MATKAPUHELIMEN TURVALLINEN KÄYTTÖ

4.10.2022

Henri Brandt
Dark Amber Softworks

(Kuva: Pexels.com.) Mikä tässä kuvassa on pielessä?

KYBERTURVAN ABC YRITTÄJILLE

XAMK Kaakkois-Suomen ammattikorkeakoulu
Euroopan unioni Euroopan sosiaalirahasto
Vipuvoimaa EU:lta 2014–2020
Elinkeino-, liikenne- ja ympäristökeskus

Miksi?

Tietoturvassa ei ole kyse pelkästään haittaohjelmista.
Turvallisuus (verkkoympäristöissä) on **asenne ja tapa toimia.** Se ei ole ainoastaan mekanismeja tai laitteita.

Kaikkein suurin riskitekijä on minkä tahansa verkkoon kytketyn laitteen **käyttäjä.**

Riskinottokyky. Kuinka paljon olet valmis häviämään?

Mobiililaite kulkee mukana kaikkialle. Se ei ole **“pelkästään” puhelin**.

Mobiililaitteiden mukana kulkee paljon **henkilökohtaista tietoa** (maksukortti, terveystietoja, henkilökohtaisia preferenssejä, perheenjäsenten tietoja)
ja yrityksen omistamassa puhelimessa on lisäksi yritykseen toimintaan liittyviä tietoja, jopa **liikesalaisuuksia** ja salassapidettäviä tietoja (asiakkaat)**.**

Matkapuhelin on muuttunut digitaaliseksi assistentiksi, jolla tehdään aivan kaikkea, esimerkiksi verkko-ostaminen kännykällä on ollut jyrkässä nousussa jo pari vuotta.

Nykyään puhelimella hoidetaan samat asiat kuin tietokoneella; teet ostokset, luet sähköpostit, maksat laskut, käytät some-tilejäsi ja tallennat luottamuksellisia tietoja laitteen muistiin. Usein kuitenkin unohtuu, että puhelinta käyttäessä on samat tietoturvauhat kuin tietokoneellakin.

Tietoturva-sovellus tulisi erityisesti asentaa Android-laitteisiin, sillä Android on mobiilikäyttöjärjestelmistä ylivoimaisesti haavoittuvin.

Tyypilliset puhelinuhat

Jos jokin on liian hyvä ollakseen totta, silloin se luultavimmin ei ole totta.
*Jos se on ilmaista, silloin **sinä olet se myytävä tuote.***

Huijausviestit

- Posti/DHL/Amazon/Pankki. Suojautuminen on suhteellisen helppoa.
  Älä avaa niitä viestejä tai älä ainakaan klikkaa mitään **linkkejä**, joita niissä on.

95% ihmisistä avaa tekstiviestin keskimäärin alle 3 minuuttia sen saapumisen jälkeen. Tämän takia ns. “smishing” (SMS + fishing) eli tietojenkalastelu tekstiviesteillä on nousussa.

Sovellusten/appien oikeudet

- Sovellus/appsi haluaa täyden pääsyn osoitekirjaan, mikrofoniin, paikannustietoihin ja viesteihin.

Harmittoman näköinen mobiilipeli saattaa kerätä taustalla käyttäjän tietoja ja vuotaa niitä rikollisille tahoille, tai lukita koko laitteen ja esittää lunnasvaatimuksen. Varsinkin Android-laitteisiin on syytä hankkia kunnollinen tietoturvaratkaisu.

Maalaisjärjen puute

Ruotsalainen ministeri huusi työpuhelimeensa taksijonossa ennen Nato-hakemuksen jättämistä, että nyt ne suomalaiset hakee ja meidän on pakko hakea kanssa. Toimittaja seisoi samassa jonossa kuuntelemassa keskustelua.

Perheen lapset asentelevat työpuhelimiin ihan mitä sattuu.

Puhelimessa on sovellus, jossa on esimerkiksi koko yrityksen asiakasrekisteri, mutta puhelimessa itsessään ei ole edes pääsykoodia.

Suomessa mobiiliverkot (4G, 5G) ovat maailman mittapuun mukaan hyviä.
Mobiili(data)verkot ovat pääasiallisesti turvallisia tavallisen käyttäjän kannalta.

Ulkomailla, varsinkin Euroopan ulkopuolella, saattaa tulla houkutus käyttää **ilmaisia WiFi-verkkoja**. Kirjautuminen näihin verkkoihin yleensä vaatii sähköpostiosoitteen antamisen. Voin taata, että jos näin tekee, niin sähköposti on sen jälkeen täynnä spämmiä.
Jos ei mitään muuta mahdollisuutta ole, tee itsellesi “ylimääräinen” Gmail-osoite ennen reissua, vaikka tekaistulla nimellä, ja käytä sitä.
Tämä ei poissulje sitä, että mobiililaitteesi on tämän jälkeen mahdollisesti korkattu.

Sosiaalinen media ja Google

Jenni ostaa kengät verkkokaupasta. Verkkokauppa jakaa tämän tiedon Facebookille. Facebook tallentaa tiedon Facebookin ulkopuolella tehtyjen toimintojen kansioon. Nyt Facebook tietää, että Jenni vieraili verkkokaupassa ja että Jenni teki ostoksen verkkokaupassa. Myöhemmin Jenni näkee mainoksen 10 prosentin alennuksesta kyseessä olevaan verkkokauppaan.

Facebookin keräämän tiedon määrä on valtava. Nyt Facebook dumppaa tiedot käyttäjän syliin ja toteaa, että päättele siitä, millä tolalla tietosuojasi on.

Koko kuva muuttuu, kun ihmisen Tinder-selailut ja taksimatkat yhdistetään tapahtumiin, joihin hän on ilmoittanut osallistuvansa Facebookissa.
(“Minulla ei ole mitään salattavaa…”)

Tietojen poistaminen ei kuitenkaan tarkoita, että sovellukset ja sivustot lopettaisivat tietojen jakamisen Facebookille. Tämä jatkuu halusit tai et.

Sen sijaan voit säätää tilisi asetuksia niin, että jatkossa Facebookin ulkopuolisista tekemisistäsi kerättyjä tietoja ei yhdistetä sinun tiliisi. Tiedot kerätään, mutta niitä ei käytetä mainosten kohdistamiseen, sinulle.

Facebook-tilin poistaminen ei myöskään lopeta tietojen keräämistä. Silloin Facebook vain luo sinusta varjoprofiilin. Ja sen profiilin tietoja sinulla ei ole oikeus hallinnoida senkään vertaa.

Ainoa tapa välttää Facebookin ja/tai Googlen seuranta, on lopettaa internetin käyttö.

Voit tarkistaa omat tietosi:
https://myactivity.google.com/
https://www.facebook.com/your_information

Perusasioita

ANDROID

- Osta puhelin luotettavalta valmistajalta ja pidä puhelin ajan tasalla päivitysten osalta.
- Älä tallenna kaikkia salasanoja puhelimeen. Harkitse salasanojen hallintasovellusta.
- Tarkista mitä oikeuksia sovelluksilla on.
- Käytä 2-vaiheista tunnistusta.
- Androidiin on rakennettu turvallisuusominaisuuksia. Käytä niitä.
- Pidä huolta, että WiFi verkko, johon olet kytkeytynyt on turvallinen. (Kenelle muuten annat kotiverkon salasanan?)
- Käytä Androidin turvallisuussovelluksia.
- Ota varmuuskopio myös puhelimestasi esimerkiksi Google Driveen.
- Hanki sovellukset ainoastaan Google Play'sta.
- Kryptaa puhelimesi ja vaihda salasanasi säännöllisesti.
- Käytä VPN:ää (Virtual Private Network) Selitys täältä: https://fi.wikipedia.org/wiki/VPN

IPHONE

- Pidä käyttöjärjestelmä ajan tasalla.
- Aktivoi "Find my iPhone" -ominaisuus.
- Tee laitteen pääsykoodista pidempi kuin pakollinen 4-numeroinen.
- Käytä 2-vaiheista tunnistusta.
- iPhonessa on ominaisuus, jonka avulla laitteen tiedot saa automaattisesti tuhottua, jos pääsykoodi näppäillään väärin 10-kertaa.
- Vaihda säännöllisesti salasanasi. Käytä Apple Keychain Access -ohjelmaa.
- Pidä huolta, että WiFi verkko, johon olet kytkeytynyt on turvallinen.
- Poista mahdollisuus käyttää Siriä lukitulta näytöltä.
- Älä anna sovellusten käyttää kameraa, mikrofonia tai paikannusta, jos ne eivät sitä tarvitse. Jos tarvitsevat, salli ainoastaan "*käytettäessä*".

https://fi.wizcase.com/blog/parasta-ilmaista-virustorjuntaa-androidille/ (Linkki)

Identiteettivarkaus on yksi viheliäinen seuraus huonosta tietoturvasta.
Yksityiselle henkilölle se tarkoittaa hirveästi työtä ja mahdollisesti rahallista menetystä.
Apua kuitenkin löytyy ja yleensä ymmärrystä viranomaisilta.

Yksityisyrittäjä on yleensä hyvin yksin tällaisten tapauksien kanssa.

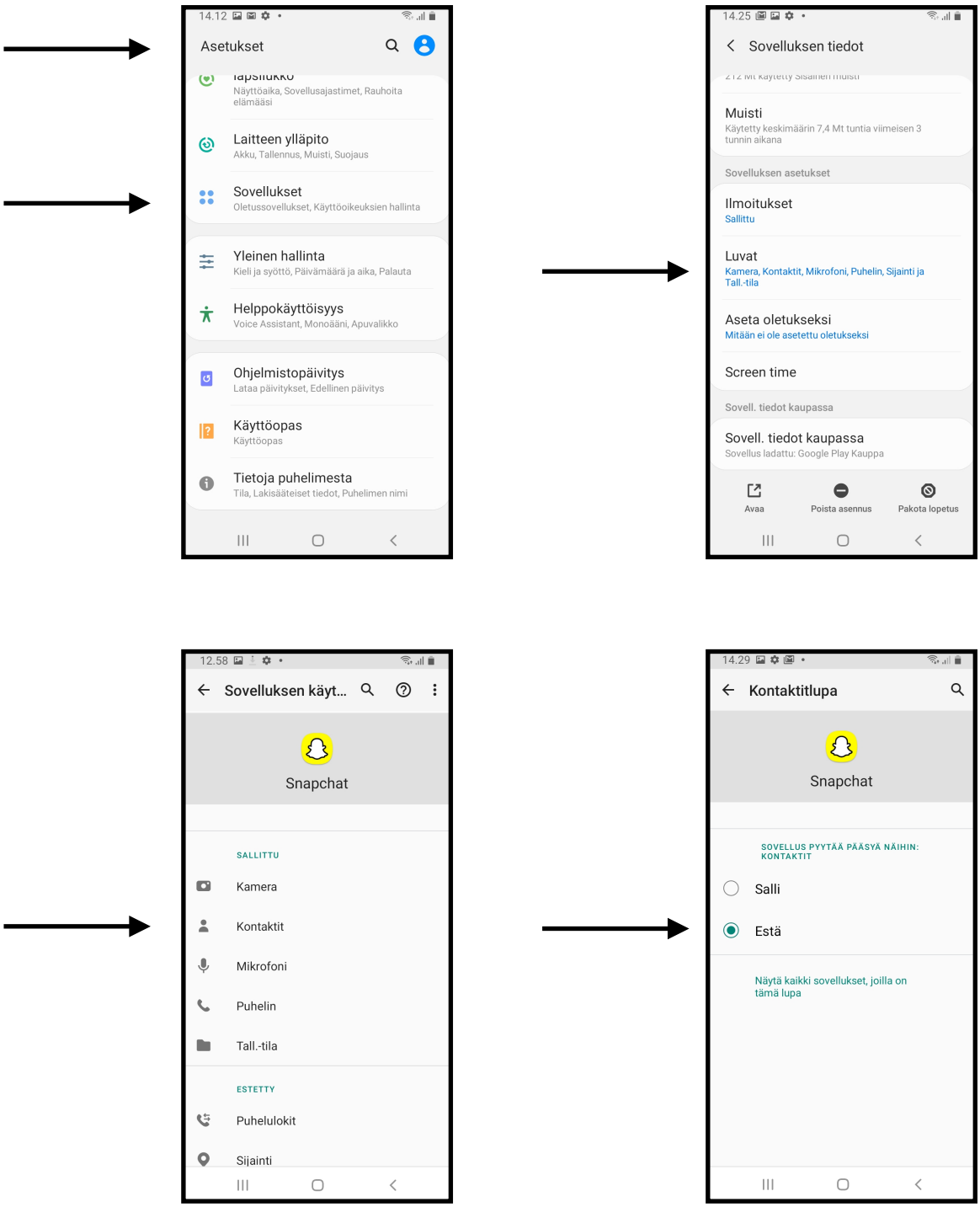
Sovellusten/appien oikeudet

Sovelluksille on olemassa kahdenlaisia oikeuksia: ns. *normaalit ja vaaralliset*. Ilman mitään oikeuksia yksikään sovellus/appsi ei itse asiassa toimi.

Normaaleja oikeuksia pidetään lähtökohtaisesti perusteltuina ja kutakuinkin turvallisina. Vaaralliset oikeudet ovat sellaisia, jotka mahdollistavat tietojen kalastelun ja saattavat vaarantaa laitteen. Sellaisia ovat:

- ACCEPT_HANDOVER
- ACCESS_BACKGROUND_LOCATION
- ACCESS_COARSE_LOCATION
- ACCESS_FINE_LOCATION
- ACCESS_MEDIA_LOCATION
- ACTIVITY_RECOGNITION
- ADD_VOICEMAIL
- ANSWER_PHONE_CALLS
- BODY_SENSORS
- CALL_PHONE
- CAMERA
- READ_CALENDAR
- WRITE_CALENDAR
- READ_CALL_LOG
- WRITE_CALL_LOG
- READ_CONTACTS
- WRITE_CONTACTS
- READ_EXTERNAL_STORAGE
- WRITE_EXTERNAL_STORAGE
- READ_PHONE_NUMBERS
- READ_PHONE_STATE
- READ_SMS
- SEND_SMS
- RECEIVE_MMS
- RECEIVE_SMS
- RECEIVE_WAP_PUSH
- RECORD_AUDIO
- USE_SIP

Hyvä analogia sovellusten oikeuksien hallintaan on oma koti. Jos putkimies tulee katsomaan keittiön vuotavaa hanaa, niin varmaan annat hänelle luvan hoitaa asian kuntoon keittiössä. Jos putkimies haluaa päästä “vilkaisemaan” makuuhuoneen tai olohuoneen kaappien sisältöä siinä samalla, niin varmasti ei ole kaikki ihan kohdallaan.



Sovelluksien lupien hallinta Android-laitteissa:

Asetukset > Sovellukset > (Sovelluksen Nimi) > Luvat > Sallittu > Valitse lupa, jota et halua antaa > Estä

Katsokaa myös “käyttöoikeuksien ylläpito”. Sieltä näkee yhdellä silmäyksellä minkä tyylisiä oikeuksia sovelluksille on jaettu.

Viestien filtteröinti

Android (tästä on kaksi eri versiota Androideissa)

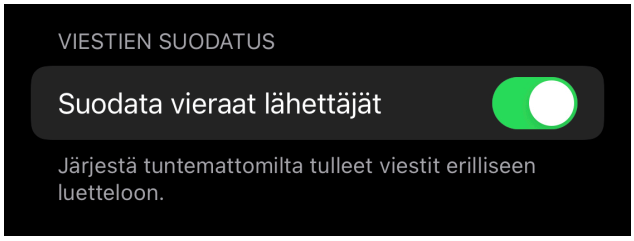
1. Mene puhelin-sovellukseen.
2. Paina kolmea pientä pistettä, yleensä ruudussa oikealla yläkulmassa.
3. Valitse asetukset
4. Laita päälle “Soitt. Tunnus ja roskap. suojaus”.

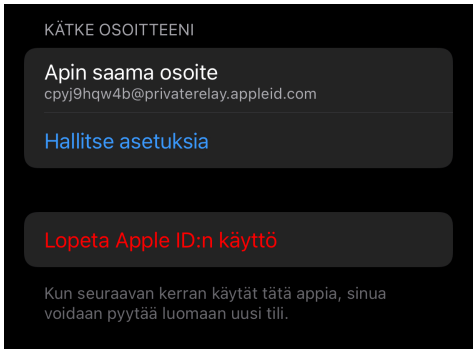
Tai

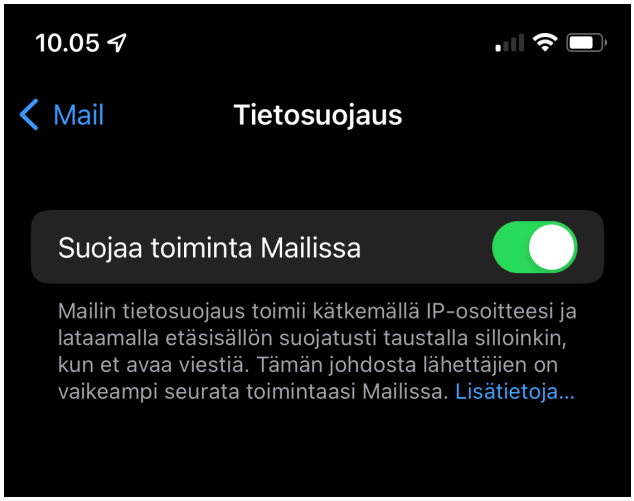
1. Mene viestit-sovellukseen
2. Paina kolmea pientä pistettä, yleensä ruudussa oikealla yläkulmassa.
3. Valitse asetukset ja lisää asetuksia.
4. Laita päälle “Roskapostisuojaus”

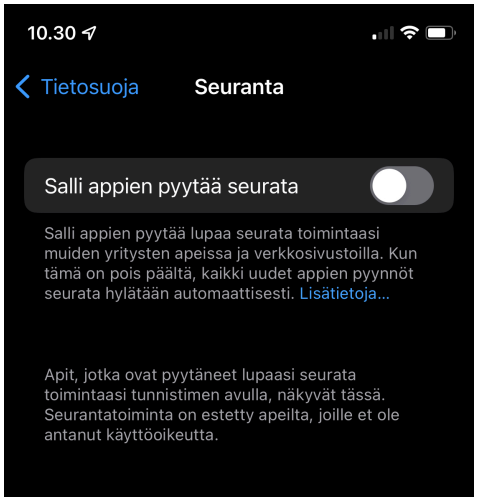
iPhone

1. Mene “Asetukset”
2. Valitse “Viestit”
3. Skrollaa alas “Suodata vieraat lähettäjät”
4. Laita päälle.

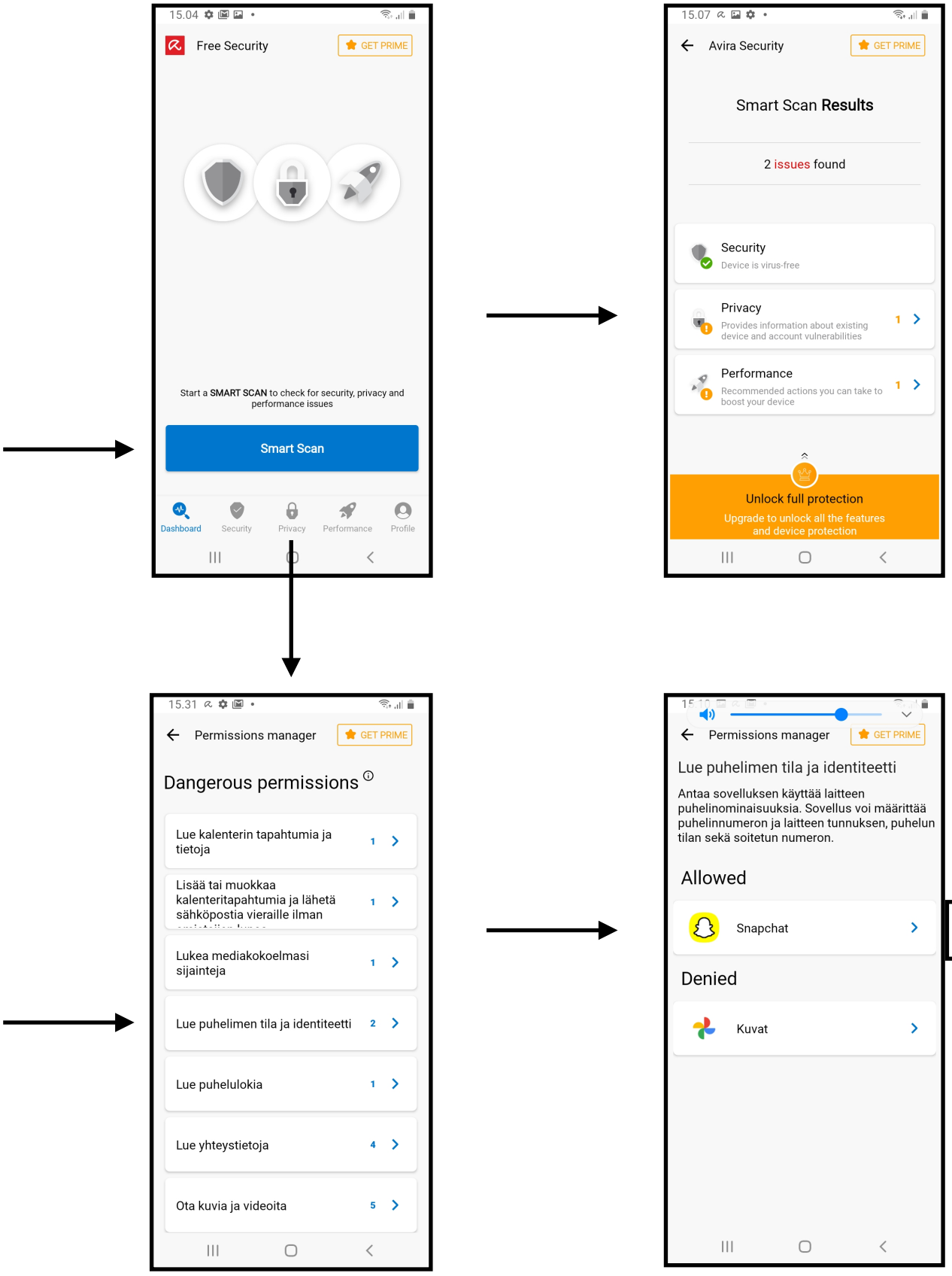








Avira Free Security Android puhelimiin



SALASANOJEN HALLINTA

Pandemian aikana ja vielä sen jälkeenkin yhä useampi ihminen on joutunut työskentelemään kotona. Tällöin turvallisuusasiat, kuten työpaikan sovellusten salasanojen suojaaminen nousee entistä tärkeämpään rooliin.

Hyvä salasanan hallintaohjelma ei ainoastaan helpota muistamaan lukuisten eri käyttäjätilien salasanoja, vaan se auttaa pitämään ne myös turvassa vahvoilla salasanoilla, joita on mahdoton arvata. Lisäksi ne pidetään tallessa turvallisesti suojatussa holvissa.

Apple-käyttäjät ovat melko mukavassa asemassa Applen oman **Keychain Access** -ohjelman kanssa.

Googlen salasananhallinta mukana Android-järjestelmä ja se on sisäänrakennettu Chromeen ja kaikkiin Android-sovelluksiin. Sinun ei tarvitse ladata lisäsovelluksia tai asentaa selainlaajennusta. Voit suoraan käyttää tätä Android-salasanojen hallintaa kaikentyyppisten salasanojen ja tilitietojen tallentamiseen.

Voit käyttää Android-salasanojen hallintaa Chromessa avaamalla Google Chrome -selainsovelluksen, napauttamalla kolmen pisteen valikkopainiketta oikeassa yläkulmassa ja siirtymällä **Asetukset.** Valitse sitten **Tallenna salasanat** vaihtoehto.

Kun haluat tarkastella ja hallita tallennettuja salasanoja Android-puhelimellasi, voit siirtyä “tallenna salasanat” -käyttöliittymään, napauttaa tiettyä salasanaa ja muokata sitä.