資訊安全教育訓練

羅 源 發

崴航國際股份有份有限公司

課程大綱

- 安全政策
- 密碼設定
- 電腦使用注意事項
- 個人習慣
- 中毒特徵
- 個人資料備份

歲航資訊安全政策

- 正確安全持續運作。
- 防止駭客入侵破壞。
- 防止人為不法使用。

密碼設定

- 應用系統主機應設定使用者使用者帳號及密碼
- 帳號及密碼由使用者保管，不應透漏給第三者，以確保他人不當進入使用系統。
- 密碼時必須8個字元，英文二位及數字混合且不含特殊字元(^&*...)。
- 三個月更新一次。

電腦使用注意事項 上網習慣

- 逛網站逛到跳出什麼要你安裝東西的視窗，除非你非常確定、肯定你要裝的是什麼東西，不然請一律拒絕
- 逛到一些需要輸入帳號密碼的網站，請把其他所有正在瀏覽網站的視窗都關閉再輸入，以免被盜錄，如果能使用螢幕小鍵盤更好
- 在外面網咖或用別人的電腦上網，請不要輕易登入重要的網站，因為你不能確定這台電腦是不是安全
- msn有人傳網址給你 請務必向對方確定那是什麼東西再點

電腦使用注意事項　留意破解版軟件及防毒

- 有很多破解版軟件都內含病毒,
- 這類病毒大部份都不會影響軟件本身的功能,所以要留意喔!其實大部份軟件都有相應的免費或開源版本,功能都不比收費的軟件差,有些更比收費的更好.在取破解版之前,不如先找找免費的版本吧!.

電腦使用注意事項 不要什麼都答是

- 上網時, 電腦都會問很多問題, 不要什麼都答是
- 無論是在安裝軟件還是上網時, 電腦都會問很多問題, 不要什麼都答是, 提示或警告的內容應該先詳閱才按確定.例如一些軟件會在安裝時問是否需要安裝其他某某軟件(通常是工具列, 廣告軟件), 這類軟件通常都是易請難送! 如果按了確定, 那電腦又多一件無用的垃圾軟件, 又多一個小問題嚕...久而久之就會引起大問題

電腦使用注意事項 不要什麼都答是

- 要電腦不中電腦病毒，不中間諜程式，不讓駭客入侵，在這個網路的時代，老實講，似乎很難！
- 因為，即使我們安裝了最強的防護程式，只要個人使用電腦的習慣不良、任意連到來路不明的網站、隨意開啟電子郵件的附件（附檔名多為：exe 、com 等）、、、，仍然會讓電腦中毒。所以我們必須要做最好的準備，給自己一個最乾淨安全的使用電腦環境，降低中毒的危險。

電腦使用注意事項 公私要分

- 許多資安事件(電腦病毒，資料外洩等..)有許多都是公私不分。辦公室的工作做不完，用隨身碟拷貝回家作，或回家連到公司主機來作。近來的隨身碟病毒之所以防不勝防，許多都是從家用電腦的隨身碟、記憶卡、數位相機、手機、Mp3播放器擴散出來的。
- 家用電腦本來問題就多，尤其病毒、木馬、間諜程式、廣告程式。

電腦使用注意事項 公私要分

- 對於下班後還拿工作回家做的人本應感謝的，但基於資安政策仍要有配套的安全措施。否則還是不要把公事拿回家作比較好。國內外幾個重大的資料外洩許多是從家用電腦安裝分享軟體或被植入木馬後門間諜程式等外洩的。許多狀況是把家裡的工作拿來辦公室做，而家用電腦又是病毒最多的地方。像借用辦公室的印表機印作業、印相片等。借用辦公室較快的頻寬來下載MP3並利用隨身碟拿回家用電腦使用等，都是企業中毒的重要兇手。

電腦使用注意事項 防毒軟體百毒不侵？

- 市場上防毒軟體的品牌多如過江之鯽，說明了所有的防毒軟體都無法百分之百防毒。
- 如果有的話，廠商就會主動提出保證與漏毒的連帶賠償合約。現在是網際網路的光速時代，每幾秒就產生新的或變種的病毒，這是電腦使用者結合防毒軟體業者與病毒開發者(甚至是集團)的戰爭，戰場就在大家的電腦。

電腦使用注意事項 防毒軟體百毒不侵？

- 除非防毒廠商獲得所有的病毒樣本(**這是不可能的**)
- 因為有了病毒樣本再去分析成為病毒定義檔也要花一些時間)，並且防毒軟體的更新是**持續不停地更新**-但你的電腦大概什麼事都不用作了。
- 沒有完全獲得所有的病毒樣本及更新之前，任何新型或變種的病毒都可能感染你的電腦。

電腦使用注意事項 密碼問題

- 密碼為作業系統的一項重要的保護機制。

- 就一般的使用者而言，在為方便使用電腦而忽略密碼設定的安全性〈簡單易猜，甚至無密碼設定〉，導致門戶大開，很容易成為病毒或駭客攻擊及入侵成功的目標。。

電腦使用注意事項 收發E-mail的最新風險

- **對企業而言，E-mail的重要性與電話是一樣重要，更甚於電話，由E-mail衍生的風險也與日俱增。**
- 絕大部份的企業已經在Mail Server 或Mail gateway端安裝防毒軟體，讓有問題的郵件或附件不會進入到企業內部。越來越多的惡意程式(包含病毒、病蟲、木馬、間諜程式)也躲避了這樣的防護機制，利用郵件夾帶網路連結位址-URL。讓使用者不小心或好奇地連到有問題的URL。

電腦使用注意事項 收發E-mail的最新風險

- 除非已建置Web Filter的防護機制，能保護經由Http/Https/Ftp的流量，否則透過有問題的URL的連接，使用者幾乎是沒有招架的能力，任人宰割。沒有人知道按了這個URL連結之候，接下來會有什麼風險，有可能被安裝的木馬、後門、間諜程式、病毒，也有可能電腦就開不起來了、硬碟的資料全毀損了。
- 許多人安裝了防毒軟體之後，膽子就大起來了。天不怕地不怕，以為可以赴湯蹈火。

電腦使用注意事項 收發E-mail的最新風險

- 一直以來，使用者被教育不開啟有問題的郵件附件檔案及圖片。

- 現在應該多加一項-不開啟有問題的連結，不管來自e-mail或即時通訊。

建立良好個人習慣

1.不開啟來路不明的郵件、附件、檔案和網站

2.安裝軟體&開網頁時注意，不要隨便同意加裝東西

3.使用合法的軟體程式，不要隨意下載或拷貝非法軟體

4.不使用即時通訊、遊戲的外掛，因常有木馬或廣告插件在內

5.從網路、別處取得的資料先用掃描軟體偵測

6.定期掃毒、更新病毒碼與作業系統更新Windows Update

7.避免在多人共用的電腦存取資料和密碼

8.經常做好資料備份，以預防病毒入侵破壞

9.螢幕保護程式5分鐘啟動，並需要輸入密碼後才能繼續使用

10. USB裝置未經申請，禁止使用

個人資料備份

- 1. 點開始， 點執行
- 2. 輸入\\192.168.1.242
- 3. 按確定後，出現各單位的資料匣
- 4. 滑鼠按右鍵，連線成網路磁碟機
- 5. 選 X ，按確定
- 6. 以後的執行動作，點我的電腦，點入 X 磁碟機，
- 7. 就會看到您的資料匣(以751為例)請再點進去
- 8. 在重要文件的圖案上，按右鍵，複製過去
- 9. 在mail的圖案上，按右鍵，複製過去