網上晒照隨時被盜 冒充身份欺詐親友

AI催生新騙案 偷聲換臉不勝防

焦點追蹤

ChatGPT方興未艾，「AI孫燕姿」剛剛爆火，就在世人迎來「AI元年」之時，AI換臉這種新型騙術已經悄然出現。近日內蒙古包頭警方公布，一男士遭遇騙子AI換臉冒充好友，結果10分鐘淺聊，就被騙走430萬元（人民幣，下同）。騙術之新、數額之巨，以及防不勝防的狀況，都讓人瞠目結舌。有專家提醒公眾，盡量不要在公開平台大量晒出個人照片和視頻，以免給犯罪分子盜用冒充身份。

大公報記者 張寶峰北京報道

▶有網民戲將影星周潤發的臉換到其他演員臉上。

在包頭案中，受害人郭先生的好友突然通過微信視頻聯繫他，稱自己的朋友在外地競標，需要430萬元保證金，想借用郭先生公司的賬戶轉賬。基於對好友的信任，加上已經視頻聊天「核實」了身份，郭先生在10分鐘內，先後分兩筆把430萬元轉到了對方的銀行賬戶上。然而事後，郭先生撥打好友電話才得知被騙。原來騙子通過AI換臉和擬聲技術，佯裝好友對其實施詐騙。「當時是給我打了視頻的，我在視頻中也確認了面孔和聲音，所以才放鬆了戒備。」郭先生事後說。

肆虐全球 上當比率近100%

事實上，郭先生的遭遇並非個案，從中國內地到歐美各國，形形色色的AI換臉騙案紛紛出現，且不少都是如郭先生案例般涉及上百萬巨額的詐騙案例。今年5月，湖北網警巡查執法發布消息稱，AI技術改變了詐騙手段，而新騙局來襲後，詐騙成功率竟接近100%。

據了解，在AI換臉的騙局中，犯罪分子會先以各種手段套取擬冒充對象的聲音、臉容資料作為合成的素材，如通過騷擾電話錄音等來提取某人聲音，又或是在社交平台上獲取公開的相片，甚至是直接駭入冒充對象的手機或社交賬號。除了事先製作AI換臉視頻播放，有的軟件還可以實時捕捉替換人臉，並且直接接替攝像頭，讓騙徒透過視頻聊天獲取受害人信任，實施詐騙。

▲郭先生向包頭警方致送錦旗，感謝警方幫助討回騙款。

在有效監管尚未及時跟進的背景下，各種圍繞AI技術帶來的新問題甚至犯罪行為，已經成為業內外不得不正視的熱點話題。清華大學人工智能研究院等部門發布的《深度合成十大趨勢報告（2022）》顯示，創作者在互聯網平台中發布的深度合成內容的數量高速增長，以視頻為例，2021年新發布的深度合成視頻的數量，較2017年已增長10倍以上。

專家：遠程轉賬務必多重驗證

對此，中國互聯網協會發出公告提示，伴隨着深度合成技術的開放開源，深度合成產品和服務逐漸增多，利用AI換臉、換聲等虛假音視頻進行詐騙、誹謗的違法行為屢見不鮮。

為了保護好自己的「錢袋子」，用戶在進行遠程轉賬務時，必須進行多重驗證。如果有人自稱家人、朋友、老師、領導以各種方式和理由誘導你轉賬匯款，務必第一時間提高警惕。

北京民商事律師李斌25日則對大公報表示，其實公眾更應該將這種保護與防範前置化，也就是保管好自己的圖像和視頻。比如，盡量不要在公開平台大量晒出個人照片和視頻，以免給犯罪分子以可乘之機。另外，在社會上辦理業務或者拍攝照片、視頻時，一定要注意及時收回或徹底刪除底版，以免被他人濫用。

觀言察色 分辨AI「換裝術」

原圖

AI生成

- 臉上有模糊的痕跡
- 多數AI假臉是用睜眼照片合成，極少甚至不會眨眼
- 畫面停頓或變色
- 情緒和臉部表情不符
- 語音和口部動作不協調

大公報記者張寶峰整理

▶不少賣貨直播主都以AI換成當紅明星臉。圖為AI將Angelababy的臉（左）換成迪麗熱巴。

「AI換臉視頻套餐」月費僅1萬元

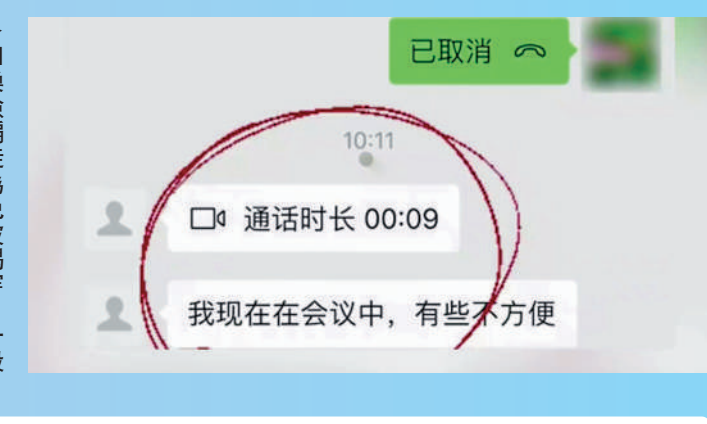
成行成市

近日，不少網友反映，無意間點開某直播間，發現賣貨的竟然是「迪麗熱巴」「楊冪」等當紅明星。但仔細觀察才發現，原來這些所謂的「明星」只不過是商家普通主播的「AI換臉術」。而就在商家以此為噱頭吸引消費者，公眾也權當笑話並不在意之時，這背後的各種法律風險其實已經迫近眼前。

據了解，現在甚至有商家推出「AI換臉視頻」套餐，售價為每月1萬元。一家出售「AI換臉特效插件」的商家對媒體表示，軟件售價數百元，對電腦配置有一定要求，購買後，使用者只需更換素材照片，軟件就能自己運行完成「換臉」。這款軟件不僅能對圖片進行換臉，也能在視頻上換臉。

實際上，AI換臉技術並非是近期才興起。早在2017年，一位名為DeepFake的網友將情色電影中的女主角換臉成荷里活明星蓋爾・加朵，這也是AI換臉技術首次出現在公眾視野當中。後來由於大量投訴者表示不滿，其賬號被官方封禁。此後的AI換臉技術則以他的名字命名為「DeepFake」。

而在內地，2019年初，一段通過AI技術將《射鵰英雄傳》中黃蓉扮演者朱茵的臉替換為楊冪的視頻在網絡上熱傳，成為內地使用AI進行影視劇二創的開端，也帶出了AI是否會侵犯肖像版權的問題。



▶AI換臉騙徒為免被揭穿，一般與受害人視頻通話短時間就藉故轉為文字溝通。

揭秘AI換臉騙術

1.篩選目標
- 騙子首先分析公眾發布在網上的信息，根據所要實施的騙術，通過AI技術篩選目標人群

2.截取聲畫
- 騙子通過盜號或社交平台公開的相片、視頻等提取冒充對象的聲音、人臉素材

3.網聊欺詐
- 騙子利用素材合成聲音、AI換臉，在視頻通話中利用假聲假臉騙取信任，實施騙局

多地AI詐騙案例

冒充友人詐騙

近期，包頭市公安局電信網絡犯罪偵查局發布一起AI電信詐騙案，不法分子利用AI換臉、合成聲音，以視頻通話冒充被害人親友聯繫被害人，博取被害人信任後實施詐騙。

不雅視頻勒索

2021年，浙江溫州公安曾發布消息稱，受害人小陳在與女網友視頻聊天後，被對方利用AI換臉技術，將小陳視頻中的面部合成到不雅視頻中，藉此對其實施勒索。

▲ **散播恐慌造市**

5月22日，一張由AI生成的五角大樓附近地區發生爆炸的圖片（上圖）在社交網絡上瘋傳，推文稱五角大樓附近地區發生了爆炸，造成金融市場恐慌，美股一度下挫，金價和美債攀升。

偷聲音盜存款

最近英國一位能源公司CEO在不知情的情況下被騙子以AI合成了他的聲音，並用這段聲音電話轉賬了22萬英鎊到騙子自己在匈牙利的賬戶，後來本人才發現這宗騙局。

大公報記者張寶峰整理

法律利劍阻嚇 算法模型堵漏

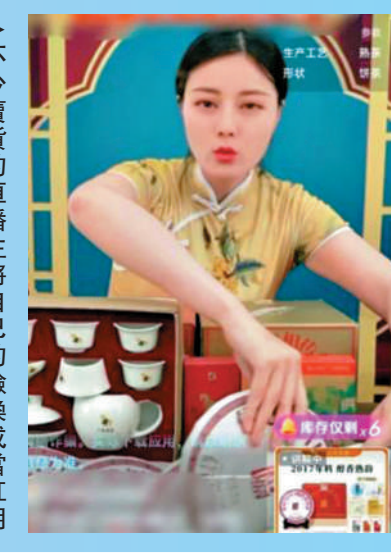
專家建言

面對「AI換臉」新型詐騙的出現，北京民商事律師李斌25日對大公報說，針對AI換臉案中的情形，現在的民法、刑法都有相應的法律，可以作為維權依據，因此，一旦遭遇類似騙局，人們一定要及時拿起法律武器。

「換臉直播用於公開傳播可能涉嫌侵犯他人的肖像權。如果涉及直播帶貨等商業行為，會成為加重情節。」北京岳成律師事務所高級合夥人岳屾山對媒體分析說，只要未經肖像權人同意，在直播中通過技術手段把自己的臉換成了別人的臉，就是對肖像的侵權。只是根據不同情況，承擔的後果可能不同而已。

去年12月發布的《互聯網信息服務深度合成管理規定》曾明確規定：深度合成服務提供者對使用其服務生成或編輯的信息內容，應當添加不影響使用的標識。提供智能對話、合成人聲、人臉生成、沉浸式擬真場景等生成或者顯著改變信息內容功能的服務的，應當進行顯著標識，避免公眾混淆或者誤認。

「伴隨應用場景日益廣泛以及使用頻次快速增長，人工智能安全風險發生的範圍和可能性持續提高。」清華大學人工智能研究院名譽院長張鈸近日亦公開表示，從長遠看，人工智能安全問題需要從算法模型原理上尋找突破口。



▶不少賣貨的直播主將自己的臉換成當紅明星。

社區網購群埋伏 盜頭像竊語音

猝不及防

雖然近期曝光的AI換臉罪案中，騙徒瞄準的都是上萬甚至上百萬的大額錢財，但也有騙徒進行「惡作劇」式的小騙局。北京女孩郭蕊蕾前段時間就險些中招。

▲目前市面上充斥了大量AI換臉的應用程式。

「當時，一個網購群中突然有人向我發起視頻通話。接通後，竟然是拉自己進群的鄰居。」小郭對大公報說，「當時我沒有多想，但對方讓我充購物卡的時候，我就留了一個心眼，心想對方為什麼不直接私信我，而是在群裏打電話，這就很奇怪。」

後來，見小郭很猶豫，對方也直接承認了是一齣「惡作劇」。原來對方在跟小郭鄰居視頻時，截取了對方的頭像和語音資料，又用「AI換臉」軟件嘗試向社區購物群中的熟人推薦購物卡。「雖然當時沒有中招，但我覺得還是非常危險。」小郭說，如果是年長的人，或者疏忽大意的狀態，很容易被「熟臉」引上鉤。

針對此次引發公眾高度關注的AI換臉詐騙案，中國互聯網協會表示，在AI時代，文字、聲音、圖像和視頻都有可能是深度合成的，在轉賬匯款、資金往來這樣的典型場景，要通過回撥對方手機號等額外通信方式核實確認，不要僅憑單一溝通渠道未經核實就直接轉賬匯款，無論對方是誰。