Wireless attacks

You are out for coffee with a friend at your local coffee shop, when glancing down at your phone, you realize you don't have any data. No problem, you just connect to the free WIFI provided by the shop. Its free WIFI right? Well sadly, sometimes the free things in life can cost you. In this week's article, I will go through why in the future, you may need to be cautious on what you connect your devices to.

One of the most common (and sometimes difficult to spot) attacks is an evil twin attack. This usually involves a malicious user setting up another access point and imitating a legitimate access point. Users usually don't know the difference and connect to this illegitimate device, giving the malicious user access to their data. The way to prevent this is simple. Don't use free WIFI, especially when it doesn't have a password. Some businesses require you to buy an item to get access to the WIFI, these can be more secure but still aren't fool proof. Be extremely wary if when you scan for WIFI on your device, you see two access points with the same SSID (access point name). If you are working on sensitive data on the go, I would recommend using your phone as an access point, because at least with that you know its secure.

The next wireless attack that you should be aware of is bluejacking and bluesnarfing. As you might guess, these both involve the use of Bluetooth for malicious purposes. Blue jacking is when a malicious user looks for all available devices nearby with Bluetooth on, then proceeds to send unsolicited messages to that user. This attack isn't as much dangerous but can be annoying. Bluesnarfing, however, can be more dangerous. Bluesnarfing is when the malicious user can gain access to the device via Bluetooth. There is one simple way you can prevent both attacks: make sure you are not leaving your Bluetooth on when not connected to a device. Think of Bluetooth as an outlet. If you left an electrical outlet out in public, any passerby can just connect to it, if they have a plug.

The final wireless attack I will discuss is shimming and card skimming. Card skimming is when a malicious user plants a scanner on a credit card machine slot and gets your data when you swipe your card. For skimming, your best bet to fight them would be to cover your hand when entering your pin (in case the user planted a camera nearby). Make sure the ATM you are using is in a public, well lit area. Give the reader part a tug and see if anything is loose. If it feels even a little loose, there could be a skimmer planted on top the real card scanner. Card shimming involves the scanning of the microchip on your card when you use it. To counter this, use a touch and go scanning method available on some credit cards, or feel for resistance when inserting your card. If you feel a significant amount of resistance, don't use it.

As our wireless technology advances, so do the thieves. It can seem like a never ending battle, but keeping current in wireless attacks is pivotal to keeping yourself from device or financial trouble.

If you have any questions about the wireless attacks, please give us a call at 509.433.7606 or submit a service request online at http://support.simplepowerit.com/