ALPS
Practice Management Pointers

With Free Wi-Fi Be Worried. Be Very Worried.

Mark Bassingthwaighte, Esq.
mbass@alpsnet.com

I like convenience as much as the next guy but I also exercise caution whenever I see the word "free." Why? Because the old adage "With free you get what you pay for" does mean that sometimes you either end up with nothing at all or with more than you bargained for. I become particularly concerned whenever I see the words "free" and "Internet" together and so should you.

In this day and age, unsecured Wi-Fi networks are practically ubiquitous. You will find them in airports, hotels, office buildings, coffee shops, restaurants, malls, and even municipalities. While this is convenient when you want to buy a new book on your e-reader, check your e-mail on your laptop, or rebook a flight on your tablet, doing so in the unsecured Wi-Fi environment can create a real problem days, weeks, or even months later. Consider the following. In 2010 a free Firefox browser add-in named Firesheep was released that enabled the user of Firesheep to hijack the social media accounts of anyone else who happened to be using the same unsecured network that the Firesheep user was on. Facebook, Google, Twitter, Windows Live, and Yahoo are just a sampling of the sites Firesheep targeted. While this type of attack was not new, it was now far easier for anyone to become a hacker. Hacking became a readily available opportunity for the masses and things haven't gotten any better since. If you remain skeptical, try entering the search term "hacking software" into Bing and draw your own conclusions.

Unsecured Wi-Fi networks are insecure by definition and, if for no other reason than the inconveniences that come from securing them, these networks will remain unsecured. That's just the way it is. Given this, one should never connect to an unknown network particularly if the connection is free and understand that just because a connection claims to be Hilton's, Jet Blue's, or Starbucks', doesn't mean that it actually is. Always inquire as to what the proper SSID (the public name of the network) is before connecting to any unfamiliar network. I know that some will say that the Starbucks signal is free, they've used it many times and they never had a problem. In response, remember hacking is now available to the masses. This isn't just about who made the signal available, it's also about not knowing who else may be using that same free signal but now to your detriment if you're there with them.

Unfortunately there is an overabundance of perceived "legitimate" networks out there that are also unsecured to include those found in hotels, airports, coffee shops, and even some law offices so not

only should you verify the proper SSID but only connect to the unsecured Wi-Fi network if you have the ability to secure the connection yourself. This can be done by using a VPN connection which basically means you will be encrypting your data stream. VPN stands for virtual private network and allows you to create a secure tunnel between your remote computer and the home office. There are a number of ways to do this (e.g. LogMeIn, OpenVPN, VPN Unlimited, and Cisco VPN) so my best advice would be to discuss the options with your IT staff or consultant who should be able to recommend an appropriate solution for your specific situation.

I wish that I could stop here but I can't. With the rapid proliferation of smart phones and tablet computers coupled with the shift to tiered data pricing, additional avenues of exposure arise as users can and will use these devices to connect to the Internet via a wireless signal. In this day and age of bring your own devices to work, who wants to waste their precious data on work? Everyone wants to save their data in order to be able to stream the latest episodes of whatever reality TV show is currently in vogue. The Verizon signal is turned off, the Wi-Fi connection enabled and off to work they go. Just be aware that there are software solutions available that provide mobile security on such devices thus protecting them from viruses, malware, and hacking. There are also other software solutions that allow the mobile device user to connect to the home office via a secure VPN connection. Again, talk with your IT staff or consultant and heed their advice. In light of the risks associated with unsecured Wi-Fi, a little convenience simply isn't worth it because in the end you get what you pay for in terms of security and that would be nothing.

Risk Management Questions?

Mark Bassingthwaighte, Esq. is the Risk Manager for ALPS Property & Casualty Insurance Company. He is available to answer risk management questions and can be reached at 1-800-367-2577 or mbass@alpsnet.com.

Disclaimer:

ALPS presents this publication or document as general information only. While ALPS strives to provide accurate information, ALPS expressly disclaims any guarantee or assurance that this publication or document is complete or accurate. Therefore, in providing this publication or document, ALPS expressly disclaims any warranty of any kind, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Further, by making this publication or document available, ALPS is not rendering legal or other professional advice or services and this publication or document should not be relied upon as a substitute for such legal or other professional advice or services. ALPS warns that this publication or document should not be used or relied upon as a basis for any decision or action that may affect your professional practice, business or personal affairs. Instead, ALPS highly recommend that you consult an attorney or other professional before making any decisions regarding the subject matter of this publication or document. ALPS Corporation, as well as any of its subsidiaries, affiliates and related entities shall not be responsible for any loss or damage sustained by any person who uses or relies upon the publication or document presented herein.