



**Watch Out !**

病毒郵件

本文由「電腦家庭出版集團」協助提供

---

儘管垃圾郵件十分惱人，但若消費者不予理會也不點閱這些莫名其妙的信件，尚不會對個人資訊安全造成嚴重威脅。不過，當「電子郵件」與「病毒」結合，便極有可能造成個人電腦使用的大危機！

通常夾帶病毒的郵件與一般垃圾郵件無異，同樣是由不特定的寄件者寄出，信件標題也是千奇百怪。當消費者點閱這些病毒垃圾郵件時，情況輕者，可能是將這封問題信轉寄給個人通訊錄內的所有聯絡人；嚴重者，則可能導致個人的電子信箱無法在收發郵件，甚至造成整台電腦當機、硬碟毀損！

## 預防郵件病毒的六種方法

如果不希望夾帶病毒的垃圾郵件對個人電腦造成無可彌補的危害，身為一個每天都會使用的 E-mail 的網路消費者，有一些正確的觀念與動作則是必須要建立與完成，這樣才能有效防堵病毒垃圾郵件！

### 1. 要輕易開啓不明郵件的附加檔案

如要檢查寄來郵件中的付價檔案，最好可利用「另存新檔」的方式先下載至電腦中，並等待防毒軟體檢查之後，才進行執行或開啓檔案的動作。此外，也可多多利用各網站為免費電子信箱提供的附加檔案病毒檢查軟體，透過事先過濾的動作，大幅減少電腦中毒的機會。當然，若要完全避免遭受夾帶病毒的垃圾郵件攻擊，千萬記得不要輕易點選來歷不明的電子郵件！

### 2. 認識高危險群的郵件附加檔案

如果發現電子郵件的附加檔案為「.EXE」、「.COM」等副檔名的檔案，都是直接執行檔，有大部分的病毒則會透過這種形式的執行檔案加以散播。因此，若是收到夾帶此些副檔名的電子郵件，更是要提高警覺，確認寄件人是否為朋友或是垃圾郵件發送者。

### 3. 對於 Office 也不可掉以輕心

部分 MS Office 的檔案，如「.DOC」及「.XLS」等檔案，由於可以內含巨集指令，因此極容易被電腦病毒利用。儘管近來利用巨集檔案夾送電腦病毒的案逐漸減少，但是仍然不可掉以輕心。

#### 4.關閉郵件預覽功能

部份免費電子信箱的提供網站為讓使用者更便利且快速的閱覽個人電子郵件，皆提供有電子郵件預覽功能，讓使用者在看到郵件標題的同時，便能看到信件內容。這種功能也可見於 Outlook。對於多數收件人而言，如此功能確實省時又方便。但是這項功能卻也潛藏危機！因為當收件者未經過濾便直接閱覽郵件內容時，即有可能便被電腦病毒感染；或是直接回應了垃圾郵件發送者，提供對方未來一個可不段寄送垃圾郵件的有效信箱。

#### 5.隨時更新 Outlook 或其他電子郵件軟體版本

為因應電腦病毒不斷翻新，各家防毒軟體業者則時時提醒消費者不但要更新病毒碼，更要升級個人電腦內的防毒引擎！同樣的道理亦可運用於電子郵件收件軟體，因為沒有一個軟體能夠保證永遠不會被病毒入侵、軟體設計不會被有心人士找出漏洞而加以攻擊。所以，要確保電子郵件收件的安全性，時時記得更新電子郵件收件軟體便是其中一種方法。

#### 6.安裝防毒軟體

消費者無論在免費電子信箱或是 Outlook 收取電子郵件，多多利用業者與系統提供的既有措施防堵夾帶病毒的垃圾郵件，確實是一種不錯的方法。但是若要雙重保障個人的電腦使用與資訊安全，加裝防毒軟體更是不能忘記的動作。目前每一種防毒軟體，都能將夾帶病毒的垃圾郵件列為清除對象。因此，只要記得安裝，都能提高消費者使用電子郵件的安全性！