Privacy Café

How to leave fewer traces while you're surfing

Each time you visit a website, you give away information about yourself to the site owner, unless you take precautions. Remember that the Internet is a network of networks. Accessing one website on the Internet is never done via a direct connection. Many computers owned by many different companies and individuals are involved. In addition, your browsing on the Internet may be tracked by the sites you visit and partners of those sites.

What you search for is of great interest to search companies, advertisers and others. Google, Bing, and most other search engines collect and store your search queries. Some travel agencies may even charge you higher rates based on your devices (Apple, Microsoft, Linux), software and your browsing habits.[1]

CHOOSE A SAFE BROWSER

It is wiser to trust open source browsers like Mozilla Firefox (free download at https://www.mozilla.org/firefox) as they can be more readily security audited.

HTTPS: Whenever you write and send something in a browser - be it an email, Facebook posts or other personal information -, you should always ensure to use so-calles SSL/TLS encryption for the entire session. For instance, if using a browser to check your email, you should verify if the mail server supports SSL sessions by looking for the "S" in the "https://" at the beginning of the web address. If not, be sure to turn it on in your email account settings, such as Gmail or Hotmail or just add the "S" manually to the address.This ensures that any data transmitted to the web server is encrypted.

INSTALL IMPORTANT ADD-ONS

All add-ons recommended below are open source and available for free for Mozilla Firefox. They greatly increase your protection against malicious websites, unwanted advertisements and against commercial, tracking software. They are kindly provided by non-profit organisation such as the Electronic Frontier Foundation or by volunteer communities.

Note that those add-ons do not provide anonymity. To surf the web anonymously, it is highly recommended to use Tor (https://www.torproject.org).

1. **HTTPS Everywhere**: Enables HTTPS by default on many websites, straightforward and very easy to use. Protects you silently in the background, you basically forget that it's there.
2. **Ad-block Edge**: Blocks a huge amount of advertisements. Instead of wasting time to load ads, websites appear clean and neat. Again, after a while you just forget that the add-on is there and you'll never want to use a browser without it again.
3. **Web Of Trust**: Protects you from malicious or fake websites by showing a coloured rating for each website and link. A green cirlce means good, a yellow circle means attention, a red circle warns you of sites you should probably not visit. All ratings are based on information collected from a large user community.
4. **Privacy Badger**: Blocks requests from advertising websites. Such requests are mostly built into existing websites such as news sites, search engines and, of course, social networks. Privacy Badger impedes advertisers to collect private information from you.

[1] http://www.wsj.com/articles/SB10001424052702304458604577488822667325882

access
EDRi
LIGA VOOR MENSENRECHTEN