

國教署 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 (以下節錄摘要內容)

112 年 4 月

一、目的

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，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。

二、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。

備註：電子郵件格式為帳號@mail.edu.tw 或@tngs.tn.edu.tw 者皆屬參與人員。

三、演練說明

1. 演練方式：每次演練作業，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。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。
2. 演練時程：自本(112)年 5 月至 11 月止，期間辦理 2 次演練。
3. 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、演練評量項目及目標值

1. 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)。
2. 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)。
3. 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)。

五、演練結果

各次演練作業結束後，將彙整演練成果報告概要，對於演練成績不良者，本署將函請演練對象擬定改善措施並追蹤改善情形。