Lawyers Take Note! Microsoft Offers Current Advice on Cybersecurity

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

As October ends, it's a great time for lawyers to spend a few moments reflecting on tips and lessons learned during the annual Cybersecurity Awareness Month. There have been vast changes in the cybersecurity realm over the past year, including the dominance of Artificial Intelligence (AI) and its effect on cybersecurity, both the good and bad, and the persistence of phishing attacks. With each passing day, month, and year, cybersecurity challenges continue to grow for lawyers.

Microsoft has released its rundown on the year in review, offering simplified advice and cybersecurity steps to help protect your data and systems. Lawyers love it when complex technical jargon is broken down into easy-to-understand concepts with steps to implement, especially when the information is free.

Use Strong Passwords and a Password Manager

Microsoft now recommends that passwords never expire. Yes, you read that correctly. You can increase your firm's Secure Score (a percentage value of your Microsoft 365 environment security settings compared to firms of similar size and industry) by setting up your users with passwords that do not expire.

That seems contradictory to the last twenty years of password policies. By using a complex password of 14 characters or more, in coordination with a password manager, users no longer must change their passwords every 30, 60, or 90 days – in many cases, users by habit will just increase the number at the end of the password or write the password down on paper (or keep it in a Word file) if too complex. Users should be using a password manager, so they don't have to remember strong, complex passwords – let the software do it for you! This also can eliminate password reuse between different accounts – another big cybersecurity *no-no*. There are many different password managers out there, including the Microsoft Authenticator app – which you probably are already using for MFA (and it's free).

Here is a gentle reminder for all lawyers. Do not save your passwords within your browser. It doesn't matter which browser you use, Chrome, Firefox, Edge, or Safari, do not do it. Close out of the prompt or select the Never option when the browser prompts you. If your computer were to be compromised, attackers would have quick access to all the keys to your firm's kingdom.

Turn on Multifactor Authentication

There's not much to expand on here and we are well beyond the complaining about the "inconvenience to users" phase of this foundation for a strong cybersecurity posture. If MFA is offered by your service provider, which it probably is these days, turn it on. Only MFA can

prevent up to 99.99% of business account takeover attacks and keep the attackers out of your mailbox and bank accounts.

Learn to Recognize and Report Phishing

Phishing attacks remain the number one concern of IT and cybersecurity departments and continue to cause long, sleepless nights for firm management. The primary way for users to get better at detecting a phishing email and not falling victim to it is through training. Mandatory cybersecurity awareness training with phishing simulations is the best way to educate your users and increase their ability to detect. When a user doesn't pass the simulation test, they can be presented with short, educational videos to help reinforce detection concepts.

Training, in coordination with a strong email protection solution, can help keep those persistent phishing attempts out of your inbox. Phishing emails are getting harder and harder to recognize with the use of AI to generate the content for them. And yes, users should never provide credentials when clicking on a link from an unrecognized sender, let alone enter their MFA code. Instead, users should report the phishing attempt to IT support, and shift-delete the email out of the mailbox.

Keep your Software Updated

Vulnerabilities should never be overlooked or forgotten. Zero-day exploits and critical security patches and updates to fix them are released frequently throughout the year, by most vendors. Keeping your systems and software updated continues to remain a priority in a good, well-established cybersecurity plan.

Taking users out of the equation is the best course of action. Automating both operating system updates and third-party software updates is key to patches being applied rather than put off by users – a common reaction to the pesky Windows prompts that updates are ready to be installed and the computer restarted. If your firm is using Microsoft Intune for device management, you can create a policy to apply to your devices to automate this process at no added cost.

If your firm is working with a managed IT services provider, ask them about automating the process for you, since they probably have Remote Monitoring and Management (RMM) software installed on your endpoints. For mobile devices, users should download and install the updates when they're prompted.

See, that wasn't too bad. These four simple steps can be quickly implemented by lawyers at no or little additional cost. One day firm management may be able to sleep well at night, but not anytime soon. Especially if you haven't started to take the most basic cybersecurity steps to protect your accounts and client data.

Michael C. Maschke *is the President and Chief Executive Officer of 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.*

Sharon D. Nelson *is the co-founder of and consultant to 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 the co-founder of and consultant to Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), a Certified Ethical Hacker (CEH), and a nationally known digital forensics expert. He is a co-author of 18 books published by the ABA. jsimek@senseient.com*