PRWeb®

Â□Drive-By HackersÂ□ Target Wireless Computer Networks

Wireless Internet technology causes security concerns. Dallas area security firm demonstrates vulnerabilities.

(PRWEB) June 2, 2004 -- New wireless computer technology has left thousands of Texas families and businesses susceptible to "drive-by hacking," allowing access to the private data stored on their computers as well as their internet accounts.

"It's like running a network cable out to the street and inviting anyone to plug in," said Jim Whitesell of HomeNetworkDefenders.com, a Denton, Texas area security consultant.

The culprit is the new wireless network technology called Wi-Fi, which allows users to connect all the computers in the house without running wiring everywhere. Wireless networks are inexpensive and easy to set up, but are not secure unless additional steps are taken, according to Whitesell.

Wireless networks are great - and have become very popular. "But people don't realize that the signal usually goes well beyond their own walls, and anyone with a portable computer and wireless access card can probably connect to their network as easily as the owner." said Whitesell. "Anyone can Â□borrowÂ□ your internet connection to visit illegal sites, send spam, or upload viruses, and it all is traceable back to the network owner. Hackers may also be able to gain access to the data stored on your hard drive, including passwords, banking information, credit card numbers, etc."

Whitesell demonstrated how common these wireless networks are. Armed with a regular laptop computer and specialized software connected to a GPS receiver, he randomly drove along several Denton streets and found 130 wireless networks in about an hour. Of these, 67% had no security at all. "Wireless networks are incredibly easy to set up. Simply take them out of the box and plug them in. Most people don't realize how vulnerable their computers are once their wireless networks are working." Whitesell added.

Are people really trying to break in through wireless networks? Absolutely. Late last year, two Michigan men repeatedly hacked into the Lowe's home improvement chain's national computer system, getting access to credit card and other information, the federal government says. How did they do it? While sitting in the parking lot with a notebook computer, they were able to access LoweÂ□s computer system through LoweÂ□s wireless network.

There are several steps taken by HomeNetworkDefenders.com to make computers and networks harder to access by unauthorized users. The company visits customersÂ□ homes or businesses and conducts inexpensive security audits, and configures the computers and networks for the highest level of security available. More information is available on the company's web site, www.HomeNetworkDefenders.com.

Media Note:
Local Computer Security Expert Available for Interview

What: As the popularity of wireless computer networks continues to grow, most consumers and small businesses are not aware that their data may be at risk. Travel with a local wireless network security expert as he demonstrates how prevalent the problem is. Armed with only a notebook computer and specialized software, heÂ□ll show how easy it is to receive wireless network connections that allow access to these unprotected networks.

Who: Jim Whitesell, principal of HomeNetworkDefenders.com

Where: Interviews are available in the D/FW area to local media outlets
When: Interviews and demonstrations can be scheduled weekdays.

Contact Information
Jim Whitesell
PROFESSIONAL INTERNET
http://www.HomeNetworkDefenders.com
214-764-0984

Online Web 2.0 Version

You can read the online version of this press release here.

If you have any questions regarding information in these press releases please contact the company listed in the press release. Our complete disclaimer appears here - PRWeb ebooks - Another online visibility tool from PRWeb