一觸即發

就在七夕情人節來臨之際！東漢建安208年七月曹操統一北方揮師南下，企圖一舉消滅樊城的劉備與江東的孫權！

此時位於江東的小喬在情人節到來更加思念駐守前線赤壁的夫君周瑜，小喬心想此時應寫一封信給周瑜以表思念及慰問之意，當小喬打開電子郵件時收到一封來路不明網路訂購情人節花卉及宅配到府服務電子郵件時，心想應訂購一束花給周瑜，於是便點開此封電子郵件附件檔案，上網訂購花卉，當小喬點開訂購花卉網站時，發現是不是電腦出了問題，怎麼圖片均無法正常顯示，原來是要安裝某個檔案才能正常顯示，於是小喬便點選安裝！

「這會不會是曹操透過電子郵件社交工程入侵東吳的網路系統，藉以盜取軍事機密！」

曹操大軍欲掃平江南，不得已重用降將張允、蔡瑁，因此周瑜在網路上毀謗二人，散佈此二人欲出賣曹軍之訊息，此消息被曹操參謀蔣幹發現，轉知曹操。曹操未經查證，即將張、蔡二人解雇。此後曹軍水師群龍無首，導致日後曹軍的慘敗。

因有線與無線網路通訊發達，人們溝通與取得資訊容易且迅速，因此不當資訊也伴隨而來，目前網路使用者最擔心的網路安全問題主要是電腦中毒，其次是中毒後所造成的個資外洩成為詐騙對象以及網路帳戶被盜用。因此，資訊安全管理及資料遺失防護的觀念相形重要。

另外近來網路誹謗及校園網路霸凌事件層出不窮，甚至演變成新型的暴力行為，因此，如何因應與應具備的法律常識更不能少。

本單元主要探討不當資訊（包含電腦病毒、垃圾郵件　）、個人資通安全基本認知及網路誹謗、網路霸凌之案例與相關法律探討，並瞭解網路中惡意程式特徵如圖4-1及其危害與防範之道，確實做到網路安全人人有責。

雙管齊下

不當資訊的主要類型有以下幾種：

(一)惡意程式（Malicious Code）

惡意程式泛指所有不懷好意的程式碼，包括電腦病毒、木馬程式、電腦蠕蟲或其混合型等會影響電腦系統運作的程式。以下分別加以介紹：

1.電腦病毒(virus)

所謂「電腦病毒」是指會將本身程式碼複製到其他檔案或開機區的程式。當使用者執行到已受病毒感染的檔案或以磁片開機時，這個程式就以相同的方式繼續散播出去。通常電腦病毒被設計成會在某特定時期發作，輕者影響電腦運作，嚴重則會破壞電腦裡的資料。

從1987年的DOS（Disk Operating System , DOS）檔案型病毒、開機型病毒、常駐記憶體型病毒；到1993年的Windows檔案型病毒、1995年的巨集型病毒；針對32位元作業系統的檔案型病毒、常駐型病毒（如PE_CIH）以及能夠同時感染32位元可執行檔及Word文件的「跨應用程式感染型病毒」，電腦病毒的型態不停的在演變。電腦病毒的作者為了讓自己的程式碼更難被破解及偵測，「變體引擎」（Polymorphism）、「壓縮」（Compression）、「加密」（Encryption）等各項技術都被大量運用在各種類型的病毒上。

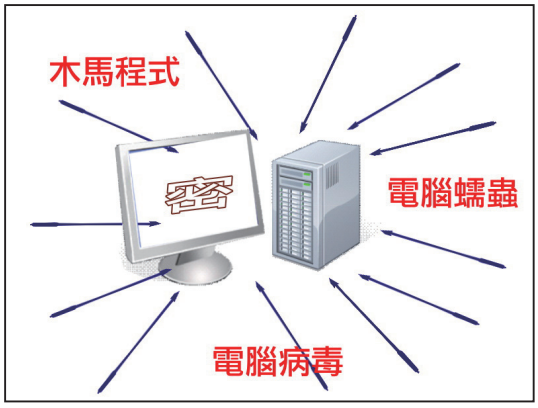
2.特洛伊木馬程式（Trojan）

特洛伊木馬程式（本文簡稱木馬程式），不像電腦病毒一樣會感染其他檔案，程式會將自己偽裝成一些特殊工具來吸引使用者下載並執行，或是電腦駭客直接入侵電腦主機將惡性程式植入系統以破壞或竊取重要資料（如格式化磁碟、刪除檔案、竊取密碼等）或是進行大規模的「阻斷服務」（Denial of service , Dos）攻擊行動。Keylogger木馬程式便是一例，被植入Keylogger的電腦，會記錄使用者按哪些鍵，駭客便有機會竊取機密資料。

3.電腦蠕蟲（worm）

電腦蠕蟲不會感染其他檔案，但是會複製出很多「分身」，然後像蠕蟲般在網路中遊走，最常用的方法是透過區域網路（Loca1 Area Network , LAN）資料夾分享或是網際網路（Internet）E -Mail來散佈自己。電腦蠕蟲著名的例子為「VBS_LOVELET-TER」。

電腦病毒、木馬程式、電腦蠕蟲原都是各自獨立的程式，近年來單一型態的惡意程式愈來愈少了，大部份都以「電腦病毒」加「電腦蠕蟲」或「木馬程式」加「電腦蠕蟲」的型態存在以造成更大的影響，比率以前者居多。因大家習慣稱影響電腦運作的惡意程式為「病毒」，本單元也以「病毒」稱之。



惡意程式（Malicious Code）

4-1惡性程式比較表：

	電腦病毒	特洛伊木馬程式	電腦蠕蟲
感染其他檔案	O	X	X
被動散播自己	O	O	X
主動散播自己	X	O	O
造成程式增加數目	一般隨電腦使用率提高，受染感檔案數目則增加	不增加	視網路連結狀況而定，連結範圍愈廣，散佈的數目多
破壞能力	視寫作者而定	視寫作者而定	X
對企業的影響性	中	低	高

〔註1〕

(二)即時通訊軟體的不當資訊

網路族能很便利的透過即時通訊軟體與好友進行線上對談、分享資訊，但很多使用即時通的網路族都在不知情的狀況下中毒。例如：不小心按了朋友傳的不明網址，造成電腦立即中毒，即時通就自動發出這些網址給正在聊天的朋友；這種病毒會自動一直傳網址給你的好朋友，一不小心很多朋友就會按到，病毒便快速散播開來，造成慘重的災情。

某些不明的網址會仿製成入口網站的登入頁面，並要求輸入個人帳號及密碼，因為仿製的頁面與知名大站很像，使用者在輕忽的情況之下，很容易直接輸入個人帳戶和密碼資料，導致資料被盜用，結果就是變成網路犯罪的工具。

(三)垃圾郵件（Spam Mail）

根據世界知名的網路及軟體安全業者賽門鐵克公司2009年2月公布的報告，臺灣被列為全球第9大發出垃圾郵件的國家；根據統計，臺灣一年有1053億封垃圾郵件在網路流竄，平均每人每天收到29封，光是刪除垃圾信件這個動作，一年下來會讓民眾浪費30個小時，可見目前對於網路使用者而言，垃圾郵件是非常的泛濫。

一般所稱的垃圾郵件是將一份內容相同的電子郵件，未經收信人許可就大量寄給不同的人，郵件內容多數是與收信人不相干的商業廣告。另一種垃圾郵件為大量轉寄未經篩選或處理的信件給通訊錄中的郵件群組，通常是你的親朋好友。垃圾郵件並不侷限於一般網際網路上的郵件，已擴及無線通訊中的短訊或簡訊。由於同時寄發大量郵件，常造成網路壅塞、郵件伺服主機負擔過重，收信人需花費金錢、時間去收這些垃圾郵件。

(四)社交工程(Social Engineering)

係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破資通安全防護，遂行其非法的存取、破壞行為，一般專門指不用程式即可獲取帳號、密碼、信用卡密碼、身分證號碼、姓名、地址或其他可確認身分或機密資料的方法，這些方法多半是使用與人互動的技巧。

社交工程的攻擊方式如下：

1. 利用電話佯裝資訊人員，騙取帳號及通行碼。

2. 偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。

3. 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。

4. 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。

5. 利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式、p2p下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。

6. 利用即時通訊軟體(如MSN)，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

(五)資料拼圖

又稱懶人密碼，所謂資料拼圖，即是將不同來源取得的個人資料比對後，拼湊出完整的資料，再利用一般民眾喜歡用生日、電話號碼等特殊數字作為密碼的習慣，直接上網「測試」各種可能的帳號密碼組合。一旦成功，即可以合法的身份登入使用者帳號，直接觀看使用者的個人資料與各種記錄，讓資料更完整。

(六)網路誹謗

有關「網路誹謗」之定義為：凡意圖透過電子郵件、個人部落格、BBS討論區、聊天室、留言版等發表不當或惡意中傷的言論，而構成當事人名譽毀損及身、心受創，稱為「網路誹謗」。

網路誹謗因為匿名的特性，沒有人知道真實的身份而更加猖獗，若真的要訴諸法律行動，需要透過網路警察，以追查IP的方式設法找到真凶。

(七)網路霸凌(Cyber bullying)

近來網路霸凌的事件頻傳，網路霸凌是指施暴者使用資訊和傳播科技，譬如e-mail、手機和網頁文字訊息、即時訊息、個人網頁、部落格、線上遊戲和線上個人投票網站等，去支持企圖傷害他人的個人或團體其刻意的、重複的和惡意的行為。

霸凌行為會使受害者產生長期的情感和行為上的問題，譬如孤單、沮喪、焦慮，導致低度自信感和情緒低潮，甚至有自殺的可能，隨著網路的普及與青少年法律知識不足，使網路霸凌成為新興的校園問題。

三思而行

以下針對電腦病毒、垃圾郵件、個人資料保護基本認知及網路誹謗、網路霸凌之案例與相關法律加以探討。

一、電腦病毒的傳播

除了傳統的磁片、網路上檔案流通以外，到底還有那些主要感染管道呢？

（一）以合法管道進行非法存取

以「TROJ EXPLOREZIP 探險蟲」為例，它開創病毒行為新模式，感染「探險蟲」病毒的電腦，會透過網路自動複製到其他電腦，並試圖刪除有分享資料夾的電腦中該分享資料夾中的檔案。這樣的行為對於電腦作業系統而言，是完全合法的，因為只要權限足夠，可以對任何設定為資源分享的資料夾做存取的動作，而這也是為什麼「探險蟲」病毒的災情不斷在世界各地傳出的主要原因。

另外只要是作業系統漏洞，就有可能被惡性程式入侵，最近的例子為殺手病毒(Sasser）利用作業系統廠商公佈的漏洞，感染的電腦會產生倒數計時關機畫面，造成使用者無法工作。

（二）閱讀或預覽電子郵件時自動散播

病毒電子郵件通常存在於附件（Attachment）檔案，所以有人認為在使用電子郵件時，只要不執行或開啟附件就不會遭受病毒感染，但「VBS_BUBBLEBOY泡泡男孩」是用VBScript 語言所寫成的病毒，即使是僅開啟電子郵件也可能遭受到病毒的威脅。

「泡泡男孩」病毒是以電子郵件的型態在網路上傳播。當我們收到這封不含有任何附件的電子郵件時，不論我們是直接開啟這封郵件或是在預覽窗格中看到這封郵件內容，其實泡泡男孩病毒已經開始執行了。它會自動尋找使用者的通訊錄，再把同樣的郵件自動寄給通訊錄內的地址，當你的朋友正在閱讀你的來信時，病毒又從你朋友的通訊錄中散播給其他人了。

（三）藉由電子郵件主動散播

談到能藉由E-Mail主動散播的病毒，就非「梅莉莎」病毒莫屬了。梅莉莎病毒利用已受感染的電子郵件產生一個Microsoft Outlook物件，然後寄出含有病毒的文件給通訊錄中所有的收件者。短短一週內擴散全球，許多知名大企業的郵件伺服器（E-Mail Server）也都因梅莉莎病毒所引起的郵件風暴，導致伺服器不堪負荷而紛紛當機。

（四）瀏覽器檢視HTML 網頁中毒

Script 類型病毒是以Script程式語言（VBScript或JavaScript，是網頁常用的語言）撰寫而成。當使用者用瀏覽器（有開啟Script功能）檢視HTML網頁時，內嵌在HTML檔中的Script類型病毒便會自動執行來進行破壞。

（五）惡性程式偽裝成重要通知或有趣遊戲、美麗圖片等，例如：

1.E-Mail說有重要修正程式，請執行「更新程式.EXE」

2.偽裝成防毒公司寄發「解毒程式.EXE」

3.偽裝成銀行或卡務中心寄發「信用卡確認程式.EXE」

4.偽裝成「有趣、好看或色情網頁文件等」

5網路釣魚（Fishing)，偽裝成有名的網站首頁，引導你將資料彙傳到預設的收集主機，盜取你的個人重要資料。

二、預防與中毒處理

（一）預防病毒

病毒爆發到下載能辨識該病毒的病毒碼為防毒空窗期，是電腦用戶遭感染的高峰期。有的病毒甚至會關閉防毒軟體或是阻擋更新病毒碼。

《防治病毒123》

1.加快病毒碼自動更新的頻率，並即時下載更新掃毒引擎程式才是上策。

2.關閉電子郵件預覽視窗，或者安裝郵件病毒掃描程式，不要開啟來路不明的電子郵件。

3.設定作業系統自動更新修補通知，接獲通知後立即下載作業系統修補程式，防止病毒利用系統漏洞入侵。

（二）中毒處理

1.要立即到資訊安全公司的網站下載最新病毒碼或掃毒程式。

2.清除病毒。

3.更新系統。

4.若仍無法清除病毒，儘可能在不連接網路的情形下重灌系統。

三、處理垃圾郵件

（一）拒收無主郵件

在仔細分析垃圾郵件後，我們可以發現其中許多郵件的收件人或發件人欄位是空白的。

（二）過濾特定郵件

發送垃圾郵件者大多有一定的目的，比如進行商業廣告、推銷產品、發佈資訊等，這些郵件的發件人位址、主題或內容中都會有一些相關的字句，因此只要把握其中常用的詞語，就能利用設置郵件過濾規則攔截掉大部分的垃圾郵件。

（三）使用郵件遠端管理

遠端郵箱管理可使你在下載郵件伺服器上的所有郵件之前，直接對伺服器上的郵件進行操作。這樣對於你不想接收的垃圾郵件，可直接在伺服器上將它刪除。

（四）慎用自動回信功能

許多朋友在郵件系統中設置使用了　自動回信”功能，這樣會讓發垃圾信者測試信箱是否常用，而決定列入寄發名單中。

四、個人資通安全基本認知

在現今資訊科技便利的時代，個人資料遭盜用與個人隱私遭受侵害的事件不斷發生，因此，當我們在享受便利的資訊生活的同時，更應重視個人資通安全及資料保護的觀念，以降低個人資料被盜用的機會。

以下說明個人資料保護的基本認知：

(一)個人電腦應安裝防毒軟體，並經常修補系統漏洞。除定期更新病毒碼與系統漏洞修補程式外，每次開機使用前，建議可以先檢查是否已更新病毒碼及將系統漏洞修補至最新版本。

(二)為避免感染病毒，建議關閉電子郵件預覽窗格功能。

(三)對於來路不明之電子郵件，不宜隨意打開，以免啟動惡意程式執行檔，使個人電腦與資訊系統遭到破壞。

(四)為避免導致他人電腦感染電腦病毒，不任意轉寄來歷不明之電子郵件。

(五)不瀏覽任何可疑或非法網站。

(六)不使用電腦時，宜採取登出、設定螢幕保護功能、關機或其他適當之保護措施。

(七)個人電腦應啟用螢幕保護程式功能，並設定密碼保護，於電腦暫時無人使用時可自行啟動，啟動螢幕保護程式的時間設定可依個人的使用狀況調整。

(八)審慎選擇個人帳號的密碼，密碼最好6碼以上且必須包含大小寫英文字母、數字及符號。

五、網路誹謗案例與相關法律

刑法第三百一十條誹謗罪規定：「意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金(第一項)。散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或一千元以下罰金(第二項)。對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限(第三項)。」

刑法第三百一十一條規定：「以善意發表言論，而有左列情形之一者，不罰：一、因自衛、自辯或保護合法之利益者。二、公務員因職務而報告者。三、對於可受公評之事，而為適當之評論者。四、對於中央及地方之會議或法院或公眾集會之記事，而為適當之載述者。」

網路誹謗案例：

宋小文是某大學機械系三年級的學生，也是機車一族，舉凡上學出遊都是靠他的野狼一二五。某日，宋小文前往居家附近的一家機車行，詢問有關機車輪胎的價錢，但是當天他並沒有在該機車行更換機車輪胎。

事後，他在某網站留言版上，發表了一篇標題為「黑店」的文章，該文章的內容是有關他詢問該機車行機車輪胎的心得感想，該文章中指稱該機車行是「黑店」，以及「將二手胎整理得跟新的一樣，還拿來當作全新輪胎賣」等，具體指責該車行誇大商品的效果，並抬高售價欺騙消費者的行為。該文章還以該機車行的老闆丁恤背後印著「非常機車」的字樣，調侃該老闆「應該是二手車店騙不夠，再出來騙的吧！」。

該機車行老闆王大宇原本並不知道被人上網批評，後來經由上網友人的告知，並將

宋小文的文章列印下來給他看，王大宇得知後氣憤難耐，認為宋小文在網站留言版上張貼內容不實的文章，供不特定人上網瀏覽觀看，並任人轉寄散佈，已經嚴重損害他的商譽，導致該機車行生意一落千丈，王大宇先是向該網站留言版的版主提出抗議，其後並向警政署刑事警察局偵九隊提出毀謗罪告訴，並要求宋小文賠償損失新台幣十萬元。

本案例中，宋小文在未經查證即意圖散佈於眾，故意在網路上發表及散佈足以毀損王大宇名譽之不實的言論，造成王大宇名譽上的損害，已觸犯了刑法第三百一十條第一項之誹謗罪。在網路上利用電子郵件，將宋小文毀謗王大宇的「文章」轉寄給他人之人，如果符合意圖散佈於眾，而「傳述」足以毀損他人名譽之事者，亦構成刑法第三百一十條第一項之誹謗罪。

誹謗罪為告訴乃論之罪，依刑事訴訟法第二百三十七條的規定，王大宇須在六個月內提起告訴，並可依民法第一百八十四條第一項前段之規定：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。」，起訴請求宋小文與轉寄誹謗文章之人，賠償其名譽所受之損害。

誹謗罪為告訴乃論之罪，依刑事訴訟法第二百三十七條的規定，王大宇須在六個月內提起告訴，並可依民法第一百八十四條第一項前段之規定：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。」，起訴請求宋小文與轉寄誹謗文章之人，賠償其名譽所受之損害。

六、網路霸凌之案例與探討

網路霸凌在臺灣也發生過不少案例，有些用留言癱瘓對方部落格留言板，有些則是以辱罵信件塞爆對方信箱，或將不當影片上傳至網路影音平台，這些行為都可能觸犯妨害名譽罪。例如：

北部某高中發生十五名同學砸教室桌椅，共同圍毆一名同學，還由另一位同學用手機全程錄影，P0上部落格炫耀，少年警察隊介入調查，學校把十二名肇事學生退學，但受害同學已有創傷後遺症。

中部一所國中班級有人掉了錢包，許多同學都到班級的留言版匿名留言，懷疑是某個同學偷的；雖沒有證據證明是那個同學偷的，不過因為錢包事件，造成大家都覺得他是可疑份子，漸漸不跟他往來，也使該同學心靈受創。

當我們遇上網路霸凌時，應該：

(一)勇於終止：發現時應該先將網路不當的資訊紀錄存證並向網路管理人投訴及要求刪除不當資訊，包括影片、圖片、文字等，使其不再傳播。

(二)勇於求助：尋求家長、學校老師或警察的協助，千萬不可因害怕脅迫而屈服退讓。

(三)勇於通報：發現同學遭受網路霸凌時，應通知學校老師進行處理。

四通八達

問題一：哪些因素讓惡意程式（電腦病毒、木馬程式或是電腦蠕蟲），能快速散播？

問題二：電腦病毒和駭客有什麼不同？

問題三：如何判斷電子郵件是可以信任的？

五經四書

■進一步了解可參閱

林宜隆（2009）。**網路犯罪理論與實務**。中央警察大學出版社出版。第三版。

中小學教師網路素養與認知網站http://eteacher.edu.tw/

臺灣電腦網路危機處理協調中心http:// www.cert.org.tw/

國科會資通安全資訊網http://ics.stic.gov.tw/

教育部校園資訊安全服務網http://cissnet.edu.tw/index.aspx

教育部電子計算機中心 http://www.edu.tw/moecc/index.aspx

中華民國資訊安全學會http://www.ccisa.org.tw/

政府網路危機處理中心http://www.gsn-cert.nat.gov.tw/

國家資通安全應變中心http://www.ncert.nat.gov.tw/

CERT （英文網站）http://www.cert.org/

臺大資通安全服務小組http://cert.ntu.edu.tw/

賽門鐵克Norton http://www.symantec.com.tw/

趨勢科技http://www.trendmicro.com.tw/

Mcafee http://us.mcafee.com /

資安人http://www.isecutech.com.tw/

行政院國家安全資通會報http://www.icst.org.tw/online/

國家資通安全會報技術服務中心http://www.icst.org.tw/

■本文參考資料

吳清基、林宜隆（2004）。**資訊素養與倫理－高中版教材**。臺北市政府教育局。

林宜隆（2009）。**網路犯罪理論與實務**。中央警察大學出版社出版。第三版。

趨勢科技http://www.trendmicro.com/tw/home/enterprise.htm

賽門鐵克http://www.symantec.com/region/tw/

蕃薯藤網路謠言http://feature.yam.com/urbanlegends/

政府網路服務網-垃圾郵件http://spam.gsnmm.gov.tw/

問題一參考答案：

1.網路設備完善及作業系統普及。

2.資通安全防護（防毒、防駭）不足。

3.使用E-Mail隨意轉寄信件。

問題二參考答案（註：參考趨勢網站）：

所謂電腦駭客（Hacker）指的是以非法手段侵入別人電腦，來竊取或修改電腦中重要資料的人，或利用系統本身漏洞，來攻擊散播駭客工具。

電腦病毒與駭客，原本不可混為一談，但紅色警戒病毒（CodeRed）將兩者的特性結合，進而繁衍出強大的破壞力。

4-2病毒與駭客比較表「註2」

	電腦病毒（Virus）	駭客（Hacker）
入侵對象	沒有特定目標	鎖定特定目標
隱喻	某人持有合法護照，但在出入境時，攜帶的行李被放置槍砲彈藥等違禁品（病毒程式）海關（如同企業網的Gateway）並沒有察覺，於是在突破第一道關卡後，這些違禁品進入國境（個人電腦或企業網路），隨時產生破壞動作。	被限制出入境者（非企業網管人員），以幾可亂真的Password 欺瞞海關守門員（如同企業網路的Gateway），進入國境〈 企業網路〉 後，鎖定迫害對象（各企業電腦主機）進行各種破壞動作；或針對系統的漏洞加人攻擊或散播。
舉例說明	一個合法的使用者在有意無意問所「引進」病毒，其管道可能是直接從網際網路下載檔案、或是開啟E-Mail中含有病毒的附加檔案（Attachment）所感染。	沒有合法身份認證的電腦駭客通常都會先想辦法取得一個合法的通行密碼，就可以藉著這把鑰匙在網路上通行無阻，或利用系統本身漏洞，來攻擊散播駭客工具。

問題三參考答案（註：參考微軟資訊安全中心）：

如果你使用電子郵件，每天會收到很多封郵件，哪些電子郵件是垃圾信、哪些可能含病毒或散佈謠言信，你如何知道哪些可以信任？請檢查下表各項：如果主旨列只是亂碼或無意義的字，則可能是垃圾郵件，其使用無意義的標題，是企圖通過尋找特定文字的垃圾郵件篩選器。

項次	檢查內容	是	否
1	你認識這封電子郵件的寄件者嗎？		
2	這是你知道且信任的個人、組織或公司嗎？		
說明：如果是你之前從未聽說過的人或從未訂閱的來源收到郵件，則應該小心			
3	你先前曾從這個來源接收過沒問題的電子郵件嗎？		

如果你不確定收到的電子郵件是否足以信任，請勿開啟它，更不要回覆它。開啟郵件之前先檢查，比事後從電腦清除病毒要容易許多。

一個應採取的基本動作是：

在你開啟含有附件的任何電子郵件之前，請確定你的防毒程式是最新且開啟的。如此可讓防毒程式利用最強的防護機制掃描附件。

記住!請用大腦思考控制滑鼠，不要只用手指!

註釋：

「註1」趨勢科技。

http://tw.trendmicro.com/tw/threats/vinfo/general/index.html

「註2」趨勢科技。民93 年11 月月11 日，取自：

http://www.trendmicro.com/tw/security/general/guide/overview/guide06.htm