克隆意大利防長聲音成功詐騙企業家：AI深偽犯罪出現哪些新趨勢？｜Whatsnew

除財產詐騙外，AI深⿒技術也開始被廣泛用於虛假的政治宣傳、間諜活動等政治目的。

2019 2 12　　Reuters TV via Reuters/

國家領導人致電大企業家，請求他們提供數百萬美元，以解救被拘留在中東的公民。只不過，電話的另一頭不是真的政治家，而是詐騙犯——這個電影般的情節如今真的發生了。

2025年2月初，有詐騙分子用人工智能（AI）模擬意大利國防部長Guido Crosetto的聲音，詐騙了至少九位意大利最富有的企業家。接到詐騙電話的企業家包括時尚設計師Giorgio Armani、軍工集團Beretta家族，以及鞋業品牌Tod』s的董事長Diego Della Valle。其中，國際米蘭前主席Massimo Moratti向一個香港賬戶支付了約95萬歐元。這筆錢後來被意大利警方追回。

這類事件反映出「深⿒」（deep fake）詐騙方式愈發流行，且變得更加「高端」。

在AI助力下，「深⿒」技術讓詐騙犯罪變得觸手可及，成本更低，而且犯罪分子無需掌握計算機技術或編程知識，只需購買現成的成套軟件，就可以迅速發起大規模詐騙，並在瞬間抹去痕跡、消失無蹤。

南韓深偽色情群組引發社會強烈關注，深偽色情成困擾世界難題｜⋯

延伸閱讀 ⟶

詐騙分子會尋找已上傳至網絡的視頻，複製目標人物的說話方式。如今，只需十幾秒的檔案，人工智能便可以進行語音克隆。隨後，詐騙分子會給親朋好友打電話或發送語音郵件，要求他們緊急匯款。

這類騙局存在已久，如以前的「總裁騙局」——騙子假冒公司董事的身份，說服公司員工向一個假冒的賬戶轉賬。但隨着AI技術的進步，欺詐和⿒造的規模達到了前所未有的程度，可能引發的後果

也越來越令人擔憂。

德勤（Deloitte）金融服務中心預測，到2027年，生成式人工智能可能導致美國每年的欺詐損失達到400億美元，而2023年這一數字為123億美元。如真如此，這一「產業」的年均複合增長率將達到32%。

「新的生成式人工智能工具的廣泛可用性，使得深度⌧造視頻、虛假聲音和虛假文件對不法分子而言變得更加廉價且易於獲取。目前，暗網上已經形成了一個完整的詐騙軟件行業，這些軟件的售價從20美元到數千美元不等。這種惡意軟件的『民主化』正在削弱許多現有的反欺詐工具的有效性」，報告寫道。

根據《衛報》2024年9月的報道，數字貸款機構Starling Bank發布的研究發現，「28%的人在過去一年中至少遭遇過一次AI語音克隆詐騙。然而，46%的人甚至不知道有這種類型的騙局，另有8%的人表示，即使他們認為親人打來的電話似乎很奇怪，他們也可能會按照對方的要求匯款」。

2025 2 13 Tesla SpaceX Omar Sultan Al Olama
AI DOGE Amr Alfiky/Reuters/

除普通人外，跨國大企業也成了受害者。2024年1月，香港一家大型跨國公司的員工將公司的2600萬美元轉賬給了詐騙分子。根據警方的說法，該員工參加了一次視頻會議，而實際上，所有其他與會者都是由深⌧技術⌧造的。詐騙分子通過YouTube找到了公衆可以訪問的視頻和音頻，用人工智能模仿聲音，並篡改了談話內容和嘴脣動作。所有內容都是事先錄製好的。

法國政府反網絡詐騙平台Cybermalveillance.gouv.fr在2024年的一份報告裏指出，網絡釣魚（Phishing）仍然是個人、企業和政府機構的最大威脅。在2024年多倫多的一次會議上，Booking信息安全主管Marnie Wilking報告道：「在過去的一年半里，全球各行各業受到的攻擊，尤其是網絡釣魚攻擊，增加了500%到900%」。她同時指出，在ChatGPT推出後不久，即2022年底，網絡釣魚的情況就開始增多。通過使用AI工具，詐騙分子現在可以用多種語言工作，語法也比以前更好。

另一種在近年大幅增加的詐騙手法是「情感詐騙」（Romance Scam），又稱浪漫騙局或「殺豬盤」：騙子通過網絡接觸受害者，與其建立情感聯繫，最終騙取錢財。此外，犯罪團伙也開始⌧造視頻，聲稱掌握了受害者的不利信息，並以此對其進行勒索。

除財產詐騙外，AI深⌧技術也開始被廣泛用於虛假的政治宣傳、間諜活動等政治目的。

例如，2023年9月，意大利總理梅洛尼接到了自稱非洲聯盟委員會成員的來電。在對話中，她透露西方盟友已對烏克蘭問題感到「疲倦」，還談及自己與歐盟領導人在移民問題上的分歧。兩個月

後，她的通話內容的完整錄音被俄新社（Ria Novosti）公布。

全球首個人工智能監管峰會在英國召開，達成了什麼共識？｜⋯

延伸閱讀 →

事實上，梅洛尼通話的對象是通過「深⊠」技術⊠造聲音的兩名俄羅斯喜劇演員——Vovan和Lexus。這對搭檔此前已經成功戲弄過多位國際政要，包括德國前總理默克爾（Angela Merkel，梅克爾）、英國前首相約翰遜（Boris Johnson，強森）、法國前總統奧朗德（François Hollande）、土耳其總統埃爾多安（Recep Tayyip Erdogan）等。

2023年，俄羅斯發起「Doppelgänger」行動，利用⊠造網站和鏈接冒充政府機構及多家歐洲媒體的官方網站。點擊這些鏈接後，用戶會被引導至模仿原網站風格和視覺設計的虛假文章頁面，這些文章旨在宣傳俄羅斯，同時抹黑烏克蘭及其支持者。

2024年春季，Meta和OpenAI發現了一場由以色列政府策劃的宣傳行動：在X、Instagram和Facebook 上，數百個虛假賬戶發布的內容都是通過ChatGPT生成的。而在美國總統競選期間，一家由俄羅斯情報機構資助和操控的機構製作多個經過AI⊠造的視頻，並在網絡傳播。

法國《世界報》報道，在1月29日發布的一份報告中，Google指出，其生成式AI模型Gemini被多個外國機構使用，主要來自伊朗，但也包括中國和俄羅斯：「德黑蘭利用AI進行內容創作和操控，包括撰寫文本、以特定語調改寫文本以及優化文本以提高傳播效果，而北京和莫斯科則將其用於研究工作」。

報道同時指出，中國開源AI模型DeepSeek的出現引起了前Facebook安全負責人、現任網絡安全公司SentinelOne專家的Alex Stamos的警覺。這位專家推測，不法分子將優先使用開源或非西方的AI工具，以規避政府和主要科技公司的檢測。