

Identity thieves can lurk at Wi-Fi spots

By Jon Swartz, USA TODAY

SAN FRANCISCO — Coffee shop Web surfers beware: An evil twin may be lurking near your favorite wireless hotspot.

Thieves are using wireless devices to impersonate legitimate Internet access points to steal credit card numbers and other personal information, security experts warn.

So-called evil-twin attacks don't require technical expertise. Anyone armed with a wireless laptop and software widely available on the Internet can broadcast a radio signal that overpowers the hot spot.

How to avoid an 'evil twin'



- Install personal firewall and security patches.
- Use hot spots for Web surfing only.
- Enter passwords only into Web sites that include an SSL key at bottom right.
- Turn off or remove wireless card if you are not using a hot spot.
- Avoid hot spots where it's difficult to tell who's connected, such as at hotels and airport clubs.
- If hot spot is not working properly, assume password is compromised. Change password and report incident to hot spot provider.
- Do not use insecure applications such as e-mail instant messaging while at hot spots.

Source: AirDefense

Then, masquerading as the real thing, they view the activities of wireless users within several hundred feet of the hot spot.

"It could be someone sitting next to you on a plane or in a parking lot across the street from a coffee shop," says Jon Green, director of technical marketing at Aruba Wireless Networks, which makes radio-wave-scanning equipment that detects and shuts down bogus hot spots.

"Wireless networks are wide open," says Steve Lewack, director of technology services for Columbus Regional Medical Center in Columbus, Ga.

The facility uses software and sensors to monitor 480 wireless devices used by medical personnel at 110 access points. Last month, it stopped about 120 attempts to steal financial information from medical personnel and patients — double the number of incidents from a few months earlier.

The recent surge in evil-twin attacks parallels phishing scams — fraudulent e-mail messages designed to trick consumers into divulging personal information. Though the problem is in its infancy, it has caught the attention of some businesses heavily dependent on wireless communications.

But most consumers aren't aware of the threat, security expert Green says.

Wi-Fi, or wireless Internet, sends Web pages via radio waves. Hot spots are an area within range of a Wi-Fi antenna.

As the technology has grown — there are now about 20,000 hot spots in the USA, up from 12,000 a year ago — so too have security concerns. Anil Khatod, CEO of AirDefense, a maker of software and sensors, estimates break-ins number in the hundreds each month in the USA.

Companies employing hundreds of people with wireless laptops are especially vulnerable to evil-twin scams. When a worker's information is filched, it can expose a corporate network.

"It presents a serious, hidden danger to Web users," says Phil Nobles, a wireless-security expert at Cranfield University in England who has researched the threat. "It's hard to nab the perpetrator, and the victim has no idea what happened."