ANDROID PRIVACY & SECURITY GUIDE

Smartphones store a lot of personal information, including email or social media accounts, reminders and notes, the number of steps we take each day, and even personal biometric data, such as fingerprints. While all this can make life easier, abusers and stalkers can also misuse this information to monitor, control, and harass victims.

Android phones are the most commonly used smartphones in Australia. This guide will help users enhance security and privacy when using their Android smartphone. Although all android phones use the same operating system, depending on who made the phone (Samsung, Motorola, HTC), each phone's settings can be quite different. Use this handout as a general guide, rather than step-by-step instructions.

Essentially, there are two areas to look at when increasing your smartphone's privacy and security: (1) the privacy and security mechanisms built into your device (which may be slightly different depending on the maker of your phone) and (2) the Google account (which is essential to all Android smartphones) associated with your smartphone.

ANDROID DEVICE SETTINGS

Although each Android phone will have slightly different settings, there are some standard privacy and security settings you can use that will give you more control over the information on your device. Although time-consuming, one of the best ways to ensure that your phone is as private and secure as possible, is to go through each setting. This will help you learn what each setting does, how much control you have over your device, and how much information is stored and potentially shareable on your device. It's best to go through each setting; however, the following are some major privacy or security settings to start with.

Screen lock and passcodes

The most obvious, but important security setting you should start with is securing your Android phone with a passcode. This will prevent anyone from picking up your device and going through it while unattended. Depending on your Android phone, you will probably have many passcode options to choose from. The most common pass code is a 4-digit code. Other options include a custom numeric code, an alphanumeric code (combination of numbers and letters), or a pattern. Some Android phones include options such as face recognition or fingerprint recognition. Although it may seem that the face recognition is most secure (since only you have your face – unless you're an identical twin), for now, facial recognition as a passlock isn't very secure. On most Androids, you can find the passcode options under Settings / Lock screen and security.

Some Androids will have additional settings, such as deciding whether notifications or shortcuts should be visible even when your phone is locked. Whether you choose to display that information depends on whether you would be comfortable if someone picked up your device and saw that information. You can find this under Settings / Lock screen and security.

Smart lock

The newer Android OS has a feature called Smart Lock, which will unlock your phone if you are at a "trusted location," such as at home; if the smartphone wants to connect to a "trusted device," such as your Bluetooth speaker; on your body; if the person looking at your phone is recognised as a "trusted face," or if your device recognises your voice as a "trusted voice." Under these circumstances, your smartphone will unlock without you needing to put in a passcode. While Smart Lock can be convenient to use – for example, you're juggling bags and opening doors and need to unlock your phone – it can also make it easier for someone else to have access to your phone. Think about your own privacy concerns and balance convenience with privacy and security. You can generally find this setting under Settings / Lock screen and security / Secure lock settings/ Smart Lock.

Location settings

Location is another setting you should check on your Android. You can generally find this under Privacy and safety. Under Location settings, you have the option of turning your location on or off (globally for all apps). Under this setting, you will also be able to see which apps have recently requested your location. If you don't want a specific app to have access to your location, you will need to go into each specific app and manually turn the location off. For the most privacy, turn off the location if you aren't using it. You can always turn the location back on when you need to use the app.

Another setting under Location is to decide how your location is accessed, whether it is via GPS, Wi-Fi, mobile networks, all those options, or a combination of those options. In general, when all location options are turned on, your location will be most accurate. This is important if you are using safety apps that need to know your exact location. Some people may choose GPS or mobile networks only, to save their battery.

Bluetooth settings

Another setting to turn off if you're not using it is Bluetooth. If you've ever connected with a Bluetooth device, which could be your car, speakers, or even a printer, it could automatically connect once you're in range. Turning off Bluetooth will prevent the automatic connection and you can turn it back own when you need it. This setting can generally be found under Settings / Bluetooth.

App's access to device content

When you download an app, you will get a window message that tells you what content on your smartphone the app will need access to, such as: contacts, calendar, photos, camera, microphone, sms, sensors, storage, etc. On the latest Android OS, you can pick and choose which content a particular app can have access to under Settings / Apps / App Permissions. Under each category, you will see which app wants access to that content and you can turn on or off the access to that content. On Android phones running older operating systems, you may need to go to the "application manager" and go through each app manually.

In some cases, you may not have an option to deny a particular app's access to your smartphone content, or if you don't allow it to access, the app may not work properly. For example, Google maps need access to your location in order to give you directions. In these situations, determine if you're comfortable allowing the app access to your device content vs. how much you need to use the app.

Installing apps from unknown sources

Another setting to turn off is not allowing apps outside of the Google Play store to be installed on your device. Unlike the iPhone, your Android phone allows you to install apps outside of the Google Play store, such as from a website or via your computer. This is often how smartphone spyware and other malware gets installed, so it's important that this is turned off. You can find that setting under Lock screen and security / Unknown sources.

Encryption

Your device is likely already encrypted by the manufacturer if you are running Android OS marshmallow or above. Otherwise, if you're really concerned about security, one more setting to turn on is encryption, which can be found under Settings / Security / Encryption. An encrypted phone will make it more difficult for someone to access the data on your phone unless they have the encryption key, which is usually your passcode.

You can also choose to additionally encrypt your SD card (even if your phone comes already encrypted). You can generally find this setting under Lock screen and security/ Encrypt SD card. Note that encrypted SD cards can only be read on the device used to encrypt them.

Backup and reset

Android phones offer many ways to back up the data on your phone. Google Back up & Restore not only backs up your phone content, it also will back up all your Google app data, such as calendar, Chrome browser, contacts, photos. Once backed up, if you have to set up a new phone, just log in with your Google account and all your data will be synced. While incredibly convenient, it's important to ensure that your Google account is secure. Take advantage of Google two-step notification so if someone else were to sign into your account, you will know.

Another method of backing up your account data is through online cloud services, such as Google Drive or Dropbox. Many people use these services to back up their photos or videos. Again, while convenient and helpful in clearing up space on your Android, be sure that your account is secure when using these services.

GOOGLE ACCOUNT AND SERVICES

Since the Android mobile operating system is built by Google, your Android smartphone is intimately connected to the Google platform. In order to purchase apps through the Google Play store, you will need a Google account. For most users, that Google account will also be used for all the other Google products and services on the device, including Gmail, calendar, contacts, Chrome browser, YouTube, etc. Having all those services connected to one account can be convenient and helpful. For example, when you look at a website on your Android's Chrome browser, the Chrome browser on your laptop will remember it in its history. Your browser history is saved to your account, as well as on the specific device.

Depending on your situation, you may find it really valuable and helpful to have your information saved and integrated across devices under one account, or you may require more privacy and not want your information to be remembered across devices. If all those services were under one account and someone should gain access to your Google account, they will learn quite a lot about your phone activity. The good news is that Google does give users a lot of privacy options. Below are some suggestions for more privacy and less connection.

Go through Google Settings

Google gives you a lot of choices to increase your privacy and security while using their products, which you can find in Google settings. You can access these settings on your Android by going to Settings / Google. You can also access these settings online (via a web browser) at https://myaccount.google.com. We suggest going through all the settings. This is the best way to be aware of and increase your privacy and security. An easy way to do this is to go through Google's "Security Check Up" as well as their "Privacy Check Up" (both can be done from within your settings on your phone or via your browser). Below are some settings to go through, but keep in mind that this is not an exhaustive list, and we highly encourage you to go through all your Google settings to meet your specific privacy and security needs.

Minimise Google's collection of device activity

One way to prevent Google from collecting your information is to go through your settings and set it to not collect your activity. You can find these settings under Settings / Google / Personal info & privacy / Activity controls. Here, you can go through and set up your preferences regarding which of your activities Google remembers and saves to your Google account (i.e. "Web & App Activity," "Location History," "Device

Information," "Voice & Audio Activity," "YouTube Search History," and "YouTube Watch History"). Choose "pause" to stop Google from collecting this information. Keep in mind however, that pausing the tracking of any of the above activities does not delete previously recorded activities. To delete those, you will need to do that separately through the "Review Activity" settings. This can be accessed through your settings / Google/ Personal info & privacy /My activity. Also keep in mind that even if the setting is paused, Google may still temporarily track some of your activities (i.e., web searches to improve the quality of your current search session).

Pay special attention to location history
Another area to turn off is Location History. When this is turned on, Google will track everywhere you go through your smartphone. (This is different from using Google maps.) The purpose of this is so Google can recommend improved map searches, etc. However, from a privacy perspective, if someone were to gain access to your Google account they could see everywhere you have gone (and possibly predict where you will go). Determine if your privacy risks of someone knowing everywhere you go outweighs the convenience of a quicker map search or a Google recommendation based on your current location. Turn off location history by going to Settings / Personal info & privacy / Your personal info / Location sharing.

Find my phone
Many people will use the "find my phone" feature to track down their phone's location if it is lost or stolen. However, if someone were to have access to your Google account, they could sign into your account and find where your phone is through this feature. Whether you use this setting is up to you. Consider the security of your Google account and how likely it could be that someone could use this to track your location vs. the security of being able to find your phone it is lost or stolen.

Remove connected devices and apps

Your Google account can be logged onto from multiple devices (such as an android and laptop). To help you manage where you've connected, Google will tell you which devices have accessed your account in the last 28 days or are currently logged in. You can find this from your settings on your phone under Google / Sign-in & security / Recently used devices. If there are connected devices you don't recognise or you logged in somewhere and forgot to log off, this is where you can remove those device's access. This is also helpful if you lose your Android and need to disconnect the device from your Google account.

Remember that your Google account can also be logged into other accounts, such as apps or other online services. Unless you know your Google account is secure and you are comfortable using it to sign into other accounts, it is generally best to create new username and passwords when signing into other online accounts. However, if you do choose to use your Google account, you can check which apps and or online accounts your Google account is signed into. Go to Settings / Sign-in & security / Connected apps & sites to check or remove access to any apps or accounts.

Sign out of Google products on the Android

While some Google services require you to sign in to be able to access it – such as Gmail or the Google Play store, not every Google product requires you to sign in for it to work. When you are signed out, what you do on those apps will not be saved into your Google account. However, keep in mind that while your Google account won't remember your activities, the app on your Android will remember. For example, if you're not logged in while using the Chrome app on your Android, your Google account won't remember what websites you visited, but your website browsing history will be saved in your Android's Chrome app. If you don't want any trail, consider deleting your Chrome browsing history or use the Incognito mode.

ADDITIONAL ANDROID SECURITY

Security apps

While the Android phone itself has built-in security settings, if you're very concerned about the security of your phone, you can download a security app. Third-party security apps have a wide range of features, including malware and virus protection, tracking your phone if it gets lost or stolen, or remotely wiping all the data off your phone.

You could also download specific anti-malware apps, which will protect your phone for getting viruses or prevent other types of malicious software from installing. Depending on the type of Android smartphone you have, it may already come with anti-malware protection. If it does not (or you want to explore other options), you can go to the Google Play store and do a search for anti-malware apps. Another way of looking for good anti-malware apps is to google "best anti-malware apps for Android" and read the reviews.

When downloading third-party apps from the Google play store, look at the reviews. The closer it is rated to 5 stars, the better, but also look at how many people have downloaded the app, and check out the reviews.

"Rooting" your Android

Some people will "root" their Android, which is a process that allows you to modify the Android operating software code and install other software blocked by the manufacturer (the equivalent term for Apple devices is jailbreaking). Unfortunately, a rooted phone can be more vulnerable to malware and spyware, void your warranty, and make software updates impossible. Software updates are important because they can include security patches and make your phone less vulnerable to hacking. One possible way to know if your Android is rooted is to download a root-checker app from the Play Store. To "unroot" your phone, Google instructions online for detailed instructions since there is more than one way to "unroot" your Android.