Being 'Grounded' Is a Good Thing

By Kim Stokes, Editor-in -Chief, kstokes@cahners.com

Security is a primary concern in our society. Everyone worries about national security, security of personal property, and financial security. But unless you are the head of a corporation, how many of us really worry about wireless network security? As wireless networking becomes stronger in the wireless industry and infiltrates our personal lives, we need to be prepared for the security issues that will pop up.
Wi-Fi (also known as 802.11) allows users to send information over unregulated raido waves. As with any public concern, some critics and analysts warn about Wi-Fi's lack of security, while the Wireless Ethernet Compatibility Alliance (WECA) assures that their Wired Equivalent Privacy (WEP) security protocol will ward off hackers and protect our data through encryption.
A growing concern is that hackers can obtain data traveling through air if a Wi-Fi network isn't properly grounded. Security experts say that approximately 10% of users install the basic safeguards. Basic? One place the public encounters these networks is during curbside check-in at an airport. Because Wi-Fi uses a range that can be easily picked up by hackers, it would not be difficult to obtain and alter scanned luggage, and airline information for their own benefit. I don't think I'll be using curbside check-in until my data traveling through the air is a little more secure.
At the beginning of this year, some companies that deal with sensitive data actually banned or encouraged customers to move away from wireless networks in their facilities &#151 Livermore Labs (nuclear weapons); M.D. Anderson Cancer Research (to protect patient data); Aeronautical Radio (provides communications services to airlines and the government) &#151 until they can be determined more secure.
Five days after the start of the 2002 Winter Olympics, the International Olympic Committee announced that equipment based on 802.11 won't run the operation of any Game until at least 2008.

WEP has been further threatened with the debut of AirSnort, a program that automates the attack process so that anyone with a Linux box and a wireless networking card can download the program and, well, hack away. The upside of this wonderful little program is that it could lead to faster developments in securing Wi-Fi networks. By presenting AirSnort to the public, maybe people will be more aware that any data sent on a "basic grounded" network should be considered public information.

While the popularity of Wi-Fi continues to grow because it is an ideal way to link users to the Internet and to send data between consumer electronics and personal computers, its security concerns need to be resolved. Every person transmitting data wirelessly &#151 even just talking on a cell phone &#151 needs to take responsibility for what they are transmitting. If you don't want hackers to have access to sensitive information, be careful as to what you are transmitting.

Source URL (retrieved on *03/13/2014 - 4:23pm*):
http://www.wirelessdesignmag.com/product-releases/2002/02/being-grounded-good-thing?qt-blogs=0