109 年臺灣學術網路
防範惡意電子郵件社交工程演練計畫

109 年 5 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「資通安全事件通報及應變辦法」第 8 條略以，每半年辦理一次社交工程演練。辦理如下：

1、 演練對象：部屬機關（構）、各大專校院、臺灣學術網路區域網路中心及各直轄市及縣市教育網路中心等。

2、 受測人員包括機關正、副首長、各級主管及一般行政人員；範圍涵蓋上述機關之全體人員，其全體人員定義為「具備機關郵件帳號之相關人員」即須納入受測人員名單，身分不侷限於正式公務人員。

參、 演練說明

1、 演練方式

1. 統一由本部集中辦理演練，隨機選取受測對象 100 名，其中主管(科組長以上)占 40%、一般行政人員占 60%，每人每次演練寄送 10 封郵件。

2、 演練時程

2. 提報演練名單：請各參演單位指派專案聯絡人，做為演練期間聯絡窗口，並詳實填具演練計畫附錄「受測人員電子郵件帳號列表」，於本（109）年 5 月 29 日（五）前函送本部。

3. 演練時程：自本（109）年 6 月至 11 月止，期間進行 2 次演練。

1. 如有任何未竟事項，請聯繫本部演練計畫聯絡窗口：資科司-李紀緯先生，聯絡方式（02）7712-9090，moe_infosec@mail.moe.gov.tw。

1、 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。
1. 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。

1、 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**（開啟惡意郵件之人數 / 機關受測人數）：

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，始認定為測試成功。

(1) **惡意連結點擊或附件下載率**（點閱惡意郵件所附連結或開啟附件之人數 / 機關受測人數）：

受測人員點選信件內文中之連結網址或開啟郵件附件，將被記錄為測試成功。

1. 各單位之惡意郵件開啟率**應低於 10%以下**；惡意連結點擊或附件下載率**應低於 6%以下**。
2. 附錄「受測人員電子郵件帳號列表」之填報正確率：

因填寫錯誤導致演練期間發送錯誤，將納入機關扣分。

肆、 演練結果

1、 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處，並選取成績優良單位及待改善單位。

2、 演練成績優良單位，將依權責辦理相關人員敘獎事宜。

3、 演練成績不良單位，提報後續改善作為，於收到成績後 2 周內，提交初步改善計畫，並將持續關注下次演練績效改善。

肆、 附錄：受測人員電子郵件帳號列表

教育部 109 年臺灣學術網路防範惡意電子郵件社交工程演練

機關名稱：_____

受測人員包括機關正、副首長、各級主管及一般行政人員；範圍涵蓋上述機關之全體人員，其全體人員定義為「**具備機關郵件帳號之相關人員**」即須納入受測人員名單，身分不侷限於正式公務人員。**共_____員**

項次	員工姓名	電子郵件	單位名稱	職稱	類別
1	王 O 明	xxx@xxx.com	總務處	處長	主管
2	陳 O 麗	ooo@xxx.com	會計處	專員	一般人員

(請自行增列)

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. 為利資料彙整便利，請使用 ODF Calc 檔（.odf）。
5. 請將正、副首長及主管人員列為受測對象，並於職稱欄標註。.