# Third-party Cookie - what it is, why tracking matters, and simple ways to limit it

Gridinsoft Help Center

## What it is

A third-party cookie is a small tracker set by a site you aren’t visiting directly. For example, a page loads an ad or "Like" button from another company, and that company drops its own cookie in your browser. As you browse other sites that use the same ad/analytics code, that cookie helps build a profile of your activity across the web.

## Why it matters

These cookies can follow you from site to site, shaping ads and revealing a lot about your interests. If poorly secured, they can also leak identifiers that tie your activity to you. While they don’t normally store your passwords, they can still reduce privacy and increase the value of your data to attackers and data brokers.

## How it works

- A webpage includes third-party content (ads, widgets, analytics).
- That content sets/reads its own cookie in your browser.
- When you visit another site using the same third party, it recognizes you again.
- Over time, this creates a cross-site browsing history for targeting or analytics.

## Red flags

- Ads or recommendations that seem to "know" what you just looked at on other sites.
- Lots of third-party requests on a page (you can see this in browser dev tools or privacy reports).
- Cookie banners that default to "accept all" with dozens of "partners."

## Do it right

- In your browser settings, block third-party cookies or use "Strict"/"Enhanced" tracking protection.
- Use privacy features: reader mode, private windows, and "clear cookies on close."
- Limit extensions and only keep the ones you trust.
- Log out of accounts on shared devices and review each site’s cookie settings.