# Beginner's Guide To Securing Your Phone

*Guide · Lock Screen, Find My, Biometrics, App Permissions, Lockdown Mode — The Full Mobile Hardening.*

**Who this is for: anyone whose phone holds more sensitive data than their computer (which is everyone now). This guide hardens iOS and Android in about 30 minutes.**

## Why Phones Need Special Attention

Your phone holds your email (which can reset every other account), your banking apps, your photos, your messages with everyone you know, your location history, your biometric data, and probably your password manager. A lost or compromised phone is a much larger event than a lost laptop. Plus phones get lost, stolen, and dropped 4× more often than laptops.

## Lock Screen — The First Line

- **Strong passcode** set: 6+ digits or alphanumeric. NOT 1234, 0000, your birthday, or your address.
- **Face ID / Touch ID** enabled (faster unlock without compromising security).
- **Auto-lock** set to 30 seconds.
- **Lock-screen notifications** hidden — don't show preview content when locked. (iOS: Settings → Notifications → Show Previews → When Unlocked.)
- **Wallet, Camera, Control Center** disabled from lock screen if you carry payment cards.
- **Siri / Google Assistant** disabled from lock screen — voice commands can sometimes leak info.

## Find My / Find My Device — Don't Skip This

- Find My iPhone (iOS) / Find My Device (Android) is ON.
- Send Last Location enabled — sends location before battery dies.
- Activation Lock is on — prevents reset and reuse if stolen.
- Trusted family members added to Family Sharing for shared finding.
- Find My works even when phone is offline (iOS 15+ and Android 12+ both have this).

## App Permissions — The Quarterly Audit

Most apps don't need the access they ask for. Review every category every 90 days:

- **Location** — Settings → Privacy → Location Services. Set 'While Using' or 'Never' for anything that doesn't actively need location.
- **Microphone** — only voice apps and select social apps need this.
- **Camera** — only photo/video apps and select messaging apps.
- **Contacts** — only messaging and contact-management apps.
- **Photos** — most apps don't need full library access. Use 'Selected Photos' instead.
- **Health data** — extremely sensitive; only fitness/health apps you actively use.

- **Bluetooth** — disable for any app that doesn't have a clear reason.

## System Security

- Operating system on latest major version. Auto-updates ON.
- App Store / Play Store updates auto-installing.
- **Lockdown Mode** (iOS) considered if you're a journalist, activist, executive, or other high-risk user. Restricts attack surface significantly.
- **USB Restricted Mode** (iOS): Settings → Face ID & Passcode → USB Accessories → OFF.
- **SIM PIN** set: prevents your stolen phone from being moved to a new SIM and used for SIM-swap attacks.
- **Carrier porting protection**: call your carrier and add a porting PIN — without it, attackers can call and impersonate you to move your number to their SIM.

## App Hygiene

- Delete apps you haven't used in 60 days.
- Only install apps from the official App Store / Play Store.
- Review subscription list (Settings → Apple ID → Subscriptions; or Play Store → Subscriptions). Cancel anything you forgot you were paying for.
- Sign out of any accounts in apps you don't use weekly.
- Be sceptical of 'free' utility apps (battery savers, RAM cleaners, free VPNs). Most are spyware.

## Network Behaviour

- Disable auto-join for unknown networks. (Settings → Wi-Fi → Auto-Join Hotspot → Off.)
- Use a VPN on public Wi-Fi.
- Verify the network name with venue staff before joining anything called 'Free_Hotel_WiFi.'
- Bluetooth and AirDrop / Nearby Share: only on when you're actively using them. Set to 'Contacts Only' or 'Receiving Off' otherwise.

## Lost / Stolen Phone Plan

Practice this plan once a year so it's muscle memory when you need it:

1. **Mark as Lost** via Find My from another device or icloud.com / android.com/find. Locks the phone and shows a return-to message.
2. If not recoverable in 24-48 hours, **Erase** the device remotely.
3. **Notify your carrier** to suspend service (deters resale).
4. **Change passwords** on critical accounts from a clean device.
5. **Contact your bank** if banking apps were active.
6. **File a police report** if stolen — required for insurance and helps with potential recovery.
7. **Replace recovery codes** for MFA on critical accounts (in case the phone had authenticator-app codes accessible).

## Where To Go Next

- **Use the Mobile Phone Security Checklist** — full step-by-step.
- **Use the Phone Hardening Cheat Sheet** — quick visual reference (iOS + Android).
- **Run the Personal Device Security Audit** — score this phone (and others).

DID YOU KNOW?

### 1 In 4 Americans Reuses A Password Across 5+ Sites.

If yours is one of them, a single breach exposes your whole life. The fix is the password manager you've been putting off — Day 9 of our 30-Day Sprint walks you through it.

**Visit Making Sense Of Security →**