

VPNs — What They Really Do



1. What is a VPN?

A VPN (Virtual Private Network) creates an encrypted tunnel between your device and the VPN provider.

It hides your internet traffic from:

- Your internet provider
- Anyone snooping on the local network

...but the VPN provider can now see that traffic instead.

A VPN doesn't make you anonymous. It just moves who you're trusting.

2. When a VPN is useful

- Public Wi-Fi (hotels, airports, cafés)
- Hiding browsing activity from your ISP
- Accessing region-locked content (e.g., BBC iPlayer abroad)
- Avoiding local network restrictions (e.g., school, workplace, hotel blocks)

3. When a VPN is not needed

- Home Wi-Fi (already encrypted)
- Banking, shopping, anything HTTPS
- General browsing on trusted networks
- If the VPN provider is untrustworthy

Modern HTTPS already protects most traffic.

4. The “Trust Shift”

Without a VPN → you trust your ISP

With a VPN → you trust your VPN provider

A VPN doesn't remove trust — it changes who you trust.

5. Types of VPNs

Type	Protects	Doesn't Protect	Good For
Browser VPN (Opera, Edge)	Browser only	Apps, email	Light privacy, region switching
Antivirus VPN (Norton, McAfee)	Whole device	Depends on provider	Convenience
Standalone VPN (Mullvad, Proton, Nord)	Whole device	Still requires trust	Better privacy policies

6. Do you need one?

- Home users: optional
- Travellers: useful
- Public Wi-Fi users: recommended
- Privacy-conscious users: depends on trust in provider

7. Simple Demo

1. Visit an “IP checker” website. (<https://whatismyipaddress.com>)
2. Turn on VPN
3. Refresh
4. Watch the location change

Shows the concept instantly.