Top 10 Tips: Effective Cybersecurity Awareness Training for Law Firm Employees
by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

We can speak authoritatively about cybersecurity awareness for law firm employees because we give this training so often. Here are some of our tips to ensure you maximize the effectiveness of your training.

1. **Take cybersecurity awareness training seriously and do it right.**

A significant recent statistic is that human beings are involved in the success of 82% of cyber attacks. They tend to have crummy passwords, they reuse and share passwords, they click on links or attachments without thinking, they get emails which seem improbable and yet respond to them, and the list goes on and on.

We used to say that you should do training once a year but as things are moving faster and faster, we think it's better to do it twice a year.

Employees need reiterative training. They simply forget what they were taught. Also, the threats and the defenses keep changing, so it really is hard to keep up. We would advise not to be tempted to use in-house IT to do the training for budget reasons. They're not training professionals and they don't carry the big bat needed to hit the lessons home. If you're going to hire some to train, which is what most people now do, get some referrals from your friends.

Effective presenters have to be good entertainers as well as good teachers. Our own one-hour training sessions are either $500 or $1,000 depending on the customization involved. Small law firms can afford that. We recommend training be limited to one hour because after that, the attendees do tend to go numb. You can do a lot in an hour!

Training is definitely better live but it is not likely the predominant way of the future. Most law firms are now having virtual training and we see that continuing for the most part. Make sure you track the attendance and ask those who are giving the training to give you a recording to use later in case some employees can't make it which always seems to happen.

2. Train employees on phishing tactics and ransomware.

In the early days, ransomware was just a way to encrypt your data and then hold you hostage until you paid a ransom in order to procure the decryption key and regain access to your information.

Now we have what the authors call ransomware version 2.0. That's not an official industry term but the evolution of ransomware has become much more targeted. The tactics have changed because cybercriminals have realized that a lot of law firms have improved their backup mechanisms so they didn't have to pay the ransoms anymore. They were just restoring from their backups and that dried up the money well. They figured out a new tactic: Now they access your network and steal the data before they encrypt it. So, if you decline to pay the ransom for the decryption key, the criminals point out that they have exfiltrated your data – now there's another reason to pay a ransom before they expose or sell that data. You now have a bigger headache too as the exfiltration of your data means you have to report the event as a data breach.

Law firms have a big bullseye on their backs. They are one-stop shops for the data of many clients. The data you have is valuable and you are ethically required to protect it. Training must go into some depth about

ransomware and phishing to drive the message home to employees – it's all about creating a culture of cybersecurity.

77% of current ransomware attacks now include the threat to leak stolen data. Phishing is most often the entry point used by criminals to insert ransomware.

The recommendation for training twice a year is because the phishing techniques change, including how they trick the users to engage in clicking or opening things they shouldn't. 57% of the respondents in a Proofpoint survey experienced some sort of successful phishing attack. 67% of the users didn't even know what ransomware was or they gave an incorrect response, which is deadly. If you don't understand your enemy, you won't understand how to defeat that enemy.

We show employees a dozen or so phishing examples in the training so that they can look at it and say, "Yeah, I got something like that once and I didn't click it," or they groan and say, "Yeah, I clicked on it."

3. Teach your employees to take their hands off the keyboard before hitting 'Send'.

It's a simple matter to take your hands off the keyboard before you sit 'send'. Most lawyers acknowledge that they move too fast when they are working. We think we're multitasking and we're more efficient because we're doing that, but the experts tell us that isn't true. What we are doing is shooting short bursts of attention here and then there, which makes us much more likely to make an error. When we ask audiences who has ever sent an email to the wrong person or sent the wrong attachment or forgotten the attachment entirely, almost every hand in the room goes up.

If they take their hands off the keyboard and review who the email is going to, that's the first step. Auto complete is not your friend. Important communications are often misdirected. If there is an attachment, make sure that the attachment to the email is the correct attachment. Even more fundamental, make sure you remember to attach the attachment!

4. Train your employees about the dangers of Business Email Compromises (BEC).

Ransomware is the #1 enemy, but BEC is number two – and it nets more money. In BEC attacks, the cybercriminal is trying to get the victim to wire money, send employees' W-2 information or procure gift cards, etc. Huge sums of money have been wired to the wrong place because of BEC attacks.

If your email account is compromised and someone has full access to your content, now they've got all the information about your contacts and they've got all your emails. They know what vendors you've been working with. They know who your clients are and what cases you're working on. Teach employees to be hyper vigilant about wire transfers – and to confirm any changes in instructions by calling a known good number for the person the email purports to come from. This can save a world of angst.

5. Teach employees about social engineering.

Social engineering can take many forms. Examples are great and drive the point home. For instance, there is phishing by phone, sometimes known as vishing with a V because it is voice phishing. The bad actors are generally trying to get information. They're going to ask who pays the bills or wires its funds on behalf of a law firm. You'd be surprised how many people answer those questions. They may ask who the managing partner is or the CEO or CFO, looking for anyone who gives authorization for payments or wiring funds. Those are the

people they want to pretend to be through compromising or spoofing their email - even by using deep fake audio. There are an increasing number of those cases.

They might even call to ask who your IT managed service provider is because then they can call pretending to be that provider. They will perhaps research some names there, perhaps through LinkedIn, which is a big help to the bad guys, however inadvertently. Your employees are much more likely to give their law firm credentials to someone pretending to be from your IT provider perhaps pretending to be in the middle of fending off an attack and needing an employee's ID and password right away. Giving your employees real-life examples and teaching them to be suspicious is a good thing for the security of your data.

6. Pay attention to work-from-home security.

Many law firm employees are working partly from home. They use consumer grade equipment and they're not up to date with patches on their home machines. They're using consumer-grade routers. Surveys show that only 35% of users change the default router password on their home networks. Cyber criminals know this and exploit the vulnerabilities. They know that people are using RDP (Remote Desktop Protocol) for remote access. They're also using VPNs (Virtual Private Networks). Those are what they attack. Train employees on how to secure themselves at home – better yet, give them a work-issued laptop and make that laptop part of your firm's network security.

Make sure those working from home apply patches quickly. Cybercriminals watch for notices of newly discovered vulnerabilities. They know that employees don't tend to patch promptly.

Don't allow any of your family members to use any equipment that you use to access client data. If you have a law firm-issued laptop, that's certainly the best approach. Hopefully, the security of that laptop is managed by the law firm.

7. Stop sharing and reusing credentials!

Sharing your law firm ID and password is just plain stupid, but more than 50% of people do it. Often, partners share their credentials with paralegals or secretaries who monitor emails. There seems to be a million reasons why people share their credentials but none of them make any darn sense. Sharing credentials creates an enormous security threat.

Reusing passwords is as incredibly common as it is incredibly stupid. Once a bad guy/gal has your password from one place, the databases of known compromised passwords makes it easy for the cyber criminals to try that password in as many places as they want. We always stress that the law firm ID and password should be regarded as particularly sacred and never be reused anywhere.

8. Stress the urgency of using two-factor authentication.

You've probably heard the term two-factor authentication or 2FA, sometimes referred to as multi-factor authentication (MFA). More and more vendors are forcing you to turn on MFA. Our message is always to configure MFA. Use MFA everywhere that it's available. Studies have shown that having multi-factor authentication enabled will stop 99.9% of credential-based account takeovers. Microsoft's own studies have proven that. Microsoft believes that MFA is so important that it's now included free with all their subscriptions. You don't have to pay for it, but it's not turned on and configured. Some employees don't like the inconvenience of 2FA, but in today's world, they have to be persuaded to get over it. Security comes first.

9. **Teach employees about drive-by infections, baiting, piggybacking, and tailgating.**

Drive-by infections are where you visit a website that automatically downloads malware invisibly while you are on the site. The lesson there for employees is not to go to places you don't know. Name brands are much more reliable. They don't have that stuff on their sites.

Talk about baiting where flash drives are left on airplanes, public park benches or conferences. The employee picks up a flash drive, curious about what's on it or maybe wanting to return it to its owner and bada bing - they inadvertently download a malicious payload when they stick the drive in a law firm laptop.

Physical security is important. Piggybacking is when someone strikes up a conversation with you as you enter the building or office with a ProxCard key, keypad or whatever form of entry you use. They seem to have authority to be with you so they get in. Related is tailgating, where someone, as an example, pretends to be talking on their phone until you have opened the door successfully and then they pretend to hang up their call and they grab the open door. Not liking confrontation, we tend to let them in with us. Teach employees to be suspicious!

10. Teach employees current about alluring cyber attacks, particularly those that involve phishing.

Cyber criminals are clever – they know what will attract people. A subject line may talk about vaccines, expiring passwords, changes in vacation policies, and all manner of other things that folks are likely to click on.

Many emails reference shared files with links in the email (and they may pretend to come from another law firm or a client). Spoofing emails is simple – and of course email accounts also get compromised so bad guys may have in-depth info to use when they "bait the hook" when they go phishing.

Who won't click on a link in a message purported to be about a delivery, whether Amazon, UPS, or FedEx? One of the surveys we saw indicated that in Q4 of 2020, the five most successful subject lines were "password check required immediately", "touch base on meeting next week", "vacation policy update", "remote work policy update" and "dress code changes." They do their best to entice, so you have to call employees' attention to what works – so it will stop working!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*.