Who is this guide for?
If you have an Android phone, this guide will help you review how your phone is configured. This means that we will review important settings that determine what information is collected, where it is saved, and with whom it is shared. It is particularly oriented towards intimate partner violence threats.

What does this guide cover?
- Securing your phones Google Account configuration
- Locating and securing back ups
- Checking for stalkerware and spyware
  - Sensitive permissions
  - Google PlayProtect
- Understanding and screening for rare attacks

Aspects to take into account
- We strongly recommend that you talk to a domestic violence or other appropriate organization to make plans for your safety if you are worried about violence. Information about safety planning and/or local domestic violence agencies can be found [https://thehotline.org](https://thehotline.org).
- Some steps in these guides may, directly or indirectly, notify an abuser of your actions. For example, they may receive an alert that you have changed a password or notice that they can no longer read your messages.

Be careful!
- This action could be visible to the abuser

- All images included in this guide are for educational purposes only.
Introduction

Android phones refer to phones running an operating system developed by Google. An operating system is the non-physical software that runs on the physical device and makes it work. Unlike Apple phones where the operating system software can only run on the physical devices made by Apple, Android phones can run on physical devices made by almost any phone manufacturer, such as Samsung, LG, Motorola, Blackberry, Nokia, and more. If you do not have an Apple phone, you most likely have an Android.
This makes Android phones highly customizable, but it means that developing a single guide across all types of manufactures is difficult, as menus and settings may vary across manufacturers. Consequently, screenshots may not reflect exactly what you see on your Android. Nonetheless, we have made an effort to develop a guide that is as general as possible, and point out along the way where there may be some variation.

Shared Phone Plans

If you share a phone plan with another person, they will be able to have access to information about what your phone is doing, especially if they are the account holder. The owner of the account (or anyone authorized to manage the account) can view information such as call logs, phone numbers of people who have been texted from that phone, and potentially other information.

The information in this guide can increase the security of your device, but it cannot prevent information from being accessed via a shared phone plan. The only solution is to leave the shared phone plan. The Safe Connections Act is a federal law requiring phone companies to allow survivors of domestic violence and their dependents to leave a phone contract. It requires documentation such as an attestation from a social worker or an order of protection. If you are interested in this option, please discuss it with a local domestic violence response professional.

Configuring Your Google Account(s)

While it is possible to use an Android phone without a Google account (or Gmail account—they are the same thing), in practice, most users create or register a Google/Gmail account. A Google account is the same thing as a Gmail account. You can view the Google/Gmail accounts registered to most Androids by going to Settings → Google. In this section, we review steps to take to ensure the reader is aware of which Google accounts are connected to their Android phone and that each account is secure.

Google/Gmail Account Safety

Because Android phones are often registered to a Google/Gmail account, we strongly recommend that the first step the reader takes is to review how their Google/Gmail account is set up in our Google + Gmail Safety Guide on our resources page.

⚠ If the registered account is compromised, an unauthorized user or abusive person may be able to see sensitive information such as location information, emails, text messages and more.

We have linked to this guide here. At the end of the guide, it will direct the reader back to this guide.
Check which Google accounts are attached to your Android

First, navigate to the main Settings page. This may depend on which version you have. On newer versions:

- Tap on the notification bar at the top of the home screen and pull down to view the notifications and quick settings.
- Then tap on the quick settings section and pull down again to view more settings.
- You should see a small gear icon among other settings. Tap on this to get to settings.

If this does not work for you, you can try the following:

- Go to All Apps, by tapping on it or swiping up.
- Search for Settings and tap on it.
On Android version 11:

On Android version 11 or older, scroll through Settings and tap on Accounts. You will see a list of associated Google/Gmail accounts.

On Android version 12+:

On Android versions 12 or later, go to Passwords & Accounts from the Settings menu. There you will see accounts associated with your phone under “Accounts for”.

Remove unrecognized Google/Gmail accounts

Be careful!
This action could be visible to the abuser
If you see a Google or Gmail account that you do not recognize on any version of Android, you can tap on the account for more information, where you will have the option to remove it. Removing an account will notify anyone with access to the account, so be especially careful to consult with a trained advocate if you are concerned about retaliation.

Finding and Securing Backups

What is a backup application?

A backup application is software that automatically saves a copy of information from a device in another location. It is similar to making a photocopy of a physical document and storing it separately from the original document, in case the original is damaged or lost. A properly configured backup is useful if your phone is damaged or lost, but it is important to make sure that you know who has access to the backups. An unauthorized user or abusive person with access to backups may be able to see, for example, text messages, emails, and photographs.

Many Android phones come with a backup application pre-installed. Android phones will often use an application called Google One as the backup application. Depending on the phone manufacturer, there may be multiple backup applications. For example, Samsung also has Samsung Cloud in addition to Google One, while OnePlus has its own cloud application.

Backups may have old text messages, photos, videos etc that have been deleted from your phone. This may be helpful, in that you can recover missing and needed data like text messages and photos. It can also be harmful, in that an abusive person could still see items that you believe you have deleted.
Google One
Google’s official documentation for this is here: Back up or restore data on your Android device. The following can be backed up using Google One:

- Apps
- Call History
- Device Settings
- Contacts
- Calendar
- SMS (Pixel phones only)
- Photos & videos (Pixel phones only)

Check if backup to Google One is turned on

To check if you are using Google One for a back up, go to Settings → System → Backup. You will be able to see if it is turned on or off from the menu. Tap on Backup for more information.
If Backup to Google One is currently turned off:

If backup to Google One is currently turned off, you will see the above screen and have the option to turn it on. This can have benefits, like freeing up space on your phone, and allowing you to recover information if your phone is lost or stolen.

However, it is very important to make sure that the Google account that you are using with Google One (blacked out in the image above, before @gmail.com) is an account that belongs to you and one that you have taken steps to secure. **If you enable back up to a Google account that an abuser may have access to, they will be able to see sensitive information in your phone.** To check the security of your Google account, [Google/Gmail Account Safety Guide](https://accounts.google.com/AccountSettings?hl=en&authuser=0).
If Backup to Google One is turned on:

If backups to Google One are turned on, you have the option to turn it off by selecting the blue toggle.

Be careful!

This action could be visible to the abuser

Turning off backups will not delete data that has already been backed up, and may alert anyone actively monitoring Google One for backups. You can delete backed up data by selecting a backup item and tapping delete.
Managing backups through Google Drive on a laptop or desktop

You can also manage Google-driven backups on a laptop or computer. To do so, open up a web browser and go to https://drive.google.com. You will need to log-in to the Google account associated with your Android using the email and password if you are not already logged in.

On the left hand side menu, click on Storage.

At the top right, click on Backups. This page will show you a list of back ups for your device. You may delete individual back ups or click on them to learn more information about them.

Turn on extra security for Google Cloud Drive

Google Cloud Drive is managed by the same settings as your Google/Gmail account. Thus, it is again important to make sure that you have secured the associated Google/Gmail account. See our guide on Configuring Your Google Accounts for more information.

Checking for Other Backups

Your device may have other backups associated with it depending on the maker. Usually, you will see the backup application listed in the “Backups” menu. Some of the most common alternative backup applications that come with Android phones are listed below, along with links to their guides to manage their back ups.

- Samsung Cloud for Samsung devices
To manage Samsung Cloud backups, see their guide: [https://www.samsung.com/levant/support/mobile-devices/how-to-manage-samsung-cloud-on-the-browser/](https://www.samsung.com/levant/support/mobile-devices/how-to-manage-samsung-cloud-on-the-browser/)

- OnePlus:
  - To manage, see their guide: [https://www.oneplus.com/uk/support/answer/detail/op35](https://www.oneplus.com/uk/support/answer/detail/op35)

- LG Android:

---

**Issues Logging Into Google Account**

If your phone is attached to a Google account and you would like to manage the settings for it, but you are unable to log into the Google account (because you have forgotten the password or an abusive person has taken over the account), then it can unfortunately be difficult to manage or recover your backup information or Google settings.

Google has some limited steps you can take to try to recover an account here: [https://support.google.com/accounts/answer/7682439?hl=en](https://support.google.com/accounts/answer/7682439?hl=en)

However, if you are unsuccessful in recovering a Google account, there are limited options as there is no customer support for this issue.

Some suggestions are:
- Remove the account from your phone if possible.
- Take steps to set up a new Google account that is safe to use with your device.
- Register your device with the new and safe Google account.

---

**Checking for Spyware/Stalkerware**

Spyware, stalkerware, and malware are all names for applications that can be installed on a phone with the purpose of secretly collecting information and sharing it without the knowledge or permission of the phone’s owner. In general, it is very difficult for someone to install spyware on an updated Android phone unless they had physical access to the phone. That is why we first recommend checking your Android software version.

**Checking Your Android Software Version**

Modern versions of Android have more protections against stalkerware and spyware. The following instructions will help you find which Android version you have and update it if an update is available.
1. Open your phone’s Settings app.
2. Tap About phone → Android version.

In the menu below, the **Android version** field tells you your current Android version. **Android security update** will tell you if there is an available update for your phone. We recommend installing all security updates.

### Check if Google PlayProtect is Turned Off

Stalkerware or spyware would likely need to turn off Google PlayProtect to be installed. Note that this is not true for dual-use apps.

To check if Google PlayProtect has been turned off, open the **Google Play app**, either on the home screen or by searching all applications. The icon may look different depending on your version but usually has an icon similar to the one below:

![Google Play icon](image)

Tap on the Google Play icon, and then tap on the profile icon upper right hand corner (circled in red. Then tap **PlayProtect** from the menu that opens up.
In the next screen, **PlayProtect** will alert you if any harmful apps have been found. If so, you can tap on the app for more information. You will also be able to uninstall the app. If the app is being used by an abusive person to monitor your phone, please be aware that uninstalling the app may send a notification to that person; if you have concerns about your safety, consider reaching out to a local domestic violence agency to plan for your safety.

![Be careful!](image)

**Be careful!**
This action could be visible to the abuser

To double check that PlayProtect is scanning all your apps, you can tap on the gear icon in the upper right corner.

The first toggle ensures that the PlayProtect is being used to scan applications on your phone, which we recommend. The second toggle does not directly affect PlayProtect’s effectiveness, but sends information to Google so they can modify the app.

**Manually Checking for Spyware**

If your Android software version is not up-to-date, or you believe someone with physical access to your phone may have installed something malicious on your phone, you can manually check for spyware. Spyware will need to ask for permissions from the Android operating system to view sensitive information such as location, text messages, or keyboard access. We recommend screening for spyware by examining applications asking for sensitive permissions.
Checking Apps that Request Location Permissions

One of the most common permissions that spyware would request is the location of the device. Even if an app is not spyware and has a legitimate purpose, if the app has sharing features or if an abusive person is also logged into the app, it may inadvertently share your location. Thus, it is good to know which apps are tracking your location. The official Google documentation about Location permissions is here: https://support.google.com/accounts/answer/6179507?hl=en

To review apps with access to location information, open the Settings app. Go to Location -> App Location Permissions. Then review apps that have access to your location.

![Settings](image)

Be careful!

This action could be visible to the abuser

If you see an application that you don’t recognize or don’t trust, then you can revoke its location permission access.

Looking at App Permissions

Suspicious or spying applications need to request permission from the Android operating system to access sensitive information. If you are unsure if an app that is downloaded on your phone might be spyware, you can check to see if it has requested suspicious permissions. The official Google documentation about App Permissions is here: https://support.google.com/googleplay/answer/9431959?hl=en

Open up the Settings app, and then scroll down until you see Apps. For the app that you are concerned about, tap on that app in the list and then tap Permissions. You can then see a list
of permissions requested.

Be careful!
This action could be visible to the abuser

If you see an app that you do not recognize and it is requesting many permissions, especially sensitive permissions such as SMS, Location, Microphone, and Keyboard then you may want to search for more information about the app or remove it.

Understanding and Fixing “Rooted” Android Devices

“Rooting” an Android device means taking full control over the phone, removing the limits on software that are put in place by default. This can allow someone to install malicious software or change the functionality of existing apps. Rooting requires physical access to the device and also typically requires more work and a higher degree of technical knowledge than other forms of technology abuse, like installing spyware. We find that, in practice, rooting attacks are not very common, and abusers are more likely to use simpler methods to harm their targets.

Determining whether a phone has been rooted can be difficult. However, if you are worried that your phone has been rooted because it is an older model or a person with high technical knowledge has had physical access to your phone, you can factory reset your phone which will
Warning!!!! A factory reset will delete all of your data from the phone, including contacts, text messages, and photos. It is an extreme step to take if you are concerned about your phone being ‘rooted.’ Keep in mind that if access to your phone is coming from an improperly configured app or Google account, factory resetting the phone will not solve the issue but you will lose a lot of data. It is important to back up any information on your phone that you would not want to lose before beginning a factory reset. We encourage you to speak with an IT specialist if you are interested in factory resetting your phone but are not sure about how about to back up your information.

On most Android phones, you can perform a factory reset by going to Settings → General and Back up → Reset → Factory data reset → Reset device and confirming your choice.