



GENERAL WIRELESS SECURITY ISSUES AND THREATS

As wireless computing gains popularity with public “hotspots” appearing world wide, be aware of possible threats to your computer and how to protect yourself. This article helps you learn more about wireless security.

WHAT IS WIRELESS? WHAT ADVANTAGES DOES IT OFFER OVER WIRED CONNECTIVITY?

Wireless connectivity refers to the ability to access the Internet, your files and others, without the use of cables, wires or fixed points (phone jacks and power plugs). This is most commonly accomplished through Wi-fi technology. Wireless provides convenience and mobility unavailable with other network connections.

WHY IS WIRELESS SECURITY A CONCERN?

Unlike wired, wireless technology transmits data using radio waves, through walls and floors into public space. This makes the data vulnerable for others to intercept. With wireless network ranges of 75-100 feet in a home or office, and up to a 1 mile outdoors, wireless security is important.

WHAT IS A ROGUE ACCESS POINT? WHAT DANGERS ARE POSED BY ROGUE ACCESS POINTS?

A rogue access point (AP) is an unauthorized access point, connected to a corporate or home network to leverage wireless capability. These APs leave the network, regardless of how secure or how enclosed it may be, open to hackers and snoops to access valuable corporate or personal data. Because rogue points appear just like any other user on the network, they are difficult to detect. Software such as AirSnort and WEPCrack help detect rogue APs by “sniffing” them out.

WHAT IS AN EVIL TWIN? WHAT IS WPHISHING?

Most common in public hotspots, hackers set up rogue access points and create a network that mimics the look and behaviour of the network users expect to connect to. This is known as an Evil Twin. Unknowingly, users connect to the hacker’s network instead of the intended network. Users enter passwords, account information, credit card information etc. The hacker intercepts all of this information for his own use, then sends the user on to the real network. Hackers have become so clever as to even mimic the page to which users normally first connect. Just like a fisherman reeling in fish that have taken the bait, the hacker reels in users’ confidential information, hence the term Wphishing.

WHAT IS A WAR DRIVER? WHAT IS WAR CHALKING? HOW DO THESE INDIVIDUALS AND ACTIVITIES POSE THREATS TO WIRELESS SECURITY?

A war driver is someone who drives around equipped with a Wi-Fi enabled laptop or PDA, looking for wireless networks for free Internet access or confidential corporate information. Similarly, war chalking refers to individuals driving around looking for open wireless networks, that once found, are made public by drawing special symbols on nearby lamp posts or walls.