NAWA Media

Browsing and Trackers

Section: 3.8

Online Tracking: How does it work?

If you've ever been online shopping one day and continue to see ads for that website everywhere you look in the digital sphere, you too have fallen victim to your browser and your search engine tracking you. Given the prevalence of e-commerce, tracking has become more commonplace but it has also become very intrusive.

Through tracking cookies, websites and browsers are able to track the things you are searching for and this coordinates with the attempts and business interests of larger brands. Once this information exchange takes place, you are identified as a potential customer or buyer and are then inundated with ads. This exchange happens in seconds.

Preventing Tracking

The first question people often about this, is how to stop it from happening. There are a few things that you can do for this.

- Disable syncing from your phone to your Google account. Most people use Google Chrome and the automatic syncing allows for a lot of exchange of information.
- Use incognito mode as much as possible.
- Use VPNs to encrypt your activity as much as possible. This isn't a foolproof way of avoiding tracking but since the technology for digital tracking has evolved so much, there are multiple things one has to do to avoid it.
- Use search engines like DuckDuckGo, which doesn't track you and are open source and secure.
- Install extensions like HTTPS Everywhere on your browser to create secure connections between you and the websites you are on.
- Frequently clear your cache as tracking cookies can silently live on your devices.
- Chrome and Firefox have a 'Do Not Track' feature that sends out a message to the websites you visit to not 'track you'.
- Chrome and Firefox also have automatic features that clear your cache and cookies, but they're not enabled. Going through the disabled security features already available on these browsers can significantly bolster your security.

Anti-Tracking Tools

Tools such HTTPs Everywhere and Privacy Badger can also be used as browser extensions to ensure that your browsing is safe and secure.

HTTPs Everywhere is a free and open-source browser extension for Google Chrome, Mozilla Firefox, Opera, Brave, Vivaldi and Firefox for Android. It automatically switches thousands of sites from insecure «http» to “https” to ensure that your browsing enjoys greater levels of encryption.

Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking users as they visit websites. Privacy Badger automatically blocks that advertiser from loading any content on your browser without the permission of the user.

NAWA Media

BCMCR | Birmingham Centre for Media and Cultural Research

BIRMINGHAM CITY University

MEEDAN

Check

Sida