When I think about keeping my personal information safe online, my first step is making my web browser harder to track. There are several tools and extensions that can help with this.

- **HTTPS Everywhere (built into most browsers now)** makes sure I connect to sites using encryption instead of plain text. This stops anyone from spying on what I'm doing.
- **uBlock Origin** blocks adverts, trackers and even scripts that try to use my computer for things like crypto mining.
- **Privacy Badger** is made by the Electronic Frontier Foundation. It learns which sites are following me around and blocks them automatically.
- **NoScript** gives me control over what scripts can run on each website. That way, only trusted pages can load active content.
- **Cookie AutoDelete** clears cookies when I leave a site. This prevents websites from building a long history of my activities.
- **NordVPN** adds another layer of privacy. It hides my IP address and encrypts my traffic, making it much harder for advertisers or even my internet provider to log everything I do.

Why am I tracked on every click?

Most websites and advertisers want data. They use cookies, fingerprinting and third-party scripts to follow me across the internet. Every click, search or purchase gets recorded. This data is valuable for targeted ads, selling to other companies and even shaping what content I see.

Can I stop tracking completely?

I can reduce it a lot, but I can't fully stop it. Extensions like Privacy Badger or uBlock Origin make a big difference. A VPN like NordVPN or even the Tor Browser hides my activity further. The problem is that fingerprinting can still identify me based on my device and browser setup. So in reality, I can only limit how much I'm tracked, not remove it completely.
