CYBER UPDATE

MST INSURANCE SOLUTIONS

Deepfake Scammers Con Company Out of Over $25 Million

At a briefing on Friday, Feb. 2, 2024, Hong Kong police revealed that a recent cyber incident involving deepfake technology resulted in a finance professional at a multinational firm being manipulated into wiring more than $25 million in company funds to fraudsters. This event showcased the widespread damage that can be caused by deepfakes, which typically utilize artificial intelligence (AI) to analyze existing images, videos and audio recordings of an individual to generate sophisticated forgeries of the person's likeness. The following article provides more details on this incident and offers tips for businesses to prevent future deepfake-related losses.

Incident Details

According to Hong Kong police, the finance employee initially received an email from an account claiming to be the multinational company's chief financial offer (CFO) and requesting the deployment of multiple confidential transactions. The employee suspected the email was a phishing scam, but he reportedly felt more at ease after joining a video call with individuals who looked and sounded like the CFO and several of his colleagues. On this call, the employee was again asked to conduct a series of money transfers using company funds. Convinced he was communicating with trusted members of the firm, the employee moved forward with the transactions, ultimately making 15 total transfers to five separate bank accounts. The transactions totaled 200 million Hong Kong dollars, which is equivalent to roughly $25.6 million in the United States.

The finance professional didn't realize he had been tricked until he discussed the matter with the firm's head office afterward. From there, the incident was reported to the authorities. Upon investigation, Hong Kong police determined that the perpetrators developed AI-generated deepfakes of the finance worker's CFO and colleagues by leveraging existing video and audio files of these individuals from online conferences and virtual company meetings. Every individual on the video call with the finance employee was a fraud, and these scammers likely walked away with all of the funds from the various money transfers. At this time, it remains unclear whether Hong Kong police will be able to identify the perpetrators or retrieve the stolen funds.

Tips for Businesses

This event emphasizes how important it is for businesses to have appropriate cybersecurity measures in place that can help protect against deepfake-related losses. Here are some best practices for businesses to consider:

- **Train employees.** Employee training is critical to minimize the risks of deepfakes and associated damage. After all, employees are often the first line of defense against cyberattacks. As such, employees should be routinely educated on deepfakes, including what this technology is and how it may be used against businesses. By simply raising awareness of deepfakes, employees will be better equipped to spot them, allowing businesses to respond quickly and effectively to possible incidents.

- **Utilize detection software.** While AI can be used to make deepfakes more convincing, this software can also be leveraged to help detect and mitigate potential deepfakes. In fact, large corporations such as Facebook and Microsoft use AI and similar software to identify and remove deepfake videos from their platforms. When it comes to deepfakes, the earlier these scams can be detected, the better; this allows businesses to act quickly and reduce related harm.

- **Establish response strategies.** If and when businesses become targeted in deepfake-driven attacks, it's crucial to have proper response strategies in place. Such strategies should center around crisis mitigation and loss control. This includes outlining individual responsibilities, determining escalation practices and communicating appropriate response protocols. Additionally, if businesses haven't already, they should be sure to include deepfake scenarios in their cyber incident response plans.

As deepfake technology continues to evolve, businesses should make it a priority to consistently review their potential exposures and update their mitigation techniques whenever necessary. Contact us today for additional risk management guidance and insurance solutions.