# Smartphone Stalkerware Detection Checklist

Reviewed and revised September 30, 2026

This checklist helps you look for common signs that an iPhone or Android phone may be monitored, review location-sharing and account access, check for unknown Bluetooth trackers, and identify settings that deserve closer examination. It cannot prove that a device is clean or compromised, and it is not a substitute for a professional forensic examination. This checklist is general educational information only and does not constitute legal, security, or professional advice. No attorney-client or professional-services relationship is created by use of this checklist.

**Safety first.** If you suspect an abusive partner, stalker, or other person is monitoring you, changing settings, deleting an app, removing a tracker, resetting the phone, or researching the issue on that phone may alert the person monitoring you. When safety is a concern, consider using a different trusted device to seek help and preserve relevant evidence before making changes. The FTC specifically warns that cutting off stalkerware access can cause an abuser to escalate. [1]

**Scope:** U.S.-focused general information, provided as-is without warranty of any kind. Safe Harbor Advisory assumes no liability for any harm arising from use of or reliance on this checklist. Menu names and features change by operating-system version and phone manufacturer. A legitimate work/school management profile, accessibility service, VPN, or location-sharing feature can look unusual without being malicious. Do not delete something solely because you do not recognize it; document it first and determine what it is. For immediate danger, call 911 or go to a safe public location.

## Immediate action checklist

☐ If personal safety may be at risk, use a safer device to contact a trusted person, advocate, attorney, law enforcement, or qualified security professional before changing the suspected phone. [1]

☐ Document suspicious behavior before altering the device: unexpected alerts, unknown apps or profiles, unusual account sessions, tracker notifications, and relevant dates/times. Take screenshots when safe.

☐ Do not assume fast battery drain, heat, high data use, or crashes prove stalkerware. They are warning signs only and have many ordinary causes. [1]

☐ Review account access as well as the phone itself. A person with access to your Apple Account, Google Account, shared location, cloud services, or passwords may be able to monitor you without installing stalkerware.

☐ Check for unknown Bluetooth trackers in your belongings or vehicle. Both current iPhone/iPad and Android systems can warn about compatible trackers moving with you. [2][7]

☐ If the device may be evidence in a criminal, civil, employment, or family-law matter, consider professional preservation or forensic help before factory-resetting or discarding it.

# Signs that justify a closer look

- Someone repeatedly knows your exact location, private conversations, messages, browsing activity, or plans without an obvious explanation.
- The person had physical access to your unlocked phone or knows/guessed your device passcode.
- You find an unfamiliar app, account, configuration profile, device-management entry, VPN, accessibility service, or signed-in device.
- Your phone shows an unwanted-tracker alert, or you find an unfamiliar AirTag or compatible Bluetooth tracker.
- Battery drain, data use, overheating, or unexpected restarts changed significantly without another explanation. These symptoms are not proof of surveillance. [1]



# iPhone and iPad review

### 1 Use Apple Safety Check

On iPhone with iOS 16 or later, go to **Settings > Privacy & Security > Safety Check**. Apple provides two approaches: Manage Sharing & Access for a guided review, and Emergency Reset to quickly stop sharing with people and apps and review account security. Safety Check can also help change the device passcode or Apple Account password. [3]

**Important:** Safety Check does not cover every possible source of monitoring. Apple notes that other accounts, social-media sharing, and information shared from other devices may require separate review. [3]

### 2 Review Apple Account devices and device access

☐ Go to **Settings > [your name] and review the devices associated with your Apple Account**. If a device is unfamiliar, document it before removing it when evidence may matter. Apple allows an unknown device to be removed from the account. [4]

☐ Review trusted devices and Apple Account security information. An unknown trusted device can receive verification codes or access Apple services until access is removed. [4]

☐ Check for unexpected Face ID appearances or Touch ID fingerprints and change the device passcode if someone else may know it. [4]

☐ Review installed apps for anything you do not recognize or remember installing. An unfamiliar app is a reason to investigate, not automatic proof of stalkerware. [4]

### 3 Check configuration profiles and device management

Go to **Settings > General > VPN & Device Management**. If you do not see any profiles, Apple says no device-management profiles are installed. Profiles and mobile-device-management (MDM) tools are commonly legitimate for employers and schools, but they can manage settings and may permit access to data or location information. If a profile is unexpected, document it and determine who installed it before deletion. Removing a profile can also remove settings, apps, or data associated with it. [5]

### 4 Review location and app access

- ☐ In **Settings > Privacy & Security, review Location Services and the apps allowed to use location, microphone, camera, photos, contacts, Bluetooth, and other sensitive data**.
- ☐ Pay particular attention to apps with access that does not make sense for their function, or apps you do not recognize.
- ☐ Review Find My, Family Sharing, shared calendars/photos, and other sharing features if another person may be receiving information through normal Apple sharing rather than hidden software.

### 5 Check for unwanted Bluetooth trackers

If an AirTag, compatible Find My accessory, or compatible Bluetooth tracker appears to be moving with you, iPhone/iPad can issue an unwanted-tracking notification. In Find My, review Items > Unknown Items Detected with You (wording can vary by OS). Apple can provide a map, play a sound, and in supported cases help locate the item. If you find a tracker, save its serial/device information before disabling it when safe. Turning off Bluetooth, Location Services, or your phone does not itself disable the tracker; follow the manufacturer's disable instructions. [2]



# Android review

Android varies by manufacturer. The paths below reflect current Google/Android guidance; Samsung, Motorola, Pixel, and other devices may use different labels. Use Settings search when a named menu is not present.

### 1 Review every installed app and sensitive permission

- ☐ Open **Settings > Apps (or Apps > See all apps) and review the complete app list**. Investigate apps you do not recognize. Some monitoring software may use an innocuous or system-like name. [1]
- ☐ Open **Settings > Security & privacy/Privacy > Privacy dashboard**. On supported Android versions, the dashboard shows which apps accessed sensitive permissions and when. Review location, microphone, camera, contacts, SMS, phone, files/photos, and nearby-device access. [6]
- ☐ Review apps allowed to use Location 'all the time.' Google allows location access to be managed by app and, on supported devices, precise location can be limited. [8]
- ☐ On Android 12 and later, a green indicator appears when an app is using the camera or microphone. Tap the indicator from Quick Settings to see which app/service is using it. [9]

### 2 Confirm Google Play Protect is on

Open the **Google Play Store > profile icon > Play Protect > Settings and confirm Scan apps with Play Protect is enabled**. Google says Play Protect checks installed apps for harmful behavior, including apps from outside Google Play, and may warn, disable, or remove potentially harmful apps. Play Protect is useful but a clean result is not proof that no monitoring exists. [10]

### 3 Review elevated access

Use Settings search to review Device admin apps/device administrators, Accessibility services/installed services, VPN, Install unknown apps, and other 'special app access' categories available on your phone. Monitoring or remote-control apps may rely on elevated permissions, but legitimate security, work-management, accessibility, password-manager, and VPN apps may use them too. Document unfamiliar entries and verify their purpose before disabling them.

### 4 Review Google Account sessions

Go to your **Google Account > Security & sign-in > Your devices > Manage all devices**. Review devices and sessions. Google allows you to sign out sessions you do not recognize and recommends securing the account if activity is unfamiliar. [11]

### 5 Scan for unknown trackers

On supported Android devices, go to **Settings > Safety & emergency > Unknown tracker alerts > Scan now**. On some older Android versions the path is **Settings > Google > Personal & device safety > Unknown tracker alerts**. Google says the scan can identify compatible trackers currently nearby and separated from their owners. Automatic alerts can also warn when an unknown tracker appears to be moving with you. [7]

Do not rely on Airplane Mode, Bluetooth-off, or Location-off as a way to disable a physical tracker. Google and Apple both explain that stopping your phone's radio/location features does not necessarily stop the tracker itself from reporting its location through other nearby devices. Follow the tracker's disable instructions after documenting it, if safe. [2][7]



# If you find something suspicious

### Preserve before you remove

- ☐ Take screenshots or photographs of the suspicious app/profile/service, permissions, device/session details, tracker alert/map, serial number, and relevant dates/times when safe.
- ☐ Write down what led you to suspect monitoring: what the other person knew, when it happened, and any threats or admissions.
- ☐ If litigation, a protection order, employment action, insurance claim, or criminal investigation may follow, consider qualified forensic or legal guidance before changing the device. This checklist does not address the full scope of evidence-preservation obligations that may apply. Ordinary screenshots are useful context but are not a substitute for forensic preservation.

## Choose the response that fits the risk

| Situation | Safer next step |
|---|---|
| Possible intimate-partner or stalking risk | Use a separate trusted device to seek help. Make a safety plan before removing access; the FTC warns that removal can alert an abuser and may lead to escalation. [1] |
| Unknown physical tracker | Move to a safe public location if needed; save the alert/map and serial or device information; consider law enforcement; disable the tracker only when safe. [2][7] |
| Unknown Apple/Google account device or session | Document it, then secure the account from a trusted device: change the password, review recovery methods and multi-factor authentication, and remove/sign out unfamiliar devices. [4][11] |
| Unexpected iPhone management profile | Determine whether it belongs to an employer/school. If unauthorized, document it and consider expert guidance before removal; removing it can delete associated settings/data. [5] |
| Unknown Android app or elevated service | Document the app name, source, permissions, and elevated access. If personal safety/evidence is not a concern, revoke unnecessary access and uninstall suspicious software; otherwise seek qualified help first. |

© 2026 Safe Harbor Advisory

### Resetting or replacing the phone

The FTC says a factory reset may remove stalkerware, and in some cases a new phone with an account the suspected abuser cannot access may be the safer option. The FTC also cautions against restoring apps from a backup of the suspected phone because doing so could reinstall unwanted software; instead, reinstall needed apps from the official app store. A factory reset permanently erases all data on the device and cannot be undone. Preserve evidence and important data first, and consider the safety implications before making a change that may alert another person. [1]

### Reduce the chance of reentry

☐ Use a new, unique device passcode that the suspected person cannot guess; do not reuse a known passcode.

☐ Change Apple/Google and primary email passwords from a trusted device when compromise is suspected. Use unique passwords and enable multi-factor authentication/passkeys where available.

☐ Review account recovery phone numbers/emails, trusted devices, active sessions, and connected apps.

☐ Install operating-system and app updates promptly. Keep Google Play Protect enabled on Android. [1][10]

☐ Keep physical control of the phone. Stalkerware installation often depends on physical access, account access, or weakened device security. [1]



## What this checklist can and cannot tell you

Consumer checks can identify many common exposure paths: shared accounts, location sharing, unknown trackers, suspicious apps, unexpected management profiles, elevated permissions, and unfamiliar account sessions. They cannot rule out every form of surveillance, and completing this checklist does not guarantee that a device is free from monitoring.

- A phone can be monitored through compromised cloud or email credentials even when no stalkerware app is installed.
- A physical tracker may be hidden in a bag, vehicle, clothing, or other property rather than attached to the phone.
- Some sophisticated compromises may leave few visible signs. A professional mobile-device forensic examination may be appropriate when the stakes are high or suspicious behavior continues after account/device remediation.
- Conversely, battery drain, heat, data usage, or an unfamiliar technical entry can have benign explanations. Avoid declaring a device 'hacked' based on one symptom.

## Quick review worksheet

☐ Safety risk considered before making changes

☐ Suspicious behavior/events documented

☐ Apple/Google account devices and sessions reviewed

☐ Device passcode and account recovery methods reviewed

☐ Installed apps reviewed

☐ Location permissions reviewed

☐ Microphone/camera and other sensitive permissions reviewed

☐ iPhone VPN & Device Management checked (iPhone/iPad)

☐ Android Privacy Dashboard checked (supported Android)

☐ Android Play Protect confirmed on

☐ Elevated Android access reviewed (device admin/accessibility/VPN/special access)

☐ Unknown Bluetooth tracker alerts/history reviewed

☐ Physical belongings/vehicle considered if tracker warning exists

☐ Evidence preserved before removal/reset where relevant

☐ Professional forensic/legal/safety support considered when stakes are high



## Support and escalation

- Immediate danger: call 911 or go to a safe public location.
- National Domestic Violence Hotline (U.S.): 1-800-799-SAFE (7233); text START to 88788; thehotline.org. The FTC recommends contacting an advocate from a device that is not suspected of being monitored. If the phone may be compromised, a phone call from a different device is safer than texting, because text messages may be visible to a person with access to the device or account. [1]
- Law enforcement: consider when a tracker, threats, stalking, extortion, unauthorized account access, or other suspected criminal conduct creates a safety concern.
- Qualified mobile-device forensic professional: consider when you need evidentiary preservation, the suspected compromise is sophisticated, or ordinary checks do not explain continuing surveillance.

# Sources supporting this checklist

Sources checked September 30, 2026. Operating-system menus, device features, support pages, and procedures can change without notice. Safe Harbor Advisory does not control, endorse, or guarantee the accuracy or continued availability of these third-party sources. These sources support the general guidance; they do not establish whether a particular device is compromised.

[1] Federal Trade Commission - Stalkerware: What To Know
Open source

[2] Apple Support - What to do if an unknown AirTag or compatible Bluetooth tracker is with you
Open source

[3] Apple Support - Safety Check / Personal Safety User Guide
Open source

[4] Apple Support - Checklist 1: Limit device and account access
Open source

[5] Apple Support - Review and delete configuration profiles
Open source

[6] Android Help - Manage permissions from the Privacy Dashboard
Open source

[7] Android Help - Find unknown trackers
Open source

[8] Android Help - Manage location permissions for apps
Open source

[9] Android Help - Check if your Android camera or microphone is on or off
Open source

[10] Google Play Help - Use Google Play Protect
Open source

[11] Google Account Help - See devices with account access
Open source