Essential Security for Your Smartphone

A Wealth of Sensitive Information: There is an abundance of very personal information on your smartphone, including pictures, email conversations, text/SMS messages, phone records, a record of where you have been (location services), possible access to bank accounts, credit card information, passwords to social networking apps and other websites, buying habits, a record of Internet sites visited, etc. Therefore, smartphones are the new target for malware and hacking, as well as being susceptible to being lost or stolen.

Real-time Surveillance: Not only does your smartphone have a record of where you have been and what you have done, it can be used as a real-time tracking device, showing your current location, listening to your live phone conversations, actively reading your text/SMS conversations, revealing connections to other people (electronically or physically by GPS proximity), etc. If you consider yourself a possible target for real-time monitoring, you need to consider this real possibility and take appropriate precautions. (For more information, see the "Spy Software" section at the bottom of this document.)

Hostile Environments vs. Everyone: Before reading my recommendations for smartphone security, you need to consider your own situation, assess the level of security you need (i.e. based on your risk) and act accordingly. The items in the first section of recommendations here are meant to keep you from identity-theft and other schemes to defraud you; they mean to provide basic security for the average person living in an environment with a (relatively) non-hostile government, such as in the USA. If you believe you may be a high-profile target, or are extra concerned about your information being leaked, then please also see the few items in the "Hostile Environments" section of this document (as well as following the advice for "everyone"). Depending on your situation, you may need further expert advice besides these basic recommendations.

To understand the reasoning behind and importance of these security steps, see the document "How an Adversary can Use a Smartphone for Surveillance"

Everyone: Everyone must follow these basic smartphone security practices:

Software Security

1) **Regularly update the version of software (operating system) on your smartphone, including all regularly released Security Updates (patches). (This is critical; just do it!)**
   a) Vulnerabilities are constantly being discovered for every piece of electronic equipment, especially high value targets like smartphones. Updates to software versions patch these vulnerabilities and help secure your device.
   b) **iPhones/iOS**: When a new version of iOS is offered for your iPhone, update it. (Actually, you should probably wait a week or so to make sure there are no major issues associated with the new version. Do an online search to confirm any negative issues.)
      i) (*As of this writing*) You should be at iOS version 14 or 15 (with the current update). Anything older than this is considered insecure, as Apple is no longer providing regular updates or security patches for older versions.
      ii) If you have a device that is no longer supported or won't install the latest iOS version, then it is time to upgrade!
   c) **Android**: The Android OS is produced and supported by Google, but most Android smartphones are repackaged by a phone manufacturer (e.g. Samsung, LG, etc.) and a cell carrier (e.g. Verizon, AT&T, etc.) before sold to you. A major problem with this distribution model is that manufacturers and carriers control the update process and have been slow to send out security and version updates; you may be forced to live with major vulnerabilities due to unapplied patches. This is not acceptable!
      i) The one exception to the Android update problem is the **Pixel** smartphone; since Pixel is created by Google, makers of the Android OS, they are updated more regularly, without waiting for your phone carrier, and thus tend to be more secure.

ii) If you own a non-Pixel Android smartphone, you must use a phone manufacturer that supplies updates (like Samsung), and use a carrier that provides regular updates (e.g. most major-tier U.S. carriers have started to do this). Check the date of the last "Security Update" on your phone; it should be within the last couple of months. Otherwise, buy a newer Samsung and switch carriers!
iii) (*As of this writing*) You must at least be running Android version 8.1 with the latest updates, but should upgrade to a later version very soon. If your smartphone does not support this version or is no longer getting security updates, then get a new smartphone!

2) **Regularly update all apps installed on your smartphone.**
   a) Vulnerabilities are constantly being discovered for apps installed on your device. Many updates include security patches as well as new features. You must get those security updates!
3) **Don't click on unsolicited links or attachments sent to you via email or SMS/text messages. (And be wary of links and attachments sent to you by "friends".) Stop! Think! Act Prudently.**
   a) Clicking on a legitimate-looking malicious link (or opening a booby-trapped attachment sent via email or otherwise) is the easiest way to get malware on your smartphone.
4) **Be careful on open/public WiFi networks.**
   a) All Internet traffic sent on public WiFi can be read, including all passwords. Whenever doing important things in public, such as entering a password for an online account, banking, etc., you should turn on your Virtual Private Network (VPN) software to encrypt all traffic.
      i) See my "Essential Security Measures for Home Computers" document for VPN details.
   b) Pop-up messages can be generated by hijacked networking equipment. Never click a pop-up offering to update software or phone settings in a public location, as it may actually install malware.
   c) If you think you need to install an update, do it at home by visiting the website/location you would normally use to update your apps or device.

Physical Security

5) **Set a strong/complicated PIN or Password to lock your phone.**
   a) The PIN should be at least 6 digits. If you are really concerned about privacy (or traveling in a hostile environment), then use a more complicated password/PIN, including letters.
   b) If you use a simple passcode (e.g. 1111, 4567, etc.) then it is trivial for someone to hack into your phone. Don't do this!
6) **Set your smartphone screen to lock when it is idle for a certain amount of time.**
   a) Based on your risk situation, you may choose 30 seconds or between 1 and 5 minutes.
7) **Set your smartphone to erase all data after 10 wrong PIN attempts.**
   a) This keeps someone from hacking into your phone if it is lost or stolen.
   b) Make sure to have a backup of your personal data first!
   c) If you have small children, you may not want to set this security feature. :-)
8) **Encrypt your filesystem.**
   a) This is done automatically on the iPhone; it must be initiated on most Android devices (although manufacturers of newer Android phones may be activating this feature by default). See online documentation for your particular device.

Miscellaneous Important Security Practices

9) **Use separate, strong passwords for important apps (email, banking, Facebook, etc.)**
   a) Reusing passwords makes it simple for crooks to hack into many of your accounts. This happens all the time; don't do it! Use strong, unique passwords for any account you want to remain private.
   b) I suggest you use a password manager program that remembers and encrypts your passwords. Consider using Dashlane, LastPass, or 1Password.
      i) Never let a web-browser "remember" your passwords as these are easy to hack into and steal.

ii) Newer versions of iOS [11 or later] offer to store passwords securely in the Keychain. This is secure, and thus fine to use if it works for you, but it is not as full-featured as these other recommended password programs.

10) **Only download Apps from certified sources (Apple Store or Google Play Store)**
    a) Please note that some apps (especially free ones) may have viruses that may secretly steal your personal information. Be wary about downloading newer apps that have not been vetted over time. (This is more likely to happen with Android apps than iPhone apps.)
    b) Android allows you to install apps from other locations. Don't!
11) **Don't jailbreak your iPhone or root your Android.**
    a) If you don't know what this means, then you are good! :-)
    b) Don't jailbreak your Apple device in order to get apps not available in the App store.
    c) Although at one time you (as a techie nerd :-) might have rooted your Android device to implement more security, you should no longer do so for any reason I am aware of.
12) **Wipe the data off an old phone before you recycle or sell it.**
    a) You should delete all data and set it back to factory default settings before getting rid of it.

Optional but Important Security Practices

13) **Backup your data (contacts, docs, photos, etc.). You can backup to your computer, or to an online/Cloud account.**
    a) See the smartphone section of my "Simple Backup Strategy for Home Computers" document.
    b) If you allow items from your phone to be stored in the Cloud (like Apple's iCloud, etc.), then make sure to have VERY strong security and password for your Cloud/online account, including 2FA enabled.
14) **Run a Mobile Threat Defense (MTD) program (like Antivirus on a computer)**
    a) MTD programs defend against malicious apps and network attacks.
    b) Some of the most highly rated and respected in the corporate arena may have free versions, such as: Lookout and Symantec Endpoint Protection (SEP) Mobile.
15) **Install a Security App to help find your lost phone and remotely wipe data if necessary**
    a) For the iPhone, you can use the built-in "Find My" app. Just activate it on your device.
    b) For Android, you need a third-party app to do this. (Consider the Lookout app.)
    c) See Resources below for links to other anti-theft software.

For the Extra "Privacy Conscious" User: If you are especially sensitive about your privacy, please consider the following additional steps:

16) **Manage your Location Settings. Consider which apps you allow to track you, especially when you are not using the app!**
    a) Read the permissions an app is asking for when you install it. Be aware and don't give away more information about yourself than you mean to.
    b) Some apps can be configured to only allow location services when you are using that app; this is preferred for a good balance of usability and privacy.
17) **Consider disabling access to "Siri" or "Google Assistant" (etc.) when your smartphone is locked.**
    a) The more convenience items you allow into your phone (without entering your PIN) make it easier to find out more information about you and your associates if it falls into the wrong hands. Consider your risk situation versus the convenience you require.
    b) Also, consider, do you always want your smartphone (and thus Apple or Google) listening to everything you say?! (It must do this in order to hear when you say, "Hey Siri"; think about it.)

Hostile Environments: If you live or operate in a hostile environment (e.g. where your government may oppress freedom of speech, or there are sophisticated militant groups, etc.), or if you are especially concerned about security due to the nature of your business, then you should strongly consider these following steps, besides getting professional consulting for personalized advice.
Make sure the read the "**Real-time Surveillance**" paragraph at the start of this document.

18) **You must take the advice in #1 and #2 above very seriously!! Make sure to have a smartphone that allows you to regularly apply security updates, and keep it (and all apps) updated.**
    a) If you don't do this, then you must assume that your phone can easily be compromised and thus ALL your communications are being read, including all emails, all text/SMS messages, and anything you type or say using any app (even if you think you are using a "secure" app like Signal, etc.).
    b) Furthermore, you should **not buy refurbished smartphones**. If you get a phone that has not been controlled from the manufacturer to the point of sale, then you have no idea of the types of spyware or surveillance software that could be installed on the device.
    c) Consider **where you purchase** your device. Be aware that some countries (such as Russia and China) may require distributors to pre-install software on a device purchased in that country. These apps can be used to track you.
    d) Androids: This also most likely means that you should **not buy a cheap Android** smartphone! Most cheap Androids from less-well-known manufacturers will NOT regularly push out the security patches that come from Google.
        i) The same caution should be applied to certain cell phone carriers since Android updates must come through your carrier. If you believe your phone service provider is working with the government and could insert surveillance capabilities in a software update, then you should consider a different cell phone provider (if possible); or just assume you are being tracked and act accordingly.

19) **If you are concerned about text/SMS messages being intercepted, use an end-to-end encrypted app, such as WhatsApp, Signal, Wickr, or Skype.** (Do not use Skype in China.)
    a) Standard text/SMS messages between phones can be read by the government or your phone service provider. If you want your text/SMS messages to be encrypted in transit, it is best for all parties to use an app such as WhatsApp, Slack, Signal, Wickr, or Skype.
        i) However, when you text from one iPhone to another (using the built-in iMessage app), the message is encrypted by default.
        ii) The same cannot be said about any Android messaging app; just assume texts/SMS messages sent on built-in Android apps are unencrypted and can be read by your cell phone carrier and the local government.
        iii) Be aware that WhatsApp is owned by Facebook/Meta; if you contact someone via WhatsApp, then Facebook will see them as a potential connection; that data may be more easily leaked.

20) **If you are concerned about eavesdropping on voice/phone calls, use an end-to-end encrypted app that allows for real-time voice conversations, such as WhatsApp, Signal, Wickr, FaceTime** (iPhone only)**, or Skype.** (Do not use Skype in China.)
    a) Voice conversations using wired phone or cellphone communication can be heard by the government or your phone service. If you want your voice conversations to be encrypted in transit, it is best to use an app such as WhatsApp, Signal, Wickr, FaceTime, or Skype.
    b) Be aware that WhatsApp is owned by Facebook/Meta; if you contact someone via WhatsApp, then Facebook will see them as a potential connection; that data may be more easily leaked.

21) **Biometric access (i.e. fingerprint or facial recognition) will be less-secure in a hostile situation.**
    a) Using your fingerprint or facial recognition for accessing your smartphone is an excellent option in a semi-friendly environment, but it should be turned off in a hostile environment or before crossing international borders (or other forms of security checkpoints).

b) If someone has detained both you and your smartphone, they can use your biometrics to unlock the device without your permission.

22) **If your smartphone has been in the hands of an advanced adversary or government employee (especially if it is "unlocked"), then assume it is compromised and everything you do is being read/monitored.**
   a) Once you lose physical control of your smartphone, stealthy spy software can be installed on your phone. It will track your every move (physical location) and read everything you type, say, or do on (or in the presence of) your smartphone.
   b) Even a "locked" smartphone may be compromised by a sophisticated threat actor.
   c) You should completely wipe your phone and set it back to default to remove this software. Depending on the sophistication of your adversary, you may want to consider just getting a new device altogether.

23) **Your phone can be used to track your location, as well reveal all the phones near you.**
   a) Government actors, in conjunction with telephone companies, can use your phone as a real-time surveillance device, to track your location, as well as listen to your conversations.
   b) Furthermore, other phones in your vicinity can be associated with your location, thus making connections between you and others. Associations between individuals can be used as incriminating evidence.
   c) To combat this threat, you must either remove the phone battery, or put your device in a Faraday bag, or wrap in a couple layers of tinfoil (where NO electronic signals can get to it). Turning your phone "off" does not stop these associations from occurring.

24) **Even if your smartphone is turned "OFF", it can still be used as a microphone.**
   a) Government actors, in conjunction with telephone companies, can use your phone as a real-time surveillance microphone, even if it is turned off . "Off" mode is merely a software setting; it is not "physically" turned off.
   b) To combat this threat, you must either remove the phone battery, or put your device in a Faraday bag, or wrap it in a couple layers of tinfoil (where NO electronic signals can get to it).

Resources for Smartphone Security

- See this site for information on preventing device theft: www.ctia.org/consumer-resources/preventing-device-theft

iPhone Security (These articles show actual steps to make secure.)
- 7 Tips to Improve iPhone Security: www.lifewire.com/tips-to-improve-iphone-security-2000265
- iPhone Security Secrets: 8 Apps and Settings You Must Know: www.makeuseof.com/tag/iphone-security-apps-settings
- Things To Do on Your iPhone to Stop Government Spying: www.lifewire.com/stop-government-spying-on-iphone-4129071

Android Security
- What are Android Security Updates and Why do They Matter? (includes a section on which manufacturers and carriers are best and getting out security updates): www.androidauthority.com/android-security-updates-960483
- 6 Easy Ways to Keep your Android Phone Secure: www.pcworld.com/article/3187451/android/6-easy-ways-to-keep-your-android-phone-secure.html
- Other Android antivirus solutions: www.tomsguide.com/best-picks/best-android-antivirus or www.av-test.org/en/antivirus/mobile-devices/

Spy Software – Be aware that commercially and custom-made spy software is available, especially for repressive governmental regimes. If someone installs this on your smartphone, it is "game over" as far as having any semblance of privacy. If someone gets physical control of your device and installs software like this, you won't even know it is there. For instance, just read the features of this one as an eye-opening example: https://xnspy.com/features.html

Examples of Smartphone Hacking – KEEP YOUR DEVICE PATCHED!

- Zero-Click 'Wormable' Wi-Fi Exploit to Hack iPhones: thehackernews.com/2020/12/google-hacker-details-zero-click.html "The exploit makes it possible to view all the photos, read all the email, copy all the private messages and monitor everything which happens on [the device] in real-time"
- Pegasus software used to hack into iPhones: www.washingtonpost.com/technology/2021/09/13/pegasus-spyware-new-exploit-apple/ "The "zero click" capability of Pegasus allows the spyware to install itself on a phone without the owner doing anything, such as clicking a link. The spyware can then turn the phone into a spy device, recording from its cameras and microphones and sending location data, messages, call logs and emails back to NSO's client."
- Q&A: A guide to 'spyware' "How Pegasus works, who is most vulnerable and why it's hard to protect yourself from hacks" www.washingtonpost.com/technology/2021/07/18/what-to-know-spyware-pegasus/