

# 國立彰化師範大學附屬高級工業職業學校

## 114 年度國教署防範惡意電子郵件

### 社交工程演練計畫注意事項

114-04-23

#### 壹、演練說明：

1. 演練期間：114 年 5 月至同年 11 月止，期間辦理 2 次演練。
2. 演練方式：每次演練作業，依演練對象提交之參與人員名單，按人員類型隨機選取 35 人為受測人員，未滿 35 人者則全數列入。主管人員被挑選為受測人員原則佔參與人員總數 30%以上（主管類型如有不足 30%則視情況調整），每次測試會針對每位受測人員寄送 4 封(含)以上社交工程演練測試郵件。
3. 社交工程演練郵件型態：以偽冒公務、個人或公司行號等名義，發送社交工程演練郵件給受測人員，包含 3 種不同郵件，主題分別為八卦、休閒、保健、財經、新奇、時事、模擬等類型實際社交工程郵件，包含社交工程郵件開啟、內文連結網址開啟、附件檔案開啟等社交工程樣態。
4. 本校承辦人窗口：資安小組廖茂松，分機 207 或 223

#### 貳、評量標準

一、演練評量項目(各次演練作業，各演練對象分別計算)

##### (一)社交工程郵件開啟率

1. 由國教署統一計算，計算方式：參與單位開啟演練郵件人數/參與單位總受測人數。
2. 郵件透過預覽或點開方式開啟，且信件內文之圖片亦完成下載，始認定為誘騙成功。

##### (二)社交工程郵件連結點閱率

1. 由國教署統一計算，計算方式：參與單位點選演練郵件內文連結網址之人數/參與單位總參與人數。
2. 參與人員點選郵件內文中之連結網址，將被記錄為遭誘騙成功。同封郵件內文如包含多個連

結，參與人員不論點選幾個都將記錄為 1 次。

3. 因將來路不明的危險信件轉寄給他人會造成更大傷害，故這類行為所導致之郵件開啟、連結點選，將列入轉寄者之受測紀錄。

### (三) 社交工程郵件附件開啟率

1. 由國教署統一計算，計算方式：參與單位開啟演練郵件附件之人數/參與單位總參與人數。
2. 參與人員開啟郵件內文中之夾檔附件，將被記錄為 遭誘騙成功。同封郵件參與人員不論點選幾次附檔，都將記錄為 1 次。
3. 因將來路不明的危險信件轉寄給他人會造成更大傷害，故這類行為所導致之郵件開啟附檔，將列入轉寄者之受測紀錄。

## 二、演練目標

- (一) 社交工程郵件開啟率：各次演練作業，各演練對象開啟率應低於 10%(含)。
- (二) 社交工程郵件連結點閱率：各次演練作業，各演練對象點選率應低於 6%(含)。
- (三) 社交工程郵件附件開啟率：各次演練作業，各演練對象附件開啟應低於 2%(含)。

## 參、演練結果

- 一、由國教署彙整及統計各次演練結果，於作業完成後一個月內，將執行情形及成果報告送交教育部；演練成果報告之概要，亦將函送各參與對象。
- 二、社交工程演練完全由國教署主持，所有的演練記錄皆存放在國教署，國教署會將演練結果呈報教育部，人員誤點演練信件都會有個人記錄，請師長同仁多加注意自身權益。
- 三、誤點演練測試信件師長同仁將依國教署規定提報改善計畫進行教育訓練。

## 肆、注意事項

- 一、請務必將教育雲電子信箱預設信件讀取方式(包含使用其他收信軟體)改為『純文字』，降低風險！
- 二、禁止將教育雲公務信箱『轉寄』至其他私人信箱。

- 三、手機欲收教育雲信件請使用 Mail2000 APP 收信，勿使用手機內建軟體收信。
- 四、何謂電子郵件社交工程？可參閱彰師附工社交工程演練專頁相關說明，網址：  
<https://sites.google.com/g-mail.sivs.chc.edu.tw/social-engineering/>
- 五、點閱信件前，請多注意該信件是否為您所要之信件，不要因好奇而點閱。

伍、對於防範電子郵件社交工程，一般使用者可多注意以下細節。

郵件讀取：

1. 檢查確認寄件者(是否為認識的人或業務需要)。
2. 檢查確認郵件主旨(是否為奇怪的主旨或與寄件者不搭配)。
3. 不輕易開啟郵件中的超連結以及附件。
4. 重要檔案可雙方約定密碼，並對檔案加密後傳送。
5. 開啟超連結或檔案前，確認對應軟體(如 Windows、IE、Office)都保持在最新的修補狀態。
6. 檢查是否有必要提供個人資訊。
7. 若懷疑郵件來源，透過電話或其它方式向寄件人於開啟前確認。

轉信或寄信：

1. 未經查證之訊息，不要轉寄。
2. 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址轉寄出去。
3. 寄送郵件給群體收件者時，應將收件者列在密件副件，以免收件人資訊外洩。
4. 勿將公務信件轉寄私人電子信箱地址。

變更收信軟體的設定，也可以提高安全性。

1. 不要自動下載圖檔。
2. 關閉郵件預覽功能。
3. 以純文字開啟郵件。