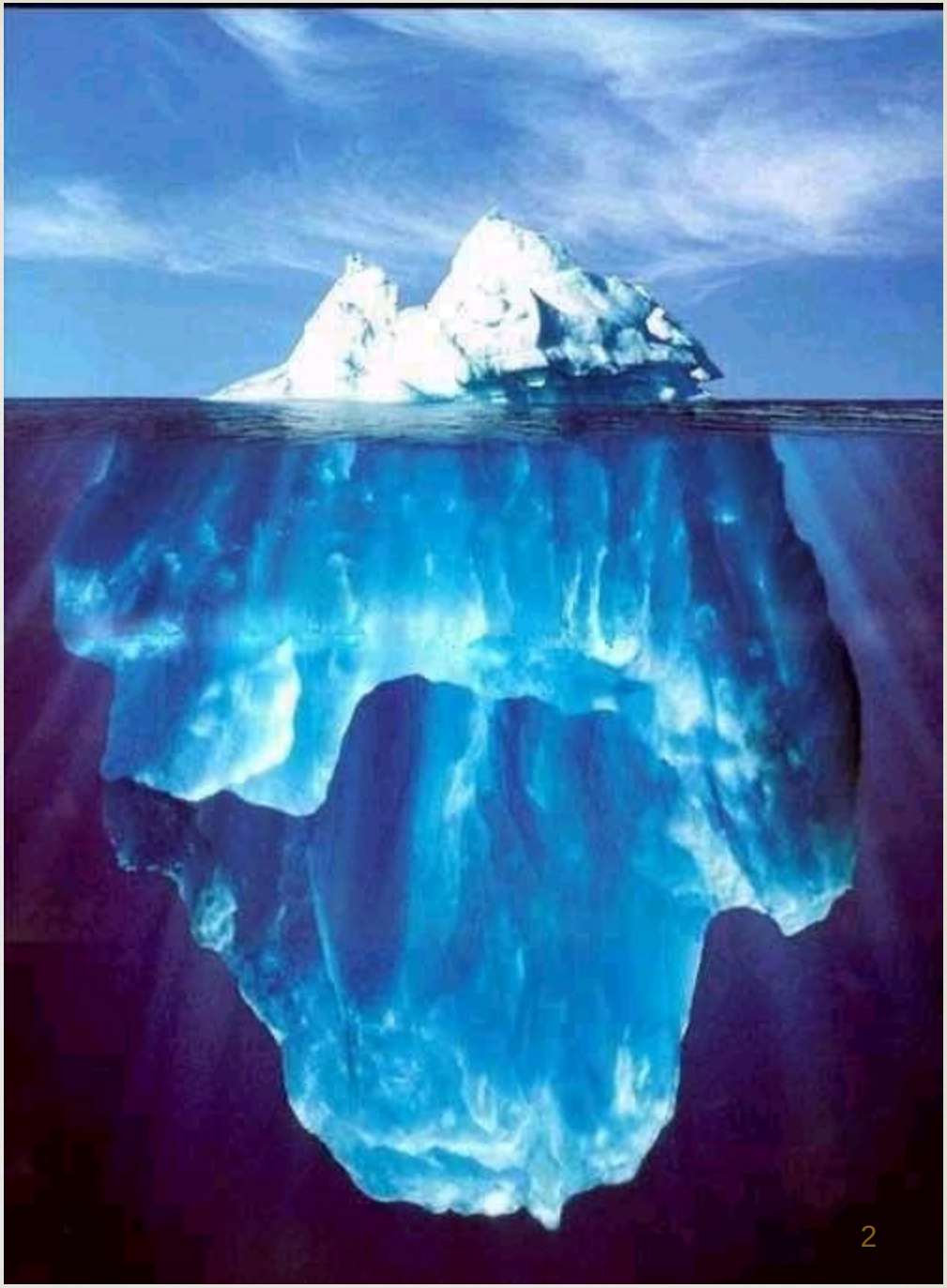
資訊安全防護

簡報單位　：　國科會資訊小組
簡 報 人　：　李主任筱瑜、陳信翰
簡報日期　：　100年11月3日

冰山一角

許多許多時候，事務呈現的表象或結果，背後往往隱藏了更大更深的事實。

涉及到資訊安全的領域，尤其如此。



以下資料摘自國家資通安全指導小組簡報

案例介紹1 -Stuxnet超級工廠蠕蟲病毒

它是世界上第一個專門針對工業控制系統撰寫的破壞性病毒，有「網路導彈」之稱。一旦攻擊成功，能夠控制計算機監控系統，破壞工廠正常運行；這可能是全球第一種投入實戰的網路武器，開啟了網路軍備競賽的新時代。

案例介紹1　Stuxnet超級工廠蠕蟲病毒

潘朵拉的魔盒被打開

啟動了現代社會沒有寧日的夢魘……。

案例介紹2 –中國網軍概況

資料來源：**國家資通安全指導小組簡報**

- 網軍人數：按2010年1月美國聯邦調查局研究指出，中共網軍人數約有18萬人（網路特工3萬人、民間部分15萬人）。
- 編　　組：在總參謀部下設有全軍網絡戰指揮中心及網絡作戰局，主管網絡戰能力建軍與訓練，並由總參謀部統一指揮，任何單位和個人不得擅自實施攻擊。
- 民間部份：主要網羅資訊科技從業人員或民間駭客，組成電腦駭客及民兵網絡站分隊等組織。

案例介紹2 -中國網路民兵

- 英國「金融時報」10月13日在「網路之戰」系列報導，指出中國解放軍過去10年中，已積極在全國各地網路公司和大學中建立有數千個網路民兵部隊。
- 河北衡水市南昊科技公司（Nanhao Group）係一專門製作線上評分軟體等產品的科技公司。自2006年起，公司500名員工中所有30歲以下者同時亦為中國人民解放軍組織的網路民兵部隊之一員。
- 南昊公司副總裁白國良證實，網路民兵係歸由當地軍方指揮

案例介紹2 -中國駭客入侵實例

2011/08	美防毒軟體McAfee指中國駭客過去5年入侵14國，72個政府、組織或企業網站，受害國家包括台、美等政府網站及聯合國、奧委會等
2010/01	Google指部分中國維權人士的Gmail信箱，從2009年底屢遭駭客入侵，調查發現駭客來自上海交通大學，及中國軍方的山東藍翔高級技工學校，中方否認
2009/03	加拿大指中國「鬼網」入侵103國家的1295台電腦，包括各國外交部、使領館、新聞媒體及非政府組織的電腦，加國稱台灣是遭入侵最嚴重的國家
2007/12	英國軍情五處警告300名英國銀行執行長，他們的IT系統恐遭「中國國家單位」入侵，竊取商業情報

資料來源：蘋果日報

簡報大綱

- 資訊安全面臨的挑戰
- 資訊安全設定
- 資訊安全日常工作
- 其他資訊安全注意事項
- 實體隔離
- 個人資料保護法

資訊安全面臨的挑戰

駭客的種類

- 組織型、個人型

駭客的目的

- 商業性、政治性、技術性、針對性
- 個人名聲、金錢利益

資訊安全面臨的挑戰

駭客入侵的管道

- 上網電腦

  網頁、E-mail、MSN、遊戲、軟體漏洞、P2P

- 實體隔離電腦

  行動碟

駭客入侵的結果

- 資料外洩、殭屍電腦

釣魚網站

https://www.phish-no-phish.com/tw/default.aspx

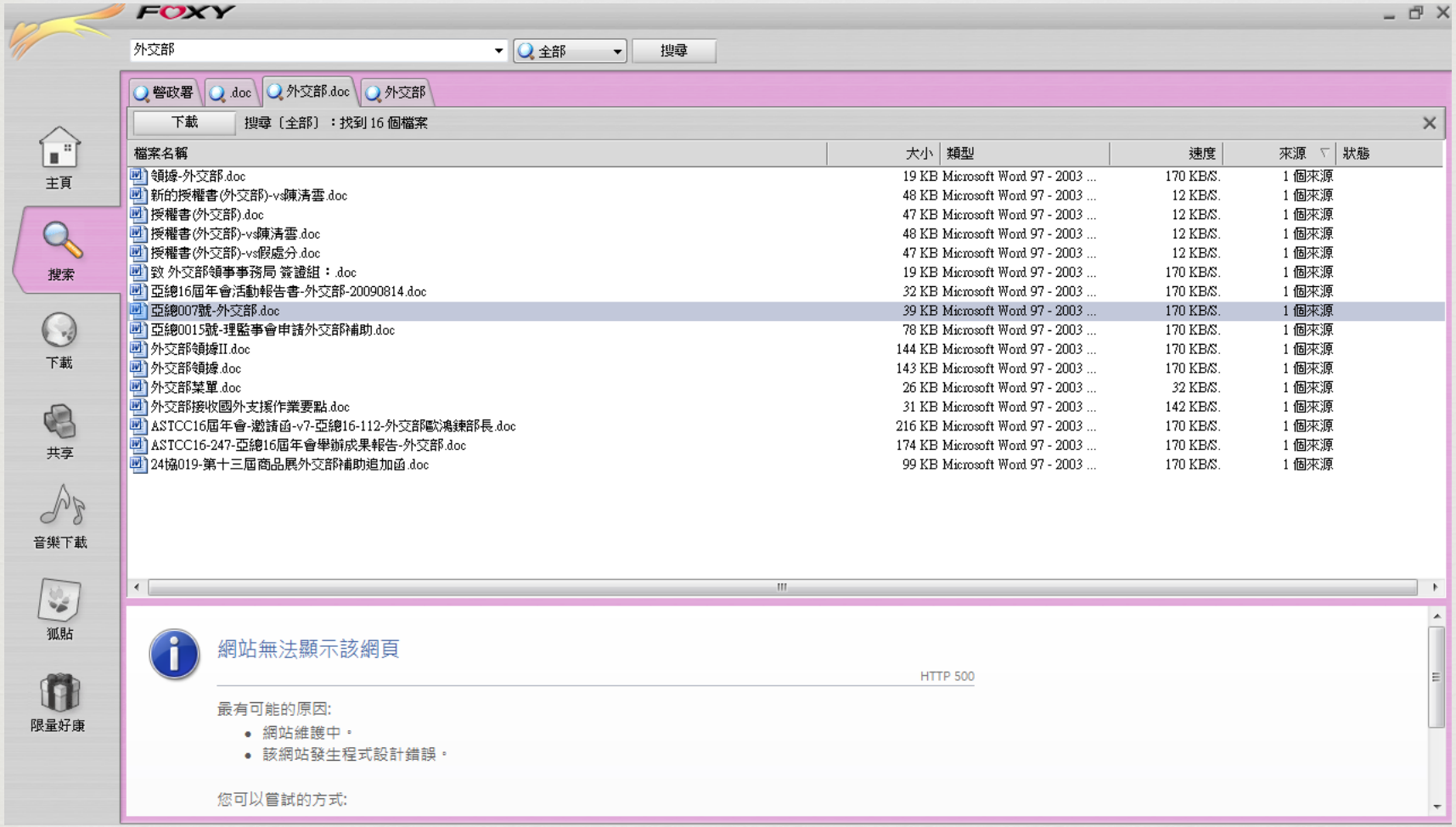
VeriSign

看看為何這是假的網站。

2 / 10

下一頁

P2P 軟體工具洩漏


FOXY
外交部
全部
搜尋
警政署
.doc
外交部.doc
外交部
下載
搜尋〔全部〕：找到 16 個檔案
檔案名稱
大小
類型
速度
來源
狀態
領據-外交部.doc 19 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
新的授權書(外交部)-vs陳清雲.doc 48 KB Microsoft Word 97 - 2003 ... 12 KB/S 1 個來源
授權書(外交部).doc 47 KB Microsoft Word 97 - 2003 ... 12 KB/S 1 個來源
授權書(外交部)-vs陳清雲.doc 48 KB Microsoft Word 97 - 2003 ... 12 KB/S 1 個來源
授權書(外交部)-vs假處分.doc 47 KB Microsoft Word 97 - 2003 ... 12 KB/S 1 個來源
致 外交部領事事務局 簽證組：.doc 19 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
亞總16屆年會活動報告書-外交部-20090814.doc 32 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
亞總007號-外交部.doc 39 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
亞總0015號-理監事會申請外交部補助.doc 78 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
外交部領據II.doc 144 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
外交部領據.doc 143 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
外交部菜單.doc 26 KB Microsoft Word 97 - 2003 ... 32 KB/S 1 個來源
外交部接收國外支援作業要點.doc 31 KB Microsoft Word 97 - 2003 ... 142 KB/S 1 個來源
ASTCC16屆年會-邀請函-v7-亞總16-112-外交部歐鴻鍊部長.doc 216 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
ASTCC16-247-亞總16屆年會舉辦成果報告-外交部.doc 174 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
24協019-第十三屆商品展外交部補助追加函.doc 99 KB Microsoft Word 97 - 2003 ... 170 KB/S 1 個來源
主頁
搜索
下載
共享
音樂下載
狐貼
限量好康
網站無法顯示該網頁
HTTP 500
最有可能的原因:
網站維護中。
該網站發生程式設計錯誤。
您可以嘗試的方式:

網路攝影機

2008-12-1

字型：+ − | 看推薦 | 發言 | 列印 | 轉寄

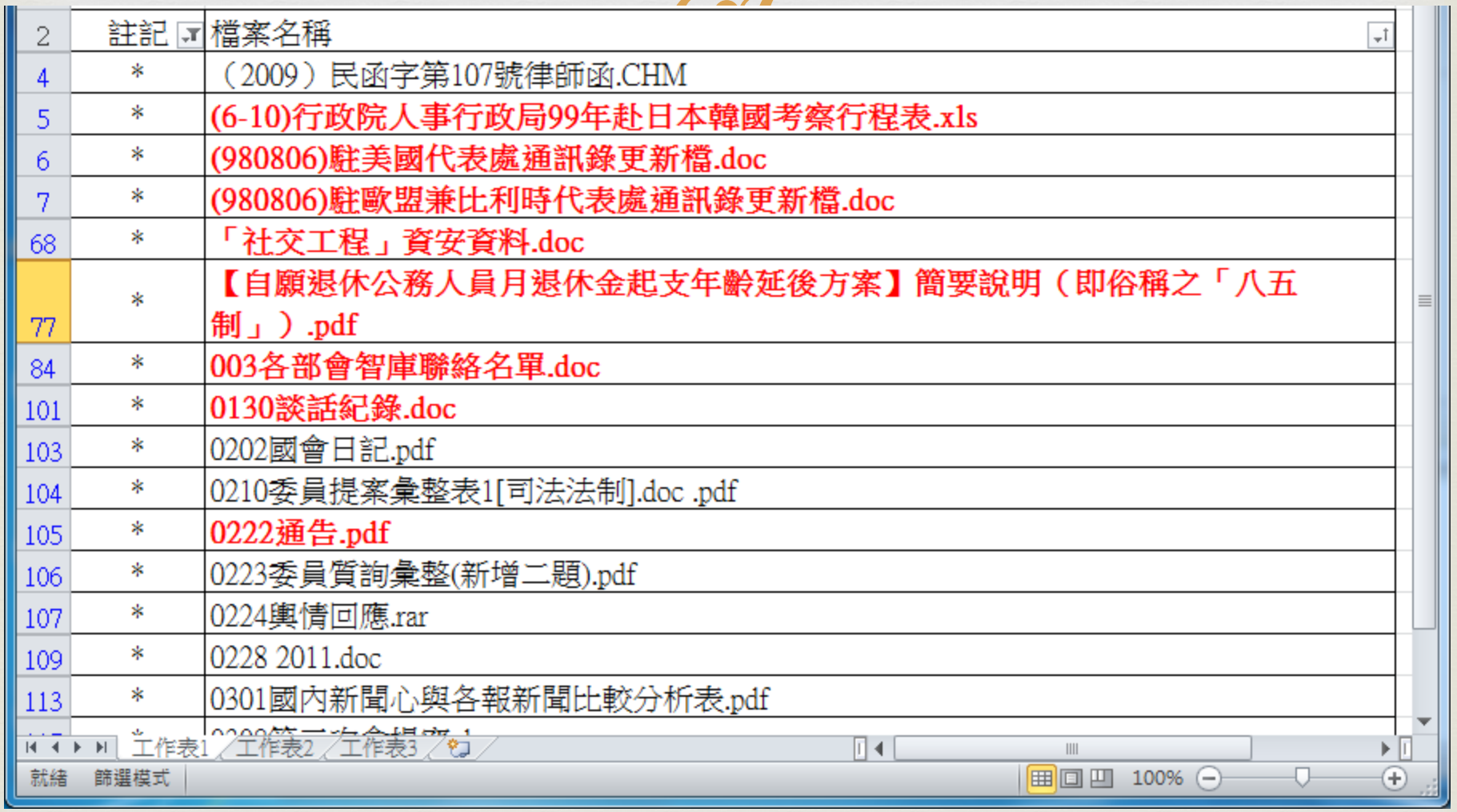
駭客入侵拍女子裸照 PO她部落格嗆聲

〔記者黃良傑／屏東報導〕還在連線的電腦不要亂放，並時常留意鏡頭有無不正常開機，因為駭客就在你身邊，小心全裸被偷拍還不自知！

男大學生扮駭客炫耀

新竹縣21歲曾姓男大學生扮駭客，侵入屏東縣一名陳姓女子的電腦，植入可自動開啟、恢復、傳輸的「彩虹橋木馬程式」，再透過網路遠端遙控，開啟女子電

E-mail 社交工程



2	註記	檔案名稱
4	*	（2009）民函字第107號律師函.CHM
5	*	(6-10)行政院人事行政局99年赴日本韓國考察行程表.xls
6	*	(980806)駐美國代表處通訊錄更新檔.doc
7	*	(980806)駐歐盟兼比利時代表處通訊錄更新檔.doc
68	*	「社交工程」資安資料.doc
77	*	【自願退休公務人員月退休金起支年齡延後方案】簡要說明（即俗稱之「八五制」）.pdf
84	*	003各部會智庫聯絡名單.doc
101	*	0130談話紀錄.doc
103	*	0202國會日記.pdf
104	*	0210委員提案彙整表1[司法法制].doc .pdf
105	*	0222通告.pdf
106	*	0223委員質詢彙整(新增二題).pdf
107	*	0224輿情回應.rar
109	*	0228 2011.doc
113	*	0301國內新聞心與各報新聞比較分析表.pdf

工作表1 工作表2 工作表3

就緒 篩選模式 100%

MSN 帳號被盜

微軟與警方合作　MSN帳號被盜24小時內可停權

林保宏
2011年7月9日 22:36

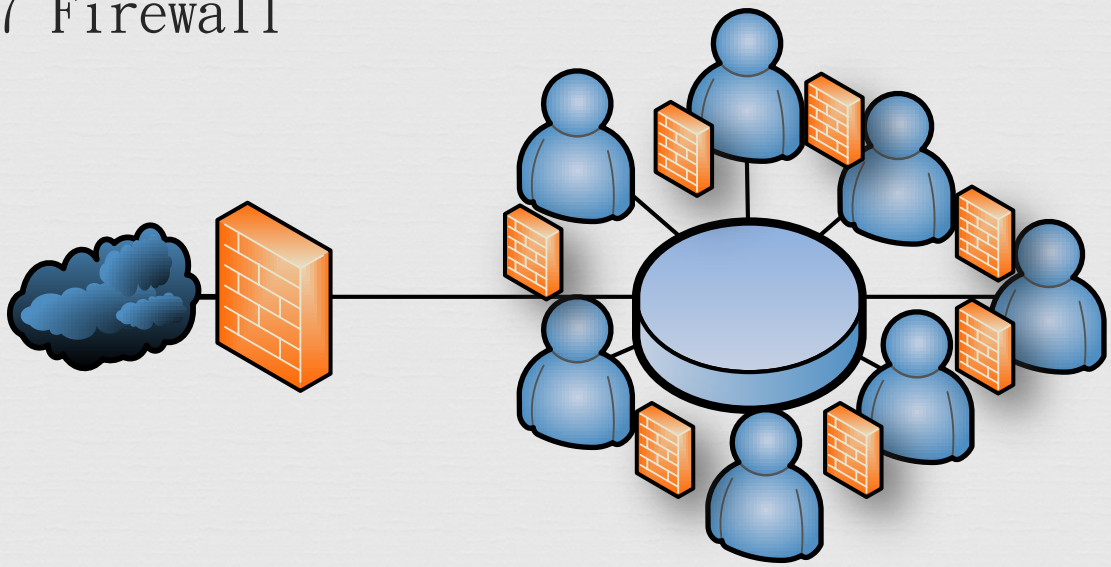
生活中心／綜合報導

近年來，網路連繫互動頻繁，但不少民眾發現在使用網路聯繫互動工具時，發現個人資料與帳號頻遭駭客入侵竊取資料，甚至遭盜用事件頻傳。刑事局昨日(8日)與微軟合作，建立一套快速封鎖被駭網路帳號的機制，以往網友MSN帳號被駭，需花一個月時間才能停權，現在只要撥打165專線或向各地警察局報案，統一由165單一處理窗口線上通知台灣微軟，24小時內完成停權。

微軟與警察局合作，未來網友如果有帳號被盜用情形，只要立即通報警方，微軟即會在24小時內完成停權。(圖／取自中央社)

資訊安全設定

1. 啟動個人防火牆
   - Windows XP Firewall config
   - Windows 7 Firewall



資訊安全設定

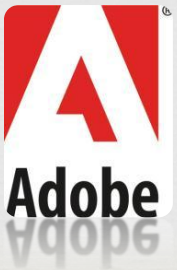
2.個人電腦安全設定

- IE 移除密碼記憶、清除Internet TEMP
- Mail設定純文字模式開啟信件
- 郵件規則有無設定自動轉寄不明人士
- 驗證身份(Email電子簽章，如國內自然人憑證PKI)
- 清除暫存檔(檔案怎麼刪也刪不掉)
- PC關閉自動讀取功能

  下載程式 Microsftfixit50471(disable).msi

資訊安全日常工作

1. 更新軟體修補程式
   - Microsoft Update (Windows、Office、SQL、IIS…)
   - Java Update
   - Adobe Update
   - Firefox Update
   - 其他：請到”官方”下載官方版本與更新



資訊安日常工作

2. 使用防毒軟體

- 防毒軟體安裝
- 隨時注意防毒軟體定期更新/手動更新(隔離電腦)
- 防毒軟體即時掃描/定期掃瞄/手動掃瞄

其他資訊安全相關注意事項

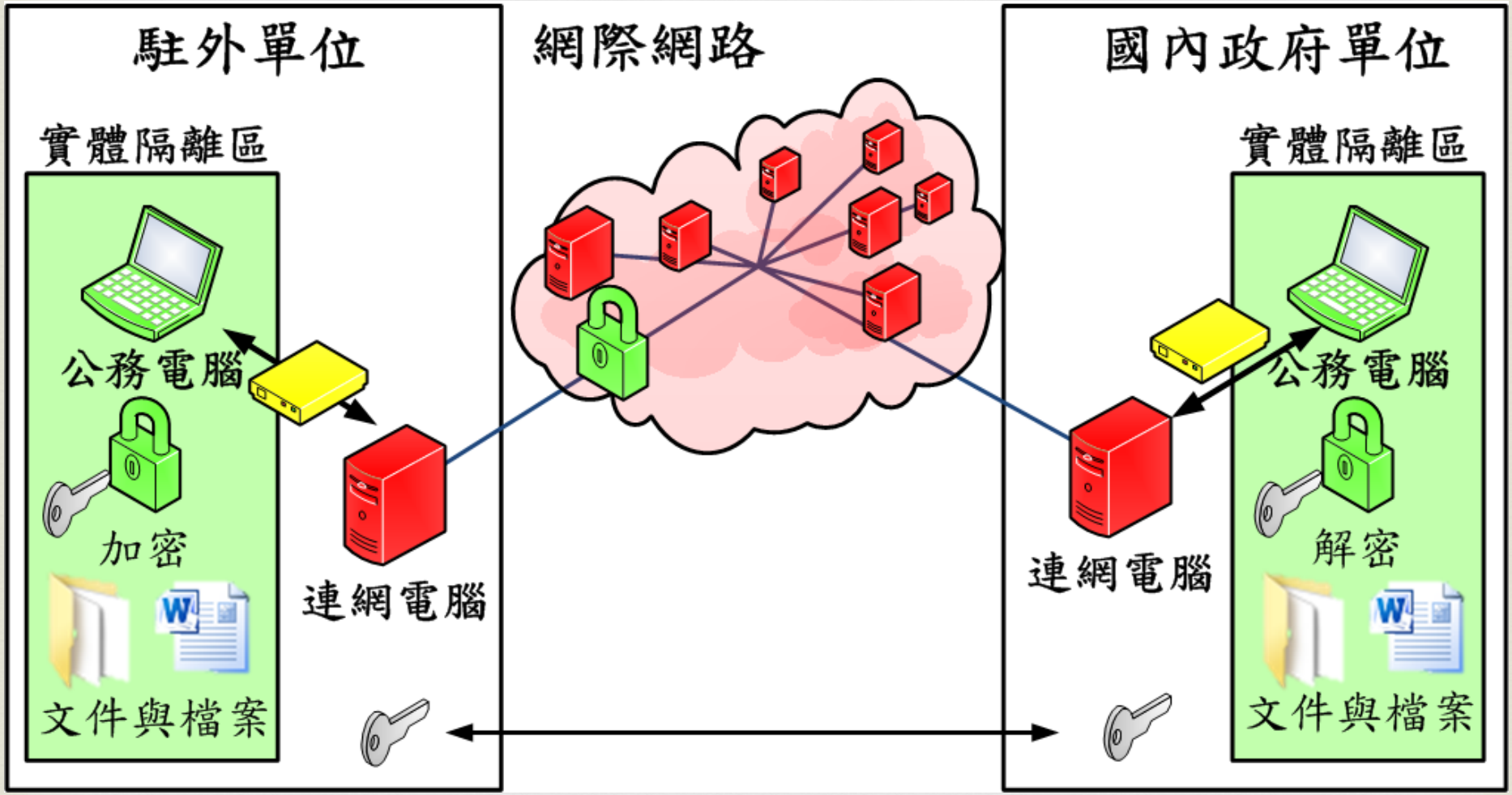
- 定期備份資料
- 慎灌軟體
- 勿將公事檔案下載回家
- 公務文件使用公務信箱
- 不要使用P2P分享軟體
- 螢幕設定鎖定畫面

其他資訊安全相關注意事項

- 注意假網頁、慎選點廣告頁
- 晶片卡及自人憑證移除
- 勿存重要資料
- 時時自我檢測電腦
- 注意防毒軟體更新

實體隔離

駐外單位公務傳輸架構圖



行動碟防護

使用操作

- 使用專用交換檔案的行動碟
- 交換前要先格式化
- 檢查行動碟狀態(於DOS下執行Dir /S)

行動碟電腦防禦措施

- 行動碟內放置（隱藏唯讀的檔案）

  autorun.inf（資料夾）0 Kbyte

  System Volume Information(檔案) 0 Kbyte

  RECYCLER(檔案) 0 Kbyte

  一旦發現檔案遭到置換就可能中毒了。

公文資料加密與傳輸

- 公文離線製作後，於上傳前會產生3種檔案。

  .sw（交換機關資訊）

  .dis（加密檔案）

  .di(未加密備份檔)、請移到加密碟內保存

- 請注意!!公文附件並未加密。

文件檔案加密與傳輸

檔案加密：

- 密碼長度至少8碼，可延長破解的時間。
- 密碼強度：數字、大、小寫字母、符號。

檔案傳輸：

- 加密過後的檔案，選擇安全的傳輸方式。
- （如：使用SSL 加密過的HTTPS://webmail）
- 透過加密傳輸可以更安全。

實體隔離規定

- 隔離電腦應隔絕網路並專用於公務作業
- 隔離電腦使用硬碟等載具傳送，使用前後需格式化
- 隔離電腦不可與上網電腦共用印表機
- 隔離電腦變更用途前須先格式化
- 資料加解密須在隔離電腦進行

個人資料保護法

- 個人資料保護法於99年4月27日立法院院會中完成三讀程序。施行細則目前正制訂中，預計100年11月25日公布。

- 個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

個人資料保護法

- 高達新台幣二億元的賠償上限與強調企業組織需負舉證責任的規範內容。
- 如果企業負責人（代表人、管理人或其他有代表權人）未能證明已盡防止義務，主管機關處以「罰鍰」來處罰企業負責人。
- 除賠償當事人外，經手個人資料的員工也要面臨2年刑期或20萬元以下罰金，
- 若是故意違法利用個人資料來營利，刑期更是加重到5年以下有期徒刑，或併科罰金1百萬元。

法務部全國法規資料庫 http://law.moj.gov.tw/

總結

面對資訊安全的不對稱性（易攻難守）以及攻擊手法之日新月異

如何做好資料保護是資訊安全的終極防線。

參考資訊

行政院國家資通安全會報

法務部全國法規資料庫

簡報完畢 敬請指教