



Monroe County
 Appeal
 Paris, MO
 Circ. 1856
 From Page:
 10
 11/5/2009
 19921



can, Secretary.

APPEAL PHOTO

Don't fall victim to wi-fi hackers ⁶¹

Traveling Internet users tap into any public wireless hotspot at local restaurants, coffee shops and libraries to check e-mail and visit Web sites on the road. An April 2009 study by Pew Research Center showed that 56 percent of adult Americans have accessed the Internet through a wireless network. Unfortunately, cyber criminals are taking advantage of these conveniences, causing headaches for Wi-Fi users across the country.

The greatest concern with Wi-Fi networking is the increased use of sniffers. A sniffer is a tool to help monitor network traffic. If used illegitimately, a sniffer can capture any unencrypted data being transmitted over a Wi-Fi network. This data may include bank account and credit card numbers or passwords to services such as Facebook or Gmail.

Dave Sill is an IT Manager for Socket, a Missouri-based telephone and Internet provider.

"It is extremely easy for scammers to download sniffers and capture private information from unsuspecting surfers," said Sill. "Fortunately, there are things Internet users can do to protect themselves."

Sill recommends using encryption to scramble data before it is transmitted, neutralizing the threat of sniffers. Most modern operating systems and security software

programs will automatically present a warning if the network is unencrypted. While no encryption is perfect, its use generally makes the job of cyber criminals much more difficult.

If a wireless network is not encrypted, Sill warns it is unsafe to transmit private information, even if the network is password-protected. A Wi-Fi password can easily be given out and sometimes purchased along with a cappuccino at the coffee shop. Also,

while a password helps prevent unauthorized off-site use of a Wi-Fi network, it does little to protect users from those sitting across the room.

"Pay attention to security warnings on your computer and don't take the privacy of your data on a public network for granted," said Sill. "If you're not certain a Wi-Fi connection is secure, pretend a cyber criminal is looking over your shoulder and act accordingly."

Sill suggests a few other security precautions when using a public Wi-Fi network:

- Switch off the Wi-Fi when not in use.

Most laptops have an external switch for this purpose.

- Identify the hotspot as "Public."

Selecting this option causes the computer to use more secure network settings.

- Connect through a Virtual Private Network (VPN) if possible.

Many companies use VPNs to connect multiple offices or enable telecommuting. They also encrypt data at one end and decrypt it at the receiving end, making a connection more secure.

- Verify the padlock symbol on a Web browser.

This indicates a secure Web site and is especially important when connecting to sensitive services such as online banking or shopping Web sites. It is also important to not ignore warnings about the authenticity of certificates, which can indicate a possibly untrustworthy Web site.

Public Wi-Fi is here to stay, and security becomes more important with each new user. Most hotspots offer some level of protection; however, users are ultimately responsible for the safety of their own data. Use common sense and a good security software program to avoid becoming a victim.