

# Understand the role of VPNs in protecting privacy and secure communication

## 1.Choosing a reputable free VPN service and signed up



## 2. Connecting to a VPN server

## 3. Verifying IP address has changed

❖ IP address before connecting to vpn

## ❖ IP address after connecting to vpn

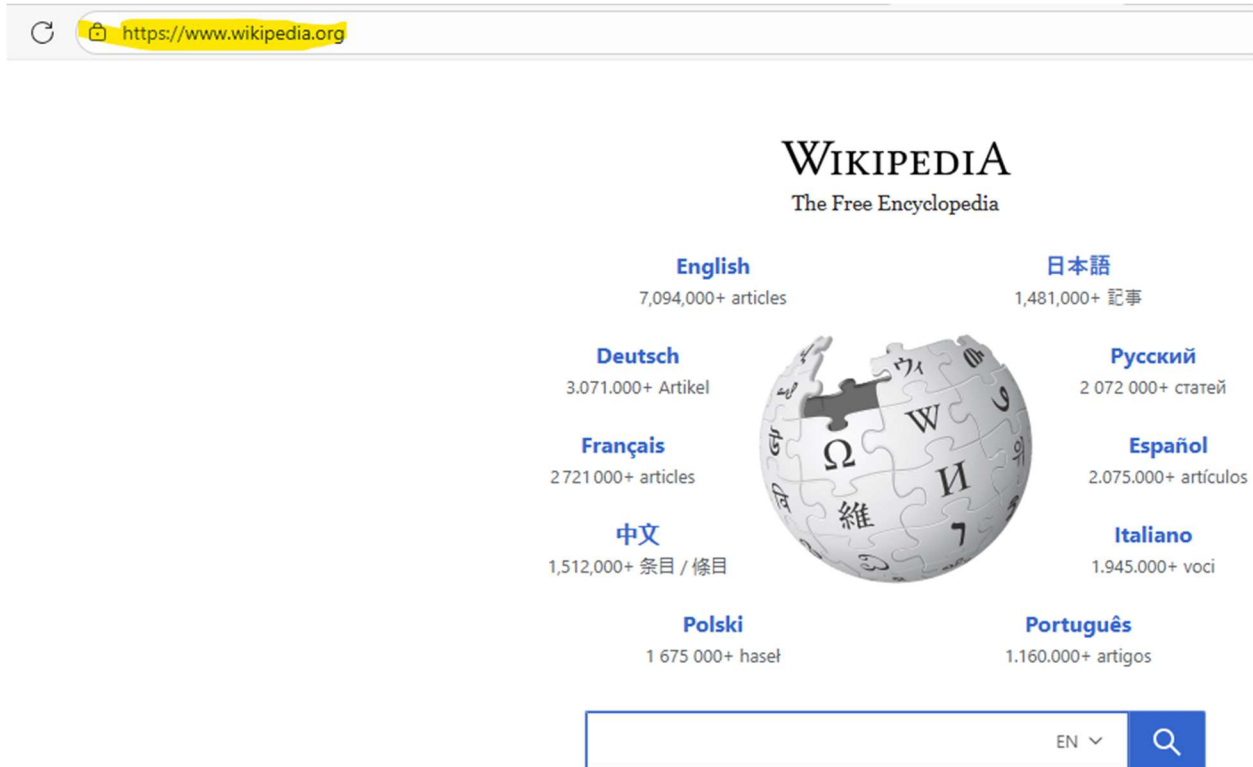
The screenshot shows the homepage of WhatIsMyIPAddress.com. The main content area displays the following information:

- My IP Address is:**
  - IPv4: [146.70.250.7](#)
  - 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!** (Message in a blue speech bubble)
- RATE YOUR VPN** (Red button)
- [Show Complete IP Details](#) (Green link)
- Location not accurate?** (Text)
  - [Update My IP Location](#) (Green link)

The website header includes a search bar, navigation links (ABOUT, PRESS, PODCAST, SUPPORT), and a menu (MY IP, IP LOOKUP, HIDE MY IP, VPNS, TOOLS, LEARN). A Windows activation watermark is visible in the bottom right corner.

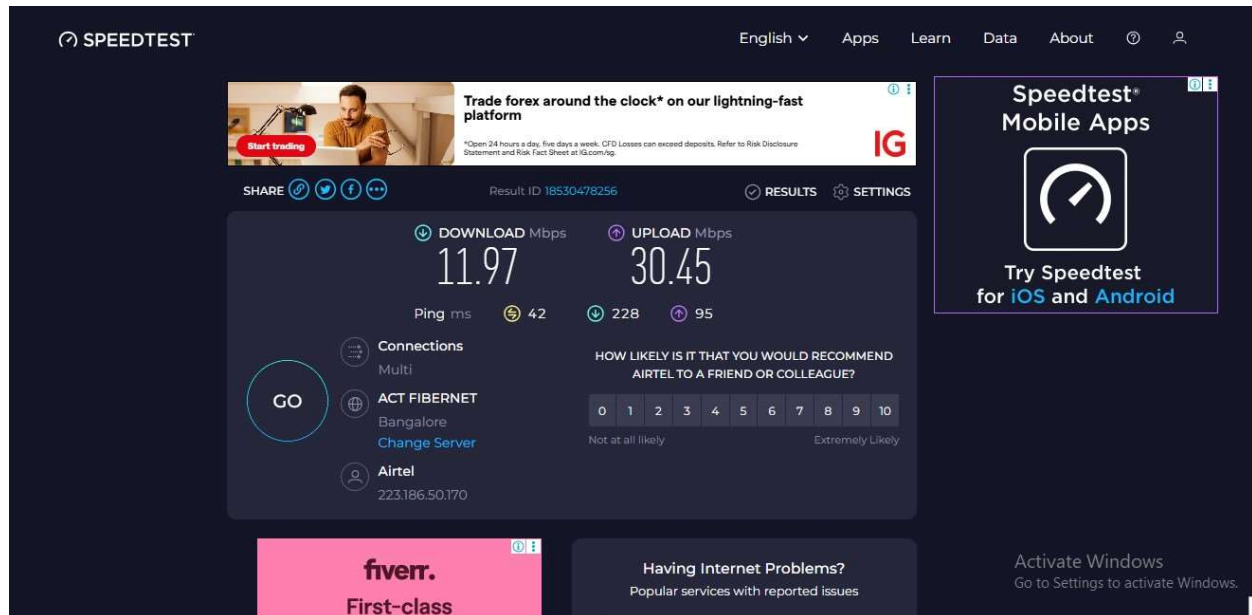
#### 4. Browsing a website to confirm traffic is encrypted

This can be confirmed by seeing see “**https://**” and a **lock icon**



## 5. Disconnecting VPN and compare browsing speed and IP.

❖ Before connecting to vpn:- usually faster, lower ping



❖ After connecting to vpn:- usually slower, higher ping



## 6. Research on VPN Encryption & Privacy Features

### 1. Encryption Standards

VPNs use strong encryption to protect your internet traffic.

- **AES-256 (Advanced Encryption Standard 256-bit)**
  - Industry standard
  - Used by banks and militaries
  - Very strong, currently unbreakable by brute force
- **ChaCha20**
  - Fast and secure alternative
  - Often used with the Wire Guard protocol
  - Good for mobile devices because it's lightweight

These encrypt your data so no one (ISP, hackers, network owners) can read it.

### 2. VPN Tunnelling Protocols

Protocols decide *how* your encrypted data travels.

- **OpenVPN**
  - Very secure, open-source, widely trusted
  - Supports AES-256 encryption

- **Wire Guard**
  - Newer, faster, modern, lightweight
  - Uses ChaCha20 encryption
  - Better performance for gaming/streaming
- **IKEv2/IPSec**
  - Stable on mobile networks
  - Quickly reconnects when switching Wi-Fi / mobile data

These protocols affect speed, security, and stability.

### **3. No-Logs Policy**

A no-logs policy means the VPN claims not to store your online activity such as:

- Websites visited
- IP addresses
- DNS queries
- Download history

A *strict* no-logs policy should also be backed by:

- Independent audits
- Clear privacy policy
- No collection of personal browsing data

This ensures your activities cannot be traced back to you.

## **4. Kill Switch**

A kill switch blocks internet traffic if the VPN disconnects.

This prevents:

- Real IP address leaks
- DNS leaks
- Unencrypted traffic exposure

It keeps you protected even when the connection drops.

## **5. DNS & IPv6 Leak Protection**

A VPN should route all DNS requests through its encrypted tunnel.

This prevents:

- Your ISP from seeing what websites you access
- Leaks that expose your real identity

Leak protection also includes:

- DNS leak protection
- IPv6 leak protection
- WebRTC leak protection

## **6. Multi-Hop (Double VPN)**

Your traffic goes through two VPN servers instead of one.

Benefits:

- More privacy
- Harder for attackers to trace

Used mostly for high-privacy tasks.

## **7. Perfect Forward Secrecy (PFS)**

PFS changes encryption keys frequently.

So even if someone captured old data:

- They cannot decrypt past sessions
- Each session uses new keys

This protects long-term privacy.

## **8. RAM-Only Servers**

Some modern VPNs use RAM-only servers, meaning:

- Data is never stored on hard drives
- When the server restarts, all data is erased automatically

This increases privacy and reduces the risk of logs being recovered.

## **9. Obfuscation**

Obfuscation hides VPN traffic and makes it look like normal HTTPS traffic.

Useful for:

- Bypassing restrictions
- Avoiding VPN blocks
- Using VPN in countries with censorship

## **10. Split Tunneling**

Lets you choose which apps use the VPN and which use normal internet.

Example:

- Browser → through VPN
- Banking app → direct internet

Improves control, speed, and compatibility.

## **7. summary on VPN benefits and limitations**

- ❖ A VPN enhances online privacy by encrypting internet traffic and hiding your real IP address, making it harder for ISPs, websites, and attackers to track you. It protects users on public Wi-Fi, prevents data interception, and can offer limited access to geo-restricted content. VPNs also reduce exposure to common cyber threats by creating a secure encrypted tunnel.
- ❖ However, VPNs have limitations such as slower browsing speeds, server congestion, and possible connection drops. Free VPNs may include data caps, fewer server options, or weaker privacy policies. A VPN improves security but is not a complete protection tool on its own.