

深偽變臉換聲全球蔓延 港設防騙刑警未雨綢繆

警方教絕招：叫對方鏡頭前動手指搖頭便顯破綻

網絡騙案防不勝防，「有圖有真相」已成過去，接下來即將面臨「有影片也難有真相」的挑戰。AI人工智能「換臉」、「換聲」的「深偽技術」開始運用於詐騙，正在全球迅速蔓延，香港今年以來也收到兩宗涉及AI詐騙的查詢。儘管因技術和成本等原因尚未成為詐騙案的主要類型，香港警方仍提醒，隨著AI技術日趨成熟，市民應及早提高防範意識。警方日前講解和分析「深偽技術」騙局的趨勢及現存的「穿煲」弱點，建議市民可叫對方在鏡頭前做指定動作來識破「真人假象」，同時提醒市民避免接聽陌生人的視像電話，保護好個人臉部、聲音等生物特徵信息，免被騙徒收集成數據用來「換臉」、「換聲」造假行騙。

◆香港文匯報記者 廖傑堯



▲警方示範AI「變臉」，當模擬頭像（右）側面時會露出破綻，面部輪廓較為模糊。



◀測試AI「變臉」可叫對方用手指橫過面前，如果像右邊畫面出現模糊的影像便要小心。

香港文匯報記者廖傑堯 攝



◆網罪科網絡安全組警司陳純青（中）帶同4名「防騙刑警」講解日新月異的詐騙手法及預防知識。

利用人工智能(AI)技術生成的deepfake(深度偽造技術)，是透過人工智能作深度學習的方法，模擬特定對象的多角度面部特徵和聲音，製成高仿真的模擬聲響，有海外個案顯示此技術被騙徒利用來行騙。

四督察首次出任「防騙刑警」

香港警方網絡安全及科技罪案調查科首次委任4名警務督察作為「防騙刑警」，包括高級督察吳柏慧、高級督察陳智穎、高級督察張文瀚及督察梁珮筠，日前向香港文匯報等媒體分享包括AI「深偽技術」在內的科技罪案趨勢和手法以及有效防騙策略。

目前香港警方尚未接獲涉人工智能詐騙案的舉報，但警方獲悉有兩宗涉及香港元素的個案查詢。今年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，殊不知是騙徒以深偽技術製造新聞女主播推介投資項目及專訪CEO的報道。日漢信以為真，最終被騙購買1,570港元的點數卡，他其後致電到涉案銀行尋找該名CEO，該銀行指並沒有此人，男子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。

今年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「深偽技術」將其頭像移花接木到色情影片，然後向事主勒索1萬元。事主拒絕付款，但他只是通知警方，沒有正式報案。因此，香港警方暫時未有接到利用「深偽技術」實施詐騙的報案。

至於早前內地有報道指有科技公司老板被AI偽術騙去數百萬元，國家反詐中心已澄清沒有相關案件舉報。不過，近期以「深偽技術」進行實時「換臉」、「換聲」的騙案再度成為網民熱搜對象。

眨眼視線變化等易露破綻

警方分析指，理論上AI「深偽技術」也可使用在網戀騙案、電郵騙案、釣魚騙案中。現階段，騙徒通常需要收集大量被模擬對象的原始影像及語音數據，才



◆騙徒利用AI「深偽技術」製造假新聞，詭稱香港銀行有賺錢投資計劃。

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，加上現時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的動作會較不自然，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。

警方日前向記者演示利用人工智能「變臉」的手法，以數星期時間搜集及模擬到的一名警司臉部資料，將其套用在另一人身上並作實時視像聊天，可見因數據不完善，畫面中被偽冒人物的眼神、口型出現不協調，臉部邊緣線不自然。

手指動作變得模糊和遲滯

警方指出，要特別留意手指在鏡頭擺動的動作，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，便可看出上述破綻，即可判定這可能是一個假影像。

根據警方了解，現時騙徒使用的所謂「變臉」片段，都是騙徒預先製作，並且透過視像的通訊播放，為免「夜長夢多」露出破綻，往往只會播放數秒鐘，便會以不同借口結束視像聊天，然後返回傳統的詐騙「劇本」，用即時通訊軟件繼續行騙。

警方指出，利用「深偽技術」做視像電話，其實都是增加受害人信任度的一個行騙手段，無論人工智能發展到何地步，只不過是其中一個接觸受害人的手段，整體行騙套路與傳統的手法大致相同。不過，科技發展一日千里，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，有圖並不一定為真相」。

警方提醒

樣貌聲音慎上載 可疑App勿下載

香港文匯報訊（記者 蕭景源）利用「深偽技術」的偽造影片需要大量的影片，作為人工智能學習的模本來建構高仿真度的模型，故其質素取決於收集影片的數量及製造影片的硬件先進程度。一般情況下，警方相信騙徒較難向普通市民收集大量的影像及聲音，但在科技不斷發展下，不能一概而論斷定犯罪分子不能做到，所以市民在公眾平台上載自己樣貌、聲音時，要有所警惕，應保護好個人生物信息特徵。

勿接陌生視像電話

據警方了解，騙徒會以不同手段，在社交平台公開的影像中盜取冒充對象的聲音、臉部信息等，提醒市民切勿輕易提供人臉、指紋等生物信息辨識資料，避免接聽陌生人打來的視像電話，以免聲紋和臉部特徵被盜取。日前警方在偵破裸聊詐騙集團時，也提醒市民切勿下載不明來歷的App，因為有些App會要求受騙人同意使用其手

機相簿內圖片和影片的使用授權，有可能被騙徒盜取電話簿內親友的个人影像等資料，用來偽造假象在受害人親友間行騙，故市民應拒絕開放使用授權。

警方提醒市民，無論騙徒使用何種手法，市民任何情況下都應緊記查證對方的身份。警方在網上發現虛假資料或影片時，會主動要求網上平台將虛假資料下架，市民也要避免轉載假資料和假影像。根據紀錄，香港發生的騙案繼續攀升，今年首5個月共錄得15,792宗，較去年同期的9,988宗上升近58%，損失金額則高達21.1億元，即平均每日損失1,300萬元，每10分鐘便發生1宗騙案。

不過，警方今年的騙案破案率亦有提升，至今共拘捕1,739人。警方將在今年7月和8月「防騙季」加強宣傳，並舉辦「大灣區青少年人工智能及網絡安全挑戰賽」，提升青少年的數碼素養和網絡安全意識。

「深偽」採樣要多 名人紅星易中招

香港文匯報訊（記者 蕭景源）AI科技日趨成熟和普及，由於「深偽技術」須收集大量被模擬對象的原始影像及語音數據，才能達到理想的偽造效果，故此騙徒絞盡腦汁打造幾可亂真的「犯案工具」犯案。一些經常曝光的公眾人物或明星首當其衝成為受害者，如在內地早前便有騙徒以AI變臉變聲的「深偽技術」，將直播間推銷員搖身變成「楊冪」、「楊穎」、「迪麗熱巴」等女星帶貨，推高銷量，有詐騙之嫌。

本港有「廟街歌王」之稱的男歌手尹光，近期亦被人以AI製造「翻唱」歌曲在YouTube頻道播放。尹光早前向傳媒表示，聽過由AI模仿自己聲音唱出林家謙、姜濤等的歌曲後，「覺得好笑，都唱得好似，不過與自己真人唱肯定有分別。」

歐美騙案佔比飆升

至於在歐美等發達國家，近年涉及「深偽技術」的詐騙案不斷上升。今年5月，有網絡公司發布多國首季涉及「深偽技術」的詐騙案比例的統計數據顯示，與去年同期相比，美國已從0.2%上升到2.6%，加拿大則從0.1%飆升到4.6%。而在英國、德國、意大利等的「深偽技術」詐騙案所佔比例都超過了5%。

今年3月在加拿大，當地便有一對夫婦接獲騙徒利用AI模仿其兒子的聲音來電，被騙2.1萬加元（約12萬港元）。

據悉，騙徒是在電話上利用以AI合成其兒子的「聲線」致電該對夫婦，詭稱因駕車撞死一名美國外交官，現身處監獄，急需金錢支付律師費。數小時後，騙徒又再伴稱是其兒子的代表律師致電，聲稱開庭前需要2.1萬加元。

有香港資訊科技專家表示，隨著AI科技和工具的不斷進步，「變臉」、「變聲」的製作成本逐漸降低。內地早前便有不法分子指只需3.5萬元人民幣，就可以買張「明星臉」，30分鐘便可將訓練好的AI模型送到買家手上。

不過，專家則對此說法有所保留，因為AI的「深偽技術」製作均需專業的硬件，以及運算需時，短時間內完成，本身肯定已是「詐騙」。

專家不排除日後科技發展，「變聲」、「變臉」的電腦案將會增加，市民須提高警覺。但從現時的程度看來，技術仍有不少缺陷，例如聲音會較「生硬」及「粗糙」，市民若收到懷疑是模擬家屬的聲線電話時，應保持冷靜，可先嘗試聯絡當事人，以確認對方的現況，切勿輕易將金錢轉給別人。

預防AI詐騙小貼士

資料來源：警務處 整理：香港文匯報記者 蕭景源

◆在視像對話中要求對方在鏡頭前做指定動作

◆向對方提問，測試對方身份真偽

◆切勿輕易提供人臉、指紋、聲音等生物辨識信息

◆若有「親友」在視頻或錄音中提出匯款要求，要特別警惕

◆避免接聽陌生人的視像通話來電

◆不要輕易相信網上資訊

◆養成事實查證習慣

◆如懷疑文字或圖片被竄改，可試用搜尋器查出處

◆多從不同媒體查找資訊，以多角度查找真相

◆在解讀「消息指」、「已Fact Check」等訊息時應保持懷疑態度

◆如懷疑是假資訊，應避免轉載，並向有關機構查詢

◆撥打防騙易18222熱線或使用防騙視伏器App，留意警方最新防騙消息