教育部103下半年度電子郵件社交工程演練結果說明

教育部103下半年度電子郵件社交工程演練，本校受測人數為908名（含一、二級行政主管），未通過演練人員共204名，為了提高本校教職員工的資安意識，本中心將持續宣導資通安全的觀念外，**對於未能通過教育部演練人員，將列為日後加強資通安全宣導及教育訓練的對象**。將來這類性質的演練，教育部或行政院每年度會不定期地實施，因此，整理這次演練資料與結果，以及提供注意事項供本校使用者參考。

教育部演練目的及結果

教育部為強化教育機構教職員對資安意識的落實與對社交工程等攻擊行為的資安警覺意識，於2014年9月5日至2014年9月30日期間進行電子郵件社交工程演練，藉由模擬駭客寄送各種誘騙信件的手法，測試教職員點選各類誘騙信件的比率。

測試信件摘要表

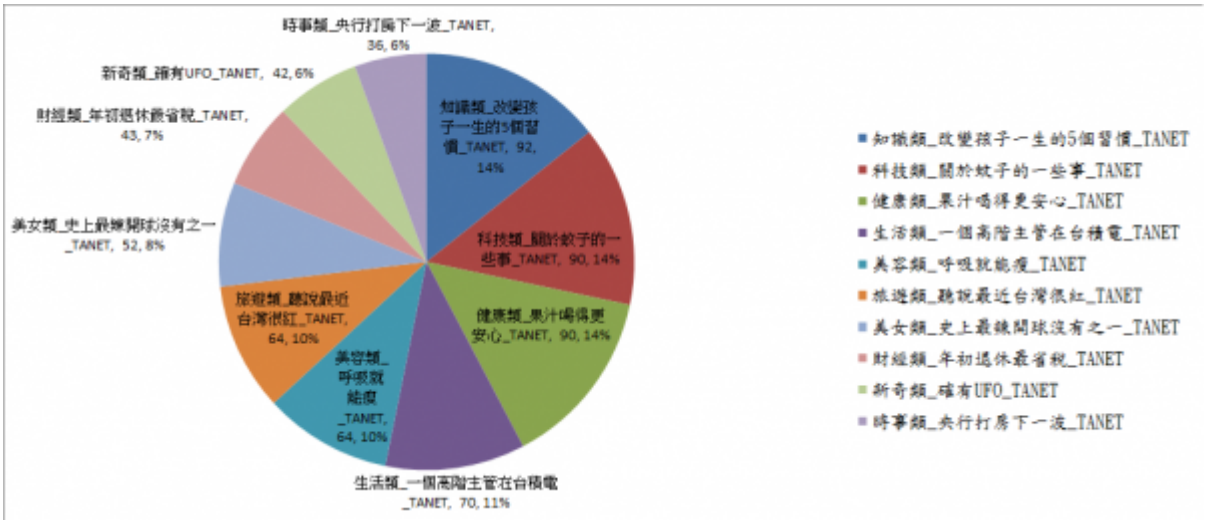
組別	信件類別	信件標題
Letter 1	生活類	【必看瘋傳】一個高階主管在台積電【賣命癌症過世後給大家的啟示】
Letter 2	知識類	改變孩子一生的5個習慣
Letter 3	科技類	關於蚊子的一些事
Letter 4	美女類	瑜珈女神性感誘惑　史上最辣開球沒有之一
Letter 5	美容類	呼吸就能瘦　美女中醫示範腹式呼吸法
Letter 6	旅遊類	【驚奇景點】聽說最近台灣很紅！最受國際矚目的台灣旅遊奇觀登場
Letter 7	時事類	央行打房下一波？　專家：桃園、新竹恐遭殃
Letter 8	財經類	提早規劃財務 年初退休最省稅
Letter 9	健康類	看清這10點，讓你果汁喝得更安心！
Letter 10	新奇類	智利政府認證：確有UFO□詭異飛行器不是戰機！

測試定義

1. 信件開啟：偵測受測者於收到警覺性測試信件後，預覽或開啟信件圖片或內容，因而被記錄者。
2. 連結點選：偵測受測者於收到警覺性測試信件後，開啟信件並連結到信件中之URL或開啟附檔連結網址或附檔，因而被記錄者。

結果分析摘要

1. 信件類別比率分析： 以Letter 2(知識類□14□)□Letter 3(科技類□14□)□Letter 9(健康類：14%)較高外，其餘差別不太大。



2. 信件動作分析：以開啟信件（81%）數量最多，開啟附檔（16%），點擊信件中之URL□3□□□這些動作都可能造成惡意程式的攻擊。

本校受測結果

教育部通知這次測試結果，本校共抽908人受測，開啟信件率19.2%，點選連結率7.9%。

一級單位

單位	人數	單位	人數
研究發展處	37	總務處	23
學生事務處	13	理學院	13
共同教育委員會	12	計算機與通訊中心	12
工學院	12	科技管理學院	11
秘書處	11	原子科學院	11
電機資訊學院	9	圖書館	9
教務處	7	主計室	6
生命科學院	6	人文社會學院	4
全球事務處	4	副校長室	2
人事室	1	清華學院	1

使用者注意事項

電子郵件社交工程型攻擊的目的在於誘騙收信者提供個人資料(如：帳號、密碼)，或**引誘收信者透過下載方式來執行以圖片、連結、夾檔所偽裝的惡意軟體(malware)**，讓電腦中毒成為入侵者所控制的殭屍網路電腦(botnet)□

由於這類的攻擊，如：下載圖片、點選連結，實際惡意軟體的資料是由使用者電腦直接向提供者下載取得，並不會經過郵件伺服器的防毒機制，即使過濾夾檔也有零日病毒(Ⓦzero-day virus)的問題，在郵件伺服器端僅能過濾已知的病毒，因此，**最佳防範這類社交工程型態攻擊的方法，就是使用者要有資安警覺**，收到電子郵件時，注意下列幾件事：

1. **不要開啟不明信件**：開啟信件前，務必先檢視寄件者資料，如有疑問，千萬不要開啟。最好**設定郵件軟體安全性為「不要自動下載圖片」**，以免不小心按到開啟信件時，會自動下載到有問題的檔案，而讓電腦產生安全漏洞。

2. **不點擊不明信件內的連結**
3. **不開啟不明信件的夾檔**

其他參考資料

- 國立臺南大學 - 電子郵件社交工程演練資訊網
  - 郵件軟體安全性設定
    - Outlook Express設定方式說明網頁
    - Microsoft Outlook 2003設定方式說明網頁
    - Microsoft Outlook 2007設定方式說明網頁