

## Pag-secure sa Iyong mga Device

Nagbibigay ang resource na ito ng ilang praktikal na unang hakbang para sa pag-secure ng mga device laban sa mga karaniwang anyo ng pag-track sa device at sinasaklaw nito ang mga aksyon gaya ng pag-off sa Bluetooth, WiFi, at pag-share ng lokasyon; pag-rename ng iyong device; pagsusuri para sa spyware at mga pahintulot ng app; at paggawa ng factory reset.



Mga pangkalahatang tip ang mga ito para mapanatiling secure ang iyong mga device. Ang mga eksaktong hakbang ay posibleng naiiba para sa magkakaibang device at magbago sa paglipas ng panahon.



Sa mga iPhone at iPad, karaniwang makikita mo ang isang setting sa pamamagitan ng pag-tap sa “Settings (Mga Setting)” sa Home Screen, pagkatapos ay pag-swipe pababa para ipakita ang search bar. (Para sa tulong, tingnan ang <http://tiny.cc/iphonesearch>.)



Sa mga Android device, mag-swipe pataas mula sa Home Screen: may lalabas na search bar na nagsasabing “Search Your Phone and More (Maghanap sa Iyong Telepono at Higit pa)”. I-type ang setting na hinahanap mo sa search bar.

### I-off ang Bluetooth at WiFi kapag hindi mo ginagamit ang mga ito

Nakikita ng iba pang device ang iyong device dahil sa Bluetooth at WiFi. Kapag hindi mo ginagamit ang mga ito, i-off ang mga ito sa pamamagitan ng pagpunta sa **Mga Setting** o pag-tap sa mga icon ng **Bluetooth** at **WiFi**.

Puwede ka ring pumunta sa mga setting ng iyong Bluetooth (**Mga Setting > Bluetooth**) at maghanap ng anumang device na nakapares sa telepono mo. Kung may anumang device na hindi mo nakikilala, i-unpair ang mga ito.

### I-off ang pag-share ng lokasyon

Gumagana pa rin ang pag-share ng lokasyon at mga app tulad ng “Find my Phone (Hanapin ang Aking Telepono)” kung naka-off ang iyong telepono, kaya kailangan mong i-off ang mga ito sa mga setting. Sa isang iPhone, buksan ang **Mga Setting > Privacy (Pagkapribado) > Location Services (Mga Serbisyo sa Lokasyon)** o maghanap para sa “Location Services (Mga Serbisyo sa Lokasyon)”, at i-off ang pag-share ng lokasyon.

Sa isang Android device, buksan ang **Maps (Mga Mapa)**, i-tap ang iyong larawan sa profile at pagkatapos ay Location sharing (Pag-share ng lokasyon). I-tap ang larawan sa profile ng sinumang *hindi dapat* nakakakita sa iyong lokasyon, at pagkatapos ay i-tap ang “Stop (Itigil)”.

#### Icon key



Mga Setting



Bluetooth



WiFi



Toggle



Maps



Tatlong dot

# Pag-secure sa Iyong mga Device

## I-rename ang iyong mga device

Kahit na hindi mo kailanman binago ang pangalan ng iyong telepono, may pangalan pa rin itong tumutukoy rito. Sa isang iPhone, i-tap ang **Mga Setting** > General (Pangkalahatan) > About (Tungkol dito) > Name (Pangalan), o maghanap para sa “Name (Pangalan)”, pagkatapos ay maglagay ng bagong pangalan at i-tap ang “Done (Tapos na)”.

Sa isang Android device, i-tap ang **Mga Setting** > About phone (Tungkol sa telepono) > Device name (Pangalan ng device), o maghanap para sa “Name (Pangalan)”, pagkatapos ay ilagay ang bagong pangalan at i-tap ang “OK”.

## Tingnan kung may spyware

Ang ibig sabihin ng “spyware” ay mga app na nagbibigay-daan sa ibang tao na matiktikan ang iyong device. Tingnan para malaman kung may anumang app na hindi mo nakikilala. Sa isang iPhone, mag-swipe pakanan sa Home screen hanggang sa makita mo ang App Library.

I-tap ang search box sa itaas ng screen, pagkatapos ay mag-scroll sa listahan ng mga app at alisin ang anumang hindi mo nakikilala.

Sa isang Android device, pumunta sa **Mga Setting** > Apps and notifications (Mga app at notification) > See all apps (Tingnan ang lahat ng app), o maghanap para sa “Apps (Mga app)”.

May mga magagamit ka ring app tulad ng *Certo* at *Incognito* na isa-scan ang iyong mga device para sa spyware, pero dapat alam mong palaging may posibilidad na posibleng may spyware pa rin sa iyong telepono.

## Tingnan ang mga pahintulot ng app

Puwede mo ring pigilan ang anumang app sa pagkolekta o pag-share ng mga bagay tulad ng iyong lokasyon. Sa isang iPhone, i-tap ang **Tatlong dot** > Privacy & Security (Pagkapribado at Seguridad) > App Privacy Report (Ulat sa Pagkapribado ng App) para makita kung ano ang shine-share ng bawat app, o maghanap para sa “Privacy Report (Ulat sa Pagkapribado)”. I-tap ang bawat app para baguhin ang mga setting.



Sa isang Android device, i-download ang *DuckDuckGo* app sa Play store at pagkatapos ay buksan ito. I-tap ang **Mga Setting** > App Tracking Protection (Proteksyon sa Pag-track ng App) at pagkatapos ay i-slide ang **toggle** pakanan.

## Factory reset

Kung nagawa mo na ang lahat at sa tingin mo ay may nagta-track pa rin sa iyong telepono, puwede kang gumawa ng factory reset. Gayunpaman, ide-delete nito ang lahat ng data, kabilang na ang anumang ebidensya sa iyong telepono. Kung ire-reset mo ang iyong telepono, hindi ka makakapag-restore mula sa na-save na backup dahil posibleng ma-load ulit ang kung anuman ang nagta-track sa iyo: kailangan mong magsimula ulit sa umpisa.

Kung sigurado kang gusto mo itong gawin, sa isang iPhone, puwede mong i-tap ang **Mga Setting** > General (Pangkalahatan) > Transfer or Reset iPhone (Ilipat o I-reset ang iPhone), pagkatapos ay Erase All Content and Settings (Burahin ang Lahat ng Content at Setting). Puwede mo ring hanapin ang “Reset (I-reset)” para makita ang setting na ito.

Kung may iPhone ka, puwede mo ring i-on ang Lockdown Mode, na magpoprotekta sa iyo laban sa karamihan sa mga uri ng spyware. Nililimitahan din nito kung gaano mo magagamit ang mga app tulad ng FaceTime at Safari. Tingnan ang <https://support.apple.com/en-ca/HT212650> para sa higit pa tungkol sa Lockdown Mode.

Sa isang Android device, magsimula sa pamamagitan ng pagpunta sa **Mga Setting**, pagkatapos ay maghanap para sa “Reset (I-reset)”. Maghanap ng resulta tulad ng “Factory reset” o “Erase all data (Burahin ang lahat ng data)” at i-tap ito.