

教育部99上半年度電子郵件社交工程演練結果說明

教育部99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102所大學)第48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2010年5月24日至2010年6月04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	您的報稅內容正確嗎？申報綜所稅7大錯誤
Letter 2	美女類	！！台灣最美獸醫 連桃太郎都驚艷！！
Letter 3	健康類	炎炎夏日 防曬不能少！
Letter 4	知識類	地震時如何有效的保護自己
Letter 5	旅遊類	上海世博會 台灣館 天燈造型 驚艷全場
Letter 6	趣味類	我家有小車神～七歲展現停車特技的小女孩！
Letter 7	社會類	美《時代》百大人物 愛心婦陳樹菊入列
Letter 8	時事類	2011順向坡位置大分析
Letter 9	科技類	陽明團隊揭密 基因 Cisd2 讓人長壽
Letter 10	財經類	史上最難搶「鐵」飯碗 錄取率僅1.25%

測試定義

1. 信件開啟：受測人員開啟測試信件並且完成圖片下載之動作，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，因而被記錄者。

結果分析摘要

1. 信件類別比率分析：除 Letter 6(趣味類)較低外(6%)□Letter 4(知識類)較高外(17%)，其餘差別不太大。
2. 信件動作分析：以開啟信件（71%）數量最多，開啟附檔（20%），點擊信件中之URL□9□□□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380受測，開啟信件率16.32%，點選連結率8.16%，平均12.24%，排名為B級單位(全國102所大學)第48名。

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([W 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:
<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
http://net.nthu.edu.tw/netsys/security:email_test_99_1

Last update: **2010/09/02 15:10**

