

中國醫藥大學 防範電子郵件社交工程演練 因應措施

中國醫藥大學
蔡益吉

kai@mail.cmu.edu.tw

- 演練是資安人員的事？
- 資安人員做什麼事？
- 參與演練人員做什麼事？
- 失敗人員懲處
- 防範電子郵件社交工程改善計畫

資安人員的事？

- 教育部來文誰收？
- 演練信件是寄到誰的信箱？
- 參與演練人員皆有責？

資安人員做什麼事？

■ 教育訓練

- 演練前教育訓練
- 寒暑假定期教育訓練

■ 自辦演練

- 找出對社交工程演練意識與防護能力較薄弱的演練人員
- 失敗人員電話關切，了解原因，立即解決
- 重複失敗人員斷網，直至簽署檢核表，保證了解並完成相關工作

自辦演練

- 記錄受測人員IP位址，比對收信來源IP。
- 演練結果：

2010						
時間	4月29日	4月30日	5月1日	5月3日	5月3日	5月5日
開啓	11	6	3	4	2	1
點選	1	0	3	1	0	0
時間	5月5日	5月6日	5月17日	5月21日	7月15日	7月16日
開啓	1	2	0	0	0	0
點選	0	0	0	0	0	0

自辦演練

- 記錄受測人員IP位址，比對收信來源IP。
- 演練結果：

2011							
時間	4月20日	4月21日	5月2日	5月3日	5月3日	5月6日	5月6日
開啓	14	15	2	1	4	1	0
點選	6	7	2	0	2	1	0
時間	5月9日	5月12日	5月15日	5月18日	5月19日	5月20日	
開啓	2	1	1	0	0	1	
點選	0	0	0	0	0	0	1

參與演練人員做什麼事？

- 參加教育訓練
- 修改收信軟體設定
- 不開啓跟自己無關的郵件及附件檔
- 不隨便開啓郵件中的超鏈結
- 不要任意的轉寄信件
- 不連線至未知網站
- 不提供密碼或其他個人資料

失敗人員懲處

- 行文知會演練失敗人員及單位主管
- 演練失敗人員提出說明及改善方法
- 演練失敗中斷校外網路6個月
- 簽回防範電子郵件社交工程檢核表

電子郵件社交工程演練結果

	部定目標值(B級)		全國平均值(B級)		本校值	
	開啓率	點選率	開啓率	點選率	開啓率	點選率
98上	< 26%	< 15%	8.38%	1.25%	8.06%	0.30%
98下	< 16%	< 9%	16.62%	12.27%	17.91% (提改善計畫)	7.46%
99上	< 10%	< 6%	18.09%	10.55%	0%	0%
99下	< 10%	< 6%	11.40%	4.59%	1%	0%
100上	< 10%	< 6%	17.99%	7.93%	0%	0%

防範電子郵件社交工程改善計畫

- 分析演練失敗原因
- 改善計畫
 - 加強教育訓練
 - 定期教育訓練
 - 失敗人員懲處
 - 自辦演練
 - 防範電子郵件社交工程檢核表