106年
防範惡意電子郵件
社交工程宣導

長庚大學　資訊中心

目錄

一、106年度教育部社交工程演練

測試對象及時程

- 測試對象：校長、副校長、一級主管占40%、
  一般行政人員占60%
- 第1次集中演練：4-6月
- 第2次集中演練：7-9月
- 演練結果揭露：預定於6月及10月
  （若開啟檢測信須接受講習）

社交工程演練測試信件摘要表

主旨看似正常，卻都是教育部的檢測信！

信件類別	寄件者	信件標題
時事類	1Thome<1theme@yahoo.com.tw>	駭客攻擊8 家券商 金管會：恐還有下波
知識類	黃泰豐<larry1217@gmail.com>	「食色性也」不是孔子說的
健康類	綠色地球<xm4nk499@yahoo.com>	別再用寶特瓶裝水了！各項研究告訴你它可怕的真相！
美容類	Hellen<hellen520@gmail.com>	染唇妝過時啦！2017跟著李聖經擦上微醺MLBB唇才最潮
生活類	韓流最前線<girlpretty@hotmail.com>	變更嬌小，惹人疼！「胖胖單品」逆轉勝
新奇類	李蓉芬<melody8056@msa.hinet.net>	小二生超狂造句 讓網友驚呼：他超懂人性
美女類	杜肯<kentdo5717@outlook.com>	正妹車服員神到了 曾是黑澀會美眉
科技類	新北資訊通<newtaipeinews@yahoo.com>	新北打造智慧城 力推手機無線充電服務
旅遊類	LIME news<limemews@hotmail.com>	領務局LINE 新功能 出國旅遊添保障
財經類	巨富網<richnessnet@outlook.com>	貨幣戰開打？中國單月狂拋660億美元美債！創5年新高

演練方式

- 偽冒郵件類型：以公務、個人或公司行號等名義
- 郵件主題：政治、公務、健康養生、旅遊等類型
- 郵件內容：包含**連結網址**或**word附檔**
- 開啟郵件或點閱郵件所附連結或檔案時，即留下紀錄。
- 若**使用自動預覽功能**，因該應用程式自動執行開啟才能供使用者預覽，**等同開啟該封電子郵件**。
- 開啟惡意郵件或點閱惡意郵件附件內容人員，需進行教育訓練。

演練目的

- 為提高學校人員警覺性
- 降低社交工程攻擊風險
- 強化人員資安意識
- 檢驗社交工程防制宣導成效

防範方式

- 關閉預覽視窗避免誤擊社交工程信件
- 發現不明帳號信件不開啟且立刻刪除
- 避免使用公務信箱開啟非公務信件

二、社交工程

何謂社交工程?

利用人性弱點，
應用簡單的溝通
和欺騙技倆。

獲取帳號、
密碼、
身分證號碼或
其他機敏資料。

突破校園的
資通安全防護

行非法的存取、
破壞行為

攻擊目的

竊取
機密檔案
及文件

蒐集
針對性
資料

蒐集
使用者
個人資料

竊取
部落格或
社群網站之
帳號密碼

竊取
商業機密
資料

成為
跳板、
殭屍電腦

監控
使用者行為

竊取
網路服務之
有價財產

各種社交工程攻擊手法

利用電話
佯裝資訊人員，
騙取帳號及
密碼。

偽裝維護人員、
上級單位人員，
騙取帳號及密碼。

利用電子郵件
誘騙使用者
登入偽裝網站，
騙取帳號及
密碼。

利用電子郵件
誘騙開啟檔案、
圖片，以植入
惡意程式、暗中
收集機敏性資料。

利用工具軟體、
檔案、圖片誘騙
下載，乘機
植入惡意程式，
暗中收集
機敏性資料。

利用通訊軟體，
偽裝親友來訊，
誘騙點選連結後
植入惡意程式。

三、如何防範惡意電子郵件

惡意電子郵件常見攻擊手法

假冒寄件者

利用與業務、
聳動的時事
電子郵件主旨

含惡意程式
的附件

利用應用程式
之弱點，包括
零時差攻擊

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）維持最新更新狀態。

電子郵件停看聽-轉信或回信

- **我是否應該轉寄這封郵件?**
  - ☑不轉寄未經查證之訊息及不明信件。
  - ☑轉寄郵件前應先刪除他人郵件地址，避免別人郵件地址傳出。
  - ☑寄送信件給群體收件者時，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。

四、電子郵件安全設定
關閉郵件預覽

- **Webmail**

  1.選取【查看】→【Reding Pane】→選擇【關閉】

  2.選取【偏好設定】→選擇【郵箱】→【顯示郵件】的【郵件預覽】不勾選【顯示郵件清單中的細微項目】→【儲存】

- **Gmail**

  1.右上方齒輪按鈕→【設定】→【研究室】→【預覽窗格】→選擇【停用】→【儲存變更】

  2.右上方齒輪按鈕→【設定】→【一般設定】→【文字片段】→點選【沒有部分資訊】→【儲存變更】

- **Outlook 2007 / 2010 / 2013 / 2016**

  選取【檢視】→【讀取窗格】→選擇【關閉】

- **Outlook express**

  選取【檢視】→【版面配置】→不勾選【顯示預覽窗格】

- **Windows Live Mail**

  選取【檢視】→【版面配置】→【讀取窗格】→選擇【關閉】

使用純文字開啟郵件

- **Webmail**

  選取【偏好設定】→【郵箱】→【顯示郵件】中【郵件顯示方式】點選【作為文字】→【儲存】

- **Outlook 2016 / 2013 / 2010**

  選取【檔案】→【選項】→【信任中心】→【信任中心設定】→【電子郵件安全性】
  →勾選【以純文字讀取所有標準郵件】

- **Outlook 2007**

  選取【工具】→【信任中心】→【電子郵件安全性】→勾選【以純文字讀取所有標準郵件】

- **Outlook express**

  選取【工具】→【選項】→【讀取】→勾選【以純文字方式讀取所有郵件】

- **Windows Live Mail**

  選取【工具】→【選項】→【讀取】→勾選【以純文字方式讀取所有郵件】

關閉外部圖片下載功能

- **Webmail**

  選取【偏好設定】→【郵箱】→【顯示郵件】不勾選【自動顯示外部傳入HTML郵件中的圖片】→【儲存】
- **Gmail**

  右上方齒輪按鈕→【設定】→【一般設定】→點選【顯示外部圖片時，必須先詢問我】→【儲存變更】
- **Outlook 2016 / 2013 / 2010 / 2007**

  選取【檔案】→【選項】→選擇【信任中心】→【信任中心設定】→【自動下載 】→ 勾選【不自動下載 HTML 電子郵件訊息或 RSS 項】 、【 當編輯、轉寄或回覆電子郵件時，在下載內容前先警告我】，以及其餘選項不勾選 →【確定】
- **Outlook express**

  選取【工具】→【選項】→【安全性】→勾選【阻擋HTML電子郵件中的圖片及其他外部內容】 →【確定】
- **Windows Live Mail**

  點選左上方的【展開鈕】 → 【選項】→【安全性選項】→勾選【阻擋 HTML 電子郵件中的影像和其他外部內容】→【確定】

Thank You

長庚大學　資訊中心