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

社交工程(Social Engineering)

定義	係指透過與他人的合法交流，影響對方心理狀態，使其做出某些動作或者是透露一些機密資訊的互動過程。
途徑	➢ 利用人性的弱點，使對方產生行動或回應。 ➢ 透過電子郵件、手機APP、實體接觸等途徑。
目的	➢ 竊取資訊。 ➢ 詐騙受害人。 ➢ 影響個人或團體行為。

社交工程仍為資安風險之首

iThome 2025 CIO & CISO 大調查：2025資安風險排名

政府學校三大首要資安風險：網路釣魚、DDoS攻擊和個人資料外洩

資料來源：iThome 2025 CIO & CISO 大調查，2025年

%數值為將該項資安風險視為高衝擊、未來一年發生風險很高的企業比例。數值高於該類平均的項目，列為該類首要資安風險

社交工程常見的攻擊管道

QR Code

- 利用假 QR Code 導向釣魚網站或惡意下載頁面
- 常見於活動海報、包裹通知、停車繳費等

社群平台

- 假冒熱門貼文、影音連結或抽獎活動
- 連結可能導向釣魚網頁或誘導下載惡意程式

Email

- 偽裝成官方通知、訂單確認或內部信件
- 夾帶惡意附件或誘導點擊釣魚連結

Line或簡訊

- 透過熟人或官方名義降低戒心
- 內容包含釣魚連結、假客服或假優惠訊息

社交工程電子郵件範例

- 駭客通過模仿公務機關名義發送社交工程郵件，試圖竊取企業與個人的敏感資訊。

資料來源： https://www.twcert.org.tw/tw/cp-104-10015-84f6f-1.html

社交工程的關鍵脆弱點

- 目前**沒有任何產品或安全系統**可以為電子郵件社交工程提供100%的防護並同時兼顧電子郵件使用者的個人需求。
- **員工對安全防護認知的不足與輕忽**成為資通安全的一大漏洞，即使投資了各種網路防護的軟硬體，並安排資安教育訓練課程等，其結果仍可能不堪一擊。

常見的網路社交工程手法

- **常見的詐騙與攻擊手法：**
  - 假冒為同事或新進員工
  - 假冒廠商、客戶或政府單位
  - 假冒具有權威的人
  - 假冒系統廠商，表示欲提供系統修補程式或更新程式
  - 假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援...等。
  - 使用**流行或特定關心的議題**

都有一個假網址

- **社交工程攻擊常鎖定的目標：**
  - 一般人員
  - 新進員工或特定業務人員

社交工程電子郵件防範

Tip 1
誰寄的？

別相信呈現的「寄件者名稱」及「email地址」

- 釣魚信件常用的技巧之一就是假冒電子郵件的顯示名稱，甚至email 地址都可以假冒
- **【技巧】將滑鼠移到寄件者名字上會出現相關訊息**

Tip 2
信件主旨

留意信件主旨中的緊急或威脅字眼

- 常見的釣魚/詐騙手法就是企圖激發收信者著急或恐慌的反應
- **【技巧】不要緊張，先根據其它要點判斷信件真偽**

資料來源：台灣大學 https://www.cc.ntu.edu.tw/mailtips/index.html

社交工程電子郵件防範

Tip 3
信件寫法

睜大眼睛看清楚拼字是否正確

- 假冒信件常會用混淆視聽手法，故意把網址或email address拼錯
- **【技巧】正式通知信件絕對不會使用簡體或英文內容**

Tip 4
信寫給誰的？

信中的稱謂很重要！

- 信件開頭稱謂如果是很模糊的稱謂，例如：親愛的用戶、尊敬的用戶、Dear Google user、Dear Sir/Madam等，最好提高警覺！

資料來源：台灣大學 https://www.cc.ntu.edu.tw/mailtips/index.html

社交工程電子郵件防範

Tip 5
信是誰寫的？

注意信件的署名

- 信件末尾若未提供詳細的署名或聯絡方式，很可能就是釣魚信件
- **【技巧】相關通知信件一定會留下單位名稱及承辦人連絡方式**

Tip 6
看清網址連結

看看就好，不要點下去！

- 請注意網址URL和來信方的關係，詐騙信件經常會故意混淆或拼錯網址
- **【技巧】把滑鼠游標移到信件中的連結上，就會顯示連結的真正網址**

資料來源：台灣大學 https://www.cc.ntu.edu.tw/mailtips/index.html

社交工程電子郵件防範

Tip 7
小心信件附件

切勿點開信件附檔

- 若非認識或正在等待的信件，**切勿打開任何信件的附檔**
- 附檔類型是可以偽裝的，看起來是圖片，可能實際上內藏惡意程式

Tip 8
注意回信內容

千萬不要在信中提供個人資訊！

- **來路不明**或無聯繫的政府機關、校方、銀行、企業信件**絕對不會主動要求**在電子郵件中提供個人資訊
- 不要在信件中提供帳號和密碼！

資料來源：台灣大學 https://www.cc.ntu.edu.tw/mailtips/index.html

社交工程電子郵件防範

- Q:為何我會收到這封郵件?
  - 寄件人不認識就不要開啟
- Q:我是否應該收到這封郵件?
  - 與業務或本身職務無關主旨不要開啟
  - 信件主旨雖與業務有關，但寄件者郵件非公務信箱
- Q:我是否應該開啟這封郵件?
  - 與業務或本身職務無關
  - 不隨意點選郵件超連結

養成良好習慣杜絕社交工程攻擊

- 勿瀏覽來路不明或未受信任的網站。
- 勿下載來源不明的檔案或安裝未知軟體。
- 勿使用來源不明的 USB、記憶卡等外接儲存裝置。
- 勿點擊不明連結或開啟可疑電子郵件附件。
- 勿隨意掃描來源不明的 QR Code。
- 接獲要求提供帳號、密碼或驗證碼時，應先查證對方身分。
- 啟用多因素驗證（MFA），降低帳號遭盜用風險。
- 定期更新作業系統、瀏覽器及應用程式。
- 外寄含有個人資料或機敏資訊之檔案時，應採取加密保護措施。
- 發現可疑郵件或訊息時，應立即通報資訊單位或相關窗口。