

# 107 年度臺灣學術網路 防範惡意電子郵件社交工程演練服務計畫

107 年 4 月

## 壹、目的

為提高教育體系各學校人員警覺性以降低社交工程攻擊風險，特訂定本計畫，舉辦相關資安教育訓練與宣導、規劃辦理演練服務作業，以強化人員資安意識並檢驗機關宣導社交工程防制成效。

## 貳、對象

依「政府機關(構)資通安全責任等級分級作業規定」(如附件 1)，辦理對象如下：

- 一、資安等級 A 級單位—教育部(以下簡稱本部)、臺灣大學醫學院附設醫院、成功大學醫學院附設醫院、陽明大學醫學院附設醫院。
- 二、資安等級 B 級單位—臺灣學術網路(TANet)區網中心及縣(市)教育網路中心、各公私立大學、教育部各部屬機關(構)。
- 三、受測人員包括學校正、副校長(正、副首長)、一級主管及一般行政人員。

## 參、演練說明

### 一、演練方式

統一由本部集中辦理演練，每單位每次演練寄送 100 封郵件，其中正、副校長及一級主管寄送 30 封，一般行政人員寄送 70 封。

### 二、教育訓練

1. 依 105 年 6 月 23 日行政院頒「國家資通安全通報應變作業綱要」

辦理，各機關應按其資安等級，每年定期舉辦防範惡意電子郵件社交工程演練。

2. 資安教育訓練應納入社交工程防制有關之認知宣導，並著重攻擊實例說明，各機關學校人員每年至少需接受 1 小時社交工程防制宣導講習。
3. 宣導課程應分兩階段辦理：
  - (1) **第一階段（於演練作業辦理前）**：各機關學校應針對單位所有一級主管、行政人員，全面性實施教育訓練。
  - (2) **第二階段（於演練作業完成後）**：針對開啟惡意郵件比例較高、點閱惡意郵件所附連結或檔案之人員再次進行教育訓練加強宣導，以強化其警覺性。

### 三、演練時程

1. 提報演練名單：請於 4 月 13 日前提報受測人員之電子郵件帳號（如附件 2），並標記正、副校長及一級主管，演練名單資料請直接以電子郵件方式寄送給教育部資科司 李紀緯先生 (moe\_infosec@mail.moe.gov.tw)。
2. 本部進行第 1 次集中演練：107 年 4 月。
3. 納入本部演練單位針對開啟惡意郵件或點閱惡意郵件附件內容人員，進行加強宣導：自 107 年 7 月至 107 年 8 月上旬。
4. 本部進行第 2 次集中演練：107 年 9 月。

### 四、社交工程郵件型態

1. 由本部資訊及科技教育司以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象，郵件主題分為政治、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。
2. 當各單位收件人開啟郵件或點閱郵件所附連結或檔案時，即留下紀錄，俾利進行後續各單位惡意郵件開啟率及惡意連結(或檔案)點擊率之統計。

3. 由本部資訊及科技教育司以偽冒公務、個人或公司行號等名義發送惡意郵件的內容請參閱教育部本部 107 年 4 月份郵件樣版，請各單位資安人員協助暫時豁免內容相關主題的垃圾郵件過濾處理。

## 五、評量標準

1. 各單位之惡意郵件開啟率及惡意連結(或檔案)點擊率計算方式如下：
  - (1) 惡意郵件開啟率：

信件透過預覽或點開方式開啟，且信件本文內所含圖片亦完成圖片下載之動作或開啟信件內文中之附檔，始認定為測試成功。

開啟惡意郵件之人數 / 機關提報人數。
  - (2) 惡意連結(或檔案)點擊率：

受測人員點選信件內文中之連結網址，將被記錄為測試成功。

點閱惡意郵件所附連結或檔案之人數 / 機關提報人數。
2. 各單位之惡意郵件開啟率應低於 10% 以下；惡意連結(或檔案)點擊率應低於 6% 以下。

## 肆、演練結果：

- 一、預定於 6 月及 10 月，由本部資訊及科技教育司彙整演練報告，陳報行政院資通安全辦公室，並選取成績優良單位及待改善單位。
- 二、演練成績優良單位，將依權責辦理相關人員敘獎事宜。
- 三、演練成績不良單位，提報後續改善作為，並列為後續本部資安輔訪對象。

附件 1：政府機關（構）資訊安全責任等級分級

作業名稱 等級	資訊系統分類分級	ISMS 推動作業	資安專責人力	稽核方式	業務持續運作演練	防護縱深	監控管理	安全性檢測	資安教育訓練 (一般主管、資訊人員/資安人員、一般使用者)	專業證照
A 級	1. 完成資訊系統分級(104 年底 前) 2. 完成資訊系統資安防護基準要求(105 年底 前)	1. 全部核心資訊系統完成 ISMS 導入(105 年底 前) 2. 全部核心資訊系統通過第三方驗證(106 年底 前)	指派資安專責人力 2 人	每年至少 2 次內稽	每年至少辦理 1 次核心資訊系統持續運作演練	1. 防毒、防火牆、郵件過濾裝置 2. IDS/IPS、Web 應用程式防火牆 3. APT 攻擊防禦	SOC 監控(104 年底 前)	1. 每年至少辦理 2 次網站安全弱點檢測 2. 每年至少辦理 1 次系統滲透測試 3. 每年至少辦理 1 次資安健診	1. 每年資安人員(資訊人員)至少 2 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練 2. 每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過課程評量	每年維持至少 2 張國際資安專業證照與 2 張資安職能訓練證書之有效性
B 級	1. 完成資	1. 至少 2	指派資	每年至	每 2 年至	1. 防毒、防	SOC 監控	1. 每年至少	1. 每年資安人	每年維持

107 年度臺灣學術網路防範惡意電子郵件社交工程演練服務計畫

作業 名稱  等級	資訊系統 分類分級	ISMS 推 動作業	資安專 責人力	稽核方 式	業務持 續運作 演練	防護縱深	監控管理	安全性檢測	資安教育訓練 (一般主管、資 訊人員/資安人 員、一般使用 者)	專業證照
	訊系統分 級(104 年 底前) 2. 完成資 訊系統資 安防護基 準要求 (105 年 底前)	項核心資 訊系統完 成 ISMS 導入(106 年底前) 2. 至少 2 項核心資 訊系統通 過第三方 驗證(107 年底前)	安專責 人力 1 人	少 1 次 內稽	少 辦理 1 次核 心資訊 系統持 續運作 演練	火牆、郵件 過濾裝置 2. IDS/IPS 3. Web 應 用程 式防火牆 (機關具 有對外服 務之核 心資訊系 統)	(105 年 底前)	辦理 1 次 網站安全 弱點檢 測 2. 每 2 年 至少辦 理 1 次 系統滲 透測 試 3. 每 2 年 至少辦 理 1 次 資安健 診	員(資訊 人員) 至少 1 人次須 接受 12 小時以 上資安 專業課 程訓練 或資安 職能訓 練 2. 每年 一般使 用者與 主管至 少須接 受 3 小 時資安 宣導課 程並通 過課程 評量	至少 1 張國際 資安專 業證照 與 1 張 資安職 能訓練 證書之 有效性
C 級	依各主 管機關 規定	自行成 立推動 小組規 劃作業	依各主 管機關 規定	依各主 管機關 規定	依各主 管機關 規定	1. 防毒 2. 防火 牆 3. 郵件 過濾裝 置(機關 具有郵 件伺	依各主 管機關 規定	依各主 管機關 規定	1. 依各 主管機 關規定 資安人 員(資 訊人員) 資安專 業課程 訓練或 資安職	依各主 管機關 規定

107 年度臺灣學術網路防範惡意電子郵件社交工程演練服務計畫

作業 名稱  等級	資訊系統 分類分級	ISMS 推 動作業	資安專 責人力	稽核方 式	業務持 續運作 演練	防護縱深	監控管理	安全性檢測	資安教育訓練 (一般主管、資 訊人員/資安人 員、一般使用 者	專業證照
						服器)			能訓練要求 2.每年一般使 用者與主管至 少須接受 3 小 時資安宣導課 程並通過課程 評量	

## 附件 2：受測人員電子郵件帳號列表

教育部 107 年度臺灣學術網路防範惡意電子郵件社交工程演練

機關名稱：\_\_\_\_\_

機關編制內行政人員（含約、聘僱、及技工友，不含工讀生）共\_\_\_\_\_員

編號	電子郵件帳號	單位名稱	姓名	職稱	備考
1	xxx@xxx.com	總務處	王 O 明	專員	範例
2	ooo@xxx.com	會計處	陳 O 麗	專員	範例

註：

1. 演練人員資料涉及個資之部分，由各單位自行評估去識別化之方式，以各單位可分別實際人員為原則既可。
2. 資料請依格式上傳，未依格式製作致無法演練單位不予計分，表格不足使用請依格式製作。
3. 為利演練計畫進行，本表格收集之資訊為各機關公務使用之公開郵件帳號及姓名，相關資料將在演練計畫完成後 3 個月內銷毀。
4. 為例資料彙整便利，請使用 Excel 檔(.xls / .xlsx) 或 LibreOffice Calc 檔(.ods)。
5. 請將正、副校長及一級主管人員列為受測對象，並於職稱欄標註。