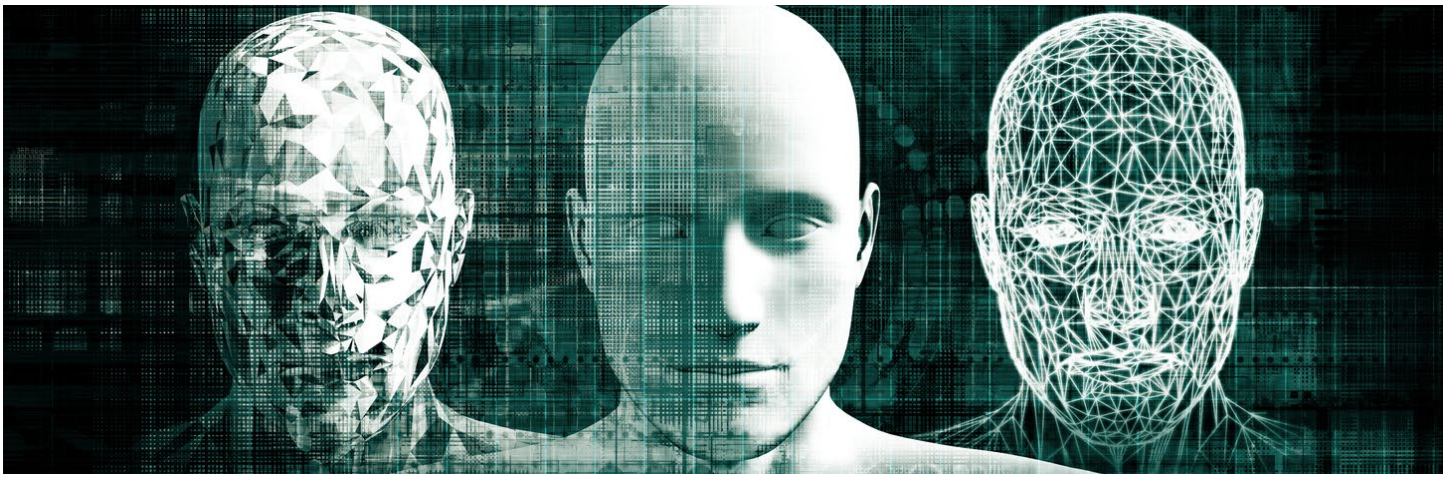
Protecting Your Data

Deepfake Technology Used to Fool Employees



THE NEWEST cyber and financial fraud threat facing businesses is deepfake technology, which criminals are using to extract money from unsuspecting accounts payable personnel.

A finance worker at a multinational company in Hong Kong was duped into transferring $25 million to criminals who had used deepfake technology to pose as the business's chief financial officer during a video conference call, according to local police.

A deepfake is an artificial image or video generated by a special kind of machine learning called "deep" learning. The creations have grown increasingly sophisticated and harder to detect.

How it happened

The worker received an e-mail from what he thought was the company CFO, inviting him to attend a teleconference with him, other company executives and staff, according to Hong Kong police. The digitally recreated version of the CFO then ordered money transfers during the video conference call.

Based on instructions the employee got during that call, they transferred 200 million Hong Kong dollars ($25.6 million) to various Hong Kong bank accounts in a series of transactions.

The employee did not interact with the deepfakes during the video conference, and he later told police that others on the call looked and sounded like people he knew in the organization.

In fact, all of the other people on the call were fakes of real people in the company. The criminals had used deepfake tech to alter publicly available video and footage found online to create convincing digital versions of the others in the meeting.

Police said that the case was one of several recent incidents in which criminals had used deepfake technology to change publicly available video and other footage to steal from people and companies.

Warning to US businesses

This type of attack is essentially an extension of the wire transfer fraud, a threat that's been growing in recent years.

These scams usually start with e-mails or even phone calls from scammers posing as someone higher up in an organization, a client or vendor. The end goal is to convince an employee with access to the company's payment systems to transfer funds to the criminals.

Deepfake technology adds a dangerous new arrow to wire-transfer fraud criminals' quivers, making the scam even easier to fall for.

To avoid being victimized, the law firm of Fischer Phillips recommended in a November 2023 blog that businesses:

Provide deepfake training to staff. You should already be training and providing refresher meetings on preventing cyber attacks of all sorts.

Consider educating them about the dangers of deepfakes and provide the Hong Kong case as an example. Cover ways to spot deepfakes, including:

- Blurry details,
- Irregular lighting,
- Unnatural eye and facial movements,
- Mismatched audio, and
- Absence of emotion.

Urge staff to be suspicious. Your employees should be able to comfortably question the legitimacy of information and be urged to report suspicious activity.

Use strong authentication protocols. Put in place robust measures — like multi-factor authentication and similar tools — for accessing sensitive information and systems.

Insurance coverage

If your organization has a cyber insurance policy, it might cover a wire transfer fraud loss.

The coverage provided by cyber insurance can vary significantly between insurance companies and policies. Some cyber policies may explicitly cover wire fraud, while others require additional endorsements or riders to provide adequate protection.

A commercial crime policy will cover losses resulting from the use of a computer to fraudulently transfer funds from inside the business premises or the insured's bank to an outside party.

However, policies may only offer coverage if an employee was fraudulently involved in the wire transfer fraud. This type of funds transfer fraud is basically the only computer-related coverage that a crime policy offers. ❖