

Security on the Go

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

© 2006 Sensei Enterprises, Inc.

These days, we all seem to be in love with the extreme ease of information access. This access can be from our home computers, our laptops, our PDAs, our Smartphones or the public computer in the hotel lobby. Our confidential information can be stored on our laptop hard drives, our telephones or those cool (and easily lost) thumb drives. What is available to secure our communications and storage of information? Should we really worry overmuch about protecting our data? How can we continue to maintain mobility and still operate in a secure fashion? In a world where laptops are among the most frequently stolen items, and data theft is on the ramp, a little reassurance is in order. So we'll identify some obvious and some not-so-obvious things that you can do to protect your data and still sleep well at night.

Data Storage

Thumb drives, flash drives, jump drives, etc. are all names for small electronic storage devices that appear as another disk drive to a computer. We copy our client files to a thumb drive and take them home for the weekend so that we can continue to work on the case. We may keep our firm's financial data on a thumb drive as a backup. No matter what we store on these wonderful, small devices, it is subject to theft if we happen to lose the thumb drive. Some vendors provide a lanyard so that you can hang the device around your neck, but how many of us do that? More often than not, we attach it to our keys or just stick it in our pocket since it is hard to insert in a computer with our keys attached. The bottom line is that the data is stored on these portable devices in an easily accessible fashion. Pull out your wallet and accidentally have your thumb drive fall on the ground. Put your thumb drive on your desk and walk to the restroom to find that it has vanished upon your return. Leave it accidentally on your hotel room desk only to find it grew legs while you were out at dinner. Anybody that finds your lost thumb drive can connect it to a computer and read the contents...unless you encrypt. Don't bother to password protect your documents unless you intend on using strong (letters, numbers, and symbols) passwords. There are many password-cracking tools that will blow through any document passwords. Some vendors provide encryption software that have the ability to define a secure area of the drive for encrypted storage. The alternative is to use a third party software package to encrypt the thumb drive contents.

Laptops

The first thing that most people think about is securing their laptop. Laptops are the number one item lost or stolen at airports (and high on list of items stolen from hotels) so protection is imperative. The first defense is to configure a power-on password so no one can operate your computer from the outset without this password. This is a simple thing to do and is achieved by changing the setting in the BIOS (Basic Input/Output Setting). Don't think that you are totally safe just because you have set a power-on password. If someone really wants to gain access to your data and steals your laptop, they would just

remove the hard disk from the laptop, connect it to a special adapter and then connect it to another computer in order to read the drive contents. Some models of the Lenovo ThinkPads prevent this type of access by requiring that the hard disk be inserted in the ThinkPad, effectively “marrying” the hard drive to the actual laptop.

If you are in the market for a new laptop, consider buying one with biometric access. Just like restricting access to thumb drives, encrypt the contents of the hard disk. You can do complete drive encryption or just a portion of the drive. PGP Desktop Home 9.0 is \$99 and can create a virtual PGP encrypted disk. You merely mount the PGP disk, which shows up as another hard drive to your computer. Drag and drop files to the virtual disk and they are stored encrypted. Don’t forget to unmount the virtual disk when you are done. Encrypting the complete drive is a little more risky, especially if you forget your passphrase and can’t access the hard drive. If you encrypt the whole disk, make sure that you create an administrative override ID that can unlock the drive in an emergency.

Spyware

It is no longer an option merely to have anti-virus software installed on your computers. Obviously, you need the standard protection from viruses, worms, Trojans, etc., but spyware installations are growing by leaps and bounds and demand more particular attention. You’ll need to install anti-spyware along with your anti-virus installations so don’t flinch at the additional time and expense – the confidentiality of your client data is worth it! Ad-Aware and Spybot Search & Destroy are two of the most popular free anti-spyware packages. The main issue with the free packages is that there is no real-time protection or automated updates. You have to remember to manually update and scan your systems. Would we take that risk? Nope. We’ll fork over the cash gladly to remove the “idiot factor” (us) from the equation.

Two highly rated anti-spyware applications are Webroot’s (<http://www.webroot.com>) Spy Sweeper for \$30 and Sunbelt Software’s (<http://www.sunbelt-software.com>) CounterSpy for \$20. You should run at least two anti-spyware applications since no single package will catch everything. Purchasing one of the two previously mentioned packages and periodically running a manual scan with one of the free products is a good starting point. Since we have very little success convincing our own clients to run **two** anti-spyware programs, go ahead and start with one. Better something than nothing. Over time, the depth and breadth of this problem may persuade you to add a second line of defense.

Why do you need to worry about spyware? Normal Internet browsing activity exposes your computer to the installation of spyware that may be capturing your keystrokes, search terms or personal information and transmitting it to a third party without your knowledge. Not only do lawyers have to be concerned with the loss of their own personal data, but they have an ethical responsibility to safeguard their clients’ information. Remember the only “prudent man” standard? Have no doubt, the prudent man would attend to the threat of spyware!

Firewalls

Certainly you need to have a firewall for your communications connections to ensure privacy. The simplest and easiest for a home or office network is to install a router that does NAT (Network Address Translation). This means that there is one public IP address on the “outside” of the router that connects to the Internet and the internal network is translated into a private network. Typically, the internal network will be a 192.168.x.0 network. To further secure your network, change the default network address to something other than the factory setting. As an example, if the default network is 192.168.1.0 then change it to something like 192.168.198.0. This makes it a little harder for the potential hacker to discover.

Windows XP with Service Pack 2 contains a software firewall. Make sure that it is enabled. A firewall doesn't do you any good if it isn't operational. Doh. Trust us, there are a lot of “Homers” out there and you don't want to join the club. Also, consider replacing the Windows firewall with a third party software product like Symantec Personal Firewall or Zone Alarm. The Windows firewall does not monitor suspicious activity that originates from your own computer, whereas products like Zone Alarm monitor for activity that may indicate a compromise of your system. As an example, you may have spyware installed that has turned your computer into a zombie machine, capable of transmitting spam without your knowledge. The third party firewalls “watch” for symptoms such as this and either block or warn you of the activity.

Secure Connections

Everyone seems to get real excited about the prospect of free wireless Internet access while staying in a hotel or the wide-open wireless cloud at the local deli or coffee shop. Certainly, insecure wireless clouds make it very easy to connect to the Internet and begin work on your e-mail or client files. The problem? Yes, it's easy for you to work but it also easy for someone else to monitor your traffic since it is sent in clear text. So you love that free wireless cloud at all those legal conferences? Are you sure you are secure when you're working? We cannot tell you how easy it is for us monitor the actions of the others and secure their data, though we hasten to add that we have only done this for demonstration purposes.

The sheriff in town is the VPN (Virtual Private Network). The VPN encrypts the connection between your computer and the receiving machine. As a minimum, use a VPN connection when connected to public hotspots. As with other security measures, don't believe that no one can monitor your transmissions if you use a VPN. What if there is a keystroke logger installed on your computer that you don't know about? Here's one scary scenario of your laptop being compromised when you thought you were safe.

Prior to taking a business trip with your laptop, you allow your teenage son to use your laptop to surf the Internet from your home network. He installs a P2P (Peer-To-Peer) file sharing application to download music files. Unfortunately, the P2P software also installs a keystroke logger and Trojan horse. Your son had no idea that this was happening, but

that sure as heck doesn't change the result. Off you go on your trip to take depositions of the opposing witnesses. While away, you decide to check your e-mail at the local Starbucks. You are very aware of the insecurities at public hotspots. Not to worry...you fire up your VPN software and connect to the law firm's network. Thank God that you are using an encrypted communication connection. Sorry, but the keystroke logging software captures your user ID and password for invoking the VPN software and sends it to the bad guys. Once the information is transmitted, and they see that they have a juicy target (a lawyer's computer – wa-hoo!) they decide to monitor your connection and see all of your e-mail messages (with attachments too) and read your responses in real-time. The scent of malpractice, as well as Sumatra coffee, may be in the air.

Smartphones

With the recent worries over the BlackBerry network, more and more people are moving to alternate devices and also replacing their cell phones with convergent or Smartphones. Smartphones are cell phones that also have the ability to send and retrieve e-mail, run applications, process e-mail attachments, manage calendaring, contacts, etc. Besides the BlackBerry, popular models from Palm (Treo) and Samsung are being purchased by many lawyers wanting a full range of functions from a single device.

How do we secure the information on the Smartphone? As a minimum, configure a password should your phone be lost or stolen. In addition, set the phone to lock after a period of inactivity, thereby requiring a password. Many lawyers see this "lock out" or screen saver type of function to be an inconvenience and will not enable it. If you think entering a password to unlock your phone is inconvenient, try explaining to your largest client that you just lost your phone containing your latest deposition schedule, expert witness contact info, strategy meeting reminders and case notes. Also, consider getting some encryption software for your phone too. Smartphones may have alternate network communications ability too. The phone could be equipped with Bluetooth, WiFi and/or infrared abilities, all of which can be scanned and monitored. Disable the communications methods you don't need and only turn them on when you need to use them.

You can even remotely wipe data from a phone if you have Exchange 2003 with SP2 and a Windows Mobile 5 device with the Messaging & Security Feature Pack. How cool is that? The administrator can remotely issue a wipe command to a lost phone or it will automatically wipe after a certain number of invalid login attempts. This is a particularly cool advance in defeating the bad guys of the world. As cartoon villain Snidely Whiplash would say, "Curses! Foiled again!"

Wireless Networks

We've already touched on some of the issues with wireless connections and VPNs, but let's go into a little more depth about wireless networks. As a minimum, change all of the default settings. This includes the administrator access (ID and password), the network addressing and the network name. Don't broadcast the name (SSID) of the network

either. Consider configuring a MAC (Media Access Control) filter. This means that you enter the hardware addresses for only those devices you want to connect to the wireless cloud. It is easier to spoof the hardware address for a wireless device than a wired one, but it's better than nothing. The practical side is that a hacker will go to another cloud if there are even the slightest difficulties in getting connected. There's a lot of "low hanging fruit" out there. This is just exactly like having a big "Protected by ADT Security" sign in your front yard when the system belonged to a previous owner and you have no security at all. At the very first hint of trouble, hackers will go for the "wide open door" and leave you alone unless you are specifically their target.

Lock It!!

It still amazes us that more of our colleagues don't lose more of their equipment. It is fairly easy to physically secure your equipment in your office or home. You know where it is and people have limited access to the equipment. However, when you are mobile do you always know where or how secure your equipment is? Your laptop and telephone are the two major pieces of mobile equipment to protect. Normally, the phone is always surgically attached to your hip or ear. However, the laptop is another story. A large number of people just leave it in their room when they go out to breakfast, dinner or the workout room. This leaves the laptop totally unsecured and a tempting target for the cleaning crew. It is really inexpensive (less than \$50) for a security cable lock. Lock the laptop up when you leave and make sure you attach it to something secure in the room. We often use the mattress frame, as a for instance. Good hotels are not immune to thieves – and do you really want to take any chances.

The Bad New World

In years gone by, it was common to go outside on cold mornings and start the car so it could warm up. A recent report from Maryland says that those cars are now the cars most commonly stolen. We've always had credit card fraud and identity theft, but only recently has it gotten so bad that you can't turn on the TV without hearing another horror story. In sum, perils beset us on all sides. The smarter we get, the smarter the bad guys get. But in the end, we must do the very best that we can to ensure that our clients' data remain secure. It is possible for you to try your very best and fail, but as attorneys, we dare not fail to try.