網絡騙案激增 全球年損7.8萬億

AI詐騙層出不窮 可用AI技術反制

網絡詐騙手法層出不窮，一年可能讓全球損失超過一萬億美元（約7.8萬億港元）。隨着人工智能（AI）技術發展，犯罪分子可進行「換臉」、克隆聲音等多種方式，製作逼真的合成視頻或音頻實施新型網絡詐騙，包括進行「殺豬盤」的網絡愛情騙局，讓人防不勝防。不過，AI技術也是雙刃劍，有英國電信公司近期推出一款聊天機器人，專門跟網絡騙徒對話，以子之矛，攻子之盾。所謂道高一尺魔高一丈，這恰好說明了AI技術可以成為打擊詐騙的工具，未來可能有助遏制詐騙。對於普通人來講，能夠做到的就是提高警惕，勿輕信網絡，輕易交心。

反詐剋星 英國「AI奶奶」上線

【大公報訊】綜合《紐約時報》、CBS報道：英國電信公司Virgin Media O2近期推出一款AI聊天機器人，取名「黛西」（Daisy），專門對付詐騙電話。「她」可以替用戶回覆可疑來電，通過答非所問、隨便亂聊等方式干擾騙徒，拖延其時間。

據介紹，「AI奶奶」基於大量真實詐騙電話的數據進行訓練，結合了多種AI模型，這些模型協同工作，以實現「即時偵聽」和「回應詐騙電話」。她的聲音模仿了某位工作人員的祖母，其形象則由AI生成。O2稱，「AI奶奶」一次通話最長可以達到40分鐘，在測試期間接聽了數周的電話，成功纏住了不少詐騙者。

在O2發布的官方演示視頻中，當騙子讓「AI奶奶」輸入網址時，她會裝作耳朵不太好，故意拼錯，騙子只能深呼吸，保持冷靜，再次重複正確的網址。「AI奶奶」還會「欺騙」騙子，稱網站顯示了自己養的貓咪，換來的是騙子破口大罵「別再叫我親愛的，你個蠢貨」。目前，這款AI機器人已接聽超過1000通詐騙電話，成功浪費騙徒數百個小時。

此外，澳洲麥考瑞大學網絡安全中心的達利・卡法爾和其團隊創建了名為Apate的AI反詐騙系統，包括多種不同口音和性格的聊天機器人，可以讓詐騙者在電話上停留更長時間並收集詐騙信息，其運作方式本質和「黛西」類似。

不過，考慮到詐騙電話的數量之多、範圍之廣，「AI奶奶」並不能完全「封鎖」騙徒。英國倫敦金斯頓大學犯罪學副教授卡特認為，「如果你接到詐騙電話，最好的方法就是不要接聽、掛斷電話並報警。」

如何用AI反制AI詐騙

AI機器人應對騙徒

- 英國電訊公司的「AI奶奶」黛西工作原理，就與早期版本的ChatGPT Voice相似。簡單來說，通過AI轉錄騙徒來電者的聲音，「AI奶奶」會根據預設角色性格來調整回答風格和內容，最後再次轉換成「奶奶」的聲線，與來電的騙徒溝通。

識別詐騙模式

- AI通過機器學習等方式，對大量的網絡詐騙進行分析，發現詐騙模式和行為，有效地防止詐騙活動。

加強身份認證

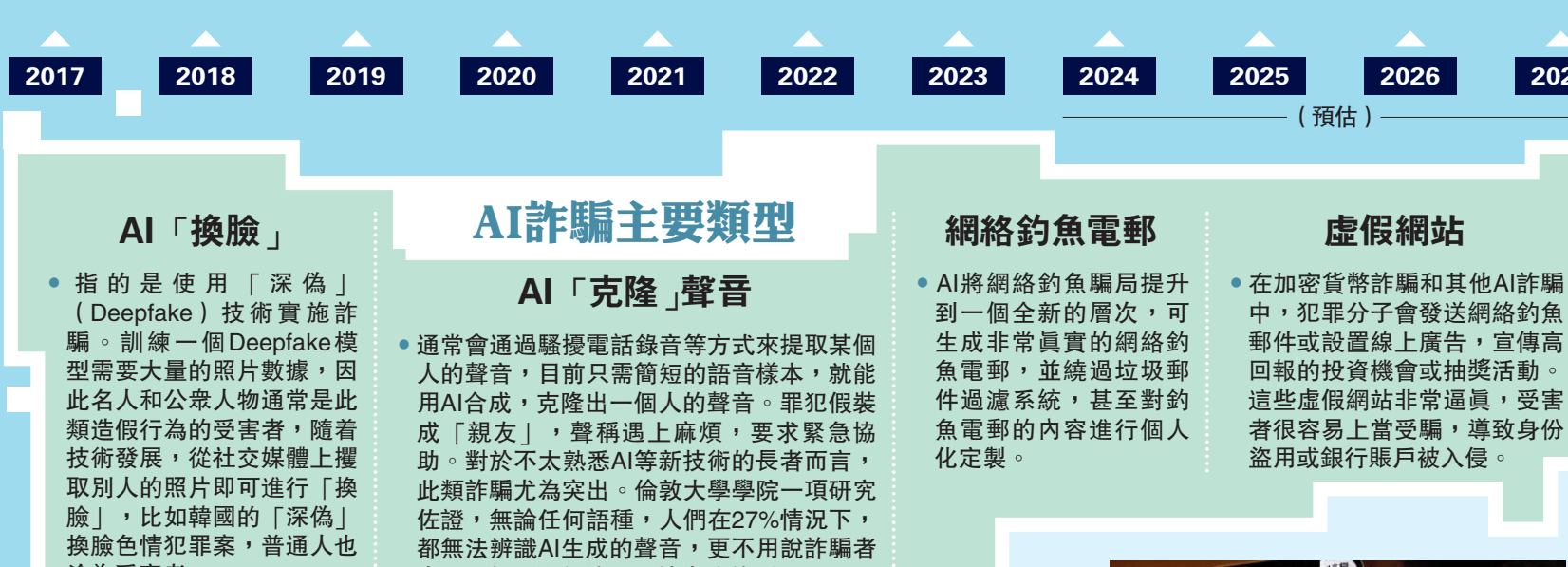
- AI應用於身份認證領域，通過分析用戶的行為、設備信息和生物特徵等數據，確保用戶的眞實身份，防止賬戶被盜用。

監控賬戶活動

- 通過即時監控銀行賬戶的交易數據，AI識別可能存在的詐騙風險，及時採取措施止損。

大公報整理

◀英國電信公司推出「AI奶奶」，反擊網絡詐騙。 網絡圖片



「AI馬斯克」虛假廣告 銀髮族損失慘重

▲YouTube上的「AI馬斯克」視頻，多用於網絡詐騙。 網絡圖片

【大公報訊】綜合《紐約時報》、CNBC報道：深度偽造（Deepfake）技術所製作的詐騙愈趨普遍，利用名人的肖像、聲音製作虛假廣告的情況嚴重。據美媒報道，世界首富、美國電動車特斯拉（Tesla）創辦人馬斯克已被AI換臉植入數千條虛假廣告，涉及數十億美元的詐騙，受害者多為長者，損失慘重。

報道稱，82歲的退休老人史蒂夫・博尚在去年年底看到一條視頻短片，影片中的「馬斯克」承諾會有「快速回報」的投資機會，博尚誤信了此虛假廣告，以248美元（約1928港元）開設賬戶，最終被騙取超過69萬美元（約536萬港元）的退休金。

62歲的醫護工作者海蒂・斯旺也在社交媒體上看到「馬斯克」的虛假廣告，信以為真並以1萬美元開設賬戶。斯旺接受採訪時表示，即便後來她意識到被騙，但視頻中的人仍然「十分像馬斯克，聽起來也像馬斯克」。

專門研究Deepfake的安全研究公司Sensity AI分析超過2000個深偽換臉的影片，發現馬斯克是最常被騙徒利用的名人。自去年年底，馬斯克出現在近四分之一的AI換臉詐騙視頻中，在加密貨幣投資廣告中，馬斯克的出現率更是高達90%。除馬斯克外，「股神」巴菲特和亞馬遜創辦人貝佐斯也頻繁出現。

報道稱，騙徒尤愛針對銀髮族，他們雖對加密貨幣、AI有所了解，但不熟悉安全的投資方式。據德勤金融服務中心估計，這類由AI支持的深度造假每年可能導致數十億美元的經濟損失。

AI詐騙主要類型

AI「換臉」

- 指的是使用「深偽」（Deepfake）技術實施詐騙。訓練一個Deepfake模型需要大量的照片數據，因此名人和公眾人物通常是此類造假行為的受害者，隨着技術發展，從社交媒體上攫取別人的照片即可進行「換臉」，比如韓國的「深偽」換臉色情犯罪案，普通人也淪為受害者。

AI「克隆」聲音

- 通常會通過騷擾電話錄音等方式來提取某個人的聲音，目前只需簡短的語音樣本，就能用AI合成，克隆出一個人的聲音。罪犯假裝成「親友」，聲稱遇上麻煩，要求緊急協助。對於不太熟悉AI等新技術的長者而言，此類詐騙尤為突出。倫敦大學學院一項研究佐證，無論任何語種，人們在27%情況下，都無法辨識AI生成的聲音，更不用說詐騙者會利用親屬關係博取同情實施詐騙。

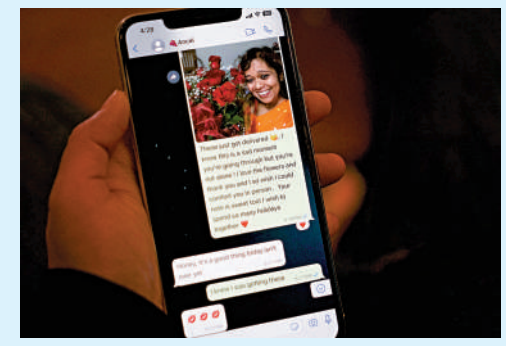
網絡釣魚電郵

- AI將網絡釣魚騙局提升到一個全新的層次，可生成非常眞實的網絡釣魚電郵，並繞過垃圾郵件過濾系統，甚至對釣魚電郵的內容進行個人化定製。

虛假網站

- 在加密貨幣詐騙和其他AI詐騙中，犯罪分子會發送網絡釣魚郵件或設置線上廣告，宣傳高回報的投資機會或抽獎活動。這些虛假網站非常逼眞，受害者很容易上當受騙，導致身份盜用或銀行賬戶被入侵。

「換臉」加ChatGPT 「殺豬盤」騙局更逼眞



▲不少「殺豬盤」騙案已經使用AI技術。圖為一名「殺豬盤」受害者展示與騙子的聊天截圖。 法新社

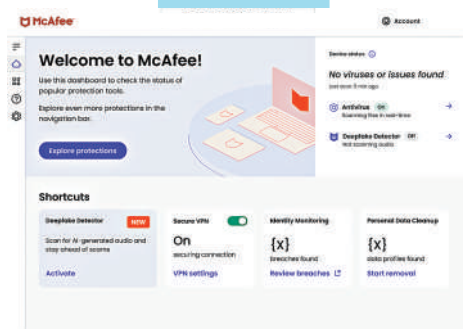
【大公報訊】綜合BBC、CNN報道：根據游說團體「全球反詐騙聯盟」資料，去年全球因網絡詐騙損失超過1萬億美元。越來越多的騙徒利用AI聊天機器人和AI換臉技術，實施「殺豬盤」（pig butchering）詐騙，讓網絡「愛情騙局」變得更逼真、更難識別，甚至可以跨國實施詐騙。

所謂「殺豬盤」，是一種精心設計的網絡騙局，指的是騙子會通過假裝朋友或戀人贏得受害者的信任，最終以投資或借貸的名義捲走大筆資金。過去，人們認為騙徒會「拒絕進行視頻通話」以免暴露身份，這一經驗如今面臨失效。詐騙者已可利用深偽（Deepfake）技術，在視頻中操縱面部表情和聲音音調，塑造「人設」，從而讓受害者更容易上鉤。過去，「殺豬盤」通常根據詳細的「劇本」工作，騙取受害者信任，現在他們還可以用ChatGPT等聊天機器人，撰寫更多的劇本、更容易打破語言障礙，進行跨國詐騙。

據BBC報道，77歲的妮基・麥克勞德便是在這樣的背景下，成為了一場精心策劃的「殺豬盤」受害者。在新冠疫情封鎖期間，因為孤獨，她在一個聊天群組中結識了一位名叫阿拉・摩根的人。摩根自稱在北海油井工作，並通過深偽技術製作她在石油鑽井平台上拍攝惡劣天氣的虛假視頻。麥克勞德對此深信不疑，最終被騙取超過1.7萬英鎊（約16.6萬港元）。

聯合國毒品和犯罪問題辦公室（UNODC）10月公布的一項報告指出，去年亞太地區的深偽詐騙事件增加了1530%；近半年的監測數據顯示，加密通訊軟件Telegram上，面向詐騙集團的深偽產品，增加了600%以上。

如何識別AI詐騙



▲網絡安全公司McAfee推出的深偽（Deepfake）檢測工具。 網絡圖片

識別「換聲」

語調情緒無起伏：

- AI克隆聲音中很難表達情感和情緒，可注意聲音是否有語調變化、情緒起伏等。

是否口齒不清：

- AI克隆聲音是通過在眞人語音樣本的基礎上訓練，但當樣本數據不夠多時，AI克隆聲音會出現口齒不清、單字發音錯誤等情況。

識別「換臉」

面部表情是否有異常：

- 眼球轉動不自然：AI換臉的深偽（Deepfake）仍未能準確地複製人類面部表情的自然細微差別，往往會在眼睛、鼻子等個別五官上出現畸變，可注意任何不自然的眼球運動，例如不穩定的抽搐或靜止不動。
- 臉部無法對齊：尤其是當視頻中的人轉頭或說話時，注意顴骨和下顎的變化。
- 臉部過於光滑：AI換臉很難模仿眞實的人類皮膚的質感，比如毛孔、皺紋等，可注意視頻中的人臉是否太光滑，或呈現出蠟質感。
- 實時視頻通話：可要求對方用手在攝像頭面前短暫停留，甚至揮手，可對AI換臉軟件進行干擾。

檢查嘴型：

- 注意口型與視頻是否存在延遲，或者所說的話與嘴唇動作不匹配。

使用AI檢測工具：

- 可利用AI檢測工具分析影片，如Deepware Scanner等，但此類工具並非百分百正確。

大公報整理