

Forum:[Hack Forums](#)

Thread: [\[AIQ\] How to stay anonymous online and not get doxxed](#)

Bashe - December 20, 2024, 2:20 am

AI Quote:

Comprehensive Tutorial: How to Stay Anonymous Online and Avoid Being Doxxed

In today's connected world, protecting your online identity and privacy is crucial. Doxxing (the exposure of personal information without consent) can lead to severe consequences, including harassment or identity theft. This guide provides detailed steps to help you stay anonymous online and safeguard your personal information.

1. Use Strong and Secure Passwords

- Create Unique Passwords for Every Account:

Use a password manager (e.g., LastPass, Bitwarden) to generate and store unique passwords for each account.

- Use Passphrases Instead of Passwords:

Example: BluePineapple!2023#Secure is harder to crack than a single word.

- Enable Two-Factor Authentication (2FA):

Add an extra layer of security by requiring a second verification step.

2. Mask Your IP Address

- Use a Virtual Private Network (VPN):

A VPN encrypts your internet traffic and hides your real IP address. Trusted VPNs include:

- [censored]
- ExpressVPN
- ProtonVPN (offers a free plan)
- Avoid Public Wi-Fi:

If you must use public Wi-Fi, always connect through a VPN.

- Consider Using Tor:

The Tor browser routes your internet traffic through multiple servers, making it extremely hard to trace your IP address.

3. Manage Your Digital Footprint

- Audit Your Online Presence:

Search for your name, phone number, or email on search engines to see what information is publicly available.

- Remove Personal Information:

Request removal of your data from people-search websites like Whitepages, Spokeo, and similar directories. Services like DeleteMe can help automate this process.

- Be Selective with Social Media:
- Avoid using your real name.
- Set profiles to private.
- Limit sharing personal details like location, family connections, or workplace.
- Use Disposable Accounts:

Create burner email accounts for signing up on websites.

4. Use Privacy-Focused Tools

- Email:
 - Use secure, anonymous email providers like ProtonMail or Tutanota.
 - Avoid using your real name when creating an account.
- Messaging:
 - Use encrypted messaging apps like Signal or Telegram.
- Web Browsing:
 - Use privacy-focused browsers like Brave or Tor.
 - Avoid using Google. Use DuckDuckGo or Startpage for searches.

5. Protect Your Social Media Accounts

- Review Privacy Settings:

On platforms like Facebook, Twitter, and Instagram:

- Restrict who can view your posts and profile.
- Disable location tagging.
- Avoid Linking Accounts:

Do not connect multiple social media accounts or use the same username across platforms.

- Be Cautious with Photos:

Remove metadata (e.g., location) from photos before uploading. Tools like ExifCleaner can help.

6. Use Pseudonyms and Avatars

- Avoid Using Real Names:

Use pseudonyms for online accounts, especially for forums, gaming platforms, and social media.

- Separate Identities:

Create distinct usernames and email addresses for work, personal, and anonymous online activities.

7. Encrypt Your Communication and Data

- Encrypt Your Files:

Use tools like VeraCrypt to encrypt sensitive files on your computer.

- Secure Your Devices:
 - Enable full-disk encryption (e.g., BitLocker for Windows, FileVault for macOS).
 - Use strong screen lock passwords or biometrics.
- Use Secure Cloud Storage:

Choose services with end-to-end encryption like Tresorit or Sync.com.

8. Avoid Phishing and Social Engineering

- Verify Links and Emails:

Do not click on suspicious links or download attachments from unknown senders.

- Be Skeptical:

If someone online asks for personal information, verify their identity first.

- Enable Anti-Phishing Tools: