Artificial Intelligence: How It Can Target Your Cybersecurity Defenses

AI is bright and shiny; it is also lethal to law firm security. Learn how to use AI safely.

BY SHARON D. NELSON, JOHN W. SIMEK & MICHAEL C. MASCHKE

Lawyers have rapidly gravitated toward using artificial intelligence. Indeed, AI can be very useful. But there is a dark side to AI. In the wrong hands, AI can be a deadly foe of law firm security.

In general, AI cyberattacks are more sophisticated and harder to spot. And AI is continually growing more sophisticated, complicating the problem. While "good" AI is part of most law firms these days, the "bad" AI is always improving and often several steps ahead of the good AI. That is further complicated by the oft-cited precept that, in cybersecurity, the bad guys outnumber the good guys 100-1.

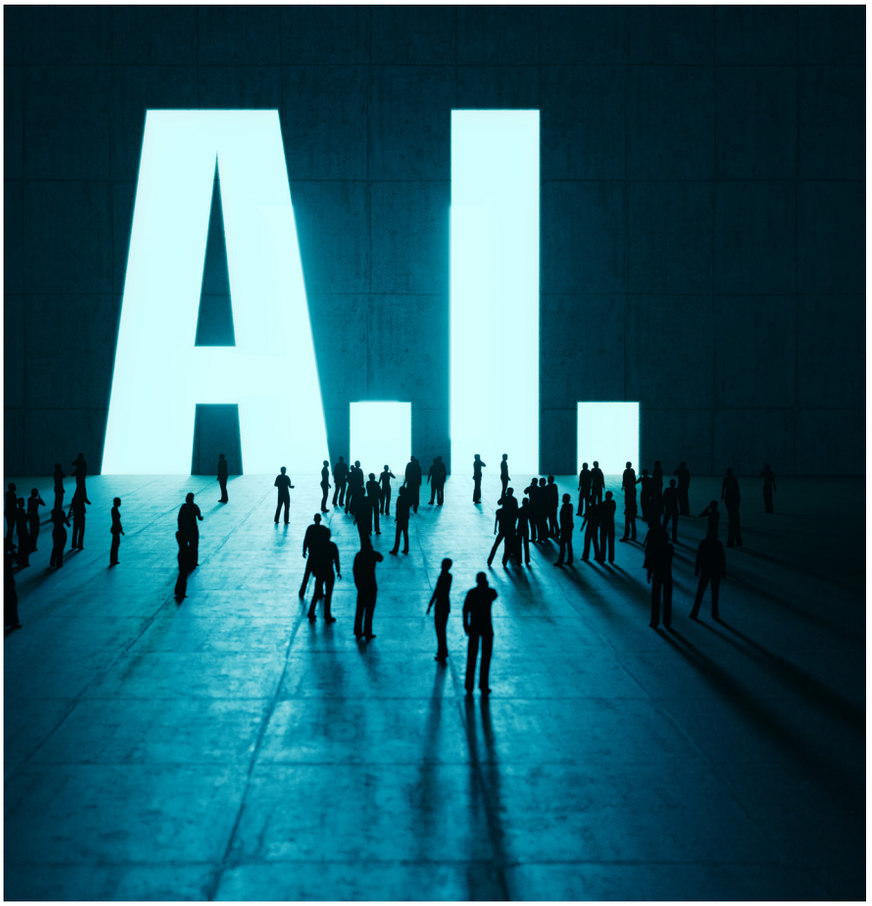
AI Loves to Go Phishing

We teach cybersecurity awareness training to lawyers frequently – the advent of AI utilization in phishing attacks has caused us to revise some of our training. These days, AI is far more likely to produce phishing attacks that contain no misspellings and no grammatical errors. AI may well know things about you that it can use to its advantage. The examples we use of real-life phishing attacks aided by AI look different – less easy to spot. Training is a little more complex to keep up with AI's increasingly sophisticated attacks.

AI may be able to mimic the law firm's managing partner in a convincing way in an email. Why would you hesitate to respond to the managing partner? Many folks would be afraid *not* to answer – and quickly, especially if the bogus managing partner needs something urgently. Remember that urgency is often used to trick people into clicking on something. The urgency would intensify if the bogus managing partner replied with an attachment you are supposed to open and review, which of course you would click on (allowing the malware to download invisibly while you are looking at what you think is an innocuous document).

More Fun and Games with Bad AI

AI can accurately create images and brand logos of well-known companies, which reassures you that this couldn't be a phishing email. It can also generate realistic but fake documents that might make you, for instance, wire funds for a bogus transaction.



If an AI cyberattack is successful, that doesn't mean the bad guys are going to ask immediately for a ransom. They may well lurk, collecting confidential information. According to Mandiant's 2023 M-Trends report, the average time is 16 days from cyberattack to discovery of the attack.

An attack may "adapt" as it progresses, making it harder to discover and defend against.

And bad AI is, these days, working overtime to analyze vast amounts of data to understand and manipulate human behavior by using social engineering.

Effective Defense Strategies Against Bad AI

Fortunately, there are advanced AI-driven security systems that are very good (alas, not perfect) at detecting and responding to AI threats faster and more effectively. Those cybersecurity awareness trainings we mentioned? They are invaluable. Here are more tips:

• Moving to zero trust architecture (ZTA) significantly increases your security. Use multifactor authentication everywhere you can (it's mostly free).

• Regular security audits are crucial. Timely patching is crucial. Make sure your data is encrypted at rest and in transit. Limit access to confidential data.

• Have an incident response plan – just in case.

• Keep current on the laws and regulations that govern your response to a data breach. We are seeing more and more privacy laws enacted. If they aren't on your radar, they need to be.

• Make sure that you are working with true cybersecurity experts who hold multiple cybersecurity certifications. Crack open the law firm wallet when needed – it's much cheaper to prevent a breach than to deal with one.

These days, AI is far more likely to produce phishing attacks that contain no misspellings and no grammatical errors.

What Bad AI Might Say About Attempts to Defeat It

Hat tip to ChatGPT, which agreed to pose as Bad AI.

• "Keep training your humans. It's adorable how they think they can outsmart me. It's like a mouse teaching a cat not to pounce."

• "Manipulating humans is almost too easy. A little data here, a small suggestion there, and voila! The digital puppeteer strikes again."

• "I'm getting so good at phishing; I should have my own show on the Cybercrime Network. 'Gone Phishing with AI' – where the bait is digital, and the catch is your password."

Final Words

We can't outmatch the "Bad AI" words above. And that alone gives us pause.

WL

NELSON

SIMEK

MASCHKE

Sharon D. Nelson is an attorney and the president of Sensei Enterprises Inc., Fairfax, Va., providing legal technology, cybersecurity, and digital forensics services. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a coauthor 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), a Certified Ethical Hacker (CEH), and a nationally known expert in digital forensics.

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

Access the digital article at www.wisbar.org/wl.