網路攻防戰 之
實務案例分析
個資防護篇

資安顧問 呂守箴

大綱

- 上網的個資防護
  - 網路相簿
  - 網路購物
  - 網路搜尋
- 電子郵件社交工程的個資防護
  - 傳送郵件的考量
  - 接收郵件的考量
  - WebMail的傳送與接收
- 網路使用的個資防護
  - 即時通訊軟體
  - P2P軟體
  - USB隨身碟
  - 軟體修補
  - 清除、救援、銷毀個人資料

上網的個資防護

網路相簿
網路購物
網路搜尋

網路相簿

- **上古時代：**
- 相片是沖洗出來放在相本裡收集，老的時候一頁一頁翻出來看。

- **中古時代：**
- 相片是用彩色噴墨、相片印表機印出來，將四周圍貼滿自己的得意作品隨時看。

- **網路現代：**
- 相片是用手機、數位相機拍好後直接放上網路，迫不及待想跟認識的及不認識的人分享，自己看還不夠，深怕別人看不到。

網路相簿

- 知名相簿網站：

- 無名小站 (www.wretch.cc)
- 痞客邦 (www.pixnet.net)
- Xuite (www.xuite.net)
- yam天空部落相簿 (blog.yam.com)
- 網路家庭相簿 (photo.pchome.com.tw)
- Flickr相片分享 (www.flickr.com)

網路相簿

- 可是？
- 將相片放在網路上就安全嗎？

- 基本防護設定：
- 我有設定「禁止按右鍵」另存照片。
- 我有設定「相簿鎖密碼」過濾訪客。

- 這樣應該就安全了吧！

網路相簿

- 雖然「禁止按右鍵」無法另存照片，但是可以利用「抓檔軟體」，遠端下載。

網路相簿

- 那使用「相簿鎖密碼」過濾來訪客，沒有密碼就無法看圖呢？

- 重點是？
- 你確定你的密碼設定的很完善？
- 不會被有心人士隨便猜一猜就猜到？
- 或者只要使用網路通通都設相同的密碼？

最常見也危險的密碼：123456

Awakening台灣醒報 更新日期：2009/10/10 01:42　李柏勳

【台灣醒報特約記者李柏勳報導】網路時代來臨，動不動就要設密碼。一看，「密碼最少六個字」，隨手就打123456？小心，不只你這麼想，大家都這麼想，連駭客也這麼想！專家呼籲最好每隔90天就更換一次密碼。

日前傳出，有超過一萬筆

密碼設定的相關事項

- 需包含英文大小寫、數字及符號。
- 密碼需要 7~8 個字以上。
- 不可以另外寫下　或　存在電腦檔案裏。

密碼背不起來怎麼辦？

- 用鍵盤上　注音符號　的位置。
- Xm3　　g.3　　5p

- 不會注音符號？
- 發音不正確導致密碼輸錯？
- 改用其他輸入法(倉頡、大易)等
- 測試密碼強度：www.passwordmeter.com

- 當然使用「自己的姓名」當密碼，是個『不好的建議』。
- 比較正確的方法是用：
- 古詩，例如：五言絕句

- 某個自己記得起來的語彙，例如：
- 1 9 6 b 4 u g 0 r u p 4

陳冠希：以為檔案移到回收筒就是刪除了 沒想到還要清理

中廣新聞網 更新日期：2009/02/24 18:35

因爲不雅照片事件被散佈而掀起軒然大波的香港藝人陳冠希，控告電腦工程師非法竊取他電腦資料的官司，星期一在加拿大溫哥華開庭；陳冠希在庭上，除了透露有一部分艷照，是當事女性自己拍攝送給他欣賞，不是他拍的之外，也表示他以爲把檔案放到資源回收筒，就等於刪除了檔案，言下之意，就是他似乎不知道要完全刪除檔案，還需要在資源回收筒中再做一道清理的手續，也因此給了竊取照片者機會。

據香港明報報導，陳冠希在庭上表示，在網路流傳的相片中，有些是女性自行拍攝的，有些是他自拍的，但不管是誰拍的，這些相片都是在未經強迫，而且是在雙方都知情，而且同意的情況下拍攝的，而且這些照片是非常私人的。

正常使用：

- 搶救硬碟內誤刪資料。
- 搶救隨身碟內的誤刪資料。
- 搶救記憶卡內的誤刪資料。

異常使用：

- 竊取硬碟內誤刪資料。 (維修時？)
- 竊取隨身碟內的誤刪資料。 (COPY資料時？)
- 竊取記憶卡內的誤刪資料。 (沖洗照片時？)

網路相簿的注意事項

- 不要上傳太私密的照片。
- 相簿要記得鎖密碼。(英文大小寫、數字、特殊符號)
- 不要在網路相簿網站留下太多個人資料。
- 想要上傳照片就要知道會有被他人下載及流傳的風險。
- 網路相簿也不是無限空間，免費服務能放的照片有限，通常會要求付費才會有更大空間及其它服務。
- 就算照片放在硬碟內也是一樣，當電腦維修時，同時就是資料外洩的最好時機。

網路購物

- 網路購物有二大風險：
- 購物網站本身：
  - 購物網站管理不當(產生漏洞、植入木馬)
  - 購物程式設計不當(產生被人入侵的管道)
  - 購物的流程管理不當(經手訂單的員工、廠商疏失)

- 消費者本身：
  - 電腦本身遭受感染木馬被竊取
  - 每個網站均使用同一組帳號及密碼而洩漏
  - 誤入假的購物網站遭騙
  - 於網拍貪小便宜匯款卻收不到商品

網路購物的注意事項

- 購物網站端：
- 做好網站及程式設計的安全控管。
- 落實客戶資料的保護。

- 使用者端：
- 定期更改密碼。
- 多留意購物網站的公告及新聞。
- 做任何金融交易前，請先確認所使用的電腦當時環境是[乾淨且無毒]的。
- 確認該[購物網站]網站是正確的。
- 定期更新防毒軟體的病毒碼並搭配線上掃毒。

網路搜尋

- 網路搜尋的惡意手法有二：
- 利用「特殊語法」取得隱藏資訊(Google Hacking)
  - 成功後，利用該資訊取得個人資料，或不公開的文件。
- 利用「關鍵字廣告」連結惡意網頁
  - 成功後，利用該惡意網頁植入木馬後竊取個人資料。

如何防止 Google Hacking

- 在網站伺服器上的根目錄，增加一個 robots.txt 檔案。
- 然後在這個檔案中加入「User-agent: allow: Disallow:」這參數進行設定，一般來說都可以阻止有道德的搜尋引擎程式讀取並儲存您的網頁。
- 例如：
- User-agent:Googlebot
  Disallow:/*.*

網路搜尋的注意事項

- 點選搜尋引擎所提供的連結之前，請先注意該連結的網址是否正確。
- 盡量不要使用「不具有惡意連結提醒」的搜尋引擎。
- 可行的話封鎖來自於「中國」的網址。
- 就算真的感染只要防毒軟體與修補程式有更新，至少可以有一定程度的防護。

上網重點項目

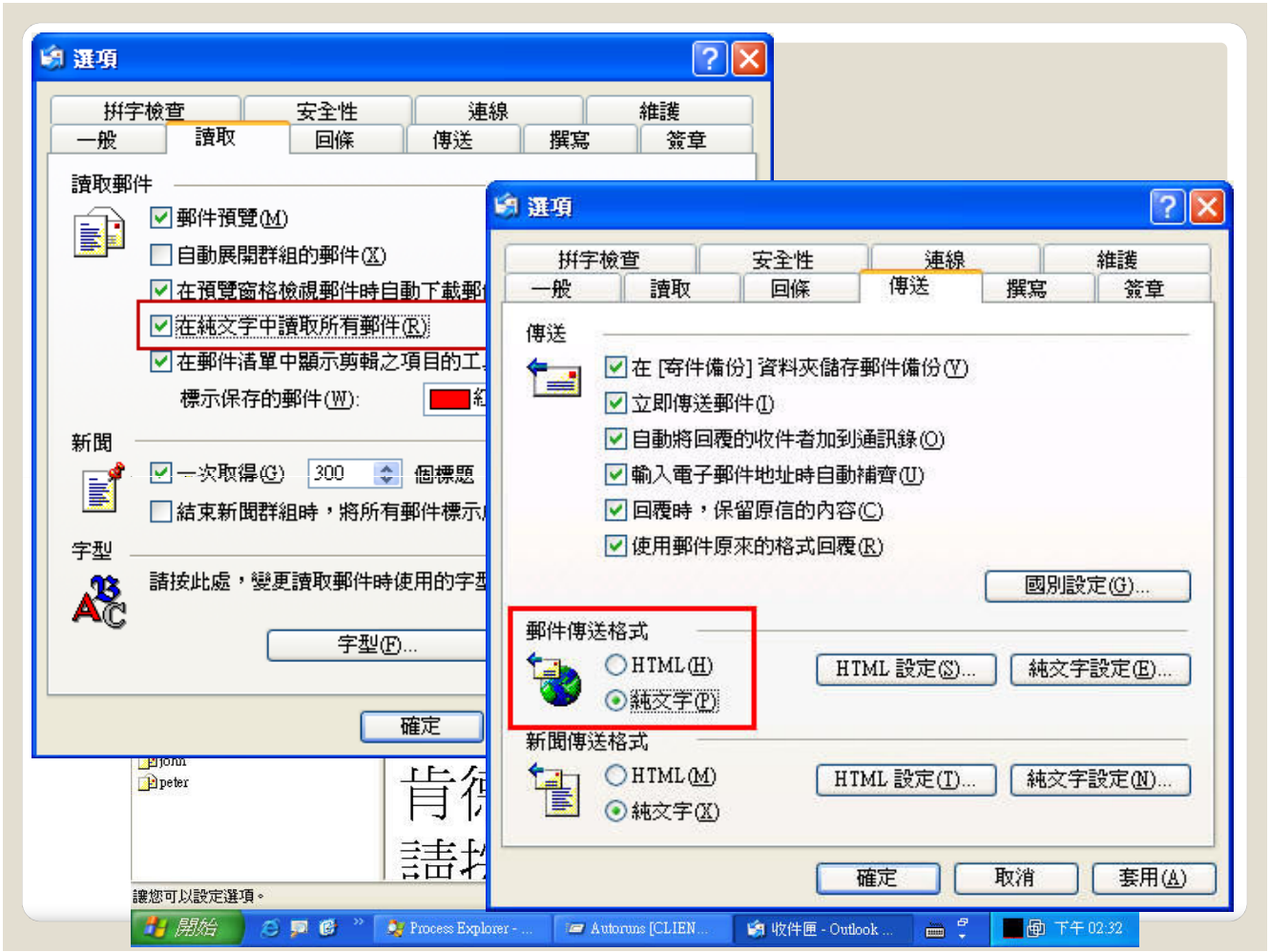
- 請勿上傳不適合公開的照片。
- 請勿點選看似好康的「超連結」。
- 做任何網路購物交易前，請記得再掃毒一次確保電腦在無毒的狀態。
- 防毒軟體不要只是有安裝，卻從來沒有全機掃毒過。

電子郵件社交工程的個資防護

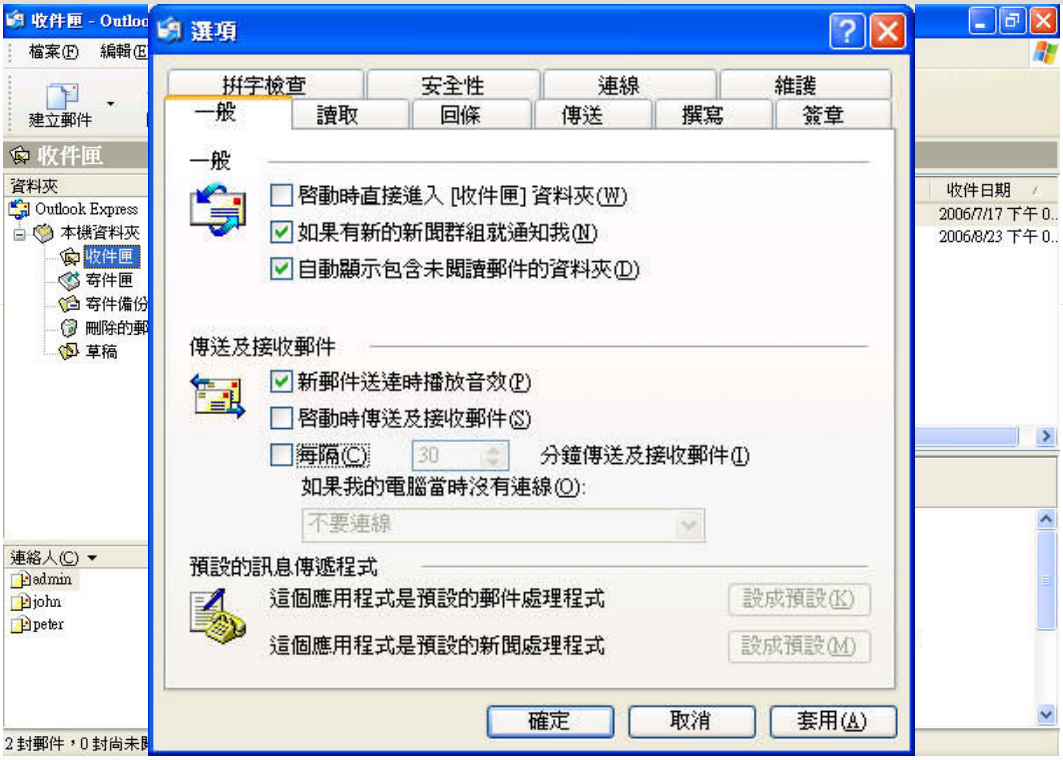
傳送郵件的考量
接收郵件的考量
WebMail的傳送與接收

傳送郵件的考量

- 可行的話將郵件傳送格式從「HTML」格式改用「純文字 txt」格式。(工具→選項→讀取 及 傳送)
- 關閉「啟動時傳送及接收郵件」、「每隔幾分鐘傳送及接收郵件」的功能。
- 公務用 (xxx@mail.xyz.gov.tw) 與 個人E-Mail (xxx@yahoo.com)信箱請 分開使用
- 搭配「自然人憑證」確認身份。
- 寄件人改用「密件副本」。
- 在通訊錄加上「！0000」這個收件人防止病毒寄送？ (道高一尺、魔高一丈。這已經沒效了。)



關閉「啟動時傳送及接收郵件」



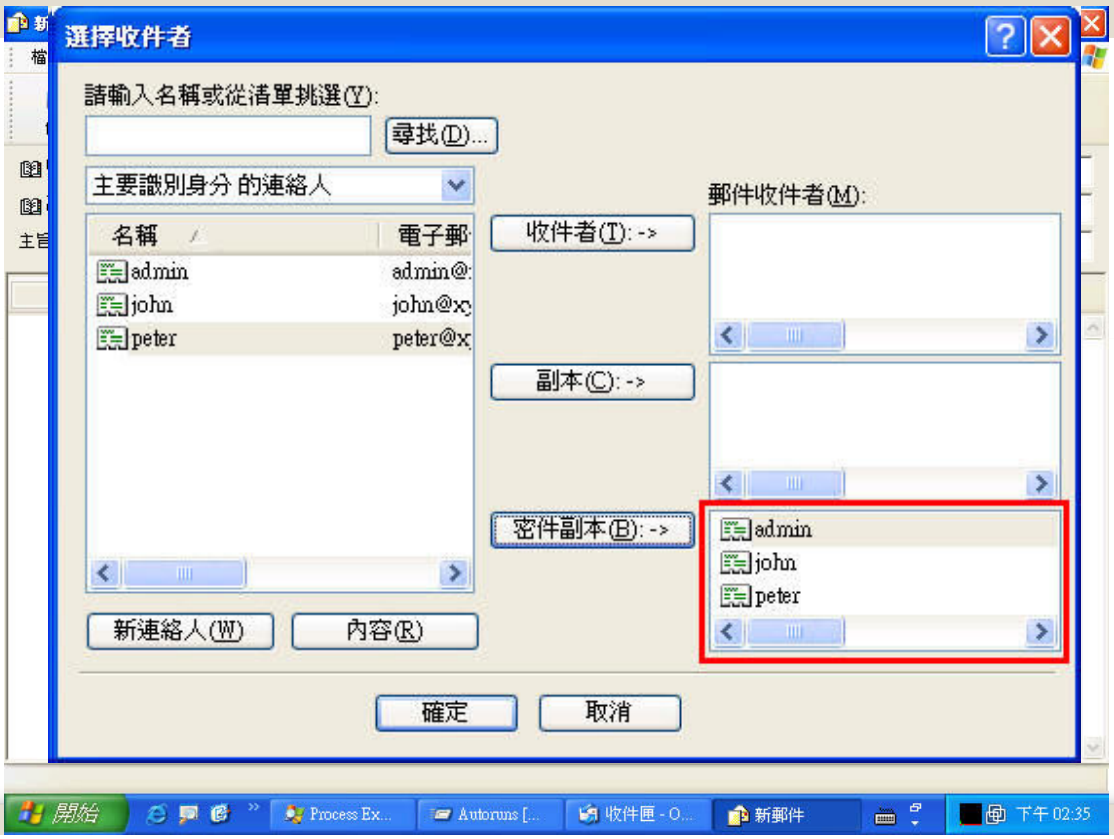
自然人憑證

- 「自然人憑證」是可以在網路上作資料交換時，如同網路身分證辨識雙方身分。
- 自然人憑證包含了「數位簽章」跟「公開金鑰」。
- 使用自然人憑證的好處：
- 在網路上可辨識每個人的身分。
- 在網路加密後上傳資料可確認資料正確性。

自然人憑證相關資料

- 內政部憑證管理中心 (http://moica.nat.gov.tw)
- 相關檔案下載 (http://moica.nat.gov.tw/html/download_1.htm)
- 保密郵件暨應用說明操作手冊 (http://moica.nat.gov.tw/html/faq6-023-033.htm)
- 安全電子郵件介紹 (http://61.57.42.3/upload/PL93EG05A17/online/LRNViewer.htm)

密件副本



接收郵件的考量

- 垃圾郵件、匿名郵件及偽造郵件攻擊
- 關閉郵件預覽功能
- 落實郵件附件檔掃毒

垃圾郵件、匿名郵件及偽造郵件攻擊

- 利用匿名郵件　　(例如：要求回信)
- 利用好康郵件　　(例如：程式下載、中獎)
- 利用連鎖信　　(例如：佛像郵件)
- 利用尋人郵件　　(例如：尋找失蹤兒)
- 利用愛心郵件　　(例如：骨髓配對、勵志小故事)
- 利用銀行郵件
- 利用廣告郵件　　(例如：折價卷)
- 利用情色郵件

郵件附件檔

- 將附件檔「另存新檔」後掃描病毒，不可以直接點選2下打開。
- 修補「Microsoft Office」、「Adobe Reader」等的相關讀取程式的弱點。
- 如果不確定所收到的檔案是否有問題，使用「可疑檔案上傳分析」確認。

可疑檔案上傳分析：

- 利用各家防毒軟毒軟體的掃描引擎，同時對單一一個檔案，作是否為病毒、木馬檔案的分析可協助檢測確認檔案本身是否異常。

- VirusTotal：免費線上病毒和惡意軟體掃瞄
- http://www.virustotal.com/zh-tw/

- VirSCAN.org：線上防毒引擎掃描網站 v1.00 目前支援 36 款防毒引擎
- http://www.virscan.org/

- Online malware scan
- http://virusscan.jotti.org/

WebMail的傳送與接收

- WebMail的使用原則，跟本機Mail的注意事項也是一樣的。
- 但WebMail更需要注意「預覽視窗」以及「超連結」的點選。
- 雖然WebMail的附件檔並沒有收下來，但若不注意仍有可能發生點選到有毒附件檔。
- WebMail更需要經常「變更密碼」，來避免被他人竊取。
- 盡量避免在他人或公用電腦中使用WebMail，有可能該電腦已經中毒。如果一定要用，使用前先掃毒、離開前請『登出』並要「清除瀏覽器的Cookie」，避免帳號密碼被記住。

電子郵件重點項目

- 請勿開啟及預覽任何人所寄來的匿名、垃圾郵件。
- 就算是開啟了也請勿點選「超連結」。
- 開啟任何郵件的附件檔前，請記得「另存新檔」掃毒後再開啟。

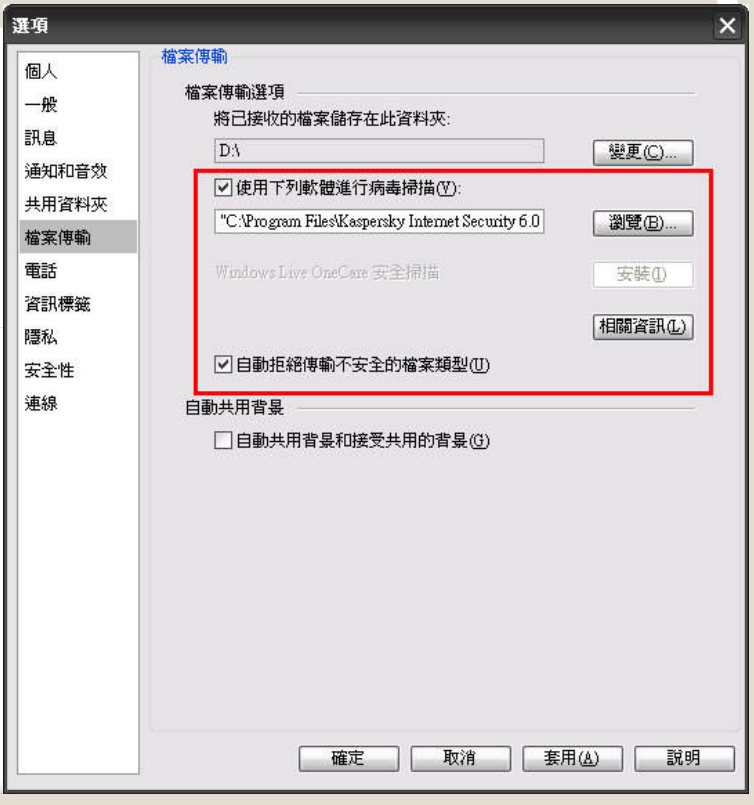
網路使用的個資防護

即時通訊軟體
P2P軟體
USB隨身碟
軟體修補
清除、救援、銷毀個人資料

即時通訊軟體

- 使用即時通訊到底會不會中毒？

- 會。不過，不是及時通訊軟體本身中毒，而是傳送「惡意超連結」、「傳輸病毒檔案」而造成。



即時通訊軟體

- 所以我只要不點選連結及檔案，是不是使用上就沒有問題？

- 不是。因為聊天過程中所輸入的文字，因為沒有加密功能，所以你在聊天過程中只要在「相同的網路區段環境(例如：家庭、宿舍、速食店、咖啡廳)」是可以被「側錄或監看」的。

即時通訊軟體：訊息加密程式

- MSN 訊息加密程式
- 程式名稱：MSN Shell
- 下載網址：http://my.msnshell.com
- 程式名稱：SimpLite for MSN Messenger
- 下載網址：http://www.secway.fr/us/products/simplite_msn/getsimp.php

- Yahoo訊息加密程式
- 程式名稱：SimpLite for Yahoo! Messenger
- 下載網址：http://www.secway.fr/us/products/simplite_yahoo/getsimp.php

- 註：以上這些軟體僅適用裝在家用電腦，不適合裝在「辦公室」的環境中。

即時通訊軟體的注意事項

- 最好不使用，如果要使用請記得：
  - 不要隨便接收檔案
  - 不要隨便點選網址
  - 注意訊息傳輸的加密
  - 以及落實掃毒的程序

- 即時通訊軟體也需要經常更新，來避免遭受攻擊。

- MSN更新： http://get.live.com/zh-cht-tw/messenger/overview
- 即時通更新： http://tw.messenger.yahoo.com
- Google Talk更新： http://www.google.com/talk/intl/zh-TW

P2P軟體

- P2P軟體下載已經漸漸取代傳統FTP檔案功能，使得一些地下管道，在頻寬不夠之下漸漸採用點對點分享。(一般稱呼使用P2P下載稱為「養動物」)

- 常用軟體名稱：電驢(eMule)、BT、FOXY

- 為什麼P2P軟體大家都要「禁用」？
- P2P技術現在被濫用於下載有版權的音樂、影片、程式等，做為非法的網路傳輸。且這些經不當管道取得的檔案，對內常發現挾帶病毒與木馬程式、對外常因使用者設定不正確「被動外洩個資與機密文件」。

為何Foxy它那麼熱門？

- 比起BT要去找資源檔、eMule要找伺服器來的快速且方便，適合對電腦網路都不是很了解的「初學者」。
- 變相的搜尋引擎，尤其是想找到「見光死」的影片、軟體等所謂的好東西。
- 只要頻寬夠大幾乎沒有甚麼東西是下載不下來的，比起BT會斷種、eMule會斷頭來的有效。

- 經歷了「警局筆錄洩漏」、「軍方演習報告洩漏」、「報稅資料洩漏」等事件後新聞媒體的炒作，使得不知道的人也通通都知道了這個「致命的小東西」。

P2P軟體的注意事項

- 辦公室電腦：禁用。
- 家用電腦：最好不使用、不使用、不使用，是最保險的方法。
- 如果不小心使用請記得：
  - 請設定好分享的目錄(上傳區跟下載區)。
  - 請設定好分享的權限。
  - 請設定好分享的網路頻寬。
  - 每個下載檔案(音樂、影片、檔案等)均要掃毒後才開啟。

- P2P軟體也需要經常更新，來避免遭受攻擊。

USB隨身碟使用注意事項

- 隨意將由「網路上下載」或「郵件的附件檔」COPY至隨身碟(大拇哥)中，易造成辦公場所與家用電腦『交互感染病毒與木馬程式』。
- 請搭配防毒軟體掃描隨身碟內的檔案。

防制USB病毒的有效的方法

- 打開原本防毒軟體掃描USB的功能或插入後先掃毒
- 由於USB病毒變種快又多，請勤更新病毒碼
- 插入USB進入電腦請多留意是否有隱藏檔案
- 一但中毒除原來防毒軟體外可搭配USB病毒移除工具。
- 天啊！我的隨身碟又中毒了
- http://anti-hacker.blogspot.com/2008/02/ithome.html
- USB隨身碟病毒刪除法
- http://anti-hacker.blogspot.com/2007/11/usb.html

軟體修補

- Windows Update (僅更新作業系統本身的漏洞)
- Microsoft Update (會更新Office及所有微軟產品)
- IE 7
- XP SP3
- Adobe Reader
- 壓縮軟體
- 音樂播放軟體

Service Pack

- Microsoft 發行 Windows XP /Vista 的更新程式，其中會包含在這5年中發行的所有修正程式和增強功能。這些更新程式 (稱為 Service Pack) 提供了方便、全部合一的方式，以存取最新的驅動程式、工具、安全性更新程式、修補程式以及客戶要求的產品變更等。

- 官方下載 光碟 ISO檔：
- Windows XP SP3
- http://www.microsoft.com/downloads/details.aspx?FamilyID=2fcde6ce-b5fb-4488-8c50-fe22559d164e&DisplayLang=zh-tw

- Windows Vista SP2
- http://www.microsoft.com/downloads/details.aspx?familyid=F25F9C49-1A3A-4336-ADE6-32E34A448608&displaylang=zh-tw

Adobe Reader

- Adobe Reader 軟體是電子文件分享的全球標準。這是唯一可開啟所有 PDF 文件並與之互動的 PDF 檢視器。 使用 Adobe Reader 對 Adobe PDF 檔案進行檢視、搜尋、加上數位簽名、驗證、列印和協同作業。

- 官方下載：
- http://get.adobe.com/tw/reader/

- 更新：
- 在Adobe Reader點選→說明→現在檢查更新

軟體修補的注意事項

- 除了使用「Windows Update」更新作業系統的漏洞外，也需要利用「Microsoft Update」更新Office等應用程式的漏洞。

- 可以使用「XPSP3」一次修補到近期的修正程式，但之後還是仍要Update。

- 常使用的軟體例如：Adobe Reader、壓縮軟體、音樂播放軟體等也需要更新。

清除、救援、銷毀個人資料

- 手工清除個人資料
- CCleaner 資料清除軟體
- Recuva 檔案救援軟體
- File Shredder 檔案銷毀軟體

手工清除：IE 的上網暫存資料

- 定期刪除 Cookies
- 定期刪除 暫存檔
- 定期清除 記錄

- 方法：
- 在 IE 中
- 工具\網際網路選項

手工清除：其它 的上網暫存資料

- 定期刪除 Temp 資料夾裡面的資料
- 定期刪除 Temporary Internet Files 裡面的資料

- 方法：
- 在 檔案總管 中
- C:\Documents and Settings\帳號\Local Settings

CCleaner 資料清除軟體

- 官方下載：
- http://www.ccleaner.com

- 功能：
- 刪除Cookies，保護隱私。也可以自訂清理時不要刪除的Cookies。

- ［清道夫］功能針對網路瀏覽器、系統記錄檔、系統暫存檔、系統垃圾檔、和各種應用程式的無用檔案進行清潔的工作。有效增加硬碟空間，避免垃圾檔案影響硬碟效率。

- ［登錄檔］清理功能可以有效刪除無用的登錄資料，保持電腦的穩定性與執行效率。如果你發生因登錄檔錯誤而造成不能安裝某些軟體的狀況時，到這裡清潔一下，有時候問題就解決了。

Recuva 檔案救援軟體

- 官方下載：
- http://www.recuva.com

- 功能：
- 每個檔案儲存在硬碟時都會占據一個位置，當你在硬碟刪除檔案後，其實檔案的痕跡還是會遺留在原本的磁區上，只要這個磁區位置還沒有被新的檔案占去，那麼妳就有機會救回誤刪的檔案。而「Recuva」正是利用了這個原理，幫你去掃描、搶救已經刪除的檔案（已經從資源回收桶中移除、或直接刪除的檔案），而從其原理來看，一個很重要的前提是，Recuva 通常只能救回最近刪除的檔案，當你發現不小心誤刪了某個檔案時，不要去進行其它操作，立刻搶救檔案比較有效。

File Shredder 檔案銷毀軟體

- 官方下載：
- http://www.fileshredder.org

- 功能：
- 是一套免付費的軟體，檔案大小約1.15MB，安裝便利、操作也很簡單。安裝只要利用加入檔案或資料匣的方式，選擇要完全清除的檔案或資料匣。

- 這套軟體具備5種不同的檔案覆寫等級，包含簡單的單次與兩次複寫，以及合乎美國國防部標準的「DoD 5220-22.M」，或是7次複寫的「NSA」與35次複寫的最高粉碎等級「Guttman」。

- 不僅可以銷毀單一檔案或資料夾，也可清除無用檔案，騰出硬碟空間。

清除、救援、銷毀個人資料的注意事項

- 使用這些軟體可以有效清除在「家用電腦」上，所存放的個人資料。如果是「辦公室電腦」則需參考資訊安全政策的規定。
- 但如果個人資料是放在相簿網站、購物網站、交友網站上，則這些軟體是清除不到的，所以仍然需要注意上網、收發信件的個資安全。
- 使用「資料銷毀軟體」時請特別留意，因為如果被拿來惡作劇，是沒有藥可以救的。

徹底銷毀硬碟資料的7大方法

1. 低階格式化
2. 泡水法
3. 焚毀法
4. 刀割碟片法
5. 滴鹽酸法
6. 消磁法
7. 鐵鎚敲擊法

- 請問哪一個比較有效？

常用工具：檔案偵測(免費)

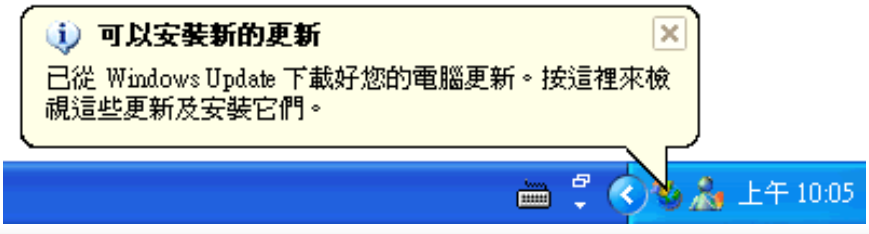
- Microsoft TechNet Windows Sysinternals
- http://www.microsoft.com/taiwan/technet/sysinternals/default.mspx

- Process Explorer for Windows v10.21
- http://www.microsoft.com/taiwan/technet/sysinternals/Security/ProcessExplorer.mspx

- 有經過pack加工的惡意程式會變成紫色，按右鍵 → Kill 刪除。

電腦安全性的七大步驟

1. 評估使用電腦的風險，隨時提高警覺不要亂點選
2. 使用防毒軟體及防間諜軟體，並搭配線上掃毒
3. 保持更新作業系統及應用程式等軟體為最新狀態
4. 檢查您的作業系統及IE安全性設定
5. 使用個人(單機)防火牆
6. 建立穩固的密碼
7. 執行日常工作安全性維護，例如：更新、掃毒



結論

- 上網的個資防護
  - 網路相簿
  - 網路購物
  - 網路搜尋
- 電子郵件的個資防護
  - 傳送郵件的考量
  - 接收郵件的考量
  - WebMail的傳送與接收
- 網路使用的個資防護
  - 即時通訊軟體
  - P2P軟體
  - USB隨身碟
  - 軟體修補
  - 清除、救援、銷毀個人資料

- E-Mail：shooujen@gmail.com

- 部落格：
- 網路攻防戰：http://anti-hacker.blogspot.com
- 綻嵐的天空： http://openblue.blogspot.com

- Twitter推特： http://twitter.com/openblue
- Plurk噗浪： http://www.plurk.com/openblue
- FaceBook： http://www.facebook.com/openblue