資訊安全宣導_11403

布萊德·彼特成詐騙高手?醒醒吧戀愛腦，不要被戀愛沖昏頭了!

114 年 03 月 03 日

中國信託證券股份有限公司

文件制／修訂記錄

版次	日期	說明	作者	修訂中	定稿
1.0	114.03.03	初稿	何彥甫		V

【目　　錄】

【圖 目 錄】

壹、 簡述

近年來，隨著人工智慧（AI）技術的興起，帶動需多產業的發展及技術的革新，然而伴隨 AI 技術出現的深偽技術（Deepfake）被詐騙集團利用，假冒知名投資名人進行詐騙活動，造成了嚴重的財產損失和社會危害。 深偽技術是利用 AI 生成虛假影像或聲音的技術，能夠逼真地模仿特定人物的外貌和聲音。詐騙集團利用這項技術，製作假冒投資名人的影片或音頻，在網路上發布詐騙廣告，誘騙受害者進行投資，一但受海者投入夠多的金額，詐騙集團就會開利用各種理由拒絕出金，將受害者的財產據為己有。

詐騙集團利用深偽技術可能出現的詐騙手法包含:

1. 假冒名人影片：不法分子利用深偽技術製作知名投資名人的假影片，聲稱有高回報的投資機會，並通過社交媒體廣泛傳播。
2. 假冒名人通話：詐騙分子通過深偽技術生成的假音頻，冒充投資名人直接與受害者通話，誘騙受害者相信虛假的投資計劃。
3. 假冒名人廣告：利用深偽技術製作假廣告，在互聯網上投放，吸引潛在受害者點擊並參與投資。

貳、 布萊德·彼特成詐騙高手?醒醒吧戀愛腦，不要被戀愛沖昏頭了!

近期發生一起令人震驚的詐騙案，一名婦人被 AI 冒的充布萊德·彼特（Brad Pitt）的愛情詐騙犯騙走了 83 萬歐元，約台幣 2836 萬元。這個故事再次敲響警鐘，提醒我們愛情詐騙的手法有多麼高明，尤其在 AI 技術的加持下，更具欺騙性。愛情騙子是一個由三到四人組成的詐騙團體，他們還會冒充基努·李維等其他明星進行詐騙。

受害者安妮（化名），是一名室內設計師，誤以為自己與好萊塢巨星布萊德·彼特展開了一段長達一年多的戀愛關係。詐騙集團利用精心編輯的照片和個人化訊息，營造出與彼特戀愛的逼真假象，讓安妮深信不疑。

安妮起初收到自稱「布萊德·彼特媽媽」的訊息，推薦她給自己的兒子。儘管一開始有所懷疑，但在「布萊德·彼特」長達一年半透過假的社交媒體和 WhatsApp 帳戶傳送給安妮情書、情詩、偽造的護照和求婚攻勢下，她逐漸卸下心防。雖然兩人未曾謀面，但詐騙集團善用 AI 影像生成技術，製作出幾可亂真的「彼特」，透過照片、視訊與她聯繫。

詐騙情節隨後升級，「冒牌彼特」告知安妮他需要進行癌症治療，卻因與安潔莉娜·裘莉的離婚官司導致帳戶凍結，因此需要借錢應急。為了增加可信度，詐騙集團甚至傳送了 AI 生成的「彼特」住院照片，營造出病重急需用錢的假象。安妮看著視訊中與螢幕形象無異的小布，深信不疑，陸續匯出 83 萬歐元，約台幣 2800 萬。直到女兒提醒她可能受騙，她仍執迷不悟，認為等「布萊德·彼特」現身後，女兒就會明白真相。

在長達 18 月的時間裡，安妮每天都與「冒牌彼特」交流，對方對她的工作表現出濃厚的興趣，並展現出極高的溝通技巧，安妮事後回憶道。這段時間裡，詐騙集團成功地與安妮建立了深厚的情感連結，為後續的詐騙行為鋪路。

安妮與「冒牌彼特」談話的內容之一，是關於她自身巨額的離婚贍養費，這也讓詐騙集團鎖定了她作為目標。在「冒牌彼特」以腎臟治療為由要求財務援助後，安妮陸續被說服向愛情詐騙犯匯款 83 萬歐元，她以為自己是在幫助未來的老公。直到 2024 年夏季，媒體拍到真正的布萊德·彼特與女友伊妮絲·迪·拉蒙的合照時，安妮才如夢初醒，意識到自己被騙了。

圖1　布萊德·彼特住院照

參、 布萊德·彼特詐騙案：典型的愛情詐騙，AI 成新幫兇!

這起詐騙案清楚地展現了愛情詐騙的常見手法，更突顯了 AI 技術在詐騙行為中扮演的新角色：

1. AI 生成內容：詐騙犯利用 AI 生成照片、影片和訊息，模仿名人或特定人物，建立更具說服力的虛假身份。
2. 長期情感操控：透過長時間的日常交流，詐騙犯與受害者建立深厚的情感連結，操控受害者的情緒和判斷力。
3. 捏造危機：詐騙犯會捏造各種危機，例如疾病、意外或財務困境，以引發受害者的同情心和恐慌，進而要求財務援助。
4. 財務剝削：所有鋪陳最終都導向財務剝削，騙取受害者的金錢，高達 85 萬美元。

這起事件也提醒我們，面對日益精進的詐騙手法，尤其是在 AI 技術的助長下，我們更需要提高警覺。除了先前提供的六個危險信號外，更要留意以下幾點：

1. 對網路上認識的人保持懷疑：不要輕易相信網路上認識的人，即使對方使用看似真實的名人照片或影片。
2. 謹慎看待涉及金錢的要求：任何涉及金錢的要求都應該格外謹慎，切勿輕易匯款給不熟悉的人。
3. 留意 AI 生成的內容：學習辨識 AI 生成的圖像、影片和文字，例如檢查是否有不自然的細節或不連貫的地方。
4. 尋求親友或專家的意見：如果對網路上的關係或訊息感到懷疑，不妨向親友或專家尋求意見。

肆、 愛情詐騙:六個危險訊號

請留意以下危險信號。如果發生其中一個或多個情況，請仔細考慮您的下一步行動，並尋求信任的家人、朋友和/或專家的指導。

1. 對方身在遙遠的地方。
2. 他們的個人資料看起來好得令人難以置信。
3. 關係發展非常迅速。
4. 對方食言，沒有來訪或親自見面。
5. 他們需要錢（無論是什麼藉口）。
6. 更糟糕的是——他們特別要求某種付款方式。

圖 2　愛情詐騙示意圖

伍、 個人電腦使用其他注意事項

一、 參考附錄：

1. 個人密碼屬機密資料，由個人所有並需加以保護，密碼長度必須為 8 碼以上並且英文及數字混合，不可明碼儲存、記錄於書面、張貼於電腦螢幕、鍵盤、隔版、桌面...等可視區域；不得共用且不可公開，個人電腦之登入密碼必須定期變更。(CTSWI0027 個人電腦與周邊設備管理規範)、(CTSWI0025 行動資訊設備管理辦法)

2. 為防止他人窺視、不當使用或竄改資料，應設定電腦於五分內啟動內建之螢幕保護程式並設定密碼保護；離開使用中之電腦時，應先啟動內建之螢幕保護程式鎖定螢幕，並視情況結束連線登出(LOGOFF)。(CTSPY0005 資訊安全政策)

3. 考量各營業單位隨時輸單之需求，有關 Key-In 及營業員之個人電腦將不執行螢幕保護程式之設定，但仍需於離開座位時手動執行鎖定電腦功能(請同時按[Ctrl]鍵 ＋[Alt]鍵 ＋[Delete]鍵後，點選[鎖定電腦]之功能)，以確保資訊資源之安全。(CTSPY0005 資訊安全政策)

4. 電腦軟體之安裝與使用悉依本公司軟體採購(使用)標準，詳細軟體安裝清單請參閱(CTSFR0071 個人電腦標準安裝軟體清單)。新軟體之使用須經資訊單位評估無虞並納入採購(使用)標準後方可採購(使用)。(CTSWI0027 個人電腦與周邊設備管理規範)

5. 使用類似網路磁碟功能分享資料時，請符合下列事項。(CTSWI0027)個人電腦與周邊設備管理規範)

6. 非業務執行需求，避免設定資源分享。

7. 不應將整顆硬碟（C槽或D槽）設定為資源分享，以避免電腦系統及資料檔案遭到不可預期之複製及破壞。

8. 設置資源分享之資料夾，均應設置密碼及設定存取權限，並於使用後立即關閉分享。

9. 於本公司使用行動資訊設備(僅限各部門申請之筆記型電腦等設備，非公司採購之設備嚴禁攜帶至公司使用)，使用人均需填寫 OA 系統之[(CTSFR0070)資訊設備 IP 位址暨行動資訊設備申請單]，經需求單位主管簽核後，向資訊部權責單位提出需求申請。(CTSWI0025 行動資訊設備管理辦法)

10. 使用行動通訊設備必須設定硬碟密碼鎖，無此功能之行動資訊設備則不需設定。(CTSWI0025 行動資訊設備管理辦法)

11. 行動資訊設備若為該單位公用電腦，使用人員必須於歸還前清除個人資料以確保該行動資訊設備之資訊安全。(CTSWI0025 行動資訊設備管理辦法)

12. 未經資訊單位核准，具備連接本公司網路或存取本公司資訊資源能力之資訊設備，在本公司辦公處所使用時，不得再同時連接無線網路(WiFi)、行動網路與撥接網路(Dial-Up)串連公司以外網路。(CTSWI0027 個人電腦與周邊設備管理規範)

13. 敏感資料（如客戶資料）不應儲存於個人電腦。如因執行業需要暫存，於作業完成後應立即移除，如必須留存時，建議使用壓縮軟體來加密封存該敏感資料。((CTSWI0027)個人電腦與周邊設備管理規範）

14. 使用行動通訊設備必須設定硬碟密碼鎖，無此功能之行動資訊設備則不需設定。(CTSWI0025 行動資訊設備管理辦法)

15. 行動資訊設備若為該單位公用電腦，使用人員必須於歸還前清除個人資料以確保該行動資訊設備之資訊安全。(CTSWI0025 行動資訊設備管理辦法)

16. 未經資訊單位核准，具備連接本公司網路或存取本公司資訊資源能力之資訊設備，在本公司辦公處所使用時，不得再同時連接無線網路(WiFi)、行動網路與撥接網路(Dial-Up)串連公司以外網路。(CTSWI0027 個人電腦與周邊設備管理規範)

17. 敏感資料（如客戶資料）不應儲存於個人電腦。如因執行業務需要暫存，於作業完成後應立即移除，如必須留存時，建議使用壓縮軟體來加密封存該敏感資料。((CTSWI0027)個人電腦與周邊設備管理規範）

18. 資料檔案列印時應確認輸出的印表機裝置是否正確，確認無誤後再行列印，取回列印文件或報表時如有發現其他列印資料時，應協助確認該列印資料為何人列印並通知取回，如確認後仍無人認領應協助銷毀該列印資料。

19. 使用電子郵件傳送機敏資料時，需對機密性及敏感性資料加密後再傳送。

20. 避免使用公司電子郵件住址註冊各種網站之會員，以防止收取垃圾郵件及詐騙信件。

21. 嚴禁透過網咖、學校...等公共場所之網路環境使用遠程簽到，以避免遠程簽到登入帳號與密碼遭留存而致他人利用。(CTSWI0039)遠程簽到管理規範

表1　各地區電腦聯絡人員

單　位	電腦連絡人員	電子信箱	駐點分機
總　公　司	符前智	adam.fu@ctbcsec.com	2715 2584
三重分公司	陳威羽	harvey.chen@ctbcsec.com	199
忠孝分公司	陳威羽	harvey.chen@ctbcsec.com	199
永康分公司	李永宏	luhpro@ctbcsec.com	199
文心分公司	李奇峰	clay.le@ctbcsec.com	199
新竹分公司	鄧和榮	helong.den@ctbcsec.com	199
松江分公司	陳威羽	harvey.chen@ctbcsec.com	199
嘉義分公司	李奇峰	clay.le@ctbcsec.com	199
中壢分公司	鄧和榮	helong.den@ctbcsec.com	199
高雄分公司	鄭宗武	jan@ctbcsec.com	199
資　訊　部	張志鴻	cch@ctbcsec.com	2380
資訊安全小組	吳　洲	chou.wu@ctbcsec.com	2390

二、 社交工程演練相關懲處建議：

期間	觸發條件	對應措施及建議懲處方式
一年 (12 個月/次) 區間： Q4 ~ Q3	未開啟任一封郵件者，視為相對安全人員	無須對應
	僅開啟郵件，而未開啟郵件內連結或附件者，視為低風險人員	無須對應
	累計開啟任一封郵件內連結或附件者，視為中風險人員	1. email 通知該員及部門主管、資訊安全長、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數

	累計開啟任兩封郵件內連結或附件者，視為高風險人員	1. email 通知該員及部門主管、資訊安全長、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數 3. 記警告乙次 4. 重新執行資安教育訓練
	累計開啟任三封郵件以上，且皆有開啟郵件內連結或附件者，視為極高風險人員	1. email 通知該員及部門主管、資訊部主管、總經理 2. 年度資安遵循評核影響部門主管 KPI 分數 3. 記警告(含)以上乙次 4. 直屬主管陪同重新執行資安教育訓練

特此提醒同仁收到不尋常的 email 信件，務必提高警覺並依以下建議因應：

1. 同仁可檢視 email 主旨欄，若被標示【外部郵件】，則該 email 係來自外部，而非內部寄件者，請謹慎確認後再開啟。
2. 同仁可檢視 email 主旨欄，若標示【中信銀行郵件】，則該 email 寄件者係來自中信銀行，依此類推。
3. 同仁可檢視 email 主旨是否與工作業務相關，如若與公務無關應直接刪除，勿任意開啟。

陸、 參考資料

https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1887&serno=284b7728-56a0-4191-b794-4df960ed3f96

https://blog.trendmicro.com.tw/?p=86263

https://laws010.com/blog/criminal-offense/fraud/romance-scam