S

Spyware: Warning Signs, Detection, Removal, and Prevention

Learn what spyware can collect, how commercial stalkerware differs from other malware, which warning signs matter, and how to remove it safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is spyware malware?
02 Common types of spyware
03 How spyware gets installed
04 Warning signs
05 How to check a computer
06 How to check a phone safely
07 Removal and account recovery
08 How to avoid spyware
09 Spyware vs. browser hijacker

Spyware is software that secretly or deceptively collects information about a device or user and sends it to another party. It may capture browsing, credentials, messages, location, screenshots, audio, or financial data. Some unwanted applications combine surveillance with advertising or browser changes.

Related terms describe different parts of the problem: trackware emphasizes tracking behavior, while anti-spyware describes tools used to detect and remove unwanted monitoring. Neither label replaces checking what was collected and which accounts were exposed.

Monitoring software can have legitimate, disclosed administrative uses. It becomes abusive or malicious when installed without valid authorization, hidden from the user, or used to exceed an agreed purpose.

01 What is spyware malware?

Spyware is a category of malware defined by covert monitoring and data collection. It does not need to replicate like a virus. Some spyware records only one type of data, such as keystrokes, while an information stealer may collect browser passwords, cookies, documents, and cryptocurrency-wallet data in one operation.

02 Common types of spyware

- Credential and information stealers.
- Keyloggers and clipboard monitors.
- Browser extensions that collect browsing or change search behavior.
- Mobile stalkerware that tracks location, calls, or messages.
- Screen, camera, or microphone surveillance tools.
- Commercial monitoring tools abused outside lawful and disclosed use.

03 How spyware gets installed

Common paths include phishing attachments, fake updates, cracked software, malicious ads, unwanted bundles, exposed remote access, stolen cloud credentials, and physical access to an unlocked device. Mobile surveillance may also abuse accessibility, device-administrator, notification, backup, or cloud-sync permissions.

04 Warning signs

Possible signs include unusual battery or data use, overheating while idle, unexpected accessibility or administrator permissions, microphone or camera indicators, unfamiliar extensions, changed search settings, new login alerts, or security tools being disabled. Many have benign causes, and sophisticated spyware may show none.

05 How to check a computer

1. Review installed applications, browser extensions, startup items, services, and scheduled tasks.
2. Check active sessions and connected applications for major accounts.
3. Install operating-system and application updates.
4. Run reputable, updated security scans.
5. Review unusual processes and outbound connections with qualified help when needed.

A clean scan is useful but cannot prove the absence of every surveillance method.

06 How to check a phone safely

Review device-management profiles, accessibility services, device administrators, VPNs, certificates, app permissions, battery use, and account sessions. Update the operating system. If intimate-partner surveillance is possible, changes may alert the person monitoring the device. Use a safer device to seek specialized support and plan before removing software.

07 Removal and account recovery

Disconnect or isolate the device when appropriate, preserve evidence, and remove malicious apps and persistence using trusted tools. Change important passwords from a known-clean device, enable phishing-resistant MFA, revoke sessions, and correct recovery details. Rebuild or factory-reset when privileged compromise cannot be ruled out, then restore only necessary, verified data.

08 How to avoid spyware

- Install software only from official sources and avoid cracks.
- Keep devices, browsers, and applications updated.
- Use screen locks, unique passwords, and MFA.
- Restrict physical access and review account alerts.
- Remove unused extensions and excessive app permissions.
- Do not grant remote control to unsolicited “support.”

09 Spyware vs. browser hijacker

A browser hijacker primarily changes search, homepage, or traffic behavior, while spyware focuses on collection. One program can do both. Investigate the whole device and account activity instead of fixing only the visible browser setting.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com