

Forum:[Hack Forums](#)

Thread: [how to stay anonymous \(GUIDE\)](#)

jane - March 27, 2025, 9:11 am

welcome to my tutorial. I figured it was time to give something to the community.

If I'm missing anything please reply below.

Staying anonymous online is increasingly important in today's digital age, where personal data is constantly being collected and shared. Here's a comprehensive tutorial to help you maintain your anonymity while browsing the internet.

1. Use a Virtual Private Network (VPN)

A VPN encrypts your internet connection and masks your IP address, making it difficult for anyone to track your online activity. When choosing a VPN, look for:

- No-log policies
- Strong encryption standards
- A good reputation (check reviews)
- Servers in multiple locations

2. Browse with Privacy-Focused Browsers

Switch to browsers that prioritize user privacy. Some popular choices include:

- Tor Browser: Routes your connection through multiple servers to obscure your original IP address. It also blocks trackers.
- Brave: Automatically blocks ads and trackers and offers a built-in Tor option for anonymous browsing.
- Firefox: With privacy settings adjusted (e.g., Enhanced Tracking Protection), it can provide a good level of anonymity.

3. Use Search Engines that Don't Track You

Opt for search engines that prioritize privacy, such as:

- DuckDuckGo: Does not track or store user information.
- Startpage: Combines Google search results with privacy protection.
- Qwant: A European search engine that respects privacy.

4. Adjust Your Privacy Settings

Review and modify the privacy settings on your devices and accounts:

- Social Media: Limit what you share publicly and adjust your privacy settings to restrict who can see your information.
- Browser: Disable third-party cookies and tracking features.
- Mobile Devices: Turn off location services and limit app permissions.

5. Be Cautious with Public Wi-Fi

Public Wi-Fi networks can be unsecured and expose you to risk. To stay safe:

- Avoid accessing sensitive information (like banking) on public networks.
- Use a VPN when connecting to public Wi-Fi.
- Consider using mobile data for sensitive transactions.

6. Use Anonymous Email Services

Consider using email services that don't require personal information, such as:

- ProtonMail: End-to-end encryption and no personal data required for sign-up.
- Tutanota: Focuses on privacy and security without tracking users.

7. Limit Personal Information Sharing

Be mindful of the information you share online. Avoid using your real name, address, or phone number on websites. Use pseudonyms where possible.

8. Use Secure and Encrypted Messaging Apps

Switch to messaging apps that prioritize security and privacy, such as:

- Signal: Offers end-to-end encryption and doesn't store your data.
- Telegram: Provides secret chats with end-to-end encryption.

9. Regularly Clear Your Data

Make it a habit to clear your browsing history, cookies, and cache regularly. This minimizes the amount of data available to trackers.

10. Stay Informed About Phishing and Scams

Be cautious of unsolicited emails or messages that ask for personal information. Always verify the identity of the sender before engaging.

Conclusion

Maintaining anonymity online requires a combination of tools and practices. By implementing these strategies, you can significantly enhance your online privacy and reduce the likelihood of your personal information being exposed. Always stay vigilant and keep yourself updated on

pein - March 27, 2025, 4:12 pm
nice.

using a DNS service can reset the ISP blocks and do quicker connections. Cloudflare 1.1.1.1 and gOOGLE 8.8.8.8 or 8.8.4.4 or the mix of two is good

cloudflare has a new program/app that seems to be pretty good, fixed my wifi on trains, but my trial expired. honestly expensive vpns do the same mostly, I don't really need anonymous access, there are free ones when I do. I had issues with vpn servers being far away and ruined my connection.

best browsers in my opinion: Slimjet and Vivaldi

I like chromium that is not chrome. even the barebone chromium or comodo is ok.

brave and opera have some modifications, same for edge, not all extensions work on them.

best adblocker: ublock origins. didn't load in the ads so it saves ram, others generally make it transparent only so you click and still redirects you. on mobile you can get 1dm, it's premium but has filter lists like ublock. works mostly, but they make new ads too often on the sites I use so maybe only in older sites. honestly vivaldi opens every popup on new page and it's easier to kill a tab than an ad.

intuition - March 31, 2025, 2:43 pm
Well, thanks I guess - haha.

Shrdw - April 5, 2025, 8:49 pm

I do have a question about the recommendation to use signal and telegram both currently have flaws after more recent disclosures.

It would be amazing if you could break down how using these services safely can be done because nothing is absolute. Assuming we are talking basics to intermediate disclosing anything that falls under, Personal identifiable information.

I understand enough when gathering information but i am not being targeted nor have i had anyone target me directly thus far at least.

You seem to be more well versed in this topic so i was curious how to put theory into practice.

Example, by the way i type you can tell i am at minimum a fluent in English and use US based phrasing vs EN_UK etc. Hopefully this explains more about the question since you said people could ask questions.