Cybersecurity Statistics in 2024

Is Your Law Firm Protected?

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

2024 State of the Phish

Maybe it's a quirky name, but we sure enjoy perusing this report from Proofpoint every year. The foundation of the report is a survey of 7,500 end users and 1,050 security professionals. This year's report indicates that 71% of users confessed they had taken a risky action, reusing or sharing a password, clicking on links from senders they didn't know or giving log-in credentials to someone they didn't know. 96% of them knew they were taking a risk. If this doesn't convince you that your employees need cybersecurity awareness training at least annually, we don't know what will!

Over 1 million attacks are launched with MFA (multifactor authentication) bypass framework Evil Proxy every month, but 89% of security professionals believe MFA offers total protection against account takeovers. Our own view is that, while MFA is not a complete solution, it is far better than NOT having MFA – and the more secure your MFA is, the better.

69% of organizations were infected by ransomware. It remains a plague. Any dimwit can buy a Ransomware-as-a-Service toolkit for around $35 and wreak havoc.

Lessons Learned from the State of the Phish

One of the most valuable lessons is that with most cybersecurity awareness trainings (and thankfully, 99% of respondents said they had such training), less than a third of their training programs covered all "the big three" – remote work, password hygiene and internet safety.

The top training topics were malware, Wi-Fi security, ransomware and email phishing – which are all important, but they don't cover the full range of risks. Where was phishing using SMS texts? Where was the use of deepfake audio and video? Where was the social engineering of employees?

Only 34% of respondents performed simulated phishing attacks, which surprised us. Simulating phishing attacks are very helpful, not only in educating employees, but in pinpointing the employees whose behavior is most risky.

The New Threat Landscape

Unsurprisingly, many of the attacks were phishing, business email compromise (BEC) and ransomware. All are a continuing problem, no doubt of that.

But we have growing threats to address. One is telephone-oriented attack delivery (TOAD) where a message appears benign, containing only a phone number and some erroneous information. When the victim calls the listed number for help, the attack chain is activated.

Rest assured that cybercriminal call centers operate around the world, persuading victims to grant them remote access, reveal sensitive information and credentials, or even infecting their organizations with malware. Proofpoint's data shows that an average of 10 million TOAD messages are sent each month.

Increasing attacks used advanced techniques to bypass multifactor authentication (MFA). How do they work? They use proxy servers to intercept MFA tokens, which allows attacks to evade the security provided by one-time codes and biometrics. This is a huge problem because 89% of cybersecurity professionals still think of MFA as a "silver bullet" in preventing account takeovers.

Finally, there has been an increase in the use of QR codes (for the record, we have preached for years that you never really know where you're going if you click on a QR code). We think it's getting worse in part because so many people click on QR codes all the time. They simply do not see the danger. Clicking on a QR code may lead to a phishing site or a malware download.

AI is Now Part of the Threat

Artificial Intelligence (AI) facilitates cyber-attacks. To begin with, you are less likely to see all the spelling errors and misuse of grammar. Are all the AIs transparent about what happens to the data you input? Often they are not.

There is now a link between BEC attacks and AI, as attackers use AI to create more convincing and personalized emails in many languages. Proofpoint's data shows an average of 66 million targeted BEC attacks every month.

Any More Bad News?

Sure! While Microsoft is the most abused product in malicious email, other companies with the same problem include Adobe, DHL, Google, AOL, DocuSign and Amazon. We have been particularly plagued by phishing emails purporting to come from DocuSign and Amazon.

And our old "friend" ransomware is still a major issue – 69% of businesses (up 5% over last year) faced a ransomware attack. Of those who had a ransomware attack, 96% now have cyberinsurance, which certainly suggests that cyberinsurance is a necessity for all businesses, including law firms.

Final Words

From the venerable cybersecurity expert Brian Krebs: "*If you didn't go looking for it, don't install it*." – an excellent rule of safety.

Sharon D. Nelson *is an 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*.*