INCREASING PRIVACY AND SECURITY WHEN USING GOOGLE

If you use any of Google's products (Maps, Gmail, YouTube), Google is probably collecting personal information about you, your activities when using their services, and even your location all the time. Some of this information could be saved onto your account or device activity logs. For survivors of sexual assault, domestic violence, stalking and harassment, this comprehensive information of their life and habits could be used for malicious intent by their perpetrators. The ability to maximise the privacy and security of their Google account is crucial. The good news is that Google gives users a lot of privacy and security options.

Sign out of Google

The simplest way to minimise how much information Google collects about you is to sign out of your Google account. While some Google services require you to sign in to use them, such as Gmail, not every Google product requires you to sign in for it to work. However, keep in mind that while your Google account won't remember your activities, the Google app on your device will remember your activity unless you delete the browsing activity history. (Tip: if you're using Google Chrome, consider using the Incognito mode, which doesn't keep a history of your browsing activity. Remember, however, to close out of the app when you're done.)

Use two-step verification

The first step to increase security is to make sure you have a strong password to your Google account that others can't guess or know about. Additionally, an important security feature you may wish to turn on is two-step verification; when this feature is on, anytime you log into your account from a different device or location, you will need to provide secondary verification to prove that it's you logging in. Typically, the second verification is a code sent via text message to your phone. Find this setting under: Account/ Sign-in & security/ Signing in to Google.

Review location access

If your phone is connected to your Google account, there could be many ways in which Google is tracking your location.

"Find your phone"

For most Android phone owners, their Google account is the account set up on the phone. In the event that your phone is lost or stolen, you can track your phone through the Android Device Manager. From your Google account, you can try to locate your lost or stolen phone (either by ringing your phone or getting the GPS coordinates of where your phone is located), lock your phone, sign out of your Google account from your phone, or erase all the data on your Android. This means that if someone knew your Google account, they could use it to locate your phone. Make sure that your Google account is secure and that no one else can access your account when using this feature. The settings for this feature can be found from the web browser under: Account/ Sign-in & security. From your Android, you can generally find this feature under Settings/ Security.

"Location History"

Another way Google tracks your exact location is if Location History is turned on. Google will track everywhere you go while your location is on via your phone or tablet and you're signed into Google Maps. The purpose of this is so Google can recommend and improve map searches, etc. However, from a privacy perspective, if someone were to gain access to your Google account they would know exactly where you have been. Determine if the 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. The settings for this feature can be found under: Account/ Personal info & Privacy/ Your personal info.

Check to see where you're logged in

Because you can use your Google account on multiple devices (such as another phone, tablet, and laptop), Google lets you know which devices have accessed your account in the last 28 days or are currently logged in. If there are connected devices you don't recognise or you forgot to log off, you can see which devices are connected to your account and remove those devices' access. You can get to that setting from your Google account's "device activity & notification." This is also helpful if you lose your Android and need to disconnect the device from your Google account. The settings for this feature can be found under: Account/ Sign-in & security/ Device activity & notification.

Remove connected accounts and apps

For convenience, many apps and online services allow you to use your Google account to sign in. Although it is convenient to use your Google account to log into other apps or online services, be sure that your Google account is secure. If someone were to know your Google account and password, they could get into those other apps and services as well. From your Google account settings, you can review which apps and services are connected to your Google account and remove ones that you don't recognise or no longer use. The settings for this feature can be found under: Account/ Sign-in & security/ Connected apps & sites.

Minimise the information that Google collects about you

Google tracks and collects information about how you use their services to improve your Google experience. You can "pause" Google's collection of personal activity, whether it is web searches or browsing history in Google Chrome, Location History via your Google Maps, Voice or Audio clips that are saved to Google when you do a voice search, information from your smartphone when it's connected with your Google account, or YouTube Search & Watch Histories. The settings for controlling this access can be found under: Account/ Personal privacy & info/ Manage your Google activity/ Activity controls.

You can "pause" to stop Google from collecting this information. Keep in mind, however, that pausing the tracking of these activities will not delete previously recorded activities. To delete those, you will need to do that separately through the "Review Activity" settings (also in the Personal info & privacy section). Also be aware that even if the setting is paused and deleted from the "Review Activity" settings, some of your activities may be stored locally; for example, Google searches might be stored in the browser history of your phone or tablet.

Minimise information sharing between your smartphone and Google

If you have an Android phone or are a Google user, it might be difficult to separate your smartphone content from Google. However, Google does give you some options to minimise how much of your smartphone content gets shared with Google. Under "Activity controls," review "Device Information" settings and limit the information it shares. Device content can include contacts, calendars, apps, music, and other device data.

Use Google's Check Ups

One way to check all your settings at once is to go through Google's Security Check Up and Privacy Check Up. Each check up will walk you through each privacy or security setting to ensure that you are choosing security and privacy settings that work best for your situation or preferences. This is one of the easiest ways to ensure that your privacy and security settings are right for you.