ILLINOIS ATTORNEY GENERAL LISA MADIGAN

PRESS RELEASE

www.IllinoisAttorneyGeneral.gov

For Immediate Release
Contact: Melissa Merz
312-814-3118
877-844-5461 (TTY)
mmerz@atg.state.il.us
January 17, 2006

*******CONSUMER ALERT*****CONSUMER ALERT*******

MADIGAN WARNS COMPUTER USERS ABOUT "EVIL TWIN" ATTACKS AT WIRELESS HOTSPOTS

Chicago – Attorney General Lisa Madigan today warned consumers about a security threat to wireless hotspot users. When people are using wireless networks found in public places such as shops and cyber cafes, attackers can mimic the characteristics of the legitimate wireless network. As a result, hotspot users can unknowingly connect to the attacker's computer (sometimes referred to as an "Evil Twin") instead of the intended wireless network.

Madigan said that attackers operating Evil Twins can hijack data, such as passwords and credit card information, and deploy malicious computer codes. Evil Twins even can control which Web site appears when the user accesses the Internet, often mimicking the user's intended Web site to capture their private information.

"An 'Evil Twin' can rob a computer user of personal and financial information instead of providing a safe connection to the Internet," Madigan said. "By taking precautions, wireless hotspot users can decrease their chances of having a run-in with an Evil Twin."

Madigan recommended that wireless network users exercise caution and provided the following list of precautionary steps to help users avoid becoming victims of wireless network attacks:

- Disable your laptop's wireless card unless you are planning to use it;
- If you decide to use a public wireless connection, ask the provider for the exact name of its wireless network (also called a "SSID"). Be cautious of similarly named wireless networks, especially those using network names indicating that access is free when a public provider in the same location requires a service fee;
- Do not configure your computer to auto connect to a non-preferred wireless access point;
- Avoid sending sensitive information when using a wireless network;

- Use a personal firewall, keep your software and operating system updated and turn off file sharing;

- Use hotspot providers that provide secure encrypted connections and a list of trusted hotspot locations. If you are not sure whether a wireless connection is secure, assume you are using an “open” hotspot and that as a result, all of your communications to and from the wireless network can be monitored;

- If you must use an open hotspot for sensitive communication (e.g., reading email, making online purchases, etc.) make sure the Web site you are using supports SSL or other types of secure connections. A padlock symbol appears in Web browsers when users communicate with a secure Web site; and

- Be aware of your environment. Crowded public hotspots increase your risk of being a victim of a wireless attack. Additionally, try to prevent other people around you from reading sensitive information appearing on your computer screen.

For more information or to report a suspected Evil Twin attack, please contact Madigan’s High Tech Crimes Bureau at 312-814-3762.

-30-

Return to January 2006 Press Releases