DOMESTIC SAFETY

How To Detect Stalkerware On A Phone You Share

Plain-English how-to. ~30 minutes. The exact signs, the technical checks, and how to act safely if you find it.

Stalkerware is the commercial name for surveillance software designed to be installed on someone else's phone without their knowledge — often by an intimate partner, a controlling parent, or an estranged spouse. The marketing material almost always frames it as "parental monitoring" or "employee productivity tracking," but research from Norton, ESET, and the Coalition Against Stalkerware shows the dominant real-world use is intimate-partner surveillance. The Federal Trade Commission has taken enforcement action against multiple stalkerware vendors for facilitating illegal surveillance and concealing detection.

What stalkerware does is comprehensive. Once installed, it can read every text and iMessage, log every call (and often record audio), report GPS location continuously, copy photos, scrape contacts, and in some cases activate the camera and microphone silently. Most operate without showing an icon, without sending notifications, and without appearing in the standard installed-apps list. The victim's phone behaves normally; the abuser's dashboard shows everything in real time.

The damage extends far beyond privacy. For survivors of domestic violence, stalkerware on the phone they use to seek help is a direct safety threat. A call to a shelter, a text to a friend planning an exit, a search for restraining-order information — all become visible to the abuser, often before the survivor leaves the house. Multiple homicide investigations have traced the immediate trigger to stalkerware-detected exit planning. This is not a hypothetical risk.

The detection problem is harder than it sounds. Stalkerware is designed to evade casual inspection. Battery drain, occasional slow performance, and overheating are the most common symptoms — but those have many innocent causes. Searching the app drawer rarely helps because the icons are hidden. Modern stalkerware also auto-reinstalls if removed without breaking root, and aggressive removal can alert the installer. Detection has to be careful and the response — if confirmed — has to be planned, ideally in coordination with a domestic-violence professional.

Most online "how to detect stalkerware" articles tell readers to run a virus scan and call it a day. That misses the point. Real detection involves a specific sequence of checks (admin permissions, accessibility services, hidden processes, device profile inspection), a careful assessment of whether the suspected installer might react badly to discovery, and a safety plan before removing anything. Removing stalkerware without a safety plan can escalate the situation.

By the end of this guide you'll know the eight specific technical checks that find the most common stalkerware on iOS and Android, the behavioral signs that should prompt a check, the warning about not removing without a plan, and the trusted resources — the National Domestic Violence Hotline (1-800-799-7233), the Coalition Against Stalkerware, and the Safety Net project at NNEDV — that help with the safe-exit version of this problem. The technical part takes 30 minutes. The safety planning, when needed, is what matters most.

Quick snapshot

What you'll learn	How to detect stalkerware on iOS and Android, and what to do safely if you find it.
Skill level	Beginner-friendly · Safety-critical
Time required	30–60 minutes plus safety planning if found
What you'll need	Access to the phone, a quiet place to check, optionally a domestic-violence advocate
Risk if you skip this	Continued covert surveillance; immediate safety risk for abuse survivors
PDF kit	■ Download at the bottom of this page

Why this matters

Stalkerware is a documented tool in intimate-partner abuse. The Coalition Against Stalkerware and the Safety Net project at NNEDV both track its use and provide professional support to survivors. Multiple homicide investigations have traced the trigger to stalkerware-detected exit planning — when an abuser sees the victim reaching out for help, the danger escalates sharply.

The FTC has taken enforcement action against multiple stalkerware vendors for facilitating illegal surveillance. Stalkerware installation without consent is a federal crime in the US under the Computer Fraud and Abuse Act and the federal wiretap statute. Several states have additional dedicated stalkerware laws with criminal penalties.

Detection without a safety plan can escalate abuse. If you suspect stalkerware and you're in a controlling relationship, please call the National Domestic Violence Hotline (1-800-799-7233) before removing anything. They have technical-safety experts trained specifically for this scenario. The hotline is free, confidential, and available 24/7 in English, Spanish, and over 200 other languages.

Before you start

If you are in immediate danger, call 911. If you suspect stalkerware in the context of an abusive relationship, please call the National Domestic Violence Hotline at **1-800-799-7233** before doing any technical checks. They have technology-safety advocates who can help you plan.

If you are checking a phone for non-abuse reasons (a curious teen, a workplace device, a borrowed phone), the technical steps below are safe to run on your own.

Block uninterrupted time. Don't check in spurts that could be observed. If you share a phone, do the check when you have private access.

Step 1 — Recognize the behavioral signs

Common signs: rapid battery drain, unusually warm device, increased mobile-data usage, the device powering on or screen lighting up without input, calls or texts you don't remember making, the abuser knowing things they shouldn't.

These signs are not definitive but they're worth a check. Multiple signs together — especially the 'abuser knew something they shouldn't' signal — should prompt action.

Step 2 — Check Device Administrators (Android) / Profiles (iOS)

Android: Settings → Security → Device admin apps. Unknown admins are a red flag.

iOS: Settings → General → VPN & Device Management. Unknown profiles or MDM enrollments are a red flag. Stalkerware often installs as a configuration profile to gain elevated access.

Step 3 — Check Accessibility services (Android)

Android: Settings → Accessibility. Many stalkerware apps abuse accessibility services to read screen content and inject input.

Anything you don't recognize — especially something with a generic name like 'System Service' or 'Phone Helper' — is suspicious. Disable and uninstall.

Step 4 — Audit installed apps carefully

Android: Settings → Apps → See all apps. Sort by recent install date. Look for unfamiliar apps.

iOS: Settings → General → iPhone Storage. Same — look for unfamiliar apps you didn't install.

Step 5 — Check battery and data usage by app

Settings → Battery → App battery usage. Settings → Mobile data → App data usage. Stalkerware often shows high background activity.

An app you don't recognize with high battery/data is a strong signal.

Step 6 — Check granted permissions

Android: Settings → Privacy → Permission manager. Review which apps have location, microphone, camera, SMS, and contacts.

iOS: Settings → Privacy & Security. Review same permissions. Revoke anything that shouldn't have access.

Step 7 — Run a reputable scanner

Malwarebytes for Android (free) and TrendMicro's iOS scanner detect many known stalkerware families. They don't catch everything but they catch the common ones.

Don't rely on the built-in store's reviews — many stalkerware apps are sideloaded or installed via configuration profiles, bypassing Play Protect and App Store review.

Step 8 — Plan before removing

If stalkerware is confirmed in an abuse context: pause. Call NDVH 1-800-799-7233 to plan removal safely. Sudden disappearance of the stalkerware can alert the installer and escalate.

If it's a non-abuse context (curious teen, workplace device): factory reset is the surest cleanup. Back up first; reset; restore essentials manually rather than from cloud backup (which may carry the malware back).

PRO TIP

Don't Remove Stalkerware Without A Safety Plan.

If you're in an abusive relationship, call NDVH 1-800-799-7233 before removing.

Sudden removal can alert the installer and escalate.

Document evidence (screenshots, app names) before removing — useful for orders of protection.

Factory reset is the surest cleanup; restore essentials manually, not from full backup.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Use a secondary 'safe' device

A cheap prepaid phone used only for sensitive calls — kept hidden from the controlling party.

Trade-off: requires keeping it hidden and charged.

Power-user upgrade #2 — Run iVerify or similar on iOS

iVerify scans for jailbreak indicators, suspicious profiles, and configuration anomalies that may indicate stalkerware.

Trade-off: $5/mo subscription.

Power-user upgrade #3 — Use Signal for sensitive communication

End-to-end encrypted messaging with disappearing messages. Reduces what stalkerware can capture from the messaging app itself.

Trade-off: doesn't help if keylogger/screen-reader stalkerware is installed; combine with detection.

Power-user upgrade #4 — Subscribe to Coalition Against Stalkerware alerts

Keep up with newly identified stalkerware families and detection guidance.

Trade-off: occasional email.

Power-user upgrade #5 — Document everything carefully

Screenshots, app names, dates, and access patterns — useful evidence for orders of protection and law-enforcement reports.

Trade-off: extra step; saves cases later.

Power-user upgrade #6 — Get a domestic-violence safety plan

NDVH and local DV agencies offer formal safety planning that integrates tech, financial, legal, and physical safety.

Trade-off: takes a phone call; saves lives.

Common mistakes & pitfalls

Mistake — Mistake

Fix — Removing stalkerware abruptly without a safety plan. Can escalate abuse. Pause and call NDVH first.

Mistake — Mistake

Fix — Restoring from cloud backup after factory reset. May re-install the stalkerware. Restore essentials manually.

Mistake — Mistake

Fix — Confronting the suspected installer directly. Almost always unsafe; go through professional advocates.

Mistake — Mistake

Fix — Assuming a virus scan catches everything. It catches common families, not all.

Mistake — Mistake

Fix — Ignoring profile / MDM enrollments. These are how modern stalkerware gains elevated access.

Mistake — Mistake

Fix — Discussing the discovery on the same device or on accounts the installer can see.

Pro tips

Pro tip 1. National Domestic Violence Hotline: 1-800-799-7233. Free, confidential, 24/7.

Pro tip 2. Coalition Against Stalkerware lists known apps and detection guidance: stopstalkerware.org.

Pro tip 3. Safety Net project at NNEDV: technical-safety advocates trained specifically for this.

Pro tip 4. If you've been hit physically or threatened, that's an emergency — call 911.

Pro tip 5. Document, plan, then act. The order matters.

Frequently asked questions

How common is stalkerware really?

Common enough that major antivirus vendors track it separately. Norton, Kaspersky, ESET, and Malwarebytes all maintain dedicated stalkerware detection.

Can iPhones get stalkerware too?

Yes, primarily via configuration profiles, MDM enrollment, or in some cases jailbreaks. Less common than Android but real.

What if I share a phone with my partner?

Same checks apply. If you suspect non-consensual surveillance, please call NDVH 1-800-799-7233.

Will factory reset definitely remove stalkerware?

Yes for standard stalkerware. For very rare firmware-level implants (extremely uncommon outside high-threat-model scenarios), a new device may be necessary.

Can stalkerware be installed remotely?

Rarely — almost all stalkerware requires brief physical access to the device. The exception is when the abuser knows the device password and can install while the victim is away from the phone.

Is stalkerware legal?

Installing on someone else's device without consent is illegal in the US under federal wiretap and computer-fraud statutes.

What if I find stalkerware and don't know who installed it?

Document, then plan. Local law enforcement and DV advocates can help. Don't tip off potential installers prematurely.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

If in abuse context — call NDVH 1-800-799-7233 BEFORE doing technical checks.

Look for behavioral signs: battery drain, data spike, overheating, knowledge they shouldn't have.

Check device admins / profiles / accessibility services / installed apps / permissions.

Run a reputable scanner (Malwarebytes, TrendMicro).

Document evidence with screenshots before any removal.

Plan removal with a DV advocate if applicable; otherwise factory reset.

Restore essentials manually rather than from full cloud backup.

Change all critical account passwords from a clean device after removal.

Mini glossary

Stalkerware: Commercial surveillance software installed covertly to monitor calls, texts, location, and more.

Device admin: Android permission level that grants apps elevated control over the device.

Configuration profile: iOS mechanism for installing policies and settings; often abused by stalkerware.

MDM: Mobile Device Management — legitimate enterprise tool sometimes abused for personal surveillance.

Accessibility service: Android permission that allows apps to read screen content and inject input.

NDVH: National Domestic Violence Hotline: 1-800-799-7233, free and confidential 24/7.

Safety plan: Comprehensive plan for safely leaving an abusive situation, ideally developed with an advocate.