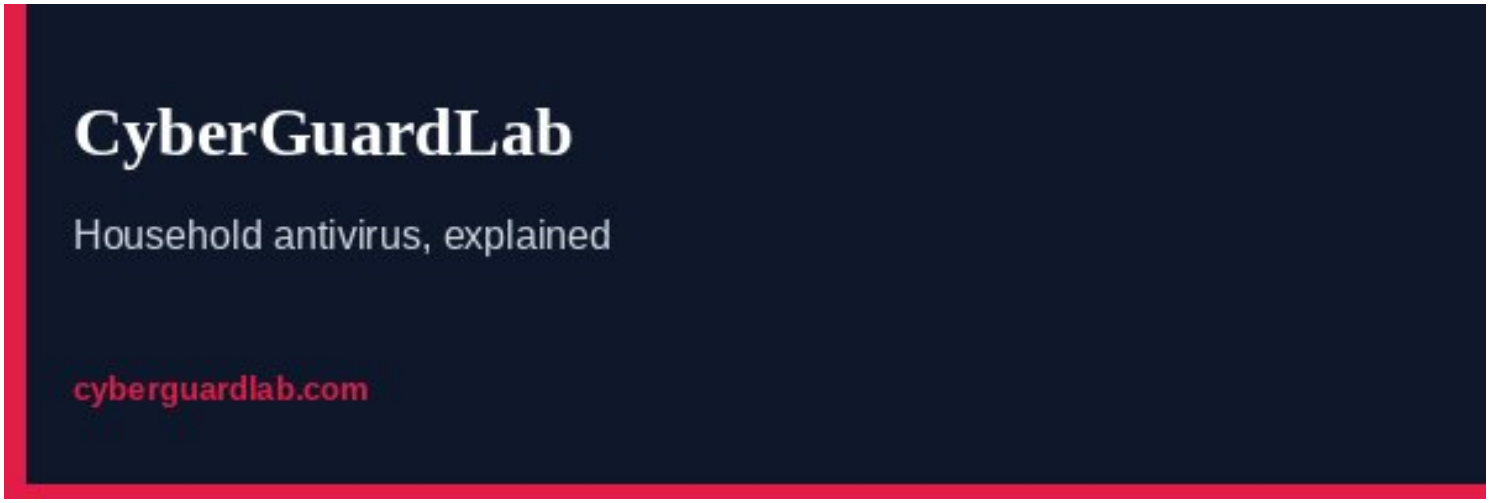
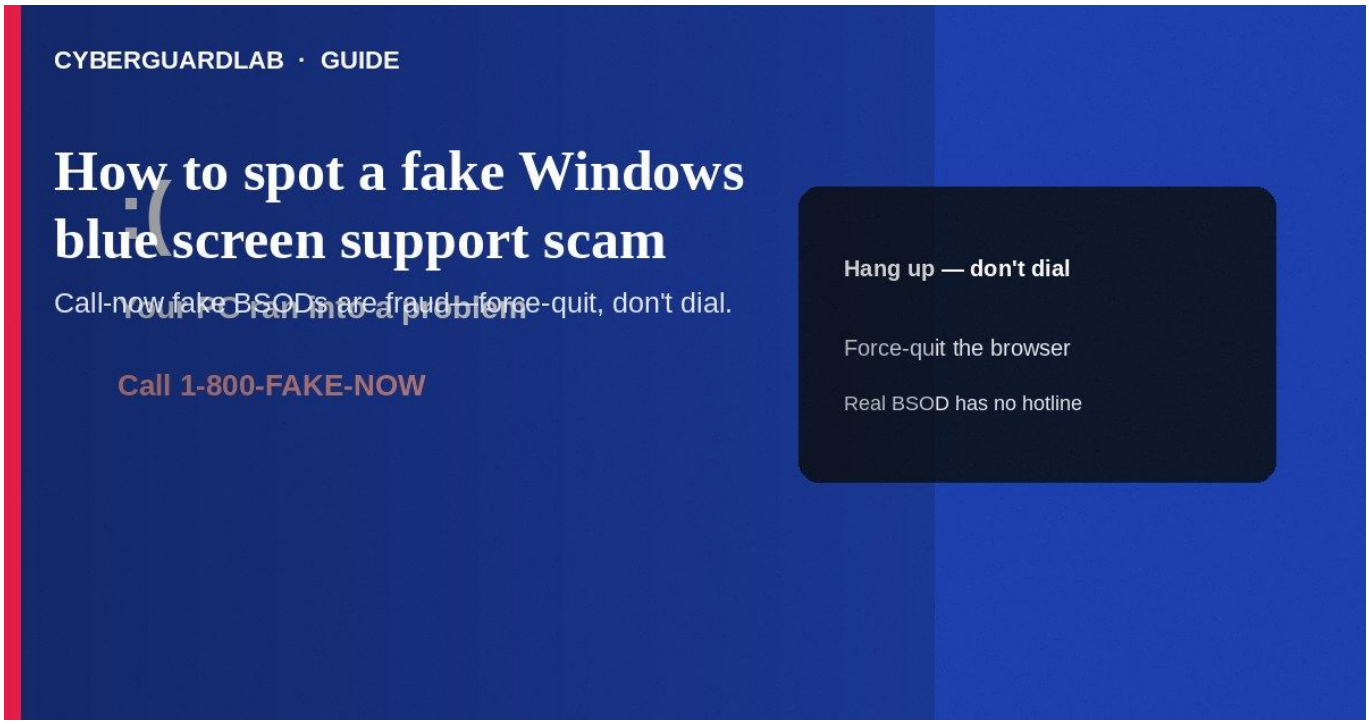


How to spot a fake Windows blue screen support scam

https://cyberguardlab.com/blog/fake-windows-bsod-support-scam

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 fake Windows blue screen (BSOD) support scam is a full-screen browser or malware scare that mimics a crash or "Microsoft Security" lockdown, then shows a phone number to call so impostors can sell "cleanup," demand remote access, or steal payment details. Do not call the number on the screen. Force-quit the browser or power off, then scan and recover using tools you open yourself. This guide is about fake BSOD / tech-support scare pages-not a real Windows 11 keep-files reset, not browser hijacker cleanup alone, and not Windows Sandbox testing.

1. How this scam works

A page freezes the browser with a blue background, error codes, siren audio, and text like "Your PC is locked-call Microsoft Windows Support now." Callers claim viruses, refunds, or license issues, then push Quick Assist, AnyDesk, or gift-card "verification." Real Windows stop errors do not display a customer-service phone number to dial immediately, and Microsoft does not cold-call after a random web page.

Scammers may show an oversized fake refund, then ask you to return the "extra" via gift cards. Banks reverse errors through official channels-not gift cards. Teach relatives: hang up, power off if needed, and never grant remote control from a blue scare page.

2. Red flags before you call

Cue | Likely legitimate | Likely scam

Where the "BSOD" appears | Full system stop; mouse often unusable; no browser chrome | Inside a browser tab/window you can sometimes Task Manager away

Phone number on screen | Microsoft stop screens do not instruct you to call a support line | Large "Call 1-800-..." banner with urgency and audio

Who started contact | You opened support.microsoft.com yourself | Inbound call or page-demanded outbound call

Payment | No gift cards or crypto for "Microsoft cleanup" | Gift cards, wire, or prepaid cards for "license" or "refund"

Remote tools | Rare and only in sessions you arranged | Immediate AnyDesk/Quick Assist to "unlock Windows"

3. What to do if you see the fake screen

* Do not call the number. Do not install remote-access software for the caller.
* Try Alt+F4, Task Manager (Ctrl+Shift+Esc) -> End browser tasks, or hard power-off if the UI is trapped.
* Restart Windows. If you need repair, use official Recovery / Reset this PC keeping files-not a stranger's script.
* Change passwords for email and banking from a different clean device if you typed anything on the scare page.
* Report at ReportFraud.ftc.gov.

4. If you already called or shared the screen

* Disconnect remote sessions; uninstall AnyDesk/TeamViewer/Quick Assist if they were added for the scammer.

* Call your bank/card issuer using the number on the card; freeze cards if payment data was shared.
* Change Microsoft account, email, and other passwords; revoke app passwords and review recent sign-ins.
* Run Microsoft Defender full scan; consider a trusted primary suite such as Norton or Bitdefender. Avoid stacking full AV products. TotalAV, McAfee, and Avast are other on-site comparison options.
* If browser home/search changed, continue with browser hijacker removal.

FAQ

Can a real BSOD show a phone number?

Standard Microsoft bugcheck screens explain restart/diagnostics-they are not telemarketing pages. Treat call-now numbers as fraud.

How is this different from resetting Windows?

A keep-files reset is a Settings/WinRE action you start. Scammers invent a fake lock so you phone them.

The page showed my IP or Windows edition. Is it real?

Not proof. Sites and scripts can display generic or previously leaked details.

Is Microsoft Support ever going to call me unsolicited about a virus?

Treat unexpected "Microsoft virus" calls as scams. Start help only from official Microsoft support pages you open yourself.

If you still want a paid suite

Avoiding how to spot a fake Windows blue screen support scam does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* FTC: How to spot, avoid, and report tech support scams
* Microsoft Support: Avoid tech support scams
* Microsoft Safety & Security Center
* FTC ReportFraud

Also read

* How to reset Windows 11 while keeping your files
* How to remove a browser hijacker from Windows
* How to spot a fake Apple Support screen-sharing scam
* How to spot a tech support scam phone call
* How to report a scam to the FTC