

VPN – Virtual Private Network

Internet ci rende sempre più visibili e trasparenti. I dati che comunichiamo attraverso il nostro comportamento di navigazione, come le ricerche che effettuiamo, vengono utilizzati da aziende e criminali per i propri interessi, p. es. per condurre analisi di mercato o agire illegalmente. Questi dati si possono proteggere con le VPN.

Suggerimenti per l'uso delle VPN

- Utilizzate solo un provider VPN serio e affidabile, p. es. [ProtonVPN \(https://protonvpn.com/it/\)](https://protonvpn.com/it/), [NordVPN \(https://nordvpn.com/it/\)](https://nordvpn.com/it/) o [ExpressVPN \(https://www.expressvpn.com/it/\)](https://www.expressvpn.com/it/)
- Non dimenticate che nemmeno un provider VPN può garantire sicurezza al 100%.
- Ricordate che è protetta solo la connessione fino al provider VPN (server VPN).

VPN: un «tunnel» sicuro attraverso Internet

Normalmente, quando si visita un sito Internet o un negozio online, il browser contatta direttamente il server web corrispondente. Dati come la posizione dell'utente vengono trasmessi direttamente. Se il sito Internet viene aperto tramite un provider VPN, si aggiunge un elemento come tramite della comunicazione. Il browser quindi si rivolge come prima cosa al provider VPN attraverso una connessione crittografata e questo stabilisce il contatto con il sito in questione. Ricordate che la connessione dal provider VPN al sito potrebbe non essere protetta.

La VPN non va confusa con il protocollo «https». A differenza della VPN, «https» assicura soltanto che la comunicazione tra il browser e il sito visitato è crittografata. La VPN, invece, crittografa tutte le comunicazioni tra il vostro dispositivo e il server VPN, ad esempio anche le comunicazioni via e-mail.

Una VPN può essere impostata come parte integrante delle impostazioni del dispositivo.

Windows

In Windows 11, una connessione VPN può essere inclusa direttamente nelle impostazioni di rete («Impostazioni VPN») oppure si può utilizzare il programma offerto dal provider VPN. In ogni caso è necessario un provider VPN, p. es.:

- [ProtonVPN \(anche in versione gratuita\) \(https://protonvpn.com/it/\)](https://protonvpn.com/it/)
- [NordVPN \(https://nordvpn.com/it/\)](https://nordvpn.com/it/)
- [ExpressVPN \(https://www.expressvpn.com/it/\)](https://www.expressvpn.com/it/)

macOS

In macOS, una connessione VPN viene inclusa direttamente nelle impostazioni di rete dopo che si è scaricato e installato l'app. La VPN può essere attivata anche usando il programma offerto dal provider. In ogni caso è

necessario un provider VPN, p. es.:

- [ProtonVPN \(anche in versione gratuita\) \(https://protonvpn.com/it\)](https://protonvpn.com/it)
- [NordVPN \(https://nordvpn.com/it/\)](https://nordvpn.com/it/)
- [ExpressVPN \(https://www.expressvpn.com/it\)](https://www.expressvpn.com/it)

📱 Smartphone e tablet

Per smartphone e tablet installate e utilizzate l'app offerta dal provider VPN, p.es.:

- [ProtonVPN \(anche in versione gratuita\) \(https://protonvpn.com/it\)](https://protonvpn.com/it)
- [NordVPN \(https://nordvpn.com/it/\)](https://nordvpn.com/it/)
- [ExpressVPN \(https://www.expressvpn.com/it\)](https://www.expressvpn.com/it)

Una VPN può rappresentare una buona scelta in diverse situazioni:

- **Home office e remote work:** se lavorate da casa o da un altro luogo che non è il vostro ufficio, una VPN vi permette di accedere alla rete aziendale in modo sicuro.
- **Protezione della privacy:** le VPN sono utili anche se volete proteggere le vostre attività online dagli sguardi indiscreti. Per esempio potete impedire che i vostri dati siano accessibili ai criminali o alle aziende che analizzano il vostro comportamento per presentarvi pubblicità mirate.
- **Navigazione su WLAN pubbliche:** le reti WLAN pubbliche spesso non offrono una protezione sufficiente. Se utilizzate una VPN, i vostri dati sono protetti meglio anche su queste reti.
- **All'estero:** se utilizzate una VPN all'estero, beneficate di un anonimato maggiore. Se cambiate posizione, durante le vacanze potete per esempio continuare a guardare i programmi televisivi nazionali senza restrizioni. Nei Paesi in cui vi sono forti limitazioni per Internet, una VPN vi consente di accedere a siti che altrimenti non si aprirebbero. Quando programmate un viaggio in una destinazione lontana, tenete presente che in alcuni Paesi le VPN sono vietate e un loro uso non attento potrebbe mettervi in contrasto con le leggi del luogo. Le VPN sono vietate soprattutto nei Paesi in cui esistono forme di censura riguardo a Internet.
- **Acquisti online:** una VPN può essere utile anche se volete risparmiare con lo shopping online. Cambiando posizione, infatti, potete accedere a offerte più convenienti riservate ad altri Paesi.

Bisogna sottolineare che una VPN non offre una protezione al 100%. Succede solo che cambia il punto debole: invece che tra il dispositivo e il sito Internet, i dati possono essere intercettati tra il server VPN e il sito. E in teoria anche il provider VPN stesso potrebbe accedere ai vostri dati.

Come faccio a trovare il provider VPN giusto?

Di provider VPN ce ne sono sempre di più ogni giorno, visto che questi servizi sono sempre più popolari. Quindi trovare quello giusto può essere difficile. Tra i vari requisiti per essere serio e affidabile, un provider VPN deve offrire una crittografia robusta, non registrare le azioni eseguite sulla VPN e non condividere nessun dato.

Quindi tenete presenti queste indicazioni se dovete scegliere un provider VPN:

- **Sede del provider:** fate attenzione alla sede dell'azienda. Alcuni Paesi hanno leggi sulla protezione dei dati più rigorose di altri. In Paesi come la Svizzera o la Germania, in generale i vostri dati godono di una protezione migliore.
- **Reputazione:** cercate le recensioni online soffermandovi sia su quelle positive che su quelle negative.
- **Crittografia e protocolli di sicurezza:** prestate attenzione al fatto che il provider VPN utilizzi una crittografia robusta (p. es. AES-256) e protocolli di sicurezza solidi come OpenVPN o IKEv2 che impiegano p. es. lo standard AES-256, attualmente considerato sicuro.
- **No alla registrazione delle attività (politica «no log»):** scegliete un provider che segua una rigorosa politica no-log, ossia che non memorizzi alcun dato su ciò che fate in Internet.

Una Virtual Private Network (VPN) è un «tunnel» crittografato instaurato in Internet tra il vostro dispositivo e il provider VPN.

In genere una VPN viene utilizzata per creare, su una rete non sicura (p. es. Internet), una connessione sicura tra un dispositivo e una rete sicura (p. es. la rete aziendale). Durante il trasporto i contenuti vengono cifrati (crittografia end-to-end).