Wigington Security Group

Privacy consulting for individuals and families

VPN Selection & Setup Guide

Choose a trustworthy VPN and configure it properly

What You'll Learn:

- What VPNs actually do (and don't do)
- How to identify VPN scams and marketing lies
- Trustworthy providers: Mullvad, IVPN, ProtonVPN
- When to use a VPN (and when you don't need one)
- Setup on Windows, Mac, iOS, Android, Linux
- Kill switches, DNS leaks, and split tunneling
- Common mistakes and how to avoid them

The VPN Industry Has a Problem:

- 90% of VPN advertising is misleading or false
- Major review sites are paid affiliates
- "Free" VPNs often sell your data
- Many "no-log" VPNs secretly log everything
- Celebrity endorsements mean nothing
- You probably don't need a VPN for what you think

This guide cuts through the BS.

February 2026 • 22 Pages • Free Download

wigingtonsecurity.com

Contents

1 Understanding VPNs: What They Actually Do

1.1 VPN Basics

What VPN stands for: Virtual Private Network

What it actually does:

1. Creates encrypted tunnel from your device to VPN server
2. Your internet traffic goes through this tunnel
3. To websites, your traffic appears to come from VPN server's location
4. Your ISP sees encrypted tunnel, not your actual activity

Visual representation:

```
Without VPN:
You → ISP (sees everything) → Website

With VPN:
You → Encrypted Tunnel → VPN Server → Website
     ↑                                  ↑
ISP sees tunnel              Website sees VPN server
(not your activity)          (not your real IP)
```

1.2 What VPNs Actually Protect Against

VPNs ARE useful for:

- **Public WiFi protection:** Prevents others on same network from intercepting your traffic
- **ISP tracking:** Prevents ISP from seeing which websites you visit
- **Geolocation bypass:** Access region-locked content (Netflix, BBC iPlayer)
- **Hiding IP address:** Websites don't see your real IP address
- **Government censorship bypass:** Access blocked websites in restrictive countries
- **Price discrimination prevention:** Avoid dynamic pricing based on location

1.3 What VPNs Do NOT Protect Against

CRITICAL

VPNs do NOT provide:

- **Anonymity:** You're not anonymous. VPN knows who you are.
- **Complete privacy:** You're shifting trust from ISP to VPN provider
- **Malware protection:** VPNs don't block viruses or malicious websites
- **Protection from logged-in accounts:** Facebook knows who you are even through VPN
- **Legal immunity:** Illegal activity is still illegal through VPN
- **Protection from government surveillance:** Most VPNs comply with lawful data requests
- **Cookie/tracker blocking:** VPN doesn't stop website tracking technologies
- **Faster internet:** VPNs typically slow your connection

1.4 The VPN Marketing Lie

What VPN ads claim:

- "Military-grade encryption" (meaningless term)
- "Complete anonymity online" (false)
- "Protection from hackers" (not what VPNs do)
- "Bank-level security" (marketing nonsense)
- "No logs, guaranteed!" (many lie about this)

Why VPN marketing is so aggressive:

- High profit margins (80%+)
- Recurring subscription model
- Affiliate programs pay $100+ per signup
- Review sites are all affiliate marketers
- YouTubers get massive sponsorship deals
- Fear-based marketing works

Warning

Trust no VPN review that:

- Contains affiliate links
- Is sponsored by a VPN company
- Claims one VPN is "best for everyone"
- Doesn't mention limitations
- Ranks 5+ VPNs with minor differences
- Uses language like "military-grade" or "unhackable"

99% of VPN reviews online are paid affiliate content disguised as journalism.

1.5 When You Actually Need a VPN

You should use a VPN if:

Action Checklist

- [ ] You regularly use public WiFi (coffee shops, airports, hotels)
- [ ] You want to prevent ISP from seeing browsing history
- [ ] You access region-locked content (streaming services)
- [ ] You travel internationally and want access to home content
- [ ] You live in country with internet censorship
- [ ] You want to prevent websites from knowing your location
- [ ] You're a journalist, activist, or at-risk individual
- [ ] You torrent and want to hide activity from ISP

You probably DON'T need a VPN if:

- You only use home WiFi with HTTPS websites (already encrypted)
- You think it will make you "anonymous" (it won't)
- You think it protects against viruses (it doesn't)
- You think it will speed up your internet (it slows it down)
- A YouTuber told you to get one (they're paid to say that)

2 Trustworthy VPN Providers

2.1 Selection Criteria

We only recommend VPNs that meet ALL of these criteria:

Action Checklist

Non-negotiable requirements:

- **No-logs policy** verified by independent audit
- **Jurisdiction** outside 5/9/14 Eyes surveillance alliances
- **Open-source apps** (or security audits)
- **Accepts anonymous payment** (cryptocurrency, cash)
- **No email required** for signup
- **Kill switch** that actually works
- **WireGuard or OpenVPN** protocols
- **No history** of data breaches or scandals
- **Clear ownership** (not shell companies)

2.2 The Three We Recommend

Only three VPN providers meet our strict criteria:

1. **Mullvad** — Best overall, most private
2. **IVPN** — Close second, excellent transparency
3. **ProtonVPN** — Best for beginners, great free tier

Why only three? Because we won't recommend services we don't fully trust. Most VPNs fail our criteria.

2.3 Detailed Comparison

Feature	Mullvad	IVPN	ProtonVPN
Price	€5/month	$6/month (Standard)	Free, €10/month (Plus)
Jurisdiction	Sweden (good)	Gibraltar (excellent)	Switzerland (excellent)
No-logs verified	Yes (audit 2024)	Yes (audit 2024)	Yes (audit 2023)
Email required	No	No	Yes (but can use ProtonMail)
Anonymous payment	Yes (cash, crypto)	Yes (cash, crypto)	Yes (crypto)
Account system	Number only (no email)	Number/email	Email required

Feature	Mullvad	IVPN	ProtonVPN
Open source	Yes (apps)	Yes (apps)	Yes (apps)
Protocols	WireGuard, OpenVPN	WireGuard, OpenVPN	WireGuard, OpenVPN, IKEv2
Kill switch	Excellent	Excellent	Good
Servers	850+ in 40+ countries	120+ in 40+ countries	6,000+ in 110+ countries
Speed	Excellent	Excellent	Good to excellent
Streaming	Works (not guaranteed)	Works (not guaranteed)	Works well
Simultaneous devices	5	7 (Standard)	10 (Plus)
Free tier	No	No	Yes (limited servers)
Port forwarding	Yes	Yes	Yes (Plus)
Split tunneling	Yes	Yes	Yes
Warrant canary	No (but publishes transparency)	Yes	No
Company history	15+ years, pristine	15+ years, pristine	10+ years, good
Best for	Privacy maximalists	Balance of features and privacy	Beginners, free tier users
Our rating	A+	A	A

2.4 Mullvad — Our Top Pick

Why Mullvad is our #1 recommendation:

- **Account system:** You get a random account number. No email, no name, nothing.
- **Payment:** Can literally mail them cash in an envelope
- **Logging:** Independently audited no-logs policy
- **Transparency:** Publishes police raid responses, warrant disclosures
- **Pricing:** Single flat rate, no tiers, no upsells
- **No bullshit:** Doesn't make false security claims
- **Open source:** All apps are open source
- **WireGuard:** They helped develop WireGuard protocol

Downsides:

- Fewer servers than competitors (but still plenty)
- No free tier
- Streaming support not guaranteed (works but not priority)
- Account number can be lost (no email recovery)

Best for: Privacy-conscious users, anyone who wants maximum anonymity
Price: €5/month (~$5.30/month), no annual discount
Website: https://mullvad.net

2.5 IVPN — Excellent Alternative

Why IVPN is also trustworthy:

- **Transparency:** Publishes detailed transparency reports
- **Audits:** Regular independent security audits
- **No BS marketing:** Honest about what VPNs can/can't do
- **Anonymous signup:** No email required
- **Payment:** Accepts cash and crypto
- **Jurisdiction:** Gibraltar (outside 14 Eyes)
- **Open source:** All apps open source
- **Multi-hop:** Option to route through 2 VPN servers

Downsides:

- More expensive than Mullvad
- Smaller server network
- Two-tier pricing (Standard vs Pro)

Best for: Users who want warrant canary and multi-hop
Price: $6/month (Standard) or $10/month (Pro)
Website: https://www.ivpn.net

2.6 ProtonVPN — Best for Beginners

Why ProtonVPN is third choice:

- **Free tier:** Actually usable free version (limited servers, one device)
- **Company:** From makers of ProtonMail (good reputation)
- **Jurisdiction:** Switzerland (strong privacy laws)
- **Audited:** Independent no-logs audit completed
- **Secure Core:** Routes through privacy-friendly countries first
- **Streaming:** Works well with Netflix, others
- **User-friendly:** Best apps for beginners
- **Integration:** Works with ProtonMail ecosystem

Downsides:

- Requires email (but can use ProtonMail)

- More expensive at top tier
- Some features locked behind Plus tier
- Not quite as minimal as Mullvad/IVPN

Best for: Beginners, users who want free tier, ProtonMail users
Price: Free (limited) or €10/month (Plus)
Website: https://protonvpn.com

2.7 VPNs We Do NOT Recommend

Warning

Avoid these popular VPNs:

- **NordVPN:** Data breach in 2018, aggressive misleading marketing
- **ExpressVPN:** Owned by Kape Technologies (former malware company)
- **CyberGhost:** Also owned by Kape Technologies
- **Private Internet Access:** Also owned by Kape Technologies
- **Surfshark:** Merged with Nord, same concerns
- **IPVanish:** Logged user data despite "no-logs" claims
- **HideMyAss:** Gave logs to authorities, admitted logging
- **Hola VPN:** Not a real VPN, peer-to-peer botnet, dangerous
- **ANY free VPN:** If you're not paying, they're selling your data

Red flags:

- Owned by Kape Technologies / Gaditek
- Based in US, UK, Australia (Five Eyes)
- No independent audit
- Requires extensive personal info
- Aggressive affiliate marketing
- Celebrity endorsements
- "Lifetime" subscriptions (unsustainable, will shut down)

3 VPN Setup and Configuration

3.1 Mullvad Setup (Recommended)

3.1.1 Account Creation

Action Checklist

1. Visit https://mullvad.net
2. Click "Get started"
3. Click "Generate account number"
4. **CRITICAL:** Save your account number immediately
   - It's a 16-digit number
   - This is your ONLY login credential
   - If you lose it, your account is gone forever
   - Save it in password manager
   - Write it down on paper as backup
5. Add time to account (payment options):
   - Credit/debit card
   - PayPal
   - Cryptocurrency (Bitcoin, Bitcoin Cash, Monero)
   - Cash by mail (anonymous)
   - Swish (Sweden), bank wire
6. No confirmation email—you're done

3.1.2 Windows Setup

1. Download: https://mullvad.net/download/app/
2. Run installer (MullvadVPN-*.exe)
3. Open Mullvad app
4. Enter your account number
5. Click "Login"
6. App connects to nearest server automatically

Configure settings:

Action Checklist

- Settings → Enable kill switch (always on)
- Settings → Auto-connect: On (connects on startup)
- Settings → Protocol: WireGuard (recommended)
- Settings → DNS: Use Mullvad DNS
- Advanced → Enable LAN sharing (if needed for home network)
- Test: Visit https://mullvad.net/check to verify connection

3.1.3 macOS Setup

1. Download from https://mullvad.net/download/app/
2. Open DMG file
3. Drag Mullvad to Applications
4. Open Mullvad from Applications
5. Enter account number
6. Grant VPN permission when macOS prompts

Configure (same as Windows above)

3.1.4 iOS Setup

1. Download "Mullvad VPN" from App Store
2. Open app
3. Enter account number
4. Tap "Login"
5. When iOS prompts: "Mullvad wants to add VPN configurations" → Allow
6. App connects to nearest server

iOS-specific settings:

Action Checklist

- Settings (in Mullvad app) → Always require VPN: ON
- Settings → Protocol: WireGuard
- iOS Settings → VPN → Connect On Demand: Enable

3.1.5 Android Setup

1. Download from Google Play Store or https://mullvad.net/download/app/
2. Open Mullvad app
3. Enter account number
4. Tap "Login"
5. Android prompts: "Connection request" → OK
6. App connects

Android-specific settings:

Action Checklist

Settings → Always-on VPN: Enable

Settings → Block connections without VPN: Enable

Protocol: WireGuard

3.2 Kill Switch Explained

What it is: Feature that blocks all internet if VPN disconnects.
Why it matters: Prevents accidental data leaks if VPN drops.
How to verify it works:

1. Connect to VPN
2. Visit https://ipleak.net and note your VPN IP
3. Manually disconnect VPN
4. Try to visit any website
5. If kill switch works: No connection, pages won't load
6. If kill switch fails: Pages load, you're exposed

All three recommended VPNs have reliable kill switches.

3.3 DNS Leak Protection

What DNS leaks are: Even with VPN, your DNS queries might go to ISP.
Why it matters: ISP can see which websites you visit even through VPN.
How to test for DNS leaks:

1. Connect to VPN
2. Visit https://dnsleaktest.com
3. Click "Extended test"

4. Check results:
    - Good: DNS servers belong to VPN provider
    - Bad: DNS servers belong to ISP or Google

Fix for DNS leaks:

- Mullvad: Settings → DNS → Use Mullvad DNS
- IVPN: Settings → AntiTracker DNS
- ProtonVPN: Automatically uses Proton DNS

3.4 Split Tunneling

What it is: Route only some apps through VPN, rest through normal connection.

Use cases:

- Banking apps work better without VPN
- Local streaming services block VPNs
- Want to access local network printer while VPN is on
- Gaming with lower latency

Setup (Mullvad example):

1. Settings → Split tunneling
2. Add apps that should bypass VPN
3. Those apps use normal connection, everything else uses VPN

Security consideration: Apps in split tunnel are not protected by VPN. Use carefully.

4 VPN Best Practices and Common Mistakes

4.1 When to Use VPN

Always use VPN for:

Action Checklist

- Public WiFi (coffee shops, airports, hotels)
- Torrenting
- Accessing region-locked content
- Travel in countries with censorship
- Preventing ISP tracking

Don't bother with VPN for:

- Home WiFi browsing HTTPS websites (already encrypted)
- Banking (may trigger fraud alerts)
- Local services (may break local access)
- When you need maximum speed

4.2 Common Mistakes to Avoid

4.2.1 Mistake 1: Thinking VPN Makes You Anonymous

Warning

VPN Anonymity
You are NOT anonymous when using a VPN if:

- You're logged into accounts (Google, Facebook, etc.)
- You're using same browser fingerprint
- You're accessing personal email
- Websites use cookies to track you

VPN hides your IP from websites. It does NOT hide your identity from websites where you're logged in.

For actual anonymity: Use Tor Browser, not VPN.

4.2.2 Mistake 2: Using Free VPNs

CRITICAL

Free VPNs are never free. You pay with your data.
Free VPN business models:

- Selling your browsing data to advertisers
- Injecting ads into your browsing
- Using your device as exit node (like Hola)
- Malware and tracking
- Harvesting personal information

Rule: Never use a free VPN. Period.
Exception: ProtonVPN free tier is legitimate (but limited).

4.2.3 Mistake 3: Trusting VPN Marketing Claims

Marketing lies you'll see:

- **"Military-grade encryption":** Meaningless marketing term
- **"Unhackable":** Nothing is unhackable
- **"Complete anonymity":** False, VPNs don't provide anonymity
- **"No logs guaranteed":** Many VPNs lie about this
- **"Protects from hackers":** Not what VPNs do
- **"Speeds up your internet":** VPNs slow down internet, not speed it up

Reality check: If a VPN makes extraordinary claims, it's lying.

4.2.4 Mistake 4: Not Using Kill Switch

Scenario: VPN disconnects (server issue, network change, etc.)
Without kill switch:

- Your traffic continues unencrypted
- Your real IP is exposed
- ISP sees your activity
- You may not even notice

With kill switch:

- Internet cuts off immediately

- No data leaks
- You notice right away
- Reconnect VPN before continuing

Always enable kill switch.

4.2.5 Mistake 5: Using VPN on Untrusted Devices

- Work computer with employer monitoring: They can see your VPN use
- Public computer: Don't log into your VPN account
- Borrowed device: Don't enter your VPN credentials

Why: VPN doesn't protect against local surveillance (keyloggers, screen monitoring).

4.3 Multi-Hop / Double VPN

What it is: Traffic routes through two VPN servers instead of one.
Example: You → VPN Server 1 (Sweden) → VPN Server 2 (Switzerland) → Internet
Pros:

- Extra layer of protection
- Even VPN provider can't correlate entry and exit traffic
- Useful in high-risk scenarios

Cons:

- Significantly slower (double encryption)
- Higher latency
- Probably overkill for most users

Availability:

- IVPN: Built-in multi-hop feature
- ProtonVPN: "Secure Core" feature
- Mullvad: Can configure manually

Recommendation: Only use if you have specific threat model requiring it.

4.4 VPN + Tor

Two approaches:

1. **VPN → Tor:** Connect to VPN, then use Tor Browser
   - Hides Tor usage from ISP
   - Tor entry node doesn't see your real IP
   - Useful if Tor is blocked in your country
2. **Tor → VPN:** Connect to Tor, then VPN (complex setup)
   - Exit node doesn't see your real IP
   - VPN knows you're using Tor
   - Rarely necessary

For most privacy use cases: Tor alone is sufficient. Don't overcomplicate.

5 Advanced Topics

5.1 VPN Protocols Explained

Protocol	Description	Speed	Security
WireGuard	Modern, fast, open source. Best choice.	Excellent	Excellent
OpenVPN	Older, slower, but battle-tested. Reliable fallback.	Good	Excellent
IKEv2/IPSec	Fast, good for mobile. Less popular.	Excellent	Good
L2TP/IPSec	Outdated, avoid.	Poor	Compromised
PPTP	Obsolete, broken security. Never use.	Fast	Broken
SSTP	Windows-only, less audited.	Good	Good

Recommendation: Use WireGuard if available. Fall back to OpenVPN if needed.

5.2 Server Selection Strategy

Factors to consider:

- **Distance:** Closer = faster. Connect to nearby server when speed matters.
- **Load:** Overloaded servers are slow. Check server load in app.
- **Jurisdiction:** For maximum privacy, choose servers in privacy-friendly countries (Switzerland, Iceland, Sweden).
- **Streaming:** Some servers work better with streaming services. Test different locations.
- **Torrenting:** Some VPNs designate P2P-friendly servers. Use those for torrents.

Privacy-friendly server locations:

- Switzerland: Strong privacy laws, outside 14 Eyes
- Iceland: Strong privacy protections
- Sweden: Good privacy laws (but technically 14 Eyes)
- Netherlands: Good infrastructure, privacy-friendly

Avoid if privacy is critical:

- US, UK, Australia, Canada, New Zealand (Five Eyes)
- China, Russia, North Korea (authoritarian surveillance)

5.3 Port Forwarding

What it is: Allows incoming connections to your device through VPN.

Use cases:

- Torrenting (better peer connectivity)
- Running servers
- Gaming (hosting)

- Remote access

  Security consideration: Port forwarding reduces anonymity. Only use if necessary.
  Availability:

- Mullvad: Supports port forwarding
- IVPN: Supports port forwarding
- ProtonVPN: Supports (Plus tier)

5.4 VPN on Router

Pros:

- Protects all devices on network automatically
- No per-device setup needed
- Covers devices that can't run VPN apps (smart TVs, IoT)
- Single VPN connection counts toward device limit

  Cons:

- Slower (router does encryption)
- All devices must use VPN (can't exclude)
- More complex setup
- If VPN drops, entire network loses internet

  Compatible routers:

- FlashRouters (pre-configured)
- DD-WRT compatible routers
- GL.iNet travel routers (easy VPN setup)

  Setup: Beyond scope of this guide. Check VPN provider documentation.

5.5 Torrenting with VPN

Why VPN for torrents:

- Hides your IP from other peers
- Prevents ISP from seeing torrent activity
- Avoids ISP throttling
- Reduces copyright notice risk

Best practices:

Action Checklist

- Use VPN that allows P2P (all three recommended do)
- Enable kill switch (critical—prevents IP leaks if VPN drops)
- Bind torrent client to VPN interface (prevents leaks)
- Use port forwarding for better speeds
- Test for IP leaks: https://ipleak.net

Binding torrent client to VPN (example: qBittorrent):

1. Tools → Options → Advanced → Network Interface
2. Select VPN interface (e.g., Mullvad, IVPN, ProtonVPN)
3. This ensures torrents ONLY work when VPN is connected

6 Troubleshooting Common Issues

6.1 VPN Won't Connect

Try in this order:

1. Check internet connection (disconnect VPN, verify internet works)
2. Try different server location
3. Switch protocol (WireGuard OpenVPN)
4. Restart VPN app
5. Restart computer/device
6. Check firewall isn't blocking VPN
7. Reinstall VPN app
8. Contact VPN support

6.2 Slow Speeds

Speed reduction is normal. VPN adds overhead. Expect 10-50% slower speeds.

If speeds are extremely slow:

☑ Action Checklist

- Try servers closer to your location
- Switch to WireGuard protocol (faster than OpenVPN)
- Check server load (choose less crowded server)
- Test your base internet speed without VPN
- Disable kill switch temporarily (test if it's the cause)
- Try different time of day (peak hours = slower)

6.3 Streaming Services Block VPN

Why this happens: Netflix, Hulu, BBC iPlayer actively block known VPN IPs.

Solutions:

1. Try different server in same country
2. Contact VPN support for streaming-optimized servers
3. Try different protocol
4. Use residential IP servers (if VPN offers)
5. Accept that some streaming services effectively block all VPNs

Reality: Cat-and-mouse game. VPNs find workarounds, streaming services block them, repeat.

6.4 Banking Site Blocks VPN

Why: Banks block VPNs to prevent fraud (reasonable security measure).

Solutions:

1. Disconnect VPN for banking
2. Use split tunneling to exclude banking app
3. Connect to server in your home country
4. Call bank to whitelist your VPN IP (unlikely to work)

Recommendation: Just disconnect VPN for banking. Your bank's website is already encrypted (HTTPS).

6.5 Can't Access Local Network Devices

Problem: Printer, NAS, smart home devices unreachable while VPN is on.

Solution:

- **Mullvad:** Settings → Enable LAN sharing
- **IVPN:** Settings → Allow LAN access
- **ProtonVPN:** Preferences → Allow LAN connections

This allows local network traffic while keeping internet traffic through VPN.

7 Final Recommendations

7.1 The Bottom Line

Do you need a VPN?

- **Probably yes** if you use public WiFi regularly
- **Maybe** if you want to hide browsing from ISP
- **Probably no** if you only use home WiFi and don't torrent

Which VPN should you choose?

- **Most users:** Mullvad ($\tilde{\$}5$/month)
- **Want free tier:** ProtonVPN (free is limited, upgrade to Plus if needed)
- **Want warrant canary:** IVPN ($6/month)

What to avoid:

- Free VPNs (except ProtonVPN free tier)
- VPNs owned by Kape Technologies
- VPNs with no independent audit
- VPNs making ridiculous marketing claims
- VPNs based in Five Eyes countries

7.2 Setup Checklist

Action Checklist

After choosing and installing VPN:

- [ ] Enable kill switch
- [ ] Set to auto-connect on startup (optional but recommended)
- [ ] Choose WireGuard protocol
- [ ] Use VPN's DNS servers
- [ ] Test for DNS leaks: https://dnsleaktest.com
- [ ] Test for IP leaks: https://ipleak.net
- [ ] Verify kill switch works (disconnect VPN, internet should stop)
- [ ] Save account credentials in password manager
- [ ] Install on all devices you'll use
- [ ] Configure split tunneling if needed

7.3 Ongoing Maintenance

Action Checklist

Monthly:

- [ ] Update VPN app when prompted
- [ ] Check for IP/DNS leaks

Quarterly:

- [ ] Review VPN provider (any scandals, audits, changes?)
- [ ] Test kill switch functionality
- [ ] Verify payment is current

Annually:

- [ ] Re-evaluate if you still need VPN
- [ ] Check if better VPN options available
- [ ] Review this guide for updates

7.4 Additional Resources

VPN provider websites:

- Mullvad: https://mullvad.net
- IVPN: https://www.ivpn.net
- ProtonVPN: https://protonvpn.com

Testing tools:

- DNS Leak Test: https://dnsleaktest.com
- IP Leak Test: https://ipleak.net
- Mullvad Check: https://mullvad.net/check

Independent VPN analysis:

- Privacy Guides: https://www.privacyguides.org/en/vpn/
- That One Privacy Site (archived): https://thatoneprivacysite.net

WigSec guides:

- Phone & Device Hardening (includes VPN on mobile)
- Email Security & Privacy
- Complete Data Broker Removal

- Password Manager Setup

All free at: https://wigingtonsecurity.com/guides

Need Help Choosing or Setting Up a VPN?

We offer personalized VPN consultation and setup assistance.

Services:

- VPN Selection Consultation ($50)
- Complete Setup & Configuration ($75)
- Network-Wide VPN Setup ($150)
- Business VPN Strategy ($200)

Contact: https://wigingtonsecurity.com/contact
Schedule: https://wigingtonsecurity.com/services

Remote and in-person support available

Document Version 1.0 • February 2026

https://wigingtonsecurity.com