網路交易犯罪之偵查要領—以網路詐欺犯罪為例

Investigation Principles of Cybercrime — By Example of Internet Frauds

林宜隆
中央警察大學資訊管理研究所
桃園縣龜山鄉大崗村樹人路五十六號
paul@sun4.cpu.edu.tw

楊鴻正
台北市政府警察局資訊室
(110)台北市中正區延平南路九十六號五樓
yangyeh@webmail.tmpd.gov.tw

摘　要

電子商務的發展是未來不可避免的世界潮流，雖然利用網路交易的方式改變了以往傳統交易方式的限制，為我們的生活帶來很多的便利性，但也衍生了一些難以避免的問題，尤其是日益嚴重的網路交易犯罪問題，它已對國家社會的經濟活動構成重大的威脅，甚至可能戕害國家的繁榮發展。而隨著網際網路的普及運用也連帶使犯罪的手法更新，網路交易犯罪事件也越來越多，而能被發現或被查獲定罪的案件恐怕為數甚少，這就是我們所深以為憂的，因此偵查資訊犯罪專責警力的建立與偵查能力的提升已是刻不容緩的事。

關鍵字：網路交易犯罪、網路詐欺、電子商務、網路犯罪偵查、網路監聽

壹、前　言

在政府大力支持與民間企業積極參與下，電子商務成了國內目前最熱門的話題之一。藉由網路的特性，業者與消費者在彈指間就能完成一筆一筆的交易。這樣的便利與效率，給予買賣雙方無限的憧憬與期待。然而，隨著現實案例的增加，各種可能阻礙電子商務市場發展的問題，也一一浮現出來。其中最引人關切的，以網路交易犯罪莫屬。網路交易犯罪對電子商務市場的發展，可說是一個最大的威脅。如果無法建立買賣雙方對彼此的信心，所謂「潛力無窮的電子商務市場」，恐怕永遠只是大家心中美好的想像。

在中共、美國「駭客攻防戰」進行得如火如荼之際，台灣的駭客則因為入侵網路銀行盜領他人存款而遭警方逮捕。這起國內首宗的駭客入侵網路銀行案件，也暴露了網路銀行安全性的問題。

台北市警局刑警大隊電腦犯罪專責組於本（九十）年五月一日偵破國內首宗駭客侵入網路銀行，盜領客戶存款及洗錢案。失業男子邱志宏利用網路咖啡店電腦連接網路銀行，破解客戶密碼，盜領存款百萬餘元轉帳到人頭戶洗錢，再使用金融卡提款轉存到兒子帳戶。辦案人員指出，網路新興的電子銀行，主要是金融機構方便客戶轉帳，程式設計上，使用者只要輸入身分證字號的代碼及自行設定的密碼，兩組數字號碼符合即可開啟帳號進行轉帳。

由於嫌犯邱志宏曾是網路銀行客戶，他進入網路銀行索取認證後，點選任何一個姓或公司行號首字，網路銀行就會在螢幕上列舉所有該姓氏客戶名字及公司行號名稱。氏接著點選其中一名客戶名字，就會顯示客戶名字及身分證字號。問題出在部分客戶為圖方便及習慣性，常將身分證字號，取其中四個數字列為密碼，邱志宏就使用隨機抽樣、重組，測試出客戶密碼進入客戶的帳戶動手腳盜領。

根據邱嫌供稱，他因曾在網路銀行開戶，了解轉帳只要輸入身分證字號及密碼即可轉帳，由於他知道許多存款者所設密碼常是由身分證字號中隨便抽出四個數字當密碼，他才不斷由身分證字號測試出密碼進行盜領、洗錢。

台北市刑大將邱嫌依詐欺、偽造文書罪嫌移送偵辦。警方另查出邱已破解兩家科技公司及十名客戶密碼，隨時可進行盜領。警方指出，網路銀行開設時間不久，安全機制可能尚未成熟，存款人轉帳所設密碼應與身分證字號不同，以免讓歹徒有機可乘。

由以上案例可以得知，目前網路交易環境的安全性實在非常脆弱，也可以說是非常不堪一擊，其原因除了使用者毫無安全意識之外，電子商務的業者對於網路安全機制的建立是否達到令人放心的程度，亦是吾人所最為擔心的。

本文擬從國內外網路交易犯罪之現況談起，並根據前述可能之犯罪原因加以探討司法機關或警察機關對此專業知識犯罪之偵查方法與要領，以提升我國司法警察打擊網路交易犯罪之能力，健全國內日益蓬勃發展的電子商務環境。

貳、網路詐欺犯罪

現實世界中因交易所生的犯罪問題，在網路交易中恐亦難避免，可能產生的網路交易犯罪包括詐欺（例如虛設電子商店廣告售物藉機詐財）、贓物（新修訂的刑法第 323 條已將電磁紀錄列為竊盜罪的客體，因此購買他人所竊取的數位商品即犯本罪）、賭博、販賣槍砲彈藥刀械毒品或猥褻物品、媒介色情、偽造文書（例如擅用他人名義與人締約）、侵害商標與著作權（例如販售的數位商品係違法重製物）、販賣公平法第 20 條所定的仿冒商品、與違法吸金（銀行法第 29、125 條有處罰明文）等。惟吾人認為電子商務將成為今後網際網路最為重要的活動之一，電子商務市場亦是各國政府目前最為重視的網路應用，在以上的網路交易犯罪類型中尤以網路詐欺犯罪對於電子商務的傷害最為嚴重，因此我們有必要對於網路詐欺犯罪的型態清楚瞭解。

儘管各國政府都在努力打擊網路交易犯罪，但是根據美國消費者聯盟 2000 年１１月公佈的報告指出，美國消費者因為網路詐欺犯罪所損失的金額，還是從 1999 年的每人平均 310 美元，增加到 2000 年（9 月為止）的 412 美元。另外依據美國聯邦貿易委員會(Federal Trade Commission)2000 年 10 月 31 日所公佈的「掃蕩網路之詐欺犯罪報告」表示，網際網路上十大網路詐欺犯罪手法包括下列十種：

一、網路拍賣。類型包括：

(一)拍賣人要求消費者在網路上競標，消費者在得標付款後，卻未收到產品。

(二)消費者收到商品，但所得實物與拍賣時賣方宣稱者相差甚多。

(三)拍賣人偽裝為其他消費者，一同參與競標，藉以哄抬最後得標價格。

(四)拍賣人在消費者得標後，以其他理由要求加價。

二、網路服務。類型包括：

(一)提供原本免費的服務而收取費用。

(二)收取線上或網路服務費用，但未提供服務。

(三)收取線上或網路服務費用，卻提供不實服務。

三、信用卡詐欺。類型包括：

(一)欺騙信用不佳的人申請發卡。商家承諾消費者可以輕易獲得信用卡，但在申請者提供申請信用卡相關資料，並依約預付頭期款後，卻可能從未收到信用卡，還必須負擔因為別人「盜刷」信用而產生的負債。

(二)對針對商家的詐欺。這是目前美國所有申報的網路交易犯罪案件中所佔比例最高的一種。根據美國 Meridien 顧問公司研究調查指出，1999 年全球網路購物金額約計 $150 億美元，但包含消費者拒付部份之總詐欺量約達 $15 億。由商家及軟體公司組成的打擊網路詐欺組織 Internet Fraud Prevention Advisory Council 則表示，網路的信用卡詐騙情形依商業類別不同，比例可從 2%到達 40%不等。一般網路上詐騙的多半是能兌換成現金或可經由網路傳遞的商品，例如貴重寶石、禮券、消費性電子商品等。根據 CyberSource 的估計，銷售數位商品的網站有高達 30%的詐欺交易額。

四、國際數據器撥號

某些成人網站業者，藉由提供網友免費上網瀏覽色情內容廣告做引誘，截斷上當網友原來的數據機，轉接上昂貴的國際長途電話。

五、提供免費網頁取得信用卡號碼

這樣的案例亦多與色情網站有關。色情網站業者會在網頁上宣稱，網友可以免費瀏覽網頁，但要網友先輸入信用卡號，以證明自己已成年。網友在輸入卡號後，即會陸續接到高額帳單。

六、非法多層次傳銷

有些網站會以「不須費您太多的時間或金錢，就能賺得優渥之報酬之工作機會」，或者「提供您一個網際網路相關事業的賺錢途徑」等說詞，在網站上刊登或以電子郵件寄發廣告。事實上，這些大部分都是非法多層次傳銷業者所偽裝之商業機會。

七、物美價廉的旅遊機會

業者在網路上刊登或利用電子郵件寄發廣告，推銷俗又大碗的旅遊機會。消費者親到當地後，才發現實景實物與網路上宣稱的有很大的差別。原本預期的豪華郵輪，可能只是一艘港口的拖船；廣告中美景如畫的渡假勝地，可能只是一個與世隔絕的荒涼村落。如果消費者想升級或更改行程，則必須付比平常更多的費用。

八、商業機會

店家利用電子郵件或在入口網站上刊登廣告，宣稱他們有目前最時髦的快速致富方式，如在世界貨幣市場上套匯賺取無止境的利潤；這些簡訊中通常都描述著各種輕鬆賺錢的機會。

九、投資

業者會以網路廣告或電子郵件的方式告知消費者，某項投資將可獲得可觀的投資報酬率，且宣稱沒有任何風險，以吸引投資消費大眾。這些信函中對投資本身描述模糊，但卻強調高報酬率。在此類案例中，業者多是利用後加入者的錢支付給較早加入者，使先加入者相信投資方法確實有效，而鼓勵他們投資更多。最後如果沒有足夠的錢繼續刺

激收入，整個投資計劃終將失敗，損失的仍是一般投資人。國內目前也已出現數起網路詐騙集團，假借知名金融構名義，於網路上宣傳短期資金周轉業務，而實際上卻為從事地下錢莊高利貸放款行為，從中不法牟利。

十、中獎與獎品。類型包括：

(一)要求中獎者先付稅金再領獎品。贈品贈獎郵件告知消費者必須先繳交『郵寄包裝費用』或『15%的所得稅』，方可領取獎品。但最後消費者往往收不到中獎的獎品，或者所收獎品的實際價格低於消費者之前所付的稅金或郵寄包裝費。

(二)贈品贈獎廠商要求消費者先付費加入成為會員，才能得到贈品。

(三)引介他人加入俱樂部會員。業者利用網路告知消費者可免費成為俱樂部會員，但必須先拉其他人加入該俱樂部。

參、網路交易犯罪之類型及案例

當我們展開雙臂歡欣鼓舞地迎接網路時代來臨時，網路金融犯罪的問題似乎是我們不得不重視的隱憂。我國財政部於一九九九年五月二十五日公布「個人電腦銀行業務及網路銀行業務服務契約範本」，開放銀行申請開辦電子銀行業務。自契約範本公布後，已有十多家銀行向財政部提出申請。一時之間，我們似乎可以預見未來網路銀行之榮景。但是，最近剛剛爆發了入侵網路銀行盜款百萬及以前曾發生過的冒牌銀行網站等網路犯罪事件，這種新式的犯罪手法，防不勝防，令我們眼花撩亂。看來網路時代，金融業者的責任是愈來愈艱鉅了。除了駭客入侵之外，金融業者還需提防電腦病毒感染、客戶資料外洩、網路洗錢、網路詐欺等各式各樣的網路交易犯罪。以下簡介著名的網路交易犯罪的類型與案例，藉以提醒網路業者、網路使用者、金融業者與消費者防範網路交易犯罪。

3.1 駭客入侵

一、國外知名銀行遭入侵案：

一九九五年，國外的花旗銀行遭一群蘇俄的駭客入侵，損失一千萬元。除了金錢的損失以外，其後遺症是，有六家花旗銀行的對手銀行，立刻鎖定花旗銀行的前二十大客戶，遊說他們轉換銀行，這些銀行所持的理由是他們的電腦系統比較安全。

二、中共銀行駭客案：

兩個中國大陸的網路駭客入侵銀行的網路系統，竊取人民幣 260,000 元（約合美金三萬一千四百元）的金額。據報導指出，這兩個駭客是兄弟檔。哥哥郝金龍（譯音），是某工商銀行的會計，管理該銀行的網路系統。他們用不同的戶名在該銀行的某分行開了十六個帳戶。並且在銀行電腦終端機植入一個控制的裝置。去（民 87）年九月，他們利用該裝置，將虛擬存款 720,000 人民幣（約合美金$86,975）電匯進入銀行帳戶內。之後，他們成功地從該銀行的八個分行領出真實的鈔票--人民幣 260,000 元。後來這兩名駭客遭江蘇省的楊州法院（Yangzhou Intermediate Court）判處死刑。但死刑的判決引起國際嘩然，質疑是否過於嚴厲。

三、券商遭入侵案：

此案並非典型的網路駭客案，其癥結點在於券商的股市即時查詢系統有很大的漏洞。周姓嫌犯涉嫌藉由證券公司的股市即時查詢系統，取得各大法人、大戶的委託買賣及成交資料，再通知類似「股友社」的特定對象，以低於法人委賣價「跟單」，造成受害法人必須以更高價才能買進或以更低價賣出特定股票，相對的讓特定對象從中獲取差價暴利。

四、美國股票交易所與 NASDAQ 的網站疑似遭駭客入侵：

美國股票交易所與 NASDAQ 的網站於一九九九年九月中旬遭自稱「聯合借款持槍歹徒」（the United Loan Gunman）的團體入侵，該團體留下訊息說它的企圖是要「讓股價戲劇性地上揚，使投資人高興，希望投資人在他們的賓士車上的汽車標語寫著『感謝 ULG』」。但是，NASDAQ 的官員對於該網站是否遭入侵並未確認，也未否認。

五、國內某銀行遭入侵之傳言：

在一九九八年十一月三十日、十二月一日國內各大報報導指出據傳位於台北市的某銀行遭駭客入侵，被盜領五千萬。但其後皆未見後續報導。此傳言亦未獲證實。

3.2 信用卡犯罪

一、在網路上截取他人信用卡號於電子商店消費：

很多發卡銀行常提醒持卡人，勿在網路上輸入信用卡號消費。為的就是防止持卡人的卡號被他人盜用。發卡銀行的立意良好，也反映了一般人對於交易安全的疑慮，乃是推行電子商務必須克服的難題。

實務上，根據台東地方法院檢察署研討電腦網路犯罪法律問題研討記錄，其曾就網路上截取他人信用卡號碼，並利用該卡號在網路上購物的行為所觸犯的刑責加以討論。初步的結論以及高等法院檢察署的研究意見認為，應成立竊盜、行使偽造私文書及一般詐欺的牽連犯。

二、利用信用卡號產生器產生卡號，公布在網路上供人下載：

曾有國外駭客破解了通行於世界的信用卡號編排邏輯，而且把信用卡號產生器（Credit Wizard 1.1）程式公布在網站上，供人自由下載。使得不肖人 士得以透過該信用卡號產生器程式獲取卡號，再以冒用之卡號上網購物。有一個曹姓被害人所持有的卡號就連續被盜刷，經其向發卡銀行申訴，發現該筆帳只有卡號相同，卡的有效日期及持卡人基本資料姓名、地址等卻完全不同。要注意的是，即使將卡號公布在網路上的人本身並未利用卡號上網購物，但其將卡號公布在網路上供人自由下載的行為可能觸及我國刑法一百五十三條煽惑他人犯罪罪嫌。

3.3 網路詐欺

一、冒牌銀行網站：

據報載，林姓嫌犯涉嫌拷貝中國信託商業銀行的網路銀行網頁，貼在網路公司免費提供的網頁空間，再超鏈結接到其他提供搜尋引擎的公共服務網站上。國內多個公共服務網站都被林姓嫌犯登記超鏈結連接，民眾只要在搜尋引擎上查詢中信商銀，就會同時出現兩個中信商銀網站，在二選一狀況下，民眾有一半機會連接到嫌犯之冒牌銀行網站使得三十多名不知情的中信客戶進入冒牌的網站中，被騙走密碼。中國信託商業銀行發現該冒牌網站後，立即主動提報檢調單位調查，所幸並無客戶遭受實際損失。

此一偷天換日的網路犯罪手法為國內首見，也不易防範。雖然這並不是銀行本身遭受入侵，而是消費者遭受網路詐騙的案子，但是會影響消費者的信心。此案例可能觸及的法律如下所列：

(一)刑法三三九條第二項詐欺得利罪，意圖為自己或第三人不法之所有，以詐術得財產上不法之利益或使第三人得之者。可處五年以下有期徒刑、拘役或科或併科一千元以下罰金。林姓嫌犯利用設立冒牌的網路銀行網站使被害人中信客戶陷於錯誤的行為，為一種「詐術」。

(二)刑法二百十條偽造私文書罪，偽造私文書，足以生損害於公眾或他人者，處五年以下有期徒刑。林姓嫌犯設立冒牌的網路銀行網站的行為，涉及偽造中國信託銀行的文書。

(三)著作權法九十一條第一項重製罪，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，得併科新台幣二十萬元以下罰金。林姓嫌犯擅自複製中國信託銀行的網頁，此為擅自重製的行為。

對於消費者來說，日後在網路上進行任何交易，除了螢幕的畫面內容之外，更要小心檢視瀏覽器所顯示的網址，是否有異狀。

二、網路詐騙炒股票案：

美國有一男子名叫 Gary Hoke，他是 PairGain 公司以前的員工，擁有該公司的股票，他想要賣掉這些股票獲取暴利。因此他就在網路上散布假消息，聲稱 PairGain 公司將被一家以色列的公司以一億美元收購。這個杜撰的消息使得 PairGain 公司的股價暴漲，直到他被逮捕。美國法院判決他必須賠償九十三萬美元以上的金額給因他的假消息受害的投資人。

三、騙取帳號，高價販書案：

網路上曾經出現三封信，A 信的內容是高價販賣「駭客防衛手冊」。B 信的內容是有人自稱讀了該「駭客防衛手冊」後，成功破解了多人的帳號與密碼，他不但將這本書大大地吹噓了一番，並且提供一些已破解的密碼，供人測試。C 信的內容是撥接帳號大贈送，只要在網路上填一些資料，即贈送免費帳號。

其實，這三封信都是出自同一個人的手筆，其目的是要詐騙網友以高價來買這本書。他想藉由 B 信來讓人誤以為讀了這本書，就可以成功破解盜用他人密碼。而其所提供的已破解之密碼，並非根據這本書的敘述破解得來。這些破解的密碼的來源是 C 信。C 信告訴網友撥接帳號免費大贈送的好消息，但要求網友填寫將來此免費帳號所要用的密碼。

一般會上網看到此消息的人，多半已有帳號，而多數人如果擁有兩個帳號，為免麻煩，會取相同的密碼。因此很多人就乖乖地把他們在其他帳號的密碼填上，密碼於是就輕易洩漏出去了。此案觸犯了刑法三三九條普通詐欺罪。這個網路詐騙案利用的是一般人的惰性與貪小便宜的心裡。

四、網路購買燒錄機變烏龍茶案：

有人在網路上販售便宜的燒錄機，因為網路傳播快、散布廣的特性，很多網友信以為真花錢購買，寄來的卻是烏龍茶。此案所觸犯的也是刑法三三九條普通詐欺罪。

3.4 存假鈔、領真鈔

據報載，有一蔡姓嫌犯以一比三的代價（例如一萬元真鈔可以購買三萬元偽鈔），向他人購買偽鈔。他順利將偽鈔存入無人銀行自動櫃員機，帳款入帳之後，迅速至其他櫃員機，以提款卡領出真鈔。該行為構成刑法新修正條文三三九條之一，「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」。

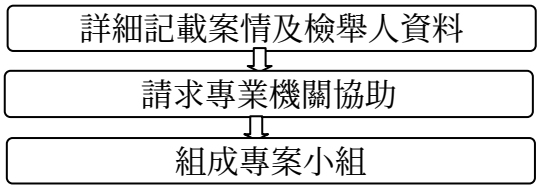
肆、網路交易犯罪之偵查要領

在一般的犯罪偵查過程中，必須循一定之法則，按步就班、循序漸進，以蒐集情報和現場處理為基礎，運用科學方法和技術，進行清查、核對與鑑定，汰蕪存菁，然後深入分析研判，期能發覺偵查線索，確定偵查方向，訂定偵查計畫，進而佈署分工，採取適當之偵查行動，以迅速發現事實真相，藉以確定犯人及犯罪事實。

網路交易犯罪也是電腦網路犯罪的一種，因此一般偵查電腦網路犯罪之程序及要領在偵查網路交易犯罪案件時也同樣適用、二者大同小異。不過由於網路交易犯罪具有某些特殊性，因此本文擬將在偵查網路交易犯罪程序中特別應注意之事項詳加介紹。

4.1 受理報案

有關「受理報案」程序之處理流程如圖一：



圖一：「受理報案」程序之處理流程圖

網路犯罪開始實施偵查的原因不外乎分為主動發現與被動接受報案檢舉兩部分，與一般傳統刑事案件相同，偵查機關主動巡邏發現犯罪比例偏低，絕大多數犯罪均藉由民眾向警察機關受害報案或發現檢舉，但網路交易犯罪此種現象似更為明顯，而且可以說幾乎所有網路交易犯罪案件的偵查開端都是來自被害民眾或金融機構、公司企業的受害報案。

一、詳細記載案情及檢舉人資料

許多的網路交易犯罪是由電腦玩家所為，有的電腦玩家會自成一個小集團，共同研究及實施電腦犯罪。然而常因感情因素或分贓不均，以致以電話相互向警方告密。遇此情況，受理報案人員除應詳細記載其所述案情，並盡量套出密告人之真實基本資料、口音、年齡等，以利追查。

二、請求專業機關協助

網路交易犯罪案件之偵查常有高度之技術性，因此在較先進之國家，常規定偵查機關遇有網路交易犯罪案件時，須先通報其他機關，由專家共同處理。以免一般警察機關土法煉鋼，延誤時機或毀損證據。

在我國，網路交易犯罪之處理程序與一般犯罪案件並無不同，因此實務上只有在遇有偵查困難時，才會主動請求其他機關，例如資策會、銀行公會、會計師公會或電腦公會協助調查，實際上網路交易犯罪常具有高度之技術性，如果能夠有其他機關之指導，破案之機會應大為增加。尤其是對於大型電腦之搜索扣押、電腦資料真偽之判讀、以及如何蒐證及扣押才不致嚴重妨礙電腦系統之正常運作，這些工作都不是一般偵查人員所

能勝任的，因此有必要請求專家之協助。

不過，選任專家時，除應重視其專業素養外，並須注意其立場是否中立。如果是選任被害人或被告一方之人員來擔任，都應注意其立場及可能之動機，否則其可能為了袒護一方而插入不明指令，或將資料刪改，或是故意略過重點。即使被選任之專家並無任何不法行為，也可能因其立場而使當事人雙方有抗辯電腦資料真偽之藉口。

尤其犯罪人為掩飾其犯行，可能會將電腦資料銷毀或加密，銷毀的方法可以物理方式為之，例如將磁碟燒毀；也可以電腦技術方式為之，例如將資料刪除、格式化、存入新資料以覆蓋原資料、或是將檔案 WIPE 等，此時就必須借助電腦專家的專業知識來解決或挽救資抖。

三、組成專案小組

由於網路交易犯罪案件在我國實務上所發生的案例還不是很多，而且一般基層警察對電腦原理之認識亦多不充分，一般之偵查人員未必能夠勝任或迅速進入狀況，因此有必要組成偵查小組，其成員應包括會計師、電腦專家、稽核人員、通訊專家及電腦法學專家。欲延攬此類專家，可向電信局、資策會、銀行公會、電腦公會等單位請求協助。

我國警方目前目前對於偵查電腦犯罪之常設小組，雖在刑事警察局已成立專責打擊資訊犯罪之偵九隊，而在縣市警察局及台北市、高雄市各分局亦成立電腦犯罪專責組，惟都還是任務編組，且除了刑事局偵九隊人員較有電腦專業知識且對電腦犯罪之偵查工作較有經驗之外，其餘縣市警察單位所成立之電腦犯罪專責組人員均係由一般刑事偵查人員與資訊室人員來共同組成，或僅有偵查經驗或僅具電腦知識，實在無法立即勝任當前的電腦犯罪偵查工作。反觀，在歐美電腦較為普及之國家，多在中央警察單位設有專門打擊電腦犯罪之專案小組。例如法國巴黎刑警局即成立「調查資訊技術作弊處」，其主要任務為調查資訊處理、傳輸、儲存等電腦舞弊行為，此外還提供其他機構之技術支援，並負責培訓警方之專門偵查人員。另外美國聯邦調查局設有「電腦分析及回應小組」專門擔任有關電腦鑑識之工作。

4.2 犯罪情資蒐集與案情研判

一旦確定電子交易犯罪存在且經警察機關受理報案，案件即進入偵查階段，網路交易犯罪偵查的首要步驟，即在蒐集與該犯罪案件有關的所有資訊情報，並依據所獲得的資訊研判案情。此階段偵查主要目的係在研判作為確立偵查基礎之案情內容，其不斷從所獲得的資訊研判案情，再從案情研判中發現所需資訊反覆循環進行，直至釐清所有案情疑點為止。

網路交易犯罪通常蒐集的資訊情報主要有下列三類，主要提供者則來自負責管理該作業系統或應用系統、網址、電子郵件帳號之網路管理者與網路服務提供者（ISP），系統網路管理者與 ISP 業者之配合，顯然為網路交易犯罪偵查成功的重要因素：

一、電腦稽核紀錄（Log File）：包括使用者帳號、連線 IP 位址、起訖時間及使用時間等。

二、客戶登錄資料：申請帳號時所填註登記之基本資料，包括姓名、聯絡電話、地址等。

三、犯罪事實資料：證明該犯罪事實存在資料，包括本文、螢幕畫面、原始程式之列印等。

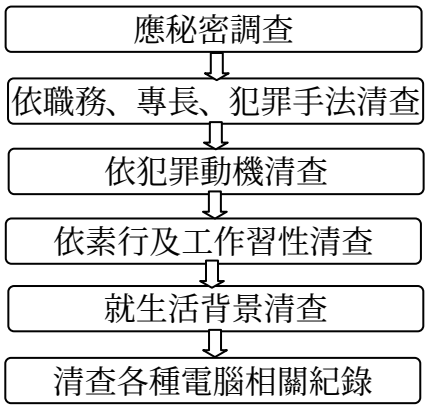
該資訊情報不僅為引導偵查進行之重要依據，亦為日後控訴犯罪嫌疑者之法庭證

據，故偵查人員對於證明該犯罪事實存在的犯罪事實資料亦應儘可能蒐集，並可作為於嫌犯住所搜索扣押所獲物證比對之用。此外，對於系統網路管理者、ISP 業者與其他案件關係人的案情訪談，瞭解可能的犯罪嫌疑者，亦為報資訊來源之一。

從所蒐集的情報資訊中，即可研判分析本案係屬於何種犯罪類型，並進而瞭解犯罪嫌疑人之職業身分、動機目的、犯罪手法等，以縮小犯罪嫌疑人之範圍，並有助於偵查人員於實際案例偵辦中，迅速正確研判案情與犯罪嫌疑人可能範圍。

4.3 追查犯罪嫌疑人之要領

有關「追查犯罪嫌疑人」程序之處理流程如圖二：



圖二：「追查犯罪嫌疑人」程序之處理流程圖

一、應祕密調查

由於網路交易犯罪極具隱密性，犯罪之證據亦容易被銷毀，因此偵查時應避免逕行傳訊可疑人物，而應祕密調查，以免打草驚蛇，使嫌犯警覺後立即湮滅證據或逃逸。

祕密調查的另一個好處是可以提高被害人配合的意願。網路交易犯罪的受害者大部份均為銀行、證券公司或大型企業，這些機關或公司最重視企業形象及信譽，許多被害的企業為了顧及顏面及公司形象，都希望偵查機關能為其保守祕密，如果偵查人員大張旗鼓，被害之企業恐怕不願意合作，甚至會湮滅相關證據，以保護自己，而且從此以後對於偵查機關不再信任，而自行採用其他自保或自救的方式來加以因應。

二、依職務、專長、犯罪手法清查。

三、依犯罪動機清查。

四、依素行及工作習性清查。

有網路交易犯罪或其他前科者再犯之可能性極高。另外，舉止異常、行為詭異或工作隱密者，都可能是在進行網路交易犯罪或其他方面之電腦犯罪。

五、就生活背景清查。

在生活方面有下列之情況者，是網路交易犯罪之「高危險群」：

(一)財務發生困難者。可能會因此鋌而走險。

(二)生活奢侈、支出與正常收入不成正比者。可能已挪用公款。

(三)對組織心懷不滿者。例如認為升遷不公、不受重視或待遇過低，可能會對組織報復。

(四)生活遭受重大挫折者。例如離婚、喪失家人等。可能因情緒低落而意志不堅。

(五)自命為電腦天才而輕視他人者。可能將電腦犯罪視為有趣的挑戰。

(六)經常跳槽者。可能是有不良之素行而遭解僱。

(七)無故自願放棄升職者。可能是害怕升職後無法繼續掩飾犯行。

六、清查各種電腦相關紀錄

(一)文書記錄。包括各種原始書面資料、電腦報表。

(二)錄影記錄。可過濾可疑之進出人員。

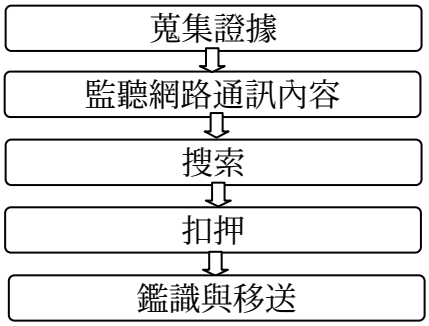
(三)電腦記錄。

(四)分析稽核軌跡。

一般大型之網路多安裝有稽核軟體，其能產生稽核軌跡(audit trail)，記錄下任何重要之網路活動，包括使用者進入電腦之時間，所取用之資料、檔案、程式，由哪個終端機操作、印出哪些報表、何時離開系統、以及哪些行為被拒絕。循著這些電子指紋，就可以找出究以何人之名義所為，使用者來自系統內部或外部。

4.4 蒐集、搜索及扣押電腦資料證據之要領

有關「蒐集、搜索及扣押電腦資料證據」程序之處理流程如圖三：



圖三：「蒐集、搜索及扣押電腦資料證據」程序之處理流程圖

一、蒐集證據：

在發現可疑嫌犯後，最重要的是蒐集證據，以作為日後逮捕及起訴之依據。在網路交易犯罪案件中，對一般實體證據之蒐集，其要領與一般之犯罪案件並無不同，惟在蒐集電腦資料證據時應特別注意下列事項：

(一)電磁資料之證據能力

電磁資料是否有刑事訴訟法上證據能力，在海洋法系之國家爭議已久。由於海洋法系國家多由陪審團認定事實，陪審團則由一般民眾臨時所組成，未受過專業之法律訓練，容易受誤導，故對於證據力較為薄弱，或易於偽造之證據，均予以排除，陪審團不得將此類證據作為形成心証之依據。由於電磁資料多係直接輸入，並無原本，而且電磁資料如遭刪改，極難發現，因此易使陪審團形成錯誤之心証，故有人認為電磁資料證據應無證據能力。

不過我國係大陸法系國家，事責之認定由法官依自由心証為之，而法官乃受過嚴格法律訓練之專家，不易被誤導，故刑事訴訟法對證據能力之設限極少，電磁資料之證據能力法律既無明文排除，其具有證據能力應無爭議，惟其證據力之強弱則由法官自由認定。

(二)持續監控

如果不法行為是連續或繼續進行，應持續監控追蹤。許多電腦玩家在嘗試突破安全措施時，都是持之以恆，此時除非可能對被害人產生立即而明顯之危險，否則不宜立即

變更安全措施、斷線或是予以警告，以免打草驚蛇，又有些網路交易犯罪的手法例如資訊竊聽法、模擬交易法都必須要利用相當長的時間才能完成其犯罪行為，對於這些行為應利用網路管理軟體持續監控，以便蒐集更多之線索與證據，作為追蹤及起訴之依據。

二、監聽網路通訊內容

以監聽電話通訊內容來作為偵查犯罪利器的作法，在我國行之已久。法務部為了解決監聽在刑事訴訟法上地位之曖昧，並防止政府機關或私人濫行監聽，已於「通訊保障與監察法」明定其程序及要件，以保護人民隱私權，非法監聽並得處以刑責。

八十八年六月二十二日立法院三讀通過「通訊保障及監察法」。這個法主要規範的對象是執法單位，目的是要透過種種法律規定，使通訊監察制度化，有所制衡，不致浮濫。但為了更有效保障人民通訊秘密的自由，也明訂了一般人違法監察他人通訊的刑罰。

所謂「通訊監察」簡單地說，是指用截收、監聽、錄音、攝影、開拆、檢查、影印或其他類似的必要方法來得知他人的電信（如電話）、郵件、書信、談話、言論等內容。但為避免過度侵犯人民隱私，特別規定不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。隨著網路科技日漸普及，網路也是現代人常用的通訊設備之一。網路犯罪也日漸猖獗，而網路監察是網路犯罪偵查上的重要技巧，若要進行網路監察，依此法第三條第一項規定，通訊包括「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。」，則網路監察應可適合此條文規定，而納入「通訊監察及保障法」的規範。

為了使通訊監察不致浮濫，「通訊監察及保障法」設下一些限制，以規範執法人員，重點約略如下：

(一)要件嚴格：並不是所有的犯罪偵查都可以實施通訊監察，唯有重大的犯罪，方可，例如：最輕本刑在三年以上有期徒刑的罪、詐欺罪、引誘容留未滿十八歲者為性交易...等罪。除了必須是重大的犯罪之外，還必須同時符合以下要件：危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者。

(二)書面監察原則：實施通訊監察，必須有通訊監察書。究竟誰有權核發通訊監察書呢？原則上是檢察官與法官。比較特別的是，國家安全情報工作機關首長為了避免國家安全遭受危害，可以監察外國勢力或境外敵對勢力的通訊，如果通訊的一方在境內設有戶籍，則應先經最高法院檢察署檢察官的同意。

(三)透明化原則：執行機關於監察通訊結束後，應即報請通訊監察書核發人許可，通知受監察人。

(四)若執法人員違法則重罰：執行或協助通訊監察的公務員或從業人員，如果假借職務或業務上的權力、機會或方法進行違法監聽，會被處以六個月以上五年以下徒刑。

除了執法機關以外，依法規定電信事業及郵政機關（構）有協助執行通訊監察的義務，而且其通訊系統應具有配合執行監察之功能。此法案施行後，業者若不協助執行監察或其系統不具備配合執行監察的功能，則會被交通部處以新台幣五十萬元以上二百五十萬元以下罰鍰，若仍不遵行，會被連續處罰，甚至撤銷許可。

另外此法對於徵信業習以為常的監聽行為亦訂定相關的處罰規定，凡意圖營利而違法監察他人通訊，可處一年以上七年以下有期徒刑。而若不是意圖營利，而違法監察他

人通訊也會被處以五年以下有期徒刑。

對於進行通訊監察的相關程序雖然已有規範，不過以監聽電腦通訊內容作為偵查方法，在我國偵查機關尚無聽聞，可能是因為偵查人員多半對電腦一知半解，加以實務上受理電腦犯罪案件數量極少，因此未曾採用。「通訊監察及保障法」亦無明確規範，似乎電腦監聽已淪為不法份子之專利。

實際上監聽電腦與監聽電話具有相同之功效，都是打擊犯罪、蒐集證據的利器。許多電腦犯罪的資料都是以電腦資料的形式來儲存或傳輸，為了蒐集證據，法官或檢察官固然得簽發搜索狀搜查電磁資料，但直接搜查容易打草驚蛇，其要件及程序也較監聽嚴格，因此在案情不明朗或證據不充份之情況下，宜以監聽之方式來蒐集電腦資料。惟須注意監聽前應先獲得檢察官或法官之授權，以免觸法。

三、搜索

搜索是一種強制處分，其可分為對人之搜索、對物及對其他處所之搜索。在電子交易犯罪案件中，對人與處所搜索之要領與一般案件相同，故我們不再贅述，本文僅就電腦系統搜索時之應注意事項加以介紹。

(一)申請搜索票

搜索又可分為要式搜索及不要式搜索，前者須由法官或檢察官簽發搜索票始得執行；後者不須搜索票即得逕行執行。大部分的電子交易犯罪案件都是事後才被發覺，屬於非現行犯之案件(刑事訴訟法八十八條)；檢察官或法官也甚少親自搜索(刑事訴訟法一二九條)；此類案件也多不構成緊急拘提之附帶搜索要件(刑事訴訟法一三一條)，因此絕大多數之案件須要申請搜索票才能進行搜索。

由於大部分之法官或檢察官對電腦均極為陌生，因此要說服其簽發搜索票，就必須先向其解釋電腦之相關理論，此時如涉及較深奧之理論，不妨由電腦專家為之，才能節省時間，事半功倍。尤其依刑事訴訟法第一二入條規定：「搜索票應記載搜索之處所及物件。」搜索之客體如涉及艱澀之專業名詞更需要電腦專家之協助，才能記載清楚。

(二)執行搜索應注意之事項

由於電磁紀錄極為脆弱，可能一不小心便將其毀損或變更。例如電磁紀錄一經磁化，其內容即消失殆盡，因此不可使其靠近磁鐵或Ｘ光機等會產生磁場之物件；又暫存於隨機記憶體之資料如尚未儲存，電源一經切斷，其資料便隨之消失，因此須確定所有暫存區之資料均已存檔，才能關機；又例如有些軟體有定時自動儲存之功能，即使其內容未改變，但經自動儲存後，其原始日期亦會被當時之日期取代，因此，在調取檔案時應特別注意其原始日期和時間。此外，為保護資科完整性及原始性，在執行搜索時應注意下列事項：

1.管制現場

一經實施搜索應立即控制現場，避免閒雜人等隨意進出，被搜索物件之所有人固然依法得在場(刑事訴訟法一四八條)，但為防止其趁機湮滅或變更證據之內容，應將其與被搜索之物件隔離。

2.切忌隨意操作電腦

電腦犯罪具有高度之隱密性，大部分的電腦犯罪案件都不易找出犯罪之第一現場。如果發現犯罪之現場(多為電腦之所在地)，應由電腦專家從旁協助，切忌隨意動手操作電腦，否則容易因誤觸指令或陷阱而將證據毀損。有些檔案係以隱藏檔之方式儲存，或

是經過加密，這些情形都需要電腦專家協助。此外最先動手操作電腦之人在訴訟程序中常會被傳喚，以確定原始電磁資料之狀況，因此應詳細記錄其進入電腦後之相關作業情形。

四、扣押

(一)相關證物應一併扣押

除了電磁資料外，現場附近之相關物件例如小紙條、列印報表、磁碟片、相關文件、及所使用軟體之磁片，如有必要，均宜一併扣押，以便抽絲剝繭，全盤了解。尤其電磁資料及相關文件之內容通常極為龐大、難以在現場一一清查過濾，此情況宜將全部之電腦系統扣押，待日後再行清查。

不過在執行扣押時，亦應考量物件被扣押後對所有人可能產生之不便與困擾。許多被害人不願意配合調查之理由之一，便是害怕偵查單位會濫行扣押，致使其業務無法順利進行。因此務必衡量扣押所得利益與損害是否合乎比例原則。如非必要，應盡量以複本代替；扣押後如認為已無扣押之必要亦應立即發還。

(二)製作電磁資料之副本

電磁資料多係直接輸入，並無原本，電磁資料如遭竄改，極難發現，如遭消磁，即無從回復。因此，為避免電磁資料在偵查或審判過程中因故意或過失之原因以致遭到毀損或變更，扣押後應立即備份封存，以作為日後比對之用。

備份的方法包括將資料印出及複製至其他磁片、磁碟或磁帶。備份時最好由立場超然之電腦專業人士為之，並由嫌犯、被害人或在場人共同確認，以免日後滋生爭議。

(三)妥善搬運及保管電磁資料

電磁資料極為脆弱，如經消磁即無法回復，因此不應靠近磁性之物品；又磁帶或磁片發霉或潮濕，即難以讀取，因此應置於防潮之容器。在搬運及保管之過程中應置於防碰撞之容器，不可只以紙袋或塑膠袋封存。

(四)訊問嫌疑人及證人

由於網路犯罪常涉及電腦之專業知識，一般偵查人員未必了解，因此，訊問嫌疑人或證人前宜先向電腦專家諮詢，以了解案情之癥結及重點；訊問時專家不妨在場指導，以便更能深入了解案情。

五、鑑識與移送

(一)鑑識：

有關網路交易犯罪案件數位化資料鑑識應注意事項：

1.重大特殊案件之電腦證物遭毀損、刪除、格式化或經加密無法解讀，必須將證物送刑事警察局資訊室鑑識解析。

2.鑑事前應先將重要資料備份以完整保存證據，必要時可全部備份。

3.電腦鑑識時應於備份資料執行非破壞性鑑識，必要時得以原始資料鑑識解析。

4.如電腦資料、檔案或證據已遭刪除或格式化，應還原被刪除或格式化的資料、檔案或證據。

5.如電腦資料、檔案或證據被隱藏，應還原被隱藏的資料、檔案或證據。

6. 如電腦資料、檔案或證據被設定密碼，應將所設定之密碼解密。

(二)移送：

警察機關偵查網路交易犯罪案件，於全案調查完畢後，應將全案移送管轄法院或檢察署辦理，有關移送工作之相關要領如下：

1.移送報告書之填寫應注意事項如下：

⑴犯罪嫌疑人之各項資料應詳填，如未能確定其姓名者，可先不予記載，於查明後再行補移送。

⑵關係人：應載明刑事訴訟法上之關係，如告訴人、告發人、證人及被害人、共犯等。

⑶犯罪時間：應載明犯罪之啟訖時間、以定追訴時效。

⑷拘捕時間：隨案移送案件，應載明到案日期及時間。

⑸犯罪地點：凡犯罪行為地及結果地均應記載。

⑹犯罪事實：應簡要敘明犯罪經過情形及據以認定之證據理由。

⑺破案經過：敘述發覺犯罪經過及偵查破案情形。

⑻所犯法條：由於網路交易犯罪為一新型犯罪型態，許多行為尚無法律條文可加以規範，所認定移送之法條最好先請示檢察官或相關電腦法律之專家學者，以免引用法條錯誤。

⑼對本案意見：就犯罪嫌疑人之犯罪情節輕重、坦白陳述案情與否及是否具有悔意等情形均應詳敘記載。

⑽附送：載明附送人犯、文件資料、電腦設備及贓證物品等，如數目繁多，應另附目錄清單。

2.對於人犯移送應注意事項如下：

⑴一般所查獲之網路交易犯罪嫌疑人均為非現行犯，惟其犯罪情形易對社會經濟造成傷害，所以對於犯嫌之移送與否，應先請示檢察官，以符刑訴法之規定。

⑵人犯解送應視案情使用適當之交通工具，並派遣適當人員解送，亦應注意解送沿途之交通安全及犯嫌之人身安全，以免衍生不良事端。

⑶對於長途解送人犯時，應顧及嫌疑人之名譽及安全，同時對於膳宿之問題亦要特別謹慎小心。

3.對於證物移送應注意事項如下：

⑴由於我國法院或地檢署並不無多證物庫之空間可供存放犯罪之贓證物，因此常常要求警察機關對於大型贓證物要自求保管，必要時再移送法院或地檢署，因此對於涉及網路交易犯罪案件所查扣之證物是否隨案移送，應先請示檢察官，以免徒勞往返。

⑵對於電腦或主機之移送，應使用原設備包裝，以避免受損影響其證據力，並小心使用適當之交通工具及謹慎拆裝搬運。

⑶對於磁碟片及光碟片等高感光儲存媒體之搬運，應避免長時間至於強光、高溫、磁場附近及灰塵場所。

對於網路交易犯罪案件之偵查程序與要領與一般刑事犯罪之情形大同小異，不過因為網路交易犯罪屬高度智慧型犯罪，亦屬一般警察人員所未熟知之高科技犯罪，因此仍有許多偵查要領與一般刑事案件不同，所以對於日漸增多的網路交易犯罪案件，身為打擊犯罪的警察人員就必須瞭解偵辦此類型犯罪案件的要領與程序，才能真正作到保護民眾生命、財產、安全及維護社會治安之職責。

伍、結　論

高科技的犯罪，就必須有高科技的警察人員來進行偵查；網路犯罪在無人可管、無人會管的情況下，肆無忌憚地穿梭在網路空間中，面對這些網路犯罪的人士，若無取締、追捕的能力與人力，勢必造成網路犯罪者更加無法無天、網路業者不堪虧損而警察士氣大挫之情形，更形成國家、社會的不安，經濟及政局的動盪，因此加強網路犯罪專責人員的人力素質及偵查能力絕對是必要且必然的趨勢。

電子商務的發展是未來不可避免的世界潮流，雖然利用網路交易的方式改變了以往傳統交易方式的限制，為我們的生活帶來很多的便利性，但也衍生了一些難以避免的問題，尤其是日益嚴重的網路交易犯罪問題，它已對國家社會的經濟活動構成重大的威脅，甚至可能戕害國家的繁榮發展。而隨著網際網路的普及運用也連帶使犯罪的手法更新，網路交易犯罪事件也越來越多，而能被發現或被查獲定罪的案件恐怕為數甚少，這就是我們所深以為憂的，因此偵查資訊犯罪專責警力的建立與偵查能力的提升已是刻不容緩的事。

宏碁集團龍偉業總監曾經表示，網際網路帶來的是人類科技典範的轉移。這應該是繼機械革命後，影響人們生活最大的一項發明。網路的虛擬特性，給予了網路使用者無限的憧憬與期待。然而，當商務交易市場隨著科技列車躍上網路，毫無保障的虛擬空間，卻讓網路交易犯罪行為的溫床，使得 B2C 商務市場發展受到嚴重阻礙。本文建議，除呼籲業者與消費者自律及自我保護之外，相關法制建設亦應及時趕上科技發展之腳步，國內應成立偵查網路交易犯罪或資訊犯罪之專責警力，並加強電腦、網路、電子商務等方面的知識，以提升偵查網路交易犯罪的能力，建立業者與消費者對網路交易安全的信心，才能促使電子商務蓬勃發展，開創台灣成為擁有「資訊奇蹟」美名的國家。

參考文獻

[1] 林宜隆，“網路警察火線出擊”，*資訊與電腦*，1998 年 8 月號 217 期：頁 69-76。
[2] 林志峰，“論電腦紀錄之證據能力及證明力”，*司法周刊*，1995。
[3] 林宜隆，*網際網路與犯罪問題之研究*，桃園，中央警察大學，2000：頁 229-253。
[4] 林佳蓉，“網路詐欺知多少？--淺談網路詐欺之現況及消費者與業者因應之道”，網路犯罪防治網站：網路詐欺篇。
[5] 尚青松譯，*電腦判客*，天下雜誌，1994。
[6] 莊忠進，*電腦犯罪偵查與立法之研究*，1994：頁 26 及頁 35。
[7] 陳文雄，“電腦犯罪之預防與偵查”，中央警察大學，*研究所碩士論文*，1995。
[8] 張維平，“我國網路犯罪現況分析”，網路犯罪防治網站：網路犯罪總論篇。
[9] 張維平、李相臣，“我國網路犯罪發展趨勢”，網路犯罪防治網站：網路犯罪總論篇。
[10] 楊再華，“網路的安全管理與控制”，*網路通訊雜誌*，1992：頁 51。
[11] 蔡美智，“電腦駭客入侵的法律問題”，*資訊與電腦*，1998 年 8 月號 217 期：頁 63-68。
[12] 蔡美智，“一邊喝咖啡，一邊搶銀行--電子金融犯罪案例簡介”，*資訊與電腦*，1999 年 11 月號 232 期：頁 88-91。
[13] 褚劍鴻，*刑事訴訟法論*，台灣商務印書館，1992。

[14] 趙森嚴、林吉鶴合著，*犯罪偵查原論*，桃園，中央警察大學，1985：頁 63-73。

[15] 鄭厚坤，*犯罪偵查學*，桃園，中央警察大學，1986：頁 99。

[16] 內政部警政署，*犯罪偵查規範*，內政部警政署印行，1999。

[17] 聯合報系，“聯合新聞網站”，社會新聞相關報導，九十年五月一日至五月七日

[18] Marc D. Goodman, “Why the Police Don't Care About Computer Crime”, Vol 10, Number3, Harvard Journal of Law & Technology, Summer 1997.

[19] David Icove, Karl Seger and William VonStorch, *Computer Crime*, O’Reilly & Associates, Inc. 1995：P175-194.