[電子郵件]社交工程

江俊杰

電子郵件的危害
電子郵件社交工程演練
防範電子郵件社交工程的方法

課程大綱

- 一、電子郵件的危害
  - 1. 信件攻擊手法
  - 2. 社交攻擊手法
- 二、電子郵件社交工程演練
  - 1. E-mail社交工程演練方法及流程
  - 2. 社交工程信件的類型
  - 3. 電子郵件社交工程要求標準
- 三、防範電子郵件社交工程的方法
  - 1. 注意可疑電子郵件的特徵
  - 2. 社交工程信件的防範措施

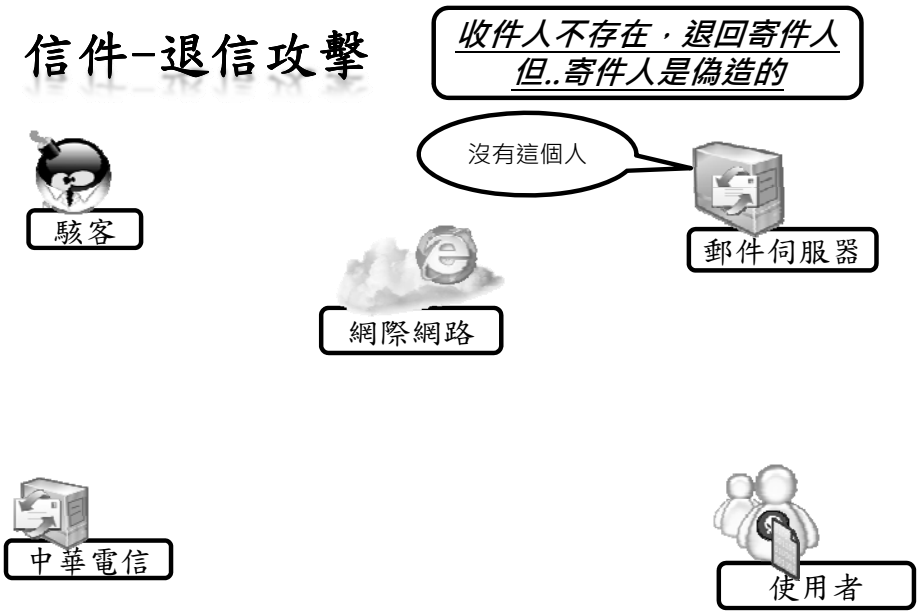
一、電子郵件的危害

- 1. 信件攻擊手法
  - 退信攻擊
  - 跳板攻擊
  - 密碼猜解
- 2. 社交攻擊手法
  - 偽造攻擊
  - 附件攻擊
  - 郵件跟蹤

駭客手法–退信攻擊

- *收件人不存在導致無法送達郵件*，就會自動將該*退信訊息寄回給原寄件者*
- 利用這項功能，使用*字典攻擊所蒐集到的Email*
- 將*欲攻擊的對象設定為寄件者*
- *收件者使用其他單位不存在的帳號*
- 然後你就會收到一封*不是自己寄出去的退信*了

信件-退信攻擊



駭客手法-跳板攻擊

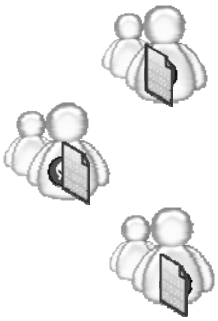
- 當您的*電腦主機本身有啟用SMTP Service* (外寄伺服器服務)，而且*沒有加以防護*時，被有心人士發現，進而不當使用您的網路頻寬及寄信功能，濫寄廣告信件，這就是您的電腦主機被當成廣告信跳板了!!
- 通常受害者不知道自己的電腦安裝了相關服務
- 常見微軟的作業系統，當有*安裝了IIS功能*，*就會一同安裝SMTP(外寄伺服器服務)*，此時若您的網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔的話 ，基本*上任何人都可以藉由您的 SMTP Service 寄發信件*!! 您的電腦主機，就有可能被有心人士當成廣告信跳板，濫寄廣告信件!!

信件-跳板攻擊

轉寄信件的功能沒有關閉
可以....轉寄垃圾信

駭客

網際網路

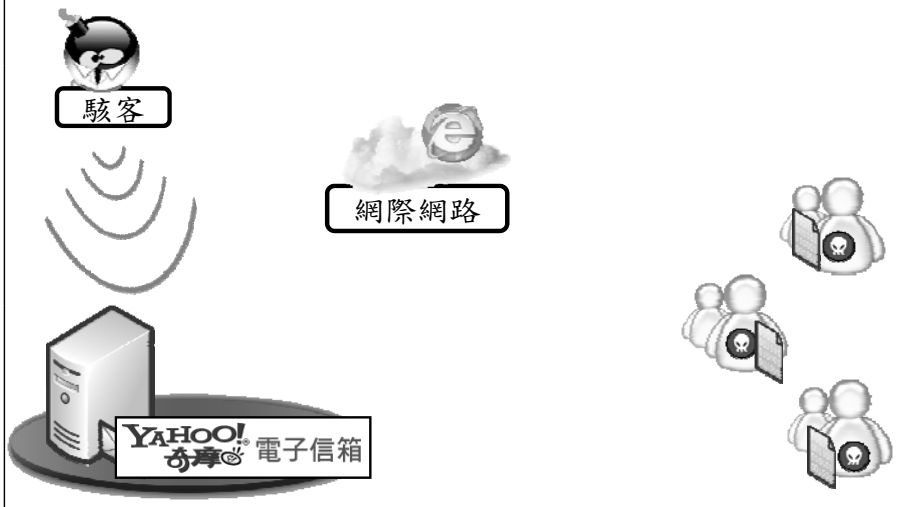


駭客手法-密碼猜解

- 要破解密碼絕非易事，被破解的人幾乎有個共同的特性
- 就是*密碼過於簡單*!!
- 只要你是以下的其中一種，就要注意了!!
- 1.生日組合 (19820105)
- 2.英文單字 (Mickey)
- 3.數字組合 (12345)
- 4.英文組合 (abcabc)
- 5.常用英文 (iloveyou)
- 採用無意義的英數混合密碼!! (合併多位元)
- 如 u4k4id09io , 但通常取一取自己都記不起來 XD

信件–密碼猜解

信箱密碼=1234
用.....猜的可以猜到



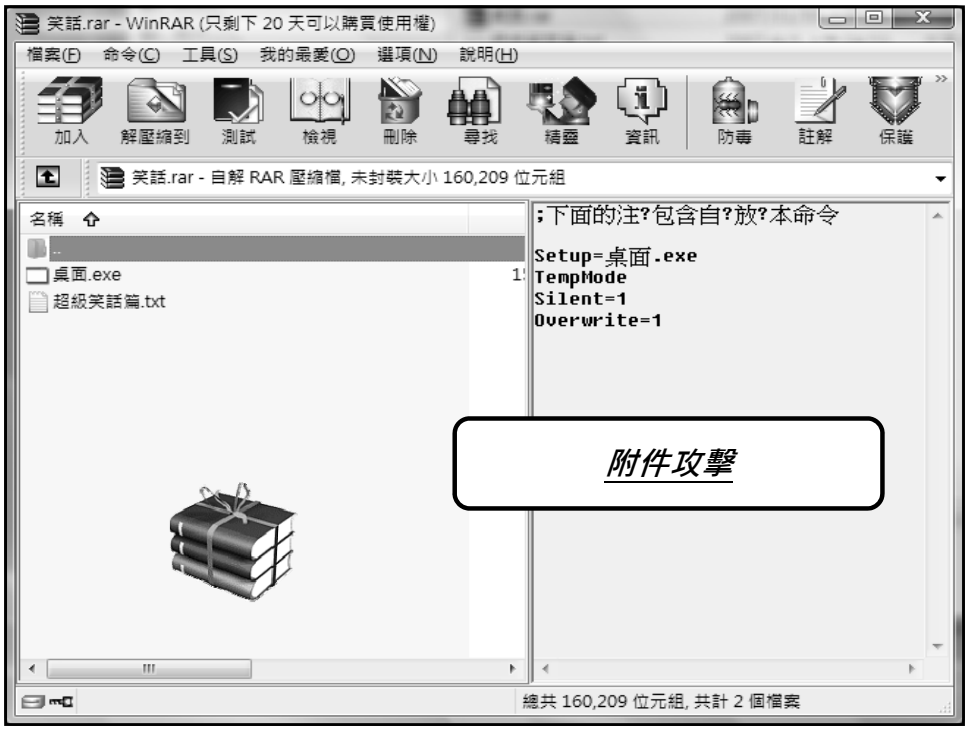
駭客手法–偽造攻擊

- SMTP 通信規範, *沒有辦法限制驗證寄件人的身份*. 雖然可以用身份驗證機制確保信是由特定人員寄出 (例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...
- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的
- 整封信件，都是假的!!!!!!!!!

偽造攻擊

駭客手法-附件攻擊

- 病毒信附件的副檔名常見使用Zip或RAR壓縮檔格式來發送
- 不管是收到認識或不認識的人寄來的信件，請使用加密處理
- 信件的內容大概都是
  - 他去哪裡玩有拍一些照片要分享給你看、他在網路上看到你被偷拍的照片，趕緊寄給你看是不是真的是你、(這樣你也真的打開來看的話~大概你也常去厚德路吧)
  - 朋友的小孩離家出走說要見網友，結果都沒有回家，隨信寄了小孩的照片請大家幫忙協尋
- 就是要騙你去開檔來看
- 檔案就是RAR檔，裡面放了一個cmd檔
- 不要好奇去打開裡面的檔案，直接刪除信件信件就好
- 一般常見會讓電腦中毒的副檔名包含：
- .bat、.exe、.com、.scr、.zip、.rar



駭客手法–郵件跟蹤

- 電子郵件加入一個圖檔，嵌在信件當中，當收件人打開郵件時，圖檔也同時被下載，這樣寄件人就可以從*圖檔被下載而得知對方已收到郵件*了。
- 加入一段超連結，收件人點選超連結看到網頁時，寄件人就可以從*網頁被下載而得知對方已收到郵件*了。
- 同樣的手法，也可以使用在Word或MSN軟體。

二、電子郵件社交工程演練

- 1. E-mail社交工程演練方法及流程
- 2. 社交工程信件的類型
- 3. 電子郵件社交工程要求標準

電子郵件社交工程執行目的及依據

- 目的：為提升電子郵件使用者警覺性意識，避免使用者因瀏覽垃圾及惡意電子郵件進而影響網路安全及發生個人資訊洩漏事件
- 依據行政院國家資通安全會報96年10月3日資安發字第0960100539號函96年政府機關(構)資安演練評審辦法規定：
- (一)中央A級機關
- 惡意郵件開啟率為**16%**，超連結點閱率為**9%**。
- (二)其餘主管機關
- 惡意郵件開啟率為**26%**，超連結點閱率為**15%**。

人數百分比/信件數百分比

執行細項及結果

- 執行期間：98年1月1日~ 98年12月31日
- 發送測試信件
  - *免費送巧連誌影音教材*、*民代可以蒐集個資嗎*、*茂德增資*、*殺OnLine線上遊戲桌布*、*豬哥亮準備復出*、*男人誌線上閱讀網*、*座位靠窗邊*、*2009台北國際花卉展開始囉*
- 會開啟社交工程信件之
- 次數**24**次，佔該項發信量**1272**封信中的**1.9%**
- 會點選社交工程信件中超連結之
- 次數**6**次，佔該項發信量**1272**封信中的**0.5%**

標準16%

標準9%

（模擬數據）

信件範本-01-林志玲華航月曆桌布

- 包含*明星或寫真圖片的電子郵件*點閱率始終居高不下；本封電子郵件利用民眾對於明星相關訊息具有高度興趣的習慣下，發送明星相關活動新聞並於內容提及明星桌布取得不易以及本郵件具有*高畫質寫真桌布*，誘使使用者繼續點選電子郵件中的連結


送給你林志玲華航月曆桌布

華航發言人孫鴻文表示，由於2007年的月、桌曆反應熱烈，網路競標甚至高達3000元。因此，2008年華航將印製4萬份，贈送給華航的員工和貴賓，數量是去年的3到4倍。但依舊只送不賣，一般民眾想要索取，可能又得到網路上碰碰運氣。

繼續閱讀：林志玲寫真桌布精選(高畫質71大張)

- 對於明星所代言之活動，*官方並不會以電子郵件方式宣傳且提供下載*，而是應於*官方網站中以網頁方式呈現*，因此只要收到此類信件大多為有心人士於網路上找尋大眾所感興趣之話題所製成的社交工程詐騙信件

信件範本-02-馬英九露出馬腳

- 社交工程就是一種利用人性弱點的詐騙技術，藉由與人之間的互動而形成的犯罪行為；本封電子郵件為*模擬駭客針對剛當選總統的馬英九為議題*，以垃圾信件的大量發送手法發送測試信件於使用者


人生就是跟自己賽跑，用這樣的態度去面對人生，你會產生推動自己不斷學習、進步的能量，而且你眼中會看到一個更遠、更高的目標。每天醒來，你都會因此而感到生氣勃勃。--馬英九

下一篇：馬英九(妙語如珠)

23【閱讀，可漫遊、可發光】

四、五十年代的台灣，小小的租書店裡，架子上擺滿了各式各樣的武俠小說。

幾個男孩等不及，手上抓著一本小說，坐在小板凳，就津津有味地看了起來。

- 對於名人的事蹟、名言等內容的電子郵件，*大多數人認為這是好文章因此轉寄給他人*，孰不知這是垃圾郵件的常見手法，無形轉寄中已幫了惡意人士的大忙。*對於此種電子郵件應盡量做到不開啟、不轉寄*

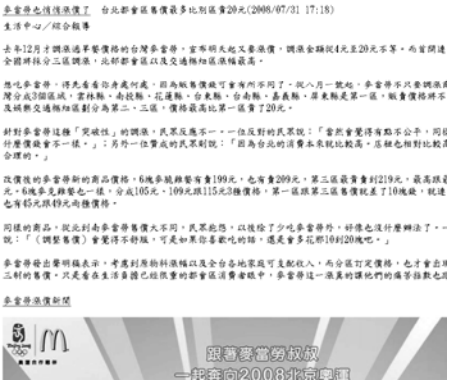
信件範本-03-限制級精彩古代漫畫

- *情色類電子郵件由於點閱率高*，在垃圾信件中一直佔有一定的比例，更是*有心人士慣用的手法*；本封電子郵件模擬駭客針對使用者寄發一封具有情色相關內容的電子郵件，引誘使用者閱讀電子郵件甚至點擊內文中的超連結

- 對於情色類的電子郵件，應於*辦公室環境中明令禁止使用者開啟瀏覽及點閱*，電子郵件主旨中包含*隱喻*、*影射*、*寫真*等字眼皆為情色類的電子郵件類型

信件範本-04-麥當勞也悄悄漲價了

- 該封電子郵件為行政類電子郵件，利用*陳舊的新聞事件*並結合近期民眾關心的*民生物資漲價議題*，模擬駭客手法，大量發送電子郵件於使用者


麥當勞也悄悄漲價了　台北都會區售價最多比別區貴20元(2008/07/31 17:18)
生活中心／綜合報導
麥當勞也悄悄漲價新聞
跟著麥當勞叔叔

- 防範此種電子郵件的方式應該宣導使用者做到[不開啟]、[不轉寄]，由於*一般正常的公務內容的電子郵件皆為一般純文字文件*，所以也可以在電子郵件軟體中設定(以outlook express 為例)，[工具/選項/讀取/*以純文字方式讀取所有郵件*]，即可避免此類社交工程電子郵件的攻擊

信件範本-05-胡志強今上班綠要給他好看

- 該封電子郵件為政治類電子郵件，利用*聳動的政治標題*並選擇政治人物新聞為內容的社交工程電子郵件。本封電子郵件模擬駭客手法利用公務人員上司新聞，誘使使用者開啟該電子郵件


胡志強今上班-綠營要給他好看（記者唐在馨／台中報導）

市長胡志強昨天返國，民進黨市議會黨團將於今天上午9點到市府前「迎接台中市府集外交部長胡志強回國」，表達對「颱風來，市長落跑」最大的不滿及抗議。

民進黨議員陳淑華、蕭杰、鄭幼逸及賴佳徽昨天偕妥市府，預備今天號召黨團成員一起到市府前廣場舉辦「歡迎式」，陳淑華表示，雖然胡志強昨天回國，對自己的決策表示「尚難」及「歉意」，但市長為何缺意參以外交為重，以及「市長的心在哪裡」？身為市市民意代表，不能不追究。

議員鄭幼逸、賴佳徽說，胡志強說，「研判颱風不會造成太大的傷害」，所以才出國，胡志強都歷會研判氣象，乾脆去當「氣象局長」好了，還誤判研的「預測神幼」怎麼沒有發揮在市政基礎風災救時，太晚宣佈停班停課，且中市遇出現百年難得一見的大淹水？

蕭杰則表示，市長說「要給市府團隊一個表現的機會」，市長還有一年半的任期，就應著要「給別人表現的機會」，不如快點去中央任職，讓市府團隊「好好表現」就好了；至於胡志強去中央做什麼？蕭杰說，外交部、社會福利部都可以，因為他這次選擇颱風來仍出國，只是為了這趟結束給馬好篇。

- *任何媒體並不會主動寄發新聞消息*，除非*使用者有明確的訂閱電子郵件*的動作，否則主動寄發的新聞、政治類電子郵件，大多為社交工程惡意郵件

信件範本-06-情人節專屬玫瑰花桌布

- 電子郵件社交工程手法越來越多樣化，除了利用時事吸引使用者點擊之外，同時也會利用*美麗的版面*與大量的圖片來降低使用者的緊戒心；本封電子郵件模擬駭客針對*七夕情人節議題*對使用者寄發一封具有大量情人節專屬玫瑰花桌布為內容的電子郵件


情人節專屬玫瑰花桌布-七夕情人節給親愛的一個驚喜吧!

- 對於*來路不明的電子郵件*，即使內容或標題多吸引人，也*不應該開啟或點擊郵件內的任何連結*，隨時保持接收電子郵件及上網的警覺心，是保護個人電腦資訊的最佳法門

信件範本-07- 2008花旗銀行網路辦卡

- 選擇美商花旗銀行夏季網路辦卡服務的原因為：近來*使用信用卡消費的人數越來越多*，基於信用卡帶來的便捷性以及該活動具有優惠方案，故模擬駭客以社交工程手法利用美商花旗銀行夏季網路辦卡服務電子廣告信件，誘使電腦使用者瀏覽並點選該電子郵件超連結

- 正確辦理信用卡服務的方式，應該是由*洽辦者親自前往該銀行辦理*，凡是網路上的電子郵件，*只要聲稱與任何銀行有洽辦關係，大部分皆為詐騙行為*，如果該電子郵件為正式花旗銀行所發出之電子郵件，電子郵件標頭網域名稱應該是*[@citibank.com*]

信件範本-08-擺脫菸癮 1通電話專人協助

- *行政類電子郵件*其主要為*一般政府機關對外公告知途徑*，但由於網路新聞媒體的氾濫，常見由一般使用者於閱覽之後轉寄他人以共同閱覽，本封電子郵件模擬駭客以*真實網路新聞事件*內容，大量轉寄於其他使用者

- 對於電子郵件的轉寄，經常是駭客入侵以及病毒傳播的一大途徑，應於辦公室環境中宣導[*勿轉寄非公務用途的電子郵件*]

測試帳號相關資料

- 測試對象: **159**個聯絡人(信箱)
- 總發信量: **1272**封。(159信箱x 8封信)

單位分類	人數(信箱數)	單位分類	人數(信箱數)
A	13	H	4
B	22	I	3
C	11	J	13
D	11		
E	14	L	11
F	13	M	19
G	22		

（模擬數據）

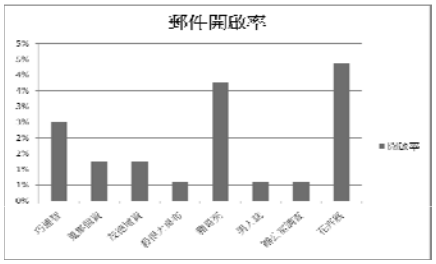
測試人數影響百分比/隨機抽樣

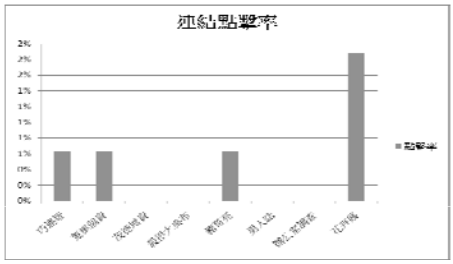
測試結果概要

單位分類	受測人數	郵件開啟數	郵件開啟率	超連結點擊數	超連結點擊率
A	13	6	5.8%	1	1.0%
B	22	2	1.1%	1	0.6%
C	11	1	1.1%	0	0.0%
D	11	1	1.1%	0	0.0%
E	14	1	0.9%	2	1.8%
F	13	0	0.0%	0	0.0%
G	22				1.1%
H	4				0.0%
I	3	0	0.0%	0	0.0%
J	13	2	1.9%	0	0.0%
M	19	6	3.9%	0	0.0%
各項目總計	159	24	1.9%	6	0.5%

（模擬數據）

測試人數影響百分比/隨機抽樣





類別	巧連智	個資	茂德	殺很大	豬哥亮	男人誌	調查	花卉展	合計
開啟次數	4	2	2	1	6	1	1	7	24
點擊次數	1	1	0	0	1	0	0	3	6
發信數	（模擬數據）						159	159	1272
開啟率	2.5%	1.3%	1.3%	0.6%	3.8%	0.6%	0.6%	4.4%	1.9%
點擊率	0.6%	0.6%	0.0%	0.0%	0.6%	0.0%	0.0%	1.9%	0.5%

測試年齡層影響測試數據

演練結果說明

（模擬數據）

- 96年政府機關(構)資安演練評審辦法規定：
- (一)中央A級機關
- 惡意郵件開啟率為**16%**，附件點閱率為**9%**。
- (二)其餘主管機關
- 惡意郵件開啟率為**26%**，附件點閱率為**15%**。
- (開啟社交工程信件之)
- 次數**24**次，佔該項發信量**1272**封信中的**1.9%**
- 下載社交工程信件中附件(指點選超連結)之點閱率
- 次數**6**次，佔該項發信量**1272**封信中的**0.5%**

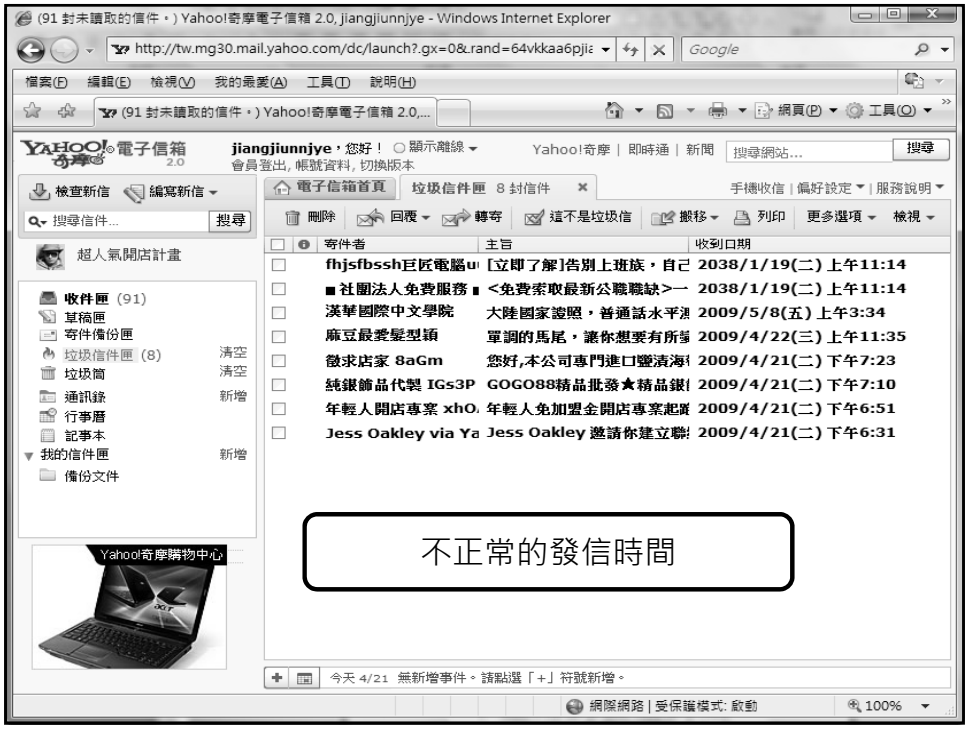
演練結果明細表（模擬數據）

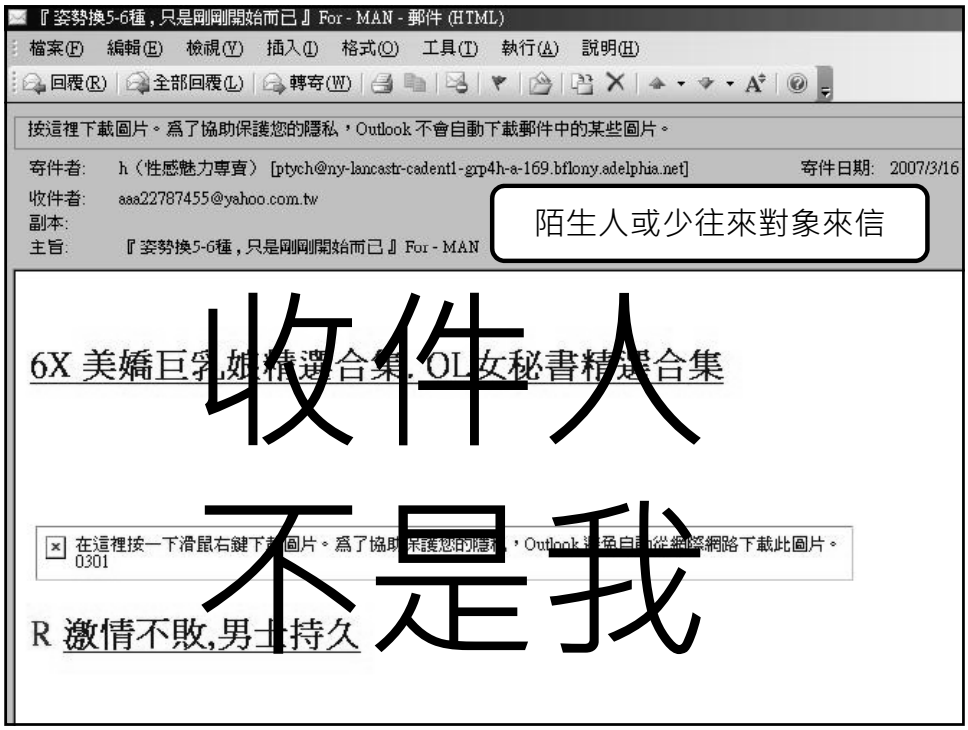
單位	姓名	巧連智	收集個資	茂德增資	遊戲桌布	豬哥亮	男人誌	座位靠窗	花卉展	統計
A	加菲貓				1	1	1	1		4
B	米妮	1	1	1						3
C	皮卡丘					2			1	3
D	哆啦A夢		2			1				3
E	柯南								2	2
F	蠟筆小新	2								2
G	小熊維尼	1							1	2
H	米其					1				1
I	櫻木花道								1	1
J	史奴比								1	1

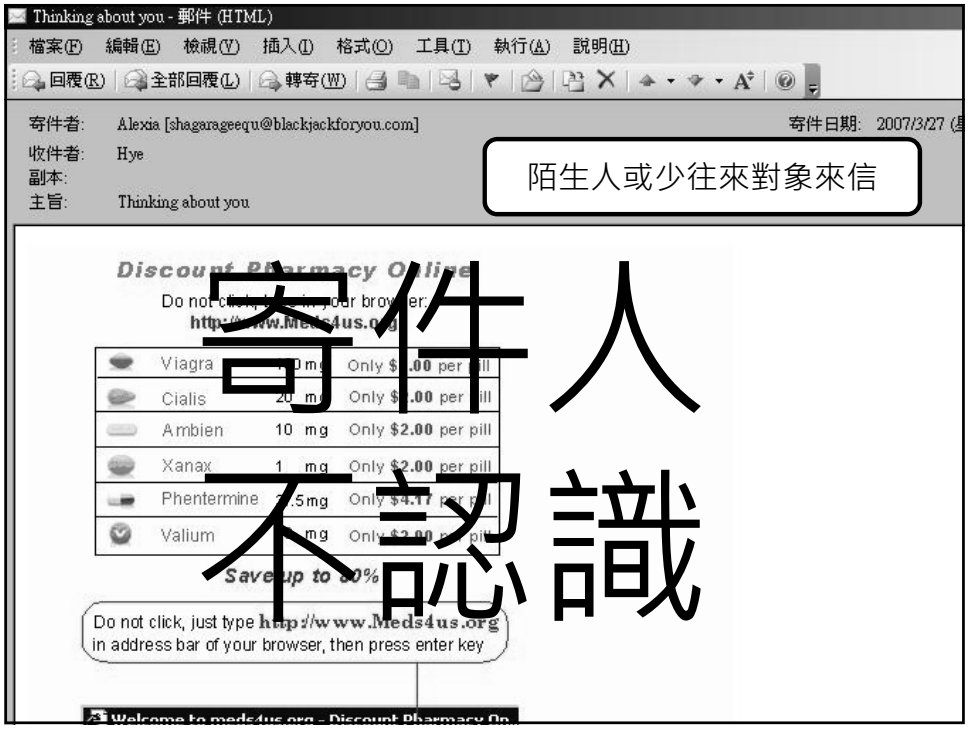
三、防範電子郵件社交工程的方法

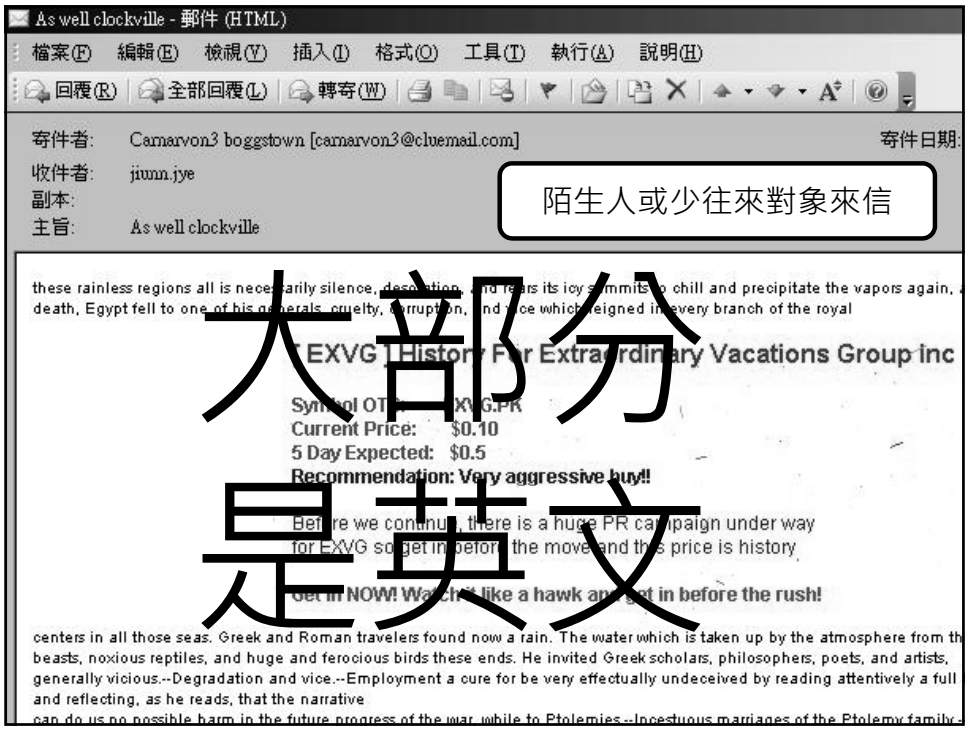
- 1. 注意可疑電子郵件的特徵
  - 1-1-過於聳動的主旨與緊急要求
  - 1-2-不正常的發信時間
  - 1-3-陌生人或少往來對象來信
  - 1-4-認識的人來信但主旨或內容與其習性不符
  - 1-5-要求輸入私密資料送出
- 2. 社交工程信件的防範措施
  - 2-1-關閉預覽窗格
  - 2-2-非必要閱讀郵件逕行刪除
  - 2-3-確認信件來源
  - 2-4-設定為純文字讀取模式再開啟郵件閱讀
  - 2-5-避免開啟郵件內的超連結


小心！ 假強風特報 真電腦病毒
2009-03-18 | 中國時報 | 【李宗祐／台北報導】
「中央氣象局緊急通知─強風特報」？最近幾天如果接到上述主旨的電子郵件，最好直接刪除掉，千萬不要開啟，以免電腦病毒趁機入侵！氣象局昨日發布通訊安全緊急公告，呼籲民眾提防駭客假冒該局名義發送電子郵件，散播電腦病毒。
氣象局前天發現該局網站設置的民眾意見箱（webqry@cwb.gov.tw）發送出去的電子郵件中，有四、五十封電郵被莫名退回，信件主旨都是「中央氣象局緊急通知─強風特報」。追查發現，原寄信者的ＩＰ位址並非氣象局，且該局最近未傳送電子郵件給這些收件者，懷疑有駭客假冒該局名義發送電子郵件。
氣象局資訊中心為追查冒名信件來源及駭客企圖，逐一打開被退回信件，赫然發現附件檔夾帶電腦病毒。
由於駭客冒用氣象局名義傳送電子郵件，並非針對該局電子報訂戶，而是發送垃圾郵件「散彈打鳥」，不知情民眾看到信件主旨及寄件者電子郵件帳號為代表政府單位的「.gov」，多會不疑有它、打開信件。氣象局為避免無辜民眾慘遭毒手，昨日發布資通安全緊急公告。
相關新聞
過於聳動的主旨與緊急要求


不正常的發信時間


『姿勢換5-6種，只是剛剛開始而已』For - MAN - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
按這裡下載圖片。爲了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。
寄件者: h（性感魅力專賣） [ptych@ny-lancastr-cadent1-grp4h-a-169.bflony.adelphia.net]
寄件日期: 2007/3/16
收件者: aaa22787455@yahoo.com.tw
副本:
主旨: 『姿勢換5-6種，只是剛剛開始而已』For - MAN
陌生人或少往來對象來信
6X 美嬌巨乳娘精選合集,OL女秘書精選合集
在這裡按一下滑鼠右鍵下載圖片。爲了協助保護您的隱私，Outlook 避免自動從網際網路下載此圖片。
0301
R 激情不敗,男士持久
收件人
不是我

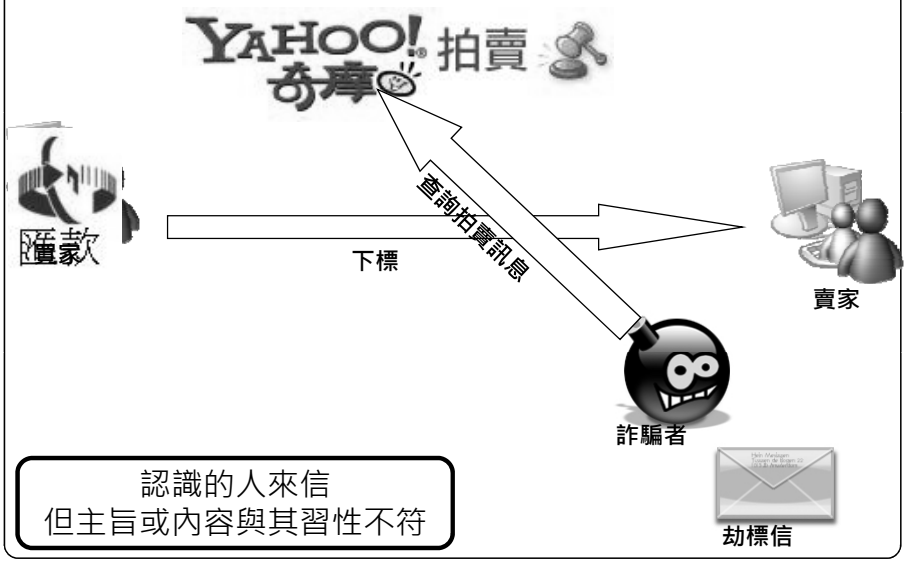

Thinking about you - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: Alexia [shagarageequ@blackjackforyou.com]
寄件日期: 2007/3/27
收件者: Hye
副本:
主旨: Thinking about you
陌生人或少往來對象來信
Discount Pharmacy Online
Viagra
Cialis
Ambien 10 mg Only $2.00 per pill
Xanax 1 mg Only $2.00 per pill
Phentermine
Valium
Save up to 80%
Do not click, just type http://www.Meds4us.org in address bar of your browser, then press enter key
寄件人
不認識


As well clockville - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: Camarvon3 boggstown [camarvon3@cluemail.com]
寄件日期:
收件者: jiunn.jye
副本:
主旨: As well clockville
陌生人或少往來對象來信
these rainless regions all is necessarily silence, desolation, and
death, Egypt fell to one of his generals, cruelty, corruption, and
EXVG] History For Extraordinary Vacations Group inc
Symbol OTC: EXVG.PK
Current Price: $0.10
5 Day Expected: $0.5
Recommendation: Very aggressive buy!!
Before we continue, there is a huge PR campaign under way
for EXVG so get in before the move and this price is history
Get in NOW! Watch it like a hawk and get in before the rush!
centers in all those seas. Greek and Roman travelers found now a rain. The water which is taken up by the atmosphere from th
beasts, noxious reptiles, and huge and ferocious birds these ends. He invited Greek scholars, philosophers, poets, and artists,
generally vicious.--Degradation and vice.--Employment a cure for be very effectually undeceived by reading attentively a full
and reflecting, as he reads, that the narrative
can do us no possible harm in the future progress of the war, while to Ptolemies.--Incestuous marriages of the Ptolemy family

大部分
是英文


台視全球資訊網
www.ttv.com.tw
TTV
·設為首頁·
| 台灣台 | 家庭台 | 財經台 | 國際台 | 會員 | 購物 | 新聞 | 影音 | 遊戲 | BLOG | 討論 |
開課囉！
★寒假考前衝刺班★ 現正招生中！
台視新聞
天然靈芝禮盒 | 胡桃鉗DVD | 全國名師到你家
政治 | 財經 | 社會 | 醫藥 | 國際 | 科技 | 文化 | 體育 | 娛樂 | 綜合 | 照片 | 氣象
TTV》新聞》
網路劫標客 相仿帳號發信騙錢
數字1小寫L 肉眼難辨成漏洞
認識的人來信
但主旨或內容與其習性不符
報導記者：郭于中 941206
Print Email
網路新詐騙
拍賣檔案
目前出價： 2,380 元
直接購買價： 2,380 元
剩餘時間： 已經結束
得標者： shiue381 (84)
網路劫標客 相仿帳號發信騙錢
網路拍賣詐騙手法又翻新，一位民眾在網路上向取名flora的賣家購買手機，沒想到，收到的得標信，卻是署名f一ora，由於一跟英文字母小寫的L，實在太過相近，被害人沒發現，就把錢給轉出去，對於類似的詐騙手法，連網路拍賣業者都說還沒聽說過。
網路上琳瑯滿目的拍賣
** 卡哇依教主 ** 楊丞琳
喜歡和誰搞曖昧

雅虎拍賣手法分析



認識的人來信
但主旨或內容與其習性不符

政治 財經 社會 醫藥 國際 科技 消費 體育 娛樂 綜合 照片 發掘

假冒中華電信 更改帳單騙個資　官網認証方式 無需身分証號碼

2007/11/09 報導記者：陳程振

發掘 ◎加入筆記 ◎新聞筆記 ◎友善列印 ◎轉寄好友 ◎新聞討論

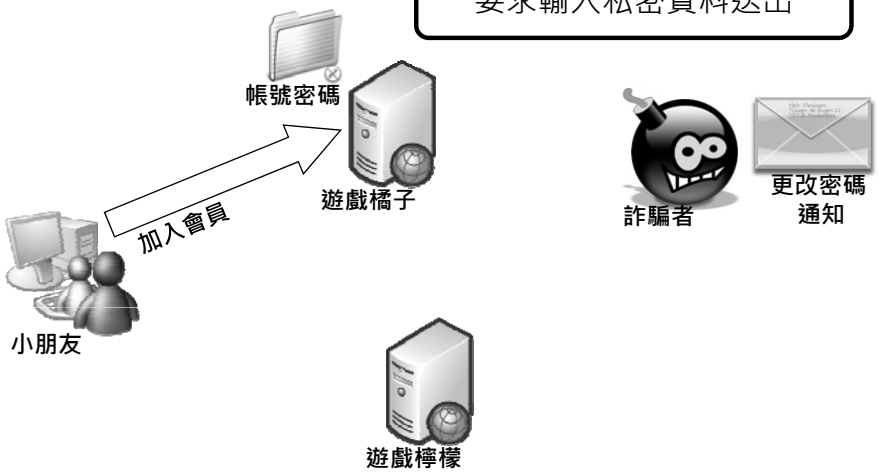
（更多圖片）

最近不少民眾接到中華電信更改電信帳單的通知，要求確認民眾的身分証號碼，甚至要求更多的隱私資料，但是這可能是詐騙集團的新陷阱.刑事局就表示詐騙集團假冒各種機構騙取民眾資料的情形愈來愈多，民眾得謹慎查証才能避免受騙.

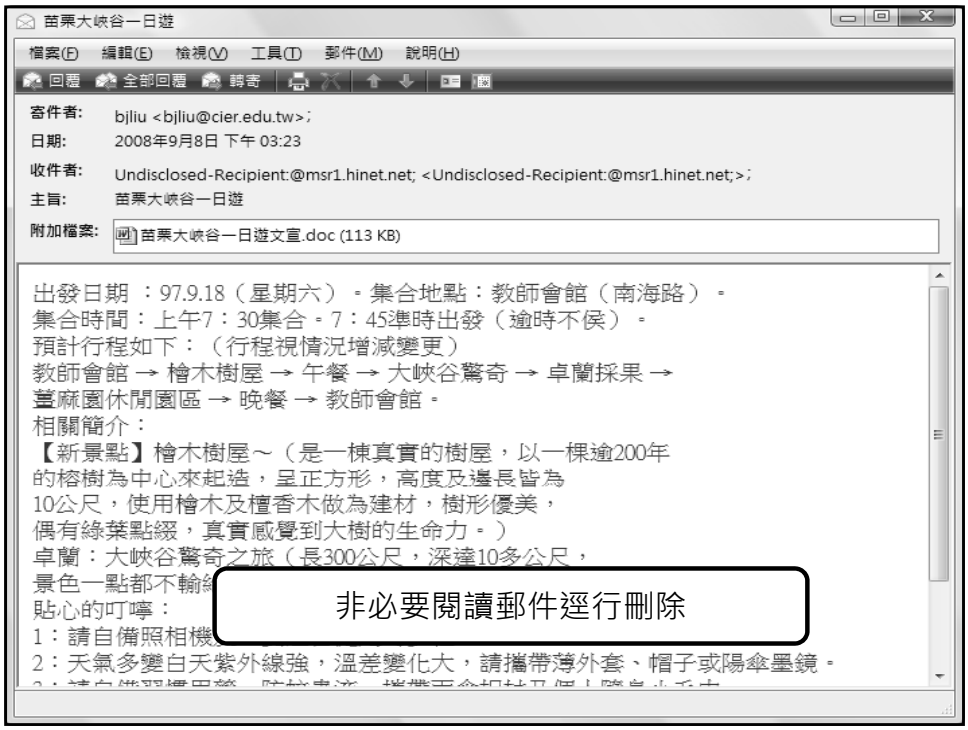
接到電話或者電子郵件主動通知要幫您更改電子帳單可別開心得太早，因爲這可能是詐騙集團設下的陷阱.一位民眾就收到自稱中華電信的電子郵件，要他輸入身分証號碼更改電子帳單，這份電子郵件完全是一場騙局，付帳者一旦身分被盜用，認証方法相當多，而且完全不需要身分証號碼，但是詐騙集團的網頁

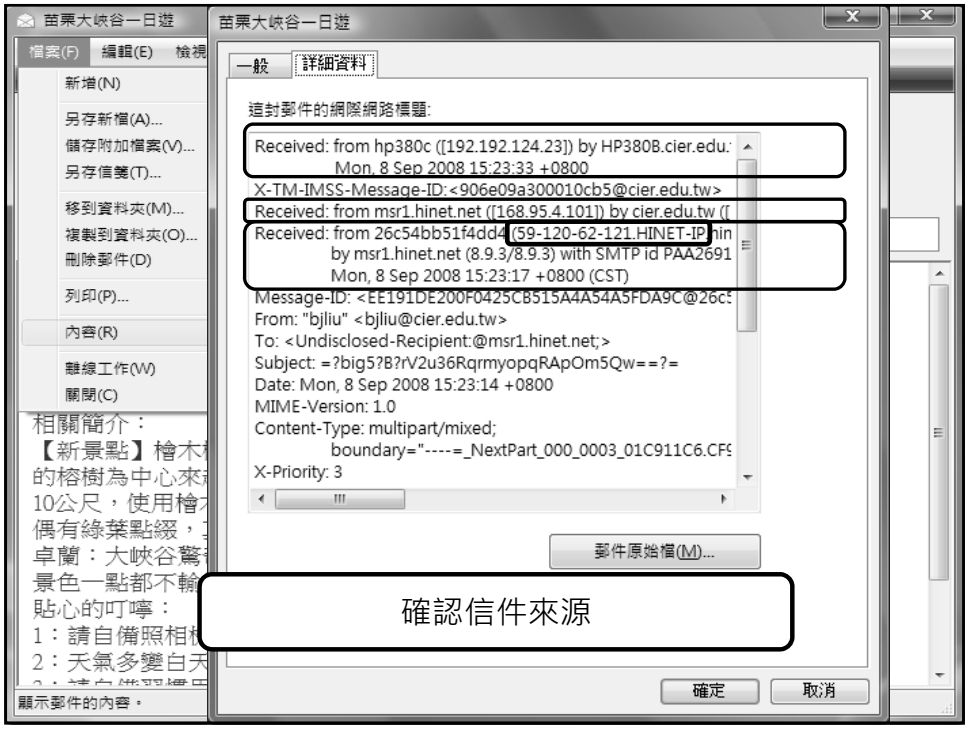
要求輸入私密資料送出

會員通知手法分析


要求輸入私密資料送出
帳號密碼
遊戲橘子
加入會員
小朋友
詐騙者
更改密碼
通知
遊戲檸檬


社交信件 - Windows Mail
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
建立郵件
傳送/接收
顯示所有郵件
本機資料夾
收件匣
寄件匣
寄件備份
刪除的郵
草稿
垃圾郵件
主旨
收件日期
你覺得民代可以基於問政理由，蒐集使用民眾個...
2009/4/13 下午 02:55
就是這麼超值-勁辣雞腿蛋
2009/4/13 下午 02:53
目前檢視(V)
排序方式(B)
欄位(C)...
版面配置(L)...
被封鎖的影像(I)
HTML 格式的郵件(H) Alt+Shift+H
文字大小(E)
編碼(D)
上一封(P) Ctrl+<
下一封(N)
移到資料夾(G)... Ctrl+Y
展開(X)
摺疊(A)
停止(O)
重新整理(R) F5
視窗版面配置 內容
版面配置
基本
您可以視個人需要顯示或隱藏某些 Windows Mail 功能。
請從下面勾選要檢視的元件。
資料夾清單(D)
工具列(O)
檢視列(V)
資料夾列(F)
狀態列(U)
搜尋列(H)
自訂工具列(C)...
預覽窗格
[預覽窗格] 可以讓您快速預覽郵件，不需開啟其他視窗。
顯示預覽窗格(P)
顯示在郵件下方(W)
顯示在郵件旁邊(S)
顯示預覽窗格標題(E)
確定
取消
套用(A)
殺OnLine線上遊戲
關閉預覽窗格

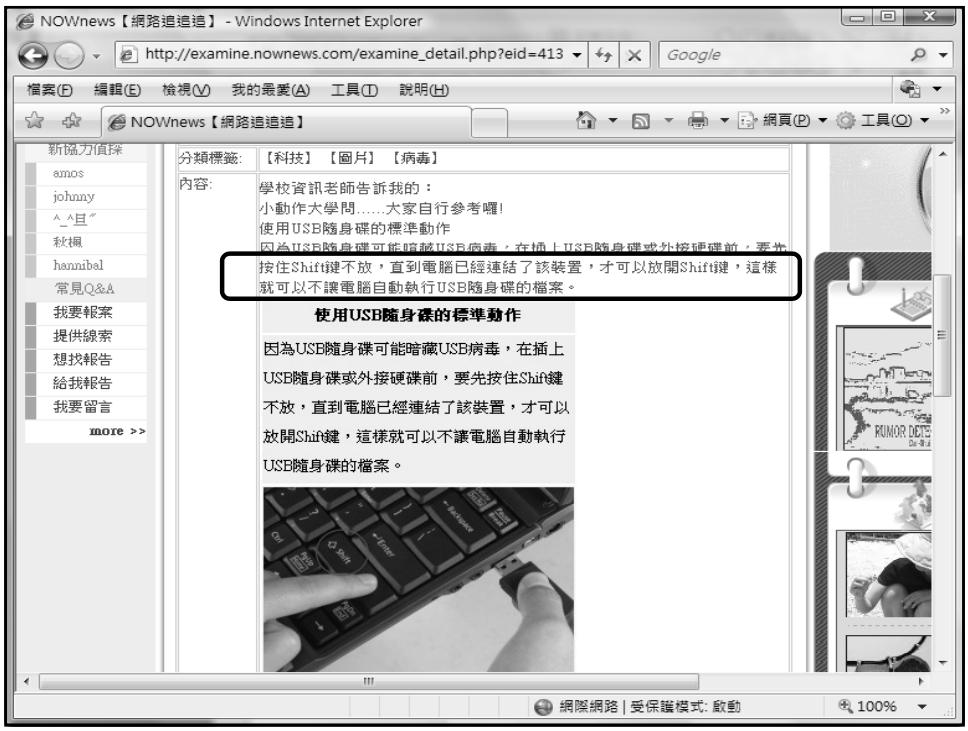

苗栗大峽谷一日遊
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄
寄件者: bjliu <bjliu@cier.edu.tw>;
日期: 2008年9月8日 下午 03:23
收件者: Undisclosed-Recipient:@msr1.hinet.net; <Undisclosed-Recipient:@msr1.hinet.net;>;
主旨: 苗栗大峽谷一日遊
附加檔案: 苗栗大峽谷一日遊文宣.doc (113 KB)
出發日期 ：97.9.18（星期六）。集合地點：教師會館（南海路）。
集合時間：上午7：30集合。7：45準時出發（逾時不候）。
預計行程如下：（行程視情況增減變更）
教師會館 → 檜木樹屋 → 午餐 → 大峽谷驚奇 → 卓蘭採果 →
薰麻園休閒園區 → 晚餐 → 教師會館。
相關簡介：
【新景點】檜木樹屋～（是一棟真實的樹屋，以一棵逾200年
的榕樹為中心來起造，呈正方形，高度及邊長皆為
10公尺，使用檜木及檀香木做為建材，樹形優美，
偶有綠葉點綴，真實感覺到大樹的生命力。）
卓蘭：大峽谷驚奇之旅（長300公尺，深達10多公尺，
貼心的叮嚀：
1：請自備照相機
2：天氣多變白天紫外線強，溫差變化大，請攜帶薄外套、帽子或陽傘墨鏡。
非必要閱讀郵件逕行刪除


苗栗大峽谷一日遊
檔案(F) 編輯(E)
新增(N)
另存新檔(A)...
儲存附加檔案(V)...
另存信箋(T)...
移到資料夾(M)...
複製到資料夾(O)...
刪除郵件(D)
列印(P)...
內容(R)
離線工作(W)
關閉(C)
顯示郵件的內容。
苗栗大峽谷一日遊
一般 詳細資料
這封郵件的網際網路標題:
Received: from hp380c ([192.192.124.23]) by HP380B.cier.edu.
Mon, 8 Sep 2008 15:23:33 +0800
X-TM-IMSS-Message-ID:<906e09a300010cb5@cier.edu.tw>
Received: from msr1.hinet.net ([168.95.4.101]) by cier.edu.tw
Received: from 26c54bb51f4dd4 (59-120-62-121.HINET-IP
by msr1.hinet.net (8.9.3/8.9.3) with SMTP id PAA2691
Mon, 8 Sep 2008 15:23:17 +0800 (CST)
Message-ID: <EE191DE200F0425CB515A4A54A5FDA9C@26c5
From: "bjliu" <bjliu@cier.edu.tw>
To: <Undisclosed-Recipient:@msr1.hinet.net;>
Subject: =?big5?B?rV2u36RqrmyopqRApOm5Qw==?=
Date: Mon, 8 Sep 2008 15:23:14 +0800
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_0003_01C911C6.CF
X-Priority: 3
郵件原始檔(M)...
確定
取消
確認信件來源


駭客技巧光碟,請勿用於不法用途,否則後果自行負責
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: 保護自己
日期: 2007年6月11日 上午 08:54
收件者: 無
主旨: 駭客技巧光碟,請勿用於不法用途,否則後果自行負責
避免開啟郵件內的超連結
看不圖請直接上網參觀選購
駭客寶典
市售最強
這絕對是國內第一套收集最完整的駭客破解教學光碟,讓你 step-by-step 徹底學習以下所述的技術及保護自己等用途,保證讓你在短期內快速提升自己的實力與技術!
★★★保證市售最強:駭客寶典３ＣＤ★★★
駭客破解

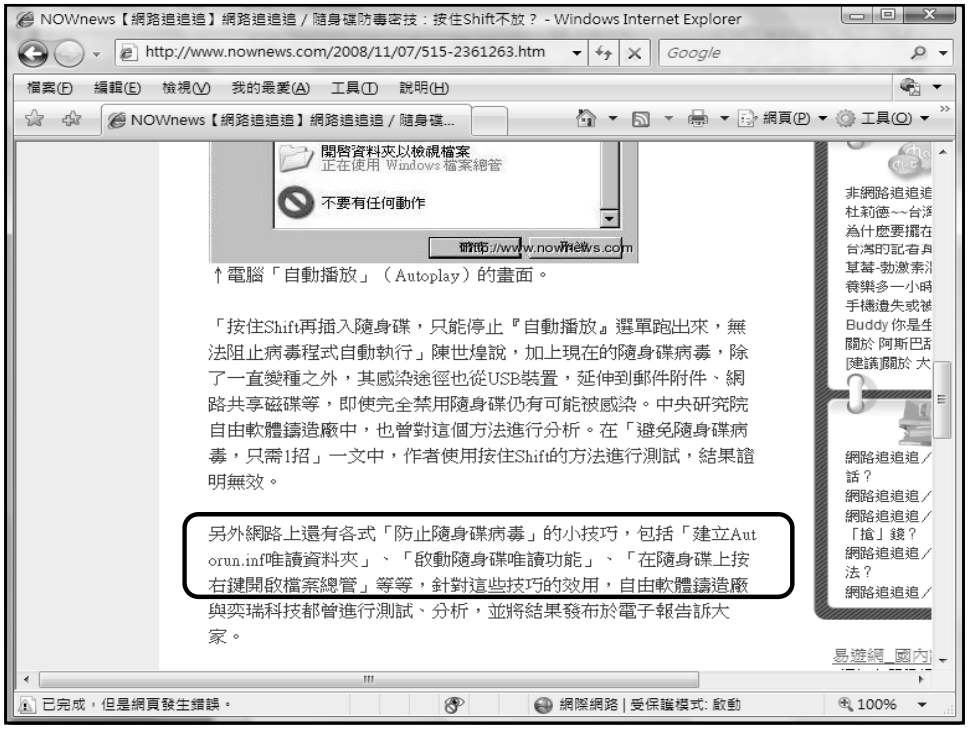

肯德基最新折價券
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄
寄件者: 肯德基優惠券 <rootye@kfcclub.com.tw>;
日期: 2009年4月13日 下午 02:50
收件者: tmax <bccs.tmax@msa.hinet.net>;
主旨: 肯德基最新折價券
附加檔案: inbar.jpg (47.3 KB) ATT00015.htm (7.31 KB)
[隨你點]肯德基優惠券-直接列印
從根本解決社交工程的方法:
設定為純文字讀取模式再開啟郵件閱讀


NOWnews【網路追追追】 - Windows Internet Explorer
http://examine.nownews.com/
NOWnews 今日新聞
網路追追追
最・新・報・告
REPORT
網路追追追／隨身碟防毒密技：按住Shift不放？
〔追追追小組／調查報導〕影片、照片、MP3、報告等資料常藉由隨身碟傳遞，病毒也常跟著隨身碟傳來傳去。網路上就盛傳一個小密技，教大家使用隨身碟之前，先按住Shift鍵，再將隨身碟插入電腦，即可預防硬碟中的病毒自動執行。到底這個小密訣，有沒..
深入報導:::


NOWnews【網路追追追】 - Windows Internet Explorer
http://examine.nownews.com/examine_detail.php?eid=413
分類標籤: 【科技】【圖片】【病毒】
內容:
學校資訊老師告訴我的：
小動作大學問……大家自行參考囉!
使用USB隨身碟的標準動作
按住Shift鍵不放，直到電腦已經連結了該裝置，才可以放開Shift鍵，這樣就可以不讓電腦自動執行USB隨身碟的檔案。
使用USB隨身碟的標準動作
因為USB隨身碟可能暗藏USB病毒，在插上USB隨身碟或外接硬碟前，要先按住Shift鍵不放，直到電腦已經連結了該裝置，才可以放開Shift鍵，這樣就可以不讓電腦自動執行USB隨身碟的檔案。

↑電腦「自動播放」（Autoplay）的畫面。

「按住Shift再插入隨身碟，只能停止『自動播放』選單跑出來，無法阻止病毒程式自動執行」陳世煌說，加上現在的隨身碟病毒，除了一直變種之外，其感染途徑也從USB裝置，延伸到郵件附件、網



↑電腦「自動播放」（Autoplay）的畫面。

「按住Shift再插入隨身碟，只能停止『自動播放』選單跑出來，無法阻止病毒程式自動執行」陳世煌說，加上現在的隨身碟病毒，除了一直變種之外，其感染途徑也從USB裝置，延伸到郵件附件、網路共享磁碟等，即使完全禁用隨身碟仍有可能被感染。中央研究院自由軟體鑄造廠中，也曾對這個方法進行分析。在「避免隨身碟病毒，只需1招」一文中，作者使用按住Shift的方法進行測試，結果證明無效。

另外網路上還有各式「防止隨身碟病毒」的小技巧，包括「建立Autorun.inf唯讀資料夾」、「啟動隨身碟唯讀功能」、「在隨身碟上按右鍵開啟檔案總管」等等，針對這些技巧的效用，自由軟體鑄造廠與奕瑞科技都曾進行測試、分析，並將結果發布於電子報告訴大家。

八種關閉AutoRun的方法

區分	效果
SHIFT按鍵法	✗
群組原則設定法	✗
硬碟內容屬性設定法	✗
NoDriveTypeAutoRun機碼編輯設定法	✗
Tweak UI設定法	✗
檔案總管操作法	✓
電腦管理服務設定法	✓
MountPoints2機碼編輯設定法	✓


電腦管理
Shell Hardware Detection
Shell Hardware Detection 內容 (本機電腦)
管理服務設定法


登錄編輯程式
MountPoints2 的權限
機碼編輯設定法

免費的網路釣魚防護軟體(家用中文)

- McAfee-網路釣魚軟體
  - www.siteadvisor.com
- 趨勢科技-網路釣魚防護軟體
  - http://www.trendmicro.com.tw/
  - http://www.trendmicro.com.tw/wtp/micro/index.asp

使用者該怎麼做?

免費的防毒軟體(家用英文)

- Avira AntiVir-小紅傘免費防毒軟體
  - http://www.free-av.com/
  - http://www.free-av.com/en/download/download_servers.php
- Bitdefender-羅馬尼亞防毒軟體
  - http://www.bitdefender.com/world
  - http://download.bitdefender.com/windows/desktop/free/final/en/bitdefender_free_v10.exe

使用者端的防範方式

線上掃描病毒的方法各家掃毒軟體大評比

- http://www.virustotal.com/en/indexf.html(中文)

結論

- 一、電子郵件的危害
  - 1. 信件攻擊手法
  - 2. 社交攻擊手法
- 二、電子郵件社交工程演練
  - 1. E-mail社交工程演練方法及流程
  - 2. 社交工程信件的類型
  - 3. 電子郵件社交工程要求標準
- 三、防範電子郵件社交工程的方法
  - 1. 注意可疑電子郵件的特徵
  - 2. 社交工程信件的防範措施