F

Fake Antivirus (FakeAV): Warning Signs, Removal, and Recovery

Fake antivirus warnings use fear to sell useless software, obtain remote access, or steal payment details. Learn how to distinguish a web pop-up from installed FakeAV and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Three situations that look like fake antivirus
02 Fake antivirus warning signs
03 If it is only a browser pop-up
04 How to remove an installed FakeAV program
05 If you paid or granted remote access
06 How to avoid FakeAV
07 Frequently asked questions
08 Authoritative guidance

Fake antivirus, also called FakeAV or rogue security software, imitates a legitimate security product and claims to find urgent infections that may not exist. Its goal may be to sell useless software, collect payment details, persuade the victim to call a scammer, obtain remote access, or install additional malware.

A frightening alert in a browser is not proof that an antivirus scan found malware. Websites cannot normally perform a complete scan of local files merely because a page is open. Close the page without calling its number or downloading its recommended tool, then verify the device through security software opened directly from the operating system.

01 Three situations that look like fake antivirus

Situation	How to recognize it	Immediate action
Browser scare page	Full-screen warning, countdown, siren, phone number, or page that resists closing	Do not interact; close the tab or browser and revoke its notification permission
Installed rogue security app	Unknown program runs at startup, reports predetermined infections, and demands payment	Disconnect if needed and scan from a trusted security environment
Tech-support scam	A caller or pop-up requests remote access, gift cards, crypto, bank transfer, or account movement	End contact, remove remote-access tools, and contact financial providers
Legitimate security alert	Appears in the installed product's own interface and can be verified from system settings	Open the product independently and review its detection path and action

02 Fake antivirus warning signs

- The message claims to know your device has many viruses before any trusted scan runs.

- It uses a countdown, alarm sound, flashing colors, or threats of data loss and account blocking.
- A browser warning tells you to call a phone number. The FTC notes that real security pop-ups do not ask you to call support this way.
- Payment is demanded by gift card, wire transfer, cryptocurrency, payment app, or cash withdrawal.
- The operator wants remote control or asks you to read one-time codes and banking information.
- An unfamiliar app prevents trusted security tools from opening or repeatedly returns after removal.
- The supposed scan lists impossible paths, generic names, or the same result on every device.

03 If it is only a browser pop-up

1. Do not click Allow, Scan, Clean, Back, or the page's close button if it looks suspicious.
2. Use the browser or operating system controls to close the tab. If necessary, force-quit the browser.
3. Reopen the browser without restoring the suspicious session.
4. Remove notification permission for the site and review recently added extensions.
5. Clear site data for the offending domain and update the browser.
6. Open your installed security product from system settings, update it, and run a scan.

If nothing was downloaded, executed, installed, paid, or disclosed, the event may end with browser cleanup. If you followed commands, allowed remote access, or entered credentials, continue with the compromise steps below.

04 How to remove an installed FakeAV program

1. **Disconnect the device** if the program communicates with a scammer, blocks security controls, or additional malware is suspected.
2. **Record evidence.** Save the program name, paths, screenshots, phone number, website, receipts, and remote-access session details.
3. **Use a trusted scanner.** Update the built-in or established security product and run a full scan. Use an offline scan or trusted recovery environment if the rogue app interferes.
4. **Remove related software.** Uninstall unknown security, optimizer, browser, and remote-access applications; inspect startup items and extensions.
5. **Verify after restart.** Confirm that warnings, processes, proxy changes, exclusions, and persistence do not return.
6. **Rebuild if trust is lost.** Reinstall from known-good media when remote control occurred, administrator commands were run, or a backdoor or stealer was present.

05 If you paid or granted remote access

- Contact the bank, card issuer, payment app, or transfer provider immediately and ask about blocking or reversing the transaction.
- From a clean device, change exposed passwords, revoke sessions, and enable multifactor authentication. Start with email and financial accounts.
- Tell the financial institution if the scammer viewed accounts or persuaded you to move money to a supposedly safe account.
- Remove remote-support software and check for unattended-access settings and newly created users.
- Monitor statements and credit reports as appropriate, and report the scam to the relevant national fraud authority.

Do not pay a recovery service that contacts you unexpectedly. Victims are often targeted again by people falsely promising to recover lost funds.

06 How to avoid FakeAV

- Install security software from the operating system, app store, or vendor's typed official address, not a search advertisement.
- Keep the operating system, browser, and security tools updated.
- Block unwanted browser notifications and remove extensions you do not need.
- Never give remote access to an unsolicited caller or pop-up operator.
- Back up important data using a method that malware cannot silently overwrite.

07 Frequently asked questions

Can a website really scan my computer for viruses?

A normal web page has restricted access and cannot perform the comprehensive local scan claimed by scare pages. A trusted web scanner may inspect a file you explicitly upload, which is different.

Is FakeAV the same as scareware?

FakeAV is a form of scareware focused on security claims. Scareware is broader and includes other false urgent warnings designed to force a purchase or action.

Should I call the number in a virus pop-up?

No. Close the page and contact a trusted provider through contact information you independently obtain from its official site.

08 Authoritative guidance

- FTC: How to spot, avoid, and report tech support scams

- FTC: Protect against, detect, and remove malware
- Bitdefender: Remove a fake antivirus infection

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