5 WAYS HACKERS ARE TARGETING VACATIONERS AND WHAT YOU CAN DO ABOUT IT

The tourism industry is increasing with over 7.1 million international tourists in 2018 up from 6.6 million travelers the year prior. But, a growing concern is the number of hacking incidents that travelers can fall prey to.

Cybersecurity experts are finding that the increase in travel with airlines, cruises, and hotels make travel destinations hotspots for cybercriminals. Travelers might not realize the dangers of using free wifi in their hotels or in travel destination cafes making them prone to all kinds of attacks. Specifically, there are newer malware threats designed to bypass cybersecurity detection which can lead to other types of attacks.

A few types of suspicious attacks to look out for include:

Man in the Middle Attacks

The Federal Trade Commission (FTC) reported an estimated 2.7 million fraud incidents were reported that resulted in a loss of $905 million. Despite cybersecurity programs and free wifi warnings about internet imposters, 1 in every 5 Americans was a victim of some type of online scam.

With the man in the middle attack, unsuspecting tourists use free wifi at their travel destinations. They're unaware that hackers have set up an access point nearby and they mimic the hotspot for the cafe, airport or hotel.

It's recommended that travelers use a virtual private network (VPN) that can encrypt their data online. This prevents their personal information from being shared with attackers who eavesdrop on network traffic. Having the right internet security in place can safeguard a traveler and protect their personal information.

Outdated Software

An easy way for hackers to gain access to a traveler's computer is if they haven't updated their security protocols. Hence, it's important to always update the software on all devices, PCs, phones, gaming devices, and tablets.

Software vulnerabilities are security holes that let attackers in. All they need to do is write code for the vulnerability and they can exploit the traveler's computer and steal their information.

Travelers are not Paying Attention to Phishing Scams

Being away on holiday isn't the time to let one's guard down. It's important for travelers to pay attention to emails that ask for personal information. Maybe it's an urgent request about a package that's lost in the mail. Or, a friend shares an urgent email that they're stranded without money. The

unsuspecting tourist clicks on the link in the email which is actually a phishing email sent by a scammer.

To help travelers know the difference, double-check the wording in every email and look for misspellings and typos like FeDExx. Or an email might have extra wording like help.fedex.contact.com instead of simply fedex.com. These might confirm that the email isn't real. And, if the person contacts that friend in need, they might find that it was the friend's email that was compromised and they never sent a message of concern.

The Same Password is Used for Multiple Accounts

Online attackers are sophisticated. A cyber attacker can record keystrokes on a computer at an internet cafe the person is using. From there, all they have to do is use the same password for the traveler's other accounts.

Travelers should change their passwords often and use a combination of numbers, symbols, and letters. For people that don't want the inconvenience of multiple passwords, they can store them with their preferred cybersecurity software.

Travelers are Sharing Too Much on Social Media

An attack can come in different ways including social media. When tourists post that they're in a new location and sharing pictures of their surroundings, a hacker might try to send an attack from another computer pretending to be a friend.

All the cybercriminal has to do is send a message to "check out a bar here" or "visit these top restaurants". They can secretly embed malware in a link and then the person clicks on the link and receives malware on their phone or another device.

Attackers can also monitor what the traveler writes on social media for key information they can use to steal the person's identity. They might look for the person's mother's maiden name, first pet or first street address. These are all used with security passwords.

Date: 2019-07-12

Article link: https://www.tourism-review.com/hackers-are-targeting-holidaymakers-news11135