

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

8 ways to tell a virus warning popup is fake

<https://cyberguardlab.com/blog/8-ways-to-tell-a-virus-warning-popup-is-fake>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



A full-screen "virus" page that tells you to call a number is almost never Windows Security. A common household variant changes the scare every time you reboot: new wording, new phone number, same lock on the browser. That is a tech-support scam, not a lab detection. The Federal Trade Commission describes the pattern: pop-ups that impersonate a well-known company, demand a call, then ask for remote access or payment. Close the page. Do not call. Do not pay with gift cards. Microsoft Defender and Windows Security are where a real threat notice lives. Buying a paid suite is not the way to kill the popup. Buying nothing after you close it is valid.

FEDERAL TRADE COMMISSION
CONSUMER ADVICEShopping
and
Donating ▾Credit,
Loans, and
Debt ▾Jobs and
Making
Money ▾Unwanted Calls,
Emails, and Texts ▾Identity Theft and
Online Security ▾

Scams

[Home](#) / [Articles](#)[Vea esta página en español](#)

Article

How To Spot, Avoid, and Report Tech Support Scams



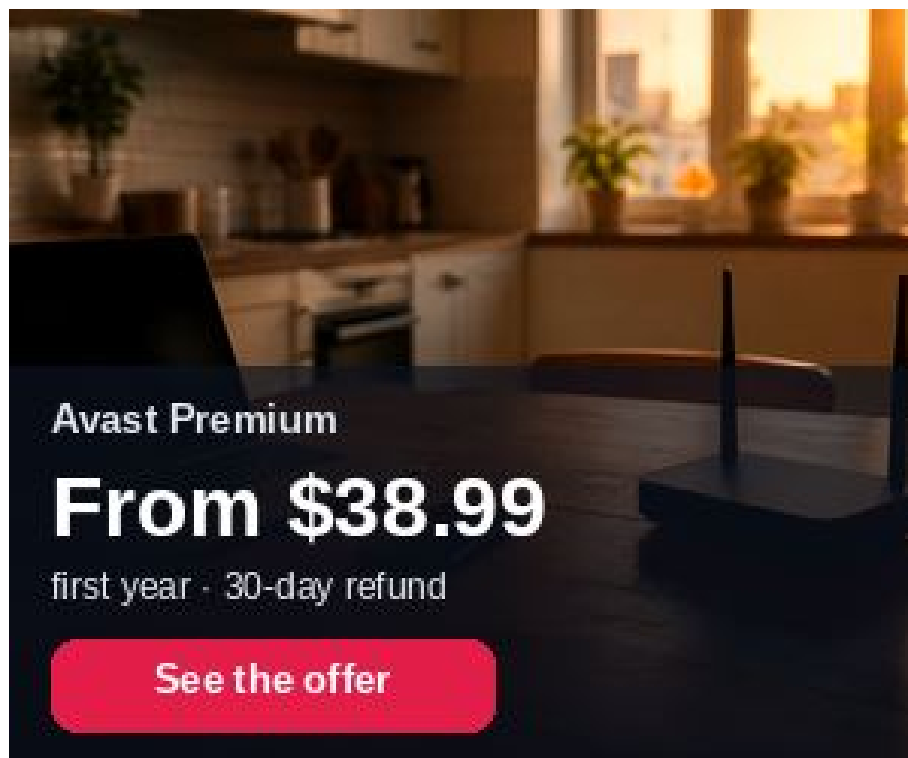
Tech support scammers try to scare you into believing there's a problem with your computer. They tell lies to get your financial information or remote access to your computer. Their goal is to steal your money, or worse, steal your identity.

[How a Tech Support Scam Works](#)[Other Types of Tech Support Scams](#)[How To Avoid a Tech Support Scam](#)[What To Do if You Were Scammed](#)[Report Tech Support Scams](#)

1. It fills the screen and tells you to call a number

Real Windows alerts do not take over Chrome or Edge with a siren and a phone number. The FTC's consumer page, How to spot, avoid, and report tech support scams, is the official US write-up. Microsoft's own note is Protect yourself from tech support scams. If the page says "call this number now," treat it as a scam even if it uses a Microsoft-like logo.

Paid link**Avast Premium | See the Avast first-year offer**



[See the Avast first-year offer](https://cyberguardlab.com/avast)

Offer page: <https://cyberguardlab.com/avast> Hop: <https://trysecurities.com/offer/avast?dtm=gg&cid=>

2. It locks the browser so Back does nothing

Scareware often traps the tab with repeated dialogs. That is a web page, not a kernel-level virus. Another tell: the scare changes every boot because the page is just a new tab or a hijacked shortcut, not a single infection that a second antivirus will "unlock."

3. A countdown is counting to nothing

A ticking clock that says your files will be deleted in 4:59 is theater. We do not use countdowns on this site, and Microsoft does not either. Ignore the timer. Do not type a card number to "stop" it.

4. Grammar and logos do not match Microsoft

Broken English, mixed fonts, and a shield that is almost-but-not the Windows Security icon are cheap tells. Official pages live on microsoft.com or support.microsoft.com. A random page with a blue window is not that.

5. The address bar is not a Microsoft page

Look at the URL before you read the red text. If it is not a Microsoft domain, it is not a Microsoft warning. Press Alt+Tab if the page hid the address bar. Full-screen (F11) can be exited with F11 or Esc.

6. It asks for gift cards or remote-access software

No real vendor asks you to pay a virus fine with gift cards. No real Microsoft agent will tell you to install AnyDesk, TeamViewer, or "support" software from a popup. Hang up if you already called. Report the attempt at reportfraud.ftc.gov. If money or an account may already be gone, use [IdentityTheft.gov](https://identitytheft.gov) as well.

7. Task Manager can close it

Press Ctrl+Shift+Esc. End the browser task. If the scare returns when you reopen the browser, it is a pinned tab, a homepage hijack, or a desktop shortcut - not proof you must buy a suite. Clear the hijack as in step 7 of our 9-step cleanup.

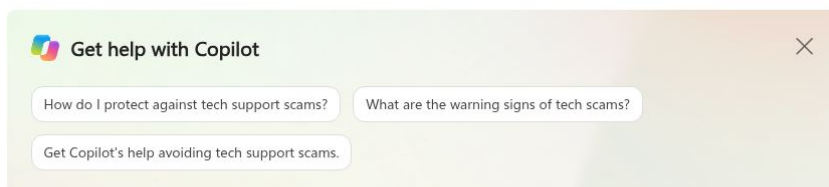
Then run a scan in Windows Security. If detections return, use Defender Offline from that same guide.

8. A real warning lives in Windows Security

Open Windows Security from the Start menu - not from a link in the scare page. Virus & threat protection shows official detections. A clean Protection history plus a browser trap is a scam page, not a failed paid product. After the popup is dead, lock the router: unique admin password, WPA2/WPA3, no WPS. That work is in how to check if your home Wi-Fi is safe and the home privacy checklist. A Wi-Fi inspector is an optional extra after those steps, not the way you close a fake alert.



Protect yourself from tech support scams

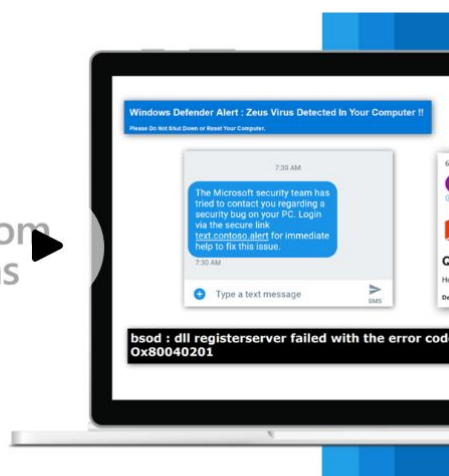


Tech support scams are an industry-wide issue where scammers use scare tactics to trick you into unnecessary technical support services to supposedly fix device or software problems that don't exist.

At best, the scammers are trying to get you to pay them to "fix" a nonexistent problem with your device or software. At worst, they're trying to steal your personal or financial information; and if you allow them to remote into your computer to perform this "fix," they will often install malware, ransomware, or other unwanted programs that can steal your information or damage your data or device.

Microsoft 365

Protect yourself from
tech support scams



How tech support scams work

Stay on Microsoft Defender if the scan is clean. A paid Wi-Fi inspector is optional after you kill the popup and lock the router - not as the fix for the scare itself.

If the scare arrived as email instead of a popup, see how to spot a phishing email.

Sources

- * FTC: How to spot, avoid, and report tech support scams
- * Microsoft Support: Protect yourself from tech support scams
- * FTC ReportFraud
- * IdentityTheft.gov
- * FTCvideos: How scammers pretend to fix your computer

Also read

- * How to check if your home Wi-Fi is safe before you pay for antivirus
- * Home privacy checklist for US families in 2026
- * 9 steps to clean a virus-infected Windows PC at home