眼見未必真 慎防AI深偽詐騙

騙徒手法層出不窮，近日社交平台再出現假冒名人「教」人投資的騙案。有騙徒懷疑以特首李家超出席活動後會見傳媒的畫面，配上以人工智能(AI)生成的聲音，以「深偽技術」(Deepfake)假冒特首教人投資聲稱高回報的投資計劃，又稱獲得的利潤可以免稅。政府已就此嚴正澄清，有關影片全屬偽造，事件轉交警方跟進調查。究竟何謂「深偽技術」？又如何用肉眼識別？破解AI詐騙又有什麼貼士？現在一文睇清相關資訊，幫助大家避免上當。

什麼是「深偽技術」?

認為須加以偵察，以及限制其使用。

十分容易，引起公眾對於以假亂真的深度偽造製成品的關注，的信任，因而引起大眾關注。現在要取用創作深度偽造的工具傳播的錯誤訊息或虛假訊息可能會侵蝕企業的聲譽和社會之間由於深度偽造惡意用於製造假視像、偽造圖像和金融欺詐，所部表情。AI「換臉」、「換聲」的「深偽技術」開始運用於詐騙，正在全球迅速蔓延。近年，像或音頻，其中一個應用例子就是修改電影片段，而非重新拍攝或於後期製作中修改臉

即是利用人工智能(AI)／深度學習技術無中生有，製作出看似可信和逼真的視像、圖

類。

平則按媒體的來源和所需的合成結果分可分為視覺和音頻兩類，而屬性操作水重組為合成視像、圖像或音頻。技術大致別臉部和聲音的重要參數，並學習將參數

深度偽造技術包括一系列的演算，用於識

技術原理有什麼?

音。

編輯語音：修改語音，調節出完全不同的聲通。

音，並以十分準確及相似的語調與他人溝人工智能從錄音樣本中演算出真人的聲

逼真的人工智能語音：使用合成語音的的說話。

語音製作器將文本轉換為聽起來自然

文本轉換語音合成：使用逼真的旁白是某人所說，但事實並非如此。

信以為真的說話，語音聽起來就像

■ 音頻的深度偽造技術用於偽造令人

不變。

臉部操作：通過修改特定區域來改變一個人的臉部外觀，但同時保持其他不相關的區域

全臉合成：製造不存在但逼真的人臉。

視像上。

臉部再現：採用即時演算把所操作的目標人物臉部表情呈現在形與操控的語音輸入脗合。

同步口形：製造目標人物的合成視像，令受操作的視像中的口

換臉：將原來視像中的人臉更換為目標人臉。

圖像或視像中的人轉換為其他人的肖像。

■ 視覺的深度偽造技術用於偽造視像，將現有

■ 撥打防騙易18222熱線或使用防騙視伏器App，留意警方最新防騙消息。

■ 如懷疑是假資訊，應避免轉載，並向有關機構查詢。

■ 在解讀「消息指」、「已Fact Check」等訊息時應保持懷疑態度。

■ 多從不同媒體查找資訊，以多角度查找真相。

■ 如懷疑文字或圖片被竄改，可試用搜尋器查找出處。

■ 養成事實查證習慣。

■ 不要輕易相信網上資訊。

■ 避免接聽陌生人的視像通話來電。

■ 若有「親友」在視頻或錄音中提出匯款要求，要特別警惕。

■ 切勿輕易提供人臉、指紋、聲音等生物辨識信息。

■ 向對方提問，測試對方身份真偽。

■ 在視像對話中要求對方在鏡頭前做指定動作。

如何預防被詐騙?

■ 影像或音頻的質量差。

■ 口形與語音不同步。

■ 不自然的語調或機器人語氣。

■ 不一致的光照或語義完整性。

■ 不自然的眨眼或動作。

■ 留意異常的圖案、顏色或標誌。

如何用肉眼識別?

利用人臉識別作為活體偵測的可靠性。

■ 使用合成臉部表情或複製語音等以削弱獲取經濟利益的「幽靈欺詐」(欺詐性交易)。

■ 使用虛假身份資料進行欺詐，例如冒充死者以冒詐騙(例如身份盜用)。

■ 冒充受信任的人並獲取個人訊息，以進行魚叉式仿

■ 深度偽造可促成網絡攻擊和詐騙。

促成網絡攻擊

使用。

錄音、視像等電子證據的糾紛，只有其真實性通過法證水印工具鑑定方可

致法律問題。同樣，洩露或更改某人的個人資料亦可能構成侵犯私隱。在法庭訴訟中，涉及

深度偽造可能涉及在未經擁有人准許的情況下複製和分發版權材料，而不當使用或會導

製造法律問題

描述虛假事件以誹謗企業，從而推動市場情緒，引發股市動盪。

影響經濟活動

導致受害人的聲譽嚴重受損，例如利用某些名人的臉孔或聲音被用來散布謠言。

製造負面的輿論

會造成什麼影響及後果?