

Turvallinen puhelimen (työ)käyttö



Ohjelmistojen ajantasaisuus

Säännölliset käyttöjärjestelmän ja sovellusten päivitykset ovat keskeisiä tietoturvan kannalta

ja päivitykset tulee asentaa mahdollisimman nopeasti niiden tultua saataville.

Päivitykset sisältävät usein korjauksia ja parannuksia, jotka suojaavat puhelintasi tunnetuilta

haavoittuvuuksilta.

Puhelimen automaattisten päivitysten salliminen helpottaa ja nopeuttaa vakavilta ohjelmistohaavoittuvuuksilta suojautumista, joten käytä tätä aina kun mahdollista.



Turvalliset salasanat ja monivaiheinen tunnistautuminen

Käytä puhelimen lukituksessa vahvaa salasanaa tai biometristä tunnistusta, kuten sormenjälkeä tai kasvojentunnistusta. Vältä helppoja arvattavia salasanoja ja käytä eri salasanoja eri palveluissa sekä laitteissa.

Jos mahdollista, käytä palveluissa monivaiheista tunnistautumista.

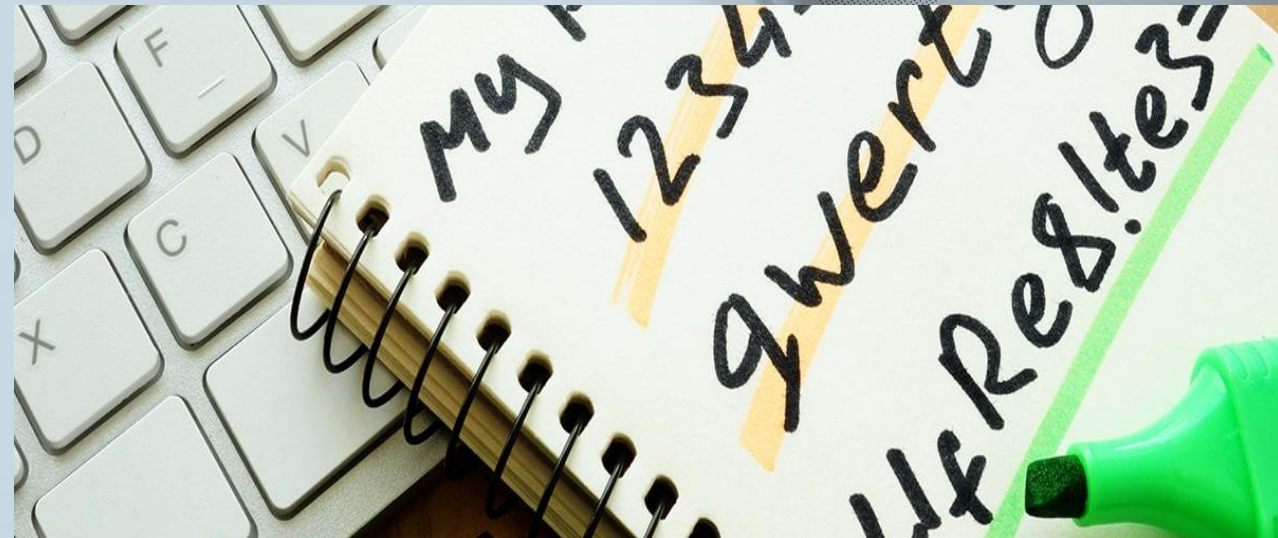
Hyvätaoisen eli vahvan salasanan ominaisuudet:

- pituus vähintään 10 (mieluusti 12) merkkiä
- sisällettävä isoja ja pieniä kirjaimia
- sisällettävä kirjaimia ja numeroita
- sisällettävä jokin erikoismerkki

Salasanan käyttäminen

ÄLÄ käytä samoja salasanoja eri käyttötarkoituksissa.

ÄLÄ käytä palveluitten oletussalasanoja. Paraskaan salasana ei auta, mikäli se on muitten saatavilla.



Wi-Fi ja vapaat verkot

Jos käytät julkista verkkoa, harkitse VPN-palvelun käyttöä, joka salaa tietosi ja suojaa verkkoyhteyden.

Puhelimesta on myös suositeltavaa ottaa pois käytöstä automaattinen tuttuihin WI-FI-verkkoihin liittyminen.

Vapainen julkisten WiFi-verkkojen liikenne ei oletusarvoisesti ole suojattua.

Käytä WiFin sijaan kodin ja työpaikan ulkopuolella mieluummin puhelinliittymän dataliittymää, myös jos käytät esim. kannettavaa tietokonetta tms. omien verkkojesi (koti- tai työverkko) ulkopuolella.



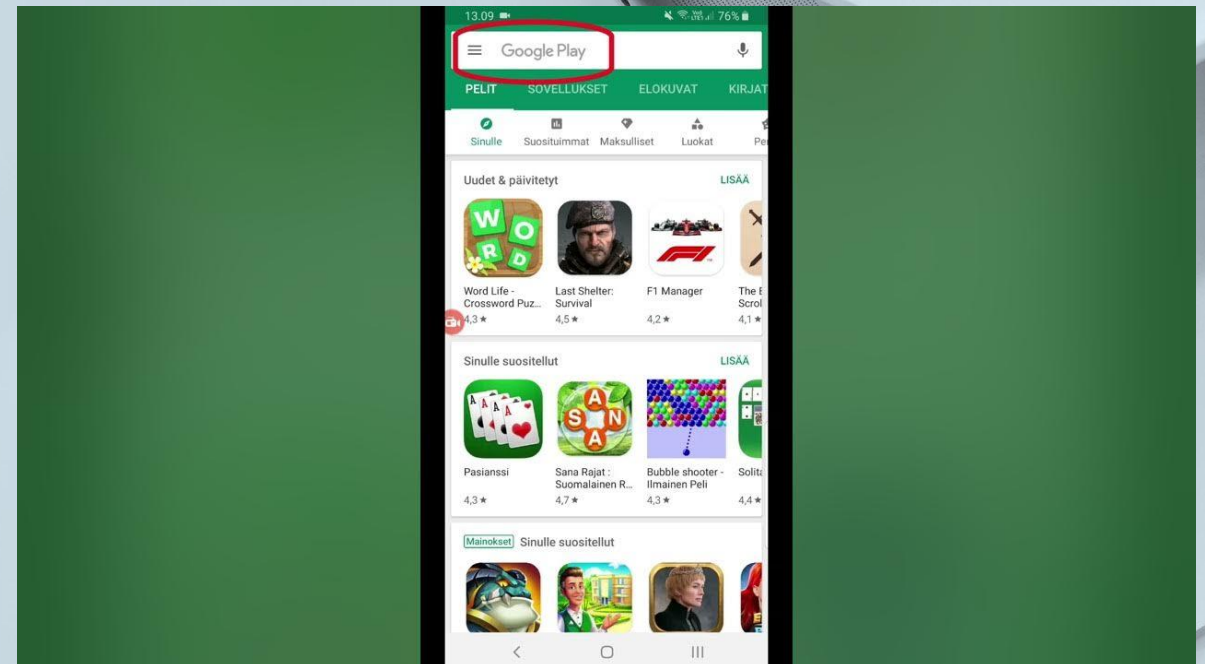
Ohjelmistojen lataaminen ja linkkien avaaminen

Hanki sovellukset puhelimeesi ainoastaan virallisista sovelluskaupoista. Nämä lähteet suodattavat haitallisia sovelluksia ja tarjoavat paremman tietoturvan. HUOM. Ei ole 100% varma tapa, käytä aina harkintaa.

Älä avaa viestejä tai linkkejä tuntemattomilta lähettäjäiltä äläkä asenna Mitään linkkien kautta, erityisesti jos ne esim. houkuttelevat sinua jakamaan henkilökohtaisia tietoja.

Muista, että harva pankki esimerkiksi sisällyttää lähettämäänsä viestiin linkin, joka ohjaa pankin verkkosivuille.

HUOM! Viivakoodin luku voi avata linkin tai ajaa ohjelmiston, ole huolellinen mitä koodeja luet.



Tarkista sovelluksien käyttöoikeudet

On suositeltavaa tarkastaa mitä käyttöoikeuksia asentamasi sovellus pyytää.

Käyttöoikeuksista käy ilmi, jos sovellus haluaa luvan seurata sijaintiasi tai käyttää puhelimesi mikrofonia. Anna sovelluksille vain tarvittavat käyttöoikeudet ja harkitse tarkkaan mitä tietoja ja toimintoja jaat niiden kanssa.

Arvioi tarvitseeko sovelluksesi kaikkia sen esittämiä oikeuksia, esim kameran käyttö.



Käytä virustentorjuntaohjelmistoa

Hyvä virustentorjunta turvaa päivittäistä puhelimesi käyttöä.

Käytä tunnettua ja päivitettyä virustorjuntaohjelmaa, joka tarjoaa reaaliaikaista suojaa.

HUOM. Rikolliset voivat yrittää ujuttaa haitallista ohjelmaa puhelimeen naamioimalla sen näyttämään Virustorjuntaohjelmalta -> lataa ohjelmistoja vain sovelluskaupoista, harkiten



Ota varmuuskopioita säännöllisesti

Varmuuskopioimalla puhelimesi sisällön säännönmukaisesti ja tarpeeksi usein voit palauttaa puhelimesi sisällöt (ohjelmistot, tiedostot, asetukset jne), kun

- Joudut vaihtamaan puhelinta
- Puhelimeesi kohdistuu haittaohjelma
- Tietoja tai tiedostoja häviää

Helpoin ja varmin tapa on antaa puhelin tehdä varmuuskopioita automaattisesti, esim. Google – tilille.

Määrittele varmuuskopiointi tapahtuvaksi tarpeeksi usein, jotta mahdollisesti kopiointien välissä muuttuneiden tietojen määrä ei kasva liian suureksi



10 kohdan muistilista:

1. Suojaa laitteesi fyysisesti ja digitaalisesti

- Käytä **vahvaa PIN-koodia**, salasanaa tai biometrisiä lukituksia (sormenjälki, kasvojentunnistus).
- Ota käyttöön **automaattinen lukitus** lyhyellä aikavälillä (esim. 30 sekunnin jälkeen).
- Älä jätä puhelinta valvomatta julkisilla paikoilla.
- Käytä **suoja-kuorta ja näytönsuojaa** myös fyysisten vaurioiden ehkäisemiseksi.

2. Päivitä ohjelmistot ja sovellukset säännöllisesti

- Asenna aina uusimmat **käyttöjärjestelmäpäivitykset** ja **sovelluspäivitykset** – ne sisältävät tietoturvakorjauksia.
- Poista sovellukset, joita et enää käytä, vähentääksesi mahdollisia tietoturvariskejä.

3. Vältä julkisia Wi-Fi-verkkoja ja käytä VPN:ää

- Älä yhdistä tuntemattomiin Wi-Fi-verkkoihin ilman VPN-yhteyttä.
- Jos joudut käyttämään julkista Wi-Fiä, vältä kirjautumista pankkipalveluihin ja muihin arkaluonteisiin palveluihin.
- Käytä **VPN-palvelua** suojataksesi verkkoliikennettäsi.



4. Lataa sovelluksia vain luotettavista lähteistä

- Asenna sovelluksia vain **virallisista sovelluskaupoista** (Google Play, App Store).
- Tarkista sovellusten **käyttöoikeudet** ja rajoita pääsyä tarpeettomiin tietoihin (esim. sijainti, kamera, mikrofoni).
- Vältä "ilmaisia" sovelluksia, jotka saattavat kerätä tietoja tai sisältää haittaohjelmia.

5. Suojaa tietosi ja varmuuskopioi säännöllisesti

- Ota käyttöön **automaattinen pilvivarmuuskopiointi** (esim. Google Drive, iCloud).
- Säilytä varmuuskopioita myös **ulkopuolisilla laitteilla** (esim. tietokoneella tai ulkoisella kovalevyllä).
- Salaa arkaluontoiset tiedot ja tiedostot, jos tallennat niitä laitteellesi.

6. Varo tietojenkalastelua ja huijausviestejä

- Älä avaa epäilyttäviä linkkejä tai liitteitä sähköposteissa tai tekstiviesteissä.
- Tarkista aina lähettäjän tiedot ennen kuin klikkaat viestiä.
- Älä jaa salasanojasi tai arkaluontoisia tietoja tuntemattomille.
- Käytä **salasanan hallintaohjelmaa**, jotta voit hallita ja säilyttää turvallisia salasanoja.

7. Käytä kaksivaiheista tunnistautumista (2FA, MFA)

- Ota **2FA käyttöön** kaikissa tärkeissä palveluissa, kuten sähköpostissa, pankkitileillä ja sosiaalisen median tileillä.
- Käytä mieluiten **autentikointisovellusta** (esim. Google Authenticator, Microsoft Authenticator) tekstiviestien sijaan.



Lähde: Arter.fi

8. Hallitse sijaintitietojasi

- Poista **sijainnin jakaminen** sovelluksilta, jotka eivät sitä tarvitse.
- Älä jaa reaaliaikaista sijaintiasi julkisesti sosiaalisessa mediassa.
- Tarkista ja hallitse **sijaintiasetuksia** laitteesi tietoturva-asetuksista.

9. Poista laitteesta tiedot ennen myyntiä tai hävittämistä

- Palauta tehdasasetukset ennen kuin luovutat tai myyt vanhan puhelimesi.
- Poista kaikki henkilökohtaiset tiedot ja varmista, että **tallennusmuisti on tyhjennetty pysyvästi**.

10. Ota käyttöön "Etsi puhelimeni" -toiminto

- Ota käyttöön **Find My iPhone (Apple)** tai **Find My Device (Android)**, jotta voit paikantaa ja tarvittaessa etätyhjentää laitteesi, jos se katoaa.
- Aktivoi **etälukitus**, jos puhelin varastetaan tai katoaa.



Lähde: Arter.fi

Tämä materiaali on osa Digiäly käyttöön –hankkeen toimenpiteitä.

Hanketta toteuttaa Suomen Yrittäjäopisto. Hanke on saanut EU:n maaseuturahoitusta.

- **Lue lisää hankkeesta täältä:**
- <https://www.syo.fi/yritysten-kehittamishankkeet/digialy-kayttoon-hanke/>



**Euroopan unionin
osarahoittama**