



長庚學校財團法人長庚科技大學

114年度資通安全教育訓練

☑資通安全系列課程

★課程名稱：資安風險識別與個資保護

★授課時數：3 小時



講師：鍾文魁 Mark

現職：邦尼管理顧問有限公司 資深顧問

學歷：東吳大學法律學系科技法律組 碩士
(關鍵資訊基礎設施保護法制面建構與分析)

華梵大學資訊管理學系資通安全組 碩士
(惡意電子郵件攻擊之研究)

經歷：



大綱

一 資安風險與資安防護基礎

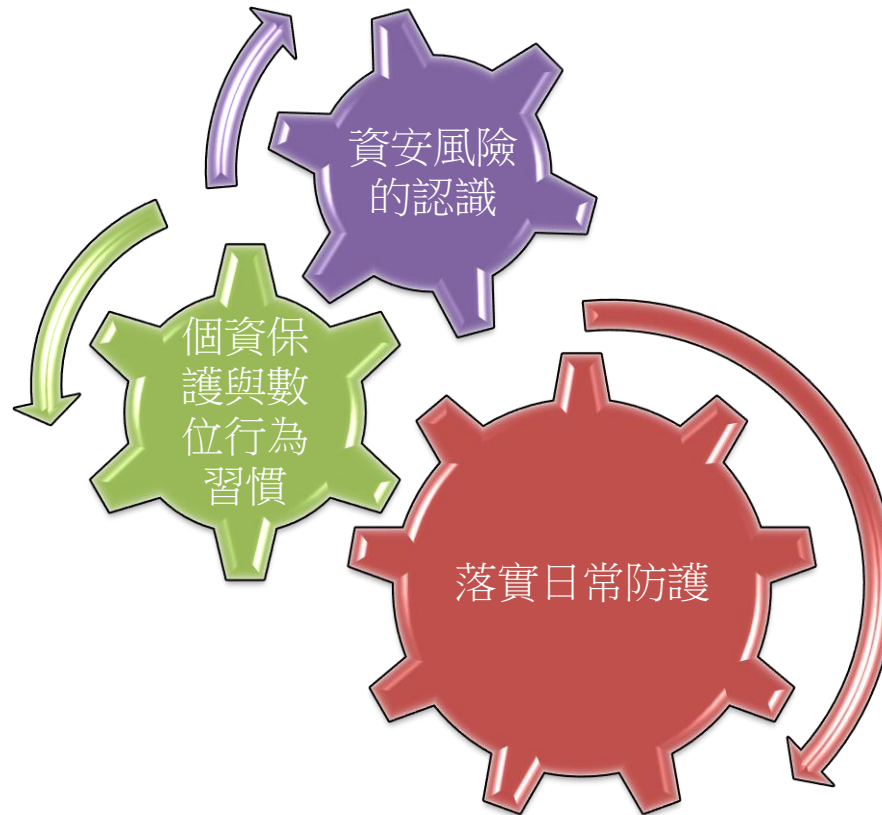
二 行動裝置與新興技術下的個資挑戰

三 雲端與整體資安思維建構

四 回顧與討論

課程目的與目標

課程目的



課程目的與目標

課程目標

社交工程與密碼風險

雲端、IoT、AI等技術中的資
安重點

行動裝置與個資保護能力

大綱子題

一 資安風險與資安防護基礎

1 社交工程攻擊的陷阱與防範

2 身份與密碼管理的重要性

資安風險與資安防護基礎

社交攻擊簡介

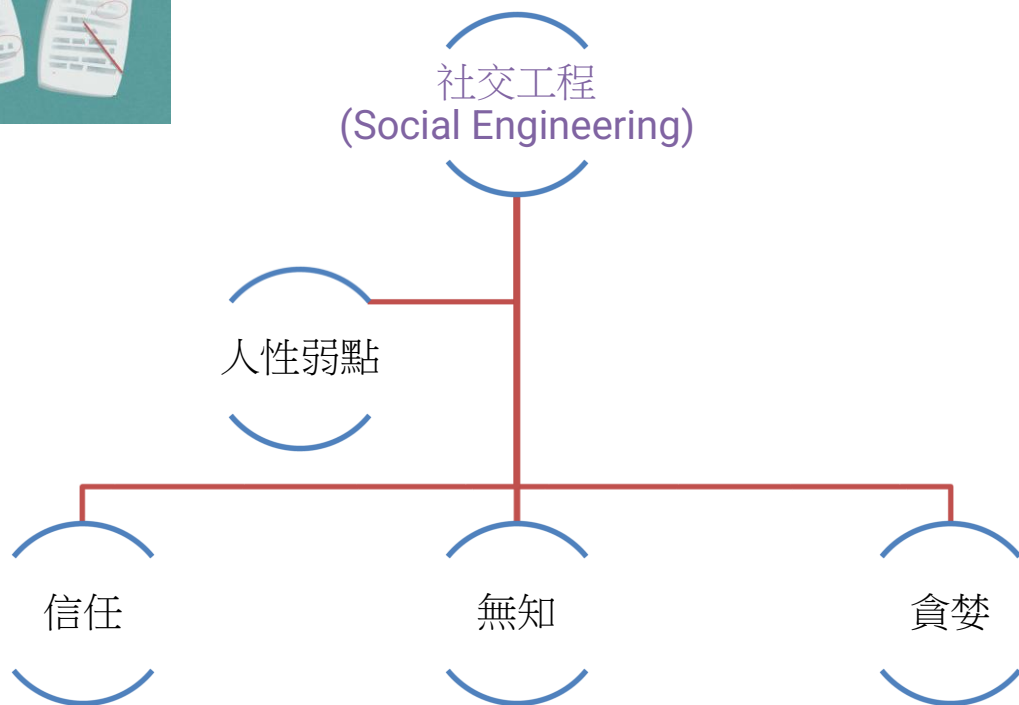
俗話說得好，資安最大的漏洞就是「人」。社交工程攻擊用的不是高深的電腦技術，而是用詐騙的方式要到關鍵人物的驗證資訊，進而取得登入權限。



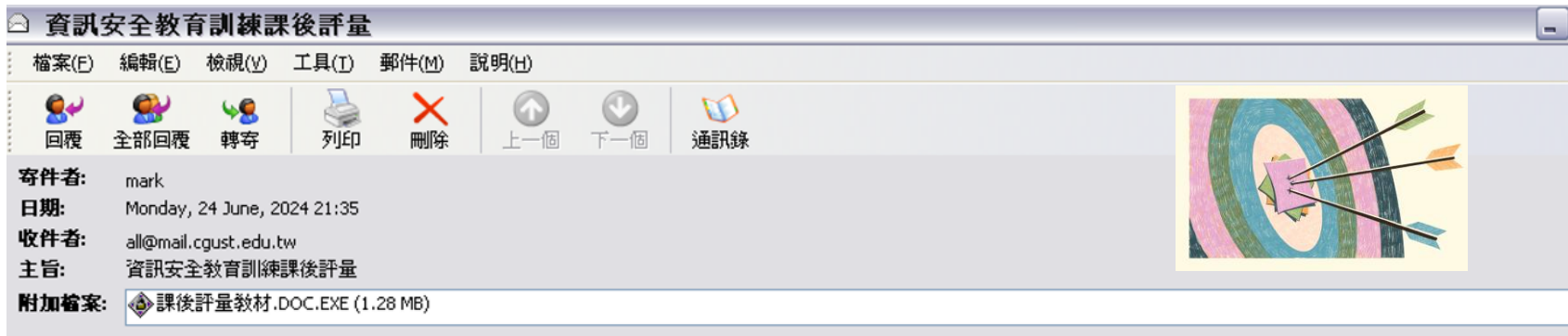
一

資安風險與資安防護基礎

社交攻擊簡介



社交攻擊簡介



一

資安風險與資安防護基礎

社交攻擊簡介

釣魚攻擊
(Phishing)

假冒技術支援
(Tech Support
Scam)

尾隨入侵
(Tailgating)

誘餌攻擊
(Baiting)

網路釣魚網站
(Spear Phishing
/ Clone Sites)

社交攻擊防範

防範對策	說明
不輕信陌生來信／簡訊	留意語氣是否不尋常，有無錯別字與奇怪連結
驗證對方身份	接獲可疑來電時，可主動回撥公司總機確認
不點擊不明連結或附件	寧願慢一點，也不要貿然點擊不熟悉的檔案或網站
定期教育訓練	提高員工警覺性與防範能力，建立「人是防線」的文化

資安風險與資安防護基礎

身分管理

確保在資訊系統與服務中，**個體**（如員工、外包人員、訪客、應用程式、裝置等）之身份的建立、管理與移除能受到妥善控管，以**防止未經授權的存取或濫用**。

登入系統

輸入您的電子郵件地址和密碼。

帳號

請輸入email

密碼

請輸入密碼



登入

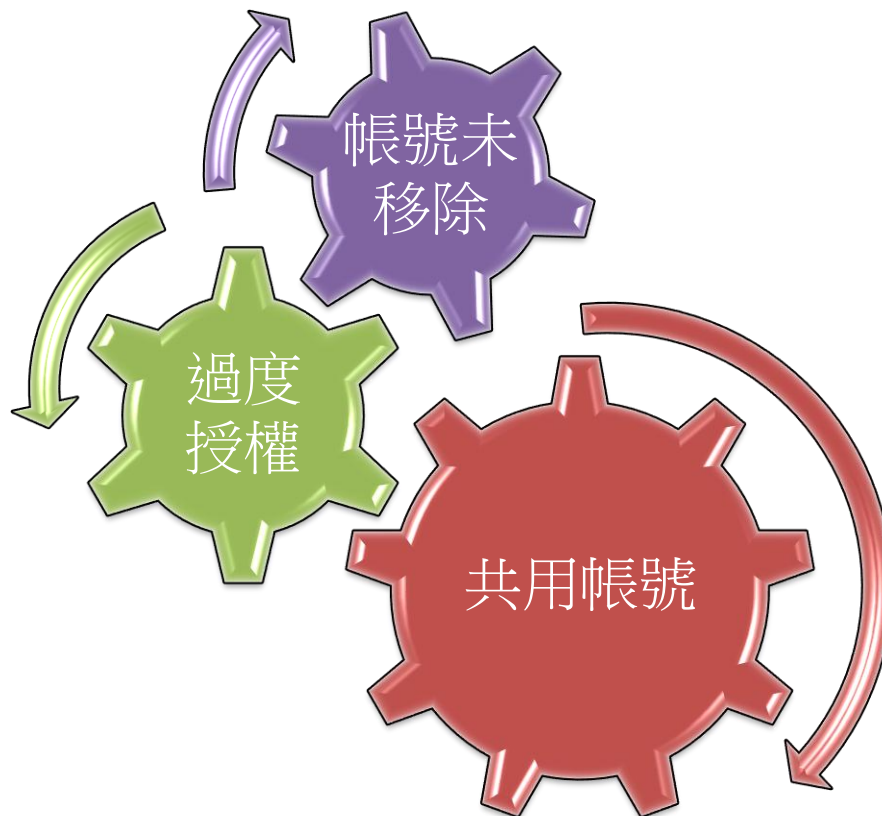
我是經過授權
系統管理者

我是經過授權
的系統使用者

一

資安風險與資安防護基礎

身分管理



一

資安風險與資安防護基礎

身分管理

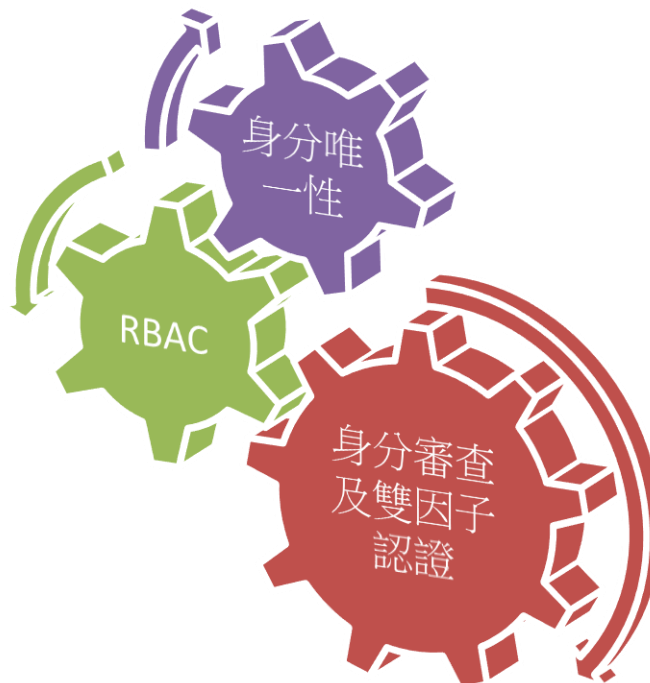
建立

啟用

修改

停用

移除



資安風險與資安防護基礎

密碼管理

確保在資訊系統與服務中，**個體**（如員工、外包人員、訪客、應用程式、裝置等）之身份的建立、管理與移除能受到妥善控管，以**防止未經授權的存取或濫用**。

登入系統

輸入您的電子郵件地址和密碼。

帳號

請輸入email

密碼

請輸入密碼



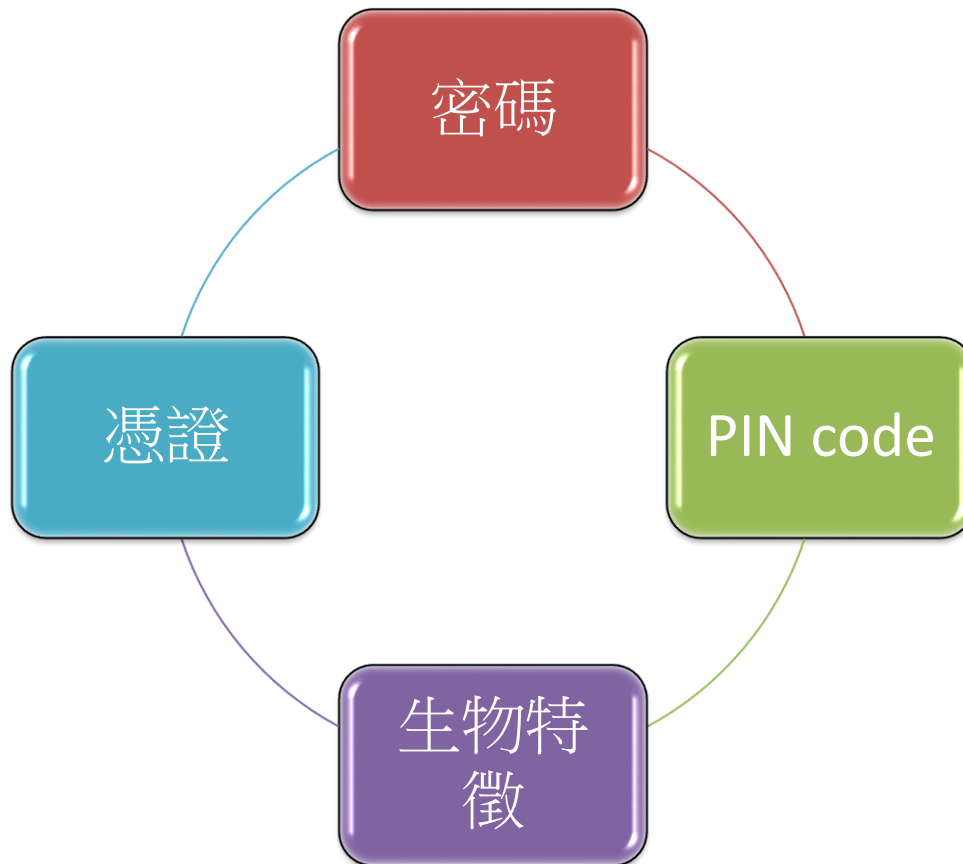
登入

我是經過授權
系統管理者

我是經過授權
的系統使用者

密碼管理

防止未經
授權的存
取、揭露、
濫用或竄改



密碼管理

鑑別資訊的保
密性與完整性

密碼政策與複
雜性要求

防止密碼洩漏
與重複使用

自動保護機制

密碼管理工具
與多因素驗證

存取權限控制

登入系統

輸入您的電子郵件地址和密碼。

帳號

請輸入email

密碼

請輸入密碼



登入

我是
系統**管理**者

我是
系統**使用**者

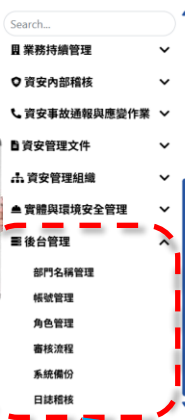


資安風險與資安防護基礎

存取權限控制



我是
系統管理者



儀錶板

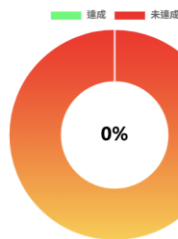
資訊安全目標及控制措施量測

2024年度

各類控制措施績效量測結果:



控制措施績效量測結果:



資安長

我是
系統使用者

20

一 資安風險與資安防護基礎

存取權限控制

7 大構面	29項控制措施
✓ 存取控制	帳號管理;最小權限;遠端存取
事件日誌與可歸責性	記錄事件;日誌紀錄內容 ;日誌儲存容量;日誌處理失效之回應 ;時戳及校時 日誌資訊之保護
營運持續計畫	系統備份;系統備援
✓ 識別與鑑別	內部使用者之識別與鑑別;身分驗證管理;鑑別資訊回饋;加密模組鑑別 ;非內部使用者之識別與鑑別
系統與服務獲得	系統發展生命週期需求階段;系統發展生命週期設計階段;系統發展生命週期開發階段 ;系統發展生命週期測試階段 ;系統發展生命週期部署與維運階段;系統發展生命 週期委外階段 ;獲得程序;系統文件
系統與通訊保護	傳輸之機密性與完整性;資料儲存之安全
系統與資訊完整性	漏洞修復;資通系統監控;軟體及資訊完整性

大綱子題

二 行動裝置與新興技術下的個資挑戰

1 行動裝置與個人資料安全

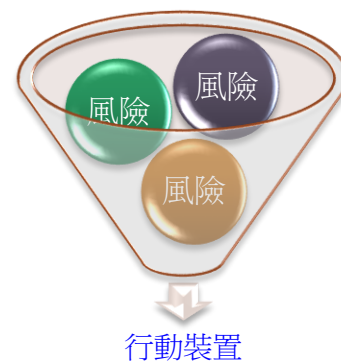
2 物聯網與AI使用中的個資風險

行動裝置 與個資安全

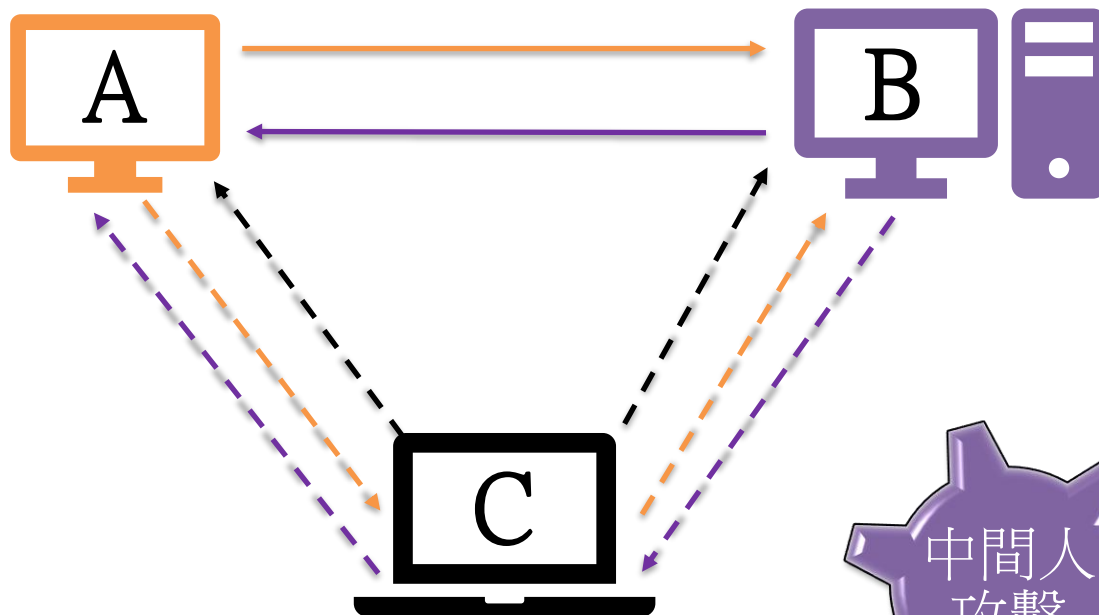


行動裝置與新興技術下的個資挑戰

行動裝置 與個資安全



行動裝置 與個資安全

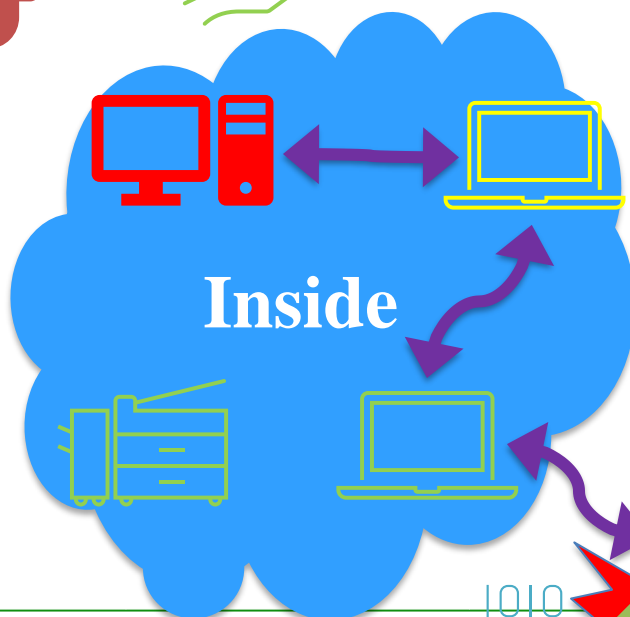


二

行動裝置與新興技術下的個資挑戰

行動裝置
與個資安全

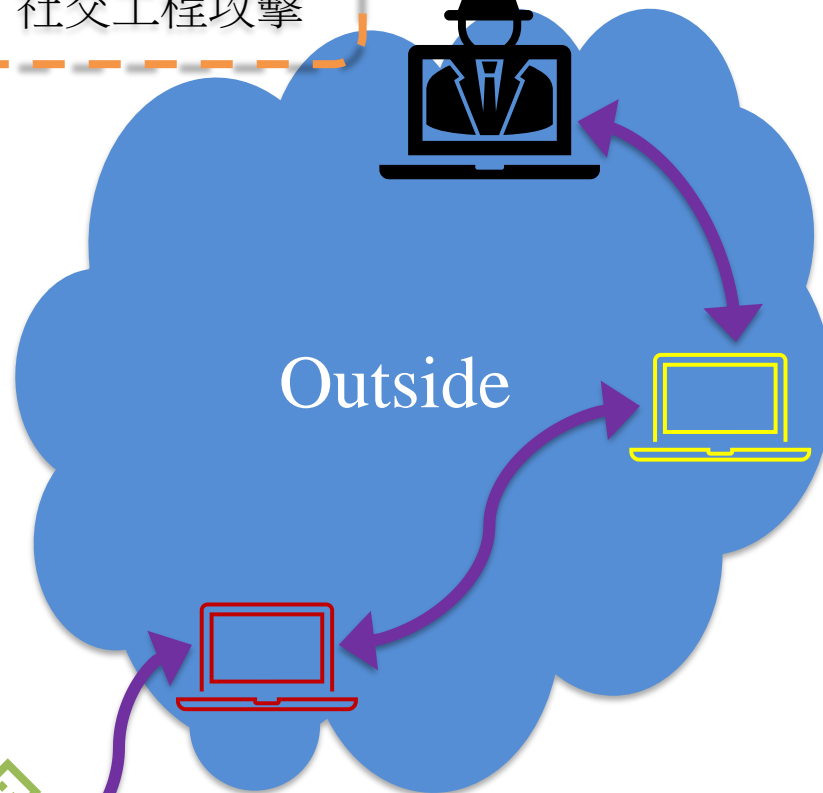
網路區隔之迷失



Inside



社交工程攻擊



Outside

1010
1010



1010
1010

行動裝置 與個資安全



學生發現，當Meta智慧眼鏡結合臉部辨識軟體和搜尋引擎，可以輕易地識別出陌生人的各種個資，包括姓名、年齡、住處等等，引

行動裝置 與個資安全



傳產西進 遭商業間諜入侵系統

作者：張維君 -11/28/2011



許多企業認為自己不是機敏政府單位、也不是知名大廠，不會是駭客攻擊目標。但現今傳出有傳統產業業者到大陸設廠擴點，就被對手僱用商業間諜駭客入侵系統，導致商業機密疑似外洩。西進大陸前，請先做好資安。即便不是設點，只是一般商務出差，也有人使用智慧手機連接無線網路使用Skype通話，導致談話內容全被側錄外洩，研判是因為連結到偽冒的無線基地台。出差大陸前，請先確保行動裝置安全。上週六在淡江大學舉辦的2011聯合國際研討會，與會專家談到現今企業成為入侵攻擊目標的問題已逐漸擴大。

資安人
INFO SECURITY
作對事、用對方法、找對夥伴

警政署資訊室巡官叢培侃指出，駭客攻擊有一套標準作業程序，一旦進到內網就先攻擊AD伺服器，接著側錄所有員工密碼，在更多電腦上安裝木馬、後門程式，以便後續利用。只要一台電腦沒有清理乾淨，駭客還是會繼續自由進出，所以現在的入侵事件很難完全清理乾淨。企業IT人員需要提升對惡意程式的偵測監控能力，不能認為只靠廠商進行一兩次事件調查處理就能解決。

許多的入侵事件，不管是一般駭客入侵，或是所謂進階持續威脅(APT, Advanced Persistent Threat)攻擊。都是從使用者好奇開啓一封信的附件或點選惡意連結開始的。Xecure Lab線上提供免費APT鑑識服務XecScan，如果收到可疑郵件，可將附件檔案上傳做分析，可判別是否為惡意文件及CVE漏洞編號等資訊。

行動裝置 與個資安全

你的手機正在偷拍你？揭露 App 背後的監控真相



你的手機攝影機可能在偷錄你：App 背後的暗黑邏輯

物聯網與AI使用的個資風險



寶寶監視器突傳陌生男說嗨 家長批評系統遭駭不安全

2024-08-02 17:29 聯合新聞網／綜合報導

+ 駭客



Video captured the moment a strange man hacked a Ring camera and whispered to a five-year-old boy in his bedroom

麥可李德的兒子聽見聲音後，驚恐地盯著鏡頭。圖擷自每日郵報

行動裝置與新興技術下的個資挑戰

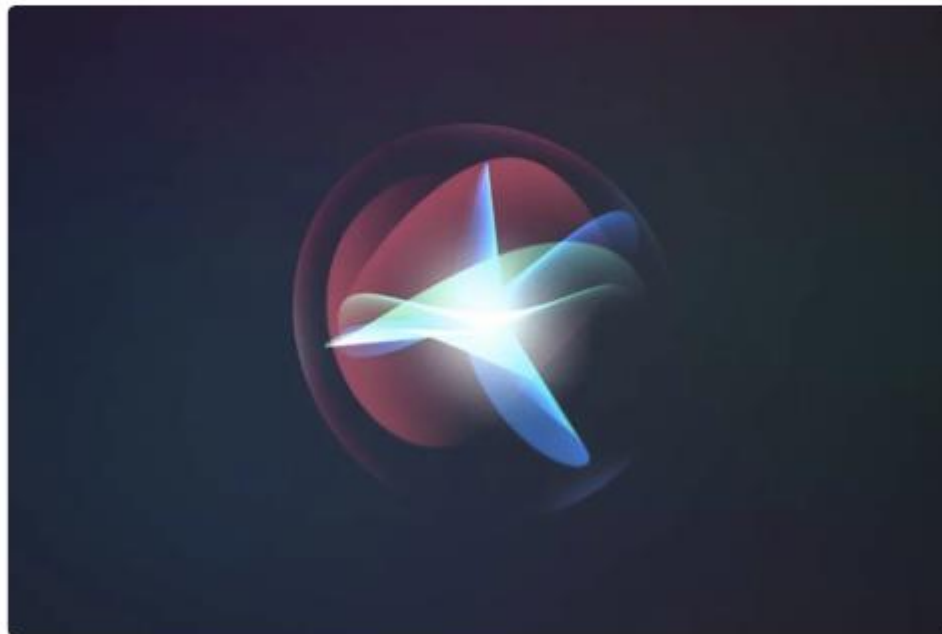
物聯網與AI使用的個資風險

智慧助理成隱私漏洞？小心「同音詞」誤觸...個資、病例全外洩！




林欣穎

2020年3月23日 · 2 分鐘 (閱讀時間)



物聯網與AI使用的個資風險

DeepSeek 資料外洩事件



DeepSeek AI 是一家中國人工智慧公司，專注於大型語言模型和深度學習。該公司被指控抄襲 OpenAI，並且面臨其他版權索賠。此外，外界對其用戶隱私保護及與中國政府的關係也有所疑慮。

近期，DeepSeek 再次陷入風波，超過一百萬用戶的敏感數據遭到洩漏。研究人員在發現 DeepSeek 旗下的一個公開資料庫後，意外獲得了完整的資料庫控制權，能夠訪問內部資料並執行操作。這次洩漏事件中，兩個資料庫被曝光，包含超過百萬條日誌記錄，內含聊天記錄、API 金鑰、後端細節等高度敏感資訊。更嚴重的是，這一漏洞可能允許攻擊者提升權限，進一步掌控 DeepSeek 環境。

這並非 DeepSeek 首次遭遇資安攻擊。事實上，該公司在成立僅一週後就曾遭遇大規模攻擊。此外，DeepSeek 已被多個國家和組織禁用，而這次數據洩漏事件進一步證明了該應用程式的潛在風險。

物聯網與AI使用的個資風險

OpenAI 資料外洩事件



OpenAI 疑似數據外洩：2,000 萬組帳號流出待售

作為 ChatGPT 和其他先進 AI 模型的開發公司，OpenAI，一直處於人工智慧研發的領先地位。然而，即使是資源最豐富的 AI 企業，也無法倖免於網路安全威脅。

近日，暗網（Dark Web）上的駭客聲稱已竊取並洩漏 2,000 萬組 OpenAI 用戶的登入憑證，這可能是一次重大資料外洩事件。一名匿名駭客在論壇上發佈了一則貼文，聲稱掌握了這些帳號資訊，並提供了一部分樣本數據，其中包含電子郵件和密碼，並以低價出售。

駭客有時會誇大這類洩漏事件，以吸引關注或吸引買家，但這次事件的規模已引發警惕。OpenAI 尚未確認或否認該洩漏，但表示正在「認真對待」這些指控。駭客有時會誇大此類說法以引起關注或吸引買家，但這次指控的規模已引起人們的警覺心。OpenAI 尚未證實或否認此次洩漏事件，但表示正在「認真對待」這些指控。

行動裝置資安 風險防範建議

項目	防範措施
裝置安全性	啟用螢幕鎖（指紋、Face ID、強密碼），啟用遠端清除功能
APP 權限管理	安裝前審查APP權限，定期檢查設定，禁用無關存取（如天氣APP存取聯絡人）
加密與連線	使用 VPN 保護資料傳輸，不在公用 Wi-Fi 下登入機敏帳戶
資料備份	定期備份個人資料至安全雲端或本地端

物聯網資安風 險防範建議

項目	防範措施
身分認證	改變預設帳密，設定強密碼，若支援則啟用雙重驗證
設備選購	選擇有資安聲譽、明確隱私政策的品牌
網路隔離	IoT 裝置使用獨立 Wi-Fi 網段，避免與主要工作網段混用
韌體更新	定期檢查並更新韌體，避免使用過時裝置

AI資安風險 防範建議

項目	防範措施
資料匿名化	傳送前移除可識別資訊（如姓名、電話、ID）
公司政策	建立 AI 使用政策，規定不得輸入客戶資料、內部機密
第三方服務 審查	選擇符合 GDPR、個資法規之 AI 平台
權限控管	限定特定角色可使用 AI 工具，並保留操作紀錄

大綱子題

三

雲端與整體資安思維建構

1

雲端資安與個資保護

2

資安行為的建立與組織角色

雲端資安 與個資保護

常見威脅與資料外洩情境

威脅類型	說明
共享連結未設限	使用者將檔案設定為「任何知道連結者可檢視」
權限管理不當	檔案共享給過多不必要的人、離職員工仍保有權限
雲端帳號被駭	密碼弱、未使用 MFA，導致駭客登入雲端帳戶
第三方應用濫用存取權限	連結某些APP或插件取得Google帳號或雲端資料的權限
同步資料未加密	在多裝置同步時，傳輸過程無加密

雲端資安 與個資保護

常見弱點說明

誤設為公開連結、
誤傳機敏資料

使用者操作
不當

無監控機制

無法追蹤誰存取
了哪些雲端檔案、
何時下載

老員工、外部合
作對象仍持有存
取權限

權限未定期
檢查

缺乏安全設
定

未啟用多因素驗
證 (MFA)、未
加密資料

威脅

弱點



風險

雲端資安 與個資保護

使用雲端服務時的安全設定與加密技巧

項目	建議設定
啟用多因素驗證（MFA）	確保即使密碼被竊，駭客也無法登入帳戶
定期檢查分享清單	查看哪些檔案被分享、對象為誰、是否公開
設定明確的存取角色	使用「僅限查看」、「可編輯」、「擁有者」等角色控制
帳戶登入通知與異常活動警示	開啟通知設定，一旦異常登入立即得知

帳戶層級設定（以 Google Drive / OneDrive 為例）

雲端資安 與個資保護

使用雲端服務時的安全設定與加密技巧

資料層級 加密技巧

方法	說明
上傳前手動加密	使用 7-Zip、VeraCrypt 等工具 先將檔案加密後再上傳
雲端原生加密功能	Google Workspace 與 Microsoft 365 提供企業級加密選項
備份資料分層保存	不將所有資料集中存放，避免 一處外洩即全面影響
限制可下載/列印/轉寄權限	可在共享設定中調整，如「僅 檢視、不可下載」

雲端資安 與個資保護

雲端使用安全守則（Google Drive、OneDrive）

項目	安全守則
檔案分享原則	僅分享給需要的人，並設定存取期限（例如 7 天後失效）
禁止公開連結分享機密文件	機密資料請使用特定帳號驗證才能查看
定期清查「已分享項目」	每月一次審查分享紀錄，清除過期或無效的分享對象
勿使用個人帳號處理公司資料	個資法/公司資安政策應強制使用企業帳戶
避免上傳身份證、護照、信用卡等圖片或掃描檔	若需保存，請壓縮加密後再存放，並標註為敏感等級
裝置安全也不能忽略	若手機電腦被盜用，雲端資料仍可能被同步竊取

三

雲端與整體資安思維建構

資安行為的建立
與組織角色

從意識到習慣

不當行為	潛在風險
點擊可疑連結、信件	容易中毒或遭勒索軟體攻擊
密碼設定太弱或重複使用	導致帳號被竊取
將資料私自上傳雲端、用個人裝置處理業務	造成資料流失、外洩風險
不鎖螢幕、裝置借人用	資料未經授權被存取
未定期更新軟體、韌體	系統存在漏洞無法修補

資安行為的建立與組織角色

建立良好資安行為

行為養成與文化 (Culture)

- 將資安視為日常工作的一部分，而非「IT部門的事」
- 鼓勵同仁回報可疑事件、形成「資安即責任」的氛圍



制定政策與流程 (Policy)

- 建立《資安政策》、《個資處理規範》、《可接受使用政策 (AUP)》等
- 對各部門行為做明確界定，例如禁止使用個人信箱處理公務

教育訓練與持續提醒 (Awareness)

- 定期舉辦資安宣導、釣魚信演練、密碼管理教學等
- 使用短影片、海報、Email提醒、螢幕保護圖等多元管道

資安行為的建立與組織角色

角色	職責內容
高階管理層（如董事會、總經理）	提供資源與決策支持，核准資安政策、風險接受範圍
資安主管（CISO / 資安長）	制定資安策略、風險評估、對外稽核、法規遵循
IT 部門 / 系統管理員	維護基礎設施安全、系統更新、權限設定與監控
使用者（全體員工）	遵守資安政策、妥善保護帳號密碼、回報異常事件
資料擁有者（如業務、HR）	確保其管理的資料分類、授權正確，資料使用符合法規
資安稽核與合規人員	定期審查資安執行情況，追蹤缺失與改善成效
外包/協力廠商	遵守組織資安標準、簽訂資安合約（如NDA、SLA）

雲端與整體資安思維建構

資安行為的建立與組織角色

資安行為與組織角色的正確觀念

資安不是技術問題，而是人與行為的問題

資安不是技術問題，而是人與行為的問題

建立制度 ≠ 建立安全；讓制度落實才是真正安全

組織每個人都是資安防線的一部分

管理層態度、制度明確性與教育訓練頻率，是成功關鍵

四 討論