

Welcome to Securing Your Digital Footprint

Mobile Devices-

Smartphones, cellphones, iPads and tablets (iPads) allow us to take the power of a desktop computer with us anywhere but they can leave us vulnerable to online security breaches like fraud, information leaks, and privacy invasions. Below, I have listed a number of ways to increase the security of data on your devices against unauthorized access.

1. Use a pass code. Don't use something that anyone could guess about you, birthday, anniversaries, etc. If you have the option, pick a six digit passcode as it is more secure. Keep in mind that a limitation of passcodes is that the keypad you use always appears in the same place on the screen, this may leave a tell-tale pattern of fingerprints on your screen. Of course, if you never clean the screen and leave fingerprints everywhere this may not matter at all. [Source:](#)
If you own an iPad be aware there is a new hack to break through your [passcode protected](#) device.
2. If you are using a thumbprint - Stop!!! You can be compelled by Local Law Enforcement (LLE) to open your phone using this. Tip: If you are using thumbprint and are arrested, quickly turn off your phone, when they turn it back on it will ask for your passcode and they can't force you to open it using that.
3. Turn on Anti-Tamper Self Destruct Mode (Remote Wipe) even if you don't have 'sensitive' data on your device. This setting will automatically wipe all the data on your iPad/iPhone should the wrong passcode be entered more than a set number of times. Instructions for [Enabling the iPad's Data Wipe on Failed Passcode](#) setting can be found here. Fear not, Android also has a similar [feature](#).
4. Tell Siri to Never Talk to Strangers. If you have the Siri personal assistant enabled, you may be allowing it to bypass your lock screen security for certain functions. Check out [how to Secure Your Siri Assistant](#). [Source:](#)
5. Enable two-form-authentication. A notification will pop up on your locked screen, showing the code. On your phone, Settings/Passcode, look for the section "Allow Access When Locked." Turn off all features in this section.
6. Consider 'Find My iPad/iPhone' or 'Android Device Manager' to track your phone if its stolen, lock your phone, and delete data remotely. There are mixed feelings about this feature. The locator system has to be on ALL the time for it to work. Or wifi must be connected if you have an iPad and it feature has to be used with iCloud. If you decide to use this service, here are the [instructions](#) to set it up. If you do, safeguard your Apple device so [thieves can't disable](#) it. Remember that devices are literally homing beacons, as they constantly ping cell towers, or look for wifi networks or broadcast their location through Bluetooth.

On an Apple device:

- a. Settings
- b. Privacy

On Android devices:

- a. From your home screen, enter your Settings menu. *If running Jelly Bean OS, swipe your notification bar down, and tap the Settings icon. On a Samsung device, from your home screen you can tap Menu>Settings.
- b. Scroll down to the “Personal” section.
- c. Tap on “Location services” or “Location access” – whichever your phone shows.
- d. From this screen, toggle on or off any of the location services your phone offers. On most phones, that includes your carrier’s and Google’s location services, plus standalone GPS services.

Basics of Each Service:

- Carrier location services: When checked, it uses your carrier’s cell towers to help to pin-point your location.
- Google location services: This mostly uses WiFi signals to help determine your location.
- Standalone GPS services: This uses the GPS unit in your phone in order to determine your location.

7. Turn off the locator service/GPS - no reason to put a target on your back.
8. Keep only the information you need on your devices. If you’re only texting and calling, don’t keep contacts emails, snail mail addresses, birthdays, etc..
9. Securing your phone and text messages is a must as each mobile phone provider has practically unlimited access to (and ability to intercept) all text and voice messages sent via its network. Phone providers, in most countries, are legally obligated to keep records of all communications. Voice and text communication can also be tapped by third parties in proximity to the mobile phone using inexpensive equipment.
10. Replace FaceTime and Skype with [Wire](#). It's free and works with Android, iOS (iPhones, iPads) and Macs. Wire provides free phone calls that are secured on both ends. They also provide texting and image sharing but these are not secure.
11. Consider [Signal](#). It's free, works with Android and iOS, and you can send high-quality group, text, picture, and video messages secure on both ends.
12. When accessing the internet, use a [browser](#) that won't track you and hides your actions.
13. Keep your device with you at all times. Never leave it unattended. Avoid displaying it in public.
14. Physically mark (draw on) the SIM card, additional memory card, battery, and device with something unique (not immediately noticeable to a stranger). Make a small mark, drawing, letters or numbers, or try using ultra-violet marker (invisible in normal light). Place printed tamper-proof

security labels or tape over the joints of the device. This will help you easily identify whether any of these items have been tampered with or replaced (e.g. the label or tape will be misaligned or leave a noticeable residue).

15. When disposing of your device, make sure you are not giving away any information that is stored on it or on the SIM or memory card (even if the device or cards are broken or expired). Disposing of SIM cards by physically destroying them is your best option. If you plan to give a device away or sell your device, make sure all data is deleted.
16. Use only trusted phone dealers and repair shops. This reduces the vulnerability of your information when getting second-hand devices or having your device repaired. Consider buying your device from an authorized but randomly chosen dealer – this way you reduce the chance that your device will be specially prepared for you with pre-installed spy software.
17. Make a note of the 15-digit serial or IMEI (International Mobile Equipment Identity) number and keep it separate from your device. This number could help you trace and prove ownership quickly if it is stolen. [Source](#): Access by keying *#06# into most phones. For most devices, look behind the battery or check the settings.
18. Keep in mind that your device can be set to record and transmit any sounds within the range of its microphone without your knowledge which could allow eavesdropping. Some can be switched on remotely and brought into action, even when they look as though they are switched off.
19. Get informed about cell blockers. They are inexpensive devices that others can use to block or disrupt any cellular, wifi, or Bluetooth networks in your vicinity and render your device useless for communication. This can be very serious with the new wave of wifi home security systems on the market.

I hope, armed with this knowledge, you choose to take the next steps in online security concerning your mobile devices and that you are empowered to get in the habit of keeping your data and communications more secure.