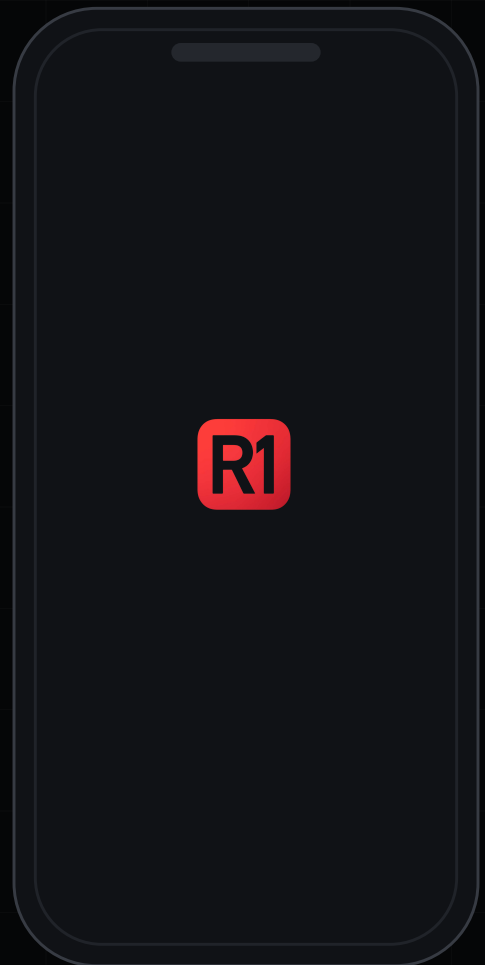




2026 FIELD GUIDE

iPHONE PRIVACY GUIDE

A risk-calibrated checklist for stronger device,
account, and communications security.



START HERE

Protection without guesswork

Optimizing your iPhone's security and privacy protects personal data, financial information, and online identity. The checklist below provides clear steps and habits to maximize protection across your device and accounts.

● Important Note on Trade-Offs

Some hardening steps reduce convenience or change familiar features. Choose options that match your risk profile. Items are organized by their day-to-day impact compared with a standard, non-hardened iPhone.

01

LOW IMPACT

Recommended for everyone

Minimal disruption

02

MEDIUM IMPACT

Recommended for most users

May affect everyday use

03

HIGH IMPACT

For higher-risk users

Maximum attack-surface reduction

Apply settings deliberately and confirm that critical communications and recovery options still work.

01

Low Impact

MINIMAL DISRUPTION

These improve security and privacy with minimal disruption. Recommended for all users.

01

Software Updates

Enable automatic iOS updates

1. Open Settings.
2. Go to General → Software Update → Automatic Updates.
3. Turn on "Download iOS Updates" and "Install iOS Updates."

Install new updates promptly

1. Settings → General → Software Update.
2. Tap "Update Now" when available.

Keep all apps updated

1. Settings → App Store → turn on "App Updates."
2. In the App Store, tap your profile icon → "Update All" when needed.

02

App Store and Download Controls

Enable automatic app updates

1. Settings → App Store → "App Updates" → On.

Disable automatic app installations from other devices (if not needed)

1. Settings → App Store → Automatic Downloads → "Apps" → Off.

Turn off Background App Refresh for nonessential apps

1. Settings → General → Background App Refresh.
2. Choose Off (entirely) or Wi-Fi only, or turn Off per app.

03

Require Face ID for Sensitive Apps

Add Face ID lock to individual apps (where available)

1. Touch and hold the app icon → choose "Require Face ID" or "Hide and Require Face ID" (if shown).
2. Or go to Settings → Face ID & Passcode → "Locked & Hidden Apps" → select apps.

Use in-app locks (if provided by the app)

1. Open the app's settings.
2. Enable Face ID/Passcode or the app's "Lock" feature.

04

Reduce App Bloat

Remove unused apps to reduce data leakage and attack surface

1. Touch and hold an app → Remove App → Delete App.
2. Or: Settings → General → iPhone Storage → select app → Delete App.

05

Web Browsing Settings

Prevent cross-site tracking in Safari

1. Settings → Safari → turn on "Prevent Cross-Site Tracking."

Enable advanced anti-fingerprinting protections (if available)

1. Settings → Safari → Advanced → Advanced Tracking and Fingerprinting Protection → set to "All Browsing."

Block cookies (only if compatible with your browsing needs)

1. Settings → Safari → "Block All Cookies" → On.

Clear history and website data regularly

1. Settings → Safari → "Clear History and Website Data" → Clear.

Consider privacy-focused search and browsing for sensitive tasks

1. Settings → Safari → Search Engine → select a privacy-focused option such as Duck-Duck-Go.
2. Install a privacy-focused browser such as Firefox Focus and use it for sensitive browsing.

Understand Safari's "Hide IP Address"

1. Settings → Safari → Hide IP Address.
2. Note: this is not a VPN; choose settings based on your threat model.

Optionally disable metadata-sharing features

1. Settings → Safari → turn off "Privacy-Preserving Ad Measurement."
2. Settings → Safari → turn off "Search Engine Suggestions" and "Safari Suggestions."
3. Settings → Safari → turn off "Fraudulent Website Warning" only if you prefer not to share browsing metadata (may reduce phishing protection).

06

Apple ID and iCloud Security

Enable Two-Factor Authentication (2FA)

1. Settings → [your name] → Password & Security → "Turn On Two-Factor Authentication."

Use a strong, unique Apple ID password and rotate periodically

1. Settings → [your name] → Password & Security → Change Password.

Review signed-in devices

1. Settings → [your name] → scroll to devices.
2. Tap a device → "Remove from Account" if unrecognized.

Review iCloud sync and disable unnecessary categories

1. Settings → [your name] → iCloud → toggle off items you do not need synced.

Enable Advanced Data Protection (end-to-end encryption)

1. Settings → [your name] → iCloud → Advanced Data Protection → Turn On.
2. Ensure passcode and 2FA are enabled first.

Turn off Automatic Verification (reduce verification-signal sharing)

1. Settings → [your name] → Password & Security → "Automatic Verification" → Off.

07

Restrict Changes to Face ID, Passcode, and Account Settings

Require a separate Screen Time passcode for changing sensitive settings

1. Settings → Screen Time → Turn On Screen Time.
2. Tap "Use Screen Time Passcode" and set a passcode different from your device passcode.
3. Tap Content & Privacy Restrictions → On.
4. Under "Allow Changes," restrict "Account Changes," "Passcode Changes," and others as desired.

08

Data Protection and Encryption

Ensure device encryption (passcode required)

1. Settings → Face ID/Touch ID & Passcode → "Turn Passcode On" (if not already).

Require passcode immediately

1. Settings → Face ID/Touch ID & Passcode → Require Passcode → Immediately.

Use a trusted password manager; optionally turn off iCloud Keychain

1. Install and set up your chosen password manager.
2. To disable Keychain: Settings → [your name] → iCloud → Passwords and Keychain → Off.

Turn off AutoFill Passwords for high-risk apps

1. Settings → Passwords → Password Options → "AutoFill Passwords" → Off (or deselect specific apps).

Shorten iMessage retention

1. Settings → Messages → Keep Messages → select "30 Days" or "1 Year."

Remove location data from photos/videos before sharing

1. In Photos, tap Share → Options → turn off "Location."

09

Find My and Lost-Device Protection

Enable Find My and verify Activation Lock

1. Settings → [your name] → Find My → Find My iPhone → turn on "Find My iPhone" and "Find My network."
2. Activation Lock is enabled when Find My iPhone is on with your Apple ID.

Review and update trusted recovery contacts

1. Settings → [your name] → Password & Security → Account Recovery → Add/Manage Recovery Contacts.

Calibrate to your risk model (limit or disable if location privacy outweighs recovery)

1. Settings → [your name] → Find My → adjust or turn off as desired.

10

Safety Check and Emergency Reset

Locate Safety Check and know how to use it

1. Settings → Privacy & Security → Safety Check.
2. Use "Emergency Reset" to immediately stop sharing and review account security.

Periodically audit sharing

1. Safety Check → "Manage Sharing & Access" → review People, Apps, and Device Access → stop sharing where unnecessary.

02

Medium Impact

STRONGER CONTROLS

These changes are highly effective and may affect everyday use. Recommended for most users.

11

Limit Wired Access

Restrict cable/data access while locked

- 1. Settings → Face ID/Touch ID & Passcode.
- 2. Ensure "USB Accessories" is Off (prevents accessories from connecting while locked).
- 3. If your iOS version shows Accessories/Wired Accessories permissions, set them to "Ask."

12

Screen Unknown Callers and Senders

"Screen Unknown Callers" and "Screen Unknown Senders"

- 1. Settings → Phone → "Silence Unknown Callers" → On.
- 2. Settings → Messages → "Filter Unknown Senders" → On.

13

Device Lock and Passcode

Use a strong alphanumeric passcode

- 1. Settings → Face ID/Touch ID & Passcode → Change Passcode → Passcode Options → Custom Alphanumeric Code.

Keep biometrics enabled for convenience and security

- 1. Settings → Face ID/Touch ID & Passcode → set up Face ID or Touch ID.

Disable lock-screen access to sensitive items

- 1. Settings → Face ID/Touch ID & Passcode → "Allow Access When Locked" → turn off items you do not need (Control Center, USB Accessories, Siri, Wallet, etc.).

Remove lock-screen widgets and hide notification previews

- 1. Long-press the Lock Screen → Customize → remove unneeded widgets.
- 2. Settings → Notifications → Show Previews → Never.

Consider auto-erase after failed attempts

- 1. Settings → Face ID/Touch ID & Passcode → "Erase Data" → On.

14

App Permissions and Privacy Controls

Location permissions per app

1. Settings → Privacy & Security → Location Services → select app → choose "While Using" or "Ask Next Time"; turn Off if not needed.

System Services that use location

1. Settings → Privacy & Security → Location Services → System Services → turn off items you do not need (Alerts, In-App Web Browsing, Networking & Wireless, Suggestions, Significant Locations, Product Improvements).

Microphone, Camera, Photos, Contacts, Calendars, Files access

1. Settings → Privacy & Security → each category → review and disable for apps that do not need access.

Bluetooth and Local Network access

1. Settings → Privacy & Security → Bluetooth → review/disable per app.
2. Settings → Privacy & Security → Local Network → review/disable per app.

App tracking

1. Settings → Privacy & Security → Tracking → "Allow Apps to Request to Track" → Off.

Apple advertising personalization

1. Settings → Privacy & Security → Apple Advertising → "Personalized Ads" → Off.

Analytics & Improvements

1. Settings → Privacy & Security → Analytics & Improvements → turn off "Share iPhone Analytics," "Share iCloud Analytics," and any "Improve" toggles you do not need.

Research Sensor & Usage Data (if available)

1. Settings → Privacy & Security → Research Sensor & Usage Data → Off.

Motion & Fitness

1. Settings → Privacy & Security → Motion & Fitness → "Fitness Tracking" → Off (if not required).

Exposure Notifications

1. Settings → Exposure Notifications → turn off if not needed.

Journaling Suggestions and "Discoverable by Others"

1. Settings → Privacy & Security → Journaling Suggestions → turn off suggestions.
2. Turn off "Discoverable by Others" if you prefer stricter privacy.

Sensitive Content Warning

1. Settings → Privacy & Security → Sensitive Content Warning → Off if you do not want on-device analysis of photos/messages.

15

Network and Connectivity Security

Avoid auto-joining untrusted Wi-Fi and prune old networks

1. Settings → Wi-Fi → tap the info (i) next to a network → "Auto-Join" → Off for unfamiliar networks.
2. Tap "Forget This Network" for old or untrusted SSIDs.

Limit app access to Bluetooth and Local Network

1. Review regularly using the steps above under App Permissions and Privacy Controls.

16

Use an Encrypted, No-Logs VPN

Add a reputable VPN, especially on public Wi-Fi

1. Install a VPN app such as Proton VPN or Nord VPN from the App Store.
2. Open the app, complete setup, and allow VPN configuration.
3. Activate the VPN from the app or via Settings → VPN.

17

Apply DNS Configurations

Use a private DNS provider (for example, NextDNS)

1. Option A - Per-Wi-Fi DNS:
 2. Settings → Wi-Fi → tap (i) next to your network → Configure DNS → Manual.
 3. Add server addresses → Save.
4. Option B - System profile (if provided by the DNS service):
 5. Install the configuration profile.
 6. Settings → General → VPN & Device Management → verify the profile is installed and active.

18

Limit AirDrop Until Needed

Restrict AirDrop

1. Settings → General → AirDrop → set to "Receiving Off" or "Contacts Only."
2. Or open Control Center → press and hold the connectivity tile → AirDrop → choose setting.

Turn off AirPlay & Handoff features you do not use

1. Settings → General → AirPlay & Handoff → turn off features you do not need (Handoff, Transfer to HomePod, etc.).

03

High Impact

MAXIMUM REDUCTION

Apply these when you require maximum reduction of attack surface. Recommended for high-risk users.

19

Limit or Disable iCloud

Reduce cloud exposure

1. Settings → [your name] → iCloud → turn off categories you do not want in the cloud.
2. For full sign-out: Settings → [your name] → Sign Out. Ensure you have local backups and alternate storage first.

20

Disable iMessage and FaceTime

Remove Apple messaging services

1. Settings → Messages → "iMessage" → Off.
2. Settings → FaceTime → "FaceTime" → Off.
3. Use end-to-end encrypted messengers and privacy-centric email providers (for example, Signal, Proton).

21

Disable Siri

Turn off Siri and delete history

1. Settings → Siri & Search → turn off "Listen for 'Hey Siri'" and "Press Side Button for Siri."
2. Scroll down and disable Siri Suggestions you do not need.
3. Settings → Siri & Search → Siri & Dictation History → "Delete Siri & Dictation History."

22

Enable Lockdown Mode

Maximum protection against targeted attacks

1. Complete other configurations first (for example, VPN/DNS profiles).
2. Settings → Privacy & Security → Lockdown Mode → "Turn On Lockdown Mode" → "Turn On & Restart."
3. Be aware that many features and content types are restricted while Lockdown Mode is active. Plan the order of operations accordingly.