修平科技大學

資訊網路技術系

電腦網路犯罪及詐騙

指導老師：沈良澤老師

組長：YN99053 王靖傑

組員：YN99038 洪煜軒

YN99013 陳致遠

YN99050 鄭惟中

指導老師：_____

中華民國 103 年 1 月 4 號

目錄

摘要

本小組專題以「電腦及網路犯罪」，網路犯罪問題從歷史觀點而言係先從電腦犯罪漸演化而來，一般而言，有關「電腦及網路犯罪」的定義仍是以學者林山田之分類為主，而可分為廣義說、狹義說與折衷說。

目前我國學界通說係採折衷說，即認為「電腦及網路犯罪」乃指行為人濫用或破壞電腦而違犯具有電腦特質的犯罪行為，所謂「電腦特質」則以行為的犯、追訴或審判是否需要電腦的專業知識為斷。國人對網路依賴程度越來越深。交通部統計發現，與 2 年前相較，國內上網人口又增加了 145 萬人，已達 1237 萬人，且家庭使用寬頻上網比例已逼近 83%，在網咖上網及使用電話撥接上網比例相對下降；而且，網路族每天上網比例也提高 10%，平均每周上網時數更增加至 15.7 小時，比 2 年前多了 3.6 小時，等於每天有超過 2.2 小時是泡在網路上。和 2 年前相比，每天都要上網的人已逾 64.2%，成長 10.5%，顯見國人依賴網路漸深；每天隨時都有成千上萬人在網際網路上瀏覽網頁、進行電子商務、線上遊戲、線上聊天、傳送電子郵件等事宜，在如此眾多的上網人口中存在有多少不為人知的犯罪秘密？有多少是在進行駭客行為？有多少是為了獲得金錢利益？有多少是為了線上遊戲中寶物？伴隨著而來的網路色情、網路賭博、販賣盜拷、販賣禁藥、販賣槍械、網路恐嚇、網路誹謗、網路駭客、電腦病毒、網路竄改等事件不一而足，加之網際網路便利性，跨國性的犯罪集團行為，讓各類犯罪行為的偵查更加的困難，面對越來越多樣化的網路犯罪問題，對警察機關來說更是不得不重視的主要課題。

第一章簡介

1.1 簡介

升上四年級這個暑假，因為透過老師讓我們知道網路上的犯罪及詐騙的案件非常多及普級，藉由老讓我們研究「網路犯罪」案例，試著去分析如何解決網路犯罪及詐騙的案例，試著找出許多的方法來解決並防止更多人受到網路詐騙的這個的不法行為。

網路技術越來越日新月異，雖然使得增加許多的便利性，因此也讓人跟人之間的距離越來越遠，利用人性的弱點導致網路犯罪的事件有一直增加的趨勢，因為網路的方便使得一些店家在網路上販賣商品帶來商機，也讓經濟成長了許多，但有些不法商人利用人的貪婪讓消費者卸下心防詐騙，以前多看報紙新聞就可以了解時事趨勢但是現在看報紙新聞已經成不了秀才要利用電腦網路來連接才能因應趨勢變化。

電腦網路已成為人們生活上不可缺少的一項資源。

1.2 研究動機

近年來常常發生個人資料外洩的新聞，除有購物頻道的消費者因業者外洩個人資料，而遭到詐騙集團鎖定行騙外。政府機關處理民眾的個人資料亦有疏忽之情事。

某市政府法規會，把民眾申請國賠的資料全都開放提供檢索不僅個人資料外洩，連就醫紀錄都被張貼網站上，顯見目前對於個人資料的保護還不夠落實。

而國家機關為履行國民所付託之國家事務，從事一定國家行為前均先掌握必要資訊資料作為決策執行時之參考依據。當該資訊資料涉及國家安全利益而列為應秘密者，自屬不得對外公開。

公務員負有保守國家機密之義務，建立人民對於政府之信賴以利國家事務之推動。

若公務員得以任意公開或洩漏政府以立法、民眾申報義務或其他行政管制手段所取得有關人民之資訊，輕則侵害人民。資訊自主之權利，重則足以影響國防、外交、經濟市場秩序。

民國 84 年 8 月 11 日公布「電腦處理個人資料保護法」期間鑒於電腦科技日新月異，利用電腦蒐集、處理、利用個人資料之情形日漸普遍，各類型商務行銷廣泛大量蒐集個人資料，個人隱私權之保護造成莫大威脅為使該法規範內容得以因應急速變遷之社會環境。

1.3 研究目的

在網際網路發達後，原先對單一電腦所構成的犯罪型態，已經擴大到由多數電腦所構成網際空間的犯罪行為。

如網上從事散布猥褻文書、圖畫、影像；在網上詐欺、賭博、公然侮辱、毀謗他人，或者癱瘓他人電子信箱、盜用撥接帳號、散布病毒、暗中植入特洛依木馬程式、攻擊他人主機，入侵電腦系統、竄改資料庫內容、網上媒介性交易等等。

「電腦犯罪」是泛指行為人破壞電腦、操縱電腦系統及其相關設備的正常運作，或者是對電腦所處理的資訊內容為偽造、變造、洩漏、竊取，進而侵害他人法益的犯罪行為 。

侵犯電腦資料與系統機密性、完整性與可利用性的犯罪：包括非法入侵、非法截取、資料干擾、系統干擾、設備濫用 ，都會造成網路犯罪。 與電腦應用有關的犯罪：包括利用電腦偽造文書、電腦詐欺。

1.4 文獻探討

不管在什麼樣的社會或時代中，「犯罪」這個問題可說是無法完全消滅的，換言之，不管社會如何改變，時代如何進步，犯罪的問題依然都會存在於社會之中。犯罪學家涂爾幹表示，犯罪現象乃一個社會中正常且必須的存在，甚至有助於社會釐清道德是非，並幫助社會衝突調和。然而隨著生活環境的變遷，犯罪的種類與型態也會隨之改變；在網路發展如此迅速的現代社會裡，網路犯罪的相應產生也就不足為奇了；而所謂「網路犯罪」(從歷史的角度來看，其可說是由「電腦犯罪」的型態及概念逐漸演化而來，但網路之特性終究與電腦之使用行為不同，網路犯罪係利用網路之特性所為之犯罪手段或為犯罪工具之網路濫用行為。所以在談網路犯罪時，首先必需先將「網路犯罪」與「電腦犯罪」作一區別。

長久以來中外學者將犯罪歸類於法律所不允許的一種行為，發展至今其型態趨於多樣，乃因社會結構多元發展的結果所導致。因此論述犯罪型態的定義應由當時社會的行為模式為準則，較能將犯罪形式清楚界定。然而資訊科學主導社會的今日，網際網路的產出，讓人類在實體社會裡藉由虛擬的方式達到溝通、聯繫與知識傳遞等目的，促使人類漸漸依賴這樣的訊息模式把實體社會的行為帶入虛擬社會裡運作，犯罪即為人類典型的行為，正如恩格斯所言：「人類每跨出一步即加大對自我的懲罰力度」。絢麗多姿的網路世界有如「潘朵拉」魔盒在給人類帶來希望之同時也釋放世紀的烏雲：網路犯罪。 犯罪型態定義應根據其行為及模式，因此網路犯罪就是利用網路作為犯罪

空間或客體來達成犯罪目標稱之為網路犯罪。但綜觀歷史角度網路犯罪乃從電腦犯罪演變而來，最初關於電腦犯罪係由歐洲經濟合作與發展組織定義為：「在自動資料處裡的過程中任何非法、違反社會與道德，且未經允許的行為均為電腦犯罪」。德國犯罪學家認為電腦犯罪是利用電子資料處理設備作為犯罪的工具與犯罪的目標的一種犯罪行為稱之。美國電腦犯罪專家清楚認定電腦濫用是指電腦使用的故意行為導致受害人財產遭受損失並涉及法律所禁止的行為，也就是行為人實施犯罪過程中直接使用電腦導致犯罪客體的產生。 中國對於電腦犯罪的定義分做 2 個方面：其一為人對電腦的犯罪；其二為人利用電腦來犯罪，無論犯哪一種罪名，犯罪主體都是行為人，所以電腦在犯罪裡的地位是被界定為工具和對象，再者犯罪行為也必須與電腦有關才能屬之。自網際網路普及之後，與電腦系統結合成為了電腦犯罪的另一項延伸，網路被當作一個場所，甚至被當作一個客體，所以依據電腦犯罪的定義來推論，網路犯罪應定義為：「網路是電腦系統與通訊的結合且具有網際網路特性的犯罪，亦即犯罪者需在犯罪過程中借助網際網路與電腦設備方能達到遂行犯罪目的，稱之為網路犯罪」。網路犯罪的發生與人類的心理意圖和行為有密切的因果關係，因此為了建構網路犯罪的預防必須先探討如何讓犯罪事先得到控制和降低人的犯罪意圖以至於減弱犯罪行為達到事前預防之目的。

第二章電腦犯罪之定義

依我國國內學者之見解,凡電腦不正常使用(如電腦處理、傳遞、保存資料加以不當的操作之一切行為,或為處理自己之資料而擅自使用他人電腦)、資訊之不當取得（不當取得、洩漏、利用電腦處理資訊之結果或是在處理過程中之資料程式等)、破壞電腦（指藉由電腦之物理或韌體破壞而使他人無法使用資料處理之功能）等，均可稱之為電腦犯罪。

國內學者林山田教授將電腦犯罪定義成廣義說、狹義說、以及折衷說等三類：

一、 廣義說:

即泛指所有與電腦科技或電腦系統有關的犯罪,或泛指所有與電子處理有關之犯罪學行為，簡言之，即與「電腦有關的犯罪」,均屬於廣義之電腦犯罪。

二、狹義說:

狹義說所謂的電腦犯罪,則界定為限於財產法益的犯罪，換句話說,即所有與電子資料處理有關之故意且違法破壞他人禪產法益的犯罪行為，如故意竄改、盜取、毀損、無權存取使用其數據資料或電子設備之違法且破壞財產法益等行為。

2.1 網路犯罪分析

1. 以電腦及網路為一般犯罪之通訊連絡工具

2. 以電腦及網路為犯罪之場所

3. 以電腦及網路為犯罪之工具

網路已成為現代人新興傳播工具電腦網路徒有高科技形象

屬智慧型犯罪。

下七類：

1. 及傳佈色情

2. 販賣違禁、管制物品、盜版光碟、贓物、侵犯他人著作權及商標權

3. 利誘人犯罪

4. 網路詐欺

5. 網路

6. 毀謗妨害名譽(偽造文書)

7 駭客侵入與散佈電腦病毒. 網路賭博

2.2 電腦網路犯罪的特性

1. 散布迅速：網際網路具有無遠弗屆、迅速廣泛散布的特性，其影響極大。
2. 身分易藏：網際網路的來源網址可以假造，如阻斷服務攻擊極 難追查。
3. 證據有限：電腦犯罪可能沒有現場、兇刀、血跡、槍彈、血衣 等實體的跡證。
4. 毀證容易：電腦內部駭客程式、不法取得之資料，祇要按下刪除鍵或執行格式化指令，即能於瞬間銷毀證據。
5. 適法困難：然而電腦科技進步日新月異，現在修法解決的，只是過去面臨的問題；網路科技帶來的新問題，往往令立法及執法機構追趕不及。
6. 跨國管轄：網路世界不易分辨你我及疆界，在網路上漫遊世界 輕而易舉，這也造成網路犯罪具有跨國管轄的特性。
7. 偵查不易：以上幾個特性致使網路犯罪不易偵查，甚至無法偵查各國法律與實務對於某些行為是否違法的判斷標準不同（如槍、賭、色情的認定），也使得跨國性網站的非法行為，造成在偵查上困難度。

2.3 網路媒介傳佈色情設立色情網站

一.情交易中心，媒介或自行設立網路一夜情銷售色情光碟影片聊天網站或其他方式進行援助交際自拍、情色貼圖公然猥褻 散播情色資訊於網路聊天室間或公眾領域。

二. 網路販賣違禁、管制物品、盜版光碟、贓物、侵犯他人著作權及商標權在網路上販賣 FM2、頭丸毒品、他禁藥賣槍、路販賣盜版光碟：如俗稱泡麵或大補帖的盜版光碟、電影 VCD 或音樂 CD 等等。贓物仿冒品交易偽鈔

三. 教唆他人犯罪

軍火教父、殺手冊

四. 網路詐欺

網路銷售商品，收錢沒送貨

五. 網路恐嚇：網路千面人

六. 毀謗侮辱 妨害名譽(偽造文書).

七. 駭客侵入與散佈電腦病毒

截取銀行帳號,密碼截取其他個人隱私資料、金融犯罪、木馬式、窺伺資料、破壞或移植、駭客大戰、散佈電腦病毒。

八.網路賭博

在網路上架設網頁，並提供賭博網站之功能，連續公然煽惑不特定之人上網賭博財物犯罪。

2.4 電子郵件及網路使用行為分析

台灣地區 12 歲以下之民眾有 92 萬人曾使用過網路；12 歲 以上之民眾有 1,083 萬人曾使用過網路；總計 0-100 歲之民眾有 1,175 萬人曾使用過網路。

根據調查 台灣網路使用族群中有八成以上的網友曾經使用 Webmail 功 能來瀏覽信箱與收發電子郵件，超過一半以上網友利用標準功能 POP3 及 SMTP 來收發電子郵件 的。

收發電子郵件 emai 已經成了為網路族群每天必須使用的功能之一，以 Webmail 來說，平均每人每 天會檢視電子信箱 2 次， 若是以 POP3 及 SMTP 收 發電子郵件，則是平均每天收發電子郵件一次。

以男性略高於女性，男性約佔 60.73%(583 萬 人)，女性約佔 53.62%（499 萬人)。以「16-20 歲」、「21-25 歲」最高，各佔 94.68%（163 萬人） 90.68%（180 萬人)；其次為「12-15 歲」，約佔 88.08%（113 萬人)；其中，「46-55 歲」之上網比例較 低，約為 35.89%（106 萬人)；而「56 歲以上」之上網比例最低，不 及 1 成。

科技的發展與電腦及網路使用的普及，雖然帶給我們極大的便利，卻也出現了一些利用網路來從事犯罪行為之人，這些犯罪帶給人們的損害，較以往傳統犯罪更是為甚，學者之間便稱此類犯罪為「網路犯罪」。關於「網路犯罪」，因其多為利用電腦系統之操作進而連結至網路，始得在網路上進行犯罪之行為而成立網路犯罪，所以目前多數學者。

認為其係「電腦犯罪」的下位概念或將之與電腦犯罪混為一談，因其認為網路犯罪係於電腦犯罪中藉由網路之管道而達成其犯罪目的之謂，係從電腦犯罪中逐漸衍生出來的一種犯罪型態；而網路犯罪固屬電腦犯罪之延伸，是一種利用網路獨有之特性，而為犯罪手段或為犯罪工具之網路濫用行為。但隨著網際網路的蓬勃發展，連接網路的方式不再由以往的僅藉由電腦設備如此單一，在可見的未來，結合無線通訊 3G，手機、PDA、行動導航系統，甚至是家電用品皆有可能連接上廣大無垠的網路世界，網路犯罪將不再單純是電腦犯罪的延伸。

故「網路犯罪」目前雖為電腦系統與通訊網路相結合之犯罪行為，但其較偏重於網路科技之應用，而具有網路性質的犯罪；也就是說行為人故意或過失所違犯的犯罪行為，應具有網路之特性者，始可謂為網路犯罪；此為與電腦犯罪只偏重於電腦或相關設備之使用及破壞之犯罪行為有所區別。

2.5 分析資料表

分類目的	特點	常見型態	之熟悉程度	偵查難度
以網路罪空間為犯罪場所(被動)	被動性質，引誘吸引一般人進入	網路色情 網路援交 販賣盜拷 網路賭博 網路遊戲 販賣槍械 教授製仿炸彈	高	低
以網路為犯罪工具(特定目標)	針對特定目標予以侵害性質，藉由網路作為犯罪工具	網路恐嚇 網路誹謗 網路詐財	中	中
以網路為犯罪客體(為攻擊目標)	對網路或電腦系統的攻擊性或破壞性	網路入侵散播電腦病毒 網路竄改 SQLInjection	低	高

2.6 網路隱私權維護概念

電腦處理個人資料保護法之修正， 企業定期對員工進行安全教育訓練是必要的，根據公司的安全政策，權衡每個部門所需的訓練程度，針對不同的安全政策，設計不同的安全課程，員工經過訓練後，更能強制執行既定的安全政策，檢視每位員工是否需要接觸機密資料，嚴格限制使用權限，如果確實有業務需求，也應該留下存取記錄以便查核，藉此追溯問題的源頭，必要時企業可以要求員工簽署保密同意書，以避免人為因素導致機密資料遭竊，或是工作流程中產生資安漏洞。

另外一種侵犯他人隱私權的型態是在網路上張貼或公開傳輸他人照片，雖然肖像權的保護案例不多，但其屬於民法人格權的侵犯幾無異議者，隨著日本網站未經過當事人同意張貼他人照片，遭判處侵犯肖像權，網路肖像權問題也成為國內網友熱烈討論的話題，不過國內網路發展較早，已經形成互相尊重的公約，像是日前知名 BBS 站台曾經出現照片風波，站方都會以個人權益為由，迅速刪除張貼照片文章，以保障網友的權益。

是否在 BBS 站上發表意見即進入公共領域，得由他人任意檢視，不受著作權法保護，也放棄隱私權保障？國內的學術網路多數是系統與事務分開，兩者互不相涉，這種體制上的瑕疵容易造成站長群私下處分，不會對外界公開說明原委，更不可能累積經驗形成一種共同監督機制，因此，未來應該更清楚向網民交代隱私權保障的重要性，形

成自律與他律共存共榮的形勢，也讓身懷重任的站長、板主自我警惕。但網友最關心的還是如何利用技術達到保護個人隱私資料，其實這是相當侷限的作法，因為沒有不能破解的防火牆，故正本清源之道仍然是儘量不要在網路論壇提出個人隱私資料。至於在法律上如何規範站長或其他網友偷看使用者私人信件，我國法律採取雙管齊下做法，除了違反電腦處理個人資料保護法外，也可能涉及刑法刪除他人電磁記錄或妨害電腦使用罪。

在網路交易機制中，為了落實隱私權保障，行政院消費者保護委員會訂定「網路交易定型化契約應記載及不得記載事項指導原則」，無論是從事電子商務的企業或個人，倘若外洩消費者個人資料，要負損害賠償責任，單一事件求償金額以 5000 萬元為上限，就算是免費提供交易平台的拍賣網站，也得負連帶賠償責任。業者有責任建立安全交易機制，當消費者告知帳號密碼遺失或遭冒用時，立即停止網路交易，不得拒絕，並應採取相當的保護措施，一旦系統遭到入侵，消保會要求業者不得約定免除賠償責任，且不得約定所有使用消費者帳號和密碼進入該電腦系統後的行為，均視為該帳號及密碼持有人的行為。當消費者與網路業者發生消費糾紛時，業者亦不得限制以本身所保存的電子交易資料為認定標準。

網路中的 BBS 站或是即時通訊軟體既是人際關係和消息來源，也兼有公務連絡的效果，不過也如兩面刃，不管好壞消息、對錯資訊，傳出去的速度都一樣驚人，讓不少使用者只能在安全與自由權衡後作選項，因此，個人隱私權與民眾的知情權維護之平衡。

2.7 隱私權之探討及認知

我國實務見解對於民法上隱私權之定義係參照近年來司法院大法官會議關於憲法上隱私權之解釋，強調人格權為保障人的尊嚴及個人意思自主決定之一種基本權利。此處須辨明者為，侵權行為法上之隱私權乃為私法上之權利，侵害隱私權須負侵權行為責任，並非基於其被肯認為憲法上基本權利，蓋憲法上之基本權對於私人之間並不具直接效力，是以實務上目前仍以憲法上基本權之角度出發，進而發展出民法上之隱私權，尚待斟酌。

其次，我國實務見解目前對於侵權行為法上隱私權之保護範圍，最為主要之概念為:「若非揭露他人難堪之私人事務或造成公眾誤解，隱私權必須以『獨處生活領域』為保障之要件，是以雖為私人活動，然活動之場合卻為不特定人得共見共聞之情形時，則此私人活動因不具有隱密性而欠缺合理之隱私期待。拍攝地點若屬於公眾得自由出入之場所或公眾得共見共聞其行為之地點，要無具有隱密性。因被拍攝者無合理期待之隱私可言，自無侵害其等隱私。」而目前我國學說通說亦普遍接受此一概念，亦即否定公共隱私權之概念及受侵害之可能性。然而，個人生活在群體社會中，應受保護之隱私固須有所界限，亦即對隱私須於主觀要素具有合理期待，以作為限定受保護隱私之基準。

鑒於合理隱私期待法則之抽象化與不確定性，難有統一之判斷標準，本文認為就涉及公共場所或科技工具之相關案件，個人資訊中何

者屬隱私範疇，何者非屬隱私範疇？甚或何者屬高度私密敏感之隱私核心，何者屬低度私密敏感之隱私外緣？或許可選擇從「個人自主決定」之角度切入，以解決目前的判斷困境。

從「隱私權」和「私人的」二者在字源上的關係，不難發覺「隱私」的要求是對私人領域的承認和尊重。與公共領域相對，私人領域是與公共無涉，保留給個人，並由個人做決定的領域。承認此一領域之目的不在於將個人封閉，會給予個人隱藏自己的空間，用以防衛外來的侵擾，而是對個人自主的尊重。個人領域即「不可侵犯的人格」的一部。

這種不可侵犯的人格並非消極地去避免侵害，而是積極地給予自己行為和決定的基礎。因此，侵權行為法上隱私權之核心概念旨在於保護個人在其私生活領域之自主，即個人得「自主決定」其私生活之形成，不受他人侵擾，及對個人資料「自主控制」。質言之，隱私權是對個人領域的事務的控制權，就是個人對於自身事務的掌控和自主。對於隱私權之侵害，指對於這項「控制權」的侵害，即對於「個人自主性」之侵害。此外，隱私權之主體為個人，但亦有擴大及於法人團體的趨勢。其保障範圍包括：「私生活不受干擾」，即個人得自主決定是否及如何自公眾引退、幽居或獨處，而保有自我內在空間；資訊自主，即得自主決定是否及如何公開關於其個人的資料。

基於隱私權之核心概念乃係保障個人對其私生活領域及個人領域內事務之自主與控制，為使個人能夠呈現出多樣化的自我，依不同

的時間、場合對不同的相處對象呈現不同風貌的自我形象，以保障每一個體享有一免於受外界不當干涉的自主領域，則此等事務是否構成個人領域之事務，除以在某特定個案中，被主張應受保護之隱私利益出現之物理空間位置究係公共場所或私密處所為判斷之標準，本文以為似乎亦得以客觀上隱私範圍之界定加上當事人本身主觀認知作為一種判斷標準。蓋隱私本身具備某種主觀之特性，而具有「高度屬人性」，因而每個人對於其個別所認定之隱私範圍及隱私程度，皆會有不同之認定，原則上應依該涉及之權利人之感知自行決定，當事人是否享有合理之隱私期待若僅以客觀上物理性場所地點作為唯一區分，與隱私之概念與個人自主控制保障之特性畢竟有所扞格。並且，以法院所認知之社會整體上對於個人隱私之認識，加以認定某一事項是否屬於隱私之範圍，其實是以社會共同多數之承認或認識加以決定隱私之定義及範圍大小，然而隱私既涉及私人事務，則私人事務之認定涉及每個特定個人對於該事務私人性質之感知，且這樣的感知本來就是最為私人性的，為求對於個別個體自我感知之尊重，隱私範圍之認定應係該個人私人之權限，而非概以「合理之隱私期待」作為「客觀」之判準而交付社會公決之，只要個人能證明該事務係具有個人特徵或與人格發展呈現有密切關連，而該事務其本身又認為應該是隱私，則該事務對其而言即為隱私，而不應以此事務是否為社會認為屬於隱私作為唯一判斷標準。縱使隱私與否之認定委由權利人自行決定之主張，於現實上可能導致社會運行阻滯，然而經濟上之不便不能構成基本人權自身在成立上之否定事由，亦即不能構成否定以權利人個人之主觀為基準自行決定其「私密空間」與「個人資訊」之正當理由。

自合理之隱私期待言，傳統上之看法認為，場所之性質對於是否構成隱私權之侵害呈現有意義的區分作用，而實質地影響了隱私利益之成立與相對應之不同強度。同樣是二人間之談話，在人聲鼎沸的學校操場，或是在下課時間眾人來往的教室，抑或是在夜深人靜四無旁人的研究室，論理上皆應因而相對應出不同的隱私強度，儘管談話的內容可能是一樣的。之所以會如此，是因為當此情況中具體的行為人通常係有意識地認知到其場所所營造出之整體環境，相應著此一認知，行為人因而產生了一定對隱私之期待，並進而為一定之行為。

惟對應到資訊化時代個人揭露於公共場所之行為或影像，此一傳統見解理當因應時代變遷做出不同於以往之解釋。傳統見解認為，行為人於公共場所中，既然有意識地認知到其在該場所所做出之具體行為，將被該場所週遭附近之眾人無障礙地「清楚觀看」甚至記錄著，即因而相對應地對自己身體或行為採取不同之束縛程度或開放程度。例如，個人前往自家巷口之便利商店時，由於其主觀上之認知僅係步出家門數百公尺處，且至多只會遇見附近熟識之鄰居，可能因而採取了較為休閒或甚至稱得上邋遢的穿著打扮，同時可能趁四下無人之際做出些許不雅動作。

2.8 資訊網路安全

網路是電腦蓬勃發展的主要原因之一，網路的內容可深可廣，從最簡單學習的網際網路應用，到進階的網路安全與網路管理，是很長遠的一條路。而網路原理也是許多科系中經常被選修的一門課程。

在現代網路已經成了一般人生活中，幾乎可說是不可或缺的一部份，網路已逐漸的融入每個人的生活中。像現代從網路延伸出來依靠網路發展的就有網路電話、網路傳真機、網路即時訊息、網路視訊會議之類的，這些產品被開發出來後都還會製造其它更龐大的商機，這些也都是因網路的蓬勃發展而出現的。

連網路本身也因時代的進步，也跟著進化，以前電話上網只能用數據機 5Kbyte 的上網速度，到現在家庭幾乎都是寬頻上網如非對稱數位式用戶線路簡稱 ADSL 和纜線數據機，跟網路蓬勃發展初期的頻寬差太多了，頻寬是指在一個單位時間內所傳輸的資料量，通常被視為是判定傳輸資料的重要指標。也可說是，頻寬愈大的單位時間資料傳輸量較大，而頻寬愈小的資料傳輸量則較小。在電腦設備中，大部份的頻寬以 BPS 來表示，即每秒可傳輸之位元數。

網路是不同的單一個體，透過特定資訊傳遞的方法。而一個網路流程是從傳送端拿到準備發送出去的訊息，透過網路環境，傳送到接收端，接收端確認收到正確訊息後，才完成整個網路傳送流程。

而網路又有分成許多種網路，最常在辦公地點看到的是區域網路，區域網路是由比較近的電腦和網路所組合而成的網路區域，如辦公室內的有架起區域網路，就可以分享印表機、分享檔案，使工作更加容易，也可以因多人共用一台印表機，節省成本。像學校的電腦教室、辦公室、宿舍網路，也都各別分為一個區域網路。區域網路的類似又按照資源分享的而有所不同，有分成點對點形態的網路，這種形態的網路是沒有特定伺服器的，在這個網路內每一台電腦都等級都是平等的，可以同時扮演客戶端，與伺服器端的角色。只要分享出資源來，就可以成為伺服器，此種網路有幾項優點，就是沒有特定的伺服器，所以也不需要特定的管理員來管理伺服器。成本低，因為不需要一台專用的伺服器。大部份的作業系統都能支援。有優點就一定有缺點，缺點就是資源分散，管理起來時很不容易。另外一種區域網路是以伺服器為主要架構的網路，在這種形態的網路，所有的資源，也都集中起來由伺服器來決定資源的使用權，此類似的網路由於資源集中管理，所以成本比較高，但也比較安全也比較容易整合區域內所有的資源。

在網路發展初期有三種主要的技術，不過現在的網路大部份都是屬於乙太網路，是目前世界上使用率最高的網路模式。它具有高速且穩定的特性。也普遍為一般人所使用。

網路發展也是有許多學者共同開發研究出來的，也使網路有更多技術使之更穩定、更快速、更安全，網路可說是越來越進步，從有線到無線，從絞線到光纖，這些都是網路時代的進步所展現出來的成果。

資安事情層出不窮，大部分都是人為疏失而導致為居多。網管人員或者是程式設計師能多留意一些，我想駭客要找漏洞來進行攻擊應該是不容易的。多一份留意，少一份危險。

就拿「資通安全學程」的網站來舉例，在伺服器方面，本身會定期的更新修正檔，將系統的漏洞補起來，並且加裝防火牆及防毒軟體來達到有效管控整個系統安全。

在網站安全方面，透過伺服器的一些模組來協助過濾 SQL Injection 的問題，在網站的程式方面會加入語法過濾掉一些會產生漏洞的字或字串。並且在 GET 和 POST 傳輸前會先將資料經過加密器加密，在傳輸到後台再透過解密器解密在進行資料的處理，所以全程都是處於加密狀態，然後 COOKIE 部分也是採用加密技術來加密，並且驗證碼會隨機產生，在一定的時間內會自動註銷，使得無法假冒，較重要的資訊則會採用存在伺服端方式以防駭客取得。

在讓使用者登入的部分會在加上一道防護措施，採用 SSL 的加密技術能在傳輸的過程中受到保護，而且還採前端和後端雙層驗證。即使駭客是透過 URL 來揣測漏洞或攻擊也是不可行的，因為 URL 部分也是有經過加密的，如果駭客使用 URL 的方式來攻擊，經過解密器還是會被解譯成無效的字串。雖然層層的防護，還是防不勝防，必須管理者長期的去觀察和檢察，才能達到最完善的防駭。

最後主講者 他後面示範的用 GOOGLE 來找漏洞的方式對「資通安全學程」的網站也是不可行的。因為每一頁都是須經過認證的，所以沒有照正常的程序登入，是無法看到內容，還會被強制傳回首頁。多一份用心，少一份擔心。

第三章實際案例

案例一:

台東縣刑大昨偵破一起網路詐騙案,除跨縣市拘提或傳喚十二名涉嫌人到案，並查扣電腦主機、帳戶存摺、金融卡、快遞提貨單等犯罪工具；警方調查，以范姓男子為首的詐騙集團，以新興「三角詐騙手法」，冒用正當網拍商家名號，詐取買家購物再轉賣圖利，不法獲利近三百萬元，訊後，依詐欺、偽造文書罪嫌移送台東地檢署偵辦。縣刑大偵二隊屢接獲民眾報案，稱網購付款後均未收到商品，質疑受騙，隨即成立專案小組蒐證，發現就讀北部某大學、有詐欺前科的范姓學生，夥同另十一名共犯，冒用正當商家的名義網路販物，在買家登入其設下的虛擬拍賣商家購物時,一邊要求買家匯款至正當商家的受款金融帳號,一邊向正當商家宣稱已匯款，要求郵寄及詐領買家網購商品，再轉賣圖利。新興「三角詐騙手法」，導致買家匯款後無法收取所購物品,而賣家雖收到了買家匯款,卻將商品郵寄給詐騙集團,兩個月就約有一百一十人受騙，不法所得近三百萬元。專案小組前天清晨動員四十餘名警力分赴桃園、台北等地同步展開拘提，搜索十九個處所，計拘提或通知十二嫌犯到案，

心得分享:

以前要買東西是要到商家的店裡看,但現在的網路方便了也多，許多商家為了消費者的方便,而自己建立了個人的網拍平台,但有歹徒看到商家的龐大利潤動了歪腦經。

歹徒利用了「三角詐騙手法」,讓賣家和買家都透過歹操作，此種詐騙最難防範,除了小心以外,千萬提醒利用交易平台並採用正常交易手續進行,當真的遇上此種詐騙徒的操作,也會有”cow591”交易平台的保障，並會協助受害者提出告訴。

案例二:

台中一名女網友，就是和網友到新竹出遊，結果一上車喝了對方給的咖啡後，就昏迷並遭到性侵。而被控迷姦女網友的呂姓男子，則是被依強制性交罪名，判刑三年八個月。 據了解，台中一名女網友，去年在網路上認識住在南投的呂姓男子，兩人相約到新竹賞花，女網友一上車就喝了一杯呂姓男子提供的咖啡，不料喝完咖啡後就全身無力、昏昏欲睡，被害人接著就被呂姓男子開車載到汽車賓館性侵害得逞。事後被害人在網路中向呂姓男子表達不滿，也向友人哭訴遭到呂姓男子迷姦。由於呂姓網友死不認錯，兩人還在網路上吵了起來，被害人憤而提告。全案法官在審理時，也調閱兩人網路交談的內容，呂姓網友在對話中也坦承自己太急，希望有機會能挽回犯下的錯誤，顯示呂姓男子的確違反被害人的意願，法官因而依強制性交罪名，判處被告呂姓男子三年八個月的有期徒刑。新竹市刑大科技隊指出，每年暑假是網路犯罪的高峰期，不但女網友遭性侵案件層出不窮，也發生不少青少年為了急著賺錢，被騙在網路上販毒；最常見的是網路交友被誘拐而離家出走。警方也呼籲網路交友要特別謹慎，尤其為人父母者，不要以為暑假子女都在家中上網，沒有出門就不會有問題，還是要注意子女網路交友的對象，以免發生憾事。學校及社工一直提醒青少年在網絡上交友時應小心，避免成為網路不肖之徒的獵物。青少年應明白不要隨便向陌生人透露自己的地址、個人資料及自己詳細的生活習慣，因網友不一定百分之百說實話，他們可能會隱瞞自己的真實身分。

心得分享:

不喝陌生人及初次見面人的飲料,即使見面也要保持距離並且攜帶朋友一起出遊,避免單獨出去,發生遺憾,即使是在網路上的交友,不要隨意邀約見面,不隨意給住家資料,聯絡方式。出來見面攜帶2位已上身邊友人,不獨處,去人多並且明亮的地方,例如夜市、商圈,人口密集之地方。

案例三:

民國八十六年九月，某私立大學資訊系陳姓學生，在學校網站建立「無政府份子文件集」個人網頁。他並將國外相關討論群組中介紹各種炸藥製造方法、過程與威力的文章，轉載張貼於個人網頁上，供不特定人觀看、討論。由於各類炸彈或爆裂物非經中央主管機關許可，任何人不得製造，若有未經許可為製造者，即屬犯罪，對於該行為人應依槍砲彈藥刀械管制條例第十一條規定科以刑責，台北地院認為陳姓學生將介紹炸彈等爆裂物之製作方法的文章轉載張貼在其個人網頁上，顯係刺激慫恿他人犯製造炸彈等爆裂物之犯罪，而該個人網頁並未設定密碼，不特定人進入電腦網際網路後，均得任意再進入陳姓學生之個人網頁閱覽上開文章，陳姓學生刺激慫恿之煽惑行為已置於不特定人得以共聞共見之公然狀態，係觸犯了刑法第一百五十三條第一款之以文字公然煽惑他人犯罪，且因其先後多次以文字公然煽惑他人犯罪之犯行，時間緊密，犯意概括，為連續犯，以一罪論，並加重其刑，結果是判決十個月，緩刑三年，並交付保護管束。

心得分享

不能隨意張貼之未授權之文件，必且不能隨意提供別人觀看且分享重要之文件，重要文件要設定密碼，及保護的程式防範措施，文件未經同意許可轉載，屬於竊佔罪，是屬於他人文件要經過他人同意轉載，才能轉載，不能私自轉載，這種行為也是不好喔

案例四:

去年十月七日,台中徐先生接到來自高雄縣警察局員警的電話,並告知徐先生因為利用數位電信聲請之ＡＤＳＬ,公然在名為〝高苑貼圖區〞的情色網站上散佈十多張猥褻圖片,已經觸犯了妨害風化罪,請他到局說明。然而徐先生確實並無前往該網站的事實,對於員警的認定大感不解。在他前往警局接受偵訊,並表明自己是無辜且有請律師協助解決的意願時,員警卻以此罪判的輕、律師花錢、罪證確明、不認罪判重刑等說法慫恿徐先生直接認罪。雖然員警說法讓徐先生心生恐慌,不過為了自己的清白以及往後名聲,然堅持自己是無辜的。在聯晟法網律師群接下此案件後,開始做相關證據的蒐證與整理,而在整個證據中,一項證據證明了徐先生的清白:聯晟律師於徐先生家中蒐證時,發現徐先生的家中所裝設的ＡＤＳＬ上網是以無限網路發射方式使用的,而且住家又住於人口密集的集合式住宅區。經判斷後,應係不詳人士利用無線網路的特性,經由徐先生所裝置之無線發射器,張貼該猥褻圖片。而當初警方是以該貼圖區上所顯示的張貼人ＩＰ位址,往下循線抓人的。然而只單以查詢ＩＰ位址為徐先生所有,就認定徐先生為該嫌犯實為欠妥,按犯罪事實應依證據認定之,無證據不得認定犯罪事實。刑事訴訟法第一百五十四條第二項有明文:「又認定不利於被告之事實,須依積極證據,苟積極證據不足為不利被告之事實之認定時,即應為有利於被告之認定」。最高法院三十年上字第八一六號著有判例,在聯晟律師積極幫忙下,徐先生終洗脫冤屈獲得不起訴處分。

心得分享:

這位徐先生被不明的 IP 位置竊取，以偽造身分公然猥褻圖片，這種行為已經觸犯了妨害風化罪，但是這位不名人士在一個大城市裡面警方也很難找到他的確切 IP 位置，所以用無線傳輸網路時，很容易被不法人士冒用 IP，所以使用網路時，要謹慎的小心附近的住戶，可能會竊取你的 IP 位置。

案例五:

台北蔡先生因熱愛線上遊戲「天堂」,平時除了自己練功賺取天幣及寶物外,亦會從事買賣行為,日前突然發現自己所有的帳號均遭遊戲橘子鎖定,經了解後發現被嘉義縣警方以犯罪嫌疑人為由要求鎖定。不久之後,就接到警方通知要求偵訊,原因是所賣出的寶物為贓物,並將蔡先生列為「妨害電腦使用罪」犯罪嫌疑人。偵訊後發現蔡先生當初登錄在橘子的基本資料並非他本人更加主觀認為有犯罪嫌疑。

由於警方遲遲不將鎖定解除,造成蔡先生許多損失。蔡先生透過網路尋求本網協助,在律師徹底了解案情之後,先陪同蔡先生至警局釐清案情確認他並非犯罪人員之後,順利幫他由犯罪嫌疑人身份轉為證人身份。接著並發律師函請遊戲橘子儘快解開被鎖定的帳號,在本網的律師不斷的協商及努力下,最後也順利幫蔡先生解開所有帳號,帳號被鎖,相信是每一個玩家最深的痛,每多過一天,損失是難以估計的,但由於現在警務繁忙及行政程序的緩慢,玩家若不積極處理,往往要花費許多時日,才能解決問題,在此奉勸各位玩家,若遇到此類問題,一定要主動,不要讓你的權益睡著了。

由於電腦及網路已成為一般人生活上極重要工具,為因應電腦駭客對電腦、網路系統的攻擊,動輒造成嚴重損失,政府在刑法部分新增妨害電腦使用罪專章,專門對付電腦和高科技的犯罪行為,其中３９５條無故取得刪除或變更他人電腦或其相關設備之電磁紀錄,致生損害於公眾或他人者,處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

心得分享:

雖然在網路上面交易是虛擬的,但是有些遊戲幣是可以用台幣來買的,看了上列敘述,那些盜寶人真的很不應該,雖然買家至要得到東西就好,但是賣家只想要賺錢,就會動用點腦經走歪路,跟賣家買的時候沒有確認對方這種寶物是從何處得來的,也不清楚賣家的身分,所以要做好雙方的保障,以免受罪。

案例六:

網路交友詐騙被害人在國際交友網站 imatchi 上，於 98 年 3 月在網站交友認識一男網友，自稱名為陳仁忠、是台中人，在馬來西亞 CCIB 銀行 VIP 部門上班，被害人與這名男網友 MSN 線上聯絡約一個月，先取得你的信任從朋友變成情人，每天在網路或電話中聊天、噓寒問暖、以柔情攻勢(甜言蜜語~說有多愛你~讓你迷失自己)並表現出他思維成熟、穩重、上進、孝順、專情的樣子，而且要求你用視訊給他看，以解相思之苦，使出渾身解數來取得你的好感及信任(佈局 2-6 個月不等)後，告知被害人某 VTP 客人無法參加一項高獲利投資案，謊稱這投資案非一般人可參予，因獲利非常高回收快。

因此，冒險竄改客人資料要被害人投資，一開始被害人不願意，假稱說是為了兩人的將來，且日後可以在一起。在男網友甜言蜜語攻勢之下，被害人勉強湊了 11 萬參加此項投資。今年 4 月 23 日當日被害人在彰化銀行用西聯匯款方式匯了 11 萬台幣(3245 美元)。過了幾天；4 月 29 日馬來西亞 CCIB 銀行 VIP 部門公司的一位自稱是李處長的打來，謊稱說此次獲利金額為 2668 萬，便交代被害人幾件注意事項，其中提到公司幫被害人人負擔了 3%的證交稅；15%的海外投資所得稅。且說金額太大要分三個帳戶匯款，被害人亦給了他三個帳戶，本說要匯款了；卻又說此次獲利金全數匯入台灣的金額太大，怕被台灣當地政府注意，所以要求手續費要被害人自付，被害人本覺得有問題，因為男網友一直勸說下，被害人在 4 月 29 日匯入 267000 元台幣匯給一個他們說是駐台的會計師帳戶(楊景玟)。

之後，有一位自稱是馬來西亞銀行的行員說要匯款了，需先核對被害人資料，確認後，銀行有打來說匯款被退回，因為身分不對，說

是被害人是台灣人不是大馬地區人士，所以海外投資所得稅應為 18%不是 15%，被害人便問那位李處長，他說是我不該給對方我的 ID 讓他們知道被害人是台灣人，他說他有交代，但被害人記得他並沒有說明，後來李處長又說公司要負擔那 3%差額($801000)，但因公司已送出資料，最快的方式就是要被害人這邊把 3%補足，不然公司改資料又會產生一些稅務單位的麻煩，講了一大堆藉口，便要被害人再匯款，此時被害人驚覺有些不對勁，加上被害人並沒有這筆錢，被害人開始懷疑，男網友一直說若被害人沒處理，負擔那 3%差額($801000)，被公司知道他竄改資料，會吃上官司，並且說要被害人一起想辦法湊錢，到 5 月 14 日被害人懷疑自己被騙，打到 165 專線報案才知被騙。

有關女網友遭網路男蟲詐騙的特點：

「網路男蟲」在交友網站施展-「養、套、殺」三步曲將對方財務物搜括一空再落跑。

一、養：被害人常上網交友尋找感情寄託或結婚對象，具有高學歷，有英文會話的能力，且有高薪工作、單身及不少存款，以 ICQ、MSN、SKYPE 或手機作為聯繫工具，表達想要確立戀愛的關係。

二、套：網路詐騙男蟲常隱身在國際交友網站，獲得對方好感後；外約見面，歹徒皆謊稱自己有良好家世背景，在銀行或投資公司任職高階主管，及偽造有巨額存款的存摺，出門開名車進出高檔場所，出手闊綽每天在網路或電話中聊天、噓寒問暖、以柔情攻勢(甜言蜜語~說有多愛你~讓你迷失自己)並表現出他思維成熟、穩重、上進、孝順、專情的樣子，讓你踏入溫柔陷阱騙取被害人的感情及信任。

三、殺：開始編造各種理由(例:投資、資金周轉困難)借錢，藉著被害人對其感情及信任，謊稱可幫其投資高獲利或投資馬會或六合彩等

中大獎，或裝可憐在投資失利或在公事 上出事要被害人幫忙解決，博取被害人的同情及信任要求被害人匯款，甚至更惡劣者在聊天過程中慫恿被害人裸體視訊藉以側錄勒索錢財。多次詐財得逞後發現已無利用價值，藉故疏遠避不見面。

心得分享:

網路交友要小心，這種假借交友、徵婚為幌子詐騙，因涉及隱私女性被害人多不願報案，從而降低犯罪者風險，女性網友最好紀錄該網友的 IP 位址、交談紀錄。避免一對一見面，上網交友應並向家人告知去向、保持聯絡!

對於個人資料的登錄要十分小心謹慎：在網路上儘量避免留下真實姓名、電話、住址、信用卡帳號等基本資料，並對於此類資料的登錄要十分小心。

免單獨的邀約：儘量避免進入聊天室與陌生人一對一聊天，不要隨便允諾網路上網友的單獨邀約見面，記得以匿名身份進入聊天場合。保護自己，不要將個人的照片寄給他人，或藉由網路散佈照片；如果網友傳送任何猥褻或令人覺得不舒服的訊息，千萬不要回應。

遵守網路交友的原則，切勿輕易答應不明人士的邀約，而且要知道利用網路交友彼此都見不到面，對於對方的了解也相當有限，所以，儘量將交往限定在聊聊天通通信的範圍之內，不要涉及金錢往來借貸關係，以免出問題而後悔。

案例七:

「娜娜」99 年 3 月間在 facebook 結識一名自稱 Welling Gordon Jones 男子,經過 1 月網路交友後,該男子佯稱於前往台灣會面途中，停留馬來西亞交易物品，遭馬國海關要求繳交稅金，該男子向受害者借錢,「娜娜」不疑有他，以跨國匯兌（西聯匯款）方式共匯美金 3200 元給該名男子，後來受害者警覺受騙上當。警方指出近來國人遭受活躍於馬來西亞境內，由西非人士（奈及利亞、迦納）組成之詐騙集團詐欺案件日益增加，案情多為國人透過網路平台交友時慘遭詐騙財物與感情。被害人於交友網站上結識國外網友，交往多時後，詐騙分子以各種藉口誘使被害人匯款至馬國，被害人多為高學歷女性，個案損失金額最高多達新台幣 1 千多萬元。

心得分享:

人類不斷的進步，相當的科技也不斷的進步，以前的交友方式都是雙方見面聊天或者書信交換認識彼此,但現在網路的也可以交友，當然也造成現在許多社會案件發生。

這件案件的娜娜或許心想他是外國男士,比較紳士而借錢給他，但出乎他意料，反而被騙了錢。

被騙錢算是小，錢再賺就有了，甚至有些女性而被騙了身體，而留下一輩子不可抹去的陰影。

案例八:

現在成年人受到網路詐騙的話，每次損失的金額都相當高，且許多先進國家都有一樣的狀況！

賽門鐵克諾頓在 15 日發布「諾頓報告」，說明全球網路犯罪研究結果。報告指出：網路犯罪的成人受害者人數降低，但平均錢財損失卻提高 50%。且 48%的智慧型手機和平板電腦使用者未多加設置基本的預防措施，例如裝防護 APP，使他們的個資就像「裸奔」一樣，暴露在風險之中。

更驚人的是，全球一年中因網路犯罪造成的損失，高達 1,130 億美金（折合新台幣超過 9 千億），平均一人損失 298 美金（折合新台幣約 8752 元）在詐騙上！

誰最常受到網路犯罪攻擊？據調查，其中男性佔了 64%，推測可能是男性使用網路頻率較高。且七、八年級生受害人數佔了 66%。

現在大家都有智慧型手機，卻沒有做好資料保護。報告指出，有 48%的智慧型手機和平板電腦都未採取基本的預防措施，例如設定密碼、安裝安全軟體或備份行動裝置上的檔案。

賽門鐵克技術長 Stephen Trilling 表示，現今網路犯罪者，會使用愈趨複雜的攻擊方式，如勒索軟體和魚叉式網路釣魚，賺進比以往更多的錢財。諾頓報告指出，有 49%的行動裝置使用者，工作與娛樂都用同一支手機或平板，這使企業面臨全新的安全風險，因為網路犯罪者可隨時竊取公司的重要資訊。

賽門鐵克台港區總監許淑菁表示，行動裝置在生活中扮演的角色越趨重要。根據諾頓報告顯示，近一半受訪者表示，睡覺時也離不開手機。然而，消費者只注意做好電腦安全防護，對於智慧型手機和平。

心得分享:

現在人手上手拿每人一支手機,科技發達不肖業者利用一些不明軟體與不明網站來利用這個軟體與網站能賺錢。不肖業者首先穿著正式,在利用網路的發達來拉攏人們的貪心與你約在咖啡廳裝作著很高尚然後和你說一堆別人公司真正努力成功的案例來吸引你能賺多少錢而要你簽下不肖業者假裝的公司來要你付錢給它們導致許多人一時的貪念而上當輕者而被騙了幾萬塊重者傾家蕩產。但這種手法已經被識破很多次了,扔然許多不肖業者繼續用這種手段來欺騙人們無知的心。

案例九:

在德國漢堡一個名為 Chaos Computer 的俱樂部, 有一個俱樂部成員剛完成一隻新型態的病毒-----這隻病毒可以找出 Internet 用戶的私人銀行資料, 還可以進入銀行系統?將資金轉出, 不需要個人身份證明, 也不需要轉帳密碼。這是科幻小說嗎? 很遺憾它並不是。 當使用者在瀏覽全球網站時, 這個病毒會自動經由 Active X 控制載入。Active X 控制可搜尋使用者硬碟, 來尋找 Intuit Quicken 這個已有全球超過九百萬使用者的知名個人理財軟體。一旦發現 Quicken 的檔案, 這個控制程式會下轉帳指令,並將這個指令混在其它同樣在等待轉帳的使用者中, 當這筆款項支付時, 仍然沒有人知道他是誰。 有一個 ActiveX 控制稱之為"Exploder" , 在安全層面中廣被討論。它會關閉微軟的 Windows 95, 且如果你的電腦有能源保護的 BIOS 時, 它還會自動關掉電腦。儘管這個感染並不像一般大問題一樣嚴重,但這個控制功能卻說明了這些新病毒的控制能力有多強。任一型態的工作站, 不管是 Mac、PC、Unix, 或是 VAX, 甚至即使在工作站及 Internet 之間有防火牆在, 仍然得冒這樣的危險。 更嚴重的, 像這樣具安全破壞性的, 不只是 Active X 而已, 由昇陽電腦所開發的 Java 語言也被認為有類似的情形出現。由 Java 所撰寫的 Application macros、Navigator plug-ins 及 Macintosh 應用程式等都可能包含惡性程式碼。

心得分享:

今日的病毒有超過五萬種病毒存在,然而常見的病毒只有一百種左右。

「電腦病毒」的意思就是電腦程式,與一般電腦程式不同的地方,是病毒程式會惡意地複製自己,將病毒程式植入其他電腦檔案。有這種舉動的程式,便可稱是「病毒」。電腦病毒在特別的設計下,電腦使用者無法察覺,造成電腦系統的損害或使用者的困擾。

電腦病毒是我們應要注意也是要防範的,病毒的分類有很多種,是輕微的病毒很嚴重的病毒還有的是特定系統的病毒,病毒侵略的地方有很多種方法,有的是只要一開機,就很有可能會中毒,到時候你的電腦就必須要讓專業人士送修,有的會讓硬碟受損而電腦就讓你無法讀取到檔案,有的會讓電腦系統進不去,最慘的是連開機都有問題的吧,到那時候真的只能請人來修理了,而非常多病毒是由電子信箱傳開來,甚至會藉由電子信箱裡傳去給它裡面所有聯絡人的電子信箱依此下去擴散效應就會讓很多人受害,只能靠電腦本身的防火牆能不能夠來阻擋看看,這些故意散撥病毒的人。

所以保護自己的電腦的方法並不要被病毒入侵,只能夠不要開啟網路上來路不明的檔案,若需要開啟請先掃毒或者是開啟 E-mail 前,需注意是否為不明的郵件,必要時,開啟仍必須要做掃毒工作。

第四章網路與電腦犯罪之預防

網路犯罪在二十世紀末興起，在二十一世紀如雨後春筍般的盛行，犯罪者利用網路透過一個前所未見、前人無法想像的虛擬空間為相關不法行為致影響現實空間的犯罪行為，而傳統的犯罪防制方法對於網路犯罪雖亦有部分可資適用之對策，惟畢竟網路空間實迥異於現實空間，故傳統犯罪防制措施實已不無法完全預防網路犯罪。

網路空間的產生雖造就了新的人類文明與生活，卻也形成傳統犯罪預防策略所不能防制的黑暗角落，以致網路犯罪預防工作漏洞層出不窮，終致網路犯罪不斷增加及不斷擴大，故網路犯罪防範對策的研究，為面臨網路犯罪泛濫今日的我們所必須正視的重要課題。

預防更勝於治療，在了解電腦、網路犯罪之偵查、追訴之困難與限制後，我們更應該著眼於建立全民正確使用網路的概念，避免更多因無知而被害的案例發生。

4.1 網路犯罪預防之概念

學者林宜隆與學者黃讚松根據對網路使用者的調查與網路犯罪問題分析，形成的網路犯罪預防概念，經由預防概念而提出的預防機制運轉模式。

首先是「有明確的網路行為規範」，以使網路使用者能遵守網路共同規範，在網路上何種行為可為，何種行為被禁止，網路行為越明確，網路使用者對於網路評價越有共識，當違犯共同價值標準時，接受懲罰。

其一是「減網路犯罪動機」：網際網路經由良好教育宣導與環境設計，使網路使用者易於遵循網路規範，當網路規範機制不足時，網路使用者在普通的情境下就容易變成犯罪者，藉由抑制犯罪動機消除潛在的網路犯罪。

其二是「快速有效的嚇阻」：對於已有犯罪的傾向與實行網路犯罪者而言，迅速有效的查緝嚴懲，對實施犯罪的可收到特別的預防，對一般潛在的犯罪者而言，亦可收到一般的預防效果。網路犯罪因具有網路特性限制，在預防工作上會比一般傳統犯罪更難做到預防成效。

4.2 網路犯罪預防之策略

層次一：

找尋促使網路使用人為犯罪行為之一般因素，採取一般性的防範措施用以改善網路社會中的環境，使一般的網路使用者，不會因為網路外在環境的設計不當或不良，而成為網路使用者為犯罪行為之直接因素。是以本層次的主要目的在於改善網路環境，防範於未然（如實施網路分級制度、裝設過濾性軟體及提高網路犯罪破案率等）。

層次二：

針對網路社會中具有犯罪可能性的網路使用者，先行預測其網路犯罪之危險性，並事先採取相關措施加以輔導。本層次之主要目的在於利用網路犯罪預測之手段，輔導對於可能為網路犯罪行為之使用者予以輔導，以減少網路犯罪的發生（如病毒程式設計者、駭客網站成員或以網路為報復目標之網路使用人等）。

層次三：

對已為網路犯罪之使用者，藉由刑罰的威嚇作用，與刑事司法體系的相互配合，用以矯治網路犯罪者，以避免其再為網路犯罪之行為；此種行徑同時進一步達到威嚇潛在犯罪人的效果。本層次之主要目的在於藉由刑事司法之作用，以收矯治犯罪人及預防犯罪之效果。

上述三個層次為網路犯罪預防模式的基本策略，然而在網路犯罪預防工作的實踐上，經常需要有多方面的配合才得以奏效，在此種模式下所採取的各種防預措施或策略，亦如傳統犯罪預防方式一般，並沒有單一的方法可以解決，亦即不可能以單一政策而達到所有的預防效果。勢必得對於不同的個案、環境，給予不同的處遇，或是數種方法策略合併綜融，才能達到預防網路犯罪行為發生的效果。

4.3 電腦犯罪預防之策略

這幾年電腦犯罪已成為新型態的犯罪模式，當大家都還在摸索「電腦犯罪」的同時，它已藉由隱密性、多樣性及殺傷力強大等特質而對社會造成傷害，類似上述之案例也不勝枚舉，研究者以犯罪偵防觀點為出發，如后提出幾點，以供如何預防電腦犯罪及偵查實務的幾項策略

一、 司法人員要加強教育訓練及增加軟硬體設施，應具備相關知識，方有能力處理類似案件目前所移送之電腦犯罪案件，大多是由具備電腦專業知識的專人負責，但未來這類案件將大幅增加，亦不限於某些地區，因此所有司法人員皆應具備相關知識。

一、 電腦犯罪偵查與預防亟需民眾協助，全民參與 因為網路的無遠弗屆，網路咖啡屋的處處林立，均增加犯罪者更大的隱匿空間，若無民眾熱心提供線索，單以有限的偵查人力與設備，恐有實際難處，所以電腦犯罪的偵查與預防須把民眾納為一份子。

二、 為預防網路咖啡屋成為電腦犯罪的溫床，應儘速訂定管理辦法政府管理速食店、網咖或是露天咖啡業者等有提供無線網路者，可考慮採取會員制，以掌握使用者資料；並要求業者保存使用紀錄，以利事後追查；裝設閉路電視並錄影，以提供必要時查對身分。

三、 隨時更新電腦作業系統的漏洞，並安裝適當的防火牆、防毒軟體加強電腦安全措施，修補系統漏洞，隨時檢查稽核紀錄，以防止駭客入侵電腦系統所造成的損害。

四、 協調國內網路業者加強用戶認證及保留完整使用紀錄，以供檢警偵查之用。

目前國內網際網路服務提供業者所開發的撥接帳號產品，使用者在一般便利商店皆能購得來上網，勿需登錄使用者身分資料，所以不法人士便能利用此管道上網，或登錄假資料，或冒用他人身份登記，因此常有檢警執行搜索時發現地點或對象不對而撲空之情事發生，若能從源頭即給予較嚴格的把關，相信亦能有效的控制以及嚇阻潛在的電腦犯罪者。

第五章結論

在近兩三年間，電腦網路在國內快速擴張成長，網路使用者激增，但多半還是以年輕男大學生為主，使用者多居住在北部地區，而且多在住處上網。熱門的網站，以大分類來看是以資訊、術數和休閒為主，在以個別網站排名，則前三十名當中有二十個網站是和色情與命相有關，也就是說「性」和「命」是上網者最感興趣的。從這些調查和統計，我們看到了資訊網路在臺灣的發展還不成熟，而更有濫用這個高科技工具從事性命相關的非理性乃至反科學性的活動。

不過，在經過對查尋資料、網路論壇、社會運動等網路現象進行進一步研究分析後，我們發現資訊網路對臺灣社會確實有積極的影響。限於研究的時間和規模，我們並不能對網路對社會文化的衝擊做具體的評估，但從一些所收集到的資料，在網路上，學術界已經建立了許多資料庫，例如中央研究院的電子化古籍已經上網，這些電腦化的資料不只對學術研究和文化的發展極有助益，一般民眾也可以透過網路，查尋古籍的資料。這種知識性資訊的實質而快速的成長是網路化社會發展的重要基礎之一。在網路論壇上，人們開發了一個新的而參與者相互平等的對話和討論的機會，對某些議題和問題的討論有正面的積極作用，不過，由於在網上的言論多較為簡短，推論不完整，論壇的意義就在本質上有了顯著的缺陷。網路可以是有效的社會運動的動員工具，國內在網路上推動社會運動已經形成了風氣，但在實際動員效果上如何尚難定論。只是透過支持者在網路上連署，可增強參與者的認同和投入。最後，關於算命，網路上一方面反映了社會上實際的需

求，在另一方面卻也推波助瀾，多少造成更進一步的流行。至於色情網站的盛行，對社會固然有負面的影響，但由於需求和制度上的缺陷，恐怕一時還不易解決。

關於電腦網路對文化衝擊的研究還處於起步階段，本計畫僅有半年的時間進行，並不能做很深入的分析和評論。其間，尚有諸多問題須經更多研究才能克服，更積極地規劃並執行有關電腦科技與人文社會相關連之研究才能真正有所得。

參考文獻

網路犯罪分析

http://www.internet-recordor.com.tw/crime.html

我國網路犯罪案例現況分析

http://jitas.im.cpu.edu.tw/2003-2/6.pdf

案例

http://www.libertytimes.com.tw/2013/new/sep/28/today-south4.htm

案例

http://tw.news.yahoo.com/

電腦犯罪預防

http://www.im.cpu.edu.tw/