DORSEY
DORSEY + WHITNEY LLP

The New Face of Fraud: Deepfakes and the Emerging Cyber Threats in Hong Kong

by Janet Wong and Steven C. Nelson

Almost from the very beginning of the internet era, the world has been increasingly afflicted with cyberfraud, exploiting the internet's potential to enable fraudsters to induce unsuspecting victims to transfer money to overseas bank accounts using another relatively recent technological innovation, electronic funds transfer. Hong Kong is a destination particularly favored by fraudsters for such transfers, due to its open banking system and the ease with which funds can be retransferred from there to mainland China, from which many of the fraudsters operate and where recovery of funds is much more difficult, if not impossible.

Recently, a new breed of deception has emerged, in Hong Kong as well as elsewhere, using the power of deepfake technology. Despite robust government measures to combat fraud, fraudsters are getting creative and discovering new methods to take advantage of people. This eUpdate will review the most recent fraud statistics and what the government is doing to stop it in Hong Kong, take a closer look at the worrying increase in deepfake scams, and provide practical guidance for everyone to better protect themselves from these growing online dangers.

Alarming Statistics

According to the statistics announced by the Hong Kong Police Force (HKPF) on February 6, 2024 (the "2023 Statistics"), deception cases in 2023 surged by 42.6%, totaling 39,824 cases. Internet-related scams accounted for approximately 70% of the reports, involving over HK$9 billion (US$1.15 billion). Common fraudulent activities included online shopping scams (8,950 cases, a 2.5% increase), investment fraud (6,330 cases, a 1.2-fold increase), phishing scams (4,322 cases) – newly covered in January 2023, employment fraud (3,930 cases, a 31.2% increase), social media deception (3,372 cases, a 6.5% decrease) and telephone deception (3,213 cases, a 13.5% increase).

Government Anti-Deception Efforts – "Scameter+"

In our last eUpdate published in June 2023, we discussed the various measures

Related People

- Janet Wong
- Steven C. Nelson

Related Capabilities

- Privacy & Social Media
- Financial Services Regulatory
- Hong Kong

implemented by the Hong Kong Government in response to the rising deception cases. As part of these efforts, the HKPF launched the one-stop scam and pitfall search engine "Scameter+" in February 2023 to assist the public in identifying fraud and online pitfalls.

According to the 2023 Statistics, "Scameter+" has recorded over 2.13 million searches and issued nearly 360,000 alerts on frauds and cyber security risks. The HKPF plans to enhance the "Scameter+" app by introducing new features, such as enabling it to send alerts when users encounter suspicious websites or receive suspicious calls, as well as introducing a public reporting mechanism within the "Scameter+" app.

Deepfake Scams

Despite the government's anti-deception efforts, there were 3,238 cases of deception reported in the first month of 2024, accounting for 42% of all crimes. The number of deception cases is on the increase worldwide. In the rapidly changing world of cybercrime, fraudsters are constantly seeking new opportunities to exploit vulnerabilities. Their newest tool? Deepfake Technology! This cutting-edge AI-driven technique allows scammers to create highly convincing fake videos and audio recordings, blurring the boundaries between reality and deception.

In February 2024, the Hong Kong office of a multinational company fell victim to a sophisticated scam involving deepfake technology. The fraudsters created digital replicas of the company's chief financial officer and other employees, who appeared to participate in a video conference. By convincingly replicating the appearance and voices of the targeted individuals using publicly available video and audio footage, the fraudsters deceived an employee of the Hong Kong office into making 15 transfers, totaling HK$200 million (US$25.6 million), to multiple bank accounts. This incident marked the first known case in Hong Kong where victims were deceived in a multi-person video conference setting.

It is particularly concerning that the company officials only became aware of the scam about a week later and subsequently reported to the HKPF. The delayed realization underscores the importance of raising awareness and educating employees about the risks associated with deepfake technology, as well as other forms of cyberfraud. It is crucial for organizations to implement internal security measures and provide regular training to the staff so that they can recognize and respond to such scams effectively.

While deepfakes currently constitute only a small portion of Hong Kong's wider cyber fraud landscape, it remains imperative that we proactively take steps to safeguard ourselves. As individuals, we play a crucial role in safeguarding our digital lives and ensuring online security. Here are proactive steps to take:

- Stay Informed: Keep up-to-date with the latest trends in cyberfraud, common scams and deceptive techniques to better recognize and avoid falling victim to fraud.
- Verify Sources: Exercise caution when receiving requests for sensitive information or financial transactions, especially during video calls. Verify the authenticity of individuals by asking them to perform specific actions, such as moving their heads, or by answering questions that confirm their identity.

- Use of Technology: Leverage AI-driven tools to detect anomalies and inconsistencies in communications. These advanced technologies can help identify potential deepfakes or other fraudulent activities, providing an additional layer of protection.
- Act Quickly: If you suspect wire fraud, contact your bank immediately to report the incident and request a hold on the transaction, or to recall funds. Engage a trusted lawyer who has experience in fraud as soon as possible.

To learn more about email wire fraud and business email scams, we recommend reading our in-depth guide on protecting against such scams and recovering funds wired to Hong Kong. Our experienced Hong Kong and U.S. wire fraud lawyers have handled numerous cross-border wire fraud cases and are well-equipped to provide expert assistance and guidance. Please visit our International Cyber Crime and Asset Recovery page.

[1] See HKSAR Press Release on 6 February 2024

[2] See South China Morning Post, "*Hong Kong police log 15 per cent surge in scams in January, despite integration of anti-fraud app into major payment system*" dated 12 March 2024

[3] See RTHK News "*Deepfake colleagues trick HK clerk into paying HK$200m*" dated 4 February 2024