I limiti reali delle VPN: cosa possono (e non possono) fare per la tua privacy

Maria Cattini | 10/08/2025 | Sicurezza digitale

Quando si parla di VPN, è facile cadere nelle promesse altisonanti: protezione totale, anonimato garantito, scudo contro hacker e governi. Ma cosa fanno davvero le VPN? E, soprattutto, cosa non fanno?

□□ VPN: cosa sono davvero

Una **Virtual Private Network** crea un tunnel crittografato tra il tuo dispositivo e un server esterno. Così, tutto il traffico internet sembra partire da quel server, e non dalla tua connessione reale. In pratica, nasconde la tua posizione e il tuo indirizzo IP al tuo provider e a chi gestisce la rete a cui sei connesso.

□□ Quando servono davvero

Le VPN sono utili soprattutto in due casi:

• Aggirare restrizioni geografiche o censura: ad esempio in scuole, aziende o Paesi con accesso limitato a internet.
• Accedere alla rete aziendale da remoto, per lavorare come se si fosse in ufficio.

□□ Cosa*non* fanno le VPN

Ecco alcuni falsi miti da sfatare:

• Non rendono anonimi: anche se nascondono l'IP, i siti possono tracciarti con cookie, fingerprinting o altre tecnologie. E il provider VPN stesso può vedere tutto il tuo traffico.
• Non ti proteggono del tutto su Wi-Fi pubblici: molti siti usano già HTTPS, che protegge i contenuti. Se però sei in una rete non sicura e non conosci chi la gestisce, una VPN può aiutare a nascondere i metadati.
• Non sono uno scudo contro le forze dell'ordine: molti provider salvano dati o sono obbligati per legge a fornirli su richiesta. Dipende dalla giurisdizione in cui operano.

□□ Come scegliere una VPN (senza farsi fregare)

Se pensi che una VPN possa esserti utile, ci sono alcuni aspetti da valutare con attenzione:

□□ Le promesse

Diffida di chi dice di garantire "protezione totale" o "zero tracciamenti" senza prove concrete. Controlla le politiche sulla privacy e cerca conferme da fonti indipendenti.

□□ La trasparenza

Alcuni provider si sottopongono ad audit di sicurezza da parte di terzi e pubblicano i risultati. Non è

una garanzia assoluta, ma è un buon segno.

□□ Il modello di business

Come si sostiene il servizio? Se è gratuito, potresti pagare con i tuoi dati. Se è a pagamento, controlla le clausole di rinnovo automatico.

□□ Chi c'è dietro

Cerca notizie sull'azienda e sul team: chi la gestisce? Ha una buona reputazione nel mondo della sicurezza? Se non trovi nulla, potrebbe essere un segnale d'allarme.

□□ Cosa registra

Anche se un provider dice di non tenere log, verifica nel dettaglio quali dati raccoglie. Alcuni potrebbero salvare IP, timestamp o dati di connessione, utili per identificarti.

□□ Tipo di crittografia

Evita VPN che usano protocolli vecchi come **PPTP**. Meglio scegliere servizi che supportano **OpenVPN** o **WireGuard**, molto più sicuri.

□□ Alternative alla VPN: quando Tor è meglio

Se il tuo obiettivo è **l'anonimato**, Tor è una scelta più adatta: il traffico passa attraverso più server e nessuno può vedere tutto quello che fai. A differenza delle VPN, dove il provider può osservare il tuo traffico.

□□ Non è una bacchetta magica

Una VPN da sola non basta a proteggerti. Meglio combinare più buone pratiche:

• Password robuste
• Autenticazione a due fattori
• Aggiornamenti regolari
• Blocco dei tracker
• DNS criptati
• Modalità HTTPS-only

Usare una VPN ha senso in contesti specifici, ma **non è un lasciapassare per la privacy assoluta**. È uno strumento utile, sì, ma solo se conosci i suoi limiti e scegli con consapevolezza. Prima di installarne una, chiediti: *mi fido davvero di chi gestisce questo servizio?*

Quando si parla di VPN, è facile cadere nelle promesse altisonanti: protezione totale, anonimato garantito, scudo contro hacker e governi. Ma cosa fanno davvero le VPN? E, soprattutto, cosa non fanno?

□□ VPN: cosa sono davvero

Una **Virtual Private Network** crea un tunnel crittografato tra il tuo dispositivo e un server esterno. Così, tutto il traffico internet sembra partire da quel server, e non dalla tua connessione reale. In pratica, nasconde la tua posizione e il tuo indirizzo IP al tuo provider e a chi gestisce la rete a cui sei connesso.

□□ Quando servono davvero

Le VPN sono utili soprattutto in due casi:

• Aggirare restrizioni geografiche o censura: ad esempio in scuole, aziende o Paesi con accesso

limitato a internet.
• Accedere alla rete aziendale da remoto, per lavorare come se si fosse in ufficio.

Cosa *non* fanno le VPN

Ecco alcuni falsi miti da sfatare:

• Non rendono anonimi: anche se nascondono l'IP, i siti possono tracciarti con cookie, fingerprinting o altre tecnologie. E il provider VPN stesso può vedere tutto il tuo traffico.
• Non ti proteggono del tutto su Wi-Fi pubblici: molti siti usano già HTTPS, che protegge i contenuti. Se però sei in una rete non sicura e non conosci chi la gestisce, una VPN può aiutare a nascondere i metadati.
• Non sono uno scudo contro le forze dell'ordine: molti provider salvano dati o sono obbligati per legge a fornirli su richiesta. Dipende dalla giurisdizione in cui operano.

Come scegliere una VPN (senza farsi fregare)

Se pensi che una VPN possa esserti utile, ci sono alcuni aspetti da valutare con attenzione:

Le promesse

Diffida di chi dice di garantire "protezione totale" o "zero tracciamenti" senza prove concrete. Controlla le politiche sulla privacy e cerca conferme da fonti indipendenti.

La trasparenza

Alcuni provider si sottopongono ad audit di sicurezza da parte di terzi e pubblicano i risultati. Non è una garanzia assoluta, ma è un buon segno.

Il modello di business

Come si sostiene il servizio? Se è gratuito, potresti pagare con i tuoi dati. Se è a pagamento, controlla le clausole di rinnovo automatico.

Chi c'è dietro

Cerca notizie sull'azienda e sul team: chi la gestisce? Ha una buona reputazione nel mondo della sicurezza? Se non trovi nulla, potrebbe essere un segnale d'allarme.

Cosa registra

Anche se un provider dice di non tenere log, verifica nel dettaglio quali dati raccoglie. Alcuni potrebbero salvare IP, timestamp o dati di connessione, utili per identificarti.

Tipo di crittografia

Evita VPN che usano protocolli vecchi come **PPTP**. Meglio scegliere servizi che supportano **OpenVPN** o **WireGuard**, molto più sicuri.

Alternative alla VPN: quando Tor è meglio

Se il tuo obiettivo è **l'anonimato**, Tor è una scelta più adatta: il traffico passa attraverso più server e nessuno può vedere tutto quello che fai. A differenza delle VPN, dove il provider può osservare il tuo traffico.

Non è una bacchetta magica

Una VPN da sola non basta a proteggerti. Meglio combinare più buone pratiche:

• Password robuste

• Autenticazione a due fattori
• Aggiornamenti regolari
• Blocco dei tracker
• DNS criptati
• Modalità HTTPS-only

Usare una VPN ha senso in contesti specifici, ma **non è un lasciapassare per la privacy assoluta**. È uno strumento utile, sì, ma solo se conosci i suoi limiti e scegli con consapevolezza. Prima di installarne una, chiediti: *mi fido davvero di chi gestisce questo servizio?*