



School of Continuing Education
Marketing

NEWS RELEASE

FOR IMMEDIATE RELEASE

January 19, 2006

Issued by Justin A. Smith, smithj@uwm.edu or 414-227-3153

UWM Cautions Wireless Internet Users

Milwaukee—The latest Federal Trade Commission reports show that in 2004 of the 2,646 reported cases of identity theft in Wisconsin over 25 percent occurred in the city of Milwaukee and 75 percent of the victims were between 18 and 49 years old. The FTC also reports that 42 percent of the identities stolen were used in banking and credit card fraud.

Now that Milwaukee is in an elite rank of communities that provide city wide wireless internet access, there are several security challenges that residents will face. By using the convenience of wireless technology the dangers of internet identity theft become more prevalent. Users of the new public network will still have to be concerned about the standby methods of stealing personal information, “phishing”, “pharming” and spyware. Additionally they will have to be prepared to join a public and unsecured wireless internet network.

“The primary security danger of a wireless network, especially a public one, is information theft. Unsecured wireless networks allow even a novice thief the ability to capture personal information sent over the network without the sender or intended receivers knowing or giving permission,” says Mark McFadden, instructor of the Wireless Network Security and IT technology courses at the University of Wisconsin-Milwaukee School of Continuing Education.

He says that learning and implementing the latest in security technology will protect users of the proposed network. It could save them a lot of money and the many headaches caused by identity theft.

Most businesses use sophisticated firewalls and encrypting software to safeguard their sensitive information. However some individual users do not have these capabilities and there is a chance that their information could be literally snatched right out of the air.

According to McFadden the casual users of the public network are at increased danger when sending and receiving information through the wireless system. He says that without taking the proper security measures this could add up to real trouble for city residents.

“Wireless networks are a great convenience, but in public places the ability of thieves to capture and abuse personal information is a danger most computer users are not ready for. Just as you wouldn’t walk down the street showing your credit cards to strangers, you shouldn’t use an unsecured public network to share private information,” warns McFadden.

“Companies that deal with wireless networking have focused on ease-of-use. However, sometimes the simplest solutions are not the best. In the case of wireless networks, the default, “out-of-the-box” settings leave all the security features turned off. In the privacy of your own home that may make sense, but on a public wireless network it’s a scary scenario.”

There are real and significant risks with using an unsecured wireless network. If an unprotected user is paying bills, making purchases or checking their bank accounts online via the public network, all of that information is susceptible to a thieves prying eye. Email, instant messages and even private files stored within your computer’s hard drives are also at risk on an unprotected machine using a public network.

For information on IT security, usage trends for Milwaukee’s current wireless network and to learn more about what users should do to protect themselves on a public network please contact Mark McFadden at mcf@uwm.edu or 227-3243.