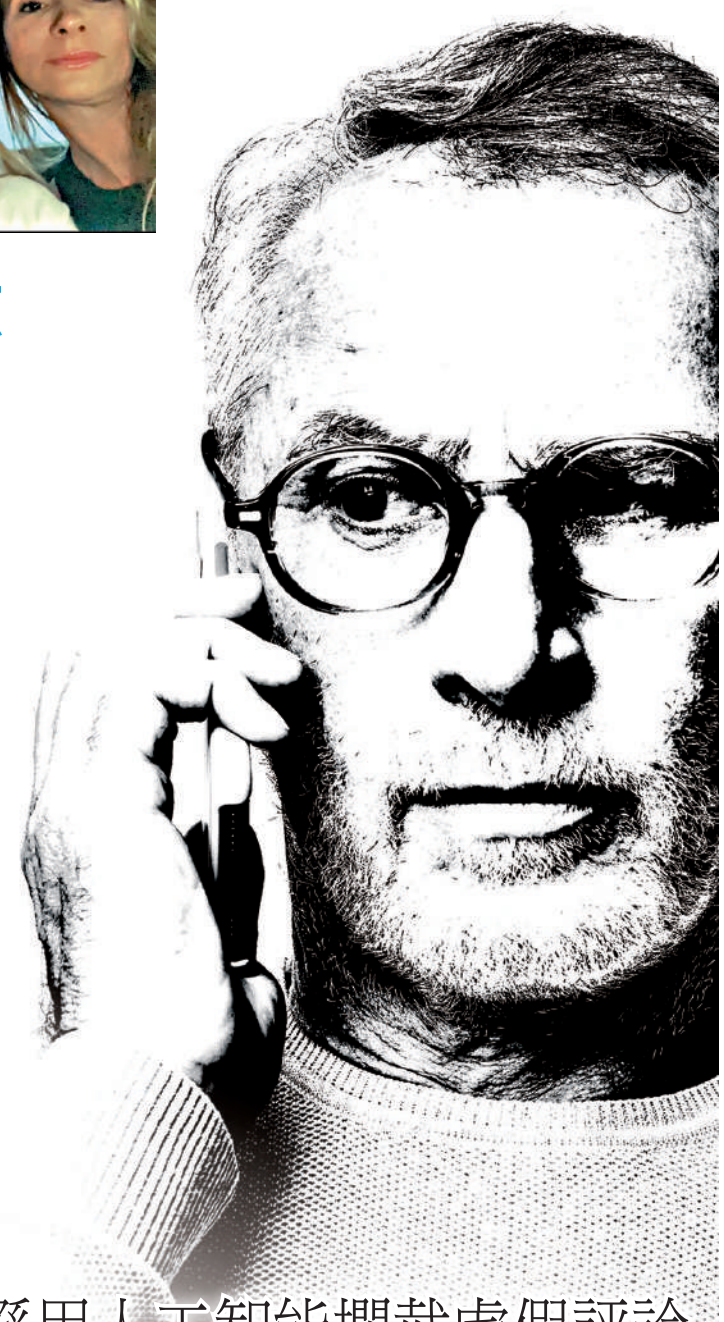
千奇百趣

【大公報訊】綜合法新社、CNN報道：人工智能技術不斷更新，網絡詐騙案的手段也花樣百出。美國有騙徒使用網絡上幾可亂真的人工智能（AI）語音克隆工具，假冒受害者親朋好友騙錢。根據聯邦貿易委員會的數據，去年，美國人在冒名頂替詐騙中損失26億美元（約202.8億港元）。專家表示，AI對人類最大的威脅，是模糊了真實和虛構的界線，讓詐騙犯利用廉價又有效的AI技術來散播假信息。

◀德斯特凡諾（右）接到語音克隆電話，騙徒聲稱綁架了她的大女兒（左）。 網絡圖片

美國每年冒名頂替騙案損失逾200億

AI語音以假亂真 電話詐騙更猖獗



AI普及後，電信詐騙犯只需要在網上下載一個免費AI軟件，再利用某人幾秒鐘的聲音樣本，就能創造新的對白。總部位於美國的McAfee Labs上個月發布報告，在一項針對美國等九個國家共7000人的全球調查中，四分之一的人表示，他們自己或身邊的人經歷過AI語音克隆騙局。70%的受訪者表示，他們不確定自己能否「分辨出克隆聲音和真實聲音之間的區別」。

Blackbird.AI行政總裁哈立德表示：「AI語音克隆現在與真實人聲幾乎無法區分，這讓騙徒能夠更有效地從受害者那裏獲取信息和資金。」哈立德說，通過一個簡短的音頻樣本，AI可以生成語音文本、郵件，甚至可以製作實時語音轉換器，詐騙者可以使用不同的口音、性別，模仿受害者親屬的說話方式，創造出令人深信不疑的假音頻。

美國聯邦調查局（FBI）特工約翰遜表示，美國家庭平均在每次虛假綁架騙局中損失11000美元（約8.58萬港元）。根據聯邦貿易委員會的數據，去年，美國人在冒名頂替詐騙中損失26億美元（約202.8億港元）。

哭泣聲與女兒一模一樣

1月20日下午，住在亞利桑那州的母親德斯特凡諾接到一通陌生來電，德斯特凡諾本想掛斷，但一想到15歲的大女兒布麗安娜正在進行滑雪比賽訓練，德斯特凡諾不由擔心女兒是否出了意外，她接起電話，電話那頭傳來尖叫和哭泣聲，「媽媽！幫幫我！」德斯特凡諾後來接受採訪時回憶，她當時十分確信電話那頭是女兒的聲音，女孩連哭泣的音調都與布麗安娜一模一樣，「我沒有一秒懷疑。」

電話那頭很快傳來詐騙者的聲音，對方聲稱綁架了布麗安娜，要求德斯特凡諾支付100萬美元贖金。德斯特凡諾手足無措，試圖說服對方降低贖金金額，並讓一旁的小女兒打給與布麗安娜一起前往滑雪場的父親，但父女兩人一直杳無音信。好在旁邊的路人幫忙打電話報警，警方獲悉後判斷德斯特凡諾遭遇詐騙，布麗安娜也在數分鐘後打電話向母親報平安，這才讓德斯特凡諾免於錢財損失。

幾秒聲音樣本即可克隆

美國聯邦官員表示，諸如此類的冒名頂替騙局已經存在多年，騙徒青睞聯繫受害者的祖父母等親人，謊稱他們的孩子出事，藉此詐騙錢財，綁架者通常會使用通用的尖叫錄音。但官員警告說，AI普及後，此類騙案正變得越來越難識破，因騙徒能夠輕而易舉克隆聲音，並創造「對白」。

加州大學伯克萊分校計算機科學教授法里德表示，AI在詐騙者手中被武器化，「一段不到一分鐘的音頻，就能創建一個相當完整的克隆語音，有些人甚至說只需幾秒鐘就足夠了。」法里德補充說，在AI軟件的幫助下，每月只需5美元就能輕鬆實現語音克隆。不過，法里德指出，據他所知當前版本的AI軟件無法通過克隆聲音來表達各種情緒，但不能完全排除已經出現更先進的技術。

今年早些時候，AI創業公司ElevenLabs承認，其語音克隆工具可能被濫用於「惡意目的」。此前，有用戶利用該公司的軟件發布了一段演員艾瑪華森閱讀希特勒自傳《我的奮鬥》的深度偽造音頻。

風險投資公司Team8技術總監霍赫伯格說，人們很快無法再相信網絡上所見的一切，需要有新的技術來幫助確認網絡對面的到底是不是自己認識的人。

AI監管的五大主要挑戰

明確AI定義

- 歐洲議會花費兩年時間才敲定人工智能（AI）的明確定義，即可以「根據一組給定的人類定義目標，生成影響他們與之交互的環境的產品，例如內容、預測、建議或決策」的軟件。歐洲議會本周正在就AI法案進行投票，這是首個關於AI的法律規則。

達成全球協議

- AI的影響超越國界，但迄今仍未建立起一個全球性的AI監管機構。歐盟擬對AI實施的監管最為嚴格，包括對AI產品進行分級；英國正在將AI監管納入現有機構；美國只要求開發商自願規範行為。

確保公眾信任

- AI在某種程度上可以改善人類的生活，例如幫助解決氣候變化等問題。但AI也會助長犯罪，歐洲議會希望公眾了解每種AI產品的風險，違反規定的公司或被處以3000萬歐元或全球年營業額6%的罰款。

誰來決定規則

- 專家指出，如果AI公司過度參與制定規則，可能會將利益擺在第一位，重要的是不僅要傾聽企業的聲音，還要讓民間社會、學術界以及受AI影響的人們參與進來。

迅速採取行動

- ChatGPT六個月前才開始公開使用，現在已經能撰寫論文並通過專業考試，AI技術正在以驚人的速度發展。歐盟技術負責人維斯塔格表示，AI法案至少要到2025年才會生效，已經太遲。

來源：BBC

AI詐騙形式及防範

主要形式

- 騙徒可以通過錄音來提取某人的聲音，主要的手法是撥打騷擾電話，在獲得一定的「聲源」後，將聲音進行合成，進而形成「對白」。
- 騙徒會通過安裝語音文件或特定插件等方式，實現語音轉發功能。在盜取賬號後，騙子可能會轉發號主之前的聊天語音，向其好友騙錢。
- 人臉往往更容易騙取受害人的信任，騙子通過AI換臉技術，偽裝成和受害人有親密關係的人的面部，通過視頻博取受害人信任。

- 騙徒會通過AI分析公眾發布在網上的各類信息，鎖定目標群體後根據其個人特點制定詐騙話術，例如向經常發布理財分析的人實施金融詐騙。

防範措施

- 如果有人自稱熟人，通過社交軟件、短訊以各種理由誘導匯款，務必要通過回撥對方手機號、見面等渠道核驗對方身份。
- 不輕易提供人臉、指紋等個人生物信息給他人，不點擊陌生鏈接，不下載陌生軟件，不要隨便添加陌生好友，防止手機、電腦中病毒。
- 牢記執法機關沒有安全賬戶，警察不會網上辦案，如果有自稱警察的人員來電，讓對方聯繫警署或撥打報警電話。

大公報整理

亞馬遜用人工智能攔截虛假評論

【大公報訊】據BBC報道：電商巨頭亞馬遜（Amazon）表示，該公司正在使用最新的人工智能（AI）技術，識別並打擊虛假評論。

亞馬遜長年受到虛假評論困擾，評論者使用第三方平台購買、銷售和發表虛假評論。亞馬遜報告稱，2022年有超過2.3萬個社交媒體團體，它們擁有超過4600萬名成員和追隨者，製造了大量虛假評論。

虛假評論會影響顧客的消費決定，有人會付錢發表好評以提高賣家的評分，或抹黑競爭對手的公司。消費者組織「Which？」表示，在英國，約七分之一的在線評論是虛假的，該組織表示，虛假評論使消費者選擇劣質產品的可能性增加了一倍以上。

亞馬遜客戶信任團隊負責人梅塔近日表示，亞馬遜通過AI來搜尋可疑賬戶、追蹤留下評論的買家賬戶與賣家賬戶之間的關係、賬戶的評論歷史等，識別異常行為。梅塔說，通過將先進AI與審查手段相結合，亞馬遜可以在客戶看到虛假評論前予以攔截。

亞馬遜表示，AI去年已經幫助屏蔽了超過2億條可疑的虛假評論，並將「繼續構建保護客戶的複雜工具」，亞馬遜呼籲私營部門、消費者團體和政府之間進行更多合作，以使該戰略更加有效。亞馬遜最近對NiceRebate.com的運營商採取了法律行動，該網站是一家專門針對英國客戶的虛假評論中介。

▲亞馬遜利用AI識別假評論，圖為亞馬遜工人舉標語「我不是機器人」。 路透社

韓國擬將AI教科書引入中小學

【大公報訊】據韓聯社報道：韓國教育部8日表示，將於2025年開始在當地中小學引入AI數字教科書，以滿足多樣化的學習內容，計劃於2028年完成全學科、全年級覆蓋。

韓國教育部表示，從2025年起，小學三、四年級以及初高中新生將使用數學、英語、信息學的AI數字教科書，在之後數年將會逐漸擴大應用學科與年級。2028年，AI數字教科書將覆蓋除了音樂、藝術與體育等活動型學科外的所有中小學學科，並應用於小學二年級以上的所有中小學生。

AI數字教科書是韓國政府數字教育創新計劃的一部分，通過擴展元宇宙和交互型AI技術，為學生提供多樣化的學習內容。韓國教育部長李柱鎬表示，AI數字教科書可以根據不同學生的學習狀況，提供定製教育計劃，它能夠為「慢速學習者」推薦基本學習任務，例如明辨基本概念；為「快速學習者」推薦深度學習任務，例如論文寫作。

▲首爾展覽中心1月12日展出數字教科書。 網絡圖片

AI數字教科書還能為來自多元文化家庭的學生提供多語言的翻譯服務。韓國教育部的資料顯示，2021年，在韓國約580萬來自多元文化家庭的中小學生中，約有11.8%的學生對韓語課本存在理解困難。

韓國教育部相關負責人表示，AI數字教科書將與紙質教科書同時使用，直到「所有學生、家長和教師都能熟練使用」。