How to Be More Anonymous Online

Being fully anonymous is next to impossible—but you can significantly limit what the internet knows about you by sticking to a few basic rules.

By Matt Burgess

Jan 05, 2024 07:00 AM · 2 min. read · View original

On the internet, everyone wants to know who you are. Websites are constantly asking for your email address or trying to place tracking cookies on your devices. A murky slurry of advertisers and tech firms track which websites you visit, predicting what your interests are and what you may want to buy. Search engines, browsers, and apps can log each search or scroll you make.

At this stage of the internet, being totally anonymous across your entire online life

is incredibly hard to achieve. Phones, SIM cards, browsers, Wi-Fi networks, and more use identifiers that can be linked to your activity. But there are steps you can take to obscure your identity for everyday browsing.

If you're looking to be truly anonymous or to protect your identity for a specific purpose—such as whistleblowing or activism—you should consider your threat model and individual security situation. But many of the changes you can make, which are listed below, are straightforward switches that can stop you from being tracked as much and apply to most people.

Block the Trackers

You're constantly being tracked online. Often the main culprit is the advertising industry and the tech companies heavily reliant on advertising to make money (think: Google and Meta). Invisible trackers and cookies embedded in websites and apps can follow you around the web.

Start with your web browser. Ideally, you want to block invisible trackers and ads

that have tracking tech embedded. Advertisers can also track you using fingerprinting, a sneaky profiling method where the settings of your browser and device (such as language, screen size, and many other details) are used to single you out. If you want to see how your current browser tracks you, the Electronic Frontier Foundation's Cover Your Tracks tool can run a real-time test on your system. Using Chrome, the world's most popular browser, neither tracking ads nor invisible trackers are blocked for me, and my browser has a unique fingerprint.

For the most anonymity, the Tor Browser is best. Downloadable in the same way as any other browser, it encrypts your traffic by sending it through a number of servers and also deploys anti-censorship, anti-fingerprinting, and other privacy measures. Because of its advanced protections, however, Tor can sometimes be slower than other browsers. Several privacy-focused browsers such as FireFox, the Mullvad Browser, and Brave offer enhanced protections against trackers and offer further customizable privacy settings.

If you don't want to switch browsers, there are some browser extensions that can block trackers within Chrome. Both the Ghostery extension and EFF's Privacy Badger will block trackers, with the latter not blocking ads unless they are specifically tracking you. On Walmart's homepage, while using Chrome, for example, Privacy Badger blocked four trackers that were in use, while Ghostery identified five.