Introduction to Private Surfing

Your IP (Internet Protocol) address is the address or logical location of your computer when connected to the Internet.

You can learn a lot from an IP address… Its everything about you when you are online.

It may not give your exact address but they can tell your geolocation.

Your ISP (Internet Service Provider)… your browser… and sites visited ...all collect information about you and sell it.

They collect information about your browsing habits and target you with IP specific ads..... even your job and health searches information is collected.

Visiting the top 50 websites will install over 3000 tracking files on your computer. Your ISP (Internet Service Provider) can now save and sell your browsing history.

The Government is also tracking usage.

Have you ever done price comparison for flights or cars online and find the price changes as you search, this is all part of the tracking.

This may not trouble some of you but for others it's a major concern.

I believe that everyone should be entitled to surf the net privately.

To that end… I would like to offer some suggestions.

Epic browser and a couple other options that will improve your privacy.

Epic is one of the many browsers you can download for free.

It is a small download that can be installed within minutes.

It can be used in alongside your regular browser.

It provides safer browsing from some things, it is not something that should be used in every situation.

It is a safe browser because it uses a VPN. (Virtual Private Network)

I use the epic browser because it is free, there are many others as well.

Likewise you can also subscribe and pay five to $10 per month for a private VPN service which may or may not throttle back your connection speed as much.

When browsing privately there are three types of safety you can use.

1. Incognito mode.
2. VPN.
3. Proxy.

Incognito mode.... is a privacy feature on some browsers that does not store local data for later retrieval. It also disables storage of flash and standard cookies.

VPN ...Encrypts and tunnels information providing a secure anonymous connection.

Proxy....Is a gateway for masking an IP address and providing misdirection.

Using a VPN. (Virtual Private Network)

To provide anonymity while surfing.

To prevent your ISP spying on what you do online, collecting data and using it to profit from your surfing habits through advertising.

To access country specific data when using YouTube and other programs.

To be more secure in a public Wi-Fi situation.

To manipulate your IP address to make it appear as though you're coming from somewhere else.

To break out of restrictive networks at work or school.

To cloak your VOIP (Voice Over Internet Protocol) phone calls.

To use search engines without having your search logged.

Price quotes from competitors online.

Using a VPN for Facebook,online email,Banking or PayPal may cause some hiccups when it points to a different country.

Torrenting is usually discouraged by most VPNs.

All reputable banking sites use HTTPS (Hyper Text Transfer Protocol Secure) so they should be considered safe.

Do not log onto Google with an account when using Epic, if you are logged into Google Gmail then Google can track your searches.

Now back to the Epic browser.

Epic browser is a chromium-based product .....many other browsers use chromium....I E Google.

Epic has a built-in ad blocker, blocks all ads as well as a host of ad trackers and tracking techniques.

Epic can be set to show the trackers.

Hidden reflex, the browser maker, says it does not send any information about analytics to google.

For maximum privacy when you use epic you can set plug-ins to to be disabled or click to play.

Epic provides good protection against known fingerprinting scripts by simply blocking those scripts. Epic also directly blocks many prevalent finger printing methods including image canvas data, font canvas data, ultrasound signals, audio context, and battery status.

Once downloaded and installed there are several settings you can do to change the security.

Go through settings on browser.

Show what's my IP after setting changes.

Other options are DuckDuckGo which is a stand alone search engine or an add on to your existing browser.

Traffic between your device and DuckDuckGo is encrypted but your ISP can still see and knows the source and destination of your search.

Going beyond the initial search page the rest of the Internet can see your search history and you will be subjected to ads.

While this search engine does offer some privacy it does not delete the search history on your computer, you have to do that. It is still saved in plain text on your computer.

An excerpt from the DuckDuckGo webpage “We also save searches, but again, not in a personally identifiable way, as we do not store IP addresses or unique User agent strings. We use aggregate, non-personal search data to improve things like misspellings.

Similarly, we may add an affiliate code to some eCommerce sites (e.g. Amazon

& eBay) that results in small commissions being paid back to DuckDuckGo when you make purchases at those sites”

Another option might be searchencrypt.com which offers better security than DuckDuckGo.

Explore other options for yourself.

All private search engines still show your IP.

Tor is another browser of a different sort using nodes to direct traffic and is usually more secure and much slower. Tor is usually a browser associated with the dark web.

Privacy add-ons ...added to your browser can access all your browsing searches and almost everything you type in your browser.

There are plenty of free VPNs out there, this is the one I have used with great success.

11 Core Browser Privacy Leaks That Epic Blocks

Address bar and url tracking removed

1. No Address Bar Suggest.

2. No URL Check.

3. Auto-Translate Removed.

4. No URLTracker.

Installation tracking removed

5. Installation-ID Removed.

6. RLZ-Tracking Number Removed.

7. Default Updater Removed.

8. Installation Time stamp Removed

Error tracking removed

9. No Alternate Error Pages.

10. No Navigation Error Suggestions.

11. No Error Reporting.

Epic's default is extreme privacy

No History.

No Web Cache.

No DNS Pre-Fetching.

No DNS Cache.

No Third Party Cookies.

No Rogue Extensions.

No Spell-Check.

No Autofill.

No Password Saving.

No Google Sync..

No Automated "Most Visited Websites".

No Auto-Suggest.

No Alternate Error Pages.

Comprehensive, always-on private browsing mode.

On close, Epic deletes:

Databases.

Shortcuts.

Data related to current tabs.

Extension states.

Topsites.

Web, Flash & Silverlight Cookies.

History.

Visited links.

Pepper Data.

Local storage.

Preferences.

Origin bound certificates.

Current session.

Media cache.

History provider cache.

Favicons.

Indexed DB.

Login data.

Application & DNS cache.

Jumplist Icons Data

Comprehensive Ad & Tracker Blocking

Epic includes built-in protection against thousands of Tracking Scripts, Tracking Cookies & Other Tracking Agents, Ad Networks, Cryptocurrency Mining Scripts (such as Coinhive), dangerous Malvertising, and Third-Party Widgets.

Services such as address bar autofill are done locally in your system so your browsing never goes through our servers.

NO Data Collection. Unlike other tracker blockers & privacy tools, Epic NEVER collects, shares or sells any data from our users!

One-Click Encrypted Proxy

Epic's encrypted proxy when turned on hides your IP address and encrypts your browsing. DNS requests are also routed through the encrypted proxy This protects your browsing history from your ISP, your employer, your government, data collectors, and other network snoops It secures you when you're on public WiFi (WiFi protection). The encrypted proxy also lets you access websites that may be blocked or that offer different content by country such as Netflix, Hulu, YouTube, Pandora, Spotify and others. Please note that plugins may leak your actual IP address. For stronger IP

protection, disable plugins or set them to click-to-play in Epic's settings.

All Epic users now can access our free VPN servers in the US, Canada, Singapore, France, Germany, India, the Netherlands, and the UK.

Referer header data not sent

Unlike other browsers, we don't send data about search terms you've entered to other websites when you click on links from a search engine

Do not track signal always-on

We request every website you visit not to track you. Don't worry, we also actively block them from tracking you!

Fingerprinting Protection

Epic blocks dozens of tracking scripts that fingerprint you. Epic also blocks widely used fingerprinting methods such as accessing image canvas (which is why WhatsApp's desktop app doesn't work in Epic), font canvas, and audiocontext data. Epic blocks ultrasound signals which are sent from websites to be picked up by your mobile phone in order to coordinate tracking (no, we're not making this method up!). More fingerprinting protection is in progress. For maximum fingerprinting protection in Epic's settings, set Plugins to click-to-play or disable them.

Local Address Bar Auto-Complete

Epic auto-complete urls as you type them in its address bar via a database stored locally on your computer. Enjoy both great convenience and great privacy. Other browsers send what you type in the address bar to their servers or analyze your browsing history to make suggestions -- this means they know virtually every search you make and website you visit. We've designed Epic without web-based services for maximum privacy.