Cybersecurity for Senior Lawyers

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

When we were asked to do this article for senior lawyers, our first question was: "Are they still practicing law?" The answer was that the majority of readers were likely retired but certainly not all. We were therefore asked to do a general cybersecurity piece where the advice would apply to those still practicing as well as to those who have retired but want to ensure their personal security.

We thought the best way to do this might be through short, plain English tips. Technology makes the "plain English" goal a bit challenging, but . . . away we go!

1. **Social engineering**. We can't tell you how many times senior lawyers have called us after getting a call from Microsoft Tech Support telling them that their machines were infected and sending reports of the infection to Microsoft. In any amazing number of cases, the lawyers (by the time they had called us) had allowed the folks on the phone access to their computers by following the instructions the callers gave. No reputable company will call you to tell you that you have an infection. It is a scam, pure and simple. Either they want you to pay money for "fixing" the computer or they want access to your computer to get personal data that they can use themselves or sell for identify theft. If the caller says they are from YOUR IT company, but they are asking for your password and ID, they not from your IT company. Don't be duped by this form of social engineering.

2. **Phishing**. These days, breaches are, 91% of the time, a result of a phishing e-mail. There are all kinds of phishing e-mails – those that go to anyone with a machine running operating systems or software with unpatched vulnerabilities or those that are targeted specifically to you (this is called spear phishing). Phishing e-mail can look diabolically real. However, most have something that should tip you off that there's something wrong. Perhaps the e-mail appears to come from a court or someone you know (it's very, very easy to spoof – or hack – someone's e-mail), but you weren't expecting it. There's nothing personal in the body of the text, but there is an attachment or

a link to click on. Chances are, once you click, you'll have downloaded malware that will allow access to your machine. Other clues? Poor English, the promise of a client or money, a sender's domain name that is just one letter (or sometimes a number replacing a letter) off from the real one – things like that. Most legitimate e-mails are obviously legitimate. But look at any e-mail with an attachment or a link to click on with an extra level of suspicion.

3. **Business e-mail compromises**. These are also known as CEO scams and the FBI reports that they have netted more than 3 billion dollars thus far. From January 2015-June 2016, there was an increase of 1500% in successful attacks. That's one heck of a statistic. Basically, someone who has authority to order money wired appears to be writing someone who actually does the wiring. Law firms have been hit hard by these scams, so it is critical that employees understand how they work and that they be conditioned to seek affirmation of any order to transfer significant monies. If you're lucky enough to be retired, this tip applies only to those still practicing.

4. **Back-up**. We're pretty sure most of you have heard of ransomware which encrypts your data and requires the payment of a ransom (normally in bitcoin) to give you the key to decrypt your data. The way you avoid this is to make sure that you always have one good backup that is not connected to your network. Many of you are backing up to an external hard drive, which is a fine solution, but unplug it when the backup is done. If you get hit with ransomware while that drive is connected, you're toast. Both your active data and your backup files will be encrypted. Have a third backup somewhere – the cloud is fine – to protect yourself. There are many fine choices but we particularly like Carbonite, which will allow you to hold the decryption key. And make sure you do periodic test restores from your backup just to make sure that everything is working as it is supposed to.

5. **Change the defaults**! Every 12-year old knows how to get online and get the default ID and password for almost any device. Many of you will have routers for your wireless networks at home. Make sure you change that default ID and password. We can't tell you how many people have found themselves facing a search warrant because their

network was being used to download child porn. Your neighbor can do that if you don't change the default ID and password.

6. **Encryption is your friend.** Your smartphones should be encrypted. If you have a PIN on your iPhone, that encrypts the data. It is better to have more than four (or 6 with the latest version of iOS) characters in your PIN. Turn off 'Simple Passcode' in order to enter more than the 4 or 6 digits. Why? Because there is software available that can brute force an iOS 4-digit PIN in several minutes. If you are running the Marshmallow or Nougat operating software on your Android, your data is automatically encrypted when you configure a lock code or swipe. If you are running Lollipop or earlier versions of the Android operating system, you simply have to check a box. Very easy to Google the location by simply asking how to encrypt a particular Android operating system.

7. **Your wireless network.** It must be encrypted with WPA2 encryption. WEP and WPA were cracked years ago. So make sure your home router is running WPA2. If it is too old to support WPA2, buy a new one – they are not very expensive. And if you on the road and using a wireless network, make darn sure, when you look at available wireless networks, that the one you choose is protected by WPA2. Many smartphone users will connect to wireless networks in order to avoid the data charges associated with accessing the 3G/4G data network of the cellular provider. Using wireless networks is not a problem, but make sure you are connecting to a secure wireless network.

8. **Security Suites –** Long gone are the days when an anti-virus program was enough. Now you need a security suite that protects you from all kinds of malware, spam and phishing e-mails. Any of the major products are fine. We are keen on Trend Micro and Kaspersky.

9. **Install patches promptly.** Yes, patches can be annoyingly long, especially when you want to get out the door. But there is a reason that manufacturers release them – they fix vulnerabilities in software which can be exploited by hackers. Failure to patch promptly is one of the major reasons people get breached. For operating system and browser patches, in particular, you may want to automate the patching process so you take your human frailties out of the equation.

10. **Passwords.** Don't use the same password over and over. If you're compromised in one place, you'll be compromised everywhere. The rules of passwords have changed recently. It is now widely agreed that length outweighs complexity, so make your passwords 14 characters or more, but make a passphrase that you can easily remember, something like "Ilovebeingaserniorlawyer!". If 2-factor authentication (2FA) is available, make sure you use it, especially for confidential data.

11. **Password managers.** Can't remember all your passwords? Neither can anyone else, senior moments or no senior moments. Any of the major password managers are fine, but we'll recommend eWallet for Senior Lawyers for three good reasons: it is cheap, it can be shared across multiple devices, and you can put in all sorts of things that aren't passwords, including all your medicines, your doctor contact info, your air and hotel rewards info, your passport number, your AARP number – and almost anything else you'd want to have with you on your smartphone. Darn handy.

12. **Software that is out of support**. Just don't use it. Ever. Out of support means it isn't receiving security updates. There are still a lot of lawyers using Microsoft XP – and yes, it still works. But it is unsupported, with well-known vulnerabilities that bad guys exploit. Besides Microsoft XP, Server 2003 and Office 2003 are now out of support as well as Internet Explorer 10 and earlier. Office 2007 and Exchange 2007 both go out of support in 2017, meaning that you must plan an upgrade if you are using the. Many hacks occur through outdated Adobe software, including Adobe Acrobat and Reader. If you downloaded this products a long while ago and haven't updated them, you may well have versions 8, 9 and 10 (all out of support). For planning purposes, Adobe Acrobat and Reader XI will go out of support in 2017. Using unsupported software is another very preventable cause of data breaches.

13. **Lost and Stolen Devices**. Make sure they are encrypted to protect the data. But also make sure you can remotely wipe the devices. A laptop is lost or stolen every 53 seconds in the U.S. and over two million cell phones are stolen each year as well. Assume the worst and protect yourself. On an iPhone, users would enable the 'Find My iPhone'

feature through iCloud. The ability to locate your smartphone must be turned on before you lose your phone, something many lawyers seem unaware of. Android users can install the free Lookout application, which has device location capabilities. Location services are included in the latest version of the Android OS so no add-on product is required.

14. **Cloud computing**. Most senior lawyers tend to use Gmail or another cloud-based e-mail system. We often find that lawyers are using cloud computing without knowing it. If the data isn't stored on your system, you are using the cloud. Clouds are not fail proof, but any reputable provider will undoubtedly protect your data better than you will. As previously mentioned, make sure you enable two-factor authentication for your cloud services.

15. **File synching software**. Many senior lawyers use Dropbox, which seems have laid claim to the beachhead. But realize that Dropbox holds the decryption key – not you. So don't put anything sensitive in Dropbox unless you encrypt it first using a third party product such as Boxcryptor, Viivo, Sookasa, etc..

16. **Public computers**. If you are in a hotel business center, a public library or an Internet café, it's fine to check last night's game score, but don't do any legal work or access any of your financial data online. Studies have shown that these public computers have an average of seven pieces of malware on them – at least a couple are sure to be keystroke loggers which can record everything you type. Don't print your airline boarding pass either since you'll have to logon to your account, meaning the bad guys can "steal" your miles.

17. **Social Media.** Be careful out there. Don't post client information – or your own personal information. Social media posts tend to live forever so think before you post.

Our list of tips is endless, but if you follow the advice above, you'll go a long way toward keeping your data safe!

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