



# Mobiililaitteen tietoturva

Pikaopas mobiililaitteen tietoturvalliseen käyttöön kun sekä työ että yksityiskäyttö on samalla laitteella.

## 1 Kuka hallitsee laitettasi?

### Oma hallinta (Apple/Google)



Vastaat itse laitteen päivityksistä, varmuuskopioista ja tilien palautustiedoista. Suojaa tilit vahvalla salasanalla ja MFA:lla.

### Yrityshallinta (MDM)



Työnantaja voi vastata päivityksistä, varmuuskopioista ja tilien palautustiedoista. Henkilökohtaiset tiedot pysyvät lähtökohtaisesti yksityisenä tässäkin vaihtoehdossa.

## 2 Kultaiset säännöt



### PÄIVITYKSET

Asenna käyttöjärjestelmä- ja sovelluspäivitykset heti.

### LUKITUS

Käytä vähintään 6-numeroinen pin-koodi ja biometria. (Kasvoja/sormenjälki)

### MFA & PASSKEY

Ota monivaiheinen tunnistautuminen aina käyttöön jos saatavilla.

## 3 Tunnistaudu fiksusti

### PASSKEY - Salasanojen korvaaja

Laitteeseen sidottu digitaalinen avain. Vaatii biometrisen tunnisteen (FaceID/sormenjälki). Turvallisempi ja helpompi. Ei voi kalastella.



### PASSWORD MANAGER - Salasanahallinta

Käytä ohjelmaa luomaan ja tallentamaan jokaiselle tilille uniikki, vähintään 16-merkkinen salasana. Älä koskaan käytä samaa salasanaa kahdella eri palveluissa.



## 4 Sovellusten 4 vaiheen suoja

### 1 Lähde

Lataa sovellukset vain virallisista kaupoista.

### 2 Maine

Katso arvostelut ja latausmäärät. Varo täysin uusia julkaisijoita.

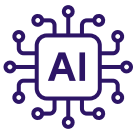
### 3 Oikeudet

Mene asetuksiin ja kytke pois turhat oikeudet.

### 4 Siivous

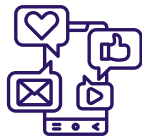
Poista käyttämättömät sovellukset kuukausittain.

## 5 Tekoäly ja Some



### TEKOÄLY (AI)

Älä syötä yrityksen liikesalaisuuksia, asiakasdataa tai koodia julkiseen tekoälyyn (esim. ChatGPT).



### SOMESSA

Varo kuvien taustalla näkyviä tietoja (näytöt, kulkukortit). Pidä työ- ja yksityisprofiilit erillään.

## 6 Mitä jos...

### Toimintaohje

Laite kadonnut tai epäilet tietomurtoa? Toimi heti!



### Ilmoita IT-tuelle



### Käytä Etsi laitteeni -toimintoa

Päaset takaisin tileillesi palautuskoodilla (Recovery Codes).



Lue lisää Traficom  
Kyberturvallisuuskeskuksesta