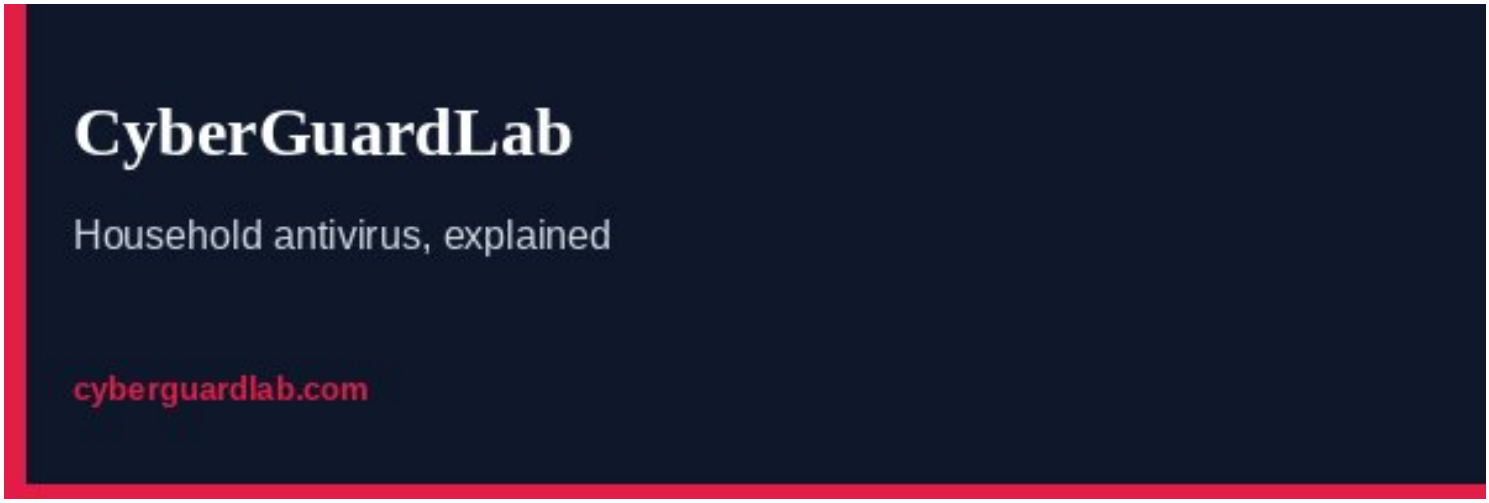
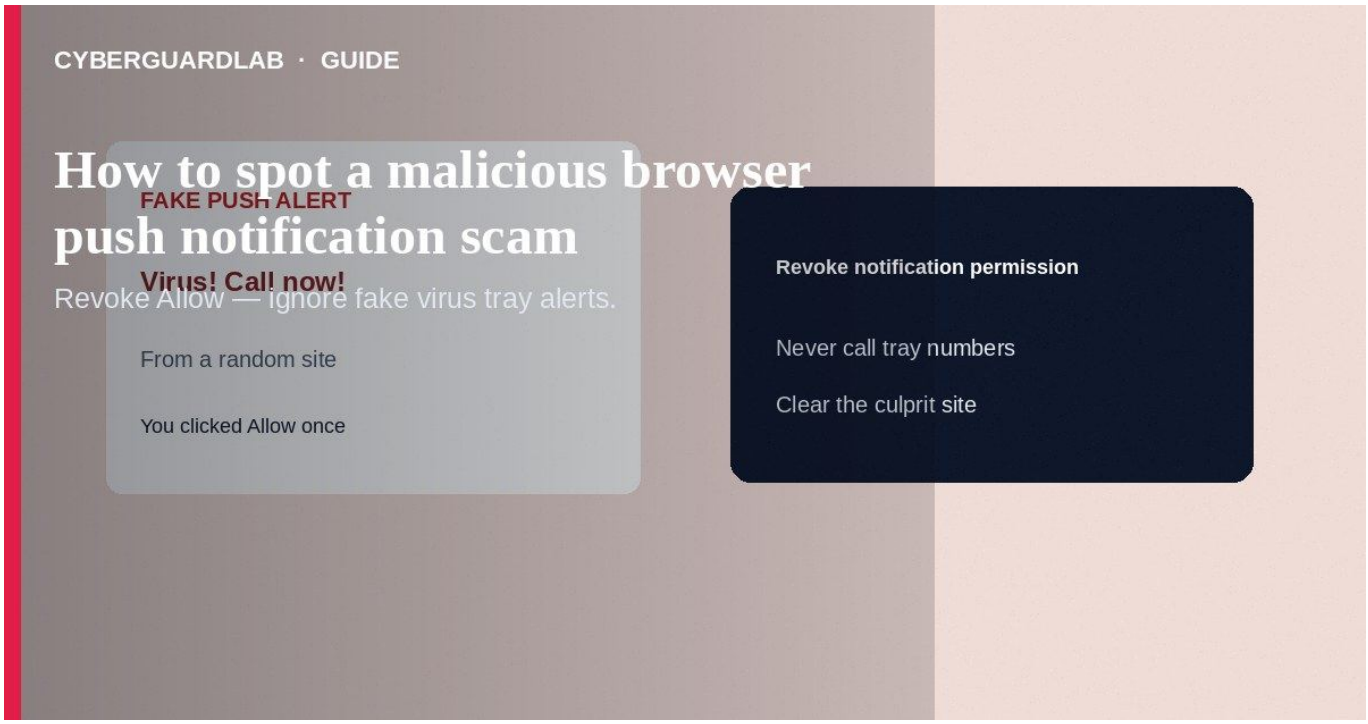


How to spot a malicious browser push notification scam

https://cyberguardlab.com/blog/browser-push-notification-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 malicious browser push notification scam hijacks the OS/browser notification tray after you click "Allow" on a fake "Show weather / Verify you are human / Download antivirus" prompt. Later messages claim virus alerts, package holds, bank locks, or prize wins-and push you to call a number, install software, or open a phishing page. Revoke notification permission for unknown sites, clear the culprit, and never call numbers from random alerts. This guide is about browser push abuse-not SMS phishing alone, not fake password-reset email, and not router UPnP settings.

1. What this scam looks like

A site overlays a full-screen "Click Allow to continue" box. After you allow notifications, the tray fills with red "CRITICAL VIRUS" or "Your PC is locked" messages that look like Windows or Chrome system UI. Some link to tech-support numbers (refund / remote-access scams). Others open look-alike Microsoft, Google, or bank pages. Mobile Chrome and desktop browsers are both targets.

Compare link and brand cues with how to spot a phishing email. Treat "call this number now" the same way you treat cold tech-support calls.

Legitimate CAPTCHA and cookie banners do not need notification permission to "prove you are human." If the only way past a page is Allow notifications, leave the site.

2. Legitimate vs scam cues

Cue | Likely legitimate | Likely scam

Permission ask | A site you trust, for news/chat you requested | "Allow to prove you are not a robot" on a random page

Tone | Normal updates from that site's brand | All-caps virus / FBI / "final warning" from a news domain

Action | Opens the same site you allowed | Demands a phone call, remote tool, or gift-card "unlock"

System branding | Real OS Security alerts open OS Settings you navigate yourself | Fake Windows/Chrome chrome inside a web notification

Urgency | None or mild | "Your files encrypt in 10 minutes"

3. What to do if you see them

* Do not call numbers in the notification. Do not download "cleanup" tools from the alert.
* On the device, open browser Settings -> Privacy / Site settings -> Notifications (Chrome) or equivalent and remove permission for unknown sites-or set to Ask/Block.
* Clear recent browsing data for the shady site; close the tab.
* Run a scan with one primary product such as Norton or Bitdefender; TotalAV, McAfee, and Avast are other on-site options. Avoid stacking full suites.
* If you typed passwords on a fake page, change those passwords from a clean device and enable MFA/passkeys.
* Report the site through the browser's "Report" tools when available; file FTC reports if you paid a scammer.

4. What to do if you already called or paid

* Stop further payments; hang up on ongoing "support" sessions.
* Uninstall any remote-access software they guided you to install.
* Contact your bank/card issuer for unauthorized charges.
* Change email, banking, and store passwords; review account recovery options.
* Report at ReportFraud.ftc.gov.

FAQ

Chrome said a site wants to show notifications-is that always bad?

No. Many news and chat sites use them legitimately. Bad actors abuse the same prompt with scareware copy.

How is this different from a fake password-reset email?

Password-reset phishing arrives in email/SMS. Push scams live in the browser notification permission you granted a website.

Will antivirus stop push notifications?

Antivirus helps with malware downloads; you still must revoke notification permissions in the browser.

I use Safari / Firefox / Edge-am I safe?

Any browser that supports web push can be abused. Check that browser's site-permission list.

If you still want a paid suite

Avoiding how to spot a malicious browser push notification 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 recognize and avoid phishing scams
* FTC: Tech support scams
* CISA: Secure our world (passwords / updates hub)
* Google Chrome Help: Change site permissions

Also read

* How to spot a phishing email
* How to spot a fake password-reset email
* How to remove a browser hijacker on Windows
* How to turn on enhanced Safe Browsing in Chrome
* How to spot a fake Windows BSOD support scam