THE SAFETY OF PUBLIC WI-FI FOR TRAVELERS

Accessing open WLAN (Wireless Local Area Network) is easy - whether at the airport, train station, café, hotel or fast-food court. In most cases, surfing is free and a password-free connection is established in no time. But the tempting offer has a catch. According to VPN experts, one in four travelers who used public Wi-Fi abroad has been hacked. IT experts provide tips for emergencies and reveal how you can protect your data.

Unencrypted hotspots offer online crooks the best opportunities to spy on their victims' smartphones and laptops and to access and manipulate sensitive, personal or corporate data. But it's not just users' carelessness that leads to hacks; **travelers, especially abroad, often don't know what trustworthy WLAN networks are and rely on companies offering public WLAN**. But that's exactly what hackers are taking advantage of. With the so-called "man-in-the-middle attack," they force their way into communication and deceive both sides. This is because they pretend to be the receiver to the sender and the sender to the receiver. For example, attackers can intercept login data or credit card information when logging into social networks or making online bookings via smartphone.

What To Do When You Have Been Hacked?

Victims of cybercrime often don't notice immediately when they've been hacked. It only dawns when the bank contacts them, the email account is blocked or acquaintances complain about strange postings or messages in the messenger service. Experts provide some tips on what to do if the worst comes to the worst.

Get out of the network, the public Wi-Fi! To prevent further data theft, the device in use must be disconnected from the network or, better still, switched off completely. This way, no more data can be sent over the Internet. It’s also recommended to check connected USB sticks or external hard drives for infected malware using an antivirus program. Even if this involves additional costs, it can be advisable and ensures greater security if an IT technician takes another look at or into the devices and cleans them up.

New passwords! If accounts have been hacked, all passwords must be changed. What seems practical, but carries a high-security risk, is a general password for all cases. IT experts point out that all other accounts are no longer secure if one of them has been hacked. The experts, therefore, recommend creating different passwords for different accounts.

A good password consists of at least eight characters. It contains upper and lower case letters, numbers and special characters - preferably a combination that looks random. Dates of birth, names from the family, number sequences such as 123456 - and the word 'password' are unsuitable.

Passwords should also be changed regularly and replaced with new, strong passwords. IT experts also recommend two-factor authentication everywhere, with customers additionally confirming their identity for electronic payments with a password, TAN or fingerprint.

Inform everyone involved! If it is clear what exactly has been attacked - the entire device or "only"

one or more accounts - then it is important to act quickly and inform all affected persons. This applies not only to friends and family, but also to social media platforms and providers where sensitive data (account data, addresses, etc.) has been stored. It’s also advised to contact your employer immediately if a company device has been hacked.

Protect Your Data

As a user of an open WLAN, it is very possible to make it more difficult for hackers to steal data. IT experts recommend encrypting data connections and taking security precautions. Encrypted data connections are easy to obtain. You can ask the operator for the correct WLAN ID in the café or hotel and select it manually. In addition, file sharing can be deactivated in the network settings of the operating system. Personal USB sticks or external hard drives should only be connected if the PC has an up-to-date virus protection program.

Experts also recommend disabling automatic connection from the smartphone or laptop to any public network that is not protected by a password. **The entry of login data in public spaces should also be discreet.** A useful tip: special protective films that shield the display from the prying eyes of unauthorized persons. And even if it's nice, easy and fast to do on the move, experts advise against booking hotels or airline tickets while connected to a public network.

Date: 2022-10-24

Article link:
https://www.tourism-review.com/the-dangers-of-public-wi-fi-while-on-the-road-news12768