Staying Safe When Using WiFi

Reid Goldsborough

WiFi is everywhere these days. We use it on laptops at home and in coffee shops, on tablets in airports and hotels, on phones to save money when viewing video, on TVs if we've cut the cord with our cable or satellite TV service and don't otherwise have a corded connection, and elsewhere.

Short for wireless fidelity, WiFi or Wi-Fi is a wireless networking technology based on radio waves. Devices connect to the Internet over the air instead of through a physical cable. Like digital technology in general, WiFi gives us more freedom and power. But there are negatives associated with the positives, risks you should be aware of to reduce them.

It has been said that using an unsecured public WiFi network is as safe as having unprotected sex in public with strangers. This is an overstatement, but there is software out there that can enable fellow hotel guests or coffee shop patrons to snoop on what you're doing over the same WiFi network, even nabbing your credit card information, checking account login, and Social Security number. In other words, you can have your identity stolen.

You hear lots of scary sounding jargon about WiFi security risks, including the Evil Twin gambit, Firesheep attacks, and sniffing. Some of the fear is no doubt fanned by security companies trying to drum up business for their software or services and some by computer wonks showing off. But some is real.

One trick is for a bad guy to set up a rogue WiFi network that looks like the legitimate one of the library or coffee shop you're visiting but that lets the crook see and harvest the information needed to steal from you. To avoid this, before connecting, verify the name of the network by asking a staff member or checking any signs that are posted for instructions.

Make sure any sites you connect to in which you have to sign in using a password use TSL (Transport Layer Security) or SSL (Secure Sockets Layer) security. With such sites, the web address begins with "https." Most do, but it doesn't hurt to check, particularly when buying, banking, or doing similar activities.

The most secure option with public WiFi is using a virtual private network (VPN) service such as Hotspot Shield (www.anchorfree.com), Private WiFi (www.privatewifi.com), and WiTopia (www.witopia.net). Such services, which often come in free, ad-supported versions and ad-free and faster pay versions, encrypt all data that flows between your device and anything you connect to over the Internet.

Home WiFi networks also present security challenges. Some people don't turn on security when setting up a home WiFi network, which can enable a neighbor to capture your personal information or freeload off your Internet connection. Securing your home WiFi simply requires using the software that comes with your router to type in the passkey whenever you add a new device to the network for the first time.

Another trick sometimes recommended with new routers is choosing an intimidating sounding network name (SSID) such as c:\virus.exe to scare off nosy neighbors or passers-by. Alternately, you can disable SSID broadcasting, which hides your network's name.

Other commonly recommended security precautions will also help you stay secure with WiFi. Keep current with operating system and program updates. But whenever possible, it's best to do updates over connections you're sure are secure rather than using public WiFi.

Use firewall and anti-virus software and keep it current, whether a pay service such a Norton Security (www.norton.com), which does it all, or a free service such as AVG Free (free.avg.com), which you can use in combination with your operating system's own firewall.

Set your browser to block pop-up windows. Be especially wary of updating software through a pop-up window when you connect to a website.

Don't use the same password over multiple sites, particularly sensitive shopping or banking sites.

Opt for two-factor authentication when it's available. With this, along with typing a password, you have to answer a question or receive a text, which is more secure.

It's better to use long passphrases instead of short passwords. For help in remembering passphrases, you can make each a variation of a theme, changed in a standard way based on the site you're connecting to.

Some people use a password management program such as Lastpass (www.lastpass.com) and KeePass (www.keepass.info). Others store their passwords in a word-processing document and encrypt it themselves. Don't keep passwords on scraps of paper stuck on your computer's screen, which defeats their purpose.

Reid Goldsborough is a syndicated columnist and author of the book *Straight Talk about the Information Superhighway*. He can be reached at reidgoldsborough@gmail.com or reidgold.com.