INVESTOR'S BUSINESS DAILY®

TECHNOLOGY

Free Wi-Fi Can Cost You A Ton In Terms Of Lost Privacy, Security

JULIE VALLONE 4/26/2016

This year, journalist Steve Petrow got his computer hacked while using the in-flight Wi-Fi service on American Airlines. He described the experience in a USAToday column, explaining that the hacker was another passenger aboard the plane who approached him at baggage claim. The hacker told the journalist he had read his emails on the flight, along with those of other passengers.

The hacker, Petrow explained, wanted to show him what it was like to have his privacy violated, since Petrow had been writing about the Apple-FBI privacy issues.

Point made. Indeed, when it comes to security, Wi-Fi can be trouble.

Getting into data over a shared Wi-Fi network isn't hard to do, says Josh Wright, a Providence, R.I.-based security consultant and author of "Hacking Exposed Wireless."

"When you join a Wi-Fi Network, and I can join that same network, I know that I can attack your computer," Wright said. "And the Wi-Fi hot spot provider, whether it's a coffee shop or whatever, really has no interest in providing additional security for you because that's an added cost for them."

How Hackers Can Attack

While Petrow's hacker seemed to want to make a point about privacy, other hackers often have more nefarious plans:

Gary Griffiths is CEO of **iPass** (**IPAS**), which offers a cloud-based service that helps people connect more easily and securely to Wi-Fi hot spots worldwide. He identified several ways hackers can invade your privacy when your Wi-Fi network is not secure. These include:

- Accessing and modifying your data without your knowledge, or that of the receiver.

- Capturing unprotected (unencrypted) data like passwords and user names to get access to your other data.

- Freezing up your computer and preventing you from using it.

- Assuming your identity (through your IP address), then modifying, rerouting or deleting your data.

- Inserting themselves into an online conversation and impersonating one of the parties to get information intended for someone else.

“From a settings point of view, once data is leaving your computer and going into the air, it can be intercepted,” Griffiths said. “So unless you’re doing something to encrypt that data, it is vulnerable.”

Mobile Wi-Fi Security Tips

There are safer ways to get on Wi-Fi when you’re away from home, says Wright. For example, if you are doing work for a company and have access to its Virtual Private Network, be sure to hook into it.

“VPNs provide a layer of protection between your computer and your workplace. So now all your data goes out to your workplace, instead of going out unencrypted. It offers an extra level of security,” Wright said.

If you’re self-employed, it becomes harder because there’s no big company VPN to hook into. But there are options.

Here are a few that Wright, Griffiths and other experts suggest:

- Check with the hot spot provider to see if the network is encrypted and password protected.

- Find out whether the apps or programs you’re using have any encryption or other protections.

- If not, and you have a phone with hot spot technology, consider using it instead of the free Wi-Fi. Granted, it could suck up costly data, so that

decision might depend on your data plan, and how badly you need to use the Wi-Fi.

- Subscribe to your own VPN service. There are now many companies offering this service for monthly fees of under $10.

- Simply decide to not use the Wi-Fi, and wait till you get home to send sensitive information.

Ways To Boost Protection At Home

Once you do get home, you can do several things to keep your data safe. One of them, says Wright, is to make sure your wireless router's encryption is set to the Wireless Protection Access 2, or WPA2, standard. Contact the manufacturer if you need instructions on how to do this. (Some have the instructions on their websites.)

And don't give the network password out to many people, such as to friends or extended family, says Wright. If you do, try to change the password at least four times a year, or just let everyone outside your immediate family use your guest network. It's not protected like your home network, but people will have access if they want it.

Also, make a backup of your data that is not connected to your computer, or even in the house. Wright says he backs up his family's data (like photos they don't want to lose) onto a separate drive and keeps that in a bank lockbox. Another option, he says, is to subscribe to a third-party backup service, if you don't mind paying the fee. **Alphabet** (**GOOGL**) offers the Google Drive service, and other leaders in this area include **Box** (**BOX**) and Dropbox.

On its website, the Federal Communications Commission shares tips for setting up your home wireless network to help ensure protection there. These include:

- Turning on the router's firewall. Most routers are built with firewalls designed to filter traffic coming to your computer and protect you from online intruders. But these may be turned off when you buy the router.

- Change the default administrator passwords for setting the devices. These are different from the ones you use to access your wireless. Hackers may be familiar with the default admin passwords.

- If you're not going to use your network for a long period, turn it off.

- Use anti-virus and anti-spying software on all computers connected to your network.

When you're back on the road with your computer, be sure to know the network you're using.

"So-called free Wi-Fi is hardly free if your personal information has been compromised, or your data has been intercepted," Griffiths said. "It can be a pretty expensive proposition."

TECHNOLOGY

Alarm.com Sees Growth Opportunity In Wellness Market

PATRICK SEITZ 12:09 PM ET