資拓宏宇國際股份有限公司
International Integrated Systems, Inc.

社交工程宣導教材

資拓宏宇永遠與您一起創新前進
always innovative always IISI

簡報大綱

一. 為什麼進行社交工程演練?

二. 社交工程是什麼?

三. 社交工程攻擊目的

四. 社交工程攻擊手法

五. 社交工程攻擊流程

六. 常見可疑電子信件特徵

七. 防範社交工程

為什麼進行社交工程演練?

駭客偏好利用社交工程滲透單位網路，成功機率高，使用者不易發現，風險不容輕忽。為有效強化防護能力，需透過社交工程演練，模擬駭客寄送具誘騙性的電子郵件，測試使用者之警覺性與反應，藉此測試及確保：

- ✓ 受測者資安意識的落實狀況
- ✓ 受測者對攻擊行為的防護與警覺能力
- ✓ 受測者使用電子郵件良好的使用習慣

📌唯有結合使用者良好的操作習慣與組織有效的管理措施，才能降低社交工程攻擊帶來的風險。

社交工程是什麼?

社交工程的攻擊對象
主要是人，而不是系統

- 利用人性的弱點或心理特性操縱、欺騙他人
- 從而取得資訊、存取權限、金錢或進一步入侵系統的手法。與傳統駭客技術不同，

社交工程攻擊目的

1. 騙取**帳號與密碼**
2. 蒐集**個資與敏感資料**(如:信用卡資訊)
3. 誘導下載**惡意程式**或附件
4. 誘使**執行高風險行為**(如:關閉防毒軟體)

社交工程攻擊手法

網路釣魚（Phishing）
-假冒Email或網站，誘騙使用者輸入帳號密碼或點擊惡意連結

魚叉式攻擊（Spear Phishing）
-有針對性地攻擊特定個人，內容精準，信任度高

語音釣魚（Vishing）
-假冒客服或機關來電，誘導提供帳號、OTP或信用卡資料

簡訊釣魚（Smishing）
-假冒簡訊通知（如：包裹、警示），附帶惡意連結或QR碼

假冒（Pretexting）
-假裝是親友、同事或主管，編造情境誘騙交出資料或操作設備

社交工程演練攻擊流程

INVESTIGATION 調查

1. 做攻擊前準備

- 確定受害者
- 收集背景訊息
- 選擇攻擊方法

HOOK 鉤

2.欺騙受害者以獲得立足點

- 吸引目標
- 編造故事
- 控制目標

PLAY 執行

3.獲取一段時間內的訊息

- 擴大立足點
- 執行攻擊
- 破壞業務或/和竊取數據

EXIT 離開

4.關閉互動不引起懷疑

- 刪除惡意軟體
- 覆蓋足跡
- 使攻擊自然結束

為什麼進行社交工程演練?

駭客利用社交工程滲透單位網路，成功機率高，風險不容輕忽。

為有效強化防護能力，需透過社交工程演練，

模擬駭客寄送具誘騙性的電子郵件，藉此測試及確保：

- ✓ 受測者資安意識的落實狀況
- ✓ 受測者對攻擊行為的防護與警覺能力
- ✓ 受測者使用電子郵件良好的使用習慣

📌唯有結合使用者良好的操作習慣與組織有效的管理措施，才能降低社交工程攻擊帶來的風險。

常見可疑電子信件特徵

- 非業務相關或非平時有業務往來信件。/ 陌生人或少往來對象來信。
- 認識的人來信，但來自奇怪的email或信件主旨、內容與習性不符。
- 署名政府機關，或附加檔案名稱及內文看似公務信件，但由非政府機關網域.gov.tw（如gmail, yahoo...等）寄出。
- 過於聳動的主旨與緊急要求。
- 不正常的發信時間。
- 信件內文含簡體字或大陸用語。
- 要求輸入敏感資料(如身份證號、帳號、密碼)送出。
- 附加檔案有開啟密碼,且密碼可見於郵件本文。

防範社交工程-郵件安全三步驟

停 我為什麼會收到這封信？

? 確認**寄件來源是否可信**
? 想一想：我是不是應該收到這封郵件？
? 是否**與目前的業務工作有關**？

看 這封信內容合理嗎？

? 檢查**郵件主旨是否正常、有無誇大恐嚇字眼**
? 檢查**寄件人信箱是否與身分相符**
? 檢查是否**包含不尋常附件或連結**

聽 我需要開啟或點選嗎？

若不是日常業務信件 → 建議不要開啟

點擊前請先：

✓ 滑鼠移至連結上方 → **確認網址是否正確**
✓ 附件請先「**另存新檔並掃毒**」再開啟