

Hit the Road Jack: Secure Mobile Computing

By Sharon D. Nelson, Esq. and John W. Simek

© 2009 Sensei Enterprises, Inc.

It's been several years since we've dealt with remote access solutions. Wow, have things changed fast. Technology advances in this area have come at warp speed. Gone are the days when you carried around a fifty foot phone cord and kept looking for an analog phone jack that could be used with the modem in your laptop. Being über geeks, we then carried along a splitter, coupler and additional phone cords so that we could work comfortably on the bed or desk while we traveled around the nation. No more. It's even difficult to purchase a modern day laptop with a modem. Wireless is the word these days. More and more hotels, motels, conference centers, coffee shops, book stores, cafes etc. are offering wireless access solutions.

Software

Before we jump into the boring details, let's cover some solutions that should be on your laptop no matter what other technology you use for remote connectivity. It goes without saying that you should have some sort of anti-virus solution installed on your laptop. It should be configured for automatic updates and perform a periodic full scan (we do weekly scans) to catch anything that may have "landed" before the signatures were updated. It would be just your luck to catch a virus on day one and be the first kid on the block to suffer the effects. In addition, you should have anti-spyware software installed. Many of the anti-virus vendors also have anti-spyware capability. Normally the Internet Suite products will contain both as well as other security features like firewalls, spam control and anti-phishing.

Encryption

Secure mobile computing must contain some method of encryption to protect the valuable personal and client data. We prefer whole disk encryption. This means that everything on the hard drive is encrypted. We don't have to remember to put files into special folders or on the encrypted virtual drive. All too often, humans are in a big hurry and may not save the data in the special protected encrypted areas. Many of the newer laptops have built-in whole disk encryption. To state the obvious, make sure you enable the encryption or your data won't be protected. Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe to power on. Failure at that point leaves the computer hard drive fully encrypted. A very comforting thought if laptop thieves, who constitute a large club these days, make off with your laptop.

Wireless

What's next? We won't cover modem access in the traditional sense since dial-up isn't desirable or effective these days. Wireless is the rage of all the road warriors. There are two basic types of wireless access you'll encounter. The first type is generically termed a "wireless hot spot" and is what you find at your local Starbucks, Barnes and Noble, hotel or at the airport. You may or may

not have to pay for these wireless connection services. Many businesses are offering free wireless as a way to attract customers. Most of these “hot spots” are unsecured. This means that it is possible for your confidential data to be viewed by the customer at the next table or the one sitting on the park bench outside the café.

Does this mean you shouldn't use any of these wireless clouds? If you have a choice, we would say these clouds are best avoided by those who are technology-adverse and don't understand how to operate securely in an unsecured cloud. Read on, and determine whether you can safely be trusted to do what follows. Here are the precautions you should take. See if there is an option to have a secure connection to the cloud. This would be indicated if you use https:// as part of the URL. Typically, the connections are unsecured and do not provide an encrypted session like the https:// connections do. Be especially careful if you have to pay for the wireless connection. Be wary when you are at the screens that have you input your credit card and billing information. DO NOT enter any of this sensitive information without a https:// connection. Once you've established a connection to the wireless cloud, be sure to use your VPN (Virtual Private Network) or other secure (https://) access to protect your transmissions.

Some hotels may give you a wireless cloud that is already secured. Typically, these wireless implementations use WPA (Wi-Fi Protected Access) to secure the data. The cloud will be visible to your computer, but you will be required to provide a password before your computer connects. Once connected, your data is encrypted and secure.

AirCard

Another wireless connection method is commonly called an AirCard. These are cards that are used to connect to the high speed wireless networks of the cellular phone providers. The major technologies in use today are EV-DO and 3G. Don't be swayed by the vendor claims for speed and availability. Make sure that you will be able to have service in those areas you travel to the most. Reliability is another consideration as well as whether you already have a cellular plan.

The AirCard itself is a hardware device that you connect to your laptop. They come in USB or PC Card formats. Since they are an external device, they can be used on any laptop. Some newer laptops have the electrical circuitry built-in so no additional hardware is required. The built-in capability means you have nothing to lose, but it is “married” to the laptop and can't be transferred between machines. The external devices can cost several hundred dollars, but most providers offer significant discounts. As an example, Sprint currently offers a USB antenna for no cost after discounts and rebates.

The service itself can be monthly or daily. The monthly plans measure the amount of data you transfer over the connection and charge you for any overage usage. Typically, the data plans limit your usage to 5GB a month and will run about \$60 per month. Verizon offers a day pass, where you can get 24 hours of secure high speed connectivity for \$15 a day.

Obviously, you will want to purchase a monthly plan if you travel a lot or will use the service for more than 4 days a month. The AirCard is the preferred wireless connection since the data is secured from the very beginning. You do not have to worry about whether you have a https:// session or not. The electronic circuitry itself and the cellular carrier provide a fully encrypted session immediately.

Remote Access

We've dealt with some of the more common methods to provide secure communications. Now that you have the secure connection, what's next? E-mail access is pretty simple from most laptops, but what about working on client files? Larger firms will have an environment where you connect to virtual computers. We have a Microsoft Terminal Server environment, where multiple users connect to virtual machines. You connect and login just like you would while you're in the office. You would then have access to all your data just as if you were sitting in your desk chair. Citrix is another technology solution that provides the same function.

Smaller firms typically use something like GoToMyPC or LogMeIn. These products take control of a remote machine and pass keystroke, mouse movement and screen updates across the connection. This does require that the remote machine be powered on prior to you connecting. Be sure that you have a screen saver password set on the computer so nobody can sit at the keyboard at the office and access your computer. Cleaning crews are known to do this! These remote control solutions are very cost effective and all communications are over a secure encrypted connection.

Public Computer Usage

A word of warning here. Be very careful about using a public computer such as those in the library or business center of the hotel. Even if you are only accessing your web-based e-mail account, the data is temporarily written to the local hard disk. There is also the risk that some keystroke logging software is installed on the computer, thereby capturing everything that you do on the machine.

Does that mean all public computers are off limits? Not at all. We are big fans of the IronKey hardware encrypted USB flash drive. Besides the drive encryption and secure management of passwords, the IronKey has portable applications that are intended to be used with public computers. As an example, there is a specially modified version of the Firefox browser that doesn't write any data to the computer. All data stays on the IronKey, thereby making it secure and keeping it with you when you leave. Of course this does mean that the computer has to accept the insertion of USB devices. Some business center machines are locked down and do not allow USB devices to be inserted, because it is a security risk to the business – USB devices can be used to introduce malware to the machine or network.

Final Words

The options for secure remote access have certainly changed quickly over the years. Talk to us in four years and we're sure the world will have changed again. For now, make sure that you are aware of all the issues to securely transfer your data and that you are not relying on "antique" knowledge. You must assume that there is absolutely no protection of the communication stream between your laptop and your remote device. We've seen hotel networks that didn't have a firewall so all traffic was allowed to flow through. We immediately saw probing attacks on our computers, which were stopped by our firewalls on the laptops. It's the Wild, Wild West out there and you're the only marshal in town. Good luck Wyatt.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com