How to Improve your Web Browser Security and Privacy

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/how-to-improve-your-web-browser-security-and-privacy/

By Vipin PG | Published March 19, 2020 | Updated January 4, 2026 | Format: Guide | 4 min read

Quick answer

If you have not configured your browser privacy, likely, your browser is not as secure as you would like. From cookies, pop-ups, and location tracking, web browsers are full of loopholes that compromise your security.

If you have not configured your browser privacy, likely, your browser is not as secure as you would like. From cookies, pop-ups, and location tracking, web browsers are full of loopholes that compromise your security. Here are a few ways to improve your web browser security.

Choose a secure browser

Most people use Safari, Chrome, Internet Explorer and Firefox, not in any particular order. However, this does not limit you to these choices, as many types of secure browser alternatives exist. These include GNU IceCAt, Tor, or Iridium browser, among others. Whichever browser you use, rest assured no browser could claim to be 100% safe. However, you can add to a browser's security by locking settings and other measures.

Lockdown your privacy settings

Configuring a browser's privacy setting is crucial in securing your browser. Most browser settings, by default, expose your personal information. It would help if you did the following to lock down your privacy settings.

- Disable re-directions and pop-ups, which are annoying and are potential malware transmitters.
- Disable automatic downloads: These downloads may contain viruses and malware. Ask for prompts before any downloads.
- Check your cookies: Delete the cookies and disable third-party cookie access after a browsing session.
- Restrict access to the microphone, camera, and location: Let your browser prompt permission to access these features.
- Deactivate ActiveX: ActiveX is outdated and is a security risk as well. Deactivate JavaScript and Flash too.
- Enable the 'Do Not Track: This helps in the prevention of websites tracking you, though it is not a guarantee

Keep browser up to date

No browser, however secure, can protect you from the latest malware if the browser is not updated. Each browser is different in its software updates. Here is how to update Chrome, Firefox, and Safari.

- Google Chrome: New updates automatically trigger when the browser closes. To check if it is updated, go to the top left corner of your browser: Chrome then About Google Chrome.
- Firefox: Allows you to turn the automatic updates on or off. Check under Firefox>Preferences

- Apple Safari: Click on the top left corner of your browser and click on: Safari> About Safari. You can also choose to configure the Safari extensions to update automatically.

Use a VPN while browsing

A web browser cannot keep your surfing activities private from your ISP provider, school, or employer, no matter how secure. For this reason, you need to consider getting a VPN extension. A VPN is the safest means of securing your web browser. A VPN does the following:

- Disguising your location and IP address: A VPN hides your IP address , preventing your Internet Service Provider (ISP), websites, and search engines from tracking you.
- Encrypts your data: A VPN scrambles any data sent via the internet. A hacker cannot gain access to your data, which is especially useful over public Wi-Fi systems

Browse using incognito mode

Browsing in incognito or private mode does not give you total privacy, and your IP address and browsing activities can be tracked. However, the private mode only prevents your browser cache, cookies, form data, and web history from being stored after a browsing session. What this means is that the next person to use the browser cannot access your browsing activities.

After you browse using incognito mode, ensure you completely close the browser after using it. Hiding or minimizing will not clear your browsing history.

Install browser security extensions

With most browsers, you can install security extensions to help boost your browser's privacy and security. When establishing such an extension, ensure the extension has the browser's endorsement. Enable updates to ensure the extension is up to date.

Install browser extensions with caution, and do not install security add-ons from untrusted sources. Do not install add-ons from any website that insists that you pre-run the software before accessing the site. It might be malware disguised as an add-on.

A few of the best extensions include:

- HTTPS Everywhere: HTTPS everywhere is compatible with Chrome, Opera and Firefox, and encrypts your data on most major websites. Be wary of sites that do not use HTTPS
- Adblock Plus: This is an open-source extension for Firefox, Chrome, Safari, Internet Explorer, Opera, Edge (beta), Yandex Browser, and Maxton and prevents ads from popping up on your videos and pages.
- Click and Clean: This extension works on Firefox and Chrome and erases all private data such as cache, browsing history, cookies, form data, local storage, and passwords.

Conclusion

You can never be too cautious when it comes to online privacy. You need to take every possible measure to ensure your private data stays secure. When you browse, ensure your browser is protected by using the highlighted steps and use a dose of common sense. If something feels wrong, it probably is. Do due diligence and stay safe.

You may also read

- Use of Virtual Private Network (VPN) in the Real World
- Types of Internet Connections: Speed, Providers, and Accessibility
- Differences Between Google Chrome and Microsoft Chromium-based Edge Browser

References

1. computer.howstuffworks.com - update-internet-browser.htm - https://computer.howstuffworks.com/update-internet-browser.htm