ch27 互聯網上的保安及威脅(一)

保安威脅

惡意軟件	電腦病毒/ 蠕蟲/ 木馬程序
間諜軟件	暗中取得用戶資料
廣告軟件	廣告以跳出式視窗

木馬(假裝有用程序)盜取資料信用卡碼

傳播方法

唯讀光碟,軟磁碟傳播,電郵傳播(通訊錄)

互聯網 P2P 檔案分享軟件,

存貯媒體 (USB 快閃記憶體）

保安應用軟件

抗電腦病毒軟件	有效運作
隔離或刪除	定期更新病毒資料
還原程序碼	電腦運作時同時啟動
利用病毒識別碼檢查	檢查收到的檔案

抗間諜軟件程序 偵測不正常系統活動

防火牆軟件 檢查網絡流量，決定接受或拒絕來源地和目的地協定位址/類型

瀏覽器的保安問題

支援互動功能

外掛程序擴展瀏覽器功能

ActiveX 及 Java 應用程序

VBScript/JavaScript 指令碼

防病毒軟件/ 操作系統/ 軟件修正檔

自動檢查軟件更新

垃圾電郵

設立灰名單

黑白名單

條件過濾

家中連接至學校網絡

虛擬私人網絡

學校安全使用電腦指引

不下載/執行不明檔案

不開來歷不明電郵附件

未經防毒軟件掃描,避用可攜式

ch28 互聯網上的保安及威脅(二)

互聯網對私隱的威脅

駭客入侵	擅自存取他人電腦資料
垃圾郵件	1. 浪費時間檢查,
	2. 減慢網絡存取速度
	使用垃圾郵件過濾軟件
仿冒詐騙	仿冒電郵,仿冒官方網站的超連結,要求輸入個人資料
	1. 切勿開啟來源不明電郵
	2. 檢查是否真正官方網

保護私隱的方法

匿名瀏覽	代理伺服器作為中介(翻牆)
瀏覽時	刪除瀏覽暫存檔 Cookies
	停止電腦檔案分享
	只用可信的無線網絡
保護密碼	不用易被猜中的資料作密碼
	如：身份證號碼和出生日期
	密碼以數字+符號+大小寫字母混合
	不記錄在紙或裝置上/ 定期更改密碼
	不要在不同系統上使用同一組密碼

加密技術

香港的公開密碼匙基礎建設(PKI)

非對稱密碼匙

香港郵政證明公開密碼匙的真偽

香港郵政核證機關負責提供,簽署和管理「電子證書」/ 數碼證書

P2P 軟件引致

容易分享翻版

增加病毒傳播

超連結 vs P2P

優:出處較可靠

缺:傳送時中斷,重新下載

存取控制 - 認證及授權

認證方法	授權
用戶名稱、密碼	存取控制表：記錄網絡上存取時保安權限 (存取模式：唯讀/ 寫入/ 修改)
IP, 數碼證書	
指紋/ 臉部特徵	

保護網上交易

數碼證書(電子證書)

確認個人身份的電子簽署

一條公開及一條私人密碼匙

公開匙 - 通訊時向對方發送

私匙 - 代表個人或機構身份(自行保管）

辨別網上交易雙方的身份

應用：保密電郵, 網上理財

https = 超文本傳輸協定(http) +保密插口層(SSL)

防止他人截取和翻譯傳輸途中的數據封包

其他保安措施

雙重認證 (與密碼及用戶名稱一併使用)

保安令牌	硬件裝置並提供一次性密碼
短訊服務(SMS)	發送一次性密碼

最新保安措施

前攝監視/生物認證技術:指紋,臉部,瞳孔,語音識別

無線網絡使用指引

1. 設定用戶名稱及密碼
2. 不使用時關閉連線
3. 停用資源共享協定
4.切用公眾網絡傳敏感料