資訊安全宣導

資訊安全人人有責

01

電子郵件

01

惡意電子郵件常見攻擊手法

- 假冒的寄件者名稱。
- 利用業務、聳動的時事電子郵件主指。
- 網路釣魚 (Phishing) 是透過電子郵件手段的一種社交工程，藉由誘惑使用者點選網頁連結。
- 網路釣魚連結範例：
  - https://www.paypal.com (真)
  - https://www.paypa1.com (假)
- 含惡意程式的附件。

01

電子郵件停看聽 (收信)

- 為何我會收到這封郵件？
  - 審慎查證寄件來源及寄件者。
  - 不明郵件應立即刪除。
- 我是否應該開啟這封郵件？
  - 確認郵件主旨是否與業務工作相關。
  - 確認有沒有威脅利誘的字眼？有沒有詐騙的可能？
- 我是否應該點選這封郵件附檔及連結？
  - 評估不開啟連結或檔案是否有影響。
  - 不直接開啟檔案，另存新檔案後再使用相關軟體開啟。
  - 開啟連結或檔案前，確認對應軟體 (如：瀏覽器、Office、壓縮軟體) 維持最新的更新狀態。

01

電子郵件停看聽 (轉信或回信)

- 我是否該轉寄這封郵件？
  - 不轉寄未經查證之訊息及不明郵件。
  - 轉寄郵件前應先刪除他人郵件地址，避免別人的郵件地址傳出。
  - 寄送信件給群組收件者時，應將收件者列在密件副本，以免收件人資訊外洩。
- 我是否應該回覆這封郵件？
  - 審慎查證寄件來源及寄件者。
  - 不輕易填寫個人資料、帳號密碼。

02

電腦應用

02 應用軟體安裝

- 個人電腦原則僅安裝業務所需軟體，安裝前應確認取得合法授權。
- 不得將授權軟體轉借或給予未經授權人員使用。
- 不得任意關閉、移除或卸載公司所安裝之資安防護軟體。
- 使用私有、試用、免費共享軟體時應考量系統安全性，避免危及公司電腦或網路安全。
- 如發現使用非授權的軟體，由使用者自行負責相關法律責任。

02 應用系統更新

- 當軟體使用一段時間後，通常會出現一些小問題或安全漏洞，這些漏洞也是駭客容易利用的弱點，零時差攻擊是目前駭客最喜歡利用的手法。
- 大部分軟體都會提供「自動更新」功能，隨時注意軟體更新的相關資訊，尤其是安全性的更新，必要時須立即採取更新動作。
- 檢查電腦作業系統之「Windows Update」是否已更新至最適狀態。

02 安全的密碼原則

- 以注音輸入法按鍵來當成密碼。
  - 範例：你好嗎 → su3cl3a87
- 以英文字或數字穿插。
  - 範例：Sister + 456789 → S4i5s6t7e8r9
- 以英文的一句諺語或一段歌詞取每個英文字字首當成密碼。
  - 範例：Best wishes for a happy New Year！ → BwfahNY！

03

網路應用

03 使用網路注意事項

- 不得任意更改個人電腦 IP 位址與網路卡相關資訊。
- 不得將私人個人電腦、筆記型電腦連接公司網路，若因公務需要請向資訊部門申請及登記相關網路 MAC 資訊。
- 不得使用點對點 (Peer-to-Peer, P2P) 分享軟體。

END