# VPN Usage and Privacy Report

Prepared by: Mohammad Arshan Dafedar

This report documents the process of setting up and testing a Virtual Private Network (VPN) as part of the cybersecurity internship training. The primary goal was to verify IP masking, traffic encryption, and understand the benefits and limitations of VPN usage.

## VPN Service Selected

Proton VPN (Free Tier) was selected due to its strong reputation for privacy, no data limits on the free plan, and use of secure encryption protocols.

## Process

- Signed up for a free Proton VPN account via the official website.

- Downloaded and installed the Proton VPN client for Windows.

- Connected to a VPN server located in Germany.

- Verified IP address change using whatismyipaddress.com — the IP successfully changed from an example original (203.0.113.45) to the VPN server IP (198.51.100.23).

- Browsed multiple HTTPS websites to confirm encryption; padlock icon in browser indicated secure connection.

- Disconnected from VPN and confirmed IP reverted to original public IP.

- Performed speed tests before and after VPN usage, noting a minor reduction in download and upload speeds.

## VPN Encryption and Privacy Features

Proton VPN uses AES-256 encryption with OpenVPN and WireGuard protocols, ensuring secure and private connections. The service maintains a strict no-logs policy and is based in Switzerland, offering strong legal protections for user privacy.

## Summary

VPNs are effective tools for enhancing privacy and security online by encrypting traffic and masking IP addresses. They help protect users on public Wi-Fi and allow access to region-restricted content. However, free VPN tiers may have limitations such as reduced server options, potential speed drops, and occasional service blocks by certain websites. During testing, the VPN successfully masked the IP, encrypted browsing activity, and maintained a stable connection, albeit with a slight decrease in speed.