Browsing Anonymously

A walk-through of safe(r) browsing recommendations.

This guide will provide practical advice for multiple threat-levels.

Threat	Description
Level 1	Privacy for Family & Friends, Browsing on Public Computers
Level 2	Personal/Identity Concerns, ISP Logging, Geographic Restrictions
Level 3	Law Enforcement, Journalists, Bloggers, Activists, Lawyers
Level 4	Whistle-Blowers, Intelligence Operators, State-Level Threats

Disclaimer:

- We are not lawyers, and this is not legal advice.
- Technology is constantly evolving, and this information could be outdated.
- Following this advice does not guarantee protection against every threat.
- You accept responsibility for your actions and the repercussions of following this advice.

We believe all individuals should have awareness in regards to their personal privacy, and browsing activity is one of the most exploited areas of the internet.

There are many reasons a person may want or need anonymity. For more information about such cases, **The Tor Project (https://www.torproject.org/about/torusers.html.en)** has great demonstrations of several legitimate applications.

Level 1 - Basic Private Browsing

This is where most general users will be. These recommendations will only be useful against other non-technical threats. If you have any concerns about privacy that goes beyond the most basic protection, realize this level will do ZERO to protect you from a more sophisticated threat. If you're using a public terminal you'll definitely want to follow these steps.

Use your browser in “private” mode.

This prevents your browser from saving a browsing history and caching any cookies or data. Once you end your session and close the browser window, all local evidence is gone.

PLEASE REMEMBER: *an IT admin at work, a user on your local network, an ISP, and state-level agencies can still capture packets and analyze your traffic. A majority of this traffic is unencrypted. If you care about this, escalate to a higher level.*

Select your browser:
Mozilla Firefox (https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history)
Google Chrome (https://support.google.com/chrome/answer/95464?hl=en)
Safari (OSX) (https://support.apple.com/kb/PH19216?locale=en_US)
Safari (iPhone/iPad/iPod Touch) (https://support.apple.com/en-us/HT203036)
Internet Explorer (http://windows.microsoft.com/en-us/windows7/protect-your-privacy-using-internet-explorer-9)
Microsoft Edge (http://windows.microsoft.com/en-us/windows-10/browse-inprivate-in-microsoft-edge)

Clear your cache, cookies, and history.

If you forgot to browse in a private mode, or want to make sure everything is clean by your own doing, you'll need to clear the cache and history for your browser manually.

Select your browser:
Mozilla Firefox (https://support.mozilla.org/en-US/kb/how-clear-firefox-cache)
Google Chrome (https://support.google.com/chrome/answer/95582?hl=en)
Safari (OSX) (https://help.apple.com/safari/mac/9.0/#/sfri11471)
Safari (iPhone/iPad/iPod Touch) (https://support.apple.com/en-us/HT201265)
Internet Explorer (http://windows.microsoft.com/en-us/windows7/how-to-delete-your-browsing-history-in-internet-explorer-9)
Microsoft Edge (http://windows.microsoft.com/en-us/windows-10/view-delete-browsing-history-microsoft-edge)

Level 2 - Browsing Via Proxy

Open Web Proxy

If your goal is to avoid geographic restrictions or mask your IP address from *some* remote sites it may be appropriate to use an open web proxy. These proxy servers provide little protection against advanced threats. Many of them are blocked on most servers and resources but with persistence you can usually find a combination that will work.

Proxy.org Homepage (http://proxy.org/)

Level 3 - Utilizing Encryption

Tor/VPN

A better option is to utilize a VPN or Tor client. These tools help to improve privacy and security by encrypting traffic before it leaves the host and is then routed through a series of nodes before being passed on to the remote server. There are many free and paid options. Some accept payment in BTC or other cryptocurrencies. Using a VPN/Tor alone is not enough to prevent eavesdropping and traffic correlation from state level threats. Also, traffic can also leak identifying information about you that doesn't get piped through the tool.

- The Tor Project (https://www.torproject.org/)
- That One Privacy Guy's VPN Comparison Chart (https://docs.google.com/spreadsheets/d/1FJTvWT5RHFSYuEoFVpAeQjuQPU4BVzbOigT0xebxTOw/edit#gid=0)

Level 4 - Advanced Anonymity

Public Wi-Fi

Using a public Wi-Fi source can provide minimal anonymization. Without utilizing other protocols, this alone leaves your device's MAC address and browser fingerprinting data to be logged. Not to mention your device being open to attack and traffic sniffing while exposed on the public network.

Using a VPN/Tor on Public Wi-Fi.

Even better but still has weaknesses. Your host can still leak traffic that can be used to identify you.

Tails

Tails is a Linux distro designed with security and privacy in mind. It runs from a live DVD/CD or USB. Tails allows you to spoof your device's MAC address during the boot process. Tails also routes all of it's traffic through Tor. If you have the resources to use a 'burner' device that has no paper trail connected to you, even better.

Tails Homepage (https://tails.boum.org/)