盜身份證呃貸款 騙徒「深偽」換面得手

瞞過金融機構辨識系統掠7萬元 高科技欺詐「殺到埋身」

◆警司高迪交代案件詳情。

香港警方近期根據情報，獲悉有騙徒利用其他人的身份證申請網上貸款，調查後鎖定一個本地詐騙集團，相信他們由2022年9月至今年7月期間，盜用至少8名本地市民身份證，向20間不同的銀行和財務公司，合共遞交90次貸款申請，以及54次銀行戶口開戶申請。這些申請絕大部分透過網上進行，其中有4次貸款申請獲批核，共涉款20萬港元。

網絡安全及科技罪案調查科科技罪案組警司高迪昨日公布案情指，隨着科技日趨發達，不少金融活動如借貸和開戶均可在網上進行。金融機構會要求申請人掃描並上傳申請人的身份證明文件，以及提供即時自拍照片，有關機構再透過人臉識別系統核實申請人與身份證明文件上的照片是否脗合，以防止有騙徒冒充他人申請。

騙徒最少試20次 其中一次得手

據了解，在4宗獲批的貸款申請中，有一宗為騙徒使用了「深度偽造」人工智能換臉技術。騙徒利用市民已報失的身份證，冒充報失人申請貸款，在掃描身份證後，騙徒要在人臉識別系統中拍照顯示面容，但他利用電腦「深偽」程式，將自己的容貌變成被盜身份證主人的容貌，但並非次次成功。警方調查發現，騙徒最少使用了20次，其中一次得手竄過漏洞，最後騙去7萬元。

在另外3次騙貸中，騙徒使用最低層次的手法，即持盜來或他人報失的身份證，直接到銀行櫃台辦理，警方已向有關銀行提供建議，提升員工的防騙技能。

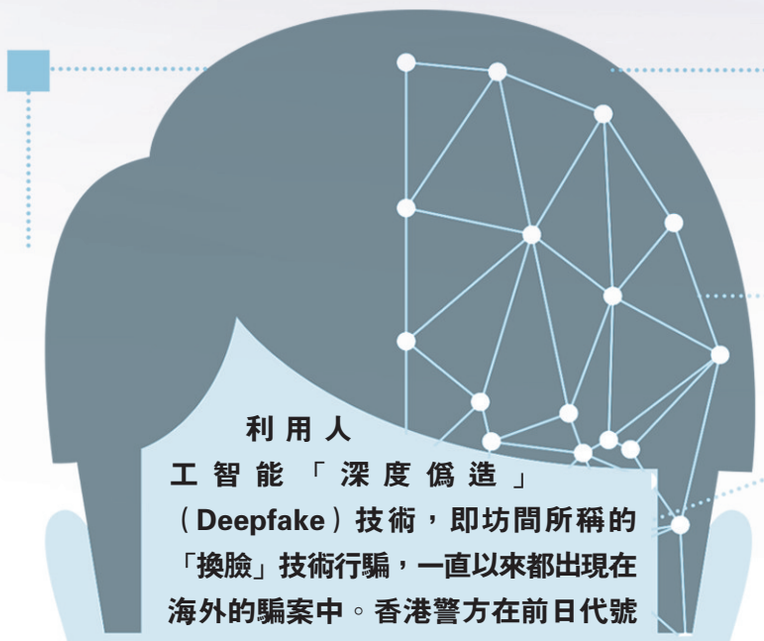
警方又發現該詐騙集團曾盜用8名市民報失的身份證，實名登記超過30張預付費電話卡，並在今年4月至5月期間，發送出超過7,200個釣魚詐騙電話短訊，冒充電訊商以提供積分回贈為由，誘騙市民登入假網站提交信用卡資料。至今，警方接獲一宗相關報案，受害人表示誤信釣魚詐騙信息而被盜用信用卡資料，被騙徒用來作購物。

警提醒市民「有圖未必有眞相」

警方提醒市民，科技發展一日千里，「有圖未必有真相」，高科技欺詐工具令人防不勝防，提醒市民需時刻提高警覺，保護個人資料，提防受騙。如果有任何懷疑，市民可以致電警方防騙易熱線18222，或者利用「防騙視伏器」或「防騙視伏App」查核懷疑的網址、電郵、電話號碼、社交平台賬戶、收款賬戶等。

警方已經給予金融機構適當建議，提升防騙保安措施，同時會繼續積極和各行各業的持份者交流。

◆警方網罪科和金管局代表今年7月5日舉辦「數碼詐騙工作坊」。 資料圖片



利用人工智能「深度偽造」（Deepfake）技術，即坊間所稱的「換臉」技術行騙，一直以來都出現在海外的騙案中。香港警方在前日代號「解詐」行動中，瓦解針對金融機構申請貸款和開設銀行戶口的詐騙集團，首次發現有騙徒將人工智能換臉術應用在眞實案件中，更瞞過金融機構人臉辨識系統騙取7萬元。雖然涉及金額不多，但已敲響AI變臉騙術「殺到埋身」的警號。行動中，警方拘捕6人，包括集團主腦。有關機構已按警方建議提升系統防偽水平，已成功堵塞漏洞。

◆香港文匯報記者 蕭景源

預防AI詐騙小貼士

- 在視像對話中要求對方在鏡頭前做指定動作
- 向對方提問，測試對方身份眞偽
- 切勿輕易提供人臉、指紋等生物辨識信息
- 若有「親友」在視頻或錄音中提出匯款要求，要特別警惕
- 避免接聽陌生視像通話來電
- 不要輕易相信網上的資訊
- 養成事實查證習慣
- 如懷疑文字或圖片被竄改，可試用搜尋器查找出處
- 多從不同媒體查找資訊，以多角度查找眞相
- 在解讀「消息指」、「已Fact Check」等信息時應保持懷疑態度
- 如懷疑內容屬假資訊應避免轉載，並向事實查證機構查詢
- 撥打防騙易18222熱線或使用「防騙視伏器」或App，留意警方最新的防騙消息

資料來源：警務處 整理：香港文匯報記者 蕭景源

◆若想測試是否AI「變臉」，可叫對方用手指橫過面前，如像右邊畫面出現模糊影像，便要小心。 資料圖片

手指橫過臉部若模糊 或為假影像

特稿

兩個月前，香港在AI「深偽技術」換臉行騙方面仍是零個案，但前日香港警方搗破的犯罪集團首次發現換臉騙案，反映問題已「殺到埋身」。隨着「變臉」、「變聲」技術的不斷成熟和製作成本下降，其運用在不同劇本的網上騙案中，殺傷力不容小覷。警方分析，在理論上，AI「深偽技術」也可能會使用在網戀騙案、電郵騙案、釣魚騙案中。

網絡安全及科技罪案調查科在今年7月就騙徒可能運用AI「深偽技術」行騙的伎倆和技術狀況，向傳媒演示利用人工智能「換臉」的手法。他們以數星期時間搜集一名警司的臉部資料，再用「深偽技術」套用在另一人身上並作實時視像聊天，雖有幾分神似，但被偽冒人物的眼神、口型出現不協調，臉部邊緣線不自然，反映經數星期收集的數據仍不完善。

警方解釋，現階段騙徒通常需要收集大量被模擬對象的原始影像和語音數據，才能達到理想的偽造成果，過程要配合高運算力的電腦，需時費力，加上目前的技術尚無法作非常細緻的處理，例如眨眼、視線變化或臉部抽搐等動作會較不自然，通常在畫面邊緣處會出現不協調，故利用「深偽技術」實時對話較易露出破綻。

警方提醒，一個較直接可見的破綻是，當對方的手指在鏡頭前擺動，可能因數據不完整及電腦運算力不足，無法應對突然改變的畫面，令手指動作變得模糊和遲滯。所以，市民若有懷疑，只要叫對方在視像中做出用手指橫過臉部的動作，就可以看出破綻，判定這可能是一個假影像。

為免露破綻 騙徒或只播數秒

根據警方了解，目前騙徒使用的「變臉」片段均由騙徒預先製作，然後透過視像通話播放。為免「夜長夢多」露出破綻，他們往往只會播放數秒鐘，然後以不同藉口結束視像聊天，再返回傳統的詐騙「劇本」行騙。因此，市民必須時刻保持警惕，提高防騙「免疫力」，謹記「眼見不一定為實，有圖並不一定有眞相」。

◆香港文匯報記者 蕭景源

警與銀行界持份者協作 增防騙能力

話你知

「人工智能」（AI）是科技新趨勢，隨着其普及化，有網絡犯罪分子將之用作犯罪工具，反網上詐騙成為一場科技攻防戰。隨着金融服務數碼化，騙徒的目標移向金融機構和企業，全球銀行都花大量資源以防止金融科技詐騙，採用漸趨成熟、應用成本逐步下降的生物認證技術，包括指紋和人臉識別已應用於客戶身份認證，但同樣騙徒也在試圖運用「深偽技術」攻破人臉識別。

由於近年騙徒盜取個人銀行戶口資料活動趨增，甚至可破解銀行核實客戶身份程序，包括涉及一次性密碼的雙重認證，故香港的金融機構不斷提升防範措施，包括就高風險的交易或操作增加多重認證，陸續加設以人臉識別的認證方法來核實客戶身份，以減低客戶因詐騙活動而蒙受損失的風險。

警網罪科和金管局上月辦工作坊

針對近月釣魚騙案有上升趨勢，以及有騙徒利用「深偽技術」（Deepfake）對銀行和財務機構進行詐騙，警方網罪科和金管局代表今年7月5日舉辦「數碼詐騙工作坊」，向140位來自70間銀行和財務機構的代表分享了釣魚騙案的常見手法，並即場示範騙徒如何利用「深偽技術」換臉，試圖瞞騙銀行和財務機構的人臉識別系統；更分享業界可透過不同技術偵測假冒網站，以及強化認識客戶（Know Your Customer，KYC）與身份認證的流程，防止騙徒有機可乘。

警方表示，會因應騙徒的行騙手法和技術的改變，和銀行業界相關持份者保持密切信息交流和協作，提升銀行業界的防範能力。

◆香港文匯報記者 蕭景源

專家倡用政府「智方便+」雙重核實

專家之言

香港警方首次發現有騙徒利用人工智能換臉技術，向金融機構進行詐騙，顯示騙徒的詐騙「能力」又再提升，令市民防不勝防。香港資訊科技商會榮譽會長方保僑昨日在接受香港文匯報訪問時亦指出，隨着科技日益發達進一步便利市民生活，但同時亦增加了騙徒可乘之機，建議金融機構須在進行身份認證時加多一層程序，甚至同時倚靠特區政府的「智方便+」作雙重核實，以提高對市民和機構本身的保障。

方保僑表示，若僅靠一張身份的資料和身份證上的小小黑白照片，騙徒難以成功透過人臉識別「過關」，「但當掌握了身份證上的名字等資料，自然有機會找到事主的社交媒體並獲取其照片等，再冒認身份開戶口。」

他指出，目前的「深偽技術」已非常先進，可以憑照片和影片學習事主的容顏，再將之套落騙徒上，「今次騙徒利用人工智能換臉程式試了約20次就成功了一次，比率很高呢！就算1萬次中一次都有問題啦，何況二十中一？」

籲身份認證加多一層程序

所謂「道高一尺、魔高一丈」，方保僑認為，現時騙徒隨時僅靠WhatsApp、WeChat和FaceTime等就可以盜取用家身份冒認，故建議金融機構應在進行身份認證時加多一層程序，「例如除了要求認證者扭一扭頭外，也要求對方用手觸摸胸前；要求提供住址的同時也應一併要求提供任職的公司等更多資料，令騙徒有更大機會『穿崩』。」他同時建議可一併倚靠「智方便+」作雙重核實。

◆香港文匯報記者 費小燁

助洗黑錢集團清洗4.7億 458人被捕

香港文匯報訊（記者 蕭景源）洗黑錢集團收買傀儡戶口收取和轉移騙案，令網上騙案更猖獗。警方財富情報及調查科由本月7日至23日，統籌展開代號「雋語」行動打擊洗黑錢，17日內出動2,880名警員，搜查全港400個住宅和商業大廈處所，共拘捕458人，包括3個犯罪團夥。他們涉嫌透過銀行戶口、儲值支付工具等不同金融工具，清洗最少314宗本地或海外各類騙案贓款，涉款4.7億元。

行動中被捕的330男128女年齡介乎15歲至82歲，包括423名本地人、18名內地人和17名非華裔人士，主要為傀儡戶口持有人，分別涉及串謀洗黑錢、洗黑錢等罪名。

與被捕人有關的314宗罪案多為騙案，包括投資騙案、求職騙案、網購騙案、網上情緣騙案等，其中損失金額最大一宗案件，為去年4月至9月，多達32名受害人接獲自稱虛擬貨幣投資專家來電，誘使他們參與高回報投資。受害人合共匯款3,368萬元至多個傀儡戶口，但其後未能取回款項，警方至今已就案件拘捕8人。

在其中一個代號「義門」行動中，警方於本月7日拘捕一名洗黑錢集團骨幹和7名傀儡戶口持有人，檢獲大批銀行文件、提款卡、手提電話、電腦和約32萬元現金，成功搗破洗黑錢集團。他們涉嫌以300元至1,500元誘使他人賣出銀行戶口，並在去年10月至今年6月期間，以現金提取及買賣加密貨幣方式，清洗1.1億元黑錢。

本月14日至16日，警方又搗破另一個黑社會操控的洗黑錢集團。該集團由2020年1月至今年2月期間操控傀儡戶口，收受逾2.1億元非法賭注，其中一個戶口涉及網購本地酒店度假套票騙案，案中40名受害人共損失9萬元。本月23日，警方拘捕了洗黑錢集團兩名主腦，涉替賣淫集團清洗逾2,200萬元犯罪得益。

虛擬銀行戶口洗黑錢案有上升趨勢

財富情報及調查科高級警司呂智豪昨日表示，警方留意到利用虛擬銀行戶口洗黑錢案有上升趨勢，相信與市民只需要有手機和身份證，便可在短時間內開設不同虛擬銀行賬戶有關。

部分被捕人為騙案受害人

他指出，是次行動中部分被捕人本身亦是騙案受害人，分別因誤信網上情人、虛假僱主招聘廣告等而交出其個人網上銀行登入密碼，甚至將個人銀行卡寄往海外給犯罪集團犯案。有被捕人則被利誘協助領取銀行現金回贈，誘使他們交出身份證及手機自拍相，暗中利用他們資料開設虛擬銀行戶口清洗黑錢。

警方在過去半個月的「反洗黑錢宣傳月」，透過一系列宣傳活動、社區教育和執法工作，提醒市民唔賣、唔租和唔借，保護個人戶口和密碼，防範戶口被利用洗黑錢罪行。

◆警方總結「雋語」反洗黑錢行動成果。 香港文匯報記者劉友光 攝