**Nome:** _____ **Data:** _____ **Punteggio:** _____

## PUNTO DI CONTROLLO 10

# Domande frequenti sulle VPN

*Scheda di lavoro interattiva e guida allo studio*

Basato su la guida alle VPN di VPN.com: **https://www.vpn.com/it/vpn/**

Scheda di lavoro: che cos'è una VPN

# Punto di controllo 10: Domande frequenti di base sulle VPN (Parte A)

Rivedi le domande e le risposte più comuni che i potenziali clienti pongono sull'uso delle reti private virtuali.

### Q1: Che cos'è una VPN e come funziona?

Una Virtual Private Network (VPN) cifra la tua connessione Internet e instrada il tuo traffico attraverso un server remoto sicuro. In questo modo maschera il tuo indirizzo IP pubblico e limita ciò che gli osservatori della rete locale e il tuo ISP possono vedere del traffico instradato attraverso il tunnel VPN.

### Q2: Perché dovrei usare una VPN?

Una VPN protegge la tua privacy digitale, mette al sicuro la connessione sulle reti Wi-Fi pubbliche (come bar o aeroporti), può ridurre il throttling basato sull'attività quando l'ISP non riesce a identificare il tipo di traffico cifrato, aggira le restrizioni geografiche per accedere a contenuti globali e aiuta a proteggere le risorse di lavoro da remoto.

### Q3: Una VPN mi rende completamente anonimo online?

No. Anche se una VPN nasconde il tuo indirizzo IP e crittografa il traffico, puoi comunque essere tracciato tramite i cookie del browser, gli account attivi (come Google o Facebook), il fingerprinting del browser o se il tuo provider VPN registra i tuoi dati.

### Q4: Una VPN rallenterà la mia connessione a internet?

Sì, leggermente. Il processo di crittografia e la distanza fisica dal server VPN aggiungono latenza e overhead. L'impatto varia in base a provider, protocollo, distanza del server, dispositivo e condizioni di rete.

### Q5: Usare una VPN è legale?

L'uso di una VPN è legale in molti paesi, ma alcune giurisdizioni limitano, regolamentano o bloccano i servizi VPN. Gli utenti dovrebbero verificare le leggi locali vigenti prima dell'uso. Per maggiori dettagli, consulta le guide sulla legalità su VPN.com.

# Punto di controllo 10: Domande frequenti di base sulle VPN (Parte B)

Rivedi le domande e le risposte più comuni che i potenziali clienti pongono sull'uso delle reti private virtuali.

### Q6: Posso usare una VPN gratuita?

Le VPN gratuite possono basarsi su pubblicità, funzioni limitate, analisi di utilizzo, limiti di dati o altri modelli di monetizzazione. Gli utenti dovrebbero esaminare l'informativa sulla privacy, la proprietà, gli audit e il modello di business del fornitore prima di usarla.

### Q7: Cos'è una politica di "no-logs" (assenza di registri)?

Una politica no-log descrive quali dati di attività e di connessione un provider dichiara di non conservare. L'ambito esatto varia, quindi i lettori dovrebbero consultare la politica e i risultati degli audit indipendenti.

### Q8: Come scelgo la VPN migliore?

Cerca politiche no-log sottoposte ad audit, protocolli solidi (WireGuard, OpenVPN), posizioni dei server sicure, velocità elevate, server solo RAM, una funzione kill switch e una giurisdizione al di fuori delle alleanze di condivisione dell'intelligence (come i 5/9/14 Eyes).

### Q9: Posso usare una VPN sul telefono e sulla smart TV?

Sì. I provider VPN moderni offrono app dedicate per iOS, Android, macOS, Windows, Linux e smart TV, oltre a configurazioni per router che proteggono tutti i dispositivi della tua rete domestica.

### Q10: Che cos'è un Kill Switch?

Il Kill Switch è una funzione di sicurezza che scollega automaticamente il dispositivo da Internet se la connessione VPN cade. In questo modo i tuoi dati non cifrati o il tuo vero indirizzo IP non vengono esposti.

# Punto di controllo 10: Domande frequenti avanzate sulle VPN (Parte C)

Esplora gli aspetti tecnici e strutturali delle reti private virtuali e dei protocolli di tunneling sicuro.

### Q1: Qual è la differenza tra WireGuard, OpenVPN e IKEv2?

WireGuard è un protocollo moderno e leggero (solo circa 4.000 righe di codice) che offre velocità elevate e tempi di connessione rapidi. OpenVPN è un protocollo open source molto sicuro e collaudato. IKEv2 è eccellente per i dispositivi mobili grazie alla capacità di riconnettersi rapidamente quando si cambia rete. [4]

### Q2: Che cos'è il routing a doppia VPN o Multi-Hop?

Il multi-hop instrada il tuo traffico attraverso due o più server VPN in sequenza. Questo aggiunge un secondo livello di crittografia e aiuta a mantenere nascosto il tuo vero indirizzo IP al secondo hop se un server viene compromesso.

### Q3: Cos'è la fuga WebRTC e come la previene una VPN?

WebRTC è un protocollo del browser che può rivelare i tuoi veri indirizzi IP locale e pubblico anche quando una VPN è attiva. Le VPN premium bloccano o falsificano le richieste WebRTC nelle loro app desktop/mobili e nelle estensioni del browser.

### Q4: Cosa sono i server solo RAM e perché sono importanti?

I server tradizionali scrivono i dati sui dischi rigidi, che possono essere sequestrati o compromessi. I server solo RAM (senza disco) funzionano interamente nella memoria volatile (RAM). Quando il server viene riavviato o spento, i dati conservati in memoria vengono cancellati.

### Q5: Come aggira i blocchi VPN l'offuscamento?

L'offuscamento (o "Stealth VPN") fa apparire il traffico VPN come normale traffico HTTPS (porta 443). Questo può aiutarlo a superare la Deep Packet Inspection (DPI) usata da governi o reti scolastiche e aziendali per bloccare le VPN.

# Punto di controllo 10: Domande frequenti avanzate sulle VPN (Parte D)

Esplora gli aspetti tecnici e strutturali delle reti private virtuali e dei protocolli di tunneling sicuro.

### Q6: Cos'è lo Split Tunneling e quando dovrei usarlo?

Lo Split Tunneling ti permette di scegliere quali app instradare attraverso il tunnel VPN crittografato e quali connettere direttamente a internet. Usalo per instradare nella VPN le app bancarie sensibili mentre i giochi locali si connettono direttamente, evitando la latenza aggiunta dalla VPN.

### Q7: Come funziona la Forward Secrecy (Perfect Forward Secrecy)?

La PFS garantisce che per ogni singola sessione venga generata una chiave di cifratura univoca e temporanea. Anche se in futuro una chiave privata venisse compromessa, non potrebbe essere usata per decifrare sessioni passate o future, perché hanno usato chiavi indipendenti.

### Q8: Cosa sono le alleanze 5/9/14 Eyes e perché dovrebbero interessarmi?

La giurisdizione può influire sul procedimento legale a cui un provider può essere esposto, ma il rischio pratico per la privacy dipende anche dai dati che il provider conserva, dalla sua architettura tecnica, dalla proprietà, dai rapporti di trasparenza e dalla cronologia degli audit.

### Q9: Cos'è la protezione dalle fughe DNS?

La protezione dalle fughe di DNS costringe il tuo dispositivo a inviare le richieste di ricerca dei siti web (richieste DNS) attraverso i server DNS privati e cifrati della VPN anziché quelli del tuo ISP. Questo impedisce al tuo ISP di tracciare quali siti visiti.

### Q10: Una VPN può aggirare la limitazione della banda di Internet da parte dell'ISP?

A volte. Una VPN può aiutare quando un ISP rallenta selettivamente attività identificabili, ma non risolve la congestione, i limiti di dati, i limiti di velocità a livello di account o la scarsa qualità della rete.

# Riferimenti tecnici e fonti

Pubblicazioni citate, specifiche crittografiche e standard di documentazione ufficiali utilizzati in questa scheda di lavoro.

## RIFERIMENTI ACCADEMICI E DI SETTORE

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637