教育部111上半年度電子郵件社交工程演練結果說明

教育部111上半年度電子郵件社交工程演練，本校受測人數為100名（含一、二級行政主管），未通過演練人員共21名，為了提高本校教職員工的資安意識，本中心將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，教育部或行政院每年度會不定期地實施，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2022年4月22日至2022年05月22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	科技類	Safari漏洞或導致瀏覽歷史 Google帳戶資訊外洩
Letter 2	學術類	遠端教育訓練變更通知
Letter 3	公務類	【公告】人事異動通知
Letter 4	公務類	【公告】員工加薪通知
Letter 5	擬真類	如果您無法登入帳戶

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. 開啟信件類別分析：以「【公告】人事異動通知」最多，有 7 人開啟。
2. 點擊信件連結作分析：以「【公告】人事異動通知」最多，有 16 人點擊連結或開啟附件。

本校受測結果

教育部通知這次測試結果，本校共抽100人受測，開啟信件率 7%。

一級單位 開啟信件

單位	人數	單位	人數
教務處	1	理學院	1
計算機與通訊中心	1	工學院	1
人文社會學院	1	電機資訊學院	1
秘書處	1		

教育部通知這次測試結果，本校共抽100人受測，點選連結率 2%。

一級單位 點選連結

單位	人數	單位	人數
藝文總中心	1	全球事務處	1

教育部通知這次測試結果，本校共抽100人受測， 開啟附檔14%。

一級單位 開啟附檔

單位	人數	單位	人數
教務處	5	總務處	4
計算機與通訊中心	2	人文社會學院	1
工學院	1	電機資訊學院	1

一級單位 未通過人員統計

教育部通知這次測試結果，本校共抽100人受測，未通過總數21人，一、二級主管 7人，總未通過率 21%。

單位	人數	單位	人數
教務處	5	總務處	4
計算機與通訊中心	3	工學院	2
人文社會學院	2	電機資訊學院	1
藝文總中心	1	理學院	1
秘書處	1	全球事務處	1

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**。

個人電腦安全防護

1. 電腦應定期更新、修補作業系統及應用程式漏洞。
2. 個人電腦應安裝防毒軟體，並定期更新病毒碼，設定定期主動掃描檢查作業。

3. 密碼需定期更換，並開啟密碼複雜度設定，長度應至少8碼。
4. 開啟螢幕保護程式並設定螢幕保護密碼，可避免人員離開座位洩漏螢幕資訊。
5. 建議關閉電子郵件軟體的郵件預覽功能，並勿開啟來源不明的電子郵件。
6. 勿任意下載、安裝來路不明的軟體。
7. 建議禁止使用點對互連□P2P□軟體或提供分享檔案。
8. 建議禁止於上班時間瀏覽不良網站（如暴力、色情、賭博等）及非公務用途網站，以避免遭駭客植入惡意程式及造成網路壅塞。
9. 電腦內重要資料文件應定期異地備份，避免遭受勒索軟體威脅。
10. 定期自動化掃描潛藏的惡意程式或勒索軟體，已遏止發生資安事件。

其他參考資料

* 郵件軟體安全性設定

- 各種郵件軟體不下載遠端圖片的設定方式

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

Permanent link:
https://net.nthu.edu.tw/netsys/security:email_test_111_1

Last update: **2022/09/28 09:27**