

Anonymous Web Browsing

Introduction

When performing online research and any online activities in general it is possible for web server operators to track your usage. Server operators can use a number of different identifiers to track your usage over time. The most obvious identifiers are IP address, cookies, web cache, web browser type, and specific usage habits. If privacy or anonymity is a concern certain measures can be taken to reduce your web footprint.

Options for Anonymity

- **Virtual Private Network (VPN) Providers:** A VPN is a special network that allows computers to securely and privately access resources through them. Computers configured to use a VPN can forward all traffic through the VPN and obscure their actual IP address. Examples of commercial VPN services:

- Strong VPN (<http://www.strongvpn.com>)
- Black Logic VPN (<http://blacklogic.com/>)
- Pirate Party VPN (<http://www2.piratpartiet.se>)
- HotSpotVPN (<http://www.hotspotvpn.com>)



- **The Onion Router (TOR):** TOR is a global Internet anonymity and privacy system. It utilizes between 800-1500 computers spread across the world to forward Internet traffic anonymously.

- A user installs TOR and configures their web traffic to move through the TOR network.
- This makes the user's traffic appear to originate at a random computer on the Internet.



- **DSL/Cable Modem power cycling**

- Unplug your Cable or DSL modem and leave it unplugged for several minutes.
- This will cause the modem to obtain a new IP address. This IP address *could* be different than the old one; check your current IP address at www.whatismyip.com before you turn the modem off, then again after you turn it back on.

- **Anonymous Web Proxies**

- A web proxy takes your requests for websites and forwards them as its own, and returns the results to you. An anonymous proxy allows you to surf the web through another computer. It will appear that the other computer is talking to the web

servers you visit.

- There are hundreds of anonymous proxies for public use. A quick Google search will turn up lots of them.
- Firefox plug-ins for using anonymizing proxies:
 - ProxySel, <https://addons.mozilla.org/en-US/firefox/addon/4457>
 - Switch Proxy, <https://addons.mozilla.org/en-US/firefox/addon/125>
 - FoxyProxy, <https://addons.mozilla.org/en-US/firefox/addon/2464>
- **Dial-up Internet access.**
 - Use a dial-up modem and provider such as Earthlink, Juno, or NetZero to connect to the Internet.
 - Every time you dial in and connect to the Internet there is a very good chance that your IP address will be different.
 - Calling different access numbers (different cities, different States even) will increase the chance of getting a unique IP address.
- **Rented servers as web proxies.**
 - Rent relatively high speed servers on the Internet.
 - Configure these servers to allow web proxying or Point to Point VPN for all web traffic, and rent a new server from a new provider each month.
 - Although expensive and more technically challenging, this is an excellent method to hide your true location on the Internet.

General Tips

Skilled web server operators may be able to identify your usage patterns or the fact that you're using TOR, dial-up access from a single provider, or popular anonymous proxies. Following these tips can help mitigate these risks:

- Clear browser cookies, Flash cookies, and browser cache after every browser session or when you want to change your online identity. We would recommend using Firefox plugins to make this easier. (see Stealther, <https://addons.mozilla.org/en-US/firefox/addon/1306>).
- It is recommended to change up usage patterns:
 - Operate at different times of day or on different days of the week.
 - Periodically try to use a different web browser or operating system if possible.
 - Periodically change the Agent String that identifies your web browser
 - Be aware of your Internet footprints, examples:

- Referrer field can give away where you found a site (From some forum, Google Site, etc) .
- Disallow Javascript from any site that you do not fully trust. Javascript can be used to defeat some of the anonymity mechanisms mentioned above.
- Disable Flash and ActiveX Plug-ins. They can also be used to defeat some anonymity mechanisms listed above.

Operational Security

Don't use your anonymous session for anything but research. Don't openly discuss tactics or anonymity sites with anyone that is not completely trusted . Don't ever post to news groups or web forums anything that could identify yourself as one who does this type of work.

For more information on anonymity and how operational security can help secure your network and computing resources, and for more information on Linux and Mac-based security, contact VeriSpect Security Services and Consulting – we're experts on securing your data and can create a custom security plan to fit your needs and your budget. More information is available on the web at www.Verispect.net or through email at [info @ verispect.net](mailto:info@verispect.net).