

# 111 年度國立臺南特殊教育學校 防範惡意電子郵件社交工程演練計畫

111 年 10 月

- 一、為提高國立臺南特殊教育學校(以下簡稱本校)及資安警覺性以降低電子郵件社交工程攻擊風險，規範電子郵件社交工程防制年度目標、舉辦相關資安教育訓練及宣導、規劃辦理演練作業，以強化人員資安意識並檢驗各機關宣導電子郵件社交工程防制成效，特訂定本施行計畫。
- 二、本施行計畫演練時間係採無預警不定期方式，每年至少辦理一次電子郵件社交工程演練。
- 三、參與電子郵件社交工程演練為本校所有教職員工，參與演練人數為具有公務電子郵件人數之四分之一以上。
- 四、本施行計畫之教育訓練要點如下：
  - (一) 依行政院函頒之「資通安全責任等級分級辦法」，各機關應按其資安等級，每年定期舉辦資安教育訓練。
  - (二) 資安教育訓練應納入電子郵件社交工程防制有關之認知宣導，並著重攻擊實例說明。
  - (三) 要求本校所有教職員工之個人電腦、電子郵件軟體，關閉郵件自動預覽功能，並將郵件設定為純文字閱覽模式，可在第一時間讓使用者再次確認該封郵件是否為社交工程電子郵件，避免誤點閱該郵件。
- 五、本施行計畫之演練方式：
  - (一)、演練時程：自本即日起至 12 月底為址，期間辦理 1 次演練。
  - (二)、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，郵件主題分為八卦、休閒、保健、財經、新奇、時事、模擬實際社交工程樣本等類型，郵件內容包含連結網址或 附檔。
- 六、電子郵件社交工程演練結果處理如下：
  - (一) 本部資訊處於完成演練作業後，應檢討辦理情形及演練結果，並將演練情形報告彙整後，於每次演練完成後送管理審查會備查。
  - (二) 演練未達基準者，應提出檢討及改善計畫(格式如附件一)。
  - (三) 對演練時開啟或點閱社交工程電子郵件人員，由首長(單位主管)予以口頭告誡，並強制要求參加至少一小時之補強教育訓練及測驗。
  - (四) 演練時開啟或點閱社交工程電子郵件人員如因故無法參加補強教育訓練者，應於一週內自行至相關公務人員數位學習平台網站完成相關課程，並經測驗合格後方算完成。未完成者停止其電子郵件之使用至完成為止。已參加補強教育訓練，但測驗仍不合格者比照辦理。

## 附件一：電子郵件社交工程演練未達基準檢討與改善計畫

### 電子郵件社交工程演練未達基準檢討與改善計畫

#### 一、演練結果概述：

(說明及比較分析去年度演練結果)

#### 二、未達基準原因檢討：

(瞭解歸納同仁開啟演練信件原因以為預防)

#### 三、改善策略及作為：

(含本部要求辦理之教育訓練對開啟人員口頭告誡等各項措施以及機關(單位)自訂之改善策略及作為，如對重點對象(連續 2 次演練均開啟、開啟多封演練信件)之加強措施等)

#### 四、改善辦理情形：

(說明前項相關改善策略及作為之辦理情形)

#### 五、結語：