

## Identity theft growing, getting harder to stop

Publication Date  
**09/14/2009**  
Source:  
**Miami Herald (FL)**

MIAMI \_ With a few keystrokes, computer security expert Esteban Farao can find all the wireless networks in use in a half-block radius from a Starbucks.

One of them, it appears, is intended for guests at the Marriott. Others are private networks for individual businesses.

Farao, of Coral Gables-based Enterprise Risk Management, said the security of any of those networks could be compromised \_ a la Albert Gonzalez.

"It's a matter of time," Farao said, even for networks that are encrypted and password protected.

Gonzalez, of Miami, pleaded guilty last month to 19 felony charges in a Massachusetts indictment for tapping into the computer networks of T.J. Maxx, OfficeMax and other stores, stealing customers' data and selling it overseas. Federal prosecutors say he stole 40 million credit card numbers as a part of that scheme. He faces charges that he stole millions more from other companies.

Whatever tools an identity thief is using, whether Dumpster diving for individual credit card numbers, or stealing identities by the millions \_ "the damage that you can do to someone is exactly the same," said Wayne Ivey, a Florida law enforcement officer who has specialized in identity theft investigations for more than 15 years.

But this rapidly evolving crime is becoming more difficult to stop, Ivey said: Only one in 700 identity thieves is ever arrested.

"We're looking at a crime that has reached epidemic proportions," he said.

While a credit card company might forgive charges you claim you didn't make because your card was stolen, some craftier crooks can take the credit card information, coupled with other personal data, and apply for more credit, buy cars, a home, even get a job \_ or get arrested \_ using someone else's identity.

"The average person will expend over 400 hours trying to get their credit restored," Ivey said. "And the (Federal Trade Commission) estimates the average length of time between when identity theft occurs and the victim finds out is more than 12 months."

Much of the burden remains on consumers to protect themselves \_ and urge companies to take better care of their customers' data.

"Hopefully, the American public will start to realize what's going on and push for more security," said Sean Arries, a security expert with Terremark in Miami. He helps companies detect security problems and provides advice on how to fix them.

While many major retailers have updated the security of their networks, many smaller stores have not.

A recent survey by the National Retail Federation showed that small merchants that have never been breached may have an unrealistic expectation of their security: 72 percent of them believe the risk their company faces from a data compromise is low, or not possible, while 67 percent of merchants who have been breached call the risk high.

As a result, the survey showed, the latter group typically spends more to help secure their businesses.

With the right gear \_ which sells for only a few hundred dollars \_ a hacker can be as far as a mile from a place with a wireless network and break in, undetected, Arries said.

In the early days of wireless computer networks, there was no encryption \_ the process that masks information as it travels from one place to another, Arries said. Early on, criminals who managed to tap into others' wireless networks could easily read the information traveling over the network.

One of the first encryption systems, WEP, was riddled with security problems, he said.

But WEP is still widely used \_ especially in homes, Arries said.

"At your house, you need to make sure you're not using WEP," Arries said, noting that some older routers aren't equipped with the newest, more secure types of encryption, WPA and WPA2.

Arries also cautions against using public networks \_ at a coffee shop, airport or the like \_ for anything more than browsing the Internet.

It took him less than a minute to demonstrate how simple it is for someone to grab information streaming from a computer using an public wireless network.

When he logged onto his Facebook page, the intercepting computer was able to read his username and password \_ in plain text.

If you are using an open network and you're asked to approve an SSL certificate before continuing to the website you want to see, Arries said, it's likely you are approving someone else to view your information.

Aside from having unencumbered access to your Facebook page, a hacker might also capture the password you use for more sensitive information, your date of birth and other personal data.

"If I'm using a public network," Arries said, "I don't even check my Facebook page."