# VPNs Demystified: What They Can and Can’t Do for Your Privacy

Administrator | 03/08/2025 | Online Safety

**“A VPN keeps you safe online.”**
That’s the marketing line we hear everywhere. But what does “safe” really mean? If you think a VPN makes you invisible or immune to surveillance, it’s time to get a clearer picture.

This article walks you through what VPNs actually do, what they don't, and how to choose one that doesn’t backfire.

## □□ What a VPN *Really* Does

A **Virtual Private Network (VPN)** creates an encrypted path between your device and a remote server. From that moment on, all your internet traffic appears to originate from that server, not your actual location.

This offers two key advantages:

1. **It masks your IP address**, hiding your approximate location.
2. **It bypasses local restrictions**, making it appear like you’re browsing from another country or region.

It’s like wearing a digital mask in a room full of cameras.

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com

## When a VPN Makes Sense

- **Avoiding local censorship**: If you're on a network that blocks certain sites (like in schools, offices, or authoritarian countries), a VPN can help you get around the block.
- **Remote access**: VPNs are commonly used by employees to securely connect to their company's internal systems from anywhere.

But that's where the magic ends.

## What a VPN Can't Do

Let's break a few myths.

### It doesn't make you anonymous

While it hides your IP, websites can still track you via cookies, browser fingerprinting, and more. And guess what? **Your VPN provider sees everything you do.**

### It doesn't protect you from all Wi-Fi risks

If a network is compromised or malicious, an outdated VPN client won't help much. Today, most websites use HTTPS encryption by default — that already protects your data better than many people think.

### It doesn't keep the government out

VPN companies can — and often do — comply with legal requests for data. Some store logs. Others don't. And if you log into your Google account, well… that's game over for anonymity.

## Choosing a VPN That Doesn't Betray You

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com

Here’s what to actually look for:

### □ Privacy Policy

Don't fall for “we don’t log your data” slogans. Read the fine print. Do they keep timestamps, IP addresses, DNS queries?

### □ Audit Reports

Some providers submit to third-party audits. That’s a green flag — but check when the audit happened and who did it.

### □ Encryption Standards

Look for **OpenVPN** or **WireGuard**. Avoid outdated protocols like **PPTP**, which can be cracked easily.

### □ Business Model

If the VPN is free, you’re probably the product. Look for clear explanations on how the company makes money.

### □ Jurisdiction

Where is the company based? Some countries force VPNs to hand over data without notice. Research local laws before you trust the provider.

## □□ What to Use Instead (Sometimes)

If anonymity is your goal, **Tor** is far more effective. It routes traffic through multiple relays, making it very hard to trace. Tor isn't perfect — but it’s designed for anonymity, whereas VPNs are not.

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com

## □□ A VPN is Not a Security Swiss Army Knife

For most people, **better privacy begins with better habits**, not a subscription.

□□ Combine VPN use with:

- Strong, unique passwords
- Two-factor authentication
- Regular software updates
- HTTPS-only mode
- Tracker blockers
- Secure DNS (like DNS over HTTPS)

## □□

A VPN can be helpful, but it's not the digital invisibility cloak it’s often made out to be. **Trust matters. Research matters.** And knowing what a VPN is *not* designed for will protect you more than any feature checklist.

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com