Hit the Road, Jack

Secure Mobile Computing

By Sharon D. Nelson and John W. Simek

It's been several years since we've dealt with remote access solutions. Wow, have things changed quickly. Technology advances in this area have come at warp speed. Gone are the days when you carried around a 50-foot phone cord and searched for an analog phone jack that could be used with the modem in your laptop. Being übergeeks, we then carried along a splitter, coupler, and additional phone cords so 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, cafés, and other public places 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.

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice and risk management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content.cfm or call our Helpline at (800) 341-9715 to speak with a practice management advisor.

—JoAnn Hathaway and Diane Ebersole, Practice Management Advisors

Encryption

Secure mobile computing must contain some method of encryption to protect valuable personal and client data. We prefer whole disk encryption, meaning everything on the hard drive is encrypted; you 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 data in protected encrypted areas. Many newer laptops have built-in whole disk encryption. To state the obvious, make sure you enable 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 & Noble, hotel, or 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 wireless hot spots, or "clouds," are unsecured. This means that it is possible for your confidential data to be viewed by the customer at the next table or someone 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 averse 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. Precautions you should take include determining if a secure connection to the cloud is an option, as indicated by a URL that begins with https://. Typical wireless connections (URLs that begin with http://) are unsecured and do not provide an encrypted session like the https:// connections. Be especially careful if you have to pay for a wireless connection. Be wary when you are at screens requiring you to input your credit card and billing information. *Do not* enter any of this sensitive information without an 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 cards are used to connect to the high-speed wireless networks of cellular phone providers. The major technologies in use today are EV-DO and 3G. Don't be swayed by vendor claims for speed and availability. Make sure you will have service in areas you travel to the most. Reliability is another consideration, as is whether you already have a cellular plan.

The AirCard itself is a hardware device you connect to your laptop. It is available in USB or PC card formats. Since they are external devices, the cards 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 the card 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, data plans limit your usage to 5 GB monthly and cost about $60 a month. Verizon offers a day pass, which allows you 24 hours of secure high-speed connectivity for $15 a day.

Obviously, you'll want to purchase a monthly plan if you travel often or use the service for more than four days a month. The AirCard is the preferred wireless connection since the data is secured from the very beginning. You don't have to worry about whether you have an 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 in which you connect to virtual computers. We have a Microsoft Terminal Server environment, in which multiple users connect to virtual machines. You connect and log in just as you would when you're in the office. You 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 before you connect. Be sure to set a screen saver password on your office computer so others can't access your files. These remote solutions are very cost-effective, and all communications take place over a secure encrypted connection.

Public Computer Usage

A word of warning here: Be very careful about using public computers, such as those in the library or business center of a 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 keystroke logging software is installed on the computer, thereby capturing everything that you do on the machine.

Does this 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 intended for use 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, 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 don't allow USB devices to be inserted because they can introduce malware to the machine or network, creating a security risk to the business.

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, be aware of all the issues for securely transferring your data and don't rely on "antique" knowledge. You must assume that the communication stream between your laptop and your remote device is not protected. We've seen hotel networks without a firewall, allowing all traffic to flow through. We immediately saw probing attacks on our computers, which were stopped by the firewalls on our laptops. It's the Wild, Wild West out there, and you're the only marshal in town. Good luck, Wyatt. ■

Sharon D. Nelson and John W. Simek are president and vice president, respectively, of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, Virginia. They can be reached at (703) 359-0700 or www.senseient.com.
