INCREASING PRIVACY AND SECURITY WHEN USING GOOGLE

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of June 2025.

If you use any of Google's products, such as Maps, Gmail, YouTube, Meet, or Chat, it is likely that Google is tracking your location and collecting information about you and your online activities while using their services. This information may be stored in your account or device activity logs. For survivors of sexual assault, domestic violence, stalking, and harassment, this detailed personal information could be misused by a perpetrator. Therefore, it is crucial to maximise the privacy and security of your Google Account. The good news is that Google offers users a wide range of options.

Sign out of Google

The simplest way to minimise the amount of information Google collects about you is to sign out of your Google Account when you're not using it. While some Google services, like Gmail, require you to be signed in for them to function, not all Google products have this requirement. Remember that although your Google Account won't track your activities, the Google app on your device will unless you delete your browsing history.

Tip: Consider using Google Chrome in Incognito mode, as it doesn't save your browsing activity. Also, sign out of the account or app when you're done rather than just closing the current window to end the browser session.

Use 2-Step Verification

To enhance your security, the first step is to create a long, strong passphrase for your Google Account that is difficult for others to guess or decipher. A highly important security feature you should consider enabling is 2-Step Verification. When this feature is enabled, you will need to provide a secondary verification whenever you log in from a different device or location. This typically involves entering a code sent to your phone via text message. Still, a more secure option in most cases is a code generated from an authenticator app. This setting is under ***Account > Security > How you sign in to Google > 2-Step Verification***.

Review location access

If your phone is connected to your Google Account, Google may track your location in several ways.

Find My Device

Android phone owners need a Google Account to activate various phone features. Once a device is linked to a Google Account, the owner can track the phone using the Android Device Manager if it is lost or stolen. Through their Google Account, they can locate their lost or stolen phone — either by ringing it or retrieving its GPS coordinates. They also have the option to lock their phone, sign out of their Google Account, or wipe all the data on it.

Tip: *To secure or erase an Android device, ensure that the device has power, is connected to mobile data or Wi-Fi, is signed in to a Google Account, has* ***Find My Device*** enabled and is visible on ***Google Play***.

What this means is that if someone gains access to your Google Account, they could potentially locate your phone or do any of these things. Therefore, ensuring that your Google Account is secure and that no unauthorised person or device has access is vital. You can Manage Settings under ***Account > Security > Your devices.*** On your Android device, this setting is under ***Services > Security***.

Timeline

Google tracks your exact location through mobile devices using Google Maps when the Timeline feature and location are enabled and the battery saver is turned off. This tracking helps improve search recommendations and map functionality. However, from a privacy standpoint, if someone gains access to your Google Account, they could find out exactly where you are and where you have been. Consider whether the privacy risks of sharing this information outweigh the convenience of faster map searches or localised Google results.

If you want to pause this feature, you can navigate to ***Account > Data & privacy > Things you've done and places you've been > History settings > Timeline***. In this section, you can also manage your past activity or choose to 'Auto-delete' your activity history after 3 months, 18 months or 36 months.

Google Maps

You can apply the date filter to manage past activity via the Google Maps app under ***You > Explore Timeline***.

"Web & App Activity"

Google also tracks your location through Web & App Activity, even when using an Incognito window. To pause this feature, navigate to ***Account > Data & privacy > Things you've done and places you've been > History settings > Web & App Activity***. You can also request Google to manage past activity or 'Auto-delete' your activity history.

"Location Sharing"

While the real-time Location Sharing feature, located under: ***Account > Data and privacy > Info that you can share with others > Location sharing***, can be helpful in staying connected and safe, it also carries risks. If someone with malicious intent gains access to your account, they could misuse this feature. Ensure to check that you are not accidentally sharing this information when you don't want to be sharing it.

Check to see where you're logged in

You can use your Google Account on multiple devices, including phones, tablets, and laptops. To track which devices have accessed your account in the last 28 days or are currently logged in, navigate to ***Account > Security > Your devices > Manage all devices***. If you see any devices that you don't recognise, that you know shouldn't be connected, or that you forgot to log out of, you can review the device name and general location before deciding whether to remove access permissions. This is also useful if you lose an Android device and need to disconnect it from your Google Account.

Remember that if you have granted access to third-party apps on your device, such as Google Chrome, those apps may still be able to access your Google Account. If this is the case, you will receive a notification to revoke access under ***Account > Security > Your connections to third-party apps and services > See all connections***.

Remove connected accounts and apps

For convenience, many apps and online services allow you to sign in using your Google Account; therefore, it's essential to ensure that your account is secure. If someone gains access to your Google Account login credentials, they could also access those other apps and services.

To manage security, you can review which apps and services are linked to your Google Account from your settings. If you notice any that you don't recognise or no longer use, you can remove them by navigating to: ***Account > Security > Your connections to third-party apps and services > See all connections.***

Minimise the information that Google collects about you

Google tracks and collects information about how you use their services to enhance your experience and for marketing purposes. You can "pause" Google's collection of personal activity under ***Account > Data and privacy > Things you've done and places you've been > History settings > My Activity***.

This pauses activities including:

(a) Web searches and browsing history in Google Chrome,
(b) Location History through Google Maps,
(c) Voice or audio clips saved by Google when you perform a voice search,
(d) Information from your mobile device related to your Google Account, and
(e) YouTube search and Watch Histories

You can "pause" Google from collecting your information, but this will not delete any previously recorded activities. To manage this easily, navigate to ***Account > Data and privacy > Things you've done and places you've been > History settings***. Keep in mind that even if you pause the setting and delete activities from My Activity, some of your actions may still be stored locally. For instance, Google Chrome searches might remain in the browser history on your phone or tablet.

Minimise information sharing between your smartphone and Google

If you use an Android phone or have a Google Account, managing your smartphone content separately from Google can be challenging. However, Google provides options to control which content is shared under ***Account > People and sharing***. We recommend checking the settings and adjusting them to suit your current situation.

Utilise Google's Security and Privacy Checkups

To review all your settings at once, you can use Google's Security and Privacy Check-up tools. Access the Security Check-up under ***Account > Security > You have security recommendations > Security Check-up***. If your account states "Your account is protected", you're all good! For the Privacy Check-up, navigate to ***Account > Data and privacy > Take Privacy Check-Up***. Each will guide you through various privacy and security settings, helping you ensure that your account is as private and secure as necessary to suit your situation and preferences.

When you are concerned someone else has accessed your account

If you suspect that another person has accessed your Google Account, we recommend taking the following steps:

1. Review your recent logins to check for any unfamiliar activity.
2. Verify that your recovery email and phone number are current, secure and accurate.
3. Ensure that your emails are not being forwarded elsewhere without your permission.
4. Secure your account by creating a new, long, and strong passphrase using a safe device and a secure network.

We also recommend that you periodically download your data for documentation purposes. Head to ***Account > Data and privacy > Data from apps and services that you use > Download or delete your data > Download your data > Google Takeout***.