電子郵件安全

電子郵件是 21 世紀現代社會重要的資訊傳送管道，現代人透過電子郵件進行資料傳輸、溝通訊息、處理公務、聯絡感情等，是便利且迅速的資訊交流方式，但是隨之而生的電子郵件安全性議題，從許多媒體及資安事件中，發現電子郵件已成為發生資訊安全事故的重要傳播載體，維護電子郵件的安全不僅僅只針對您的帳號設定「安全」的密碼而已，以下幾項說明或可幫助您確保在使用電子郵件上的安全。

一、使用任何電子郵件軟體前，必須確認以下認知：

1. 避免在不安全的網路環境使用電子郵件：

儘量避免使用公共場所的電腦收發電子郵件，若使用公共場所的電腦完畢，必須記得清除自己的使用紀錄及敏感資料，以免有心人士竊取或登入冒用，且儘量不要在沒有經過加密的連線環境下讀取您的電子郵件。

2. 建立電子郵件驗證機制：

市面上有許多商用軟體及免費數位簽章軟體可用，可在您所發送的電子郵件中加上數位簽章，機關(構)或公司也可依據需求自行建置 CA(Certification Authority，憑證授權)提供服務，在進行身分認證時請進行加密，否則可能會遭到駭客竊取您的帳號密碼。

3. 以純文字模式開啟信件：

不要讓電子郵件軟體使用 html 或 xhtml 網頁格式開啟信件，應該設定電子郵件不以 html 格式打開，而以純文字的方式開啟，否則可能會被駭客利用甚至植入惡意程式。

4. 關閉「自動完成」的功能：

許多電子郵件軟體都有提供「自動完成」的功能，也發現許多意外出現在選取收件者時發生。例如在 Microsoft Outlook 的收件者欄位中，我們常可看到 Outlook 會跳出下拉式選單讓我們選取收件者，不過有時候會選到排序上相鄰的聯絡人，如果今天這封電子郵件是要討論相當機密的事情時，發生選錯聯絡人的情況是相當嚴重的。

二、收發信件時必須注意：

1. 當您發送給多人的電子郵件時，請將收件者以密件副本方式傳送，若是將收件者放在「密件副本」的欄位，則每位收件者只會看到自己的電子郵件地址而看不到其他人的。

2. 請再三確認電子郵件中的收件者，尤其是使用 mailing list 群組時，有些人當收到 mailing list 裡面的電子郵件後，會按「回覆」以發表自己的意見，而這封電子郵件會直接回覆給 mailing list，讓 mailing list 中的其他人看到您所回覆的內容，倘若今天您加入某個 mailing list 中，而回覆這封 mailing listh 則有可能對上百人洩漏您的秘密。

三、平時注意事項

1. 請將電子郵件存放於安全的地方，當您收到加密過的重要私密郵件時，您會將這封郵件進行解密後以明文的方式儲存在您的機器中，記得將資料存放在安全的地方，若您的電子郵件服務商或您的機器所處的網路環境不夠安全的話，這些郵件的內容便有可能外洩，此外定期備份郵件信箱的資料，刪除不重要及過時的郵件，以騰出較多的空間，才能維持個人電腦的運作效能。

2. 不要公開私人的電子郵件帳號，若有越來越多的垃圾郵件廠商或釣魚網站偽造成您的電子郵件地址，導致您的電子郵件地址被 ISP(Internet Service Provider，網際網路服務提供者)阻擋，勢將造成您在使用電子郵件上的困擾。

四、最後的小小提醒

1、職場上對於電子郵件的安全管理，可於員工任用合約、規範、員工訓練、宣導等多重管道中宣導，要求配合並落實安全使用電子郵件，實務上我們發現電子郵件的便利性也容易讓人公、私務混用，但電子郵件存在的威脅是不論公務或私務，正確使用電子郵件及相關操作，才能避免被駭客利用社交工程等手法入侵得逞。

2、近年來迅速走紅的網路即時通訊(如 MSN、Yahoo Messenger…)其便利性眾所周知，方便之餘相對也帶來潛在威脅，已逐漸成為電子郵件後的另一項入侵管道，諸如惡意網址連接、蠕蟲模式的攻擊等手法，唯有加強使用的安全性認知，不查閱轉寄來路不明的郵件，更不任意點閱不明的連結或開啟附件檔案，再配合相關安全性的設定，才能有效減少受到惡意程式的入侵及攻擊，正確使用軟體才能享受網路帶來的便捷，避免自己成為被駭客入侵的下一個目標。

（本文摘自清流月刊）

新竹區監理所政風室製作關心您