

眼見為憑？耳聽為證？

「深偽技術」

— AI換臉變聲如何成為詐騙犯罪工具 —



反詐騙小金剛



臺北市政府警察局刑事警察大隊

什麼是「深偽技術」？



「深偽」(Deepfake)係由深度學習(Deep Learning)以及偽造(fake)二詞組成，是運用人工智慧(AI)概念的一種技術，可應用於各式媒體素材如圖片、影像、聲音的合成，達到換臉、變聲的效果

電影《玩命關頭7》便是用類似的技術，讓拍攝途中因車禍意外離世的男星保羅沃克，其五官及聲音得以「重生」於大銀幕前。



然而這樣的技術，卻被有心人士拿來惡作劇，製造**假新聞、假訊息**，甚至是成為詐騙手法的工具……

反詐騙小金剛



臺北市政府警察局刑事警察大隊

詐騙集團會如何利用「深偽」？

「猜猜我是誰」



詐騙集團假冒成親戚朋友，撥打電話給受害人，並稱因故急需用錢，請求儘速匯款應急……

或是將換臉技術用於視訊，偽裝成公司高層，向下屬發出轉帳的指示……



利用深偽技術成產出的**合成影像、圖片及語音**，讓這些騙術變得更加真實

反詐騙小金剛



「不雅照恐嚇信」



有多位知名大學教授，其肖像遭詐騙集團移花接木，拿來合成不雅照片。

再以此寄送恐嚇信向這些教授勒索，威脅說若不繳交封口費便將照片散布出去……

臺北市政府警察局刑事警察大隊

該怎麼加以預防？



針對來電匯款要求，保持警覺，主動確認

透過深偽製作的合成語音，可能讓受話者難辨真偽，誤認為是真正的親戚或朋友打來，碰到類似情形，應主動暫停通話，並透過其他管道聯繫對方以確認真實性，多一層警覺，謊言將不攻自破！

《刑法》第339-4條**加重詐欺罪**，也為因應這種手法新增了**第4款**的行為態樣



以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法而犯詐欺罪者，處**1年以上、7年以下徒刑**，得併科**100萬元以下罰金**。

反詐騙小金剛



臺北市政府警察局刑事警察大隊