Working and understanding VPN

---

1. Choose a Reputable Free VPN Service and Sign Up

Recommended VPN: Proton VPN Free

Reason: Proton VPN is widely regarded as a trustworthy free VPN due to its unlimited data, strong encryption, no-logs policy, and open-source apps audited by third parties. It's based in Switzerland, which has robust privacy laws.

Steps to Sign Up:

- Visit **ProtonVPN.com**.

- Click on "Get Proton VPN Free" to create an account.

- Provide an email address or use guest mode (available on iOS/Android in 2025). No personal information is required for the free plan.

- Confirm your account via email (if required) and log in.

Note: The free plan limits you to servers in five countries (Japan, Netherlands, Poland, Romania, USA) and one device connection.

---

2. Download and Install the VPN Client

Steps:

- Go to **ProtonVPN.com** and navigate to the "Downloads" section.

- Select the appropriate client for your device (Windows, macOS, Linux, Android, or iOS). Proton VPN supports all major platforms.

- Download the installer file.

- Run the installer and follow the on-screen instructions to complete installation. For example:

  - On Windows: Double-click the .exe file, accept the license agreement, and install.

  - On Android/iOS: Download from Google Play or the App Store.

- Log in using your Proton VPN credentials.

Security Tip: Ensure you download the client directly from the official Proton VPN website to avoid malicious or fake apps.

---

3. Connect to a VPN Server

Steps:

- Open the Proton VPN client.

- Log in and select the "Quick Connect" option, which automatically connects to the fastest available server (often the closest geographically for better speed).

- Alternatively, manually select a server from the available free locations (e.g., USA, Netherlands). The client displays server locations in a list or map view.

- Click "Connect." The app will confirm when the connection is established.

Recommendation: Choose a server closest to your physical location to minimize latency. For example, if you're in the USA, select a US server.

---

4. Verify Your IP Address Has Changed

Steps:

- Open a browser and visit **whatismyipaddress.com**.

- Note your original IP address and location before connecting the VPN (if not already done).

- After connecting to the VPN, refresh the page or revisit **whatismyipaddress.com**.

- Confirm that the displayed IP address and location match the VPN server's location (e.g., Netherlands if you chose a Dutch server) and differ from your original IP.

Expected Outcome: The website should show an IP address assigned by Proton VPN, not your ISP's IP. This confirms the VPN is masking your real IP.

---

5. Browse a Website to Confirm Traffic Is Encrypted

Steps:

- While connected to the VPN, visit a website (e.g., **www.google.com** or **www.bbc.com**).

- Look for the padlock icon in the browser's address bar, indicating the site uses HTTPS, which ensures end-to-end encryption when combined with the VPN's encryption.

- To further verify encryption:

  - Proton VPN uses AES-256 encryption (or ChaCha20 for WireGuard) for its free tier, ensuring your traffic is encrypted between your device and the VPN server.

  - You can use a tool like **ipleak.net** to check for DNS or WebRTC leaks. No leaks should be detected with Proton VPN's kill switch and leak protection enabled.

Confirmation: If the website loads normally and no leaks are detected, your traffic is encrypted and routed through the VPN.

---

6. Disconnect VPN and Compare Browsing Speed and IP

Steps:

- Disconnect from the VPN by opening the Proton VPN client and clicking "Disconnect."

- Revisit **whatismyipaddress.com** to confirm your IP address reverts to your ISP's original IP and location.

- Test browsing speed:

  - Visit a website (e.g., **www.bbc.com**) or run a speed test using **speedtest.net** while disconnected.

  - Reconnect to the VPN and repeat the test on the same website or **speedtest.net**.

- Compare the results:

  - **IP Address**: Without VPN, it should show your real IP; with VPN, it should show the VPN server's IP.

  - **Speed**: Expect a slight speed reduction with the VPN due to encryption overhead. Proton VPN's free plan averaged a 16% download speed loss in 2025 tests, which is better than many free VPNs.

---

7. Research VPN Encryption and Privacy Features

Proton VPN Free Encryption and Privacy Features (based on recent data):

- **Encryption**:

  - Uses **AES-256** (OpenVPN/IKEv2) or **ChaCha20** (WireGuard) encryption, both industry-standard and virtually uncrackable. AES-256 is used by banks and militaries.

  - Supports **Perfect Forward Secrecy**, ensuring new encryption keys are generated for each session, protecting past sessions if a key is compromised.

- **Protocols**:

  - **OpenVPN**: Secure, open-source, widely trusted for privacy.

  - **WireGuard**: Faster, modern protocol with ChaCha20 encryption, optimized for performance.

- **Stealth Protocol**: Designed to bypass censorship (e.g., in countries like China), though availability may be limited on the free plan.

- **Privacy Features**:

  - **No-Logs Policy**: Independently audited (last in 2023), ensuring no user activity, IP addresses, or browsing history is stored.

  - **Kill Switch**: Prevents data leaks by cutting internet access if the VPN disconnects. Available on all platforms, including free tier.

  - **DNS Leak Protection**: Ensures DNS requests are routed through the VPN, preventing ISP tracking.

  - **Open-Source Apps**: Code is publicly available for inspection, increasing transparency.

  - **Swiss Jurisdiction**: Based in Switzerland, which has no mandatory data retention laws, enhancing privacy.

- **Additional Notes**:

  - Proton VPN's free plan does not include advanced features like **multi-hop** (routing through two servers) or **NetShield** (ad/malware blocker), which are available in paid plans.

  - Recent research indicates iOS devices may be vulnerable to VPN leaks due to Apple's system design, though enabling the kill switch and using OpenVPN can mitigate this.

General VPN Encryption and Privacy Insights:

- Most reputable VPNs use **AES-256** or **ChaCha20** for encryption, with protocols like **OpenVPN**, **WireGuard**, or **IKEv2** for secure data transmission.

- Privacy depends on a **no-logs policy**, ideally verified by independent audits, and a jurisdiction outside surveillance alliances like Five Eyes.

- Features like **split tunneling** (routing specific apps through the VPN) and **obfuscation** (hiding VPN usage) enhance flexibility and access in restrictive regions.

---

8. Summary of VPN Benefits and Limitations

Benefits of Using a VPN:

1. **Enhanced Privacy**:

   - Masks your IP address, preventing ISPs, websites, or hackers from tracking your location and online activities.

   - No-logs policies (e.g., Proton VPN's audited policy) ensure your browsing history isn't stored.

2. **Data Security**:

   - Encrypts traffic with AES-256 or ChaCha20, protecting sensitive data (e.g., passwords, financial details) on public Wi-Fi from man-in-the-middle attacks.

3. **Bypass Geo-Restrictions**:

   - Access content restricted by region (e.g., streaming services like Netflix, though Proton VPN's free plan has limited streaming support).

4. **Prevent ISP Throttling**:

   - Hides your activity from ISPs, preventing speed throttling during streaming or gaming.

5. **Censorship Circumvention**:

   - Obfuscated servers (limited in free plans) can bypass firewalls in countries like China.

6. **Anonymity for Sensitive Tasks**:

   - Useful for privacy-critical professions (e.g., journalists) when combined with other tools like Tor.

Limitations of Using a VPN:

1. **Speed Reduction**:

   - Encryption and server routing can reduce speeds. Proton VPN's free plan averages a 16% download speed loss, and free servers may be congested.

2. **Limited Features in Free Plans**:

   - Proton VPN Free restricts users to five server locations, one device connection, and no manual server selection or advanced features like multi-hop or ad-blocking.

3. **Streaming Restrictions**:

- Free plans often don't support streaming services like Netflix due to server limitations. Paid plans are better for this.

4. **Not Complete Anonymity**:

   - VPNs hide IP addresses but don't prevent tracking via cookies, browser fingerprinting, or account logins.

5. **iOS Vulnerabilities**:

   - iOS devices may leak data due to Apple's VPN handling, requiring workarounds like enabling Always On VPN or using OpenVPN.

6. **Legal and Regional Issues**:

   - VPNs are banned or restricted in countries like China, Russia, and Iran. Free VPNs may not reliably bypass these blocks.

7. **Trust in Provider**:

   - You rely on the VPN provider to uphold its no-logs policy. Free VPNs may sell data or show ads, though Proton VPN is an exception

Conclusion:

Proton VPN Free is a reliable choice for basic privacy and security, offering unlimited data and strong encryption without ads. It's ideal for secure browsing on public Wi-Fi or masking your IP for general use. However, its free plan is limited by server locations, device connections, and lack of streaming support. For advanced features like streaming, torrenting, or multi-hop, a paid VPN like NordVPN or ExpressVPN may be necessary. Always verify your VPN's performance using tools like **ipleak.net** and understand that VPNs are part of a broader cybersecurity strategy, not a complete solution.[](https://www.safetydetectives.com/best-vpns/)[](https://cyberinsider.com/vpn/best/)