Countering the New Frontiers of Fraud
應對詐騙新形勢

While the fundamental goals of fraudsters that target banks and their customers have remained largely unchanged for several decades, the significant difference today is the way that fraudsters utilise AI to craft and execute complex social engineering attacks and synthetic identity theft at unprecedented levels of speed, reach and scale.

數十年來，騙徒針對銀行及銀行客戶的基本目的大致不變，但今天的行騙手法大有不同，騙徒運用人工智能，精心設計和執行複雜的社交工程攻擊和合成身份盜竊，其行騙速度、覆蓋範圍和規模前所未見。

As fraud networks become more sophisticated, cyber-enabled fraud attacks are no longer standalone events, they have evolved into multi-layered financial crime threats, perpetrated by scammers who deploy coordinated AI systems. Highlighting how fraudsters are master adapters and the various ways that banks can build defences against them, a recent Thomson Reuters Confirmation webinar event brought together a panel of speakers who shared insights and observations on the prevalent attack and defence trends within the banking and professional services environment. As AI-empowered fraudsters continue to develop new ways to target banks, financial institutions and their customers, panel speakers David CHAN, Chief Information Security Officer at Hang Seng Bank, Hong Kong; Amelia CHING, Founder and CEO of Singapore training and consulting firm AgilenLite; and Ross WIDDOWS, Partner and Consulting Leader, NSW, at BDO Australia, explained that static cybersecurity defence systems are no longer sufficient to counter today's sophisticated cyber threats.

In order to meet the surge in AI-led threats and vulnerabilities, banks need to transition the cybersecurity operating model from a reactive defence model to a proactive offence model, the panel speakers explained. "For decades banks have built defensive operations, but now they need to act offensively," Mr CHAN noted. While financial regulators increasingly request banks and financial institutions to adopt "prevention-first" frameworks, transitioning from cybersecurity risk mitigation to an offensive posture is still a work in motion for many banks. Put simply, the panellists explained, an offensive cybersecurity posture involves identifying risks and vulnerability gaps before a cybercriminal else does. Knowing that risks exist is merely the starting point. The panellists agreed that effective offensive strategies depend on combining an understanding of what is being protected, how vulnerabilities can be exploited, and the bank or financial organisation's capacity to remediate. This requires implementing a full scope of integrated systems and strategies that not only probe and test a bank's defences, but also evaluates the incident response and post-incident capabilities of the defensive team. For example, using the same tactics as malicious actors, but conducted by ethical hackers or a bank's own cybersecurity team, penetration tests or "pen tests" probe for misconfigurations or unpatched software before adversaries can. "Pen tests should not be tick-box exercises," Mr WIDDOWS cautioned, adding that tests should be conducted regularly and not as one-off yearly or bi-yearly exercises.

詐騙網絡日趨精密，網絡詐騙攻擊不再是單一事件，而已演變為多層的金融犯罪威脅，騙徒以協調一致的人工智能系統犯案。Thomson Reuters Confirmation 最近舉行網上研討會，邀請多位講者分享銀行及專業服務領域常見的攻擊手法和防範措施新發展，指出騙徒是適應力強的高手，以及銀行防範騙徒的不同方法。研討會講者包括香港恒生銀行首席信息安全官陳致言、新加坡培訓諮詢公司 AgilenLite 創辦人兼首席執行官 Amelia CHING，以及澳洲 BDO Australia 新南威爾斯州合夥人及諮詢業務主管 Ross WIDDOWS。騙徒持續運用人工智能設計新方法，針對銀行、金融機構及其客戶，講者認為靜態的網絡安全防禦系統，已不再足以應對今天精密複雜的網絡威脅。

New twists on an old problem

Describing fraud as "an old problem with a new technology twist", Mr WIDDOWS explained as AI systems rapidly develop, fraud scams are being executed faster and more convincingly than ever before and are harder to detect. Compounding the threat level further, the democratisation of AI technologies, which has lowered the barrier to entry, enable fraudsters — often operating as coordinated, well-organised gangs — to test, execute, and redeploy scams across regional and global markets in a fraction of the time it used to take to launch a fraudulent activity. Today's fraud campaigns frequently target multiple institutions and geographies at the same time, Mr WIDDOWS observed. Additionally, fraudsters embed AI into their routing architectures, which make location detection difficult to verify.

In the hands of cybercriminals, AI tools can make fake documents appear more authentic and phishing attacks more difficult to detect. For example, scams can be personalised by using personal data and cloned voices scraped from social media platforms to generate realistic synthetic IDs and deepfakes. Mr WIDDOWS cited examples of deepfake videos of executives being used to deceive unsuspecting employees into transferring corporate funds and revealing sensitive data.

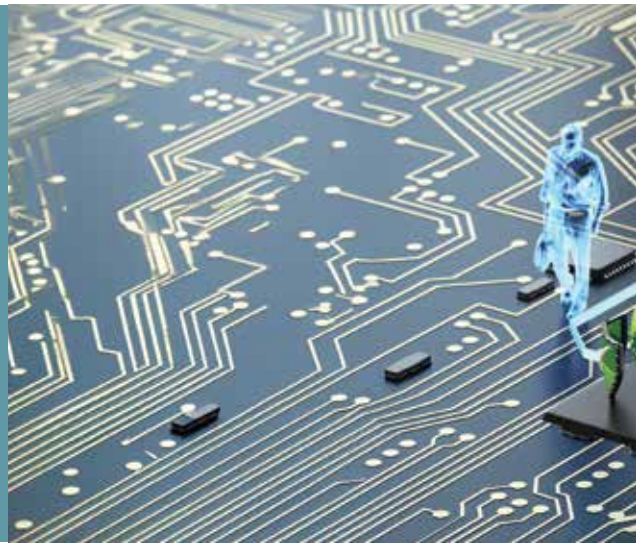
For Ms CHING, boosting banking practitioners' awareness of the threat deepfakes pose requires hands-on experience of how deepfake impersonations are created using AI-simulated audio and video. "People only really take deepfakes seriously once they have experienced how easily a deepfake can be put together," she said. Once people understand how easy it is to create a deepfake, it is about putting the appropriate hygiene factors in place. Similar to personal hygiene, cybersecurity

研討會講者表示，面對人工智能主導的威脅和網絡漏洞，銀行有需要改變網絡安全營運模式，由被動防禦模型改為主動防禦模型。陳先生說：「數十年來，銀行建立了防守措施，但現在得主動出擊。」金融監管機構日漸趨向要求銀行及金融機構建立事先預防的制度，而許多銀行仍然處於由緩解網絡安全風險轉變至主動出擊的過程中。講者表示，簡單地說，主動式網絡安全模式是要先於網絡罪犯識別風險與漏洞。知道風險存在，只是個起點。講者同意，有效的主動策略，須結合對保護對象的了解、對漏洞可如何被人利用的認識，以及銀行或金融機構採取補救措施的能力；當中涉及實施全面的整合系統和策略，既可探查和測試銀行的防禦系統，也可評估防禦團隊的事故回應和處理能力。例如由道德黑客或銀行自身的網絡安全團隊使用與惡意攻擊者相同的手法，進行滲透測試，先於敵人找出錯誤設定或未修補的軟件。WIDDOWS先生提醒：「滲透測試不應敷衍了事」，又說測試應經常進行，而不應只是每年或每兩年進行的一次性工作。

老問題的新變化

WIDDOWS先生形容詐騙是「老問題的新科技變化」，表示人工智能系統發展迅速，騙局比從前較快實行，也更有說服力，更難以偵測。除了威脅程度提高以外，人工智能技術的普及化降低了門檻，讓騙徒更快在區域和全球市場測試、實行和重複騙局；以往要長時間才可實現的詐騙行為，現在極短時間內便可實行。WIDDOWS先生留意到，騙徒往往是有組織的團夥，經常同時在多個地域攻擊多家機構。此外，騙徒亦在路由架構中利用人工智能，使自己的藏身之所難以偵測和核實。

> *"While financial regulators increasingly request banks and financial institutions to adopt 'prevention-first' frameworks, transitioning from cybersecurity risk mitigation to an offensive posture is still a work in motion for many banks."*



hygiene involves routine deploying preventative maintenance, such as following cybersecurity processes, operating system updates, separating web activities, providing employee training and awareness, and protecting data. Ms CHING recommends maintaining a high level of scepticism. "Never trust anything at first sight," she said. For example, due to the quality of deepfakes being capable of meeting the validation requirements of single-channel verification, it is essential to apply independent, multi-channel verification to verify the authenticity of customers, especially at the on-boarding stage.

Mobile device account management

Subscriber Identity Module (SIM), commonly known as "SIM hijacking", is another area Mr WIDDOWS highlighted as a common target area for fraudsters. SIM hijacking involves the use of AI-generated text messages and emails to deceive telecom operators and unsuspecting mobile device users into transferring phone numbers, passwords and SIM activations to a SIM card in their possession. Aimed at combating telecommunications fraud before service activation, legislation was introduced in Hong Kong in 2022 requiring complete real-name registration for all applications for SIM cards (including SIM service plans and prepaid SIM cards) issued by local telecommunications service providers for use in Hong Kong. In a further bid to combat phone scams, in 2025 the Hong Kong government proposed lowering the maximum registration limit for individuals from the current 10 prepaid SIM cards per service provider to three. The proposed amendment is expected to be presented before the Legislative Council for scrutiny during 2026. While Hong Kong does not maintain a distinct category exclusively for SIM card fraud, identity theft accounted for 34% of losses among consumers who reported digital fraud in 2025.

網絡罪犯有了人工智能工具，便可把虛假文件造得更像真，使網絡釣魚攻擊更難以偵測。例如在社交媒體平台擷取個人資料和聲音，生成逼真的合成身份和深偽形象，便可製造個人化的騙局。WIDDOWS先生舉出一些例子，當中騙徒利用機構高層的深偽影片，誘使毫無戒心的職員轉移機構資金，透露敏感資料。

CHING女士表示，若要提高銀行從業員的意識，教他們明白深偽的威脅，便須讓他們親身體驗如何利用人工智能合成的聲音和影片來製作深偽內容。她說：「人們經歷過這個過程，知道深偽作品很容易製作後，才會認真看待深偽。」人們明白深偽內容很容易製作後，接下來就要培養適當的網絡衛生習慣。正如個人衛生一樣，網絡安全衛生涉及實施例行的防禦維護措施，例如遵從網絡安全程序、安排作業系統更新、分隔不同的網頁活動、提供培訓和提高員工意識，以及保護數據。CHING女士建議抱持高度懷疑的態度：「千萬不要相信第一眼看到的東西。」例如深偽物品質素良好，可以通過單一途徑驗證的要求，因此必須實施獨立的多途徑驗證，核實客戶的身份。這程序在接受新客戶的階段尤其重要。

流動裝置帳戶管理

WIDDOWS先生特別提出，電話卡劫持是另一種常見的詐騙手法。騙徒利用人工智能生成的短訊和電郵，欺騙電訊商和毫無戒心的手機用戶，讓他們把電話號碼、密碼和電話卡開通流程轉移至騙徒的電話卡。為打擊在服務開通前的電訊詐騙活動，香港在2022年通過法例，要求向本地電訊商申請在香港使用的電話卡時（包括電話卡服務計劃和預付電話卡），必須實名登記。為進一步打擊電話騙案，香港政府在2025年建議個人登記預付電話卡的上限，由每名電訊商10張減至三張，修訂建議預計在2026年內提交立法會審議。香港沒有單獨統計電話卡騙案的數字，但2025年數碼騙案受害消費者的損失當中，34%是由身份盜竊引致。

> *"金融監管機構日漸趨向要求銀行及金融機構建立事先預防的制度，而許多銀行仍然處於由緩解網絡安全風險轉變至主動出擊的過程中。"*

The human factor

With research indicating the human element is often the target for instigating cybersecurity breaches, Mr CHAN pointed out that taking advantage of human vulnerabilities remains one of the most exploited attack surface used by fraudsters. With mobile phones often functioning as a one-stop device for managing banking apps and personal data, and often used while walking or multitasking, thereby reducing vigilance and logical thinking, the customer end of a bank's digital platforms is often the weakest link, Mr CHAN added. "We have seen a lot of malware that target phone users' mobile apps," he said, citing the example of a wave of malicious SMS messages that impersonated government agencies and logistics companies that first targeted unsuspecting individuals in Singapore, followed by individuals in Hong Kong. "People clicked the malicious link, which installed malware and practically handed attackers control of their phones and their credentials, Mr CHAN explained. Adding a layer of complication to the deception, user credential checks are bypassed when a legitimate customer unknowingly authenticates a transaction that has been manipulated by cybercriminals.

Taking the view that no single method can serve as a definitive indicator of authentication, Mr CHAN said it is really about defence in depth. "There is no single tactic or strategy capable of mitigating cyber-attacks," Mr CHAN said. A multi-pronged defensive shield requires new approaches, such as using AI to identify behavioural signals, including a login from a location that is not associated with the customer, comprehensive scanning for malware and detecting injection attacks, the process by which malicious code or commands are introduced into an application or system, tricking it into exposing sensitive databases, bypassing security and executing unauthorised actions.

While banks in Hong Kong and across the region are setting up joint centres to utilise AI for fraud detection and share suspicious activity information, the panellists suggested that collaboration should extend beyond banks and financial institutions to include regulators, law enforcement agencies, telecommunications providers and technology firms. Looking ahead to the post-quantum cryptography era — taking the level and scope of encryption used in the banking environment into account — the panellists advocated that now is the time for banks to focus on developing tools and systems that use AI to identify encryption architectural weaknesses and novel attack paths. BT

人的因素

研究顯示，人的因素往往是網絡安全事件針對的目標；陳先生指出，人性弱點始終是騙徒最常利用的攻擊面之一。手機通常是一站式管理銀行應用程式和個人資料的工具，而且往往是在行走時或處理多項事務時同時使用，使用者的警覺性和邏輯判斷能力會因而下降，因此銀行數碼平台的客戶端通常是最弱一環。陳先生說：「有許多惡意軟件特別針對攻擊手機使用者的流動應用程式。」他舉例說，曾出現一連串冒充政府機構和物流公司的惡意短訊，最初以新加坡毫無防備的個人為詐騙對象，後來擴展至香港。他解釋：「人們點擊惡意連結，從而安裝了惡意軟件，實際上讓攻擊者控制了自己的手機和登入憑證。」更複雜的是，真實的客戶無意中認證了網絡罪犯操縱的交易後，便會繞過核實用戶憑證的步驟。

陳先生認為，沒有任何單一方法可確切認證用戶身份。他說：「實際上是需要縱深防禦。沒有單一手段或戰略可緩解網絡攻擊。」多管齊下的防禦盾，要採用新方法，例如運用人工智能識別行為上的訊號（包括在與客戶無關的地點登入）、進行全面掃描以找出惡意軟件，以及偵測注入攻擊（即把惡意程式碼或指令注入應用軟件或系統，誘使軟件或系統洩露敏感資料庫、繞過安全檢查及執行未經授權的操作）。

香港和區內的銀行正設立聯合中心，利用人工智能偵測詐騙行為，並交換可疑活動的資訊。研討會講者建議擴大合作範圍，除銀行及金融機構外，監管機構、執法機關、電訊商和科技公司亦應參與。展望後量子密碼年代，考慮到銀行業界使用加密技術的程度和範圍，研討會講者提出，銀行現時應專注開發工具和系統，利用人工智能識別加密架構的弱點和新的攻擊路徑。BT