數位生活

全世界60億人瘋傳

你是否曾在網路上看過標題很聳動的文章，例如：「所有人都驚呆了」，或是「這個小男孩的行為，讓全火車的人都為之沉默了」等等，這類的文章會無所不用其極的在標題或內容上動手腳，來引誘網友進入網站，但點進去之後，看到的往往是各種聳動激情、低素質、胡亂堆疊的資訊。

內容農場(Content Farm)是指圖謀網路廣告等商業利益的專業公司，以取得流量為主要目標。內容農場製造的文章多半低素質、不具參考價值而且摻雜著許多廣告式的連結，這是因為其文章可能是由多數人所寫的片段所組成，或配合機器自動編湊產出。(資料來源：維基百科)

在這資訊爆炸的世代裡，慎選閱讀的內容非常重要，若無法判斷文章的真偽，最好的方法就是不點擊、不分享、不轉貼，別讓自己變成「會移動的內容農場」。

資訊超載與資訊焦慮

資訊的生產突飛猛進，資訊與消息已成為人們最大負擔，帶來「資訊焦慮」與「資訊超載」的煩惱。管理大師杜拉克說過「資訊時代是為了那些能運用資訊的人而預備的」。這種能運用資訊自如的人，即是具備「資訊素養」的人。

藍斯・蕭(Lance Shaw)表示:「在我們這個對資訊狂熱，而且充分飽和的社會，已經開始出現一種病症；症狀是：一種偏執的迫使自己遍讀一切可讀之物，當吸收的閱讀量超過消化所需的能量時，超出的部分日積月累，最後因壓力與過度刺激轉化為所謂的資訊焦慮症。」

雖然資訊如此重要，但若未加以管理，就會形成資訊過多或缺乏資訊的情形。因為人類從環境接受輸入的容量是有限的，當人類所具有的內在過濾或選擇程序無法處理增加的資訊時，就會發生資訊超載。

CHAPTER 05

資訊安全與倫理

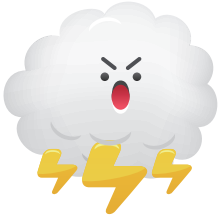
本章摘要

5-1 資訊安全與防護

網際網路爲人類社會帶來了前所未有的便利，同時也衍生出許多資訊安全上的問題，迫使我們必須正視網路安全與管理的重要性，了解資訊社會所帶來的各種安全顧慮，並學習如何處理與防範安全上的漏洞，才能無虞享受資訊生活帶來的便利。

5-1-1 導致資訊不安全的因素

❋ 天然災害



許多的天然災害會導致電腦硬體設備、資料被破壞等問題，像是：地震、火災、水災等天然災害。這些天然災害可能會造成軟、硬體的損壞，導致整個資訊系統失靈。爲了防止不可預測的天然災害發生，定期備份電腦中的資料是非常重要的一件事。

❋ 人為因素

人爲因素在資訊安全中是最難防範的，由於人爲的作業疏忽所造成的資訊損毀、硬體設備損壞等，都會造成資訊安全的問題。常見的人爲因素有：怪客入侵、員工操守等。

- 怪客入侵：所謂的怪客(Cracker)是指一群未經許可便透過網路入侵他人電腦系統，進行竊取機密資料或去篡改資料等犯罪行爲的人；而駭客(Hacker)則是指熱衷於程式撰寫與熟悉作業系統的專業人士，他們並不會惡意破壞他人電腦。不過目前在一般用語上，普遍已將兩詞混用。然而，無論是否造成系統的破壞，未經他人允許而任意入侵他人電腦，都是不正當的行爲。

  企業要避免怪客入侵電腦竊取資料，可以在系統與網際網路間架設一個網路安全的防火牆(Firewall)。

- 員工操守：員工的操守對於資訊安全的維護是非常重要的，員工操守若不好，可能會將公司的機密性資訊洩露，而導致資訊安全的問題產生。對於此點，可以先對員工進行教育宣導、調查及分類，以防止問題的產生。

5-1-2 認識惡意程式

惡意程式(Malicious Code)是指所有不懷好意的程式碼，例如：電腦病毒、電腦蠕蟲、特洛伊木馬程式、後門程式、間諜軟體等。網際網路的無遠弗界，讓惡意程式找到一條最好的散布管道。藉由網際網路開放的網路架構，就可以散播得更快速、更無孔不入、也更防不勝防。

❋電腦病毒

電腦病毒(Computer Virus)是由意圖不軌的人所撰寫的程式，這些病毒設計者，有些是爲了報復、有些只是單純的惡作劇、有些則是爲了炫耀自己的電腦程式設計能力，因爲動機不同，所以電腦中毒後所遭受的破壞也會有所不同，輕則損失一些檔案，重則損毀整個硬碟，導致無法再啓動電腦。

電腦病毒具有高度的傳染性，一旦使用了有毒的磁片，病毒就會潛伏在電腦系統內，待時間一到就會破壞電腦中的資料。雖然電腦病毒的種類非常多，但常見的種類如表5-1所列。

▼ 表5-1 電腦病毒的種類

病毒種類	病毒說明
開機型病毒	這類的病毒會寄生在磁碟的啓動磁區裡或是磁片中，當我們使用已感染病毒的磁片開機時，病毒便會感染系統。常見的開機型病毒有：米開朗基羅病毒、4789病毒等。
檔案型病毒	這類的病毒通常會寄生於可執行檔(*.exe、*.com)中，當我們執行該類的檔案時，病毒就會發作。常見的有：耶路撒冷病毒、龍貓病毒等。
混合型病毒	這類的病毒包含了開機型和檔案型病毒的特徵，它不僅會感染可執行檔，也會感染開機系統區。常見的有：FLIP反轉病毒、Hammer大榔頭病毒。
巨集型病毒	這類的病毒會感染文件中的巨集指令，凡是具有巨集功能的軟體均有可能被感染。常見的有：台灣NO.1病毒、釣魚台病毒等。
千面人病毒	這類的病毒經過繁殖過後便會變換結構，以不同的病毒碼再傳染到別的地方。常見的有：Marburg病毒。

NOTE

製作電腦病毒、木馬程式、電腦蠕蟲程式等電腦程式，專供自己或他人犯罪，導致發生損害於公衆或他人的情況，觸犯刑法第362條罪則，可處五年有期徒刑。

❋ 電腦蠕蟲

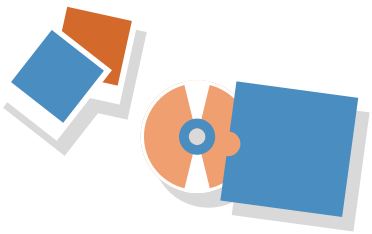
電腦蠕蟲(Worm)可以自我複製出許多「分身」，並透過網路連線或電子郵件等方式進行進行散播。與電腦病毒不同的是，它通常不會感染其他檔案，其主要危害在於引發一連串的指令或動作，佔用大量電腦資源或網路頻寬，進而癱瘓電腦主機、網路或郵件伺服器。

❋ 特洛伊木馬

特洛伊木馬(Trojan Horse)是一種透過網路的遠端遙控程式。通常潛伏在惡意網頁中，或是僞裝成有趣的小程式，吸引使用者下載或執行，然後伺機在受害者電腦中安裝惡意程式，使入侵者具有與電腦使用者相同的權限，並藉此執行一些惡意行爲，像是刪除檔案、竊取密碼與機密資料、或利用受害電腦進行非法行爲等。

5-1-3 惡意程式的防範

要預防惡意程式，最好的方法就是養成良好的電腦使用習慣及在電腦中安裝防毒軟體。



不使用來路不明的檔案或盜版軟體，如果常使用來路不明的磁片或光碟片時，那麼電腦中毒的機率就非常的大。

隨時注意特殊的檔案(例如：COMMAND.com、EMM386.exe、WIN.com、SMARTDRV.com等)的長度與日期，以及記憶體使用情形，並重視電腦系統所發生的異狀。

不要隨便開啓來路不明的電子郵件。當收到來路不明或帶有電腦病毒的郵件時，常常會將這些病毒再傳播給你通訊錄中的朋友，而導致他人電腦也一併中毒。

任何可以儲存資料、傳輸資料的地方都有可能是病毒傳播的途徑，從網路上下載檔案也是電腦病毒的傳播途徑，下載檔案時，請確認該檔案是沒有病毒的。

❋安裝防毒軟體

爲了保障自己電腦的安全，記得在電腦中安裝一套防毒軟體，並且別忘了時常進行病毒碼的更新，如此才能讓電腦得到最佳的保護。

目前市面上常見的防毒軟體有PCCillin、Norton AntiVirus、Kaspersky Anti-Virus 等，亦有免費的防毒軟體ClamWin可供下載使用(圖5-1)。

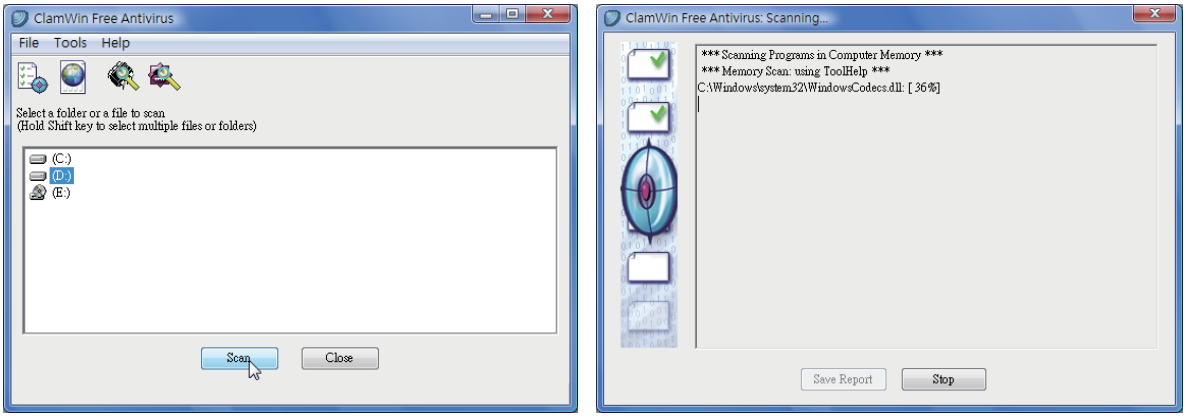


圖5-1 「ClamWin」是一套免費的防毒軟體，該防毒軟體具有排程掃描、線上更新病毒碼、即時偵測等功能。對該軟體有興趣者，可以至http://www.clamwin.com網站中下載。

❋行動裝置防毒軟體

近年來行動裝置的使用率激增，智慧型手機與平板電腦等行動裝置已成爲駭客網路攻擊的鎖定目標。若擔心自己成爲駭客的攻擊對象，建議可安裝專門爲行動裝置所設計的防毒軟體，保護行動裝置與資料的安全，並攔截網路釣魚威脅，防止惡意或高風險的網址和App。

許多知名的防毒軟體公司，如：趨勢科技、賽門鐵克等，目前都有推出使用於行動裝置的防毒軟體(圖5-2)，若有需要，可至該公司網站購買，或下載試用版試用。

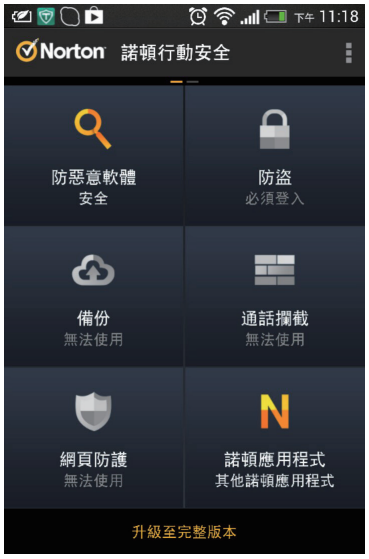


圖5-2「諾頓行動安全」防毒App。

5-1-4 常見的怪客攻擊手法

了解怪客常用的攻擊手法，以防範怪客攻擊，確保電腦系統與資料不被破壞或竊取。表5-2所列爲常見的怪客攻擊方式。

▼ 表5-2 常見的怪客攻擊手法

攻擊手法	說明
散布惡意程式	電腦怪客會撰寫並散布惡意程式(如特洛伊木馬程式)，藉此盜取他人機密資料以獲取不法利益。
入侵網站	電腦怪客透過網路入侵他人的網站或電腦系統，篡改或盜取其中的資料或紀錄，再將這些資料轉手販賣或用以從事不法行為。
網路釣魚	網路釣魚(Phishing)是指不法人士透過E-mail或網路廣告，假冒知名網站的超連結來進行誘騙，將不知情的使用者引誘到他們所製作的冒牌網站，也就是所謂的「釣魚網站(Phishing Site)」，然後藉著讓使用者在假冒的釣魚網站中輸入個人資料的同時，竊取帳號、密碼、信用卡號碼、身分證字號等個人機密資料。
殭屍網路	電腦怪客透過網路散播木馬程式，待集結大批受感染的電腦，形成殭屍網路(BotNet)之後，再遠端操控這些被控制的電腦，使其成為犯罪工具，進行惡意的攻擊行為，例如：癱瘓他人電腦、濫發垃圾郵件，或竊取他人機密資料等。
網站掛馬攻擊	電腦怪客會設立一個網站或部落格，以各種方式吸引民眾瀏覽，或是在一般正常網站中植入隱藏性的惡意程式，使用者若是瀏覽這些隱含惡意程式的網站，就有可能自動下載惡意程式到電腦中。
邏輯炸彈	邏輯炸彈(Logic Bombs)是特洛伊木馬的一種，它會因某特定事件而進行攻擊。例如：某程式設計師在某系統中植入了邏輯炸彈，若該程式設計師被公司資遣，便會啓動破壞行為。
鍵盤側錄程式	鍵盤側錄程式(Key-logger)是一種會記錄使用者所敲擊的鍵盤按鍵，主要用來竊取他人竊取網路帳號密碼或機密檔案。
阻斷服務攻擊	阻斷服務(Denial of Service, DoS)攻擊的主要目的是癱瘓系統主機或網站，使其無法正常運作。
分散式阻斷服務	分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊是DoS攻擊的方式之一，它是透過網路上的多部電腦主機同時發動DoS攻擊，以分散攻擊來源。
勒索軟體	勒索軟體(Ransomware)透過釣魚郵件入侵，將受害者電腦的檔案全數加密，導致檔案無法存取，受害人需要向他們付款才可復原，否則將毀損解密金鑰。最廣為人知的勒索軟體是CryptoLocker。

NOTE

當遇到網頁綁架軟體或是勒索軟體時，可以試試「RogueKiller」這套國外相當多人愛用的流氓軟體清除工具(http://www.adlice.com/software/roguekiller/)，主要功能是掃描電腦中的惡意程式、網頁綁架、彈出廣告、流氓軟體與各種討人厭的綁架程式。

攻擊手法	說明
間諜程式	間諜程式(Spyware)是在使用者不知情、且未經使用者同意的情況下，自行將軟體安裝在使用者電腦中，並觀察使用者的使用行為與監督電腦活動。有些間諜軟體則會取得使用者的帳號、密碼等資訊，進行不法勾當。
跨站腳本攻擊	跨站腳本攻擊(Cross-Site Scripting, XSS)是一種網頁漏洞攻擊方式，電腦怪客利用合法網站上的漏洞，在某些網頁中插入惡意的HTML與Script語言，藉此散布惡意程式，或是引發惡意攻擊。當不知情的使用者在觀看這些網頁的同時，便引發這些惡意網頁程式的執行，導致瀏覽器自動下載網頁中隱含的惡意程式。

5-1-5 資訊安全的防護

面對這麼多的資訊安全問題，就更應該做好資訊安全的防護動作，以避免電腦系統受到傷害，以下列出一些資訊安全的防護方法，供你參考。

❋ 實體安全的維護

實體安全指的是建築物與周遭環境的安全考量，這方面必須注意到人員的門禁管制、資訊線路的管制、消防設備及災害應變的計劃、定期的維護硬體以降低故障機率、備援與容錯系統的建置等。

- 加強人員及門禁管制：爲了防止人員的蓄意破壞，必須注意哪些人員可以進入公司的電腦系統中，並在電腦系統的周圍加裝監視器、保全系統等，以防止違法的入侵者。電腦進行維修時，應有相關人員在場監控，進入資訊部門時，應先辦理登記，以確保進出人員的合法性。
- 防範災害設施：電腦應設置於通風良好、乾燥之冷氣房中，勿直接曝曬陽光，機房應選用耐火、絕緣、散熱性良好的材料，並擺放防火滅火設備，嚴禁易燃易爆物品。電腦應加裝不斷電系統(Uninterruptible Power Supply, UPS)、穩壓器等設備，以防範天然災害的發生，而導致資料損毀。

❋ 資料安全的維護

- 建立電腦資料輸入輸出制度：各項資料在進行輸入輸出時，最好能設定密碼之管理制度，並時常更新密碼，以確保資料不致外流。對於重要性及機密性較高的資料，應加設資料存取控制，以防止資料外流。若資料輸入需要委外處理時，可以將資料分成數部分交給多人繕打，以提高安全性。

- 建立資料備份回復系統：預防資料被毀損最好的方法就是時常將電腦中的資料進行備份，而這些備份的資料，最好做到異地備份，儲存於不同媒體中或是別的地方。有了良好的備份習慣，以便災害發生後能夠將傷害降至最低。
- 建立電腦資料稽核制度：依據電腦的使用狀況，定期或不定期的稽核電腦資料及檔案管理情形。
- 制定使用權限：建立電腦設備及資料的使用者權限是非常重要的，電腦系統應設定每個使用者的權限。

NOTE

備份的類型有：

完整備份(Full Backup)：將所有的程式、檔案及資料全部進行備份。

差異備份(Differential Backup)：只針對上一次完整備份後有變更的檔案進行備份。

增量備份(Incremental Backup)：只針對上一次完整備份或增量備份後有變動的資料進行備份。組織可配合本身的資料更新頻率，搭配不同的資料備份類型來制訂備份策略。

❋ 帳號與密碼的使用

不管是上網或是收發電子郵件，都要輸入「帳號」和「密碼」，而這個帳號和密碼主要是保護我們的資料，以防止別人盜用，在設定帳號與密碼時，請注意以下幾點：

- 設定密碼時，最好不要使用個人的資料當作密碼，例如：英文名字、電話號碼、生日、身分證字號、1111、123456789等懶人密碼。
- 設定密碼時，密碼長度最好不要少於6個字元，密碼要夾雜使用字母及數字的方式設定，不要使用規則性的單字或連續的數字。
- 密碼不要儲存在電腦檔案中或是寫在某個地方。
- 定期更換密碼。

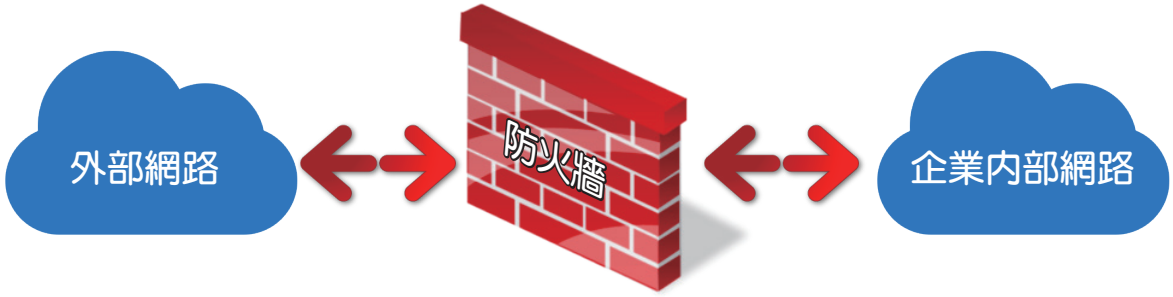
NOTE

根據刑法第358條，無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

❋ 防火牆

防火牆(Firewall)是網路安全的防護設備，可能是軟體也可能是硬體，它是內部網路和外部網路之間的橋樑，如圖5-3所示。防火牆可以管制資料封包的流向，並限制外界僅能存取指定的內部網路服務，藉此可以保護主機中的資料。

除了架設於企業網路與外部網路之間的防火牆設備外，一般個人電腦的使用者通常也會使用防火牆軟體來保護自己的電腦。例如：Windows作業系統中即內建防火牆軟體，網路上也有一些防火牆軟體供使用者下載。



▸圖5-3 防火牆是企業內部網路和外部網路之間的橋樑與屏障，它會分析網路中傳送的資料，並採取適當的防護措施，進而保護企業內部網路中的電腦，防止怪客入侵。

隨堂練習 5-1

( ) 1. 防治天然災害威脅資訊安全措施，何者不適宜？(A)設置不斷電設備 (B)設置空調設備 (C)設置防災監視中心 (D)經常清潔不用除濕。

( ) 2. 下列哪個選項不屬於電腦病毒的特性？(A)電腦關機後會自動消失 (B)可隱藏一段時間再發作 (C)具自我複製能力 (D)可附在正常檔案中。

( ) 3. 藉由寬頻網路大量且迅速蔓延，致使網路癱瘓的電腦病毒名稱為？(A)蠕蟲病毒 (B)巨集病毒 (C)特洛伊病毒 (D)千面人病毒。

( ) 4. 下列何類電腦病毒包含了開機型和檔案型病毒的特徵？(A)巨集型病毒 (B)混合型病毒 (C)千面人病毒 (D)特洛伊木馬。

( ) 5. 在電腦作業中，下列敘述哪一項非維護作業安全的主要工作？(A)維持電腦的正常作業 (B)維護設備的安全 (C)保護資料的安全 (D)軟硬體都應投保。

( ) 6. 仿製一個以假亂真的著名網站，吸引網友進來進行誘騙，這樣的行為屬於下列何種網路詐騙行為？ (A)字典式攻擊 (B)殭屍網路 (C)跨站腳本攻擊 (D)網路釣魚。

( ) 7. 使用密碼維護安全的最有效的方式是什麼？(A)經常更換密碼 (B)使用相同密碼登入個人電腦、網路及不同的網路帳號 (C)將所有密碼存在一份文件內，並設定另一組密碼保護文件 (D)用姓名、生日或紀念日等好記的字串作為密碼。

5-2 智慧財產權及相關法律責任介紹

當我們在使用電腦工作時，有些使用的規範是必須注意的，例如：尊重智慧財產權、不使用拷貝或未經合法授權使用的軟體、不可侵犯他人的智慧成果等，以下說明智慧財產權與軟體的授權。

5-2-1 智慧財產權與著作權法

智慧財產權(Intellectual Property Rights, IPR)是指人類精神活動的成果而產生的財產價值。爲了保護創作發明者的權益，而以法律創設的一種權利，著作權正是著作權法賦予著作人的權利。我國目前已完成立法的智慧財產權有：專利法、營業祕密法、積體電路布局保護法、商標法與著作權法。

❋ 認識著作權法

平常所使用的電腦軟體、歌曲、圖畫等，都是透過他人努力而創作出來的，這些創作稱爲「著作」，而著作權則是屬於創作出來的人所擁有。

著作權法主要是在保護該著作之表達，但並不包括其所表達之思想、程序、製程、系統、操作方法、概念、原理、發現等。例如：在腦海裡的概念或思想，因爲別人無法感受到它的存在，故未達到成爲著作的階段，所以概念和思想並不受著作權法的保護(資料來源：著作權法第10條之一)。

❋ 著作權的合理使用

著作權法雖保護著作人之權益，亦須兼顧社會大眾利用著作之權益，畢竟著作人之創作絕非憑空產生，而是傳承前人之智慧，同時受當代社會之教化影響，因此，不得絕對地壟斷創作之成果。於是著作權法在特定情形下對著作人之權益做限制與例外規定，允許社會大眾爲學術、教育、個人利用等非營利目的，得於適當範圍內逕行利用他人之著作，此即所謂「合理使用」(資料來源：經濟部智慧財產局http://www.tipo.gov.tw/copyright)。爲了避免侵犯著作人之著作權，在使用他人著作時，先檢視自己是否有合理使用權。

- 獲得同意權：使用他人著作時一定要先獲得對方同意，可使用授權書進行授權，授權書之內容最好包括：使用者、著作者基本資料、聯絡方式、使用目的、範圍等。
- 註明資料出處：使用他人著作時，應清楚註明出處、作者、書名、出版商等。
- 合理的引用量：著作權法並無明文規定合理的引用量，故在引用時，最好是在授權書中約定。
- 注意著作標示：在網路上你可能會常常看到「××公司 版權所有 © 2008-2013 All Rights Reserved.」的文字，這段文字指的是該公司對於該著作於上述期間享有著作財產權。

5-2-2 創用CC授權條款

目前的著作權法中，著作人對於其著作都是以「保留所有權利(All Rights Reserved)」爲主，任何「合理使用」之外的使用，都必須要事先取得著作權人的同意授權。所以，Creative Commons組織，提出了「保留部分權利(Some Rights Reserved)」的作法，Creative Commons以模組化的簡易條件，透過各種排列組合，提供六種不同的公共授權條款(表5-3)，創作者可以挑選出最合適的授權條款，透過標示，將自己的作品釋出給大眾使用，同時也保障自己的權益。

▼ 表5-3 Creative Commons Licenses 3.0台灣版各種要素組合與說明

姓名標示	姓名標示 - 禁止改作	姓名標示 - 非商業性 - 禁止改作
		
姓名標示 - 非商業性	姓名標示 - 非商業性 - 相同方式分享	姓名標示 - 相同方式分享
		

各圖示說明	
姓名標示	您必須按照作者或授權人所指定的方式，表彰其姓名(但不得以任何方式暗示其為您或您使用該著作的方式背書)。
禁止改作	您不得變更、變形或修改本著作。
非商業性	您不得為商業目的而使用本著作。
相同方式分享	若您改變、轉變或改作本著作，僅在採用與本著作相同、相似或相容的授權條款下，您始得散布由本著作而生的衍生著作。

資料來源：http://creativecommons.tw。

5-2-3 相關法律責任介紹

現行法律只要是涉及不法的行爲，即便是在網路虛擬世界中，仍屬法律規範的範圍。因此，無論是智慧財產權或是個人隱私權，在網路世界中也可以受到法律的保護。

❋ 侵害他人智慧財產權

網路上有許多豐富的資源，包括文字、圖片、影音檔案等，這些資源雖然垂手可得，但它們仍然具有著作權，若是未經所有權人同意，是不能任意引用或改製的，以免不小心觸法。

觸犯法律	罰責
著作權法第87條	有下列情形之一者，除本法另有規定外，視為侵害著作權或製版權： 一、以侵害著作人名譽之方法利用其著作者。 二、明知為侵害著作權或製版權之物而散布或意圖散布而陳列或持有或意圖營利而交付者。 三、輸入未經著作財產權人或製版權人授權重製之重製物或製版物者。 四、未經著作財產權人同意而輸入著作原件或其重製物者。 五、明知係侵害電腦程式著作財產權之重製物而仍作為直接營利之使用者。
著作權法第93條	有下列情形之一者，處二年以下有期徒刑，得併科新臺幣十萬元以下罰金： 一、侵害第十五條至第十七條規定之著作人格權者。 二、違反第七十條規定者。 三、以第八十七條各款方法之一侵害他人之著作權者。
著作權法第92條	擅自以公開口述、公開播送、公開上映、公開演出、公開傳輸、公開展示、改作、編輯、出租之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。

❋ 網路販賣盜版光碟

你可能常常收到販賣俗稱爲「泡麵」或「大補帖」的郵件，這類的郵件是某些人在販賣盜版光碟的廣告信。當收到此類的信件時，別因爲一時的心動而購買了，因爲這樣的行爲是觸犯著作權法的。

且依著作權法第91條第2項規定，意圖銷售而擅自以重製之方法侵害他人著作財產權者，處六月以上五年以下有期徒刑，併科新台幣三十萬元以下罰金。而單純銷售的話，依同法第93條第3款的規定，也要處二年以下有期徒刑，得併科新台幣十萬元以下罰金。

觸犯法律	罰責
著作權法第91條	擅自以重製之方法侵害他人之著作財產權者，處六月以上三年以下有期徒刑，得併科新臺幣二十萬元以下罰金。 意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處六月以上五年以下有期徒刑，得併科新臺幣三十萬元以下罰金。

隨堂練習 5-2

( ) 1. 下列何者非智慧財產權？(A)商標權 (B)專利權 (C)著作權 (D)土地所有權。

( ) 2. 在保護智慧財產權的各項法律中，下列何者其取得保護的方法可不須經過審查核准或註冊即產生效力？(A)專利法 (B)著作權法 (C)商標法 (D)積體電路佈局保護法。

( ) 3. 任意盜拷某公司出版的軟體並燒錄成光碟出售，此行為侵犯下列何種智慧財產權，依法可提起告訴？(A)著作權 (B)商標 (C)專利 (D)營業祕密。

( ) 4. 地下光碟複製工廠，拷貝光碟的行為，係違反下列何者有關智慧財產權的法律？(A)專利法 (B)商標法 (C)營業盜賣法 (D)著作權法。

( ) 5. 下列何種行為不會違反著作權法？(A)將市售CD借給同學拷貝使用 (B)將網路下載的圖片放在社團的網頁上 (C)在個人網頁上寫作介紹他人的文章 (D)傳送共享軟體給朋友。

5-3 網路素養與網路倫理

網際網路興起，改變了人們之間的溝通方式，它雖帶給人們在生活上的便利，但也產生了許多衝擊。爲了讓自己不成爲高科技野蠻人，網路素養及網路禮節是我們需要學習的地方。

所謂的網路素養是指，具備了解網路資源、應用網路資源、檢索、處理、利用和評估網路資源的能力。

但隨著網路科技的迅速發展，網路素養的意涵也不斷地改變。而過去的網路素養，尚須加入網路禮節的概念，包括了：使用者是否明瞭在網路上該怎麼說話、該怎麼自律、怎樣才不會觸犯法條規範等。所以這節要說明在使用網路資源時，該注意哪些禮節。

5-3-1 網路禮節

網路禮節(Netiquette)是指網路世界中的禮儀規範，主要是在使用的過程中，使用者彼此間的互動禮儀。良好的網路禮節表示尊重對方，展現自己使用網路的負責態度，以及避免帶給對方使用網路的不便及無意間產生的誤解。

良好的網路禮節是尊重對方的表現，也是展現自己負責任的態度。

而網路上應有的禮儀原則，與現實生活中無異，除了尊重別人之外，也要對自己所寫的東西負責。網路世界容易流爲不負責任的發言場所，及情緒性的攻擊與謾罵，甚至容易觸犯誹謗或公然侮辱等罪，因此在網路上我們應對自己所寫的文字負責，不要讓網路只停留在情緒性的發洩上，或造成他人閱讀的困擾。

- 使用留言版、討論區、聊天室時應事先瞭解站規或版規，了解該網站的主題與性質，並閱讀「常見問題集」、「精華區」等前人發表過的文章，以免重覆提問或發出不適當的言論。
- 傳送廣告信、連鎖信、幸運信或是來路不明的「病毒警告信」，不但容易散播病毒，也是濫用網路資源的不當行為。
- 在聊天室或留言版中留言時，應注意留言內容是否符合主題。
- 在網路上應避免公開個人隱私與基本資料，也不要將私人訊息發表在部落格或留言版上。
- 不要假借他人名義散佈訊息、留言或傳送電子郵件，以免觸法。
- 網路聊天室是公開的平台，討論的主題應符合大家共同參與的原則，不應在聊天室中處理私人事務。
- 信件往返應尊重他人隱私權，未經當事人同意，勿公開私人往來的電子郵件。

5-3-2 資訊隱私權與個資法

資訊隱私權指的是個人的姓名、身分證字號、病歷、財務、職業、婚姻狀況、指紋、特徵等資料，或者是在網路上所交談的對話、匿名所發表的文章等，都屬於資訊隱私權。因網際網路的發展，人與人之間所傳遞的資訊也隨著增加，而在傳送的過程中，個人的資訊隱私也可能正被別人侵犯。

因此，2012年4月經立法院三讀通過的新版個人資料保護法(簡稱個資法)，於2012年10月1日正式施行，以保護個人的資訊隱私權(關於個資法可參考全國法規資料庫網站http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021)。

在瀏覽或使用網站時，不要輕易洩露個人的資料，不要進入一些不知名的網站，才能避免隱私權外洩。現在也有很多網站爲了尊重及保護個人的資訊隱私權，都會在網站中宣告該網站對個人資訊隱私權的使用原則，或者是保護與政策。

個資法適用對象包括了自然人(也就是一般人)、法人(企業)或其他任何3人以上的團體，對企業而言，洩露消費者的個資，賠償金額最高可以達到2億元，最重可處五年有期徒刑。

而一般民眾從網路等管道蒐尋資料(例如：人肉找出虐貓者等基於公益的「人肉搜索」)，並無觸法之虞；在個人部落格或臉書等網站上，可張貼一般日常生活或公共活動的合照及影音資料，只要內容不結合其他個人資料就不會觸法。但若違法蒐集、處理、利用或變造個資，造成他人損害，或者意圖營利，都可處以刑責及罰金。

隨堂練習 5-3

(　　) 1. 要將信件轉寄給一群互相不認識的人，應該要以下列何種方式為佳？(A)使用「寄件人」 (B)使用「副本」 (C)使用「密件副本」 (D)使用「全部回覆」。

(　　) 2. 下列作法何者不適當？(A)先將沒有用的資訊刪除，再進行轉寄信件的動作 (B)我的好友在網路上被罵了，我應該幫他罵回去 (C)進入討論區時，先看看站規或版規 (D)在網路世界中應避免公開個人隱私。

5-4 正視網路危險

網路的蓬勃發展及上網族群年輕化的趨勢下，衍生出了網路色情、網路毀謗、網路沉迷等社會問題與犯罪事件，而我們該如何預防及安全地使用網路呢？這節就來說明。

5-4-1 常見的網路犯罪

網路犯罪(Internet Crime)導致了許多問題，更造成了社會不安，以下介紹一些常見的網路犯罪模式。

❋ 網路色情

常見的網路色情犯罪事件，是利用網路散播色情圖片，例如：架設色情網站，並提供各種色情圖片、影片、利用電子郵件夾帶色情圖檔、利用網路相簿存放色情圖片等。

觸犯法律	罰責
刑法第234條 (公然猥褻罪)	意圖供人觀覽，公然為猥褻之行為者，處一年以下有期徒刑、拘役或三千元以下罰金。 意圖營利犯前項之罪者，處二年以下有期徒刑、拘役或科或併科一萬元以下罰金。
刑法第235條 (散布、販賣猥褻物品及製造持有罪)	散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處二年以下有期徒刑、拘役或科或併科三萬元以下罰金。 意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。
兒童及少年性交易防制條例 第27條	拍攝、製造未滿十八歲之人為性交或猥褻行為之圖畫、錄影帶、影片、光碟、電子訊號或其他物品者，處六個月以上五年以下有期徒刑，得併科新臺幣五十萬元以下罰金。 意圖營利犯前項之罪者，處一年以上七年以下有期徒刑，應併科新臺幣五百萬元以下罰金。
兒童及少年性交易防制條例 第28條	散布、播送或販賣前條拍攝、製造之圖片、影片、影帶、光碟、電磁紀錄或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處三年以下有期徒刑，得併科新臺幣五百萬元以下罰金。 意圖散布、播送、販賣而持有前項物品者，處二年以下有期徒刑，得併科新臺幣二百萬元以下罰金。

❋ 網路援交

網路援交是指透過網路散播訊息，以尋求提供性服務來換取金錢的援助交際行爲，透過網路這個溝通媒介，讓有意援交的兩方人馬可以約見時間與地點以進行交易，而這樣的行爲其實已經觸犯兒童及少年性交易防制法。按照該條文之規定，只要有散布、播送或刊登足以引誘、媒介、暗示或其他促使人爲性交易之訊息，無須以「實際發生性交易」爲必要，仍然構成犯罪，且交易雙方均依該條例處罰。

觸犯法律	罰責
兒童及少年性交易防制條例第29條	以廣告物、出版品、廣播、電視、電子訊號、電腦網路或其他媒體，散布、播送或刊登足以引誘、媒介、暗示或其他促使人為性交易之訊息者，處五年以下有期徒刑，得併科新台幣一百萬元以下罰金。

❋ 網路詐欺

網路詐欺是網路上最常見的犯罪行爲，像是有些人會在網路上拍賣一些低價的物品，吸引消費者購買，而當消費者依指示將錢匯入對方帳戶後，卻沒有收到購買的商品，而此行爲可能涉及刑法第339條詐欺罪。

觸犯法律	罰責
刑法第339條(普通詐欺罪)	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。 以前項方法得財產上不法之利益或使第三人得之者，亦同。
刑法第339-3條(違法製作財產權之處罰)	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。 以前項方法得財產上不法之利益或使第三人得之者，亦同。

❋ 網路賭博

在網路上架設網頁，並提供賭博網站之功能，供群眾上網賭博財物者，就會觸犯刑法第268條的賭博罪。

觸犯法律	罰責
刑法第268條(圖利供給賭場或聚眾賭博罪)	意圖營利，供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得併科三千元以下罰金。

❋ 網路不當言論

在網路上以公開或匿名方式發表不實報導、網路恐嚇、公然毀謗或辱罵他人、侵犯他人權益、妨害他人名譽等，都可能觸犯刑法的公然侮辱罪、誹謗罪，或是恐嚇罪等。

觸犯法律	罰責
刑法第309條 (公然侮辱罪)	公然侮辱人者，處拘役或三百元以下罰金。 以強暴犯前項之罪者，處一年以下有期徒刑、拘役或五百元以下罰金。
刑法第310條 (誹謗罪)	意圖散布於衆，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。 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。
刑法第305條 (恐嚇危害安全罪)	以加害生命、身體、自由、名譽、財產之事，恐嚇他人致生危害於安全者，處二年以下有期徒刑、拘役或三百元以下罰金。
刑法第346條 (恐嚇取財得利罪)	意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付者，處六月以上五年以下有期徒刑，得併科一千元以下罰金。 以前項方法得財產上不法之利益，或使第三人得之者，亦同。

5-4-2 網路霸凌

網路霸凌(Cyberbullying)是指透過電子郵件、部落格、討論區、聊天室、即時通訊、社交網站等媒介，進行辱罵、威脅、散播謠言或刊登不雅照片等惡意行爲，使受暴者遭受欺凌、歧視或恥笑等網路暴力行爲。

由於青少年的團體性及模仿能力強，加上網路的便利性和匿名性，都是網路霸凌行爲不斷增加的原因，更因爲網路的散布速度很快，其造成的傷害可能更甚於一般霸凌行爲。因此，在網路公開空間張貼訊息前，皆須謹慎思考是否觸法或可能傷害他人。

❋ 遇到網路霸凌怎麼辦？

- 要勇於求助：一旦遇到這類行爲，不論是否提出告訴，都應該先保存證據，被霸凌者可以將這些資訊存證、投訴網站管理人刪除或是告訴有權處理的人(如學校老師、家長或警察)，千萬不要因爲害怕而忍耐退讓。(教育部「去霸凌，高關懷」專線0800-200-885)

- 要即時處理，以制止傷害擴大：不論是自己或他人遭受網路霸凌，一定要告訴家長、老師或警察被霸凌的情況，保護自己也幫助他人。
- 要終止流傳：在網路上面看到不當的言論，要立即向網站站長檢舉，甚至發現有人將暴力行為的圖片或影片貼上網，都可以報警處理，別讓這些霸凌行為繼續在網路上流傳，造成當事人更嚴重的傷害，也別讓自己加入傳播行列成為加害者。

5-4-3 網路沉迷

若發現自己在使用網路時，沒辦法控制使用時間，一上網便無法停止，且若是想要上網，卻沒辦法上網時，就會變得焦躁不安、易怒、沮喪等情形發生時，那麼你可能得了網路沉迷或成癮症(Internet Abuse or Addiction Disorder)了。

❋ 網路沉迷的原因

尋求自我認同、人際關係的渴求、體驗新生活型態、好奇心的推動、同儕的壓力、偶像的崛起等。

❋ 網路沉迷的影響

生理上：近視加深、眼乾、眼酸、肩膀酸痛、睡眠不足、飲食不正常等。

心理上：會變得憂鬱、注意力缺損、無成就感等，嚴重者甚至還會導致社交退縮、自我封閉等人格問題出現。

行為上：影響功課、延誤上學時間、人際關係疏離、生活作息不正常、語文能力退化等問題。

❋ 網路沉迷的預防

加強自己的人際關係與溝通技巧，多接觸人群，不要躲避於網路世界之中，多參與家庭活動並培養正當的休閒娛樂。

若徵兆嚴重時，可以至身心科門診醫療中心就醫，例如：台大醫院之兒童心理門診中心、台北馬偕紀念醫院之兒童及青少年門診中心、榮總醫院之兒童青少年心理中心等，都有這方面的專業醫療服務。

5-4-4 網路安全防護

網路上的危機重重，爲了能夠安全上網，並減少發生問題的可能性，必須要先認識網路上的各項風險及保護自己的方法，才能無虞享受上網樂趣。

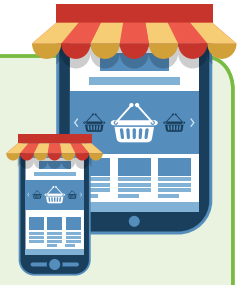
網路交友安全守則

- 進行網路交友時，最好不要將重要資料公布，像是：身分證字號、住家地址等。
- 不要將信用卡或銀行帳號登錄在網路上或告訴對方。
- 在交談時不要有任何粗俗、不雅、挑逗性的言語。
- 避免單獨與網友見面，如果要相約見面最好要請朋友或親人一同前往。見面時應選擇人多、交通便利且自己熟悉的公共場所。
- 盡量不要搭乘網友的交通工具，以免不能自主而任由網友擺布。
- 不要與網友有金錢上的往來。
- 不要假冒他人的名義或身分，交友時最好以真實的自己進行。

線上遊戲安全守則

- 進行虛擬寶物交易時，最好可以記下與玩家的交易過程，玩家的個人資料，記得將所有線上對話保留並完整記錄。
- 妥善保管個人的帳號及密碼，不要洩漏自己的帳號與密碼，更不要貪圖小利。
- 隨時留意最新資訊，了解各種犯罪行為，保持警覺。

網路購物安全守則



- 個人隱私權：詳讀公布在網站上的隱私權保護政策，以了解需提供甚麼樣的個人資料，這些資料將如何被使用及其使用目的。
- 網上刷卡的注意事項：於網上提供信用卡號碼前，先確定該網站是否有使用安全機制，例如：SET或是SSL。
- 尋找信譽良好的網路商家：確定面對的是一家具有良好聲譽的公司，具可用來辨別的標誌，以代表這家公司符合SOSA(Secure Online Shopping Association)國際高評鑑標準的「優良電子商店」標章。
- 注意售後服務及退貨政策：在訂購之前，需先了解這家公司是否接受退貨及其相關辦法。
- 查詢可靠商家：在進行購物前，可以至經濟部「網路商業應用資源中心」查詢可靠的網路商店，網址為：http://gcis.nat.gov.tw/ec/。

延伸閱讀 SET、SSL

»安全電子交易標準(Secure Electronic Transaction, SET)：為了達到交易安全，VISA、MasterCard、IBM、HP、Microsoft等公司，於1996年2月共同制定了安全電子交易標準，它是一種應用於網際網路上，以信用卡付款的電子付款系統規範，SET主要是希望能確保網路上信用卡交易的安全性。有了安全電子交易標準，不但在網路上傳遞的資料不易被竊取，也保障了交易的安全。而SET已成為國際上所公認在Internet電子商業交易的安全標準。

»安全通道層(Secure Sockets Layer, SSL)：SSL是由Netscape Communications Corporation和RSA Data Security, Inc. 開發的一個標準，大部分的瀏覽器和伺服器都有支援。而有採用SSL安全機制的網站，該網站的位址都是以「https」為開頭，而且在狀態列的左邊，會有一個已鎖上的小鎖圖案，此圖案即表示SSL保密機制已經啓動，若這個小鎖圖案是打開的狀態，那麼表示該網站未啓動SSL保密機制。若在網站中有看到如圖5-4的圖示，那就表示這個網站使用了SSL安全機制。

▸圖5-4 HiTRUST提供的交易資料保護標記。

延伸閱讀 3-D Secure

3-D Secure驗證模式係由VISA、MasterCard 及JCB國際組織推出，為改良SET安全標準而生，將資料的傳遞由四方減少為發卡銀行區域(Issuer Domain)、收單銀行區域(Acquirer Domain)和跨作業系統區域(Interoperability Domain)三方，因此稱為3-D Secure。若消費者的信用卡發卡銀行加入3-D Secure驗證，在網路上進行刷卡消費時，系統會自動跳出驗證視窗，消費者須輸入認證密碼才能進行刷付。此模式的程序不致太麻煩，而減少資料傳遞的流程，也能更降低電子交易資料外洩的安全疑慮。

隨堂練習 5-4

( ) 1. 網路電子交易日漸擴大與頻繁，網路交易的安全性更為重要，下列何者是對於安全交易的要求？(A)隨時可推翻交易，保護消費者 (B)公開交易者真實身分，以昭公信 (C)認證要求 (D)交易後，不可要求退貨。

( ) 2. 在網路交友的安全守則中，下列何者不正確？(A)不與網友有金錢上的往來 (B)進行網路交友時為了表示誠意，可以將身分證字號給對方 (C)避免單獨與網友見面 (D)在交談時不該有任何粗俗、不雅、挑逗性的言語。

( ) 3. 下列各項網路行為與習慣，何者正確？(A)在電子郵件中收到中獎通知，趕快回信填寫帳戶資料好領取獎金 (B)因為好奇在討論區中留下暗示援交的訊息，看看會不會有人回應 (C)收到幸運信直接刪除，不再轉寄給他人 (D)反正不會有人知道我是誰，就在死對頭的部落格上留言罵他。

( ) 4. 進行網路購物時，須注意？(A)詳讀公布在網站上的隱私權保護政策 (B)尋找信譽良好的網路商家 (C)確認該網站是否有使用安全機制 (D)以上皆是。

自我評量

選擇題

( ) 1. 當企業內網路與外界相連時，用來防止駭客入侵的設施為？(A)防火牆 (B)防毒軟體 (C)瀏覽器 (D)網路卡。

( ) 2. 電腦病毒係指？(A)一種破壞性軟體 (B)硬體感染病菌 (C)病菌潛入主機 (D)磁片污垢。

( ) 3. 下列何種型態的檔案，最容易感染到檔案型病毒？(A) .DOC (B) .ASM (C) .EXE (D).TXT。

( ) 4. 為防止駭客入侵企業內部網路竊取資料，下列何項是常用的預防措施？(A)禁止員工上網並定期更換使用者密碼 (B)在每部個人電腦加裝合法的掃毒軟體並定期更新版本 (C)每日將資料進行備份並儲存於可抽取式硬碟中 (D)在企業內部網路與外部網路間建構防火牆。

( ) 5. 下列哪個選項不屬於電腦病毒的特性？(A)電腦關機後會自動消失 (B)可隱藏一段時間再發作 (C)具自我複製能力 (D)可附在正常檔案中。

( ) 6. 下列有關電腦病毒的敘述何者不正確？(A)電腦病毒具有傳染的特性 (B)電腦病毒可以利用關閉電源來解毒 (C)預防電腦病毒可以使用防毒軟體 (D)檔案型電腦病毒主要寄生在可執行檔中。

( ) 7. 下列哪一類型病毒會感染文件中的巨集指令，凡是具有巨集功能的軟體均有可能被感染？(A)蠕蟲病毒 (B)巨集病毒 (C)特洛伊病毒 (D)千面人病毒。

( ) 8. 下列何者不違法？(A)以匿名的方式在網路上罵人 (B)利用別人的信用卡卡號在網路上購物 (C)攔截女朋友的電子郵件看看她有沒有移情別戀 (D)寫一個駭客程式試試看自己的電腦安全防護有無做好。

( ) 9. 電腦程式在下列哪一種法律條款中被列舉為保護對象之一？(A)民事訴訟法 (B)著作權法 (C)商標法 (D)電腦處理個人資料保護法。

( ) 10. 關於創用CC授權條款標示，下列何者正確？(A) 表示必須按照作者或授權人所指定的方式，表彰其姓名 (B) 表示允許他人對你的著作原封不動地進行重製、散布、展示及演出等利用行為，但不得產出衍生著作 (C) 表示允許他人對你的著作及衍生著作進行重製、散布、展示及演出等利用行為，但僅限於非商業性的目的 (D)以上皆是。

問答題

1. 看看以下行為犯了哪些刑責？

行為	刑責
若是在網路上竊取別人的寶物，那犯了什麼罪，處罰的刑責為何？	
在網路上寄E-mail給大家，或是留言在別人Blog，或在BBS上亂罵、毀謗別人，犯了什麼罪，處罰的刑責為何？	
販賣大補帖、MP3、影片，犯了什麼罪，處罰的刑責為何？	
在網站上販賣色情光碟、或是在公衆可進入的論壇散播色情影片、相關內容，犯了什麼罪，處罰的刑責為何？	
大金在色情網站上下載了許多色情圖片，並在自己的網路相簿中存放這些色情照片與朋友分享，試問他犯了什麼罪，處罰刑責為何？	
小翊在YouTube上看到周杰倫最近的MV，覺得超好聽的，便將該MV的連結轉貼到自己的部落格中跟大家分享。試問他犯了什麼罪，處罰的刑責為何？	
小美基於惡作劇的心態，在未告知同學的情況下，盜用同學的帳號與密碼，透過學校的選課系統上網退選同學所選的課。試問她犯了什麼罪，處罰的刑責為何？	

2. 動動腦，下列的行為觸犯了哪些權利。

常見行為	相關權利
影印書刊著作	
公布他人書信	
將各類著作電子化	
將各類著作置於網路上，供瀏覽者下載、傳閱、轉寄等	