

教育部 99 年度 學術機構分組防範惡意電子郵件社交工程演練計畫

99 年 4 月

壹、依據

- 一、96 年 2 月 15 日行政院核定修正之「建立我國通資訊基礎建設安全機制計畫」(94 年至 97 年) 辦理。
- 二、國家資通安全會報 96 年 10 月 5 日資安發字第 0960100562 號函「防範惡意電子郵件社交工程施行方案」辦理。

貳、目的

為提高公務人員警覺性以降低社交工程攻擊風險，特訂定本執行方案，規範機關自訂社交工程防制年度目標、舉辦相關資安教育訓練與宣導、規劃辦理演練作業，以強化公務人員資安意識並檢驗機關宣導社交工程防制成效。

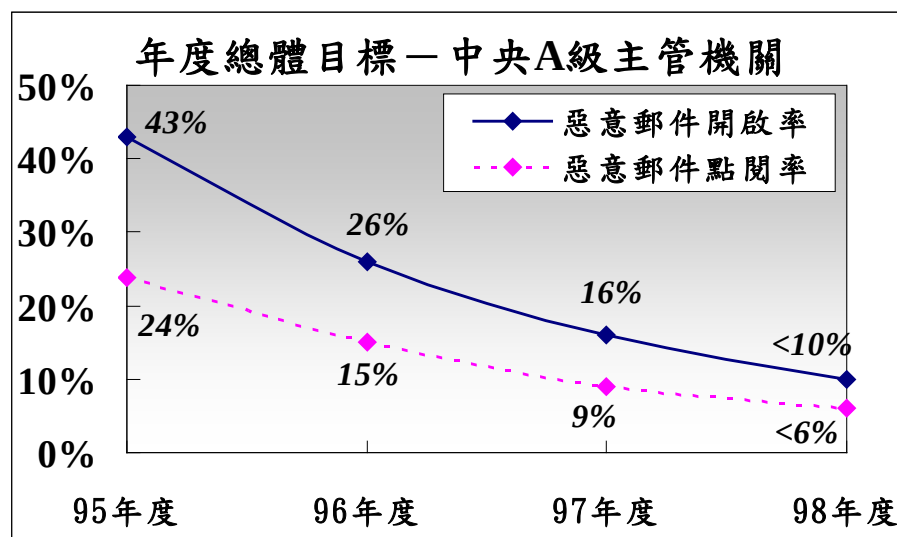
參、施行對象

教育部、台灣大學醫學院附設醫院、成功大學醫學院附設醫院、區、縣教育網路中心、各公私立大學。

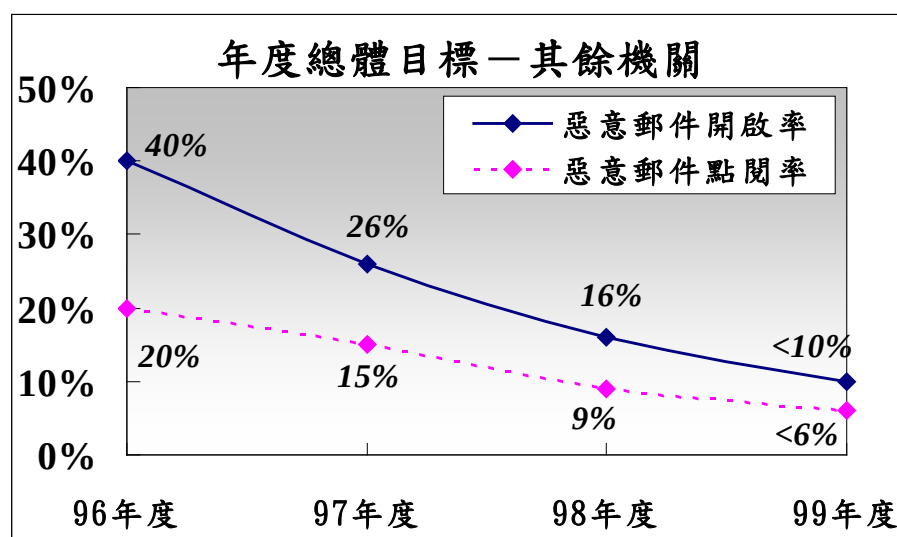
肆、年度目標

- 一、依據國家資通安全會報以惡意郵件開啟率、點閱率每年下降率 40% 為年度精進目標，參考 95 年度辦理電子郵件社交工程演練之演練結果（平均惡意郵件開啟率、點閱率分別為 43% 及 24%），訂定本部及所屬機關學校之年度總體目標。
 1. 教育部：預計於 99 年度惡意郵件開啟率、點閱率分別降至 10%

及 6%，總體目標如下圖所示。



2. 教育部以外之 A、B 級單位：預計於 99 年度(含以後年度)惡意郵件開啟率、點閱率分別降至 10%及 6%以下，年度總體目標如下圖所示。



- 二、機關目標應以惡意郵件開啟率、點閱率每半年至少下降率達 25% 為原則，直至符合年度總體目標。

伍、演練作業

一、教育訓練

1. 依 94 年 9 月 28 日資安發字第 94100802 號「政府機關（構）資訊安全責任等級分級作業施行計畫」，各機關應按其資安等級，每年定期舉辦資安教育訓練(如附件)。
2. 資安教育訓練應納入社交工程防制有關之認知宣導，並著重攻擊實例說明。
3. 各機關學校人員每年至少需接受 1 小時社交工程防制宣導講習。
4. 各機關學校可透過網路文官學院備有相關 e-Learning 課程，應加強推廣教育訓練(<http://elearning.nat.gov.tw>)。
5. 宣導課程應分兩階段辦理：
 - (1) 第一階段（於演練作業辦理前）：各機關學校應針對單位所有行政人員，全面性實施教育訓練。
 - (2) 第二階段（於演練作業完成後）：針對開啟惡意郵件比例較高、點閱惡意郵件所附連結或檔案比例較高之「應重點宣導人員」再次進行宣導，以強化其警覺性。

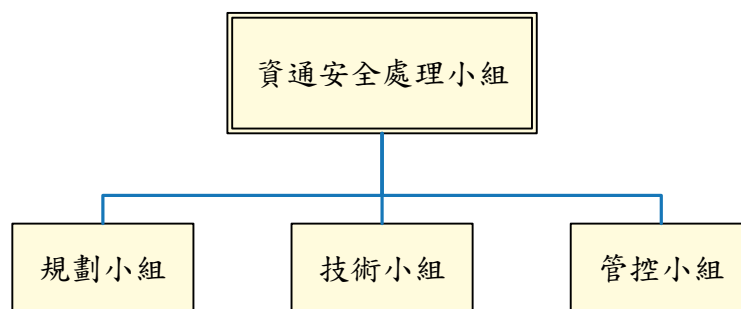
二、演練時程：

1. 國家資通安全會報演練：1 月至 12 月不定期演練。
2. 本(學術機構分組)演練：
 - (1) 提報演練名單：4 月(各機關學校提報 1/2 行政人員)。
 - (2) 各機關學校辦理教育訓練：4 月(全部行政人員)。
 - (3) 本部進行第 1 次演練：5 月。
 - (4) 各機關學校辦理再教育訓練：6 月至 8 月(開啟、點閱惡意郵件比率較高人員)。
 - (5) 本部進行第 2 次演練：9 月。

- (6) 各機關學校辦理再教育訓練：10 月 (開啟、點閱惡意郵件比率較高人員)。

三、演練作業要點

1. 教育部配合本項演練作業應組成演練任務編組，分工執行各項任務，並由電算中心負責統籌，組織架構如下：



- (1) **規劃小組**：負責規劃演練期程、遴選演練機關及提報演練成果等。
- (2) **技術小組**：負責設計模擬惡意郵件、規劃執行演練攻擊作業、彙整演練相關數據等。
- (3) **管控小組**：負責監控各項執行事宜。
2. 演練期間有關惡意郵件、惡意程式、攻擊工具、滲透破壞程度等，均需為可控制、有限度之滲透入侵，並由技術小組規劃執行。
3. 郵件主題分為政治、公務、健康養生、旅遊等類型，郵件內容包含連結網址或 word 附檔。
4. 由技術小組以偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象，當收件人開啟郵件或點閱郵件所附連結或檔案時，應留下紀錄，俾利後續統計惡意郵件開啟率及點閱率。
- (1) 惡意郵件開啟率：
- 開啟惡意郵件之人數 / 參演人數。
- (2) 惡意郵件點閱率：
- 點閱惡意郵件所附連結或檔案之人數 / 參演人數。

(3) 惡意郵件開啟下降率：

– (本次惡意郵件開啟率 – 比較基準) / 比較基準
原則上，比較基準為前次演練之惡意郵件開啟率。

(4) 惡意郵件點閱下降率：

– (本次惡意郵件點閱率 – 比較基準) / 比較基準
原則上，比較基準為前次演練之惡意郵件點閱率。

陸、獎懲規定：

預定於每年 10 月底前，由本部電算中心彙整演練情形，針對電子郵件社交工程演練結果，選取績優單位、持續改善單位、加強改善單位及未依本執行方案辦理單位，俾利各單位本於權責對有功人員辦理敘獎作業，**教育部部內行政人員超過 99 年度目標 2 倍(誤開信率超過 20%或誤點閱率超過 12%)，將依「教育部職員獎懲要點」規定辦理。**

附件：政府機關（構）資訊安全責任等級分級

內容 等級	作業 防 禦 機 制 強 度	防 護 縱 深	ISMS 推 動 作 業	稽核 方 式	資安教育訓練(主官, 主管, 技術, 一般)	專業 證 照
A 級	強度 等級 4	NSOC/SOC、IDS、防火牆 防毒	96 年通過 第三者認 証	每年至少 執行二次 內稽	(4, 6, 18, 4 小 時)/每年	96 年資安 專業鑑定 二張
B 級	強度 等級 3	SOC(OP) IDS、防火牆 防毒	97 年通過 第三者認 証	每年至少 執行一次 內稽	(4, 6, 16, 4 小 時)/每年	96 年資安 專業鑑定 一張
C 級	強度 等級 2	IDS, 防火牆 防毒	各單位自 行成立推 動小組規 劃作業	自我檢視	(2, 6, 12, 4 小 時)/每年	資安專業 訓練
D 級	強度 等級 1	防火牆 防毒	推動 ISMS 觀念宣導	自我檢視	(1, 4, 8, 2 小 時)/每年	資安專業 訓練

教育部 99 年度學術機構分組防範惡意電子郵件社交工程演練

機關名稱:_____

機關編製內行政人員（含約、聘僱、及技工友，不含工讀生）共____員

編號	職稱	姓名	電子郵件帳號	備考

資料請依格式上傳，表格不足使用請依格式製作