Law Firms Gear Up to Battle Deepfakes

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

The Rise of Deepfakes

While lawyers have certainly been aware of deepfakes for years, everyone was fighting malware infections. As we constantly remind lawyers, the cybersecurity world evolves rapidly – and the prudent law firm will evolve as well.

In the past year, deepfakes have become the second most common cybersecurity incident, lagging only behind those persistent malware infections that law firms have been battling for years.

Mind you, we are not suggesting (yet) that law firms are being deluged by deepfakes. However, having watched the rise of deepfakes in businesses, law firms know darn well that they will be invited to the party by cybercriminals – and that they must be prepared.

Cybersecurity Awareness Training

Over the years, we have given hundreds of CLEs on cybersecurity training for law firms, but for the first time, we are now including training to protect law firms against deepfakes, which may well involve such things as client voice cloning along with other forms of deepfakes.

It only takes a matter of seconds to clone a client's voice from a sample of the voice. While there are many permutations of deepfakes, a common scenario for a law firm might be a call requesting a lawyer to wire a large sum of money as part of a business transaction. It is amazing how much information cybercriminals have at their command to make such requests plausible.

Law firms hold some of the most sensitive data of their clients, and yet they are unprepared to adequate protect that data. Deepfakes may prove a considerable challenge to law firms if they don't institute adequate training.

How Can You Defend Against Deepfakes?

While each deepfake scenario may be different, there are means to defend again deepfakes! Nothing expensive or complicated about this, but why not set a secret code word? Perhaps a word unlikely to come up in a legal conversation like "dinosaur" or "hayride?" Whenever a client calls you – or communicates with you via any form of unsecure audio or video communication, ask for the code word. If they don't have it, terminate the communication.

Beware, they may say they forgot the code word. Start from the beginning – you call them at a known good number and establish a new code word. Is this perfect or all-inclusive in protecting you? No. But it's a start and it doesn't cost a cent.

Do change the code words from time to time, just in case. We're certain that legal practice management systems will (if they haven't already) build verification techniques into their systems allowing two-way authentication.

Tried and True Hallmarks of Deepfakes

One hallmark: The communication is urgent, particularly when monies are to be wired immediately. The authors all agree that you should take special care when you are asked to deal in cryptocurrencies which are still often fraught with risks.

Gifts cards? Oh yes, we have seen a law firm where an employee was asked to buy gift cards by the "managing partner." She bought $1200 worth of gift cards which ended up in the criminal's hands. And no, the firm did not reimburse her. A law firm's version of "tough love" we suppose.

Other indicators of probable fraud include "don't tell anybody what you're doing" warnings, asking for personal/confirmation information, and telling you to keep the communication itself on the "down low."

Things That Used to Identify Deepfakes

The world was a simpler place not so long ago. You could look at a deepfake video and see things like strange skin tones, odd lighting effects or jerky movements. The speech wouldn't sound quite right or was out of sync. Perhaps the eyes didn't blink or the body moved a bit strangely. You'll still see some of the old defects, but increasingly artificial intelligence is making many deepfakes harder to spot.

On the flip side, AI is often now used to detect AI-generated deepfakes, And it's very likely that, even as AI deepfakes become better and better, so will AI deepfake detection technologies. Our foe is also our friend when it comes to AI.

Final Thoughts

Worth a careful read: The story of how a finance worker at a multinational firm was tricked into paying out $25 million by a deepfake video call from the company's chief financial officer which included several members of staff on the call, all of whom were also deepfaked. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html. It is time for law firms to prepare for deepfake attacks before they too become headlines!

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.*