資安法令宣導及案例分析

講師:李雋元
Email:ericph0617@gmail.com

講師簡介

- CISCO CCNA
- Novell CNA .CNE
- Microsoft MCP. MCP+I .MCSE MCSA2003 .MCSE2003 .MCSA2003 On Security .MCSE2003 On Security
- MCTS MCITP MCT2008
- CompTIA Security+. Project+
- Check Point CCSA. CCSE
- ISO27001/BS7799 Lead Auditor
- ISO20000/BS15000 Lead Auditor
- ITIL Foundation

專案經歷

- 國防部退除役官兵就業輔導資訊安全課程講師
- 警政署微軟Windows技術課程講師
- 中華電信第三代話務系統叢集備援系統導入
- 93年國防部通訊研究所無線網路802.1X安全技術講師
- 93年警政署BS7799課程講師
- 93年警政署資訊安全課程講師
- 94年苗栗縣警局資訊安全課程講師
- 94年度境管局資訊安全及BS7799簡介課程講師
- 94年度境管局內部稽核課程講師
- 94年度氣象局資訊安全課程講師
- 95年度國稅局PKI服務管理及建置課程講師
- 95年度海軍總司令部網路安全防護課程講師
- 96年度空軍總司令部網路安全防護課程講師
- 96年度氣象局資訊安全課程講師

課程大綱

- 前言
- 最新網路應用與潛在危機
- 資安法令與標準
- 常見的威脅與攻擊案例研討
- 個人資安最佳實踐

前言

- 數位社會對人類未來生活的影響
  - 數位科技與人類未來生活已逐漸密不可分
  - 電影「網路上身」、「關鍵報告」、「全民公敵」中的電影情節有可能真實上演
- 開啟潘朵拉盒子(Pandora's Box)

課程大綱

- 前言
- 最新網路應用與潛在危機
- 常見的威脅與攻擊案例研討
- 資安法令與標準
- 個人資安最佳實踐

網路新應用 vs 資安新威脅

- 網站瀏覽，電子商務
- 電子郵件
- P2P檔案分享程式
- IM即時通訊工具
- 網路電話
- Tunneling私人隧道
- ….Many….

網頁瀏覽的隱憂 (Web2.0的應用)

- Web2.0的概念在於以消費者為主角
- 即時，互動分享為主，注重消費者的參與的新網路商業模式
- 網路內容變成集體的創作分享。
- 提供網路相簿及部落格的無名小站還有開放共同線上撰寫的「維基百科」都是Web2.0的最佳代表

Web2.0技術安全威脅

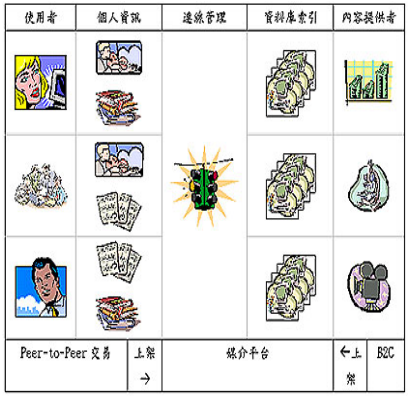
- 惡意軟體的途徑
  - Web2.0網站普及，不斷開發出更多具有互動能力的Web應用程式，為惡意程式開方便之門
- 個人資料洩密
  - 網路上透露個人所有秘密，包含你是王建民的頭號粉絲、你喜歡用網路進行股票交易等，殊不知簡單的交談卻容易洩密個人資料
- 社交工程的途徑
  - International Security Partners曾經成功模擬並執行的案例發現，駭客可以假裝到交友網站結識網友，在瞭解其興趣後取得信任，比如傳送「最喜歡的棒球選手即將被交易至其他球隊！」的運動網站報導連結，並暗中發動XSRF(Cross-site Reference Forgery 跨網站參照偽造)攻擊，藉以冒用受害網友的身份驗證資料，轉帳結清他原來的帳戶餘額。

電子郵件的隱憂

- 電子郵件的附件功能,成為攻擊的最佳管道與病毒傳播的平台
  - 病毒、蠕蟲與惡意程式等隱藏在電子郵件中，這些看似朋友所寄來的郵件，卻是應用病毒傳播的平台
- 如果員工開啟一個未經同意的電子郵件附件檔，或在開啟前沒有掃描附加文件是否有病毒；則企業就會很容易遭到病毒攻擊。確保員工不只是接受病毒的相關教育
- 開啟未預期或看起來可疑之附件檔的危險性；而且也必須讓他們知道執行病毒的後果。安娜・庫妮可娃(Anna Kournikova)與情書(I Love You)病毒是攻擊的“成功”例子，當極具吸引力的主旨激起收件人的好奇心時，便會使很多人開啟被感染的電子郵件。

對等網際網路技術（Peer-to-Peer， 簡稱P2P）

- P2P 除了檔案分享與即時通訊，也逐漸發展出不同應用，
- P2P網路的一個重要的目標就是讓所有的客戶端都能提供資源，包括頻寬、存儲空間和計算能力。因此，當有節點加入且對系統請求增多，整個系統的容量也增大。
- P2P 應用潛藏諸多風險，包括：
  - 洩漏企業內部機密資訊
  - 成為病蟲擴散的管道
  - 下載非法檔案
  - 侵犯著作權法爭議
  - 佔用大量網路頻寬
  - 影響其他系統正常運作
  - 造成員工分心，降低生產力



Skype

- Skype是支援語音通訊的即時通訊軟體
- 採用P2P(點對點技術)的技術與其他用戶連接，可以進行高清晰語音聊天
- 連線雙方網路順暢時，音質可能超過普通電話。
- 廣受歡迎原因
  - 低延遲通訊品質
  - 免費(或省錢)
  - 自由穿透防火牆
  - 全球都能通用
  - 傳大檔案
  - 跨平臺使用
  - 群組效應,多方通話
  - 撥打傳統電話
  - 傳遞內容避免被管理
  - 通話加密，在網際網路上進行傳遞能具高保密性
  - 使用簡單方便

Skype

- Skype是支援語音通訊的即時通訊軟體
- 採用P2P(點對點技術)的技術與
-

- 廣受歡迎原因
  - 低延遲通訊品質
  - 免費(或省錢)
  - 自由穿透防火牆
  - 全球都能通用
  - 傳大檔案
  - 跨平臺使用
  - 群組效應,多方通話
  - 撥打傳統電話
  - 傳遞內容避免被管理
  - 通話加密，在網際網路上進行傳遞能具高保密性
  - 使用簡單方便

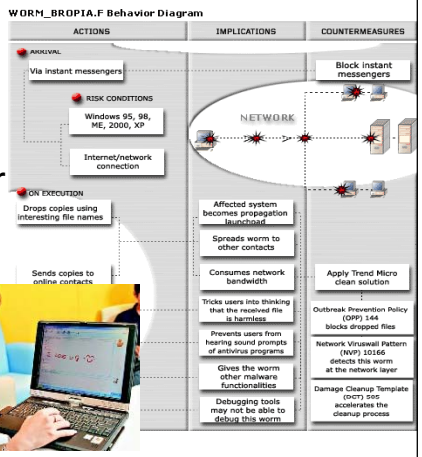
Skype的隱憂

- 使用80Port穿透防火牆
- 通話加密，無法管理傳遞內容
- 資料竊取風險大
- 後門開啟
- 使用頻寬大，約128kbps

IM的安全隱憂

Instant Messenger (IM)

- AIM (AOL IM)
- MSN
- Yahoo Massager
- ICQ
- YamQQ



課程大綱

- 前言
- 最新網路應用與潛在危機
- 常見的威脅與攻擊案例研討
- 資安法令與標準
- 個人資安最佳實踐

資訊安全的目標 (Information Security)

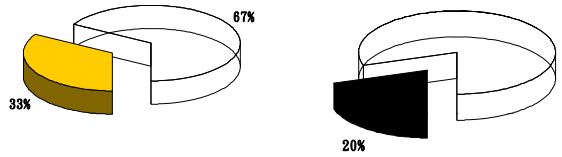
- 機密性(Confidentiality) 資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
- 完整性(Integrity)對資產之精確與完整安全保證的特性。
  - 可歸責性(Accountability) 確保實體之行為可唯一追溯到該實體的特性。
  - 鑑別性(Authenticity) 確保一主體或資源之識別就是其所聲明者的特性。
    鑑別性適用於如使用者、程序、系統與資訊等實體。
  - 不可否認性(Non-repudiation) 對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。
- 可用性(Availability)已授權實體在需要時可存取與使用之特性。
- 可靠性(Reliability)始終如一預期之行為與結果的特性。

隱私權(Privacy)與資訊安全

- 隱私權 (Privacy)
  - 指個人能控制其“私人資料”的權利,避免被揭露或未經個人同意而被使用
- 華爾街日報及美國廣播公司ABC最近民意調查美國民眾認為喪失個人隱私權是本世紀最大的顧慮,操過恐怖份子攻擊世界大戰及溫室效應

隱私權需求(缺乏信心)

- 30% 的美國民眾相信政府能確實的保護醫療計畫所涉及之個人資料隱私
- 20% 美國民眾認為醫療機構, 保險單位,政府機構及雇主曾不當的揭露其個人醫療資訊.
  其中50%認為個人有遭受困擾或損害



資安新威脅

- 根據 SANS 剛公佈的 2007 年 TOP 20 資安威脅報告書中指出：駭客的主要攻擊手法與目標
  - 漏洞入侵與零時差攻擊
  - 網路釣魚
  - P2P/IM 檔案分享功能
  - Web AP 的滲透
  - 網路設備的癱瘓

Word 瑕疵遭零時差攻擊(Zero day Word flaw used in attack)

- 微軟Word出現 “Zero Day”零時差攻擊漏洞事件，只要使用者開啟某一惡意Word檔案，就會被植入後門程式，駭客藉此即可遠端控制使用者的電腦。王應達表示：利用安全漏洞發動零時差攻擊，並藉機竊取資訊的情形並非首次發生，在此之前最近的一次是去年底的MS06-001(WMF攻擊)，這個弱點至今仍被廣泛地大肆利用，如駭客利用Bot傀儡程式用以偷竊使用者的網路銀行資料。
- 目前為數眾多的 TROJ_NASCENE特洛依木馬程式的變種也利用該漏洞，危害不少 Windows 使用者。而其得逞的關鍵，往往是使用者擋不住的好奇心誘惑，點擊附件或是連結。

PayEasy受「駭」 5400會員個資外洩

- 〔記者王珮華／台北報導〕國內第三大購物網站PayEasy昨呼籲使用者盡快更換密碼。
- 該網站表示，上週日晚間遭來自中國的不明人士，以身分證字號輸入會員帳號測試密碼達三萬九千多次，其中有五千四百筆資料帳號密碼正確被登入，隔天有十三位會員反應接到詐騙集團電話，PayEasy認為該事件非單一個案，極可能延燒到國內其他網站。
- PayEasy指出，今天上午十點起將開放會員查詢，其帳號密碼是否在此事件中被詐騙集團掌握。

PayEasy受「駭」 5400會員個資外洩

- 〔記者王珮華／台北報導〕國內第三大購物網站PayEasy昨呼籲使用者盡快更換密碼。
- 該網站表示，上週日晚間遭
會員帳號測試密碼達三萬九
正確被登入，隔天有十三位
為該事件非單一個案，極可
- PayEasy指出，今天上午十
此事件中被詐騙集團掌握。

無名小站凸槌 網友私密照曝光

- 擁有近兩百五十萬名會員，全台最大的相簿部落格「無名小站」，14日凌晨出現安全性危機，所有原本上鎖的相簿都可自由點閱，網友相簿個人隱私全都露
- 據了解，無名小站為避免類似問題發生，在會員註冊時，「申請同意書」中已載明「您使用本服務之風險由您個人負擔」，且「不保證本服務將不受干擾、及時提供、安全可靠或不會出錯」，會員隱私權益幾乎無法受到有效保障

無名小站凸槌 網友私密照曝光

- 擁有近兩百五十萬名會員，全台最大的相簿部落格「無名小站」，14日凌晨出現安全性危機，所有原本上鎖的相簿隱私全都露
- 據了解，無名小站註冊時，「申請同務之風險由您個人不受干擾、及時提會員隱私權益幾乎

網頁惡意內容攻擊

- Google最新統計，目前全台有九百八十四個網站被植入惡意程式碼，其中不乏知名的台灣奧迪汽車、ESPNSTAR體育台和眾多學術機構或商業網站。
  - 這些網站含有「隱匿強迫下載」惡意程式，網友看文章、欣賞照片時，不知不覺被安裝木馬、後門程式、間諜軟體或其他病毒軟體，電腦無故當機只是小case，嚴重時會竊取電腦中個人資料，曾在網路銀行輸入的帳號密碼，也可能被側錄。

網頁隱藏式惡意連結

- 又稱之為「網頁掛馬」
- 駭客入侵知名的網站
  - 不更改畫面下，修改網站內容，加入惡意程式碼或連結
  - 使用者瀏覽該網站時的被植入惡意程式進而竊取個人資料或當成跳板主機
  - 例:hxxp://ww2.spooots.com/index.html

P2P軟體使用洩密案

- *記者馬培治／台北報導 2007/04/13 20:51* 警局傳出筆錄因P2P軟體使用不當而外洩的事件，凸顯了P2P軟體在方便之外的安全威脅問題。 據媒體報導，國內若干警分局因員警違反資安規範，私下在警局公用電腦上安裝「Foxy」等點對點(P2P)檔案分享軟體，意外將案情筆錄等機密資料一併「分享」出去，使得相同軟體使用者可以透過搜尋檔名的方式，找到並下載筆錄等資料，造成資料外洩。
- 「從個人履歷、企業資料，乃至此次發生的警方筆錄，都已在輕忽中外洩」。

Gray ware的案例

- 美國國家電腦安全聯盟(NCSA)的調查發現：八成家庭電腦感染間諜軟體，但大多不知情。更令人驚訝的是，他們還在其中一個受訪者運行遲緩的電腦上，發現1000多個間諜軟體。

課程大綱

- 前言
- 最新網路應用與潛在危機
- 常見的威脅與攻擊案例研討
- 資安法令與標準
- 個人資安最佳實踐

為什麼需要資訊安全--法律上的要求

- 電子簽章法
- 智慧財產權保障
- 電腦處理個人資料保護法
- 與廠商的合約要求
- 刑法電腦犯罪章則
- 行政院及所屬各機關資訊安全管理要點
- 醫院電腦處理個人資料登記管理辦法
- 保險業個人資料檔案安全維護計畫標準
- 科技智財權保護有關之刑法增修條文(有關電腦犯罪部分)

為什麼需要資訊安全--法律上的要求

台灣商業軟體聯盟 (BSA) 對軟體侵權的介紹

- 使用者侵權

  通常發生於企業或員工間重製未經授權的軟體，又可分為以下幾種形式

  - 將一份獲得授權的軟體安裝在多部電腦當中
  - 將一份盜版軟體(如大補帖)安裝在多部電腦當中
  - 員工將自行取得的盜版軟體，帶到公司進行安裝或散佈
  - 員工將公司內部的軟體帶回家中進行拷貝或散佈
  - 購買升級版為軟體進行升級，卻並未擁有該軟體的合法舊版本授權
  - 不具有學術教育機構的資格，卻購買教育版軟體使用

為什麼需要資訊安全--法律上的要求

台灣商業軟體聯盟 (BSA) 對軟體侵權的介紹

- 硬碟非法預裝軟體

  某些電腦經銷商將未經授權的軟體灌裝到他們出售的電腦，以增加銷售誘因。購買新的硬體設備時，務必於驗收時確認所有硬體一同購買的原版軟體取得發票並附有授權書、磁片或光碟、以及相關文件。

P2P法律爭議~網路下載音樂

- 根據台北市消費者電子商務協會「網路下載音樂大調查」結果顯示，有85%的消費者曾經使用過網路下載音樂的服務、78%的消費者主要使用MP3或電腦聽音。網路下載音樂是無法改變的主流。
- 然而，唱片業者似乎還沒有這樣的心理準備。國內音樂交換的實際判決出來，可說是為數位音樂潮流與著作權衝突解決立了一個里程碑
- 一、P2P平台技術本身具中立性，使用該技術並不違法；
- 二、個別使用者透過P2P軟體所進行的檔案傳輸行為若逾合理使用範圍 仍屬侵權；
- 三、則是針對平台業者經營內容的侵權認定與否，將以其是否知悉其上使用者之非法使用情事做為判定標準，若不知情，則侵權責任屬使用者個人應負之 責任，若遭判定為知情者，則亦應負侵權責任。

為什麼需要資訊安全--法律上的要求

電腦處理個人資料保護法施行細則

- 第三十四條

  公務機關保有個人資料檔案者，應訂定電腦處理個人資料安全維護法令，其內容應包括資料安全、資料稽核、設備管理及其他安全維護等事項。

電腦處理個人資料保護法

- 個人資料：指自然人之姓名、出生年月日、身份證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。
- 個人資料檔案：指基於特定目的儲存於電磁紀錄物或其他類似媒體之個人資料之集合。
- 罰責為**告訴乃論**

為什麼需要資訊安全--法律上的要求

刑法電腦犯罪專章

- 第三百五十八條 (入侵電腦或其相關設備罪)

  無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第三百五十九條 (破壞電磁紀錄罪)

  無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
- 第三百六十條 (干擾電腦或其相關設備罪)

  無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

為什麼需要資訊安全--法律上的要求

刑法電腦犯罪專章(續)

- 第三百六十一條 (加重其刑)

  對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

- 第三百六十二條 (製作犯罪電腦程式罪)

  製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

- 第三百六十三條 (告訴乃論)

  第三百五十八條至第三百六十條之罪，須**告訴乃論**。

為什麼需要資訊安全--法律上的要求

- 與廠商的合約要求
  - 對象：系統開發人員、環境清潔人員、保全人員、工讀生、短期約聘人員
  - 服務水準協議（Service Level Agreement；SLA）
  - 保密協議（Non-disclosure Agreement）（個人、組織）
    - 保護各項資訊資產的程序
    - 檢查資產是否遭受破壞
    - 合約終止或在有效期間歸還或銷毀資訊
    - 對複製和揭露資訊的限制

為什麼需要資訊安全--法律上的要求

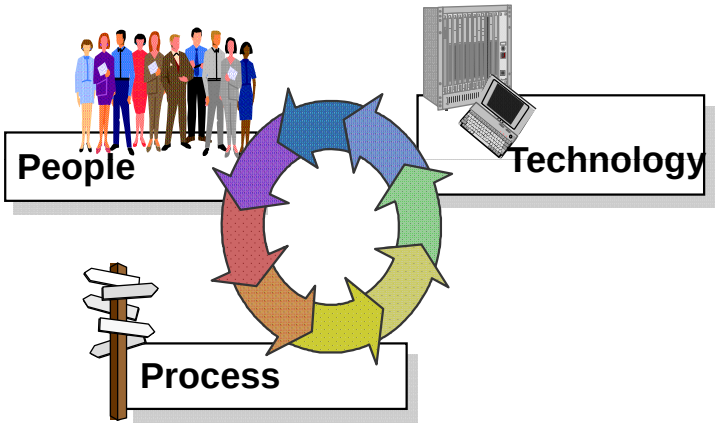
- 行政院及所屬各機關資訊安全管理要點
  - 五、各機關應就下列事項，訂定資訊安全計畫實施，並定期評估實施成效：

（一）資訊安全政策訂定。
（二）資訊安全權責分工。
（三）人員管理及資訊安全教育訓練。
（四）電腦系統安全管理。
（五）網路安全管理。
（六）系統存取控制管理。
（七）系統發展及維護安全管理。
（八）資訊資產安全管理。
（九）實體及環境安全管理。
（十）業務永續運作計畫管理。
（十一）其他資訊安全管理事項。

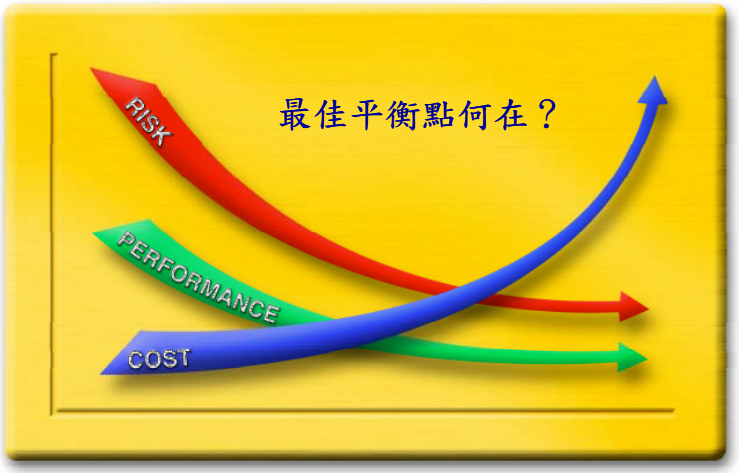
課程大綱

- 前言
- 最新網路應用與潛在危機
- 常見的威脅與攻擊案例研討
- 資安法令與標準
- 個人資安最佳實踐

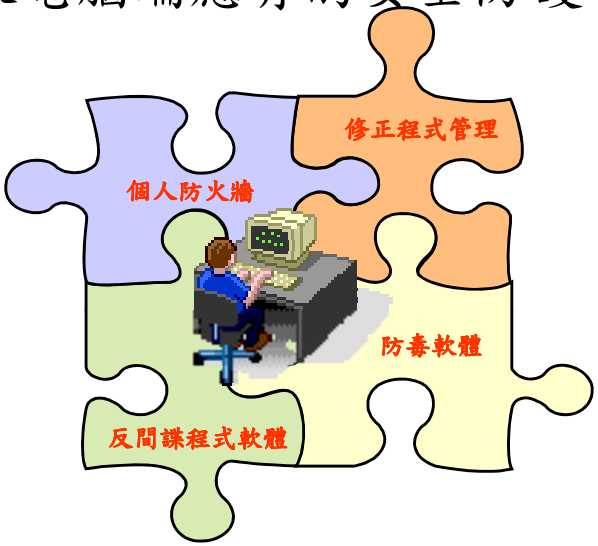
資訊安全管理的三要素



資訊安全問題無法完全根治



個人電腦端應有的安全防護



個人資訊安全實踐

- 避免下載來歷不明的檔案與安裝程式。
- 維持防毒軟體的病毒定義檔為最新狀態
- 安裝用戶端防火牆保護系統
- 來歷不明電子郵件過濾
- 避免不明來歷的檔案與安裝程式
  - Flash Game
  - Java Game
  - 免費軟體
  - 廣告軟體
  - 共享軟體

個人資訊安全實踐

- 經常性的維護系統安全-Windows Update
- 登入本機的密碼強度與複雜度
- 盡量避免網芳分享
- 避免瀏覽不熟悉的網頁
- 收信前確認病毒定義檔為最新狀態
- 收件匣避免預覽啟動
- 安裝垃圾信件過濾器
- 禁止儲存密碼於瀏覽器

網路釣魚(Phishing)的防範

- 感覺網站有點怪怪的
  注意觀察登入程序、使用者身份認證程序，或是顯示出來的訊息，是否和以往不同？
- 要求使用者提供過多的個人訊息
  網路釣魚(**Phishing**)網站通常都會要求使用者提供額外的身份辨識或是個人私密資料，這些資料大部份之前就已提供給銀行做為對照之用。
- 在瀏覽器上看不到 SSL 加密鎖的標識
  合法的網站，在要求使用者提供機密資料時，通常都會對該程序進行 SSL資料加密的動作。請使用者注意瀏覽器下方是否出現「加密鎖」的圖示，並可在該圖示上雙按滑鼠左鍵，檢查該項SSL證明是否真實無誤。
- 網址列未出現表示安全網路連線的https字樣
  當使用者進入安全的網路連線時，網址列應該是以https//開頭（多個s字母），而非原本的http://。而Pharming 網站一般都不具備 SSL 安全網路連線的能力，也就是說，既使在要求使用者提供機密資料的網頁上，其網址起始字串仍然是普通的 http://。
- 瀏覽器會出現SSL 認證有問題的警示視窗
  如果駭客對具有 SSL 認證功能的網站進行詐騙時，使用者的瀏覽器會顯示安全認識有問題的警示訊息。建議使用者最好不要忽略這些警告，把握此機會檢查認證，注意其是否為惡意的詐騙網站。

建立安全認知(Awareness)

- 使你的企業已經有安全政策，但工作尚未完成。
  政策必須要與所有人溝通且讓每個人都能瞭解。
  - 發送印刷品禮物(鉛筆、滑鼠墊等等)，並且在辦公室的牆上張貼海報與標誌，以推廣您的安全認知訊息。
  - 要求所有新員工約略的瞭解安全的情況
    - 提供他們小提示以決定什麼資訊(電腦與紙張)是機密的且如何保護這些資訊。
    - 協助他們真正的認識企業所擁有之資訊的真正價值。
    - 讓他們知道社交工程的風險。
  - 鼓勵目前的員工參加安全進修訓練。

Reminder !

- Information Protection is …
- EVERYONE'S Responsibility