VareseNews

Wi-Fi aperte: come proteggersi?

Pubblicato: Giovedì 20 Giugno 2019

Molto spesso, sia in vacanza che per lavoro, si può avere bisogno di scaricare una grande quantità di dati, oppure di guardare dei film o dei cartoni animati in streaming, ad esempio in aeroporto con i bambini per lungo tempo, e la connessione dati del proprio piano telefonico può non essere sufficiente. Per questo motivo si può utilizzare una connessione Wi-Fi gratuita, e nella maggior parte dei casi per navigare è sufficiente richiedere la password al gestore o lasciare il proprio nome e cognome, una e-mail o un numero di telefono. Si tratta di una funzione molto comoda che però presenta vari rischi, proprio perché queste reti sono pubbliche. Scopri in questa pagina i metodi più efficaci per proteggere i propri dati e le proprie informazioni quando si sceglie una rete Wi-Fi aperta.

Innanzitutto, quali sono i rischi di utilizzare una rete aperta? Le reti Wi-Fi pubbliche sono aperte. Queste reti sono disponibili per chiunque. Nel momento in cui si accede ad una rete Wi-Fi aperta, tutti i dati che vengono comunicati sono accessibili a chiunque, perché non tutte le pagine hanno i protocolli di sicurezza o sistemi di crittografia. E spesso, i sistemi dei crittografia utilizzati dai principali siti non sono sufficienti per garantire la protezione. Esiste quindi il rischio che questi dati siano rubati. Le informazioni sensibili possono essere visibili, così come tutti i siti visitati, e c'è anche il rischio che con dei software appositi si possano spiare le conversazioni e carpire le password.

Il modo migliore per proteggere le informazioni è scegliere una connessione VPN quando si decide di collegarsi ad una Wi-Fi aperta. VPN è una sigla che significa Virtual Private Network, e che permette di navigare in modo sicuro, su di una rete pubblica.

Ma dopo aver scoperto che cos'è una VPN, come funziona? La comunicazione avviene tramite un sistema che si chiama tunnelling, che permette di non rendere visibili i pacchetti di dati che vengono trasferiti tra un dispositivo e un server. Le connessioni VPN permettono il trasferimento crittografato di questi dati, e oltre a essere disponibili per PC e tablet è possibile utilizzarle anche per i cellulari.

Si può utilizzare una connessione VPN sullo smartphone?

Esistono vari tipi di connessione VPN per gli smartphone, e si tratta soprattutto di scegliere quella più indicato per le proprie esigenze.

Un buon compromesso prevede comunque che la connessione sia a pagamento, perché così può offrire il giusto livello di protezione. Le connessioni VPN per i cellulari sono generalmente sottoposte a dei piani di pagamento annuali o mensili, e prima di scegliere è utile fare qualche prova per verificare quella più adatta. ?

È utile sapere poi che i dispositivi con sistema operativo Android hanno un sistema di supporto integrato per varie connessioni VPN.

In conclusione, una connessione VPN sui dispositivi mobili è il modo migliore per proteggere i dati che si comunicano in rete, ma si consiglia comunque di dotare il proprio telefono di un antivirus e di aggiornarlo come regolarità perché il VPN non può proteggere i dati già presenti sul telefono.

Redazione VareseNews
redazione@varesenews.it