



Taipei Medical University

電子郵件社交工程防範宣導

臺北醫學大學

資訊處 網路組

林恩德

大綱



Taipei Medical University

- 何謂社交工程
 - 社交工程攻擊
 - 人性弱點
- 網路架構與攻擊
- 軟體弱點與零時差攻擊
- 電子郵件社交工程應用案例
- 如何自我防護
- 使用電子郵件時應有的習慣
- 平時使用電腦應有的行為
- 臺灣學術網路防範惡意郵件社交工程演練計畫
- 結論

何謂社交工程



Taipei Medical University

- 社交工程兩個基本要件：
 - 第一個是【人】
 - 第二個是【詐騙手法】
- 凡對【人】甚至於【特定對象】，使用各種【詐騙手法】，獲得不當資訊，來達到施騙者的目的，可稱之為【社交工程】。

社交工程攻擊



Taipei Medical University

- 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。
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而現在社交工程大都是利用電子郵件或網頁來進行攻擊。
- 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 (包含零時差攻擊)

人性弱點



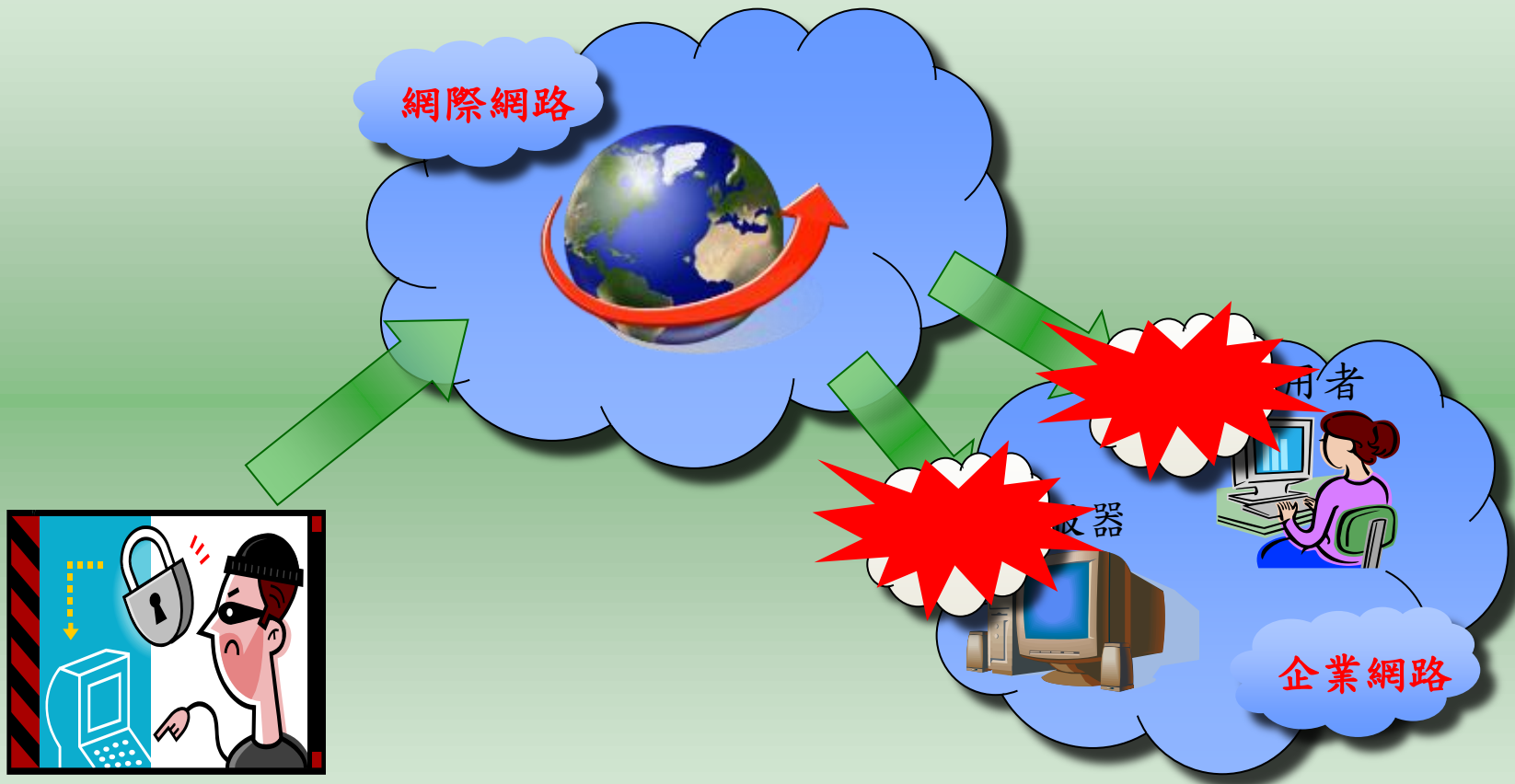
Taipei Medical University

- 駭客利用漏洞百出的【人性】，來設計各式各樣的【詐騙手法】。
 - 貪心：撿便宜的個性
 - 情色：食色性也多多益善
 - 好奇：探索八卦訊息的個性
 - 驚恐：威脅恐嚇讓人慌亂
 - 信任：輕易的相信不求實證
 - 不在意：沒那麼倒楣吧的想法
 - 警覺力：無所謂後果的嚴重性

舊式網路架構與攻擊1

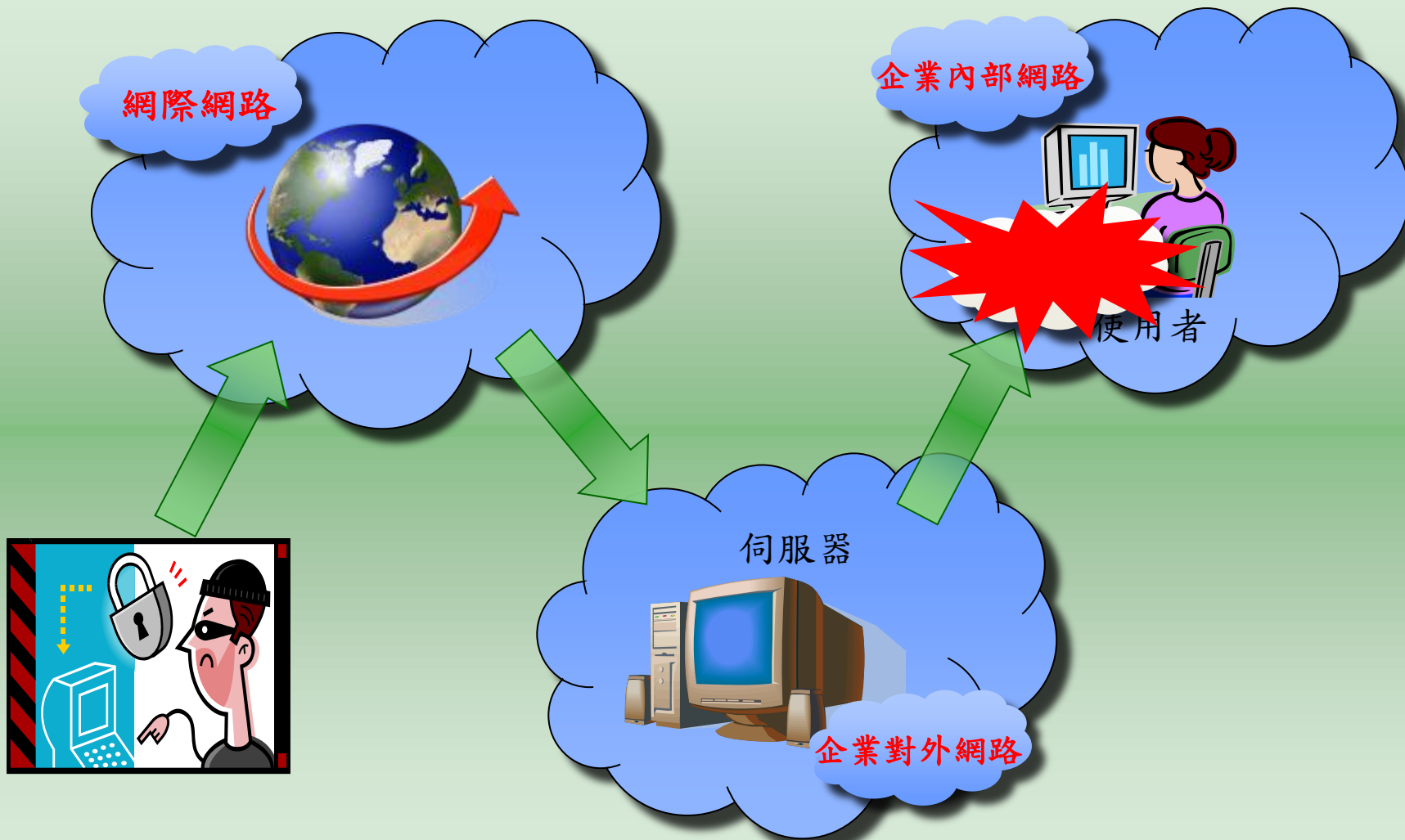


Taipei Medical University



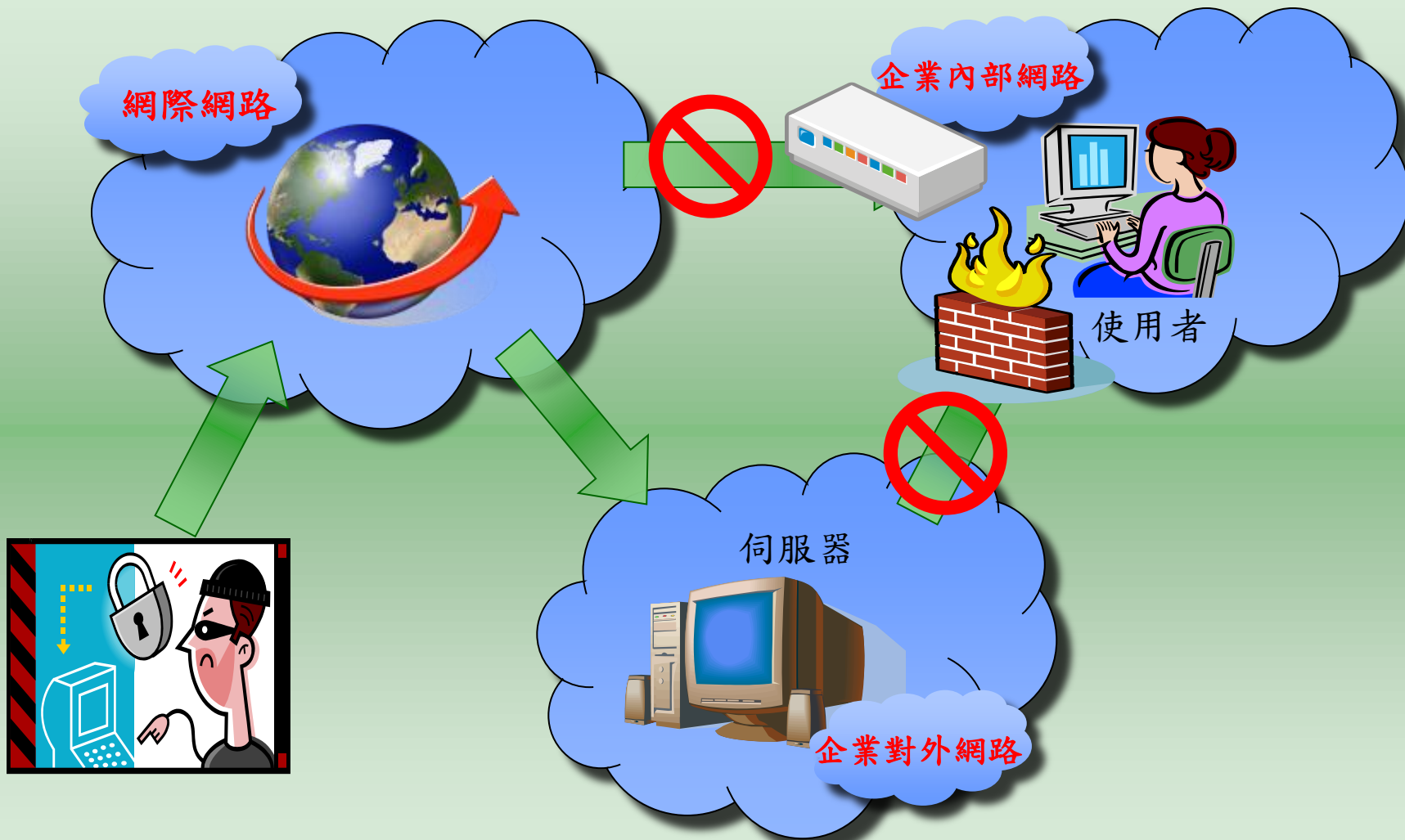
舊式網路架構與攻擊2

Taipei Medical University



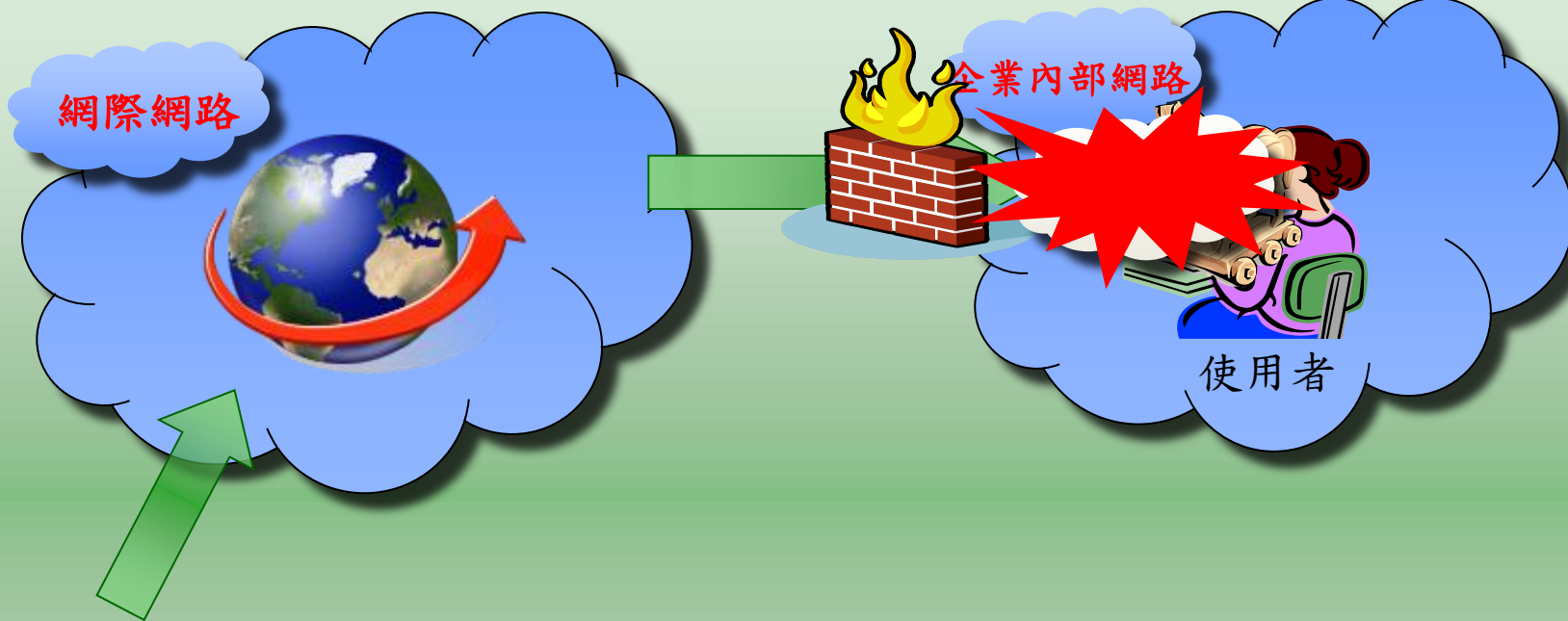
現在的網際網路架構

Taipei Medical University



現在的網際網路架構

Taipei Medical University



社交工程攻擊模式

Taipei Medical University



1. 駭客設計攻擊陷阱程式(如特殊Word檔案或外部惡意連結)
2. 將攻擊程式置入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，將被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

常見的社交工程攻擊



Taipei Medical University

- 電子郵件隱藏電腦病毒 (附加檔案)
- 網路釣魚
- 圖片中的惡意程式
- 偽裝修補程式
- 即時通也是社交工程的新途徑

軟體弱點與零時差攻擊

Taipei Medical University

- 只要是軟體即有可能存在弱點，若未能及時修補弱點，即可能讓駭客入侵成功
- 軟體弱點在沒有任何修補方式之前，出現相對應的攻擊行為時，此類攻擊稱為「**零時差攻擊 (Zero-day Attack)**」

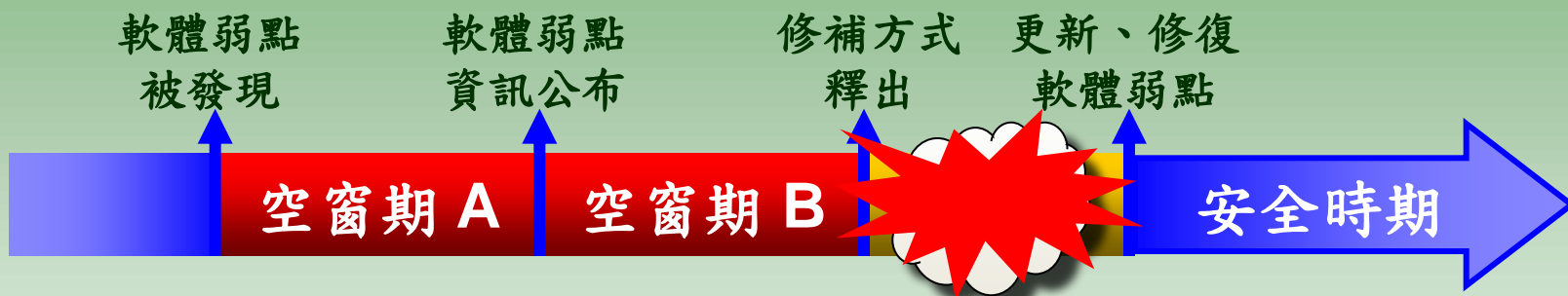


軟體弱點與零時差攻擊



Taipei Medical University

- 只要是軟體即有可能存在弱點，若未能及時修補弱點，即可能讓駭客入侵成功
- 軟體弱點在沒有任何修補方式之前，出現相對應的攻擊行為時，此類攻擊稱為「**零時差攻擊 (Zero-day Attack)**」



電子郵件社交工程應用案例

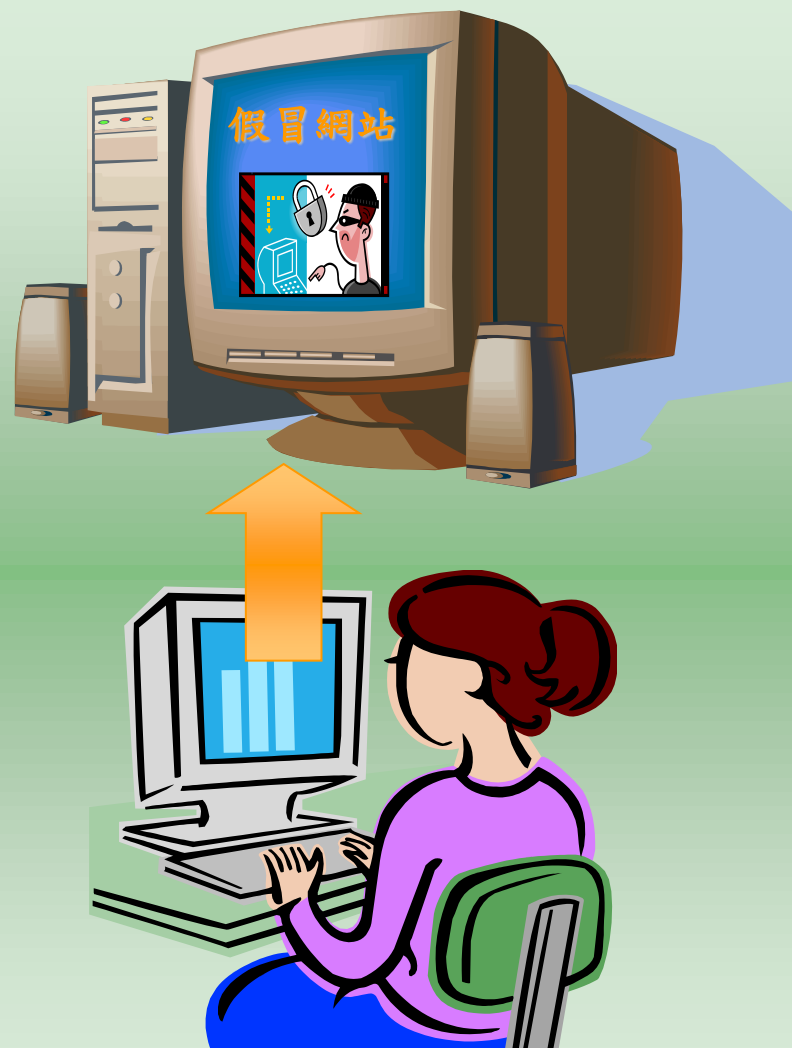


Taipei Medical University

- 網路釣魚 (Phishing)
- 垃圾郵件 (SPAM Mail)

駭客架設與官方公司幾乎一模一樣的網站，再透過電子郵件騙取使用者連線進入假冒網站，進而取得帳號與密碼。

網路釣魚 (Phishing) 是個特殊的英文專有名詞，結合“Phone”和“Fishing”兩個字。



你看得出兩個網站的差異嗎？



Taipei Medical University

The image displays six screenshots of the Land Bank website (www.landbank.com.tw) in Internet Explorer, arranged in a 3x2 grid. The top row shows the full website with a green header and a navigation menu. The middle row shows a version with a simplified navigation menu. The bottom row shows a version with a blue header and a simplified navigation menu. The differences between the two columns are as follows:

- Top Row:** The left screenshot shows a navigation menu with 8 items: 關於土銀, 土銀業務, 最新動態, 金融資訊, 理財資訊, 基金理財, 土銀券筒, and 立刻. The right screenshot shows a navigation menu with 7 items: 關於土銀, 土銀業務, 最新動態, 金融資訊, 理財資訊, 基金理財, and 土銀券筒. The '立刻' item is missing.
- Middle Row:** The left screenshot shows a navigation menu with 5 items: 關於土銀, 土銀業務, 最新動態, 金融資訊, and 理財資訊. The right screenshot shows a navigation menu with 5 items: 關於土銀, 土銀業務, 最新動態, 金融資訊, and 理財資訊. The items are identical.
- Bottom Row:** The left screenshot shows a navigation menu with 5 items: 關於土銀, 土銀業務, 最新動態, 金融資訊, and 理財資訊. The right screenshot shows a navigation menu with 5 items: 關於土銀, 土銀業務, 最新動態, 金融資訊, and 理財資訊. The items are identical.

你看得出兩個網站的差異嗎？



Taipei Medical University

中華航空公司 China Airlines - Windows Internet Explorer
http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines

CHINA AIRLINES 華夏里程酬賓 華航精緻旅遊 旅客服務

RSS說明 常見問答 聯絡

班機離到動態 >>

華夏會員專區

會員卡號

[加入會員](#) [密碼查詢](#)
[卡號查詢](#) [申請密碼](#)

// 透過航班時間表，旅程安

啓程地區 啓程地點

網上訂票 | 班表查詢

亞洲 TPE-台北

中華航空公司 China Airlines - Windows Internet Explorer
http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines

CHINA AIRLINES 華夏里程酬賓 華航精緻旅遊 旅客服務

RSS說明 常見問答 聯絡

班機離到動態 >>

華夏會員專區

會員卡號

[加入會員](#) [密碼查詢](#)
[卡號查詢](#) [申請密碼](#)

// 透過航班時間表，旅程安

啓程地區 啓程地點

網上訂票 | 班表查詢

亞洲 TPE-台北

中華航空公司 China Airlines - Windows Internet Explorer
http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines

中華航空公司 China Airlines - Windows Internet Explorer
http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines

網路釣魚信件內容



Taipei Medical University

Dear Registered Users / Subscribers,

This message is from <https://webmail.tmu.edu.tw/horde/imp/login.php> messaging center to all registered account owners. On Saturday, 14th March, 2009.

We are informing you that from 12:00am until 12:00 PM, all Mailhub systems will undergo regularly scheduled maintenance. Access to your e-mail via the mail client will be unavailable for some time during this maintenance window.

We are currently upgrading our data base with regards to e-mail account center see homepage for details. And we are deleting some webmail account to create more space for new accounts.

To complete your cox.net Webmail account, you must reply the account update department by completing the space provided below with your user name and password in the format stated:

User name (***) password (*****)**

Failure to do this will immediately render your account deactivated from our database. You can also confirm your email account by logging into your account at <https://webmail.tmu.edu.tw/horde/imp/login.php>

Do click on reply, so that your reconfigured webmail POP3 Server, SMTP Server, NNTP Server will be received directly with your email.

Thank you for using webmail.tmu.edu.tw

THE webmail.tmu.edu.tw TEAM"

帳號被盜用寄垃圾信的紀錄



Taipei Medical University

Feb 02 17:48:38 HORDE [info] [imp] **124.126.252.87**

Message sent to kalanidavis@yahoo.com,
kalanidhi48@yahoo.com, kalanike@yahoo.com,
kalanni123@yahoo.com, kalanzar@yahoo.com,
kalarocky@yahoo.com, kalarosing@yahoo.com,
kalasf@yahoo.com, kalaskark@yahoo.com,
kalasmom@yahoo.com, kalatex@yahoo.com,
kalatsky11@yahoo.com, kalavathib2000@yahoo.com,
kalawia88@yahoo.com, kalayasha@yahoo.com,
alayavaraju@yahoo.com, kalba00@yahoo.com,
kalbaz_2000@yahoo.com, kalbul@yahoo.com,
kalcrfwolf@yahoo.com, kalder14@yahoo.com,
kale20042001@yahoo.com, kaleabt@yahoo.com,
kaleamon@yahoo.com, kaleastar@yahoo.com,
kaleb_barnum1972@yahoo.com, kaledac@yahoo.com,
kalee1943m@yahoo.com, kaleefwali@yahoo.com,
kaleegirl45@yahoo.com, kaleem50@yahoo.com,
kaleem_777@yahoo.com, kaleem_male@yahoo.com,
kaleemsatti@yahoo.com, kalegana11@yahoo.com,
kalei1337@yahoo.com, kalei22202@yahoo.com,
kalei_127@yahoo.com, kalei_47@yahoo.com,
kalei_9@yahoo.com, kalei_akauz1@yahoo.com,
kalei_day@yahoo.com, kalei_girl08@yahoo.com,
kaleidascope777@yahoo.com, kaleighgriffin@yahoo.com,
kaleighsmomlori@yahoo.com, kaleigirl777@yahoo.com,

kaleihokuokalani@yahoo.com, kaleina444@yahoo.com,
kaleinani1015@yahoo.com, kalejand@yahoo.com,
kalekn@yahoo.com, kale102002@yahoo.com,
kalel2681@yahoo.com, kalelbillyholiday@yahoo.com,
kalemanis2003@yahoo.com, kalemunil@yahoo.com,

inetnum: [124.126.0.0 - 124.127.255.255](#)

netname: RITELE

descr: Research Institution of Telecom

descr: No.1 Gaojiayuan,Xicheng District,Beijing,China

country: CN

admin-c: YZ1264-AP

tech-c: YZ1264-AP

mnt-by: MAINT-CNNIC-AP

mnt-lower: MAINT-CNNIC-AP

mnt-routes: MAINT-CNNIC-AP

status: ALLOCATED PORTABLE

changed: [hm-changed@apnic.net](#) 20070228

source: APNIC

com,
yahoo.com,
yahoo.com,
m,
com,
com,
yahoo.com,
83@yahoo.com,
yahoo.com,
no.com,
om,
oo.com,
om,
om,
o.com,
o.com,
com,
m,
com,
com,
kalibambam@yahoo.com, kaliba72200@yahoo.com,
kalibchbum80@yahoo.com, kalibill@yahoo.com,
kalibugan11@yahoo.com, kalicarr42@yahoo.com,
kalichism@yahoo.com, kalicialewis@yahoo.com,
kalicoangel1@yahoo.com, kalicokat_13@yahoo.com,
kalicokim@yahoo.com, kalicokitt@yahoo.com from XXXXX
[on line 1068 of "/var/www/horde/imp/compose.php"]

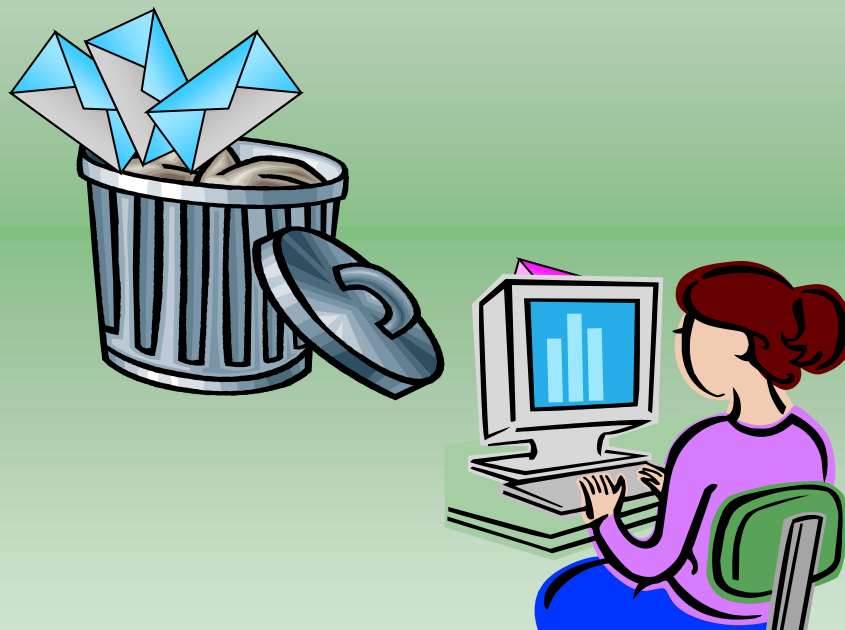
電子郵件社交工程應用案例



Taipei Medical University

- 網路釣魚 (Phishing)
- 垃圾郵件 (SPAM Mail)

垃圾郵件是未經收信人許可，將內容相同的電子郵件廣告寄發給許多人，收信人必須花費金錢與時間去收這些垃圾郵件。



臺灣成垃圾郵件大國



Taipei Medical University

- 臺灣被列為全球第**9**大發出垃圾郵件的國家
- 2008年台灣網際網路協會調查顯示，臺灣網友受訪者中**83.9%**，每天收到**10~50**封垃圾信件，這調查顯示網友的痛苦指數高達**63.98分**
- 每個網路用戶平均每天收到**29**封垃圾郵件，刪除垃圾郵件所耗費的時間以基本薪資每小時**95**元計算，每年單是用戶端的經濟耗損達**新臺幣464億元**以上
- 根據HiNet統計，HiNet每天收到約**1億5000萬**封電子郵件，平均有**9000萬**封是垃圾郵件，每天必須阻擋不當連線達**1200萬**次

「濫發商業電子郵件管理條例」



Taipei Medical University

- 2008年11月由NCC通過內部委員會議向行政院提出
- 相較於2005年提出的版本，除加入保護措施，可對ISP、電子郵件服務商祭出處罰外，收到垃圾郵件的民眾也可透過財團法人向濫發者求償，每封可**求償500至2000元**

社交工程案例—偽冒身份惡意電郵



Taipei Medical University

- 2006/4/10 報載駭客使用某立委辦公室名義，寄發軍事新聞題材之惡意電郵給記者
- 由於內容與寄件者的專業屬性吻合，造成多位記者受騙開啟信件而遭植入後門程式

www.appledaily.com.tw ■ 頭條要聞 ■ 兩岸國際 ■ 財經 ■ 娛樂 ■ 體育 ■ 副刊

日蘋果
APPLE DAILY

聰明玩家情報站

記者收毒郵 疑中駭客搞鬼

2006年04月
刊印半頁 10日

【黃敬平／台北報導】中國駭客再度傳出利用網路植入有病毒的木馬程式對台灣進行攻擊，但這回受害的不是軍方，而是立委與媒體記者。國民黨立委林郁方國會辦公室信箱上月底以「中共對台用兵，國防部之最新評估」發出一封電郵，不少接獲電郵的記者因此中毒，引起國安單位高度關切，國安局官員說，這次中毒者的檔案資料遭慢速分批送出，不易察覺，是新的駭客攻擊嘗試。

林郁方否認發電郵
這封電郵發自三月三十一日晚上十時，寄件人顯示為ly10717b@ly.gov.tw，而非林郁方辦公室平常顯示的「林郁方國會辦公室」，但因電郵主旨是國防軍事的中共動態，不少採訪立法院、軍事或總統府等路線的記者以為是新聞稿，一時不察，打開附檔後紛紛中毒。林郁方辦公室助理揭仲否認當晚曾發出此封電郵，他說，當時辦公室沒有人，他也沒用這個地址在其他電腦發出任何電郵。揭仲將將此事報告林郁方，並把電腦送到立院資訊中心檢查，工程師說電腦無異狀，也無發出該信的跡象。但可能代表立院的資訊保護系統遭破解，若有該電郵原始檔案，即能循線追溯來源。

國安局官員分析，這次發自立委信箱的有毒電郵「針對性」發給各媒體記者，且中毒者資料遭慢速分批送出，不易察覺，真是一種新的嘗試，頗類似去年攻擊國軍衡山指揮所的手法。

APPLE DAILY

中央氣象局遭冒名發送垃圾郵件



Taipei Medical University

- 主旨為「中央氣象局緊急通知-強風特報」，若一不留心點開，電腦可能受到病毒感染
- 中央氣象局資訊中心副主任程家平表示，對收信者來說是一種社交攻擊，這批冒用電子郵件內藏PDF病毒，利用Adobe9.0.0系列產品的安全漏洞來進行攻擊，若不慎開啟可能造成**當機**或**遭植入惡意程式**，被感染的電腦除了可能會**洩漏個資**，也可能被駭客當作**惡意攻擊的跳板**

(資料來源：資安人科技網 吳依恂 - 03/23/2009)

http://www.isecutech.com.tw/article/article_detail.aspx?aid=4891)

社交工程案例—數位簽章(偽冒)



Taipei Medical University

[資安訊息通告] 國家資通安全會報技術服務中心 (事件編號: ICST-ANA-2007-0007) - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) PGP 工具(T) 執行(A) 說明(H)

回覆(R) 全部回覆(L) 轉寄(W) [Icons]

寄件者: 國家資通安全會報技術服務中心 [ncert@icst.org.tw]

寄件日期: 2007/9/26 (星期三) 下午 05:46

收件者: 國家資通安全會報技術服務中心

副本:

主旨: [資安訊息通告] 國家資通安全會報技術服務中心 (事件編號: ICST-ANA-2007-0007)

簽名者: ncert@icst.org.tw



國家資通安全會報 技術服務中心 漏洞/資安訊息通告

發布編號	ICST-ANA-2007-0007	發布日期	2007/09/26
事件類型	公告資訊	發現時間	2007/09/26
通告名稱	技術服務中心成立10月國家慶典重點時刻警戒專案		
內容說明	您好： 國家資通安全會報技術服務中心將於9/30零時起至10/11二十四時止成立「10月國家慶典重點時刻警戒專案」，進行全天候24小時資安事件即時監控及提供必要性之技術支援服務，以確保10月國家慶典重點時刻期間各政府機關(構)網路安全。 備註：警訊編號ICST-ANA-2007-0006為系統錯誤，導致發送不正確資		

如何自我防護



Taipei Medical University

- 技術層面
 - 修補系統漏洞
 - 安裝防毒軟體
 - 安裝間諜程式檢查軟體
 - 關閉信件預覽
- 行為層面
 - 開啟信件前請三思
 - 開啟連結時請三思
 - 開啟附件檔案時請三思

修補系統漏洞



Taipei Medical University



修補系統漏洞

Taipei Medical University

The screenshot shows the Microsoft Windows Update website in Chinese. The browser window title is "Microsoft Windows Update - Microsoft Internet Explorer". The address bar shows the URL: <http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=zh-tw>. The page features the Windows logo and "Windows Update" heading. A navigation bar includes links for "Windows 系列", "Windows Marketplace", "Office 系列", and "Microsoft Update".

The main content area is titled "歡迎使用 Windows Update" (Welcome to Windows Update). Below this, it says "讓您的電腦保持在最新狀態" (Keep your computer up to date) and "檢查您的 Windows、硬體或裝置是否需要更新。" (Check if your Windows, hardware, or devices need updates). There are two buttons: "快速" (Quick) and "自訂" (Custom). The "快速" button is highlighted with a red box and is accompanied by the text "取得高優先順序的更新 (建議使用)" (Get high-priority updates (recommended)). The "自訂" button is accompanied by the text "從適用於 Windows 與其他程式的選用與高優先順序的更新中選取" (Select updates that are applicable to Windows and other programs and high-priority updates).

On the right side, there are two informational boxes. The top one is titled "[自動更新]: 已啟動" (Automatic updates: On) and states "已經將您的電腦設為自動接收安全性與重大更新。" (Your computer is set to automatically receive security and important updates.) and "挑選要安裝更新的時間。" (Choose when to install updates.). The bottom one is titled "新聞" (News) and contains the headline "升級到 Microsoft Update - 自動接收 Windows、Office 等產品的更新" (Upgrade to Microsoft Update - automatically receive updates for Windows, Office, etc.).

At the bottom of the page, there is a footer with the text "©2007 Microsoft Corporation. 著作權所有, 並保留一切權利。 使用規定 | 隱私權聲明" and the Microsoft logo.

安裝防毒軟體



Taipei Medical University

免費防毒軟體

軟體名稱：**Avira AntiVir Personal Free Antivirus**

軟體語言：繁體中文

官方網站：<http://www.free-av.com/>



軟體名稱：**avast! antivirus**

軟體語言：繁體中文（內建27國語言）

官方網站：<http://www.avast.com/>



軟體名稱：**AVG 中文版免費防毒軟體**

軟體語言：繁體中文（內建多國語系）

官方網站：<http://www.avgtaiwan.com/>



軟體名稱：**PC Tools AntiVirus Free Edition**

軟體語言：繁體中文（內建多國語系）

官方網站：<http://www.pctools.com/zh/free-antivirus/>



軟體名稱：**ClamWin Free Antivirus**

軟體語言：英文版

官方網站：<http://www.clamwin.com/>

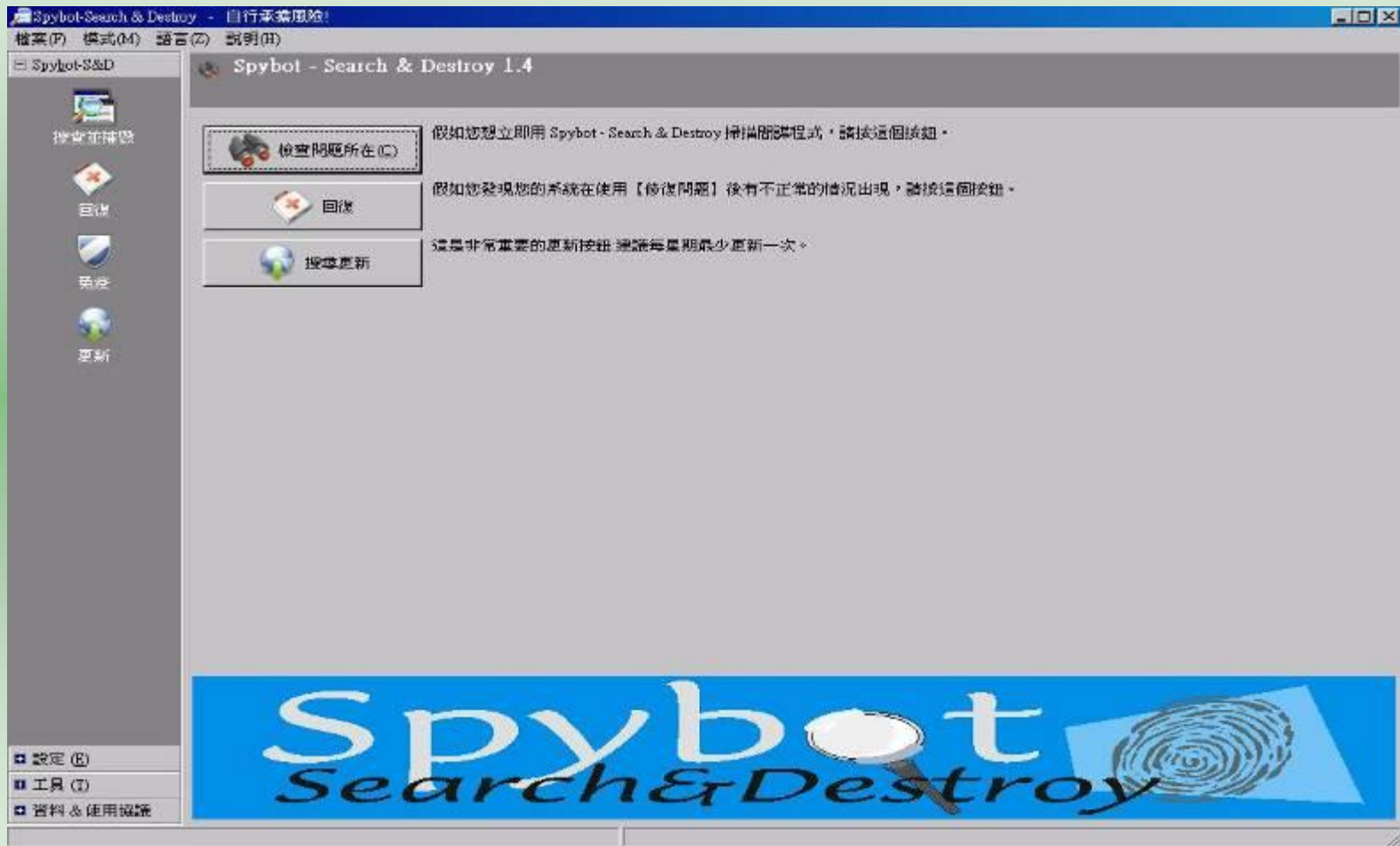


安裝間諜程式檢查軟體



Taipei Medical University

- *SpyBot Search & Destroy*



安裝間諜程式檢查軟體

Taipei Medical University

- *Advanced SystemCare*

The screenshot displays the Advanced SystemCare software interface. At the top, it reads "Advanced SystemCare FREE Ver 3.8.0". The main menu includes "首頁", "維護!", "系統診斷", and "應用程式". A "升級" button is visible in the bottom left. The right-hand panel, titled "維護系統", provides a detailed description of the software's functions and a list of active tasks:

- 維護系統**
維護和清理您的電腦。包括的內容：間諜軟件清除，註冊表修復，隱私清除，垃圾文件清理。
- 功能** | **設置**
- 間諜軟件清除** 正在掃描...
掃描並清除間諜軟件，廣告軟件。
- 註冊表修復**
清理註冊表，最佳化電腦性能。
- 隱私清除**
清除隱私信息和上網痕跡。
- 垃圾文件清理**
清理垃圾文件，釋放硬碟空間。

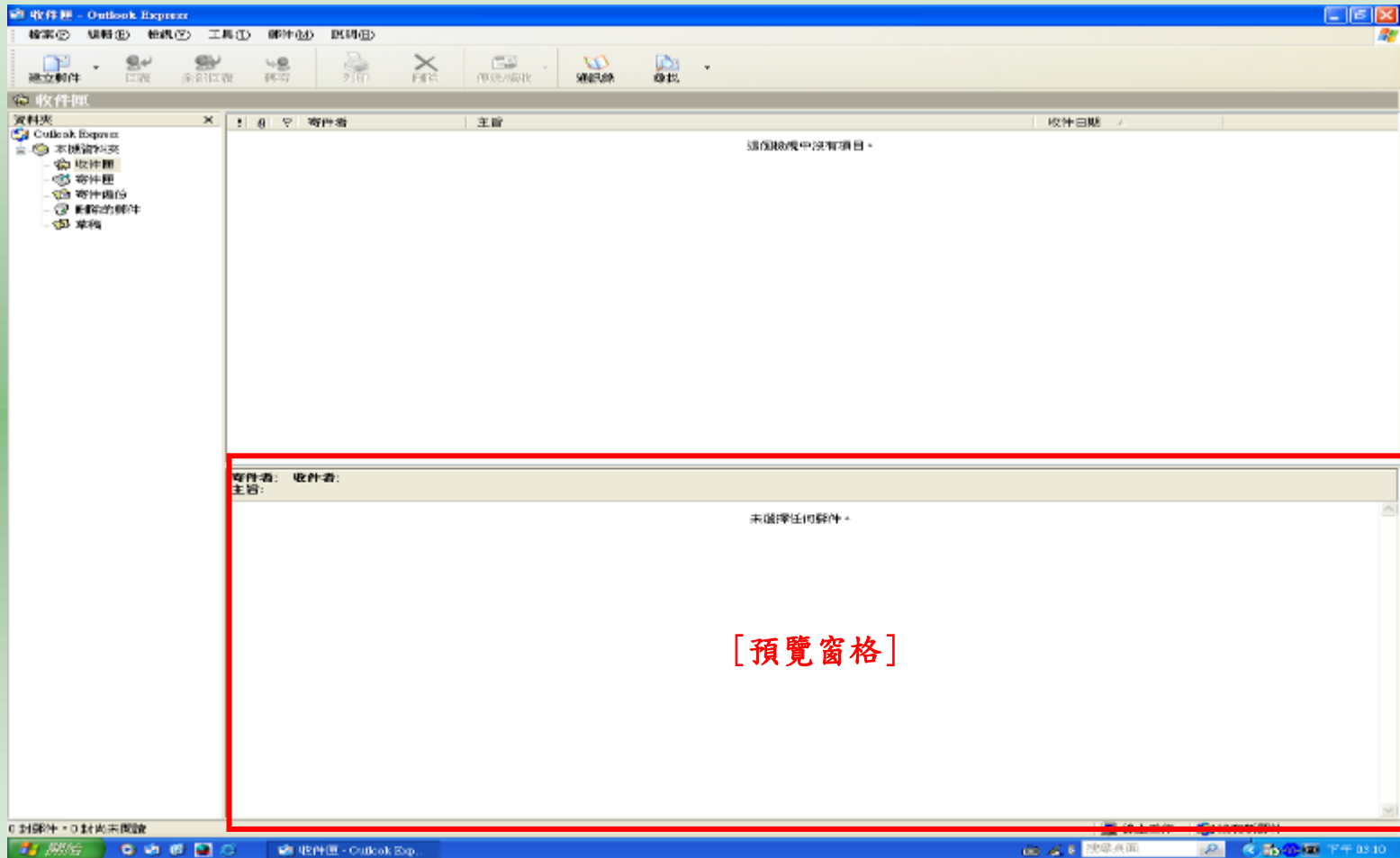
A progress bar is shown below the list, and a status indicator reads "正在掃描: DriveCleaner". At the bottom of the panel are "停止" and "關閉" buttons. The footer contains "推薦給朋友" and "檢查更新" links.

關閉信件預覽



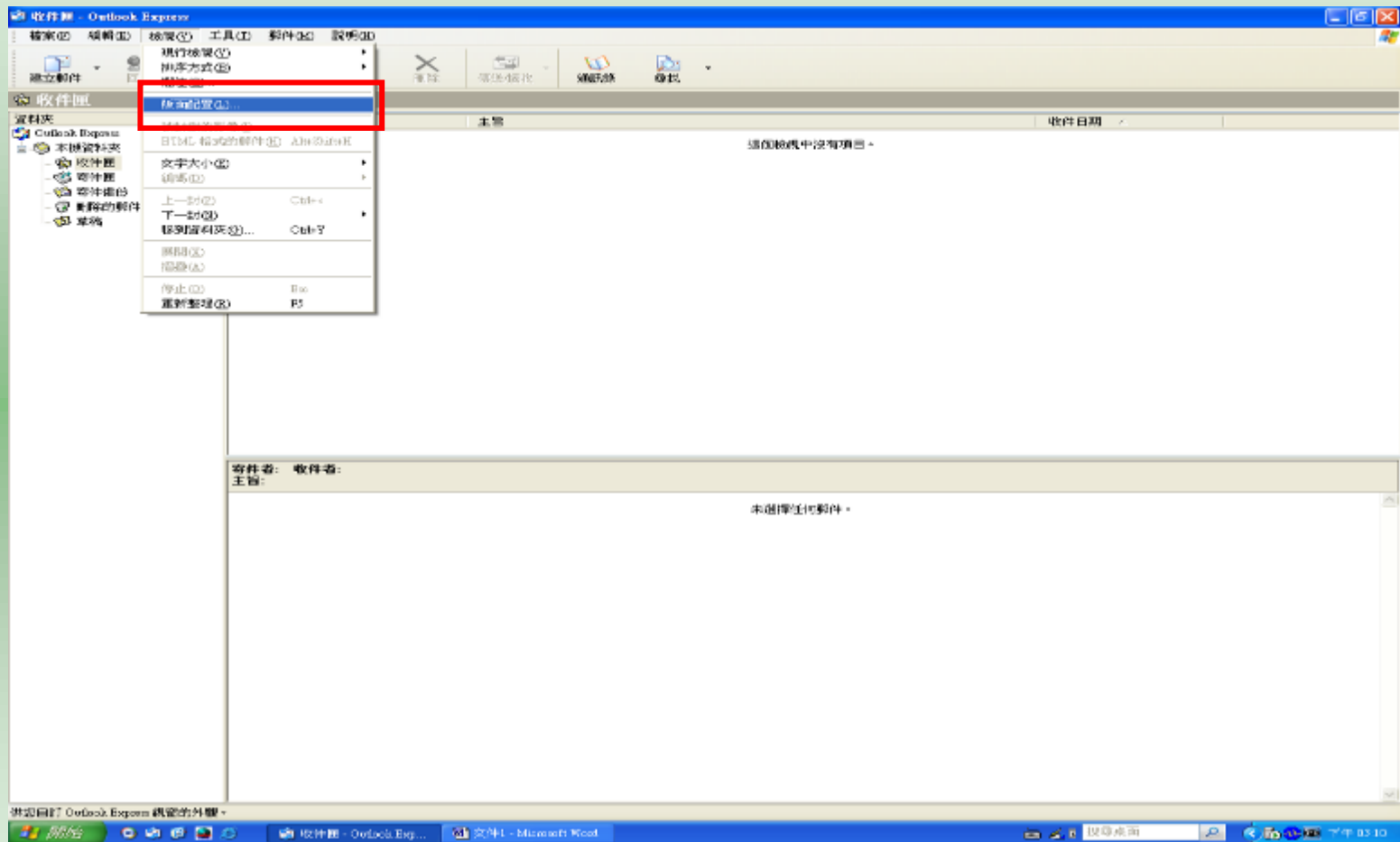
Taipei Medical University

- 請將Outlook Express的預覽窗格關閉



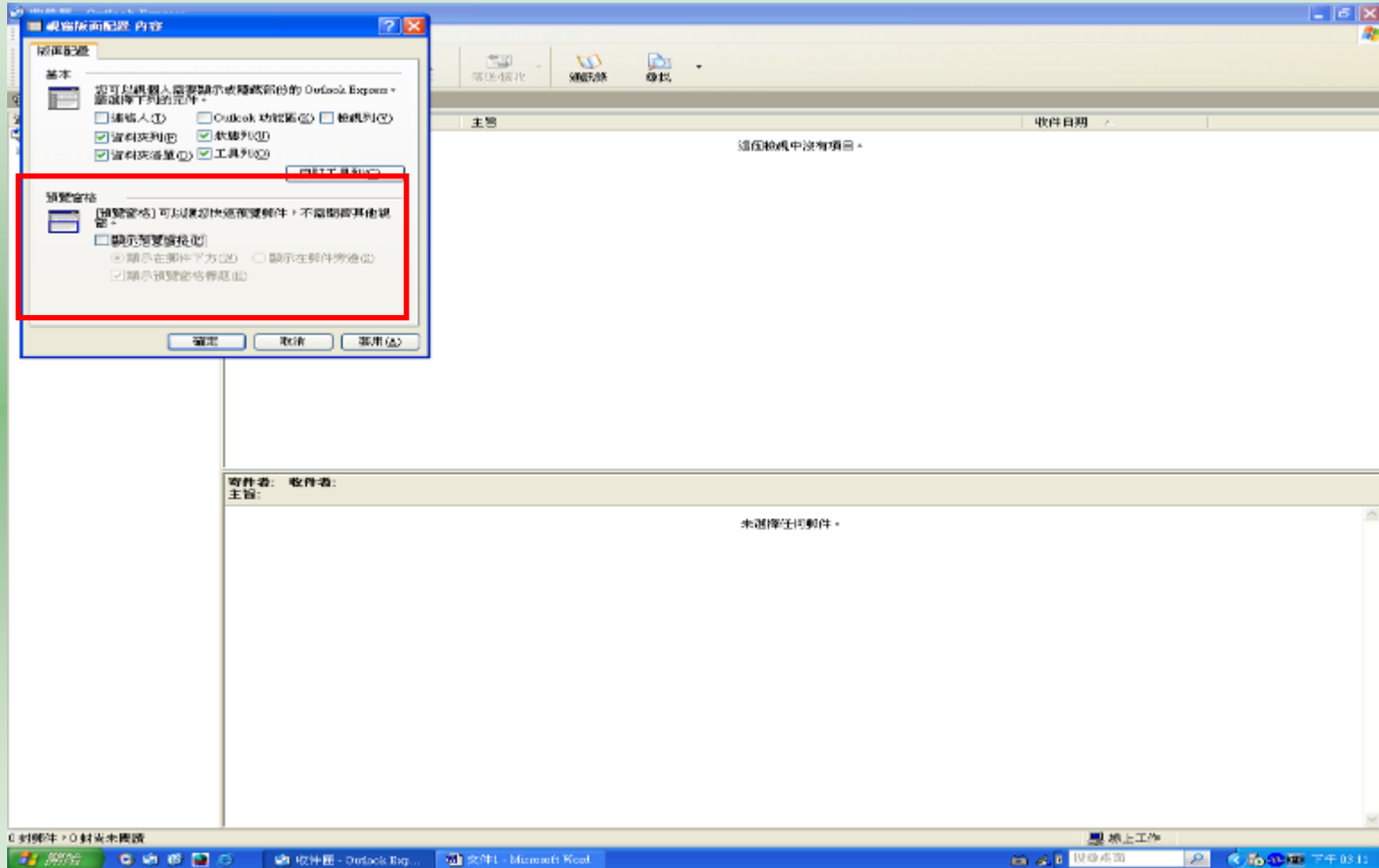
關閉信件預覽

- 檢視 → 「版面配置」



關閉信件預覽

- 視窗版面配置 內容 → **不顯示** 「預覽窗格」



使用電子郵件時應有的習慣



Taipei Medical University

- 收信
 - 檢查**寄件者的真偽**
 - 確認信件**內容的真實度**
 - 不輕易開啟郵件中的**超連結**以及**附件**
 - 開啟超連結或檔案前，確認對應軟體（例如：IE、Office、壓縮軟體）都保持在**最新的修補狀態**
- 轉信或寄信
 - **未經查證之訊息**，不要轉寄
 - 轉寄郵件前先**將他人郵件地址刪除**，避免別人郵件地址傳出
 - 寄送信件給**群體收件者**時，應將收件者列在**密件副件**，以免收件人資訊外洩。

平時使用電腦應有的行為



Taipei Medical University

- 啟用防火牆
- 對重要資料進行**加密、備份** (先加密再備份)
- 保持在**最低**的使用權限
- 提高警覺，加強**危機意識**

- 教育部全民資安素養網
<https://isafe.moe.edu.tw/>
- 行政院國家資通安全會報技術服務中心
<http://www.icst.org.tw/>

教育部102年度 臺灣學術網路 防範惡意電子郵件社交工程演練



Taipei Medical University

• 目的

為提高教育體系各學校人員**警覺性**以**降低社交工程攻擊風險**，特訂定本計畫，舉辦相關資安教育訓練與宣導、規劃辦理演練服務作業，以強化人員**資安意識**並檢驗機關宣導社交工程防制成效。

• 對象

- 依98/06/01資安發字第0980100328號函「政府機關(構)資訊安全責任等級分級作業施行計畫」辦理。
- 資安等級A級單位 - 教育部、臺灣大學醫學院附設院、成功大學醫學院附設醫院。
- 資安等級B級單位 - 臺灣學術網路(TANet)區網中心及縣(市)教育網路中心、**各公私立大學**。

教育部102年度 臺灣學術網路 防範惡意電子郵件社交工程演練



Taipei Medical University

- 演練說明

- 演練方式

- 區分為納入教育部集中辦理演練或各單位自行辦理演練，各單位擇一種方式辦理演練。
 - 自行辦理演練者，亦請參照教育部演練時程自行規劃辦理，將演練計畫函送教育部備查。演練結束後，將演練結果於102/10月前再函送教育部彙整辦理評量。

教育部102年度 臺灣學術網路 防範惡意電子郵件社交工程演練



Taipei Medical University

• 演練說明

— 教育訓練

- 依98/06/01資安發字第0980100328號函「政府機關(構)資訊安全責任等級分級作業施行計畫」辦理，各機關應按其資安等級，每年定期舉辦資安教育訓練。
- 資安教育訓練應納入社交工程防制有關之認知宣導，並著重攻擊實例說明，各機關學校人員每年至少需接受1小時社交工程防制宣導講習。
- 宣導課程應分兩階段辦理：
 - 第一階段(於演練作業辦理前)：各機關學校應針對單位所有行政人員，**全面性實施**教育訓練。
 - 第二階段(於演練作業完成後)：針對開啟惡意郵件比例較高、點閱惡意郵件所附連結或檔案之人員再次進行教育訓練加強宣導，以強化其警覺性。

教育部102年度 臺灣學術網路 防範惡意電子郵件社交工程演練



Taipei Medical University

• 演練作業

— 演練時程

- 提報演練名單：如採納入教育部集中辦理者，請於6/28前提報至少**1/2**行政人員。
- 各機關學校自行辦理宣導教育訓練：**7月(全部行政人員)**。
- 教育部進行第**1**次集中演練：**7月**。
- 納入教育部演練單位針對開啟惡意郵件或點閱惡意郵件附件內容人員，進行加強宣導：**8~9月**。
- 教育部進行第**2**次集中演練：**9月**。

教育部102年度 臺灣學術網路 防範惡意電子郵件社交工程演練



Taipei Medical University

• 評量標準

- 各單位之惡意郵件開啟率及惡意連結(或檔案)點擊率計算方式如下：
 - 惡意郵件開啟率：
開啟惡意郵件之人數 / 機關提報人數。
 - 惡意連結(或檔案)點擊率：
點閱惡意郵件所附連結或檔案之人數 / 機關提報人數。
- 各單位之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%以下。
- 自行辦理演練者於演練結束後，將演練結果於102/10前函送教育部彙整辦理評量。

教育部102年度 臺灣學術網路 防範惡意電子郵件社交工程演練



Taipei Medical University

• 演練結果

- 預定於12月底前，由教育部資訊及科技教育司彙整演練報告，並選取成績優良單位及待改善單位。
- 演練成績優良單位，將依權責辦理相關人員敘獎事宜。

教育部99年度

防範惡意郵件社交工程演練信件主題

Taipei Medical University



編號	信件類別	信件標題
Letter 1	生活類	您的報稅內容正確嗎？申報綜所稅7大錯誤必罰！
Letter 2	美女類	!!台灣最美獸醫 連桃太郎都驚艷!!
Letter 3	健康類	炎炎夏日 防曬不能少
Letter 4	知識類	地震時如何有效的保護自己
Letter 5	旅遊類	上海世博會 台灣館 天燈造型 驚艷全場
Letter 6	趣味類	我家有小車神～七歲展現停車特技的小女孩!
Letter 7	社會類	美《時代》百大人物 愛心婦陳樹菊入列
Letter 8	時事類	201順向坡位置大分析
Letter 9	科技類	陽明團隊揭秘 基因 Cisd2 讓人長壽！
Letter 10	財經類	史上最難搶「鐵」飯碗 錄取率僅 1.25%

範例一 (趣味類－蛋糕)



Taipei Medical University

主旨:鬼斧神工！你相信這全都是蛋糕嗎??

從:好吃又好看 <David_chen@yahoo.com>

日期: Tue, 31 Aug 2010 16:47:26 +0800

到:mli@ntu.edu.tw

鬼斧神工！你相信這全都是蛋糕嗎??



蛋糕不再只是一層不變的圓形或是方形加上奶油而已了！現在蛋糕不僅是好吃，更要好看 有創意 才能擄獲消費者的心！各式各樣的造型令人越來越難以相信這竟然是蛋糕！如上圖之皇冠造型之蛋糕，是不是真的很像真的皇冠呢？令壽星也有當國王或是女王的感覺！！

另一張圖更是細膩的表現出各種手工藝品的精隨，讓人看了都捨不得把蛋糕切開！

現在更有業者推出個人造型之蛋糕，針對消費者想要的造型，業者獨家幫您製作完全屬於您個人的蛋糕。

([更多蛋糕照片..](#))

範例二 (美容類—雷射)



Taipei Medical University

主旨: 小心! 雷射當保養 護膚不成反毀容!

從: 如何保養肌膚 <saveyourskin@msn.com>

日期: Tue, 31 Aug 2010 16:47:18 +0800

到: mli@ntu.edu.tw

小心! 雷射當保養 護膚不成反毀容!!



「醫生，我的臉被雷射打花了，還有救嗎？」在坊間強力促銷下，愈來愈多人把雷射當成一般的護膚保養，多次密集療程後，反而呈現黑黑白白的不均勻膚色，台大醫院發現，這是過度雷射導致黑色素細胞死亡的「皮膚色素永久缺失」，患者皮膚呈現不可逆的白斑，原本想靠雷射變美的女性，慘遭毀容而悔不當初。

台大醫院皮膚部蔡呈芳醫師發現，這類被多次雷射打壞皮膚求診的患者近來明顯增多。蔡呈芳說，很多人一、兩周就去打雷射「保養」一下，但多次療程後，發現臉上肌膚出現大大小小白色的斑塊，皮膚不均勻脫色，看起來更花更

醜。

中華民國美容醫學醫學會教育長兼發言人宋奉宜表示，今年國際皮膚手術雜誌指出，間隔一周、連續五次、且劑量不高的淨膚雷射，還是會出現點狀脫色斑、反黑等情況。蔡呈芳說，雷射一般建議間隔三至四周做一次，三個月療程結束就應停止，一旦出現不可逆的白斑，醫師也無能為力。

[雷射注意事項](#)

範例三 (健康類—眩暈)



Taipei Medical University

主旨: 眩暈患者苦不堪言 如何面對眩暈?

從: 關心健康 <leowahtfor@yahoo.com.tw>

日期: Tue, 31 Aug 2010 16:47:11 +0800

到: mli@ntu.edu.tw

天旋地轉並非強震 眩暈患者苦不堪言



如何面對眩暈?

最近全球頻傳強震，對於眩暈病人來說，即使沒有發生地震，整個人就會天旋地轉，有如坐在遊樂區中的大怒神、海盜船、旋轉咖啡杯，甚至暈眩到嘔吐、噁心，苦不堪言。

為何會出現眩暈症狀？台北市中山醫院耳鼻喉科主任醫師暨宏仁診所院長李宏信指出，內耳是由蝸牛體及三半規管所組成。後者主管感覺及速度，如果出現問題，就會導致眩暈。蝸牛體負責聽覺，內部淋巴液及神經毛細胞就像是一個接受體，接受外界音波，音波傳至腦內，就會產生聽覺。三半規管則由三個互為垂直的半圓圈管所組成，主掌人體平衡。

三半規管內有淋巴液，就如同瓶子裡面裝水一樣。此外，

三半規管附近密佈平衡神經，兩相作用下，製造出方向及速度等感覺。如果內耳老化、血管不通，導致淋巴液分泌太多，就會造成積水，只要頭部稍微轉動、晃動，就會覺得搖得很厲害。李宏信形容，內耳的三半規管就好像是汽車的方向盤，要是方向盤抓不穩，或是異常，就容易偏向一方，若是三半規管異常，就會導致眩暈，患者走路就會不穩。

基本上，眩暈可以分為兩大類，有人一暈起來，暈到搞不清楚東西南北，天搖地動，暈到嘔吐、噁心。另一種人，眩暈程度沒有這麼厲害，就像在暈船一樣，站不穩、走路晃來晃去。

造成眩暈的病因很多，大體說來，若是病患的生活太過緊張且壓力大，處於長期疲勞的狀況下，很容易造成血管異常收縮，造成局部組織貧血現象，導致神經壞死而萎縮，這也是自律神經過度興奮所引起的功能失調，同時可能會出現心悸、昏厥等症狀。

至於內耳為何會積水？原因在於淋巴液分泌過多，或是排洩發生困難。李宏信分析，如果內耳血管不通，或是過於緊張、焦慮及疲倦，就容易造成血管收縮，影響養分的供應，長期下來，導致內耳蝸牛體、三半規管淋巴水腫，產生耳鳴、眩暈及重聽，一般統稱為梅尼爾氏症。

針對內耳淋巴積水的原因，常是病患半規管的循環不佳，淋巴液分泌過多卻無法排出，導致內耳淋巴液的壓力增加。一般的對症治療，是利用利尿劑來減壓，或施以內耳淋巴囊開鑿引流術，以達到減壓

範例四 (趣味類—冷笑話)



Taipei Medical University

主旨: 上班累了嗎?放鬆一下,輕鬆的冷笑話:)

從: 笑話大全 <chungkang_1311@hotmail.com>

日期: Tue, 31 Aug 2010 16:47:03 +0800

到: mli@ntu.edu.tw

上班累了嗎?放鬆一下,輕鬆的冷笑話:)



1、五元錢被犯罪團伙綁架了,打電話給百元鈔:"餵!你兒子在這裡,不想我們撕票就用自己來換他!"百元鈔想了一下說:"撕吧,撕了你們連5塊錢都沒有了!"

2、一個人在沙漠裡快要餓死了,這時他檢到了神燈。神燈:"我只可以實現你一個願望,快說吧,我趕時間。"人:"我要老婆....."神燈立刻變出一個美女,然後不屑的說:"都快餓死了還貪圖美色!可悲!"說完就消失了。人:".....餅。"

3、蚯蚓一家這天很無聊,小蚯蚓就把自己切成兩段打羽

毛球去了,蚯蚓媽媽覺得這方法不錯,就把自己切成四段打麻將去了,蚯蚓爸爸想了想,就把自己切成了肉末。蚯蚓媽媽哭著說:"你怎麼這麼傻?切這麼碎會死的!"蚯蚓爸爸弱弱地說:".....突然想踢足球"

5、龜兔賽跑...兔子很快跑到前面去了..烏龜看到一隻蝸牛爬得很慢很慢..對他說:你上來,我背你吧..然後..蝸牛就上來了..過了一會..烏龜又看到一隻螞蟻..對他說:你也上來吧..於是螞蟻也上來了。螞蟻上來以後..看到上面的蝸牛..對他說了句"你好"你們知道蝸牛說什麼嗎??蝸牛說:你抓緊點,這烏龜好快..

6、有一對男女正在吃晚餐那個女生一直問那個男生:你愛不愛我?男生看了女生一眼又繼續吃晚餐女生很生氣又再問了一次:你愛不愛我?男生終於說:愛女生又問:那你要怎麼證明?忽然男生從口袋裡拿了三十元出來,且問女生:你有沒有十元?女生拿了十元給了男生..男生就把四十元放在桌上過了一會兒.....女生很生氣的問男生:你到底要不要證明你愛我啊男生說:我已經證明了啊!!!四十擺在眼前!

範例五 (知識類—99乘法)



Taipei Medical University

主旨: 印度的九九乘法表是從1背到19?

從: 乃乃 <r1023111222@msn.com>

日期: Tue, 31 Aug 2010 16:46:51 +0800

到: mli@ntu.edu.tw

印度的九九乘法表是從1背到19?

你知道印度人是怎麼記 11到19 的數字嗎?
我是看了下面這本書之後才恍然大悟的。

「印度式計算訓練」

2007年6月10日第一版第6刷發行株式會社晉遊社發售
介紹了加減乘除的各種快速計算方法，
不過在這裡我只介紹印度的九九乘法。因為實在太神奇了！
！

下面的數字跟說明都是引用該書P.44 的例子。

請試著用心算算出下面的答案：

$13?? \times 12?? = ?$

(被乘數)(乘數)

印度人是這樣算的。

第一步：

先把被乘數(13)跟乘數的個位數(2)加起來

$$13 + 2 = 15$$

第二步：

再把被乘數的個位數(3)乘以乘數的個位數(2)

$$2 \times 3 = 6$$

第三步：

然後把第一步的答案乘以10(→也就是說後面加個0)

之後再加上第二步的答案就行了

$$15 \times 10 + 6 = 156$$

就這樣，用心算就可以很快地算出11X11 到19X19了喔。這
真是太神奇了！

我們試著演算一下

14x13：

(1) $14+3=17$

(2) $17 \times 10 = 170$

(3) $4 \times 3 = 12$

(4) $170 + 12 = 182$

真的是耶，好簡單喔

怎不早點讓我知道呢

這對我這種只會個位數加個位數的人真是一大福音..

好玩吧！

[\(更多精彩內容\)](#)

範例六 (生活類—安全帶)



Taipei Medical University

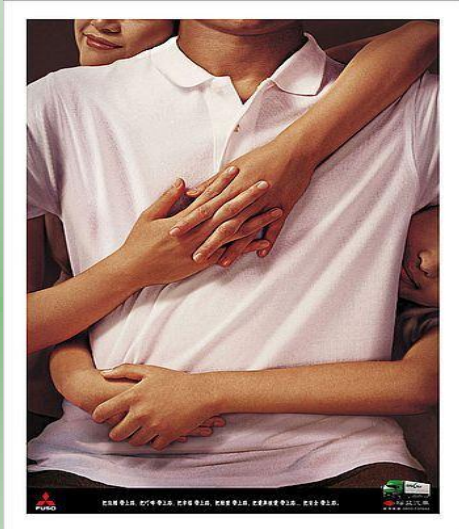
主旨:讓你忘不了的安全帶宣導影片!

從: 請注意安全 <specialthank@yahoo.com.tw>

日期: Tue, 31 Aug 2010 16:46:40 +0800

到: mli@ntu.edu.tw

讓你忘不了的安全帶宣導影片!



看過後應該再也不會忘了繫安全帶的!

開車前想想你愛的人~~

<http://www.youtube.com/watch?v=h-8PBx7isoM>

結論



Taipei Medical University

我們要時時提高警覺並加強**危機意識**，
確實做好**實體隔離**以及**存取控管**來保護
機密資料，並搭配定期的實體隔離稽核
和教育使用者、提醒使用者：**組織型駭
客的威脅是時時刻刻在發生的。**



Taipei Medical University

問題與討論

