

110 年度教育部、所屬公務機關及臺灣學術網路 防範惡意電子郵件社交工程演練計畫

110 年 3 月

壹、依據

- 一、資通安全事件通報及應變辦法第 8 條。
- 二、臺灣學術網路管理規範相關規定。

貳、目的

社交工程為駭客常用入侵管道，透過電子郵件夾帶惡意程式或連結網址等方式，輔以吸引人信件主旨及內容，誘使缺乏警戒心的使用者開啟後造成進一步破壞，嚴重損害機關或個人之權益。

為依資通安全法令規定及增進臺灣學術網路安全之目的，爰持續辦理本(110)年度本部、所屬公務機關及臺灣學術網路之社交工程演練服務，並訂定本計畫，透過實施演練作業，提升教育體系人員針對社交工程攻擊之警覺性，並檢驗機關防範社交工程成效，及透過後續持續改善降低社交工程風險。

參、對象

一、演練對象

- (一)本部（包含各單位）。
- (二)本部所屬公務機關（不含資通安全責任等級屬 D 級以下者）

- 1、部屬機關(構)（現共 14 間，國民及學前教育署、青年發展署、體育署、國家教育研究院、國家圖書館、國立海洋生物博物館、國立自然科學博物館、國立科學工藝博物館、國立臺灣科學教育館、國立教育廣播電臺、國立公共資訊圖書館、國立臺灣圖書館、國立臺灣藝術教育館、國立海洋科技博物館）及公法人（國家運動訓練中心）。
- 2、國立大專校院（現共 47 間）。

3、國立大專校院附設機構（現共 10 間，國立臺灣大學醫學院附設醫院、國立臺灣大學醫學院附設醫院雲林分院、國立臺灣大學醫學院附設醫院北護分院、國立臺灣大學醫學院附設醫院金山分院、國立臺灣大學醫學院附設醫院新竹臺大分院、國立臺灣大學醫學院附設癌醫中心醫院、國立成功大學醫學院附設醫院、國立成功大學醫學院附設醫院斗六分院、國立陽明交通大學附設醫院、國立臺灣大學生物資源暨農學院附設山地實驗農場）。

4、資通安全責任等級屬 D 級、E 級者，由自身或其上級機關視實際需要及資源另行辦理。

(三)下列之臺灣學術網路連線單位（以下簡稱臺灣學術網路連線單位）

- 1、其他公私立大專校院。
- 2、區域網路中心。
- 3、直轄市、縣(市)教育網路中心。

二、應參與演練人員

(一)人員類型包含機關、學校之正副首長、各級主管及一般行政人員。

(二)人員範圍為機關、學校全體人員（定義為具備公務電子郵件帳號者），不限於正式公務人員身分。

肆、演練說明

一、演練方式

每次演練作業，將針對各演練對象之受測人員寄送 10 封社交工程演練郵件，受測人員挑選方式如下：

(一)本部：各單位所有人員均列入。

(二)本部所屬公務機關、臺灣學術網路連線單位：依演練對象提交之演練人員名單，按人員類型隨機選取 100 人（公務電子郵件帳號），未滿 100 人者則全數列入，主管人員（科組長以上）原則佔受測人員總數 35%以上（特定人員類型如有不足則視情況調整）。

二、演練時程：自本（110）年 4 月至 11 月止，期間辦理 2 次演練。

三、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。

四、受演練對象需配合事項

(一)請指派專案聯絡人，負責演練期間與本部之作業聯繫事宜。

(二)請依式提報演練人員名單（如附錄一）並完成自我檢核（如附錄二），人員清單應包含機關、學校全體人員（負責維運臺灣學術網路區域網路中心之大專校院，得註明情形後，將該校與區域網路中心人員名單合併提供）；檔案格式應為本部指定之 CSV 檔格式，以利後續資料處理作業。

(三)請於本(110)年 4 月 2 日前，將前述專案聯絡人（含姓名、公務電話、公務電子郵件）、演練人員名單（CSV 電子檔）及自我檢核表（含簽核紀錄），以電子郵件方式回覆本部演練作業聯絡窗口。

(四)本部演練作業聯絡窗口如下：

1、資訊及科技教育司-楊小姐，公務電話：02-77129088，公務電子郵件：cjyang@mail.moe.gov.tw

2、資訊及科技教育司-林先生，公務電話：02-77129078，公務電子郵件：esora@mail.moe.gov.tw

伍、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)惡意郵件開啟率

1、由本部統一計算，計算方式：開啟演練郵件人數 / 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)惡意郵件點閱率

1、由本部統一計算，計算方式：點選演練郵件內文連結網址或附檔之人數 / 總受測人數

2、受測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，受測人員不論點選幾個都將記錄為 1 次。

3、受測人員點選郵件內文中之夾檔附件，將被記錄為遭誘騙成功。同封郵件受測人員不論點選幾次附檔，都將記錄為 1 次。

4、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、連結點選及附檔點選，將列入轉寄者之受測紀錄。

二、演練目標

(一)惡意郵件開啟率：各次演練作業，各演練對象應低於 10%(含)。

(二)惡意郵件點閱率：各次演練作業，各演練對象應低於 6%(含)。

三、其他事項

(一)如提報之演練人員名單未正確(如填寫錯誤)，或特意阻攔演練作業寄信主機來源，致演練期間無法發送成功，將視嚴重程度納入演練結果考量。

(二)建議自行訂定內部演練目標，如降低重複遭受誘騙人數等。

陸、演練結果

一、由本部(資訊及科技教育司)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主管機關行政院；演練成果報告之概要，亦將函送各演練對象。

二、各次演練作業結束後，依演練對象屬性分為「政府機關及公法人」、「大專校院及其附設機構」及「其他臺灣學術網路連線單位」等 3 組，對於分組成績表現優良者，本部將函請演練對象給予相關人員(如辦理教育訓練人員)行政獎勵，相關條件如下：

(一)惡意郵件開啟率、惡意郵件點閱率皆符合本演練計畫之目標，且惡意郵件開啟率、惡意郵件點閱率之排名(遞增排序)，皆為所屬分組之前四分之一者。

(二)落實本演練計畫相關配合事項要求，如提報演練人員名單已涵括學校

全體人員、未含錯誤資訊，且未特意阻攔演練作業寄信主機來源。

三、各次演練作業結束後，對於演練成績不良者，本部將函請演練對象擬定改善措施，相關條件及說明如下：

(一)惡意郵件開啟率或惡意郵件點閱率，未能符合本演練計畫之目標。

(二)未辦理本演練計畫相關配合事項要求且情節重大者，如逾期未提報演練人員名單。

四、本部將檢視前後兩次演練作業之績效改善情形，如演練對象連續 2 次演練作業成績皆屬不良者，須擬定改善計畫並回復本部備查。

附錄一（此為填寫範例，請使用本部指定之 csv 檔案格式）

CSV 檔下載連結：

公務電子郵件	單位名稱	姓名	職稱	人員類別	備註
aaa@xxx.com	總務處	王 0 明	處長	主管	
bbb@xxx.com	會計處	陳 0 麗	專員	一般人員	
ccc@xxx.com	資訊處	周 0 倫	程式設計師	一般人員	區域網路 中心人員