課程名稱：18509_社交工程攻擊防範與識別 課程摘要

🎯 1. 適合對象與能力門檻

- **適合族群**：企業一般員工、資安主管/同仁、MIS 系統管理員，以及金融、保險、證券等受主管機關規範需定期執行社交工程演練的產業從業人員。課程能幫助全員建立資安意識，並協助資安團隊掌握演練與防禦架構。
- **能力門檻**：入門。無需深厚的程式開發背景，課程從人性的弱點與白話社交工程案例切入，逐步延伸至演練設定與 AI 技術應用。

📚 2. 課程核心大綱與架構圖

- **章節架構**：
  - **章節一：社交工程攻擊防範與識別** — 剖析社交工程定義（利用人性弱點）、常見形式（釣魚郵件/簡訊、語音詐騙、技術支援詐騙、彈出式廣告、偽冒搜尋） 及商業詐騙（BEC 郵件偽冒、變更匯款帳號）。
  - **章節二：新型態 AI 與 Web3 社交工程威脅** — 剖析深偽（Deepfake）語音/肖像詐騙、假 ChatGPT 軟體/社團 及 Web3/NFT 加密貨幣詐騙手法。
  - **章節三：社交工程攻擊路徑與 Mail Server 漏洞實作** — 電子郵件社交工程拓撲圖、Open Relay 漏洞利用與偽冒寄件者（Sender Email/Name）實作原理。
  - **章節四：企業內部社交工程演練與測試實務** — 導讀金管會/櫃買中心相關法規、架設演練環境（Mail Spam/Server 白名單開通）與四大偵測指標（開啟信件、點選連結、開啟附件、輸入敏感資料）實作。
  - **章節五：AI 與大數據在社交工程防禦上的應用** — 剖析 NLP 自然語言處理解析內文語意、碎片化資料收集（Mail Header/流量/風格分析） 與 GAN 對抗式樣本訓練。

🛠️ 3. 必備前置知識清單

- **電子郵件基本概念**：了解電子郵件基礎收發（如 Outlook 操作、HTML 內文與附件）。
- **基礎資安與網路常識**：對 Mail Server、Mail Spam 過濾機制及網址（Domain/IP）有基本認知即可。

📖 4. 專有名詞與概念辭典

- **社交工程 (Social Engineering)**：利用人性的弱點（偽冒、恐嚇、好奇心等）採用詐騙手段竊取敏感資料（如帳密、身份證）或財產的攻擊方式。
- **Open Relay**：未設定好安全防護的 Mail Server，允許任何人透過它轉寄信件，常被攻擊者利用來大量發送偽冒社交工程郵件。
- **對抗式範本學習 (GAN 對抗訓練)**：運用 AI 模擬生成釣魚信件範本，同時訓練另一個 AI 進行識別與阻檔，透過反覆對抗學習提升偵測準確率。

💼 5. 課程學習職能對照

- **對應職能名稱**：資訊安全維護工程師 / 企業資安意識推動專員 / 資安合規稽核專員
- **主要工作任務/能力指標**：
  - **社交工程威脅識別與宣導能力**：能辨識各式新型態釣魚郵件、深偽（Deepfake）語音與商業詐騙（BEC），並提升企業全員資安意識。
  - **社交工程演練規劃與執行能力**：能依據金融/上櫃指引規範設計社交工程演練，設定 Mail Server 白名單，並精準追蹤開啟與點選等統計數據。
  - **AI 社交工程防範與偵測觀念**：能理解運用 NLP 自然語言處理與大數據解析語意與風格，協助建立前置預警機制。