Mitigating the Risk of Deepfake Fraud for Your Company

Social engineering, or social hacking, is the act of manipulating social behavior to gain access to information or spaces without permission. One common form of social hacking is email phishing, which is the act of sending fraudulent emails impersonating a trusted source to get the recipient to take some sort of action. With the growth of AI, we are now seeing forms of social hacking that leverage audio and video to take impersonations to a whole new level.

In February 2024, cybercriminals orchestrated a sophisticated deepfake fraud against a Hong Kong company, resulting in a staggering $25 million loss. The fraudsters utilized deepfake technology, powered by generative AI, to impersonate the company's top executives on a video conference call and instructed an employee to transfer funds to fraudulent accounts.

In another case, cybercriminals employed deepfake audio to execute a CEO fraud scheme, extracting $243,000 from a UK-based energy company. By using AI-generated audio that replicated the voice of the parent company's CEO, the fraudsters coerced the UK company's CEO into making unauthorized wire transfers under false pretenses.

These incidents underscore the alarming potential of deepfakes to manipulate individuals and perpetrate large-scale financial frauds.

The emergence of new generative AI technologies has empowered fraudsters to create highly realistic deepfakes, enabling them to impersonate individuals with alarming accuracy. To generate a deepfake, fraudsters simply need to obtain an audio or video recording of an individual. Recordings can often be found on sites like YouTube, LinkedIn, Facebook, TikTok, a company's website, or even a recorded telephone call. With that in hand, a deepfake video or audio recording can be created in little time.

Compounding the problem is the speed in which deep fake audio or video can be created. As AI technology becomes faster and faster, a deep fake chatbot can respond instantly and participate in a conversation. This type of interaction can create very realistic situations.

The move to remote and hybrid work has provided fertile ground for audio and video impersonation. No longer can you count on in-person meetings where you know who you're meeting with. These have been widely replaced by video meetings, instant messengers, email, and phone calls.

All of these factors have led to significantly enhanced sophistication of deepfake fraud, making it imperative for organizations to bolster their defenses against such threats.

To safeguard against deep fakefraud, companies must prioritize awareness and education among employees. Most employees are simply unaware of the extensive capabilities of generative AI. By educating staff on the existence and dangers of deepfakes, businesses can enhance their ability to detect and respond to potential threats effectively.

In addition to making employees aware of the risks, encourage them to be skeptical and report or challenge situations that don't seem right. Deepfakes can take many forms, so it's best to err on the side of caution.

Another way to safeguard against deepfake fraud is to reassess and bolster internal procedures and policies around identification, especially when dealing with sensitive information or financial transactions. Consider multi-factor or biometric authentication or using unique codes that only a specific individual would know. Also, consider requiring multiple approvals for specific actions, such as financial transactions above a certain amount.

Deepfake fraud poses a high risk to companies in an era where bad actors can exploit new AI technologies for manipulation and financial gain. By staying vigilant, fostering a culture of skepticism, and implementing comprehensive security measures, your organization can significantly reduce the threat posed by deepfake scams and protect its assets from sophisticated cybercriminal activities.

Final Thoughts

If you would like to learn more about policies and procedures to mitigate the threat of fraud in your organization, please contact our office. One of our expert advisors would be happy to discuss your unique situation.

About Larson Gross

Ted Larson and Dennis Gross founded our firm in 1949. They built the business based on excellence, passion, integrity, trust and pro-action — values still important to us more than seven decades later.

Even well into their retirement years, Ted Larson and Dennis Gross continued to have the best interest of the firm at heart. Mr. Larson would come into the office on a regular basis to meet every new face and make a personal connection with each of our team members. He remembered the name of every employee, as well as the names of their spouses and children, and would greet clients by name as he passed by the reception desk. Sometimes, you'd even find a newspaper clipping on your desk that Mr. Larson dropped off, highlighting that your son made the honor roll. This is the example of a genuine relationship we strive to embody with our people and clients.

Today, we're led by ten partners who are growing our firm with respect for where we've come from and a new vision for future success. Our 120-plus team members and three offices located in Bellingham, Lynden and Burlington make us the 10th largest public accounting firm in the Puget Sound region. While we're determined to expand our impact and help strengthen as many businesses and individuals as we can, we're also committed to remaining a locally-owned organization. We're incredibly proud of where we've come from and look forward to a future of possibility

Larson Gross
2211 Rimland Dr.
Suite 422
Bellingham, WA 98226

(800) 447-0177

contact@larsongross.com

https://larsongross.com