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

社交工程宣導教材

always innovative ,always IISI

大綱

1. 社交工程是什麼？
2. 為什麼進行社交工程演練?
3. 社交工程演練的流程
4. 常見可疑電子信件特徵
5. 停、看、聽
6. 釣魚郵件樣態

社交工程是什麼？

- 在資訊安全的背景下，社交工程是對人們進行心理操縱以執行操作或洩露機密訊息，是一種以資訊收集、欺詐或系統訪問為目的詐騙伎倆。它不同於傳統的“騙局”，因為它通常是更複雜的欺詐計劃中許多步驟之一。
- 它也被定義為「影響一個人採取可能符合也可能不符合其最佳利益行動的任何行為」。
- 社交工程的例子是在大多數需要登錄的網站上使用「忘記密碼」功能。安全性不高的密碼恢復系統可用於授予惡意攻擊者對用戶帳戶的完全訪問權限，而原始用戶將無法訪問該帳戶。

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。
- 模擬駭客寄送各種誘騙的測試信件，嘗試誘騙受測者並測試受測者之警覺性，瞭解受測者
  - 資安意識的落實狀況，
  - 對社交工程、網路釣魚等誘騙攻擊行為的防護與警覺能力。
- 使用者良好的使用習慣與有效的管理措施，才能避免此類風險。

社交工程演練的流程

1.做攻擊前準備
- 確定受害者
- 收集背景訊息
- 選擇攻擊方法

2.欺騙受害者以獲得立足點
- 吸引目標
- 編造故事
- 控制目標

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

4.關閉互動，最好不要引起懷疑
- 刪除所有惡意軟體
- 覆蓋足跡
- 使攻擊自然結束

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位址或信件主旨、內容與其習性不符。
- 署名政府機關，或附加檔案名稱及內文看似乎是公務信件，但由非政府機關網域.gov.tw（如gmail, yahoo, pchome, hinet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。
- 要求輸入私密資料(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。

停、看、聽

- 我為何會收到這封郵件？
  - 確認寄件來源及寄件者
- 我是不是應該收到這封郵件？
  - 確認郵件主旨及郵件內容是否與本身的業務工作相關
- 我是否應該開啟這封郵件？
  - 是否與業務工作相關
  - 不開啟連結是否有影響
  - 審慎查證
- 我是不是有必要開啟附件或點選連結？
  - 如需開啟注意連結是否正確
  - 開啟任何郵件的附件檔前，請記得「另存新檔」掃毒後再開啟

視為詐騙成功-開啟信件

- **透過預覽或點開方式開啟，信件本文內所含圖片亦完成圖片下載之動作，認定為誘騙成功。**
- 電腦如何防止詐騙成功
  - 收信程式安全設定為不會自動下載圖片，即使預覽功能設定為開啟，或是直接打開誘騙信件，因無下載圖片之動作，不會造成安全漏洞，將不會記錄為誘騙成功。
  - **郵件閱讀 - 應設定為純文字模式**

視為詐騙成功-點選連結

- 受測人員點選信件內文中之連結網址，將被記錄為誘騙成功。
- 如何防止詐騙成功
  - **郵件中有超連結不可點選。**

釣魚郵件樣態

信件類別	信件主旨
公務類	【公告】一百一十三年政府行政機關辦公日曆表搶先看
公務類	【公告】轉知國民旅遊卡相關事項
公務類	【公告】一百一十三年公教人員健檢辦法
公務類	【公文】檢送本部第912(擴大)部務會報紀錄1份
生活類	台電 e-Bill 113 年 5 月電費通知
購物類	您的訂單#2302RW97V1166M已送達
健康類	稀飯配「肉鬆」過量恐致癌，大腸癌增 18%
旅遊類	2024韓國旅遊美食攻略！精選8 間餐廳推薦
資訊類	【圖解】職人必收 30 組 AI 神器！
金融類	中國信託-方便付交易結果通知