教育部98上半年度電子郵件社交工程演練結果說明

教育部98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45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2009年5月11日至26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。
教育部合格標準：惡意郵件開啟率應低於10%以下；惡意連結（或檔案）點擊率應低於6%

測試信件摘要表

組別	信件類別	信件標題
Letter 1	政治、體育類	軍方賣官內幕 洋基球團虧待王建民
Letter 2	休閒娛樂類	自行車旅遊私房路線 聯合報邀您賞桐花
Letter 3	科技新知、保健養生類	USB 成病毒温床！台灣電腦今件Q1中毒率列入全球第四大 蛀牙不是病，痛起來要人命
Letter 4	投資理財、保健養生類	景氣復甦了嗎？ 新流感 H1N1 大流行期間，個人保健注意事項
Letter 5	情色、影視新聞類	瑤瑤和舒舒，你喜歡誰

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. 信件開啟比率分析，除 Letter 5 (情色、影視新聞類) 較低外(10%)，其餘差別不太大。
2. 連結點選比率分析Letter 2 (休閒娛樂類)高達39%，反應出**受測人員對旅遊資訊的警覺性較低**，尤其目前很熱門的自行車風潮，可能影響受測人員判斷的原因之一。此為社交工程攻擊手法最常利用的弱點。

本校受測結果

教育部通知這次測試結果，本校共抽278人受測，開啟信件率6.69%，點選連結率1.51%，平均4.10%，排名為B級單位(全國102所大學)第45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(Ⓦ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
- 教育部98年上半年電子郵件社交工程演練 南大獲全國第二名佳績

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

Permanent link:
https://net.nthu.edu.tw/netsys/security:email_test_98_1

Last update: **2022/09/28 09:32**