資訊安全認知與個人資料保護

主講：甫東科技-賴俊宏

日期：2012/07/24

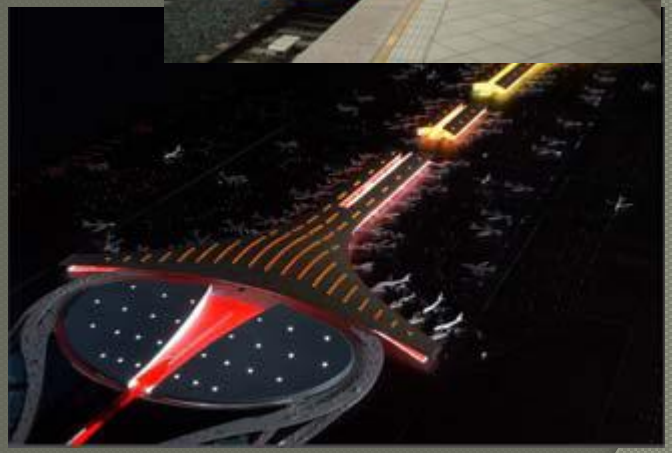
大綱

1. 資訊安全基本認知
2. 認識病毒、入侵威脅
3. 個人資料保護法
4. 案例探討

資訊安全基本認知

資訊、網路系統無所不在

- 電腦網路已深入每一個人的生活當中
  - 政府機關
    - •個人身份資料、稅務資料
  - 公共設施
    - •電力供給、瓦斯供給
  - 金融機構
    - 股市交易、信用卡、存款
  - 醫療機構
    - •病歷管理、維生系統、藥物管理
  - 交通運輸
    - •交通控制中心、自動導航、汽車電腦...
    - •飛機、高鐵、捷運...
  - 通訊系統
    - •智慧型手機、交換機系統...



思考....

假設....

系統安全出現了問題...

網路安全出現了問題....

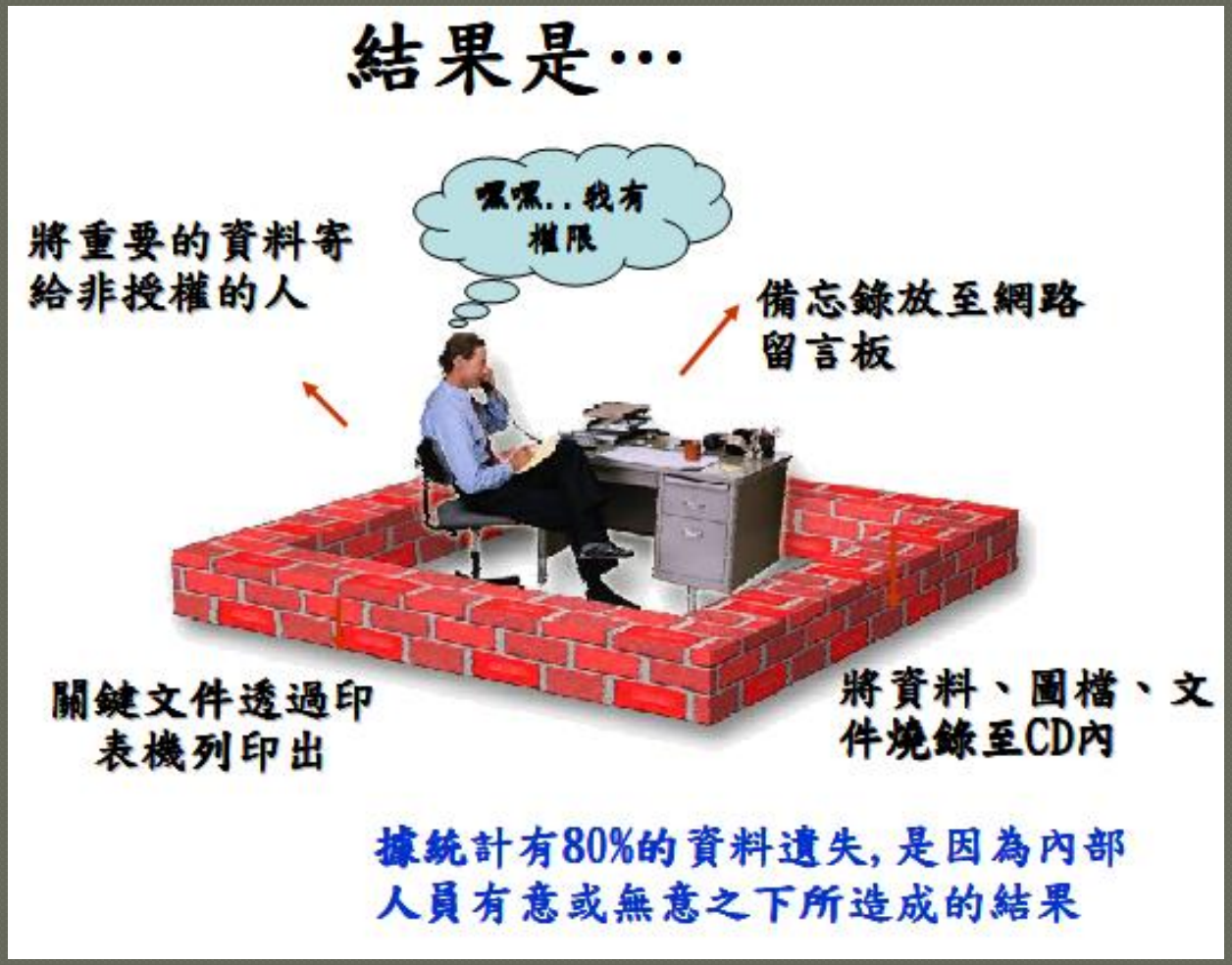
我們的生活.....還可正常運作嗎??

資訊安全認知

一般都會注意…

- 建立安全的周邊環境…

資訊安全認知


結果是…
嘿嘿..我有權限
將重要的資料寄給非授權的人
備忘錄放至網路留言板
關鍵文件透過印表機列印出
將資料、圖檔、文件燒錄至CD內
據統計有80%的資料遺失,是因為內部人員有意或無意之下所造成的結果

資訊安全防護最大的風險—人

- 多數研究調查機構均指出，資訊安全防護中最弱的一環就是『人』，而『人』的風險只能靠教育訓練。
- 不論學校內部採用多強大的防火牆系統或防毒軟體，使用者擁有良好的使用習慣，才是資安防護最有效的略策。
- 使用者具備資訊安全概念，更是低成本的資安防護略策，其效果遠勝於高價採購最新設備與技術。

資訊安全的意義

- 保密性：資訊被允許存取(Access)的多少。
- 完整性：資訊在利用、傳輸、儲存等過程中不被篡改、遺失、毀損。
- 可用性：資訊在合法使用者需要時可以立即取得。

影響資訊安全的因素

- 天然災害：水災、風災、地震、雷電等意外災害。
- 人為疏失：操作人員無意犯的錯誤。
- 人為破壞：故意或非法的竊取、竄改、刪除資料或洩密、病毒散播等，是資訊安全最為脆弱的一環。
- 環境因素：疏於防護造成潮濕、過熱、灰塵、斷電等硬體的損壞。是可以避免的。

資訊安全的項目

- 實體安全：指硬體實際設備的安全。
- 資料安全：指各種資料庫或檔案的安全。
- 程式(軟體)安全：指保持程式運作的穩定與安全。
- 系統安全：指整個資訊作業的安全

基本的資訊安全應...

- 防止資訊被竊聽
- 機密資料應專人保管
- 維護電腦的正常作業
- 加裝UPS
- 重要檔案要定期備份
- 加裝防火牆(Fire Wall)

加強個人資訊安全的方法

降低資安風險

- 不開啟來路不明的電子郵件
  - – 駭客喜歡玩的文字遊戲
  - • www.citibank.com.tw 與www.citybank.com.tw
  - • www.paypal.com 、www.paypal.com 與
  - www.paypa1.com
- • 絕不下載或開啟來路不明的檔案
  - – 圖片、影片、MP3
  - – 壓縮檔
  - – Word、Excel
- • 不使用來路不明的軟體
  - – 有趣的小遊戲
  - – 免費或共享軟體
  - – 盜版軟體

強化系統的防護能力

- 使用防火牆
  - – 防止惡意連結透過未使用到的通訊埠連線
  - – 使用IP 分享器或建立DMZ 區域
- 隨時保持系統軟體在最新狀態
  - – Service Pack、Security Patch
- 移除或停用沒有用到的軟體
- 使用最新的防毒軟體
  - – 定期更新病毒定義檔
  - – 定期掃描
- 使用複雜度及強度高的密碼
  - – 安全性低的密碼只需要數分鐘就能輕易破解
  - – 駭客或病毒會先從Administrator 帳號進行密碼猜測
  - – 字典檔內建上萬組的密碼組合，其中包含一般人經常設定的密碼組合• 0000、123456、password ...
- 定時備份重要資料

使用安全性高的密碼

- 必須包含英文字母、數字與特殊字元，英文字母須含大小寫
  - – 特殊字元為：!@#$%^&*...等符號
  - – 英文字母不可為有意義的單字，例如名字或是單位名稱
  - – 密碼長度建議在8 位數以上
  - – 需注意經常性的替換密碼(約莫90天換一次)
  - – 如何設定一個複雜度及強度高，又容易記住的密碼(善用中文輸入法的優勢)

輕鬆對抗電腦病毒及惡意軟體

- 良好的使用習慣
  - 隨時保持系統軟體在最新狀態
    - Windows Update
    - Service Pack
- 使用個人防火牆
  - Windows XP SP2以上、Windows 7
  - Symantec Client Security…等
- 使用最新的防毒軟體
  - 定期更新病毒定義檔
  - 定期掃描

面對未來資訊安全威脅應該有的認知、態度

- 【世界上沒有永遠安全的系統】
- 【凡走過、並留痕跡】
- 【資訊安全】是現代每一個人都必須關心的議題

資訊安全基本原則

一、密碼設定
二、瀏覽器使用安全
三、電子郵件使用安全
四、安裝防毒軟體
五、勿下載來路不明軟體或使用 P2P檔案傳輸軟體
六、謹慎使用即時通訊軟體(MSN、即時通)

一、密碼設定(設定原則)

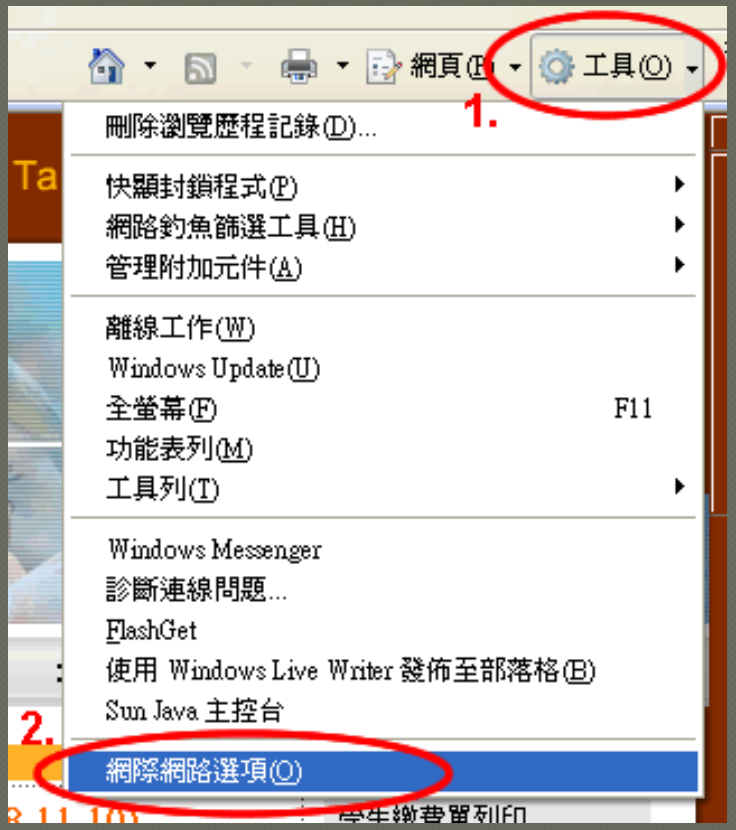
- 密碼長度與設定
  - 密碼長度至少8個字元以上。
  - 英文(大小寫)、數字、符號(@#$%&)混合。
  - 區分「重要帳號密碼」與「非重要帳號密碼」。
- 避免用簡單容易取得的密碼
  - 帳號、電話、生日、電子信箱網址。
  - 重複、連續的字。(aaa、123)
- 密碼保存與更新
  - 密碼存放於高安全性的地方(勿貼在電腦上)。
  - 至少每三個月更新一次密碼。

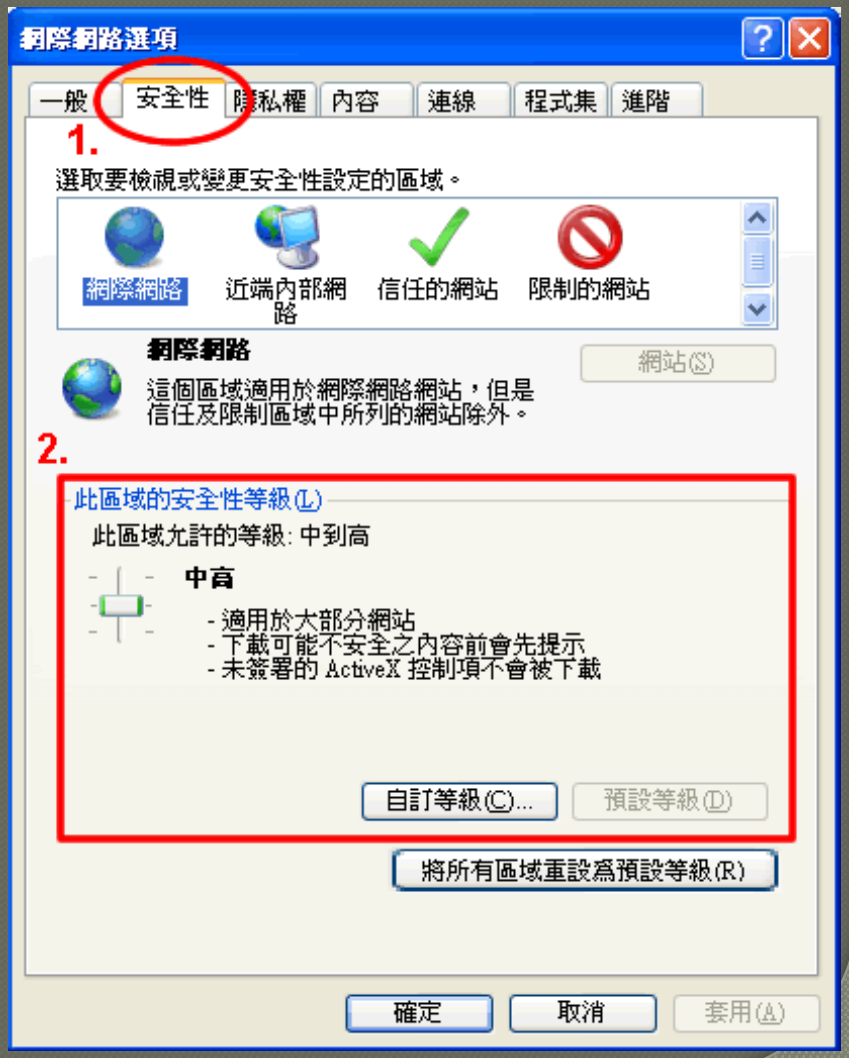
一、密碼設定(密碼強度檢測)

- 檢測密碼強度：
  - http://www.refly.net/passwordchecker/
  - https://www.microsoft.com/security/pc-security/password-checker.aspx?WT.mc_id=Site_Link

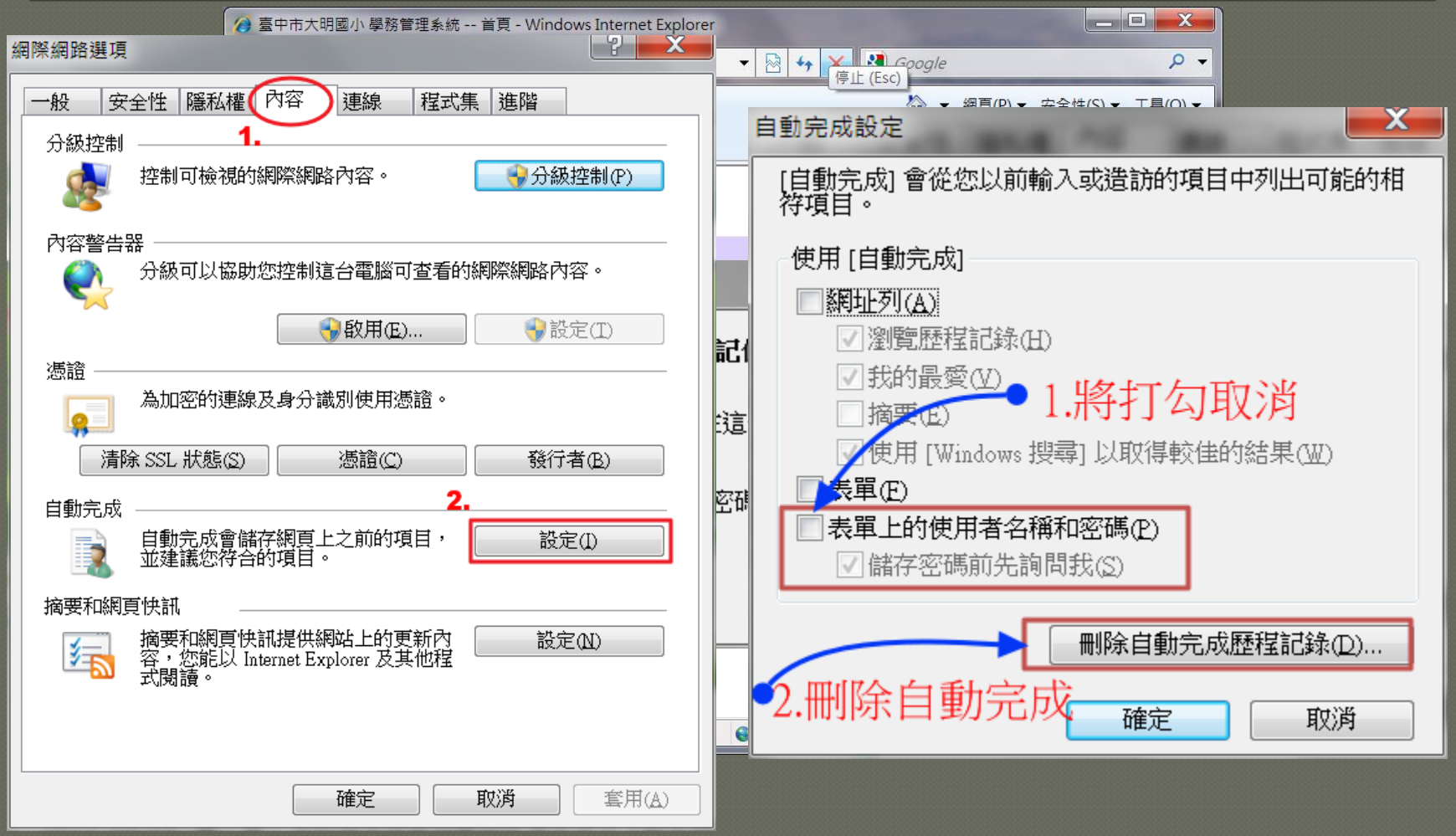
二、瀏覽器使用安全(安全性設定)

- 瀏覽器安全層級設定至少為中安全性以上。



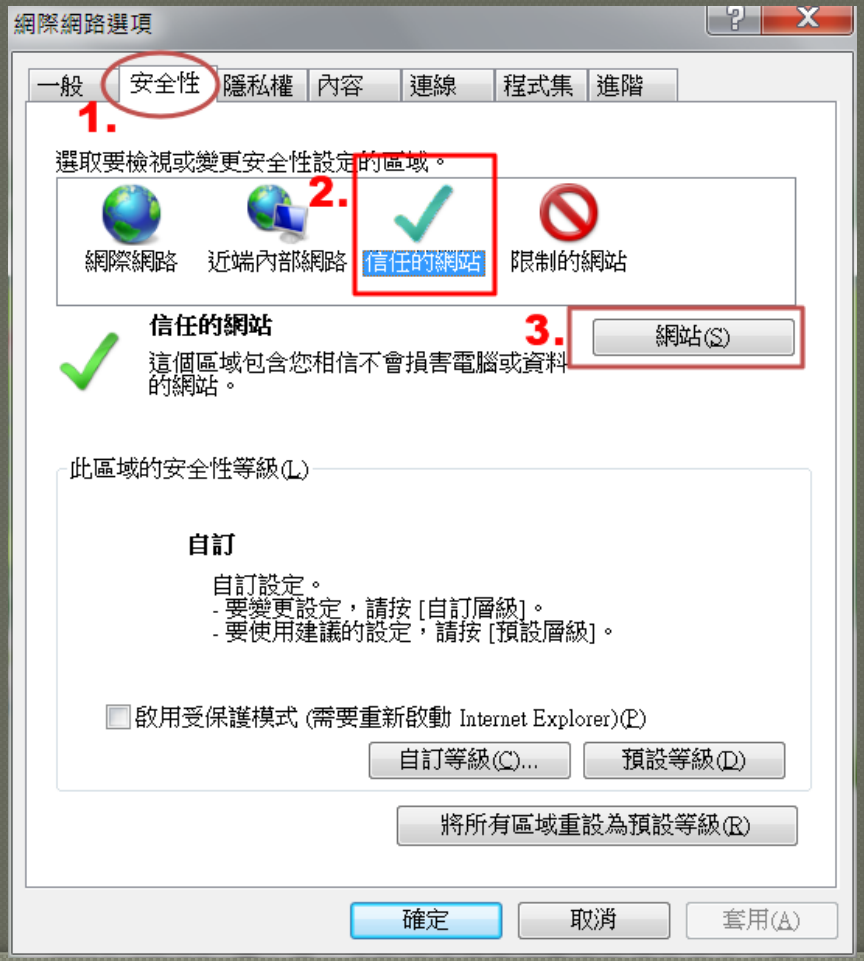


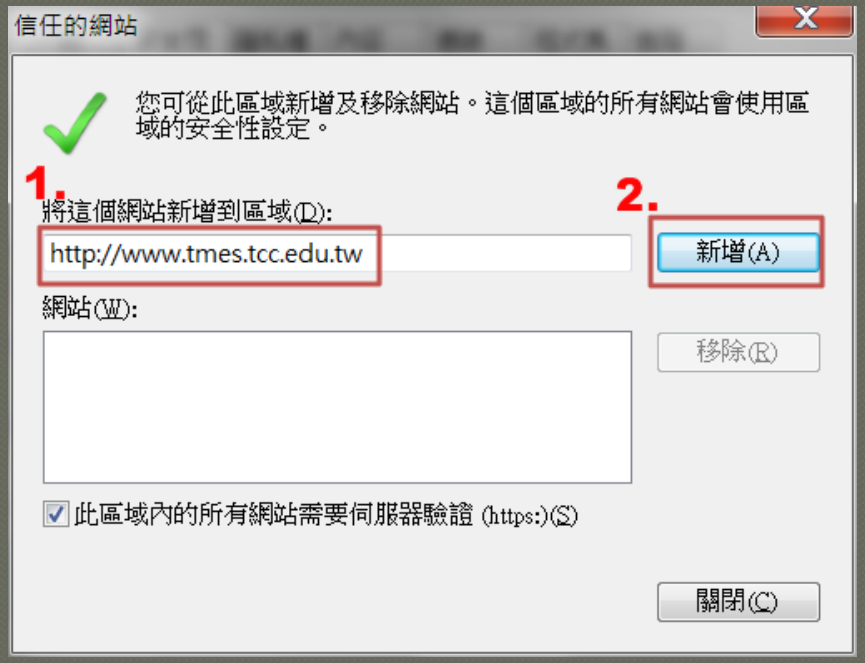
二、瀏覽器使用安全(清除自動完成)



二、瀏覽器使用安全(加入信任網站)

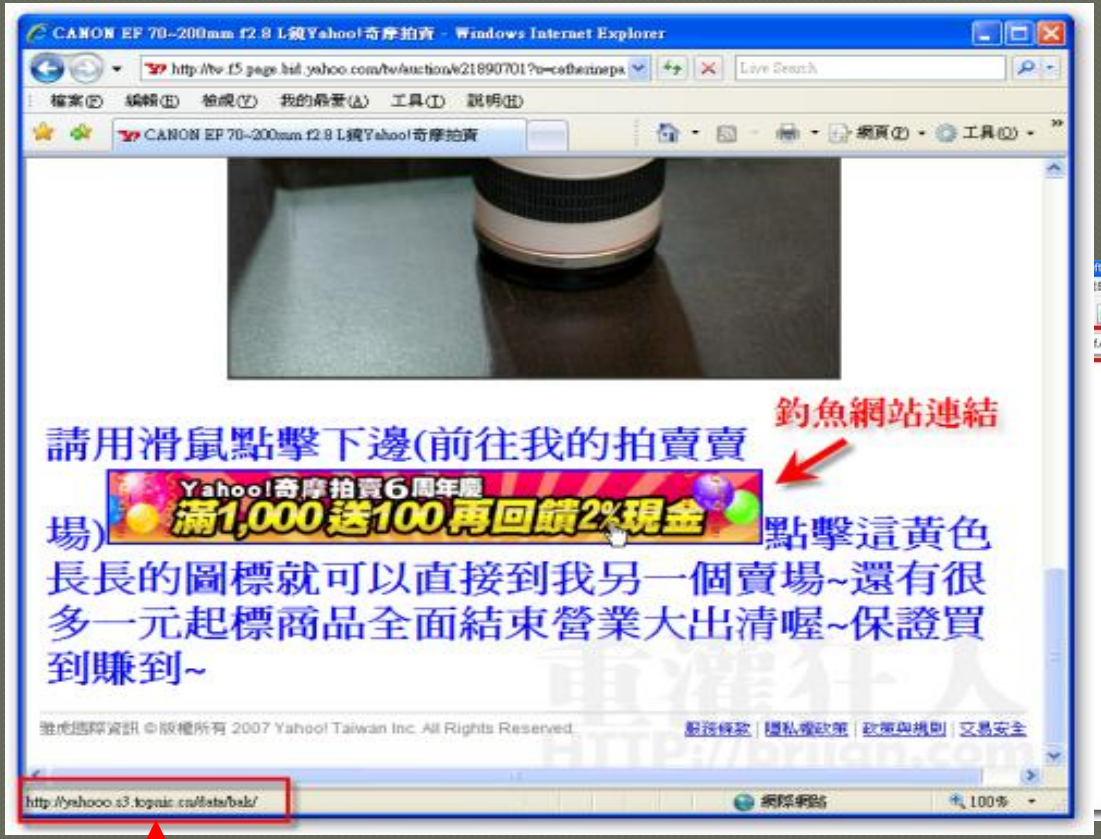
- 經常使用且可信任的網站，可加入為信任網站。





二、瀏覽器使用安全(注意釣魚網站)

- 點選「超連結」前，先檢查網址。



詐騙網址
hxxp://yahooo.s3.topnic.cn/data/bak/

詐騙網站的登入頁面

三、電子郵件使用安全

- 不點選不明電子郵件中之網址連結。
- 不開啟不明電子郵件中之附夾檔案。(rar、zip、exe、doc、ppt、xls、pdf)
- 不轉寄不明網路謠言及不明廣告信。
- 用電子郵件傳送重要檔案時，要壓縮加密。
- 防範「社交工程」攻擊。

三、電子郵件使用安全

- 社交工程攻擊：駭客以笑話、政治、健康或色情等引人好奇的電子郵件，或是假冒名義，寄送經特殊設計之word、excel、powerpoint、pdf等文件檔案，誘使收件人開啟以達成功入侵電腦之目的。
- 過去大家認為只有執行檔(exe、bat、cmd)才會夾帶惡意程式，現在已大為改觀，doc、xls、ppt、pdf檔都可能被駭客利用。
- 防範方式
  - 更新office漏洞補程式、adobe pdf reader版本
  - 安裝防毒軟體
  - 不要開啟附件

四、安裝防毒軟體

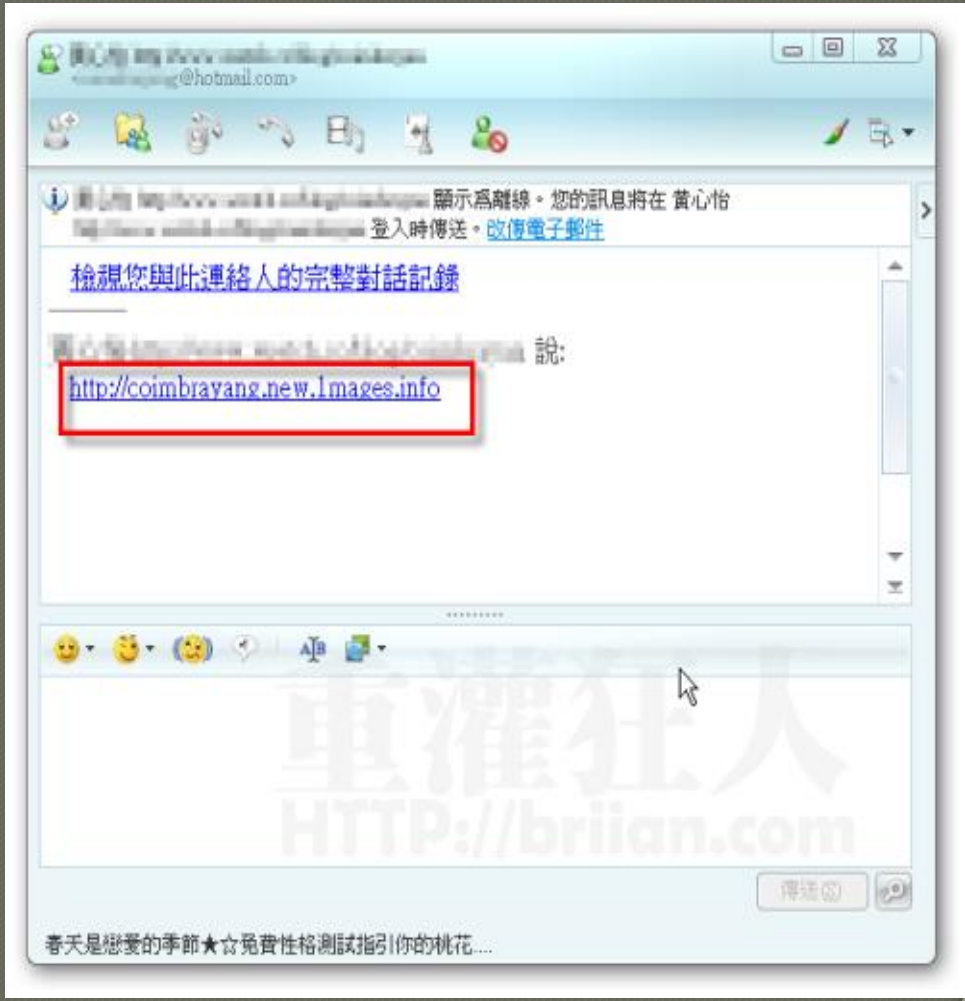
- 安裝防毒軟體
  - 免費：AntiVir、AVG、avast!
  - 付費：Pccillin、Norton、Kaspersky
- 隨時更新病毒碼
- 定期執行全系統掃毒

五、不下載來路不明軟體

- 任意下載、安裝網路上的免費軟體、或來路不明的軟體，也是感染電腦病毒、間諜軟體與木馬程式的主要途徑。
- 使用foxy、BT、eMule等點對檔案傳輸軟體、易下載含有病毒或木馬的軟體、導致電腦中重要資料外洩。

六、謹慎使用即時通訊軟體

- 即時通訊軟體(如MSN、Yahoo即時通)是快速且方便的網路溝通工具。
- 存在的風險
  - 病毒、木馬程式
  - 網路釣魚
  - 網路詐騙
  - 社交工程



認識病毒、入侵威脅

什麼是電腦病毒?

- 電腦病毒是一小段電腦程式碼
- • 電腦病毒的特徵
  - – 會不斷「自我繁殖」及「感染」
  - – 會有「潛伏期」
  - – 會直接或間接的影響電腦系統運作，損壞軟硬體或資訊
- • 電腦病毒的存在方式
  - – 隱藏在開機磁區中
  - – 寄存在可執行的檔案之中
  - – 隱藏在正常的檔案之中
  - – 偽裝成系統檔案

電腦病毒的種類

- 開機型病毒
  - – 最佳代言：CIH
- 檔案型病毒
  - – 最佳代言：Friday The 13th、MacGyvver
- 巨集病毒
  - – 最佳代言：Taiwan No1、Melissa
- • 特洛依木馬
  - – 最佳代言：Back Orifice、SubSeven、NetBus
- • 惡作劇程式
  - • VBS病毒
  - • JavaScript & ActiveX 病毒
  - • 蠕蟲(混合式威脅)

網路安全的威脅

- 系統入侵(System Hacking)
- – 系統或程式弱點
- – 密碼猜測
- • 惡意程式碼(Malicious Code)
- – 病毒、蠕蟲
- – 特洛伊木馬
- – 後門、Rootkit
- – Spyware、Adware
- • 監聽(Sniffing)
- – Sniffer
- – Keylogger
- • 服務阻斷(Denial of Service)
- • 網路釣魚(Phishing)
- • 社交工程(Social Engineering)

系統入侵的威脅

- 系統或程式弱點
  - – Windows OS、Internet Explorer、Office…
  - – WWW、FTP、SMTP…
  - – MS SQL、MySQL…
- • 密碼猜測
  - – 常用密碼字典檔
  - – 暴力破解法
  - • 其他手法
  - – SQL Injection

駭客攻擊手法

- 病毒、蠕蟲 (virus、worm)
- 木馬、後門 (trojan horse、backdoor)
- 暴力猜解密碼 (brute force)
- 阻絕服務 (dos,ddos)
- 緩衝區溢位 (buffer overflow)
- 監聽與側錄 (sniffing,key-loger)
- 欺騙與偽裝(spoof、smurf)
- 資料隱碼 (sql-injection)
- 無線網路滲入 (wireless lan)
- 社交工程 (social engineering)

木馬、後門

- 木馬 Trojan Horse
  - 木馬程式電腦病毒，此程式似合法而實際上具有破壞的程式,將其比喻為木馬，意指潛在的
- 後門 Backdoor
  - 利用非法的便利途徑，進入非授權的環境下，存取資料、程式、服務進入系統。

暴力猜解密碼

- 暴力猜解密碼是以自動化工具強制性猜測某一系統帳號的密碼，通常使用所謂的密碼檔，或是挑選字元類型及密碼長度。

- 防治方法:
  - 密碼檔加密
  - 密碼複雜度、長度及定期變更

阻絕服務

- 阻絕服務(DoS, DDoS) 攻擊手法是利用TCP/IP 協定當初設計的缺失，以及作業系統針對TCP/IP 協定實際implement 方式的不同來設計攻擊方式。
  - – 駭客使用大量封包或是特異畸形的封包來癱瘓目標主機上的服務；
  - – 輕則使目標主機服務停止，重則讓主機當機；
  - – 針對DDoS 的攻擊則往往很難抵擋，事後也很難追查真正的攻擊發起人。

緩衝區溢位

- 緩衝區溢位(Buffer Over Flow) 攻擊存在於任何一套軟體甚至是作業系統中，也可能是你我寫的程式或是你我天天在用的程式，最厲害的駭客可以精心設計出造成Buffer Overflow之後跳到他設計好的程式程序裡面，此時如果這個程序有SET UID 的程式將會使駭客擁有root的權限，他可以為所欲為而你卻完全無法察覺。
- 目前針對這方面攻擊的預防不外乎就是程式設計時不光以功能為導向，還要注意系統安全的環節，而不是趕著交差了事的心態設計程式，此外要善選安全的compiler ，對會造成問題的函式盡量不要使用。

欺騙與偽裝

- DNS Spoofing
- IP Spoofing
  - – IP Spoofing 可欺騙路由器或防火牆，假裝入侵者是來自於可信任的網路，而順利進入私人網路。
  - – IP Spoofing 會更改封包的表頭，讓封包看起來像是來自於可信任的網路而允許進入路由器或防火牆。
- • ARP Spoofing
  - – 利用系統或設備中ARP Table授受Request時，以大量偽裝MAC Address或IP來造成ARP Table Full，使系統或設備癱瘓。

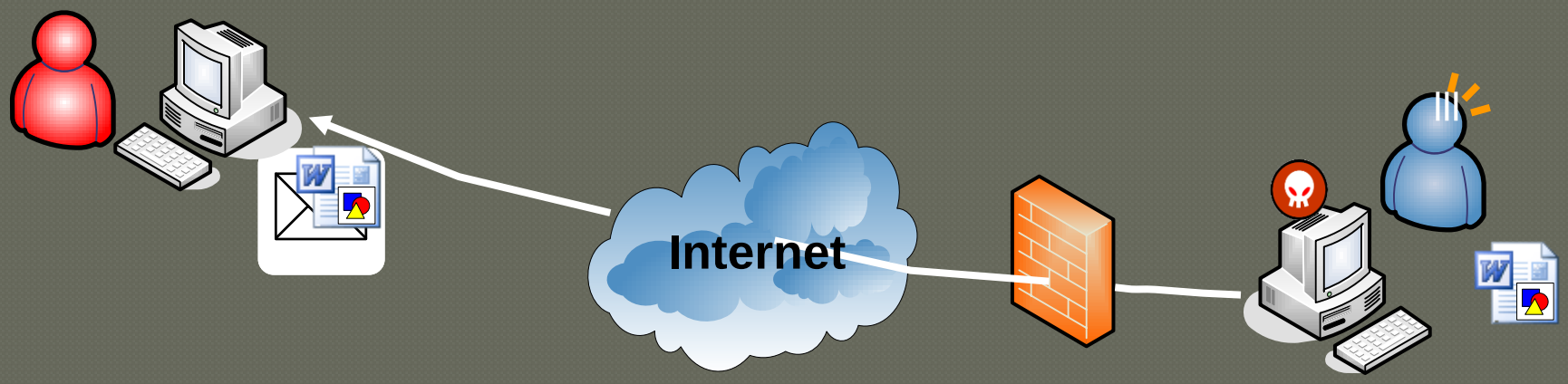
監聽與側錄

- 監聽(Sniffing)
  - – 監聽器的出現來自於網管人員對於網路流量的管理監控需求，因此需要一套軟體來記錄LAN裡面傳遞的封包資訊，流量等紀錄，但被有心人士拿來當作竊取資訊的手法。
- • 側錄(Key-Logger)
  - – 鍵盤記錄器，可將使用者所有使用鍵盤輸入的字元完整的記錄下來，並配合木馬程式可將記錄檔傳送給攻擊者，以竊取密碼和敏感資訊。

無線網路滲入

- 無線網路滲入(Wireless LAN Intrusive) 是利用企業無線區域網路存取點(Access oint)設定上的安全弱點，連接企業內部網路來進
- 行入侵與攻擊行為。

社交工程擊模式



1. 駭客設計攻擊陷阱程式(如特殊 *Word* 檔案)
2. 將攻擊程式埋入電子郵件中
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，並被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

個人資料保護法

國外經驗:
企業對於個資保護的重視

- 依據國外的經驗顯示，如金融、保險、製造等產業，因為相關法規的要求，國外很早就重視起有關資料外洩防制的問題。
  - 如美國的「醫療資料相關健康保險可攜性與責任草案(HIPAA)」、財務資料相關的「沙賓法案(Sarbanes-Oxley)」，與信用卡資料相關的「支付卡產業標準(Payment Card IndustryStandard」…等，因其訂定的鉅額罰款，使得企業負責人必須更重視資安的強化。

為何制定個人資料保護法

- 84年8月11日施行「電腦處理個人資料保護法」，用以保護個人資料，但近年來，個資外洩情況嚴重，詐騙事件日增，由於上述法令不周全，故有修法必要。

- 「電腦處理個人資料保護法」缺失：
  - 保護客體僅限於「電腦資料」。
  - 適用的非公務機關僅限於八大行業。(徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業)
  - 對「特種個人資料」保護不周。
  - 對「當事人權利」保護不足。
  - 「損害賠償」機制不完全。

個人資料保護法

- 個人資料保護法：「個人資料保護法」經立法院於99年4月27三讀通過，5月26日總統公佈 。
- 立法目的：避免人格權侵害，促進個人資料合理利用。
- 新法修正重點：

1. 擴大適用主體：
   - 打破行業別限制，適用各行各業及個人。
   - 受委託蒐集、處理或利用個人資料者，視同委託機關。
2. 擴大保護客體：
   - 以任何方式（包括紙本）留存的資料。
   - 任何方式取得個人資料。
   - 生存之特定或得特定之自然人。

3. 增訂告知義務：

- 直接蒐集及間接蒐集之告知義務。
- 當事人拒絕行銷之權利。
- 資料違法外洩之通知義務。

4. 調整賠償義務及罰則：

- 民事賠償：新台幣2千萬元→2億元。
- 刑事處罰：新台幣5萬元→100萬元。
  有期徒刑：3年以下→5年以下。
  意圖營利犯罪者為非告訴乃論。
- 行政處罰：新台幣10萬元→50萬元

台灣新舊版個資法差異的比較

- **舊版個資法**最大的問題在於，除公部門外，一般民間企業僅限於徵信、醫院、學校、電信、金融業、證券、保險及大眾傳播...等8大行業適用，不及於其他一般企業與個人。
- 而受保護的範圍，亦只有經電腦所處理的個人資料，紙本資料則不在此範圍內。

- **新版法案**則刪去「電腦處理」的字樣，更名為「個人資料保護法」，除適用主體擴大到自然人、法人、公務與非公務機關外，紙本資料也納入受保護的範圍。

解決之道

資安需求與個資法規範

- 分別由「技術」與「管理」兩方面出發，協助人員進行與個資法相關的檢驗，並提出後續的風險評估與報告。

先由自我的個資外洩風險評估做起

- 因應個資法的第一步，應先從評估企業個資外洩的風險開始做起，以了解企業內個人資料可能洩露至外部的各項管道。
- 特別是新版個資法實施之後，對於企業內的消費者個人資料，從其蒐集、保存、利用與銷毀...等階段，都有各項明確且嚴格的規定需要遵守。

合法使用者為企業機密資料的主要外洩管道

- 根據美國CSI的調查數據顯示，公司機密資料外洩的狀況有70%是由內部合法使用者所造成。
- 而ICM的研究報告亦指出，有39%的員工曾將客戶資料寄出，52%曾在離職時帶走工作資料，86%坦承習慣性將郵件轉寄他人，因此「合法使用者」才是真正危害公司安全的最大因素。

案例探討

一、網站涉洩露學師生個人資料(一)

案由：

中部某所知名大學網站因控管不當，透過Yahoo、Google等搜尋引擎，便可直接取得該校就學貸款學生名冊，名冊內含學生身份證字號、貸款金額等個人資料，讓學生資料暴露於危險之中。

一、網站涉洩露學師生個人資料(二)

預防方式：

1. 網站應指派專人管理審核內容，以避免洩漏學生、教師個人資料。
2. 不適合公開的檔案不可存放在公開之網站上。
3. 網站上過期的資料應進行檔案刪除、不可只移除超連結，以免被搜尋引擎取得而被讀取。

二、電腦失竊造成資料遺失(一)

案由：

南部某國小電腦遭竊，人事教職員資料因存放於電腦中而一並外洩、會計預算電子檔案亦於電腦中一同遺失。

二、電腦失竊造成資料遺失(二)

預防方式：

1. 行政業務資料應養成備份習慣，避免造成資料永久遺失。
2. 筆記型電腦、行動碟等儲存設備因攜帶方便、容易遺失，應設定密碼保護或資料加密，並儘可能避免存放機密公務資料，並妥善保管。
3. 辦公處所應加強門禁管制，設備遭竊應立即向所轄派出所報案。

三、學生駭客竊取帳號修改網站(一)

案由：

北區某知名高中之學生於駭客教學網站習得駭客入侵技巧，練習入侵多所學校網站，並於某小學網站發布『學校寒假延長訊息』假消息，另刪除多所學校網站重要資料。

三、學生駭客竊取帳號修改網站(二)

預防方式：

1. 加強宣導駭客行為必須擔負法律責任。
2. 建置網站開發程式應加強系統安全(如輸入欄位必須進行字元檢查)，避免產生程式漏洞，遭駭客入侵。
3. 網站作業系統、資料庫、服務軟體(如 webServer)應定期更新軟體，避免系統漏洞產生。

四、電子郵件帳號遭駭客竊取(一)

案由：

國內4所大學之郵件伺服器與駭客中繼站建立連線，且特定電子郵件帳號遭登入下載郵件查看，疑似洩漏重要資訊內容。

四、電子郵件帳號遭駭客竊取(二)

預防方式：

1. 應注意電子郵件使用安全，勿開啟來路不明之信件，以免被植入後門程式竊取資料。
2. 郵件帳號及瀏覽器應取消記憶密碼功能，以避免帳號密碼記錄被駭客利用木馬程式竊取。
3. 個人電腦應安裝防毒軟體，且作業系統及防毒軟體應隨時更新，以避免漏洞產生。
4. 電子郵件及相關系統登入之密碼應定期更換。

五、公事家辦洩密(一)

案由： (轉載自法務部)

某中央政府機關內人員習慣將公文之電子檔案，以隨身碟拷貝至家中電腦辦公並儲存。因家中電腦已遭駭客植入後門程式，以致長期大量經手之機密文書外洩，又經各媒體大幅報導，損害政府機關形象。

五、公事家辦洩密(二)

預防方式：

1. 公務機密資料攜出應依程序辦理（依國家機密保護法規定：公務機密資料攜出辦公處所，應經機關首長核准）。
2. 家中電腦之使用較缺乏定期更新軟體與防毒程式之習慣，應妥善設定自動更新機制，以防範病毒入侵。
3. 家中電腦連線上網時通常沒有防火牆保護，應加裝個人電腦防火牆，以降低遭入侵之機率。

六、8警所私灌FOXY偵查筆錄外洩(一)

案由： (轉載自法務部)

據電腦犯罪防制中心指出：8所警察機關之警員擅自安裝FOXY（檔案下載軟體）於警所電腦中，且不熟悉FOXY之設定方式，誤將電腦中所有資料開放予所有人下載，造成警所電腦筆錄資料外洩，警政署怒追究相關人員的疏失責任。

六、8警所私灌FOXY偵查筆錄外洩(二)

預防方式：

點對點（P2P ）檔案下載軟體因版本與種類繁多，軟體容易被改寫加入木馬或後門程式，故不要安裝P2P軟體，如Bittorrent（BT）、eMule、FOXY等，以免造成機密資料外洩；另P2P下載之檔案也容易含有病毒或是非法之盜版軟體，容易遭到廠商追蹤舉發而產生訴訟與巨額賠償。

七、全台近千網站植入惡意程式(一)

案由：

據媒體報導：平均每10個網頁，就有1個植入惡意程式碼，「拒絕壞程式基金會」（http://stopbadware.org）發布「全台近千網站植入惡意程式」訊息，顯示目前網站內含惡意程式碼問題嚴重。

七、全台近千網站植入惡意程式(二)

預防方式：

1. 個人電腦應安裝防毒軟體，作業系統及防毒軟體隨時更新。
2. 瀏覽器安全等級應設定為中級或更高等級。
3. 勿任意下載或安裝來路不明、有違反法令疑慮（如版權、智慧財產權等）的電腦軟體。

八、網路銀行資料遭竊取(一)

案由：(轉載自刑事警察局)

據科技犯罪防制中心指出：有犯罪集團利用假資料註冊與國內知名網路銀行、航空公司等極為類似之網址，再於各大搜尋引擎公司購買關鍵字廣告，誘使民眾連結至藏有木馬程式網頁，俟民眾電腦遭植入木馬後再導向正常網站，此時木馬程式已開始進行鍵盤側錄與竊取檔案，竊取民眾網路銀行帳號密碼，其後再進行轉帳盜取，此類損失達已數千萬元。

八、網路銀行資料遭竊取(二)

預防方式：

1. 使用搜尋引擎時需特別注意關鍵字廣告與正牌網站之區隔。
2. 個人電腦應安裝防毒與防火牆軟體，作業系統及防毒軟體應定期更新。
3. 避免將個人基本資料於網路上流傳。
4. 避免於辦公室瀏覽非公務網站。

謝謝聆聽