資訊安全的四項提「防」

隨著電腦應用的普及和網際網路的急遽發展，不僅改變了人類的生活模式，也帶來令人憂慮的資訊安全問題。因此，建立完善的資訊安全防護措施已是當務之急，唯有在安全無慮的前提下享用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個面向：

  1.硬體：對於硬體環境的掌握以及設備管理

  2.軟體：資料軟體安全和通訊管道的安全性

  3.個資：個人資料保密，隱私性等。

- 影響資訊安全的因素：

  1.未經授權侵入使用者帳戶，進行竊取或更動系統設定

  2.資料在傳輸過程中被擷取或被變更內容

  3.透過感染電腦病毒與傳播惡意程式。

諸如此類的資安問題層出不窮且手法日新月異，然而注意以下防護措施，可處理大部分的狀況：

1. **防毒**：當一隻病毒被製造出來，開始於電腦與網路設備中擴散，隨之而來系統崩潰，甚至硬體損壞，損毀了寶貴的資料。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。

2. **防駭**：隨著社群網絡和各式資訊系統的應用，駭客開始蓄意破壞、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。除了定期變更驗證方式及多種防護作為，也需隨時保持資安的警覺性。

3. **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，預防斷電造成的資料損失等。

4. **資料防竊**：有些應用程式會記錄使用者的個資，但設計這些應用程式的公司是否確實做好隱私保護？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。

我們若能認真地思考資安問題，完善規劃這些資訊系統與網路設備，定期保養與維護個人資安，便可長保資料的可用性及可靠性了。

摘自〈臺中市政府水利局政風室〉