帶動旅遊及經濟列審批準則 每年支持最多10項目
文藝盛事基金引入績效指標 刊A2

港商：數字化綠色化成產業升級大方向
53家灣區企業供應鏈科創成果吸睛 刊A4

刀郎廈門演唱會引發中國文化共鳴
兩岸歌迷齊喊「兩岸一家親」 刊A13

文匯報 WEN WEI PO www.wenweipo.com
政府指定刊登有關法律廣告之刊物
獲特許可在全國各地發行
2024年12月 1 星期日
甲辰年十一月初一 初六大雪
天晴乾燥 早上清涼
氣溫17-22℃ 濕度50-80%
港字第27270 今日出紙1疊4張半 港售10元

扮上司把聲呃錢 騙徒潛入群組「狩獵」

市民爆險中招經過 專家：疑「白撞」致電蒐聲用AI模擬

人工智能（AI）科技應用愈趨普及，但亦成為騙徒詐騙新手法，騙徒以AI模擬假扮對象的聲音甚至合成影像行騙，冒充對象以往多為知名人士，現在漸連普通市民也成受害者。有市民日前便遭騙徒假扮其頂頭上司意圖行騙，其聲線與口音均與上司相似，首通電話只相約傾談工作，未提及金錢，令他最初不以為意，惟對方其後着他代為轉數支付費用，他即時感到懷疑，向直屬上級查問上司手機號碼並致電查證後證實對方為騙徒，最終未有上當。有網絡專家提醒，騙徒可透過不斷「白撞」致電偷錄聲音，或入侵其通訊軟件盜取語音檔案，經AI解讀分析後，就可以從聲音樣本模擬發聲，模仿聲調詐騙。 ●香港文匯報記者 劉明

◀今年2月3日警方聯同學者召開記者會提醒市民提防涉及人工智能「深度偽造」科技罪案。 資料圖片

市民劉先生對香港文匯報表示，他上周五（11月29日）近傍晚6時接獲一通以手機程式WhatsApp致電的電話。對方以其上司身份約翌日早上到其辦公室傾談，「他叫得出我的名字，聲線同口音都似新任上司，而且他只約我傾談，未有提及金錢問題，我以為他是只想向前線人員了解工作情況，當時未有懷疑。」

潛通訊群獲公司信息扮「新上司」

劉先生翌日上午返回公司途中再次接到對方來電。騙徒初時稱正在辦公室內與他人處理事務，着其暫不用到其辦公室，事後會致電聯絡他。騙徒未幾再致電，聲稱要付款給兩名為其辦事的人員，但對方不收現金，要求劉先生代其先過數給對方。

劉先生即時感到懷疑，表示沒有使用轉數快和PayMe等支付工具，只有提款卡。對方着他到銀行櫃員機取款，屆時給他銀行賬戶號碼以過數，「有人不收現金已覺得有問題，更離譜是騙徒問我櫃員機可以撳到多少錢，連支付他人金額也說不出，更加深我的懷疑，我隨口說可墊支數千元，對方表示沒有問題。」

開口叫過數惹疑 事主查核識破

由於他未有儲存新上司手機號碼，但想起上司應加入WhatsApp內的工作群組，登入核對發現群組內沒有騙徒的手機號碼，只有一個標示英文名的電話。他致電直屬上級詢問該英文名是否新任上司，確認後致電上司查問，對方斷言之前致電劉先生的「絕對是假冒」。

騙徒不久再致電查問劉先生是否已在櫃員機取錢，劉先生訛稱未取錢，詢查其銀行賬戶號碼，但對方只着他先取錢，其後再致電查問，「我想知他的賬戶號碼，話一時撳錯密碼被『食卡』，叫他先給我賬戶號碼，待我聯絡其他同事過數，但他仍未肯提供有關資料。」

對方其後多次致電詢問，劉先生表示可到其辦公室面談，對方即時表示辦公室內有其他人商談事務，暫不方便，「他怕我到上司辦公室就會穿崩，不知謊言其實已被戳穿。」騙徒其後仍再次致電，「我話未搵到人過數，他即稱兩名為其處理事務的人仍在辦公室，遲遲未收到款項已不耐煩。」

同日中午12時許，騙徒第八通電話致電劉先生，「他語氣變差，追問到底能否將錢過給他，我問他全名，他應知道我懷疑他，憤怒地說：『你是什麼意思？要幫就幫，唔幫就算』，跟着掛斷電話。」

突擊回電 騙徒來不及變聲穿崩

劉先生憶述，騙徒聲線口音與上司十分相似。為核實對方身份，劉先生相隔大半天突擊致電騙徒，懷疑對方措手不及，未有開啟「變聲」系統，聲線與之前扮「上司」完全不同，更沒有鄉音。劉先生即問對方是否早上致電給他的上司，「對方先愣一愣，然後才說『是』。我問他為何聲音與之前不同，他未有回應，然後掛線，未知聲音不同是否來不及用AI扮聲。」

「騙徒或者入侵同事手機，在群組內找到我電話號碼等資料，對方聲線與上司相似，亦有可能利用AI扮聲，之前有立法會議員遭AI合成照勒索，亦有議員被騙徒以AI技術扮聲借錢，相信這類騙案會愈來愈多。」劉先生說。

●圖為今年8月，私隱專員鍾麗玲拍攝短片示範透過深偽技術實時換臉。 資料圖片

「高仿」親友語音行騙 對象「平民化」

話你知

AI模仿他人「假聲」電騙案在世界各地頻生，連普通人亦成為目標。早前，加拿大有騙徒致電一對夫婦，利用AI模仿其兒子聲音，稱在外闖禍，急需金錢支付律師費，成功騙取夫婦2.1萬加元（約12萬港元）。

台灣地區早前亦破獲首宗結合AI語音機械人行騙的詐騙集團，部分被假扮的對象是普通人，最少40名受害人報警，合共損失1億元新台幣（約2,527萬港元），其中一名六旬婦人被騙金額最高，達2,300萬元新台幣（約581萬港元）。

香港特區立法會勞工界議員周小松前日在社交平台發文，指有不法之徒懷疑利用AI模仿他的聲音，致電一名相熟的工會分會理事長誘騙轉賬，導致對方失財4萬至5萬元。他事後表示回想事件都覺得恐怖，提醒市民遇到匯款要求時，切記應仔細核對對方的身份。

上網慎防「盜臉偷聲」 警方：增宣傳教路護私隱

香港文匯報訊（記者 蕭景源）人工智能（AI）日趨普及，有騙徒利用人工智能「深度偽造」（Deepfake），以「換臉變聲」進行詐騙，全球都面對「有片有聲未必有真相」的嚴峻挑戰。由於能夠產生圖文、聲音、視頻的「生成式人工智能」，其一系列演算需要搜集足夠的數據，包括臉部和聲音的重要參數，市民保護好個人臉部、聲音等生物特徵信息變得至為重要，香港警方和私隱專員公署都加強宣傳教育，提醒市民在使用社交平台或通訊軟件時，採取保護措施築起第一道「防火牆」，慎防被騙徒「偷臉偷聲」。

生成式AI技術能模擬特定對象的多角度面部特徵和聲音，製成高仿真的模擬影聲，有海外個案顯示此技術被騙徒利用來行騙須收集大量被模擬對象的原始影像及語音數據，才能達至理想的偽造效果。不過，隨着科技的發展，不法分子用此製造深偽影聲來行騙的成本不斷降低。針對發現或接獲舉報「深偽」片段，警方自2023年11月1日起開始立項統計，至2024年5月31日，警方發現及接獲舉報共21條假冒政府官員或知名人士的深偽片段，其中兩宗由偵查發現，19宗為市民舉報，相關片段已在網上下架。

「扮官扮高層」技術成熟 已釀巨額騙案

今年1月底，警方接獲一宗「深偽技術」欺詐案。報案人收到假冒其英國總公司首席財務官的釣魚信息，聲稱要進行機密交易，邀請報案人進行多人視像會議，警方相信騙徒先下載被偽冒職員的網上公開影片及聲音，再利用深偽技術製作預錄的視像會議，因是預錄影片，騙徒和報案人並無互動，向報案人下達指示後便掛線，再以即時通訊軟件繼續指示轉賬。報案人按指示授權轉賬，損失約兩億港元。

◀早前網絡出現「AI馬斯克」偽造影像介紹投資計劃騙案。 香港警察Fb圖片

今年5月20日，有跨國貿易公司職員收到偽冒其英國總公司首席財務官的WhatsApp信息，並進行近30分鐘的視像會議，其間「假上司」指示職員轉賬近400萬港元。調查相信疑犯以網上公開資料作素材，配合深偽技術將影片內容篡改，再於視像會議中播放，以誘騙受害人進行轉賬。上述兩案均在調查中。

針對個人資料的保護，警方和私隱專員公署透過多方面的宣傳及教育工作，以推廣及提升個人資料保障的意識。其中私隱專員公署單是今年上半年，已收到近600宗有關套取市民個人資料作詐騙用途的查詢，較去年同期312宗大幅上升近九成。

公署今年初對28間機構使用AI的情況完成循規審查，未有發現違規情況，並出版了《人工智能（AI）：個人資料保障模範框架》協助機構利用AI時遵從《私隱條例》的相關規定等。

市民若懷疑個人資料被外洩，可向私隱專員公署（個人資料防騙熱線：3423 6611、電郵：communications@pcpd.org.hk）作出查詢或投訴。市民若發現其個人資料被盜用並涉及刑事罪行，亦應盡快報警。

慎防「深偽」換臉變聲詐騙貼士

- 盡量減少在社交媒體平台及即時通訊軟件分享個人生物辨識資料，包括正面照及影片，並檢視預設保安及私隱設定
- 切勿隨意點擊或掃描可疑的超連結及二維碼，不要登入可疑網站
- 避免接聽陌生視像通話來電
- 若有「親友」在視頻或錄音中提出匯款要求，要特別警惕
- 若來電者以視像形式通話，即使能道出你的個人資料，若有懷疑應先以其他聯絡方式查證來電者眞偽
- 在視像對話中要求對方在鏡頭前做指定動作，觀察影像是否有異樣
- 向來電者提問，測試對方身份眞偽
- 養成事實查證習慣，多從不同媒體查找資訊，以多角度查找眞相
- 如懷疑文字或圖片被竄改或屬假資訊，應避免轉載，並向事實查證機構查詢
- 不時查看網上銀行個人賬戶及個人電郵有否不尋常登入紀錄
- 撥打防騙易18222熱線或使用「防騙視伏器」App，留意警方最新的防騙消息

資料來源：香港警務處/ 私隱專員公署

整理：香港文匯報記者 蕭景源

網絡社交少用語音 免手機被黑「失聲」

專家之言

過往的AI電騙個案，大多模仿公眾人物說話，以「假聲」設局詐騙親友，或借用公眾人物威望博取公眾課金投資，較少扮普通人敲詐，但隨着科技發達，網絡上的隻言片語累積起來已夠AI系統活靈活現模仿普通人，外國已有不少類似例子。有專家建議市民切勿在社交平台披露個人資料，在使用即時通訊系統時減少傳送語音，以免手機被入侵遭偷聲模仿，更重要的是提防陌生人來電。

劉先生是次遇到AI電騙，而其上司非公眾人物，亦沒有公開視頻或語音資料，何以AI能扮得到？有網絡專家表示，騙徒偷錄目標對象的手法層出不窮，可透過不斷「白撞」致電收錄聲音，或入侵其通訊軟件盜取語音檔案，經AI解讀分析後，就可以從聲音樣本模擬發聲，模仿聲調詐騙。

有專家直言，騙徒利用事主「怕老闆」、服從權威等心理，即使「假聲」非百分百相似，事主往往不敢當面質疑其身份，就容易瞞天過海。

香港信息安全學院院長、智慧城市聯盟資訊科技管理委員會主席龐博文昨日在接受香港文匯報訪問時坦言，「網絡世界不會失憶，時間一長，大部分人其實都會不知不覺在網上留下大量個人信息，騙徒只要具備一定網絡專業知識，收集某個人的個人資料其實很容易。」

騙徒下一步會設定對答劇本，設計扮演的身份，並在暗網購買所需聲音語音包或視頻工具，「現在暗網世界可以很易購買行騙所需的各項技術支持。」騙徒通常以很熟悉的語氣在電話中直接說：「我換了現在的號碼，以後打這電話，明天來我辦公室一趟……」等。

多問幾句出破綻 涉錢應當面確認

騙徒雖利用AI高科技設置騙局，但並非無懈可擊。龐博文說：「只要保持警覺性，高科技騙局也有漏洞，如AI聊天機器人雖然可以用很逼真的聲音和形象按劇本對話，但只要事主多問幾句，騙徒就很難如正常人那樣對答如流。加上騙徒取得的人物背景資料畢竟有限，對話多了，往往會發現牛頭不搭馬嘴。」

他強調最重要的是，涉及金錢交易時必須當面確認，「要意識到電話和網絡可以偽裝任何人，還是真人當面交易最安全。」

●香港文匯報記者 王僖

督印：香港文匯報有限公司地址：香港仔田灣海旁道7號興偉中心2-4樓 電話：28738288 傳真：28730657 採訪部：28738260 傳真：28731451 發行中心：28739889 廣告部：28739888 傳真：28730009 承印：三友印務有限公司 地址：香港仔田灣海旁道7號興偉中心2-3樓