



Digital safety guide

Android privacy & security



The settings that keep your phone, your accounts, and your whereabouts to yourself. Go one section at a time — no need to do it all at once.

Before you start

Your phone	Menus differ by maker. Paths here follow Google Pixel phones; Samsung and others use similar names. Written for Android 15 and newer.
Find Settings	Open the Settings app (the gear), or swipe down from the top of the screen and tap the gear.
Can't find it?	Menus move. Use the search bar at the top of Settings.

✓ Do

Install updates as soon as they arrive (page 2).

Use a PIN of six or more digits, plus your fingerprint if you like.

Get apps only from Google Play or your phone maker's own store.

Keep Find Hub and theft protection on (page 3).

✗ Don't

Install apps from links in texts, emails, or pop-ups.

Give apps access they don't need. A flashlight app has no use for your contacts.

Accept Bluetooth or file-sharing requests you didn't start.

Read a code to anyone who calls you. Google, your bank, and your carrier won't ask for one.



01 Keep your phone updated

The most important protection on this list. Updates close security holes criminals already know how to use.

Android updates

Settings › System › Software updates

Install anything waiting. On Samsung, it's **Settings › Software update**. If your phone no longer gets updates, it's time to plan a replacement.

Security fixes

Settings › Security & privacy › System & updates

Also install any security update or Google Play system update listed here.

Apps

Play Store › your profile picture › Manage apps & device

Tap **Update all**, and leave automatic app updates on.

02 Lock your screen

Screen lock

Settings › Security & privacy › Device unlock › Screen lock

Choose a PIN of six or more digits, or a password. Skip swipe and pattern: a pattern is easy to guess from smudges or a glance over your shoulder. (Samsung: **Lock screen and AOD**.)

Fingerprint and face

A fingerprint is quick and safe to add. On many phones, face unlock is less secure than a fingerprint. Either way, your PIN is the real key, so keep it private.

Extend Unlock

Security & privacy › More security & privacy › Extend Unlock

Formerly Smart Lock. It keeps your phone unlocked in trusted places, near trusted devices, or while you carry it. We recommend leaving it off.



03 Prepare for loss or theft

Ten minutes now makes a lost or stolen phone an inconvenience instead of an emergency.

Find Hub

Settings › Security & privacy › Find Hub

Formerly Find My Device. Make sure **Allow device to be located** is on. If your phone goes missing, go to **android.com/find** on any computer or phone to ring, lock, or erase it.

Theft protection

Settings › Google › All services › Theft protection

Turn on **Theft Detection Lock** (locks the screen if someone snatches the phone and runs), **Offline Device Lock**, and **Remote Lock**. Remote Lock lets you lock a lost phone at **android.com/lock** with just your phone number.

Identity Check

On Android 15 and newer, turn this on in the same menu if you see it. Away from places you trust, it asks for your fingerprint or face before big changes, even if a thief knows your PIN.

Lock screen

In **Settings › Notifications**, hide sensitive content on the lock screen, so a thief can't read your sign-in codes or message previews.

Backup

Settings › System › Backup

Keep backup on, so a lost phone means a new phone, not lost photos and contacts. (Samsung: **Accounts and backup**.)

© Good to know

Find Hub needs Location turned on to show where your phone is. Instead of switching Location off entirely, limit which apps can use it (next page). And 911 can still find you: Android's Emergency Location Service works even when Location is off.



04 Control location and permissions

App location

Settings › Location › App location permissions

Set most apps to **Don't allow** or **Allow only while using the app**. For apps that just need your town, like weather, turn off **Use precise location**.

Photos

Photos can record exactly where they were taken. In your Camera app's settings, turn off **Save location** (Samsung: **Location tags**).

Google Timeline

Google Maps can keep a timeline of everywhere you've been. It's now stored on your phone rather than on Google's website. To review it or turn it off, open Google Maps, tap your profile picture, then **Your Timeline**.

App permissions

Search Settings for **Permission manager** to see which apps can use your camera, microphone, contacts, and text messages. Remove anything that doesn't make sense for what the app does.

Camera and mic

A green dot at the top of the screen means an app is using the camera or microphone right now. Swipe down twice for **Camera access** and **Microphone access** switches that block every app at once.

Why it matters

A photo taken at home can carry your home's exact map coordinates. Most social media sites strip that out when you post, but photos sent by email, text, or a shared cloud link often keep it. Turning off camera location solves it at the source.



05 Manage wireless connections

Bluetooth

Settings › Connected devices › Connection preferences

Turn Bluetooth off when you're not using it, unless you rely on Bluetooth hearing aids, a watch, or your car. Never accept a pairing request you didn't start, and remove devices you no longer use.

Wi-Fi

Settings › Network & internet › Internet › Network preferences

Turn off **Turn on Wi-Fi automatically**. Public Wi-Fi is much safer than it used to be, since most sites now encrypt your connection (look for the lock). For banking, your cell data is still the safer choice.

NFC and hotspot

If you don't use tap-to-pay, you can turn NFC off under Connection preferences. The risk is low, since it only works within an inch or two. Turn your hotspot off when you're done with it.

06 Limit ads and tracking

Advertising ID

Search Settings for "Ads," open it, and tap **Delete advertising ID**, so apps can't use it to follow you from app to app.

Google ads

Turn off personalized ads at myadcenter.google.com.

Safe Browsing

Chrome › ⋮ › Settings › Privacy and security › Safe Browsing

Choose **Enhanced protection** for stronger warnings about dangerous sites and downloads.

Browsing data

Chrome › ⋮ › Delete browsing data

Quick delete clears the last 15 minutes; **More options** clears more.



07 Protect your passwords and account

Passwords

Settings › Passwords, passkeys & accounts

Let Google Password Manager, or another password manager, create and save long, unique passwords. That's safer than reusing one you can remember. Run its **Password Checkup** now and then.

Google Account

Visit myaccount.google.com/security-checkup. Turn on 2-Step Verification, add a passkey, and make sure your recovery phone and email are current.

08 Watch for scams and bad apps

Play Protect

Play Store › your profile picture › Play Protect

Keep app scanning on. Phones rarely get computer-style viruses, but harmful apps are real, and most arrive through links and copycat app stores.

Scam warnings

Google Messages flags likely scam texts from strangers. On Pixel phones in the US, turn on call warnings too: **Phone app** › ⋮ › **Settings** › **Scam Detection**.

Want a hand with this?

We'll walk through every setting in this guide with you, at your pace.

watchstander.tech hello@watchstander.tech

Android, Google, Pixel, Chrome, and Google Play are trademarks of Google LLC. Samsung is a trademark of Samsung Electronics Co., Ltd. Watchstander Tech is not affiliated with or endorsed by either company. Steps checked October 2026; menus vary by phone and change often. © 2026 Watchstander Tech, LLC.