112 年國立高級中等以下學校及非特定公務機關防範惡意電子郵件社交工程演練計畫

112 年 4 月

目錄

壹、依據

資通安全事件通報及應變辦法第 8 條、第 18 條及第 19 條。

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，輔以吸引人之信件主旨及內容，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，爰辦理本年度(112 年)國立高級中等以下學校及本署所管轄特定非公務機關之社交工程演練，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(如附錄一)

(一)國立高級中等以下學校：共 157 校。

(二)本署所管轄特定非公務機關：共 2 基金會。

二、 應參與人員

包含持有公務電子郵件帳號、機關公發電子郵件帳號及公

務使用電子郵件帳號之國立高級中等以下學校及特定非公務機關之正副首長、正副執行長、各級主管、一般行政人員、教職人員、各單位之約聘僱人員及廠商駐點人員等都屬於本次計畫參與人員。

肆、演練說明

一、演練方式

每次演練作業，依演練對象提交之參與人員名單，按人員類型隨機選取 35 人(持有公務電子郵件帳號)為受測人員，未滿 35 人者則全數列入。主管人員被挑選為受測人員原則佔參與人員總數 30%以上（主管類型如有不足 30%則視情況調整)，每次測試會針對每位受測人員寄送 4 封(含)以上社交工程演練測試郵件。

二、演練時程：自本(112)年 5 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， 包含 3 種不同郵件，主題分別為八卦、休閒、保健、財經、新奇、時事、模擬等類型實際社交工程郵件，包含社交工程郵件開啟、內文連結網址開啟、附件檔案開啟等社交工程樣態。

四、演練對象需配合事項

（一）請指派本次計畫的專案聯絡人，負責演練期間與本署之作業聯繫事宜。

（二）請依式提報演練人員名單(如附錄二)，並完成自我檢核(如附錄三)：

1. 演練人員名單檔案應為本署指定之格式，以利演練後續各項資料處理作業，人員類別僅分為主管人員、一般人員兩種。

2. 演練人員名單應包含本署所屬國立高級中等以下學校、本署所管轄特定非公務機關全體人員(請依本計畫參、二之應參與人員提供)。

3. 請於112年5月19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署演練作業聯絡窗口-江小姐(電子郵件：e-s530@mail.k12ea.gov.tw)。

4. 本署演練作業聯絡窗口如下：

(1)本署江小姐，公務電話：04-37061509，公務電子郵件：e-s530@mail.k12ea.gov.tw。

(2)本署蔡小姐，公務電話：04-37061422 公務電子郵件：e-s516@mail.k12ea.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. 由本署統一計算，計算方式：參與單位開啟演練郵件人數/ 參與單位總受測人數。
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)社交工程郵件連結點閱率

1. 由本署統一計算，計算方式：參與單位點選演練郵件內文連結網址之人數/ 參與單位總參與人數。
2. 參與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，參與人員不論點選幾個都將記錄為 1 次。
3. 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，將列入轉寄者之受測紀錄。

(三)社交工程郵件附件開啟率

1. 由本署統一計算，計算方式：參與單位開啟演練郵件附件之人數/ 參與單位總參與人數。
2. 參與人員開啟郵件內文中之夾檔附件，將被記錄為遭誘騙成功。同封郵件參與人員不論點選幾次附檔，都將記錄為 1 次。
3. 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附檔，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，各演練對象開啟率應低於 10%(含)。

(二)社交工程郵件連結點閱率：各次演練作業，各演練對象點選率應低於 6%(含)。

(三)社交工程郵件附件開啟率：各次演練作業，各演練對象附件開啟應低於 2%(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、遺漏），或特意阻攔或過濾演練作業寄信來源主機網址或 IP 時，導致演練期間無法發送成功到參與人員電子郵件信箱時，將

視為嚴重不符合程度，並納入演練結果評分。

(二)建議參與對象可以自行訂定內部演練目標，如降低重複遭受誘騙比例等要求。

陸、演練結果

一、由本署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教育部；演練成果報告之概要，亦將函送各參與對象。

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%)	1. 得6 分：依本署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(主管人員/一般人員)等均正確。 2. 得0 分：未依規定配合辦理。
	回復資料內容完整性(6%)	1. 得6 分：回復資料包含演練人員名單、自我檢核表。人員名單已含括

		機關、學校全體人員；自我檢核表已完成檢查及主管核章。 2. 得0 分：未依規定配合辦。
	作業配合狀況(8%)	1. 得8 分：未刻意阻攔演練作業寄信來源主機，並配合演練信件寄送測試之回復確認作業。 2. 得4 分：未刻意阻攔演練作業寄信來源主機，惟未配合演練信件寄送測試之回復確認作業。 3. 得0 分：有阻攔演練作業寄信來源主機之情事，導致演練期間所有信件皆無法發送成功至受測人員。
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
	社交工程郵件連結點閱率(30%)	得分=(100%-社交工程郵件點閱率)*30
	社交工程郵件附件開啟率(10%)	得分=(100%-社交工程郵件點閱率)*10

三、各次演練作業結束後，列為成績表現優良之相關條件如下：

(一)總評分為排名前五分之一（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、社交工程郵件連結點閱率及社交工程附件開啟率皆符合本演練計畫之目標。

四、各次演練作業結束後，對於演練成績不良者，本署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、社交工程郵件連結點閱率或社交工程郵件附件開啟率，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。

五、對於連續兩次演練作業成績表現優良者，本署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。

六、本署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署備查。

附錄一、演練對象

一、國立高級中等以下學校，157 校。

1. 國立基隆女子高級中學
2. 國立基隆高級中學
3. 國立基隆特殊教育學校
4. 國立基隆高級商工職業學校
5. 國立臺灣海洋大學附屬基隆海事高級中等學校
6. 國立臺灣師範大學附屬高級中學
7. 國立政治大學附屬高級中學
8. 國立政治大學附設實驗國民小學
9. 國立臺北教育大學附設實驗國民小學
10. 國立華僑高級中等學校
11. 國立中央大學附屬中壢高級中學
12. 國立臺北科技大學附屬桃園農工高級中等學校
13. 國立關西高級中學
14. 國立竹北高級中學
15. 國立新竹高級工業職業學校
16. 國立清華大學附設實驗國民小學
17. 國立新竹特殊教育學校

18. 國立竹東高級中學
19. 國立新竹女子高級中學
20. 國立新竹高級中學
21. 國立新竹科學園區實驗高級中等學校
22. 國立新竹高級商業職業學校
23. 國立中興大學附屬高級中學
24. 國立中興大學附屬臺中高級農業職業學校
25. 國立中科實驗高級中學
26. 國立臺中教育大學附設實驗國民小學
27. 國立大湖高級農工職業學校
28. 國立苗栗高級中學
29. 國立苗栗高級農工職業學校
30. 國立苑裡高級中學
31. 國立卓蘭高級中等學校
32. 國立竹南高級中學
33. 國立苗栗特殊教育學校
34. 國立苗栗高級商業職業學校
35. 國立南投高級商業職業學校
36. 國立員林高級中學

37. 國立北斗高級家事商業職業學校
38. 國立員林高級農工職業學校
39. 國立溪湖高級中學
40. 國立員林高級家事商業職業學校
41. 國立員林崇實高級工業職業學校
42. 國立鹿港高級中學
43. 國立彰化高級商業職業學校
44. 國立秀水高級工業職業學校
45. 國立彰化高級中學
46. 國立彰化女子高級中學
47. 國立二林高級工商職業學校
48. 國立永靖高級工業職業學校
49. 國立彰化特殊教育學校
50. 國立和美實驗學校
51. 國立彰化師範大學附屬高級工業職業學校
52. 國立中興高級中學
53. 國立仁愛高級農業職業學校
54. 國立竹山高級中學
55. 國立暨南國際大學附屬高級中學

56. 國立南投特殊教育學校
57. 國立草屯高級商工職業學校
58. 國立南投高級中學
59. 國立水里高級商工職業學校
60. 國立埔里高級工業職業學校
61. 國立雲林特殊教育學校
62. 國立斗六高級家事商業職業學校
63. 國立虎尾高級中學
64. 國立北港高級農工職業學校
65. 國立西螺高級農工職業學校
66. 國立虎尾高級農工職業學校
67. 國立斗六高級中學
68. 國立北港高級中學
69. 國立土庫高級商工職業學校
70. 國立嘉義高級商業職業學校
71. 國立嘉義特殊教育學校
72. 國立嘉義高級家事職業學校
73. 國立嘉義女子高級中學
74. 國立華南高級商業職業學校

75. 國立民雄高級農工職業學校
76. 國立嘉義大學附設實驗國民小學
77. 國立新港藝術高級中學
78. 國立東石高級中學
79. 國立嘉義高級工業職業學校
80. 國立嘉義高級中學
81. 國立後壁高級中學
82. 國立新營高級工業職業學校
83. 國立白河高級商工職業學校
84. 國立新營高級中學
85. 國立臺南高級工業職業學校
86. 國立臺南家齊高級中等學校
87. 國立玉井高級工商職業學校
88. 國立臺南第一高級中學
89. 國立曾文高級家事商業職業學校
90. 國立曾文高級農工職業學校
91. 國立臺南特殊教育學校
92. 國立臺南大學附屬啟聰學校
93. 國立新化高級中學

94. 國立高雄師範大學附屬高級中學
95. 國立鳳新高級中學
96. 國立中山大學附屬國光高級中學
97. 國立高雄餐旅大學附屬餐旅高級中等學校
98. 國立臺南高級商業職業學校
99. 國立鳳山高級中學
100. 國立鳳山高級商工職業學校
101. 國立南科國際實驗高級中學
102. 國立北門高級農工職業學校
103. 國立北門高級中學
104. 國立臺南第二高級中學
105. 國立新豐高級中學
106. 國立善化高級中學
107. 國立臺南大學附屬高級中學
108. 國立臺南大學附設實驗國民小學
109. 國立臺南高級海事水產職業學校
110. 國立臺南女子高級中學
111. 國立新化高級工業職業學校
112. 國立旗山高級農工職業學校

113. 國立旗美高級中學
114. 國立岡山高級農工職業學校
115. 國立岡山高級中學
116. 國立屏東高級中學
117. 國立屏北高級中學
118. 國立屏東女子高級中學
119. 國立內埔高級農工職業學校
120. 國立潮州高級中學
121. 國立東港高級海事水產職業學校
122. 國立佳冬高級農業職業學校
123. 國立恆春高級工商職業學校
124. 國立屏東特殊教育學校
125. 國立屏東高級工業職業學校
126. 國立屏東大學附設實驗國民小學
127. 國立羅東高級工業職業學校
128. 國立蘭陽女子高級中學
129. 國立宜蘭特殊教育學校
130. 國立羅東高級中學
131. 國立宜蘭高級商業職業學校

132. 國立羅東高級商業職業學校
133. 國立頭城高級家事商業職業學校
134. 國立宜蘭高級中學
135. 國立蘇澳高級海事水產職業學校
136. 國立玉里高級中學
137. 國立花蓮高級中學
138. 國立花蓮高級農業職業學校
139. 國立花蓮高級工業職業學校
140. 國立花蓮女子高級中學
141. 國立光復高級商工職業學校
142. 國立花蓮特殊教育學校
143. 國立花蓮高級商業職業學校
144. 國立東華大學附設實驗國民小學
145. 國立成功商業水產職業學校
146. 國立臺東大學附屬體育高級中學
147. 國立臺東女子高級中學
148. 國立臺東大學附屬特殊教育學校
149. 國立臺東高級商業職業學校
150. 國立關山高級工商職業學校

151. 國立臺東高級中學
152. 國立臺東大學附設實驗國民小學
153. 國立金門高級農工職業學校
154. 國立金門高級中學
155. 國立馬公高級中學
156. 國立澎湖高級海事水產職業學校
157. 國立馬祖高級中學

二、特定非公務機關，計 2 基金會

1. 財團法人中華幼兒教育發展基金會
2. 財團法人台灣省中小學校教職員福利文教基金會

附錄二、演練人員名單回復格式

一、檔案下載位置

本署官方網站(網址：https://www.k12ea.gov.tw/)-最新消息

二、填寫範例

項次	公務電子郵件	單位名稱	姓名	職稱	人員類別	備註
1	aaa@xxx.edu.tw	總務處	王0明	處長	主管人員	
2	bbb@xxx.edu.tw	法律系	陳0麗	計畫助理	一般人員	
3	ccc@xxx.edu.tw	資訊處	周0倫	程式設計師	一般人員	

備註：本範例的表格及格線只為了協助方便讀取，實際檔案不會有此格線，且檔案格式不得為 WORD；人員類別係供電腦程式選取參與人員之使用，僅分為主管人員、一般人員兩種不得另行創立其他類別，參與對象如自創類別造成電腦程式無法判讀，將扣除演練成績。主管人員之對應職稱欄位，如校長、副校長、教務長、學務長、執行長或副執行長等相關主管職稱（僅列舉，請以此類推）。

三、檔案格式檢查方式

(一)CSV 檔案格式的欄位使用半型逗號“,”區隔(不得使用全型中文逗號 “，”)。

(二)以 Windows 記事本，開啟交付的檔案後，點選程式選單「檔案」>「另存為…」，跳出視窗之右下角編碼欄位應顯示為「具有 BOM 的 UTF-8」才能符合“UTF-8-BOM”格式要求。

附錄三、自我檢核表

112年國立高級中等以下學校及非特定公務機關防範惡意電子郵件社交工程演練演練對象自我檢核表		
填寫人姓名	（請填專案聯絡人）	
填寫人公務電話		
填寫人公務電子信箱		
演練對象（學校、基金會）名稱		
檢核項目	檢核內容	自主檢核情形（承辦人檢核）
專案聯絡人	已指派專案聯絡人，負責演練期間與本署之作業聯繫事宜。	□是
	演練期間專案聯絡人如因故變更，應即時更新相關資訊（含姓名、公務電話、公務電子郵件）予本署。	□已知悉
演練人員名單	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。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。且未含錯誤資訊。 註：人員姓名可採去識別化方式處理。	□是， 共＿＿＿＿員
	依本署指定之 csv 檔案格式（包含資料欄位順序）提供，且檔案編碼為 UTF-8-BOM 格式。	□是
	人員類別僅分為主管人員、一般人員兩種。	□是

承辦人核章：　　權責主管核章：