THE INDIANA LAWYER .com

Start Page: Not so wonderful wireless comes with hitches

Kim Brand September 11, 2013

The last personal computer you bought probably wasn't a PC. It was a 'mobile' device – a tablet or laptop or smartphone. The common denominator of these devices is their dependence on wireless connectivity to your local area network and/or the Internet. The 'jack' is gone.

Wireless Fidelity, or WiFi, has become an expectation at coffee shops, car dealers and college campuses. The modern law office too. But the technology invented in 1999 has succeeded beyond its inventors' expectations. So like our phone system, nobody was quite prepared for the uses to which it has been put.

A marvel of technology, the radios in almost every device seem to auto-magically connect to networks wherever you may roam. Once you connect, they remember your logon information and make your laptop, tablet or smartphone a part of your host's network. This is a great convenience if you need to check your email, browse the Internet or update your Facebook page, but as with most digital conveniences today you bear the risk of use.

The ubiquitous logo of the Wi-Fi Alliance: http://www.wi-fi.org/

Some WiFi providers offer Internet as an amenity. It would be odd to walk into a Starbucks today and observe the majority of their guests actually talking with one another. Mobile devices demand connectivity and WiFi is the way that is done. The service is offered on an 'as-is' basis and the vendor is usually unwilling or unable to offer tech support, so the typical wireless configuration is 'Open.' That means there is no password required and no encryption enabled. Basically, anyone sharing the same connection can snoop on what you send and receive over the host network. As an attorney this should give you pause if you are doing anything other than ordering another pair of shoes from Zappos.

The thing to know about Internet service offered as an amenity is there can be no assurance that anything you do is private. The opportunity for the host to monitor your traffic is obvious – they control the network and may have a duty to prevent certain types of activities: browsing pornography, conducting illicit hacking, spewing SPAM across the Internet, to name a few. Indeed, operators of open wireless networks have been charged with the acts of unscrupulous users. That's why you often see 'Terms of Service' pages that you must click through. It gives the operator cover in the event the FBI shows up to investigate who may have a predilection for illicit materials.

The first layer of security offered by the IEEE 802.11 standard developed by the Institute of Electrical and Electronics Engineers applied a fairly rudimentary encryption algorithm to the information you pass over the wireless connection called WEP: Wireless Equivalent Privacy. It wasn't. The standard (since 2003) has become WPA2: Wireless Protected Access II. This allows connected devices to encrypt data in a far more secure way. This method introduced more robust passwords and more secure networks. You should still be concerned.

Most law firms want to offer wireless access to their staff and guests. This demands a more complex configuration than simply plugging in a WiFi router from Fry's. The best systems employ login names and passwords that are managed by your server – but these are expensive. The advantage of this system is that an individual user can be 'deauthorized' without everyone else suffering the need to change their credentials. The minimum standard is to isolate the private from the public network by providing a different password to staff than you do to your guests. You should change the guest password frequently.

Another problem with WiFi is coverage. A small office may be well served by a single Wireless Access Point. But a firm with 10 or more offices will almost certainly need two or more. Larger networks require 'Mesh' technologies that operate like cell phone towers and hand off users from one WAP to another and share the load. More WAPs can produce congested radio traffic which is hard to mitigate. It gets very complicated very quickly.

WiFi was designed to use standard radio frequencies. The problem with that is that many other devices do too. Cordless phones, motion detectors, microwave ovens and remote control toys all play a part in the general noise within these radio frequency bands. If your WiFi connection always fails around lunch time, ask your colleagues to stop using the microwave. If your wireless network is in an area with lots of other WiFi networks (say an office building) expect the clutter to produce interference too.

Adding 'bandwidth limiting' features to prevent 'WiFi hogs' from consuming your Internet access is becoming a modern necessity. In today's world you can never get enough Internet.•

Kim Brand *is a technology expert and president of Computer Experts, Inc. in Indianapolis. He is the inventor of FileSafe, the only on-premises file server priced like a cloud service. He is also an adjunct professor of legal informatics at IUPUI. Contact Kim at info@ComputerExpertsIndy.com or call 317-833-3000. Opinions expressed are those of the author.*