Tech Safe BC

Android Smartphone Safety Guide for Survivors of Tech Abuse

Compiled by Tech Safe BC

Last Updated: February 5, 2026

Symbols and What They Mean in This Guide:

Course of action may be visible to your former or current partner.
You may want to consult with a staff of an anti-violence program in your community before removing your former or current partner's access.

Evidence documentation checkpoint. Take screenshots, pictures with a different device, or screen recordings of your former or current partner's unauthorized access.

Android is a type of operating system developed by Google that can run smartphones by many types of manufacturers, including Samsung, LG, Motorola, Blackberry, Nokia, etc. The software is highly customizable, and so settings may vary across phones. This guide is largely based on resources from Google's Android Help website. If the settings menu on your Android phone looks different than in this guide, consider using the search functionality to navigate your settings and/or find your smartphone's support website. This resource is not endorsed nor sponsored by Google.

This guide is meant to assist you in increasing the security of your device, but it cannot prevent information from being shared via a shared phone plan, such as a family plan. Because Android phones are linked to a Google/Gmail account, review the steps in that guide in addition to the settings on your device.

Before taking any steps such as removing access to suspicious accounts or turning off location sharing, it is important to consider collecting evidence and discussing any potential safety concerns as a result of these changes with your support worker.

If something in this guide is no longer up to date, or difficult to understand, please reach out to techsafe@bcsth.ca with your concerns.

Device Settings

☐ Screen Lock

If you have not already, secure your device with a pass code. You can us a 4- or 6-digit code or pattern. You can also turn on face or fingerprint recognition.

To enable screen lock

1. In your Android smartphone, tap **Settings**.
2. Tap **Security**.
3. Tap **Screen Lock**.
4. Choose a different screen lock option and follow prompts.

To restrict notifications visible when the screen is locked

1. In your Android smartphone, tap **Settings**.
2. Tap **Apps & notifications.**
3. Tap **Notifications.**
4. Below the heading 'Lock screen,' tap either **Notifications on lock screen** or **On lock screen**.
5. Tap **Don't show notifications**.

Source: Android Help Screen Lock, Restricting Notifications

☐ Extend Unlock

The "Extend Unlock" feature, sometimes known as "Smart Lock" is a feature that will keep your screen unlocked when you are in a trusted place, near a trusted device, or if it detects that it is on your body. While convenient, consider turning it off to increase the security of your device.

To enable extend unlock

1. In your Android smartphone, tap **Settings**.
2. Tap **Security & privacy**.
    - Can't find this heading? Tap **Security & location** instead.
3. Tap **More security & privacy**.
4. Tap **Extend Unlock**.
5. Input your pass code or pattern.
6. Choose an option and follow the prompts.

Source: Android Help

☐ Checking Apps that Request Location Permissions

It is good to know which apps are tracking your location. While spyware is exceedingly rare, so called 'dual purpose apps' (such as Life360 or Find My) can be used to track your location.

Safety Tip:

Before revoking an app's location permission, consult with a support worker about potential safety concerns.

To review app location permissions

1. In your Android smartphone, tap **Settings**.
2. Tap **Location**.
3. Tap **App location permissions**.
4. Tap the app(s) you'd like to change its location permission.

Source: Android Help

Backup (the 'cloud')

☐ Finding and Securing Backups

Many Android phones come with a backup application pre-installed, such as Samsung Cloud, Google Drive, Google On, OnePlus or LG Android. Similar to iCloud on an iPhone, these applications may have text messages, photos, videos etc. that have been deleted from your phone.

To stop backing up the data if you do not believe the account(s) are secure

1. In your Android smartphone, tap **Settings**.
2. Tap **Accounts and backup**.
    - Review the settings for the backup applications on your phone.
3. To review Google backup, tap **Google** instead of **Accounts and backup**.
    - Tap **Manage backup**.

Source: Android Help

Additional Android Security

☐ Understanding "Rooted" Android Devices

'Rooting an Android device' means gaining superuser access to the operating system, allowing users to bypass manufacturer and carrier restrictions and customize the device at a deeper level. Rooting a device has security risks and can allow someone to install malicious software.

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 fix the issue.

Safety Tip:

A factor reset will delete all your data from your phone. Consult with a support worker about a plan to ensure your data is backed up safely and securely.

To complete a factory reset of your phone

1. In your Android smartphone, tap **Settings**.
2. Tap **General management**.
3. Tap **Reset**.
    - If you cannot find it, search ‘reset’ in your settings search bar.

Source: Android Help

☐ Security Apps

You can download security apps or specific anti-malware apps from the Google Play Store. Look for apps with good reviews and with many downloads.

Account and Services

☐ Review Connected Accounts

Safety Tip:

Be sure to take screenshots/recordings of the unauthorized log-ins. Before tapping to log a device out, consult with a support worker about potential safety concerns.

To review the account(s) connected to your device

1. In your Android smartphone, tap **Settings**.
2. Tap **Accounts and backup**.
3. Tap **Accounts**.
    - You can also type 'account' in the search bar if you are having difficulty finding accounts on your model.
4. If you see an account you do not recognize, tap on the account for more information.

If you are reviewing your Google Accounts, consider using the Google/Gmail Account Security Guide for Survivors for support.

Source: Android Help

If you are experiencing tech abuse, you are not alone. Find support in your community by connecting with a BC Society of Transition Houses Member Program or check out our other safety resources at techsafebc.bcsth.ca.