教育部101上半年度電子郵件社交工程演練結果說明

教育部101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118所大學)第85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2012年6月14日至2012年7月3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

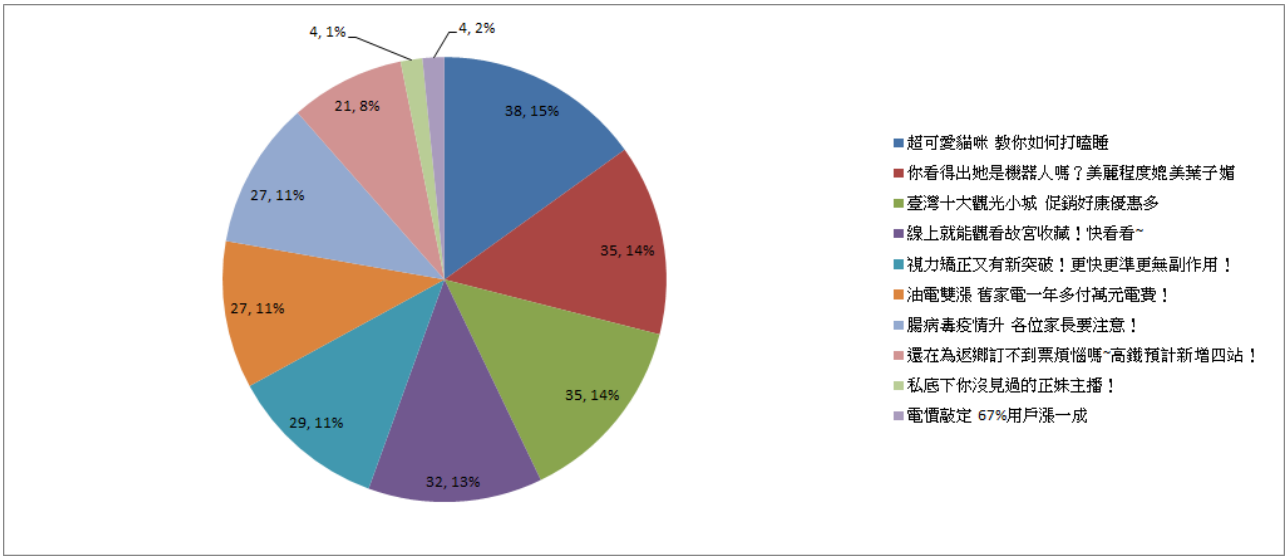
組別	信件類別	信件標題
Letter 1	生活類	還在為返鄉訂不到票煩惱嗎~高鐵預計新增四站！
Letter 2	知識類	你看得出她是機器人嗎？美麗程度媲美葉子媚
Letter 3	科技類	線上就能觀看故宮收藏！快看看~
Letter 4	美女類	私底下你沒見過的正妹主播！
Letter 5	美容類	視力矯正又有新突破！更快更準更無副作用！
Letter 6	旅遊類	臺灣十大觀光小城 促銷好康優惠多
Letter 7	時事類	油電雙漲 舊家電一年多付萬元電費！
Letter 8	財經類	電價敲定 67%用戶漲一成
Letter 9	健康類	腸病毒疫情升 各位家長要注意！
Letter 10	新奇類	超可愛貓咪 教你如何打瞌睡

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：除 Letter 5(美女類：1%) 較低外Letter 10(新奇類15)Letter 2(知識類14)Letter 6 (旅遊類：14%)、較高外，其餘差別不太大。



2. 信件動作分析：以開啟信件（80%）數量最多，開啟附檔（13%），點擊信件中之URL□7□□□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779人受測，開啟信件率17.20%，點選連結率5.52%，平均19.90%，排名為B級單位(全國118所大學)第85名。

行政單位

單位	人數	單位	人數
總務處	25	圖書館	4
研究發展處	24	環安中心	3
計算機與通訊中心	11	會計室	3
學生事務處	9	產學合作營運總中心	3
秘書處	8	國際事務處	3
教務處	5		

教學單位

單位	人數	單位	人數
理學院	11		
工學院	7		
共同教育委員會	7		
生命科學院	6		
電資學院	5		
科技管理學院	5		
人文社會學院	4		
原科院	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_101_1

Last update: **2022/09/28 09:30**