Hey! What's New? 2024-128

What Accountants Need to Know About Deepfakes

According to an article in Australia's *INTHEBLACK,* written by Megan Breen, a deepfake "is a form of synthetic media where AI and machine learning algorithms are used to create highly realistic but fabricated images, videos or audio recordings." The term is a combination of "deep learning" and "fake."

"Deepfakes can be used to create fraudulent identification documents or realistic impersonations of individuals in video calls," Breen pints out, "which can then provide unauthorized access to bank accounts or other financial resources."

Apparently, it doesn't take much to fake a video. "Free software is available online and it is relatively simple to take existing audio and video footage and create something completely new – and completely fake," says Professor Jeannie Marie Paterson, professor of law and co-director of the Centre for AI and Digital Ethics at The University of Melbourne. "There are now video generators, image generators and voice generators that do video to video, text to image, text to voice, and I think you only need about 15 seconds of voice to be able to synthesize voice in a reasonably realistic way," she adds.

While altering images, videos and voices has its genesis in computer generated imagery (CGI) for films, the potential for misuse is enormous. Paterson continues, "the problem is we haven't quite caught up on how to prevent the misuse. We're still struggling with that."

With deepfake software being so accessible and seemingly straightforward, online scams in the financial industry are evolving. Paterson notes that "we've gone from emails and texts asking people to change account numbers to a fake person and a fake voice directing how payment should be made. It is accessible to anyone and you don't need any special tech skills to pull it off."

Paul Black, partner in cyber security at KPMG Australia, says deepfake technology is already having an impact. "Fraud is already being committed using deepfakes. It's not emerging – it's here, it's real and it's happening right now. The problem is that it's incredibly difficult [to] regulate and even to monitor, so the responsibility falls to each individual business. They should be very aware that you can't put all decision making into the hands of technology. It will do a great job to a point, but you really need that human validation for security reasons."

For that reason, businesses of all sizes need to educate themselves on how to detect deepfakes and be vigilant, says Black. "As with many technology-enabled crimes, it's really a case of playing cat and mouse between the detection and the technology getting even better. Certainly, there's detection platforms that can do their best to detect deepfakes, but it's really hit and miss."

Firms should be evolving their security practices to include multiple authentication points, instead of relying on one source of authority, Paterson adds. "We don't rely on mere email instructions – we authenticate them. That idea holds true for deepfakes, too – the days are gone when we can rely on what appears to be the face of someone we know," she says.

That advice may have come in handy for the finance worker at a multinational firm in Hong Kong who was tricked into paying out US$25 million (A$40 million) to scammers using deepfake technology to pose as the company's chief financial officer in a video conference call.

Paterson advises that organizations "should have systems and processes in place so that someone wouldn't just pay the money on a written instruction. They would confirm that instruction in a different way. Apparent face-to-face video instructions are no longer reliable, either. Firms need similarly to invest in other ways of authentication – which can include checking 'liveness' or even going back to real [in person], not virtual, meetings when there may be a high risk of fraud."