R

Rogueware: Fake Security Software, Scareware, and Safe Removal

Rogueware uses false or exaggerated warnings to sell ineffective software or gain access. Follow the right recovery path for popups, installed apps, and payment scams.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

Rogueware is deceptive software that pretends to provide a useful security or maintenance service while using false findings, pressure, or obstruction to obtain money or access. Fake antivirus programs are the best-known example, but the category also includes fraudulent system cleaners, registry repair tools, driver updaters, and “technical support” apps.

A frightening browser page is not automatically an installed infection. Your response should depend on whether you only saw a popup, downloaded an app, entered payment details, or gave someone remote access.

How rogueware works

Rogueware commonly reports a predetermined list of errors or threats, regardless of the device's real condition. It then demands payment, a subscription, a phone call, or installation of another tool. Some programs make themselves difficult to remove, display persistent notifications, change browser settings, or interfere with legitimate security software.

Common delivery methods include malicious ads, fake virus alerts, bundled installers, search ads that impersonate trusted brands, and unsolicited support calls. Microsoft defines rogue security software as software that appears beneficial from a security perspective but provides limited or no security and uses misleading or fraudulent behavior.

Warning signs of fake security software

- a web page claims it scanned your entire computer without permission;
- a timer, siren, full-screen warning, or repeated popup pressures you to act immediately;
- the warning tells you to call a phone number or allow remote access;
- the product finds many problems immediately but will fix them only after payment;
- the company, publisher, price, renewal terms, or uninstall method is unclear;
- legitimate antivirus tools are disabled or the rogue program returns after removal.

Not every low-quality cleaner is malware. A legitimate but unnecessary utility may still be detected as a PUA. Stronger indicators of rogueware are fabricated results, impersonation, coercive payment, blocked removal, or unauthorized access.

If you only saw a scary browser popup

1. Do not call the number, click the scan button, download a file, or enter credentials.
2. Close the tab. If it traps the browser, use the operating system's task manager or force-quit function, then reopen without restoring the suspicious page.
3. Remove the site's notification permission and clear its stored site data. Check for unfamiliar extensions.

4. Run an updated scan if anything downloaded or the browser continues to redirect.

A web page cannot know that “five viruses” exist simply by loading. Browser notifications may make the same alert reappear even when no rogue program is installed.

If you installed the program

1. **Disconnect if remote access or credential theft is possible.** Otherwise, first record the app name, publisher, download source, charges, and detection details.
2. **Uninstall through normal system settings.** Also remove companion applications installed on the same date and unknown browser extensions.
3. **Run a full scan with updated reputable security software.** If the rogueware blocks it, use Safe Mode or a trusted recovery environment.
4. **Restore changed settings.** Re-enable security controls, check proxy and DNS settings, browser search and startup pages, scheduled tasks, and startup items.
5. **Review subscriptions.** Cancel recurring billing through the vendor only if the contact is verifiably legitimate; also tell the card issuer about deceptive charges.

If you paid or allowed remote access

Contact the bank or card issuer using the number on the card or official website, dispute unauthorized or deceptive charges, and replace the card when advised. From a clean device, change passwords, revoke active sessions, and enable strong MFA. Start with email and financial accounts.

If a caller controlled the computer, uninstall the remote-support tool, check for unattended-access settings and newly created accounts, and scan the system. A clean reinstall is the safest option if the operator had administrator access or installed unknown software. Preserve receipts, phone numbers, chat logs, and transaction details for the bank and local fraud-reporting service.

Avoid recovery scams

Scammers may contact victims again and promise a guaranteed refund or data recovery for an upfront fee. Banks, law enforcement, and legitimate security vendors do not need gift cards, cryptocurrency, or remote access to “secure” your money.

Rogueware FAQ

Is scareware the same as rogueware?

Scareware describes the fear tactic. Rogueware is the deceptive program or service being promoted; the terms often overlap.

Does closing the popup remove an infection?

If nothing downloaded and no permissions were granted, closing it may be enough. Persistent redirects, extensions, downloads, or system alerts require further checks.

Should I trust a company that calls after a warning?

No. Independently find the provider's official contact information. Never rely on a number shown in an unexpected popup.

For additional background, see F-Secure's rogueware description and the U.S. FTC's tech-support scam guidance.

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