How to avoid being tracked and sold on the Internet

On today's internet, around 80% of all websites are tracking and selling personal data about you and your browsing habits. It's at the very core of the modern internet; services like Google search, Gmail or social networks like Facebook or Twitter are not free; you pay with your data.

The worrisome part is how little control the end-user has over the information collected about them, the whole filed of data collection is still largely unregulated.

When your information is collected, it's instantly sold to data brokers who then resell that data to the highest bidder. It might end up in the hands of political campaign trying to illegally sway an election, or even in the hands of hacker groups looking to exploit you.

How are they tracking me?

Tracking is achieved through different techniques, with the most prevalent one being cookies, but new techniques emerge as adblockers evolve. One of the most advanced techniques is called ultrasonic cross-device tracking, it embeds high-frequency tones inaudible to humans in an advertisement, web-pages and even in physical retail stores. This ultrasound is picked up by the user's cellphone that then knows exactly what web page or

advertisement the user is currently watching.

Tracking cookies

This is a small file stored in your browser that helps websites you visit to identify you and load custom settings like language, login information, and items in your shopping cart. Some cookies are harmless and only store the required information for the relevant site you are visiting, and other cookies remain active on all websites. These cookies are called third-party persistent cookies and they gather information about your online behavior, what sites you visit, what links you click.

The purpose of these invasive third-party cookies is to collect information about you and sell it to the highest bidder.

Tracking Beacons

These are small transparent images loading on webpages or within emails for tracking purposes. Websites use them to get information about how many times visitors load a certain page, and advertisers use them to determine how many impressions their ads get.

Email-spammers can use them to determine if an email has been opened, letting them know the email is active for further spamming.

Fingerprinters

This is the most complex method of tracking since it creates a profile of your browser settings, screen resolution, and other metrics. This method does not require a file to be stored on your computer.

How do I stop tracking?

Since there are no laws in place to regulate the collection of personal information on the internet, it's up to you, the end-user, to take matters in your own hands. Fortunately, it's relatively simple to protect yourself from tracking using a good web browser with a handful of plugins.

Browsers:

Choosing a good browser is paramount to security and the ability to choose what tracking to block. Most browsers derive revenue from tracking your online behaviour and either selling that data to online advertisers or using it themselves to deliver ads. The biggest browsers out there like Chrome and Explorer does not even have an option to block third-party tracking cookies or other scripts, that's why our recommendation is just Firefox.

Mozilla Firefox
Get it for: Windows, Mac, Linux

Firefox is the only large web browser that takes privacy seriously. Mozilla, the company behind it, doesn't derive any revenue from ads and as such it's easier to trust them with your data

Firefox has excellent built-in tracking protection; you can either use one of its preset modes of blocking or get into the fine details, only blocking what you want.

Usage: install and forget.

Plugins:

There exists a myriad of privacy plugins for most browsers, some of them work well but some are just borderline scams, collecting the personal data they say the block. The plugins we recommend should be everything you'll ever need; they stop online tracking, remove advertisement and speed up load times while making your browsing much more secure.

Privacy Badger
Get it for: Firefox, Chrome, Opera

Privacy Badger automatically learns to block invisible trackers. Privacy Badger sends the Do Not Track signal with your browsing. If trackers ignore your wishes, your Badger will learn to block them.

Usage: install and forget.

HTTPS Everywhere
Get it for: Firefox, Chrome, Opera

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.

Usage: install and forget.

BitIDentify

Decentraleyes

Get it for: Firefox, Chrome, Opera

Protects you against tracking through “free”, centralized, content delivery. Complements regular content blockers.

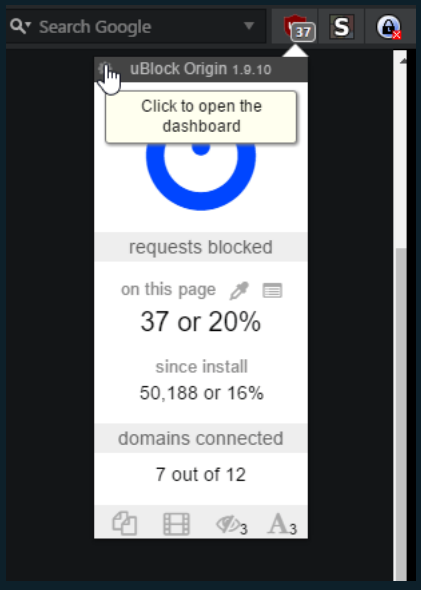
Usage: install and forget.

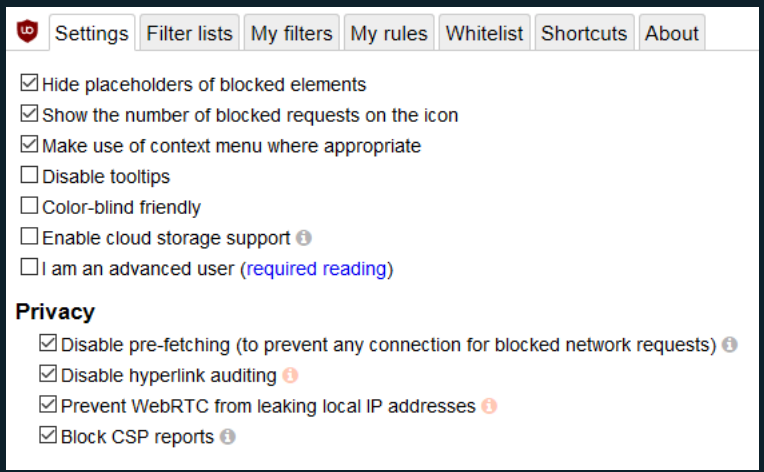
Ublock Origin

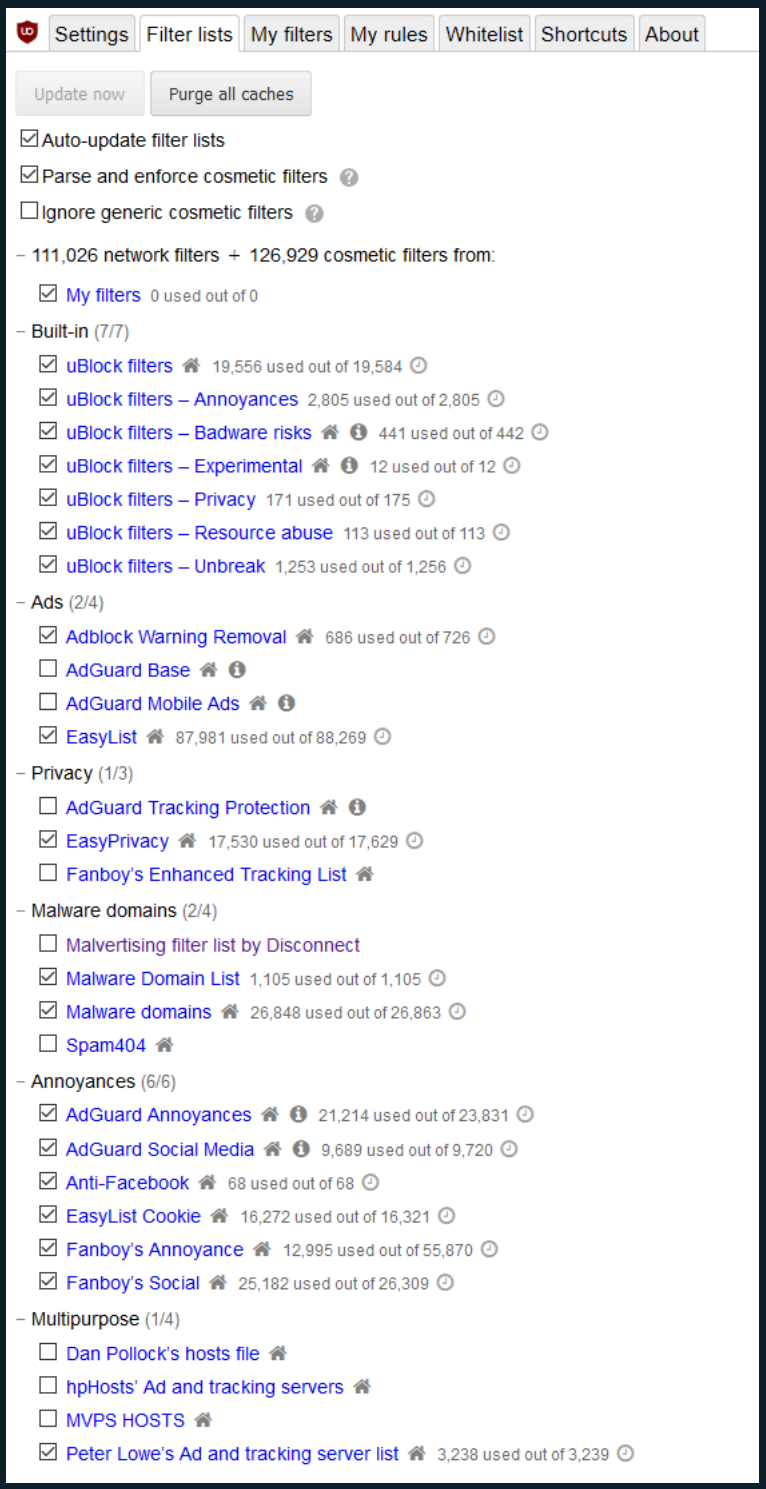
Get it for: Firefox, Chrome, Opera

Probably the single most important plugin you can use; Ublock Origin blocks advertisement, trackers and malware. There are lots of “Adblockers” out there but Ublock Origin is by far the most efficient one, and it’s also completely free and open source.

Usage: You can just install it and forget it, the default settings are good enough. But if you want to take it up a notch, spending some time on the settings is recommended.







Original post can be found at our homepage:
https://www.bitidentify.com/blog/how-to-avoid-being-tracked-and-sold-on-the-internet/