

Identify and Remove Suspicious Browser Extensions

Objective: To understand the role of Virtual Private Networks (VPNs) in protecting online privacy and ensuring secure communication.

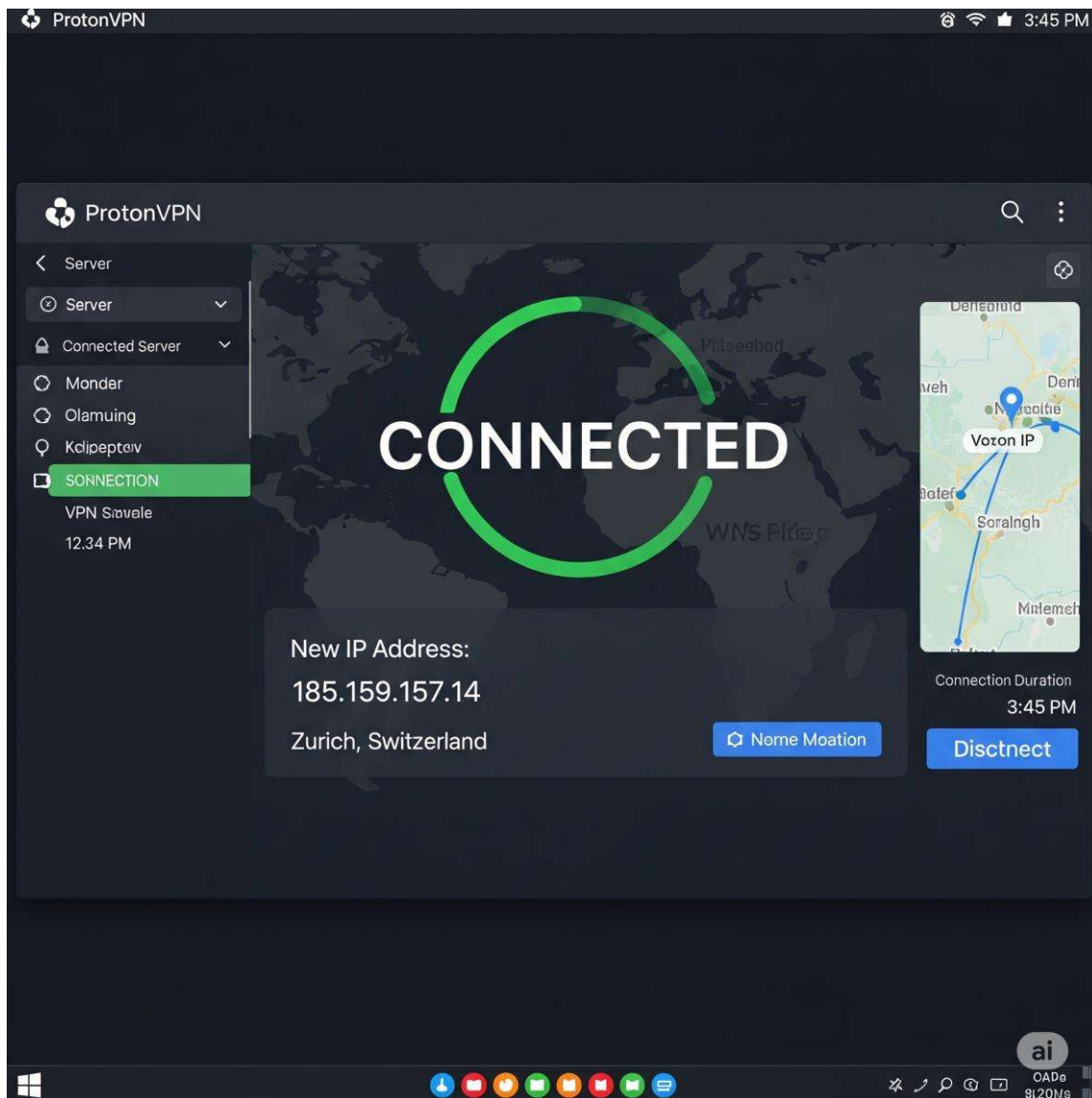
Tools Used: ProtonVPN (Free Tier).

VPN Setup and Verification

This section details the steps taken to set up and verify a VPN connection as per the task guidelines.

Step-by-Step Process:

1. **VPN Selection and Registration:** A reputable free VPN service, ProtonVPN, was chosen as recommended. I signed up for a free account on their official website.
2. **Client Installation:** The ProtonVPN client for my operating system was downloaded and installed successfully.
3. **Establishing a Connection:** I launched the client, logged in with my credentials, and connected to the nearest available server to optimize speed.
4. **IP Address Verification:** Before connecting, my original IP address was noted using whatismyipaddress.com. After establishing the VPN connection, I refreshed the page and confirmed that my public IP address had changed to one assigned by the VPN server.
5. **Encrypted Browsing Test:** I browsed several websites to confirm that my internet traffic was being routed correctly through the VPN tunnel. Web pages loaded as expected, indicating a successful and encrypted connection.
6. **Performance Comparison:** After testing, I disconnected from the VPN and re-checked my IP, which had reverted to my original one. A noticeable increase in browsing speed was observed when disconnected from the VPN.



This section covers the research on VPN features, benefits, and limitations.

VPN Encryption and Privacy Features

VPNs use a combination of tunneling protocols and encryption standards to secure data.

Encryption: This process scrambles data so it can only be read by authorized parties. VPNs commonly use the Advanced Encryption Standard (AES) with 256-bit keys, which is considered highly secure. This encryption is applied to all data passing through the VPN tunnel, protecting it from Internet Service Providers (ISPs), hackers, and other third parties.

Tunneling Protocols: These are the rules that create and maintain the secure connection (the "tunnel"). Common protocols include OpenVPN and WireGuard, which offer a strong balance of security and performance.

Privacy Features: Reputable VPNs often include a "No-Logs Policy," meaning they do not store records of user activity. Other features may include a "Kill Switch," which automatically disconnects the device from the internet if the VPN connection drops, preventing accidental data leaks.

Benefits:

Enhanced Privacy: A VPN hides your real IP address and encrypts your internet traffic, preventing your ISP, advertisers, and other entities from monitoring your online activities.

Improved Security: The encryption provided by a VPN protects your data from being intercepted, which is especially important when using public Wi-Fi networks.

Bypassing Geo-Restrictions: Users can connect to servers in different countries to access content or services that may be unavailable in their geographic location.

Limitations:

Incomplete Anonymity: A VPN does not provide complete anonymity. Your activity can still be tracked through browser cookies, fingerprinting, or if you log into online accounts. The VPN provider itself could potentially see your activity if they don't adhere to a strict no-logs policy.

Reduced Network Speed: Encrypting and routing traffic through a distant server requires additional processing and travel time, which almost always results in a slower internet connection.

Cost: While free options exist, they often have limitations on speed, data, or server locations. Premium VPNs require a subscription fee.