T

Third-Party Cookies: Tracking, Browser Changes, and Controls

Third-party cookies are read in a cross-site context and can support tracking or embedded services. Browser policies differ, and blocking has practical tradeoffs.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

A **third-party cookie** is a cookie accessed while its site differs from the top-level site visible in the browser. For example, a news page may load an advertising, social, analytics, payment, or embedded-video resource from another site; that resource may attempt to set or read its own cookie.

Third-party cookies are widely associated with cross-site advertising profiles, but the same mechanism has also supported embedded sign-in, fraud prevention, payments, and user preferences. A cookie is data, not malware; the privacy or security impact depends on what it identifies, where it is sent, and how it is protected.

First-party vs. third-party cookies

- **First-party context:** the cookie belongs to the site the user is visiting and commonly maintains login state, cart contents, or preferences.
- **Third-party context:** the cookie's site differs from the top-level site and may be recognized across other sites embedding the same provider.
- **Partitioned cookie:** the browser stores a separate third-party cookie jar for each top-level site, allowing an embedded function without a shared cross-site identifier.

Modern browser definitions are based on the web concept of a “site,” including scheme and registrable domain, rather than merely whether hostnames look different. The MDN third-party cookie guide explains these distinctions for developers.

How cross-site tracking works

1. A third party is embedded on many unrelated websites.
2. It assigns a browser identifier in an unpartitioned third-party cookie.
3. When the browser loads that provider elsewhere, it sends the same identifier.
4. The provider can associate page visits, ad interactions, and other events with one browser profile.

Blocking third-party cookies limits this technique but does not stop all tracking. First-party identifiers, server-to-server sharing, link decoration, IP-derived signals, and browser fingerprinting may still connect activity.

Current browser status

Browser behavior is not uniform. Firefox Enhanced Tracking Protection and Safari's tracking protections restrict many third-party tracking uses by default. Users can choose stricter settings, with possible breakage for embedded content or sign-in.

Chrome did not complete a universal removal of third-party cookies. In April 2025, Google said it would maintain Chrome's existing user-choice approach and would not launch a new standalone third-party-cookie prompt. Google's Privacy Sandbox feedback report records that decision. Therefore, advice claiming all Chrome users are automatically cookieless is inaccurate.

How to check and control them

- Open the browser's privacy or site-data settings and review its third-party-cookie or tracking-protection option.
- Use the browser's site-information panel or developer storage tools to inspect cookies for a specific page. A general “cookie checker” site cannot see every other site's cookies because browser isolation prevents that access.
- Block third-party cookies globally or choose a stricter tracking mode if it matches your needs.
- If a trusted embedded login, payment, or media feature fails, allow only the specific site temporarily instead of disabling protection everywhere.
- Clear site data to remove existing identifiers, understanding that this may sign you out and reset preferences.

Security and privacy limits

Blocking third-party cookies does not remove ordinary first-party login cookies. Session theft is a separate security issue and can affect either context. Sites should use HTTPS and appropriate `Secure`, `HttpOnly`, and `SameSite` attributes, minimize retention, and obtain legally required consent.

Private browsing reduces data retained after the private session but does not make a user anonymous to websites, network operators, employers, or an internet provider.

Third-party cookie FAQ

Are all third-party cookies trackers?

No. Some enable embedded services, but unpartitioned cross-site recognition creates tracking potential.

Will blocking them stop targeted advertising?

It reduces one major input, but other identifiers and contextual advertising remain.

Should I accept every cookie to make a site work?

No. Start with necessary cookies and grant optional categories only when you understand and want their purpose.

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