

教育部100上半年度電子郵件社交工程演練結果說明

教育部100上半年度電子郵件社交工程演練，本校排名為B級單位(全國129所大學)第113名。為了提高本校教職員工的資安意識，本中心除了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，教育部或行政院還會不定期地實施，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2011年5月10日至2011年6月03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

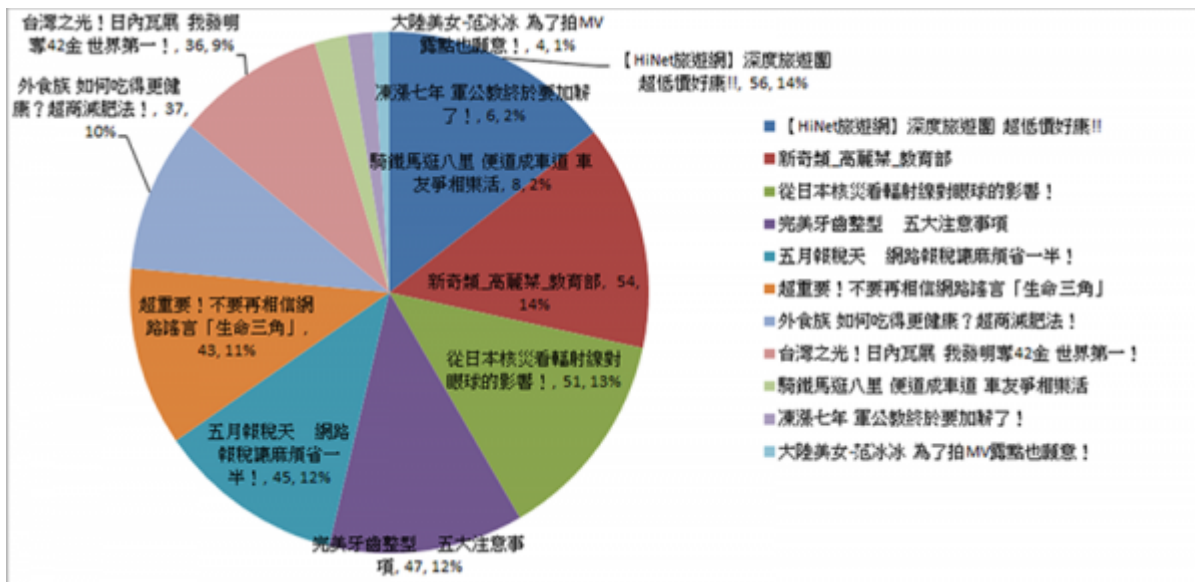
| 組別 | 信件類別 | 信件標題 |
|-----------|-------|-------------------------|
| Letter 1 | 旅遊圖片類 | HiNet 旅遊網】深度旅遊團 超低價好康！！ |
| Letter 2 | 生活類 | 五月報稅天 網路報稅讓麻煩省一半！ |
| Letter 3 | 知識類 | 超重要！不要再相信網路謠言「生命三角」 |
| Letter 4 | 科技類 | 台灣之光！日內瓦展 我發明奪42金 世界第一！ |
| Letter 5 | 美女類 | 大陸美女-范冰冰 為了拍MV露點也願意！ |
| Letter 6 | 美容類 | 完美牙齒整型 五大注意事項 |
| Letter 7 | 旅遊類 | 騎鐵馬逛八里 便道成車道 車友爭相樂活 |
| Letter 8 | 時事類 | 從日本核災看輻射線對眼球的影響！ |
| Letter 9 | 財經類 | 凍漲七年 軍公教終於要加薪了！ |
| Letter 10 | 健康類 | 外食族 如何吃得更健康？超商減肥法！ |
| Letter 11 | 新奇類 | 巨無霸高麗菜 重30臺斤超吸睛 |

測試定義

1. 信件預覽：偵測受測者於收到警覺性測試信件後，預覽信件圖片或內容，因而被記錄者。
2. 連結點選：受測人員點選測試信件中之連結網址或附檔，因而被記錄者。

結果分析摘要

1. 信件類別比率分析：除 Letter 5(美女類) 較低外(1%) Letter 1(旅遊圖片類) Letter 11(新奇類) 較高外(14%)，其餘差別不太大。



2. 信件動作分析：以開啟信件（76%）數量最多，開啟附檔（18%），點擊信件中之URL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338人受測，開啟信件率35.21%，點選連結率15.68%，平均25.45%，排名為B級單位(全國129所大學)第113名。

行政單位

| 單位 | 人數 | 單位 | 人數 |
|---------|----|----------|----|
| 總務處 | 28 | 會計室 | 7 |
| 研究發展處 | 19 | 學生事務處 | 5 |
| 圖書館 | 12 | 國際事務處 | 3 |
| 教務處 | 10 | 清華學院 | 1 |
| 共同教育委員會 | 8 | 計算機與通訊中心 | 1 |
| 秘書處 | 7 | | |

教學單位

| 單位 | 人數 | 單位 | 人數 |
|------------|----|-------------|----|
| 材料科學工程學系 | 4 | 工業工程與工程管理學系 | 2 |
| 化學工程學系 | 3 | 資訊工程學系 | 2 |
| 動力機械工程學系 | 3 | 中國文學系 | 1 |
| 物理學系 | 3 | 核子工程與科學研究所 | 1 |
| 生命科學院 | 3 | 工學院學士班/工學院 | 1 |
| 電機工程學系 | 3 | 理學院 | 1 |
| EMBA | 2 | 化學系 | 1 |
| MBA | 2 | 生命科學系 | 1 |
| 人文社會學院 | 2 | 資訊系統與應用研究所 | 1 |
| 工程與系統科學系 | 2 | 電子工程研究所 | 1 |
| 生醫工程與環境科學系 | 2 | | |

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](#)

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/security:email_test_100_1

Last update: **2011/08/24 10:00**

