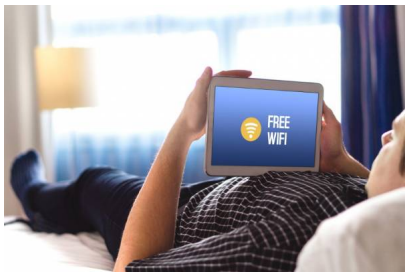
THE DANGERS OF HOTEL WI-FI CONNECTION



For many travelers it is a routine. When you arrive at a hotel or restaurant, firstly you ask about wireless connection. However, experts warn that hotel wifi may be very dangerous, though the risks can be avoided.

Upon activating WLAN search on a mobile phone, one usually gets dozens of results, regardless where he is. Whether it is a hotel, restaurant or a café. It is obviously a good thing to offer free internet to customers. More and more public places also have the so-called hotspots. **Smartphone users like to take advantage of this offer, be it because they want to save data volume or because they are in non-EU countries, for example, and have no data tariff there.**

However, experts warn that a simple connection can bring great danger. The problem is that public Wi-Fi is not the same as private Wi-Fi. The sticking point is the router that transmits the data. Anyone who has control over the router also has control over the data – and can use it for illegal purposes.

Hazardous shopping

The danger lies with shops like Amazon, in which payment data are deposited. If a criminal can access the data via the router, he can order whatever he wants via the owner's account. It gets even more critical if he can also access e-mails. As a result, he can reset passwords on Amazon, for example, and have new ones sent to him, even connect the account with another address. This leaves the phone owner somewhat helpless.

But experts say that mobile users should not panic, as "not every hotel Wi-Fi is evil". Many hotels protect their wireless networks with directing the user to a login page if they want to use the network. However, open WLANs, available at many bars, cafes and hotels, are liable to this kind of conduct. Moreover, some criminals even offer open WLANs called "honey pots". They have a name based on the official name of a nearby hotel or restaurant, so as to guarantee safety to the user.

How to stay protected while connected?

However, there are various solutions to tackle the above described issue. For example, laptops, notebooks and tablets should be equipped with the latest virus scanners and firewalls before visits. It is also highly recommended to use the newest available browsers, which have the highest security standards.

Moreover, it is recommended to shorten your stay online as much as possible. This saves battery power and protects against online crime. The less you are connected to a foreign network, the less likely it is to be spied on. But if it is necessary, one should avoid accessing the bank account.

Those who are looking to make purchases on foreign Wi-Fi networks should make sure that the website is protected via a HTTPS connection.

Another solution is also to use VPN connections. **This establishes a password-protected tunnel over which data is transmitted without anyone else being able to access it.** Many companies use VPN so that their employees can access files and programs from outside the corporate network. But there are also a number of providers that offer VPN services for end customers, both paid and freeware.

Date: 2018-06-18

Article link: https://www.tourism-review.com/hotel-wi-fi-may-be-dangerous-news10640