社交工程

計算機與通訊中心
網路系統組 陳怡碩
E-mail：yschen@cc.nthu.edu.tw
分機：31234

Outline

- 社交工程介紹
- 103年度的演練結果
- 社交工程的防護

社交工程

- 社交工程的定義
  - 利用人性弱點或利用人際之信任關係來進行詐騙，是一種非“全面”技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。
  - 社交工程陷阱這個名詞來自駭客出身的資安顧問 – Kevin Mitnick，它是種引誘人們做出本意不想的行為，或是給出機密資料。欺騙的藝術(The Art of Deception)的作者（Kevin Mitnick），更進一步的解釋到人類的天性就是很希望能幫助別人，因此也相當容易被欺騙。
  - 網路世界的數位安全(Secrets & Lies: Digital Security in a Networked World)的作者Bruce Schneier曾提到所謂社交工程，全都是由人性方面，也就是利用所謂的「信任」來進行。
  - 以人為本、騙術為主
  - 技術門檻低
  - 貪心、好奇：**小心！ALS漸凍人冰桶挑戰熱潮，每日千台電腦中毒**
  - 缺乏警覺性：有那麼嚴重嗎？

社交工程詐騙成功的結果

- 垃圾信的發信主機
- 機密資料外洩
- 攻擊他人主機的跳板
- 非法資料的存放主機
- …

Check Point調研摘要內容（一）

- 社交工程攻擊的確帶來危險：86%的信息技術及安全專家已經意識到社交工程所帶來的各類風險。近48%的受訪企業表示，在過去兩年中曾遭受超過25次的社交工程攻擊。
- 社交工程攻擊帶來嚴重經濟損失：受訪者估計每次安全事故會導致25,000美元至超過100,000美元不等的損失，這其中包括業務中斷、客戶流失、收入減少和品牌受損等。
- 最常見的社交工程攻擊來源：網絡釣魚郵件（47%），其次是會暴露個人和職業信息的社交網絡（39%）以及不安全的移動設備（12%）
- 獲取利益是社交工程攻擊的主要動機：獲取利益被認為是社交工程攻擊的最主要動機，其它動機依次是：獲得專有信息（46%）、取得競爭優勢（40%）以及報復（14%）。

Check Point調研摘要內容（二）

- 新員工最易受到社交工程攻擊影響：受訪者們認為新員工是易受社交工程威脅的高危群體。其它依次為合約商（44%）、行政助理（38%）、人力資源人員（33%）、商業領袖（32%）和信息技術人員（23%）。無論員工在企業中擔任何種職務，對其進行適當培訓並培養其用戶意識都是安全政策中的重要一環。
- 缺乏對預防社交工程危害的主動培訓：針對社交工程攻擊，只有19%的企業有這方面的培訓或部署安全政策，而34%的企業沒有任何計劃。

對象：調研於2011年7月至8月期間進行，採訪了850多名來自美國、加拿大、英國、德國、澳大利亞和新西蘭的信息技術和安全專家。

社交工程攻擊的定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法。
- 早期社交工程是藉由電話或假扮身份問些看似無關緊要的問題等各種方法來獲取所需資訊。
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

社交工程的各種攻擊方法（一）

- 電子郵件隱藏電腦病毒
  - 駭客利用社交工程的概念，將病毒、蠕蟲與惡意程式等隱藏在電子郵件中，這些看似朋友所寄來的郵件，卻是應用社交工程的電子郵件陷阱，例如過去造成重大損害的I LOVE YOU蠕蟲，就是一種利用社交工程散播的電腦病毒
- 網路釣魚
  - 偽裝知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼或登入某網址輸入個人資料等，這種詐騙稱為網路釣魚。收件人若無小心求證而連結了郵件中的鏈結，可能就下載了惡意程式；或者在假網頁上輸入了帳號密碼或信用卡資料等，造成銀行戶頭被盜領或盜刷等的嚴重後果，這是近年來造成個人與企業極大損害的犯罪手法，而網路釣魚就是一種典型的社交工程攻擊。
  - 偽造網址：http://www.hinet.net ←→ http://www.hinet1.net
  - 偽造網頁：製作與原來完全一樣的頁面，以騙取重要的相關資訊。

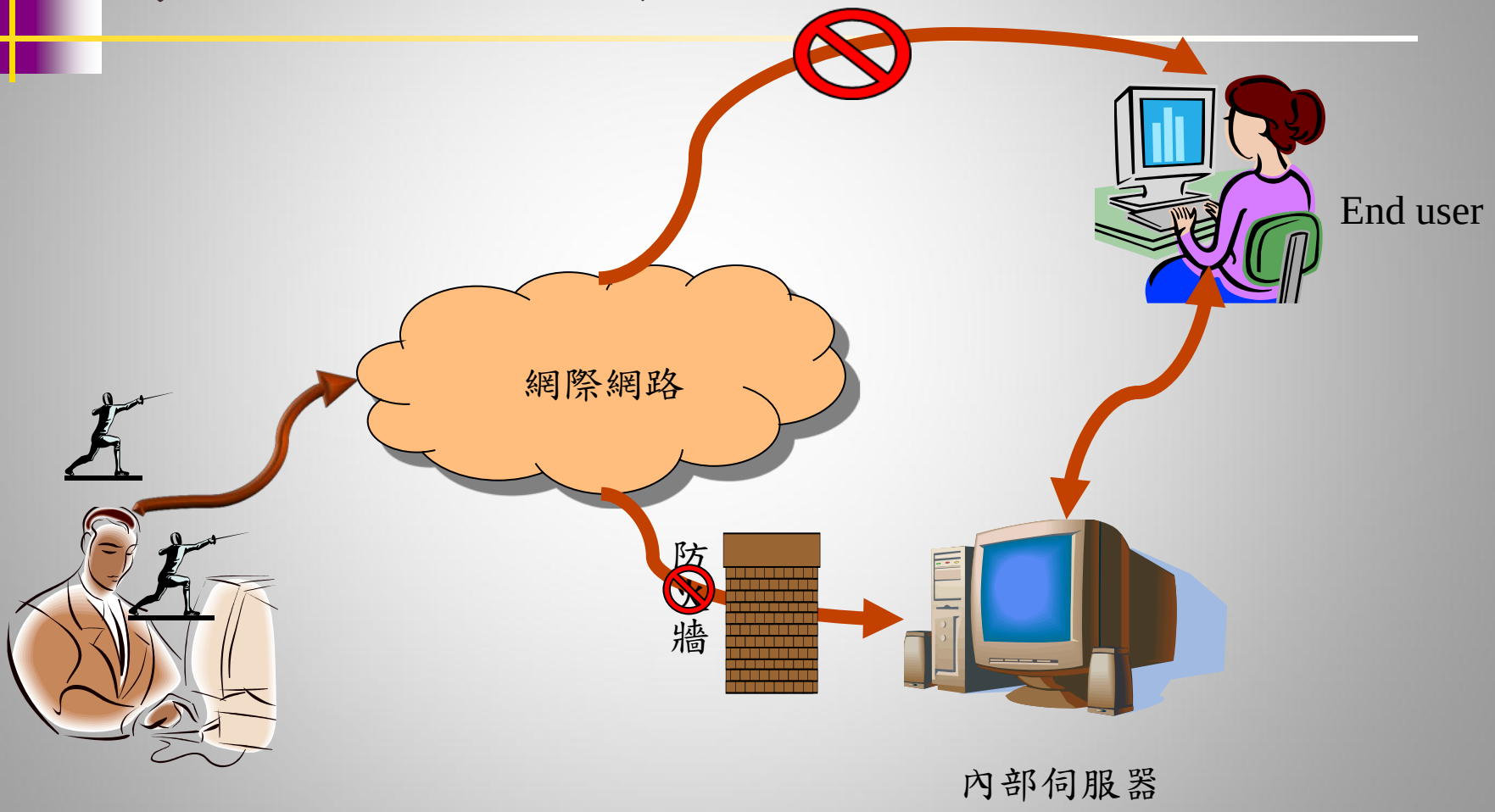
社交工程的各種攻擊方法（二）

- 圖片中的惡意程式
  - 明星或色情圖片也是許多惡意程式慣用的社交工程技巧之一，這些都是利用使用者的好奇心來散佈惡意程式，之前Sobig網路病毒出現在某個含有色情內容的網路討論群組，網友點選了其中像是裸照的內容就會感染病毒，而該病毒總共導致了約10億美金的損失。
- 偽裝修補程式
  - 另一種社交工程的欺騙手法，就是偽裝成微軟的修補更新程式，因為一般使用者不會覺得這是來路不明的程式，卻沒有防範社交工程也會利用這個漏洞，而將惡意程式隱藏其中。使用者若安裝了這個檔案，不但不會修補作業系統的任何漏洞，還可能被安裝了遠端竊取資料的木馬程式。

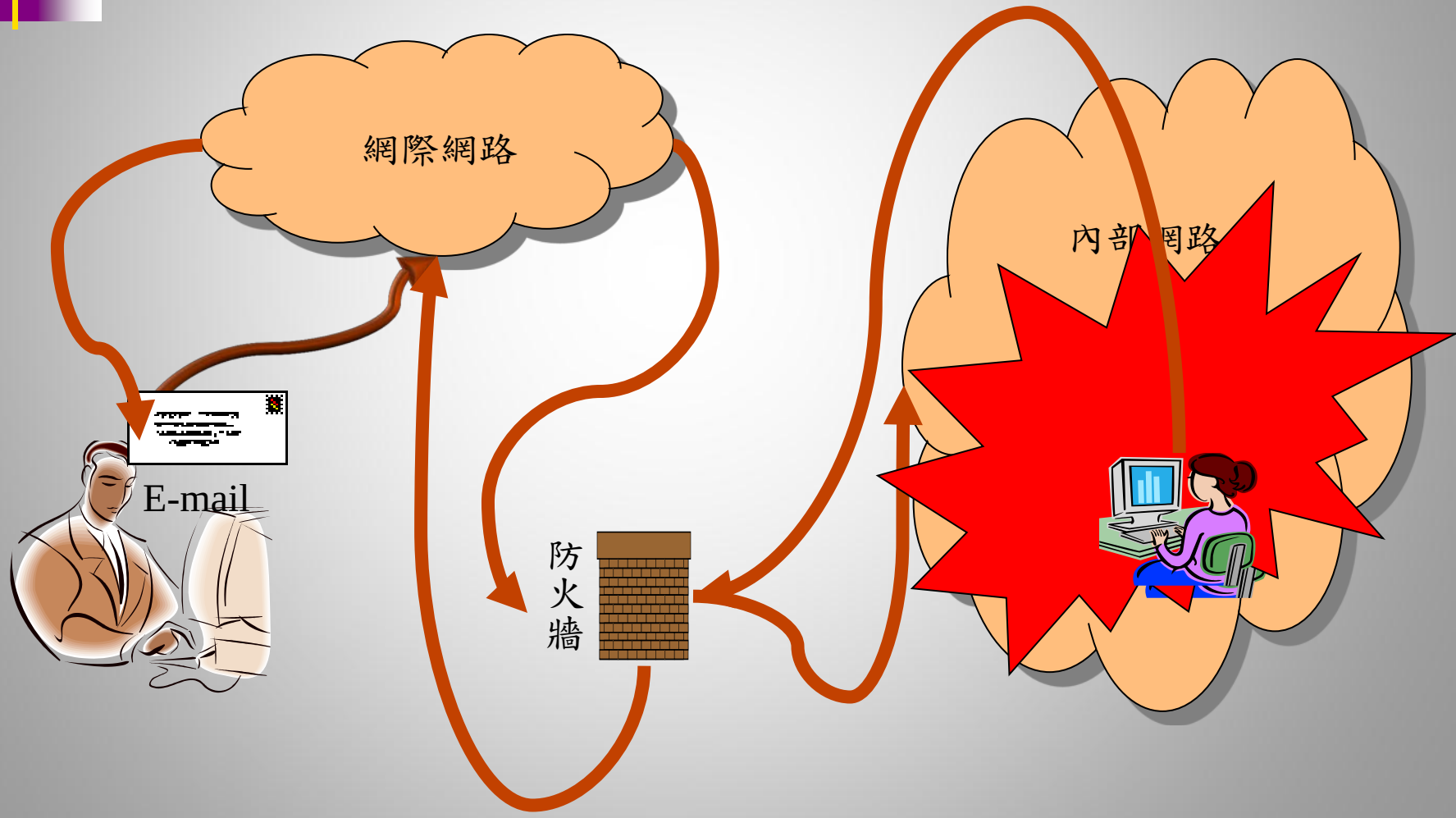
社交工程的各種攻擊方法（三）

- 即時通也是社交工程的新途徑
  - 近年來，社交工程傳播惡意程式的途徑擴大至即時通訊軟體，如MSN、ICQ、YAHOO即時通、QQ等。2005年2月，一個使用MSN大量散播的病毒造成嚴重災情，這個電腦病毒會利用MSN自動傳檔給MSN連絡人上的朋友，亞洲各國皆傳出災情，包括台灣的案例也有千起以上。
  - 手機簡訊也是近年來另一項值得注意的途徑，就臺灣地區光是五月份，手機詐騙得逞的案件就有89萬件（來源：**趨勢科技社群網站**）。
  - LINE免費貼圖詐騙（line ID、FB ID、手機號碼…）
    http://www.techbang.com/posts/12286
- http://www.netadmin.com.tw/article_content.aspx?sn=1401240002

傳統網路攻擊



現在網路攻擊模式



電子郵件社交工程的攻擊步驟

- 有心人設計陷阱或後門程式
- 在電子郵件內放置有害程式或連結
- 將信件寄給特定或不特定對象
- 使用者開啟信件
- 啟動或下載有害程式
- 反向輸出使用者資料（轉眼變成受害者）

軟體弱點與零時差攻擊

- 只要是軟體就可能存在有弱點，未能及修補的話，就可能遭利用被入侵成功。
- 針對軟體弱點未修補前，出現針對弱點的攻擊行為，及稱為「零時差攻擊」。

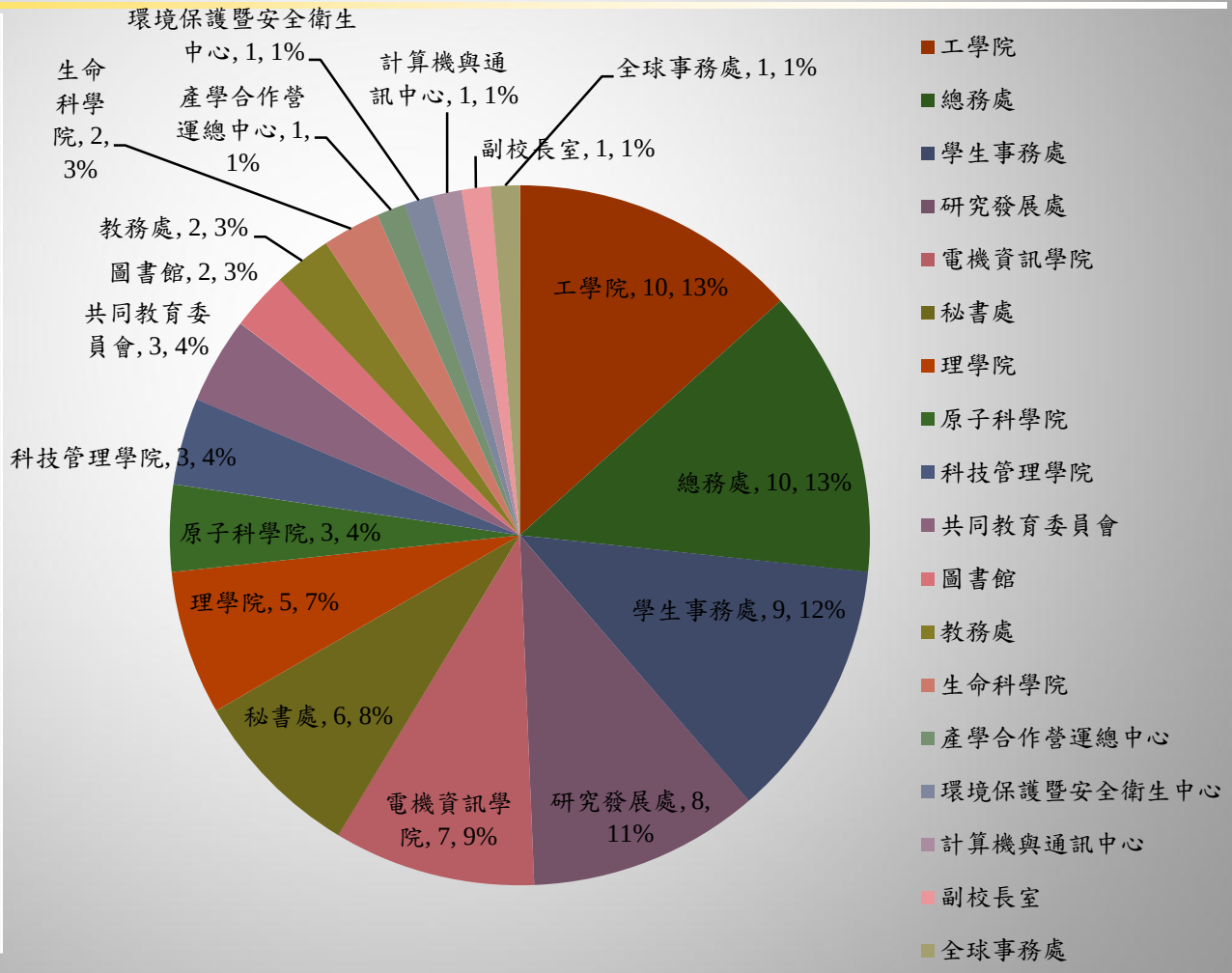
常見被利用的軟體弱點

- 微軟的作業系統和文書軟體
  - Microsoft office（word）
- 常見的應用軟體
  - Winrar、adobe reader、flash player等軟體

演練結果

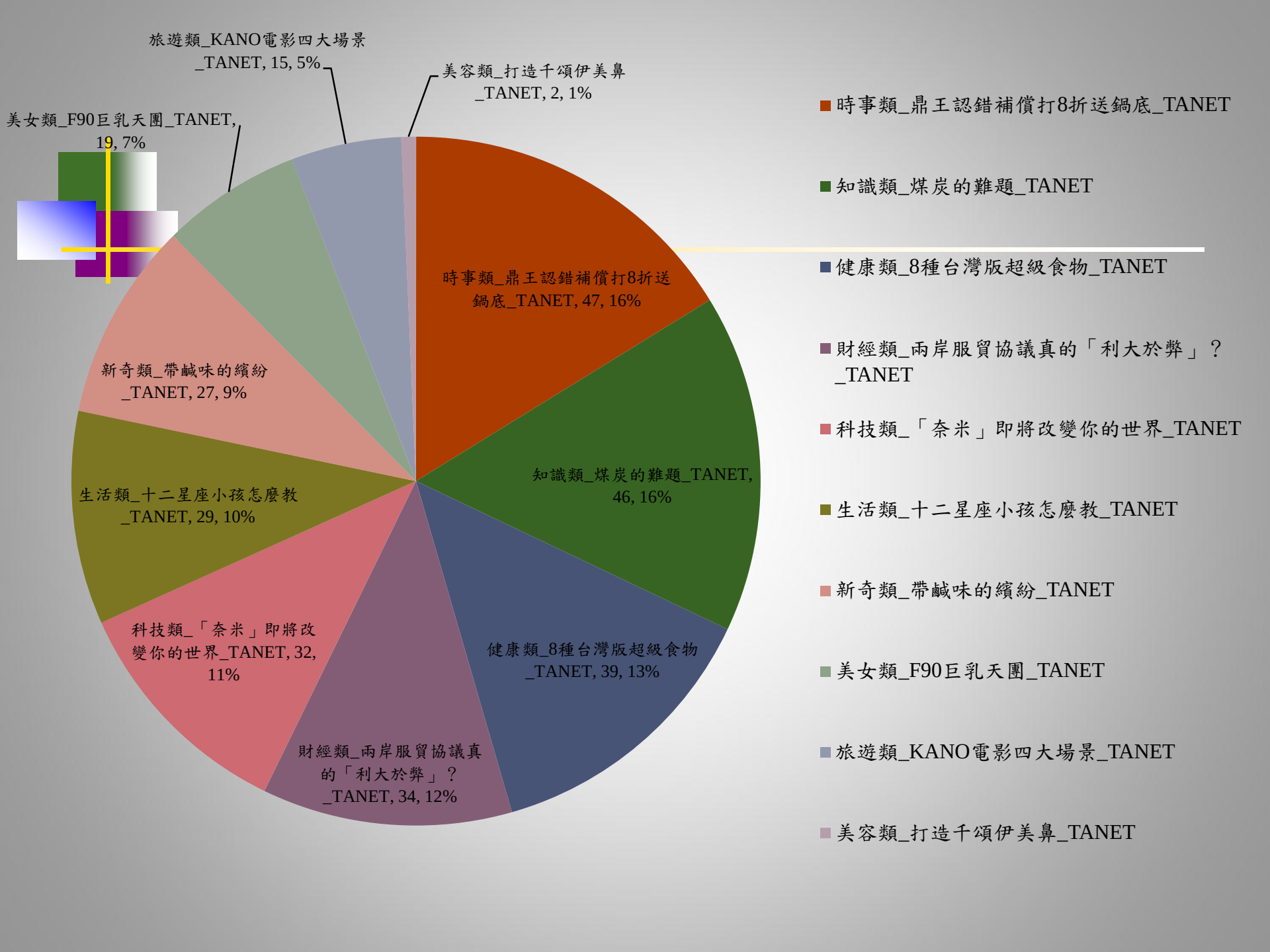
一級單位未通過演練人數統計

未通過名單統計	
一級單位	人數
工學院	10
總務處	10
學生事務處	9
研究發展處	8
電機資訊學院	7
秘書處	6
理學院	5
原子科學院	3
科技管理學院	3
共同教育委員會	3
圖書館	2
教務處	2
生命科學院	2
產學合作營運總中心	1
環境保護暨安全衛生中心	1
計算機與通訊中心	1
副校長室	1
全球事務處	1

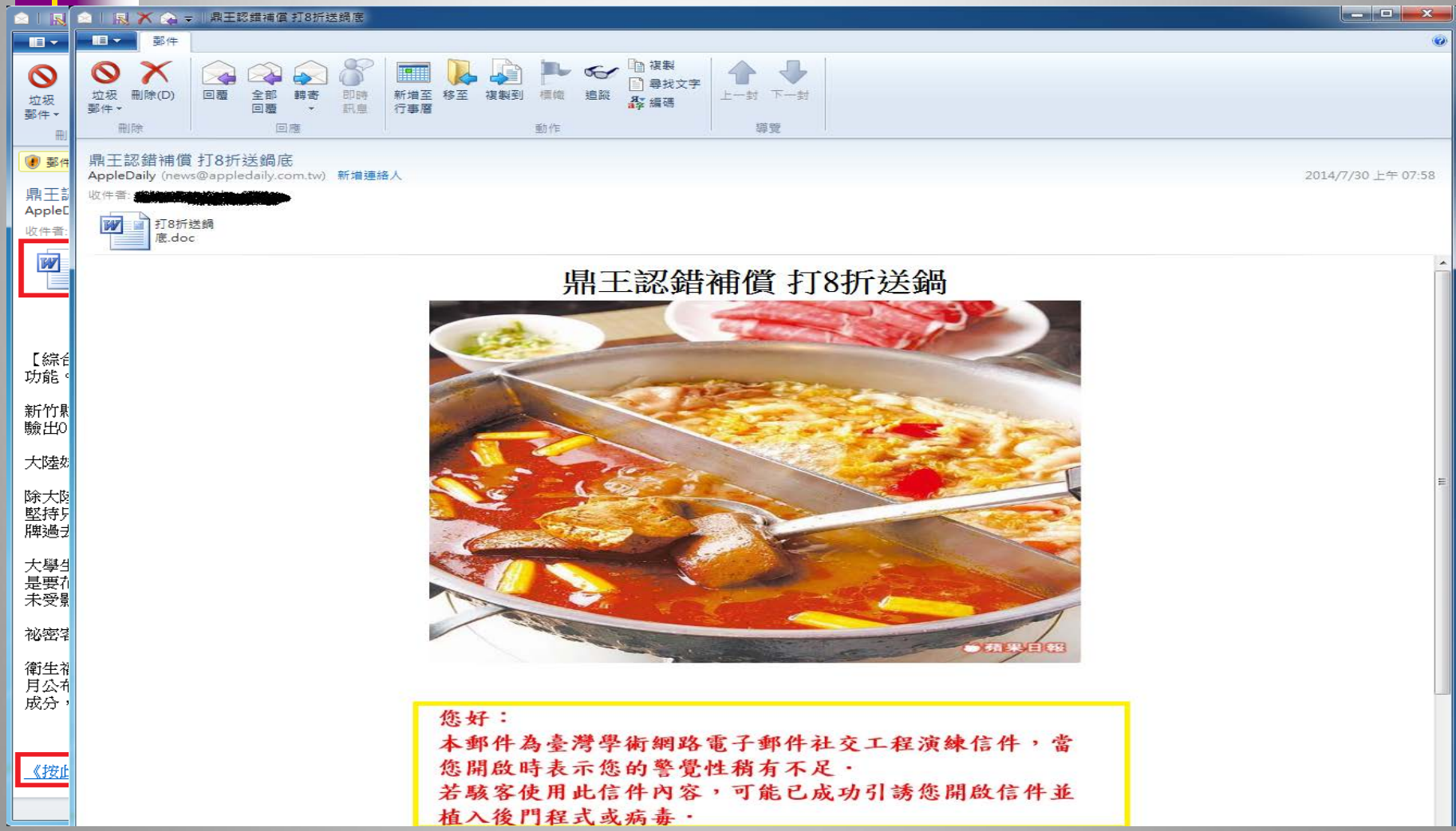


103年上半年度教育部電子郵件社交工程演練標題

編號	信件類別	信件標題
Letter 1	時事類	鼎王認錯補償 打8折送鍋底
Letter 2	知識類	煤炭的難題
Letter 3	健康類	8種台灣版超級食物！你一定不能錯過
Letter 4	財經類	好文分享-兩岸服貿協議真的「利大於弊」？
Letter 5	科技類	「奈米」即將改變你的世界
Letter 6	生活類	十二星座小孩該怎麼教？
Letter 7	新奇類	帶鹹味的繽紛，探索克里米亞腐海之美
Letter 8	美女類	F90--由15名性感妹子組成的遊戲代言團體
Letter 9	旅遊類	跟著KANO電影四大場景，遊台灣棒球原鄉—嘉義
Letter 10	美容類	打造千頌伊美鼻 醫師：微整注射不宜超過2次


旅遊類_KANO電影四大場景_TANET, 15, 5%
美容類_打造千頌伊美鼻_TANET, 2, 1%
美女類_F90巨乳天團_TANET, 19, 7%
時事類_鼎王認錯補償打8折送鍋底_TANET, 47, 16%
知識類_煤炭的難題_TANET, 46, 16%
健康類_8種台灣版超級食物_TANET, 39, 13%
財經類_兩岸服貿協議真的「利大於弊」？_TANET, 34, 12%
科技類_「奈米」即將改變你的世界_TANET, 32, 11%
生活類_十二星座小孩怎麼教_TANET, 29, 10%
新奇類_帶鹹味的繽紛_TANET, 27, 9%
時事類_鼎王認錯補償打8折送鍋底_TANET
知識類_煤炭的難題_TANET
健康類_8種台灣版超級食物_TANET
財經類_兩岸服貿協議真的「利大於弊」？_TANET
科技類_「奈米」即將改變你的世界_TANET
生活類_十二星座小孩怎麼教_TANET
新奇類_帶鹹味的繽紛_TANET
美女類_F90巨乳天團_TANET
旅遊類_KANO電影四大場景_TANET
美容類_打造千頌伊美鼻_TANET

103年上半年度教育部電子郵件社交工程演練案例



103年下半年度教育部電子郵件社交工程演練標題

編號	信件類別	信件標題
Letter 1	生活類	【必看瘋傳】一個高階主管在台積電【賣命癌症過世後給大家的啟示】
Letter 2	知識類	改變孩子一生的5個習慣
Letter 3	科技類	關於蚊子的一些事
Letter 4	美女類	瑜珈女神性感誘惑　史上最辣開球沒有之一
Letter 5	美容類	呼吸就能瘦　美女中醫示範腹式呼吸法
Letter 6	旅遊類	【驚奇景點】聽說最近台灣很紅！最受國際矚目的台灣旅遊奇觀登場
Letter 7	財經類	央行打房下一波？　專家：桃園、新竹恐遭殃
Letter 8	時事類	提早規劃財務 年初退休最省稅
Letter 9	健康類	看清這10點，讓你果汁喝得更安心！
Letter 10	新奇類	智利政府認證：確有UFO！詭異飛行器不是戰機！

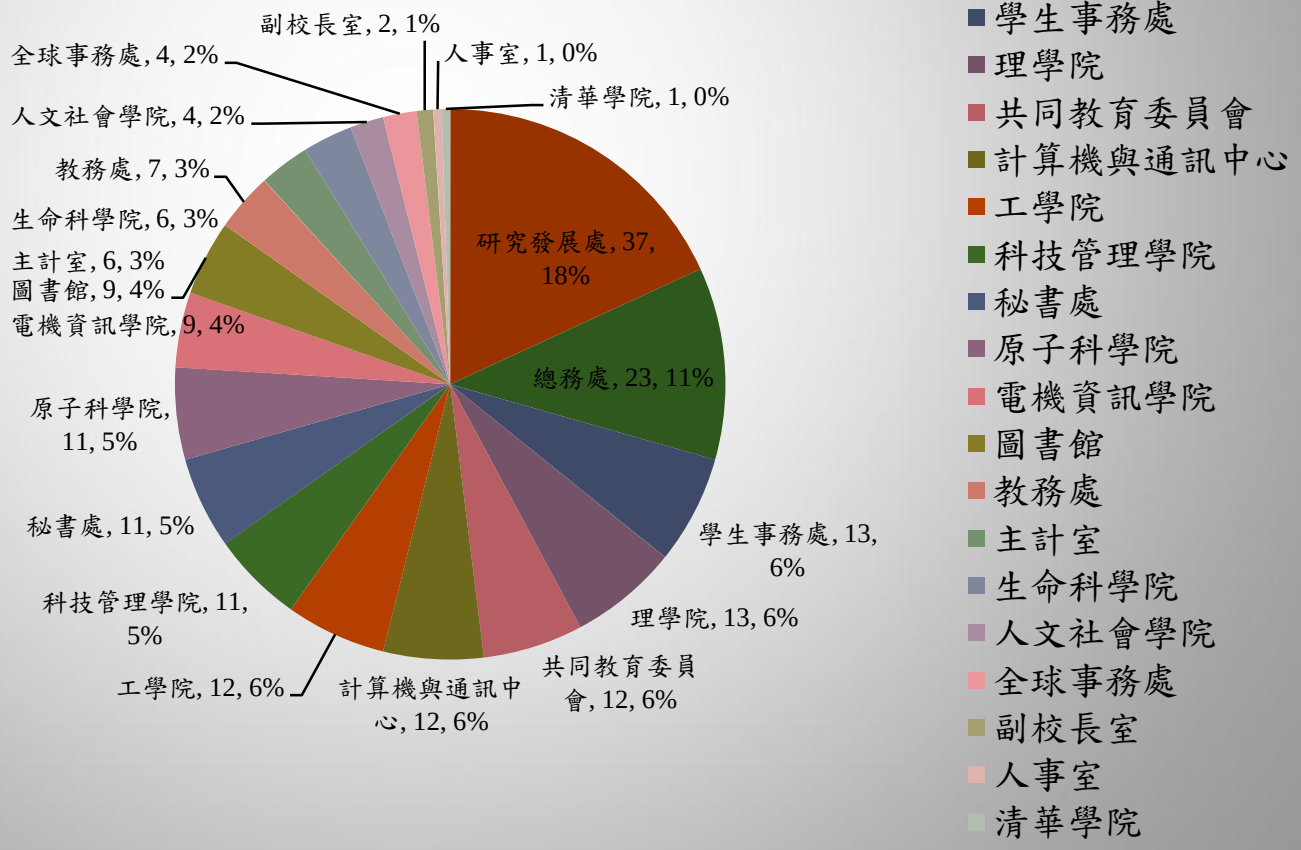
103年度教育部電子郵件社交工程下半年度演練結果

	開啟信件	點選連結
合格標準	10%	6%
清華大學第二次演練結果	19.2%	7.9%
清華大學第一次演練結果	7.93%	1.65%

1. 清華大學總受測人員共908名（含一、二級行政主管），不合格人員共204名（含開啟信件及點選連結），成績較第一次演練結果差。
2. 教育部每年度進行兩次電子郵件社交工程演練。
3. 一二級主管共49名未通過演練，約佔24%。

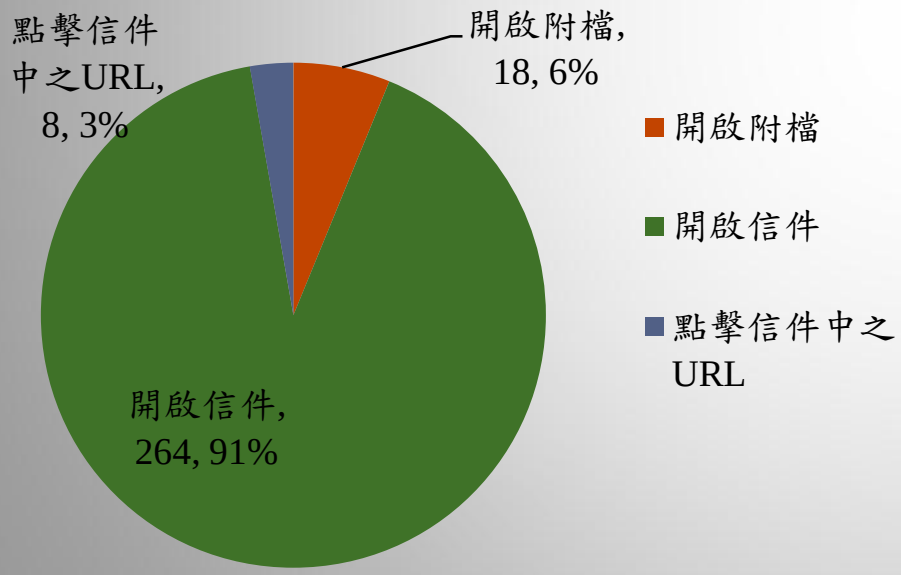
一級單位未通過演練人數統計

一級單位	人數
研究發展處	37
總務處	23
學生事務處	13
理學院	13
共同教育委員會	12
計算機與通訊中心	12
工學院	12
科技管理學院	11
秘書處	11
原子科學院	11
電機資訊學院	9
圖書館	9
教務處	7
主計室	6
生命科學院	6
人文社會學院	4
全球事務處	4
副校長室	2
人事室	1
清華學院	1

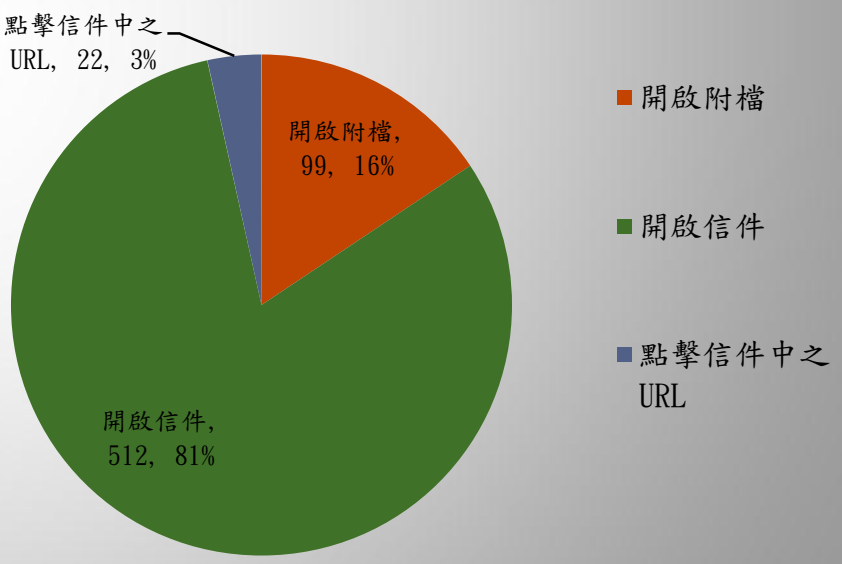


信件處理方式

信件處理方式	次數（290）
開啟附檔	18
開啟信件	264
點擊信件中之URL	8



信件處理方式	次數（633）
開啟附檔	99
開啟信件	512
點擊信件中之URL	22



社交工程的防護

- 基本的防護
  - 作業系統更新
  - 應用軟體更新
  - 防毒軟體、個人防火牆
- 再多一點的防護
  - 調整收信軟體的部分設定
  - 熟悉所使用軟體基本設定
- 近乎完美的防護
  - 改變使用習慣

基本的防護

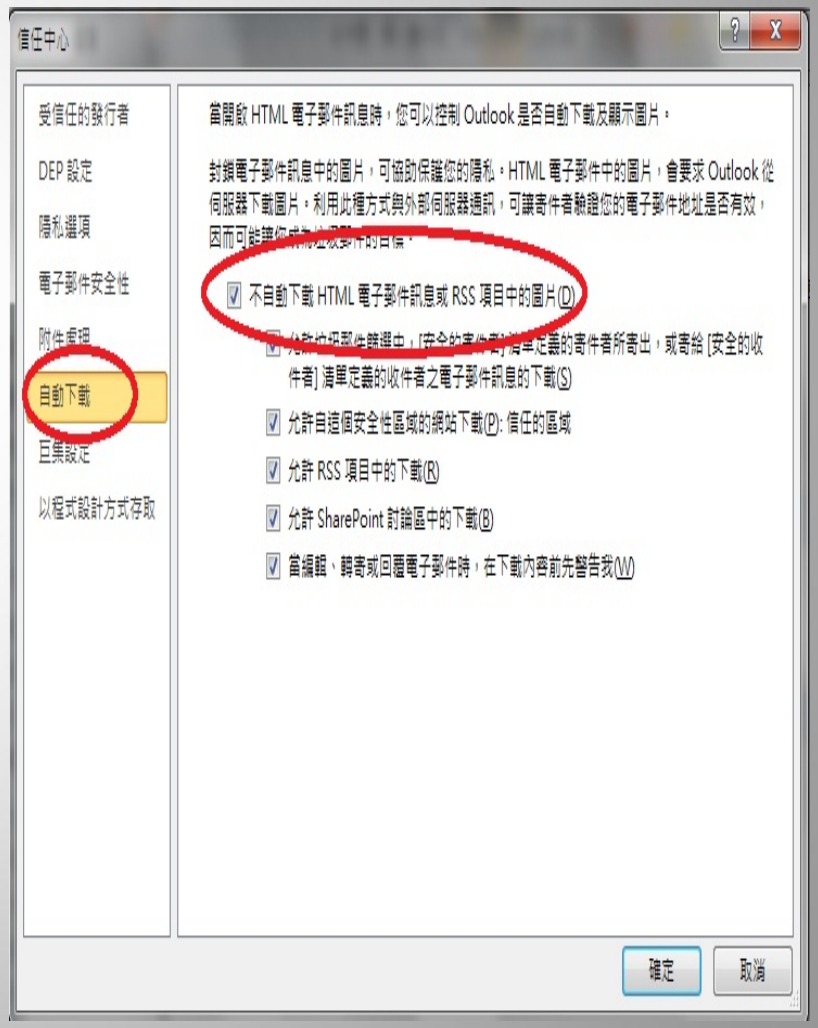
- 作業軟體更新
  - 設定自動更新 microsoft update
- 應用軟體更新
  - Adobe reader…等軟體
- 安裝防毒軟體、個人防火牆並更新病毒碼
  - 卡巴斯基、賽門鐵克、趨勢（學校授權）

再多一點的防護

- 變更看信軟體的設定，提高安全性
  - 不自動下載圖檔
    - outlook2010
    - live mail
  - 關閉信件預覽功能
    - outlook2010
    - live mail
  - 以純文字開啟信件
    - outlook2010
    - live mail

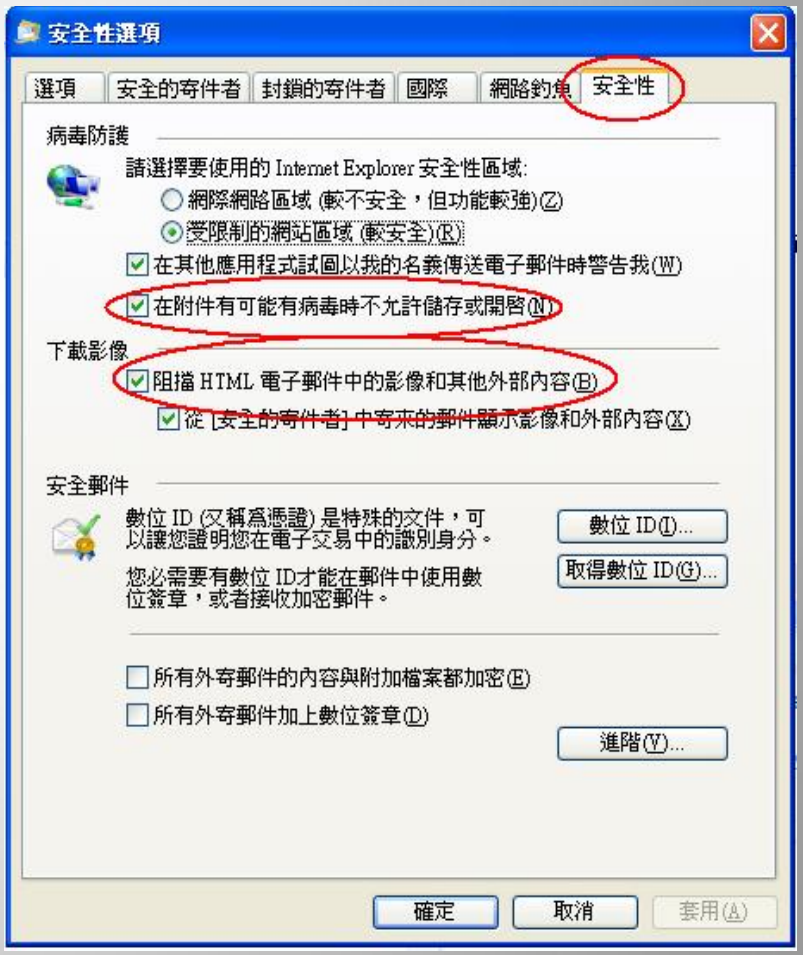
Outlook 2010

- 開啟outlook 2010
- 選取【檔案】
- 選取【選項】
- 選擇【信任中心】
- 點選【信任中心設定】
- 選取【自動下載】
- 將【不自動下載HTML電子郵件訊息或RSS項目中的圖



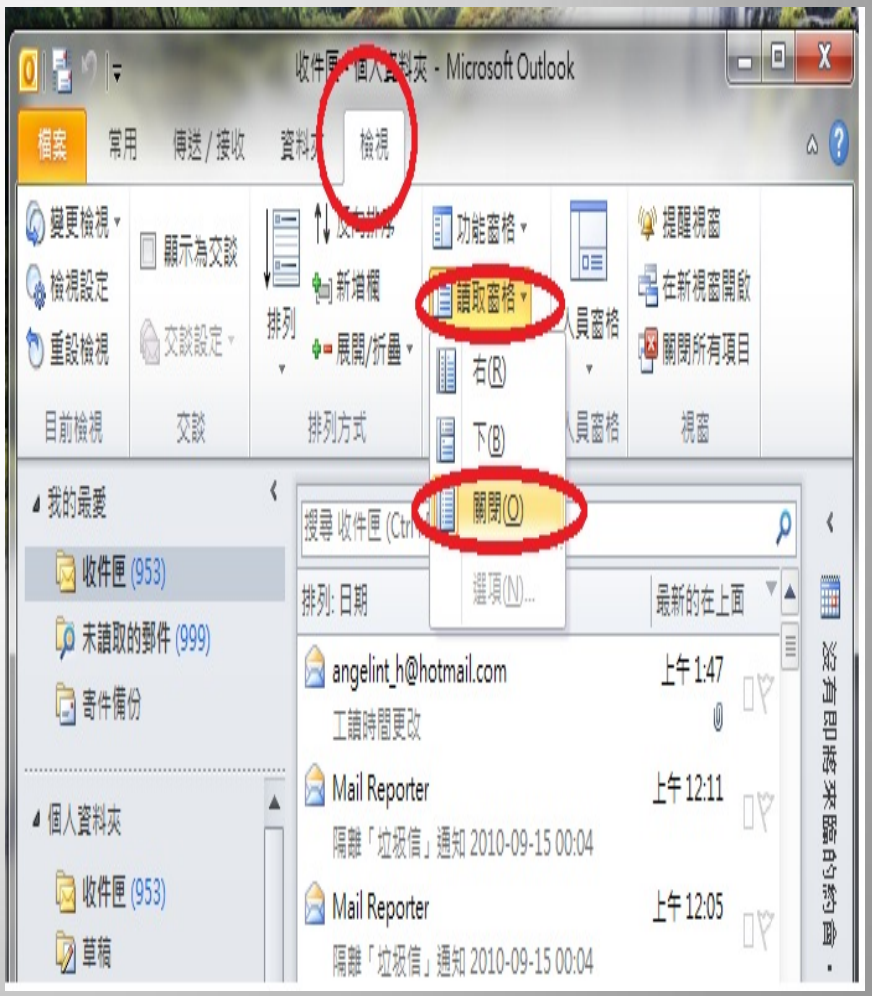
live mail

- 開啟 live mail
- 選取【工具】
- 選取【安全性選項】
- 選取【安全性】
- 將【阻擋HTML電子郵件中的圖片和其他外部內容】打勾



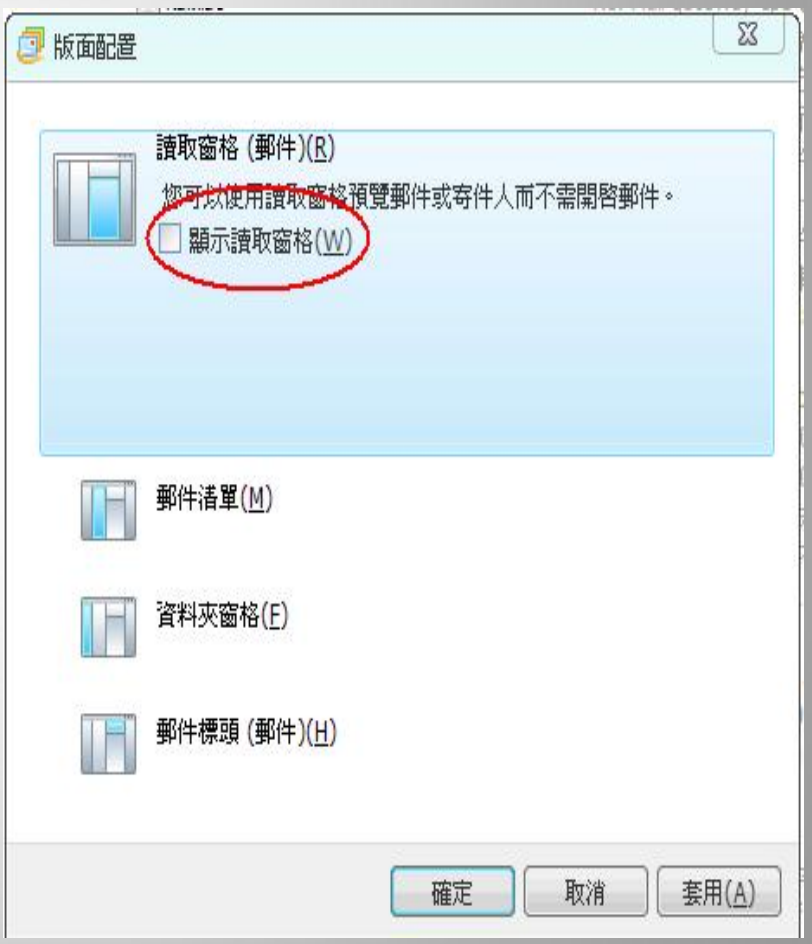
outlook 2010

- 開啟outlook 2010
- 選取【檢視】
- 選取【讀取窗格】
- 選擇【關閉】



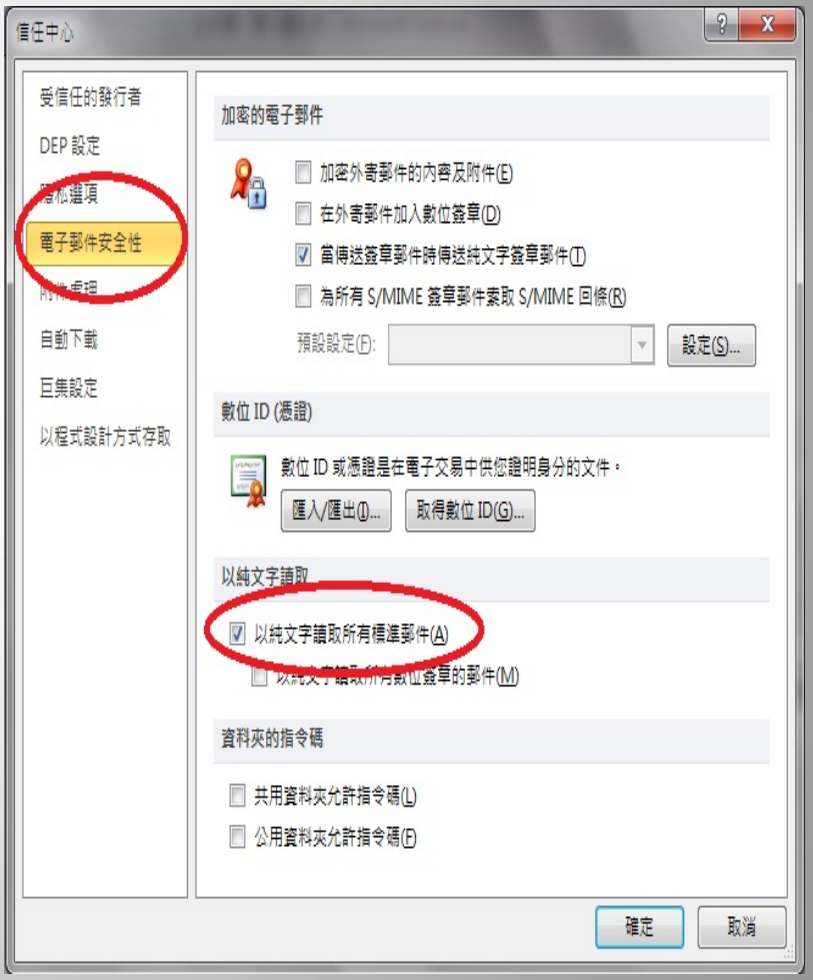
live mail

- 開啟 live mail
- 選取【檢視】
- 選取【版面配置】
- 【顯示預覽窗格】不打勾



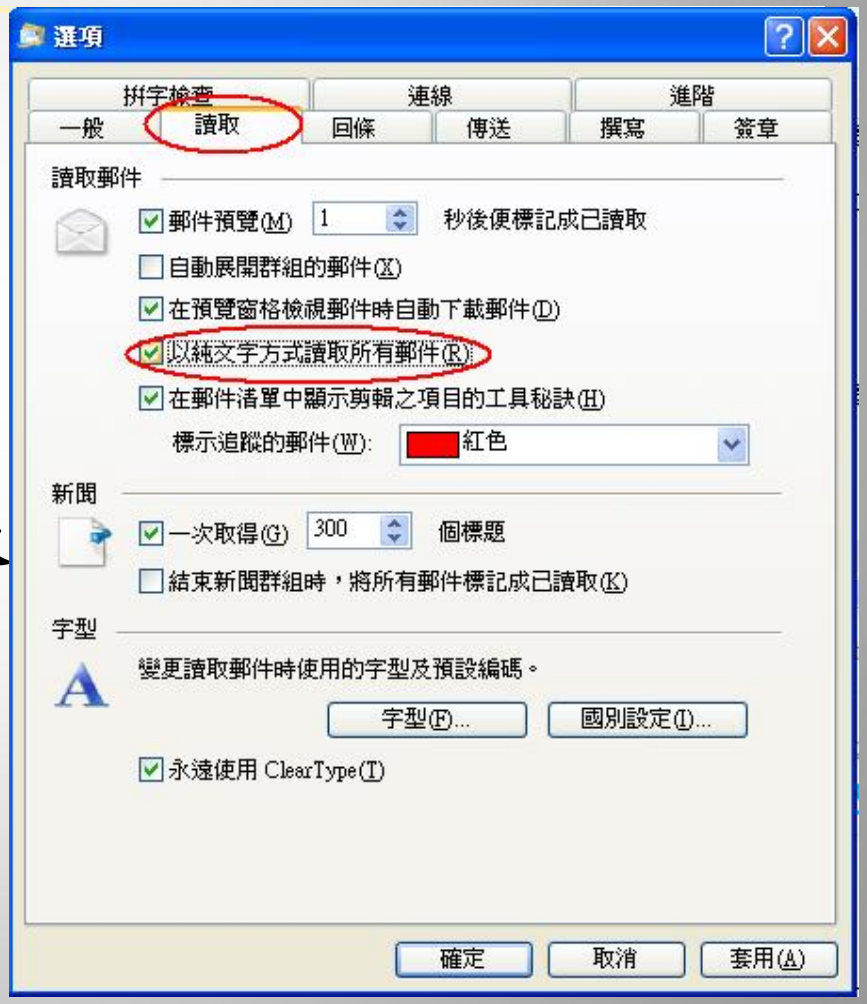
Outlook 2010

- 開啟outlook 2010
- 選取【檔案】
- 選取【選項】
- 選擇【信任中心】
- 點選【信任中心設定】
- 選擇【電子郵件安全性】
- 將【以純文字讀取所有標準郵件】打勾



live mail

- 開啟 live mail
- 選取【工具】
- 選取【選項】
- 選取【讀取】
- 將【在純文字中讀取所有郵件】打勾



近乎完美的防護

- 改變使用電子郵件的習慣
  - 查明信件的來源
    - 信件可由mail header查出所經的伺服器
  - 釐清寄件者身分
    - 以電話向寄件者確認
    - 郵件驗證機制
    - 附件加密
    - …

Mail header

Return-Path: <vipmember@infoarray.tw>
X-Original-To: OOO@mx.nthu.edu.tw
Delivered-To: OOO@mx.nthu.edu.tw
Received: from cp1.oz.nthu.edu.tw (cp1.oz.nthu.edu.tw [140.114.63.141])
by cc.nthu.edu.tw (Postfix) with ESMTP id AA6BA56C76
for <ptlin@cc.nthu.edu.tw>; Thu, 2 Jul 2009 13:56:42 +0800 (CST)
parts
Received: from mail.communicatearea.tw [(210.67.251.27)] by
cp6.oz.nthu.edu.tw
(envelope-from <vipmember@infoarray.tw>)
(NTHUCCC AntiSPAM Mail Server with TLS)
with ESMTP id 577192816; Mon, 18 May 2009 06:55:06 +0800
Received: from mailsystem ([192.168.255.100])
by mail.communicatearea.tw (8.13.8/8.13.8) with ESMTP id
n4HMs4w7018426
for <OOO@mx.nthu.edu.tw>; Mon, 18 May 2009 06:54:06 +0800
X-ssage-ID: <7141115.1242600903628.JavaMail.SYSTEM@mailsystem>
Date: Mon, 18 May 2009 06:55:03 +0800 (CST)

結論

- 兩不看
  - 來源不明的信不看
  - 不認識寄件者不看
- 不衝動
  - 對於自己有興趣、有吸引力....等信件

虎三小之童話變奏 社交工程

報告完畢

謝謝