

## 10 Tips for Keeping ID Thieves Behind Bars

By *David Milman*

Article published with permission from Small Business Technology Magazine

The pressures on small businesses are great enough without having to worry about technology. But technology changes every day, seemingly every minute. For small business owners and employees on the go, this means work doesn't stop just because you're a road warrior. In fact, many of our customers tell us they are even more productive on the road.

Protecting yourself, your equipment, your employees and your business from technological threats in this mobile world can be a dizzying challenge for any small business owner. Before you hit the road, consider these tips and best practices to steer clear of on-line identity theft:

1. Don't ignore your security updates, such as those from Microsoft Windows if you're on a PC. When that little annoying pop-up window says you have updates, pay attention! Those are critical to making sure you have the latest tools to protect your computer.
2. Always have the latest and updated antivirus and anti-spyware programs on your computers. While there are many sufficient free versions, paying for the top-of-the-line programs is always safest. Consider antivirus software programs from McAfee, Trend Micro or Symantec that often have anti-spyware tools built in. Another great anti-spyware program is Webroot Spysweeper.
3. Turn the "file sharing" setting off on your business's notebook computers. While this feature might be convenient in the workplace, it's critical to turn it off when you're traveling so that nobody can view your company or personal files. Password-protect any file that contains sensitive information. Microsoft Windows XP has this built right in.
4. When you compress a file you can secure, encrypt and password protect it. Don't forget your password. Other programs that have this ability are WinZip and WinRAR.
5. Disable the wireless radio on your notebook computer when not in use. Newer models have built-in wireless cards that are often visible when your computer's power is on.
6. When utilizing a Hot Spot to access the Internet, make sure you either pay for the access or sign in through some sort of "landing page" which tells you who the Hot Spot provider is. Avoid logging on to a "copy cat" network set up by a hacker.
7. Use a password to log on to your computer at all times—at the office and especially when traveling. Do not use any personal identification or obvious codes when creating these passwords, such as your Social Security number, birthdate or company name. Ideally, you should also use an alphanumeric password combination and change it every month.
8. When traveling, bring a travel router with a built-in firewall with you. Linksys (a division of Cisco Systems, Inc.), 3Com and NETGEAR offer mobile solutions. These routers should be configured and tested by your IT manager or consultant before you travel.
9. Voice over IP (VoIP) is becoming more popular. Executives are traveling, they can literally bring their office communications system with them. Be aware of the security gaps that can be exploited through VoIP and the preventative measures you can take. Make sure that all software security updates have been downloaded and installed before using your softphone or VoIP equipment. Also make sure your firewalls are properly configured and that your VoIP traffic is encrypted. Ask your VoIP provider about this.
10. Set up a virtual private network (VPN) for your notebook computers. This will encrypt and protect any emails or communications conducted within the VPN. But be sure to follow the other tips to protect your business.