

～資訊安全的四項提防～

資訊安全的種類可分為三個面向：

- 一、硬體的安全，包含對於硬體環境的掌握以及設備管理；
- 二、軟體的安全，包含資料軟體安全和通訊管道的安全性；
- 三、個資的安全，包含個人資料保密，隱私性等。

◎如何做到上述資訊安全的保護措施呢？

首先我們要了解影響資訊安全的因素，包括：未經授權侵入使用者帳戶，進行竊取或是更動系統設定；資料在傳輸過程中被擷取，或被變更內容；透過感染電腦病毒與傳播惡意程式。諸如此類的資訊安全問題層出不窮，且手法日新月異，然而注意下面幾點防護措施，可在面對大部分的狀況時，具備基礎的防護手段。

一、防毒：

當一隻病毒被製造出來之後，開始於電腦與網路設備中擴散，透過網絡無遠弗屆的傳遞，變成所有電腦使用者的夢魘，隨之而來的系統崩潰甚至硬體損壞，將損毀寶貴的資料。使用者防治的積極手段就是安裝來源合法的防毒軟體，並且定時更新病毒碼，以保持作業系統處於健全的防護程度。

二、防駭：

隨著社群網絡和各式資訊系統的應用，駭客由開始時半開玩笑地更動系統設定，演變到後來的蓄意破壞、資料竊取，也因此發展出了各式的系統安全通行證，包含使用者密碼、身分驗證、通訊鎖、晶片卡等設置，普遍使用於各層面。除了定期變更驗證方式以及使用多種防護作為外，也需隨時保持資安的警覺性。

三、防治天災：

這是容易忽略的一個項目，電腦硬體從來就屬於耗損型的設備，隨著時間、溫度、濕度、跳電等，甚至震動都可能導致硬體的受損；因此使用者應該以嚴肅的態度準備更完整的防治計畫，例如定期更新易耗損的硬體設備，備份重要資料，以及安裝備用電源，預防斷電造成的資料損失等。

四、資料防竊：

隨著智慧型手機的流行，現在低頭族已成為一種社會現象。而資訊的氾濫成為眾多使用者頭痛的問題，許多不同的應用程式都會記錄使用者的個人資訊，但設計這些應用程式的公司是否確實做好保護我們的個人資料？值得存疑！許多應用程式的分享與協同編輯功能權限設置不明，更是成為資料安全上的一大隱憂。因此，我們對於自身的資料處理應該抱著更謹慎的態度，切勿在網路上分享或是儲放機密資料。

臺中榮民總醫院提醒你！也關心您！