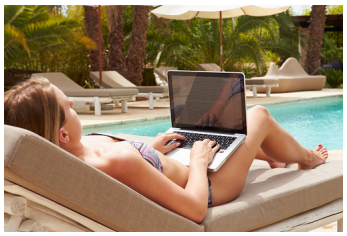
Protecting Yourself and Your Devices While Traveling

Written by Arizona Foothills Magazine

Raise your hand if you remember the days of having to totally disconnect from the world while you were traveling! Part of the fun of traveling, after all, is getting away from everything, right? It wasn't that long ago. We'd head to the airports and maybe we could work on files we already had with us, but that was it. Today, on the other hand, we get enraged if an airport wants us to pay for Wi-Fi. We're even able to connect to the cloud while we are on airplanes that are mid-flight!



We officially live in science fiction novels and it's pretty great. Unfortunately, it is also pretty risky.

For the most part, the wi-fi provided at airports, train stations, on busses, trains and planes is not secured. This means that anybody can connect to it. And that means that, if you aren't careful, anybody can connect to you. They can connect to your computer, your tablet, heck, they can even connect to your phone! Think of all of the information and data you have stored in those places. Then think about all of the things to which those devices can connect: your bank account, your employer's cloud server, etc.

Are you freaked out yet?

Here's something else that's important to know: even hotel wi-fi is vulnerable. According to a recent article in The Huffington Post, the router that most hotels use to broadcast their Wi-Fi to guests is incredibly vulnerable to hackers. That means that, even when you get to your hotel, your devices aren't perfectly safe (unless they are disconnected from the service and turned off).

This isn't just true domestically, says Market Wired. It's affecting hotels all over the world.

How's that fear level now?

Before you get really paranoid about traveling, it is important to know that there are things that you can do to protect yourself against threats. Here are just a few of them:

Common Sense

You know that you shouldn't ever leave your computer unattended when you work from a coffee shop, right? That's why you make sure that you've used the bathroom before you put in your order or you work with friends or colleagues so that if you do have to get up, you'll know that your machine is safe. The same is true in airports and in hotels. Don't leave your devices sitting out where anybody can grab them and use them.

In hotels, in particular, you'll also want to make sure that your computer is locked. This way, even if someone does try to turn it on, they won't be able to use it without a specific password. You should also consider installing software that will "brick" your device until a specific code that only you have is entered. This discourages theft.

Software Protection

By now most people operate with their firewalls turned all the way up all of the time. Even so, it is important to have protective software put on your computer. You'll want malware and hacking protection that can detect and thwart problems in real time. And don't assume that because you have an Apple device that you are immune to hacking and viruses. If you're using Apple devices, install antivirus protection for Macs, iPhones, iPads, etc.

Educate Yourself

There are new scams invented every day. For example, you probably know all about phishing and ransomware, but have you heard about pharming? Pharming is where hackers will set up "dummy" sites that look exactly like legitimate sites (usually banking and ecommerce). They exploit loopholes in routers and operating system software to redirect your web browser to these sites instead of the ones you intend to visit. Always look for security signs like the closed padlock, "https:" instead of "http:", etc. to make sure that your site is legitimate. Make sure to double check the web browser address bar for misspellings that are close to the address you typed.

Hot Spots

Many cellular companies sell devices that will allow you to piggyback your phone's cellular signal into your laptops or other devices. If you can afford these services, and you travel often, investing in one of them will allow you to bypass your hotel, plane, train, bus, airport, etc's wi-fi access point altogether and further protect your devices. Just make sure that your piggyback tech is protected as well, so that other people can't hop onto it without your permission. And, of course, make sure your data plan is hefty enough to cover your usage!

These are just a few of the things you can do to protect yourself against threats. If you follow them you should be able to keep your devices safe and threat-free.