Wi-fi Hijacking

I-Team

John Bachman
WPEC News 12
July 16, 2007 - 10:26AM

Wireless internet access has become the norm for people wanting to log online anywhere they can sit down and open up their laptop. It's available at coffee shops, fast food joints, the airport and even some car washes.

But the more places you use wireless internet, the more access you give hackers to steal your money and your identity.

Experts say you are never 100 percent safe from hackers.

And most people don't even take the simple steps to protect themselves.

At the United States Secret Service field office in Miami, Deputy Special Agent-In-Charge John Large says the convenience of Wireless Internet or “wifi" works two ways: more accessibility for you and easier access for hackers.

“It really hides their true location at that point and that makes it hard to pinpoint where exactly that system was compromised. So it's additional challenge to investigators today”, says Special Agent Large.

Most of South Florida's financial or identity theft cases are investigated at the Secrete Service's computer forensic lab.

Large says, “Today there's not a crime that we investigate that doesn't involve the use of computer or any other electronic media in some fashion.”

Agent Large says cases of identity theft using “wifi” are increasing.

“The challenge to law enforcement today is to keep up with technology because it's evolving so fast. And organized criminal groups are going to use technology to their fullest advantage,” says Large.

Security experts like Paul Henry say too many people are making it too easy for hackers.

“Most people will simply turn on their wireless access point without implementing any encryption whatsoever”, says Henry.

Henry has more than 20 years of experience as a computer security expert, but says in the last few years, hackers are way ahead of the game.

In about ten minutes with software available for free on the internet, Henry says most hackers can easily breach networks even with security features in place.

“Connecting to your bank downloading email, having a chat conversation, is all in the clear. Anyone that can get within a reasonable proximity of your residence can view that information”, he says.

That’s why Henry says everyone needs to take some simple steps to decrease the chances you'll be a victim of "wifi" hijacking.

“Absolutely, you really have to be on your guard today,” says Henry.

Everyone who uses wifi at home must turn on its security features. Use something called W-P-A or "Wifi protected access." It requires a 20 character password and gives you the best protection. You can find it in your network connection menu. Also in your network settings assign a static I-P address to your computer. This will make it tougher to hack into your network. It's also important to keep all your computer's operating system is up to date and make sure you have the latest firewall and antivirus software installed. The most simple step, perhaps, is simply turning off your pc, your cable modem, and your access point.

The bottom line if you are using wifi in a public place, don't do anything you don't want others to get a hold of.

And if you don't think you can turn on the security features yourself, there are several local services that can do for you for between $25 and $50 an hour.

A small price to pay, considering what's at stake.