P

Pop-up Ads: Identify the Source, Stop Them, and Avoid Scams

Pop-up ads can come from a website, push notifications, extensions, or adware. Learn how to identify the source, remove persistent alerts, and respond safely after a click.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 Identify the type of pop-up first
02 What to do with a fake virus pop-up
03 Remove pop-ups caused by website notifications
04 Stop pop-ups, redirects, and new tabs in the browser
05 When pop-up ads may indicate adware
06 Pop-up ads on Android or iPhone
07 What if you clicked the pop-up?
08 Prevent unwanted pop-ups
09 Frequently asked questions
10 References

A pop-up ad is a window, tab, overlay, or notification that displays advertising outside the normal flow of a page. Pop-ups are not automatically malware: websites use them for sign-in, consent, support, and promotions. They become a security concern when they imitate system alerts, force redirects, persist after the site is closed, or result from an unwanted extension or adware.

The fastest fix depends on where the message appears. A browser window, a website overlay, a push notification beside the clock, and an ad generated by installed software have different causes.

01 Identify the type of pop-up first

What you see	Likely source	First action
Ad only while one website is open	Page pop-up, redirect, or overlay	Close the tab without clicking the ad and avoid the site
Alert near the desktop clock with a browser icon	Website push-notification permission	Revoke notification permission for the sending site
New tabs or search redirects on many sites	Extension, changed browser settings, or adware	Review extensions and scan the device
Ads appear even when every browser is closed	Installed adware, notification service, or another application	Check recent applications, startup items, and security alerts
Full-screen fake virus warning with a phone number	Tech-support scam page or malicious notification	Do not call, pay, download, or grant remote access
Ads inside one free application	Application-supported advertising or bundled software	Check the product's expected behavior and uninstall if unwanted

02 What to do with a fake virus pop-up

1. **Do not click buttons inside the warning.** Even a button labeled Close, Scan, or Cancel may trigger another page or download.
2. **Do not call the displayed number.** Security companies and operating systems do not diagnose an infection by placing an unsolicited support number in a web page.
3. **Close the tab or browser using the browser controls.** If it will not close, use the operating system's app switcher or task manager to end the browser.
4. **Decline downloads and notification requests.** Do not install a cleaner, extension, profile, or remote-access tool offered by the page.
5. **Reopen the browser without restoring the suspicious tab.** Clear that site's data if the page returns through session restore.

Seeing a scam page does not prove the device is infected. Clicking its download, enabling notifications, installing an extension, or granting remote access changes the risk and requires additional checks.

03 Remove pop-ups caused by website notifications

A notification may appear when the browser window is minimized or closed because the user previously selected Allow on a site's notification prompt. The alert often carries the browser's icon, while the message itself falsely claims to come from Windows, an antivirus company, or a well-known brand.

1. Open the browser's Settings and find Site Settings, Permissions, or Notifications.
2. Review the sites in the Allowed list.
3. Remove or block domains you do not recognize or no longer trust.
4. Clear that site's stored data if the prompts or redirects continue.
5. Check whether the operating system separately allows notifications from the browser.

Do not block every browser notification if you rely on legitimate webmail or calendar alerts. Remove the abusive site first. If many random domains are allowed, review how permission prompts are handled and consider blocking new requests by default.

04 Stop pop-ups, redirects, and new tabs in the browser

1. **Update the browser.** Install the current stable release before troubleshooting extensions or settings.
2. **Review extensions.** Remove anything unrecognized, installed immediately before the problem, or granted more access than its purpose requires.
3. **Check startup pages and search settings.** Restore the expected home page, new-tab page, and search provider.
4. **Block pop-ups and redirects.** Use the browser's built-in site settings; do not install an unknown "pop-up remover" advertised by the same page.
5. **Clear data for affected sites.** Cookies and site storage can restore unwanted redirects, but clearing all browser data is not always necessary.
6. **Reset browser settings if changes persist.** A reset normally disables extensions and restores core settings, but verify what your browser preserves before proceeding.

Browser synchronization can restore a bad extension or setting on another device. After cleanup, review synced extensions and account security if the change returns.

05 When pop-up ads may indicate adware

- Ads appear in several browsers or outside the browser.
- Extensions return after removal or are marked as managed unexpectedly.
- Search results and links redirect through unfamiliar domains.
- A proxy, DNS server, profile, or certificate changed without approval.
- New applications, launch agents, services, or startup tasks coincide with the problem.

- Security tools are disabled or exclusions were added.

Run an updated full security scan and remove confirmed unwanted software. Also inspect recently installed programs and browser policies. Do not delete random system files based only on a filename from an online forum.

06 Pop-up ads on Android or iPhone

On mobile devices, first close the affected tab and revoke notification permission for the site. Review recently installed apps, especially cleaners, launchers, keyboards, QR scanners, wallpaper apps, and unofficial stores. Check which apps can display over other apps on Android and remove unnecessary configuration profiles on iPhone or iPad.

If ads appear only in one free app, they may be part of that app rather than an infection. Remove the app if its advertising is deceptive or excessive. Install replacements from the official store and verify the publisher and reviews.

07 What if you clicked the pop-up?

What happened	Recommended response
The page opened, but nothing was downloaded or entered	Close it, revoke notifications if allowed, and watch for changes
A file downloaded but was not opened	Do not run it; scan or delete it and record the source
You installed an app or extension	Disconnect if behavior is suspicious, uninstall it, scan, and check persistence
You entered a password	Change it from a clean device, revoke sessions, and enable MFA
You granted remote access or paid a caller	Disconnect the device, contact the payment provider, preserve evidence, and treat accounts as compromised

08 Prevent unwanted pop-ups

- Keep pop-up and redirect blocking enabled.
- Allow site notifications only when their ongoing value is clear.
- Install extensions sparingly and review their permissions.
- Download software from the verified publisher, not an advertisement or mirror.
- Avoid cracks, fake updates, and pages that demand you disable security protection.
- Use a reputable content blocker where appropriate, while keeping the browser's security controls enabled.

09 Frequently asked questions

Does a virus warning in a browser mean I have a virus?

Usually not. A website cannot perform a trustworthy full-device scan through a generic pop-up. Treat the warning as a scam unless a security product you installed reports it through its verified interface.

Why do pop-ups appear when Chrome is closed?

Web push notifications can be delivered in the background. Revoke notification permission for the sending site instead of repeatedly dismissing each alert.

Will reinstalling the browser remove pop-up ads?

Not always. Sync may restore settings, and system adware or managed policies can affect a fresh installation. Identify the source before reinstalling.

10 References

- Google Chrome Help: Remove unwanted ads, pop-ups and malware
- FTC: Protect against, detect, and remove malware
- FTC: Spyware and malware

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