

VPN

What the service is, what it protects, and what it does not

What this service does

You get a private encrypted tunnel to a server we run. Traffic between your device and that server cannot be read by anyone on the network in between, and sites you visit see the server address rather than yours.

It uses WireGuard, a modern protocol chosen for being fast and small enough to audit.

Setting it up

- Install the WireGuard client for your platform. It is free and published by the WireGuard project.
- Add the configuration supplied with your subscription. Each device gets its own.
- Switch the tunnel on. There is nothing to configure beyond that.

Every device needs its own configuration. Sharing one across devices causes both to drop intermittently, because the tunnel expects a single peer.

What a VPN actually protects you from

It is worth being precise, because VPNs are widely oversold.

It does protect the link between your device and our server. On untrusted Wi-Fi, that is the part that is genuinely exposed.

It does hide your address from the sites you visit, and hides which sites you visit from your local network and your internet provider.

It does not make you anonymous. Logging into an account identifies you regardless of the tunnel.

It does not stop malware, phishing or a compromised device. Those are not network problems.

It does not encrypt anything past our server. Traffic continues to the destination as normal from there.

Troubleshooting

- If nothing loads while connected, turn the tunnel off and confirm the connection works without it first.
- If it drops repeatedly, check the same configuration is not active on another device.
- Some public networks block VPN traffic outright. That is the network, not the service.

HostCommerceAI - questions about anything in this guide are worth a support ticket. This document describes the service as it works today; if something here does not match what you are seeing, tell us, because one of the two is wrong.