

# Forum:[Hack Forums](#)

Thread: [ANONYMITY - A Beginner's Guide to Staying Safe Online](#)

VKNS - July 25, 2023, 2:11 pm

This guide is aimed towards beginners looking to keep their personal information safe. If you're up to no good and expecting this thread to save you, look elsewhere.

In the digital age, privacy and online security have become paramount concerns. Maintaining anonymity online is crucial for safeguarding personal data, protecting against identity theft, and preserving your freedom of expression. This advanced tutorial will provide you with a comprehensive guide on how to stay anonymous online. We'll cover a wide range of strategies, tools, and best practices to help you maximize your online privacy.

Before diving into specific techniques, it's essential to understand what online anonymity entails. Anonymity means preventing others from identifying you or tracing your online activities back to your real-world identity. Achieving a high level of anonymity is vital, but it's essential to acknowledge that achieving absolute anonymity is nearly impossible due to the interconnected nature of the internet. With that in mind, let's explore various methods and approaches to bolster your online privacy.

## Use a VPN

A VPN encrypts your internet traffic and routes it through servers in different locations, hiding your IP address and making it harder for anyone to track your online activities. This added layer of security ensures that your data is not intercepted by hackers or malicious entities. Choose a reputable VPN service that has a no-logs policy and strong encryption protocols for maximum effectiveness.

I recommend [censored]

[censored] lies outside of the jurisdiction of the 5 eyes, 9 eyes and 14 eyes organisations (read more [here](#)).

\$3.49 Monthly

Dynamic IP Addresses as standard but can pay for dedicated address.

Comes with a Kill Switch, Split Tunneling, Camouflage Mode, Multi-hop.

Is compatible with Netflix.

If you'd like my referral link, please PM me and I'll happily give it to you.

## Use Tor Browser

Tor (The Onion Router) is a decentralized network that anonymizes your web traffic by bouncing it through multiple relays, making it extremely challenging to trace your online activities. Tor Browser is an excellent option for accessing the internet anonymously, but keep in mind that some websites may block Tor exit nodes. To counter this limitation, you can configure Tor bridges or use pluggable transports, you can read more about TOR Bridges [here](#).

## Secure DNS

The Domain Name System (DNS) is used to translate domain names into IP addresses, allowing you to access websites. However, your internet service provider (ISP) can log your DNS requests, potentially compromising your privacy. To prevent this, use a trusted and privacy-focused DNS resolver, such as Cloudflare's 1.1.1.1 or Quad9, which don't log user data.

## Encrypted Messaging Apps

Encrypted Messaging Apps: Choose end-to-end encrypted messaging apps like Signal or Telegram for secure communication with others, ensuring your conversations remain private. These apps prevent anyone, including service providers, from accessing your messages in a readable format.

## Anonymous Email

While using traditional email services can reveal your identity, consider using anonymous email services that don't require personal information during signup. ProtonMail and Tutanota are popular choices that offer end-to-end encryption for additional security. There is typically a cost to Anonymous email services, but if you care, it's worth the investment. Tutanota as mentioned earlier is a great free alternative, but they're very strict on their one-account-per-user policy.

## Secure Voice and Video

For anonymous voice and video calls, you can use apps like [Signal](#), [Wire](#), or [Jitsi Meet](#), which prioritize user privacy and security.

[XMPP](#) is also an option worth noting, but your security is only as sound as your provider. Pick a bad provider and you may as well not be using it at all!

## Secure Voice and Video

Install privacy-enhancing browser extensions such as [uBlock Origin](#), [Privacy Badger](#), [HTTPS Everywhere](#), and [Decentraley](#)es to block ads, trackers, and enhance your online privacy. These extensions protect you from various online tracking methods and safeguard your browsing experience.

## Avoid Personal Information

This one sounds obvious, but people seem to give up all sense of reason and personal security when signing up to social media. Refrain from providing unnecessary personal information when browsing, especially on social media platforms. The less data you provide, the harder it becomes for others to piece together your identity.

## Use a VM for Sensitive Browsing

For added security, you can run your more... sensitive browsing sessions inside a virtual machine (VM). This isolates your browsing environment from your host system and minimizes the risk of leaking identifiable information.

## Privacy-focused Search Engines

Instead of mainstream search engines, opt for privacy-focused ones like DuckDuckGo or Startpage that don't track your searches. These search engines prioritize user privacy by not storing search queries or personal information.

## Privacy settings and Social Media

Consider using Pseudonyms instead of your real name for social media; your friends will understand when you give them a bogus name. Any separation between your real identity and your online identity is a bonus. Personally, I abused a script a few years ago that has allowed me to have no surname on a particular social media platform; as a result - it's very difficult for people to find and add my account.

Adjust your privacy settings on social media to restrict access to your personal information and posts. Limit the information visible to the public and only allow trusted connections to see more details.

## Clear your data on a regular basis

Regularly Delete Data: Periodically delete cookies, browser history, and stored passwords to minimize your digital footprint. Clearing these traces reduces the chances of being tracked based on your browsing history. Setting alarms or even automating this is a good shout.

## Avoid Public and Open Wi-Fi

Public Wi-Fi networks can be insecure, so try to use trusted networks or a VPN when connecting to the internet on the go. Public Wi-Fi hotspots are prime targets for cybercriminals looking to intercept data. I've tried ARP spoofing and pushing a MITM attack on my neighbours in a bad mood; even something as innocuous as your neighbour's Wi-Fi could drop you in some serious doo-doo.

## Use Cryptocurrency where available

Consider using cryptocurrencies like Bitcoin or Monero for online transactions, as they offer a higher degree of anonymity compared to traditional payment methods. Keep in mind that while cryptocurrencies offer some level of privacy, they are not entirely anonymous. Practice good security measures, such as using new addresses for each transaction and avoiding publicizing your wallet addresses.

## Disposable Payment Methods

Some services offer virtual credit cards or one-time use cards that allow you to make online payments without revealing your real credit card information. These disposable payment methods add an extra layer of security when conducting online transactions.

## Secure File Storage and Sharing

Choose cloud storage services that offer end-to-end encryption to protect your files from unauthorized access. Services like [pCloud](#) and [Sync.com](#) provide client-side encryption, ensuring

that only you can decrypt your files.

### Secure Files before Sharing

When sharing sensitive files, use password-protected ZIP archives or encrypted file-sharing platforms. Tools like [VeraCrypt](#) and [Cryptomator](#) allow you to create secure containers for your files and folders.

Thank you for reading.

I hope you learned something; comments and criticism welcome.

Stay safe!

**Giga** - July 25, 2023, 2:30 pm

Very HQ post and helpful for those wanting to learn about staying anonymous. I'd recommend maybe adding a small portion about PGP even though it has limited use-cases.

**uhtred** - July 25, 2023, 2:31 pm

Great Read, implemented some things I wasn't aware of yet.

**VKNS** - July 25, 2023, 2:58 pm

Thanks for the feedback guys, appreciate it!

More to come!

(Jul 25, 2023 02:31 PM)uhtred Wrote: [\[CITE\]](#) Great Read, implemented some things I wasn't aware of yet.

Anything in particular that stood out to you?

**PalCobra** - July 25, 2023, 3:24 pm

This is the first time I have knew about the eyes and I am so glad that [censored] is out of them because it is my favorite's one.

I must reread it thoroughly.

Big like VKNS

**VKNS** - July 25, 2023, 3:30 pm

(Jul 25, 2023 03:24 PM)PalCobra Wrote: [\[CITE\]](#) This is the first time I have knew about the eyes and I am so glad that [censored] is out of them because it is my favorite's one.

I must reread it thoroughly.

Big like VKNS

Thanks!

Glad you like the thread.

5 Eyes, 9 Eyes and 14 Eyes is something that everyone should know about if they care about their privacy.

**PalCobra** - July 26, 2023, 2:43 pm

(Jul 25, 2023 03:30 PM)VKNS Wrote: [\[CITE\]](#) Thanks!

Glad you like the thread.

5 Eyes, 9 Eyes and 14 Eyes is something that everyone should know about if they care about their privacy.

I couldn't agree more. Although I usually read about privacy, this is the first time I find an article talks about this point.

Thank you again VKNS

**Transporter007** - July 28, 2023, 3:35 am

Nice post.

Keep up the good work!

**F101W** - July 28, 2023, 11:20 am

Thank you man for guiding! Actually a high quality post. But why didn't write anything about proxies and services that provide them?

**F101W** - July 31, 2023, 4:45 am

helpful guide thank you!

**VKNS** - July 31, 2023, 5:10 am

(Jul 31, 2023 04:28 AM)Focus Broken Wrote: [\[CITE\]](#) Thanks for the guide! You can also add <https://silent.link/> for burner e-sims.

SimpleX is the top tier version for this - <https://simplex.chat/>

Wasabi Wallet allows your Bitcoin transactions to become entirely anonymous, ensuring no two addresses you control are ever linked together:

<https://wasabiwallet.io/>

<https://hackforums.net/blog/Wasabi-Wallet-Guide>

Thanks for the contributions man, I'll add them in as soon as ?

**itsok** - July 31, 2023, 5:17 pm

I'm surprised to see so many folks agreeing with this guide.

You should never use a VPN if you're attempting to be anonymous. You're just giving your traffic to someone else, whomust comply with the DOJ, or they themselves risk investigation. You're better off at a library on a SOCKS5 proxy.

Oh, and you're giving your DNS traffic to cloudflare? You're boned. Quad9 is a much better approach (DNSSEC + ECS)

> Clear your data on a regular basis

No. Do not record data, if you find yourself at receiving end of an investigation deleting ('clearing') data is destruction of evidence; but if it's never recorded, there is no evidence to destruct.

> Avoid Public / open WiFi

"This advanced tutorial will provide you with..."

There is some decent information here, but I would file this under an introduction. This isn't defense in depth – it's the beginnings, which is wonderful, but just something I would consider anything beyond 101.

**VKNS** - July 31, 2023, 5:32 pm

(Jul 31, 2023 05:17 PM)itsok Wrote: [\[CITE\]](#) I'm surprised to see so many folks agreeing with this guide.

You should never use a VPN if you're attempting to be anonymous. You're just giving your traffic to someone else, who must comply with the DOJ, or they themselves risk investigation. You're better off at a library on a SOCKS5 proxy.

Oh, and you're giving your DNS traffic to cloudflare? You're boned. Quad9 is a much better approach (DNSSEC + ECS)

> Clear your data on a regular basis

No. Do not record data, if you find yourself at receiving end of an investigation deleting ('clearing') data is destruction of evidence; but if it's never recorded, there is no evidence to destruct.

> Avoid Public / open WiFi

"This advanced tutorial will provide you with..."

There is some decent information here, but I would file this under an introduction. This isn't defense in depth – it's the beginnings, which is wonderful, but just something I would consider anything beyond 101.

At this point I'd like to point out that this guide is for the GENERAL PUBLIC.

Thanks for trashing the thread, though.

**fahrenheit451** - March 9, 2024, 1:25 pm

Good guide thanks :)

**rask4l** - March 9, 2024, 2:16 pm

Pretty brief and well thought out guide on anonymity. Thanks ?

**Crexy** - March 10, 2024, 2:36 pm

atp take my monehhhh

**hlittle** - March 10, 2024, 10:14 pm

Thanks for all the info