Cybersecurity Internship Task Report – VPN & Browser Privacy

# 1. Introduction

This report documents the steps taken to complete the cybersecurity internship task focused on Virtual Private Networks (VPNs) and browser privacy. The goal was to gain hands-on experience with a VPN client, understand the encryption and privacy benefits of VPNs, and practice good browser hygiene by identifying and removing suspicious extensions.

# 2. Tools Used

- VPN Client: Riseup VPN (Free, No Signup Required)  
- Browser: Google Chrome  
- IP Test Site: https://whatismyipaddress.com

# 3. VPN Setup Steps

1. Downloaded Riseup VPN from the official website (https://riseup.net/en/vpn).  
2. Installed the client on the system.  
3. Launched the application and connected to a VPN server.  
4. Verified the IP address change using whatismyipaddress.com.  
5. Browsed HTTPS websites to ensure traffic was encrypted.  
6. Disconnected the VPN and compared the original IP address and browsing speed.

# 4. Research on VPNs

A Virtual Private Network (VPN) is a service that encrypts internet traffic and routes it through a secure server to protect user privacy. By masking the user’s IP address and encrypting data in transit, VPNs offer a higher level of security especially when using public or unsecured networks.  
  
Riseup VPN uses the LEAP Encryption Access Protocol to ensure end-to-end encryption. Commonly used VPN protocols include OpenVPN, IKEv2/IPSec, and WireGuard. Encryption prevents eavesdropping and man-in-the-middle attacks.  
  
However, VPNs do not provide complete anonymity. Websites may still track users through cookies, browser fingerprinting, or user logins. Additionally, VPNs can slow down network speeds due to the encryption and remote server routing.

# 5. Conclusion

The task demonstrated practical experience in setting up and testing a VPN, verifying encrypted communication, and improving browser security. VPNs are an essential privacy tool for secure online communication, but they are not a silver bullet. Users must combine VPN use with good digital hygiene practices such as strong passwords, careful app permissions, and avoiding suspicious downloads for holistic security.