DEVIOUS DEVICES – Companion Technology Guide – 2024.05.26

This guide is a technology companion to the 3-part DEVIOUS DEVICES presentations. Its purpose is to provide links to various recommended technologies to assist with installation and configuration of software and APPs. However, as technology changes rapidly, the links – or the information contained within – may not be accurate for the version of hardware and software you may be using.

GENERAL RECOMMENDATION: Go slow! Many of these changes can affect the way you use your Device and can be confusing if you adopt too many changes at once. Start at the beginning of the list and become comfortable with a new SYSTEM and it's use before progressing to a new technology. Each successive step will improve your privacy, so SOME improvement is better than none.

- ***Neuralink*** Brain-Computer Interface (BCI): https://neuralink.com/ is provided FYI ONLY.

- ***Faraday Bags:***

  Search https://www.amazon.ca for Faraday bags. A wide variety of bags and boxes starting from $15. Also available at many other retailers.

- ***Super Security Email Providers:***

  Microsoft: https://www.microsoft.com/en-ca/microsoft-365/buy/compare-all-microsoft-365-products?tab=1&OCID=cmmruikv4ct. Starting at $8/month

  Proton: https://proton.me/mail Free account with limited capabilities, or subscriptions starting at $4/month (USD). See additional information under the VPN section.

- ***Sanctuary APPs:***

  Wikipedia: use from a properly-configured browser www.wikipedia.org or install the APP from Google Playstore or Apple iStore.

  Brave (secure/private web browser): desktop/laptop installer https://brave.com/ or install the APP from Google Playstore or Apple iStore.

  How to change Brave privacy settings: https://support.brave.com/hc/en-us/articles/360017989132-How-do-I-change-my-Privacy-Settings. Focus on *Clear Browsing Data, Security, Cookies, and Shields settings drop-downs.*

  Firefox (secure/private web browser) desktop/laptop installer https://www.mozilla.org/en-US/firefox/ or install the APP from Google Playstore or Apple iStore.

  How to change Firefox privacy settings: https://allaboutcookies.org/firefox-privacy-settings. Use the 1st five recommendations, and at least the Disable Tracking Cookies (setting 2. Block All Cookies by Default) from the 7 advanced settings. You can experiment with the other 6 advanced settings but heed the warnings.

TIP: Creating an account in Firefox will allow you to store frequently used bookmarks for websites. With an account, bookmarks can be easily seen from desktops, laptops, and Smartphone versions of Firefox that you sign into. In addition, the desktop/laptop version of Firefox as a Bookmarks sidebar feature that allows a hierarchical and organized display of bookmarks in the sidebar to access hundreds of stored bookmarks. **Firefox account credentials are stored on a secure not-for-profit server NOT shared with any other organization.**

TIP: Install BOTH Brave and Firefox on all devices and segregate search/web browsing by security type. I use Firefox for the *super security* websites and Brave for *medium* and *low security* websites.

Startpage (search engine): can be accessed from ANY browser at https://www.startpage.com/. If offered a choice, choose to make Starpage your default search engine (banner at the top of the page).

How to configure Startpage settings when you have "cookies" disabled in your web browser (recommended): https://support.startpage.com/hc/en-us/articles/4616244515476-How-do-I-keep-my-settings-without-using-cookies. Here is a short Youtube video that describes the same process: https://www.youtube.com/watch?v=JQKS_cP0g5I

How Startpage uses Anonymous View: https://support.startpage.com/hc/en-us/articles/4455317663764-How-does-Anonymous-View-work

TIP: Install Startpage on your ALL your browsers and ALL devices and set to be the DEFAULT search engine.

KeePass (secure password storage APP): desktop/laptop installer https://keepass.info/ or install the APP from Google Playstore or Apple iStore.

Installing KeePass from the website for a desktop/laptop can be a bit convoluted. Here is a helpful step-by-step article https://www.techrepublic.com/article/how-to-use-keepass/.

Here is a step-by-step tutorial on how to use KeePass: https://keepass.info/help/base/firststeps.html

TIP 1: KeePass encrypted database files can easily be stored and transferred using a USB stick. For maximum security, store database files locally on the *Device* and periodically backup using a USB stick. Alternately, you can store the database file on a Cloud provider, but ONLY a high security cloud site (ie: Proton or OneDrive). Do NOT store on Google, Yahoo, or Apple cloud storage.

TIP 2: Use multiple KeePass database files for different levels of secure credentials or family members. Do NOT store passwords in web browsers.

TIP 3: For desktop and laptop computers , there is an advanced way that you can connect KeePass to the Firefox browser to have KeePass credentials automatically populate websites you access from Firefox. Two sites that describe this procedure are https://addons.mozilla.org/en-US/firefox/addon/keepasshttp-connector/ and https://github.com/smorks/keepasshttp-connector/blob/master/documentation/KeePassHttp-Connector.md#2-installation . **WARNING**: this is a technically complex procedure and it best performed by someone adept at browser and software configuration.

Signal (Encrypted Communications tool): desktop/laptop installer https://support.signal.org/hc/en-us/articles/360008216551-Installing-Signal Scroll down to the "Desktop" section. Or install the APP from Google Playstore or Apple iStore.

Configuration and How to Use sections are located on the same webpage as above.

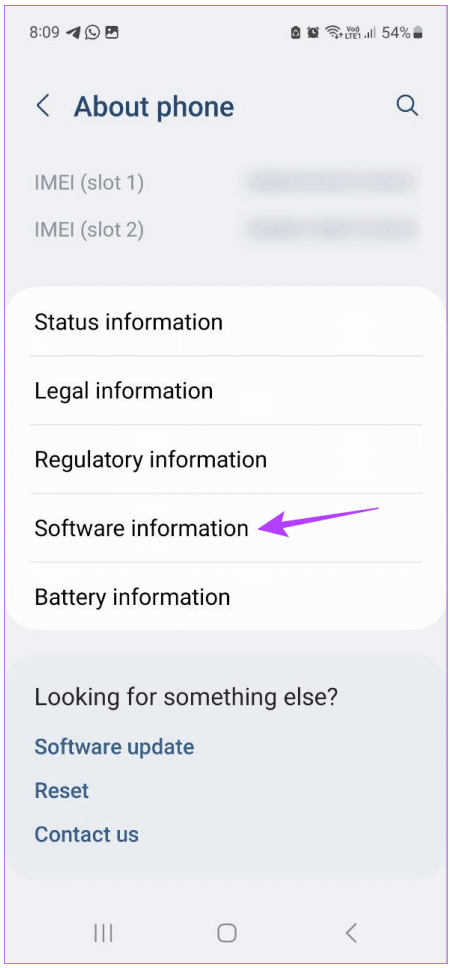
TIP: use Signal for "text" messages, voice calls and group chat with friends and family. It bypasses the SMS – Cell phone network and encrypts ALL communications. All participants must have Signal installed

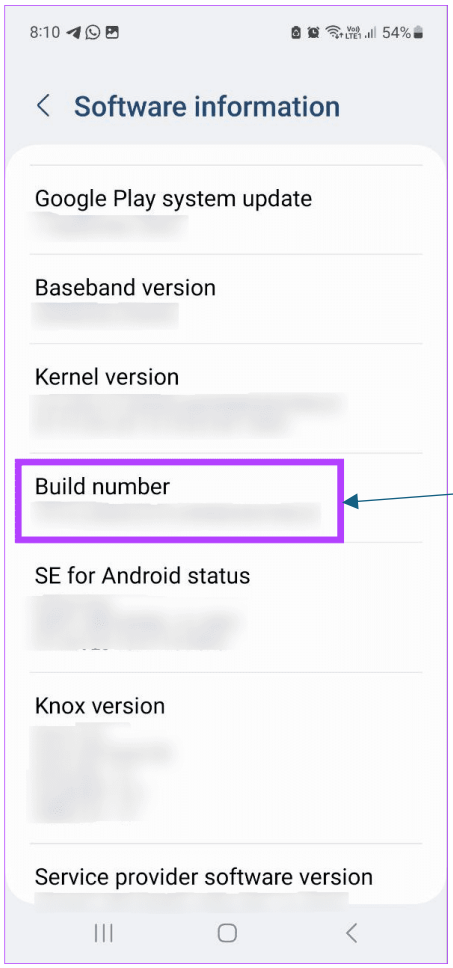
- ***VPNs (encrypted Internet data tool):***

TunnelBear: https://www.tunnelbear.com/ Good basic VPN service. Desktop/laptop installer https://www.tunnelbear.com/download or install the APP from Google Playstore or Apple iStore. Offers free usage with limited capability. Subscriptions for premium service start at $3.33/month (USD).

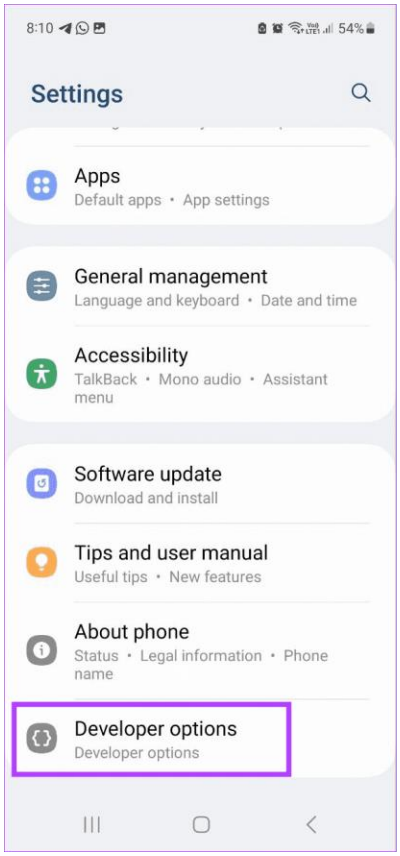
Proton: Desktop/laptop installer https://proton.me/ (follow the links from the Products dropdown menu) or install the APP from Google Playstore or Apple iStore. Advanced multi-faceted and integrated security with *VPN, Email, Calendar, Password Manager,* and *Cloud storage*. All communications and data storage are encrypted. Best rated system. VPN pricing starts at $4.49/month (USD) and ALL services package at $7.99/month (USD). High-capacity multi-user business packages also available.

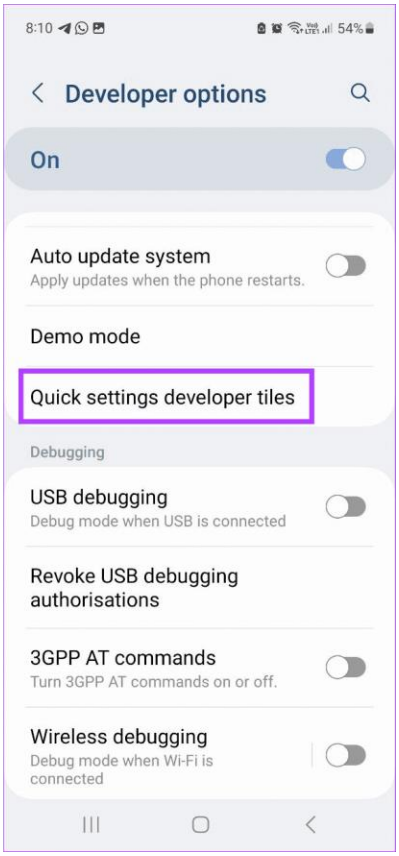
- ***Disabling Sensors on Android Devices:*** https://www.lifewire.com/turn-off-android-phone-sensors-5524799 . Also see Images below: ***NOT available for Apple devices***

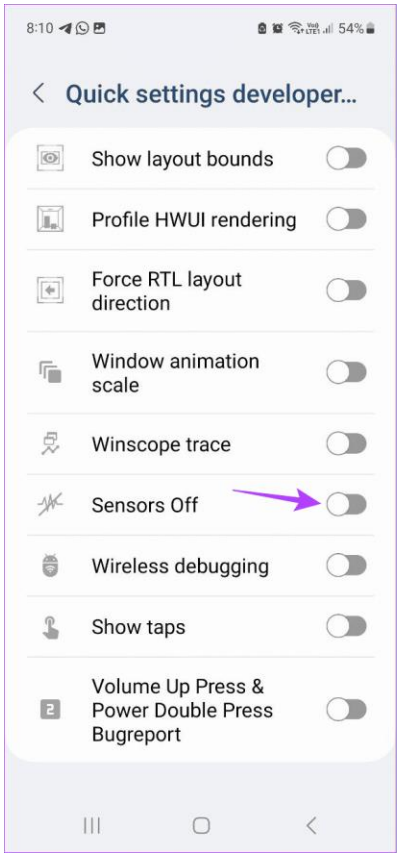


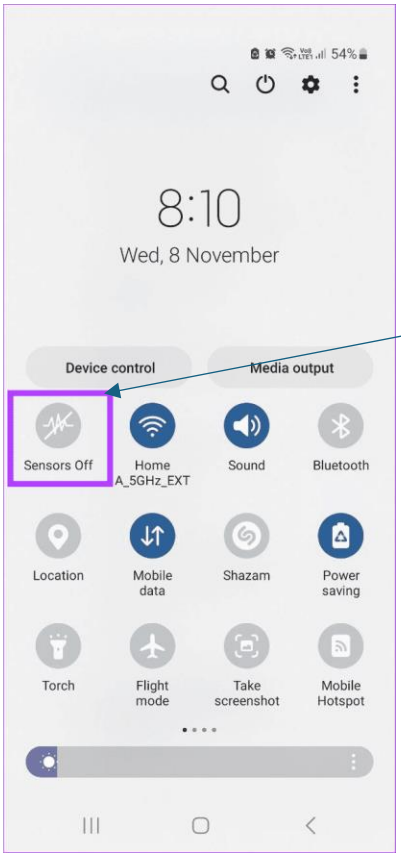


Tap 5 to 7 times until message appears that Developer Mode is enabled.









Tap to illuminate ICON - turns sensors **OFF**.

Tap again to "gray-out" ICON - turns sensors **ON**.

- ***Best Practices:***
  - Always install Android and Apple APPS from their respective “stores” on Smart Devices
  - Never talk to a Smartphone Assistant or your TV.
  - Avoid Smart Appliances & their APPs.
  - Never connect your home security or thermostat to your phone.
  - Never connect your car door locks & ignition (starter) to your phone.

- ***Worst Practices:***
  - Using banking & loyalty program APPs.
  - Using Smartphone TAP & PAY APPs.
  - Using personal health APPs & wearables.
  - Opening unsolicited Emails & Messages.