**VPN Setup Report for Privacy and Secure Communication**

VPN Service Used: ProtonVPN (Free Tier)  
Objective: To demonstrate how to securely set up and verify a VPN connection to enhance online privacy and data protection.

**1. Introduction**

A Virtual Private Network (VPN) is a security tool that creates an encrypted tunnel for internet traffic, effectively hiding the user's IP address and securing communication over public or untrusted networks. This report walks through setting up a free VPN and validating its functionality.

**2. VPN Setup Steps**

Step 1: Selecting a VPN Provider

Chosen provider: ProtonVPN Free Tier

Reason: It offers strong encryption, a trustworthy no-log policy, and unlimited data for free-tier users.

Step 2: Creating an Account

* Account created using an email address .
* Verified through the provider's secure signup process.

Step 3: Downloading the VPN Client

* Navigated to the official ProtonVPN website.
* Downloaded and installed the appropriate VPN client for Windows.
* Ensured the download was from the official source only to avoid malware risks.

Step 4: Connecting to a VPN Server

* Launched the ProtonVPN application.
* Logged in with credentials.
* Selected a free server in the Netherlands (or nearest available).
* Clicked Connect to establish the VPN tunnel.

Step 5: Screenshot of Connection

Screenshot captured post-connection showing:

* Connection status as Connected
* Server Location: [Visible]
* Virtual IP: [Hidden for security]
* Real IP: Hidden
* Account details or email: Not visible in the screenshot

**3. VPN Verification and Testing**

Step 6: IP Address Verification

* Visited: <https://whatismyipaddress.com>
* Confirmed that IP address had changed, indicating successful VPN tunneling.

Step 7: Secure Website Browsing Test

* Accessed websites like <https://example.com> and <https://duckduckgo.com>
* Verified the 🔒 padlock icon, indicating HTTPS encryption.

Step 8: Disconnect and Comparison

* Disconnected the VPN.
* Checked IP again to confirm it reverted to my original IP.
* Observed slightly faster speeds once VPN was off.

**4. VPN Security and Privacy Overview**

Encryption Used

* AES-256-bit encryption (standard for data security)
* Secure protocols such as OpenVPN and WireGuard
* DNS Leak Protection and Kill Switch enabled

Privacy Features

* No logs of user activity
* Swiss-based jurisdiction with strong privacy laws
* Protects identity and activity from ISPs and trackers

**5. Summary of Benefits and Limitations**

Benefits:

* Encrypts internet traffic
* Masks real IP address
* Allows secure browsing on public Wi-Fi
* Bypasses regional restrictions and censorship

Limitations:

* Free servers may be slower or congested
* VPNs don’t block malware/phishing by default
* Trust must be placed in the VPN provider
* Can’t ensure complete anonymity (e.g., browser fingerprinting still possible)

**6. Conclusion**

VPNs are essential tools in modern cybersecurity for anyone looking to protect their privacy and maintain secure communications. The setup process was straightforward, and all traffic was successfully tunneled through the VPN with encryption verified. While free services have limitations, ProtonVPN proved effective for learning and basic protection.