一觸即發

常聽到或遇到下列狀況嗎？

「電腦中毒了！無法清除、無法隔離……」

「系統怎麼慢得可以……」

「系統60秒倒數計時關機中……」

「眞的會有駭客入侵我的電腦嗎？」

「最近有人傳說上網會被盜取系統資料，眞的嗎？」

「一堆垃圾郵件煩死了！」

「網路流傳吃某某東西可以治病或減肥，眞的嗎？」

除非你拒絕上網，不然你一定要看下去。

雙管齊下

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，但不當資訊也伴隨而來，本單元主要探討大都是不請自來的資訊，包含電腦病毒、垃圾郵件及網路謠言。

在網際社會中，已是一人中毒親朋好友跟著遭殃，若不想被指責是病毒帶原者，就必須了解網路中惡性程式特徵及其危害與防範之道，確實做到網路安全人人有責。

一、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；針對三十二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。電腦病毒的作者爲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。

二、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

式會將自己僞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對方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。

三、電腦蠕蟲(Worm)

電腦蠕蟲不會感染其他檔案，但會複製出很多〝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（Local Area Network,LAN）資料夾分享或是網際網路（Internet）E-Mail 來散佈自己。著名電腦蠕蟲的例子爲『VBS_LOVELETTER』。

四、惡性程式（Malicious Code）

『惡性程式』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。

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性程式愈來愈少了，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性程式爲〝病毒〞，本單元也以〝病毒〞稱之。

例如：

（一）『梅莉莎』(MELISSA) 便是結合『電腦病毒』及『電腦蠕蟲』的兩項特性。該惡性程式不但會感染 Word 的 Normal.dot（此爲巨集型電腦病毒特性），而且會透過微軟郵件軟體(Outlook)大量散播（此爲電腦蠕蟲特性）。

（二）另外一個案例是結合了『木馬程式』及『電腦蠕蟲』兩項特性的『探險蟲』(TROJ_EXPLOREZIP)。探險蟲並不會感染任何檔案，但是會覆蓋掉(Overwrite)在區域網路上遠端電腦有設定分享的資料夾中重要檔案（此爲木馬程式特性），並且會透過區域網路將自己安裝到遠端電腦上設定分享的資料夾中（此爲電腦蠕蟲特性）。

五、垃圾郵件(Spam Mail)

一般所稱的垃圾郵件爲〝將一份內容相同的電子郵件，大量寄給不同的人且未經收信人許可，郵件內容多數是與收信人不相干的商業廣告〞。另一種垃圾郵件爲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。

垃圾郵件不僅限於一般的電腦網際網路上的郵件，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。

六、網路謠言

透過網路上的電子布告欄、新聞討論群、留言版或電子郵件散布未經證實或惡

意中傷的言論，製造恐懼、傳播自殘思想或是道德教訓，也有的單純只爲惡作劇。網路謠言因散播快且廣，對於網路族群中人際關係差或心智未成熟者常造成不安與焦慮。

例如網路郵件常收到朋友好心轉寄有新病毒警告信，內容大意是"如果你收到一封信，千萬別打開，因爲它會刪掉你硬碟上的一切。這是一封非常新、而且非常惡劣的人所寫的病毒，這消息可是微軟公佈的"。

上述利用大家對電腦病毒的恐懼與焦慮以及權威的單位證實，就是散布網路謠言的一種手法。該郵件在網路流傳一段時間後，還有"好心"的友人繼續轉寄呢。

三思而行

以下針對電腦病毒、垃圾郵件、網路謠言的傳播與預防處理來探討。

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』爲例，它開創病毒行爲新模式，感染『探險蟲』病毒的電腦，會透過網路自動複製到其他電腦，並試圖刪除有將資料夾分享出來的電腦中該資料夾中的檔案。這樣的行爲對於電腦作業系統而言，是完全合法的，因爲只要權限足夠，可以對任何設定爲資源分享的資料夾做存取的動作，而這也是爲什麼『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，最近的例子爲殺手病毒(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，所以有人認爲在使用電子郵件時，只要不執行或開啓附件就不會遭受病毒感染，但『VBS_BUBBLEBOY泡泡男孩』由VBScript語言所寫成的病毒，即使是僅開啓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E-Mail 時，不論我們是直接開啓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（有開啓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) 惡性程式僞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.僞裝成防毒公司寄發〝解毒程式.EXE〞
3.僞裝成銀行或卡務中心寄發〝信用卡確認程式・EXE〞
4.僞裝成〝有趣、好看或色情網頁文件等〞
5.網路釣魚(Phishing)，僞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。

6-1 病毒發展表

	1987-1993	1993-1995	1995-1998	1998-目前
電腦病毒	1.DOS 檔案型 2.DOS 常駐型 3.開機型	Win16 檔案型	針對 MSOffice 系列的巨集型病毒	1.Win32 檔案型 2.Win32 常駐型 3.跨應用程式感染型(Win32 及巨集)
特洛伊木馬程式	毀滅型（格式化磁碟）	無典型代表	竊取資料的 Backdoor 型程式	1.阻斷服務型(DoS) 2.遠程遙控的 Backdoor 型程式 Wireless 型
電腦蠕蟲	無典型代表	無典型代表	無典型代表	1.E-Mail 散播型 2.網路散播型 Network worm 3.藉由安全漏洞散播型

〔註1〕

二、病毒發展趨勢

從上表看出『傳播媒介』佔有舉足輕重的角色。『傳播媒介』表示的另一層意義是『影響程度』的高低。當傳播愈方便、愈快速、層面愈廣，此時病毒所能影響的範圍也就愈大，PE_CIH再強悍也只不過能透過一部部電腦之間相互感染，但透過E-mail 傳播的『梅莉莎』及『思欣』(TROJ_SIRCAM.A)則可以在一週內造成全球數

以萬計的電腦用戶受到波及。

現有的傳播媒介，『E-Mail』快於『LAN』(區域網路)，而LAN又快於傳統的『磁碟片』，DOS檔案型及開機型病毒幾乎已經絕跡，而單以區域網路爲散播媒介的將逐漸減少，取而代之是以 Internet爲主的 E-Mail型態病毒。

將來除了E-Mail以外，『點對點』(Peer-to-Peer）的傳播方式也值得特別注意，由於網路的普及許多人的電腦已經處於『隨時連線』的狀態，病毒的發展可能傾向於不必藉由第三者（如檔案伺服器、郵件伺服器）而直接散播至各電腦，就像廣播電臺一樣。

三、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爲防毒空窗期，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，不要開啓來路不明的電子郵件，或者安裝郵件病毒掃描程式。

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，儘可能在不連網路情形重灌系統。

四、處理垃圾郵件

(一) 拒收無主郵件

通過對收到的垃圾郵件仔細分析，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，就能通過設置郵件過濾規則將其中的大部分郵件攔截掉。

(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，可直接將它在伺服器上刪除。

（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。

五、處理網路謠言

網路謠言一樣止於智者。當你收到或看到某些議題，需要多方探討、多問問對相關言論有研究的人；若無法查證議題的眞僞，不應再散佈出去。

過去的謠言透過人們口耳相傳，內容經由不同人轉述或加油添醋或增減劇情，而與原先版本不同，惟其散佈的範圍有限。現在網路謠言透過網路論壇、新聞群組及電子郵件的圖文轉貼或轉寄，版本一致，網路傳播的速度快、廣度深，加上電腦影像合成技術日益進步，用逼眞的假圖片佐證謠言，其可信度大增。因此網路謠言所造成的影響也較過去更爲深遠，並且足以令許多舊謠言死灰復燃。

例如引發軒然大波的販賣「瓶中貓」(Bonsai Kitten) 事件，經查證後其實是麻省理工學院學生惡作劇，利用影像合成做出的一系列假照片(圖片)，卻因此引發美國聯邦調查局 (FBI) 大舉調查。類似謠言其實並不新鮮，然而配合上幾可亂眞的圖片或影像後所造成的震撼力頓時增加數倍。

網路上的E-Mail常常是沒由來的轉寄，但是似乎很少人會去證實信件的眞實度，反而多數人會順手把它轉寄出去，這樣方便的E-Mail傳遞，卻也成了最好的「網路謠言」溫床，別忽視了網路謠言的恐怖，趕快上搜尋網站輸入關鍵字〝網路謠言〞，看看討論網路謠言的網站相關訊息。

四通八達

問題一：哪些因素讓惡性程式(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：如何判斷可信任的電子郵件？

五經四書

進一步了解可參閱.....

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/

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

參考網站
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/

參考答案

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，原本不可混爲一談，但紅色警戒病毒(CodeRed)將兩者的特性結合，〔註2〕

6-2 病毒與駭客比較表

入侵對象	電腦病毒(Virus) 沒有特定目標	駭客（Hacker） 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（如同企業網路的Gatcway）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），以幾可亂眞的 Password 欺瞞海關守門員（如同企業網路的Gatcway），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入攻擊或散播。
舉例說明	一個合法的使用者在有意無意間所「引進」病毒，其管道可能是直接從網際網路下載檔案、或是開啓 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。

進而繁衍出強大的破壞力。

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，則應該要小心。		
3	你先前曾從這個來源接收過沒問題的電子郵件嗎？		
4	你是定期還是偶而接收到這個人傳來的電子郵件？		
5	你有沒有任何理由預期這個人會寄電子郵件給你？		
	說明：如果你收到的電子郵件來自你認識的人，但你以前從未收過他們傳來的電子郵件，則自問是否有任何理由現在會收到這封郵件。如果答案爲否，請在開啓它之前要小心。		
6	看見這封電子郵件時你感到驚訝嗎？		
7	收到這個人寄來的電子郵件是不尋常或奇怪的嗎？		
	說明：如果答案爲是，則開啓郵件時請小心。		
8	主旨列上的訊息與寄件者是否合理？		
9	主旨列是否提到這個人寄訊息給你是要講什麼事？		
	說明：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。		

如果你不確定收到的電子郵件是否足以信任，請勿開啓它，更不要回覆它。開啓郵件之前先檢查，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：

在你開啓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啓的。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。民93年10月月12日，取自：http://www.trendmicro.com/tw/security/general/guide/overview/guide02.htm

〔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