教育部112年度第1次電子郵件社交工程演練結果說明

教育部112年度第1次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），本次受測人員全員通過，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。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2023年07月24日至2023年08月20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	情色類	補教狼師MeToo MeToo MeToo 最美禮生控「18 歲生日遭揉胸強吻」
Letter 2	科技類	ChatGPT ChatGPT ChatGPT ChatGPT 官方APP 來了！台灣開放下載 iPhone iPhone 搶先試
Letter 3	休閒類	連假這樣請半個月都不用上班！快訂機票半月遊！
Letter 4	公務類	您已接受邀請共用此行事曆
Letter 5	財經類	夏季電費6 月上路！台電估計約378 萬戶不漲價，原因曝光

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。

教育部統整結果分析摘要

1. 開啟信件比例佔：3.63%。
2. 點擊信件比例佔：2.01%。
3. 開啟附件比例佔：0.82%。
4. 點擊連結或開啟附件比例：2.27%
5. 上述任一行為比例加總：5.13%

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 0 %、點選連結率 0 %、開啟附檔 0 %，**受測人員全員通過**

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_112_1

Last update: **2024/03/14 15:17**