深度偽造

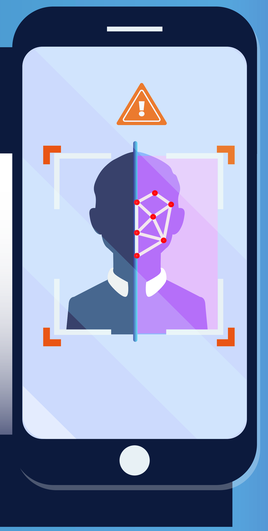
風險與應對

詳情請瀏覽
「守網者」或「香港網絡安全事故協調中心」官網：

Cyber Defender 守網者 | GovCERT.HK 政府電腦保安事故協調中心 | HKCERT 香港網絡安全事故協調中心

甚麼是深度偽造？

「深度偽造」一詞由「深度學習」與「偽造」結合而成，是指利用人工智能技術，將一個人的臉容或聲音合成至特定圖像、影片或音頻中，從而造出看似真實的偽造內容。



深度偽造的惡意用途

詐騙： 冒充受害者的親友、工作夥伴或其他可信任人士，從而騙取金錢。

勒索： 捏造對受害者造成負面影響的內容，藉威脅公開內容以敲詐受害者。

網絡欺凌： 製作冒犯或滋擾受害者的惡意內容，並於網絡上發布。

虛假資訊： 製作假新聞故意誤導公眾或影響輿論。

辨識及應對深度偽造

識別瑕疵：細心留意圖像、影片或音頻是否有不自然的動作、不協調或不合常規的地方。

評估來源：衡量發布內容的媒體的可信度。

進行事實查核：對收到的內容抱持合理的懷疑態度，並透過可靠的途徑查核內容是否屬實。

保護個人資料：切勿隨意公開個人資料，以免被利用來生成深度偽造內容。