學習新生存技能：辨別 Deepfake

什麼是 Deepfake？

「Deepfake」（深偽）這個詞是「deep learning」（深度學習）和「fake」（偽造）的組合。Deepfake 是偽造的圖片、影片或錄音。有時，其中的人像是電腦生成的假身份，看起來和聽起來都像是真人。有時人像是真實的，但他們的外觀和聲音被操縱作出他們沒有作的言行。例如，可以使用 deepfake 影片重現名人或政客說出他們從未說過的話。使用這些栩栩如生的贋品，攻擊者可以構建一個另類現實，讓您無法相信自己的眼睛和耳朵。

某些 deepfake 目的是合法的，例如電影讓已故演員起死回生以重現著名角色。但網路攻擊者開始利用深偽的潛力。他們以其佈置愚弄您的感官，並因此得以竊取您的錢財、騷擾人們、操縱選民或政治觀點，或製造假新聞。聯邦調查局警告，由於使用的合成媒體的複雜程度，未來deepfake將產生「更嚴重和更廣泛的影響」。有鑑於這些攻擊，您在閱讀新聞或社交媒體時必須更加小心自己相信的東西。

聯邦調查局警告，由於使用的合成媒體的複雜程度，未來 deepfake 將產生「更嚴重和更廣泛的影響」。學習找出深偽的跡象，以保護自己免受這些可信度極高模擬的影響。每種形式的 deepfake（靜態圖片、影片和音訊）自身都有一系列缺陷會將其暴露。

靜態圖片

您最常看到的 deepfake 是虛假的社交媒體頭像。下圖是來自網站thispersondoesnotexist.com的一個 deepfake 範例。圖片下方是五個不同的線索，表明這可能是一個deepfake。您會注意到，這些線索不容易發現並且難以識別：

1. **背景：背景通常是模糊或扭曲的，並且可能有不一致的照明，例如指向不同方向的明顯陰影。**
2. **眼鏡：仔細觀察鏡框和靠近太陽穴的鏡腳之間的連接。Deepfake 的連接通常不連貫，大小或形狀也略有不同。**
3. **眼睛：目前用於偽造個人資料圖片的 deepfake 照片似乎都會將眼睛放在畫面中的同一位置，從而導致一些人稱之為「深偽凝視（deepfake stare）」的現象。**
4. **珠寶：耳環可能形狀模糊或怪異附著。項鍊可能嵌入皮膚。**
5. **衣領和肩膀：肩膀可能畸形或不合。每側的衣領可能相異。**

影片

麻省理工學院（MIT）的研究人員開發了一個問題清單，以幫助您確定影片是否真實，並指出深度偽造通常無法「完全呈現場景或照明的自然物理效果」。

1. 臉頰和額頭：皮膚是否顯得太光滑或太皺？皮膚的年齡與頭髮和眼睛的年齡相似嗎？
2. 眼睛和眉毛：陰影是否出現在您預期的地方？
3. 眼鏡：有眩光嗎？眩光過多？人移動時眩光的角度會發生變化嗎？
4. 鬍鬚：鬍鬚看起來真實嗎？Deepfake 可能會增加或去除鬍子、鬢角或絡腮鬍。
5. 面部的痣：痣看起來是真的嗎？
6. 眨眼：這個人眨眼頻率剛好或太頻繁？
7. 嘴唇大小和顏色：大小和顏色是否搭配人臉的其他部分？

音訊/語音

研究人員表示，聲譜圖等技術可以顯示何時出現假的錄音。但是當攻擊者打電話時，我們大多數人都沒有語音分析儀這種奢侈設備。聽看看有沒有單調的聲音、奇怪的音調或情緒，以及缺乏背景噪音。偽造語音很難被發現。如果您接到來自合法機關的奇怪電話，您可以先掛斷然後回撥該機關來驗證對方是否真的來電。請務必使用受信任的電話號碼，例如聯絡人清單中已有的號碼、印在機關帳單或報表上的電話號碼，或機關官方網站上的電話號碼。

結論

請注意，攻擊者正在積極使用 deepfake。他們能夠在社交媒體上建立假帳號來連結或製作假影片以影響公眾輿論。有些人甚至在暗網上出售他們的服務，以便其他攻擊者也能夠依樣畫葫蘆。我們不期望您成為 deepfake 專家，但如果您掌握了識別偽造的基礎知識，您將能更好地保護自己。如果您懷疑自己發現了 deepfake，請將其報告給託管內容的網站或來源。

客座編輯

Kerry Tomlinson (@KerryTNews)是 Ampere News 的網路新聞記者和經過認證的 SANS 安全意識專家。她的使命是透過引人入勝、真知灼見的新聞故事和介紹，為所有知識程度的人翻譯數位世界中正在發生的事情。

參考資源

社交工程攻擊：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt5665cdf1e2dd80e4/6048fecc5aedc043351b76ce/OUCH!_Nov_2020_-_Social_Engineering_v.3-Chinese_(Traditional_Taiwan).pdf
您能識別偽造嗎？(Ampere News)： https://www.amperesec.com/news/can-you-spot-the-fake
麻省理工學院（MIT）的深偽檢測： https://detectfakes.media.mit.edu/
識別deepfake： https://www.spotdeepfakes.org/en-US

翻譯：宋亞倫 德欣寰宇科技股份有限公司