深偽高層指令匯款 呃走跨國公司兩億

騙徒「AI換臉變聲」開視像會議騙過港分部 職員向總部查詢始知大鑊

人工智能「深度偽造」技術被用來行騙，詐騙集團向一間跨國公司的香港分公司下手食「大茶飯」。詐騙集團事先在網上搜集該公司英國總部一眾高層的面部和聲音數據，透過深偽技術將騙徒換上多名公司高層的面貌和聲音，再按劇本預製「高層發言」短片，繼而以總部首席財務官名義發出釣魚信息，邀請香港公司職員參加線上「視像會議」，聽取「機密交易」匯款指令。由於與會高層都被集體「變臉」，「熟口熟面」加上聲音都似，令香港職員不虞有詐，遂按「最高指示」分多次將合共兩億港元轉賬至5個本地銀行戶口，直至日前向總部查詢始知受騙。這是本港首宗AI「多人變臉」騙案例，也是迄今損失最大的「變臉」案例。

◆香港文匯報記者 曾立本

據香港警方案情透露，被騙的是一間總部設在英國的跨國公司，在香港設有分公司。警方相信，騙徒在設置AI「變臉」騙局前，可能用「釣魚」軟件或其他網上途徑，掌握到公司內部人員架構及運作模式等資料，然後設計好行騙劇本，令受害人以為是日常商業操作。

騙徒疑摸透內部資料 準備「面具」劇本

騙徒在搜集了該公司英國高層在YouTube上公開的影像後，再利用人工智能「深度偽造」技術製造，給騙徒換上英國高層的面部和聲音。據悉，騙徒為防露出破綻，平日與香港分公司有密切工作關係的總部首席財務官面部和聲線「深偽」得仿真度頗高。今年1月中，涉案騙徒以「英國總部首席財務官」的名義，向香港分公司的財務職員發信息，聲稱公司要進行一項「機密交易」，邀請香港職員登入網上多人視像會議「開會」。視像會議的畫面上有4名至6名英國總部高層人員，包括眾人熟悉的英國總部首席財務官，其他高層也「熟口熟面」。

會議期間，該「英國總部首席財務官」要求香港分公司職員簡短自我介紹，接着其他高層簡短「討論」公司的交易決策，着「首席財務官」跟進香港分公司匯款事宜。香港職員見眾高層與真人「一模一樣」，故不虞有詐。其後，該「總部首席財務官」透過即時通訊軟件向香港分公司財務職員下達轉款指示，一星期內分15次，將合共兩億港元存入5個本地銀行戶口，作為「機密交易」資金。

「最高指示」掩飾單向播片 避免互動穿幫

今年1月底，香港公司財務職員向公司總部查詢時始揭發被騙。香港警方經深入調查，發現這次AI「變臉」有幾個特點：

一、為令受害人更加相信，騙徒用「深偽技術」偽冒多人多角色臉譜；

二、騙徒用真人換上英國高層的面部和聲音後，實際上他們在視像上的發言，是根據按事前寫好的講稿拍攝的預製片段，故會議上不能與香港職員有對話互動，即不給香港職員提問機會；

三、為免露出破綻，「視像會議」在短短數分鐘內結束；

四、所謂總部高層現身直接下指令，只是要給香港公司職員營造一個「最高指示」的場景，令職員深信是真實決策。

網絡安全及科技罪案調查科網絡安全組署理高級警司陳純青表示，利用人工智能「深度偽造」的欺詐手法，與傳統詐騙手法其實如出一轍，只是利用不同手段以取得受害人信任進行詐騙，最終目的主要是誘騙受害人將款項轉賬到騙徒指定戶口。

他強調，雖然科技發展一日千里，只要市民時刻保持警惕，養成一個高防騙意識的習慣，對任何社交平台或通訊軟件所收到信息，也要有一個查證真偽的意識及必須要有行動，謹記在人工智能「深偽技術」下，網上已經「眼見不一定為實，有圖有片亦不一定是真相」。

◆特首李家超及Tesla行政總裁馬斯克亦遭「盜臉」。

模擬「深偽」會議：如何發現破綻

香港文匯報訊(記者 曾立本)為讓市民進一步了解「深度偽造」多人視像會議騙局，網絡安全及科技罪案調查科網絡安全組高級督察陳智穎昨日在記者會上模擬騙徒「深偽」多人視像會議手法進行解說。

首先，熒光幕上分別播出由署理高級警司陳純青及自己「做主角」的一段錄播影片，影片內容是兩人以英文說出提醒市民提防騙案等相關呼籲。

熒光幕接着再播出一段3人視像會議的影片，影片顯示與會者分別為陳純青、陳智穎及一名警員，但陳純青及陳智穎的影像與較早前播出的屬同一條影片，在經過人工智能「深度偽造」配上偽冒聲音後再用於視像會議上。

兩人所說內容即變成要求與會者提供個人敏感資料等，驟眼看去不易察覺有異。陳智穎指出，人工智能「深偽技術」並非毫無破綻，並提供了防騙貼士(**見表**)。

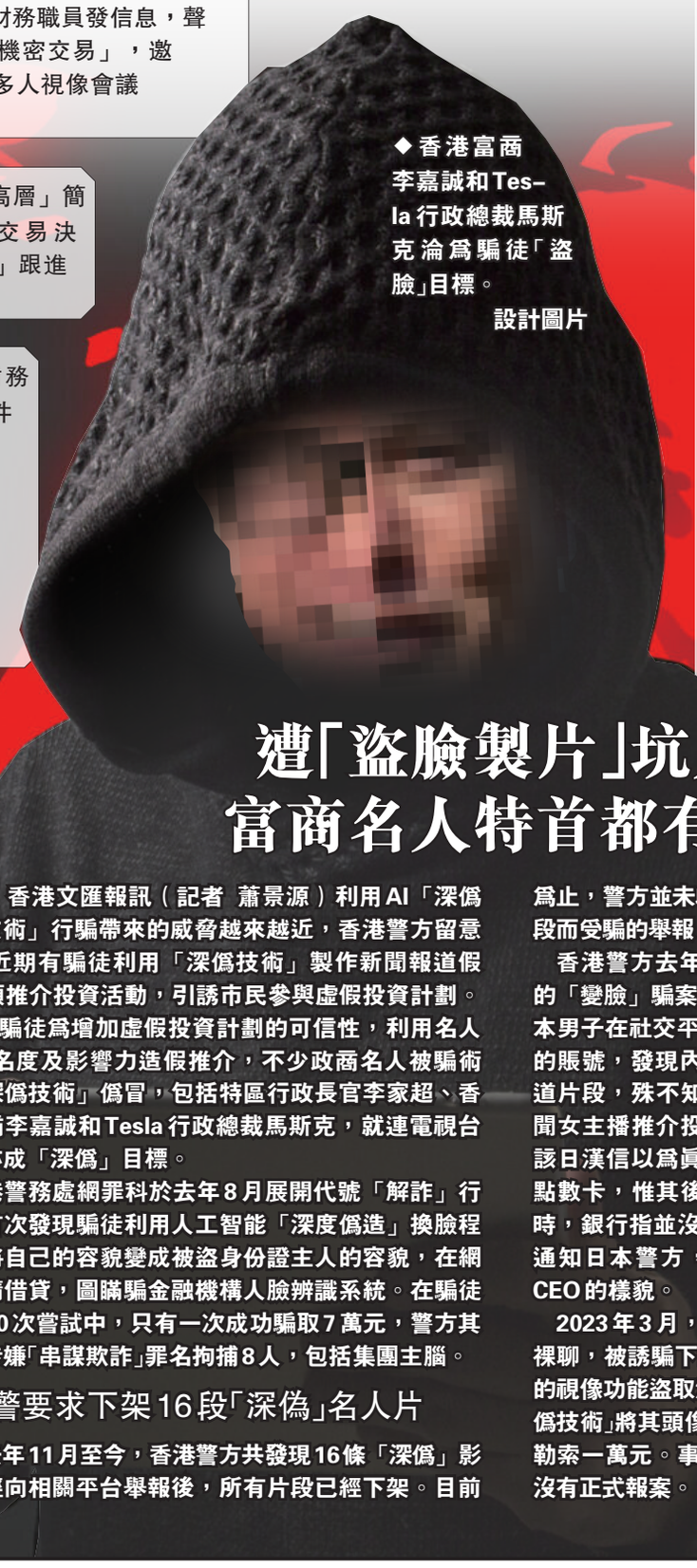
◆警方拆解騙徒利用深偽技術偽冒知名人士的行騙手法。 香港文匯報記者曾立本 攝

預防「深度偽造」騙局貼士

1. 要求對方在鏡頭前做指定動作，留意對方在熒光幕上影像有否變異，以測試是否利用人工智能技術假冒他人樣貌；
2. 當對電話或視頻上的親友有懷疑，嘗試提問以測試對方身份眞偽，例如問該名親友背景等問題；
3. 提高防範意識，切勿輕易提供人臉、指紋等生物辨識資料，以免騙徒利用犯案；
4. 當親友及公司職員在視頻或錄音中提出匯款要求時，要提高警惕，必須致電或從其他渠道一再核實；
5. 避免接聽陌生視像通話來電，以防騙案或騙徒盜取肖像利用來犯案；
6. 如有懷疑，可在「防騙視伏器」輸入電話號碼、社交媒體帳號、收款賬號等評估風險，或致電18222查詢。

跨國公司被騙兩億港元經過

1. 騙徒搜集了該跨國公司英國高層在YouTube上公開的影像後，再利用人工智能「深度偽造」技術製造，給騙徒換上英國高層的面部和聲音
2. 騙徒以「英國總部首席財務官」的名義，向香港分公司的財務職員發信息，聲稱公司要進行一項「機密交易」，邀請香港職員登入網上多人視像會議「開會」
3. 會議期間，各「高層」簡短「討論」公司的交易決策，着「首席財務官」跟進香港分公司匯款事宜
4. 該「總部首席財務官」透過即時通訊軟件向香港分公司財務職員下達轉款指示，一星期內分15次，將合共兩億港元存入5個本地銀行戶口，作為「機密交易」資金
5. 香港分公司日前向總部查詢方知受騙


◆香港富商李嘉誠和Tesla行政總裁馬斯克淪爲騙徒「盜臉」目標。 設計圖片

遭「盜臉製片」坑人 富商名人特首都有份

香港文匯報訊（記者 蕭景源）利用AI「深僞技術」行騙帶來的威脅越來越近，香港警方留意到近期有騙徒利用「深僞技術」製作新聞報道假視頻推介投資活動，引誘市民參與虛假投資計劃。這些騙徒爲增加虛假投資計劃的可信性，利用名人的知名度及影響力造假推介，不少政商名人被騙術用「深僞技術」僞冒，包括特區行政長官李家超、香港富商李嘉誠和Tesla行政總裁馬斯克，就連電視台主播亦成「深僞」目標。

香港警務處網罪科於去年8月展開代號「解詐」行動，首次發現騙徒利用人工智能「深度僞造」換臉程式，將自己的容貌變成被盜身份證主人的容貌，在網上申請借貸，圖瞞騙金融機構人臉辨識系統。在騙徒最少20次嘗試中，只有一次成功騙取7萬元，警方其後以涉嫌「串謀欺詐」罪名拘捕8人，包括集團主腦。

警要求下架16段「深偽」名人片

由去年11月至今，香港警方共發現16條「深僞」影片，經向相關平台舉報後，所有片段已經下架。目前爲止，警方並未收到市民直接因爲相關片段而受騙的舉報。

香港警方去年又收到兩宗涉及香港元素的「變臉」騙案查詢。2023年5月，一名日本男子在社交平台瀏覽到一名香港銀行CEO的賬號，發現內有關於在香港投資的新聞報道片段，殊不知是騙徒以「深僞技術」製造新聞女主播推介投資項目及專訪CEO的報道。該日漢信以爲眞，最終被騙購買1,570港元的點數卡，惟其後致電到涉案銀行尋找該名CEO時，銀行指並沒有此人。該日漢和銀行都將事件通知日本警方，得知騙徒是盜用了另一間銀行CEO的樣貌。

2023年3月，一名25歲香港男子在交友平台玩裸聊，被誘騙下載不知名手機程式。騙徒透過程式的視像功能盜取港男的樣貌及手機電話簿，再以「深僞技術」將其頭像移花接木到色情影片，然後向事主勒索一萬元。事主拒絕付款，但僅通知了警方，但沒有正式報案。

「深偽技術」如何以假亂真


1)高級督察陳智穎在原來影片主要呼籲市民提防騙案。


2)經「深偽技術」「改造」後，高級督察陳智穎在視像會議上說話內容變成要求與會者提供個人資料。

難用眼耳察覺瑕疵 「AI偵測AI」辨七成眞假

專家之言

「深偽技術」急速發展對維護網絡安全帶來挑戰。近年，具備高速運算能力的圖像處理晶片的普及和人工智能演算法不斷改進，一般家用電腦甚至手機也可憑一張相片或一段聲帶製作出幾可亂眞的「深偽」視頻或音頻。「科技罪案警政顧問小組」成員、香港專業進修學校協理副校長林森指出，「深偽」內容帶來最大的挑戰是難以利用肉眼和耳朵識別。雖然人工智能生成的影像或許仍有瑕疵，例如光線和陰影可能不太自然，影像邊緣模糊，但當大部分公眾以細小的手機熒幕觀看影像時，這些細節便不易被察覺。

技術門檻不斷降低 騙徒湧現

林森表示，隨着人工智能生成引擎的種類愈來愈多，「深偽技術」持續進化，辨別真偽的難度也會越來越大，加上該技術門檻不斷降低，將誘使更多不法分子利用「深偽技術」進行詐騙、發布失實資訊、製造社會輿論等。事實上，外國也陸續出現利用「深偽」聲頻和視頻進行詐騙的個案。

面對「深偽技術」的威脅，業界已積極着手應對，其中一種策略是研究以人工智能偵測「深偽」，即「以AI偵測AI」，通過分析不同媒體信號及相關雜訊的特點和分布來判斷真假，在特定測試場景已可達至七成或更高準確率，具體例子如Deepware及Validsoft等服務。內地如百度旗下的「度小滿」也提供防「深偽」的技術和方案。另一策略是用特定技術在發放的媒體中加入可供驗證的元素，使當該媒體被用於「深偽」時可輕易識別，具體例子如數碼水印技術和區塊鏈技術。另外也有業界或不同持份者組成聯盟如 DeepTrust Alliance 來共同應對「深偽」。

歐趕緊立法 港宜速引新技術防騙

除了技術層面外，在法律及監管層面來應對以「深偽技術」為代表的人工智能風險的工作亦已展開。歐洲議會、歐洲理事會和歐盟委員會早前已就《人工智能法案》達成協議，並即將成為全球首部人工智能監管法規，其中規定必須清楚標籤人工智能生成的內容，供應商亦須把有關內容標記為機器可閱讀的格式以便被自動偵測。內地去年下半年也推出了《生成式人工智能服務管理暫行辦法》，規範內地生成式人工智能產業發展方向。

林森認為，香港應盡快制定法例及守則規範企業與研究人員發展和應用人工智能，包括提升使用生成式內容的透明度，以防止有關技術被用作不法活動。在法例尚未制訂之前，本地跟內地應更積極展開「官產學研用」(政府、生產、學習、科研、應用)的合作，善用內地技術及人才優勢，加快先進技術的引入和落地，為應對未來人工智能等新技術帶來的挑戰做好準備，以及進一步利用人工智能打擊各類新型罪案。

◆香港文匯報記者 蕭景源

港科技罪案續飆升 大公司遭「釣魚」掠近八千萬

香港文匯報訊（記者 曾立本）香港警方最新資料顯示，去年1月至11月本港的整體科技罪案數字錄得31,843宗及損失50.9億元，較前年同期20,796宗及損失29.6億元，分別上升了53%及72%。去年損失最大一宗科技罪案涉及電郵騙案，受害人為一間國際資產管理公司，被騙徒冒認生意夥伴發電郵要求轉賬，於兩個月內被騙走7,820萬港元。

網上投資騙案是科技罪案「重災區」，去年1月至11月錄得4,703宗及損失30億元，較前年同期1,680宗及損失8.5億元，分別上升180%及254%。其中一名73歲退休婦，被男網友誘騙到虛假網上平台投資內地股票，7個月內被騙走2,800萬元。

去年11月26日開始，香港警方「防騙視伏器」與「轉數快」系統聯網，增加「可疑識別代號警示」新功能。所有為個人用戶提供以轉數快識別代號作即時轉賬服務的轉數快參與機構，包括44家銀行及儲值支付工具營運商，在該警示機制下，如收款人的轉數快識別代號資料，與「防騙視伏器」標記為紅色「高危有伏」胎合，手機熒幕就會出現警示短語。

此機制將於今年首兩季進一步覆蓋至其他轉賬機制，包括實體銀行、虛擬銀行、PayMe及Alipay等，屆時市民在銀行櫃台、ATM機或網上等不同系統轉賬過數時，都會受到「防騙視伏器」警示保護。