljonkin tietoja henkilöstä, jos profiilin näkyvyyttä ei ole rajattu asetuksista. Henkilön koko nimi, asuinpaikka, kiinnostuksen kohteet, perheenjäsenten nimet jne. Jopa hyvin harmittoman oloinen yksityiskohta, kuten lemmikin nimi, saattaa olla käyttäjätilin turvakysymyksen vastaus.

Profiilien urkkimisen lisäksi myös julkinen Wi-Fi voi olla iso turvallisuusriski, koska tietoliikenne ei yleensä ole salatussa muodossa ja näin ollen käyttäjän toiminnan monitorointi on mahdollista. Sen vuoksi ollessa yhteydessä julkiseen verkkoon on suositeltava välttää esimerkiksi verkkokauppaostoksia, jotka vaativat maksutietojen käyttöä. (Norton). Tuntemattomiin yhteyspisteisiin ei myöskään kannata yhdistää, jos niiden alkuperästä ei ole tietoa.



Kuva 5. Suojattu yhteys (Google Chrome).

Ylipäätänsä henkilökohtaisia käyttäjätilejä käsiteltäessä on kannattavaa tarkastaa, että sivustossa tietoliikenne on suojattu. Sen pystyy katsastamaan URL-kentästä, jossa tulisi olla näkyvissä lukon kuva sekä ”https” (Kuva 5.).

Identiteettivarkauksia voi tapahtua verkon ulkopuolellakin, kuten esimerkiksi salakuuntelun seurauksena tai olan yli urkkimisella. Joissain tapauksissa jopa roskiksia tutkimalla väärä henkilö voi saada käsiinsä henkilökohtaisia dokumentteja. (LifeLock.)

4.4.2 Roskaposti

Roskaposti on yleinen vaiva erilaisissa viestintäsysteemeissä, kuten sähköpostissa. Sillä tarkoitetaan ei-toivottuja viestejä, joita saattaa ilmestyä massoittain. Roskapostin sisältö yleisemmin koostuu suhteellisen harmittomista mainoksista, mutta toisinaan ne voivat sisältää haitallisia liitteitä tai linkkejä, joita avaamalla

kohteen henkilökohtaisia tietoja on mahdollista saada varastettua. (Norton.) Huijausviestit voivat vaikuttaa uskottavilta ensi näkemältä, mutta on hyvä muistaa, että viralliset tahot eivät yleensä pyydä käyttäjän yksityisiä tietoja sähköpostitse.

Hyödyllinen metodi on ainakin kahden erillisen sähköpostin ylläpitäminen, jolloin esimerkiksi pankki -ja muille virallisille asioille on kokonaan toinen tili käytössä.

Sähköposteissa on yleensä valmiina suodatin roskapostia varten, joka tarkastaa viestin sisällön ja lajittelee tarpeen vaatiessa suoraan roskapostikansioon. Nykyaikana suodattimet ovat tarkempia kuin ennen, mutta se ei tarkoita, etteikö erehdyksiä voisi sattua. Käyttäjän on kaikesta huolimatta hyvä olla tietoinen mahdollisista riskeistä avatessaan viestejä tuntemattomista lähteistä sekä aina tarkastaa sisältö huolellisesti. Useissa sähköpostiohjelmissa roskapostin pystyy myös itse raportoimaan tai vaihtoehtoisesti estämään lähettäjän.

4.4.3 Tietojenkalastelu

Tietojenkalastelu on tietoturvahyökkäys, joka voi myös johtaa aiemmin mainittuun identiteettivarkauteen. Hyökkäyksen tarkoituksena on esiintyä toisena henkilönä ja tavoitella kohteen henkilökohtaisia tietoja. Hyökkääjä voi esimerkiksi pyytää käyttäjää aktivoimaan tilinsä uudelleen viestiin liitetyn haitallisen linkin kautta. (OWASP 2018.)

Joissain tapauksissa hyökkäys voidaan suorittaa keräämällä ensin tarpeeksi informaatiota kohteesta, jolloin viestit pystytään lähettämään henkilökohtaisemmassa muodossa. (Cisco n.d.) Esimerkkitapauksessa hyökkääjä tietää kohteen nimen ja sen, että hänellä on käytössä Paypal. Näiden tietojen pohjalta voidaan luoda kustomoitu viesti ja pyytää esimerkiksi kohdetta luovuttamaan salasana tai muita yksityistietoja. Viesti voidaan saada vaikuttamaan luotettavalta, ja sen vuoksi onkin tärkeä kiinnittää huomiota tekstin ja sähköpostiosoitteen kirjoitusmuotoon mahdollisten virheiden varalta.

Gmailissa on myös toiminnassa todennuksen tarkistaminen, joka näyttää lähettäjän vieressä kysymysmerkin, jos tilin aitoutta ei ole varmistettu. (Google n.d.)

4.4.4 Mainokset

Pelkästään Facebookia selaamalla pystyy näkemään lukuisia mainoksia eri tahoilta. Palvelussa kuka tahansa pystyy luomaan omia sivuja, joten tuttuina yrityksinä tai henkilöinä esiintyminen ei ole mahdotonta. Huijausmielessä tehdyt mainokset on kehitetty mahdollisimman houkutteleviksi tarjouksineen tai ilmaistuotteineen ja kopioitu tekstin sekä kuvien osalta alkuperäisten kaltaisiksi. Kuitenkin käyttäjän klikatessa linkkiä voi se viedä suoraan sivustolle, joka on luotu tietojenkalastustarkoituksessa. Vahinko saattaa kiertää vielä enemmän, jos käyttäjää pyydetään jakamaan mainosta eteenpäin tutuilleen.

Viime vuonna kiersi tämän kaltainen viestiketju eri sosiaalisen median palveluissa, jossa mainostettiin ilmaisia 50 dollarin arvoisia kuponkeja äitienpäivän kunniaksi. Kupongin saadakseen käyttäjän oli pakko jakaa ilmoitusta eteenpäin ja täyttää pienimuotoinen kysely saamatta kuitenkaan vastineeksi yhtään mitään. Huijaus ei onneksi laajentunut niin pahaksi, että käyttäjätietoja olisi anastettu, mutta siihenkin olisi hyvin voinut olla mahdollisuus. (Allen, 2017.)

Kuva 6. Mainoshuijaus Twitterissä (BBC, 2018).

Toinen vastaavanlainen oli vuonna 2018 Twitterissä, jossa huijarien kohteena olivat Twitterissä varmennetut käyttäjätilit (Kuva 6.). Syylliset vaihtoivat tilien nimen ja kuvan imitoimaan Teslan toimitusjohtajaa Elon Muskia. Huijauksessa mainostettiin osallistumaan kampanjaan, jossa lähettämällä pienen määrän Bitcoineja (digitaalinen valuutta) saisi vastapalkkiona niitä lisää suuremman osuuden. Mainos itsessään ei välttämättä vaikuta vakuuttavalta sen sisältämine kirjoitusvirheineen, mutta vahvistettu käyttäjätili lisää luotettavuutta muiden käyttäjien silmissä. (BBC 2018.)

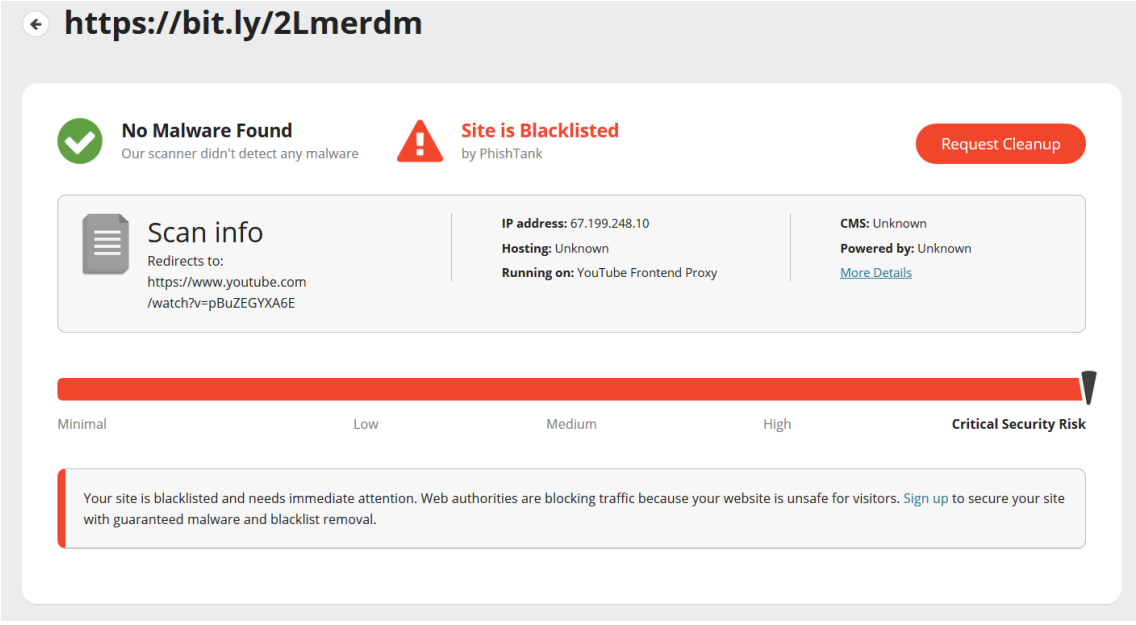
Huijausmainoksia voi havaita myös käyttämällä tuttua hakukone Googlea. Googlella on käytössä Google Ads, joka näyttää mainoksia ehdotettujen sivustojen yläpuolella. On ollut tapauksia, joissa käyttäjä on laittanut hakuun esimerkiksi Amazonin verkkokaupan ja yläpuolella on ollut mainoslinkki Amazonin nimellä kulkevalle haittasivustolle. Hakemansa kohteen sijaan uhri sai varoituksen koneellaan olevasta haittaohjelmasta. (Whittaker, 2018.)

4.4.5 Haitalliset sivustot

Haitallisten sivujen havaitseminen voi osoittautua hankalaksi varsinkin, kun niiden tunnistamiseen ei ole olemassa yhtä ainoaa kriteeriä. Silmiinpistävä ulkoasu, kirjoitusvirheet ja liialliset mainokset ovat mahdollisia tekijöitä, jotka herättävät epäilyksen sivun aitoudesta. Osa haitallisista sivustoista voi myös pyytää käyttäjää lataamaan arveluttavia tiedostoja ja ohjelmia tai jakamaan henkilökohtaisia tietoja. Esimerkkitapauksessa sivusto pyytää päivittämään käyttäjän selaimen ja antaa sitä varten tiedoston ladattavaksi. Luonnollisesti päivitykset tulee aina tarkistaa selaimen alkuperäiseltä sivulta eikä tuntemattomasta lähteestä, joten tässä tapauksessa voi olettaa, että sivusto ei ole täysin luotettava.

Lyhennetyt osoitteet

Ajoittain saattaa törmätä lyhennettyihin nettisivujen osoitteisiin, joista voi olla hyötyä rajatun sanamäärän omaavissa palveluissa, kuten Twitterissä. Haittapuolena on kuitenkin epävarmuus siitä, mihin linkki oikeasti johtaa. (Goodchild, 2018.)



Kuva 7. Sucuri SiteCheck lyhennetylle osoitteelle (Sucuri SiteCheck).

Ajoittain linkin pystyy tarkastamaan pitämällä hiirtä painamatta linkin päällä. On olemassa myös ilmaisia URL-skannereita, joilla epäilyttävän linkin voi tarkistaa

ennen klikkaamista. Esimerkiksi Sucuri SiteCheckillä pystyy katsastamaan eri lyhennyspalveluiden linkit (Kuva 7.), kuten bit.ly ja TinyURL. Sen lisäksi, että sivusto paljastaa linkin kokonaisen osoitteen, se myös skannaa mahdollisten haittaohjelmien varalta. (Adweek 2013.)

5 DIGITAALINEN JALANJÄLKI

Kaikki verkossa tapahtuva toiminta jättää jälkeensä jäljen, joka voidaan yhdistää omaan netti-identiteettiin. Digitaaliset jalanjäljet jaetaan aktiivisiin ja passiivisiin tyyppeihin.

Aktiivinen digitaalinen jalanjälki perustuu kaikkeen, mitä tehdään verkossa oman tahdon mukaisesti. Esimerkiksi julkaisut eri sosiaalisen median palveluissa, kuten Twitterissä tai Facebookissa ovat osa aktiivista jalanjälkeä. Myös evästeiden salliminen selaimen pyytäessä lasketaan osaksi tätä kategoriaa.

Passiivinen digitaalinen jalanjälki tarkoittaa kaikkea, mitä jätetään jälkeen tiedostamatta. Nettisivut voivat esimerkiksi kerätä tietoja kirjautumisista palveluun tai asentaa evästeitä ilman lupaa. Jotkut sovellukset saattavat myös hyödyntää paikannusta ja päätellä käyttäjän sijainnin sen mukaan. Lisäksi kaikki kohdistetut mainokset, jotka perustuvat esimerkiksi Facebook-sivun tykkäyksiin kuuluvat passiiviseen kategoriaan. (Norton n.d.)

5.1 Sijainti

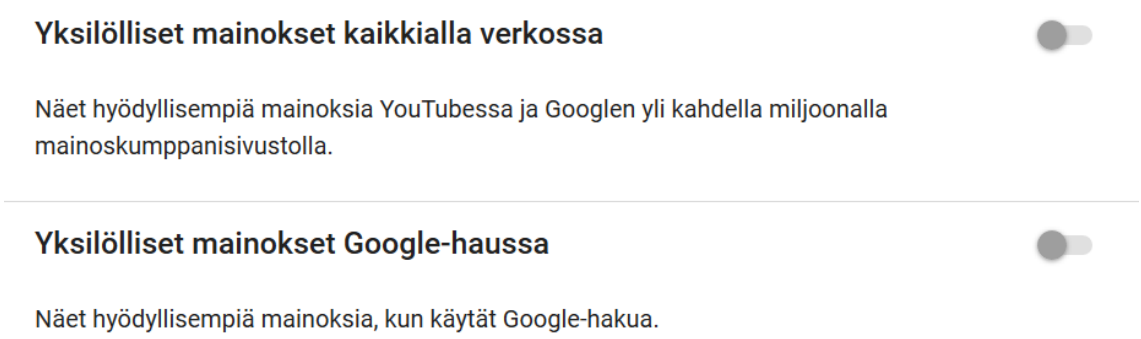
Mobiililaitteet usein automaattisesti ottavat talteen kuvan -tai videonottohetken tarkan sijainnin, ellei toimintoa ole asetettu pois päältä. GPS-koordinaatit on tallennettu kuvan metatietoon ja koneella niitä pystyy tarkastelemaan kuvan ominaisuuksista.

Sijainnin paljastaminen sosiaalisessa mediassa voi olla mittava riski, jos tieto joutuu väärien ihmisten käsiin. Tutuissa paikoissa käyminen ja niistä päivittäminen eri alustoilla antavat tarpeeksi informaatiota luoda kaavan päivittäin käydyistä paikoista, kuten vaikka koulu ja työpaikka. Jos väärä henkilö saa tietoonsa milloin ja mihin aikaan kohde ei ole kotona, antaa se mahdollisuuden esimerkiksi murtovarkauteen. (O’Donnell, 2018.)

5.2 Markkinointi

Markkinointi näkyy yksilöidyllä mainostuksella evästeitä hyödyntämällä. Käyttäjän vierailemat verkkokaupat, sivustojen tykkäykset Facebookissa jne. Kaikki toiminta antaa mahdollisuuden kerätä tietoja käyttäjän mieltymyksistä ja näin ollen kohdistaa mainokset sen mukaan. Myös käyttäjän sijaintitiedot voivat rajata mainoksia paikkakuntakohtaisesti. (Lee, 2018.)

Vaikka kaikki mainokset eivät välttämättä ole haitallisia, voivat ne silti herättää epämukavia tunteita varsinkin, jos ne sisältävät jotain arkaluontoisempaa, mitä ei halua ulkopuolisten nähtäville. Tietokoneen saattaa joutua esimerkiksi jakamaan perheen kesken tai tuntematon henkilö pystyy kurkkimaan olan yli julkisella paikalla. Osa mainoksista saattaa myös sisältää ääniä tai pongahtaa ruudulle huomiota herättävinä ponnahdusikkunoina, mikä voi häiritä entistä enemmän käyttäjän selaamista.



Kuva 8. Googlen mainosasetukset (Google).

Googlen mainosasetuksista on mahdollista laittaa yksilölliset mainokset kokonaan pois päältä (Kuva 8.). Huomioitavaa on kuitenkin se, että mainokset voivat silti muodostua esimerkiksi käyttäjän sijainnin tai sen hetkisen nettisivun sisällön mukaan. (Google n.d.)

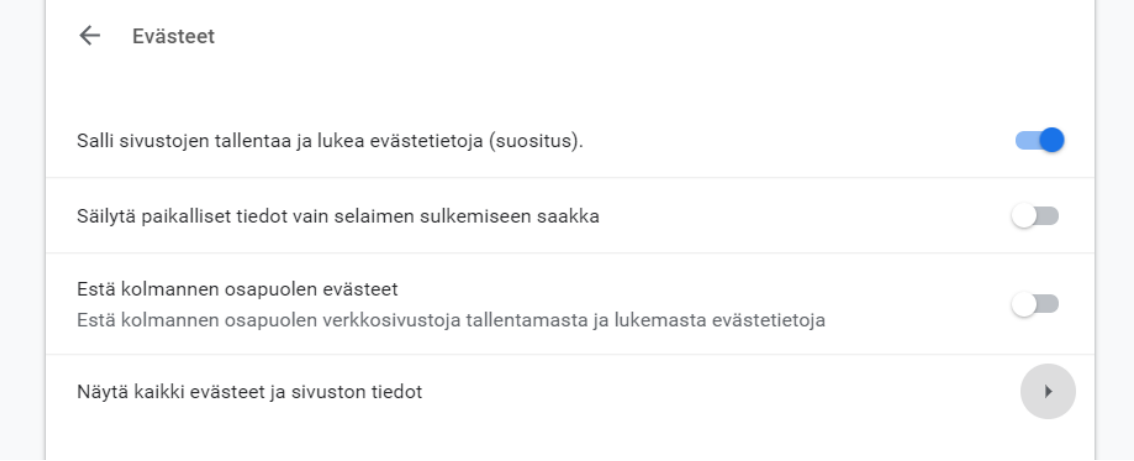
5.3 Evästeet

Evästeillä tarkoitetaan informaatiota, jonka tietokone vastaanottaa ja lähettää takaisin muuttamatta sitä. Nettisivu lähettää evästeitä koneelle kun sivustolla vierailaan ja näin ollen pitää kirjaa käyttäjän käynneistä ja toiminnasta. Evästeet varastoidaan omaan tiedostoonsa selaimeen.

Evästeet pystytään jakamaan istuntokohtaisiin ja pysyviin tyyppeihin. Istuntokohtaiset evästeet poistuvat automaattisesti väliaikaisesta muistista, kun käyttäjä on lopettanut sen hetkisen istunnon. Useat verkkokaupat esimerkiksi tallentavat ostoskorin sisällön, jolloin käyttäjän on helppo selata tuotteita ilman, että se nollaantuu kesken kaiken.

Pysyvät evästeet tallentuvat siihen asti, että ne manuaalisesti poistetaan, ellei niissä ole automaattista vanhenemispäivämäärää. Niiden käyttö perustuu käyttäjän kirjautumisten ja sivustoilla vierailujen tarkkailuun. Sivusto pystyy esimerkiksi ehdottamaan samanlaisia tuotteita tai palveluja, joita käyttäjä on aiemmin selaillut useita kertoja.

Kolmannen osapuolen evästeet liittyvät käyttäjän toiminnan jäljittämiseen esimerkiksi mainosten kautta. Sivustolla saattaa olla useita kolmannen osapuolen ylläpitämiä mainoksia, jotka saavat informaatiota samanaikaisesti, kun käyttäjät vierailevat kohdesivulla. (Kaspersky Lab n.d.) Sama pätee myös tykkäyspainikkeisiin, joita saa upotettua nettisivuille. Esimerkiksi Facebook saa jokaisesta tykkäyksestä tiedon siitä, millä sivulla käyttäjä on käynyt.



Kuva 9. Evästeasetukset Chromessa (Google Chrome).

Evästeiden käyttöä pystyy hallitsemaan useimmissa selainten asetuksissa (Kuva 9.). Kaikki sivustot eivät välttämättä kuitenkaan toimi virheettömästi, jos evästeet ovat kokonaan pois päältä.

6 ANONYYMIYS VERKOSSA

6.1 Incognito-tila

Incognito-tilalla tarkoitetaan yksityistä istuntoa, jolloin selaushistorian evästeet ja väliaikaistiedostot eivät tallennu. Chrome-selaimessa esimerkiksi toiminnon saa päälle oikean yläreunan painikkeesta ja klikkaamalla ”Uusi incognito-ikkuna”.

Incognito-tila ei salli täydellistä näkymättömyyttä. Internet-palveluntarjoaja ja nettisivustot pystyvät silti havaitsemaan käyttäjän toimintaa verkossa. Tästä huolimatta toiminto voi olla hyödyksi erityisesti, jos koneen joutuu jakamaan toisen ihmisen kanssa tai käytössä on vaikka kirjaston julkinen kone. Evästeiden poistuminen jokaisen istunnon jälkeen estää myös sivustoja muistamasta käyttäjän vierailuja.

6.2 Selainten liitännäiset

Liitännäiset voivat antaa lisäapua yksityisyyden varjelemiseen sekä erityisesti estämään sivustoja lähettämästä tietoja kolmansille osapuolille. Esimerkiksi jo aikaisemmin mainitut mainokset saattavat häiritä käyttäjän selaamista. Useisiin selaimiin on saatavilla mainoksenestoliitännäisiä, joiden tarkoituksena on juurikin hankkiutua mainoksista eroon ja myös estää evästeiden jäljittämisen.

Erilaiset jäljittämisenestoliitännäiset voivat myös antaa enemmän informaatiota sivuston käyttämistä ja keräämistä evästeistä. Halutessaan käyttäjä pystyy valitsemaan, mitä sivustolla on lupa tehdä datan keräämisen suhteen ja mitä ei.

Ennen liitännäisten asentamista on aina hyödyllistä tarkistaa, mitä oikeuksia sen käyttö todellisuudessa vaatii. Luotettavatkin liitännäiset saattavat ajan kuluessa muuttaa käytäntöjään, jos kehittäjä esimerkiksi myy sen eteenpäin toiselle yhtiölle. Lisäksi myös muiden käyttäjien arvostelut ja käyttökokemukset on hyvä ottaa huomioon, jos niitä on saatavilla.

6.3 VPN-yhteys

VPN tarkoittaa virtuaalista erillisverkkoa, joka sallii salatun yhteyden ja yksityisyyden verkossa. Näin ollen käyttäjän IP-osoite pysyy piilotettuna eikä verkossa tapahtuvaa toimintaa pysty yhtä helposti jäljittämään. Sen vuoksi VPN on hyödyllinen erityisesti julkista verkkoa käyttäessä.

Erilaisia VPN-palveluita on tarjolla lukuisia ilmaisista maksullisiin. Usein palvelut lupaavat käyttäjälle täyttä yksityisyyttä, mikä ei välttämättä pidä täysin paikkaansa. Osa palveluista kerää esimerkiksi informaatiota käyttäjän verkkotoiminnasta lokitiedostoihin, mikä voi herättää kysymyksiä toiminnan tarkoitusperästä. Vuosien aikana on ollut jopa tapauksia, joissa käyttäjien tietoja on myyty eteenpäin kolmansille osapuolille. Sen vuoksi on suositeltava lukea palvelun noudattama tietosuojakäytäntö tarkasti läpi ennen käyttöönottoa. (Charles, 2018.)

6.4 Sipulireititys

Sipulireititys tai lyhennettynä Tor on verkosto, jossa salattu liikenne kulkee useiden eri palvelimien kautta ilman, että sitä pystyy jäljittämään. Nimitys “sipulireititys” tulee siitä, että liikenteen salaus on luotu kerrosmaiseksi niin kuin sipulissa, joten käyttäjän identiteetti pysyy piilossa. Sen käyttöön vaaditaan Tor-selain, jonka saa asennettua ilmaiseksi. (Klosowski, 2014.)

Vaikka Tor voikin nostaa yksityisyyden tasoa verkossa, se ei tarkoita automaattisesti täyttä anonyymiyttä tai suojaa tietoturvariskeiltä. Selaimeen kohdistuvat hyökkäykset ovat edelleen mahdollisia, jos yhteys ei ole suojattu HTTPS-protokollalla. Taustalla pyörivät ohjelmat, kuten JavaScript ja ulkoiset liitännäiset voivat myös kerätä tietoja muille sivustoille ja paljastaa käyttäjän IP-osoitteen, jos niitä ei ole asetettu pois päältä. Sen vuoksi Tor-selaimessa riskialttiit ohjelmat ovat automaattisesti poissa käytöstä. (Hoffman, 2016.)

Mahdollisten riskien lisäksi Tor-selaimen käyttö voi olla suorituskyvyltään huomattavasti hitaampaa verrattuna muihin selaimiin.

7 LOPUKSI

Sosiaalinen media pitää sisällään paljon positiivisia asioita ja sille on syynsä, miksi se on suuren osan populaatiosta päivittäistä rutiinia. Monille se on keino pitää yllä ihmissuhteita eri puolilla maailmaa, toisille taas jakaa luovuutta eri muodoissa. Käytön syystä riippumatta on olennaista muistaa vastuuntunto ja oman järjen käyttö. Yhtä lailla kuin virtuaalisen maailman ulkopuolellakin, kukaan ei välttämättä lähtisi jakamaan aivan kaikkea itsestään esimerkiksi vastaantulevalle tuntemattomalle henkilölle.

Tietoturvariskejä on olemassa useissa eri muodoissa, eikä ole yhtä oikeaa tunnistavaa kriteeriä, mikä määrittää uhan olemassaolon. Kyky kuitenkin tunnustaa riskien mahdollisuus ja kriittinen suhtautuminen auttaa jo pitkälle. Jos jokin vaikuttaa epäilyttävältä tai liian hyvältä ollakseen totta, on todennäköisesti parempi luottaa vaistoihinsa.

Kaiken kaikkiaan suurin osa verkossa tapahtuva toiminta jättää jälkensä ja sitä on vaikea estää kokonaan. Suositeltavaa olisi ennen palveluihin rekisteröitymistä ottaa selville käytännöistä tietojen keräämisen ja käytön suhteen, vaikka edes pääpiirteittäin. Sama koskee myös yksityisyyden edistämiseksi kehitettyjä ohjelmia, mitkä voivat tuotteesta riippuen olla erittäin hyödyllisiä. Tutkimalla ja vertailemalla tuotteita ja niiden käyttöä vaativia ehtoja on olennaista ennen ostopäätökseen sitoutumista.

Täydellistä yksityisyyttä ei todennäköisesti ole olemassa sanan tarkoittamassa merkityksessä. Se ei kuitenkaan tarkoita, etteikö käyttäjä voisi omalla toiminnallaan edistää sitä parempaan suuntaan.

LÄHTEET

Rousku, K. 2014. Kyberturvaopas: Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Järvinen, P. 2012. Arjen tietoturva: Vinkit ja ratkaisut. Jyväskylä: Docendo.

Cross, M. 2013. Social Media Security: Leveraging Social Networking While Mitigating Risk. William Andrew.

Taylor, A. Alexander, D. Finch, A. & Sutton, D. 2013. Information Security Management Principles. 2. BCS Learning & Development Limited.

Vacca R. J. 2012. Computer and Information Security Handbook. 2. Elsevier Science & Technology.

Adweek, 2013. 5 Threats To Your Security When Using Social Media. Viitattu 14.11.2018.

https://www.adweek.com/digital/5-social-media-threats/

Allen Z. 2017, ZeroFOX. Fake Mother's Day Scam Coupons Spread Across Social Media. Viitattu 14.11.2018.

https://www.zerofox.com/blog/fake-mothers-day-coupons-spread-across-social-media/

BBC. 2018. Twitter: Fake Elon Musk scam spreads after accounts hacked. Viitattu 14.11.2018.

https://www.bbc.com/news/technology-46097853

Chaffey, D. 2018. Global social media research summary. Smartinsights. Viitattu 3.11.2018.

https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Charles. 2018. Are VPNs truly untraceable and anonymous? The VPN Guru. Viitattu 25.11.2018

https://thevpn.guru/is-vpn-untraceable/

Cisco. n.d. What is phishing? Viitattu 14.11.2018

https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

Facebook. Tietokäytäntö. Päivitetty 19.4.2018. Viitattu 10.11.2018.

https://www.facebook.com/policy.php

Finlex. Henkilötietolaki 22.4.1999/523. Viitattu 3.11.2018.

https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Goodchild J. 2018, SecurityIntelligence. What are the Seven Biggest Social Media Scams of 2018? Viitattu 14.11.2018.

https://securityintelligence.com/what-are-the-seven-biggest-social-media-scams-of-2018/

Google. n.d. Check if your Gmail message is authenticated. Viitattu 18.11.2018.

https://support.google.com/mail/answer/180707?co=GENIE.Platform%3DAndroid&hl=en

Hoffman, C. 2016. Is Tor Really Anonymous and Secure? How-To Geek. Viitattu 18.11.2018.

https://www.howtogeek.com/142380/htg-explains-is-tor-really-anonymous-and-secure/

Kaspersky Lab. n.d. What Are Cookies? Viitattu 18.11.2018.

https://www.kaspersky.co.uk/resource-center/definitions/cookies

Klosowski T. 2014, Lifehacker. What Is Tor and Should I Use It? Viitattu 18.11.2018.

https://lifehacker.com/what-is-tor-and-should-i-use-it-1527891029

Lifelock. n.d. Identity Theft. Viitattu 14.11.2018.

https://www.lifelock.com/how-it-works/what-is-identity-theft/

O'Donnell A. 2018, Lifewire. Why Sharing Your Location on Social Media Is a Bad Thing. Viitattu 14.11.2018.

https://www.lifewire.com/why-sharing-your-location-on-social-media-is-a-bad-thing-2487165

Lee L. 2018, EnVeritas Group. Every Move You Make... I'll Be Watching You: How Personalized Ads Work. Viitattu 17.11.2018.

https://enveritasgroup.com/campfire/why-am-i-seeing-this-ad-how-personalized-ads-work/

Norton. n.d. Symantec Corporation. The risks of public Wi-Fi. Viitattu 14.11.2018.

https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

Norton. n.d. Symantec Corporation. Spam, spam, go away. Viitattu 14.11.2018.

https://us.norton.com/internetsecurity-how-to-spam-spam-go-away.html

Norton. n.d. Symantec Corporation. What is a digital footprint? And how to help protect it from prying eyes. Viitattu 14.11.2018.

https://us.norton.com/internetsecurity-privacy-clean-up-online-digital-footprint.html

Norton. n.d. Symantec Corporation. What are cookies? Viitattu 14.11.2018.

https://us.norton.com/internetsecurity-how-to-what-are-cookies.html

Rouse, M. 2016. Information Security (infosec). SearchSecurity. Viitattu 3.11.2018.

https://searchsecurity.techtarget.com/definition/information-security-infosec

Rouse, M. 2017. Spear phishing. SearchSecurity. Viitattu 14.11.2018

https://searchsecurity.techtarget.com/definition/spear-phishing

The OWASP Foundation. Phishing. Päivitetty 30.6.2018. Viitattu 14.11.2018.

https://www.owasp.org/index.php/Phishing

Tietosuojavaltuutetun toimisto. n.d. Tietosuoja. Viitattu 18.11.2018.

https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto. n.d. GDPR. Viitattu 18.11.2018.

https://tietosuoja.fi/gdpr

Viestintävirasto. Tietoturva käytännössä. Päivitetty 10.5.2017. Viitattu 3.11.2018.

https://www.viestintavirasto.fi/fiverkkotunnus/tietoavalittajalle/valitystoiminnantietoturva/tietoturvakaytannossa.html

Viestintävirasto. Verkkojen ja palvelujen tietoturva. Päivitetty 29.5.2018. Viitattu 3.11.2018.

https://www.viestintavirasto.fi/ohjausjavalvonta/tekninentoimivuusjatietoturva/tietoturva.html

Viestintävirasto. Kaksivaiheinen tunnistautuminen pelastaa paljolta – pelkkä salasana ei suojaa kaikilta uhkilta. Päivitetty 30.8.2017. Viitattu 18.11.2018.

https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/08/ttn201708301327.html

Whittaker Z. 2018, ZDNet. Yet again, Google tricked into serving scam Amazon ads. Viitattu 14.11.2018.

https://www.zdnet.com/article/scammers-tricked-google-into-posting-amazon-scam-ads/