Wigington Security Group

Privacy consulting for individuals and families

Phone & Device Hardening Guide

Secure your iPhone and Android devices

What You'll Learn:

- iOS 18 and Android 15 security configuration
- Encryption, biometrics, and device protection
- Privacy settings that actually matter
- App permissions and tracking prevention
- Location services and ad tracking controls
- Secure backups and data protection
- What to do if your phone is lost or stolen

Current as of February 2026:

- iOS 18.3 / iPadOS 18.3
- Android 15
- Settings paths verified on latest versions
- Update quarterly as OS versions change

February 2026 • 28 Pages • Free Download

wigingtonsecurity.com

Contents

1 Understanding Mobile Device Security

1.1 Why Your Phone Is Your Most Vulnerable Device

Your smartphone is simultaneously:

- **Most personal:** Contains texts, photos, emails, location history, health data
- **Most connected:** Always online, always tracking, always listening
- **Most targeted:** Thieves, stalkers, hackers, governments want access
- **Least protected:** Most people use default settings
- **Most powerful:** GPS, cameras, microphones, sensors everywhere
- **Most lost:** 70 million phones lost/stolen annually in US alone

❗ CRITICAL

Your phone knows:

- Where you are right now (GPS accurate to 5 meters)
- Where you live and work (pattern analysis)
- Who you talk to and when
- What you search for
- Your health conditions (via apps)
- Your financial accounts
- Your photos and videos
- Your passwords (if stored insecurely)
- Your voice and face (biometrics)

If someone gets physical access to an unsecured phone, they get access to your entire life.

1.2 Threat Model: What Are We Protecting Against?

1.2.1 Physical Theft

Attacker gains physical possession of your phone:

- Opportunistic thief (wants to resell device)
- Targeted thief (wants your data)
- Domestic partner/ex-partner snooping
- Employer examining company device

- Law enforcement seizure
- Border agent inspection

Defense: Strong passcode, encryption, remote wipe capability

1.2.2 Remote Attacks

Attacker never touches your phone:

- Malicious apps collecting data
- Phishing links leading to malware
- SIM swap attacks (hijack phone number)
- Public WiFi interception
- Zero-click exploits (very rare, high-value targets)

Defense: OS updates, app vetting, VPN, two-factor authentication

1.2.3 Tracking and Surveillance

Attacker monitors your behavior:

- Apps tracking location and selling data
- Advertisers building profile
- Stalkerware installed by someone with physical access
- Cell tower tracking (law enforcement)
- Corporate MDM (Mobile Device Management) on work phones

Defense: Permission management, location controls, app audit

1.3 iOS vs. Android: Security Comparison

Factor	**iOS**	**Android**
Default Security	Strong out-of-box	Varies by manufacturer
Encryption	Always on (A7+ chips)	On if set up properly
App Vetting	Strict App Store review	Less strict, more malware
Update Frequency	5-7 years support	2-3 years (Pixel gets 7)
Privacy Controls	Excellent, user-friendly	Good but fragmented
Customization	Limited	Extensive
Known Vulnerabilities	Fewer, higher value	More, widely targeted
Price	$429-$1,599	$150-$1,800
Privacy from Vendor	Better (Apple)	Worse (Google)
Recommendation	Best for most users	Pixel for advanced users

Bottom line: iOS is more secure by default. Android *can be* very secure with proper configuration, but requires more knowledge.

1.4 This Guide's Scope

What we cover:

- **iOS:** iPhone and iPad running iOS/iPadOS 18
- **Android:** Google Pixel and near-stock Android 15

What we don't cover:

- Heavily modified Android (Samsung One UI, Xiaomi MIUI, etc.)
- Jailbroken/rooted devices
- Desktop/laptop hardening (separate guide)
- Tablets other than iPad
- Specialty devices (GrapheneOS, LineageOS)

⚠ Warning

Samsung/OnePlus/Xiaomi users: Settings paths will differ significantly. Use this guide for concepts, then search "[your phone model] privacy settings" for specific instructions. **Recommendation:** If buying new Android, get Google Pixel for best security and longest update support.

2 iOS/iPadOS Hardening (iPhone & iPad)

Tested on: iOS 18.3 / iPadOS 18.3 (February 2026)

2.1 Initial Setup Security

If setting up new device or doing factory reset:

☑ Action Checklist

During initial setup:

Do NOT restore from untrusted backup

Create new Apple ID (don’t reuse old compromised one)

Use strong alphanumeric passcode (not 4 or 6 digits)

Enable Face ID or Touch ID

Skip ”Share iPhone Analytics” (decline)

Skip ”Share with App Developers” (decline)

Set up Find My iPhone (critical for remote wipe)

2.2 Lock Screen and Passcode

Path: Settings → Face ID & Passcode (or Touch ID & Passcode)

iOS/iPadOS Settings

☑ Action Checklist

Change Passcode → Use **Custom Alphanumeric Code**

- Tap "Passcode Options"
- Select "Custom Alphanumeric Code"
- Minimum 8 characters (12+ recommended)
- Mix letters, numbers, symbols
- Store in password manager

Require Passcode → Immediately

- Not "After 1 minute" or "After 15 minutes"
- Phone locks the moment screen turns off

Allow Access When Locked → Disable most features:

- Today View: OFF
- Notification Center: OFF
- Control Center: OFF
- Siri: OFF (prevents voice commands when locked)
- Reply with Message: OFF
- Home Control: OFF
- Wallet: OFF
- Return Missed Calls: OFF
- USB Accessories: OFF (critical—prevents forensic tools)

Erase Data → ON

- Erases iPhone after 10 failed passcode attempts
- Make sure you have backups before enabling
- Protects against brute force attacks

⚠ Warning

USB Accessories when locked: This is critical. When OFF, iPhone won't connect to any USB device unless unlocked first. Prevents:

- GrayKey and Cellebrite forensic tools
- Juice jacking (data theft via charging cable)
- Unknown accessories extracting data

Tradeoff: Must unlock phone before connecting to computer or CarPlay.

2.3 Face ID / Touch ID Configuration

iOS/iPadOS Settings

☑ Action Checklist

Enroll your face/fingerprint carefully

- Face ID: Complete full range of motion during setup
- Touch ID: Register same finger multiple times for better recognition

Set up alternate appearance (Face ID only)

- Useful for glasses, different hairstyles
- Or register trusted family member

Require Attention for Face ID → ON

- Phone won't unlock unless you're looking at it
- Prevents unlock while sleeping

What Face ID/Touch ID is enabled for:

- iPhone Unlock: ON
- Apple Pay: ON
- iTunes & App Store: ON
- Password Autofill: ON

Pro Tip

Disabling biometrics temporarily:
If you need to disable Face ID/Touch ID quickly (border crossing, police encounter, suspicious situation):

1. Press and hold Side Button + Volume Button for 2 seconds
2. "Slide to Power Off" appears
3. Press Cancel
4. Face ID/Touch ID now disabled until you enter passcode

You cannot be legally compelled to provide a passcode (5th Amendment in US), but you *can* be compelled to provide biometrics. This trick requires passcode entry.

2.4 Privacy Settings

Path: Settings → Privacy & Security
This is the most important section for privacy.

2.4.1 Location Services

Path: Settings → Privacy & Security → Location Services

iOS/iPadOS Settings

☑ Action Checklist

Location Services → Keep ON (but manage per-app)

- Completely disabling breaks Maps, Weather, Emergency SOS
- Instead, control which apps get access

Review each app: Tap each app and set appropriately:

- Never — Most apps (social media, games, shopping)
- Ask Next Time — Apps you rarely use
- While Using — Maps, Uber, weather
- Always — Almost nothing (maybe Find My)

For apps set to "While Using," disable **Precise Location**

- Gives approximate location instead of exact GPS coordinates
- Works for most apps (weather, local news)
- Enable for navigation apps only when needed

Scroll to bottom → **System Services**

- Cell Network Search: OFF
- Compass Calibration: OFF
- Device Management: OFF (unless required for work)
- Find My iPhone: ON (keep this)
- HomeKit: ON if you use it
- Location-Based Alerts: OFF
- Location-Based Suggestions: OFF
- Networking & Wireless: OFF
- Setting Time Zone: ON (useful)
- Share My Location: OFF (unless sharing with family)
- iPhone Analytics: OFF
- Routing & Traffic: OFF
- Significant Locations: OFF (critical—this logs everywhere you go)
- System Customization: OFF

At bottom of System Services → **Product Improvement**

- iPhone Analytics: OFF
- Improve Maps: OFF
- Improve Siri & Dictation: OFF

❗ CRITICAL

Significant Locations: This feature logs every place you visit frequently. Apple claims it's only stored on device, but:

- Accessible if someone gets your passcode
- Included in backups (potentially exposed)
- Can be subpoenaed
- No legitimate reason to keep this on

Turn it OFF immediately. Delete history: Settings → Privacy → Location Services → System Services → Significant Locations → Clear History

2.4.2 Tracking and Advertising

Path: Settings → Privacy & Security → Tracking

iOS/iPadOS Settings

☑ Action Checklist

Allow Apps to Request to Track → OFF

- Prevents apps from asking to track you across other apps/websites
- Critical privacy protection introduced in iOS 14.5

Review list of apps below—all should say ”No”

If any app is allowed to track, revoke it

Path: Settings → Privacy & Security → Apple Advertising

iOS/iPadOS Settings

☑ Action Checklist

Personalized Ads → OFF

- Reduces ad targeting based on your activity
- You'll still see ads, just less creepy ones

2.4.3 App Permissions Audit

Review every app's permissions. Most apps request far more than they need.

Path: Settings → Privacy & Security → [Permission Type]

 iOS/iPadOS Settings

☑ Action Checklist

Go through each permission category:

Contacts — Only contacts apps, messaging

Calendars — Only calendar apps, email

Reminders — Only reminder/todo apps

Photos — Only when app needs to save/access photos

- Use "Selected Photos" instead of "All Photos" when possible
- Revoke for social media apps after uploading

Bluetooth — Only devices, headphones, fitness trackers

Local Network — Only smart home, printers

Microphone — Only voice/video calling apps

- Games should NOT have microphone access
- Social media only needs it for video recording

Camera — Only when app needs to take photos/videos

Health — Review carefully, medical privacy is critical

HomeKit — Only smart home apps

Media & Apple Music — Only music/media apps

Motion & Fitness — Only fitness apps

Focus — Only productivity apps if used

Files and Folders — Minimize, audit carefully

Rule of thumb: If you can't think of why an app needs a permission, it doesn't need it. Revoke and see if app still works.

2.4.4 Analytics and Improvements

Path: Settings → Privacy & Security → Analytics & Improvements

iOS/iPadOS Settings

☑ Action Checklist

Share iPhone Analytics → OFF

Share iCloud Analytics → OFF

Share with App Developers → OFF

Improve Siri & Dictation → OFF

Improve Wheelchair Mode → OFF (unless you use this feature)

Improve Safety → Personal choice

- Shares data when Emergency SOS/Crash Detection activates
- Consider leaving ON for public safety benefit

2.5 Apple ID and iCloud Settings

Path: Settings → [Your Name]

2.5.1 iCloud Settings

** iOS/iPadOS Settings**

☑ Action Checklist

iCloud Backup → Personal choice

- Convenient but data stored on Apple's servers
- Alternative: Encrypted local backups via computer
- If enabled, enable **Advanced Data Protection**

Advanced Data Protection → ON

- End-to-end encrypts most iCloud data
- Apple cannot decrypt even with court order
- Requires iOS 16.2+
- Critical: Set up recovery contacts or recovery key

Review what syncs to iCloud:

- Photos: Personal choice (convenient but privacy tradeoff)
- Mail: If using iCloud email
- Contacts: Convenient for backup
- Calendars: Convenient for backup
- Safari: Consider OFF (browsing history in cloud)
- Siri: OFF (voice recordings in cloud)
- Health: Personal choice (very sensitive data)

❗ CRITICAL

Advanced Data Protection is critical
Without it, 14 iCloud data categories are accessible to Apple (and thus law enforcement, breaches, rogue employees):

- iCloud Backup
- iCloud Drive
- Photos
- Notes
- Voice Memos
- And more

With Advanced Data Protection:

- 23 categories end-to-end encrypted
- Only iCloud Mail, Contacts, Calendar remain accessible to Apple (technical limitations)
- You MUST set up recovery method or you can lose access forever

Enable it: Settings → [Your Name] → iCloud → Advanced Data Protection → Turn On

2.5.2 Hide My Email

Path: Settings → [Your Name] → iCloud → Hide My Email

 iOS/iPadOS Settings

☑ Action Checklist

Use Hide My Email for signups instead of real email

- Generates random email addresses that forward to your real email
- Prevents companies from getting your real email
- Can deactivate if address gets spam

Safari auto-suggests when signing up for services

2.6 Safari Privacy Settings

Path: Settings → Safari

iOS/iPadOS Settings

☑ Action Checklist

Prevent Cross-Site Tracking → ON

Block All Cookies → Consider ON

- Breaks some websites but maximizes privacy
- Start with OFF, enable if comfortable with tradeoffs

Fraudulent Website Warning → ON

Privacy Preserving Ad Measurement → OFF

Check for Apple Pay → Personal preference

Hide IP Address → Trackers and Websites

- Routes traffic through Apple servers to hide your IP
- Requires iCloud Private Relay (iCloud+ subscription)

Scroll down → **Advanced**

- Advanced Tracking & Fingerprinting Protection: ON

2.7 App Store Settings

Path: Settings → App Store

iOS/iPadOS Settings

☑ Action Checklist

App Downloads → Require password/Face ID: Always Require

In-App Purchases → Require password/Face ID: Always Require

- Prevents accidental purchases
- Prevents unauthorized purchases if someone gets access

Personalized Recommendations → OFF

2.8 Messages and FaceTime

Path: Settings → Messages

iOS/iPadOS Settings

☑ Action Checklist

iMessage → Keep ON (end-to-end encrypted)

Send Read Receipts → OFF

- Prevents people from knowing when you read their messages

Share Name and Photo → Ask/Always Ask

Filter Unknown Senders → ON

- Separates messages from people not in your contacts
- Reduces spam

Check In → Configure for safety features

Path: Settings → FaceTime

iOS/iPadOS Settings

☑ Action Checklist

FaceTime → ON if you use it

Calls from → iPhone only (if you don't want calls on other devices)

2.9 Screen Time and App Limits

Path: Settings → Screen Time
Not just for limiting kids—useful for security:

iOS/iPadOS Settings

☑ Action Checklist

Enable Screen Time

Set **Screen Time Passcode** (different from device passcode)

Content & Privacy Restrictions → Enable

- iTunes & App Store Purchases → Require Password: Always
- Installing Apps: Allow (but with Screen Time passcode)
- Deleting Apps: Require Screen Time passcode
- Location Services → Don't Allow Changes (locks your settings)
- Share My Location → Don't Allow Changes

Why this helps: If someone gets your device passcode, they still can't change privacy settings without the Screen Time passcode.

2.10 Find My iPhone

Path: Settings → [Your Name] → Find My

iOS/iPadOS Settings

☑ Action Checklist

Find My iPhone → ON

Find My network → ON

- Allows finding iPhone even when offline
- Uses Bluetooth and other nearby Apple devices

Send Last Location → ON

- Sends location to Apple when battery critically low
- Helps find phone before it dies

Pro Tip

Remote wipe capability:
If your iPhone is lost or stolen:

1. Visit `https://www.icloud.com/find` from any browser
2. Sign in with Apple ID
3. Select your iPhone
4. Mark as Lost (locks device, displays message)
5. If recovery impossible, Erase iPhone (remote wipe)

This is why Find My iPhone must stay enabled.

3 Android Hardening (Google Pixel)

Tested on: Google Pixel 8 Pro running Android 15 (February 2026)

⚠ Warning

Important: These instructions are for Google Pixel phones running stock Android 15. Samsung, OnePlus, Xiaomi, and other manufacturers heavily modify Android—settings will be in different locations with different names.

If you don't have a Pixel: Use these instructions as a guide but expect to search for your specific model. Example: "Samsung Galaxy S24 privacy settings location."

3.1 Initial Setup Security

If setting up new device or factory reset:

☑ Action Checklist

During initial setup:

Create/use Google Account (required for Play Store)

Set strong screen lock: PIN (6+ digits) or Password

Enable fingerprint unlock

Decline all Google service opt-ins during setup

- Backup to Google Drive: Skip for now
- Use location services: Decline
- Scan apps with Play Protect: Enable (security)
- Help improve Android: Decline

Don't restore from old phone until you've hardened privacy

3.2 Screen Lock and Biometrics

Path: Settings → Security & privacy → Device unlock

Android Settings

☑ Action Checklist

Screen lock → PIN or Password

- Minimum 6 digits for PIN (8+ recommended)
- Or use alphanumeric password (12+ characters)
- Store in password manager

Fingerprint Unlock → Set up 2-3 fingerprints

- Register same finger multiple times for better recognition
- Or register multiple fingers

Face Unlock → Optional (less secure than fingerprint)

- Only available on Pixel 8 and newer
- Convenient but can be fooled by photos (older models)

Back to Security → **Lock screen preferences**

- Automatically lock: Immediately
- Lock after screen timeout: Immediately
- Power button instantly locks: ON

Pro Tip

Lockdown Mode (Emergency Biometric Disable):
To temporarily disable fingerprint/face unlock:

1. Press and hold Power button
2. Tap ”Lockdown”
3. Biometrics disabled until you enter PIN/password

Useful for: Border crossings, police encounters, suspicious situations where you might be compelled to use biometrics.

3.3 Encryption

Android Settings

☑ Action Checklist

Check encryption status: Settings → Security → Encryption

- Should say ”Encrypted” by default on modern Android
- If not encrypted: Enable encryption (will take 30+ minutes)
- Encryption requires screen lock be set

Encryption protects data if phone is stolen/lost

3.4 Privacy Dashboard and Permissions

Path: Settings → Security & privacy → Privacy

3.4.1 Privacy Dashboard

Android Settings

☑ Action Checklist

Tap **Privacy dashboard**

- Shows which apps accessed camera, mic, location in last 24 hours
- Review regularly for suspicious access
- Tap any permission to see which apps used it

3.4.2 Permission Manager

Path: Settings → Security & privacy → Privacy → Permission manager

Android Settings

☑ Action Checklist

Review each permission type:

Location

- Tap to see all apps with location access
- For each app: Deny, Ask every time, Allow only while using, or Allow all the time
- Most apps: Deny or Ask every time
- Maps/navigation: Allow only while using
- Almost nothing needs ”Allow all the time”
- For apps with access, disable **Precise location**

Camera

- Camera app: Allowed
- Social media: Ask every time (or Deny, enable when posting)
- Games: Deny

Microphone

- Phone/messaging apps: Allowed
- Voice recorder: Allowed
- Everything else: Ask every time or Deny

Contacts

- Phone/messaging apps only
- Social media: Deny (they'll upload your contacts)

Calendar, Call logs, SMS, Phone, Files

- Review carefully—most apps don't need these

Body sensors (fitness trackers)

- Only fitness/health apps

Nearby devices (Bluetooth)

- Only headphones, wearables, smart home devices

Rule: If you can't immediately explain why an app needs a permission, it doesn't need it.

3.5 Location Services

Path: Settings → Location

Android Settings

☑ Action Checklist

Use location → Keep ON (but control per-app)

- Turning completely off breaks Maps, Emergency Location

App location permissions → Review each app

- See permission manager instructions above

Location services (bottom of page)

- Emergency Location Service: ON (keep)
- Google Location Accuracy: Personal choice
- Google Location History: OFF
- Google Location Sharing: OFF
- Wi-Fi scanning: OFF
- Bluetooth scanning: OFF

! CRITICAL

Google Location History (Timeline):
When enabled, Google logs:

- Everywhere you go with your phone
- How long you stayed
- Route you took
- Mode of transportation
- Places you visited

Turn OFF: Settings → Location → Location services → Google Location History → Turn off
Delete existing history:

1. Visit https://myactivity.google.com/activitycontrols/location
2. Auto-delete → Delete all Location History

3.6 Google Account Privacy Settings

Many privacy settings are in your Google Account, not phone settings.

Path: Settings → Google → Manage your Google Account
Or visit: https://myaccount.google.com

3.6.1 Data & Privacy

Android Settings

☑ Action Checklist

Web & App Activity → Pause

- Google tracks your searches, YouTube watches, app usage
- Delete existing: Manage history → Delete activity

Location History → Pause (as mentioned above)

YouTube History → Pause if you value privacy

- YouTube watch and search history
- Disabling reduces recommendations accuracy

Ad personalization → Turn OFF

- Visit: https://adssettings.google.com
- Turn off Ad Personalization
- Review ”Your categories” and remove

3.6.2 People & Sharing

Android Settings

☑ Action Checklist

Shared endorsements → Uncheck

Location sharing → Review who can see your location

Photo sharing → Review and minimize

3.7 App-Specific Settings

3.7.1 Chrome Browser

Path: Open Chrome → Three dots → Settings → Privacy and security

Android Settings

☑ Action Checklist

Do Not Track → ON

Safe Browsing → Standard protection or Enhanced

Always use secure connections → ON

Clear browsing data → Set up regular clearing

Cookies → Block third-party cookies

Site settings → Review and revoke unnecessary permissions

Privacy Sandbox → Disable ad measurement

Consider alternatives: Firefox Focus, Brave, or DuckDuckGo Browser for better privacy.

3.7.2 Google Photos

Path: Open Google Photos → Profile icon → Photos settings

Android Settings

☑ Action Checklist

Backup → Personal choice

- Convenient but photos uploaded to Google
- Alternative: Manual backup to computer/NAS

If backup enabled:

- Backup quality: Original (not compressed)
- Backup using cellular data: OFF (WiFi only)
- Locked folder: Enable and use for sensitive photos

Memories → Turn OFF (or customize heavily)

- Disable people & pets, trips, themes
- Prevents Google from auto-creating albums

Group similar faces → Turn OFF

- Facial recognition and grouping
- Privacy concern

3.8 Google Play Store

Path: Open Play Store → Profile icon → Settings

Android Settings

☑ Action Checklist

General → Auto-update apps → Over Wi-Fi only

About → Play Protect → ON

- Scans apps for malware
- Keep this enabled

Family → Require authentication for purchases → For all purchases

General → App download preference → Over Wi-Fi only

3.9 Security Features

Path: Settings → Security & privacy

3.9.1 Security Updates

Android Settings

☑ Action Checklist

System update → Check for updates

- Android security patches released monthly
- Install immediately when available
- Pixel phones get 7 years of updates (Pixel 8+)

Google Play system update → Check for updates

- Separate from Android updates
- Updates core services monthly

3.9.2 Find My Device

Path: Settings → Security & privacy → Device finders → Find My Device

Android Settings

☑ **Action Checklist**

Use Find My Device → ON

- Locate, ring, lock, or erase device remotely
- Access at: https://www.google.com/android/find

Find My Device network → ON

- Uses Bluetooth and nearby Android devices
- Helps find phone when offline

3.10 Developer Options (Advanced)

For additional security, enable Developer Options and configure:

Enable Developer Options:

1. Settings → About phone
2. Tap ”Build number” 7 times
3. Enter PIN/password
4. Developer options now available in Settings → System

Android Settings

☑ **Action Checklist**

In Developer Options:

Stay awake → Keep OFF (battery drain, security risk)

USB debugging → Keep OFF unless actively developing

- Allows computer to control phone
- Security risk if enabled

Default USB configuration → No data transfer

- Prevents data access when plugged into unknown USB port
- Charging only by default

4 Universal Mobile Security Principles

These apply to both iOS and Android.

4.1 App Security Best Practices

4.1.1 Before Installing Apps

☑ Action Checklist

Vet apps before installing:

Check developer name—is it legitimate?

Review permissions requested—are they reasonable?

Read recent reviews (1-2 star reviews reveal problems)

Check number of downloads (very low = suspicious)

Google the app name + ”malware” or ”privacy”

If app seems too good to be true, skip it

Prefer web version over installing app when possible

4.1.2 App Audit and Cleanup

☑ Action Checklist

Quarterly app audit:

Review all installed apps

Delete apps you haven’t used in 3+ months

Update all apps (security patches)

Review permissions for remaining apps

Revoke unnecessary permissions

Check app subscriptions and cancel unused

4.2 Network Security

4.2.1 WiFi Security

Warning

Public WiFi dangers:

- Man-in-the-middle attacks intercept traffic
- Fake WiFi networks (”Starbucks WiFi” is actually attacker)
- Unencrypted WiFi exposes all traffic
- Packet sniffing captures passwords, emails

Protection:

- Use VPN on all public WiFi
- Disable auto-connect to WiFi networks
- Forget networks after use
- Use cellular data instead when possible
- Only visit HTTPS sites (check for lock icon)

4.2.2 Bluetooth Security

Action Checklist

Turn off Bluetooth when not in use

Set device as ”Not Discoverable”

Forget paired devices you no longer use

Don’t pair with unknown devices

Deny pairing requests from unknown sources

4.3 Backup Strategy

4.3.1 Encrypted Backups

iOS:

- iCloud Backup with Advanced Data Protection: Encrypted end-to-end
- Local encrypted backup via Finder/iTunes:
  1. Connect iPhone to computer
  2. Open Finder (Mac) or iTunes (Windows)

3. Select iPhone
4. Check ”Encrypt local backup”
5. Set strong password (store in password manager)
6. Back up now

Android:

- Google One backup: Encrypted in transit, not end-to-end
- Better: Use third-party encrypted backup (Titanium Backup with encryption)
- Or manual backup to computer with encryption

Pro Tip

Backup frequency:

- Before OS updates: Always
- Regular schedule: Weekly or monthly
- Before international travel
- After major life events (photos, important messages)

Test restore process annually—backups are useless if you can’t restore from them.

4.4 Physical Security

☑ **Action Checklist**

Protect your phone physically:

Use case with screen protector

Enable Find My iPhone/Find My Device before loss

Never leave phone unattended in public

Don’t store phone in easily pickpocketed locations

Use privacy screen protector (prevents shoulder surfing)

Cover webcam when not in use (rare on phones, common on tablets)

Be aware of surroundings when entering passcode

4.5 What to Do If Phone Is Lost or Stolen

Immediate actions (within first hour):

☑ Action Checklist

Use Find My to locate phone

- iOS: https://www.icloud.com/find
- Android: https://www.google.com/android/find

If nearby: Play sound, navigate to location

If stolen/unrecoverable: Mark as Lost (iOS) or Lock (Android)

- Displays message with contact number
- Locks device remotely

If recovery impossible: Erase device remotely

- Wipes all data
- Prevents thief from accessing your information

Contact carrier: Suspend service, prevent unauthorized use

File police report: Get report number for insurance

Follow-up actions (first 24 hours):

☑ Action Checklist

Change passwords for critical accounts:

- Apple ID / Google Account
- Email
- Banking apps
- Password manager (if on phone)

Review account activity for unauthorized access

Notify bank if mobile banking app was on phone

Deactivate any payment methods (Apple Pay, Google Pay)

Sign out of accounts on lost device remotely

Contact insurance (homeowners/renters may cover theft)

Monitor for SIM swap attacks (carrier notifications of SIM changes)

5 Complete Hardening Checklist

5.1 iOS Hardening Checklist

☑ Action Checklist

Lock Screen & Passcode:

Custom Alphanumeric Passcode (12+ characters)

Require Passcode: Immediately

Allow Access When Locked: Most features OFF

USB Accessories When Locked: OFF

Erase Data after 10 attempts: ON

Face ID / Touch ID configured with Require Attention

Privacy Settings:

Location Services: Managed per-app, Precise Location OFF

Significant Locations: OFF and history cleared

System Services location: Minimal enabled

Tracking: Don't allow apps to request

Apple Advertising: Personalized Ads OFF

App permissions audited and minimized

Analytics & Improvements: All OFF

iCloud & Apple ID:

Advanced Data Protection: ON

Recovery contacts or recovery key configured

iCloud sync reviewed and minimized

Hide My Email enabled

Safari & Browsing:

Prevent Cross-Site Tracking: ON

Hide IP Address: Trackers and Websites

Advanced Tracking Protection: ON

Security:

Find My iPhone: ON with network and last location

Screen Time passcode set (locks privacy settings)

Two-factor authentication enabled for Apple ID

Latest iOS version installed

5.2 Android Hardening Checklist

☑ Action Checklist

Lock Screen & Security:

PIN (6+ digits) or Password (12+ characters)

Fingerprint unlock configured

Lock immediately on screen timeout

Power button instantly locks: ON

Device encryption verified

Lockdown mode tested

Privacy Settings:

Privacy Dashboard reviewed regularly

Permission Manager: All permissions audited

Location: Per-app with Precise Location OFF

Google Location History: OFF and deleted

Wi-Fi and Bluetooth scanning: OFF

Google Account:

Web & App Activity: Paused

Location History: Paused

YouTube History: Paused

Ad Personalization: OFF

Two-factor authentication enabled

Apps:

Chrome: Third-party cookies blocked, Do Not Track ON

Google Photos: Backup configured or disabled, Face grouping OFF

Play Store: Play Protect ON, auto-update over WiFi

Unused apps deleted

Security:

Find My Device: ON with network

System updates: Latest Android version

Google Play system update: Current

Developer Options: USB debugging OFF, Default USB: No data transfer

5.3 Ongoing Maintenance

☑ Action Checklist

Weekly:

Review Privacy Dashboard (Android) or Screen Time (iOS)

Check for suspicious app behavior

Monthly:

Update all apps

Review and revoke unnecessary app permissions

Check for OS security updates

Backup device

Quarterly:

Complete app audit (delete unused apps)

Review all privacy settings (use this guide)

Change device passcode

Test Find My Device functionality

Review backup and test restore

Annually:

Consider factory reset and clean install

Review and update emergency contacts

Audit device list on accounts (remove old devices)

Update Apple ID / Google Account recovery information

6 Conclusion

6.1 Key Takeaways

Mobile devices are the most personal and most vulnerable technology we carry. Proper hardening requires:

1. **Strong authentication:** Alphanumeric passcodes, not simple PINs
2. **Permission discipline:** Apps get only what they absolutely need
3. **Location control:** Minimal location sharing, no location history
4. **Regular updates:** OS and app updates patch security holes
5. **Backup strategy:** Encrypted backups, tested regularly
6. **Behavioral security:** Awareness of physical and digital threats

6.2 iOS vs. Android: Final Recommendation

For most users: iPhone with iOS

- Better security out-of-box
- Longer update support
- More consistent privacy controls
- Less configuration required
- Higher baseline security

For advanced users: Google Pixel with Android

- Full control over device
- Can achieve excellent security with proper configuration
- 7-year update guarantee (Pixel 8+)
- More customization options
- GrapheneOS compatible (maximum security)

Avoid: Other Android manufacturers (unless you know what you're doing)

- Short update windows (2-3 years)
- Bloatware and pre-installed apps
- Inconsistent security patches
- Modified Android with opaque changes

6.3 Next Steps

1. **This week:** Configure lock screen and passcode settings
2. **This month:** Complete privacy settings configuration
3. **This quarter:** Audit and minimize app permissions
4. **Ongoing:** Monthly updates and quarterly reviews

6.4 Additional WigSec Resources

Download our other security guides:

- Password Manager Setup Guide (18 pages)
- Social Media Privacy Configuration (32 pages)
- Complete Data Broker Removal Guide (24 pages)
- Breach Response Playbook (16 pages)
- Email Security & Privacy Guide (20 pages)

All guides free at: https://wigingtonsecurity.com/guides

Need Help With Device Security?

We offer personalized device hardening and security audits.
Services:

- Device Security Audit ($100)
- Hands-on Configuration Session ($75)
- Family Device Setup ($150 for 2-4 devices)
- Lost/Stolen Device Response ($200)

Contact: https://wigingtonsecurity.com/contact
Schedule: https://wigingtonsecurity.com/services

Remote and in-person support available

Document Version 1.0 • February 2026

https://wigingtonsecurity.com