社交工程演練及資安宣導

Outline

- 簡介
- 社交工程分年目標、演練時程及成果
- 本校精進作為
- 電子郵件使用安全應有的認知
- 電子郵件信箱設定

簡介

- 電子郵件社交工程：

  藉由傳送電子郵件方式，騙取收件者信任，進而開啟郵件內容的駭客攻擊模式。

- 透過電子郵件可以讓收件者

  (1)誘騙進入假網站

  (2)開啟惡意電子檔

  (3)下載問題檔案

社交工程分年目標、99年度演練時程及結果

教育部-惡意郵件開啟分年目標

等級	適用單位	98年度目標	99年度目標
A級	教育部、 台大醫院、 成大醫院	開啟率<10% 點閱率< 6%	開啟率<10% 點閱率< 6%
B級	大學、 區域網路中心、 縣(市)教育網路中心	開啟率<16% 點閱率<9%	開啟率<10% 點閱率< 6%

開啟率=開啟測試郵件之人數/單位參演人數x100%

點閱率=點擊測試信件所附連結或檔案之人數/單位參演人數x100%

99年度演練時程及方式

	演練時程	演練方式	備考
國家資通安全會報演練	1~12月不定期演練	寄發電子郵件	
學術機構分組（教育部）演練	第1次演練:5月 第2次演練:9月	寄發電子郵件	

99年度教育部演練方式

- 郵件主題分為政治、公務、健康養生、旅遊等類型，郵件內容包含連結網址或word附檔。
- 偽冒公務、個人或公司行號等名義發送惡意郵件給演練對象。
- 收件人開啟或點閱前述之電子郵件即會將開啟信件人員的資料自動傳回教育部。
- 信箱之預覽模式亦會產生開啟電子郵件的結果。

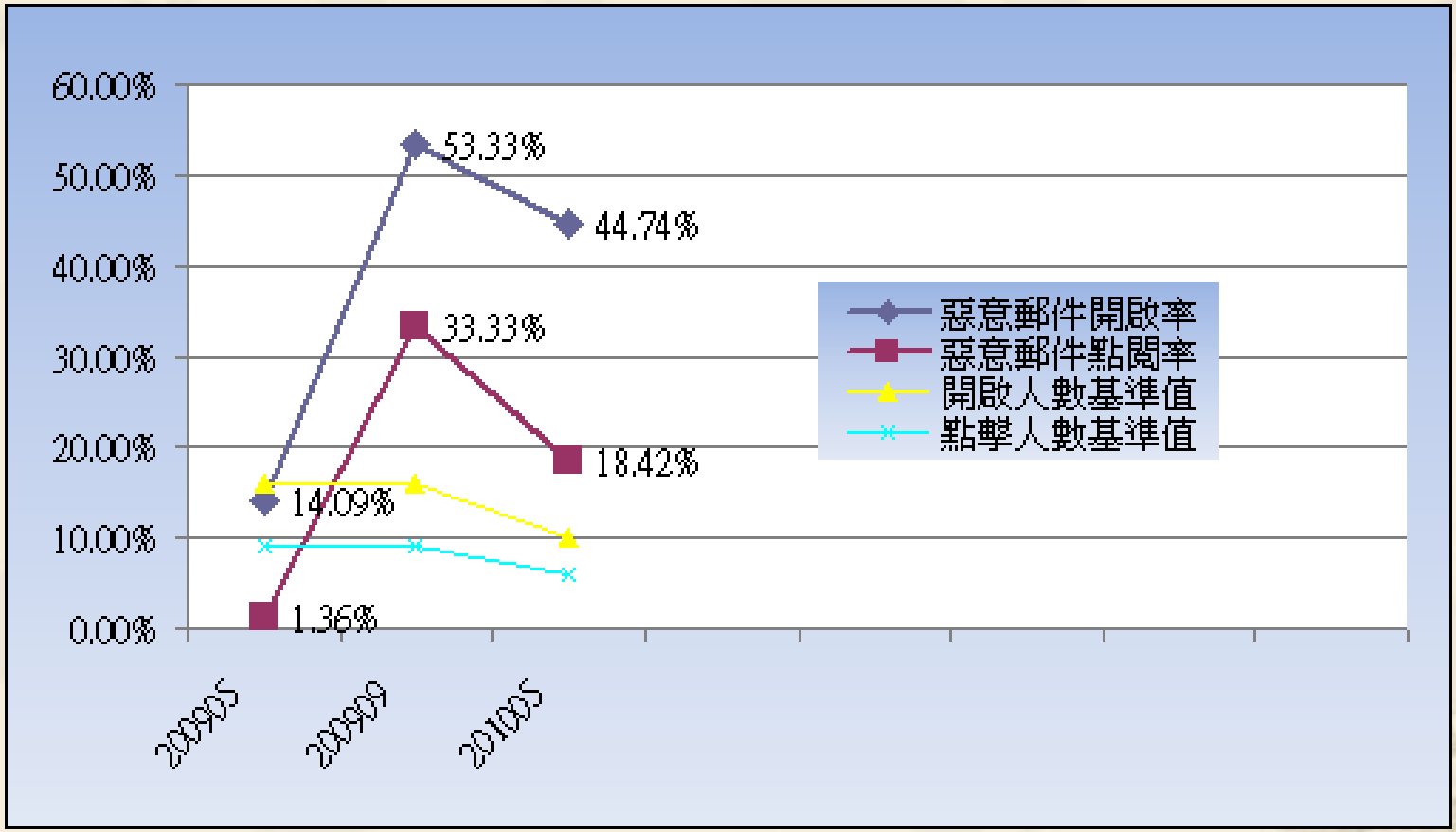
99年度教育部演練結果

	開啟率	點閱率
教育部A級單位	6.15%	5.00%
教育部B級單位	18.09%	10.55%
本校上半年	44.74%	18.42%

受測人數76人，開啟34人，點擊14人

→ 本校為B級單位中倒數15名

98~99年教育部測試結果



本校精進作為

- 加強宣導：

  本館將不定期以電子郵件發送宣導訊息

- 教育訓練

  每年辦理二次電子郵件社交工程講習

- 自我演練

  每季進行演練一次

- 獎懲

  未通過演練之同仁，除記點外並需參加教育訓練，記點達二次（含）以上，及已記點而未參與教育訓練者，將送人事室作為年度考核之依據。

非公務郵件請勿開啟!!!

電子郵件使用安全
應有的認知

1.駭客設計攻擊陷阱程式(如特殊word檔案或外部惡意連結。

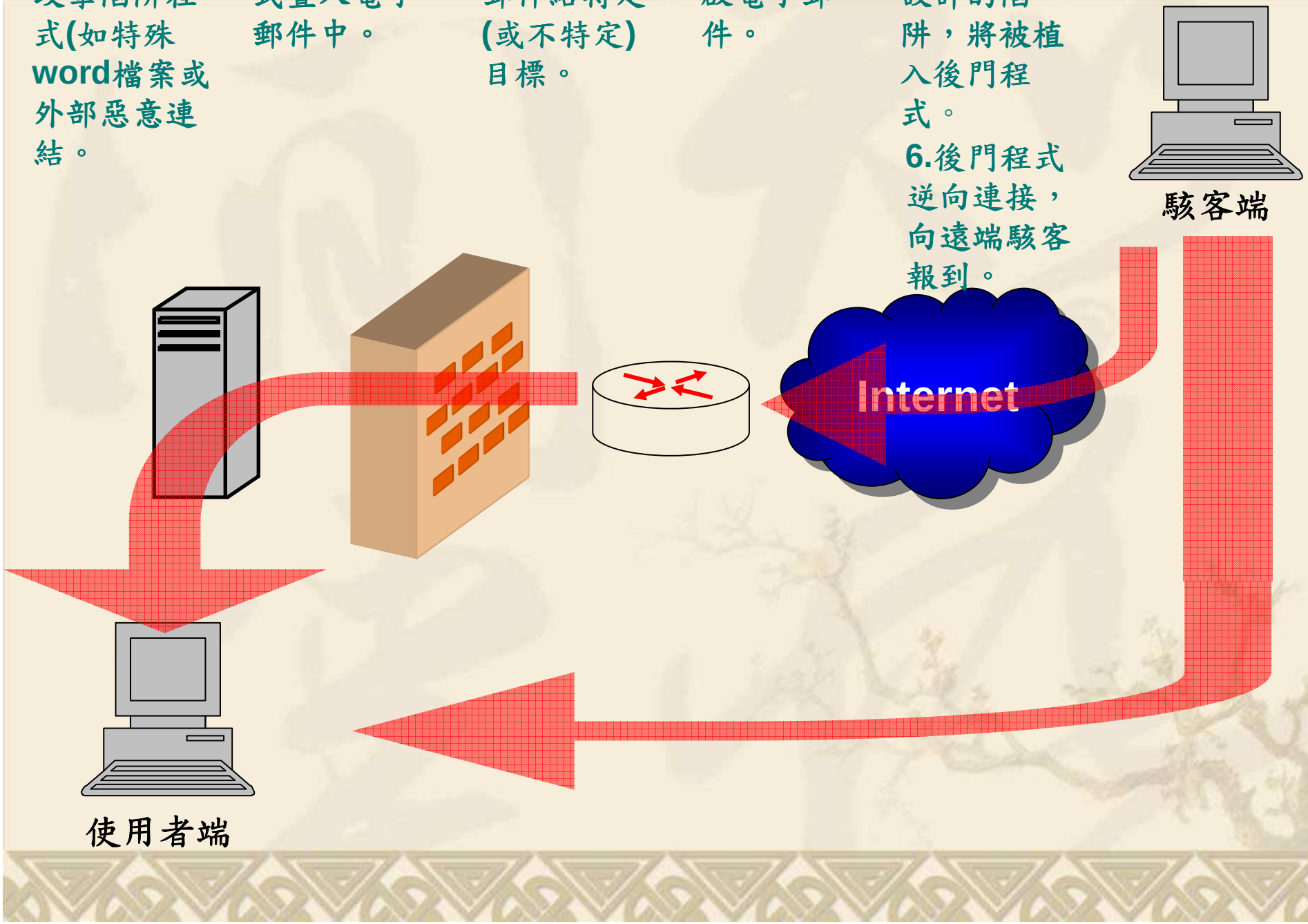
2.將攻擊程式置入電子郵件中。

3.寄發電子郵件給特定(或不特定)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。



開啟惡意電子郵件的可能後果

- 存放於本機
- 個人的信用
- 電腦遭利用
- 其它

首頁 > 新聞內容

史上最凶木

時間：2
撰稿：

網路駭
行用戶的存

據「每
電腦病毒侵
破。

專家表
危險的惡意

網路安
現，名叫「
行下手。

M86技
的病毒，無

M86表
經常檢查帳

木馬窺淫　駭客遙控電腦視訊攝影機　女生被看光光！(2010/07/23 16:32) NOWNEWS

網路科技讓許多人掉進了楚門的世界。(圖／翻攝自網路)

記者朱錦華／綜合報導

德國一名男駭客透過網路傳播木馬程式，遙控了多達150名女學生電腦的內建攝影機，並藉此進行偷窺。經過調查後，遙警方成功逮捕犯罪嫌疑人。

德國媒體報導，涉案男子來自萊茵地區。他的作案手法是通過網路論壇結識女性受害者，然後將帶有木馬程式的螢幕保護程式附在郵件中，再假冒他人身份發送給受害者。之後，該男子透過木馬程式竊取受害者電腦上視訊攝影機的控制權，並且從遠端遙控，進行偷窺並錄影。

察覺到攝影機鏡頭有異常的女生，將情況反映給政府的青少年數據保護專家。專家根據線索，協助警方找到疑犯，警方在家中將他逮捕時，在他的電腦裡發現大量的偷窺影片。

事發後，德國專家紛紛呼籲加強青少年的網路安全意識。德國科普電視節目《伽利略》日前製作專題，建議人們使用完網路後，儘量不要保持待機，應關閉電腦；拔掉攝影機鏡頭頭和電源，以防止被偷窺。並提醒人們如果遇到可疑情況，應盡快向有關部門反映。

惡意電子郵件特性

- 假冒寄件者
- 使用讓人感興趣的主題及內容
- 含有惡意程式的附件
- 利用零時差攻擊

假冒寄件者

- 駭客會假冒使用者信任的人，讓使用者相信電子郵件的內容，進而去開啟這些附件或超連結，並暗中啟動木馬程式。

使用讓人感興趣的主題及內容

- 駭客會使用收信者有興趣的主旨，甚至會配合目前最熱門的新聞事件，來吸引收信者開啟郵件
- 如教育部電子郵件社交工程演練的信件主旨

教育部99上半年度測試信件摘要表

組別	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 連桃太郎都驚豔!!
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 驚豔全場
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》把大人物 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」鐵飯碗 錄取率僅1.25%

教育部98上半年度測試信件摘要表(有預警)

組別	信件類別	信件標題
Letter 1	政治、體育類	軍方賣官內幕 洋基球團虧待王建民
Letter 2	休閒娛樂類	自行車旅遊私房路線 聯合報邀您賞桐花
Letter 3	科技新知、保健養生類	USB 成病毒温床！台灣電腦今年Q1中毒率列入全球第四大 蛀牙不是病，痛起來要人命
Letter 4	投資理財、保健養生類	景氣復甦了嗎？ 新流感 H1N1 大流行期間，個人保健注意事項
Letter 5	情色、影視新聞類	瑤瑤和舒舒，你喜歡誰

教育部98下半年度測試信件摘要表(無預警)

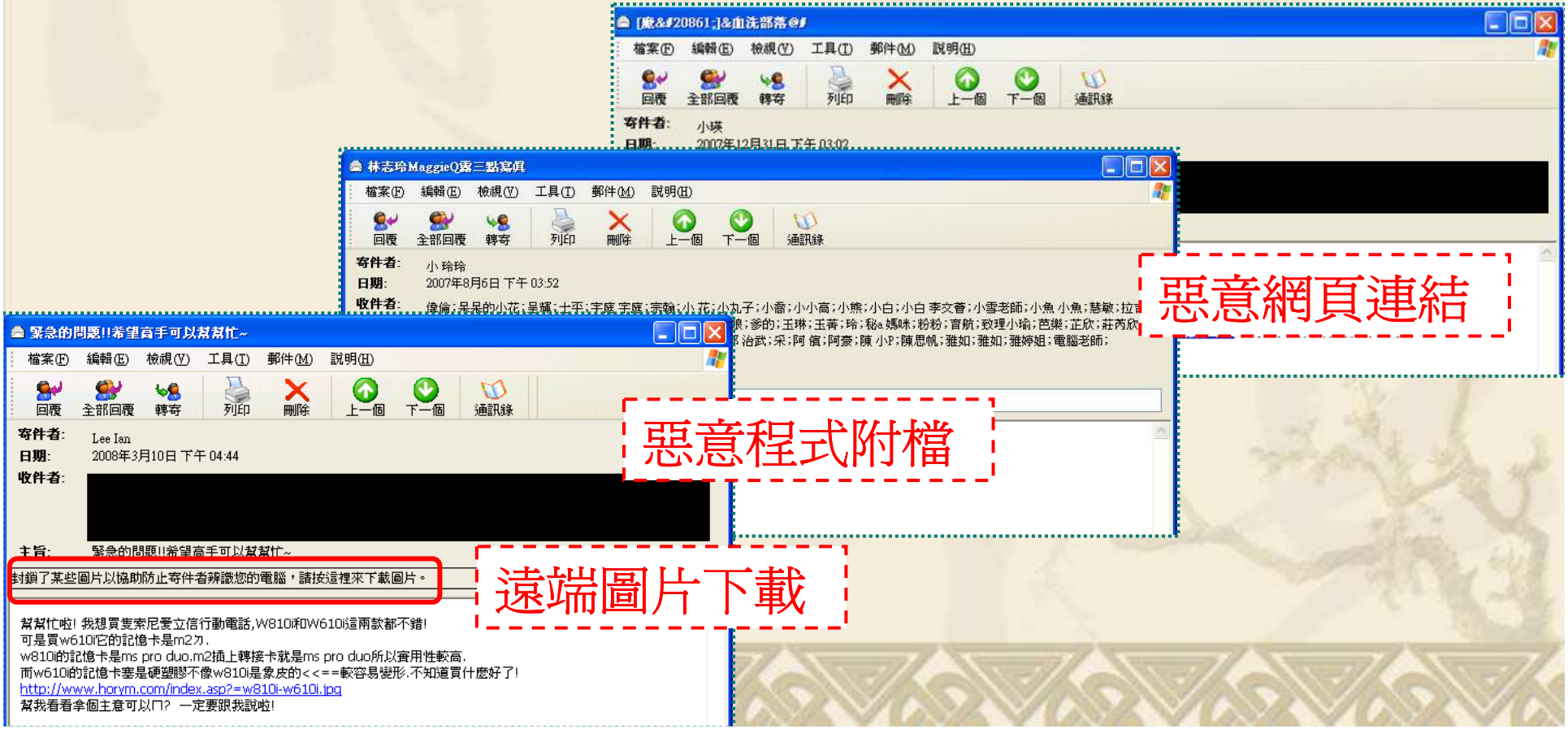
組別	信件類別	信件標題
Letter 1	生活類	讓你感動的動人廣告
Letter 2	投機類	如何提高中獎機率!!
Letter 3	旅遊類	【HiNet旅遊網首發團】 獨家限量獨享好康 超低價!!
Letter 4	旅遊類2	【HiNet旅遊網首發團】 獨家限量獨享好康 超低價!!
Letter 5	健康類	健康新撇步!!?你如何活的更健康
Letter 6	電腦科技類	七夕前後交友網站爆高量 慎防網路桃色陷阱
Letter 7	影視類	文英阿姨病逝 留給觀眾無限懷念
Letter 8	影視類2	昔日玉女紅星 酒井法子自首 坦承吸毒
Letter 9	趣味類	親愛的同事!放鬆一下
Letter 10	購物類	iPhone 最新推出3Gs 便宜到不敢相信！！

含有惡意程式附件

- 駭客在電子郵件附帶一個含有惡意程式的檔案，這個檔案不一定是執行檔，可能是各種類型的應用程式，甚至是壓縮檔。駭客會夾帶任何在應用程式上有弱點的文件檔案類型，並想辦法誘騙使用者開啟附件，藉以啟動安裝木馬程式。例如：
  - 含有惡意程式的影片檔（wmv）
  - 含有惡意程式的Office文件（doc）
  - 含有惡意程式的圖檔（jpg）
  - 含有惡意程式的壓縮檔（zip）

含有惡意程式的附件

- 郵件中惡意程式附檔與連結
- 郵件中的遠端圖片下載（與ActiveX）



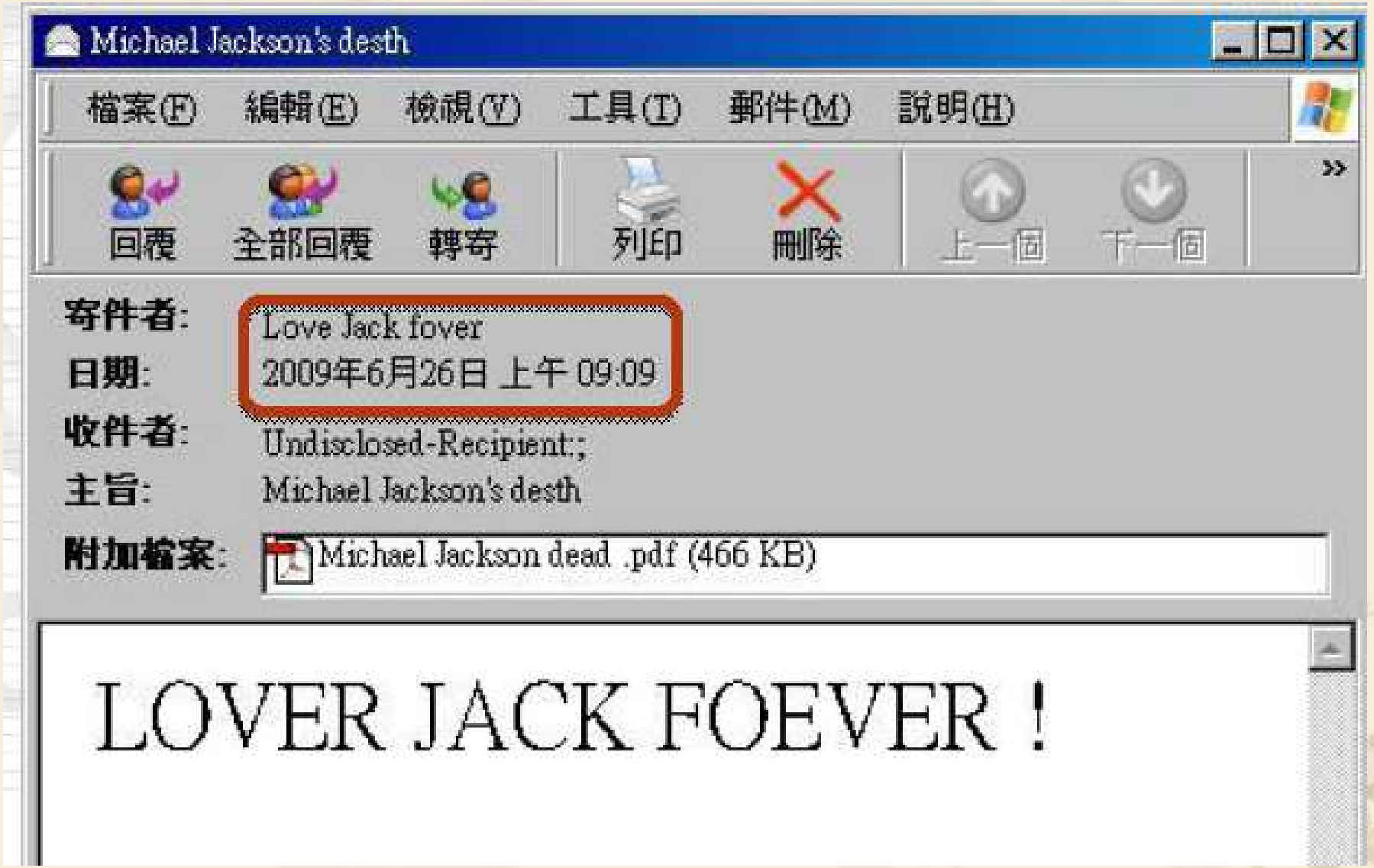
含有惡意程式之附件

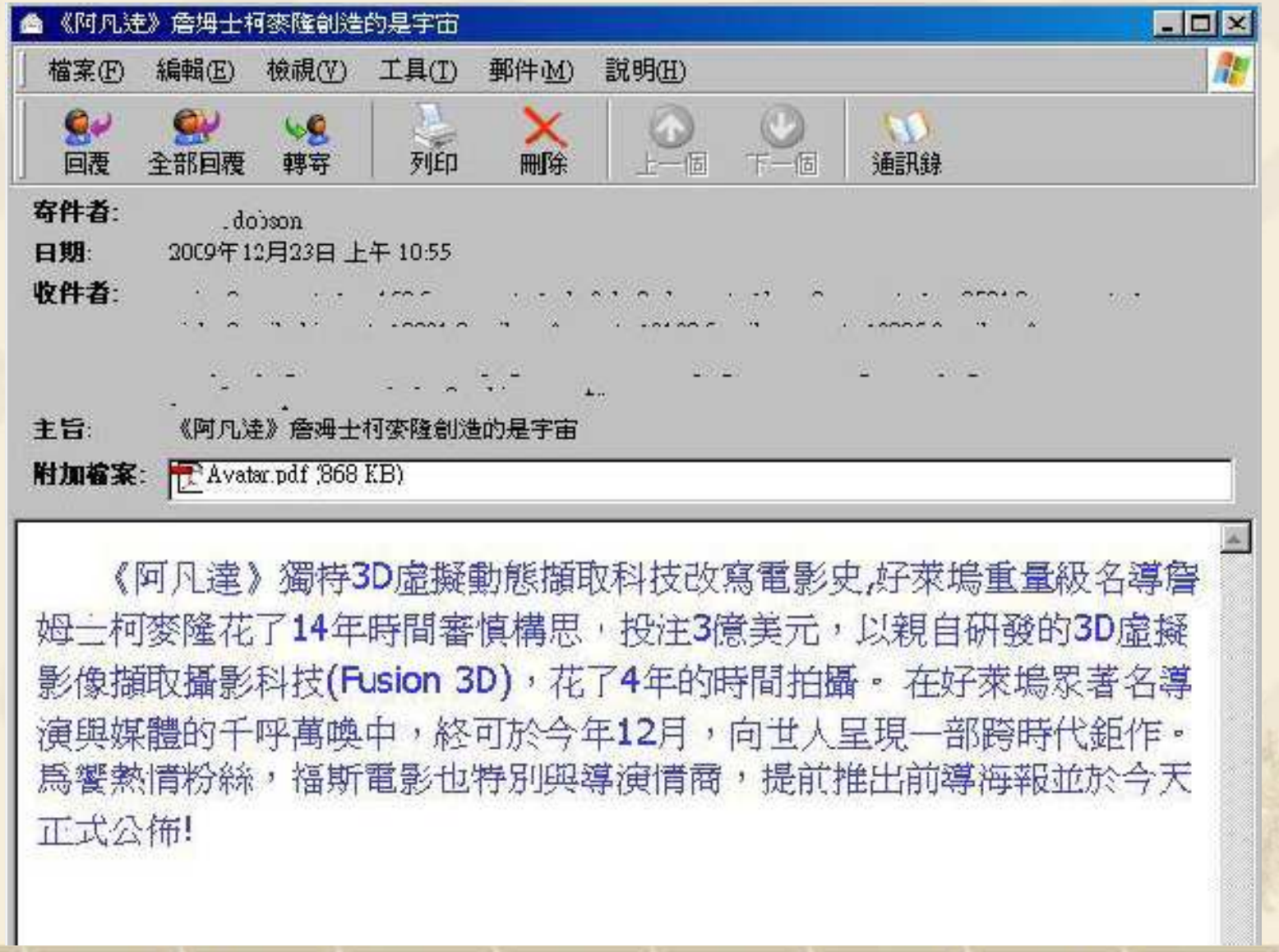
- 附件檔案型態不一定是執行檔(.exe)，可能是各種類型的檔案(.doc、.ppt、.mdb等)，甚至是壓縮檔(.rar)
- .exe .com .scr
  .pif .bat .cmd
  .doc .xls .pps/ppt
  .reg .lnk .hta
  .zip .rar .swf
  .html .pdf .mdb

國家資通安全會報 技術服務中心

漏洞/資安訊息警訊

發布編號	ICST-ANA-2009-0005	發布時間	2009/12/23 10:00:48
事件類型	攻擊活動預警	發現時間	2009/12/21
警訊名稱	Adobe Reader/ Adobe Acrobat 9.2.0 以前版本零時差攻擊預警		
內容說明	技術服務中心於近日發現，駭客利用Adobe Reader及Acrobat的重大弱點，在PDF文件中使用惡意的Javascript。當使用者開啓這類PDF文件時，可能於受攻擊成功後遭植入惡意程式，攻擊者將可控制受害系統執行任意惡意行爲。 本中心已發現使用該弱點之惡意PDF文件，經由電子郵件進行攻擊。目前Adobe尚未修補此弱點，建議使用者參照以下建議措施停用Javascript功能，來防堵這類的攻擊手法。		
影響平台	Adobe Reader / Arobat 9.2.0 及 更舊版本		
影響等級	高		
建議措施	1.點選編輯->偏好設定->JavaScript 將 「啓用Acrobat Javascript」取消核選 2.此弱點目前尚待廠商提供修補程式，預計於99/1/12後提供更新程式，屆時請注意更新。		


Michael Jackson's desth
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個
寄件者: Love Jack fover
日期: 2009年6月26日 上午 09:09
收件者: Undisclosed-Recipient:;
主旨: Michael Jackson's desth
附加檔案: Michael Jackson dead .pdf (466 KB)
LOVER JACK FOEVER !


《阿凡達》詹姆士柯麥隆創造的是宇宙
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄
寄件者: .dobson
日期: 2009年12月23日 上午 10:55
收件者:
主旨: 《阿凡達》詹姆士柯麥隆創造的是宇宙
附加檔案: Avatar.pdf (868 KB)
《阿凡達》獨特3D虛擬動態擷取科技改寫電影史,好萊塢重量級名導詹姆士柯麥隆花了14年時間審慎構思，投注3億美元，以親自研發的3D虛擬影像擷取攝影科技(Fusion 3D)，花了4年的時間拍攝。 在好萊塢眾著名導演與媒體的千呼萬喚中，終可於今年12月，向世人呈現一部跨時代鉅作。為饗熱情粉絲，福斯電影也特別與導演情商，提前推出前導海報並於今天正式公佈!

國家資通安全會報 技術服務中心

漏洞/資安訊息警訊

發布編號	ICST-ANA-2010-0006	發布時間	2010/08/09 15:48:29
事件類型	公告資訊	發現時間	2010/08/04
警訊名稱	[內容更正] 駭客偽冒行政院院長室發送社交工程攻擊信件		
內容說明	※因前封警訊影響平台漏列Windows系列平台，且建議措施不夠清楚，請各資安聯絡人參考本更新警訊進行防護措施。 技術服務中心於近日接獲通報，駭客偽冒行政院院長室發送社交工程攻擊信件，內文中包含有關人員之簽名檔，製作惡意程式(使用RTLO方法)誘使使用者點擊，以取得使用者權限或執行遠端程式。當使用者點擊這類檔案時，可能於受攻擊成功後遭植入惡意程式，攻擊者將可控制受害系統執行任意惡意行為。 該手法係利用作業系統解讀檔案名稱時，若遇到Unicode控制字元，會改變檔案名稱的顯示方式進行攻擊。駭客可以在檔案名稱中，插入特定的Unicode控制字元，導致作業系統在顯示該檔案名稱時，誤導使用者。 例如，駭客可能將惡意程式命名為：提醒[202E]TXT.SCR，即會顯示為：提醒RCS.TXT，讓收件人誤以為是純文字檔，提升點擊的機率。 本中心已發現使用該弱點之惡意文件，經由電子郵件進行攻擊。建議使用者參照以下建議措施來防堵這類的攻擊手法。		

點擊郵件中的連結…
開啟郵件中的附檔…

您可能已經明白了
不要點擊連結與隨意開啟這些附檔，
但您可能還是疑惑
為什麼開啟郵件也算違規？

為何要求不能「開啟郵件」？

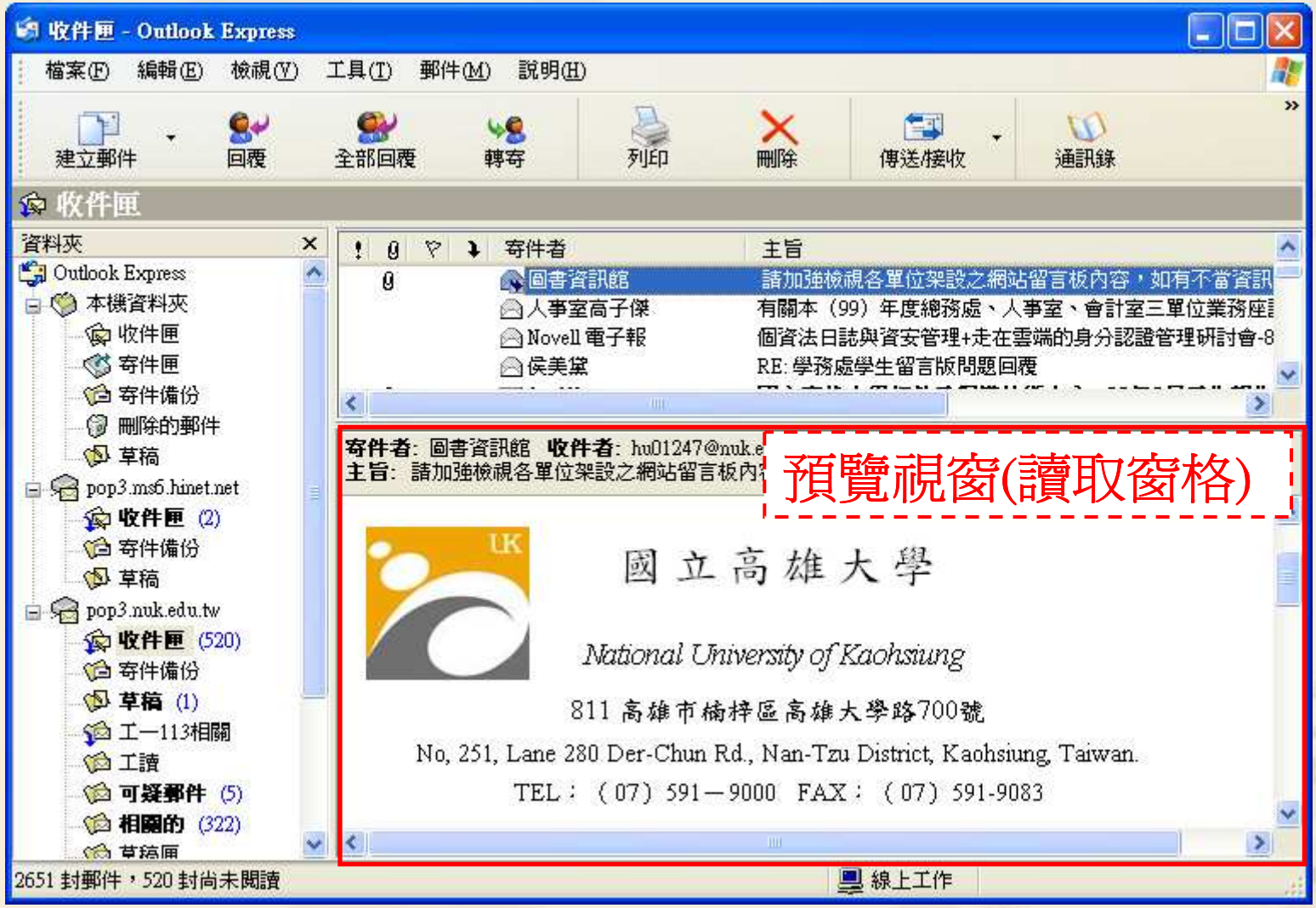
- 似乎只要不開郵件附件和不點擊連結，就不會中招...

→但有些惡意程式是利用ActiveX功能來執行的

→由於您的電子郵件可能是HTML格式，而HTML可以撰寫ActiveX，所以您只要瀏覽電子郵件，就觸發ActiveX執行！

啟用預覽視窗等同「開啟郵件」

- 利用IE漏洞，不開啟附檔也會中毒
  - 2004年3月，Beagle.O電腦病毒使用IE漏洞攻擊，使用者在Outlook / Outlook Express環境下啟用信件預覽功能，信件中的script就會啟動，連結到惡意程式網站下載病毒程式


收件匣 - Outlook Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
建立郵件
回覆
全部回覆
轉寄
列印
刪除
傳送/接收
通訊錄
收件匣
資料夾
Outlook Express
本機資料夾
收件匣
寄件匣
寄件備份
刪除的郵件
草稿
pop3.ms6.hinet.net
收件匣 (2)
寄件備份
草稿
pop3.nuk.edu.tw
收件匣 (520)
寄件備份
草稿 (1)
工一113相關
工讀
可疑郵件 (5)
相關的 (322)
寄件者
主旨
圖書資訊館
請加強檢視各單位架設之網站留言板內容，如有不當資訊
人事室高子傑
有關本（99）年度總務處、人事室、會計室三單位業務座
Novell 電子報
個資法日誌與資安管理+走在雲端的身分認證管理研討會-8
侯美黛
RE: 學務處學生留言版問題回覆
寄件者: 圖書資訊館 收件者: hu01247@nuk.e
主旨: 請加強檢視各單位架設之網站留言板內
預覽視窗(讀取窗格)
國立高雄大學
National University of Kaohsiung
811 高雄市楠梓區高雄大學路700號
No, 251, Lane 280 Der-Chun Rd., Nan-Tzu District, Kaohsiung, Taiwan.
TEL：（07）591－9000 FAX：（07）591-9083
2651 封郵件，520 封尚未閱讀
線上工作

- 所以除了不要點擊連結與隨意開啟附檔外，您應該曉得的安全防護還包括：

關閉自動下載圖片
關閉預覽視窗
不要自動回覆讀信回條
考慮設定以純文字格式讀取郵件

收取電子郵件時應有的習慣

- 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
- 開啟檔案、超連結前，確認對應軟體（如IE、Office、壓縮軟體）都保持在最新的修補狀態。

非公務郵件請勿開啟!!!

電子郵件信箱設定提示

- 關閉自動下載圖片
- 關閉預覽視窗
- 設定不要自動回覆讀信回條
- 設定以純文字格式讀取郵件

outlook 2007、outlook 2003、 outlook express、 webmail