Public Wi-Fi - Panacea or Peril?

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE

Today's technology allows for virtually instant 24/7/365 access to information, entertainment, friends and family. Wi-Fi access is everywhere – from the donut shop to the mall to hotels and restaurants. As convenient as it may be to check your e-mail at the grocery store, the ability to be connected is not without risks. Helping clients understand the drawbacks and possible danger of public Wi-Fi is another value-added service of the professional insurance agent.

Wi-Fi networks can be "secured" or "unsecured". "Unsecured" (HTTP) networks do not require a login or password. "Secured" (HTTPS) sites require a WEP, WPA or WPA2 password for access, and use encryption to make transactions safer. WPA2 is the strongest. Some websites only use encryption for the main sign in page. Look for the HTTPS on every page you visit. Encryption of data increases the safety of public Wi-Fi, but it is still not ideal, as even secure sites can be hacked. Secure networks encrypt all data. Regular users of Wi-Fi hotspots should use a Virtual Private Network (VPN) that encrypts all transactions. Disable the "auto-connect" feature on all devices.

Mobile apps are more susceptible to hacking, as many of them are not encrypted. Unlike the HTTPS designation for websites, mobile apps do not have a way for users to see if they are encrypted. When accessing sensitive sites with a mobile device, use a secure network. If a password is not required for access, then the network is most likely not secure.

There are a number of dangers of public Wi-Fi, including Man-in-the-Middle (MitM), snooping and sniffing, rogue Wi-Fi networks, malware distribution, and worm attacks. "Man in the Middle" happens when the hacker gets between the user and the site they are trying to reach. The hacker intercepts everything the user sends – emails, passwords, and credit card information. The hacker may then be able to access the user's systems at will. For those working remotely, this can expose the employer's network.

Snooping and sniffing is another form of eavesdropping. Hackers use special software in an attempt to obtain sensitive data, including passwords and login information. Worms and viruses can also be introduced into devices on public Wi-Fi. Viruses need a specific program

file to attack, but worms are standalone software that can do damage on their own.

There are suggested protocols for use of public Wi-Fi. Never leave your devices – laptops, tablets, phones – unattended in a public place. Even if you are on a secure network, someone could access the information on your device, or steal it. Public Wi-Fi should never be used to transact business on accounts containing sensitive information, such as banking and investment records. Avoid shopping online on public Wi-Fi.

Bluetooth is another feature to be aware of. Bluetooth enables the wireless exchange of data over short distances. Some versions of Bluetooth connect automatically to any nearby Bluetooth device, which opens the user up to all of the hazards of hackers and malicious acts. Be sure to turn it off when not in use.

Having internet access everywhere is a huge convenience, but it also comes with huge risks. Alerting clients to the possible dangers of connecting to public Wi-Fi is another sign of the true insurance professional.

Previously published in the Insurance Advocate®