

WORKING WITH VPNS

Introduction

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. VPNs are widely used to protect privacy, secure communications, and bypass geographical restrictions. This report documents the steps taken to set up a free VPN, verify its functionality, and analyze its benefits and limitations.

VPN Setup Steps

1. Choosing a VPN Service

For this task, I selected **ProtonVPN** (free tier) due to its reputation for strong privacy policies and no data logging.

2. Downloading and Installing the VPN Client

- Visited the official ProtonVPN website and signed up for a free account.
- Downloaded the VPN client compatible with my operating system (Windows/macOS).
- Installed the client by following the on-screen instructions.

3. Connecting to a VPN Server

- Launched the ProtonVPN application and logged in using my credentials.
- Selected a server location (chose the closest server for optimal speed).
- Clicked the "Connect" button to establish the VPN connection.

4. Verifying the IP Address Change

- Visited whatismyipaddress.com before and after connecting to the VPN.
- Observed that the IP address changed to reflect the VPN server's location.
- **Screenshot of the new IP address:**
(Insert screenshot here showing the updated IP address.)

5. Confirming Traffic Encryption

- Accessed a website (e.g., Google) while connected to the VPN.
- Verified that the traffic was encrypted by checking for HTTPS in the browser's address bar.

6. Comparing Browsing Speed and IP

- Disconnected the VPN and revisited whatismyipaddress.com to confirm the original IP address was restored.
- Noticed a slight decrease in browsing speed while using the VPN, likely due to encryption overhead.

VPN Benefits and Limitations

Benefits:

1. **Privacy Protection:** Masks the user's real IP address, making it difficult for third parties to track online activities.
2. **Secure Communication:** Encrypts data transmitted over the internet, protecting it from eavesdropping.
3. **Bypass Geo-Restrictions:** Allows access to region-locked content by connecting to servers in different countries.
4. **Public Wi-Fi Security:** Safeguards data when using unsecured public networks.

Limitations:

1. **Speed Reduction:** Encryption and rerouting of traffic can slow down internet speeds.
2. **No Complete Anonymity:** VPNs do not guarantee absolute anonymity, as some services may log user data.
3. **Limited Free Tiers:** Free VPNs often have restrictions like data caps or fewer server options.
4. **Blocked by Some Services:** Certain websites or services may block VPN traffic.

Conclusion

This task provided hands-on experience with setting up and using a VPN. While VPNs are powerful tools for enhancing privacy and security, they come with trade-offs such as reduced speed and limited features in free tiers. Understanding these aspects is crucial for making informed decisions about online privacy tools.