編者序

社會高度資訊化下，資訊網路科技的應用正在改變我們商業、工業乃至於生活的模式。根據經濟部委託資策會進行的「我國網際網路用戶數調查統計」，截至2001年12月底為止，我國網際網路使用人口已高達782萬人，網路儼然成為人們密不可分的夥伴。

悠遊於網際網路，人們可以瀏覽國際、政治、財經、科技、學術等各類資訊，滿足知識與實用上的需求。但除聯絡溝通的功用外，目前網際網路更已成為國家許多基礎建設的載具。從水電的供輸、稅賦的報繳、到交通運輸的帷幄等，皆已不復全賴人工處理，轉而藉由網路快速、便捷的特性，發揮更好的管理效能。

然而，科技技

資通安全法律
案例宣導彙編

術不斷發展、引領資訊通信普及的同時，網路亦對社會帶來負面的衝擊，如電腦病毒的散布、駭客入侵的威脅、與其他利用電腦來侵害他人財產法益之犯罪行為等。一般大眾乃至軍公教從業人員，常因法律知識不夠完整而誤觸法網。此等情況一旦發生，不獨耗損你我辛勤積累的社會成本，更可能傷害了我們於國際社會中努力經營之地位形

資通安全法律
案例宣導彙編

象。更有甚者，隨著政府各部會的全面電子化，未來的國防安全，全繫之於我國對「資訊戰」應變的良窳。若敵人趁資通安全的罅隙，癱瘓我國水電、通信、交通等重大基礎建設的運作，對國家社會的危害，將難以估計。是以，如何在虛擬與實體環境間找到良好的介面，藉以養成國民正確的資通安全觀念，實屬當務之急。

目

前，行政院國家資訊通訊發展推動小組(NICI小組)為配合六年國家經濟建設計畫，加速推動我國資通安全產業發展，實現e-Taiwan願景，正推動「國家資訊通信基礎建設方案」，以e政府、e產業、e社會及e建設四大架構為主軸，期能開創我國擁抱寬頻時代的新契機。與此同時，也積極規劃「建立我國資通訊基礎

資通安全法律
案例宣導彙編

建設安全機制計畫」，責成政府各單位於建立完善的資通安全防護機制，從而為我國資訊通信安全提供最佳保障。而資通安全法制基礎建設，即為本計畫不可或缺之一環。計畫除預定逐次檢討及增修資通訊安全相關法令外，更重視資通安全人力培訓及觀念宣導、增強執法人員專業能力，以達有效遏止網路犯罪，同時促進網路多元發展之雙

效目標。

除上述政策作為外，我們更體認到，建立國民正確資通安全技術與法律觀念，才是維護國家資通安全的基石。因此，行政院「國家資通安全會報」在今年「萬安演習」中，特地將資通安全納入演習項目。希望藉此考驗政府部門平時防護的成果與應變能力，並訓練民眾因應資訊戰的應變能力。配合此次萬安演

資通安全法律
案例宣導彙編

習，國家資通安全會報技術服務中心出版本彙編，藉由淺顯易懂的文字敘述、深入淺出的案例介紹，相信將能輕鬆建立國民正確的資通安全法制觀念。

行

政院國家資通安全會報

技術服務中心

謹誌

資通安全法律
案例宣導彙編

前言

為積極落實網路安全教育的推廣，協助各界從身邊發生過的案例中汲取經驗，本手冊因此彙整相關新聞案例，根據資通安全事件發生的成因進行分類與分析，期望建立網路使用者正確的資通安全風險意識。

網路環境的威脅來源，主要有四種：來自天然災害（如水、火）的威脅、具有自動散布性電腦病毒的威脅、電腦駭客入侵的威脅、與利用電腦進行犯罪的威脅。本手冊的第一章即介紹「天然災害的威脅」。藉由事例的描述，希望建立讀者平時即應建立「妥善選擇資料存放地點」與「資料備分」的風險概念。

第二章則是「電腦病毒的威脅」。各類病毒的蔓延，所造成的危害，常常是

資通安全法律
案例宣導彙編

難以評估的；從延宕一般使用者的工作效率，到造成企業商譽損失、阻斷政府公務正常運作，病毒的肆虐是「一視同仁」、不分彼此的。因此，完善的通資訊安全防護機制是建立在全民對網路安全的風險意識之上。

第三章為「電腦駭客的威脅」。駭客的入侵事件，除了更改網頁等表面上常見的毀損

資通安全法律
案例宣導彙編

行為外，入侵行為常是駭客進行其他犯罪前的預備行為，如為竊取他人財務資料的目的而移植木馬程式。由於這類程式在未實際運作前難以被察覺，因此造成通資訊安全防護的隱憂甚鉅。讀者不可不知。

第四章「電腦犯罪的威脅」，則羅列目前社會上常發生的電腦犯罪類型，如侵害智慧財產權、危害社

會秩序案件、與妨礙交易秩序等案例。對電腦犯罪事件造成的危害作一完整性的介紹。

一、 天然災害的威脅

台灣地理型態特殊，地震颱風頻仍，兼之以人謀不臧所造成的損害，動輒釀成極大的災情。人為傷害或可藉由改善組織管理、事先妥善預防、建立綿密監控等方式，戕傷害程度降至最低；天然災害因多屬地域性、大規模性地侵襲，除組織本體的本身的努力外，更需要政府以上層級的規劃預防及救助。

正因為天然災害對企業及任何組織資通安全性的威脅，不在其它侵害類型（如電腦病毒等）之下，對此類案例的回顧與檢討，誠有其必要。並希望藉此加強大眾對防災及安檢的觀念，以期建立更為妥適的臨災處理模式。

日期：2001/05/14

事件：東科大火

事件描述：

汐止東方科學園區大火，延燒三、四十個小時，二百多家廠商受波及。台灣最大的網路代管服務(IDC)公司在無預警狀況下暫停一百三十家客戶的網站服務。

法律意見：

此種大規模的祝融之災，動輒造成數百家廠商軟、硬體付之一炬，其對於資通安全的威脅並不亞於其他類型。硬體部分尚有保險理賠，但軟體資料一經毀損，若無事先備份，企業因此而損失的商譽及信用往往更甚於硬體的損害。根據美國明尼蘇達大學的一份研究報告指出，企業在沒有資料可用的情況下，金融業至多只能運作兩天，商業則約 3.3 天。有 25%的企業，更可能因資料的損毀而立即破產。正因天災嚴重時可造成無可補救的經濟上損害，思考如何維護政府或企業重要資料的安全、在平時即建立危機意識，實屬刻不容緩。

東科事件中，釀成火災之人，則觸犯刑法第 173-176 條之公共危險罪，最高可處七年有期徒刑。

網路代管公司雖無預警暫停一百多家客戶的網站服務，卻已表示願意賠償。但協助代管客戶投保產險實為治本之道。

在同年九月間納莉風災重創北台灣，造成北台灣多處大淹水，因大量主機皆遭泡水命運，使資訊系統更受到前所未有的傷害。接踵而來的慘痛經驗，更應使我們心生怵惕，了解建立完整事前防範（存放資料地點選擇、資料備份等）的重要性。

二、 電腦病毒的威脅

電腦病毒的威脅由來已久，但隨著網路技術的發展，電腦病毒的傳播媒介由最初的磁碟片，轉而變為藉由網際網路，甚至新興的無線通訊技術，使其蔓延的速度及範圍無數倍於以往。

根據統計，截至 2001 年 9 月，我國網際網路用戶數已達 755 萬人，連線主機數約達 134 萬部，名列全球第 8、亞洲第 2。面對如此龐大的網路流量及使用人數，若在相關軟硬體及資訊教育上未能齊頭並進，將會使電腦病毒的危害及影響更加迅速及深遠。

台灣有優異的資訊工業及資訊工程教育，也培養出大量的軟體人才。如何建立相關法制措施及充分觀念宣導，使有天份的程式設計者不致因懵懂無知而誤蹈法網，成為散播電腦病毒的災害製造者，實為我們未來必須仔細規劃的要項。

1. 對政府及學校的威脅

日期：2001/07/23

事件：思坎病毒蔓延

事件描述：

思坎病毒蔓延，藉由電子郵件進行散播，一旦電腦遭病毒感染後，病毒會尋找通訊錄中的名單，自動發送病毒郵件。該電腦病毒侵襲許多公家機關網站，使網管人員飽受電子郵件病毒侵害之苦。

法律意見：

根據一項由美國聯邦調查局（FBI）和電腦安全協會（CSI）於 2002 年 4 月 7 日所發表的研究指出，電腦病毒是駭客入侵最常用的手法。而根據 500 名研究受訪者所提供的資料，其因電腦病毒或蠕蟲入侵所損失金額約 4,990 萬美元。

由上開研究報告可知，電腦病毒早已不復只是駭客炫耀電腦功力的手法而已，每一隻病毒的發作，其背後可能表彰的是社會上經濟秩序的鉅大損害。若遭感染的對象為政府機關網路，更會造成公務的延宕及

公帑的無謂損失。縱然因政府的全面 e 化，公務員業務上大量使用網路係勢所難免，但你我應在平時即建立好充份的資訊安全意識，並對電腦病毒的感染途徑有一定認識及預防，以期減低電腦病毒對機關內電腦的衝擊。

一般而言，電腦病毒最主要的散播途徑，是透過開啟或執行電子郵件的附加檔案（尤其是附檔名為 EXE、COM、SCR 的檔案）而感染收件者的電腦。但有些最新變種病毒，如「求職信病毒」，使用者只要「預覽」病毒信件，不需執行任何附加檔案，就已經受病毒感染。一些良好使用習慣的養成（諸如不任意開啟來源不明郵件、開啟附檔前一定先掃毒、定期更新病毒碼、outlook 使用者關閉郵件預覽功能等），甚至架設個人或機關內的防火牆，皆有助於扼止電腦病毒的不法肆虐。

根據86年10 月8日增訂刑法第352條第2項之立法理由，若有「干擾他人電磁紀錄之處理，足以影響電腦正常之運作，例如：以『電腦病毒』方式，即利用程式透過電腦連線系統內進行複製，佔據記憶容量，干擾電腦之正常運作功能」，且「如其情形足以生損害於公眾或他人時，宜以刑罰加以規範」。

依刑法第352 條條文：「毀棄、損壞他人文書或致令不堪用，足以生損害於公眾或他人者，處3 年以下

有期徒刑、拘役或1 萬元以下罰金。干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，亦同」。病毒的故意散播者，實已觸犯了刑法第352 條第2項干擾他人電磁紀錄處理之罪。

日期：2001/08/06

事件：新聞病毒橫掃某市府

事件描述：

以「新聞資料」、「公文會辦單」名義散發的電腦病毒，肆虐某市府各機關，許多局科室的電腦都中毒，一開機就傳入數百封的英文信件，塞爆主機造成癱瘓，各單位因而進行緊急掃毒。

法律意見：

行為人透過網路以電腦病毒造成他人電腦硬碟損毀、致令不堪使用，即構成刑法第354 條之普通毀損罪。此外，就上述事實來看，電腦病毒的發作不但干擾了高雄市府各機關公務上電腦資料的處理，更因公務的延宕導致廣大市民的損害。

相關判決：90年度上易字1265號。

日期：2001/08/11

事件：紅色警戒病毒肆虐

事件描述：

縣府教育局與國高中小學間聯絡的資訊網絡「縣教育網」，遭到紅色警戒病毒入侵，主機中毒，網路癱瘓，受害學校無數。

法律意見：

紅色警戒（Code Red）病毒屬於一種結合電腦病毒與駭客程式的攻擊手法。其令人蹙額處，在於它能夠以一程式整合病毒、駭客、DDoS 等數種攻擊手法，使電腦一經感染，即導致多重損害。

根據防毒軟體業者趨勢科技的分析，在國外紅色警戒爆發之初，微軟即就其網路伺服器的作業程式緊急發布防範的修正檔，但僅有少數企業立刻將之更新於伺服器上，致使災情仍不斷擴大。因此可觀察到，企業光使用高階路由器、設置防火牆其實只是治標，對網站管理員資訊安全防護觀念的再強化（如例行性的更新病毒檔、系統定期修正等習慣的建立），才能做到防範於未然。

此外，若有電腦駭客利用植入紅色警戒病毒，在

網路上實施 DDoS 的行為，今後可要特別注意了。據指出，法務部草擬中的「刑法部分條文修正及增訂電腦犯罪章條文草案」，考慮以 5 年以下有期徒刑的重刑伺候駭客這種網路侵入的前段行為。法務部官員指出，在電腦網路犯罪的入侵行為中，DDoS 是屬於侵入的前段行為，以刑法的傳統說法，屬於預備犯行為，應加以處罰。

何謂 DDoS 呢？DDoS 其實是 Distributed Denial of Service 的縮寫，有人將之譯為分散式阻斷服務攻擊，是一種特殊形式的拒絕服務網路技術。這種技術是利用多台已經被駭客所控制的主機對某一台單機發動攻擊，以該單一主機能夠容納的封包，一次迴傳到該單機，在頻寬相對的情況之下，被攻擊的主機的寬頻很容易被消耗光而失去反應能力。

法務部在 91 年 4 月所提出的最新刑法修正草案中表示，網際網路的使用，應該准予更寬廣的自由度，但提供內容的網站與網路服務業者，與使用者一樣有權利受到保護，網路安全與順暢的自由也同樣要受合法維護，所以才會決定對 DDoS 的行為科以 5 年以下有期徒刑的重刑。

事實上，對電腦病毒及電腦駭客的規制，世界各地皆在如火如荼的展開中。舉例來說，中國大陸即於 91 年 3 月 1 日，由一家名叫瑪賽的公司聯合大陸上海

熱線、上海市公安局網監處，破獲一個長期以來針對大陸著名 ISP／ICP 進行 DDoS 的周姓駭客。這正說明了 DDoS 已是各國防制駭客行為中,必然約束的一種網路侵入前的不法行為。是以，手癢難耐、準備散播病毒的眾家駭客們，無論你下手的對象是國內網站抑或國外網站,可得三思而行。若是僅為滿足一時的虛榮，卻賠上寶貴的光陰和大好的前程，多令人惋惜！

2. 對企業及個人的威脅

日期：2001/10/31

事件：娜妲病毒入侵證交所電腦

事件描述：

娜妲（Nimda）變種電腦病毒自 2001 年 9 月初萌後，透過電子郵件的大量散播，已造成全球多國網路頻寬壅塞，台灣亦傳出災情。娜妲病毒日前便傳出肆虐台灣多家企業，對外網頁無法連線。

法律意見：

上開案例中電腦病毒的感染對學校、政府機關所造成的社會成本損失，已令人怵目驚心。但若將場景轉換到企業網路，其經濟上損失更可能是筆天文數字。因此對於每一個網路使用者而言，資訊安全防範意識的建立，不單是口號，更該是身體力行的義務。畢竟，也許正因為我們平時使用網路上一點小疏忽、一些壞習慣，就導致努力累積的經濟成果不明不白的耗損掉了。

三、 電腦駭客的威脅

近年來，網路駭客入侵事件層出不窮，造成的財產損害也越來越大。駭客技術的日益進步固為原因之一，網際網路的普及，使得企業資通安全威脅從封閉的企業內部網路，擴大為無限範圍的外部威脅，更是主要導因。

我國政府及企業電子化腳步相當快速，因此與先進國家同樣地開始面臨駭客危害資通安全的問題。況且因我國網咖林立，店家密度全球僅次韓國，益發增加了防堵電腦駭客上的困難。目前除刑事局在偵查網路犯罪的人力及設備上日益精進外，亦有賴企業及個人，在伺服器主機端做好更周延的安全措施，如架設防火牆、定期更新修正程式（patch files）等，不使駭客有輕易入侵的機會。

1. 對政府機關的威脅

日期：2001/01/30

事件：市府網站遭駭客入侵

事件描述：

市府斥資百萬翻新的網站，在過年期間遭到駭客入侵，首頁被換成許多簡體字及亂碼，幾名駭客還在網頁上開玩笑。市府計畫室人員上班後發現，搶救一整天仍然無法救回，整個網站完全癱瘓。類似情形在五月中旬再度上演。駭客入侵了縣議會網站，將縣議會首頁歡迎標語改成「歡迎光臨中國台南議會」，並附有中國五星旗圖。

法律意見：

這個案例讓我們體認到，資通安全不單是商業上的問題，更可能影響到我國國防安全的良窳。根據1999年美國國防部提交美國國會的「台海安全狀況評估報告」指出，目前大力發展資訊戰力的中共，有可能在2005年取得電子戰的相當優勢。屆時中共駭客可能就不只是改改網頁、加加簡體字了，而是藉網路大規模的影響我社會安定。2001年4月起爆發的中美駭客網路大戰對決，並禍及台灣網站的例子，便明確的向我們透露：上開美方報告，只怕並非僅危言聳聽。

在 4、5 兩月，台灣有上百個網站遭駭客入侵，國內的蕃薯藤網站也遭駭客入侵被更換網頁。而遭駭客破壞的學校約有 22 所，25 所學校網頁找不到伺服器或首頁無資料。比如 5 月上旬馬祖地區即傳出發現當地的一所國小網站首頁，竟然被人張貼了黑底紅字的反美文宣。由於此類跨領域駭客所在地點非我國刑事審判權所能及，我國刑法並無從發揮任何嚇止作用。因此我們每個人都應深切體會到，全國資安機制的及早建構，確實維護，實在是刻不容緩。

日期：2001/11/06

事件：駭客入侵警方網站

事件描述：

縣警察局全面改版縣警局全球資訊網，並提供網路郵局方便民眾提出建議與申訴、或透過電子信箱向各課室、分局、派出所申辦案件。然開辦才 2 小時就遭到疑似網路駭客攻擊。

法律意見：

若駭客藉網路攻擊癱瘓警政機關業務運作，造成民眾申報案件、提出建議的不便，則已觸犯刑法第 352 條第 2 項的毀損文書罪，最高可處 3 年以下有期徒刑。

2. 對學校機關的威脅

日期：2001/03/06

事件：3 小學遭駭客入侵

事件描述：

3 所中小學接獲教育部電算中心通報，指學校網站已遭駭客侵入，成為攻擊相關網站的跳板。

法律意見：

資安體制的建立，不光是法規、政策的指引，及網路安全教育的加強，也須佐以網路犯罪的有效偵查。若駭客藉由侵入他人網站做為進行犯罪的跳板，則網站管理員的疏失不啻為駭客提供了犯罪的屏蔽。因此網站管理員應有做為資通安全守護者的自我期許。

目前我國刑事局已仿效美國聯邦調查局處理重大網路安全事件的機制，對重大網路安全事件發佈警訊，並提供處理意見及因應之道，避免事件擴大。網站管理員若認為自己管理的網站資料庫已受攻擊，或要確定自己的網站是否有相關安全漏洞，可向刑事局資訊室要求協助。

當然，司法是不允許犯罪者恣意妄為的。據刑事局表示，警方已有這方面蒐證能力，除了相關單位及廠商自身應加強維護資料庫安全外，若真有網路犯罪情事發生，因應的偵查起訴，絕不寬貸。

日期：2001/10/02

事件：駭客入侵竄改選課記錄

事件描述：

大學生涉嫌以駭客攻擊竄改同學成績、選修課資料。

法律意見：

行為人以入侵學校電腦方式，不法窺視他人以加密方式封緘的電磁紀錄，已觸犯了刑法第 315 條的妨害書信祕密罪：「無故開封或隱匿他人之封緘信函、文書或圖畫者，處拘役或 3000 元以下罰金。無故以開封以外之方法，窺視其內容者，亦同」。

入侵後復對該紀錄加以竄改，更可能進一步觸犯了刑法第 210 條的偽造私文書罪。該條條文規定：「偽造、變造私文書，足以生損害於公眾或他人者，處 5 年以下有期徒刑。」依目前司法實務見解，上開兩罪間具「方法結果關係」，依刑法第 55 條規定，「從一重處斷」，行為人最重可處 5 年以下有期徒刑。

一個前途原本一片光明的年輕學子，為逞一時剛愎之氣，卻可能換來多年牢獄之災，更令苦心栽培、望子成龍的父母傷心難過。網路上的一舉一動，孰為是，

孰為非，豈可輕忽。

相關判決：90 年上易字 4014 號判決。

3. 對企業及個人的威脅

日期：2001/05/01

事件：駭客入侵網路銀行

事件描述：

國內首宗網路電子銀行遭駭客入侵轉帳盜領客戶存款的案件。嫌犯涉嫌侵入網路銀行的帳戶，利用銀行轉帳服務，將被害人戶頭存款轉帳到人頭帳戶，再以冒名申請的提款卡將錢領走，共盜走 110 萬台幣。

法律意見：

嫌犯侵入網路銀行帳戶，並將被害人帳戶內存款轉帳至人頭帳戶、繼而將錢領走的行為，係對金資機構的電腦系統大肆輸入不正指令，藉以製作財產權之得喪、變更紀錄，並由自動付款設備不法取得他人之物，嚴重干擾了金資電腦系統的正常分配運作。

核其所為，冒用他人名義開設人頭帳戶之行為，已觸犯了刑法第 216 條行使偽變造私文書、特種文書之罪；入侵銀行帳戶轉帳並自 ATM 提款機將錢提走的行為，則觸犯了第 339 條之 2、第 339 條之 3 的準詐欺罪，以及洗錢防制法第 9 條之罪。

在 86 年 10 月 8 日新增公布的刑法第 339 條之 2 第 1 項規定道：「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 3 年以下有期徒刑、拘役或 10000 元以下罰金」。同法第 339 條之 3 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 7 年以下有期徒刑」。網路上的財產犯罪，絕非無法可管，其刑度更是較真實世界的財產犯罪為重。一個指令的輸入，一個按鍵的敲打，換來的卻可能是無窮無盡的悔恨，此案例足以引為殷鑑。

相關判決：90 年度偵字第 9878 號起訴書。

日期：2001/05/27

事件：黑社會駭客勒索企業

事件描述：

台北市一家企業的公司主機日前遭駭客入侵，破壞客戶機密資料後，即接到推銷價值數十萬元的網路安全保護程式的電話，來電者表示如拒買，駭客將持續攻擊。

法律意見：

駭客入侵企業網站破壞客戶機密資料的行為，若足以生損害於該企業，則可能已構成刑法第 352 條第 2 項的干擾電磁紀錄處理之罪，最重可處 3 年以下有期徒刑。倘使繼而以駭客攻擊為脅，恐嚇企業以遂其獲得財產上不法利益之目的，則可能已構成刑法第 346 條第 2 項的恐嚇得利罪。

依刑法第 346 條的規定:「意圖為自己或第 3 人不法之所有，以恐嚇使人將本人或第 3 人之物交付者，處 6 月以上、5 年以下有期徒刑，得併科 1000 元以下罰金。以前項方法得財產上不法之利益，或使第 3 人得之者，亦同」，上開案例事實中，行為人最重可處 5 年以下有期徒刑。

日期：2001/07/02

事件：駭客入侵券商網路下單系統

事件描述：

電腦駭客張顯堂涉嫌入侵券商網路，冒用二千多名客戶名義下單買賣股票、操作特定個股的漲跌，並藉機跟進買賣股票獲利，造成券商難以估算的損失。

法律意見：

嫌犯冒用他人名義製作「電磁紀錄」，向券商下單買賣股票，算不算「偽造文書」呢？由於刑法修正後已於第 220 條第 2 項中明定「電磁紀錄」亦具有文書的性質，因此嫌犯無權製作卻冒用客戶名義製作文書、又用該文書來下單的行為，應已觸犯了刑法第 216 條的行使偽造私文書罪，最重可處五年以下有期徒刑。

再者，嫌犯透過駭客行為，使券商陷於錯誤，代為買賣其網站上客戶之股票，使張嫌得以跟進買賣股票獲利，而受有財產上利益，則可能已構成刑法第 339 條的普通詐欺罪:「意圖為自己或他人不法之所有，以詐術使人將本人或第三人之物交付者，處 5 年以下有期徒刑、拘役或科或併科 1000 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」。

一時的貪念，不但嚴重破壞經濟市場交易秩序，更令自己身陷囹圄。上開案例，足為你我謹記。

四、 電腦犯罪的威脅

除了上開散播病毒、駭客入侵等犯罪類型外，有些電腦犯罪，係利用網路特性，以網路或網路所連結的電腦作為犯罪的場所，或是犯罪的客體。比方說以電子郵件寄送恐嚇信或誹謗言論，藉網路詐欺騙人錢財等。有時網路犯罪行為可能單純出於好玩心理，有時卻可能是有心人存著僥倖心理、誤以為網路是法外之地而恣意為之。

目前國內上網人口如雨後春筍般日漸增加，但相對的企圖經由網路來實施犯罪的人數也逐漸揚升。下面案例，除了希望讓大家了解那些行為千萬不能做以外，也希望大家體認到，網路亦如真實世界般遍布荊棘，使用上仍應處處小心。

1. 侵害智慧財產權

日期：2002/03/19

事件：大 4 盜版王以「宅急便」方式販售光碟

事件描述：

22 歲的大學 4 年級學生，涉嫌自組地下燒錄工廠，同時在國內外成立「冰河工坊」等 5 個網站，透過網路販售流行音樂、知名軟體、遊戲、電影與色情等盜版光碟。為躲避警方追查，鄧某採取民間快遞（宅配通）的送貨方式，放棄易遭警方查獲的「郵局代收貨款」業務，且標榜可預定送貨時間、地點，甚至推出 7 日內退貨保證。刑事局偵 9 隊日前循線將四嫌逮捕，起出三萬五千多片盜版光碟與 29 台燒錄機，並將全案依法函送偵辦。

法律意見：

嫌犯未經著作權人授權，以營利為目的私自拷貝音樂、軟體等光碟，已構成著作權法重製權及編輯權等之侵害。其於網站上販售色情光碟的行為亦有可能觸犯刑法第 235 條散佈猥褻物品罪。該條條文規定為：「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、聽閱者，處 2 年以下有期徒刑、拘役或併科 3 萬元以下

罰金」。

或者有人以為國內智慧財產權徒具空文、取締不力，兼之以有暴利可圖，而對侵害智慧財產權的行為抱著肆無忌憚的心態。那麼以下的文字應可令其心生怵惕。事實上，保護智慧財產權一直是政府的既定政策，更是攸關國內相關產業發展與整體技術提升的關鍵。政府除已將今年訂為「推動保護智慧財產權行動年」，行政院游院長更於 91 年 4 月 3 日行政院院會時再次強調，將結合相關單位的力量，積極進行查緝及宣導工作，全力貫徹保障合法、取締非法著作。

其具體的措施，在經濟部方面，將推動該部成為政府推動智慧財產權保護的單一窗口，並由經濟部長擔任「推動智慧財產權行動年計畫」總召集人，由內政部及法務部政務次長擔任副總召集人，以統籌協調相關事宜。在警政署方面，將建立打擊侵害智慧財產權專責警力，並視實際需要考量人力編制，預計在 92 年將現行 100 名專責警力擴大為 220 名。游揆並指示教育部應該將保護智慧財產權觀念，納入教材；各級學校也應該在校內明訂違反相關規定的懲處規定。當保護智慧財產權已成為全民運動之際，你（妳）還要心存僥倖、以身試法嗎？

相關判決：90 訴字第 418 號，89 年訴字第 315 號。

2. 危害社會秩序

日期：2001/12/19

事件：「名人性愛光碟」網路上廣流傳

事件描述：

2001 年底，某雜誌因隨刊附贈「名人性愛光碟」而引起軒然大波，不但成為人們街談巷議的最佳題材，更引起檢警大規模的搜索扣押行動。但事實上同一內容的性愛影片片段，早在雜誌報導前，即以不同名稱、不同檔案格式在網路上廣泛流傳。有人公開兜售、有人置於網站上供人下載，有人以電子郵件轉寄給眾家親友。

法律意見：

若是將具猥褻性的影片放在網站上供人下載，甚至加以販售，根據刑法第 235 條散布猥褻物品罪規定，「散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其它物品，或公然陳列，或以他法供人觀覽、聽聞者，處 2 年以下有期徒刑、拘役或科或併科 30000 元以下罰金」。同條第 2 項、第 3 項並規定，「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」，「前二項之文字、圖畫、聲音、影像之附著物及物品，不問屬於犯

人與否，沒收之」。意即，就算是免費供人下載，未為營利，亦屬觸法行為。

其次，由於該名人性愛光碟係以偷拍竊錄方式作成，除了偷拍的人可能觸犯刑法第 315 條之 1「竊聽竊錄罪」之外，散布此性愛光碟因此可能同時觸及第 315 條之 2 第 3 項「製造、散布、播送或販賣竊聽竊錄內容罪」，最高可處 5 年以下有期徒刑。

好東西當然該和好朋友分享。但若分享的是猥褻物品，可得冒著被判 2 年以下有期徒刑的風險；若該猥褻物又是以竊聽竊錄得來的，刑度更升高為 5 年。下次使用 outlook 收發信件，在按下「轉寄」鍵前，可得三思而行！

相關判決：司法院大法官釋字第 407 號。

日期：2002/03/28

事件：恐嚇取財亡命之徒網路放話炸銀行

事件描述：

經過刑事局十多日追查後，發現日前以署名「亡命之徒」散佈「不付千萬贖金即引爆多家銀行及速食店」電子郵件的歹徒，發信人竟是名曾被詐騙集團威脅的大學生。警方表示，嫌犯供稱，之所以會廣寄恐嚇勒索的電子郵件，是因為之前曾遭詐騙集團恐嚇，心有不甘。為讓警方能將歹徒繩之以法，即偽造恐嚇電子郵件給眾多連鎖知名大企業，盼能嫁禍詐騙集團。

法律意見：

在上開案例中，嫌犯向企業寄發恐嚇勒索電子郵件的行為，可能已觸犯刑法第 305 條的恐嚇危害安全罪，其規定為：「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 2 年以下有期徒刑、拘役或 300 元以下罰金」。

若受恐嚇之商家及銀行因心生恐懼，允為匯款，使嫌犯因此取得財產上不法之利益，更同時構成了刑法第 346 條第 2 項的恐嚇得利罪。按法條條文規定，只要意圖為自己或他人不法之所有，以恐嚇得財產上不法之利益，即該當該條之罪，可處 6 月以上、5 年

以下有期徒刑，得併科 1,000 元以下罰金。

事實上，以電子郵件寄送恐嚇信件，雖不顯筆跡、不留指紋，警方偵查小組卻可透過發送郵件伺服器的來源，鎖定寄件人的位置，亦不難掌握嫌犯的所在。若誤以為網路是法外天堂，可別後悔莫及。

相關判決：90 年訴字第 80 號。

3. 妨礙交易秩序

日期：2001/03/10

事件：著名商號網域名稱之竊用與勒索

事件描述：

據中國時報報導，90 年 3 月間，由「崔媽媽」推薦的 5 家優良搬家公司分別遭到「網路蟑螂」的勒索，要求搬家公司以 20,000 元到 50,000 元不等的代價，「買回」公司名稱的網址。網路蟑螂甚至揚言，業者若無意贖回，將整合這些網域名稱，另外成立聯合搬家網站，與正牌公司打對台。

法律意見：

由於泛用型中文網域名稱是依照「先申請先發給」原則，只要申請人具備中華民國國民或法人身分即可申請，完全不需文件審核，致使「網站蟑螂」有生存空間。但由於網域名稱便如同企業在實體世界中所享有的商標、標章、事業名稱一般，屬辨視自己身分的一種表徵，我國對於表徵的保護規範，自然也及於網域名稱。

依公平交易法第 20 條第 1 項的規定，若侵害的他人姓名、商號、公司名稱等係屬「相關事業或消費者

所普遍認知」，亦即屬高知名度的表徵，就有相當高的可能性被認為是違反市場的公平競爭秩序。就算未具有高知名度，只要他人的侵害使用有足以妨礙市場公平競爭秩序之虞時，亦可援用同法第 24 條加以保護。

除公平法外，若網路蟑螂所為侵害他人姓名行為，已造成相關大眾的混淆誤認，受害人尚可依民法第 19 條規定請求法院除去其侵害，並得請求損害賠償。若被認定為被害人的人格權亦因之受侵害的話，並得援引民法第 195 條規定，請求賠償相當之金額，及「回復名譽的適當處分」。

日期：2001/09/13

事件：木馬程式盜「天幣」，4 學生駭客落網

事件描述：

擁有國內百萬網友會員的知名遊戲網站「天堂」，自成立以來屢傳玩家虛擬裝備「寶物」、「天幣」遭竊案件。刑事局在連續接獲數十名網友報案後著手深入調查，追出有玩家為了提升遊戲人物的等級，挺而走險盜用其他玩家的遊戲帳號、密碼，侵入竊走被害人的「寶物」、「天幣」，甚至販售謀利（目前行情是 1 萬台幣換 100 萬天幣）。刑事警察局經深入調查，逮捕 4 名大學生嫌犯。刑事局表示，嫌犯係利用一種能紀錄電腦按鍵使用情形的木馬程式，侵入網咖電腦取得他人帳號、密碼，進而盜走「寶物」、「天幣」、「遊戲點數」，甚至販售謀利。

嫌犯向警方供稱，其先在網咖的電腦逐一閱讀暫存資料夾，找到許多其他網友的帳號、密碼，並進而發現若在網咖電腦中植入一種能紀錄電腦按鍵使用情形的木馬程式，可藉此侵入網咖電腦取得他人帳號、密碼，進而盜走「寶物」、「天幣」、「遊戲點數」，甚至販售謀利。

法律意見：

刑法 86 年 10 月 8 日修正時，於第 323 條增列「電磁紀錄關於竊盜罪章之罪，以動產論」之規定。同法第 352 條亦增列第 2 項「干擾他人電磁記錄處理罪」。因此網路遊戲上的寶物、錢幣，雖屬無實體的電磁紀錄，仍可能有刑法上竊盜罪及毀損罪之適用。

因此，上開學生嫌犯以蒐集被害人帳號、密碼，藉以登入天堂網站竊取他人利益，可能觸犯了刑法第 320 條第 1 項之竊盜電磁紀錄罪。再者，嫌犯以植入木馬病毒方式取得被害人資料，如有干擾正常電磁紀錄處理的行為，構成了第 352 條第 2 項之干擾電磁紀錄罪。

其三，嫌犯以非自己所有之帳號、密碼登入天堂網站，並因之取得財產上不法利益之行為，另可能觸犯了刑法第 339 條之 3 第 2 項之準詐欺罪。

相關判決：90 年度偵字第 19875 號聲請簡易判決處刑書。

日期：2002/03/26

事件：十餘家銀行網路破功被盜千萬

事件描述：

刑事局偵四隊二組偵破林啟順詐欺集團，查出國內十餘家知名銀行的網路查詢和語音轉帳系統遭該集團破解，其中聯邦銀行更有上千份客戶極機密資料流入嫌犯手中，作為盜刷信用卡，與盜領金融卡犯罪所需。

警方說，嫌犯利用銀行銷毀過程監控不實的漏洞，到一家廢紙回收中心，竊取這批銀行報銷的客戶資料，並利用台中縣市九二一受災戶搬家遷居的機會，深入受災社區大樓，撿取災民的信用卡申請書郵件，或行竊民宅的電話帳單、信用卡帳單。

嫌犯取得客戶個人資料後，進入銀行語音和網路認證系統內，逐一破解被害人的金融密碼。嫌犯因而得以輕易破解被害人密碼，再變更被害人住址，向銀行申請補發新的金融卡和信用卡，用以盜刷、轉帳或預借現金。

法律意見：

嫌犯私自侵入銀行電腦系統，並就其所侵入系統

中之客戶檔案擅加更改，可能已構成刑法第 210 條的偽造私文書罪。若其偽造行為達毀棄、損壞的程度，並致生損害於他人，亦有刑法第 352 條毀損文書罪的適用。

嫌犯利用變更後的客戶資料向銀行重新申請金融卡和信用卡，用以盜刷、轉帳等行為則觸犯刑法第 216 條之行使偽造私文書罪及第 339 條第 2 項之詐欺得利罪。預借現金之行為，則可能觸犯了刑法第 339 條之 2 第 1 項由自動付款設備取得他人之物罪：「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 3 年以下有期徒刑、拘役或 1 萬元以下罰金」。上述數罪，若認定兼有方法結果之牽連關係，則依刑法第 55 條從一重處斷，依行使偽造私文書罪論處，最重可處 5 年以下有期徒刑。

相關判決：88 年上易字第 219 號。

日期：2002/03/27

事件：網路交易騙徒半年詐千萬

事件描述：

嫌犯利用熟悉網路操作，取得他人的信用卡資料及偽造匯款等資料，在網路上詐購物品再於網路上銷售，半年詐得近千萬元，被害人超過一百人。

警方指出，嫌犯詐購貨品的手法有二種，一為上網查到網路刷卡公司的傳真機號碼，再上經濟部網站查出這家公司的統一編號，然後向中華電信公司申請遙控轉接，在網路刷卡公司人員下班後，把電話轉接到他的租住處，以取得申請人信用卡資料和密碼，然後以這些信用卡資料在拍賣王網站盜刷購物。嫌犯另以徵司機方式取得應徵者身分資料，偽造郵局劃撥匯款收據或銀行匯款單,冒名在網路上向購物公司訂貨。

嫌犯以這兩種方式，連續向四十多家網路購物公司訂購電子商品，詐得商品後又在網路上登廣告販賣，以低於市價一到二成脫手。刑警隊網路犯罪小組已依詐欺罪將他移送法辦，將持續清查被害廠商和盜刷信用卡的件數。

法律意見：

嫌犯偽造郵局匯款收據或銀行匯款單之行為，已觸犯了刑法第 210 條「偽造、變造私文書，足以生損害於公眾或代人者，處 5 年以下有期徒刑」。行使這些偽造文書、用以冒名在網路上購物的行為，則構成刑法第 216 條之行使偽造準文書罪。

至於嫌犯冒用他人信用卡購買貨物的行為，則可能觸犯了刑法第 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 5 年以下有期徒刑、拘役或科或併科 1000 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。前二項之未遂犯罰之」。若法院認定胡嫌以犯詐欺為常業的話，依刑法第 340 條之規定，「以犯 339 條之罪為常業者」，更可能被處以「1 年以上 7 年以上有期徒刑，得併科 5 萬元以下罰金」。

為貪圖眼前一時的利益，卻得過上好幾年苦不堪言的牢獄生活，聰明的你，自然知道安份守法才是人生中最划算的選擇。

相關判決：88 年訴字第 139 號，89 年上訴字 2371 號判決。

編者序

社會高度資訊化下，資訊網路科技的應用正在改變我們商業、工業乃至於生活的模式。根據經濟部委託資策會進行的「我國網際網路用戶數調查統計」，截至 2001 年 12 月底為止，我國網際網路使用人口已高達 782 萬人，網路儼然成為人們密不可分的夥伴。

悠遊於網際網路，人們可以瀏覽國際、政治、財經、科技、學術等各類資訊，滿足知識與實用上的需求。但除聯絡溝通的功用外，目前網際網路更已成為國家許多基礎建設的載具。從水電的供輸、稅賦的報繳、到交通運輸的帷幄等，皆已不復全賴人工處理，轉而藉由網路快速、便捷的特性，發揮更好的管理效能。

然而，科技技術不斷發展、引領資訊通信普及的同時，網路亦對社會帶來負面的衝擊，如電腦病毒的散布、駭客入侵的威脅、與其他利用電腦來侵害他人財產法益之犯罪行為等。一般大眾乃至軍公教從業人員，常因法律知識不夠完整而誤觸法網。此等情況一旦發生，不獨耗損你我辛勤積累的社會成本，更可能傷害了我們於國際社會中努力經營之地位形象。更有甚者，隨著政府各部會的全面電子化，未來的國防安全，全繫之於我國對「資訊戰」應變的良窳。若敵人趁資通安全的罅隙，癱瘓我國水電、通信、交通等重大基礎建設的運作，對國家社會的危害，將難以估計。是以，如何在虛擬與實體環境間找到良好的介面，藉以養成國民正確的資通安全觀念，實屬當務之急。

資通安全法律案例宣導彙編

目前，行政院國家資訊通訊發展推動小組(NICI 小組)為配合六年國家經濟建設計畫，加速推動我國資通安全產業發展，實現 e-Taiwan 願景，正推動「國家資訊通信基礎建設方案」，以 e 政府、e 產業、e 社會及 e 建設四大架構為主軸，期能開創我國擁抱寬頻時代的新契機。與此同時，也積極規劃「建立我國資通訊基礎建設安全機制計畫」，責成政府各單位於建立完善的資通安全防護機制，從而為我國資訊通信安全提供最佳保障。而資通安全法制基礎建設，即為本計畫不可或缺之一環。計畫除預定逐次檢討及增修資通訊安全相關法令外，更重視資通安全人力培訓及觀念宣導、增強執法人員專業能力，以達有效遏止網路犯罪，同時促進網路多元發展之雙效目標。

除上述政策作為外，我們更體認到，建立國民正確資通安全技術與法律觀念，才是維護國家資通安全的基石。因此，行政院「國家資通安全會報」在今年「萬安演習」中，特地將資通安全納入演習項目。希望藉此考驗政府部門平時防護的成果與應變能力，並訓練民眾因應資訊戰的應變能力。配合此次萬安演習，國家資通安全會報技術服務中心出版本彙編，藉由淺顯易懂的文字敘述、深入淺出的案例介紹，相信將能輕鬆建立國民正確的資通安全法制觀念。

行政院國家資通安全會報

技術服務中心 謹誌

資通安全法律案例宣導彙編

前言

為積極落實網路安全教育的推廣，協助各界從身邊發生過的案例中汲取經驗，本手冊因此彙整相關新聞案例，根據資通安全事件發生的成因進行分類與分析，期望建立網路使用者正確的資通安全風險意識。

網路環境的威脅來源，主要有四種：來自天然災害（如水、火）的威脅、具有自動散布性電腦病毒的威脅、電腦駭客入侵的威脅、與利用電腦進行犯罪的威脅。本手冊的第一章即介紹「天然災害的威脅」。藉由事例的描述，希望建立讀者平時即應建立「妥善選擇資料存放地點」與「資料備分」的風險概念。

第二章則是「電腦病毒的威脅」。各類病毒的蔓延，所造成的危害，常常是難以評估的；從延宕一般使用者的工作效率，到造成企業商譽損失、阻斷政府公務正常運作，病毒的肆虐是「一視同仁」、不分彼此的。因此，完善的通資訊安全防護機制是建立在全民對網路安全的風險意識之上。

第三章為「電腦駭客的威脅」。駭客的入侵事件，除了更改網頁等表面上常見的毀損行為外，入侵行為常是駭客進行其他犯罪前的預備行為，如為竊取他人財務資料的目的而移植木馬程式。由於這類程式在未實際運作前難以被察覺，因此造成通資訊安全防護的隱憂甚鉅。讀者不可不知。

第四章「電腦犯罪的威脅」，則羅列目前社會上常發生的電腦犯罪類型，如侵害智慧財產權、危害社會秩序案件、與妨礙交易秩序等案例。對電腦犯罪事件造成的危害作一完整性的介紹。

一、 天然災害的威脅

台灣地理型態特殊，地震颱風頻仍，兼之以人謀不臧所造成的損害，動輒釀成極大的災情。人為傷害或可藉由改善組織管理、事先妥善預防、建立綿密監控等方式，戕傷害程度降至最低；天然災害因多屬地域性、大規模性地侵襲，除組織本體的本身的努力外，更需要政府以上層級的規劃預防及救助。

正因為天然災害對企業及任何組織資通安全性的威脅，不在其它侵害類型（如電腦病毒等）之下，對此類案例的回顧與檢討，誠有其必要。並希望藉此加強大眾對防災及安檢的觀念，以期建立更為妥適的臨災處理模式。

日期：2001/05/14

事件：東科大火

事件描述：

汐止東方科學園區大火，延燒三、四十個小時，二百多家廠商受波及。台灣最大的網路代管服務(IDC)公司在無預警狀況下暫停一百三十家客戶的網站服務。

法律意見：

此種大規模的祝融之災，動輒造成數百家廠商軟、硬體付之一炬，其對於資通安全的威脅並不亞於其他類型。硬體部分尚有保險理賠，但軟體資料一經毀損，若無事先備份，企業因此而損失的商譽及信用往往更甚於硬體的損害。根據美國明尼蘇達大學的一份研究報告指出，企業在沒有資料可用的情況下，金融業至多只能運作兩天，商業則約 3.3 天。有 25%的企業，更可能因資料的損毀而立即破產。正因天災嚴重時可造成無可補救的經濟上損害，思考如何維護政府或企業重要資料的安全、在平時即建立危機意識，實屬刻不容緩。

東科事件中，釀成火災之人，則觸犯刑法第 173-176 條之公共危險罪，最高可處七年有期徒刑。

網路代管公司雖無預警暫停一百多家客戶的網站服務，卻已表示願意賠償。但協助代管客戶投保產險實為治本之道。

在同年九月間納莉風災重創北台灣，造成北台灣多處大淹水，因大量主機皆遭泡水命運，使資訊系統更受到前所未有的傷害。接踵而來的慘痛經驗，更應使我們心生怵惕，了解建立完整事前防範（存放資料地點選擇、資料備份等）的重要性。

二、 電腦病毒的威脅

電腦病毒的威脅由來已久，但隨著網路技術的發展，電腦病毒的傳播媒介由最初的磁碟片，轉而變為藉由網際網路，甚至新興的無線通訊技術，使其蔓延的速度及範圍無數倍於以往。

根據統計，截至 2001 年 9 月，我國網際網路用戶數已達 755 萬人，連線主機數約達 134 萬部，名列全球第 8、亞洲第 2。面對如此龐大的網路流量及使用人數，若在相關軟硬體及資訊教育上未能齊頭並進，將會使電腦病毒的危害及影響更加迅速及深遠。

台灣有優異的資訊工業及資訊工程教育，也培養出大量的軟體人才。如何建立相關法制措施及充分觀念宣導，使有天份的程式設計者不致因懵懂無知而誤蹈法網，成為散播電腦病毒的災害製造者，實為我們未來必須仔細規劃的要項。

1. 對政府及學校的威脅

日期：2001/07/23

事件：思坎病毒蔓延

事件描述：

思坎病毒蔓延，藉由電子郵件進行散播，一旦電腦遭病毒感染後，病毒會尋找通訊錄中的名單，自動發送病毒郵件。該電腦病毒侵襲許多公家機關網站，使網管人員飽受電子郵件病毒侵害之苦。

法律意見：

根據一項由美國聯邦調查局（FBI）和電腦安全協會（CSI）於 2002 年 4 月 7 日所發表的研究指出，電腦病毒是駭客入侵最常用的手法。而根據 500 名研究受訪者所提供的資料，其因電腦病毒或蠕蟲入侵所損失金額約 4,990 萬美元。

由上開研究報告可知，電腦病毒早已不復只是駭客炫耀電腦功力的手法而已，每一隻病毒的發作，其背後可能表彰的是社會上經濟秩序的鉅大損害。若遭感染的對象為政府機關網路，更會造成公務的延宕及

公帑的無謂損失。縱然因政府的全面 e 化，公務員業務上大量使用網路係勢所難免，但你我應在平時即建立好充份的資訊安全意識，並對電腦病毒的感染途徑有一定認識及預防，以期減低電腦病毒對機關內電腦的衝擊。

一般而言，電腦病毒最主要的散播途徑，是透過開啟或執行電子郵件的附加檔案（尤其是附檔名為 EXE、COM、SCR 的檔案）而感染收件者的電腦。但有些最新變種病毒，如「求職信病毒」，使用者只要「預覽」病毒信件，不需執行任何附加檔案，就已經受病毒感染。一些良好使用習慣的養成（諸如不任意開啟來源不明郵件、開啟附檔前一定先掃毒、定期更新病毒碼、outlook 使用者關閉郵件預覽功能等），甚至架設個人或機關內的防火牆，皆有助於扼止電腦病毒的不法肆虐。

根據86年10 月8日增訂刑法第352條第2項之立法理由，若有「干擾他人電磁紀錄之處理，足以影響電腦正常之運作，例如：以『電腦病毒』方式，即利用程式透過電腦連線系統內進行複製，佔據記憶容量，干擾電腦之正常運作功能」，且「如其情形足以生損害於公眾或他人時，宜以刑罰加以規範」。

依刑法第352 條條文：「毀棄、損壞他人文書或致令不堪用，足以生損害於公眾或他人者，處3 年以下

有期徒刑、拘役或1 萬元以下罰金。干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，亦同」。病毒的故意散播者，實已觸犯了刑法第352 條第2項干擾他人電磁紀錄處理之罪。

日期：2001/08/06

事件：新聞病毒橫掃某市府

事件描述：

以「新聞資料」、「公文會辦單」名義散發的電腦病毒，肆虐某市府各機關，許多局科室的電腦都中毒，一開機就傳入數百封的英文信件，塞爆主機造成癱瘓，各單位因而進行緊急掃毒。

法律意見：

行為人透過網路以電腦病毒造成他人電腦硬碟損毀、致令不堪使用，即構成刑法第354 條之普通毀損罪。此外，就上述事實來看，電腦病毒的發作不但干擾了高雄市府各機關公務上電腦資料的處理，更因公務的延宕導致廣大市民的損害。

相關判決：90年度上易字1265號。

日期：2001/08/11

事件：紅色警戒病毒肆虐

事件描述：

縣府教育局與國高中小學間聯絡的資訊網絡「縣教育網」，遭到紅色警戒病毒入侵，主機中毒，網路癱瘓，受害學校無數。

法律意見：

紅色警戒（Code Red）病毒屬於一種結合電腦病毒與駭客程式的攻擊手法。其令人蹙額處，在於它能夠以一程式整合病毒、駭客、DDoS 等數種攻擊手法，使電腦一經感染，即導致多重損害。

根據防毒軟體業者趨勢科技的分析，在國外紅色警戒爆發之初，微軟即就其網路伺服器的作業程式緊急發布防範的修正檔，但僅有少數企業立刻將之更新於伺服器上，致使災情仍不斷擴大。因此可觀察到，企業光使用高階路由器、設置防火牆其實只是治標，對網站管理員資訊安全防護觀念的再強化（如例行性的更新病毒檔、系統定期修正等習慣的建立），才能做到防範於未然。

此外，若有電腦駭客利用植入紅色警戒病毒，在

網路上實施 DDoS 的行為，今後可要特別注意了。據指出，法務部草擬中的「刑法部分條文修正及增訂電腦犯罪章條文草案」，考慮以 5 年以下有期徒刑的重刑伺候駭客這種網路侵入的前段行為。法務部官員指出，在電腦網路犯罪的入侵行為中，DDoS 是屬於侵入的前段行為，以刑法的傳統說法，屬於預備犯行為，應加以處罰。

何謂 DDoS 呢？DDoS 其實是 Distributed Denial of Service 的縮寫，有人將之譯為分散式阻斷服務攻擊，是一種特殊形式的拒絕服務網路技術。這種技術是利用多台已經被駭客所控制的主機對某一台單機發動攻擊，以該單一主機能夠容納的封包，一次迴傳到該單機，在頻寬相對的情況之下，被攻擊的主機的寬頻很容易被消耗光而失去反應能力。

法務部在 91 年 4 月所提出的最新刑法修正草案中表示，網際網路的使用，應該准予更寬廣的自由度，但提供內容的網站與網路服務業者，與使用者一樣有權利受到保護，網路安全與順暢的自由也同樣要受合法維護，所以才會決定對 DDoS 的行為科以 5 年以下有期徒刑的重刑。

事實上，對電腦病毒及電腦駭客的規制，世界各地皆在如火如荼的展開中。舉例來說，中國大陸即於 91 年 3 月 1 日，由一家名叫瑪賽的公司聯合大陸上海

熱線、上海市公安局網監處，破獲一個長期以來針對大陸著名 ISP／ICP 進行 DDoS 的周姓駭客。這正說明了 DDoS 已是各國防制駭客行為中,必然約束的一種網路侵入前的不法行為。是以，手癢難耐、準備散播病毒的眾家駭客們，無論你下手的對象是國內網站抑或國外網站,可得三思而行。若是僅為滿足一時的虛榮，卻賠上寶貴的光陰和大好的前程，多令人惋惜！

2. 對企業及個人的威脅

日期：2001/10/31

事件：娜妲病毒入侵證交所電腦

事件描述：

娜妲（Nimda）變種電腦病毒自 2001 年 9 月初萌後，透過電子郵件的大量散播，已造成全球多國網路頻寬壅塞，台灣亦傳出災情。娜妲病毒日前便傳出肆虐台灣多家企業，對外網頁無法連線。

法律意見：

上開案例中電腦病毒的感染對學校、政府機關所造成的社會成本損失，已令人怵目驚心。但若將場景轉換到企業網路，其經濟上損失更可能是筆天文數字。因此對於每一個網路使用者而言，資訊安全防範意識的建立，不單是口號，更該是身體力行的義務。畢竟，也許正因為我們平時使用網路上一點小疏忽、一些壞習慣，就導致努力累積的經濟成果不明不白的耗損掉了。

三、 電腦駭客的威脅

近年來，網路駭客入侵事件層出不窮，造成的財產損害也越來越大。駭客技術的日益進步固為原因之一，網際網路的普及，使得企業資通安全威脅從封閉的企業內部網路，擴大為無限範圍的外部威脅，更是主要導因。

我國政府及企業電子化腳步相當快速，因此與先進國家同樣地開始面臨駭客危害資通安全的問題。況且因我國網咖林立，店家密度全球僅次韓國，益發增加了防堵電腦駭客上的困難。目前除刑事局在偵查網路犯罪的人力及設備上日益精進外，亦有賴企業及個人，在伺服器主機端做好更周延的安全措施，如架設防火牆、定期更新修正程式（patch files）等，不使駭客有輕易入侵的機會。

1. 對政府機關的威脅

日期：2001/01/30

事件：市府網站遭駭客入侵

事件描述：

市府斥資百萬翻新的網站，在過年期間遭到駭客入侵，首頁被換成許多簡體字及亂碼，幾名駭客還在網頁上開玩笑。市府計畫室人員上班後發現，搶救一整天仍然無法救回，整個網站完全癱瘓。類似情形在五月中旬再度上演。駭客入侵了縣議會網站，將縣議會首頁歡迎標語改成「歡迎光臨中國台南議會」，並附有中國五星旗圖。

法律意見：

這個案例讓我們體認到，資通安全不單是商業上的問題，更可能影響到我國國防安全的良窳。根據1999年美國國防部提交美國國會的「台海安全狀況評估報告」指出，目前大力發展資訊戰力的中共，有可能在2005年取得電子戰的相當優勢。屆時中共駭客可能就不只是改改網頁、加加簡體字了，而是藉網路大規模的影響我社會安定。2001年4月起爆發的中美駭客網路大戰對決，並禍及台灣網站的例子，便明確的向我們透露：上開美方報告，只怕並非僅危言聳聽。

在 4、5 兩月，台灣有上百個網站遭駭客入侵，國內的蕃薯藤網站也遭駭客入侵被更換網頁。而遭駭客破壞的學校約有 22 所，25 所學校網頁找不到伺服器或首頁無資料。比如 5 月上旬馬祖地區即傳出發現當地的一所國小網站首頁，竟然被人張貼了黑底紅字的反美文宣。由於此類跨領域駭客所在地點非我國刑事審判權所能及，我國刑法並無從發揮任何嚇止作用。因此我們每個人都應深切體會到，全國資安機制的及早建構，確實維護，實在是刻不容緩。

日期：2001/11/06

事件：駭客入侵警方網站

事件描述：

縣警察局全面改版縣警局全球資訊網，並提供網路郵局方便民眾提出建議與申訴、或透過電子信箱向各課室、分局、派出所申辦案件。然開辦才 2 小時就遭到疑似網路駭客攻擊。

法律意見：

若駭客藉網路攻擊癱瘓警政機關業務運作，造成民眾申報案件、提出建議的不便，則已觸犯刑法第 352 條第 2 項的毀損文書罪，最高可處 3 年以下有期徒刑。

2. 對學校機關的威脅

日期：2001/03/06

事件：3 小學遭駭客入侵

事件描述：

3 所中小學接獲教育部電算中心通報，指學校網站已遭駭客侵入，成為攻擊相關網站的跳板。

法律意見：

資安體制的建立，不光是法規、政策的指引，及網路安全教育的加強，也須佐以網路犯罪的有效偵查。若駭客藉由侵入他人網站做為進行犯罪的跳板，則網站管理員的疏失不啻為駭客提供了犯罪的屏蔽。因此網站管理員應有做為資通安全守護者的自我期許。

目前我國刑事局已仿效美國聯邦調查局處理重大網路安全事件的機制，對重大網路安全事件發佈警訊，並提供處理意見及因應之道，避免事件擴大。網站管理員若認為自己管理的網站資料庫已受攻擊，或要確定自己的網站是否有相關安全漏洞，可向刑事局資訊室要求協助。

當然，司法是不允許犯罪者恣意妄為的。據刑事局表示，警方已有這方面蒐證能力，除了相關單位及廠商自身應加強維護資料庫安全外，若真有網路犯罪情事發生，因應的偵查起訴，絕不寬貸。

日期：2001/10/02

事件：駭客入侵竄改選課記錄

事件描述：

大學生涉嫌以駭客攻擊竄改同學成績、選修課資料。

法律意見：

行為人以入侵學校電腦方式，不法窺視他人以加密方式封緘的電磁紀錄，已觸犯了刑法第 315 條的妨害書信祕密罪：「無故開封或隱匿他人之封緘信函、文書或圖畫者，處拘役或 3000 元以下罰金。無故以開封以外之方法，窺視其內容者，亦同」。

入侵後復對該紀錄加以竄改，更可能進一步觸犯了刑法第 210 條的偽造私文書罪。該條條文規定：「偽造、變造私文書，足以生損害於公眾或他人者，處 5 年以下有期徒刑。」依目前司法實務見解，上開兩罪間具「方法結果關係」，依刑法第 55 條規定，「從一重處斷」，行為人最重可處 5 年以下有期徒刑。

一個前途原本一片光明的年輕學子，為逞一時剛愎之氣，卻可能換來多年牢獄之災，更令苦心栽培、望子成龍的父母傷心難過。網路上的一舉一動，孰為是，

孰為非，豈可輕忽。

相關判決：90 年上易字 4014 號判決。

3. 對企業及個人的威脅

日期：2001/05/01

事件：駭客入侵網路銀行

事件描述：

國內首宗網路電子銀行遭駭客入侵轉帳盜領客戶存款的案件。嫌犯涉嫌侵入網路銀行的帳戶，利用銀行轉帳服務，將被害人戶頭存款轉帳到人頭帳戶，再以冒名申請的提款卡將錢領走，共盜走 110 萬台幣。

法律意見：

嫌犯侵入網路銀行帳戶，並將被害人帳戶內存款轉帳至人頭帳戶、繼而將錢領走的行為，係對金資機構的電腦系統大肆輸入不正指令，藉以製作財產權之得喪、變更紀錄，並由自動付款設備不法取得他人之物，嚴重干擾了金資電腦系統的正常分配運作。

核其所為，冒用他人名義開設人頭帳戶之行為，已觸犯了刑法第 216 條行使偽變造私文書、特種文書之罪；入侵銀行帳戶轉帳並自 ATM 提款機將錢提走的行為，則觸犯了第 339 條之 2、第 339 條之 3 的準詐欺罪，以及洗錢防制法第 9 條之罪。

在 86 年 10 月 8 日新增公布的刑法第 339 條之 2 第 1 項規定道：「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 3 年以下有期徒刑、拘役或 10000 元以下罰金」。同法第 339 條之 3 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 7 年以下有期徒刑」。網路上的財產犯罪，絕非無法可管，其刑度更是較真實世界的財產犯罪為重。一個指令的輸入，一個按鍵的敲打，換來的卻可能是無窮無盡的悔恨，此案例足以引為殷鑑。

相關判決：90 年度偵字第 9878 號起訴書。

日期：2001/05/27

事件：黑社會駭客勒索企業

事件描述：

台北市一家企業的公司主機日前遭駭客入侵，破壞客戶機密資料後，即接到推銷價值數十萬元的網路安全保護程式的電話，來電者表示如拒買，駭客將持續攻擊。

法律意見：

駭客入侵企業網站破壞客戶機密資料的行為，若足以生損害於該企業，則可能已構成刑法第 352 條第 2 項的干擾電磁紀錄處理之罪，最重可處 3 年以下有期徒刑。倘使繼而以駭客攻擊為脅，恐嚇企業以遂其獲得財產上不法利益之目的，則可能已構成刑法第 346 條第 2 項的恐嚇得利罪。

依刑法第 346 條的規定:「意圖為自己或第 3 人不法之所有，以恐嚇使人將本人或第 3 人之物交付者，處 6 月以上、5 年以下有期徒刑，得併科 1000 元以下罰金。以前項方法得財產上不法之利益，或使第 3 人得之者，亦同」，上開案例事實中，行為人最重可處 5 年以下有期徒刑。

日期：2001/07/02

事件：駭客入侵券商網路下單系統

事件描述：

電腦駭客張顯堂涉嫌入侵券商網路，冒用二千多名客戶名義下單買賣股票、操作特定個股的漲跌，並藉機跟進買賣股票獲利，造成券商難以估算的損失。

法律意見：

嫌犯冒用他人名義製作「電磁紀錄」，向券商下單買賣股票，算不算「偽造文書」呢？由於刑法修正後已於第 220 條第 2 項中明定「電磁紀錄」亦具有文書的性質，因此嫌犯無權製作卻冒用客戶名義製作文書、又用該文書來下單的行為，應已觸犯了刑法第 216 條的行使偽造私文書罪，最重可處五年以下有期徒刑。

再者，嫌犯透過駭客行為，使券商陷於錯誤，代為買賣其網站上客戶之股票，使張嫌得以跟進買賣股票獲利，而受有財產上利益，則可能已構成刑法第 339 條的普通詐欺罪:「意圖為自己或他人不法之所有，以詐術使人將本人或第三人之物交付者，處 5 年以下有期徒刑、拘役或科或併科 1000 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」。

一時的貪念，不但嚴重破壞經濟市場交易秩序，更令自己身陷囹圄。上開案例，足為你我謹記。

四、 電腦犯罪的威脅

除了上開散播病毒、駭客入侵等犯罪類型外，有些電腦犯罪，係利用網路特性，以網路或網路所連結的電腦作為犯罪的場所，或是犯罪的客體。比方說以電子郵件寄送恐嚇信或誹謗言論，藉網路詐欺騙人錢財等。有時網路犯罪行為可能單純出於好玩心理，有時卻可能是有心人存著僥倖心理、誤以為網路是法外之地而恣意為之。

目前國內上網人口如雨後春筍般日漸增加，但相對的企圖經由網路來實施犯罪的人數也逐漸揚升。下面案例，除了希望讓大家了解那些行為千萬不能做以外，也希望大家體認到，網路亦如真實世界般遍布荊棘，使用上仍應處處小心。

1. 侵害智慧財產權

日期：2002/03/19

事件：大 4 盜版王以「宅急便」方式販售光碟

事件描述：

22 歲的大學 4 年級學生，涉嫌自組地下燒錄工廠，同時在國內外成立「冰河工坊」等 5 個網站，透過網路販售流行音樂、知名軟體、遊戲、電影與色情等盜版光碟。為躲避警方追查，鄧某採取民間快遞（宅配通）的送貨方式，放棄易遭警方查獲的「郵局代收貨款」業務，且標榜可預定送貨時間、地點，甚至推出 7 日內退貨保證。刑事局偵 9 隊日前循線將四嫌逮捕，起出三萬五千多片盜版光碟與 29 台燒錄機，並將全案依法函送偵辦。

法律意見：

嫌犯未經著作權人授權，以營利為目的私自拷貝音樂、軟體等光碟，已構成著作權法重製權及編輯權等之侵害。其於網站上販售色情光碟的行為亦有可能觸犯刑法第 235 條散佈猥褻物品罪。該條條文規定為：「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、聽閱者，處 2 年以下有期徒刑、拘役或併科 3 萬元以下

罰金」。

或者有人以為國內智慧財產權徒具空文、取締不力，兼之以有暴利可圖，而對侵害智慧財產權的行為抱著肆無忌憚的心態。那麼以下的文字應可令其心生怵惕。事實上，保護智慧財產權一直是政府的既定政策，更是攸關國內相關產業發展與整體技術提升的關鍵。政府除已將今年訂為「推動保護智慧財產權行動年」，行政院游院長更於 91 年 4 月 3 日行政院院會時再次強調，將結合相關單位的力量，積極進行查緝及宣導工作，全力貫徹保障合法、取締非法著作。

其具體的措施，在經濟部方面，將推動該部成為政府推動智慧財產權保護的單一窗口，並由經濟部長擔任「推動智慧財產權行動年計畫」總召集人，由內政部及法務部政務次長擔任副總召集人，以統籌協調相關事宜。在警政署方面，將建立打擊侵害智慧財產權專責警力，並視實際需要考量人力編制，預計在 92 年將現行 100 名專責警力擴大為 220 名。游揆並指示教育部應該將保護智慧財產權觀念，納入教材；各級學校也應該在校內明訂違反相關規定的懲處規定。當保護智慧財產權已成為全民運動之際，你（妳）還要心存僥倖、以身試法嗎？

相關判決：90 訴字第 418 號，89 年訴字第 315 號。

2. 危害社會秩序

日期：2001/12/19

事件：「名人性愛光碟」網路上廣流傳

事件描述：

2001 年底，某雜誌因隨刊附贈「名人性愛光碟」而引起軒然大波，不但成為人們街談巷議的最佳題材，更引起檢警大規模的搜索扣押行動。但事實上同一內容的性愛影片片段，早在雜誌報導前，即以不同名稱、不同檔案格式在網路上廣泛流傳。有人公開兜售、有人置於網站上供人下載，有人以電子郵件轉寄給眾家親友。

法律意見：

若是將具猥褻性的影片放在網站上供人下載，甚至加以販售，根據刑法第 235 條散布猥褻物品罪規定，「散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其它物品，或公然陳列，或以他法供人觀覽、聽聞者，處 2 年以下有期徒刑、拘役或科或併科 30000 元以下罰金」。同條第 2 項、第 3 項並規定，「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」，「前二項之文字、圖畫、聲音、影像之附著物及物品，不問屬於犯

人與否，沒收之」。意即，就算是免費供人下載，未為營利，亦屬觸法行為。

其次，由於該名人性愛光碟係以偷拍竊錄方式作成，除了偷拍的人可能觸犯刑法第 315 條之 1「竊聽竊錄罪」之外，散布此性愛光碟因此可能同時觸及第 315 條之 2 第 3 項「製造、散布、播送或販賣竊聽竊錄內容罪」，最高可處 5 年以下有期徒刑。

好東西當然該和好朋友分享。但若分享的是猥褻物品，可得冒著被判 2 年以下有期徒刑的風險；若該猥褻物又是以竊聽竊錄得來的，刑度更升高為 5 年。下次使用 outlook 收發信件，在按下「轉寄」鍵前，可得三思而行！

相關判決：司法院大法官釋字第 407 號。

日期：2002/03/28

事件：恐嚇取財亡命之徒網路放話炸銀行

事件描述：

經過刑事局十多日追查後，發現日前以署名「亡命之徒」散佈「不付千萬贖金即引爆多家銀行及速食店」電子郵件的歹徒，發信人竟是名曾被詐騙集團威脅的大學生。警方表示，嫌犯供稱，之所以會廣寄恐嚇勒索的電子郵件，是因為之前曾遭詐騙集團恐嚇，心有不甘。為讓警方能將歹徒繩之以法，即偽造恐嚇電子郵件給眾多連鎖知名大企業，盼能嫁禍詐騙集團。

法律意見：

在上開案例中，嫌犯向企業寄發恐嚇勒索電子郵件的行為，可能已觸犯刑法第 305 條的恐嚇危害安全罪，其規定為：「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 2 年以下有期徒刑、拘役或 300 元以下罰金」。

若受恐嚇之商家及銀行因心生恐懼，允為匯款，使嫌犯因此取得財產上不法之利益，更同時構成了刑法第 346 條第 2 項的恐嚇得利罪。按法條條文規定，只要意圖為自己或他人不法之所有，以恐嚇得財產上不法之利益，即該當該條之罪，可處 6 月以上、5 年

以下有期徒刑，得併科 1,000 元以下罰金。

事實上，以電子郵件寄送恐嚇信件，雖不顯筆跡、不留指紋，警方偵查小組卻可透過發送郵件伺服器的來源，鎖定寄件人的位置，亦不難掌握嫌犯的所在。若誤以為網路是法外天堂，可別後悔莫及。

相關判決：90 年訴字第 80 號。

3. 妨礙交易秩序

日期：2001/03/10

事件：著名商號網域名稱之竊用與勒索

事件描述：

據中國時報報導，90 年 3 月間，由「崔媽媽」推薦的 5 家優良搬家公司分別遭到「網路蟑螂」的勒索，要求搬家公司以 20,000 元到 50,000 元不等的代價，「買回」公司名稱的網址。網路蟑螂甚至揚言，業者若無意贖回，將整合這些網域名稱，另外成立聯合搬家網站，與正牌公司打對台。

法律意見：

由於泛用型中文網域名稱是依照「先申請先發給」原則，只要申請人具備中華民國國民或法人身分即可申請，完全不需文件審核，致使「網站蟑螂」有生存空間。但由於網域名稱便如同企業在實體世界中所享有的商標、標章、事業名稱一般，屬辨視自己身分的一種表徵，我國對於表徵的保護規範，自然也及於網域名稱。

依公平交易法第 20 條第 1 項的規定，若侵害的他人姓名、商號、公司名稱等係屬「相關事業或消費者

所普遍認知」，亦即屬高知名度的表徵，就有相當高的可能性被認為是違反市場的公平競爭秩序。就算未具有高知名度，只要他人的侵害使用有足以妨礙市場公平競爭秩序之虞時，亦可援用同法第 24 條加以保護。

除公平法外，若網路蟑螂所為侵害他人姓名行為，已造成相關大眾的混淆誤認，受害人尚可依民法第 19 條規定請求法院除去其侵害，並得請求損害賠償。若被認定為被害人的人格權亦因之受侵害的話，並得援引民法第 195 條規定，請求賠償相當之金額，及「回復名譽的適當處分」。

日期：2001/09/13

事件：木馬程式盜「天幣」，4 學生駭客落網

事件描述：

擁有國內百萬網友會員的知名遊戲網站「天堂」，自成立以來屢傳玩家虛擬裝備「寶物」、「天幣」遭竊案件。刑事局在連續接獲數十名網友報案後著手深入調查，追出有玩家為了提升遊戲人物的等級，挺而走險盜用其他玩家的遊戲帳號、密碼，侵入竊走被害人的「寶物」、「天幣」，甚至販售謀利（目前行情是 1 萬台幣換 100 萬天幣）。刑事警察局經深入調查，逮捕 4 名大學生嫌犯。刑事局表示，嫌犯係利用一種能紀錄電腦按鍵使用情形的木馬程式，侵入網咖電腦取得他人帳號、密碼，進而盜走「寶物」、「天幣」、「遊戲點數」，甚至販售謀利。

嫌犯向警方供稱，其先在網咖的電腦逐一閱讀暫存資料夾，找到許多其他網友的帳號、密碼，並進而發現若在網咖電腦中植入一種能紀錄電腦按鍵使用情形的木馬程式，可藉此侵入網咖電腦取得他人帳號、密碼，進而盜走「寶物」、「天幣」、「遊戲點數」，甚至販售謀利。

法律意見：

刑法 86 年 10 月 8 日修正時，於第 323 條增列「電磁紀錄關於竊盜罪章之罪，以動產論」之規定。同法第 352 條亦增列第 2 項「干擾他人電磁記錄處理罪」。因此網路遊戲上的寶物、錢幣，雖屬無實體的電磁紀錄，仍可能有刑法上竊盜罪及毀損罪之適用。

因此，上開學生嫌犯以蒐集被害人帳號、密碼，藉以登入天堂網站竊取他人利益，可能觸犯了刑法第 320 條第 1 項之竊盜電磁紀錄罪。再者，嫌犯以植入木馬病毒方式取得被害人資料，如有干擾正常電磁紀錄處理的行為，構成了第 352 條第 2 項之干擾電磁紀錄罪。

其三，嫌犯以非自己所有之帳號、密碼登入天堂網站，並因之取得財產上不法利益之行為，另可能觸犯了刑法第 339 條之 3 第 2 項之準詐欺罪。

相關判決：90 年度偵字第 19875 號聲請簡易判決處刑書。

日期：2002/03/26

事件：十餘家銀行網路破功被盜千萬

事件描述：

刑事局偵四隊二組偵破林啟順詐欺集團，查出國內十餘家知名銀行的網路查詢和語音轉帳系統遭該集團破解，其中聯邦銀行更有上千份客戶極機密資料流入嫌犯手中，作為盜刷信用卡，與盜領金融卡犯罪所需。

警方說，嫌犯利用銀行銷毀過程監控不實的漏洞，到一家廢紙回收中心，竊取這批銀行報銷的客戶資料，並利用台中縣市九二一受災戶搬家遷居的機會，深入受災社區大樓，撿取災民的信用卡申請書郵件，或行竊民宅的電話帳單、信用卡帳單。

嫌犯取得客戶個人資料後，進入銀行語音和網路認證系統內，逐一破解被害人的金融密碼。嫌犯因而得以輕易破解被害人密碼，再變更被害人住址，向銀行申請補發新的金融卡和信用卡，用以盜刷、轉帳或預借現金。

法律意見：

嫌犯私自侵入銀行電腦系統，並就其所侵入系統

中之客戶檔案擅加更改，可能已構成刑法第 210 條的偽造私文書罪。若其偽造行為達毀棄、損壞的程度，並致生損害於他人，亦有刑法第 352 條毀損文書罪的適用。

嫌犯利用變更後的客戶資料向銀行重新申請金融卡和信用卡，用以盜刷、轉帳等行為則觸犯刑法第 216 條之行使偽造私文書罪及第 339 條第 2 項之詐欺得利罪。預借現金之行為，則可能觸犯了刑法第 339 條之 2 第 1 項由自動付款設備取得他人之物罪：「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 3 年以下有期徒刑、拘役或 1 萬元以下罰金」。上述數罪，若認定兼有方法結果之牽連關係，則依刑法第 55 條從一重處斷，依行使偽造私文書罪論處，最重可處 5 年以下有期徒刑。

相關判決：88 年上易字第 219 號。

日期：2002/03/27

事件：網路交易騙徒半年詐千萬

事件描述：

嫌犯利用熟悉網路操作，取得他人的信用卡資料及偽造匯款等資料，在網路上詐購物品再於網路上銷售，半年詐得近千萬元，被害人超過一百人。

警方指出，嫌犯詐購貨品的手法有二種，一為上網查到網路刷卡公司的傳真機號碼，再上經濟部網站查出這家公司的統一編號，然後向中華電信公司申請遙控轉接，在網路刷卡公司人員下班後，把電話轉接到他的租住處，以取得申請人信用卡資料和密碼，然後以這些信用卡資料在拍賣王網站盜刷購物。嫌犯另以徵司機方式取得應徵者身分資料，偽造郵局劃撥匯款收據或銀行匯款單,冒名在網路上向購物公司訂貨。

嫌犯以這兩種方式，連續向四十多家網路購物公司訂購電子商品，詐得商品後又在網路上登廣告販賣，以低於市價一到二成脫手。刑警隊網路犯罪小組已依詐欺罪將他移送法辦，將持續清查被害廠商和盜刷信用卡的件數。

法律意見：

嫌犯偽造郵局匯款收據或銀行匯款單之行為，已觸犯了刑法第 210 條「偽造、變造私文書，足以生損害於公眾或代人者，處 5 年以下有期徒刑」。行使這些偽造文書、用以冒名在網路上購物的行為，則構成刑法第 216 條之行使偽造準文書罪。

至於嫌犯冒用他人信用卡購買貨物的行為，則可能觸犯了刑法第 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 5 年以下有期徒刑、拘役或科或併科 1000 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。前二項之未遂犯罰之」。若法院認定胡嫌以犯詐欺為常業的話，依刑法第 340 條之規定，「以犯 339 條之罪為常業者」，更可能被處以「1 年以上 7 年以上有期徒刑，得併科 5 萬元以下罰金」。

為貪圖眼前一時的利益，卻得過上好幾年苦不堪言的牢獄生活，聰明的你，自然知道安份守法才是人生中最划算的選擇。

相關判決：88 年訴字第 139 號，89 年上訴字 2371 號判決。