慎防Deepfake詐騙學習手冊

國小高年級學生版

本手冊將帶領你

深偽技術是什麼?
Deepfake?

深偽技術的詐騙方式有哪些?
認識辨識Deepfake的方式

瞭解如何避免成為
Deepfake影片主角

手冊大綱

一、深偽技術是什麼?

深偽技術（Deepfake）是指各種藉由AI達成的以假亂真的偽造圖片、聲音或影片。舉例來說，把姐姐的臉或表情移植到妹妹的影片上，讓妹妹說出她從來都沒有說過的話，而且效果和真的幾乎一樣。

二、常見的深偽技術詐騙方式

近年來有人運用這項技術進行犯罪，例如深偽色情影像、深偽名人的投資詐騙等，除了侵害他人的隱私權和名譽之外，也對社會安定與安全造成了危害。

(一)深偽色情影像

AI新創公司Sensity（前名為Deeptrace）專注於研究不斷演進的Deepfake技術。合夥創辦人兼執行長Giorgio Patrini根據Sensity於2019年的調查表示，有高達96%的Deepfake影片是未經當事人許可合成的色情影片，所以不管是一般人還是公眾人物，都有可能是被Deepfake的對象，可能會被合成色情照片或影片，雖然當事者和周圍朋友知道這些合成的色情影像並非本人，但是這樣的行為卻已經對受害者造成了傷害。

臺灣知名網紅自2020年7月至2021年10月間，運用Deepfake技術，將超過一百名被害者的臉部影像移花接木到色情網站的女模的臉上，製作出多部色情的影片販賣，甚至在各大社群平臺上公開短片吸引網友加入付費會員觀看，累計其中不法所得高達1千萬餘元，即使法律將嚴厲懲處該名網紅，但是基於網路傳播的快速，這些合成影片上傳後可能遭網友下載、轉傳，嚴重影響到被害人的身心名譽。

【摘自yahoo新聞2024/5/9】

(二)深偽名人的投資詐騙

有心人士也有可能在網路上合成名人或政治人物，製作各種造謠影片，例如詐騙集團可能運用這些技術，謊稱自己是被綁架的家人或是公司的主管高層，以電話聯絡受害人要求匯款，或是盜取知名投資專家、演藝人員等公眾人物的影像，發布不實的投資廣告消息、邀請民眾加入投資群組，透過噓寒問暖建立感情，營造溫馨關懷的人設，然後利用對方的信任，騙取投資人的錢財等。

2024年7月，網路上流傳多則運用知名演藝人員的影像進行假投資的廣告，除此之外，在社群平臺上也出現疑似假冒知名財經專家的粉絲專頁，網頁上有多則投資宣傳影片，甚至刊登邀請民眾加入投資群組，經證實，這些都是運用Deepfake技術的影片，請民眾在網路看到聲稱投資名人發布的廣告或訊息，應小心求證，若懷疑遭遇詐騙，也應報警求助，以避免造成嚴重的財產損失。

【摘自聯合報2024/7/13】

三、辨識Deepfake的方法

目前Deepfake已經能運用深度生成技術生成影像、聲音、文字等數位內容，包括臉部特徵變換、性別與年齡轉換、圖像風格轉換等，各種技術不斷地被開發或進化，讓真假越來越難分辨，但是Deepfake產生的內容依然有破綻!

在持續發展Deepfake技術時，許多團隊同時也在研發偵測Deepfake造假的技術與工具，例如可以透過以下幾種方式辨識。

1 **放大畫面**

觀察影像裡的背景區域是否模糊，注意臉上的嘴型、表情與聲音是否吻合。

2 **觀察臉部輪廓是否自然**

注意臉部（尤其是側臉）或頭髮邊緣有沒有剪下圖形所產生不自然的參差感，輪廓的接合處是否有瑕疵、失真，或影片中的人物在大幅度移動時，畫面紋理是否正常。

3 **觀察眼睛的方向是不是永遠望著固定方向**

因為Deepfake在黏貼臉部影像時無法轉動眼珠，且生成模型生成的瞳孔通常為不規則，導致雙眼視線不一致。

4 **因為Deepfake在製作影片時需要大量的素材來生成逼真的偽造影片，在素材不足的情況下，容易導致表情、動作或角度上的變化不夠，生成的影片可能會顯得不自然或者出現明顯的破綻。**

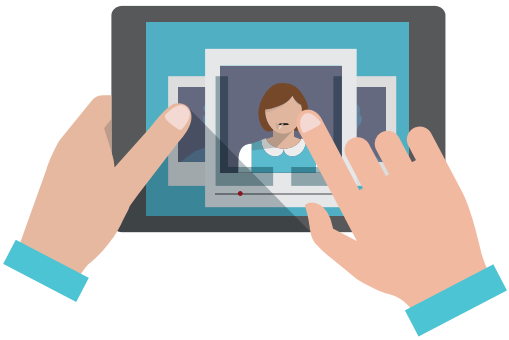
5 **如果是即時影像，要求對方轉頭90度，如果是偽造的Deepfake畫面，在側臉經常會有破碎或模糊處。**

6 **如果是即時影像，要求對方在臉前揮動手指、筆、或筷子之類的條狀物品，如果是偽造的Deepfake畫面，這些物品會呈現半透明狀態。**

四、動動腦時間

(一)阿偉的煩惱

阿偉注意到社群平臺上好像有疑似班長小琪的影片，影片內容很奇怪，是小琪一邊抽菸一邊做出疑似猥褻動作的影像，阿偉不確定影像中的人是不是班長？也不知道這件事情要不要跟老師說？萬一告訴老師，影片中的人真的是班長，那麼班長肯定會受到懲處，嚴重甚至會退學，但如果影片的人不是班長呢？



問題

1. 如果你是阿偉，你會怎麼做？

2.如果小琪發現自己變成Deepfake影片的主角，她該怎麼辦？

(二)牛刀小試

問題一：如何辨識 Deepfake 技術造假影片？

A.觀察影像中人物的肢體動作是否順暢。
B.觀察影像畫面是否清晰。
C.觀察影像中人物的頭髮、背景跟臉的交界處是否清晰。
D.以上皆是。

問題二：以下何者非 Deepfake 影片的素材要素？

A.臉上的各種表情。
B.各種拍攝角度的五官。
C.去除背景的照片或影像。
D.高解析度的照片或影像。

你答對了嗎？

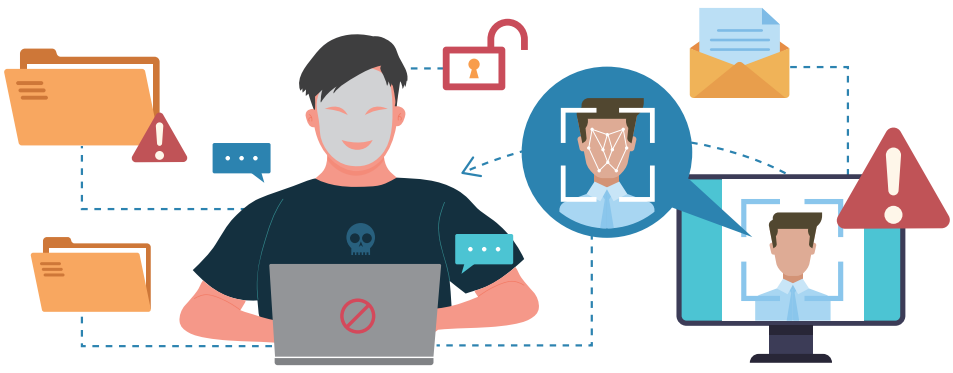
第一題的答案是 D
可以透過放大畫面觀察人物的肢體動作是否順暢、頭髮、背景跟臉的交界處是否清晰，是否有不自然的參差感，畫面是否清晰。

第二題的答案是 C
為避免成為Deepfake的主角，盡量別讓他人取得自己各種拍攝角度和表情的高解析度影片。

五、避免成為Deepfake影片主角的方法

其實各種「拼湊之後足以識別他人的資料」都是有價值的個人資料，另外e-mail、電話或是通訊軟體的好友關係，也都有利於詐騙集團聯絡到你周圍的好友，許多人常常在社交平臺上公開居住地區、就讀學校、工作地點等，也會錄製影片或拍攝清楚的五官照片上傳在平臺上，這些其實都是有風險的行為，為了避免成為Deepfake的主角，盡量別讓他人取得自己高解析度的、各種拍攝角度和表情的影片。

除了避免流傳自己臉部的素材照片或影片之外，我們也應該瞭解未經當事人授權，無論是製作或是散布Deepfake影片都是侵權或犯法的。就算你可能沒有惡意，但是將他人的臉部移植到某部影片，就已經侵害了當事人的「肖像權」以及影片原作者的「著作權」，如果將影片廣為散布，還侵犯了當事人的「人格權」。所以我們千萬不能因為一時好玩或氣憤而以身試法，造成無法彌補的錯誤也傷害到了他人。



參考資料

Patrini, G..（2019）. Mapping the Deepfake Landscape. https://giorgiop.github.io/posts/2018/03/17/mapping-the-deepfake-landscape/

網紅小玉「盜臉私密片」判5年定讞　啟動防逃機制（2024，5月10日）。Yahoo新聞。https://ynews.page.link/K4FDK

廖炳棋（2024，7月13日）。**刑事局：AI深偽名人詐騙　謝金河、吳淡如等人都受害**。聯合新聞網。https://udn.com/news/story/7315/8093260