網絡保安及知識　第二堂

流動裝置篇

視像文字稿

大家好。歡迎收看《網絡保安及知識》網上課程的第二堂：網絡保安及知識流動裝置篇。

智能手機為我們的日常生活帶來了很多便利。但我們亦往往很容易忽略了手機的保安措施，讓不法之徒有機可乘。本課會提供數個具體的保安貼士，讓你可以減低裝置上個人私隱外洩的風險。
在開始之前，大家要留意本課提供的保安設定可能會因應大家的手機型號而有所不同。大家可以按照手機的用戶手冊內的指示進行設定。

很多時候我們的手機被入侵，是因為我們沒有注意要使用的應用程式是否安全，隨意安裝和使用來歷不明的應用程式。這些來歷不明的應用程式有可能含有惡意程式碼，有機會破壞你的手機或使你的個人資料被盜取。所以我們必需限制安裝來歷不明的應用程式。
如果你的手機屬於 Android 系統，你可以開啟應用程式，點一下設定，然後再點一下鎖定螢幕與安全性，然後取消勾選未知的來源。
如果你的手機屬於蘋果系統 (iOS)，因為 iOS 本身只允許安裝來自 Apple 官方 App Store 的應用程式，一般而言是無法安裝來歷不明的應用程式的。請不要為你的 iOS 進行「越獄」。不進行「越獄」的話，就能夠避免誤裝來歷不明的軟件。

另外設定嚴謹的密碼和屏幕鎖定功能亦是非常重要。
開啟了屏幕鎖定功能的話，手機在鎖定後就需要正確解鎖才可以使用。這樣即使你遺失了手機都可以減低被其他人盜用的風險。
常見的屏幕鎖有：
圖形鎖：通常圖形鎖都是通過滑動屏幕上的圖案解鎖。因為圖形鎖容易被在你身邊的人偷看到，所以安全性比較低。
PIN 鎖：輸入數字密碼解鎖。
密碼鎖：輸入密碼解鎖。因為可以選用更嚴謹的密碼，安全性比 PIN 鎖更高。
指紋鎖：把你的手指放到指紋感應器上解鎖。
面部解鎖：用手機的前置相機拍攝你的容貌，確定是你本人之後解鎖。

抗惡意程式碼保安軟件可以偵測惡意軟件攻擊，以及為被感染的流動裝置清除惡

意軟件。
使用抗惡意程式碼保安軟件時，需注意以下幾點：
首先，要啟動自動更新功能，以確保軟件及定義檔都是最新的版本
第二是啟動抗惡意程式碼保安軟件裏的實時保護功能，並定期為你的流動裝置進行全面掃描
第三是小心提防假冒的防惡意軟件及虛假的彈出保安警告。這些假冒軟件和虛假的保安警告有可能是要誘騙你下載和安裝惡意軟件至流動裝置。
還有要保持警覺，若發現流動裝置的電池很快耗盡、速度變慢及不尋常地使用大量數據，表示流動裝置可能已被惡意軟件所感染。

隨著作業系統和軟件的推出時間越來越久，越來越多的新漏洞會被發現。我們必須要定期為智能電話進行更新，確保作業系統、瀏覽器和應用程式已更新到安全的版本，修正這些安全漏洞。
通常更新作業系統都可以於系統設定選單完成。更新前最好先確認流動裝置可以支援最新版本的作業系統。部份產品因硬件兼容問題或缺乏裝置製造商支援，會不適合更新作業系統。
除了作業系統之外，記緊時常到官方應用程式商店更新手機程式的新版本，以保證繼續有安全更新的支援。
如果無法為流動裝置進行更新，就應該要避免使用没有安全更新的流動裝置進行涉及敏感資料的活動，例如網上銀行。
過時和不需要的軟件就應該要停用及移除。
如果開啟了自動下載更新，亦要注意更新時不要使用流動數據或外地漫遊數據，以免造成額外的網絡費用。

流動裝置的資料可能因為裝置遺失或被盜而外泄。以下這些措施可以保護裝置，避免損失：
第一：設定開機密碼，使你遺失手機時手機內的資料亦不會被輕易讀取。
第二：在儲存資料到外置記憶卡前，要先啟用外置記憶卡的加密功能。這樣做的話，即使賊人從你的手機拆出外置記憶卡，亦無法讀取裏面的內容。
第三：使用保安軟件，讓你在流動裝置遺失或被盜的情況下，進行遙距追蹤、鎖定裝置或清除資料。

當我們使用 Wi-Fi 上網時，為了確保安全上網，我們需要提防連接到不可靠或虛假的 Wi-Fi 網絡
我們可以定期移除不安全和不必要的 Wi-Fi 連接描述檔，以免流動裝置自動連接到危險的 Wi-Fi 網絡
使用公眾或户外網絡時應該避免處理跟私隱有關或敏感的資料及數據。
使用無線連線後亦應把無線連線功能關閉，避免流動裝置自動連接到危險的 Wi-

Fi 網絡。

當我們安裝手機應用程式時，大家要注意應用程式會否需要全球定位(GPS) 資料權限。一些無需 GPS 資料的應用程式，應被限制取得 GPS 資料，以免在你不知情的情況下被他人知道和追蹤你的位置
如非必要，不要給予存取地理位置權限給流動應用程式
如果不給予地理位置權限會導致流動應用程式無法運作，而程式是沒有需要存取地理位置的話，應該避免使用這些流動應用程式
還有在使用需要 GPS 權限的應用程式後，應把 GPS 功能及定位服務關閉。

除了 GPS 資料權限之外，手機應用程式有時亦會要求其他權限，例如使用相機和發送短信。當你發現應用程式要求過份或不合理的權限，應該採取一些相應的措施，例如：
使用工具應用程式，偵測及移除高風險的流動應用程式，包括可存取個人和位置資料、使用拍照、錄音或更改系統設定的應用程式
安裝流動應用程式前應使用公共搜尋器做資料搜集，例如用“試用報告”、“投訴”及“比較”等關鍵字進行搜尋，確定該程式信譽是否良好
在安裝和使用流動應用程式時，應該徹底審視應用程式的所有權限要求，特別是一些涉及敏感權限的要求。
在更新應用程式時，亦要小心審視任何額外的權限要求。

當流動裝置在受惡意軟件感染、硬件故障和裝置遺失的情況下，都有可能使裏面珍貴的資料損毀或者無法讀取。定期進行裝置備份，就可以在這些情況下，從備份中復原裝置資料。
你可以使用備份軟件，備份流動裝置的資料到你的電腦，讓你可以在有需要時復原資料。
進行定期備份後，要小心保護已備份資料，確保備份內的內容不會損毀和被外洩。
如果你打算將備份資料同步至雲端服務，同步前應評估保安風險，並應避免將敏感資料自動備份至雲端平台上；以及應盡可能使用嚴謹的密碼及認證方式，例如雙重認證，保護雲端服務帳戶。

最後在更換手機時，舊手機的處理都非常重要。舊手機內的數據即使已被刪除，但仍可能透過復原軟件工具將數據復原，以致有資料外泄風險。
在轉交或棄置流動裝置前，除了使用「恢復出廠設置」的功能外，你還可以進行以下步驟，以確保流動裝置內的資料已徹底刪除。
首先：執行「恢復出廠設置」功能。
第二：使用容量較大兼無關重要的檔案，填滿流動裝置內的儲存空間。
第三：使用安全刪除工具刪除數據。

第四：重複步驟二和三，以刪除外置儲存裝置，例如外置記憶卡內的資料。
第五：開啟系統內磁碟全面加密的功能，並選用一個嚴謹的密碼。
最後：再一次執行「恢復出廠設置」功能。

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。