教育部99下半年度電子郵件社交工程演練結果說明

教育部99下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2010年09月20日至2010年10月05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

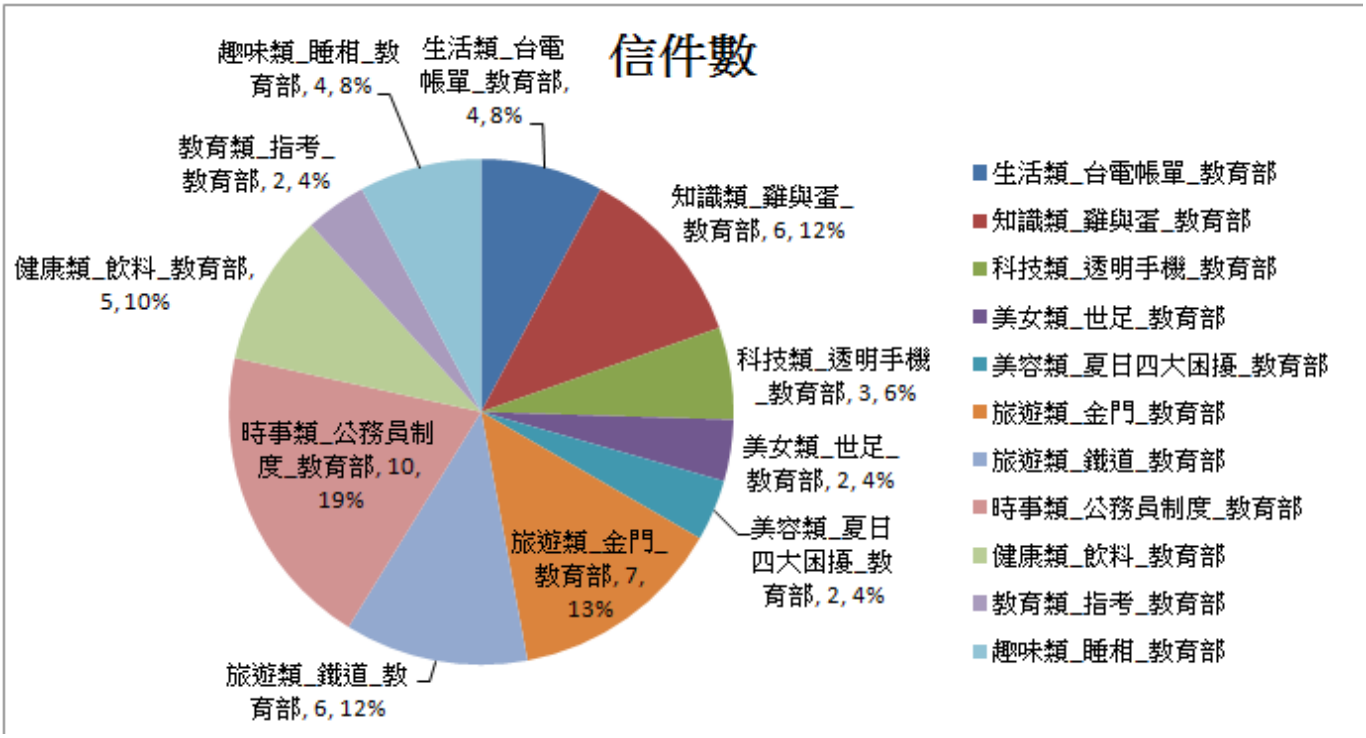
組別	信件類別	信件標題
Letter 1	生活類_台電帳單_教育部	台電烏龍帳單頻傳！你有注意過你家的電費是否合理嗎?
Letter 2	知識類_雞與蛋_教育部	到底是先有雞還是先有蛋！？答案公佈了！
Letter 3	美女類_世足_教育部	世足正妹比一比！你最喜歡哪位！
Letter 4	美容類_夏日四大困擾_教育部	女生不可不知的夏日四大困擾
Letter 5	健康類_飲料_教育部	炎炎夏日，喝杯清涼的飲料最爽快！但是你知道什麼飲料會讓你越喝越肥嗎?
Letter 6	教育類_指考_教育部	明年指考 單選題可望取消倒扣
Letter 7	趣味類_睡相_教育部	睡要有睡相！你沒看過的精采睡相….
Letter 8	時事類_公務員制度_教育部	公務員退休制度超級比一比！
Letter 9	旅遊類_金門_教育部	HiNet旅遊網】開學旅遊團 超低價好康!!
Letter 10	科技類_透明手機_教育部	全世界第一支全透明手機！未來的新趨勢~
Letter 11	旅遊圖片類_鐵道_教育部	鐵道迷的麥加！ 國定古蹟一下淡水溪鐵橋

測試定義

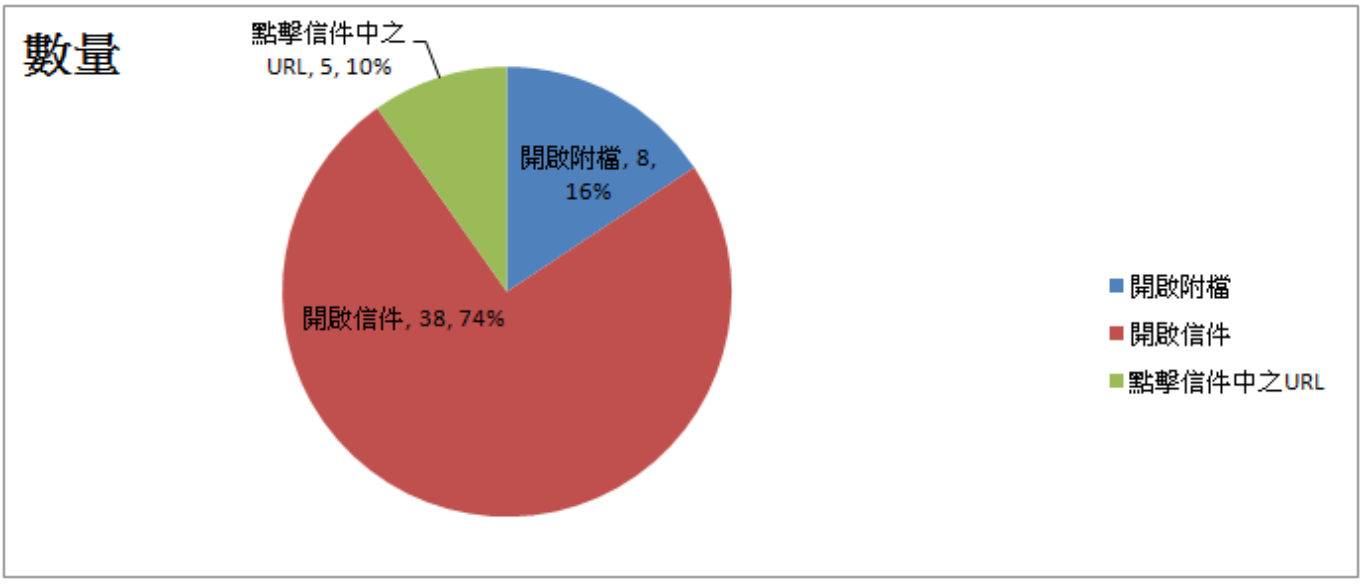
1. 信件開啟：受測人員開啟測試信件並且完成**圖片下載**之動作，因而被記錄者。
2. 開啟附檔：受測人員開啟信件中的附檔，因而被記錄者。
3. 連結點選：受測人員點選測試信件中之連結網址，因而被記錄者。

結果分析摘要

1. 信件類別比率分析：比例以時事類所佔較高外(10%)，其餘差別不太大。



1. 信件動作分析：以開啟信件（74%）數量最多，開啟附檔（16%），點擊信件中之URL□10□□□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397受測，開啟信件率5.54%，點選連結率3.02%，平均%，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

- 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_99_2

Last update: **2011/01/26 14:51**