T

Trackware: Meaning, Warning Signs, and Safe Removal

Trackware is a security term for software that collects information about user activity, often without meaningful knowledge or authorization. It may monitor browsing or application use and send data to another party. The label is used differently by vendors; investigate the actual application, permissions, behavior, and conse...

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is trackware?

02 Trackware, spyware, cookies, and monitoring tools

03 Which signs warrant investigation?

04 How to remove unauthorized tracking software

05 When removal needs a different approach

06 Preventing unwanted tracking

Quick answer: Trackware is a security term for software that collects information about user activity, often without meaningful knowledge or authorization. It may monitor browsing or application use and send data to another party. The label is used differently by vendors; investigate the actual application, permissions, behavior, and consent before deciding how to remove it.

01 What is trackware?

Older security classifications use trackware for programs that collect browsing information and may also show advertisements or change browser settings. F-Secure, for example, documents the relationship between its older Data Miner label and Trackware. The term does not identify one malware family, and unrelated legitimate products may use similar names.

A name alone therefore cannot establish whether a file is harmful. Record the full detection name, file location, publisher, and security application's explanation. Avoid deleting arbitrary files or registry entries based on a glossary term.

02 Trackware, spyware, cookies, and monitoring tools

- **Trackware:** usually emphasizes collection of user activity, with vendor-specific classification.
- **Spyware:** a broader category of covert information collection that can include credentials, messages, or other sensitive data.
- **Tracking cookies:** browser-stored data used for recognition across visits or sites; a cookie is not itself an installed executable.
- **Authorized monitoring:** workplace, parental-control, or device-management software used under an appropriate policy and authorization.
- **Stalkerware:** covert monitoring associated with surveillance of another person, requiring attention to personal safety as well as device security.

03 Which signs warrant investigation?

Unexpected extensions, unfamiliar startup applications, unexplained browser changes, or excessive permissions can justify a closer look. However, targeted advertisements do not by themselves prove that spyware is installed. Ads may reflect account activity, cookies, or information collected elsewhere. Battery drain and network usage are also nonspecific.

Check what changed and when. Compare the suspicious application's installation date with recent downloads, then inspect its requested access. Permissions to read all website content, manage the device, or use accessibility features deserve a clear explanation. On managed equipment, ask the administrator to identify the software and its purpose.

04 How to remove unauthorized tracking software

1. Record the application or extension name, detection details, permissions, and relevant symptoms.
2. On a personal device you control, remove an unwanted extension or uninstall the identified application through normal system tools.
3. Update the operating system and security software, then scan for related components and persistence.
4. Review browser settings and synchronization so an unwanted extension is not automatically restored.
5. If sensitive account information may have been exposed, use a trusted device to change credentials, review recovery methods, and revoke unfamiliar sessions.
6. Check whether the behavior returns before considering the incident resolved.

Resetting a browser removes some local settings but does not necessarily uninstall system software or revoke account access. Similarly, clearing cookies does not erase information already sent to another party.

05 When removal needs a different approach

If you suspect monitoring by an abusive partner or another person with physical access, removal can alert that person or change their behavior. Use a safer device to seek trusted support and plan your next steps. Preserve evidence when it is safe to do so. For organizational equipment, follow the incident process rather than disabling management agents yourself.

06 Preventing unwanted tracking

Install applications from a verified source, review optional offers, and keep extensions to those you need. Revisit permissions when an application changes ownership or asks for broader access. Protect the device's unlock method and associated cloud account. Private browsing limits some local history, but it does not make installed monitoring software unable to observe activity.

When a detection appears incorrect, update the scanner and request review through the security vendor's official channel. Keep the file quarantined while its purpose is uncertain; do not create a broad exclusion simply to silence the warning.

Reference: F-Secure's Data Miner and Trackware classification. Related: spyware and security software.

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