Guide to securing your Android

If technology is being used against you, use this website to secure your tech. Learn about Tech Abuse.

Note that depending on your device/updates, the steps below may vary.

Caution: Remember, depending on whether or not you are living with the person who is harming you, you may choose to take different steps. Control and coercion make some of these steps impossible or not safe. Read these cautions before taking action.
Secure your tech

Learn more about controlling tech

Step 1: Secure your Google account

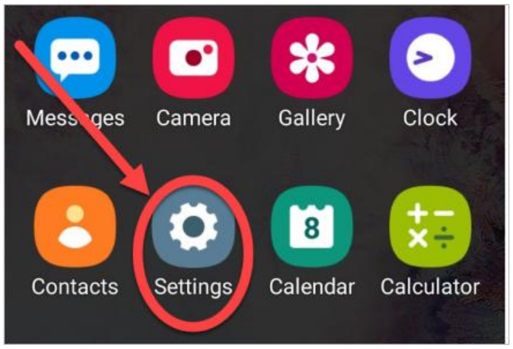
Many security and privacy settings are managed through your Google account rather than your phone. This includes changing your password, setting up Two Factor Authentication, and other security steps. You can also increase your privacy by adjusting your location, web and app activity history, and family group settings.

If you have an iPhone, use the iPhone Guide instead.

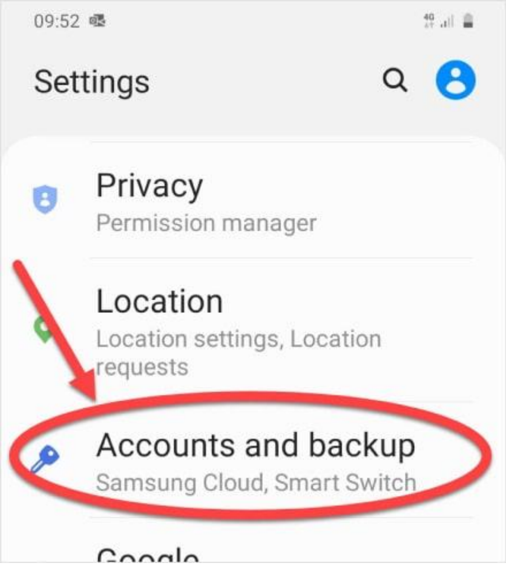
Step 2: Check other accounts connected to your phone

Learn more about access logs.

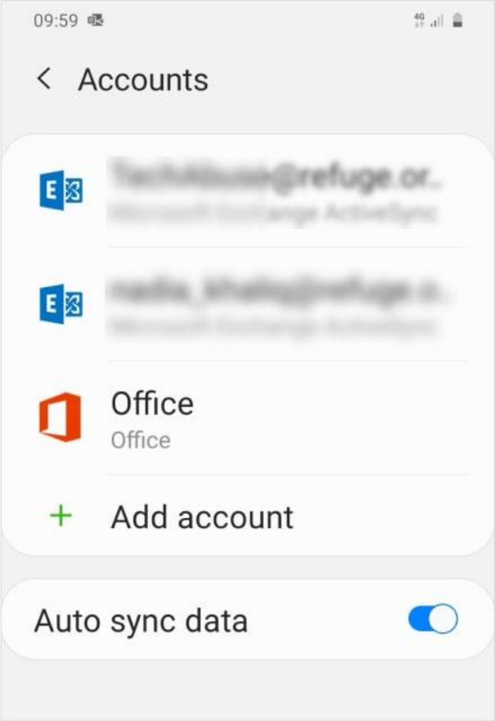
1. Open your phone's Settings app



2. Tap Accounts. If you don’t see “Accounts,” tap Accounts and backup.



3. Tap the account you want to remove, then tap Remove account.



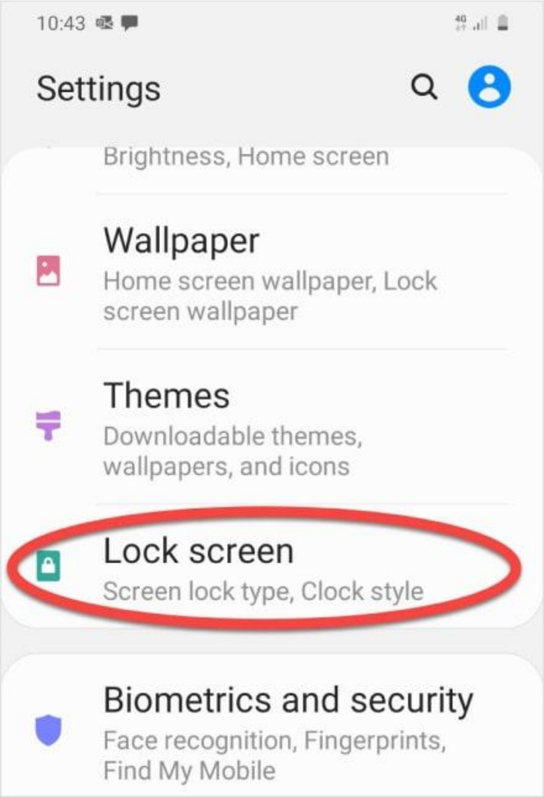
4. If this is the only Google account on the phone, you’ll need to enter your phone’s pattern, PIN, or password for security.

In the future, You can also create a separate user or temporary guest, instead of adding an account if you share the phone.

Step 3: Set up a screen lock

1. Go to Settings.

2. Tap Lock screen. You may need to tap Security first.



10:43

Settings

Brightness, Home screen

Wallpaper
Home screen wallpaper, Lock screen wallpaper

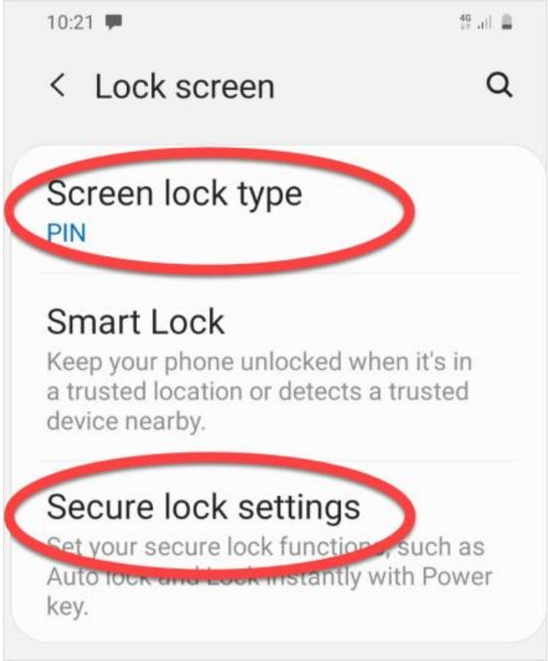
Themes
Downloadable themes, wallpapers, and icons

Lock screen
Screen lock type, Clock style

Biometrics and security
Face recognition, Fingerprints, Find My Mobile

3. Choose one of the screen lock options, which might include a passcode, a pattern, or a fingerprint or other biometric (something unique to you). **Caution**: These options might

escalate your risk if the abuser has any access to your device or account.



10:21

Lock screen

Screen lock type
PIN

Smart Lock
Keep your phone unlocked when it's in a trusted location or detects a trusted device nearby.

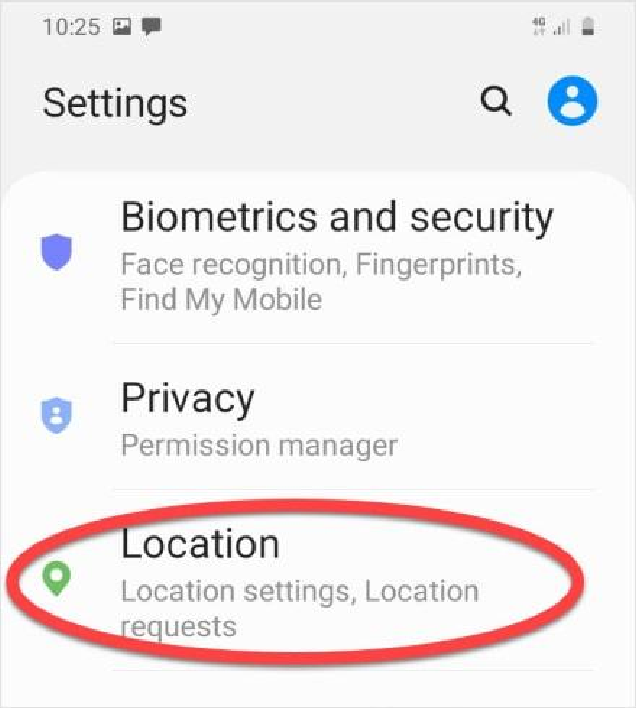
Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.

4. Set up screen lock.

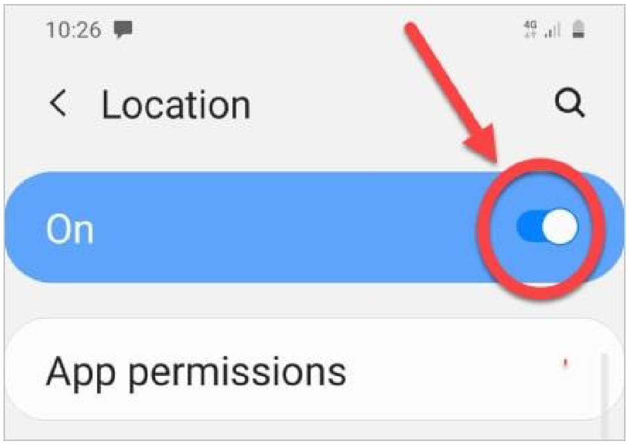
Step 4: Turn off location

1. Go to Settings.

2. Tap Location.


10:25
Settings
Biometrics and security
Face recognition, Fingerprints, Find My Mobile
Privacy
Permission manager
Location
Location settings, Location requests

3. You can turn location on or off. On some devices you can also adjust location accuracy. **Caution**: No notification will be sent, however the abuser may notice that they can no longer see your location. Some abusers may escalate their violence.



Apps have their own settings. To adjust these, you'll need to check the permissions for each app through your device's **Settings**, then tapping **Apps**.

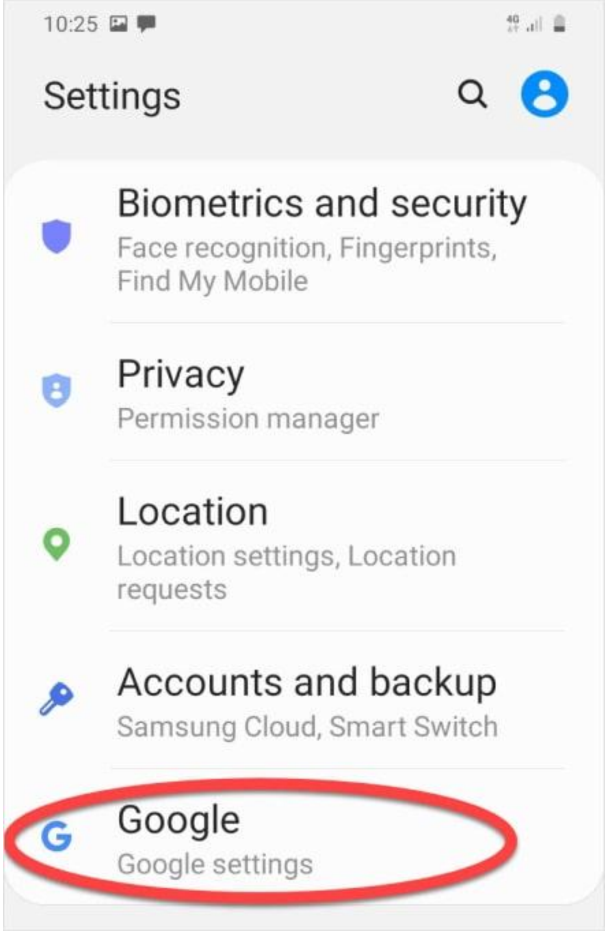
Note: Emergency services and mobile providers will always be able to see your location when your device is on. Any person you remove won't be notified, but they may notice they can't see your location the next time they look.

Step 5: Turn off "Find my phone"

You may also want to turn off "Find my phone" (or other device) on each device if you are concerned that someone else with access to your account will search for your location through your phone, or if your account is set as a "child" account in Family Link.

1. Go to Settings.

2. Tap Google.



10:25

Settings

Biometrics and security
Face recognition, Fingerprints, Find My Mobile

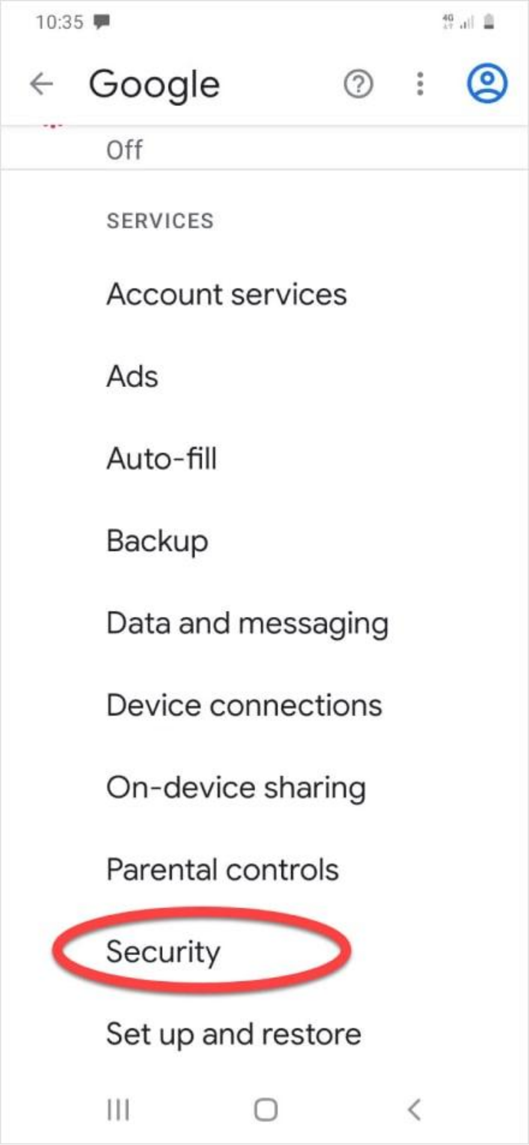
Privacy
Permission manager

Location
Location settings, Location requests

Accounts and backup
Samsung Cloud, Smart Switch

Google
Google settings

3. Tap Security, then tap Find My Device.



10:35

Google

Off

SERVICES

Account services

Ads

Auto-fill

Backup

Data and messaging

Device connections

On-device sharing

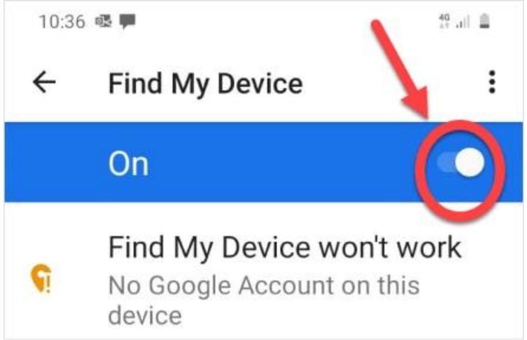
Parental controls

Security

Set up and restore

4. Turn the feature off. **Caution**: No notification will be sent, however the abuser may notice that they can no longer or see your phone's location. Some abusers may escalate their

violence.



Find My Device

On

Find My Device won't work

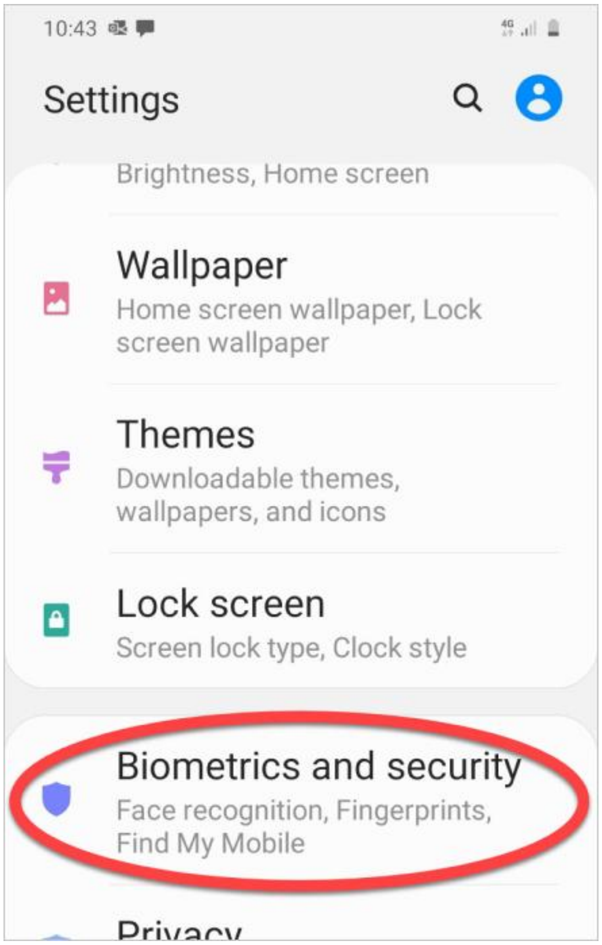
No Google Account on this device

Step 6: Check advanced settings

Depending on the manufacturer of your device, these options may vary. Check your settings to make sure:

- No guest accounts can be created when your device is locked.
- No unwanted people are listed as administrators for your device.

- Apps from unknown sources are not allowed.



10:43

Settings

Brightness, Home screen

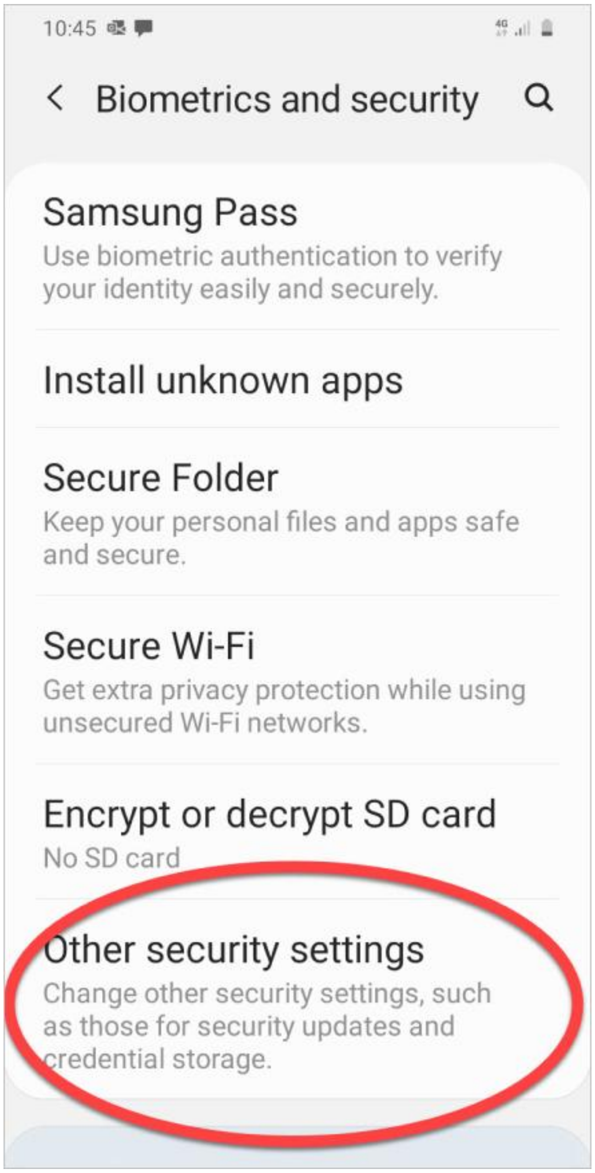
Wallpaper
Home screen wallpaper, Lock screen wallpaper

Themes
Downloadable themes, wallpapers, and icons

Lock screen
Screen lock type, Clock style

Biometrics and security
Face recognition, Fingerprints, Find My Mobile

Privacy



10:45

Biometrics and security

Samsung Pass

Use biometric authentication to verify your identity easily and securely.

Install unknown apps

Secure Folder

Keep your personal files and apps safe and secure.

Secure Wi-Fi

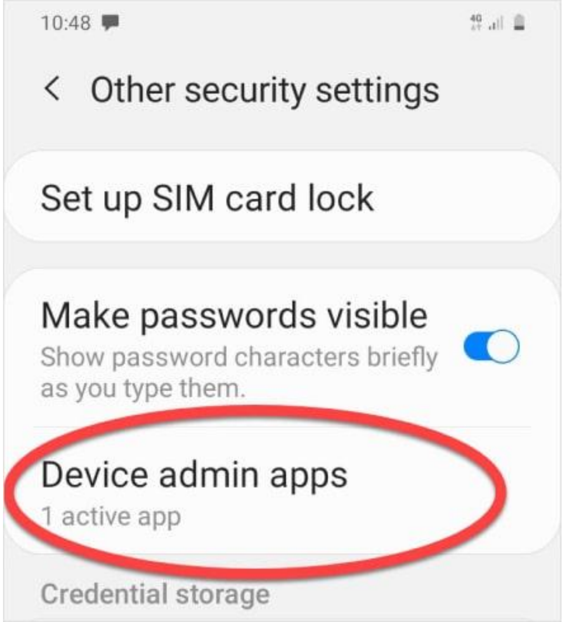
Get extra privacy protection while using unsecured Wi-Fi networks.

Encrypt or decrypt SD card

No SD card

Other security settings

Change other security settings, such as those for security updates and credential storage.



10:48

< Other security settings

Set up SIM card lock

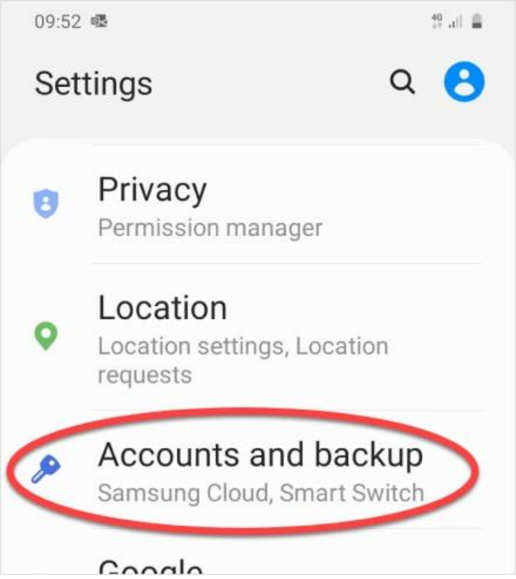
Make passwords visible ●
Show password characters briefly as you type them.

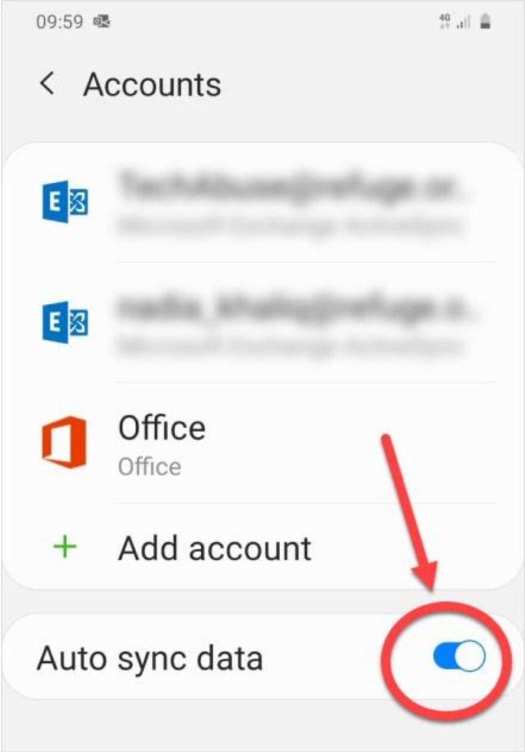
Device admin apps
1 active app

Credential storage

Step 7: Check if any apps are sync’ing or backing up to the cloud

By default, your Google account calendar, contacts, emails, documents, and more will sync to your Google cloud account. This means that information will be available on other devices that are signed into your account, or through the web. Other apps may also store data from the app to the cloud and be available to any other devices where you use the app.





Step 8: Consider these general security steps

- Set up encryption on your phone. Note that someone might still force or coerce you to give them access to the content of your phone.
- If it isn’t safe to remove someone’s access to your account, consider setting up a new account they aren’t aware of.
- Uninstall unneeded apps, and be cautious when downloading new apps.
- Use an anti-virus app on your phone, and be sure to install updates to apps and your phone’s operating system.
- Avoid public WiFi, or use a virtual private network (VPN).