

# Trackware - what it is, warning signs, and how to remove or avoid it

Gridinsoft Help Center

## What it is

Trackware is software that watches what you do on a device and sends that info to someone else. It can log the apps you use, sites you visit, searches you make, and basic system details. Some versions come bundled with "free" tools or browser add-ons; others get installed without clear consent.

## Why it matters

Collected data can be used to profile you, target ads, or sold to brokers. In worse cases, it can expose sensitive habits and make phishing or scams more convincing.

## How it works

- Collect: monitors browsing, app usage, searches, and device info.
- Store: keeps logs locally or in hidden folders.
- Send: uploads data on a schedule to a company server or third party.
- Persist: adds startup entries or extensions so it runs every boot.

## Red flags

- New browser extensions you didn't add, extra toolbars, or changed search/homepage.
- Pop-ups and ads following you across many sites.
- High background network usage from unknown processes.
- An installer that insists on "optional" offers pre-checked.

## Do it right

- Install software from official sites or app stores only; uncheck extra "offers."
- Review browser extensions and remove anything you don't recognize.
- Run a reputable security scan and reset browser settings if needed.
- Use a privacy-focused browser mode and block third-party cookies/tracking.
- Keep the OS and apps updated to close holes used by shady add-ons.