國立清華大學 防範惡意電子郵件社交工程演練計畫

中華民國110年10月09日 第9次規劃小組會議提案通過

一、目的
為提高本校人員資訊安全警覺性，降低社交工程攻擊風險，特訂定本計畫，舉辦相關教育訓練與宣導、並配合教育部規劃辦理演練服務作業及提供受測人員名單，以強化人員資安意識並檢驗本校宣導社交工
程防制成效。

二、實施對象
（一） 本校區網中心人員
（二） 本校正、副校長，一、二級單位主管及一般行政人員。

三、演練說明
（一） 演練方式
由教育部集中辦理演練，於每次演練前，向教育部提交本校所有一、二級主管及行政人員受測人員名單，再經由教育部抽出一百名受測人員，每人寄送若干不同演練信件。信件內容包括各項題型。詳細之演練方式與抽測比例由教育部決定。
（二） 教育訓練
1. 依110年8月23日行政院頒「資通安全事件通報及應變辦法」，第 18 條公務機關應配合主管機關規劃、辦理之資通安全演練作業，本校人員每年至少需接受1小時社交工程防制宣導講習。
2. 社交工程演練教育課程對象：
(1) 上半年度演練作業前：實施對象為本校單位所有一、二級主管、行政人員，全面性實施教育訓練；前一年度下半年未通過演練者為必要調訓對象。
(2) 下半年度演練作業前：針對上半年演練時開啟惡意郵件、或點閱惡意郵件所附連結或檔案之人員，再次進行教育訓練加強宣導，以強化其警覺性。
（三） 演練時程
實際時程由教育部訂之，演練時程以教育部公文為準，中心將會依公文之演練計畫進行時程公告。
（四） 社交工程郵件型態
1. 由教育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，郵件主題涵蓋政治、公務、健康養生、旅遊等類型，每年依情境不同會有所不同，其郵件內容包含連結網址或附檔。
2. 當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。
（五） 評量標準
1. 未通過：開啟惡意郵件、或點擊惡意連結或檔案。
(1) 開啟惡意郵件：
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下載。
(2) 點擊惡意連結或檔案：
點選信件內文中之連結網址或檔案。

四、 演練結果
（一） 演練結果將於教育部公佈後，通知未通過之人員，並將名單副知未通過的人員所屬一級單位主管。
（二） 未通過之演練人員列為惡意電子郵件社交工程教育訓練必要調訓對象。