

教育部98下半年度電子郵件社交工程演練結果說明

教育部98下半年度電子郵件社交工程演練，本校279人受測，5人未通過。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，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。未來教育部或行政院還會持續不定期地實施這類的演練，請本校教職員工務必詳讀注意事項及其建議，並提高資安警覺。

本校受測結果

時間	受測人數	開啟信件率	點選連結率
9月份	279人	1.08% (3人)	0.72%(2人)

/

- 未通過單位人數
 - 生科(@life.nthu.edu.tw) 1人
 - 工工(@ie.nthu.edu.tw) 1人
 - 資工(@cs.nthu.edu.tw) 3人

類型	信件標題	行為	未通過者代碼
購物類3	iPhone 最新推出3Gs 便宜到不敢相信！！	開啟附檔	A
生趣味類	親愛的同事!放鬆一下	開啟附檔	A
健康類	健康新撇步!?!你如何活的更健康	開啟附檔	A
電腦科技類	七夕前後交友網站爆高量 慎防網路桃色陷阱	開啟附檔	A
趣味類	親愛的同事!放鬆一下	開啟信件	B
生活類	讓你感動的動人廣告	開啟附檔	C
生活類	讓你感動的動人廣告	開啟信件	D
生活類	讓你感動的動人廣告	開啟信件	E
影視類	文英阿姨病逝 留給觀眾無限懷念	開啟信件	E

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

建議：為讓自己的電腦遠離危險，須調整個人電腦上收信軟體設定，以增加安全性，「**不自動下載圖片**」、「**不開啟預覽視窗**」、「**以純文字開啟信件**」，可有效避免電子郵件社交工程型的攻擊，設定方式請參閱

[「防止電子郵件社交工程攻擊 收信軟體設定建議」](#) □

參考資料

- [教育部98上半年度電子郵件社交工程演練結果說明](#)
- [防範惡意電子郵件社交工程教育訓練\(98/08/12\)](#)
- [防止電子郵件社交工程攻擊 收信軟體設定建議](#)

From:

<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

http://net.nthu.edu.tw/netsys/security:email_test_98_2

Last update: **2009/11/16 09:28**

