中醫藥從業員電子健康培訓課程 2009

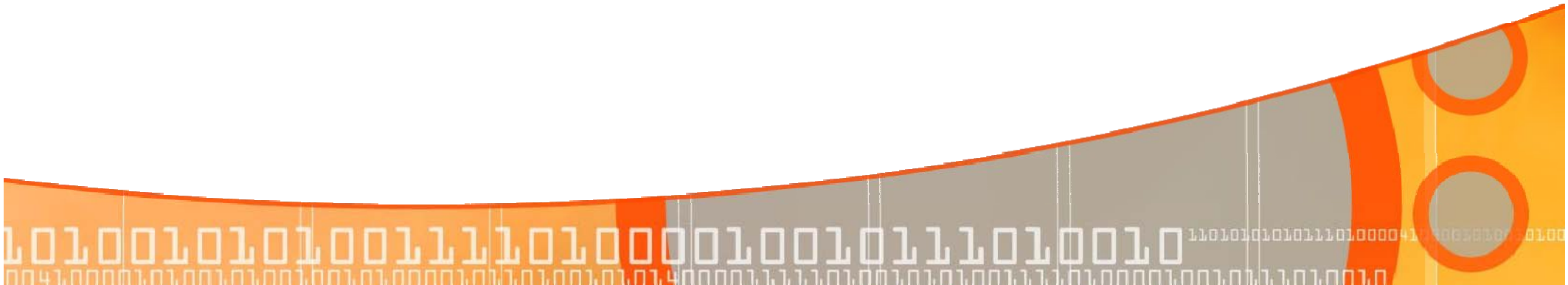
深造班　第二節 – 資訊保安及防護

講者：譚俊基先生

簡介

- 身份驗證、資料保護和加密
- 電腦病毒、防火牆、資料備份
- 防護用的資訊科技設備及服務

第一部：身份驗證、資料保護和加密



何謂資訊安全?

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。我們需要保護自己的機密資訊，因此一個組織或個人需要防衛任何可能會危害訊息機密性的惡意行動。

例如：
- 您願意將您的提款卡密碼提供給我嗎?

完整性

資訊經常需要改變。完整性是表示改變只能由授權的人或透過授權的機制來進行。

例如：
- 客戶訂單貨品數量遭惡意修改。

可用性

一個組織產生或儲存的資訊要能讓被授權者可以使用。資訊經常需要改變，這表示它必須讓被授權者存取。

例如：
- 我的電腦因為中毒所以無法開機了。

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

沒有絕對的安全

- 任何一個電腦系統都不可能做到絕對的安全，只要有連通性(Connectivity)就意味著有風險(Risk)。
- 安全原則的關鍵是
  - 使用有效的解決方案時不會增加合法用戶存取所需資源的負擔。
  - 使用複雜的安全技術並不難，但不能造成用戶漠視甚至放棄使用這些安全措施。

常發生的資訊安全事件

- 垃圾郵件
  - 你常會收到以下幾種信件嗎?
    - 廣告信件
    - 收到自己寄的信件(但是我並沒有寄)
    - 你認識的朋友寄來的信件很奇怪
    - 以上都是垃圾信件!!
  - 那我自己該怎麼處理?

常發生的資訊安全事件

- 電子郵件被盜用
  - 你認識的朋友寄來的信件很奇怪
  - 你的朋友收到您寄的奇怪信件
  - 那麼這樣的電子郵件信箱已經被盜用了
  - 為什麼會被盜用?

常發生的資訊安全事件

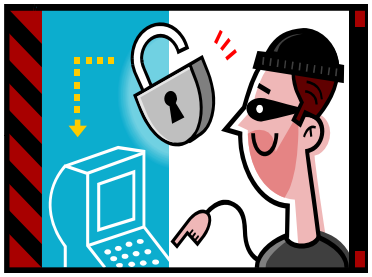
- 你有以下幾種狀況嗎?
  - 電腦速度越來越慢
  - 開機後會出現奇怪錯誤訊息
  - 網絡一直在傳送資料
  - 那你有可能已經中毒!!
- 那我自己該怎麼處理?

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）

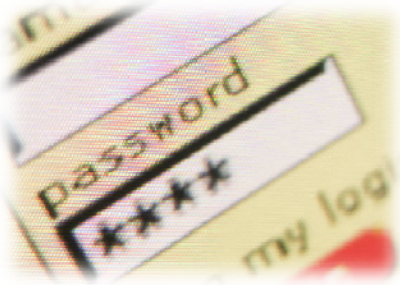
認識黑客！

- 黑客（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，黑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。



不安全的密碼設定是大問題！

- 你的密碼是不是由以下方式組成：
  - 生日組合(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



- 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（建議最少一年要變更一次）

- 不在不安全的電腦(網吧、共用電腦)輸入密碼

身份驗證

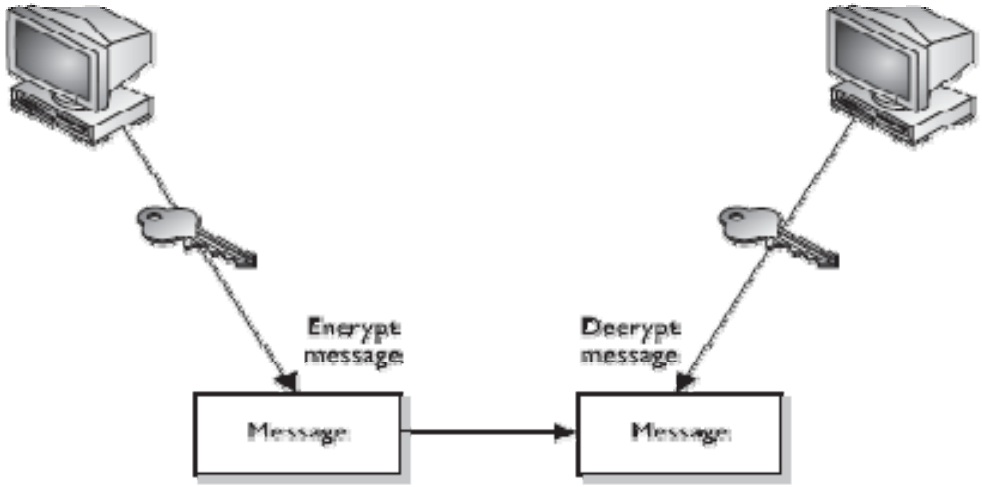
- 想要進行網上電子交易，雙方在交易前必需先確認對方身份，再進行數位訂單的簽署與電子付款，才能確保電子交易的安全。因此，需要有嚴謹的身份驗證技術，才能進行安全的電子交易。

- 身份驗證方法
  - 證實你所知道的
  - 出示你所擁有的
  - 證明你是誰

- 身份驗證加密法一般可分為兩種
  - 對稱式金鑰加密法
  - 非對稱式金鑰加密法

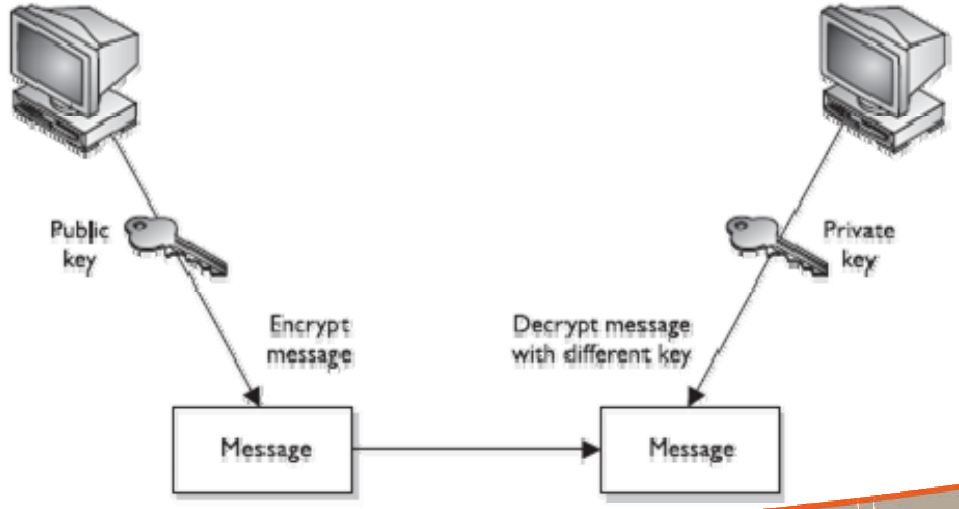
對稱式金鑰加密法

- 對稱式金鑰加密法所使用之加密及解密之金鑰，為相同一把金鑰，意指使用相同一組密碼來加解密。使用對稱式金鑰加密的好處在於其加解密速度快。



不對稱金鑰加密技術

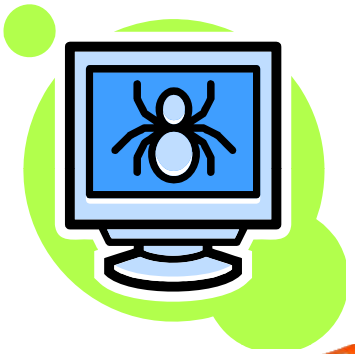
- 金鑰對中一個金鑰是公開的，而另一個是保密的。你決定向外發佈的那一半被稱做公開金鑰，另一半保密的是私密金鑰。最初分發哪一半都可以，一旦金鑰對中的一個金鑰已經被分發，則這個金鑰就要保持公有。私密金鑰也必須總保持私有，一致性是關鍵。



第二部：電腦病毒、防火牆、資料備份

電腦病毒(Virus)

- 電腦病毒雖然只是一種電腦程式，但它是一組對使用者有害而無用的程式碼。
- 它是隱藏在電腦軟體中可以自我複製的惡意程式。是一種會不斷「自我複製」及「感染」其它程式的電腦程式
- 病毒自身無法運行，它需要它所依附的主程式的運行來啟動。
- 當電腦感染上病毒時，電腦將受到不同程度的損害。
- 影響電腦正常運作(佔據記憶體…..)
- 會使電腦「發病」(格式化硬碟…..)

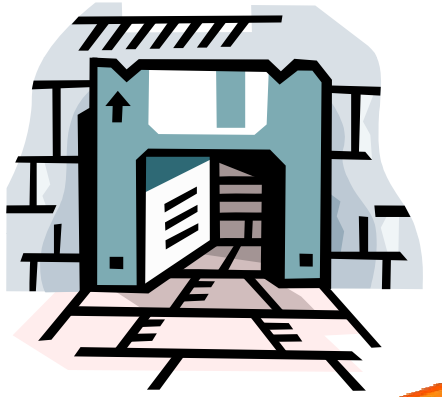


電腦蠕蟲（Worms）

- 蠕蟲屬於電腦病毒的一種，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。
- Conficker，近來一種十分流行的新蠕蟲病毒，它會利用受感染的電腦建立殭屍網絡，企圖從網上資源圖利，估計今年全球有幾百萬台電腦受影響，亦對全球企業及公共機構造成很大打擊。

暗門程式（Trapdoor）

- 暗門程式指的是程式或伺服器中未公開的秘密通口，利用暗門程式可以自由進出系統，而不被別人發現。
- 若電腦系統的管理者發現了漏洞，將漏洞補好了，黑客仍可利用早就安插好的暗門程式，繼續入侵此系統。



特洛依木馬（Trojan Horse）

- 特洛依木馬病毒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。

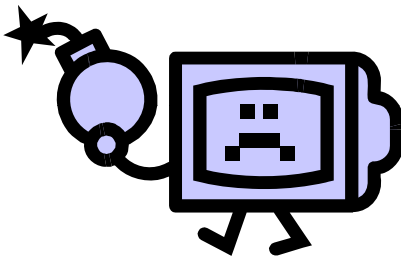
- 木馬、病毒往往是成對出現的，即木馬病毒負責侵入使用者的電腦，而病毒則會通過該木馬病毒來進行控制。現在這兩種類型都越來越趨向于整合了。 特洛依木馬程式會記載該使用者做了哪些動作，當然包括使用者所按下的密碼。

- 一般的木馬如QQ消息尾巴木馬Trojan.QQ3344，還有大家可能遇見比較多的針對網絡遊戲的木馬病毒如Trojan.LMir.PSW.60。

- 這裡補充一點，病毒名中有PSW或者什麼PWD之類的一般都表示這個病毒有盜取密碼的功能（這些字母一般都為“密碼”的英文“password”的縮寫）

邏輯炸彈（Logical Bomb）

- 邏輯炸彈屬於特洛依木馬的一種，它需隱藏在其他的程式中，當某個被預先設定的條件吻合時，它便會啟動。
- 如被公司開除的員工因心中不滿，離職前便在公司電腦裡擺置了一個邏輯炸彈，若干時日以後，炸彈啟動，自動將電腦中的資料全數銷毀。



間諜軟件(Spyware)/廣告軟件(Ad-ware)

- 間諜軟件(Spyware)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。

惡作劇病毒(Hoax)/玩笑病毒(Joke)

- 惡作劇病毒(Hoax)是對電腦病毒的虛假警告。
- 比如說在電子郵件裡面或者是在公司的內部網裡散播發現病毒的警告。
- 這些提示會進一步使用分配表然後他們會建議接受者把這個警告發給其他的人。
- 玩笑病毒(Joke)，也是惡作劇病毒。這類病毒的公有特性是本身具有好看的圖示來誘惑使用者點擊，當使用者點擊這類病毒時，病毒會做出各種破壞操作來嚇唬使用者，其實病毒並沒有對使用者電腦進行任何破壞。

語音垃圾郵件(vam)

- 語音垃圾郵件(Voice Spam)或VOIP垃圾郵件聯繫的語垃圾郵件(VOIP Spam)
- 垃圾網絡電話，也稱為語音垃圾，是通過VoIP傳播到網絡電話中的大量未驗證資訊。即使市場商人已經使用語音郵件來傳輸商業資訊
- IP電話仍然是一種更為有效的去管道，因為通話人能夠傳達大量的資訊，而不需單獨的撥號。

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。

- 網絡陷阱多，保護個人資料，建議不要急著立即回應不明電郵，檢查真假網頁的真假，不要直接按下郵件連結，避免開啟可疑附件檔，常至網路安全組織網站瀏覽，勤於修補系統或瀏覽器漏洞，安裝具防止網路釣魚的防毒軟件，安裝其他安全防護軟件，避免網路釣魚與間諜軟件聯手入侵。

惡意代碼的比較

	主要目的	損傷 可能性	複製	保護措施
病毒	損失數據 刪除 /損失	高	✓	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 廣告軟體	使用不方便 讓人反感	低	X	刪除 (手動或工具)
惡作劇病毒	讓人反感 讓人焦慮	低	X	刪除 /忽略

何謂防火牆？

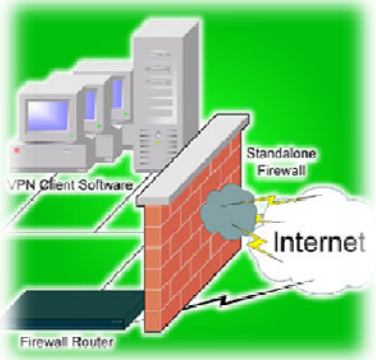
- 防火牆是一種軟件或硬件，它就像一個屏障 ，會監視與限制在您的電腦與網絡或網際網絡之間流通的資訊。如此便會提供一條界線，防止有人由防火牆之外，未經您的同意就嘗試存取你的電腦。

- 如果您是家庭使用者或小型企業使用者，保護電腦的最有效且最重要的第一步就是安裝防火牆，並在連接上公共網絡之前，首先開啟防火牆和防毒軟件。

- 你可以將防火牆想像成是一道柵欄，它會檢查來自公共網絡或內網的資訊，然後根據防火牆的設定決定將其轉向或允許它通過你的電腦。

防火牆能做什麼？

- 防火牆可協助阻擋試圖透過公網(Public Network)或內網(Internal Network)進入你電腦的黑客(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，你可以安裝並使用自己所選擇的任何防火牆。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。



防火牆不能做什麼？

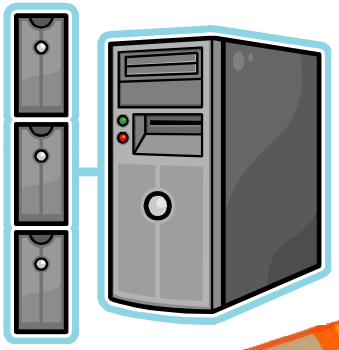
- 不能偵測或停用電腦內已有的病毒及蠕蟲。基於此理由，你也應該安裝防毒軟件並常常更新，保持在最新狀況。

- 不能封鎖垃圾或來路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。

- 不能阻止你開啟有危險附件的電子郵件。不要開啟來自不明寄件者且含附件的電子郵件。如果主旨行只是胡說八道或對您完全沒有意義，即使您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。

資料備份

- 備份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，並且放置在不同的場所，以利日後回存之用。
- 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。

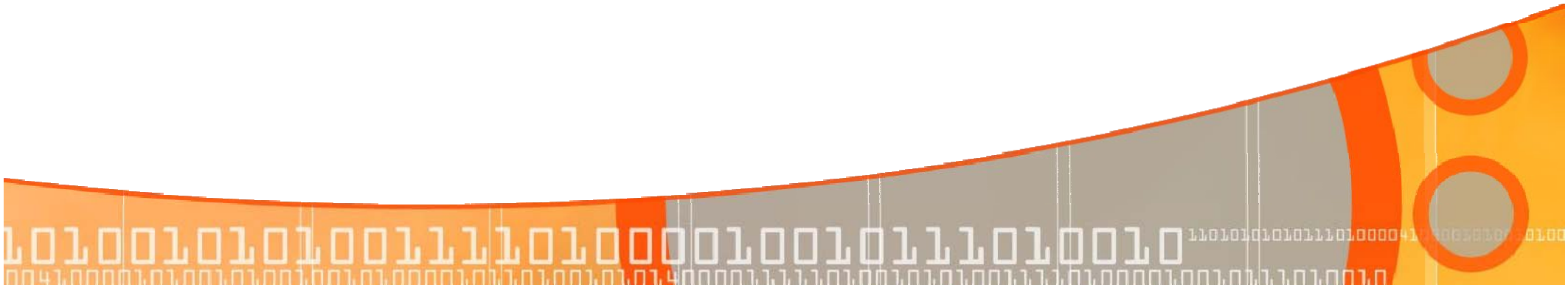


資料備份建議

- 一個500G的硬碟比二個250G的硬碟便宜，一般人都會直接選擇500G的來使用，因為竟方便又便宜，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。

第三部：防護用的資訊科技設備及服務



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
- 虛擬專用網路（Virtual Private Network）
- 數據加密軟體/ 硬件（Data Encryption Software/Hardware）

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，即會侵犯到智慧財產權。
  - 檔案來路不明，可能包含木馬或病毒程式，容易使您的個人資料曝露在網路當中。

小心重要文件遺失或受損！

- 什麼是重要文件
  - 個人資料。
  - 工作上使用的資料。
- 要如何妥善保存(以下方式建議使用)
  - 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子中並上鎖。
  - 下班時，辦公桌面應保持淨空，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，電腦應登出並有密碼保護，防範他人使用。

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
- 備份重要資料
- 穩固密碼設定
- 更新應用系統
- 升級防毒軟體
- 小心使用網路
- 過濾電子郵件

多謝

課後討論時間