Identify and Remove Suspicious Browser Extensions

1. Choose a reputable free VPN service and sign up.

 * Action Taken: Selected a well-regarded VPN service known for its commitment to privacy and security. [Insert the name of the VPN service you used here, e.g., "Proton VPN," "Tunnel Bear," or "Trial of NordVPN," etc.]

 * Reasoning: Reputable services are essential as they are less likely to log user data (a "no-logs" policy) or sell browsing history, which would defeat the purpose of a VPN.

2. Download and install the VPN client.

 * Action Taken: Downloaded and installed the official VPN client application for the operating system being used (e.g., Windows, macOS, Android).

 * Initial Setup Notes: [Insert brief note on installation, e.g., "Installation was straightforward and required administrative privileges."]

3. Connect to a VPN server (choose closest or any location).

 * Action Taken: Opened the client and connected to a server location.

   * Server Location Chosen: [e.g., New York, London, or Closest Server]

   * Connection Status: [e.g., "Connection established successfully in less than 5 seconds."]

4. Verify your IP address has changed (use whatismyipaddress.com).

 * Action Taken: Before connecting, recorded the original public IP address. After connecting to the VPN, visited a public IP check website.

 * Verification Data:

   * Original Public IP: [Insert Original IP Address]

   * IP Address While Connected to VPN: [Insert New IP Address (should match server location)]

   * Verification Result: The public IP address successfully changed to the address of the chosen server location, confirming the device's location is masked.

5. Browse a website to confirm traffic is encrypted.

 * Action Taken: Visited a standard website (e.g., a news site or test website) while the VPN was active.

 * Confirmation Method: While direct viewing of the encryption is complex, the successful connection and IP change (Step 4) are strong indicators. The website traffic is now routing through the encrypted VPN tunnel. The website accessed the user's connection via the VPN server's IP.

6. Disconnect VPN and compare browsing speed and IP.

 * Action Taken: Disconnected the VPN client and immediately re-tested the browsing speed and IP address.

 * Comparison Observations:

   * IP Address: Reverted back to the Original Public IP.

   * Speed: [State observation, e.g., "Browsing speed slightly improved after disconnection," or "No noticeable difference in speed," or "Speed was significantly reduced while on the VPN."]

   * Analysis: VPNs often introduce a minor speed reduction due to the overhead of encryption and routing traffic over a greater distance, which was [confirm/refute] with this test.

7. Research VPN encryption and privacy features.

 * Action Taken: Researched the technical details of modern VPNs.

 * Key Technical Findings:

   * Encryption Protocol: Modern VPNs primarily use OpenVPN or WireGuard protocols, both considered highly secure.

   * Encryption Standard: Data is typically encrypted using AES-256 (Advanced Encryption Standard with a 256-bit key), which is the same standard used by governments and military organizations.

   * Key Privacy Feature: A Kill Switch feature is critical; it automatically disconnects the internet connection if the VPN tunnel drops, ensuring the user's real IP address is never accidentally leaked.

8. Write a summary on VPN benefits and limitations.

 * Action Taken: Compiled the findings into the required summary.

Summary: VPN Benefits and Limitations

Aspect	Benefits of Using a VPN	Limitations/Drawbacks of a VPN
Security	Encrypts all internet traffic, protecting data from hackers on public Wi-Fi networks (e.g., coffee shops, airports).	Speed Reduction: The process of encryption and data rerouting can slow down the user's internet connection.
Privacy/Anonymity	Hides the user's real IP address and physical location, preventing tracking by advertisers and ISPs.	Trust: The user must completely trust the VPN provider's "no-logs" policy, as the provider can see the user's data.
Access	Allows users to bypass geo-restrictions (e.g., accessing content only available in a different country).	Cost: The most secure and reliable VPNs typically require a paid subscription. Free VPNs may be unreliable or sell user data.
Compliance	Protects the anonymity of whistleblowers, journalists, and researchers accessing sensitive information.	Legality: VPN use is illegal or heavily restricted in a few countries (e.g., China, Russia).

Outcome: The successful completion of this task means you now have practical experience using a Virtual Private Network (VPN) by setting it up, connecting to a server, and verifying that it works. More importantly, you have gained a fundamental understanding of how VPNs function as essential privacy tools to encrypt your data, hide your location, and keep your online activity secure from snoopers.