

Report: VPN Privacy and Security

Date: June 6, 2025 **Intern:** Muhammad Ali Khan **Organization:** ELEVATE LABS

1. Introduction

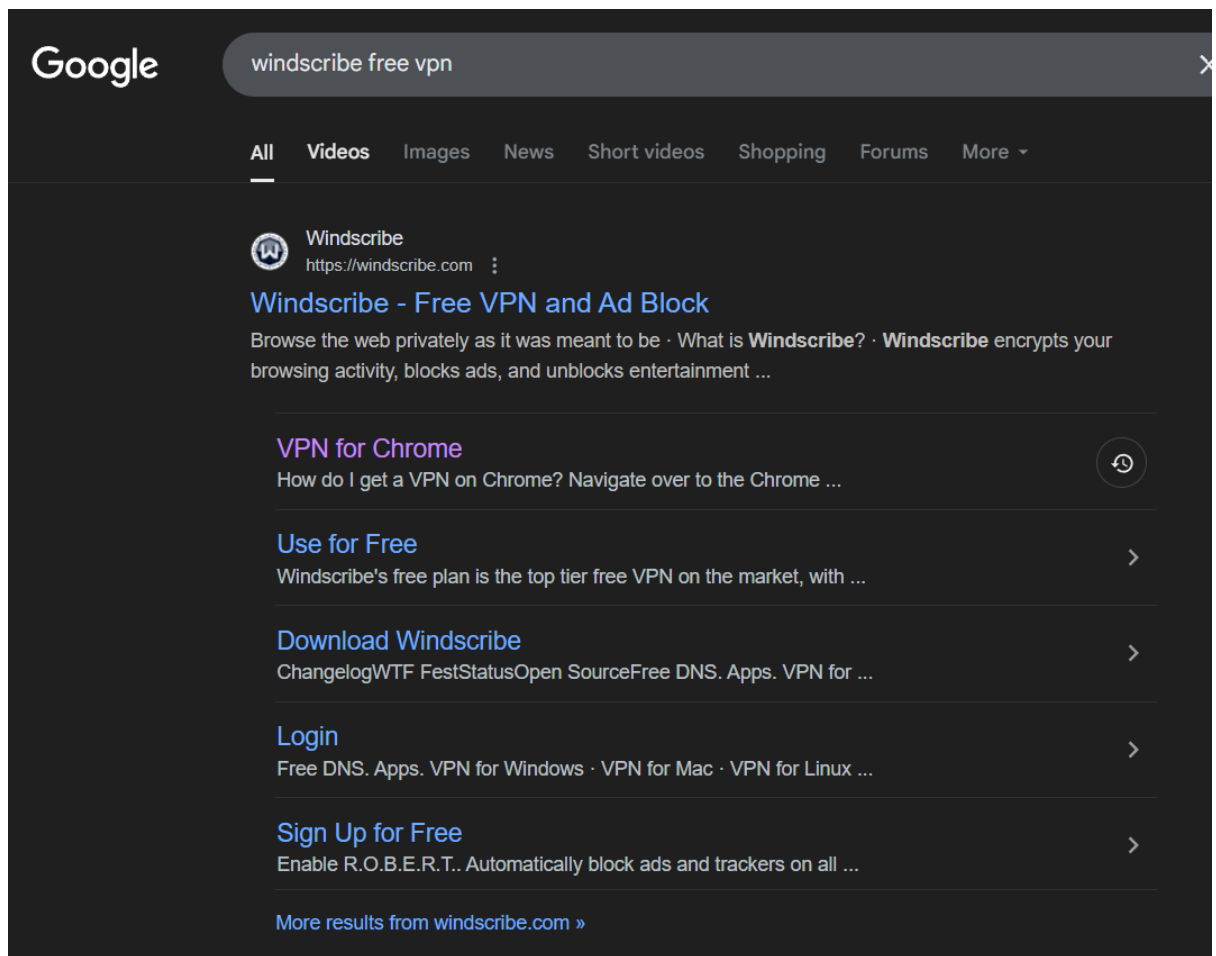
This report details the exploration of **Virtual Private Networks (VPNs)**, focusing on their critical role in **protecting online privacy and securing digital communication**. Through practical exercises using a free VPN client, we'll demonstrate the setup process, verify secure connections, and analyse the impact of VPNs on Browse experience. This document also summarizes key VPN benefits and limitations, offering a comprehensive understanding of their utility in today's digital landscape.

2. Choosing a reputable free VPN service

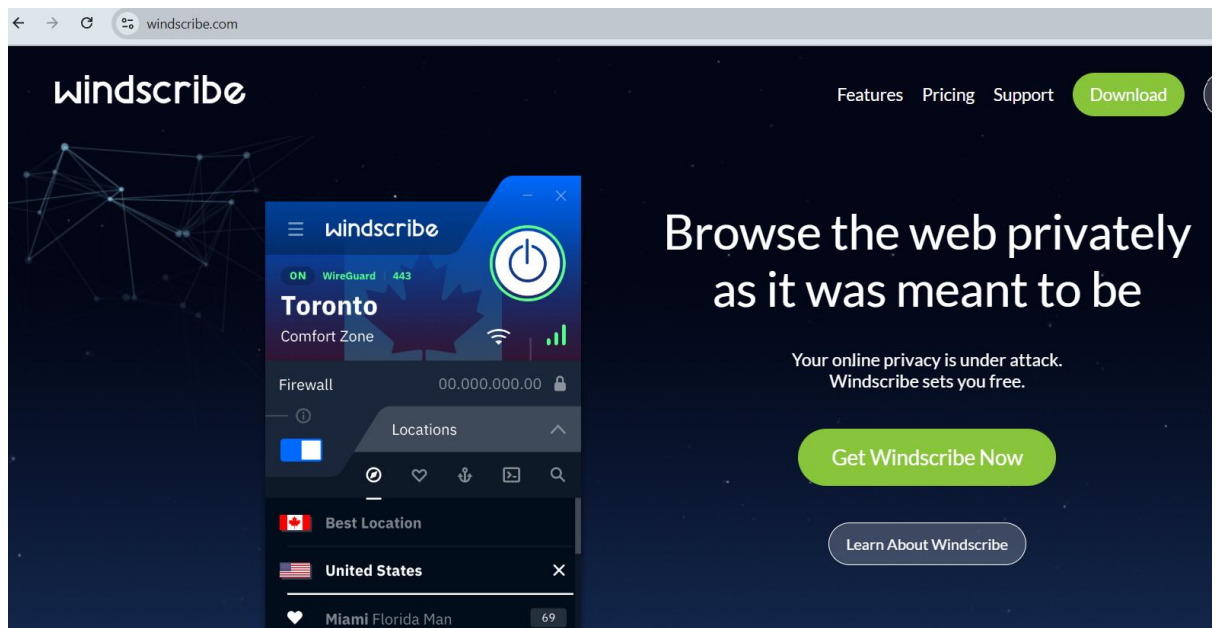
There are many free VPN solutions, I chose the free **VPN Client Windscribe Free**, which is also suggested in the description of this task.

3. Download and Install the VPN Client and sign up

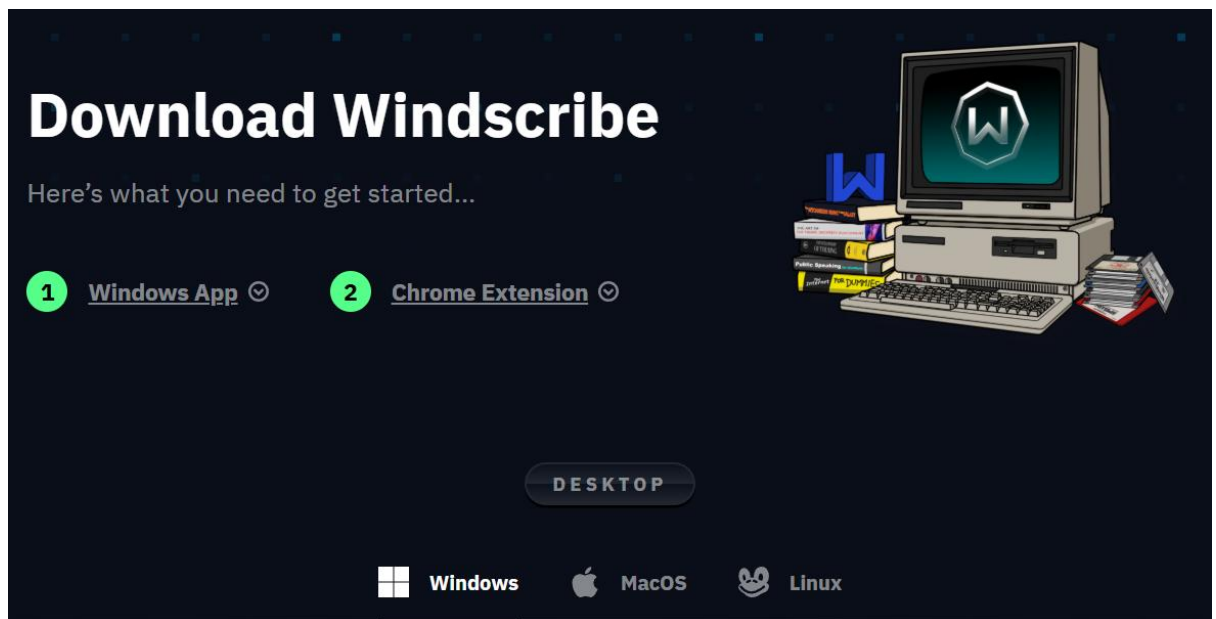
I opened my google chrome browser and searched for the VPN.



Clicked on the first listed website – windscribe.com, which opened the following page:



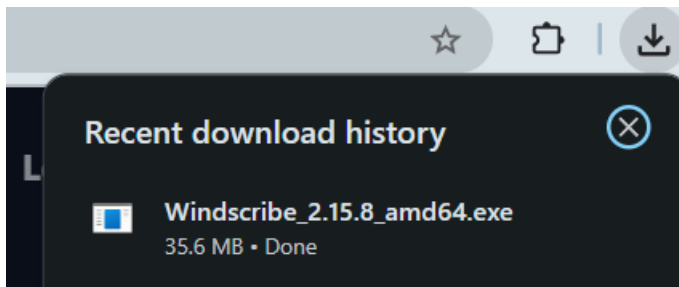
Then I clicked on the Download tab and the I was taken to another webpage for download.



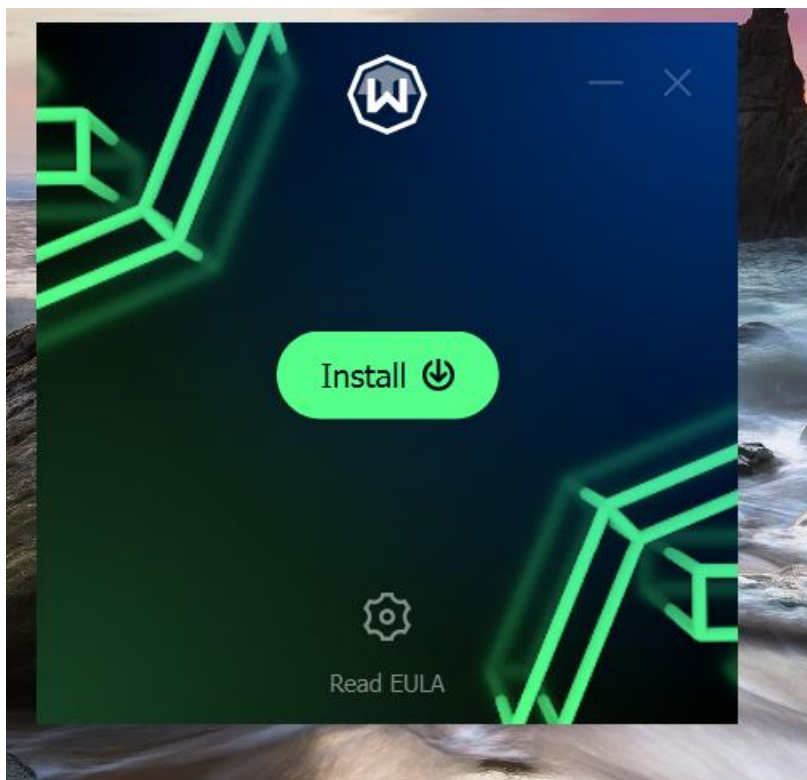
I chose the Windows option as I am running a Windows 11 OS. This took me to the following area of that page:



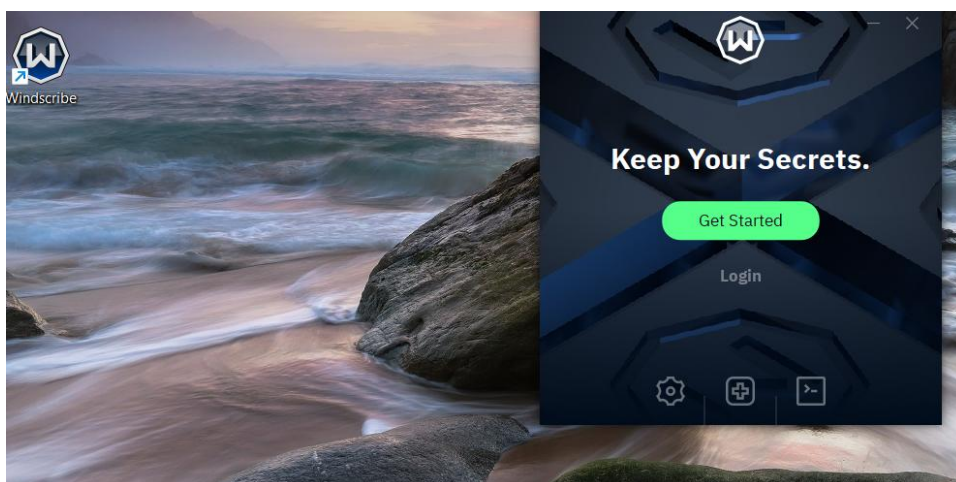
Next, I started the download. The VPN's executable file was successfully downloaded as follows:



I opened the file, and it prompted the installation. So, I clicked on the Install button, which started installing it.

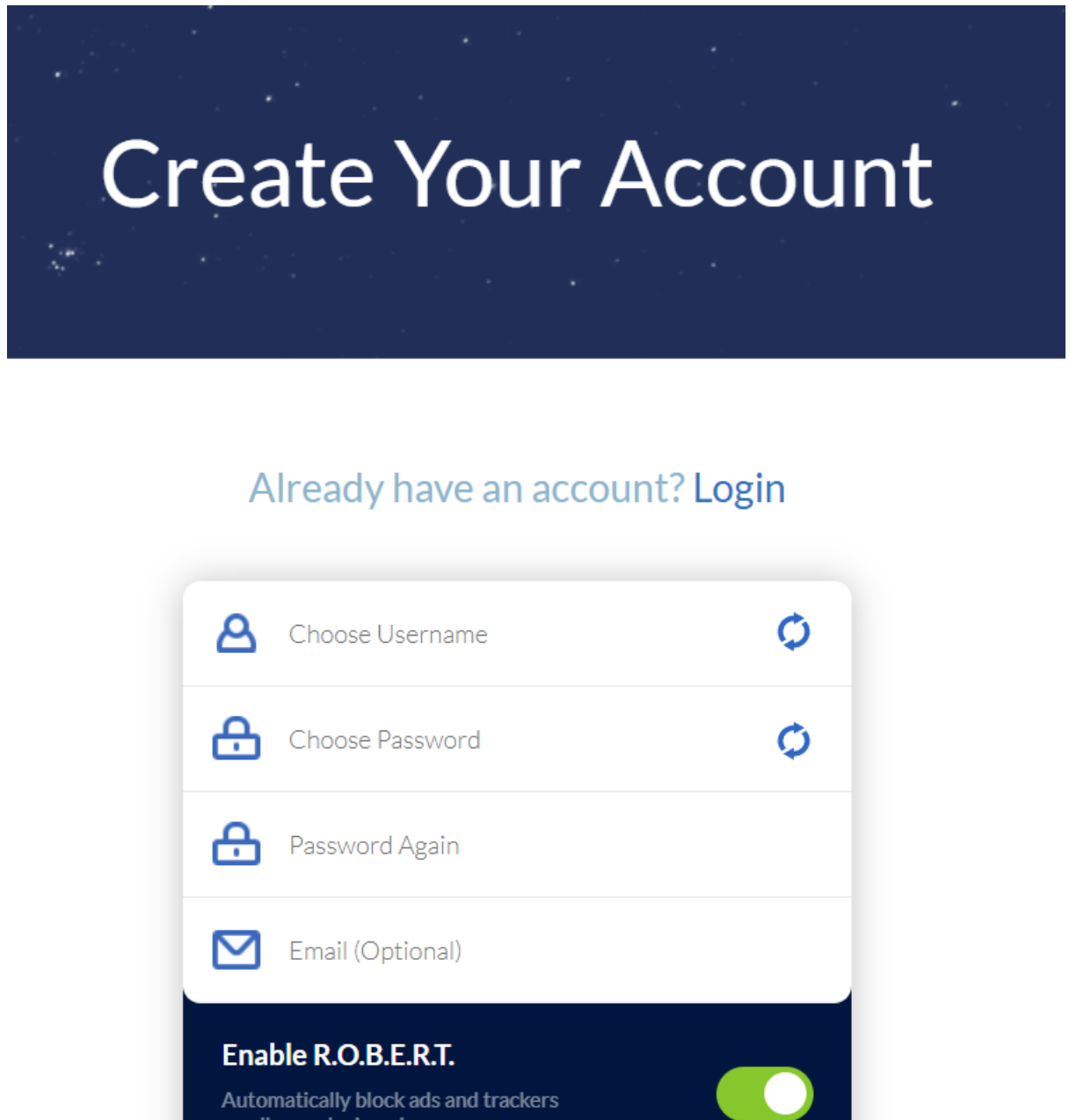


The install of our VPN Client Windscribe is successful as can be seen in the screenshot below:





Next, I clicked on the Get Started button, as I have never previously downloaded or used Windscribe. If someone already has an account then he/she can go ahead with the login credentials.



The Get Started Button opened my browser and landed me on this page:





Create Your Account


[Already have an account? Login](#)

 Choose Username 

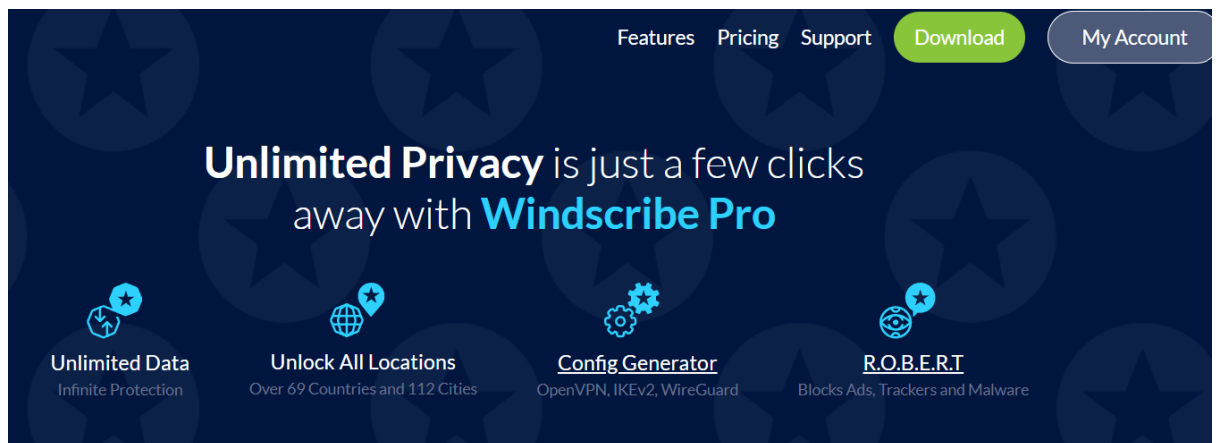
 Choose Password 

 Password Again

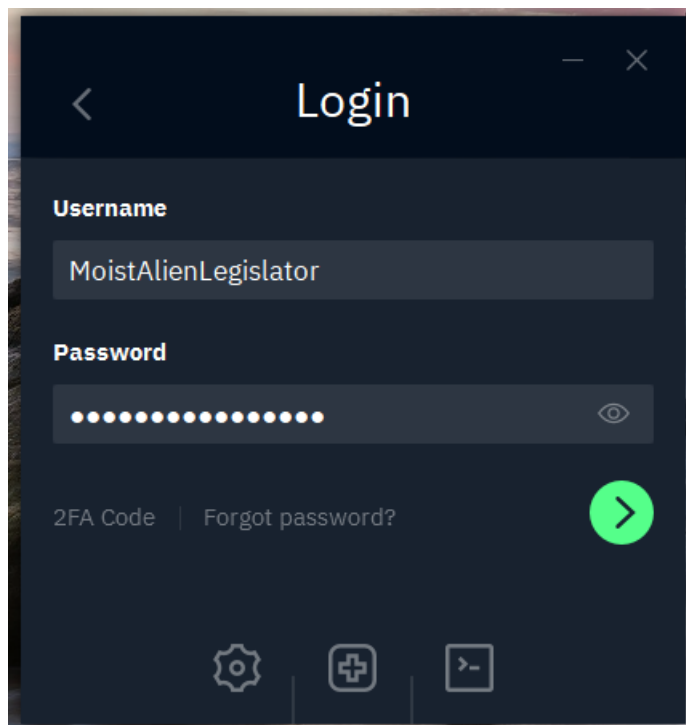
 Email (Optional)

Enable R.O.B.E.R.T.
Automatically block ads and trackers
on all your devices. [Learn more](#) 

Next, I filled in the credentials and successfully made created the account with Windscribe. Once the account is created ,the website page looks like the following:

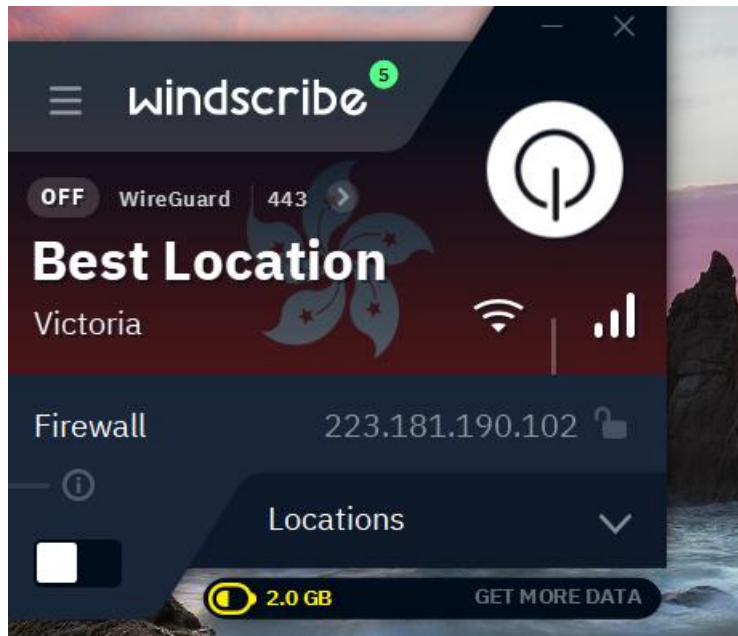


After creating the account with Windscribe, I opened it using the shortcut on my desktop which was automatically created during the installation process. This time I went ahead with the login button, as we have already created the account and it asked for the login credentials and I filled it in as follows:

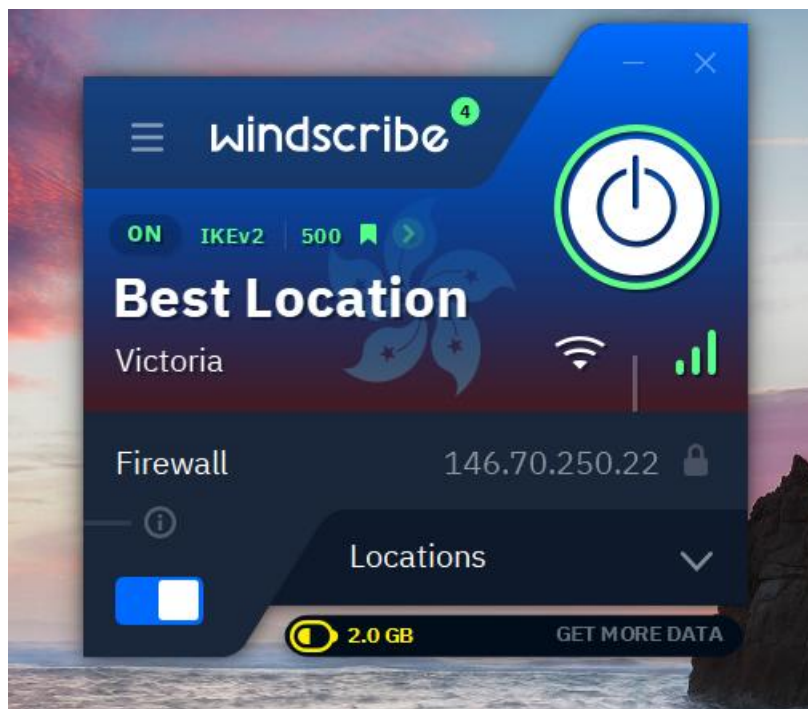


4. Turn it On. Connect to a VPN Server

After successful login, the desktop VPN is displayed as follows (Notice the current IP address as shown in the VPN – 223.181.190.102):

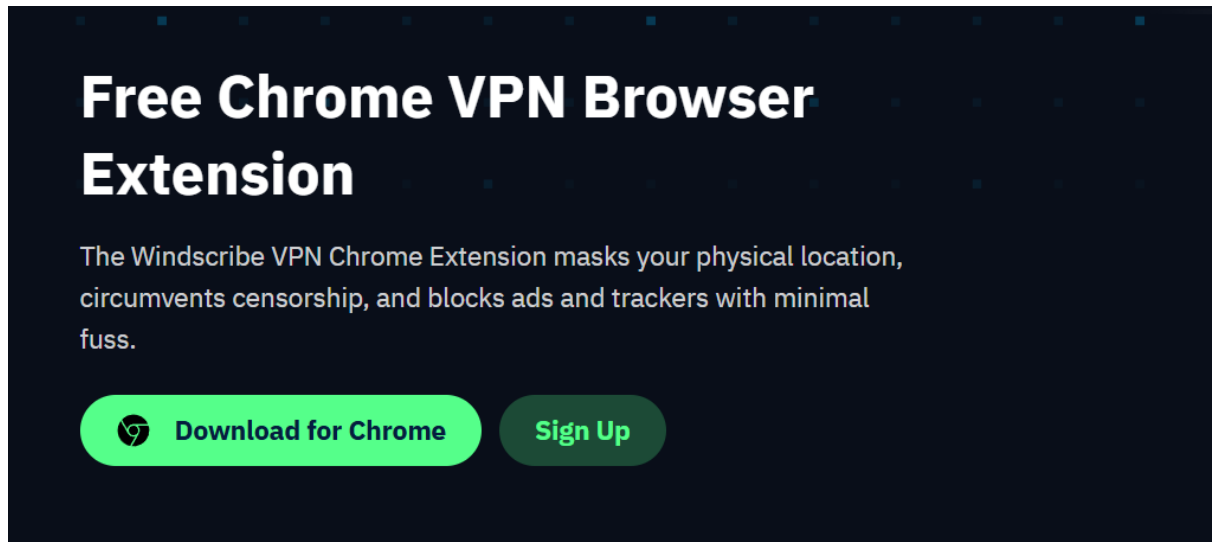


To start the VPN, I clicked on the large power button, which turned it on. (Notice the change in IP address – 146.70.250.22) After successfully establishing connection the VPN was displaying as follows:

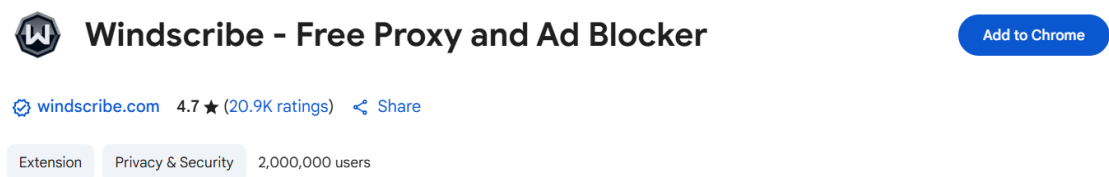


5. Adding the VPN to chrome browser's extensions

I was also prompted by the VPN to download the chrome browser extension for the VPN, which further adds functionality when browsing the Internet through google chrome browser.



I clicked on the Download for Chrome button and landed on the following page of the chrome web store:



Next, I clicked on the Add to Chrome icon for downloading it into my browser extension. Which added it successfully.

6. Verify change In Ip Address

As the VPN Client installation and sign up has been completed and we even started the VPN and successfully connected to it, now is the time to verify its functionality.

I terminated the VPN connection, and opened my chrome browser. Then went to the following website www.whatismyipaddress.com:

The screenshot shows the homepage of WhatIsMyIPAddress.com. At the top, there is a search bar with the text "Enter Keywords or IP Address..." and a "Search" button. Below the search bar, there are four navigation tabs: "MY IP", "IP LOOKUP", "HIDE MY IP", and "VPNS". The "MY IP" tab is selected. The main content area displays the following information:

- My IP Address is:
 - IPv4: **223.181.190.102**
 - IPv6: **Not detected**
- My IP Information:
 - ISP: Bharti Airtel Ltd.
 - City: Indore
 - Region: Madhya Pradesh
 - Country: India
- Your location may be exposed!
- A red button labeled "HIDE MY IP ADDRESS NOW" with a shield icon.
- A link labeled "Show Complete IP Details" in green.

The screenshot above shows my **Original IP address** assigned to my home network by my ISP. Even the location is somewhat correct up until the Region: Madhya Pradesh.

After noting the details, as stated above, I went back again to Windscribe and turned it on and came back to the browser and reloaded the webpage. The following screenshot displays the changes after turning on the VPN:

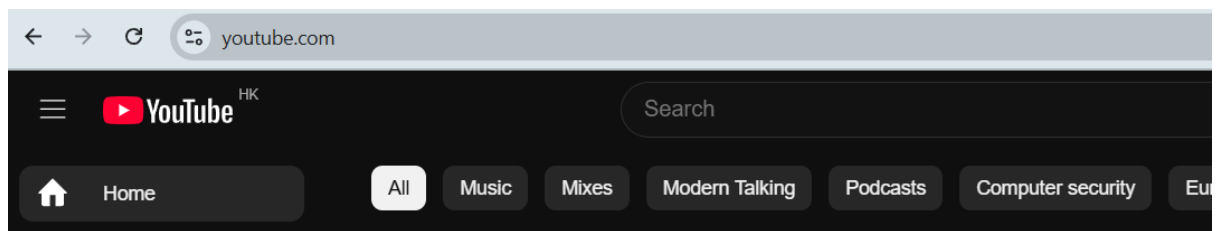
The screenshot shows the homepage of WhatIsMyIPAddress.com after using a VPN. The navigation tabs are the same, but the "MY IP" tab is selected. The main content area displays the following information:

- My IP Address is:
 - IPv4: **146.70.250.6**
 - IPv6: **Not detected**
- My IP Information:
 - ISP: M247 Europe SRL
 - Services: [VPN Server](#)
 - City: Hong Kong
 - Region: Hong Kong
 - Country: Hong Kong
- Looks like you're using a VPN!
- A red button labeled "RATE YOUR VPN" with a shield icon.
- A link labeled "Show Complete IP Details" in green.

Now, my **real Identity (IP address)** has been masked. A different IP address is being displayed, even a different ISP along with Geographical location. I being in India, the location it is showing is that of Hong Kong. However, whatismyipaddress.com has identified that I am using a VPN but that doesn't change the fact that now my online activity cannot be traced to my IP address therefore, increasing my anonymity and privacy online.

7. Browse a Website

Next, I visited a website while my Windscribe VPN was still on. I visited www.youtube.com, which took around 30-40 seconds to open.



Then, I disconnected from the VPN, and again visited [youtube.com](https://www.youtube.com) which now took a few seconds only to open. VPNs decrease the browsing speed because of the encryption and privacy features (like connecting to a different server a VPN server)

8. Virtual Private Networks (VPNs): A Comprehensive Overview

A Virtual Private Network (VPN) creates a secure, encrypted connection over a less secure network, like the internet. It acts as a private tunnel for your online data, shielding it from prying eyes.

A. VPN Encryption and Privacy Features

VPNs employ various sophisticated technologies to ensure your online activities remain private and secure.

- **Core Encryption:**
 - **How it Works:** VPNs scramble your data so that only authorized parties (your device and the VPN server) can understand it. This makes your online traffic appear as unreadable gibberish to anyone who intercepts it.
 - **Common Protocols:**
 - **AES (Advanced Encryption Standard):** This is the industry gold standard, often used with 128-, 192-, or 256-bit keys. AES-256 is considered highly secure and is used by governments and security organizations worldwide.

- **ChaCha20:** A newer, efficient symmetric encryption algorithm often used with WireGuard.
 - **OpenVPN:** A popular open-source VPN protocol known for its strong security and flexibility. It often uses AES-256-GCM.
 - **IKEv2/IPsec:** A robust and fast protocol, particularly good for mobile devices due to its ability to handle network changes.
 - **WireGuard:** A modern, lightweight, and fast VPN protocol designed for simplicity and strong encryption.
- **Key Exchange:**
 - VPNs use a combination of symmetric and asymmetric encryption. Asymmetric encryption (like RSA or Elliptic Curve Diffie-Hellman - ECDH) is used to establish a secure connection and safely exchange the symmetric encryption keys.
 - **Perfect Forward Secrecy (PFS):** This crucial feature ensures that if one encryption key is compromised, past and future session data remains secure. Each new session uses a new, unique encryption key.
 - **Privacy Features:**
 - **IP Address Masking:** A VPN hides your real IP address by routing your internet traffic through its own server, assigning you a temporary IP address from that server's location. This makes it difficult to trace your online activity back to your physical location.
 - **No-Logs Policy:** A trustworthy VPN provider commits to not logging your online activities, connection timestamps, IP addresses, or Browse history. This is vital for maintaining user privacy.
 - **DNS Leak Protection:** Prevents your Domain Name System (DNS) requests (which translate website names into IP addresses) from being exposed to your Internet Service Provider (ISP) outside the encrypted VPN tunnel.
 - **Kill Switch (or Firewall):** Automatically blocks all internet traffic if the VPN connection drops, preventing your real IP address or data from being exposed.
 - **Split Tunneling:** Allows you to choose which applications or websites use the VPN tunnel and which connect directly to the internet, offering flexibility.
 - **Multi-Hop/Double VPN:** Routes your traffic through two or more VPN servers, adding multiple layers of encryption and making it even harder to trace.
 - **Obfuscation/Stealth Protocols:** Designed to make VPN traffic appear as regular internet traffic, helping to bypass strict firewalls or VPN blocking (e.g., in countries with heavy censorship).

B. Windscribe VPN's Encryption and Privacy Features:

Windscribe VPN offers a robust set of security and privacy features:

- **Encryption:**

- **OpenVPN:** Uses AES-256-GCM cipher with SHA512 authentication and a 4096-bit RSA key. Supports Perfect Forward Secrecy.
 - **IKEv2:** Employs AES-256-GCM for encryption and SHA-256 for integrity checks. Uses ECP384 (desktop/Android) or ECP521 (iOS) for Diffie-Hellman key negotiation.
 - **WireGuard:** Uses ChaCha20 for symmetric encryption (authenticated with Poly1305), Curve25519 for ECDH, BLAKE2s for hashing, and HKDF for key derivation.
 - **Browser Extensions:** Utilize TLS 1.3, ECDHE_RSA with X25519 key exchange, and the TLS_AES_256_GCM_SHA384 cipher.
- **Privacy Features:**
 - **Strict No-Identifying-Logs Policy:** Windscribe claims not to keep connection logs, IP timestamps, or session logs. They do store minimal data like the total amount of data used in a 30-day period (for free plan limits) and the timestamp of your last activity.
 - **Windscribe Firewall (Kill Switch):** This feature acts as an "always-on" firewall, preventing any data leaks if the VPN connection drops. It ensures your internet connection only works when connected to the VPN.
 - **R.O.B.E.R.T.:** A customizable server-side tool that blocks ads, trackers, malware, and can filter specific content categories (e.g., gambling, porn).
 - **MAC Spoofing:** Available on desktop apps, this feature changes your device's Media Access Control (MAC) address each time you connect, adding another layer of anonymity.
 - **Split Tunneling:** Allows you to select which applications route through the VPN and which bypass it.
 - **Stealth and WStunnel Protocols:** These unique protocols are designed to help bypass restrictive networks and VPN blocks by disguising VPN traffic.

9. Summary on VPN Benefits and Limitations

VPN Benefits:

- **Enhanced Online Privacy:** Hides your IP address and encrypts your internet traffic, preventing ISPs, governments, advertisers, and other third parties from monitoring your online activities.
- **Improved Security on Public Wi-Fi:** Encrypts your data, making it safe to use public Wi-Fi networks (e.g., in cafes, airports) where your information would otherwise be vulnerable to interception by hackers.
- **Bypass Geo-Restrictions:** Allows you to access geo-blocked content and services (e.g., streaming platforms, websites) by connecting to a server in a different country.
- **Circumvent Censorship:** Helps users in restrictive regions bypass government firewalls and access blocked websites and information.
- **Prevent ISP Throttling:** By encrypting your traffic, your ISP cannot see what you're doing online, making it harder for them to selectively slow down your internet speed for certain activities (like streaming or torrenting).
- **Anonymous Torrenting/P2P:** Provides a layer of anonymity and security for peer-to-peer file sharing, making it harder to track your torrenting activities.

VPN Limitations:

- **Reduced Internet Speed:** Encryption and routing traffic through a remote server can introduce latency and slow down your internet connection, especially noticeable with distant servers or weaker VPNs.
- **Not a Universal Security Solution:**
 - **No Protection Against Malware/Viruses:** A VPN does not protect your device from viruses, ransomware, or other malware. You still need antivirus software and safe Browse habits.
 - **No Protection Against Phishing:** VPNs don't stop you from falling victim to phishing scams if you click on malicious links or enter credentials on fake websites.
 - **Doesn't Block All Tracking:** While it hides your IP, VPNs don't inherently prevent websites from tracking you using cookies or browser fingerprinting.
 - **Doesn't Hide What You Share Publicly:** Any personal information you post on social media or public forums remains visible, regardless of VPN use.
- **Cost:** While free VPNs exist, they often come with limitations (data caps, slower speeds, fewer servers) and may have questionable privacy practices. Quality VPN services typically require a paid subscription.
- **Potential for Blocks:** Some websites, streaming services, or online games actively detect and block VPN usage to enforce geo-restrictions or prevent abuse.
- **Trust in the VPN Provider:** Your data passes through the VPN provider's servers. You must trust that the VPN provider adheres to its no-logs policy and has robust security measures in place.
- **Legal and Regulatory Issues:** While VPNs are legal in most places, certain countries have banned or heavily restricted their use. Engaging in illegal activities while using a VPN does not make those activities legal.
- **Complexity for Some Users:** Setting up and configuring some VPNs or understanding advanced features can be challenging for less tech-savvy individuals.