# HOTEL WI-FI AND HOW SECURE IT IS

Business travelers depend on hotel Wi-Fi for their phones, tablets, or computers. Most hotels offer free Wi-Fi access, but how safe are these networks? How can guests safeguard themselves? IT experts provide tips on how to stay safe when using the Internet in hotels.

### Invitation to Hackers

Guests usually get their room card, hotel information, and Wi-Fi password when checking in. This can save data usage, especially in countries with insufficient home data rates. However, **experts caution that having a password does not guarantee safe internet browsing**.

Hackers can quickly obtain the password from the hotel, and they may use deceptive tactics like setting up fake "hotel networks" to trick guests into transmitting sensitive data. This can include account information, passwords, and pictures, which are sent over an unsecured network.

When shopping online and regularly visiting shopping portals, it is crucial to be cautious. Hackers can easily access stored payment data through the router. Additionally, data thieves may create fake WLAN networks to install malware on devices. This can be especially problematic for business travelers, as the virus can spread unnoticed to the home or company network upon their return.

### How to Protect Yourself

To increase device security, start by turning off automatic connections to available networks. It's essential to keep your operating systems and applications up to date, especially if you're a business traveler. When entering sensitive information like online banking or shopping, it's best to use your data plan instead of the hotel's Wi-Fi, even if it requires a password. If you must use the hotel Wi-Fi, connect to the correct network and disconnect as soon as you finish browsing. Otherwise, your applications may continue to exchange data with the network without your knowledge, putting your information at risk.

### Securely across the Network with a VPN

Anyone who needs to send sensitive data over the network on a business trip should use a VPN. The Virtual Private Network is a secure connection between the endpoint and the Internet. **The IP address of the endpoint is disguised, and all traffic is routed through an encrypted tunnel.** This means outsiders cannot read the traffic. According to experts, the most straightforward and usually sufficient solution for private users is to install VPN software or download a VPN as a web extension. This is often available in a subscription model for just a few dollars per month. On the other hand, free VPN services may be limited in data volume, for example, or require users to accept advertising.

Date: 2023-06-26

Article link: https://www.tourism-review.com/stay-safe-when-using-the-hotel-wi-fi-news13342