About this Article

This article outlines the major security risks facing computer users in hotels and wireless hotspots and outlines practical steps you can take to protect yourself in these environments.

Information Security Concerns in Hotels and Hotspots

By Bill Murray, CISSP
IT Risk, Security & Compliance Manager
Westfield Group

More and more of us are using our computers while we are on trips and are making use of the ever increasing number of wireless hotspots that are popping up everywhere. I want to discuss some risks associated with connectivity in these environments and offer some simple things that you can do to reduce these risks.

- Most hotels and wireless hotspots offer a number of wireless access points to connect to. Each one will appear separately in your wireless network list. You should check with the establishment you are at as to which ones are “official” and which ones are not. Many times scammers set up an access point named something similar to those provided by the establishment. These rogue access points can be set up to perform a classic “man in the middle” attack known as an “Evil Twin” to forward all your traffic to a real access point and simply capture everything you are doing online. Another scam is to offer you access at an additional fee.
- When entering your ID and password in public places, take extra care to watch for people looking over your shoulder. “Shoulder surfing” it is sometimes called. It does happen.
- Wireless connectivity can be implemented securely but if you have a choice between a wireless access point and plugging your laptop into a network jack, choose the network jack.
- It is important to have your personal firewall turned on and configured with a restrictive rule set when attached to non-trusted networks. What I mean by a "restrictive rule set" is simply configuring your firewall to allow only software you trust to access the Internet, and block all other software and network traffic. Anti-virus software should also be enabled, have real time protections turned on and be configured to download anti-virus signature updates automatically. These are relatively simple things to do.
- Use your corporate VPN (Virtual Private Network). If you are doing work for your company and they have VPN capabilities, you may be safer connecting to the Internet this way. It may sound strange – connecting to the Internet to connect to your company to connect back to the Internet – but your company has protections in place to block malicious traffic, attackers and websites. If you establish an encrypted VPN tunnel to them and surf through their network to the Internet, you are adding a few controls that can protect you.

- Keep your laptop powered off when you leave it in your hotel room. Lock it in the safe if it will fit. If you just lock the screen (control alt delete), there are vulnerabilities that could be exploited while you are not there to gain access to your software and data.
- Don't leave your laptop sitting there all alone when you get up and get another coffee or cheeseburger. It may not be there when you go back to your seat. Same goes for USB drives. It is pretty easy to swipe them without notice.
- Encrypt your hard drive and USB drives, or at least sensitive data or subdirectories on them. If the unthinkable happens and your laptop is lost or stolen, let the most significant thing the thief gets be the laptop. It may sound like a hassle but losing $1000.00 on a laptop is a whole lot better than a case of identity theft for you and any other people regarding whom you have information stored. Same goes for information about where you live, your children, relationships you are in, etc. Any of this information could be used against people you care about.

Westfield regularly publishes a blog containing practical security tips for agents and other industry participants at www.infosec.westfieldinsurance.com and I encourage you to subscribe to it. See also the "Security & Privacy" section of the ACT Web site at www.independentagent.com for additional helpful information on agency security issues.

Bill Murray is IT risk, security & compliance manager for Westfield Insurance and the major part of this article was originally published on Westfield's blog. He has authorized ACT and IIABA, its state associations and ACT members to republish it with appropriate attribution. Bill can be reached at WilliamMurray@westfieldgrp.com. For more information about ACT, visit www.independentagent.com/act or contact Jeff Yates, ACT Executive Director at jeff.yates@iiaba.net. This article reflects the views of the author and should not be construed as an official statement by ACT.