高中職版

資訊素養與倫理

第3版

單元5　不當資訊與相關法律

壹、靈根孕育源流出

故事緣起...(1/3)

- 七夕情人節來臨之際，鐵扇公主想上網購買花卉送給夫君牛魔王，沒想到當他點開廣告信件，並安裝了建議的程式後，電腦突然關機無法動彈了，他焦急地哭了起來…

故事緣起...(2/3)

- 此時孫悟空出現，說：「發生了甚麼事？我三千里外就聽到你的哭聲了」，鐵扇公主哭訴著電腦無法開機的事情，孫悟空聽後，笑笑地說：「我猜你應該是電腦中毒了吧，之前豬八戒也有遇過這種事，我記得師父有教我該怎麼處理。」

故事緣起...(3/3)

- 鐵扇公主一聽到有解決方法，馬上說：「大聖，那就拜託你幫幫我吧…」，看在鐵扇公主真心求情的份上，孫悟空開始解釋關於電腦安全的維護方法。


發生了甚麼事？我三千里外就聽到你的哭聲了。


我猜你應該是電腦中毒了吧，我記得師父有教我該怎麼處理。


大聖，那就拜託你幫幫我吧…

- 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與個資外洩，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、垃圾郵件等）、個人資通安全基本認知及網路誹謗、臉書帳號被盜用、個人資料保護之案例與相關法律探討，並瞭解網路中惡意程式特徵如圖5-1 及其危害與防範之道，確實做到網路安全人人有責。

圖 5-1 網路中的惡意程式特徵

貳、悟徹網路妙真理

一、不當資訊的主要類型

（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（DOS ,Disk Operating System）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」（Dos , Denial ofservice）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（Local Area Network , LAN）資料夾分享或是網際網路（Internet）E -Mail 來散布自己。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。

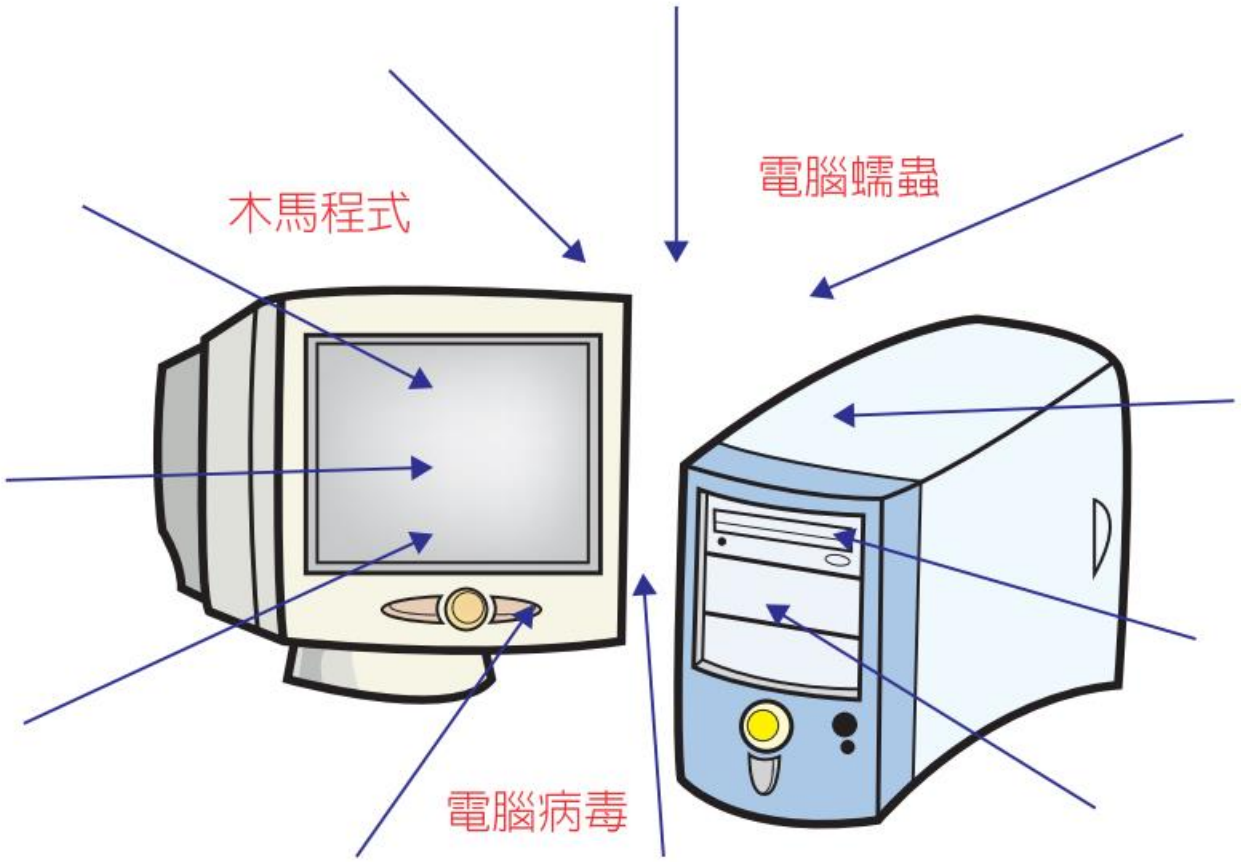

圖 5-2 惡意程式（Malicious Code）

	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，散布的數目多
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

表 5-1　惡性程式比較表

資料來源：取自趨勢科技（http://tw.trendmicro.com/tw/threats/vinfo/general/index.html）

（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、身分證統一編號或其他機敏資料，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、身分證統一編號、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Skype），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，即可以合法的身分登入使用者帳號，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分而更加猖獗，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。

(八) 個人資料

➲1. 什麼是個人資料？個人資料是一種可以讓大家更加了解我的資訊：

WHO	孫悟空，男性
WHEN	年齡1425歲
WHAT	1. 家族有師父唐三藏、我孫悟空、二師弟豬八戒、三師弟沙悟淨 2. 身高180公分,體重70公斤
HOW	電話：(02)23456789 地址：東勝神洲傲來國花果山水濂洞 電子郵件：monkey@tatang.gov.tw

- 2. 個人資料，以下為個資法的定義：（個人資料保護法第二條第一款）
- 3. 蒐集：指以任何方式取得個人資料。（個人資料保護法第二條第三款）
- 4. 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。（個人資料保護法第二條第四款）

- 5. 利用：指將蒐集之個人資料為處理以外之使用。（個人資料保護法第二條第五款）
- 6. 國際傳輸：指將個人資料作跨國（境）之處理或利用。（個人資料保護法第二條第六款）

一般資料	特種資料	其他
• 自然人之姓名 • 出生年月日 • 國民身分證統一編號 • 護照號碼 • 特徵 • 指紋 • 婚姻 • 家庭 • 教育 • 職業 • 聯絡方式 • 財務情況 • 社會活動	• 醫療 • 基因 • 性生活 • 健康檢查 • 犯罪前科 • 病歷	• 得以直接或間接方式識別該個人之資料
個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集 合。(個人資料保護法第二條第二款)		

表 5-2 個資法的定義

（九）進階持續性滲透攻擊（Advanced Persistent Threat, APT）

- 進階持續性滲透攻擊 (Advanced Persistent Threat, APT)，進階持續性滲透攻擊，Advanced 意思是指精心策畫的進階攻擊手法；Persistent 則是指長期、持續性的潛伏；APT 攻擊主要重點在於低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料。

- 所以能發動這種APT 攻擊手法的駭客，都是以長期滲透特定組織為目標，擁有高超複雜的入侵技巧，並且有足夠資金，才能支持這樣的滲透及攻擊活動。

- 2. APT 具備下列五種的特色：
  - （1）高度針對性。
  - （2）具有潛伏並保持低調的技術能力。
  - （3）擁有資料情報分析之能力。
  - （4）擁有多樣工具的多重面向攻擊方式。
  - （5）資金充裕。

	APT	一般駭客攻擊
時間	較長的時間攻擊。	攻擊時間長短不一定。
動機	竊取所需要的特定機密，包括國家安全、商業機密等。	動機不同，從彰顯自己能力和炫耀自己到竊取個人資料換取實質利益都有。
攻擊者	有組織、有計畫的團團體。	一般個人或駭客結盟。
攻擊對象	針對性、小範圍，如政府、公司行號、金融業等。	無針對性、大範圍，近年以具有大量個人資料的企業為主。
攻擊手法	長期、持續性、多樣性，經常是利用零時差系統漏洞的攻擊，確保達成攻擊目的。	多數為數戰數決，複合多種常見系統漏洞，以大量、快速、有效的單一手法入侵。

表5-3 APT 和一般駭客攻擊差異比較

參、資訊山下定心猿

- 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。

- 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布的漏洞，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、發布資訊等，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：

- 1.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。
- 2.為避免感染病毒，建議關閉電子郵件預覽窗格功能。
- 3.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。

- 4. 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。
- 5. 不瀏覽任何可疑或非法網站。
- 6. 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。

- 7. 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。
- 8. 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310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311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：嘲諷同學臉書按讚64 人被告誹謗

臉書（Facebook）上按個讚，在朋友間相當的常見，但是在臺中有一名A男生學生，在臉書嘲諷另外一個B 同學，還獲得60 多個同學按「讚」回應。這篇文章被B 學生的媽媽看到之後，非常生氣，他對PO 文的A 學生，以及所有按讚的 60 多個學生，全部都提起「誹謗」告訴。但有教育專家提醒，家長的大動作、恐怕會讓孩子遭到同學排擠，造成反效果。

- 臺中一間學校的A 學生，在臉書PO 上一篇文章，內容為嘲諷班上另外一名B 同學吹噓交了女朋友，甚至兩個人互動親密。黃同學PO 文說那都是假的，還註明雖然霸凌不對，不過如果彭同學真的被霸凌，也是有原因的。
- 文章PO 上網之後，有 60 多個同學按「讚」回應，此舉讓B 學生的媽媽非常生氣及無法接受。

== B 學生的媽媽說==

這會使人做什麼樣聯想呢？

就是A 學生要對付我的小孩子,

因為我的小孩被全部的同學這樣子在臉書上這樣回應,

那我小孩子要怎麼到學校去面對所有同學

- B 學生的媽媽越看愈生氣，認為帶有誹謗的意味，因此向學校反映，不過隔天，PO 文的A 學生找上B 學生大發脾氣，B 媽媽更氣不過，對PO 文的黃姓學生和按讚的60 多個學生，全都提起誹謗告訴。

== 校方學務主任==

本次事件有些同學不只按「讚」，

還留言，

留下一些情緒性的字眼，

我們有先約談按讚的那些學生，

學校也希望，學生可以把那些字眼刪除

- 校方表示，多次告訴學生，如果看到網路的負面文章不可以隨便按「讚」，也介入調查，不過B 媽媽一次對60 多個學生提出告訴，也造成學生們的恐慌，有人怕到不敢上網，甚至不敢跟B 學生講話，而PO 文的A 學生更因為承受身心壓力，不敢到校上課。教育專家說，父母保護孩子的心情有可原也可以理解，不過從這起事件來看，似乎不算真正霸凌，如果用這麼激烈的方式，反倒造成反效果。

== 人本基金會==

事情發生時要考慮的是

能不能達到保護他孩子的效果,

因為些事件看起來好像這樣做之後,

同學之間因為這樣更不喜歡彭姓同學,

我倒覺得這樣的方式,

反而沒辦法達到他要保護彭姓學生的目的

- 教育專家認為，這起事件並非長期以多欺少，單純按「讚」就提告，很可能引起同學之間更嚴重的排擠效應，對孩子同儕互動並無幫助，建議家長還是讓孩子自己學習溝通修補關係，比較恰當及適合。

六、網路詐騙案例與相關法律

- 刑法第339條詐欺罪規定：
- 「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金（第一項）。以前項方法得財產上不法之利益或使第三人得之者，亦同（第二項）。前二項之未遂犯罰之（第三項）。」

- 刑法第339-1條規定：
- 「意圖為自己或第三人不法之所有，以不正方法由收費設備取得他人之物者，處一年以下有期徒刑、拘役或三千元以下罰金（第一項）。以前項方法得財產上不法之利益或使第三人得之者，亦同（第二項）。」

➲刑法第339-2條規定：

➲「意圖為自己或第三人不法之所有，以不正方法由自動付款設備取得他人之物者，處三年以下有期徒刑、拘役或一萬元以下罰金（第一項）。以前項方法得財產上不法之利益或使第三人得之者，亦同（第二項）。」

- 刑法第339-3條規定：
- 「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處七年以下有期徒刑。（第一項）。以前項方法得財產上不法之利益或使第三人得之者，亦同（第二項）。」

網路詐欺案例：臉書被盜用，1 人受「駭」全家受害

- 一句「你在嗎？」小心中了詐騙陷阱。刑事警察局昨天表示，微軟即時通即將關閉，詐騙集團已將原本認證碼詐騙手法的平臺移轉到「臉書」，從2013 年初迄今，已有40 多人在臉書上被騙，是即時通的十倍之多。警方呼籲民眾提高警覺，避免一人受「駭」，全家受害。

- 家住臺北的A 男子，上月底在辦公室透過智慧型手機收到友人的臉書訊息，疑似詐騙份子的朋友表示因為手機不在身邊，要求A 男子幫忙接收網購的簡訊，A 男子於是提供給對方自己的手機號碼，不多久即收到三封網拍手機確認碼。

- 由於類似詐騙手法層出不窮，盡管業者在簡訊中特別提醒收訊者，勿將確認碼向他人或網路親友透露以防止詐騙，但A 男子仍不疑有他，將認證碼一一告知。沒想到，A 男子傳完後，對方食髓知味，要求繼續提供其他手機電話，因恰巧A男子有事閃過，後來接到朋友傳訊表示帳號被盜，才知被騙報案。

- 另外有位住南投的B 太太，則是上網收到姊夫傳訊息要他代收雅虎拍賣認證碼，於是她便馬上將收到的認證碼一一按對方指示回傳給對方；當傳到第四通認證碼時，B 太太的姊姊趕緊告知帳號遭詐騙集團盜用，才知道自己受騙上當。

- 刑事警察局表示，國內臉書使用者相當多，且分布各年齡層，詐騙集團以此為詐騙平臺，受害者眾，除提醒民眾留意此詐騙手法，也希望臉書使用者能夠經常變更密碼，防止被盜取帳號密碼。

➲為了解決上述網路詐欺犯罪問題，消費者自己應該多加留意，而且應注意下列事項：

1. 瞭解交易對象，選擇經由自律組織認可網路商家消費，切勿輕信誇張廣告，對於短期能獲取暴利機會應多加觀察勿全然相信。
2. 注意相關網站隱私權保護政策的相關說明，切勿輕易洩露重要個人資料。
3. 選擇比較安全付款方式，儘可能是使用貨到付款方式。

4. 確定訂購的產品規格及服務內容。
5. 熟悉相關申訴管道，發現問題立即告訴網路詐欺申訴中心。

七、個人資料保護案例與相關法律

個資保護案例：

北市府表示民眾網購遭詐騙，燦坤可能個資外洩

- 臺北市政府日前陸續接獲民眾投訴遭網路購物詐騙案件，知名3C 連鎖通路商網路商城消費後，立即接獲自稱商城客服人員來電表示刷卡分期作業出錯，需操作ATM 取消辦理刷退，即遭詐騙致一位市民損失10 多萬元，因詐騙集團清楚掌握時間、購買商品、金額、卡號等詳細交易資料，臺北市政府因此懷疑知名3C 連鎖通路商發生個資外洩事件，要求知名3C 連鎖通路商說明並改善。

- 根據臺北市政府的瞭解，臺北市共5 位民眾申訴，新北市有1 位，投訴民眾都是在知名3C 連鎖通路商網路商城刷卡購物後，約2 週到1 個接到自稱客服人員的來電稱作業疏失設定錯誤，原本應分期扣款卻每期扣全額，要求操作ATM解除分期付款設定，雖然5 位民眾懷有警覺心不予理會，但仍有1 位民眾受騙損失10 多萬元。

網購、Skype 為詐騙慣用手法

- 臺北市政府警察局刑事警察大隊資訊室主任林浚奕（2011）表示，經統計臺北市詐騙案例數量因這幾年政府與民間單位共同宣導下，案件數已有明顯的下降，從民國98 年356 件（電話詐騙2080 件，網路詐騙1683 件）減少到100 年的4647 件（電話詐騙859 件、網路詐騙1076 件）。雖然詐騙案件數下降，但值得注意的是宅經濟興起下，100 年網購詐騙事件已超過電話詐騙，躍居各類詐騙案件的首位。

- 根據臺北市府警察局觀察，網路詐騙慣用手法最多的是網路購物後假裝客服要求操作ATM 解除分期付款，其次則是Skype 帳號被盜用，歹徒冒用其帳號要求親友代為購買遊戲點數、借款等等，光是國內Skype 帳號被盜案例每月約發生130 多件，造成100 多萬的財產損失。

- 網購的相關詐騙，需業者加強資安防護、員工教育，並透過宣導提高民眾警覺心，而Skype 帳號被盜用部份，刑事局去年已與微軟合作，只要民眾發現帳號被盜可前往警局報案要求停權，由刑事局165 匯整資料後交給微軟停權，事後若要復權需向微軟申請。

肆、功成圓滿見真如

- 問題一： 哪些因素讓惡意程式（電腦病毒、木馬程式、電腦蠕蟲或APT），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？
- 問題四：隱私權侵犯的主要型態有那些？

伍、西天取經傳正念

一、進一步了解可參閱

- 1.林宜隆（2009），網路犯罪理論與實務（第三版）。中央警察大學出版社出版。
- 2. 詹炳耀、任文瑗、陸啟超、郭秋田（2013），資訊倫理與法律（第三版）。旗標出版股份有限公司。
- 3. CERT（英文網站），http://www.cert.org/
- 4. Mcafee，http://us.mcafee.com/

- 5. 中小學教師網路素養與認知網站，http://eteacher.edu.tw/
- 6. 中華民國資訊安全學會，http://www.ccisa.org.tw/
- 7. 行政院國家安全資通會報，http://www.icst.org.tw/online/
- 8. 政府網路危機處理中心，http://www.gsn-cert.nat.gov.tw/
- 9. 國科會資通安全資訊網，http://ics.stic.gov.tw/
- 10. 國家資通安全會報技術服務中心，http://www.icst.org.tw/

- 11. 國家資通安全應變中心，http://www.ncert.nat.gov.tw/
- 12. 教育部校園資訊安全服務網，http://cissnet.edu.tw/index.aspx
- 13. 教育部電子計算機中心，http://www.edu.tw/moecc/index.aspx
- 14. 資安人，http://www.isecutech.com.tw/
- 15. 臺大資通安全服務小組，http://cert.ntu.edu.tw/
- 16. 臺灣電腦網路危機處理協調中心，http://www.cert.org.tw/

- 17. 賽門鐵克，Norton http://www.symantec.com.tw/
- 18. 趨勢科技，http://www.trendmicro.com.tw/

二、本文參考資料

- 吳清基、林宜隆（2009）。資訊素養與倫理 - 高中版（2 版）。臺北市：臺北市政府教育局。
- 林宜隆（2009）。網路犯罪：理論與實務（第三版）。桃園：中央警察大學出版社。
- 賽門鐵克（2013 年10 月24 日）。IT 安全威脅。2013 年10 月24 日， 取自 http://www.symantec.com/zh/tw/security_response/

- 趨勢科技（2013 年10 月25 日）。安全情報分析-網際網路威脅研究。2013 年10 月25 日， 取自 http://www.trendmicro.tw/tw/security-intelligence/index.html#current-threat-activity
- 臺灣電腦網路危機處理暨協調中心（2013 年12 月20 日）。進階持續性滲透擊（APT）簡介。2013 年12 月20，取自 http://www.cert.org.tw/docfile/apt.pdf

三、參考答案

問題一

- 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.E-Mail 隨意轉寄信件。

問題二

- 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（Code Red）將兩者的特性結合，進而繁衍出強大的破壞力。（註：參考趨勢網站）

	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以攻擊或散播。
舉例說明	一個合法的使用者在有意無意間「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。	沒有合法身分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。

表 5-4　病毒與駭客比較表

資料來源：取自趨勢科技。2004 年 11 月 11 日（http://www.trendmicro.com/tw/security/general/guide/overview/guide06.htm）。

問題三

- 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布謠言信，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。（註：參考微軟資訊安全中心）

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！

問題四

美國法律學會將隱私權之侵犯分為四種型態：

➲1. 不合理地侵犯他人隱密之處。

➲2. 竊用他人之姓名或肖像。

➲3. 不合理地公開他人的私生活。

➲4. 使他人有不實形象之公開。

（註：參考資訊倫理與法律第三版，旗標出版股份有限公司）

Q & A