VareseNews

# Utilizzare un Wi-Fi pubblico può essere più rischioso del previsto

**Pubblicato:** Giovedì 10 Giugno 2021

Con l'arrivo della bella stagione, e per via del sempre maggiore allentamento delle misure di sicurezza legate alla pandemia da Covid-19, si ricomincia finalmente a trascorrere molto più tempo all'aria aperta. Oltre a uscire di casa e popolare nuovamente bar, ristoranti e altri locali pubblici, è possibile tornare a viaggiare e vedere posti nuovi, seppur con le dovute precauzioni. Di conseguenza, aumenta la probabilità (e, in certi casi, la necessità) di utilizzare il Wi-Fi pubblico messo a disposizione dalle varie attività commerciali. Tuttavia, pur essendo indubbiamente comoda in diverse occasioni, questa pratica può avere dei risvolti negativi. Infatti, spesso le reti Wi-Fi pubbliche presentano delle vulnerabilità importanti che possono mettere a repentaglio la sicurezza delle informazioni di chi le utilizza. In questo articolo verranno quindi presi in considerazione i principali rischi a cui ci si espone sfruttando il Wi-Fi pubblico.

## Attacchi informatici

Quando si utilizza una rete pubblica, è facile correre il rischio di subire attacchi informatici di diversa natura, operati da malintenzionati che sfruttano le vulnerabilità di queste reti solitamente poco o per nulla protette. Uno degli attacchi più comuni è il cosiddetto *attacco man in the middle* (traducibile in italiano come "uomo nel mezzo"), che consiste in una vera e propria forma di intercettazione. In pratica, ogni volta che ci si collega a Internet, si instaura una comunicazione tra il dispositivo e il servizio o il sito web che si desidera visitare. Sfruttando le vulnerabilità di una rete pubblica, un hacker può

letteralmente intromettersi in questa comunicazione e avere accesso alle informazioni e ai dati sensibili di utenti del tutto ignari.

## Rischio di malware

L'utilizzo di un Wi-Fi pubblico può esporre gli utenti anche al rischio di malware. Infatti, quando ci si collega a una rete pubblica con l'opzione di condivisione dei file tra reti abilitata, un malintenzionato può avere accesso alle cartelle pubbliche dell'utente e installare un malware a sua insaputa. In questo modo, l'hacker potrà avere accesso a tutte le informazioni che sono contenute sul dispositivo dell'utente e sottrarre quindi dati come quelli relativi alle carte di credito. Inoltre, potrà accedere anche a foto e documenti di diversa natura, invadendo pesantemente la privacy dell'utente.

## Hotspot non legittimi

In questo caso, il malintenzionato inganna l'utente ignaro configurando una rete Wi-Fi pubblica legittima soltanto all'apparenza. Ad esempio, quando si viaggia e si soggiorna in un hotel, spesso si sfrutta la connessione pubblica gratuita messa a disposizione dalla struttura stessa. Tuttavia, un hacker può configurare un proprio hotspot, chiamandolo con lo stesso nome di quello dell'hotel: collegandosi alla rete del malintenzionato, quindi, quest'ultimo avrà accesso a tutte le informazioni e i dati sensibili dell'utente.

## Assenza di crittografia

La crittografia dei dati è uno strumento fondamentale per tenere al sicuro le informazioni degli utenti. Infatti, le informazioni crittografate scambiate tra un dispositivo e il router sono praticamente scritte in codice, e per leggerle è necessario disporre di un'apposita "chiave" per decifrare il testo. Nel caso delle reti Wi-Fi pubbliche, però, spesso la crittografia dei dati non è abilitata, e di conseguenza le informazioni degli utenti sono visibili e possono essere sottratte dai malintenzionati.

## Come ridurre i rischi dell'utilizzo di un Wi-Fi pubblico

Come accennato in precedenza, a volte l'uso di una rete Wi-Fi pubblica è più un'esigenza che un capriccio. Ad esempio, può capitare di trovarsi fuori casa e di dover assolutamente consultare una mappa per orientarsi, accorgendosi però di aver terminato il traffico dati della propria offerta. In questo caso, collegarsi a un hotspot pubblico può risultare di fondamentale importanza. È comunque necessario adottare tutti gli accorgimenti possibili per minimizzare i rischi finora esposti. Un'ottima soluzione è quella di utilizzare una VPN (Virtual Private Network), che permette di crittografare i dati e, di conseguenza, impedire a eventuali malintenzionati di decifrarli, anche nel caso in cui dovessero impossessarsene. Inoltre, è consigliabile disattivare la condivisione dei file tra reti e assicurarsi di accedere solamente a siti che utilizzano protocolli HTTPS (di gran lunga più sicuri rispetto a quelli che utilizzano il protocollo HTTP).

divisionebusiness
divisionebusiness@varesenews.it