

## 公務機密維護— 使用電子郵件應注意事項



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造成資料外洩。
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。
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，如果您的電子郵件軟體是使用 Microsoft Outlook、Outlook Express 或是 Mozilla Thunderbird 時，您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

二、收發信件時必須注意：

1. **如果資料的私密性對您而言是相當重要的話，請使用信任的POP3(Post Office Protocol 3，郵局協議版本3)和IMAP(Internet Message Access Protocol，交互郵件訪問協議)收發信件：**  
如果電子郵件內所包含的資料對您而言是相當私密的話，請避免使用 Web-Based 的電子郵件服務，像是 Gmail、Hotmail 以及 Yahoo! Mail…等等。
2. **發送給多人的郵件時，請將收件者以密件副本方式傳送：**若是將朋友的電子郵件地址，在未經許可的

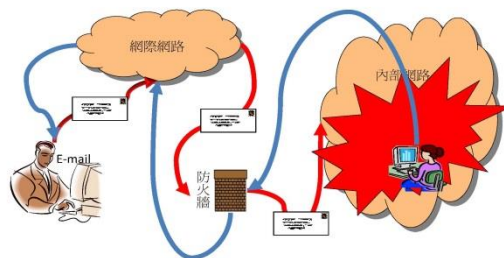
情況下分享給他人是不禮貌的。



3. 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 list 則有可能對上百人洩漏您的秘密

#### 現在網路攻擊模式

1. 在電子郵件內放置有害程式或連結 2. 反向輸出使用者資料



#### 【最後小小提醒】

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。