beazley

Article

Six-million-dollar scam reveals the extent of Deepfake AI threat

William Clarke • July 11, 2023

The industrial revolution saw humanity create machines that could replicate and enhance human effort. Machines replaced muscles and the world's productive capabilities expanded exponentially. Artificial intelligence (AI) holds the same potential. Cognitive ability can be enhanced, innovation can be prioritized over administration, as AI removes the need for repetitious activity. We have yet to scratch the surface of what this nascent technology will enable us to do. It may help us create new cures and mitigate or solve our greatest challenges.

But what about when that technology falls into the wrong hands? Or rather, is seized – and developed – by individuals who use it to defraud businesses of their hard-earned revenue? Increasingly sophisticated technology is evolving the way criminals carry out social engineering attacks and, with the help of AI, has given rise to a new wave of cyber security risk: the deepfake scam.

Social engineering scams are a fraudulent activity where a criminal poses as a figure of authority within that company and convinces an employee to transfer funds to a false account. These crimes are not a new phenomenon. Nor are phishing attacks, which trick employees into sharing information or clicking on seemingly innocent appearing links purporting to come from a trusted source that enable a cyber-criminal to access an IT network to steal valuable data and, or, money.

Historically, criminals' methods have been limited to emails or text messages which mimic the vocabulary and style of the executive or firm being impersonated. Today, the sophistication of AI means criminals can replicate voices on audio calls and faces in images and video. Also known as a 'deepfake', this deviously sophisticated technology means it is trickier than ever to distinguish between reality and AI manipulation.

CASE STUDY: SUPPORTING THE FINANCE DIRECTOR WHO FELL VICTIM TO A US$6 MILLION DEEPFAKE SCAM

Warnings of new technology can often feel far out on the horizon. However, the risks related to deepfakes generated by AI have already reached our shores.

What happened?

Earlier this year, a Chief Finance Officer (CFO) of a Beazley insured received a WhatsApp video message that initially appeared to be from the company's CEO. After a few minutes, the video started to fail, prompting the director to continue the conversation via WhatsApp chat. The CFO was informed that the company was in the midst of a crucial business transaction that required funding. The CEO assures the CFO that a lawyer will contact them to assist with the transaction.

Believing the scammer's deception, the CFO received banking information from the supposed lawyer and confirmation from the purported CEO to their personal email account. Over approximately two weeks, the CFO transferred multiple funds totalling more than US$6 million to a fraudulent bank account in Hong Kong.

How did we help?

Put simply, we paid the claim, allowing the insured to recover the significant funds lost in this fraud.

Spotting the red flags of social engineering scams, like requests to use a non-company mandated communication channels to offshore transfers and circumvent new payment verification in the interest of speed, seems common sense. However, the incredibly convincing nature of these attacks means it is not always easy to spot a scam.

Technological weapons in a criminal's arsenal are also evolving at pace. Our latest Risk & Resilience research reveals businesses are cognisant of the risk associated with technological disruption, which is a top concern for more than a fifth of businesses in the US (22%) and a quarter in the UK (25%). Alarmingly, businesses in the United States feel the least resilient to meet the growing threat, with one in three (30%) saying they do not feel prepared to face technology disruption risks.

Organizations need specialist support to stay appraised of the changing threats, and the latest learning to mitigate these evolving risks. As insurers will also need to remain vigilant, ensuring exclusions are explicit and support on offer for in-scope risks is robust.

As the use of AI becomes increasingly widespread its use for both good and bad will become clearer – but being alert to these new risks, and undertaking ongoing employee training on the risks and tactics being employed is essential if businesses are not going to end up victims of sophisticated deepfake scams.

William Clarke

Claims Team Leader - Executive Risk

beazley