Private browsing to stay safe online

Online privacy and security:

- No such thing as perfect security and privacy (unless you decide to live completely off the grid).
- Today: some practical ways (i.e. which don't require changing habits) to increase your privacy.

Why pay attention to privacy settings and privacy enhancing add-ons?

- Browsing websites generates a lot of data collected by companies and governments.
- This data can be shared or leaked (companies and governments are hacked all the time).
- This data can be used to very efficiently and accurately learn private information about you (location, shopping habits, relationship information, sexual orientation, political opinions, …).
- Not only companies and governments: individuals too (friends, family or community, not just malicious adversaries).

Tools for browsing:

Browser plugins and other tools that can be installed and ran with minor (or no) set up required. This list is an overview. You might not need all of these (overlap or no usefulness) and the list is not exhaustive either.

The add-on or extension hub of your browser will have a security and privacy section with lots of choice. Research before using! The more you add the more potential there is for bugs and exploits. Make sure to check what data these add-ons collect about you and what settings you might have to tick or untick.

- HTTPS Everywhere https://www.eff.org/https-everywhere: forces connection over HTTPS rather than HTTP whenever available. The S in HTTPS stands for *secure* which is a property of the connection, not the website content.
- Privacy Badger https://www.eff.org/privacybadger: stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web based on heuristics.
- uBlock Origin https://www.ublock.org: blocks advertisers and trackers based on lists.
- NoScript https://noscript.net/: provides control over which scripts can be run in the browser. Firefox only (with alternatives for other browsers) and requires some set up before it stops being annoying (i.e. blocking everything).
- uMatrix https://github.com/gorhill/uMatrix: allows fine grained control over browser connections, downloads and executions. Designed for advanced users.
- DuckDuckGo https://duckduckgo.com: privacy preserving search engine. Allows searching through other engines and websites (google, facebook, twitter, …) using !website (!g, !facebook, !twitter, …) in the search text.

- Proxies: you connect to a proxy which connects you to the website you want. Does not necessarily guarantee any privacy or security if your connection to the proxy is not hidden. Can help circumvent country-based censorship.
- VPN: virtual private network, simulates connection to a private network, e.g. work or university intranet. Data is encrypted and sent through a remote server. Note that the remote server (run by the VPN operator) can collect the data going through it so you have to trust them. If you're worried about your data being collected, don't use a VPN hosted in a country which has the data collection you're trying to avoid.
- Tor https://www.torproject.org: the onion router, relays your traffic through layers (other nodes) of the network to create anonymity. Note that your connection to the TOR is not necessarily hidden. See below for more.
- Surveillance Self Defence https://ssd.eff.org/en: EFF resource hub (overviews, tutorials, briefings).

TOR - The Onion Router:
The TOR protocol implements *onion routing*, what you send and receive over the internet is encrypted and goes through *layers* (relay nodes) of the TOR network. Note that the traffic does eventually go out through an exit node, except for the case of browsing .onion websites.
Unlike a VPN, TOR does not have any data about you (ip address, billing details for a paid VPN, …).
Technical: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/tor14design.pdf, https://www.eff.org/pages/tor-and-https
TOR is also be used to access .onion websites (*hidden services)* hosted on servers connected to the TOR network.

Installing and running Tor:
Easiest way to do this is through the Tor browser, based on firefox
https://www.torproject.org/download/download-easy.html.en
https://ssd.eff.org/ (Tutorials, *How to: Use Tor for…)*

Follow:
https://twitter.com/duckduckgo
https://twitter.com/torproject
https://twitter.com/EFF

Keep learning!

Any questions? Message us!
s.azouvi@gmail.com @SarahAzouvi
alexander.hicks@ucl.ac.uk @alexanderlhicks