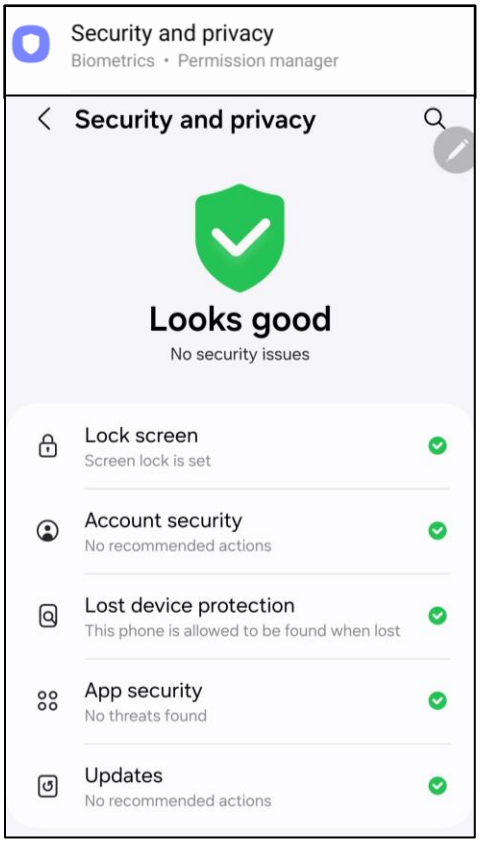
ANDROID PRIVACY SETTINGS

- Smartphones and tablets are not impenetrable. Secure your smartphone with a password or biometric lock and utilize apps such as “Find My Device” or “Prey Anti Theft” to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Consider your device when you are in certain places or having private conversations.
- Bluetooth and wireless-capable devices are convenient but easily exploitable by hackers. Use a VPN if possible, and always avoid public wireless networks.
- Prior to downloading apps on your device, read the developer’s permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- Keep location services turned off until they are needed. Otherwise, your daily movements are likely being tracked. Don’t worry, location services are always available to 911 and first responders even when turned off.
- If you have a google account, you can use your google credentials to login at “maps.google.com/location history” to see your device location history for the last year or more.

***Note:** Due to the existence of varying Android manufacturers, the instructions in this Smartcard may vary slightly depending on the device being used.

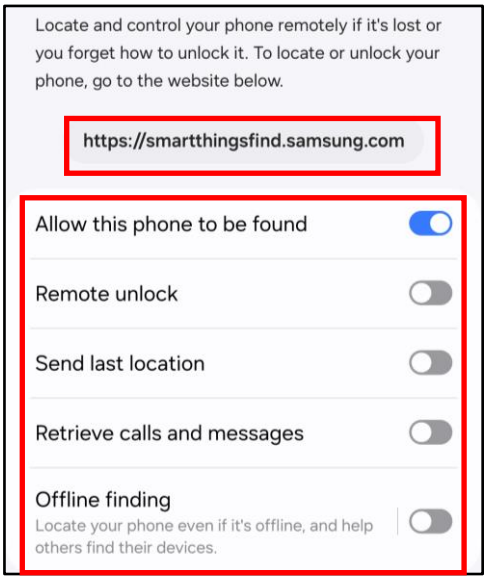
System Update: The most important thing you can do to keep your information secure is to ensure your device is updated. In order to make sure your Android is up to date with the latest version, first go to “Settings,” then scroll to the bottom and select “Software Update.”



Security and Privacy

Under the “Settings” tab, navigate down to your “Security and privacy” section. Once there it will show you the section as depicted on the left. If everything is up to date, you will see the “Looks good” with a green check mark as depicted next to it. If not there will be a red “X.” It is recommended to always make sure that your phone has the most up to date security sections. Those sections include your “Lock screen,” “Account security,” “Lost device protection,” “App security,” and “Updates.” If any of these have the red “X,” the device will walk you through how to rectify the security issue.

ANDROID PRIVACY SETTINGS

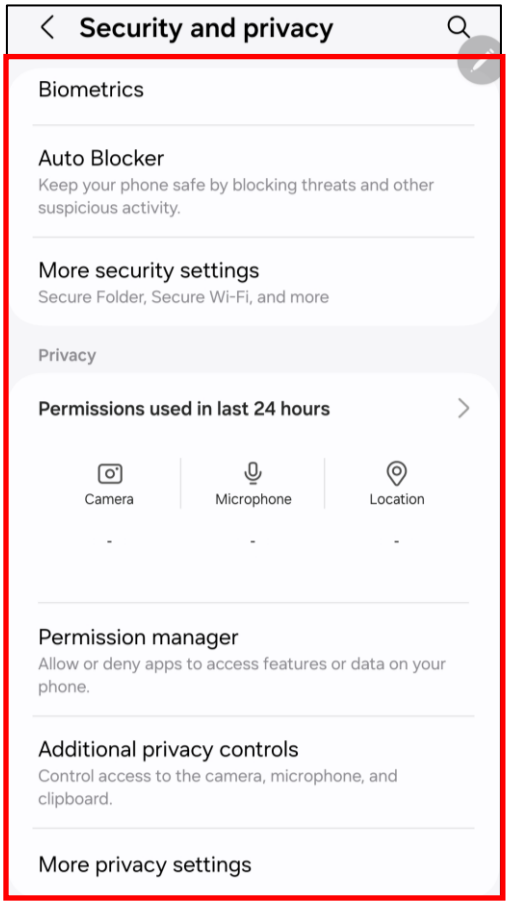


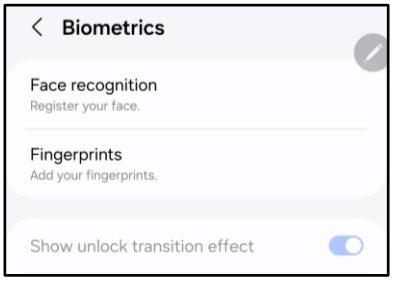
Security and Privacy

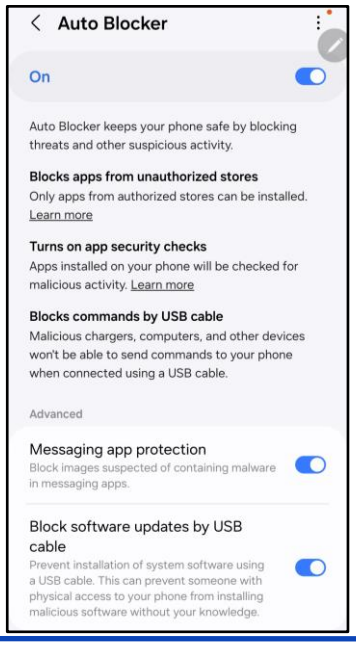
Still under the “Security and Privacy” tab, Click on the “Lost device protection” tab. Here you can go to the website listed below to locate or unlock your device. It is recommended you go through these settings and choose what is best suited to your needs.

Security and Privacy

If you continue to scroll down, you will reach the next sections “Biometrics,” “Auto Blocker,” “More security settings,” “Permission manager,” “additional privacy controls,” and “More privacy settings.” Starting with Biometrics, you can register with “Face Recognition” and “Fingerprints.” It is recommended to have facial recognition on, as if someone gets your pin, then they wont be able to bypass the facial recognition part.







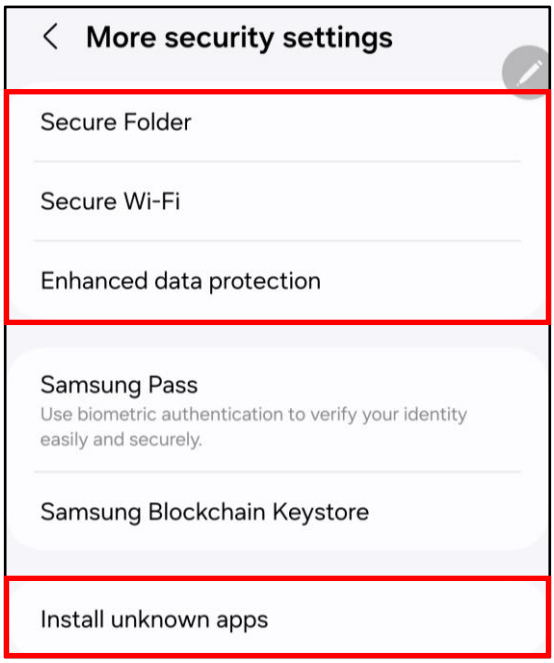
Auto Blocker

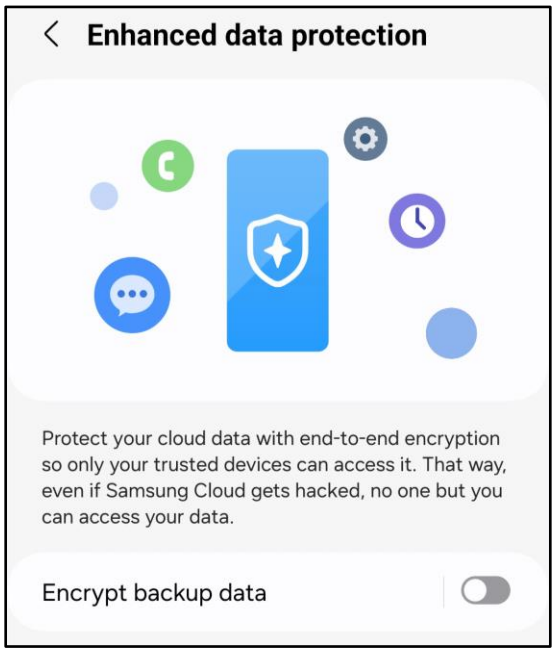
For “Auto Blocker,” it is recommended to have it turned on. “Auto Blocker’s” function is to block threats and suspicious activity from apps and commands by USB Cables.

ANDROID PRIVACY SETTINGS

More Security Settings

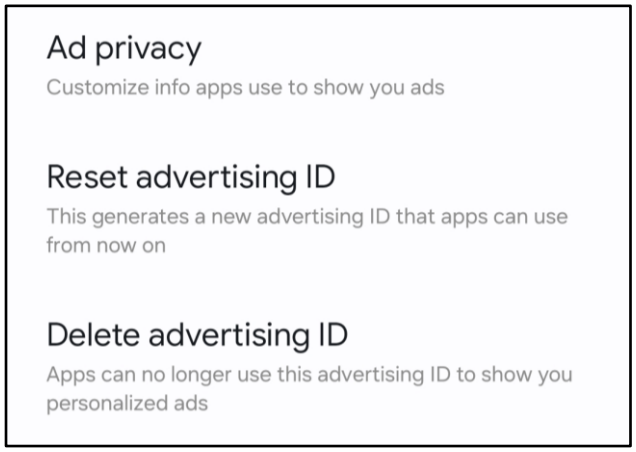
Under “More security settings,” click on “Secure Folder” if you would like to set it up where your apps on the device are password, pin, or biometric protected. *Note: If this is enabled, it may limit some actions, like sharing photos. For “Secure wifi,” it is a built in VPN to your system, if you are already using a VPN, it is recommended you leave this alone. For “Enhanced data protection,” you can choose to enable this to protect your cloud data with end to end encryption. It is **NOT RECOMMENDED** to use the “Install unknown apps” feature as you could download malicious software with it.





More Privacy Settings

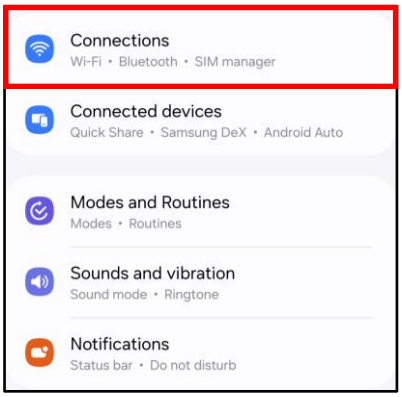
Under “More privacy settings,” navigate down to “Ads.” Here you can control your “ad privacy” settings. You are also able to “Reset advertising ID” and “Delete advertising ID.” It is recommended that you “Delete advertising ID,” so that apps are no longer to gain information from the ID.

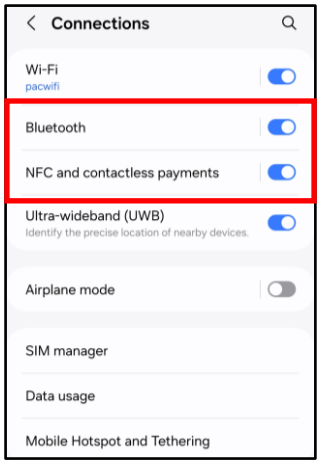


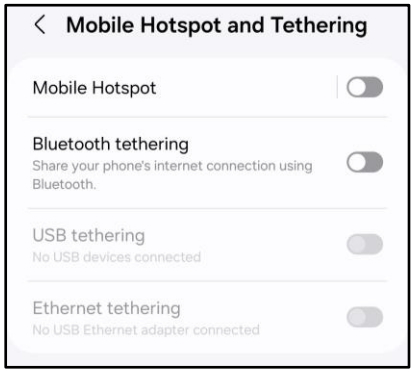
ANDROID PRIVACY SETTINGS

Mobile Hotspot, Bluetooth and Wifi

Mobile hotspot devices can be purchased and used for connecting to the Internet remotely, but without connecting to public wifi, which is always discouraged. Most Android smartphones have a "hotspot" feature that allows you to connect to the Internet (for instance on your laptop) remotely. By turning on this feature, your phone uses its cellular data to create a "Wifi Hotspot." You can turn this option on and off under "Settings" > "Connections" > "Tethering and Mobile HotSpot." Bluetooth is a wireless technology for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your device, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes, or install malware without you even knowing. To disable Bluetooth, go to "Settings" > "Connections" > and then turn off "Bluetooth."



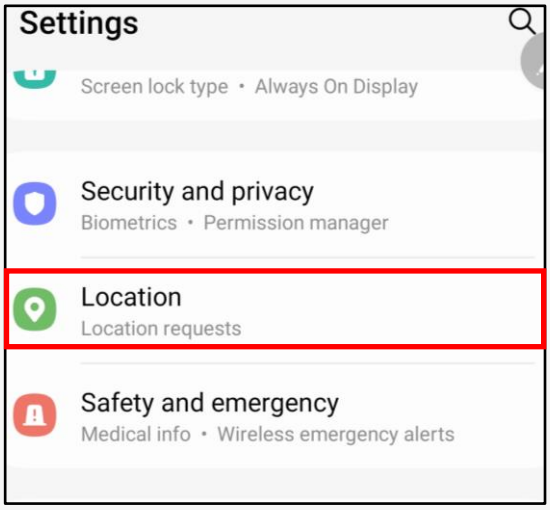




Note: We always recommend avoiding public Wifi networks because they are unsecure. If you must use one, avoid logging into accounts that require passwords, and use a VPN client to encrypt online transactions.

Location Services

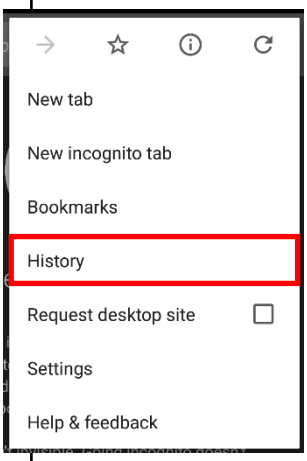
Whenever you take a photo, data on your location is saved inside of the photos (called EXIF data). When you send that photo to someone or post it online, data on where you took the photo may be available to those who know how to view it. If youpost a picture that you took from your home, anyone that can view it may be able to figure out where you live and more.
To disable your location from being shared, select "Settings" and scroll down to "Location." Disable your location services by switching the toggle to "off."

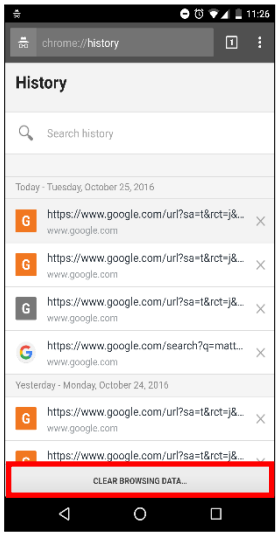


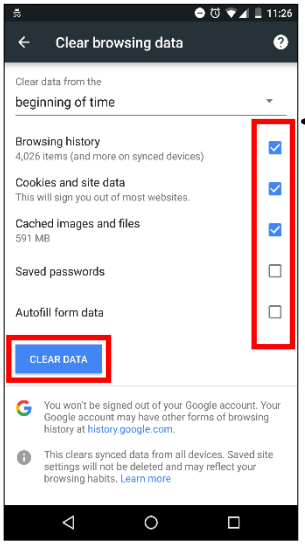
ANDROID PRIVACY SETTINGS

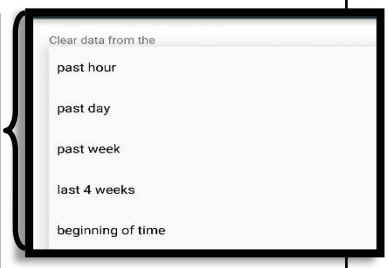
Internet Privacy Settings

Browser history and cookies are tracked when browsing the web from your mobile devices. To ensure privacy, open your browser (Chrome) and tap the three dots in the upper right-hand corner. Tap “History” then “Clear Browsing Data” at the bottom (or top) of the screen. On the next screen, select the applicable boxes (use the below screen shot as an example) and tap the blue “Clear Data” button.





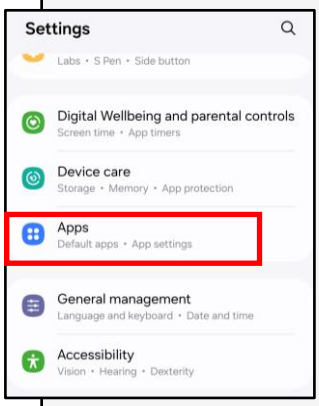


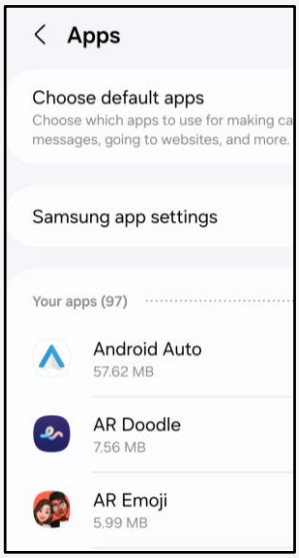


You have the option here to tap the drop-down arrow and select a date range of data to be deleted. If you get in the habit of clearing your browser history, cookies, and cache, then taking this step will become less important.

Application Manager

The applications you load access different capabilities on your device, regardless of whether they are active or working in the background. You can see, and to some degree control, what access each application has in the “Application Manager.”





Go to “Settings” > “Apps” then tap the app you want to view. Then tap “Permissions.” This will show you what permissions are granted when you accept the user agreement to download the app. In most instances these permissions can be controlled individually.