新高中資訊及通訊科技科知識增益系列：

（九）網上威脅及保安

2010年2月4日

講者：譚俊基 (Lawrence Tam)
互聯網專業協會

OFTA
電訊管理局

討論內容

- 資訊安全概念 (Security Basic)
- 資源保護 (Resources Security)
  - ✓ 終端用戶資源 (Endpoint)
  - ✓ 網絡資源 (Network)
  - ✓ 伺服器資源 (Server)
  - ✓ 資訊儲存資源 (Database)
- 結論：資訊安全的良好的習慣

OFTA
電訊管理局

第一部：資訊安全概念
(Security Basic)

OFTA
電訊管理局

資訊安全是什麼?

保護資訊資產 (Information Assets) 的
機密性 (Confidentiality)、完整性 (Integrity) 與可用性 (Usability)

機密性

機密性是資訊安全中最重要的一環，確保資訊的存取或作業是經許可及授權。

違反原則的例子：
沒有老師們的許可權或授權，學生從學校伺服器下載考試試卷

完整性

資訊經常需要更新，完整性是確保資訊和流程方法的準確和完善。

違反原則的例子：
學生交給學校的個人資料不應在沒有知會的情況下被未經授權人士更改

可用性

一個學校產生或儲存的資訊要能讓被授權者使用，可用性是確保被授權的人需要時可以獲取資訊和相關的資料。

違反原則的例子：
因為電流中斷或電腦中毒引至無法開機

OFTA 電訊管理局

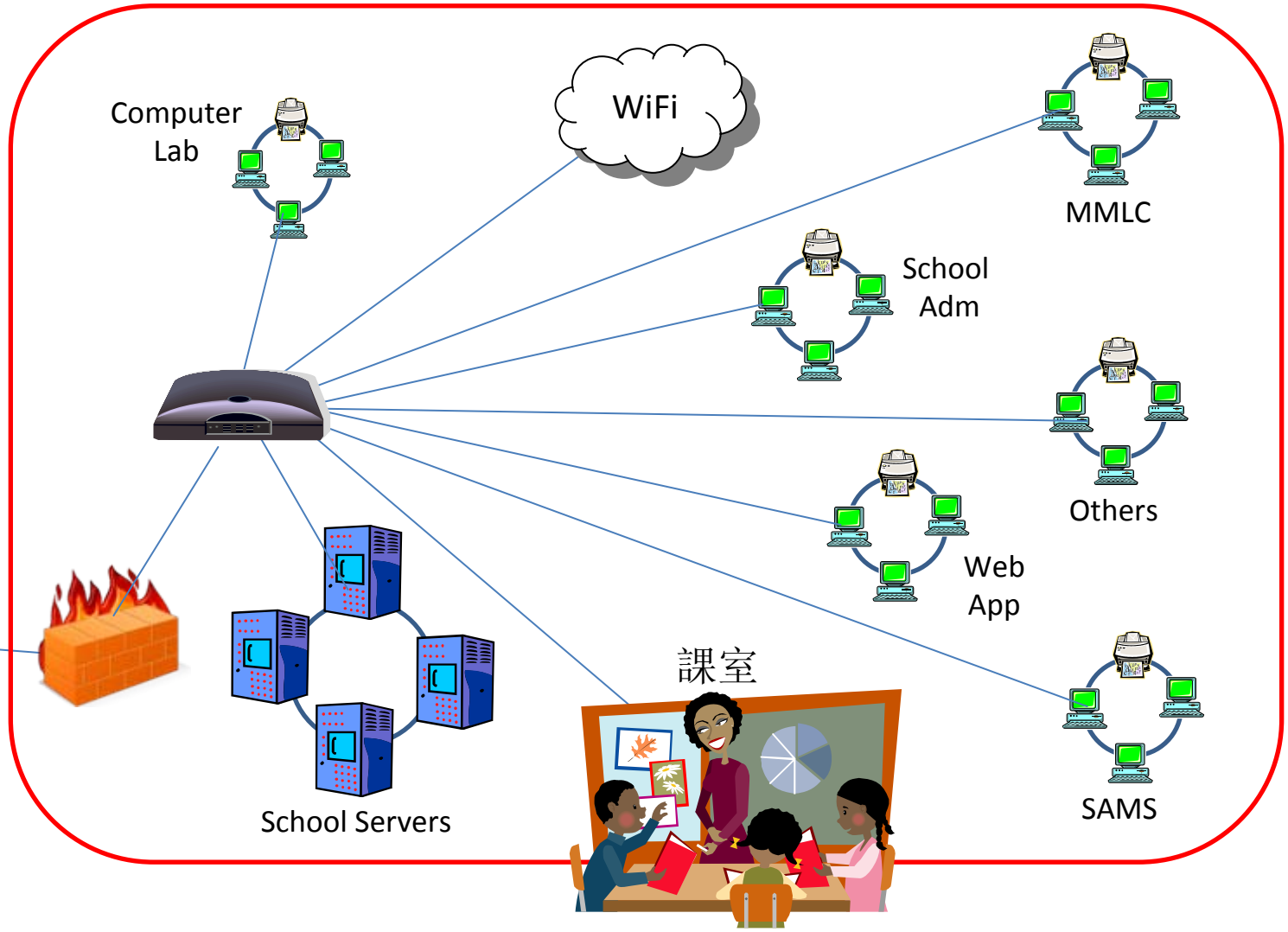
我們需要識別並消除安全威脅 (Security Threat) 和缺陷 (Venerability)

企業及學術機構資訊安全之差異性

	企業	學術機構
營運方針	商業行為主導	服務社會為主導
管理模式	中央控管	支援
管理機制	著重組織管理機制	著重設備機制組織
人員定位	明確	混淆(老師，職工，學生)

OFTA
電訊管理局

典型的學校網絡圖



OFTA
電訊管理局

學校資訊安全弱點及威脅

- 系統漏洞
- 人為疏失
- 服務需要或過於注重方便
- 無危機意識(該防未防)
- 無專人負責之系統
- 實在環境不良
- 軟性安全機制不足
- 角色定義不明確
- 無所謂 (發生問題不覺得有影響)
- 病毒
- 駭客入侵 (IPS/IDS)
- 阻絕服務 (DDoS)
- 垃圾郵件
- 資料或電腦被偷竊
- 資料竄改
- 操作不當
- 系統失效 (硬件系統、作業系統、應用系統、網絡系統)

OFTA
電訊管理局

校園資安事件案例

- 學校成為駭客目標，小學網站變駭客基地

  某小學網站頻遭電腦駭客入侵，並利用學校網站大量自我複製的惡意程式癱瘓網站，再利用網絡傳播到其他地區網站，不僅家長及師生使用不便，還引發外地網站不滿；有些學校自行刪除入侵亂碼，還遭駭客放更多病毒程式報復，令校方不堪其擾。

- 高中駭客，入侵成功很爽

  某中學發現該校兩名學生一年多以來偷遍全校辦公室財物，並利用晨間6:30到7:10空檔，使用課室內的電腦，利用燒片、複製等方式，竊走全校學生詳細個人資料，及全校教職員的帳號與密碼，並利用此帳號密碼入侵學務系統，竄改學籍資料與成績。

OFTA
電訊管理局

第二部：資源保護
(Resources Security)

OFTA
電訊管理局

資源保護

- 資源保護的分類
  - ✓ 終端用戶資源 (Endpoint)
  - ✓ 網絡資源 (Network)
  - ✓ 伺服器資源 (Server)
  - ✓ 資訊儲存資源 (Database)

OFTA
電訊管理局

第二部：資源保護 (Resources Security)

2.1 保護終端用戶資源 (Endpoint Protection)

OFTA
電訊管理局

保護終端用戶資源 (Endpoint)

- 安裝全方位的防毒軟件。
- 重要檔案要做加密，並定時做資料備份。
- 打印的機密文件應放置於櫃中並上鎖。
- 下課時，老師辦公枱應保持淨空，不將文件放置桌上。
- 個人電腦應設定螢幕保護程式，並設定密碼。
- 離開座位時，電腦應登出並用密碼保護，防範他人使用。

OFTA
電訊管理局

不安全的密碼設定是大問題！

- 電腦密碼避免用以下方式組成：
  - ✓ 生日組合或電話號碼 (990312)
  - ✓ 簡單的英文單字(health)
  - ✓ 家人、情人或寵物的名字(honey)
  - ✓ 帳號反過來打(password->drowssap)
  - ✓ 出現頻率高或連續性的密碼(admin、1234、abcd)
  - ✓ 一“碼”在手、行遍天下
- 不在不安全的電腦(網吧、共用電腦)輸入密碼
- 你的密碼應該要設定：
  - ✓ 大小寫、符號、數字混合(I+amWork@62870875)
  - ✓ 長度足夠(至少八碼)
  - ✓ 定期變更密碼（建議最少每三個月要變更一次）

OFTA
電訊管理局

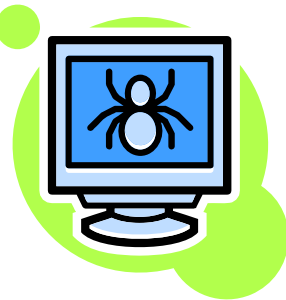
認識駭客！

- 駭客（Hacker）一詞最初是為優秀的程式設計師 (Software Developer) 所取的稱呼，他能夠把一個應用程式組合起來或拆開來去解決問題。
- 如今，駭客被定義為非法搜尋和滲透電腦網絡存取和使用資料的人。

OFTA
電訊管理局

電腦病毒

- 電腦病毒(Virus)：電腦病毒雖然只是一種電腦程式，但能在用戶不知情或批准下，自我複製及執行，並感染其他程式；電腦病毒往往會影響受感染的計算機的正常運作。
- 電腦蠕蟲(Worms)：此型的病毒不會攻擊其他程式，它只會不停的複製自己，再利用網絡傳播到其他伺服器，最後所有的伺服器將忙著複製、傳播病毒，沒空服務其他合法的使用者。
- 暗門程式(Trapdoor)：這程式利用伺服器中未公開的秘密通道自由進出系統，而不被別人發現。
- 特洛依木馬(Trojan Horse)：木馬的公有特性是通過網絡或者系統漏洞進入使用者的系統並隱藏，然後向外界洩露使用者的資訊。



OFTA
電訊管理局

電腦病毒

- 間諜軟件(Spyware)：這是一些專門在用戶不知情的情況下收集用戶的個人資料。它所收集的資料可以從該用戶平日瀏覽的網站，到諸如用戶名稱、密碼等個人資料。
- 廣告軟件(Ad-ware)：以廣告為目的，例如會不斷彈出「電腦網絡」或「系統效能低落」等廣告。許多使用者未經詳查，便會不慎地經安裝了以廣告為目的的廣告軟件。有時甚至並未經其許可自動執行，雖然大部分對電腦無害，但在系統中造成惱人效果，並影響使用。
- 語音垃圾郵件(Voice Spam)：與VOIP有關的垃圾資訊，通過網絡電話傳播大量未驗證資訊以致癱瘓全個電話系統。
- 釣魚網站(Phishing)：實際上，釣魚網站是一種以盜竊個人資料的欺騙手法，罪犯會以合法組織或知名公司，例如網上銀行等，誘導用戶在網上透露個人或財務信息，包含用戶名，密碼，信用卡，以至身份證號碼等。

OFTA
電訊管理局

各種病毒的比較

	主要目的	損傷 可能性	複製	保護措施
一般病毒	損失數據	高	✓	刪除 / 損失 資料恢復
電腦寄生蟲	迅速蔓延	高	✓	刪除 (添加個人防火牆)
特洛依木馬	損失數據 資料外洩	高	X	刪除
間諜軟體	資料外洩	高	X	刪除
廣告軟體	使用不方便 讓人反感	低	X	刪除 (手動或工具)

OFTA
電訊管理局

第二部：資源保護
(Resources Security)

2.2 保護網絡資源
(Network Protection)

OFTA
電訊管理局

保護網絡資源 (Network)

- 今天在互聯網上有很多的資源，通過不同類型的方法大部分學校都已連接到此“資訊公路“ (Information Highway)，例如：寬頻連線。
- 同時，有些學校可能會允許遠端存取資料(Remote Access)，例如老師們可能晚上需要上學校的伺服器來安排第二天的教材，在一些緊急的情況下，你的系統管理員也可能需要用家裡的電腦遠端存取學校的教學和學習網絡。
- 為了保護你的學校遠離攻擊 ，應實現相應的安全措施。此外，你應該教導一些外部網絡上的使用者(學生，家長等)如何安全地使用和監察他們的訪問。

OFTA
電訊管理局

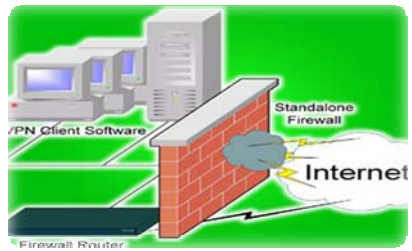
無綫網絡安全

- 無綫網絡安全往往是網絡安全中最弱的一環(the weakest link), 請不要掉以輕心。
- 不同無綫網絡的路由器(router)的預載設定不同，安裝時必須檢查設定及作適當的修改。
- 避免使用WEP (Wired Equivalent Privacy)，因為有可能在數十分鐘或數小時被攻破。
- 建議選用WPA / WPA2 (Wi-Fi Protected Access)，如用Pre-shared Key，建議用較長的字串及定期更改。
- 建議選用隱藏SSID(Service Set Identifier)設定及選用MAC Address Filtering (MAC 位址是網絡硬件唯一識別碼)。
- 不要把無綫網絡的路由器(router)放得太近窗口，從以減低外面能接收的訊號。

OFTA
電訊管理局

防火牆能做什麼？

- 防火牆是一種軟件或硬件，它就像一個屏障，會監視與限制在你的電腦與網絡或網際網絡之間流通的資訊，防止有人由防火牆之外，未經你的同意就嘗試存取你的電腦。
- 防火牆可幫助阻擋試圖透過外網(Public Network)或內網(Internal Network)進入你電腦的駭客(Hacker)、病毒(Virus)和蠕蟲(Worm)。
- 要求你的權限以封鎖或解除特定連線要求的封鎖。
- 建立安全性記錄。防火牆會記錄連線到你電腦的所有成功及失敗嘗試。這個記錄可作為有用的疑難排解工具。
- 你並不一定要使用Windows 的防火牆，你可以安裝並使用其他任何防火牆。評估其他防火牆的功能，然後決定哪個防火牆最符合你的需求。如果你選擇安裝另一個防火牆，請關閉Windows的防火牆。



OFTA
電訊管理局

防火牆不能做什麼？

- 不能偵測或停用電腦內早已有的病毒及蠕蟲。基於此理由，你也應該安裝防毒軟件並常常更新，保持在最新狀況。
- 不能封鎖垃圾或來歷不明的電子郵件使它們不出現在你的收件匣中。不過，有些電子郵件程式及防毒軟件可以幫助你做到這點。
- 不能阻止你開啟電子郵件內有危險的附件。不要開啟來自不明寄件者且含附件的電子郵件。如果郵件主題只是胡說八道或對你完全沒有意義，即使你知道並信任電子郵件的來源，請在開啟之前先向寄件者查詢。

OFTA
電訊管理局

統一反威脅管理系統(UTM)

- Unified Threat Management – 統一反威脅管理系統是最先進、最高級的防火牆。它集合硬件及軟件於一身， 除了基本防火牆功能，可以同時達到以下功能：
  - ✓ Protected Virtual Private Network (VPN) – 安全虛擬私人網絡
  - ✓ IPS/IDS - 入侵保護/入侵偵測
  - ✓ DDoS - 分散式拒絕服務
  - ✓ Anti-virus - 防病毒
  - ✓ Anti-spam - 反垃圾郵件
  - ✓ Content Filtering - 內容篩選過濾

OFTA
電訊管理局

第二部：資源保護 (Resources Security)

2.3 保護伺服器資源 (Server Protection)

OFTA 電訊管理局

物理安全 (Physical Security)

- 電腦機房位置
  - ✓ 避免放在低層及頂層，以防水浸或漏水。放在學校中層同時有一個好處是網絡線到那裡的距離都差不多，方便安裝。
- 門禁管制措施
  - ✓ 在各出入口與重點安裝監控攝影機。
  - ✓ 進入機房區必須先經刷卡確認身份，如有能力建議加指紋辨識或類同系統。
- 供電措施
  - ✓ 為了避免電力中斷, 建議最少使用雙供電迴路及不少過一小時的UPS。
  - ✓ 最好也加上調壓保護 (Power Surge Protection)來保護伺服器。
- 滅火系統 (Fire Suppression System)
  - ✓ 機房應採用防火建築材料。
  - ✓ 安裝多個滅火筒 (每年檢查)。
  - ✓ 如果可以，建議增加氣體滅火系統。

OFTA
電訊管理局

權限控制(Access Control)

- 身份驗證(Authentication)及授權(Authorization)是十分重要的保護元素，不能丟以輕心。
- 分配合適的許可權和責任給校長，全職教師、代課教師、 學生、 工作人員等。同時，根據每人的工作與需要，常常修訂使用者權限。
- 限制學校資料讀取與更改，也記錄所有訪問。
- 限制用電腦的時段及時間，所有電腦都應要求身份驗證。

OFTA
電訊管理局

第二部：資源保護 (Resources Security)

2.4 保護資料數據儲存資源（Database Protection）

OFTA 電訊管理局

保護資料數據儲存資源

- 資料分類

(Data Classification)

- 資料的備份和恢復

(Data Backup and Recovery)

- 敏感性資料保護與處理

(Sensitive Data Protection and Disposal)

OFTA
電訊管理局

資料分類

- 公共資料 (Public Data)
  - ✓ “公共”資料是指公開的資料，例如學校日曆、 校巴時間表、 活動計畫等、 一般只給所有用者讀取權限但不能修改。
- 私人資料(Private Data)
  - ✓ “私人”資料是指存儲在個人的電腦及數據庫內的文檔，只可以由擁有人讀取與修改。
- 限制資料(Restricted Data)
  - ✓ “限制”資料是指那些資料只給相關學科老師們讀取與修改(很多時候加密的，例如試卷)

OFTA
電訊管理局

資料的備份和恢復

- 備份是指將檔案系統或資料庫系統中的資料加以複製，一旦發生災難或錯誤操作時，得以方便而及時地恢復系統的有效資料和正常運作。
- 最好將重要資料製作三個，或三個以上的備份，並且放置在不同的地方，以利日後回存之用。一般做法是每天做差異備份，每週做主要資料庫備份，每月做全系統備份 (Grandfather, Father and Son System)
- 在備份的過程中，可以對資料進行各種處理，這些不同的處理方式可以改善備份速度，恢復速度，增加資料安全性，提升傳播媒介的利用率。

OFTA
電訊管理局

資料備份建議

- 安排指定人手 (例如: 系統管理員)負責做定期資料的備份和恢復。同樣重要的是定期測試備份檔案還原是否能正常運作。
- 個人電腦方面，一個500G的硬碟比二個250G的硬碟便宜，但建議用二個250G的，算是分散風險。同時建議另外購買外接式硬碟來做雙重備份，這樣才不會有遺憾的那一天。如果你的電腦有光碟燒錄機，也可以定期以光碟片(CD-R或DVR-R)來做備份。
- 同時，全學校的網絡上也建議安裝附加網絡存儲系統(NAS – Network Attached Storage)，因爲NAS十分成熟，可以給學校較穩定的數據存儲，以致于容易管理。

OFTA
電訊管理局

敏感性資料保護與處理

- 你可以考慮利用不同的加密工具來提高保護敏感性資料的安全級別 (例如：MS Windows 2000 中的EFS資料加密功能，指紋加密硬盤等)。
- 此外，你也可以考慮啟動一些軟件的密碼保護功能 (例如：Microsoft Office) 來保護包含敏感性資料的文檔。
- 同樣重要的，在換電腦或硬盤前，你應將所有資料完全清除，處理或銷毀。MS的刪除(Delete) 功能是不能完全清理數據。

OFTA
電訊管理局

防護用的資訊科技設備及服務

- 整合式威脅控管平臺 (Unified Threat Management)
- 防毒軟體 (Anti-virus Software)
- 防護管理服務 (Managed Security Services)
- 指紋辨識 USB 手指
- 加密虛擬專用網路 (Secured Virtual Private Network)
- 數據加密軟件 / 硬件 (Data Encryption Software / Hardware)

OFTA
電訊管理局

結論：資訊安全的良好習慣

OFTA
電訊管理局

沒有絕對的安全

- 安全設備非萬能，也沒有100%安全的系統，只要有連通性(Connectivity)就意味著有風險(Risk)。
- 看不見問題，並不代表沒有問題。
- 資訊安全是持續性的工作，而其防護措施也沒有極限。
- 資訊安全領域不只是網絡安全而已，還要防駭客、病毒等。
- 便利性和安全性總是相衝突的，實施的控制措施應該是在合理的平衡點(成本與效益)。(Strike The Balance)
- 了解真正問題點(弱點)，並施以正確的控制措施。
- 資訊安全措施的實施，在於降低至可接受之風險程度。

OFTA
電訊管理局

不要使用P2P軟件！

- 不要使用P2P軟件下載有版權的軟件或檔案:
  - ✓ P2P軟件是透過點對點方式傳輸檔案，例如BitTorrent、Foxy、迅雷、PPStream等。
  - ✓ 有版權的檔案或軟件未經授權而下載使用，即會侵犯到知識產權。
  - ✓ 檔案來路不明，可能包含木馬或病毒程式，容易使你的個人資料曝露在網絡當中。

OFTA 電訊管理局

FOXY

迅雷看看 www.xunlei.com

PPS.tv

資訊安全的好習慣

- 盤查不明人士
- 小心社交網站
- 登出不用電腦
- 保護機密資料
- 備份重要數據
- 鞏固密碼設定
- 更新應用系統
- 升級防毒軟件
- 小心使用網絡
- 過濾電子郵件

- ✓ 只使用合法及獲授權的軟件硬件
- ✓ 遵照互聯網絡上的使用道德準則
- ✓ 對資安事件認真了解和妥善處理
- ✓ 加強對學生及教職員的資安教育

OFTA
電訊管理局

謝謝。

OFTA
電訊管理局