K

Keylogger: How to Detect, Remove, and Recover Safely

A keylogger records what you type and may steal passwords or private data. Learn the differences between software and hardware keyloggers, warning signs, safe removal, and account recovery.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 What is a keylogger?
02 Software vs. hardware keyloggers
03 How keyloggers get installed
04 Possible signs of a keylogger
05 How to check for a keylogger safely
06 How to remove a keylogger
07 Secure accounts after removal
08 If monitoring may involve stalking or abuse
09 How to reduce keylogger risk
10 Frequently asked questions
11 References

01 What is a keylogger?

A keylogger, or keystroke logger, is software or hardware that records what a person types. A malicious keylogger can capture passwords, payment details, private messages, search terms, and other sensitive text before a website or app encrypts it. Some tools also collect clipboard contents, screenshots, form data, or active window names.

Keylogging technology is not automatically malware. It can be used for authorized testing, troubleshooting, accessibility, or disclosed monitoring on an organization-owned device. It becomes malicious or abusive when it is installed or used without informed authorization to collect another person's data.

02 Software vs. hardware keyloggers

Type	Where it operates	How it may be found
User-space software	An app, process, browser extension, or keyboard hook	Security alerts, unexpected startup items, input-access permissions, or outbound traffic
Kernel or driver level	Deep in the operating system input stack	Unexpected drivers, integrity checks, offline scanning, or forensic analysis
Web form or script capture	A compromised page or injected browser script	Website security review, browser tools, content-security alerts, or multiple affected visitors
Mobile monitoring app	An app with accessibility, keyboard, device-admin, screen, or notification access	Permission review, unfamiliar profiles or apps, battery/network anomalies, or mobile security tools
Hardware keylogger	Between a keyboard and computer, inside a keyboard, or in another physical adapter	Physical inspection of cables, ports, adapters, and the device enclosure

A software scan cannot reliably rule out a physical device. Conversely, an unfamiliar process name is not proof of keylogging; verify its file path, publisher, installation source, permissions, behavior, and role before removing it.

03 How keyloggers get installed

- A phishing attachment, malicious link, fake update, cracked program, or trojanized installer.
- A remote access trojan or information stealer that includes input capture as one feature.
- A malicious or compromised browser extension.
- Abuse of accessibility, device administration, keyboard, or screen-capture permissions on a phone.
- An attacker, insider, or abusive partner with physical or administrative access.
- A compromised website that captures form fields before submission.

Because keylogging is often one component of a larger intrusion, finding the logger is not enough. The same device may also contain persistence, remote-control tooling, session theft, or other credential-stealing malware.

04 Possible signs of a keylogger

- A security product reports input capture, spyware, an unknown driver, or suspicious persistence.
- An unfamiliar app has accessibility, keyboard, screen-recording, device-admin, or full-disk permissions.
- A previously unknown process starts with the system and sends small, regular uploads to an unusual destination.
- Browser extensions, login items, scheduled tasks, services, or device-management profiles appear without approval.
- A physical adapter or cable is present between the keyboard and computer.
- Accounts show logins or actions that suggest typed credentials were exposed.

Typing delay, crashes, high CPU use, or poor battery life are weak signals by themselves. A well-designed keylogger may cause no visible symptoms, while ordinary software problems can cause all of them.

05 How to check for a keylogger safely

1. **Decide whether evidence matters.** On a work device, notify the security team before deleting files or powering down. They may need memory, logs, and a timeline.
2. **Use a different trusted device for sensitive communication.** Do not type new passwords or investigation notes on the suspected system.
3. **Inspect the hardware.** Check the keyboard cable, USB path, adapters, dock, and accessible ports. Compare shared or high-risk workstations with an approved baseline.
4. **Review software and permissions.** Look for unfamiliar installed apps, browser extensions, startup items, services, drivers, keyboard apps, accessibility access, device-admin rights, and management profiles.
5. **Run updated security scans.** Use a trusted antivirus or endpoint tool. If available, run a full or offline scan so deeply embedded software has less opportunity to hide.
6. **Check the surrounding activity.** Review process trees, installation events, persistence, DNS and network connections, and account sign-ins. Scope other devices that received the same file or software.

Do not download random "keylogger detector" utilities from advertisements or unfamiliar websites. A fake removal tool can create a second compromise.

06 How to remove a keylogger

1. **Disconnect or isolate the device** from networks if malicious collection or exfiltration is likely. In an organization, use the approved isolation process.
2. **Quarantine confirmed malicious software** with a trusted security tool. Remove associated persistence, extensions, profiles, and payloads, not only the visible executable.

3. **Remove unauthorized hardware** and preserve it for investigation if the incident involves a workplace, stalking, fraud, or legal action.
4. **Patch the entry point** and remove the account or administrative access that allowed installation.
5. **Rebuild or factory-reset when trust cannot be restored.** Use known-good installation media and restore only verified data. A reset is a last resort for an unconfirmed suspicion, but it may be the safest recovery for a deeply compromised system.
6. **Scan other affected devices** and verify that suspicious network traffic and persistence do not return.

07 Secure accounts after removal

Change credentials from a known-clean device, not the suspected one. Start with the primary email account and password manager because they can reset other accounts. Then address banking, work, cloud, social, and shopping accounts.

- Use a unique password for every account and enable phishing-resistant MFA where available.
- Sign out other sessions, revoke app passwords and access tokens, and remove unknown recovery methods.
- Review recent logins, inbox rules, forwarding, transactions, sent messages, and security settings.
- Assume any secret typed while the keylogger was present may have been exposed, including recovery codes and encryption passphrases.
- Contact financial providers, an employer, or affected services promptly if misuse occurred.

08 If monitoring may involve stalking or abuse

Removing monitoring software can alert the person who installed it. If that could put you at risk, use a separate safe device to contact a trusted support organization or local specialist before changing the suspected device. Preserve evidence only when it is safe to do so.

09 How to reduce keylogger risk

- Install software and browser extensions only from trusted sources; avoid cracks and fake updates.
- Keep the operating system, browser, apps, and security software updated.
- Limit administrator rights and control who can load drivers or change accessibility settings.
- Use a password manager to reduce typing, while remembering that advanced malware can steal data in other ways.
- Use MFA so a captured password alone is less useful, and protect session tokens as well.
- Restrict and monitor outbound traffic on business devices and physically secure shared workstations.

10 Frequently asked questions

Can antivirus detect every keylogger?

No. Security tools detect many software keyloggers, especially by behavior, but no single clean scan proves a device is safe. Hardware devices require physical inspection, and a compromised web page must be fixed at the website.

Can a keylogger record an on-screen keyboard?

A basic keystroke logger may miss mouse clicks, but advanced spyware can capture screenshots, clipboard data, form fields, or pointer activity. An on-screen keyboard is not a dependable standalone defense.

Is changing my password enough?

No. If the logger remains, it can record the new password. Clean or rebuild the device first, then change credentials and revoke sessions from a trusted device.

11 References

- Microsoft Security: keylogger detection and response
- MITRE ATT&CK: Input Capture - Keylogging (T1056.001)

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