MOORE

JANUARY 2025

MOORE NEWSLETTER

Next Level Phishing: Deepfake Scam

INTRODUCTION

In the first half of 2024, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) handled countless cybersecurity incidents, whereas phishing cases account for around 62% of the total cases. Compared to the second half of 2023, the number of phishing cases has increased by nearly 70%.

As cybercriminals become more sophisticated, they are employing advanced techniques in their phishing attacks, increasingly targeting specific individuals rather than casting a wide net. Alarmingly, there have been multiple reports of deepfake audio and video being used to impersonate senior-level personnel, leading to substantial financial losses for organisations.

Deepfake technology leverages artificial intelligence and deep learning algorithms to create hyper-realistic videos, images, and audio that convincingly depict fictional scenarios. While innovative, this technology poses significant risks as it becomes more accessible and easier to manipulate, expanding the threat landscape for individuals and businesses. As the line between reality and fabrication blurs, it is essential to understand the implications of deepfakes in cybersecurity and develop effective strategies to mitigate these evolving threats.

Common deepfake techniques involve the following:

- **Realistic AI voice**: Use synthetic voice AI to render an authentic human voice from recording samples and communicate with others with great accuracy in tone and likeness.
- **Face swapping**: Replace the face of the person in the source video with the face of the target person.
- **Text to speech synthesis**: Use a realistic narrator voice maker to convert text into natural-sounding speech.
- **Voice attribute editing**: Modify voice attributes to modulate voice sound completely different.

DEEPFAKE CASES IN HONG KONG

In February 2024, a notable phishing scheme involving deepfake technology occurred whereas the fraudster impersonated the Chief Financial Officer of the informant's head office in the United Kingdom, using a convincing deepfake video to establish credibility. The informant was invited to a group video conference for purportedly confidential transactions. Believing the deepfake was legitimate, the informant followed the instructions given during the call and ultimately authorised the transfer of funds to five local bank accounts. This resulted in a significant loss of approximately HK$200 million. It was found that a pre-recorded video conference was created using downloaded public video clips and the voice of the impersonated officer. The meeting was recorded in advance, and there was no interaction between the informant and the fraudster.

Another deepfake case featured Hong Kong Chief Executive John Lee selling investment products, where the criminal used deepfake software to generate a fake voice of John Lee.

Both deepfake cases highlight the urgent need for heightened vigilance in communication practices. Organisations and individuals should establish robust verification protocols, especially when dealing with financial transactions or sensitive information. Additionally, training and awareness programmes are crucial for empowering individuals to recognise and respond to potential threats effectively.

IMPACT OF DEEPFAKES

The increasing realism of deepfakes makes it difficult for people to distinguish between genuine and manipulated videos, leading viewers to believe in their authenticity and share them on social media, which accelerates the spread of disinformation. This rise in deepfake technology poses significant impacts, creating a multifaceted risk landscape that demands urgent attention and robust countermeasures.

1

Cybersecurity threats

Deepfake technology allows for realistic impersonations that can evade security measures like facial recognition, heightening the risk of unauthorised access, data breaches, and identity theft.

2

Legal and ethical challenges

Deepfakes involve replicating and distributing copyrighted material without permission, leading to legal disputes over intellectual property rights. The ability of deepfakes to harm reputations through false representations creates ethical dilemmas concerning accountability for the damage incurred.

3

Financial fraud

Deepfakes can elevate phishing attacks by making fraudulent communications appear more legitimate, thereby facilitating social engineering tactics that trick individuals into making financial decisions they might not typically make.

4

Deterioration of trust

The rise of deepfakes foster skepticism towards media as people struggle to distinguish genuine content, while simultaneously enabling the manipulation of public opinion through the dissemination of false narratives, ultimately undermining trust in institutions and information sources.

COUNTER DEEPFAKE

According to Onfido's Identity Fraud Report 2024, there has been a 3,000% increase in deepfakes in 2023 compared to 2022. The increasing prevalence of deepfake technology has made it difficult to determine the authenticity of digital content. Detecting deepfakes is vital for maintaining trust in what we see and hear. In addition to technological solutions, Infosec outlined several general tips for manually identifying deepfakes.

General tips for identifying deepfakes

- Anomalies of patterns, colours and signs
- Unnatural blinking or movement
- Inconsistent lighting and semantic integrity
- Unnatural speech cadence or robotic tone
- Lip movements out of sync with speech
- Poor video or audio quality

CONCLUSION

As deepfake technology becomes increasingly widespread, cybersecurity experts encounter significant challenges. Developing effective detection methods for deepfakes is essential to mitigate their impact. This effort will necessitate continuous research and collaboration among technology companies, law enforcement agencies, and cybersecurity professionals.

Furthermore, promoting public awareness and education about deepfakes is vital, empowering individuals to recognise and respond to this emerging threat. By integrating advanced machine learning techniques and harnessing collective intelligence, we can improve detection capabilities. Meanwhile, establishing legal frameworks will address the ethical and regulatory challenges associated with deepfake misuse.

Ultimately, a comprehensive strategy that integrates technology, policy, and public awareness is crucial for navigating the changing landscape of deepfake threats and safeguarding the integrity of digital communications.

REFERENCES

Hong Kong sees three deepfake video scams since last year, says security chief | The Standard
Next-Level Phishing: The Evolving Threat Landscape (hkcert.org)
InfoSec: Deepfake
Identity Fraud Insights Report 2024 | Onfido

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SMEs to listed companies from a wide variety of industry, and public sectors including government bureaus and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

To find out more, please contact one of our experts below:

PATRICK ROZARIO
Managing Director
T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal
T +852 2738 4631
E kevinlau@moore.hk

www.moore.hk

The information provided is for general guidance only and should not be treated as professional advice. While we believe the content is correct at the time of publication, we cannot accept responsibility for any loss or inconvenience caused by actions taken based on the information herein. We recommend consulting a qualified advisor to ensure your specific circumstances are properly evaluated before making any decisions.