Privacy in hotel: sei davvero al sicuro? Ecco i consigli per evitare “furti digitali” in viaggio

Con l’arrivo dell’alta stagione estiva, gli alberghi diventano il bersaglio preferito dei cybercriminali. Camere sempre più vulnerabili, tra false reti Wi-Fi, porte USB insidiose e truffe digitali a caccia di dati personali. Il vostro alloggio è davvero sicuro? Ecco come difendere la privacy in hotel (Fonte: https://viaggi.corriere.it/ 7 agosto 2025)

Vacanze a rischio: gli hacker pronti a colpire nelle camere d’hotel

Mentre si sogna il relax della vacanza alle porte, c’è chi è già pronto a sfruttare ogni minima falla nella sicurezza degli hotel per rubare dati e informazioni personali.

Dalle reti **Wi-Fi** trappola alle prese **USB** insidiose, la camera d’hotel potrebbe nascondere più rischi di quanto si immagina.

Allarme estate 2025: attacchi informatici in crescita negli hotel

Secondo **VikingCloud**, società globale specializzata in soluzioni integrate di cybersecurity, il 66% dei responsabili IT e sicurezza alberghiera prevede un aumento degli attacchi informatici nell'estate 2025, e la metà di loro teme un’emergenza di più ampia portata rispetto al passato.

Le aree più a rischio? In cima alla lista figurano i sistemi di pagamento/ **POS** (72 %), il Wi-Fi per gli ospiti (56 %) e i sistemi front-desk (34 %).

Resort affollati e ospiti distratti

Gli hotel, insomma, sono diventati uno dei luoghi più a rischio per truffe informatiche. Anche perché i resort turistici affollati di persone rilassate, che spesso abbassano la guardia, rappresentano un’opportunità allettante per i truffatori.

“Anche nella camera d’albergo, gli hacker possono sfruttare le vulnerabilità delle reti e dei dispositivi condivisi per entrare in possesso di dati personali. I viaggiatori devono prestare molta attenzione alla sicurezza digitale, soprattutto quando si connettono a reti sconosciute all’estero”, spiega **Matas Cenys**, *senior product owner* di **Saily**, un’app **eSIM** che offre connessioni internet, sviluppata dagli esperti di **NordVPN**.

I trucchi usati dagli hacker (e come difendersi)

Tra le tecniche più diffuse ci sono le false connessioni **Wi-Fi**, conosciute come “**evil twin**”: reti che imitano quelle ufficiali dell’hotel ma servono solo a rubare password e dati sensibili.

Pure le porte **USB**, spesso usate per ricaricare dispositivi, possono essere manomesse per un attacco chiamato “**juice jacking**”, che consente di sottrarre informazioni personali direttamente dal telefono o dal tablet.

Connettersi alla Wi-Fi dell'hotel: una pessima idea

Il **Wi-Fi** pubblico negli hotel è comodo, ma rappresenta uno degli accessi preferiti dagli hacker.
I criminali informatici possono infettare le reti legittime o creare falsi hotspot, chiamati "**evil twin**", che imitano quelle ufficiali per rubare dati sensibili.

Ci sono (almeno) cinque buoni motivi per evitare il Wi-Fi degli hotel:

1. Furto di identità e addebiti sulla vostra stanza

Molti hotel chiedono di inserire nome e numero della camera per connettersi al **Wi-Fi**. Se la rete non è ben protetta, chiunque con strumenti semplici può intercettare questi dati e, nel peggiore dei casi, effettuare acquisti a vostro nome, addebitandoli direttamente sulla vostra camera.

2. Attività online pericolose attribuite a voi

Un hacker potrebbe usare il vostro nome e numero di stanza per entrare nella rete e compiere azioni illecite, lasciandovi nei guai legali, soprattutto in Paesi con leggi molto severe come **Cina** o **Thailandia**.

3. Furto di dati personali e aziendali

Anche se la rete è criptata, chi si trova nelle vicinanze può vedere quali dispositivi sono connessi e perfino impersonarvi grazie a tecniche di *spoofing*. Se un hacker riesce a violare il vostro dispositivo, può rubare password, installare spyware e accedere a dati sensibili, mettendo a rischio anche segreti aziendali protetti da accordi di riservatezza.

4. Rischio di malware e accessi remoti (RAT)

Cliccare su link sospetti o usare porte **USB** compromesse in hotel può portare all'installazione di trojan di accesso remoto (**RAT**), che permettono agli hacker di prendere il controllo completo del vostro dispositivo e usarlo per attività illegali, anche senza che voi ve ne accorgiate.

5. Hotspot mobili: non sempre la soluzione perfetta

Anche gli hotspot personali non sono immuni da rischi: possono essere monitorati, tracciati o colpiti da dispositivi falsi come gli *IMSI catcher*, che intercettano e manipolano le comunicazioni cellulari.

Cosa fare

La regola d'oro è evitare, quando possibile, il **Wi-Fi** pubblico degli hotel. Verificate sempre il nome della rete con il personale, preferite la connessione tramite dati mobili usando una **eSIM** affidabile e mantenete aggiornati i vostri software.
Usate password complesse e una **VPN** per proteggere la vostra privacy.

Attenzione alle porte USB (che possono rubare dati e privacy)

Le porte **USB** nelle camere d'albergo sono comode, soprattutto per chi viaggia all'estero, ma non sempre sono sicure.

Queste prese, pensate per facilitare la ricarica dei dispositivi, possono nascondere un rischio noto come "**juice jacking**": un attacco informatico che sfrutta la connessione **USB** per installare malware sul telefono e rubare dati sensibili come password, numeri di carte di credito e persino la posizione dell'utente.

Molti hotel offrono queste porte per comodità, soprattutto per gli ospiti provenienti da Paesi con prese elettriche diverse, ma proprio questa facilità può trasformarsi in un pericolo.

Gli hacker, infatti, possono manomettere i cavi o le porte stesse per infiltrarsi nei dispositivi collegati.

Cosa fare

Il modo più sicuro per ricaricare il dispositivo? Usare una presa di corrente. In alternativa, è consigliabile portare con sé un power bank o un dispositivo **USB** con blocco dati, che impedisce il trasferimento di informazioni.

Gli esperti avvertono: "Se il punto di ricarica sembra sospetto o manomesso, evitatelo. E se il telefono vi chiede di 'consentire l'accesso a questo dispositivo' quando lo collegate al caricatore, non accettate".

Per viaggiare tranquilli, il suggerimento è quindi di utilizzare sempre il proprio caricabatterie collegato a una presa elettrica e, per maggiore sicurezza, dotarsi di un blocco dati **USB** o di un **power bank** portatile.

Smart TV: gli hacker spiano attraverso lo schermo

Le **Smart TV** nelle camere d'albergo offrono comodità grazie a telecamere, microfoni e accesso a servizi di streaming, ma spesso sono poco protette.

Questo le rende un bersaglio per gli hacker, che possono sfruttarle per origliare conversazioni, osservare gli ospiti o rubare le credenziali degli account utilizzati sulle app.

Cosa fare

Per proteggervi, evitate di accedere con i vostri account personali e, quando non utilizzate la TV, staccate la spina. Se possibile, coprite la telecamera integrata per maggiore sicurezza.

Una **Smart TV** compromessa può diventare uno strumento di cyberstalking o una porta d'ingresso per furti di dati personali, venduti poi sul **dark web**.

Secondo **NordVPN**, la prevenzione più efficace è proprio disconnettere la TV dalla corrente quando non serve, limitando così i rischi di sorveglianza e furto d'identità.

Connessioni automatico al Wi-Fi: disattivatele subito

Gli smartphone si collegano spesso in automatico alle reti **Wi-Fi** già conosciute, ma questa funzione può trasformarsi in un pericolo quando viaggiate, soprattutto in ambienti con reti pubbliche non sicure o addirittura malevole.

I dispositivi possono connettersi senza che ve ne accorgiate, anche quando non siete nella stanza, esponendovi a possibili attacchi informatici.

Cosa fare

Per difendervi, è fondamentale disattivare la connessione automatica per **Wi-Fi** e **Bluetooth**.

Inoltre, è consigliabile attivare app di sicurezza come firewall o **VPN**, assicurandovi che si avviino automaticamente quando vi collegate a reti pubbliche.

Questa semplice precauzione riduce significativamente i rischi, proteggendo i vostri dati anche se il dispositivo si connette a reti non protette.

Truffe di phishing: come non cadere nella trappola

Un esempio di minaccia sofisticata è il gruppo di hacker **DarkHotel**, noto per aver compromesso le reti **Wi-Fi** di hotel di lusso con attacchi mirati che combinano *spear phishing*, *malware* avanzati e *botnet* automatizzate per rubare dati sensibili.

Questi attacchi prendono di mira principalmente figure di alto profilo come dirigenti, politici e rappresentanti di aziende strategiche, utilizzando e-mail di *phishing* personalizzate e molto convincenti.

Cosa fare

Evitare di cliccare su link sospetti o di aprire allegati provenienti da fonti non verificate, anche durante le vacanze.

Aggiornare costantemente software e applicazioni aiuta a ridurre i rischi di vulnerabilità.