A

Adware: Meaning, Warning Signs, Safe Removal, and Prevention

Adware displays or injects advertising, often through unwanted apps or extensions. Identify whether the source is a website, browser permission, or installed software.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

Adware is software that displays, injects, or redirects advertising, often outside the clear context and control expected by the user. Some legitimate applications are openly ad-supported. Security vendors use the term for behavior that is intrusive, deceptive, bundled without informed consent, difficult to remove, or combined with tracking and browser modification.

If a scanner supplies a specific verdict, use that context as well: Adware.Gen is a generic detection label, while Amonetize is associated with software bundling. The alert name helps frame the investigation but does not establish everything an installer did.

Adware is commonly classified as a potentially unwanted application (PUA/PUP), but some variants cross into malware through covert installation, credential theft, security tampering, or malicious downloads.

Adware vs. malicious ads and notifications

- **Installed adware:** an application or extension creates ads, redirects, or tracking behavior.
- **Malvertising:** a malicious or deceptive advertisement can appear through an ad network even when no adware is installed.
- **Website notification abuse:** a site given notification permission can send fake virus alerts outside the browser tab.
- **Ordinary website ads:** ads appear only within the page and disappear when it closes.

Common warning signs

- ads appear on pages or in applications that normally do not contain them;
- search, homepage, new-tab, proxy, or DNS settings change;
- an unknown extension, toolbar, updater, profile, or companion app appears;
- clicks redirect through unfamiliar domains or downloads start unexpectedly;
- the behavior returns after the extension or app is removed.

Targeted advertising alone is not proof of local adware. Cross-site tracking, account activity, and contextual ad systems can produce similar impressions.

A useful confirmation test is scope: close the suspect site, disable its notifications, and compare a clean browser profile. If the behavior follows one extension, profile, or installed program, that evidence is stronger than the appearance of a single advertisement.

Find the source before resetting everything

1. If alerts are notifications, review the browser's site permissions and remove the sender.
2. If only one browser is affected, inspect its extensions, managed policies, search engine, startup page, and sync account.

3. If all browsers or other applications are affected, inspect installed programs, startup entries, scheduled tasks, proxy, DNS, and system profiles.
4. Check what was installed immediately before the symptoms and preserve detection paths.

Safe removal steps

1. Uninstall the source application and related bundled software through normal system settings.
2. Remove unknown extensions and revoke abusive notification permissions from every affected browser profile.
3. Restore browser, proxy, and DNS settings only after the component changing them is removed.
4. Run an updated full security scan, quarantine detections, restart, and scan again.
5. If browser sync restores the extension or setting, remove it from the synced account rather than repeatedly resetting the local browser.

Microsoft's current software evaluation criteria emphasize informed choice, clear advertising attribution, user control, and straightforward removal.

Prevention

- use official app stores and publisher sites;
- choose custom installation and reject unrelated offers;
- keep PUA blocking enabled for downloads and installed applications;
- limit extensions and review site notification permissions;
- avoid cracks, fake updates, download wrappers, and popup system cleaners.

Adware FAQ

Is adware always a virus?

No. It is a behavior and risk category, although an adware campaign may also deliver malware.

Why did ads return after a browser reset?

An installed helper, managed policy, sync account, notification permission, or network setting may still recreate the behavior.

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