Community Policing
Keep Macao safe
We all have a part to play

Police Circular
05/02/2024

Beware of Artificial Intelligence Scam



Recently, the Hong Kong police have discovered for the first time that scammers are using AI technology to defraud businesses. The scammers use deepfake technology, a form of artificial intelligence, to impersonate a senior financial officer of a multinational company. They then asked the company's Hong Kong branch employees to attend a video conference via SMS. During the meeting, the employees convinced that the participants were indeed the company's chief financial officer and financial staff, made multiple transfers per their instructions. The transfers totaled approximately HKD 200 million. Only later, when the employees communicated with the multinational company headquarters, did they realize they had been deceived.

Although Macao has not yet received any case involving this modus operandi, the rapid development of artificial intelligence in recent years has made it increasingly difficult to distinguish between truth and deception using deepfake technology. Scammers can download real videos from the internet and use deepfake technology to alter lip movements and use fake voices to synthesize videos, which they then play during video chat to deceive the public.

The Anti-Fraud Coordination Centre of the Judiciary Police has issued an alert to remind citizens and businesses to remain vigilant to avoid losses.

Recommendations for crime prevention:

1. If you have doubts about a person's identity in a video, you can ask them to perform specific actions in front of the camera and carefully check for variations. Additionally, you can ask questions to test the other person’s identity.

2. When receiving suspicious transfer requests, verify through alternative means to reduce the risks of deception.

3. Enhance the company's supervision and management processes for allocating large sums of money, especially when transferring or remitting funds to unfamiliar accounts. Approval from multiple persons should be required for such operations.

4. On a personal level, never readily provide strangers with biometric identification data such as face or fingerprint to prevent criminals from exploiting such data.

5. If you suspect you have been deceived, please contact the Judiciary Police Anti-fraud enquiry hotline at 8800 7777 or crime report hotline at 993.