網絡保安及知識　第一堂

數碼保安介紹

視像文字稿

大家好。歡迎收看《網絡保安及知識》網上課程。在這個課程中，我們會介紹一些基本的網絡保安知識，包括惡意軟件、流動裝置保安、身份盜竊，以及使用流動支付服務的保安貼士。

經常聽說電腦病毒十分可怕，究竟甚麼是電腦病毒？其實電腦病毒是其中一種惡意軟件，會令電腦資產受到不同程度的保安風險，例如中斷電腦操作、收集敏感資料等。
本課堂介紹有關感染惡意軟件的主要途徑及所帶來的威脅，並提供保安提示，以防止電腦裝置（包括智能手機、平板電腦等）被惡意軟件入侵。

什麼是惡意軟件？
惡意軟件是惡意程式碼的簡稱。網絡罪犯會在你不知情的情況下散播及安裝惡意軟件於電腦裝置上，並盜取儲存在電腦裝置內的敏感資料或中斷電腦裝置的操作等。
最常見的惡意軟件包括電腦病毒、蠕蟲、特洛依木馬、間諜軟件、廣告軟件、rootkit、殭屍網絡、邏輯炸彈、後門程式、鍵盤側錄程式、恐嚇軟件和勒索軟件等。
某些惡意軟件甚至會表現出多種惡意程式碼行為。例如，特定程式可能既是電腦病毒也同時為特洛依木馬。

如果電腦裝置受惡意軟件感染，會帶來甚麼風險？
惡意軟件會令電腦裝置和網絡遭受破壞和產生不良的影響。當中潛在的影響包括：數據被上鎖、修改、銷毀和盜取；遭他人在未受權情況下進入系統；被執行非用戶擬使用的功能；電腦系統和網絡被干擾及關閉；受害者被索取贖金等；
惡意軟件對數據及資訊處理設備構成嚴重威脅。我們必須採取防禦措施，以保護電腦裝置免受惡意軟件攻擊。

接着我們會以勒索軟件作為例子，從原因和影響、處理方法、以及預防措施，探討惡意軟件所帶來的網路安全的問題以及應對惡意軟件的方法。

電腦裝置主要會從以下途徑受惡意軟件感染，包括：開啓可疑電郵、即時短訊或當中的附件及超連結；瀏覽包含惡意程式的網站；下載及安裝包含惡意程式的軟

件或流動應用程式；而部分惡意軟件更會嘗試透過網絡及 USB 裝置等途徑感染電腦裝置。

勒索軟件是惡意軟件的其中一種。電腦罪犯會利用這種軟件把受感染電腦裝置內的檔案鎖上。這些被鎖的檔案就好像人質一樣，受害人如要取回這些資料，便需按照勒索軟件的指示繳付「贖金」，才可把檔案解鎖。

受感染的電腦裝置及所接駁的其他儲存裝置內的檔案會被鎖上。除非已適時進行備份，否則可能會損失這些檔案。

勒索軟件會使用高強度加密技術把電腦裝置及所接駁的其他儲存裝置內的檔案加密。會被加密的檔案類別包括文件、圖片、影片、繪圖編輯檔等。
加密後，惡意程式會把加密密碼回傳到伺服器，並在受感染的電腦留下勒索訊息，要求你支付一個指定金額的「贖金」，以換取解密密碼，否則唯一的解密密碼將被刪除。這時才發現被勒索，就麻煩了！
所有檔案都會被勒索軟件鎖起無法開啟，好像被鎖入夾萬一樣，需要繳付贖金取得密碼開啟。

由於勒索軟件使用高強度加密算法，因此在沒有解密密碼的情況下，修復被勒索軟件加密的檔案相當困難。如果你有為檔案製作備份的話，從備份中復原檔案是最簡單的方法。
如果沒有備份，你可以到香港電腦保安事故協調中心（HKCERT）的網頁查看是否有對應加密你的檔案的勒索軟件的修復方案。
記緊不要交付贖金，如有需要可向 HKCERT（熱線電話：8105 6060）舉報或報警救助。

其實電腦裝置被惡意軟件感染後，有機會出現一些異常的徵兆，包括：執行程式的時間比正常情況長；系統的硬碟可使用空間突然降低；電腦裝置出現來歷不明或新建立的檔案或程式;突然彈出新視窗或瀏覽器廣告；電腦裝置異常重啓或死機；網絡流量增加；系統設定遭到更改，例如網站瀏覽器的「首頁」會變更成另一個網站;保安軟件停止或未能更新;大量檔案無法開啟或被加上某些副檔名(例如 .locky, .encrypted, .cryptolocker）等。
如果你遇到以上的異常狀況，代表你的電腦裝置可能已被惡意軟件感染。

若電腦裝置不幸受惡意軟件感染，你可考慮採取以下即時措施，包括：不要再接駁受感染的電腦裝置至網絡，以減低進一步的影響；如電腦裝置懷疑被勒索軟件感染，應關閉裝置，以避免勒索軟件將更多的電腦檔案加密；至於其他種類的惡意軟件，應使用抗惡意程式碼軟件掃描及將其清除；記下在發現感染前進行過的

操作，例如曾經使用過的程式、檔案、電郵及曾到訪的網站；在確定惡意軟件已被清除前，不要開啟任何檔案；從備份復原檔案；及向香港電腦保安事故協調中心 （HKCERT） 或香港警務處舉報。

惡意軟件對我們影響那麼大，真是聽見都害怕! 所以要想辦法保障自己!以下是一些建議大家可以採取的預防措施，包括： 定期把重要資料備份和不要把備份資料連接電腦裝置;定期為使用中的作業系統及軟件更新、安裝最新的修補程式，以防止受惡意程式感染；安裝防毒軟件、防火牆及抗惡意程式碼軟件並將識別碼更新至最新版本；還有定期全面掃描電腦裝置，以偵測及防禦惡意軟件攻擊。

此外，我們亦要經常保持警覺，不要開啓可疑的電郵、即時短訊，以及當中的附件和超連結；不要瀏覽可疑網站，或從這些網站下載任何檔案；不要從可疑的彈出式視窗或警告點擊及下載任何檔案；在任何情況都不應使用來歷不明的軟件。

我們亦可以停止或限制使用電腦系統內所有不必要的服務及功能，例如遠端桌面服務；封鎖 SMB 通訊埠以阻擋接上互聯網；關閉 Microsoft Word 、 Excel 或其他辦公室軟件內的預設巨集功能；關閉 CD/DVD 儲存光碟及 USB 裝置上的自動執行程式功能等。

最後再提提大家幾個重要的網絡保安貼士：請謹記不要開啟或點擊在可疑電郵、即時訊息或社交網絡網站上的附件或連結；不要瀏覽可疑網站或在這些網站下載任何檔案;在任何情況都不應使用來歷不明的軟件；要安裝抗惡意程式碼軟件及個人防火牆，並為作業系統和軟件產品更新，安裝最新的保安修補程式；定期備份程式和數據，避免將備份的資料連接至電腦裝置，以及要把備份的資料存放在安全地方。

多謝你收看今堂內容。再見！
本教材由新界西長者學苑聯網提供內容及製作。