

114 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

114 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，且多有實際入侵成功案例，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(114)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

- 1、部屬機關(構)(現共 13 間，國民及學前教育署、青年發展署、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)。
- 2、國立大專校院(現共 47 間)。

3、國立大專校院附設機構，資通安全責任等級屬C級以上者（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醫院癌醫中心分院、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實驗林管理處）。

4、資通安全責任等級屬D級、E級者，或國立高級中等以下學校，由自身或其上級（主管）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。
- (二)人員類型包含機關、學校之正副首長、各級主管、一般行政人員、教職員工等。

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5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（依公務電子郵件帳號），未滿100人者則全數列入。主管人員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(114)年4月至12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、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)：

1、演練人員名單檔案應為本部指定之格式(請依附錄一連結下載範本檔)，以利演練後續各項資料處理作業。

(1)人員類別僅分為主管人員、一般人員兩種。

(2)負責維運臺灣學術網路區域網路中心之人員，請於備註標示「區域網路中心人員」以利識別。

2、演練人員名單應包含機關、學校全體人員。

3、自我檢核表應確實完成檢查，並由主管核章。

(三)請於本年3月21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)計畫演練期間將會辦理演練前郵件測試，以確保本次社交工程演練測試可成功寄信至受測者，注意事項如下：

1、前述測試將於正式測試前發送前測通知信至各單位專案聯絡人信箱，請各專案聯絡人於規定時間內(於前測通知信通知演練前測試郵件寄送時間)接收演練前測試郵件，並協助執行以下動作：開啟郵件、下載附件並開啟、點擊郵件中附帶之外部連結。

2、本次前述測試為確認各單位回傳紀錄之機制正常，非社交工程演練之正式社交演練郵件，不會列入單位受測成績開啟率或點閱率計算，惟單位逾期未點擊前述信件或刻意阻攔演練作業寄信主機來源，將

會依本計畫、陸、二項下之評分方式規定扣分。

- 3、於演練期間刻意阻攔演練作業寄信主機來源視同未辦理完成社交工程演練測試，亦不列入本次成績優良單位名單，將請單位自行辦理該次單位內社交工程演練。

(五)演練作業聯絡窗口如下：

- 1、資訊及科技教育司-周先生，公務電話：02-7712-9089，公務電子郵件：kevin05@mail.moe.gov.tw
- 2、資訊及科技教育司-劉先生，公務電話：02-7736-9469，公務電子郵件：kh9469@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)社交工程郵件開啟率

- 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)社交工程郵件點閱率

- 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)社交工程郵件開啟率：各次演練作業，各演練對象應低於10%(含)。

(二)社交工程郵件點閱率：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、評分方式如下：

評分類別	評分項目	給分標準
演練作業配合度(20%)	回復資料格式正確性(6%)	<ul style="list-style-type: none">● 得6分：依本部演練人員名單回復格式提供資料檔，其格式(csv)、編碼(UTF-8-BOM)、欄位數(7)、人員類別描述(主管人員/一般人員)等均正確。● 得0分：未依規定配合辦理。
	回復資料內容完整性(6%)	<ul style="list-style-type: none">● 得6分：回復資料包含演練人員名單、自我檢核表。人員名單已涵括機關、學校全體人員；自我檢核表已完成檢查及主管核章。● 得0分：未依規定配合辦理。
	作業配合狀況(8%)	<ul style="list-style-type: none">● 得8分：未刻意阻攔演練作業寄信主機來源，並配合演練信件寄送測試之回復確認作業。● 得4分：未刻意阻攔演練作業寄信主機來源，惟未配合演練信件寄送測試之回復確

		認作業。 ● 得 0 分：有阻攔演練作業寄信主機來源之情事，致演練期間所有信件皆無法發送成功，或其餘未依規定配合辦理(含逾期)。
演練作業結果 (80%)	社交工程郵件開啟率(40%)	得分=(100%-社交工程郵件開啟率)*40
	社交工程郵件點閱率(40%)	得分=(100%-社交工程郵件點閱率)*40

註：總評分四捨五入至小數點第一位。

三、演練結果如有疑義，請於收到本演練作業成績通知一個月內，以 Email 寄送演練作業聯絡窗口受理複查成績，如需檢據佐證資料以一次為限。成績於複查後，若達到優良與不良標準者，以增額方式辦理獎懲。

四、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，列為成績表現優良之相關條件如下：

- (一)總評分為所屬分組排名前五分之一（四捨五入至個位數），其中「演練作業配合度」一項須為滿分。
- (二)落實本演練計畫相關配合事項要求，且社交工程郵件開啟率、社交工程郵件點閱率皆符合本演練計畫之目標。

五、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)社交工程郵件開啟率或社交工程郵件點閱率，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，如逾期未提報演練人員名單。

六、對於連續兩次演練作業成績表現優良者，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。

七、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。