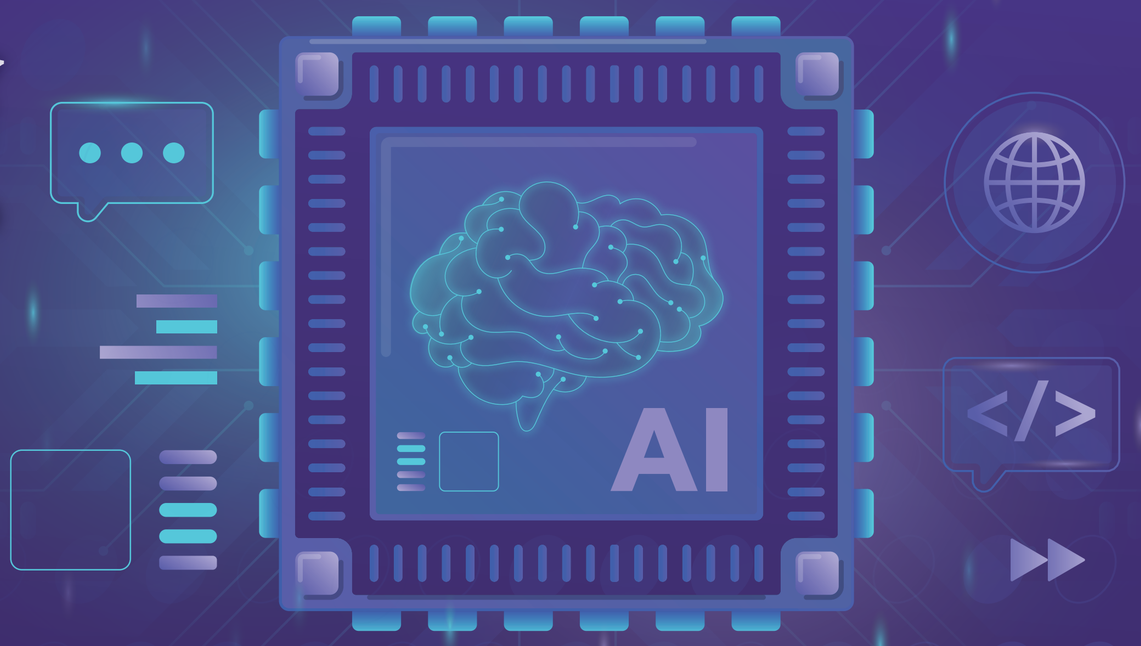
AI應用下的資安風險



課程講師 林子婷
七維思執行長

課程時間 114.07.09
13:30-17:00 (Teams線上)

課程目標

1. 了解 AI Chatbot 如何影響我們的日常生活與工作。
2. 認識使用AI時可能遇到的幾種主要資安風險（例如：被誘導說出不該說的話、看到假訊息等）。
3. 透過實際生活案例，了解 AI 風險的具體樣貌。
4. 學習保護個人資訊、辨識 AI 風險的基本方法。
5. 提升在日常使用 AI 工具時的警覺心與安全意識。

時間	主題	內容
13:30-14:00		報到
14:00-14:30	AI 聊天機器人： 是神隊友還是隱藏危機？	• 揭開 AI Chatbot 的神秘面紗：它們如何思考與對話？ • 從智慧客服到創作夥伴：AI 如何悄悄融入你我的日常？ • 是效率加速器，還是...？盤點 AI 帶來的便利與潛在變數。
14:30-15:30	小心！別讓你的 AI 變成「豬隊友」	• 風險劇本一：當 AI 被「催眠」？ （探索 Prompt Injection 的魔術） • 風險劇本二：跟 AI 說的悄悄話，全世界都知道？ （透視敏感資訊洩露風險） • 風險劇本三：眼見不為憑？AI 創造的逼真「假象」 （直面錯誤資訊挑戰）
15:30-15:40		中場休息
15:40-16:30	企業導入 AI： 不可不知的安全課題	• 當公司擁抱 AI 提升效率，潛藏的安全地雷有哪些？ • 解密 RAG：讓 AI 讀懂公司內部文件，是賦能還是引狼入室？（淺談其中的安全關卡）
16:30-17:00	AI 求生指南： 趨吉避凶，聰明駕馭	• 與 AI 共舞的「安全距離」：哪些話題是禁區？（個資與機密保護守則） • 練就「資訊判讀力」：如何在 AI 生成的內容中去偽存真？ • 數位世界的「基本功」：強化帳號密碼安全，守住第一道防線。 • 養成資安「第六感」：簡單好習慣，讓你安心暢遊 AI 新時代。
17:00-		結束／賦歸

| 主辦單位 | 數位發展部 數位產業署 Administration for Digital Industries, moda | 執行單位 | ACW SOUTH 數位產業署沙崙資安服務基地 財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY