

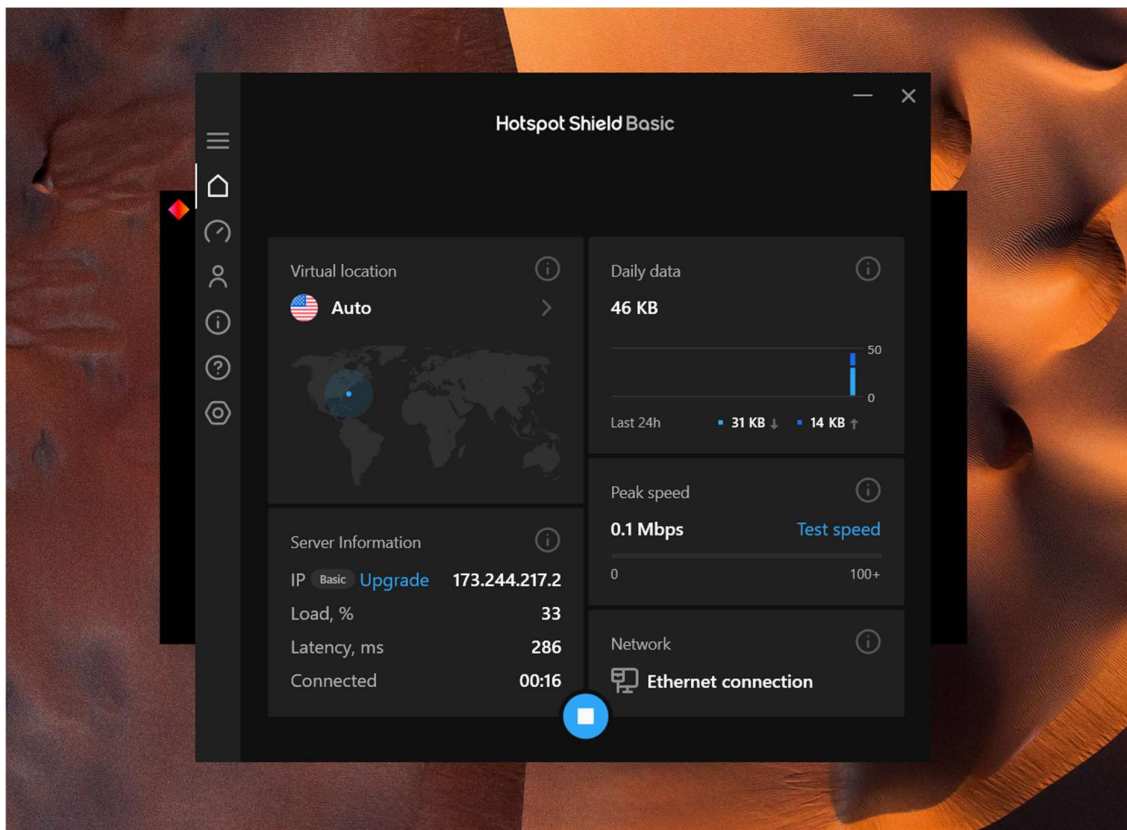
Task 8: Exploring How VPNs Work along with Considering Their Privacy Benefits

VPNs help keep connections secure on the internet protecting personal information.

Think about ProtonVPN or think about Windscribe for getting a VPN service that is free. Any preferred provider is able to give one to you also.

A VPN provider that is trusted should be selected and then installed first. Skip this step in case it's already installed. If you do not, get yourself an account then download that setup file from off of the official website for the provider.

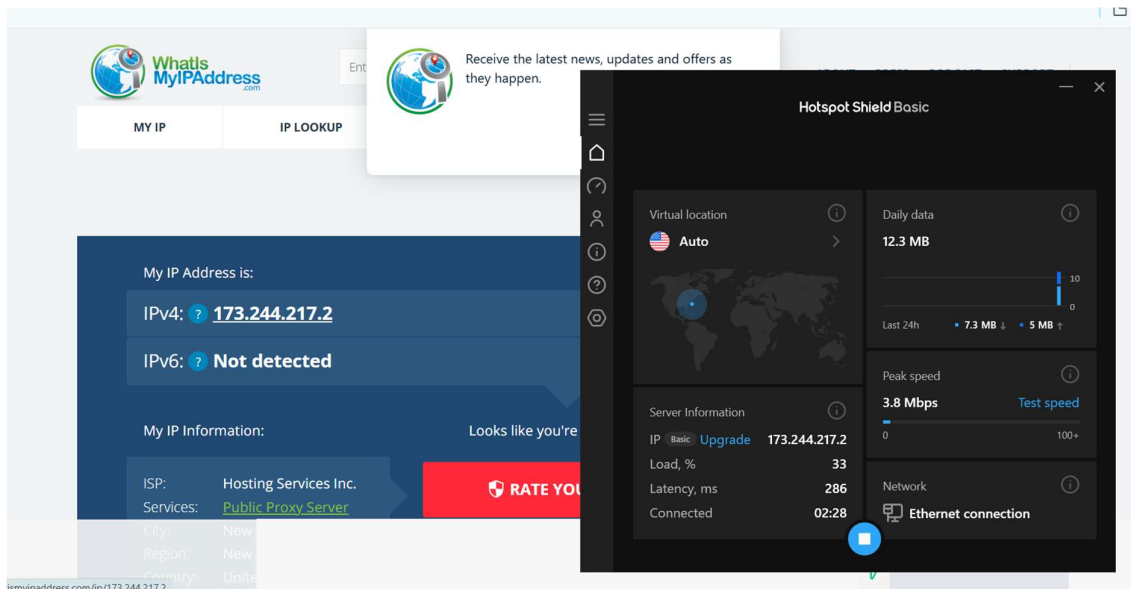
Example used: hotspotshield.com/vpn.



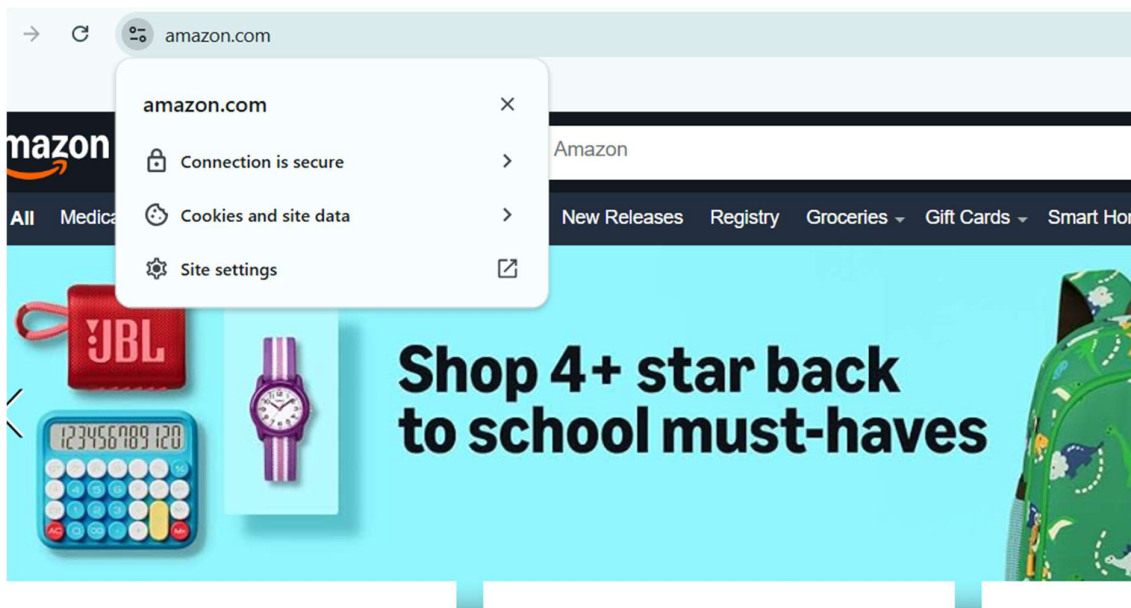
Open the VPN software when installation is complete. For setup, use default settings unless specific configuration is something you require.

Establish for yourself a VPN session by way of the app. The app is having a “Connect” option for users. Located often in the United States, most clients auto-select the fastest available server.

Visit a site such as <https://whatismyipaddress.com> to confirm your VPN is active. This visit is one that will allow for you to check on if your IP address has had changes. The IP that is shown should match the one provided by the VPN server.



Visit a protected website like <https://amazon.com>. Employ HTTPS that displays a padlock icon also ensure browsing works using the VPN.

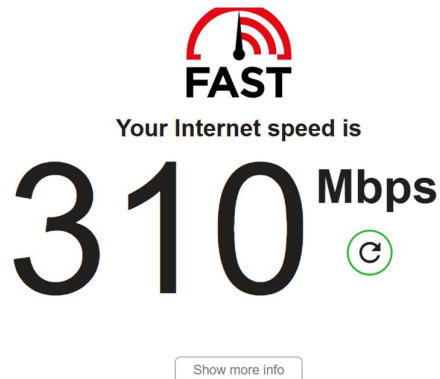


Disconnect from the VPN. Check your internet speed both when using and without the VPN active. Impact upon performance evaluation occurs.

Net Speed while vpn is connect



While vpn is not connect



VPN Security and Privacy Essentials

A VPN forms an encrypted “tunnel” between your device with the internet, and this shields your data from threats—especially over insecure networks.

Encryption Protocols: It uses the standards in regard to securing of traffic such as IKEv2, WireGuard, or OpenVPN.

- Data is only visible to sender along with recipient because of End-to-End Encryption.
- Your real IP is masked by IP Address Hiding. This masking can improve anonymity as well.
- Kill Switch: The Internet is cut off when the VPN drops in order that leaks are prevented.
- DNS Leak Protection makes certain of each of the private DNS requests.
- No-Logs Policy: Some VPNs track your online activity also save it not (verify provider policy).

With Privacy Improved, ISPs, hackers, and surveillance are not able to see browsing activity.

Protect your data within coffee shops plus airports. The public networks should be used with a sense of safety and so on.

Advantages of Using a VPN

- Bypass censorship restrictions or bypass geographical restrictions for accessing freely online.
- Prevent ISP Throttling: Stop ISPs slowing speeds based on data use amount.
- Secure Remote Access is indeed ideal. It allows for secure access into corporate systems while being remote.
- Since each and every bit of your traffic passes through VPN provider servers, choose with care.
- Rerouting and encryption could introduce latency decreasing some speed.
- VPNs do not block cookies or trackers. VPNs likewise fail at stopping malware.
- VPNs face restrictions or illegality in some countries under Legal Restrictions.
- Free services might feature ads or sell data because they are free; premium services have a monetary cost.