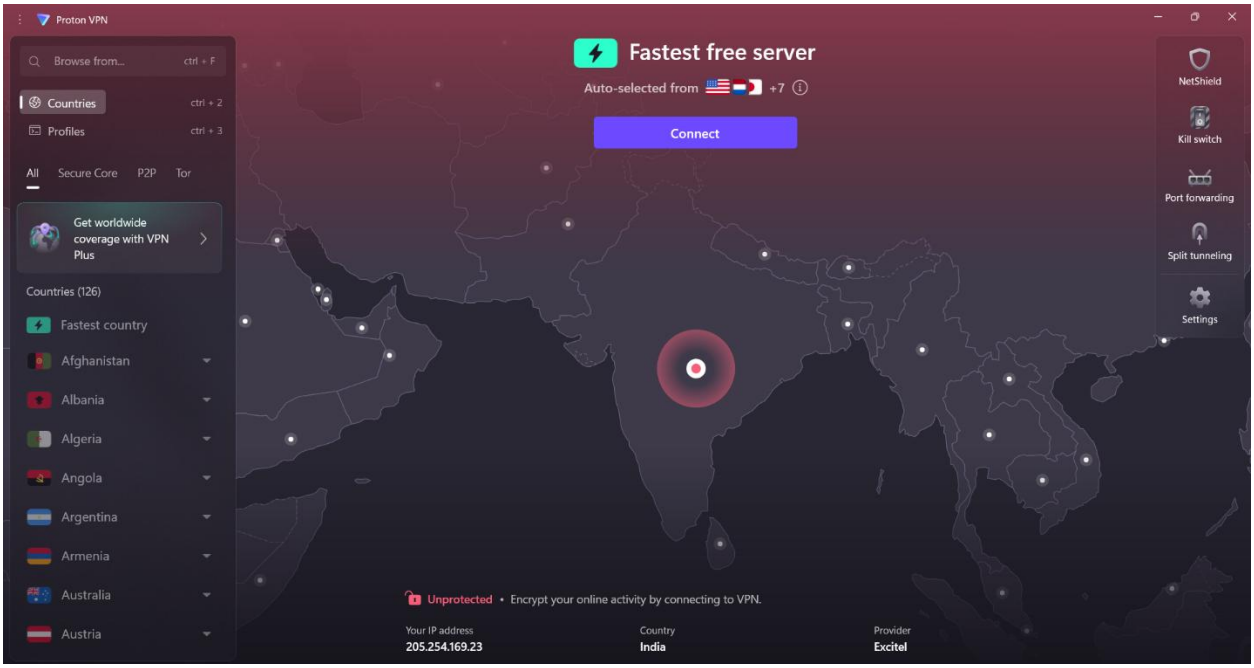
Name: satya chaitanya

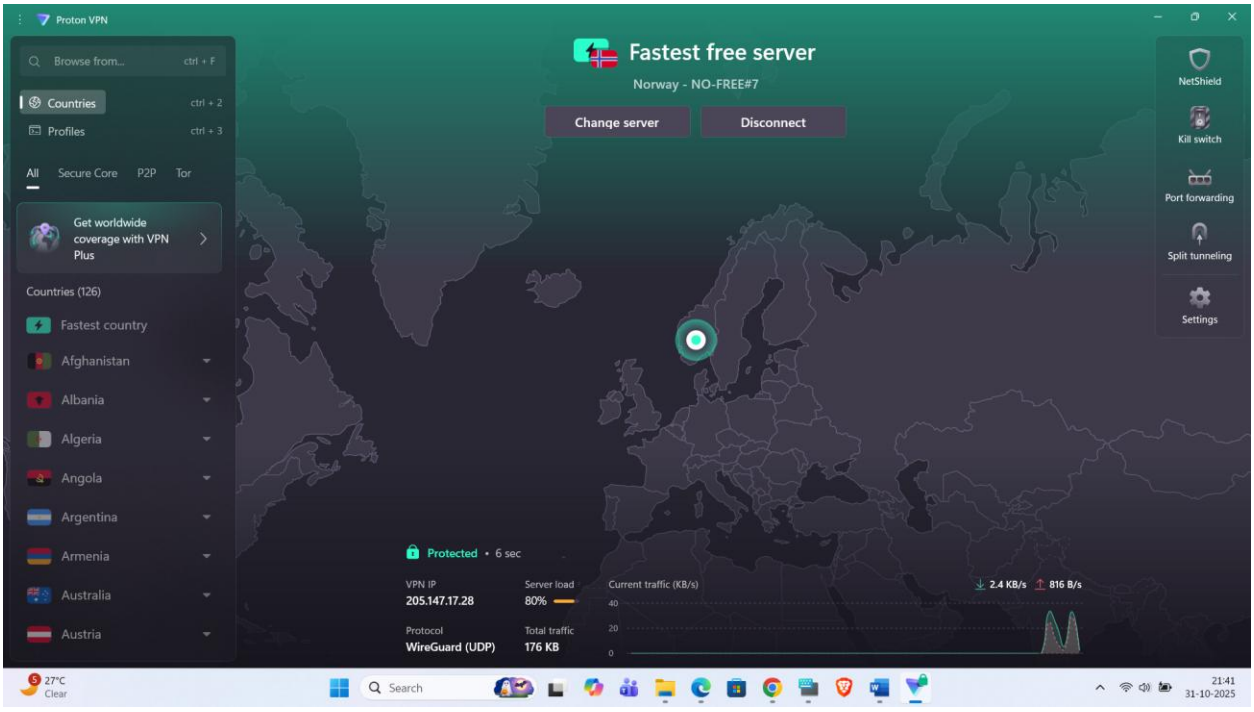
Email: satyachaitanya21@gmail.com

Task: Understand the role of VPNs in protecting privacy and secure communication**.**

Tools: proton vpn



Vpn connected

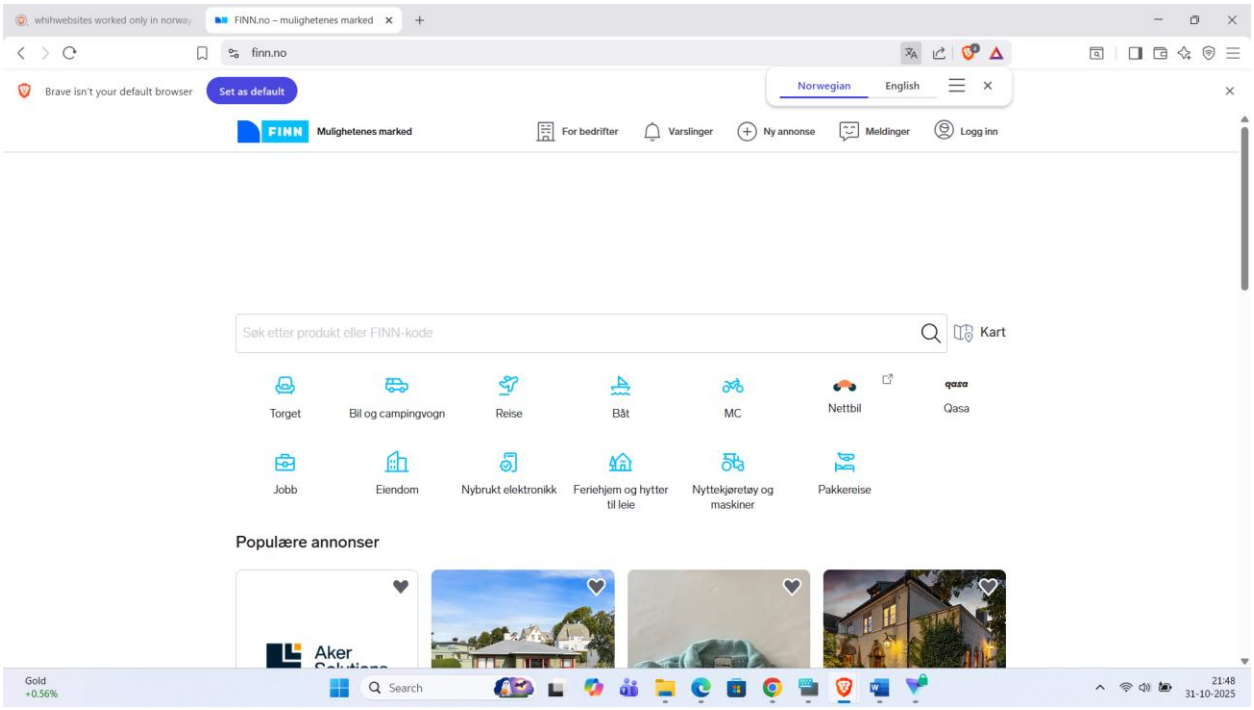


Got new ip address

Location changed from India to Norway

Browsing a website that works only in Norway. Finn.no

Moderate speed compared to normal browser usage.



VPNs use encryption to scramble your internet traffic, making it unreadable to third parties, and provide privacy by masking your IP address to hide your identity and location. Key privacy features include IP address masking, creating a secure tunnel for your data, and additional options like a kill switch, split tunneling, and multi-factor authentication.

Encryption features

Scrambles data: Encryption turns your data into "gibberish" as it travels between your device and the VPN server, preventing others from deciphering it.

Uses encryption algorithms: VPNs use algorithms like AES to encrypt and decrypt data.

Employs encryption keys: An encryption key is needed to decrypt the data, similar to a password, and longer key lengths (like 256 bits) are stronger and harder to crack.

Secures traffic: Encryption secures your data even on public networks, which are often unsecured and vulnerable to hackers.

Privacy features

- **IP address masking:** A VPN hides your real IP address and replaces it with one from the VPN server, concealing your online identity and location.
- **Creates a secure tunnel:** Your internet traffic is routed through a private, encrypted tunnel between your device and the VPN server, shielding it from your Internet Service Provider (ISP) and others.
- **Kill switch:** This feature automatically disconnects your internet if the VPN connection drops, preventing your real IP address from being exposed.
- **Split tunneling:** Allows you to route only some of your internet traffic through the VPN while other apps connect directly to the internet.
- **Multi-factor authentication (MFA):** Some services add an extra layer of security by requiring multiple forms of verification for user authentication.
- **Obfuscated servers:** These servers help hide the fact that you are using a VPN, making it more difficult for networks to detect and block VPN traffic.

Advantages of a VPN

- **Enhanced privacy and security:**

A VPN encrypts your internet traffic, making it harder for hackers, your ISP, or others to monitor your online activity. It hides your IP address, protecting your browsing history and online identity.

- **Access to geo-restricted content:**

By connecting to a server in a different location, a VPN allows you to access websites and streaming services that may be restricted in your geographic area.

- **Avoids bandwidth throttling:**

Some ISPs slow down (throttle) certain types of internet traffic, like streaming or torrenting. A VPN can prevent this by hiding your activity from your ISP.

- **Secure public Wi-Fi:**

VPNs create a secure, encrypted connection, protecting your data when you use public Wi-Fi hotspots, which are often unsecured.

- **Reduced targeted ads:**

By masking your IP address, a VPN can reduce the amount of targeted advertising you see based on your location and browsing habits

Disadvantages of a VPN

- **Slower internet speed:**

Encrypting and rerouting your traffic through a VPN server can decrease your internet speed, especially when connected to distant servers.

- **Potential security risks:**

Free or untrustworthy VPNs can be insecure, potentially logging your data, exposing you to malware, or being unable to protect you from threats like phishing. A VPN alone does not protect against all online threats.

- **Cost:**

Most reputable VPN services require a paid subscription, and premium services can be expensive.

- **VPN blocking:**

Some websites and services, particularly streaming platforms, actively block VPN connections to enforce regional restrictions, making the VPN ineffective for accessing that content.

- **Legality and other restrictions:**

Using a VPN is illegal or heavily restricted in some countries, which could lead to fines or other penalties.

- **Incomplete anonymity:**

VPNs do not guarantee complete anonymity, as they can be traced, and their level of privacy depends on the provider's logging policies.