S

Scareware: Fake Virus Alerts, Safe Removal, and Scam Recovery

Scareware uses alarming security claims to pressure people into calling, paying, installing software, or granting remote access. A web alert alone does not prove infection.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

Scareware uses alarming security or system claims to pressure someone into taking an unsafe action. It may imitate an operating-system warning, antivirus scan, browser error, or trusted company and demand a call, payment, download, notification permission, or remote-access session.

A frightening page is not proof that the device is infected. A website normally cannot perform the detailed local scan it claims to show. However, risk changes if software was installed, a file opened, credentials or payment data entered, or remote control granted.

Browser alert, notification, or installed rogueware?

- **Deceptive web page:** a tab displays a fake scan, sound, countdown, fullscreen prompt, or support number. Closing the page may end it.

- **Abusive site notification:** alerts continue outside the tab because a website was allowed to send browser or system notifications.
- **Rogue security application:** installed software reports fabricated or exaggerated problems, demands payment, changes settings, or resists removal.
- **Tech-support scam:** the alert directs the victim to a caller who requests remote access, payment, banking activity, or secrecy.

Warning signs

- a web page claims to know an exact number of infections immediately;
- the alert says to call a phone number or forbids closing the window;
- branding, URL, product name, or security-provider identity does not match the installed protection;
- payment, gift cards, cryptocurrency, remote access, or banking login is presented as the only solution;
- the caller asks to move money, hide the purpose from the bank, or share a verification code;
- notifications name a website as their sender rather than the operating system or security product.

If you only saw the page

1. Do not click its buttons, call the number, download the cleaner, or enter information.
2. Close the tab. If it traps the browser, use the operating system's app switcher or task manager to close the browser.
3. When reopening, do not restore the malicious tab. Update the browser and clear that site's permissions and data if necessary.
4. Review notification permissions and remove the site if alerts appeared outside the page.

5. Use the installed, trusted security application to scan if a download began, the page exploited a browser warning, or symptoms continue.

Microsoft's current scareware guidance describes deceptive pages that claim infection and push victims to call fake support or grant remote access.

If software or an extension was installed

1. Disconnect from the network when credential theft, remote access, or active malware is possible.
2. Record the alert URL, download, filename, installation time, application, extension, notification sender, and payment or phone details.
3. Uninstall the unwanted component through normal system or browser controls and remove related notification permissions, startup entries, and policies.
4. Run an updated full scan, restart, and scan again. If detections return or security controls were changed, seek qualified help or rebuild from trusted media.

If you called, paid, or granted remote access

- end the call and remote session and disconnect the affected device;
- contact the bank or payment provider through an independently verified number and report the transaction immediately;
- from a clean device, change credentials entered or stored during the session, revoke active sessions, and review MFA and recovery settings;
- remove remote-control software and check for new users, startup items, scheduled tasks, security exclusions, and browser changes;
- preserve invoices, chats, numbers, wallet addresses, remote-session IDs, and screenshots for the platform and authorities.

Prevention

- keep the operating system, browser, and security software updated;
- allow notifications only for sites that genuinely need them and review permissions periodically;
- download software from its verified publisher or trusted store;
- use browser protection and block potentially unwanted applications;
- teach family and staff that legitimate security alerts do not require gift cards, secrecy, or unsolicited remote access.

Scareware FAQ

Am I infected because a page showed my IP address?

No. Websites normally see the public IP used for the connection. Displaying it is a pressure tactic, not evidence of a scan.

Should I reset the browser?

Remove the specific site permission or extension first. Resetting may help persistent changes but does not remove an installed application or secure exposed accounts.

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