EU:n tietosuoja-asetus eli GDPR kuluttajan kannalta

Digisaurukset-verkoston seminaari

11.6.2024 klo 12.30–16.30

Paula Miinalainen
Oy Arbor Vitae – Finland LTD

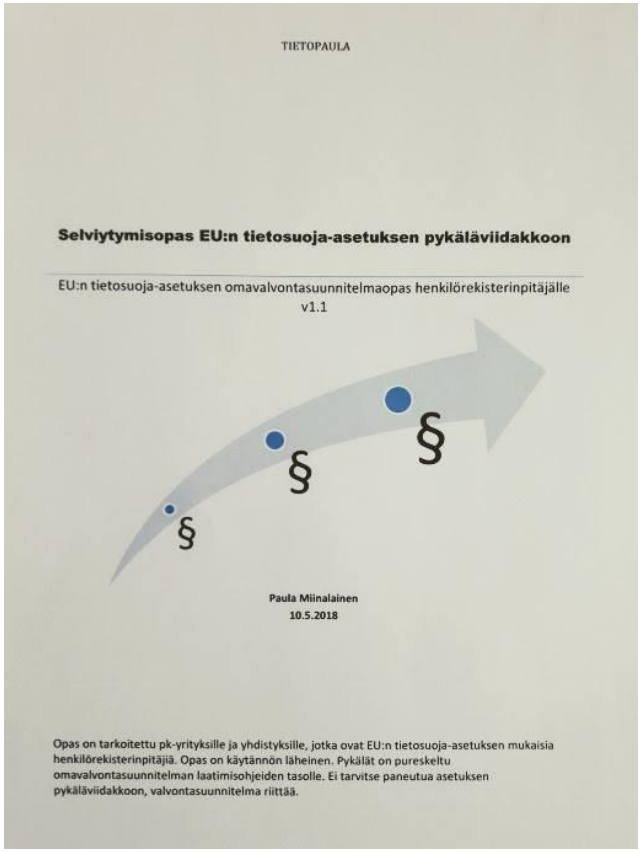
EU:n henkilötietosuoja-asetus (GDPR = General Data Protection Regulatio)

ASTUI VOIMAAN 25.5.2016

SANKTIOT ASTUIVAT VOIMAAN 25.5.2018

TIETOSUOJALAKI ASTUI VOIMAAN 1.1.2019 JA KUMOSI HENKILÖTIETOLAIN.

eKirja Holvissa saatavissa
https://holvi.com/shop/TietoPaula/



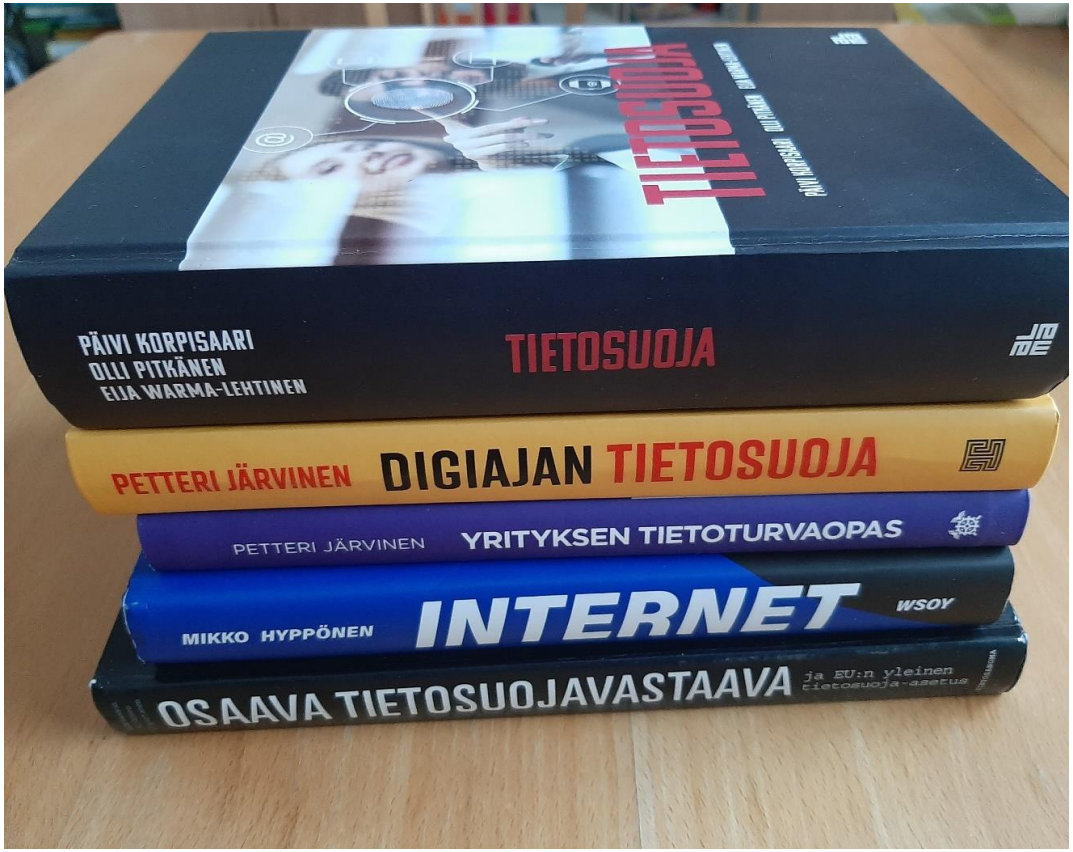
eKirja
Holvin verkkokaupasta:

https://holvi.com/shop/TietoPaula/

1 EU:n tietosuoja-asetuksen (GDPR) tarkoitus pähkinänkuoressa
2 Peruskäsitteet
3 Rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet
4 Tietosuojaseloste
5 Kumppanisopimukset
6 Rekisterien käsittelykuvaukset
7 Henkilöstön ohjeistus
8 Tietovuodon sattuessa
9 Esimerkki omavalvontasuunnitelman sisällysluettelosta

Paulan omasta hyllystä

Paulan omasta hyllystä



Ketä EU:n henkilötietosuoja-asetus koskee?

Tämä koskee kaikkia EU:n alueella toimivia organisaatioita, jotka

- keräävät
- tallentavat
- käyttävät henkilötietoja.

B2C , ei koske B2B

Henkilötietoja (personal data) ovat

Nimi

Osoite

Sähköpostiosoite

Sijaintitiedot

Verkkotunnistetiedot

Terveystiedot

Tulot ym. raha-asiat

Kulttuurinen profiili

Mitä yrityksen on tehtävä?

Suojeltava niiden ihmisten oikeuksia, jotka luovuttavat tietojaan.

”Luotava tietojenkäsittelyn suojatiet.”

Luotava vapaa tiedonkulku EU:n alueella.

Samat säännöt kaikille yrityksille, jotka käsittelevät henkilötietoja EU:ssa.

Peruskäsitteet

Rekisterinpitäjä (controller) on organisaatio, joka yksin tai yhdessä toisen tahon kanssa määrää henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity (data subject) on luonnollinen henkilö

Käsittelijä (processor) on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (esimerkiksi atk-palvelun toimittaja, joka tuottaa rekisterin atk-käsittelyn).

Rekisteri (filing system) on mikä tahansa jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein (voi olla hajautettu, keskitetty tai jaettu).

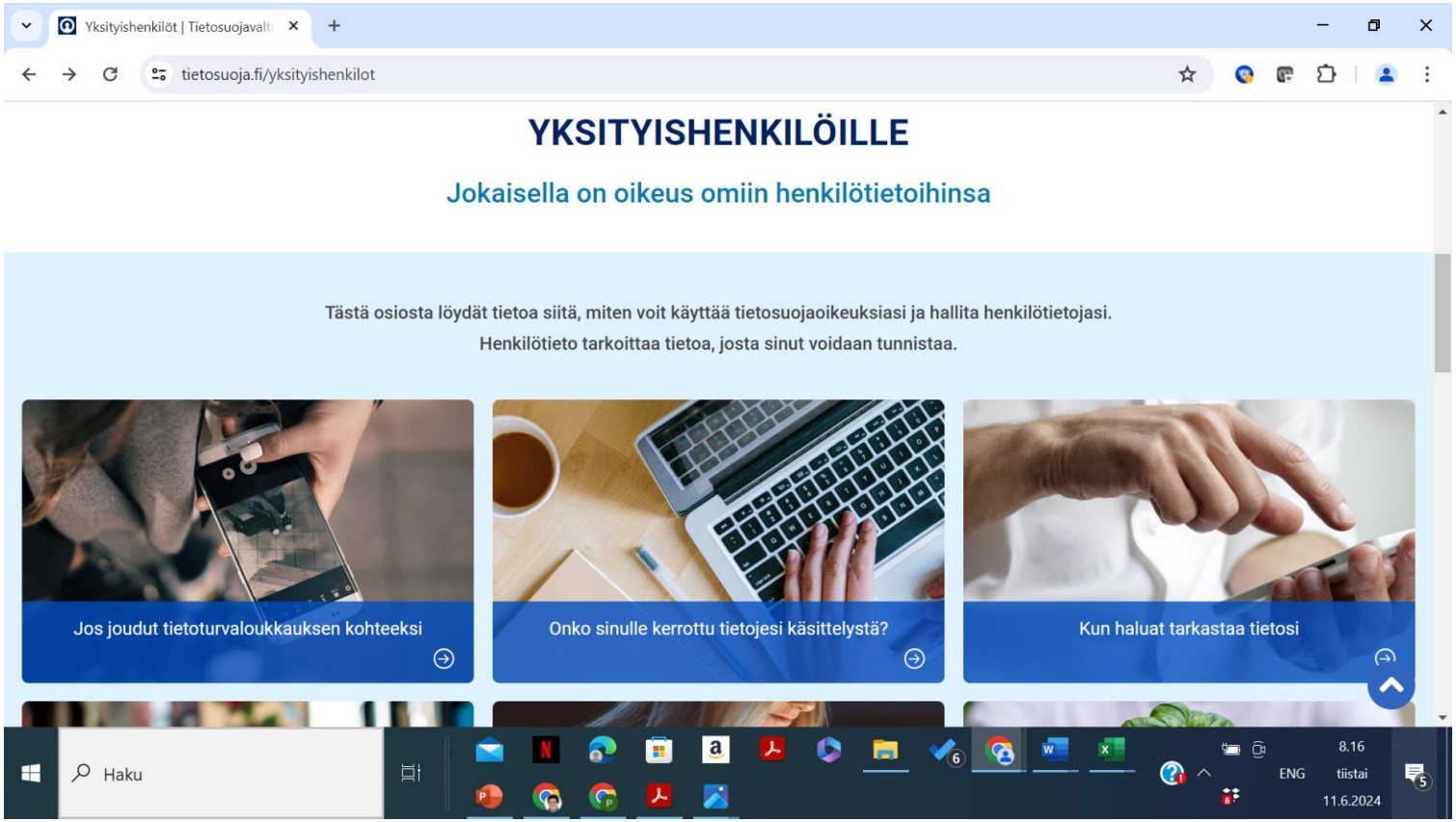
Suostumus (consent) on mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojen käsittelyn.

Tietosuojavaltuutetun toimisto valvoo tietosuojaoikeuksiasi

Tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista.

Tietosuojavaltuutetun Anu Talaksen ja kahden apulaistietosuojavaltuutetun lisäksi toimistossa työskentelee noin 55 asiantuntijaa.

https://tietosuoja.fi/yksityishenkilot



Henkilön oikeus omiin tietoihinsa eli rekisteröidyn oikeudet

Oikeus **tarkastaa** omat tietonsa.

Oikeus **pyytää korjausta** tietoihinsa.

Oikeus **vaatia tietojensa poistamista** ts. vaatimus tulla unohdetuksi.

Oikeus **kieltää suoramarkkinointi** tai rajoittaa kiistanalaisten tietojen käsittelyä kunnes asia saadaan ratkaistua.

Rekisteröidyn oikeudet

Oikeus **siirtää tiedot** johonkin toiseen järjestelmään, silloin kun tiedot ovat rekisteröidyn itsensä toimittamia ja tietojen käsittely perustuu suostumukseen tai sopimukseen.

Oikeus vastustaa henkilötietojensa käsittelyä, jos on sitä mieltä, että tietoja on käsitelty lain vastaisesti tai rekisterinpitäjällä ei ole oikeutta käsitellä niitä.

Oikeus tehdä valitus henkilötietojensa käsittelystä valvontaviranomaiselle.

Tekoäly

Jos on käytetty profilointia oikeudellisesti velvoittavien sopimusten (esim. lainat) hakemusten käsittelyyn, sinun on

Saatava tietää siitä.

Jos hakemukseesi vastataan kielteisesti, niin sinä voit varmistaa, että päätöksen on tarkistanut ihminen eikä kone.

Sinulla on oikeus riitauttaa päätös.

Yhteys rekisterinpitäjään – käytä oikeuksiasi!

Reksiterinpitäjän yhteystiedot ovat tietosuojaselosteessa kohdassa yhteyshenkilö.

Toimi selosteessa olevien ohjeiden mukaan ja pyydä tietojen tarkistusta, korjausta, poistamista, siirtämistä toiseen järjestelmään.

Voit myös vastustaa, jos tietojasi käytetään lainvastaisesti tai rekisterinpitäjällä ei ole oikeutta käsitellä niitä.

Rekisterinpitäjä on velvollinen vastaamaan sinulle 30 päivän kuluessa. Jos pyyntö on hankala toteuttaa, niin rekisterinpitäjä voi pyytää 2 kuukautta lisä aikaa.

Ilmoita tietosuojavaltuutetulle

Jos epäilet, että jokin organisaatio tai henkilö käsittelee henkilötietoja tietosuojasäännösten vastaisesti.

Epäkohta voi tarkoittaa esimerkiksi, että

henkilötietojen käsittelylle ei ole lainmukaista perustetta tai

henkilötietoja käsitellään liian laajasti käsittelyn tarkoitukseen nähden.

Ilmoituksen voi tehdä Tietosuojavaltuutetun toimiston sivuilla olevalla lomakkeella.

Ota kuitenkin ensin yhteyttä reksiterinpitäjään selvittääksesi asian, *jos rekisterinpitäjä kieltäytyy pyynnöstäsi eikä kieltäytymiselle ole mielestäsi perusteita, niin tee ilmoitus tietosuojavaltuutetulle.*
Tietosuojavaltuutettu ei lähtökohtaisesti ota kantaa sellaisiin tapauksiin, joissa rekisterinpitäjään ei ole oltu itse yhteydessä.

Asia kuulukin poliisille, tuomioistuimelle, Traficomille?

Jos epäilet, että asiassa on tapahtunut sinuun kohdistuva rikos (kunnianloukkaus, petos, salakuuntelu tai -katselu, yksityiselämää loukkaavan tiedon levittäminen tms.), ole ensisijaisesti yhteydessä **paikalliseen poliisiin**. Tietosuojavaltuutettu voi siirtää asian poliisin käsiteltäväksi, mutta se ei yleensä ole kannaltasi nopein vaihtoehto.

Tietosuojavaltuutettu ei toimi asiamiehenä eikä esimerkiksi voi vaatia vahingonkorvausta puolestasi. Yksityisoikeudelliset vaatimukset esitetään **tuomioistuimille**.

Evästeitä koskevat kysymykset (esimerkiksi milloin evästeitä saa tallentaa käyttäjän päätelaitteelle ja miten käyttäjä voi antaa suostumuksensa evästeiden tallentamiselle ja käytölle) ja evästeitä koskevan sääntelyn tulkitseminen ja noudattamisen valvonta kuuluu Liikenne- ja viestintävirasto Traficomille. Evästeisiin liittyvän valituksen voit osoittaa **Traficomille.**

Vastaamo lähes 40 000 potilaan henkilötiedot murrettu

Turvajärjestelmässä oli puutteita.

Pääkäyttäjälle ei oltu asennettu salasanaa. Kun muutti ilman kontrollia peruskäyttäjän pääkäyttäjäksi saattoi tehdä rajattomasti asioita. Käytäntö ollut näin vuodesta 2012.

Palomuuri oli asennettu väärin ja se päästi kaiken liikenteen läpi.

Potilaskantta ei ollut anonymisoitu.

Vuonna 2019 oli tapahtunut tietomurto, jonka tj. Ville Tapio salasi eikä ryhtynyt toimiin asian korjaamiseksi.

Henkilökunnan perehdytys ja koulutus olivat riittämättömiä.

Omavalvonta oli puutteellista. Toiminta oli tahallista ja huolimatonta.

Syyttäjä vaati tj. Ville Tapiolle vankeutta, koska oli syyllistynyt tietosuojarikokseen.

Vastaamo konkurssiin

Vastaamon osalta oli epäselvyyksiä, koska oli tehty yrityskauppa, vaikka tiedossa oli tapahtunut tietomurto.

Epäselvyydet ja maineen menetys johtivat konkurssiin.

Vastaamon tj Ville Tapio

Yle uutiset:

Tj Ville tapio tuomittiin 18.4.2023 käräjäoikeudessa 3 kk:n ehdolliseen vankeusrangaistukseen tietosuojarikoksesta, koska pseudonymisointi ja salaus puuttuivat.

Poliisi epäili myös it-työntekijöitä, mutta poliisi ei nostanut syytettä.

Vastaamon tietomurron uhrien oikeudet

Psykoterapiakeskus Vastaamon tietomurtojutussa on noin 33 000 uhria.

Keskusrikospoliisin tiedote 26.4.2023
Uhreilla on 30.5.2023 asti aikaa tehdä rikosilmoitus ja täyttää poliisin sivuilla oleva lomake.

Vastaamon tietomurron tekijä

Aleksanteri Kivimäki (26 v) on vangittuna epäiltynä kiristyksestä-

Kivimäki tuomittiin kuuden vuoden ja kolmen kuukauden ehdottomaan vankeusrangaistukseen yli 30 000 rikoksesta. Hänen syykseen luettiin törkeä tietomurto, törkeän kiristyksen yritys, 9 231 törkeää yksityiselämää loukkaavan tiedon levittämistä, 20 745 törkeän kiristyksen yritystä ja 20 törkeää kiristystä.

Kivimäki valittaa tuomiosta.

Helsingin kaupungin tietomurto

Keskusrikospoliisi ja poliisi tutkii törkeänä murtona.
Helsingin kaupunki on tehnyt asiasta rikosilmoituksen.

Murron kohteeksi joutuneiden ei tarvitse tehdä mitään.

Mitä tapahtui?

Helsingin kaupunki havaitsi tietomurron varhaiskasvatuksen ja koulutuksen toimialueellaan 30. huhtikuuta 2024.

Tietomurrossa hyödynnettiin etäkäyttöpalvelimen haavoittuvuutta, jota ei ollut päivitetty huolimatta saatavilla olleesta korjauspäivityksestä.

Hyökkääjä pääsi käsiksi kymmeniin miljooniin tiedostoihin, joista osa sisälsi arkaluontoista tietoa, kuten henkilötunnuksia, osoitteita, ja sähköpostiosoitteita.

Näitä tietoja verkkolevyllä

•Lapsen ja huoltajan henkilötunnukset.
•Lapsen ja huoltajan osoitetiedot (ei puhelinnumeroita, ei sähköpostiosoitteita). Turvakiellon alaisista henkilöistä ei osoitetietoja, puhelinnumeroita tai sähköpostiosoitteita.
•Lapsen äidinkieli.
•Lapsen kansalaisuus.
•Lapsen uskontokunta (tarkkuudella ev.lut. / ortodoksi / rekisteröity uskonnollinen yhdyskunta / uskontokuntaan kuulumaton).
•Mahdollisesti Santahaminan varuskunta-alueen päiväkodissa, leikkipuistossa ja koulussa vierailleiden kulkulupatietoja on saattanut päätyä tietomurron tekijälle.
•Tiedoissa saattaa olla ulkomaalaistaustaisten perheiden passinumeroita.

Lähde: Helsingin kaupunki

Mitä tiedoille tapahtuu?

Lähde: F-Secure

”Tällaiset varastetut tiedot ovat käyttökelpoisia rikollisille”, sanoi F-Securen kyberuhkatiedustelupäällikkö, Laura Kankaala.

”Niistä koostettuja sähköpostilistoja myydään tai jaetaan ilmaiseksi internetissä. Niiden avulla voi vähintäänkin kohdentaa roskapostia ja tietojenkalastelua.

Emme ole kuitenkaan vielä huomanneet, että näitä varastettuja tietoja olisi vielä julkisesti saatavilla. Suomessa on onneksi viime vuosina tehty henkilötunnusten väärinkäyttämisestä hankalampaa. Niitä voidaan silti edelleen käyttää joissain internetmaksutapahtumissa.”

Pimeä verkko
Dark web

Käyttäjät voivat toimia anonyymisti ja salatusti.

Voi viestiä suojassa seurannalta ja sensuurilta anonyymisti.

Takaa sananvapauden, vaikka internetin käyttöä rajoitettaisiin.

Pimeä verkko on täysin laillinen useimmissa maissa.

Koska mahdollistaa anonymiteetin, niin mahdolllistaa myös laittoman toiminnan.

Pimeän verkon sisältöesimerkkejä

- Huumeiden, dopingaineiden, aseiden ja muiden laittomien tuotteiden kauppa.
- Varastettujen henkilötietojen ja luottokorttien myynti.
- Ransomware-as-a-Service (RaaS) -palveluiden ja haittaohjelmien myynti.
- Keskustelufoorumit, joilla käyttäjät voivat ilmaista mielipiteensä anonyymisti.
- Itsenäiset ja poliittisesti sitoutumattomat uutissivustot.
- Verkossa luettavat lehdet ja kirjat.
- Lapsiin kohdistuva seksuaalinen materiaali.

Lähde: F-Securen sivut 9.6.2024

Tor-selain eli The Onion Router

Suunniteltu pimeän verkon käyttöä varten.

Pimeään verkkoon meneminen on laillista.

Pimeän verkon käyttö on turvallista, koska laitonta sisältöä on vaikea löytää, sillä osoitteet ovat kryptisiä ja niitä ei löydä tavallisilla hakukoneilla.

Kehitetty 1990-luvulla USA:n hallinnon käyttöön. CIA:n agentit voivat viestiä keskenään suojatusti.

Tuli tavallisten internetin käyttäjille 2000-luvun alussa ja mahdollisti tavallisten ihmisten internetin käytön anonyymisti.

Laajeni rikolliseen käyttöön.

Avoin, syvä ja pimeä verkko

Avoin: Kaikille avoin osa internettiä, jonka sivuja voi käyttää verkkoselaimilla kuten Chromella, Explorerilla ja Firefoxilla. Tähän ei kuulu julkiselta käytöltä piilotetut sivut.

Syvä: Kirjautumista vaativat intranet-sivut, verkkopankit sekä yksityiset foorumit. Pimeä verkko on osa syvää verkkoa.

Pimeä: Ei pääse tavallisilla verkkoselaimilla.

Pysy turvassa internetissä

Lähde: F-Securen sivut 9.6.2024

Käytä VPN-palvelua. VPN piilottaa IP-osoitteesi ja auttaa sinua käyttämään internetiä yksityisesti. Suojatun yhteyden ansiosta verkkorikollisten on vaikeampi seurata toimiasi verkossa. Muista kuitenkin olla varovainen, sillä VPN ei suojaa sinua kaikilta verkon uhkilta tai tee pimeän verkon käyttämisestä turvallista.

Käytä virustorjuntaohjelmaa. Pimeä verkko on täynnä viruksia ja haittaohjelmia, eikä VPN tarjoa riittävää suojaa niitä vastaan. Hanki jokaiselle laitteellesi kattava virusturva, käytitpä pimeää verkkoa tai tavallista internetiä.

Varo verkkohuijauksia. Erikoinen sähköposti tuntemattomasta osoitteesta tai viesti, joka vaikuttaa tulevan ystävältäsi voi olla peräisin pimeässä verkossa myydystä varastetusta sähköpostiosoitteesta.

Älä käytä samaa salasanaa kahdesti. Verkkorikolliset voivat päästä käsiksi kerralla useammalle tunnuksellesi, mikäli käytät samaa salasanaa usealla eri tunnuksella ja kirjautumistietosi päätyvät pimeään verkkoon. Voit estää tätä tapahtumasta käyttämällä uniikkeja ja vahvoja salasanoja. Salasanojenhallintatyökalu tekee erilaisten salasanojen käyttämisestä helpompaa sen sijaan, että sinun pitäisi muistaa niistä jokainen ulkoa.

Älä jätä laitteitasi vartioimatta. Pidä hyvää huolta laitteistasi erityisesti julkisilla paikoilla. Älä myöskään lainaa laitteitasi kenellekään, ketä et tunne.