

7月份機關安全維護宣導：資訊安全的四項提「防」

隨著電腦應用的普及和網路的急劇發展，不僅改變了人類的生活模式，也帶來了令人擔憂的資訊安全問題。因此，建立完善的資訊安全防護措施已是當務之急，唯有在安全無憂的前提下享受網路資訊帶來的便利，才是面對科技發展的正確態度。

資訊安全的種類可分為三類：一、硬體的安全，包含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防護措施呢？首先我們要面對資訊安全影響的因素，包括：務必授權重點使用者帳戶，進行抓取或更動系統設定；資料在傳輸過程中被抓取，或被變更；洩漏感染電腦病毒與傳播惡意行為。諸如此類的資訊安全問題層出不窮，且利用日新月異，但是注意下面的防護措施，可在大部分的情況下，具備基礎的防護手段。

一、防毒：當一種病毒被製造出來後，開始在電腦與網路設備中擴散，穿透網絡無遠弗屆的交接，變成所有電腦用戶的夢魘，加之收到的系統硬體損壞甚至崩潰，將損毀寶貴的資料。使用者防治的手段就是安裝來源合法的防毒軟體，並定時更新病毒碼，以保持作業系統處於預設的防護程度。

二、防恐：隨著社群網路和各類資訊系統的應用，客恐由開始時半開玩笑地更動系統設定，演變為後來的收集意破壞、資料竊取，也因此發展催生了各式的系統安全通行證明，包含用戶密碼、身份驗證、通訊鎖、表單卡等設置，普遍使用於各層面。除定期變更驗證方式以及使用多種防護作為外，還需隨時維持資安的警覺性。

三、防治天災：這是一個很容易被忽視的項目，電腦硬件從來就屬於耗損型的設備，隨著時間、溫度、濕度、跳電等，甚至驚慌都可能導致硬件的污染；因此用戶應盡快做好準備更完整的防治計劃，例如定期更新易耗損的硬體設備，備份重要數據，以及安裝電源供應器，預防電斷造成的備用電源損失。

四、資料防盜：隨著新型智慧型手機的普及，現在低頭族已經成為一種社會現象。而資訊的氾濫成為了困擾用戶的問題，許多不同的應用程式都會記錄用戶的個人資料，但設計這些應用程式的公司是否確實很好地保護了我們的個人資料？值得存疑！眾多應用程式的分享與良好的編輯功因此，我們對於自身的資料處理應該圍繞著更嚴格的態度，在網路上分享或儲存機密維護資料。我們若能認真思考資安問題，完善這些資訊系統與網路設備，定期維護與個人資安，從而長保資料的可用性及可靠性了。