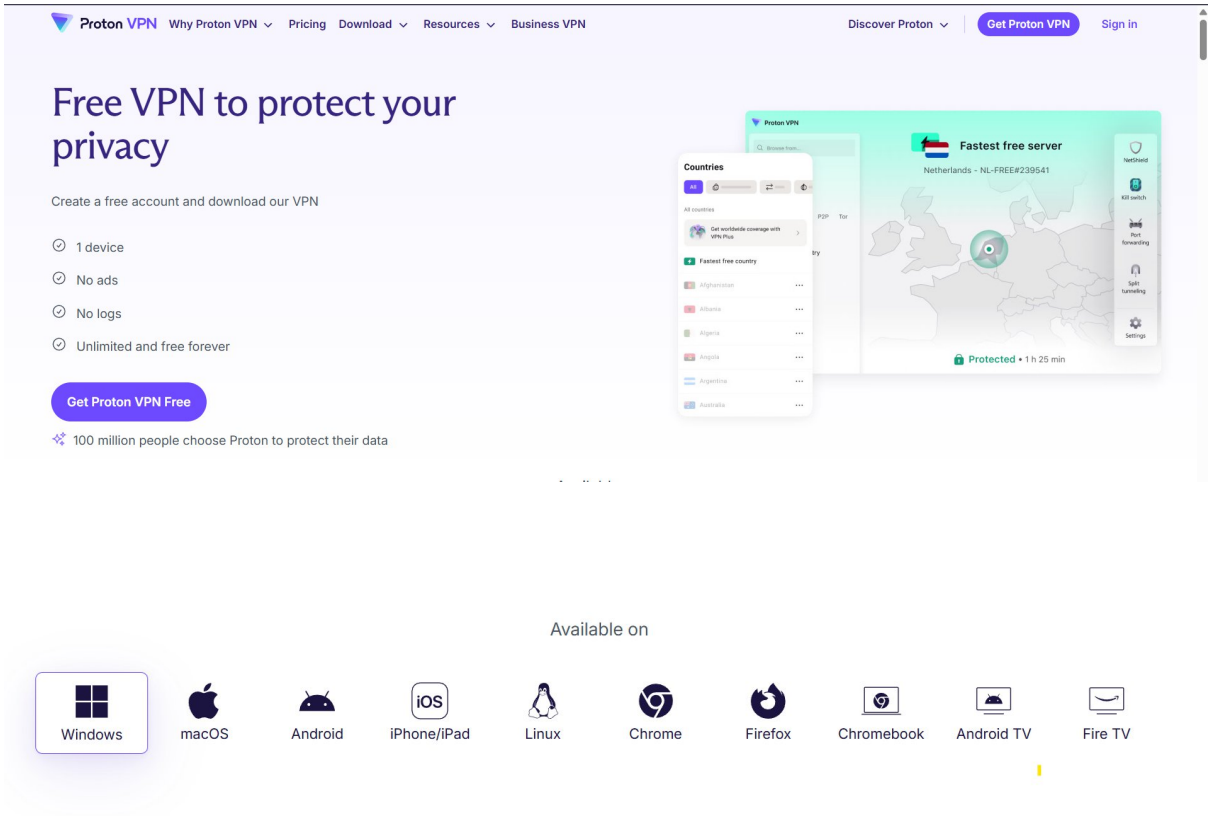
Identify and Remove Suspicious Browser Extensions

1. **Choose a Reputable Free VPN Service and Sign Up :**

To select a reputable free VPN, opt for one with a strong track record for privacy and no-logs policies, such as ProtonVPN (free tier available) or Windscribe. Avoid shady free VPNs that may sell data or have malware.

- Visit the official website (e.g., **protonvpn.com/free-vpn**).
- Click "Sign Up" or "Get Free" and create an account using an email address.
- Verify your email if required, and note any free plan limitations (e.g., data caps or server restrictions).
- Complete the signup process; no payment is needed for free tiers**.**



2. Download and Install the VPN Client :

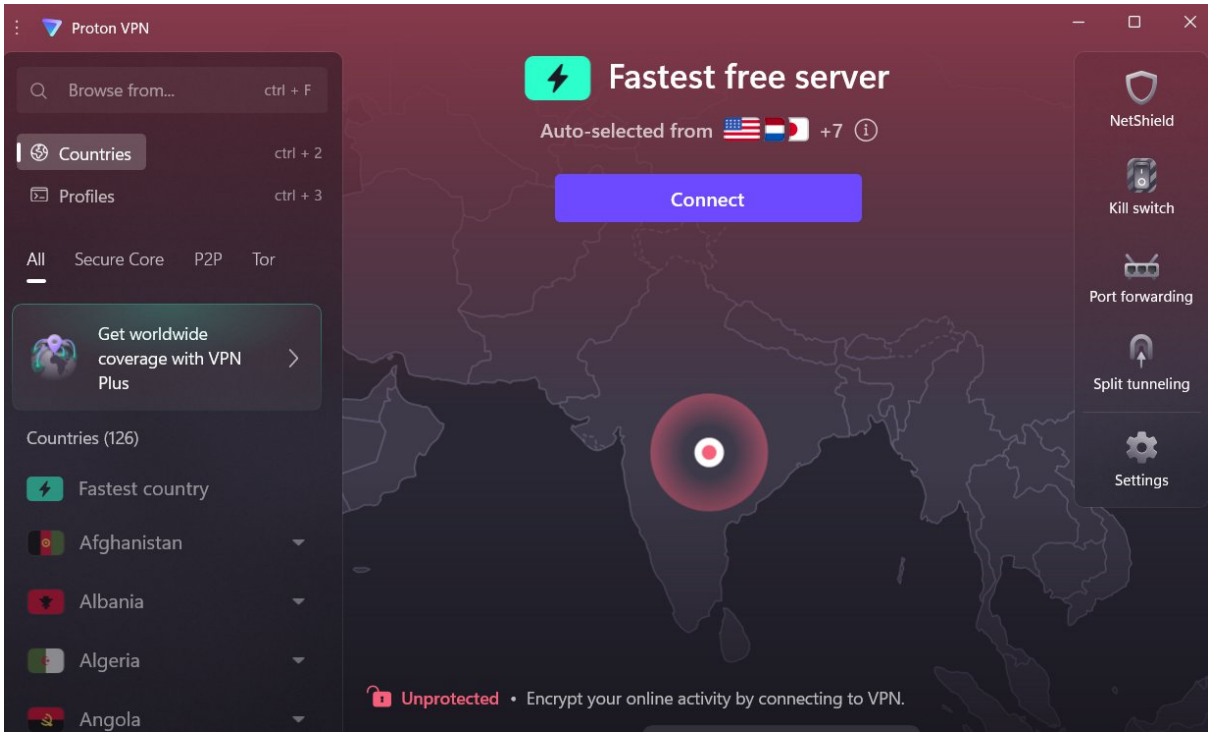
Once signed up, download the official app from the VPN provider's website (not third-party sites to avoid malware).

For ProtonVPN: Download the app for your device (Windows, macOS, Android, iOS, etc.) from protonvpn.com/downloads. Install it by running the installer and following prompts—it's straightforward and doesn't require admin rights on most systems.

Installation tips: Ensure your device is updated and has antivirus software running. Free VPNs like ProtonVPN are lightweight and shouldn't slow your system much.

Finally ProtonVpn is downloaded.

3. Connect to a VPN Server (Choose Closest or Any Location)



- Select a server: For best performance, choose one closest to your physical location (e.g., if you're in the US, pick a US server) to minimize latency.

ProtonVPN has servers in multiple countries; start with a free one like Switzerland or the Netherlands.

- Connect: Click the "Connect" button. The app will establish an encrypted tunnel. This might take 10-30 seconds. You'll see a connected status with a new IP address displayed.

4. Verify Your IP Address Has Changed (Use whatismyipaddress.com)

To confirm the VPN is working:

- Disconnect from any existing network if needed, then visit whatismyipaddress.com in your browser.
- Note your original IP (e.g., something like 192.168.x.x or a public IP from your ISP).
- With the VPN connected, refresh the site. Your IP should now show the server's location (e.g., a Swiss IP if connected to Switzerland). If it hasn't changed, try a different server or check for app errors.
- Pro tip: Use tools like ipleak.net for more thorough checks (e.g., DNS leaks, which could expose your real location).

Connected by another country.

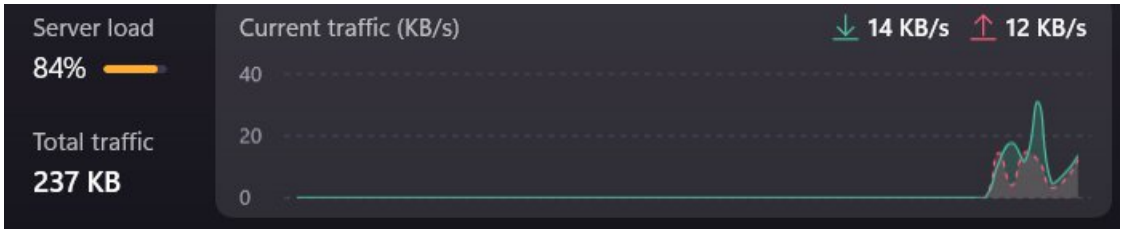
5. Browse a Website to Confirm Traffic Is Encrypted

Encryption ensures your data is scrambled and secure from eavesdroppers.

- With the VPN connected, visit a site like **https://www.cloudflare.com/ssl/encrypted-**

snooping/ or simply browse any HTTPS site (look for the padlock icon in the address bar).

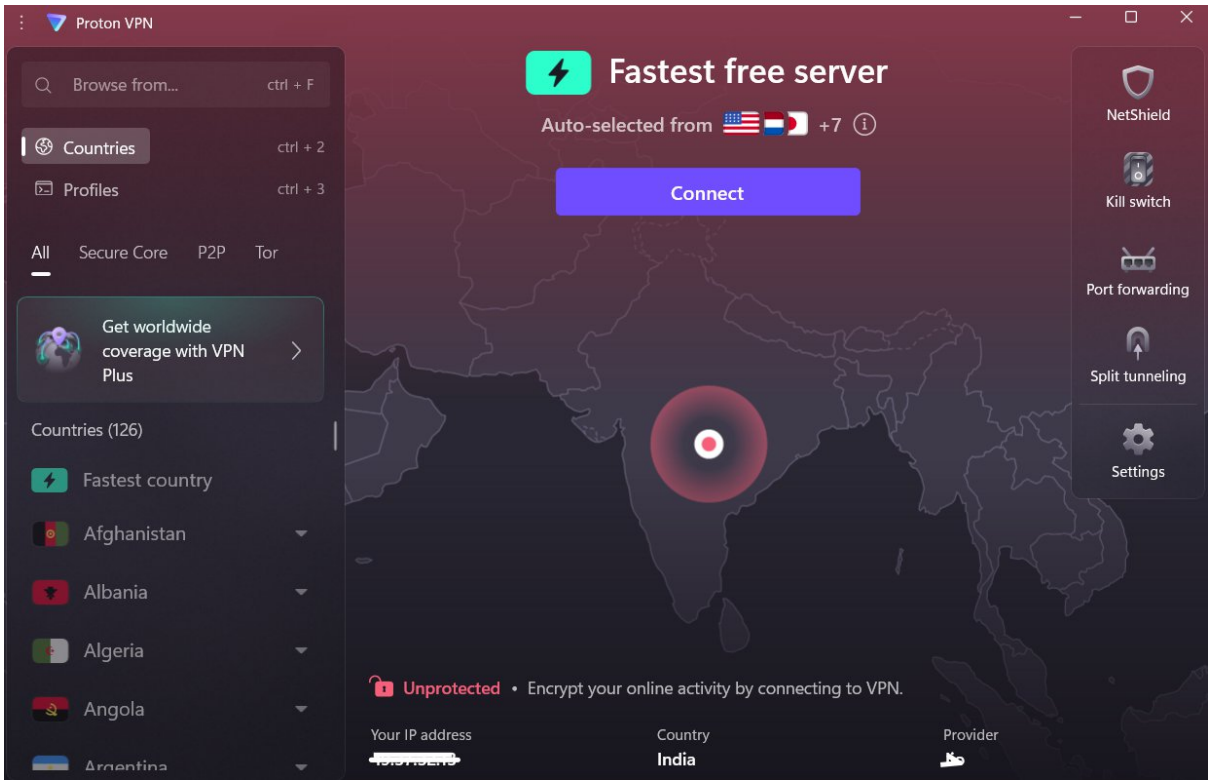
- To test deeper: Use Wireshark (a free network analyzer) to monitor traffic—without VPN, you'd see readable data; with VPN, it should be gibberish. Alternatively, check for WebRTC leaks on browserleaks.com (disable WebRTC in your browser settings if needed).
- Confirmation: If the site loads normally and no leaks are detected, your traffic is encrypted. Note any speed differences (VPNs can slow things down due to encryption overhead).



6. **Disconnect VPN and Compare Browsing Speed and IP**
    - Disconnect: In the VPN app, click "Disconnect." Your IP should revert to your original one (verify on whatismyipaddress.com).
    - Compare speeds: Use a tool like speedtest.net to test download/upload speeds with and

without VPN. Free VPNs often reduce speeds by 20-50% due to shared servers and data limits.

- IP comparison: Your real IP should return, confirming the VPN masked it effectively. If speeds are drastically slower, consider a paid VPN for unlimited bandwidth.



Disconnected the vpn.

7. Research VPN Encryption and Privacy Features

VPNs use protocols like OpenVPN, WireGuard, or IKEv2 for encryption. Research via official docs or sites like vpnMentor.com:

- Encryption: Most use AES-256 (military-grade), which scrambles data. ProtonVPN uses this with perfect forward secrecy.
- Privacy Features: Look for no-logs policies (audited to ensure no data storage), kill switches (cuts internet if VPN drops), and DNS leak protection. Free tiers might lack advanced features like obfuscation (hides VPN use from ISPs).
- Key resources: Read the VPN's privacy policy, check for independent reviews on PCMag or TechRadar, and understand risks like free VPNs potentially logging data for monetization.

8. Summary on VPN Benefits and Limitations

VPNs (Virtual Private Networks) create a secure, encrypted tunnel between your device and the internet, routing traffic through a remote server to mask your IP and enhance privacy. Here's a balanced overview:

Benefits:

- ***Privacy and Anonymity***: Hides your IP address, making it harder for ISPs, websites, or hackers to track your online activity. Useful for bypassing geo-restrictions (e.g., accessing region-locked content) or public Wi-Fi security.

- ***Security***: Encrypts data, protecting against eavesdropping, man-in-the-middle attacks, and data theft. Features like kill switches prevent accidental exposure.

- ***Bypassing Censorship***: In restrictive regions, VPNs can access blocked sites by routing through freer countries.

- ***Ease of Use:*** Simple apps make it accessible for non-tech users, with protocols like WireGuard offering fast, reliable connections.

Limitations:

- ***Speed and Performance***: Encryption adds latency; free VPNs often have slower speeds,

data caps (e.g., 500MB-10GB/month), and fewer servers, leading to congestion.

- ***Trust Issues***: Not all VPNs are trustworthy—free ones may log data, inject ads, or sell user info. Even reputable ones can be compelled by courts to share data in some jurisdictions.

- ***Legal and Compatibility Concerns:*** VPNs don't make illegal activities legal; they can be blocked by services like Netflix. Some apps/websites detect and restrict VPN traffic. Compatibility varies (e.g., not all routers support VPNs).

- ***Cost of Free Tiers:*** Limited features; for unlimited use, paid options (e.g., ProtonVPN paid at $5/month) are better. Free VPNs might compromise on privacy for revenue.

- ***Not a Complete Solution***: VPNs don't protect against malware, phishing, or device-level tracking. Combine with antivirus, HTTPS, and ad blockers for full security.