

Cybersecurity Awareness Training for Law Firm Employees Has Never Been More Critical

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

Introduction and stats

One of the most overlooked aspects of cybersecurity is training for employees. Employees are involved in more than 80% of successful attacks. It has never been more critical for law firms to implement effective risk mitigation strategies, enhancing their security posture and protecting their confidential data – which is impossible to do without educating your employees.

This is very important training in a hybrid work-from-home world and may even be required by your cyberinsurance carrier. A one-hour presentation includes recommendations for safe-computing behavior, education on spam, phishing, targeted malware attacks, and what users can do to protect themselves and their law firm – and abide by their ethical duties. And there should always be some good stories along the way to make the lessons stick.

Who should do the training?

Certainly not law firm owners. Even if they think they know something about cybersecurity. The biggest hammer is a consulting firm that clearly knows what they are talking about and can easily answer questions. They bring credibility with them because of their credentials.

If you are an Am Law 200 firm, you are likely going to hire one of the big guns with a hefty price tag. But if you are a smaller firm, there are plenty of smaller companies who do cybersecurity training. You want a company that has something of a specialty in training. Hopefully, they have sample current real-world phishing emails and tests they can give your employees to demonstrate that they are aware of security risks. If an employee repeatedly fails such tests, is that really an employee you want handling sensitive data?

Online training has been the choice of law firms since COVID. We haven't been asked to do anything but remote training for years. The good news is that it is cheaper – as an example, our training is \$500 for a one-hour session. For something so valuable to your law firm, that's an easy pill to swallow. The clear downside is that those who are viewing remotely may not pay full attention. Some firms make it mandatory to be physically present in a firm conference room which alleviates that problem.

Cyberinsurance carriers now ask if you provide annual cybersecurity training for your employees.

Training Tips

Make sure your trainers can talk about and show sample phishing emails and tests. Time of day? Best done in the morning, when folks are most alert. Spring for breakfast and keep the coffee coming. Cybersecurity can be mind-numbing if not done right.

Make it mandatory? Absolutely. Take attendance.

Be a Tattle Tale

This is the essential message of training. If you know that another employee is engaging in insecure behavior, you should inform a supervisor. “See something? Say something” is the mantra!

Don't be mad at your employer!

Employees dislike many aspects of information security. A good trainer will have your back on this one. They will explain why your security policies are needed and why they must be enforced. They'll talk about how the firm may protect its data through application whitelisting, logging of certain events, installing software or hardware that “reports” when certain files (or a certain large number of files) are accessed.

Trainers explain the importance of strong passwords – and what constitutes strong passwords is changing. The National Institute of Standard and Technology (NIST) has finally recommended that we change our notion of “strong passwords”. Trust us – you are in for a big change by the end of 2024 or the beginning of 2025. The rules keep changing, don't they? But that too is why you train on a regular basis.

And trainers will preach the value of encrypted password managers – darn near a necessity if you are going to follow the cardinal rule of not reusing passwords everywhere which often leads to one breach compromising your security, and that of the law firm, in many places rather than just one.

Social engineering

People who are experts at penetrating businesses through social engineering say it generally takes them less than an hour to get into your network. As humans, we are so anxious to be helpful. Your employees need to know that Microsoft Tech Support will never call and ask for access to their machine (yes, we've seen lawyers duped). They also need to understand that someone who calls and says they are from your IT company and need log-in credentials to fix a problem may not really be from your IT company, even if they know the company name.

Phishing

As we said before, phishing is the easiest way into law firms. Even good defensive software doesn't catch everything – and there are plenty of zero-day (no known defense) exploits sold on the Dark Web every day.

The worst threat comes from targeted phishing attacks, where the hackers are specifically targeting your law firm. Law firms are at a disadvantage here – so much legal data is public. An attacker may know what cases you are involved with, who the attorneys are, which courts cases are in, etc. And they can spoof the email address of an attorney or a court – how many lawyers can resist opening something that appears to come from a court?

Law firms are also at a disadvantage because they are “honey pots” – they hold the data of so many clients. Hackers may do a little research on the firm’s website or on an attorney’s LinkedIn page where they may find personal information that they can insert into a targeting phishing email or text. Trainers will get them to PAUSE, THINK, INSPECT and REPORT before clicking on any suspicious attachment or links in an email or text.

There are obvious phishing clues to pass on to employees:

- You don’t know the sender
- You do know the sender but if you look closely, the address is one letter off (this one happens a lot)
- Nothing in the note seems personal to you
- You weren’t expecting the email
- Reference is made to a bank/product/service you don’t use
- Words are misspelled
- The grammar is poor
- The email/text doesn’t address you by name
- The message asks for personal information
- There is an attachment which seems suspicious in conjunction with other factors or a link to a website (and no, hovering over the link doesn’t necessarily ensure that you will go to the address shown – drive-by malware infections from visiting malicious sites are quite common)

These days, trainers have to talk about artificial intelligence and how good it is at making phishing emails that succeed, in part because there are no misspellings, poor grammar, etc. As though we needed another challenge!!!

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 (CISSP), Certified Ethical Hacker (CEH) 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 Chief Executive Officer at Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity and digital forensics and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.