The Miami Herald
Posted on Fri, Aug. 20, 2010

Do you know who's looking at your Wi-Fi?

By JORGE L. VALENS
Sun-Sentinel

After someone sniffed out his password at a free Wi-Fi hotspot and successfully hacked his computer Igor Mello stays home for most of his web use.

``I trust my network more than anyone else's,'' said Mello, of Plantation, who had several social media sites compromised in the break-in.

Whether at home on their private networks or at a local coffee shop or library, Internet users should always protect themselves and their computers while surfing on Wi-Fi networks, experts say.

``It's like putting a lock on your door of your house. That's not going to stop a determined bad guy but it's going to keep the wandering neighbor from making use of your Internet connection without your knowledge,'' said Eric Johnson, a computer security expert at Florida International University.

To protect themselves at home, users can utilize security measures available in their Wi-Fi routers and access points such as Wi-Fi Protected Access versions one and two, according to Johnson, who is Systems and Networking Manager for FIU's School of Computing and Information Sciences.

WPA and WPA 2 encryption is built in to any hardware that is branded ``Wi-Fi Certified,'' a seal given to products authorized by the Wi-Fi Alliance, a nonprofit consortium of technology companies.

This type of security protects home networks by securing data between the access point and the computer with government grade encryption, according to the organization's website. WEP 2 will also randomly generate a secure password for the network and can be activated in the router or access point's settings.

Mello secures his home network using WPA 2 encryption and even then limits access to important sites like online banking to his cellular phone application, which transmits data over his mobile carrier's network, something that is much harder to penetrate.

Earlier this year, Google Street View vehicles unintentionally captured small bits of payload data, or information that is transmitted over Wi-Fi network such as website information or even passwords from open Wi-Fi access points, as they drove through cities and neighborhoods taking pictures for the street level view feature of Google Maps.

That seizure of information has sparked investigations of the matter by governing bodies world-wide, including Germany and the United States. Recently, Connecticut's Attorney

General launched an investigation of the incident and has drawn the support of 37 other states including Florida.

Leaving the default security settings switched on in a home wireless router is never a good idea.

Elias Montoya, Technology Director for Abadin Cook, a Miami-based law firm, said users should make sure to stick to a strong password, such as the WEP 2 generated password, that mixes characters, numbers, and letters rather than choosing something predictable like their home phone number or leaving the default password.

``The [Wi-Fi] user should be in the mindset that nothing is 100 percent secure. If someone is intent on hacking you, they will,'' Montoya said.

Wi-Fi use in public places, such as coffee shops, is becoming increasingly popular, but these networks are typically wide open, said Johnson.

``You should always treat any Internet activity you do at these locations as if it's being monitored,'' he said.

Johnson said people should stay away from doing anything that they would not want to be seen, such as online banking.

Many coffee shops offer free, secure Wi-Fi to customers, such as Java Boys in Wilton Manors.

Co-Owner Nicki Rose said that the free Wi-Fi is a big draw to the shop as many patrons use it as a ``home away from home'' or even come to drink coffee and run their business from the large couches and plush arm chairs.

Java Boys regulates its (AT&T) Wi-Fi network by giving customers a password to access at the front counter. The password is changed frequently to ensure that only customers that day have access to the network.

Johnson suggests that users stick to sites with a secure connection, typically denoted by a lock somewhere on the browser window and should be aware of any error messages that suggest the site is insecure.

Fort Lauderdale resident Sootie Oophe comes to Java Boys almost every day. He uses the internet for a range of different things, from paying bills to online gaming and relies on software allows him to computer's security settings depending on whether he is home or away with just a few clicks.

``I am still very aware and careful in what I do online,'' he said.