

3.2 Mobile Device Hardening

Core Concepts: Protect Your Data, Minimize Your Exposure

Your phone carries more personal data than your computer ever did, photos, messages, contacts, emails, banking apps, location history, health data, and more. It goes everywhere with you, making it vulnerable to loss, theft, and unauthorized access. It's also constantly connected to the internet, making it a target for remote attacks.

Mobile operating systems (iOS and Android) are designed with security in mind and include excellent built-in protections. The challenge is ensuring these features are enabled and properly configured.

3.2.1 Understanding Mobile Security

Mobile devices face unique security challenges:

- **Physical security:** Phones are easily lost or stolen
- **Always connected:** Constant internet access means constant exposure
- **App permissions:** Apps can access cameras, microphones, location, contacts
- **Public networks:** Frequently connect to unsecured WiFi
- **Personal data concentration:** Everything in one device

This section covers both iPhone (iOS) and Android. Follow the instructions for your device, or both if you use multiple phones or tablets.

Mobile Security Habits

Beyond settings, develop these habits:

- **Lock your phone every time you put it down:** Press the power button to lock manually
- **Don't leave your phone unattended:** Even for "just a second"
- **Be careful what you connect to:** Public charging stations can compromise phones (use your own charger with a power adapter)

- **Avoid public WiFi for sensitive activities:** Use cellular data or a VPN for banking, shopping
- **Review installed apps monthly:** Uninstall apps you don't use
- **Don't jailbreak (iPhone) or root (Android):** This removes built-in security protections

Your phone is your most personal computer. It knows where you go, who you talk to, what you buy, what you search for, and holds keys to your digital life. Protecting it isn't paranoia, it's common sense.

Mobile platforms are pretty secure by default. You just need to enable the right settings, review permissions regularly, and develop good habits. Start with The Basics, add Better Protection over time, and remember, the most important security feature is the lock screen. Use it every time.

3.2.2 The Basics

- Set a strong passcode
- Enable Find My Device
- Enable automatic updates
- Review app permissions
- Disable lock screen notifications for sensitive apps
- Enable automatic backup

Set a Strong Passcode and Enable Biometrics

Your lock screen is your first line of defense.

iPhone:

- Settings > Face ID & Passcode (or Touch ID & Passcode)
- Set up Face ID or Touch ID if you haven't already
- Tap "Change Passcode"
- Tap "Passcode Options"
- Choose "Custom Alphanumeric Code" for strongest security
- Or at minimum, choose "Custom Numeric Code" with 6+ digits
- Avoid simple patterns like 123456 or repeating digits

Android:

- Settings > Security > Screen lock
- Choose "Password" or "PIN" (6+ digits)
- Avoid "Pattern" as these are easier to observe and guess

- Set up fingerprint in Settings > Security > Fingerprint
- Or face unlock (varies by device manufacturer)

Biometrics are convenient for daily use, but the passcode is more secure against certain attacks (can't be compelled in court, can't be used while you're unconscious). See Understanding Biometrics in the Authentication topic.

Enable Find My Device

If you lose your phone, you need to be able to locate it, lock it remotely, and erase it if necessary.

iPhone (Find My):

- Settings > [Your Name] > Find My
- Turn on "Find My iPhone"
- Turn on "Find My network" (works even when offline)
- Turn on "Send Last Location" (sends location before battery dies)
- Test it: Open iCloud.com on a computer, sign in, click Find My iPhone

Android (Find My Device):

- Settings > Security > Find My Device
- Turn it on
- Make sure Location is enabled: Settings > Location > On
- Test it: Visit android.com/find on a computer, sign in with your Google account

Enable Automatic Updates

Mobile OS updates fix security vulnerabilities. Enable automatic updates so you're always protected.

iPhone:

- Settings > General > Software Update
- Tap "Automatic Updates"
- Turn on "Download iOS Updates"
- Turn on "Install iOS Updates"
- Turn on "Security Responses & System Files"

Android:

- Settings > System > System update (location may vary by manufacturer)
- Enable automatic downloads and installation

- For Google Play apps: Open Play Store > Profile icon > Settings > Network preferences > Auto-update apps > Over any network

Review App Permissions

Apps request access to your camera, microphone, location, contacts, and more. Review what you've granted and revoke unnecessary permissions.

iPhone:

- Settings > Privacy & Security
- Go through each category (Location Services, Camera, Microphone, Contacts, etc.)
- Review which apps have access
- Remove access from apps that don't need it
- For Location: Use "While Using the App" instead of "Always" when possible

Android:

- Settings > Privacy > Permission manager
- Review each permission type (Camera, Location, Microphone, etc.)
- Tap each to see which apps have access
- Change to "Don't allow" or "Ask every time" for apps that don't need constant access

Do this review quarterly; apps update and request new permissions over time.

Disable Lock Screen Notifications for Sensitive Apps

Notifications on your lock screen can reveal sensitive information to anyone who glances at your phone.

iPhone:

- Settings > Notifications
- Tap each sensitive app (banking, email, messaging, dating apps)
- Turn off "Show on Lock Screen"
- Or change "Show Previews" to "When Unlocked"

Android:

- Settings > Apps & notifications > Notifications
- Tap each sensitive app
- Turn off "Show on lock screen"

- Or choose "Don't show notification content"

Enable Automatic Backup

If you lose your phone, you need your data backed up. Enable automatic cloud backup.

iPhone (iCloud Backup):

- Settings > [Your Name] > iCloud > iCloud Backup
- Turn on "iCloud Backup"
- Backs up automatically when plugged in, locked, and on WiFi
- Free tier: 5GB (may need to purchase more storage for photos)

Android (Google Backup):

- Settings > Google > Backup
- Turn on "Back up to Google Drive"
- Select what to back up (app data, call history, contacts, etc.)
- For photos: Open Google Photos app > Profile > Photos settings > Back up & sync > Turn on

3.2.3 Better Protection

- Enable remote wipe capability
- Use encrypted backups
- Disable USB accessories when locked
- Use one-time passwords for apps
- Review location services settings
- Turn off unused wireless features
- Review privacy and tracking settings

Enable Remote Wipe Capability

If your phone is stolen and you can't recover it, you should be able to erase all data remotely.

iPhone:

- Already enabled with Find My iPhone (see Basics section)
- To erase remotely: iCloud.com > Find My iPhone > Select device > Erase iPhone

Note: After erasing, you can't track it anymore

Android:

- Already enabled with Find My Device (see Basics section)
- To erase remotely: android.com/find > Select device > Erase device

Note: After erasing, you can't track it anymore

Use Encrypted Backups

Cloud backups can be encrypted so even the backup provider can't access your data.

iPhone (Advanced Data Protection):

- Settings > [Your Name] > iCloud > Advanced Data Protection
- Turn on Advanced Data Protection
- This end-to-end encrypts most iCloud data (even Apple can't access it)
- Important: Save your recovery key; if you lose it and your devices, your data is unrecoverable

Android:

- Google backups are encrypted in transit and at rest
- For additional security, use third-party encrypted backup apps

Disable USB Accessories When Locked

USB accessories can be used to attack locked phones. Disable them when locked.

iPhone:

- Settings > Face ID & Passcode (or Touch ID & Passcode)
- Scroll down to "Allow Access When Locked"
- Turn off "USB Accessories" (requires unlocking to connect)

Android:

- Some phones have "Block USB connections while locked" under Settings > Security and Privacy > More Security Settings

Use One-Time Passwords for Apps

For email and other accounts accessed through apps, use app passwords instead of your main password.

- Gmail, iCloud, and other services offer app-specific passwords
- These passwords only work for that specific app
- If your phone is compromised, revoke the app password without changing your main password
- See the Use One-Time Passwords for Apps in the Authentication topic for more details

Review Location Services Settings

Location tracking is convenient but invasive. Review what's tracking you and when.

iPhone:

- Settings > Privacy & Security > Location Services
- Review each app
- Change apps to "While Using the App" instead of "Always" where possible
- Turn off "Precise Location" for apps that don't need exact coordinates

Android:

- Settings > Location
- Tap "App location permissions"
- Review each app
- Change to "Allow only while using the app" instead of "Allow all the time"

Turn Off Unused Wireless Features

Bluetooth, WiFi, and NFC create additional attack surfaces when not in use.

- Turn off Bluetooth when not using wireless headphones or accessories
- Turn off WiFi when out and about (prevents auto-connecting to malicious networks)
- Turn off NFC (contactless payments) when not actively using it

Use Control Center/Quick Settings for easy toggling.

Review Privacy & Tracking Settings

Apps and advertisers track your activity across apps and websites. Limit this tracking.

iPhone:

- Settings > Privacy & Security > Tracking
- Turn off "Allow Apps to Request to Track"
- Settings > Privacy & Security > Apple Advertising

- Turn off "Personalized Ads"

Android:

- Settings > Privacy > Ads
- Turn on "Opt out of Ads Personalization"
- Settings > Google > Manage your Google Account > Data & privacy
- Review "Activity controls" and turn off tracking you don't want

3.2.4 Extra Credit

- Use separate work and personal profiles
- Use secure folder / private space features
- Enable advanced privacy features
- Set up a SIM PIN
- Use lockdown mode (iPhone) for high-risk situations

Use Separate Work/Personal Profiles (Android)

Android allows multiple user profiles or work profiles to keep personal and work data separated. This may already be a requirements and set up automatically depending on where you work and how you access work data on your phone. Contact your local IT center with any questions.

- Settings > System > Multiple users
- Add a user or work profile
- Each profile has separate apps, data, and settings
- Useful for: Separating work/personal, creating a "clean" profile for sensitive activities

Use Secure Folder / Private Space Features

Some phones offer encrypted, hidden spaces for sensitive apps and files.

Samsung Secure Folder:

- Settings > Security and privacy > Secure Folder
- Encrypted space for apps, photos, files
- Separate authentication from main phone

Google Private Space (Android 15+):

- Settings > Security & privacy > Private space
- Hidden apps and data with separate authentication

iPhone:

- No built-in secure folder, but you can:
- Use the Hidden album for photos (Settings > Photos > scroll down, turn on "Use Face ID" for Hidden album)
- Use Notes app with password-protected notes

Enable Advanced Privacy Features

iPhone (iOS 15+):

- Mail Privacy Protection: Settings > Mail > Privacy Protection (hides IP address and prevents tracking pixels)
- Hide My Email: Settings > iCloud > Hide My Email (generate random email addresses for signups)
- Private Relay: Settings > iCloud > Private Relay (Safari browsing privacy, requires iCloud+)

Android:

- Privacy Dashboard: Settings > Privacy > Privacy dashboard (see which apps accessed permissions recently)
- Microphone/Camera indicators: Green dot appears when apps use camera/mic
- Permission auto-reset: Settings > Privacy > Permission manager > (gear icon) > Remove permissions if app unused

Set Up a SIM PIN

A SIM PIN prevents someone from using your SIM card in another phone (protects against SIM-swap attacks).

iPhone:

- Settings > Cellular > SIM PIN
- Turn on SIM PIN
- Default is often 1234 - change it immediately

Android:

- Settings > Security > SIM card lock
- Turn on "Lock SIM card"
- Change from default PIN

Warning: If you enter the wrong SIM PIN 3 times, you'll need a PUK code from your carrier to unlock it. Keep your carrier's customer service number handy.

Use Lockdown Mode (iPhone) for High-Risk Situations

Lockdown Mode is an extreme security mode for people facing serious targeted threats (journalists, activists, executives).

- Settings > Privacy & Security > Lockdown Mode
- Severely restricts functionality to protect against sophisticated attacks
- Most people don't need this, only use if you're at genuine risk of targeted attacks

Revision #2

Created 2026-07-12 21:31:54 UTC by Chris Landis

Updated 2026-07-12 21:47:32 UTC by Chris Landis