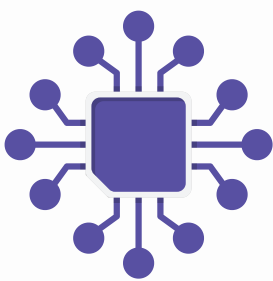# How Cookies Track You – And What You Can Do About It

What Are Cookies, and Why Should You Care?

Every time you visit a website, it stores cookies which are small files in your browser that remember who you are and what you do. Cookies are useful for staying logged in and saving preferences but they also track your behaviour across websites.

You should care because:

- Cookies track your visits, even across different sites.
- Advertisers use them for targeted ads.
- Your data can be sold or shared.
- They create a profile about you, often without consent.

Key Cookie Data (and Why It Matters)

Field	What It Means	Why It Matters
Name	Label for the cookie (e.g. session ID)	Used to identify your session or visit
Value	Unique info stored (like your ID)	Links you directly to your activity
Domain	Site that set the cookie	May be first-party or third-party
Path	Which part of the site can access it	Controls how broadly it's used
Expiration	When the cookie gets deleted	Longer expiry = longer tracking window
Secure	Sent only over HTTPS?	More secure, but still trackable
HttpOnly	Hidden from JavaScript?	Protects against script-based theft
SameSite	Limits cross-site sharing	Helps reduce 3rd-party tracking

How to Reduce Tracking Through Cookies

- **Clear Cookies**
  - Deletes tracking data and resets session links
- **Use Incognito/Private Mode**
  - Deletes cookies after the session ends
- **Block 3rd-Party Cookies**
  - Prevents advertisers from tracking you across websites
- **Use a Privacy-Focused Browser (e.g. Brave)**
  - Blocks trackers and 3rd-party cookies by default
- **Use Cookie Manager Extensions**
  - Lets you control or block unwanted cookies

Tools You Can Use to Protect Against Cookie Tracking

- uBlock Origin – blocks many trackers & cookies
- Privacy Badger – automatically blocks spying cookies
- Brave Browser – built-in 3rd-party cookie blocking
- Firefox Container Tabs – isolate site data
- Cookie AutoDelete – deletes cookies after leaving a site

TraceMe