研議網路詐騙防範措施委託研究計畫
期末報告

※本研究爲TWNIC委託財團法人資訊工業策進會科技法律中心研究，研究內容並不代表TWNIC立場

中 華 民 國 九 十 六 年十二 月

目 錄

圖目次

表目次

1. 前言

在科技發展初期，為使新興科技得以順利發展而不受到阻礙，政府及相關產業界人士往往多從產業推動的角度思考，期使利用新興科技發展出各種創新應用服務，便利人民的生活，提升產業的競爭力。然而，對於相關科技可能帶來的負面問題，卻有意或無意的忽略，惟有到了該新興科技遭到不法人士的濫用而對社會造成影響或衝擊時，社會大眾才開始注意到本來即存在的負面影響，以致於錯失了犯罪預防之先機。網際網路的發展與應用即是如此。層出不窮的詐欺手法，讓網路應用環境亮起紅燈，打擊網路犯罪因此成為各國政府目前頭痛的議題。

網路科技對執法單位帶來的最大挑戰，即是網路對犯罪者的遮蔽效果。傳統詐騙行為的發生，如金光黨利用調包方式騙取錢財，仍需透過面對面方式進行；在電話發明與普及後，大多數的詐騙行為開始以電話為工具。此時的詐欺手法，可說仍具有相當的屬地性，警方可透過清查地緣關係，透過當事人對所接觸的人、物之記憶，輔佐以查察電話號碼查緝犯罪。行動電話的興起，其可漫遊移動之特性，加劇了詐騙行為之發生；近年來更因為網路興起，讓現代的詐騙者得以透過偽造的網頁或是透過電子郵件形式寄送詐騙信件，誘使使用者自動交付帳號密碼，以後續進行詐欺轉帳或恐嚇之行為。由於網路科技具有可遠端遙控、可匿名性與可設定自動化操作的特質，讓歹徒得以更少的人力與物力，在不需要與被詐騙人面對面接觸的情況下，對更多的民眾進行詐騙行為。這類犯罪也因為分散深入到每個家戶、每個使用者信箱中，而更加難以防備與查緝。如本研究所欲探討，俗稱的「網路釣魚」(Phishing)詐欺，即為目前網路上方興未艾的犯罪手法之一。

網路釣魚詐欺手法多變，但由於其基本架構仍以一個虛設的網站為主軸，也因此外界或有誤解，認為此類詐欺的成因與網域名稱註冊機制有所關連。為釐清爭議，協助建立我國網路秩序，本研究報告擬先透過案例蒐集、分析，掌握不同網路釣魚的技術與手法，與目前各界提出可能防範策略。在完成資料初步研析後，再透過實務訪談方式，掌握實務見解，參照資訊先進國家（美國）對於網路釣魚詐騙事件發生之因應策略、相關通報機制建立之討論，最後從我國現行法制架構思考評估我國推動網路詐騙事件通報機制平台之可行性與作法，以供相關單位建立打擊網路釣魚詐欺犯罪之參考。

2. 網路釣魚之定義

所謂「網路釣魚」詐欺，目前只是一種通稱，實務與法律上並沒有明確的定義與用法；甚至這類犯罪手法在各國的認知與詞彙指涉範圍亦不相同。例如美國實務多稱為「身分竊盜」(Identity Theft)；英國常見的名詞為「身分詐欺」(Identity Fraud)；另外也有用「網路釣魚」(Phishing)、「帳號接管」(Account Takeover)或「帳號劫持」(Account hijacking)等名詞代稱這類的犯罪手法，以其主要態樣在取得潛在被害者的帳號密碼而稱之[1]。

我國新聞與資安實務界多以「網路釣魚」稱之，取英文Phishing，與Fishing發音相同。網路通說以為此字源自「飛客」（phreak）和「釣魚」（fishing），係指利用社交工程及資訊技術以竊取電腦使用者身分和金融資料，再於線上進行身分偽冒之犯罪行為[2]。另根據反網路釣魚工作小組(Anti-Phishing Working Group，以下簡稱APEG)的定義，網路釣魚是利用偽造電子郵件與網站作為誘餌，愚弄使用者洩漏如銀行帳戶密碼、信用卡號碼等個人機密資料[3]。

本研究綜合各方見解與實務犯罪手法後以為，雖然大量的電子郵件與偽造網站仍是這類犯罪最常見的手法，但其行為態樣已不斷演變，犯罪者甚至已經從被動等待使用者連線上網，到主動購買關鍵字廣告以誘騙使用者點擊，或利用真實網頁漏洞夾藏惡意程式等方式作為蒐集使用者個人敏感資料的手段。這類犯罪的興起與氾濫，就是利

---

[1] Internet-related Identity Theft, A disscussion paper by Marco Gercke, project on Cybercrime, Council of Europe, 22 Nov 2007, http://www.coe.int/cybercrime, 最後到訪日：2007年11月30日。

[2] 參見賴榮樞，資訊安全的迷思，http://www.microsoft.com/taiwan/technet/columns/profwin/17-security_myths.mspx，最後到訪日：2007年7月31日。

[3] 反網路釣魚工作小組(Anti-Phishing Working Group，APEG)是一個由業界與學界自發性成立之國際性打擊釣魚犯罪之組織，成立的目的在於打擊利用偽造電子郵件進行網路詐欺，包括誘騙合法帳號或身分資料等偷竊行為，目前已有超過250個企業會員及1000家技術廠商加入該組織。參見網址http://www.antiphishing.org/。最後到訪日：2007/3/28。

用在網路環境下，使用者身分難以確認與追查的科技特性來從事犯罪；也由於具有高度獲利的經濟上誘因，這類犯罪已迅速成為目前國內外嚴重的經濟犯罪態樣。為避免對此類犯罪的定義過於狹隘，使研究難以盡窺全貌，本研究以我國實務通說之「網路釣魚」代稱這類詐欺犯罪態樣，但泛指「利用社交工程及資訊技術以取得電腦使用者身分相關資料，再於線上進行身分偽冒，以期取得經濟利益之犯罪行為」。而不限於以電子郵件使人陷於錯誤之犯罪態樣。

3. 網路釣魚犯罪統計與特徵分析

3.1. 官方統計欠缺比較之基礎

受限於標準定義的欠缺，國內外至今對網路釣魚犯罪對經濟的影響並無權威性的統計數據。歐盟工作組蒐集各方調查數據後粗略指出，這類犯罪在英國可能造成每年 13 億英鎊的經濟損失；在美國，估計在 2005 年造成 566 億美元的損失；但在澳洲，調查結果相當分歧，從每年少於 10 億美金，到超過 30 億美金的結果皆有[4]。

我國釣魚犯罪危害之狀況並無法具體從內政部警政署公布之犯罪統計數據明顯觀察出；詐騙帳號密碼案件數目之低落亦與外界認知有所落差。本研究以為，此充分凸顯出網路釣魚犯罪在定性與追緝上的困難程度。

圖　一、96 年 1-7 月詐欺案件發生數、破獲數與破獲率

	發生數(件)	較上年同期增減數	較上年同期增減率	破獲數(件)	較上年同期增減數	較上年同期增減率	破獲率(%)	增減百分點
詐欺總計	22,134	-2,090	-8.63	18,357	3,671	25.00	82.94	22.31
電話、手機簡訊詐欺	7,741	-41	-0.53	5,832	1,613	38.23	75.34	21.13
詐騙款項	2,773	-1,365	-32.99	3,086	147	5.00	111.29	40.27
網路詐欺	2,454	235	10.59	2,037	961	89.31	83.01	34.52
偽稱買賣	2,454	770	45.72	1,554	763	96.46	63.33	16.36
假冒名義詐欺	2,404	-853	-26.19	2,272	293	14.81	94.51	33.75
拒付款項(賴帳)	680	52	8.28	543	76	16.27	79.85	5.49
刊廣告(報章)詐欺	359	-149	-29.33	353	65	22.57	98.33	41.64
虛設行號	302	-370	-55.06	269	-313	-53.78	89.07	2.46
冒(盜)領現金	265	-134	-33.58	94	-30	-24.19	35.47	4.39
彩金詐欺	130	-217	-62.54	151	-155	-50.65	116.15	27.97
詐騙帳號密碼	105	-7	-6.25	77	7	10.00	73.33	10.83
其他	2,467	-	-	2,089	-	-	-	-

資料來源：警政統計通報（96 年第 37 號）

[4] 參前註 1。

3.2.實務界的統計數據

根據「反網路釣魚工作小組」APWG的統計顯示，網路釣魚案件數從2006年1月的17,877件，到2007年1月將近30,000件[5]。另根據APWG於2007年7月所公布的報告指出，釣魚網站平均存活的天數為3.6天。最常被成為鎖定對象的產業別是金融服務業，佔所有網路釣魚行為的比率 94.4%；其次則是網路服務提供者(Internet Service Provider, ISP)及政府機構，各為2.4%；最後則是一般的零售業。

另從資訊安全公司賽門鐵克的統計數據顯示，2006 年下半年，平均每天至少有848萬筆的網路釣魚訊息發生，而被網路釣魚詐騙的對象84%與金融服務方面相關，所欲竊取的資訊包括政府核發之識別碼（如身份證統一編號、社會保險安全碼）、信用卡、銀行卡、個人識別碼以及電子郵件地址清單等，都是網路釣魚想要竊取的機密資訊[6]。此外，46%已知的釣魚網站位在美國，其次為德國的 11%，英國、法國、台灣並列第三，各占 3%。若以亞洲區排名來看，台北占全亞洲網路釣魚網站的19%，排第一位，其次為首爾(占14%)以及東京(占11%)，而台北的網路釣魚主要以詐騙國外較多[7]。

從前述統計數據當中可以發現，超過9成以上的網路釣魚犯罪都鎖定金融服務業，其他產業受到網路釣魚犯罪行為詐欺的比率明顯低於金融服務業。本研究判斷，網路釣魚犯罪之所以鎖定金融服務業，一則因為一般民眾在登入金融服務相關網站時會提供可信度較高的個人資訊，再則以金融服務產業為標的之網路釣魚犯罪犯罪所得往往最高。

---

[5] 參見Phishing Activity Trends—report for the month of January, 2007，http://www.antiphishing.org/reports/apwg_report_january_2007.pdf。最後造訪日：2007/3/29。

[6]參見賽門鐵克網路安全研究報告第11期，http://www.symantec.com/zh/tw/enterprise/theme.jsp?themeid=threatreport。最後到訪日：2007/3/28。

[7] *Id.*

以今年 2 月間，刑事局發現中國駭客以組織性的釣魚手法架設至少十家的假網路銀行網站，計畫利用台灣民眾已普遍接受並使用網路銀行之習慣，竊取民眾個人資料，再利用竊取而來的個人帳號、密碼資訊將民眾帳戶盜領一空，獲取不法利益[8]為例，由於具有經濟上的誘因，這類犯罪預期將隨著各類線上活動、電子商務的普及而氾濫，若未能有效加以遏阻，網路上的亂象將可能對我國電子商務產業之發展造成負面影響。

3.3. 行為特徵分析

根據法務部統計處的分析，95 年我國的網路犯罪，大部分為利用網路散布性交易訊息或網路色情或援交及詐欺者為多[9]。但根據資安實務界的觀察，有越來越多的犯罪目的旨在竊取機密且可獲利的資料；國內大宗且對民眾影響最深的網路犯罪，預計仍是身分資料竊取後所為的網路詐欺[10]。

根據賽門鐵克報告[11]，自 2005 年起，以竊取機密資料為目的的惡意程式數量逐漸竄升，其威脅的形式將更加多元化及複雜化。從近幾年來網路釣魚犯罪的變化觀之，目前發展趨勢有以下幾項特徵：

3.3.1. 犯罪場所國際化

資通訊網路的科技使用縮短了世界的距離，使得人與人溝通的方式更為便利，地理疆界不再是溝通的障礙，國際間資訊的傳遞變得更快更容易。然而，網路即時性、匿名性及跨國性的科技特色，卻也使

[8] 林惠君，金管會籲檢視網路銀行網址 確保交易安全，中央社，2007 年 2 月 10 日，http://tw.epochtimes.com/bt/7/2/10/n1619486.htm, 最後到訪日：2007 年 11 月 5 日。
[9] 95 年法務統計重要指標分析，法務部統計處，2007 年 4 月。
[10] Udn數位文化誌，「網路犯罪 連續三年成長逾五成」http://mag.udn.com/mag/dc/storypage.jsp?f_ART_ID=23440, 最後到訪日：2007 年 11 月 5 日。
[11] 精誠資訊，http://www.secucom.com.tw/big5/News/News_view.asp?cid=3&id=186&urlID=42, 最後到訪日：2007 年 11 月 5 日。

得網路空間的秩序不易建立，容易淪為公權力難以伸展的犯罪天堂。

根據賽門鐵克 2007 年初的調查[12]，全球各國的網路釣魚網站數量比率之排名部分，美國以 46%排名世界第一，主要是因為網頁寄存/虛擬主機供應商多位於美國，而美國也是擁有全球最多網路使用者，以及成千上萬各型網路組織的國家。其次，在亞洲，網路釣魚排名前五名的城市分別是台北、首爾、東京、香港及曼谷，而位於台北的釣魚網站則主要以詐騙外國人較多，以規避執法單位的查緝；至於利用關鍵字廣告騙取本地使用者之釣魚網站，則多半來自中國大陸。由此可見，為規避法律責任及阻礙檢警執法，釣魚網站的架設者多半會選擇個人所在地與詐騙目標地以外的第三地，作為架設網路釣魚的地點。網路釣魚的運作早有跨國犯罪情形，若僅透過單一國家的執法力量恐不易達成，仍須透過國際合作，打破司法管轄權之疆籬，始能確保網路使用之安全，以收執法之效。

3.3.2. 犯罪集團組織化

有心人士發展並散布智慧型惡意程式的趨勢有日漸升高的傾向，且這類犯罪態樣逐漸朝向組織化，上、下游分工關係的型態進行。資安業者（CA組合國際）即曾表示[13]，相較於過去的犯罪模式，惡意程式、網路釣魚和垃圾郵件的散布方式雖然同樣都是透過電子郵件，但惡意程式的開發者卻能依循其經驗，利用成功的詐騙模式不斷製作更新、更難以判別的惡意程式。這樣的現象，或許可以解釋為不同的網路犯罪集團間針對犯罪的程式及手法彼此交流，利用複合式的垃圾郵件、在電腦背景端執行之程序，達到竊取資料或植入木馬，透過不同途徑進行計畫性犯罪行為。因此，不管是網路釣魚或者其他犯罪手

[12] Taiwan.CNET，「報告，台北成亞太主要釣魚網站設立所在地」，
http://taiwan.cnet.com/news/software/0,2000064574,20116084,00.htm, 最後到訪日：2007 年 11 月 5 日。
[13] CPRO資傳網，「網釣鎖定金融業 智慧變形攻擊現身」，
http://cpro.com.tw/channel/news/content/?news_id=54652, 最後到訪日:2007 年 11 月 5 日。

法，在 2007 年間，網路犯罪已然與駭客更緊密地結合，形成更有組織的網路犯罪社群，並且以開發竊取個人、企業與金融資訊的工具為最熱門，攻擊對象與標的亦較以往更為集中。

3.3.3. 犯罪工具模組化

賽門鐵克全球網路安全威脅研究報告表示[14]，從傀儡程式數量的減少，可證明傳統大規模網路病毒與DoS攻擊已不如往常有效；2007年上半年最大的網路威脅則是來自於網站(Web)威脅，在目前所揭露的各式網站漏洞中，有 61%是網頁應用程式的漏洞。此外，模組化攻擊工具的增多，也使得網站攻擊方式變得更容易模仿與進行。該報告同時指出，網路攻擊已逐漸從被動轉變為主動，2007 年上半年最常見的網路攻擊手法正是階段式攻擊(Staged Attact)以及網路釣魚工具組。所謂網路釣魚工具組意指透過一組指令碼，讓駭客可以自動化設立一個以假亂真的釣魚網站，並產生與該釣魚網站相對應的垃圾郵件。據調查，2007 年上半年發現的釣魚網站中，有 42%來自於特定的網路釣魚工具組。由此可知，網路釣魚的行為人已經普遍利用模組化工具，快速建立釣魚網站，而過去將「駭客」一詞與「技術專才」相互連結的認知，可能因犯罪工具模組化的趨勢已不再適用於現今網路科技世界。

雖然國際間因為欠缺一致性的定義，對網路釣魚造成的危害至今無法有效評估，但資安實務界指出的網路釣魚犯罪國際化、組織化、犯罪工具模組化的發展趨勢，不容忽視。基於工作績效 80/20 法則，本研究以為，實務界的統計結果已然指出這類犯罪防制可能的思考方向。將於第 6 章以下討論之。

[14] iThome，「賽門鐵克：網路攻擊模組化工遽增多」，
http://www.ithome.com.tw/itadm/article.php?c=45972, 最後到訪日：2007 年 11 月 5 日。

4. 網路釣魚的犯罪手法與技術分析

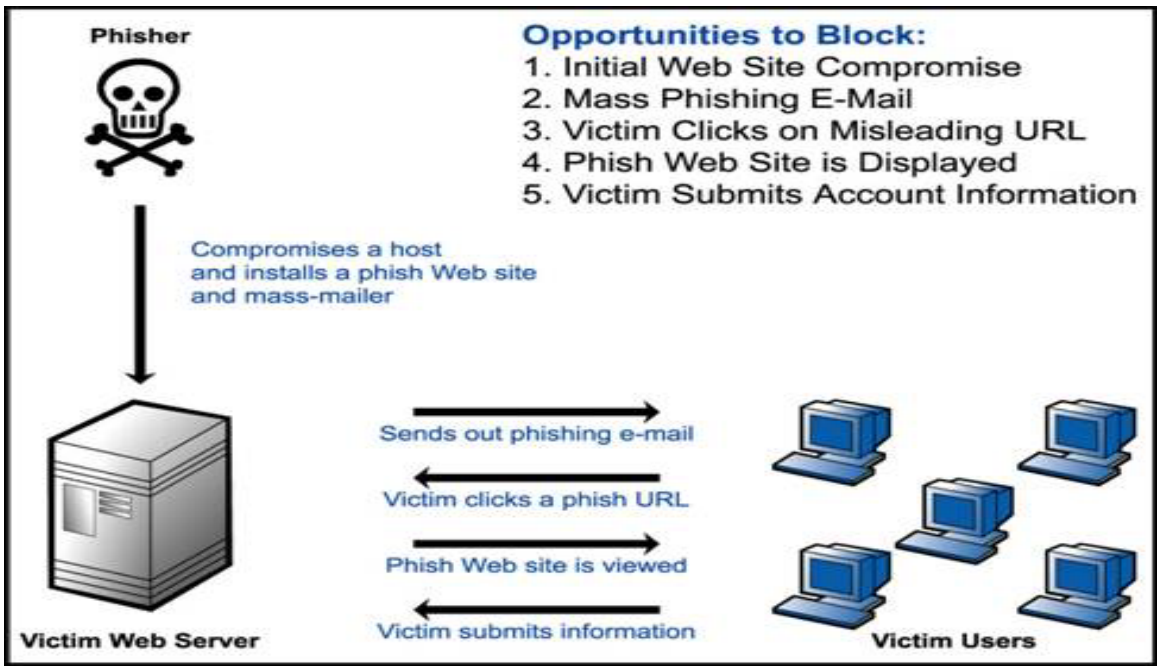
4.1.犯罪手法分析

網路釣魚手法與過去常見以退稅、中獎等名目誘使民眾自動到ATM 操作轉帳詐欺可說大同小異：歹徒先以不特定多數人為對象寄送郵件、簡訊或即時通訊，誘騙使用者上鉤以取得民眾的帳號、密碼相關個人資料後，再利用該資料進行其他犯罪行為以獲利。

相關案例在我國亦所在多有。例如從 2003 年 6 月開始，我國即破獲國內首宗利用網路釣魚手法，竊取網路使用者之銀行帳號、密碼;2004 年刑事局破獲智慧型網路駭客假冒國內銀行申請相似網址架設假官方網站詐取銀行客戶帳號、密碼，而後盜領被害人銀行款項一案；2005 年開始，陸續查獲歹徒以有利可圖之銀行帳號、拍賣帳號為主，利用鍵盤側錄程式突破網路銀行所設計的虛擬鍵盤安全措施以盜取帳號密碼。至 2007 年，網路釣魚有跨國化趨勢，兩岸駭客聯手設置變種網路釣魚網站，竊取網路銀行等企業大量個人資料(含帳號密碼)，並建立整合性的家戶檔案等。詐欺手法在技術層面有逐漸精進趨勢。

為期做到有效防禦，首應釐清網路釣魚的技術與手法，從而思考可能的因應策略。以下將網路釣魚犯罪簡單區分為三個行為階段：灑網階段、魚兒上鉤階段與實質獲利階段，就各階段行為從技術層面與行為態樣層面進行分析。從相關案例觀之，技術的演變主要發生在「灑網階段」與「魚兒上鉤」等二個行為階段。顯示行為人充分利用電腦程式具有可輕易大量複製文本與可自動執行的特性，以更廣泛的對象作為目標，除了擴大打擊層面外，也充分利用網路獨具的分散性(每個使用者都可以在家戶中聯網接取資訊)與可匿名性，躲避執法單位的查緝。可以預見的是，當電子商務越蓬勃，網路釣魚的行為人也將變得越貪婪。

圖　二、網路釣魚手法示意圖



資料來源：ICST資安論壇[15]

4.2.犯罪技術分析

4.2.1. 針對不特定對象寄發大量郵件並附帶 URL 網址

歹徒欲針對不特定多數人寄發大量郵件(實務通稱此類不請自來的郵件為「垃圾郵件」，以下稱之)，首先需要知道寄信者的電子郵件帳號。技術上蒐集電子郵件帳號的方式有三：

A. 以郵址產生器，以亂數組合產生隨機式電子郵件名單。
B. 以軟體程式透過掃描公開網站、新聞群組及網路佈告欄等方式蒐集郵件地址。
C. 以感染病毒方式，利用使用者原通訊錄中的名單為對象，偽稱使用者名義寄送郵件，同時複製病毒或植入木馬程式。

在技術上，前述二種產生寄送垃圾郵件方式對使用者的危害較侷

[15] ICST 資安論壇：http://forum.icst.org.tw/phpBB2/viewtopic.php?p=39030 最後到訪日：2007 年 7 月 10 日

限於個人端。各區域或組織的網管人員，可以程式過濾明顯可辨別的隨機垃圾郵件；而使用者只要提高風險意識，避免不必要的資訊公開，且盡量不開啟來歷不明信件、不點閱可疑連結，這類詐欺手法雖然不可能禁絕，但在縮小打擊面策略上，尚屬有控制之可能。

資訊安全界目前關注且必須重視防範的手法，為結合社交工程的第三種技術的猖獗。透過各組織與資安設備廠商的教育下，民眾目前多能有「不隨意開啟來路不明郵件」的基本維護電腦安全意識。但當1、傳送訊息者為自己所熟識之人；2、訊息標題似乎與自身權益切實相關[16]；多數使用者往往仍是不加思索的點擊隨附連結，開啟相關郵件、下載影音圖檔、或連上特定網站。病毒或木馬賴以傳輸之媒介，從電子郵件、MSN到VOIP、智慧型手機[17]等，實務上均已有案例。收信者若一時不察，結果將讓自己的電腦成為殭屍電腦(Botnet)，輕則潛藏於電腦，擷取個人資料後傳送給歹徒[18]，重則成為歹徒進行其他攻擊之跳板[19]，對網路環境的安全造成極大的威脅。

---

[16] 刑事局破獲有人以網路釣魚方式，將木馬程式植入網友電腦，側錄「WebATM」晶片密碼的案件。所謂「WebATM」，即網路化的ATM，民眾在家上網即能進行轉帳、繳稅及購物等，而網路釣魚則是駭客藉寄發E-mail，將竊取資料的木馬程式植入網友電腦內。刑事局這次破獲的案件，就是駭客冒充服務人員，將木馬程式隱藏在「讀卡機更新驅動程式」的E-mail裡。中央社 94/5/17。

[17] 今年 3 月初發現首次利用MMS簡訊散播的智慧型手機病毒武士病蟲(SymbOS.Commwarrior.A)，主要係感染內建Symbian Series 60 作業系統的智慧型手持設備，使用者一旦接收並開啟此一病毒所傳送的MMS簡訊，該簡訊將自動執行並在系統上建立檔案，循設備中聯絡人電話，自動發送MMS簡訊進行散佈。要受到Commwarrior 病毒的感染，用戶必須打開電子郵件，並下載其中偽裝為附件的惡意程式碼。為了引誘收件人，Commwarrior 病毒作者利用了 20 多種貌似正常的資訊，其中包括一個自稱包含有Symbian 軟體升級包的資訊。

該病毒後來被證實因為未確實找到系統漏洞，使得攻擊未能成真，但卻首度證實病毒可透過 MMS 傳輸，並在智慧型手機平台上自動下載程式，也表示未來發生在手持設備上的病毒攻擊，將可能複製自現有對個人電腦的攻擊行為。Cnet News 2005/4/12。

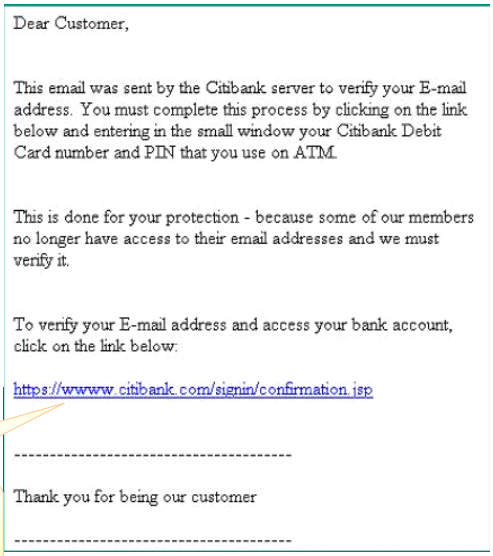
[18] 防毒公司SOPHOS呼籲，要求留意郵件標題是「視窗緊急更新」(Urgent Windows Update)與「視窗重要更新」(Important Windows Update)的E-Mail，因為文中提供的連結看似指向微軟更新網站，其實在點選後會被引領到駭客控制的網頁。

由於微軟大聲疾呼必須按時下載視窗系統的修補程式，使得註明類似標題的電子信函易讓用戶乍看之下信以為真，不過一旦點選內文中的連結，開啟「假網頁」的同時可能也被同步植入木馬程式，個人資料或信用卡密碼將有遭竊之虞。聯合新聞網 2005/04/11。

[19] 根據刑事局科技犯罪防制中心與微軟在 2006 年九月份(台灣刑事局科技犯罪防治中心,

圖　三、寄送不特定對象電子郵件

假冒的Paypal通知信函,資料來源：資傳網



click此一連結後，就中了網路釣魚者的圈套!!!

偽造的花旗通知信函

資料來源：Trend Micro Incorporated.

4.2.2. 虛假的網頁與網址

4.2.2.1.　註冊近似網址混淆使用者

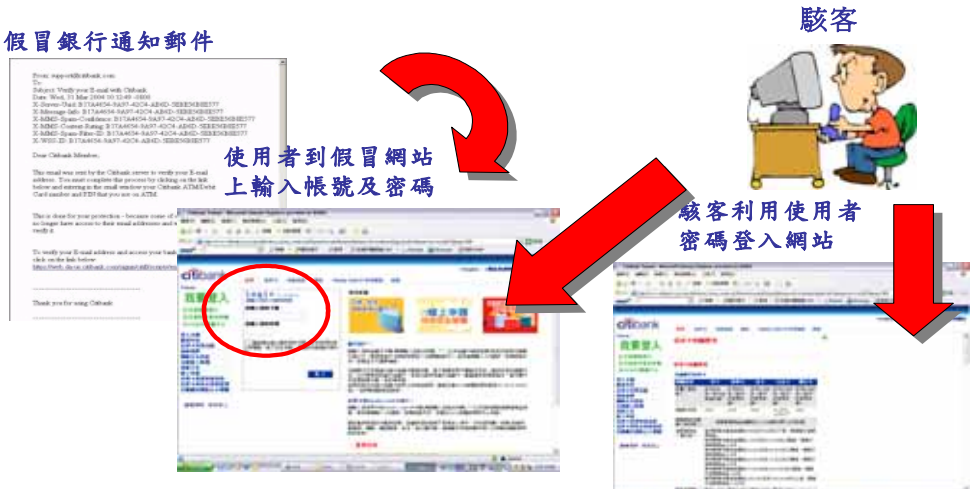
駭客事先註冊與「正牌」之真正網站名稱極為相似之網域名稱，利用極為相似之字母或數字，如英文字母小寫 l 與數字 1，n 與 h、V 與 W 等極為相似之符號以假亂真，使上網之民眾難以辨別真偽，而誤觸駭客之網路釣魚陷阱。

美國知名的代收款網站 paypal.com 即為此類手法中著名的案

2006)，針對殭屍電腦（BotNet）所做的調查結果，台灣電腦主機被污化成殭屍網路一員的數量已名列全球第六，以亞洲地區來看則僅次於韓國之後。從調查的結果來看，2006 年 2 月遭受感染的主機數為 57,783 台，但是，截至 9 月 17 日止，國內受污化的主機更高速成長到 88,136 台。短短半年之內，每天有超過 150 台的電腦不斷被「殭」化，成為名符其實的犯罪打手，被駭客們無聲地控制著、驅趕著執行秘而不宣的破壞行為。
http://thinktank.stpi.org.tw/eip/index/techdoc_content.jsp?doc_id=1182829461171&ver_id=2，最後到訪日：2007 年 7 月 20 日。

例。詐騙者在網址上以數字 0 取代英文字 O、以數字 1 取代英文字 l，或者在電子郵件中顯示正確網站連結，卻連結至其他網站主機，之後向網路使用者謊稱升級客戶服務，或更新帳戶資料，要求被害人提供帳戶密碼，以及相關隱私資料。在取得資料後，詐騙者至利用資料到真實網站竊取被害人的錢財，或者從事大筆消費，讓受害者蒙受損失。

圖　四、註冊近似網址混淆使用者



顯示網址-http://www.citiibank.com.tw
實際網址-http://www.citibank.com.tw
資料來源：本研究自製

4.2.2.2.　利用瀏覽器漏洞

A. 利用 JavaScript 技術汰換靜態的網址

駭客利用JavaScript技術置換靜態的URL網址，讓偽造網站的網址列與正牌的網站相同，難以辨認真假。當使用者上鉤並輸入資料時，相關資料將被竊取。如**圖　五、**中，駭客隱藏了真正的偽造網址，使用者所見的確實是銀行的官方網址。由於網頁程式碼可能

是利用JavaScript編寫，使用者瀏覽時無需另外安裝ActiveX元件，讓使用者失去戒心，相當難以查覺。

圖　五、利用 JavaScript 技術汰換靜態的網址

資料來源：CPRO資傳網[20]

B. 利用網址列不同語法變化

這類技術主要利用微軟瀏覽器網址顯示列可以不同語法顯示的漏洞，達到愚弄使用者的目的。例如[21]:

I.　IP 位址其他表示法

不同於慣用的十進位表示法，系統還可接受 Double Word、八進位或是十六進位表示法。例如：www.google.com的IP 位址是

[20] CPRO資傳網：http://cpro.com.tw/channel/news/content/index.php?news_id=51366 最後到訪日：2007 年 8 月 1 日

[21] 林璟瑋，財金雙月刊：http://www.fisc.com.tw/FISCWEB/FISCBimonthly/Article.aspx?Volume=42&TNo=34 ，最後到訪日：2007 年 7 月 30 日

66.102.7.147 ， 也 可 以 表 示 為 ： http://1113982867 、 http://00102.0146.07.0223 、 http://0x42.0x66.0x7.0x93 或 http://0x42660793。

II. URL 編碼

不只是 IP 位址的部份，URL 中路徑(path)部份也可用 URL-encoding、Unicode 等方式加以編碼，更不易容易解讀。例如：http://www.badsite.com/webhp?ab 可轉換為 http://www.badsite.com/w%65%62h%70?ab。

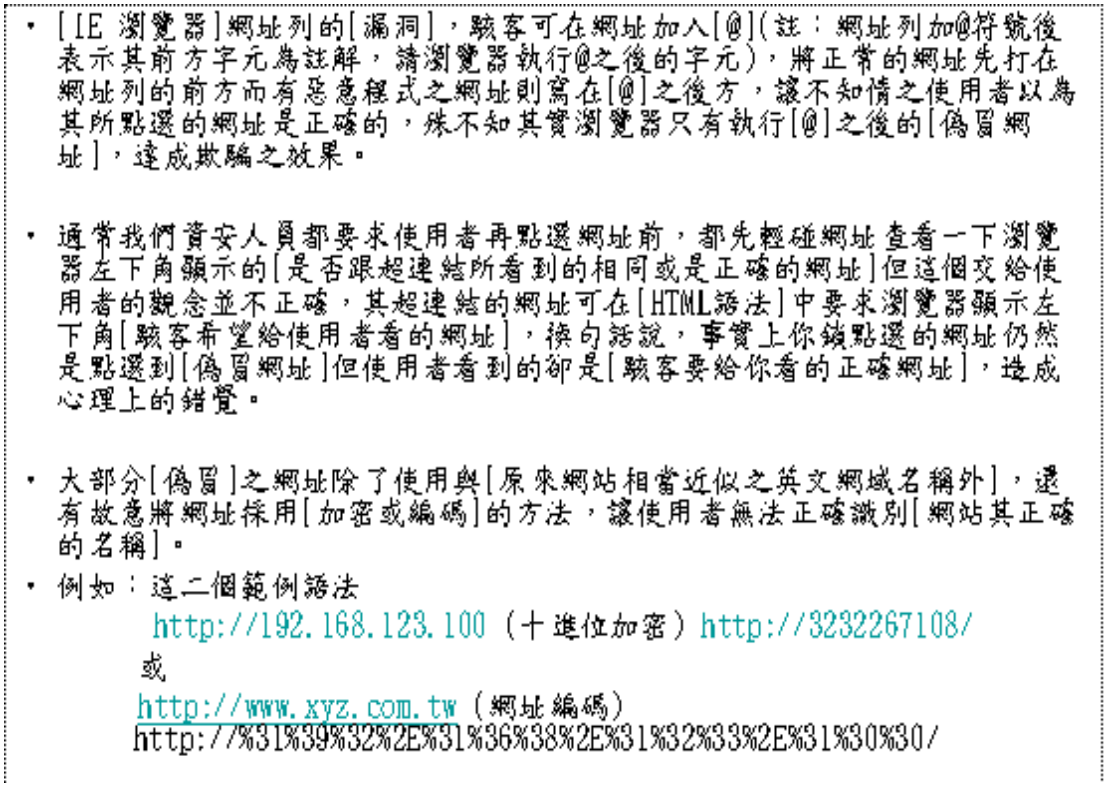
III. 借用 username:password@hostname 認證形式混淆

在 URL 中可以指定用戶認證需要的帳號與密碼。例如這樣的格式：URI://username:password@hostname/path 可被借用作為欺騙使用者；或

http://www.netbank.com@host.badsite.com/bad.cgi.prigram

乍看之下會以為要連結的網址是 www.netbank.com，事實上是連到 host.badsite.com。

圖　六、利用 HTML 語法漏洞說明



資料來源：網路攻防戰[22]

4.2.2.3.　利用網址轉稼技術

正常網路連線運作，需要透過DNS網域名稱伺服器指向功能[23]以解決機器的網域名稱與IP address的對應問題。在每一個名稱伺服器中都有一個快取暫存區(Cache)，快取暫存區的主要目的是將該名稱伺服器所查詢出來的名稱及相對的IP位址記錄在快取暫存區中，當下一次有另外一個用戶端到次伺服器上去查詢相同的名稱時，伺服器就不用在到別台主機上去尋找，而直接可以從暫存區中

[22] 網路攻防戰：http://anti-hacker.blogspot.com/2007/demourl.html，最後到訪日：2007 年 7 月 30 日。

[23] DNS分為Client和Server，Client扮演發問的角色，也就是問Server一個Domain Name，而Server必須要回答此Domain Name的真正IP地址。而當地的DNS先會查自己的資料庫。如果自己的資料庫沒有，則會往該DNS上所設的的DNS詢問，依此得到答案之後，將收到的答案存起來，並回答客戶。資料來源： DNS運作，http://dns-learning.twnic.net.tw/dns/03opDNS.htm，最後到訪日：2007 年 7 月 30 日。

找到該筆名稱記錄資料，傳回給用戶端，加速用戶端對名稱查詢的速度[24]。

網址轉稼（Pharming）的詐欺手法，即是透過向 DNS 快取記憶體下毒（DNS Cache Poisoning)的方式，向其他 DNS 伺服器提供合法網域名稱的錯誤 IP 位置，將合法網址轉接到駭客偽造的網站，讓使用者防不勝防。亦即利用 DNS 保留紀錄到更新的時間，直接在連線過程中竊取網站名稱來使用。

從技術面來看，以網址轉稼技術行釣魚詐欺的手法混合了DNS下毒、木馬程式及鍵盤側錄間諜程式(key-logging spyware)等技術。駭客首先利用垃圾郵件或正常網站的弱點，埋藏指令code在隨附檔案或網頁中，讓使用者流覽時不自覺下載該指令；下載成功後，該code即會更改使用者端的DNS伺服器設定，當該使用者擬連結到某些網頁(如銀行)在做DNS查尋時，該指令會讓使用者離開原本要造訪的合法商業網站，並且導向事先安排的假網站，當使用者輸入帳號密碼時，該等資料即直接被該釣魚網站保存log下來盜用[25]。其技術手法最早約莫出現在 2004 年，一個德國的少年綁架了

[24] 在每一個名稱伺服器中都有一個快取暫存區(Cache)，這個快取暫存區的主要目的是將該名稱伺服器所查詢出來的名稱及相對的IP位址記錄在快取暫存區中，這樣當下一次還有另外一個用戶端到次伺服器上去查詢相同的名稱 時，伺服器就不用在到別台主機上去尋找，而直接可以從暫存區中找到該筆名稱記錄資料，傳回給用戶端，加速用戶端對名稱查詢的速度。例如：

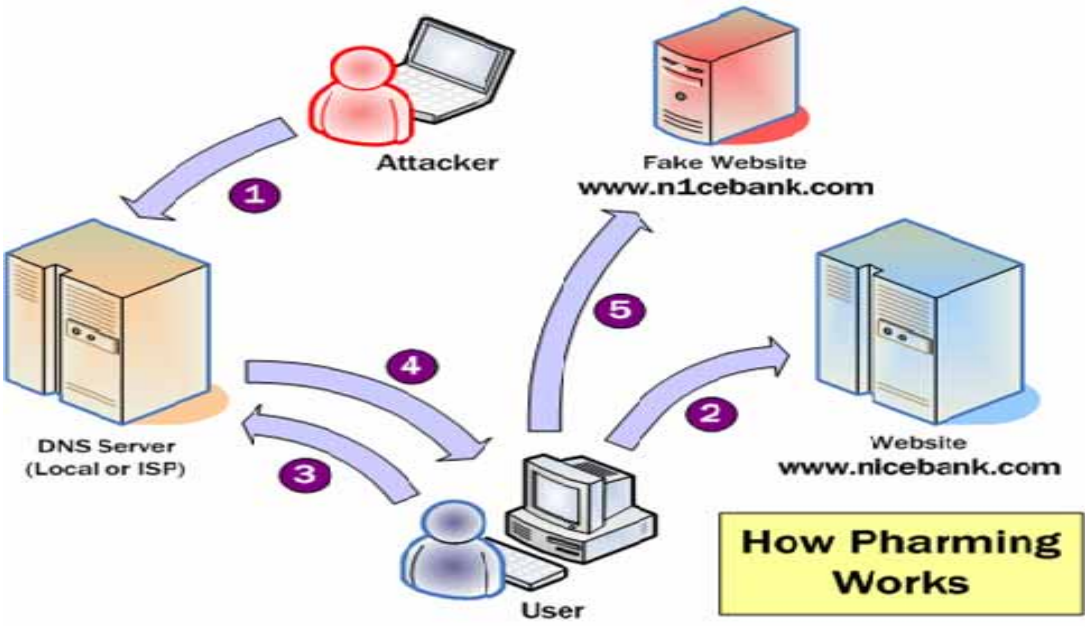
1. 當 DNS 用戶端向指定的 DNS 伺服器 A 查詢網際網路上的某一台主機名稱
2. DNS 伺服器 A 會在該資料庫中找尋用戶所指定的名稱
3. 如果沒有，該伺服器 A 會先在自己的快取暫存區中查詢有無該筆紀錄
4. 如果找到該筆名稱記錄後，會從 DNS 伺服器 A 直接將所對應到的 IP 位址傳回給用戶端
5. 如果名稱伺服器 A 在資料記錄查不到且快取暫存區中也沒有時，伺服器 A 才會向別的名稱伺服器 B 查詢所要的名稱。
6. 在伺服器 B 上也有相同的動作的查詢，當查詢到後會回覆原本要求查詢的伺服器 A
7. 該 DNS 伺服器 A 在接收到另一台 DNS 伺服器 B 查詢的結果後，先將所查詢到的主機名稱及對應 IP 位址記錄到 A 快取暫存區中
8. 最後再將所查詢到的結果回覆給用戶端

資料來源：改寫自DNS運作原理，SeedNet教室，
http://eservice.seed.net.tw/class/class09.html，最後到訪日：2007 年 7 月 30 日。

[25]參見symantec網站，
http://www.symantec.com/avcenter/reference/drive-by-pharming-animation.html，最後到訪日：2007 年 7 月 20 日

Google.de；2005 年 1 月紐約一家ISP公司Panix的網址，亦曾被稼接到位於澳洲的網站[26]。

圖　七、網址稼接手法示意圖



資料來源：Nilesh Chaudhari, CISSP[27]

4.2.3. 網頁夾帶木馬程式

從 2005 年 3 月，外電即已開始報導，歹徒開始利用跨站指令碼(cross-site scripting)瑕疵，在合法網站網址列插入其惡意內容的案例日益增加。利用這些網站，攻擊者可欺騙不知情的消費者墮入釣魚騙局。利用此種技術，民眾比較可能落入騙局，因為該網址確實屬於合法公司，只是被第三方加入其他內容。[28]

[26] Taiwan.Cnet:http://taiwan.cnet.com/enterprise/column/0,2000062893,20101093,00.htm,最後到訪日：2007 年 7 月 17 日。
[27] Nilesh Chaudhari, CISSP, palisade.plynt.com/issues/2006Mar/pharming/ ,最後到訪日：2007 年 7 月 30 日。
[28] 原文網址 ： http://taiwan.cnet.com/news/software/0,2000064574,20097312,00.htm,最後到訪日：2007 年 7 月 30 日。

根據Netcraft的調查[29]，許多公司網站使用的伺服器應用軟體都有跨站指令碼漏洞，造成若干網頁忽略不同種類的資料，具體而言，就是JavaScript碼。這使得罪犯得以將自己的JavaScript程式插入合法的網頁中。這類指令碼攻擊方式不同於前述的假網址攻擊，指令碼錯誤能讓騙徒在合法的網頁中加入類似假密碼登入系統等內容。

駭客專門針對知名企業的網站，在不更動原有的畫面下，修改網站內容，加入惡意程式碼，利用該企業的知名度或是透過社交工程郵件誘使瀏覽者瀏覽該網站程。當使用者點選「正牌」網站後，在不知不覺情況即被安裝惡意程式，以隱藏方式指向駭客預設的虛假網頁後，再自動連回「正牌」的網站，讓使用者沒有感覺任何異樣，但是實際上卻已執行了駭客暗藏的網頁程式碼，並下載多個木馬程式至使用者的個人電腦，做為竊取電腦內個人隱私資料之用。

攻擊手法又可分為：內嵌，直接在網頁中嵌入惡意程式碼；外連，將使用者導引至外部惡意網站；綜合式，綜合內嵌式及外連式攻擊方式，將使用者導引至外部惡意網站(關於網頁掛馬攻擊手法及其危害，請參「最新駭客攻擊手法展示及防範」，政府資通安全防護巡迴研討會，國家資通安全會報技術服務中心，2007 年 7 月)

4.2.4. 關鍵字廣告

歹徒透過購買網路關鍵字廣告服務，於各大入口網站搜尋行銷服務刊登「關鍵字廣告」，當使用者上網搜尋「如 xx 銀行」等詞彙時，搜尋結果的前幾列即出現歹徒刊登的「關鍵字廣告」，使用者是否點擊到正確網站，全憑機率。由於網路資訊眾多，多數使用者在使用習慣上相當依賴搜尋引擎，也因為這些虛假的廣告與網

[29]同前註 28。

站，為有心人士精心設計，希望網站管理者逐一判別廣告或連結之真偽，有其困難度，更何況一般民眾幾乎無法察覺該網站連結係假冒之網站。

而最新利用搜尋引擎為釣魚詐欺的手法，可見於當紅的iPhone手機。資安業者已發現一種新的木馬程式，可讓使用者在搜尋網站檢索iPhone資訊時，主動跳出釣魚網站視窗，誘騙使用者連結、騙取個人資訊。當使用者上網打入關鍵字「iPhone」時，系統便會自動跳出含有販售iPhone訊息的小視窗，誘導使用者點選連結至製作精美的釣魚網站，騙取信用卡號等個人資料。使用者若是自行在瀏覽器的網址列輸入iPhone.com網站，該木馬程式還會將網頁轉址至釣魚網站，但網址列卻仍會顯示正確的網址，讓使用者無從判別正在瀏覽的到底是官方網站還是釣魚網站。也由於該釣魚網站是在使用者主動搜尋後才會出現，有助於提高歹徒釣魚的成功率，使用者防不勝防[30]。

4.3. 小結

綜合以上國內網路釣魚的手法與技術的發展趨勢可知，與此一新興犯罪態樣有關的技術，早期主要集中在自動化地發送郵件灑網，目的在擴大可能的獲利來源。在各國開始制定反垃圾郵件法案，各方網管人員開始強化區域網管，主動過濾、標示明顯為垃圾郵件的電子訊息後，相關技術發展開始著重在如何騙取使用者「主動」上網，甚至是利用不相干但卻有一定知名度的網站散布木馬程式，陷使用者於錯誤而不知，自動上鉤送上個人資料。歹徒可說充分利用網際網路開放的特性，對民眾使用網路的信心與正當的商業

[30] 上網搜尋iPhone 恐落入網釣陷阱，http://taiwan.cnet.com/news/software/0,2000064574,20121476,00.htm, Cnet news, 2007年7月31日。

應用行為帶來隱憂。

另從以上對網路釣魚實施技術的分析可知，除了註冊近似網址以混淆使用者的手法可能與網域名稱申請有關外，其餘詐術之施行，均發生在資訊傳輸的兩端與傳輸過程中。此類詐欺行為得以成功的關鍵，仍在於歹徒事先預設幾可亂真的假網站，與可讓使用者誤以為真的網址遮蔽技術，該假網站是否有真實獨立的網址，實非所問。在此前提下，打擊這類犯罪的重點，可能仍在於即時發現與即時阻斷外界對該網站之接取。

行為階段	目的	手法	使用技術
灑網階段	誘騙使用者點擊連線上特定網站	針對不特定多數人寄發大量郵件夾帶URL	以郵址產生器亂數產生隨機式郵寄名單
			以軟體程式抓取公開的郵件地址
			以感染病毒方式散布郵件，同時複製病毒或植入木馬程式
魚兒上鉤階段	使用者自動key in 資料	設置虛假網頁，讓使用者陷於錯誤	註冊近似網址
			利用瀏覽器漏洞
			利用網址轉稼技術
		利用真實網站指令漏洞	網頁夾帶木馬程式
		綜合型手法	關鍵字廣告

表 一、網路釣魚手法與技術整理

5. 網路釣魚之法律責任分析

5.1. 實體法層面

以下根據網路釣魚三個階段，從我國法制分析相關之法律責任。

5.1.1. 灑網階段

針對不特定多數人散布誘餌的「灑網階段」，可說是網路釣客(Phisher)行為態樣最變化多樣，且不斷推陳出新的階段，仍應依各該行為態樣論其可能的法律責任。

若以網路釣客偽造商家名義寄送郵件並虛設網站的基本手法而言，由於資訊化社會的發展，許多的文字或圖像都已經加入電子化而足以表示其用意之證明。因此，網路釣客以商家名義向不特定多數人發送內含偽造的首頁及錯誤網址的電子郵件之行為，除可能構成我國刑法的第 220 條偽造準文書罪外，亦違反了著作權法第 91 條，而涉及侵害網頁著作人的重製權，以及使用他人商標中之文字作為來源之標識，成立商標法第 62 條的侵害商標權罪。

目前較有爭議的是，以郵址產生器、Botnet 自動散布電子郵件或即時訊息之行為，在我國仍呈現無法可管的狀態；而濫發商業電子郵件管理條例通過後，是否能有效涵蓋及此，亦有待研究。至於商家網站因設計漏洞，成為駭客借道植入惡意木馬程式工具的責任，目前國內外亦已有相關討論，惟仍未有定論。

5.1.2. 魚兒上鉤階段

於此階段，不論是網友誤入極為相似的網站自行輸入帳號密碼，或因行為人被植入木馬程式而被竊取包括帳號、密碼、出生年月日等個人資料，單純取得資料的行為，如果沒有後階段的利用行

為，在我國目前仍處於無法可罰的模糊地帶。而現行電腦處理個人資料保護法保護不足的爭議，不在此贅述。

實務上比較可能援引者，為刑法第 315 條妨害秘密罪與第 359 條的無故取得電磁紀錄罪，但如何證明個人資料已被歹徒取得既遂，與取得和損害發生間的因果關係，實務上可說相當困難。

5.1.3. 實質獲利階段

此階段為網路釣客取得個人資料後，進一步利用所取得的資料進行其他行為以實際獲利的階段。如歹徒用以製作偽卡，可能構成刑法第 201 條之 1 第 1 項的「偽造變造支付工具罪」，若更進一步加以行使則為第 2 項的「行使偽造變造支付工具罪」；如網路釣客係用以入侵網路銀行，進行電子轉帳、更改他人財物紀錄時，則視行為的階段性，可能成立刑法第 358 條的「無故入侵電腦罪」及第 339 條之 3 的「不正使用電腦詐欺罪」。此階段行為的法律責任，可說較為明確。

5.2.程序法層面

網路釣魚犯罪在實體法層面並不複雜，尤其當制訂「濫用商業電子郵件管理條例」，以刑罰防堵垃圾郵件已經是政府明確方向時，只要執法單位能抓到歹徒，法官認事用法並不會有太大困難。但目前最大的爭議與困難處，即在於如何有效追查與遏止。

蓋網路獨特的可匿名性與遠端遙控性，讓歹徒得以躲藏在網路科技背後。對於目前網路釣魚行為人利用自動提款機轉帳的詐欺手法，執法機關還可以要求銀行在各個 ATM 處加裝攝影設備、警告標示，或要求警方加強巡邏等，以發現歹徒蹤跡。但透過網路科技，使用者可以不分白天、晚上在任何地點進行轉帳交易的同時，其也

可以不捨晝夜、不留痕跡的進行犯罪活動。這類犯罪也因為分散深入到每家每戶、每個使用者信箱與電腦中而更加難以防備與查緝。

如前所述，網路釣魚詐欺行為得以成功的關鍵，仍在於網路釣客事先預設幾可亂真的假網站，與可讓使用者誤以為真的網址遮蔽技術，該假網站是否有真實獨立的網址，實非所問。在此前提下，打擊這類犯罪的重點，可能仍在於即時發現與即時阻斷外界對該網站之接取。

6. 網路釣魚之防範策略

從目前網路釣魚手法演變趨勢可以判斷，以電子郵件或即時訊息進行釣魚的手法不會絕跡，但會傾向精緻化與自動化，亦即透過木馬程式結合社交工程，駭客將嫻熟於以被害者名義發送夾帶木馬程式的信件，而一般使用者在信件外觀上將越來越無法辨別信件發送者 ID 與其內容的真偽。此外，不安全的網站業已成為隱藏木馬程式的宿主，與傳統習慣認為只有上賭博、色情網站才有可能中毒的觀念有違，使用者可能只是瀏覽一些合法商家的網站，即可能被植入惡意程式，成為釣魚犯罪的受害者。

有鑑於這類犯罪對電子商務發展帶來的危害，與對使用者上網信心的影響，美國政府從 2003 年 7 月即開始對網路釣魚事件發出警訊，並將其列為未來最嚴重的網路犯罪態樣；日本經濟產業省、中國國家計算機病毒應急處理中心等亦均陸續發佈警訊，提醒網路上的用戶要注意此類型的詐騙行為。網路釣魚詐欺行為的嚴重性是各界應正視的問題，尤其是金融業、電子商務相關業者、網路接取服務的 ISP 業者等，有必要思考採取一定的措施來降低這類風險。以下彙整國內外文獻討論的技術及非技術上可能的防範策略以供參考。

6.1. 技術上防範策略

使用者與企業經營網站者，在網路釣魚技術上的防範措施，除了應注意「魚餌信件」(phishing email)或「魚餌網站」(phishing web sites)外，目前更應注意到惡意程式(malware)帶來的威脅。

透過安裝市售掃毒軟體、定期更新防毒軟體，杜絕已知的惡意程式外，目前可看到技術人員發展以下幾種技術來警示網路使用者該網站是否為仿冒網站，或電子郵件是否為釣魚郵件：

1. 網頁快顯封鎖：防止在使用者瀏覽網頁時被自動下載、安裝惡意程式。
2. 黑白名單資料庫：透過對黑名單之比對，判別各該網站及電子郵件是否有安全疑慮。
3. 網址及網頁分析：檢測包括使用者所瀏覽網址之正確性、其進行的交易流程是否符合 SSL 認證等，協助使用者免於被引導致偽造網站進行交易。
4. 行為模式安全防護技術：透過其行為及特徵來判別網路威脅，包括病毒、蠕蟲、木馬程式、鍵盤側錄程式及網路釣魚網站等。

在防制垃圾郵件技術上，使用內容黑名單(content blacklisting)、過濾軟體及關鍵字封鎖等方式，或透過標示SenderID、及其他足以辨示偽造電子郵件網址之技術，亦有助於使用者判別相關電子郵件的安全性。

為避免使用者在上網過程中被引導至假網站，加強瀏覽器本身之安全防護，使用新版瀏覽器、定期下載修補程式可能仍是目前最可行的策略。因為包括 FireFox、Microsoft、Netscape 等各大廠商都已在 2006 年下半年推出新的瀏覽器，針對網路釣魚攻擊加強防護措施。

企業或組織除了可思考透過安全技術的應用，強化使用者認證機制，例如要求客戶進入網站時需輸入二組或二組以上的認證碼，或利用電子監視系統，避免客戶認證碼在傳輸過程中被駭客擷取外，企業或組織也必須重視網頁程式在設計撰寫時的安全議題：JavaScript程式的應用有其風險；企業或組織網站普遍使用的轉址(redirect)功能，建議取消或不要使用，以降低被駭客利用的可能性；企業或組織在網站上有提供表單(Form)輸入介面者，則建議一

定要注意資料隱碼(SQL Injection)的問題[31]及其可能帶來的危害。

6.2.非技術上防範策略

總體而言，網路釣魚犯罪如此猖獗，除了科技不斷進步之外，資訊安全教育的缺乏，民眾欠缺對個人資料妥善保護的習慣，企業與組織對網路應用風險認知不足、對網路詐欺犯罪的警覺心不足等，均是助長網路釣魚詐欺犯罪猖獗的原因。

從使用者角度，對來自網路的各類資訊，宜保持警覺性;「停、看、另循管道聯繫及查證」仍是因應網路釣魚詐欺的不二法門。

從企業主或組織角度，企業或組織有必要瞭解不同的詐欺手法，設計更安全的網路應用程式，使用符合科技發展水平與應用需求的安全設備，強化對客戶資訊安全的提醒與聯繫工作，建立明確的資訊蒐集與使用原則等，強化隊員工的教育訓練等，均有助於降低網路風險，維護企業或組織的良好信譽。

6.3.建立通報機制之討論

網路釣魚犯罪防制的另一個討論重點，為網際網路連網服務提供業者(ISP)的協助義務，因為假網站仍是倚賴 ISP 業者的服務而存在。而從網路釣魚犯罪的發展趨勢可知，這類犯罪充分利用網路傳輸跨界容易的特性，執法機關在調查與逮捕上即必須倚賴國際區域間的司法互助合作；但在執法機關申請、等待司法互助程序啟動的同時，無法預期的潛在受害者也在快速的增加中。也因此，APEC

[31] SQL Injection是一種未做好輸入查驗(Input Validation)的問題，即在撰寫應用程式時，沒有對使用者的輸入做妥善的過濾與處理，便將其組合成SQL指令，傳送給SQL server執行。因而若使用者輸入之資料中含有某些對資料庫系統有特殊意義的符號或命令時,便可能讓使用者有機會對資料庫系統下達指令，而造成入侵所帶來的損失。事實上，這樣的疏漏並不是資料庫系統的錯誤，而是程式設計師或軟體開發者的疏忽所產生的。參見國家資通安全會報技術服務中心網站，http://forum.icst.org.tw/phpBB2/viewtopic.php?p=12571&，最後到訪日：2007 年 7 月 31 日。

2005 年 6 月網路犯罪防治專家會議中，多國代表即已指出：如何加強 ISP 與其上下游業者、執法機關之互動，能即時關閉假網站，為釣魚犯罪防制重點。除了在政府端強化公權力追訴之能力外，國際間的討論亦開始思考在相關電子商務產業間建立通報平台或資訊交換機制之可能性，例如 google、Intel 等均自發性的成立產業聯盟，期能透過彼此資訊之交換，使相關電子商務業者可以在最短時間內掌握最新詐欺手法、應變措施或國際防護趨勢等相關訊息。

建立通報平台的概念，必非從今日才有。蓋隨著各行各業普遍應用網路科技的發展趨勢，網路已成為各項民生基礎建設的載具平台，但也同時也成為有心人士覬覦的目標。當網路及其週邊設備已成為有心人士的攻擊標的，攻擊手段日益複雜，且透過電腦科技自動化的特性可讓各類資安事件的影響層面不斷擴大時，國內外均有建立通報機制或平台之討論，希望透過一定的資訊交換機制，讓各產業均得在各類資安風險事件發生時能即時採取防護措施，以掌控網路應用風險，進而降低損失。

然而不可否認者，由於安全預防與犯罪的概念仍然有一定的間隔。各國在建立資安通報機制時不免面臨到：「什麼是需要通報的資訊類型」？「該向資安通報機制通報？還是向犯罪通報體系通報？」的判斷爭議[32]。如本研究所述的「網路釣魚」，是否可被認定為資安事件，利用既有資安通報機制分享資訊？抑或應被視為是犯罪案件，援用司法程序向執法單位通報？關於此點，本研究以為，仍應就「網路釣魚」是否已為我國刑事法規所規範之犯罪來決定。

[32]除了發現有部分機關(構)隱匿事件不報之情況外，有些機關(構)在發生資訊安全事件時，因處理人員無法明確區分該事件為單純的資訊安全事件或是犯罪事件，而導致通報機關(構)不一致的問題。在未建立明確通報作業程序的情形下，有些機關(構)會將資訊安全事件向FedCIRC通報、有些則會向執法機關(構)進行通報。另外因作業程序之欠缺，也有一些機關(構)處理人員於發生資訊安全事件後，只向直屬長官報告，但未向上級主管機關(構)進行通報之情事。參見美國總審計局GAO Report, Information Security—Emerging Cybersecurity Issues Threaten Federal Information System, p.29. GAO-05-231。

惟如前述網路釣魚之法律責任分析可知，釣客之行為前階段單純取得個人資料之行為，我國目前仍處於無法可罰之模糊地帶。在尚無法規可就該取得資料之行為加以具體規範前，本研究不排除網路釣魚適用資安機制進行通報之可能性。以下即探討國內外實務上目前可見的通報機制，並釐清可能的爭議，以提供主管機關及相關產業未來建立我國網路釣魚通報機制之佐參。

7. 國內外通報機制之檢視

網路應用風險升高，為完善維護資訊系統的安全，避免資安事件、網路犯罪等行為對社會帶來的重大危害，各國政府開始重視事件通報與資訊分享的重要性。但單就行政體系或是政府機關(構)進行資安事件之通報與資訊分享，顯然不足以因應網路複雜的應用態樣。目前各國均已發現此問題之重要性，開始思考將資訊通報配合義務擴及到一般民間企業，並希望能建立一套公部門與私部門間的資訊分享之機制。然在欠缺法律授權情形下，政府欲強制民間機關進行通報確有其困難度，但若透過立法，又可能遭到手段正當性或比例原則的質疑。因此目前各國多以自願性、公、私部門合作的方式進行之。

本研究以下首先簡介美國政府的資安通報機制與民間自發性的網路釣魚通報機制，繼而檢視我國目前既有的政府機關(構)資安通報應變機制、金融業之資安事件通報機制、針對詐騙事件所設立之「165防詐騙諮詢專線」通報機制、及由我國資安專家自發性建立的通報運作方式，透過比較現有的資安通報機制，再於下一章中提出本研究以為較適合的的網路釣魚通報運作模式，以供我國未來建立網路釣魚詐騙通報機制之參考。

7.1. 美國資安通報機制

7.1.1. 資訊分享與分析中心(Information Sharing and Analysis Center，ISAC)

為維護資訊系統安全，避免資安事件對社會帶來的重大危害，美國政府於 1998 年發布總統指令第 63 號(President Decision Directive 63，簡稱 PDD-63)、2003 年底並發布國土安全總統指令第 7 號（Homeland Security Presidential Directive 7)，對政府與民間企業共同防護國家基礎設施（包括實體與網路）之安全，

建立合作機制進行政策宣示。美國政府一方面建立政府機關(構)與民間單位的對口機關-「國家基礎建設保護中心」(National Infrastruckture Protection Center，簡稱 NIPC)，另一方面則積極鼓勵一般民間單位能自發性成立「資訊分享與分析中心」(Information Sharing and Analysis Center，簡稱 ISAC)，作為民間機構與政府之間資訊分享之橋樑。

在政策鼓勵下，包括金融、能源、交通、水資源等產業體系紛紛成立個別的ISAC，各體系的ISACs再進一步結合，組成資訊分享與分析協會(ISACs Council)，負責整合各產業ISAC的資訊並增進各ISAC之互動與資訊分享。根據ISACs協會之統計，目前私部門重要基礎建設約有 65%均掌握於協會成員之中[33]。

各體系的ISAC成立方式與運作模式並不一致，有些是由同類業者共同成立；有些是與政府共同合作成立，甚至由政府支持成立；有些則是附屬在同業公會下面。經費來源的部分，有些是完全自行籌措，有些則是接受政府的補助。各體系ISAC進行資訊分享的對象，有些是完全免費，或是透過加入特定會員方式為之；分享的方式，則包含透過Email、網頁公告、簡訊或是定期召開會議等方式進行之[34]。國土安全部透過發布定期警訊並標示風險警示燈的方式，彙整並與各產業ISAC分享資訊。

7.1.2. 金融服務 FS/ISAC 簡介

金融體系的 ISAC(Financial Services Information Sharing and Analysis Center，簡稱 FS/ISAC)於 1999 年 10 月成立，是各產業間最早成立資訊分享與分析機制者。根據美國總審計局報告顯

[33] GAO，Critical Infrastructure Protection-Establishing Effective Information Sharing with Infrastructure Sectors，GAO-04-699T，p.17。
[34] 同前註，p.15-17。

示，其特色如下：

A、FS/ISAC 是一個非營利的私人組織，該組織與財政部間有很強的互動關係。主導機關為美國財政部。

B、FS/ISAC 是由金融服務業所發展與擁有，其成員包括銀行業、信貸協會、信用卡組織、證券業、保險業、信用卡公司、抵押銀行、金融服務部門公用公司(Fininacial Services Sector Utilities)、金融服務事業局(Financial Services Service Bureaus)及其他相關金融單位。

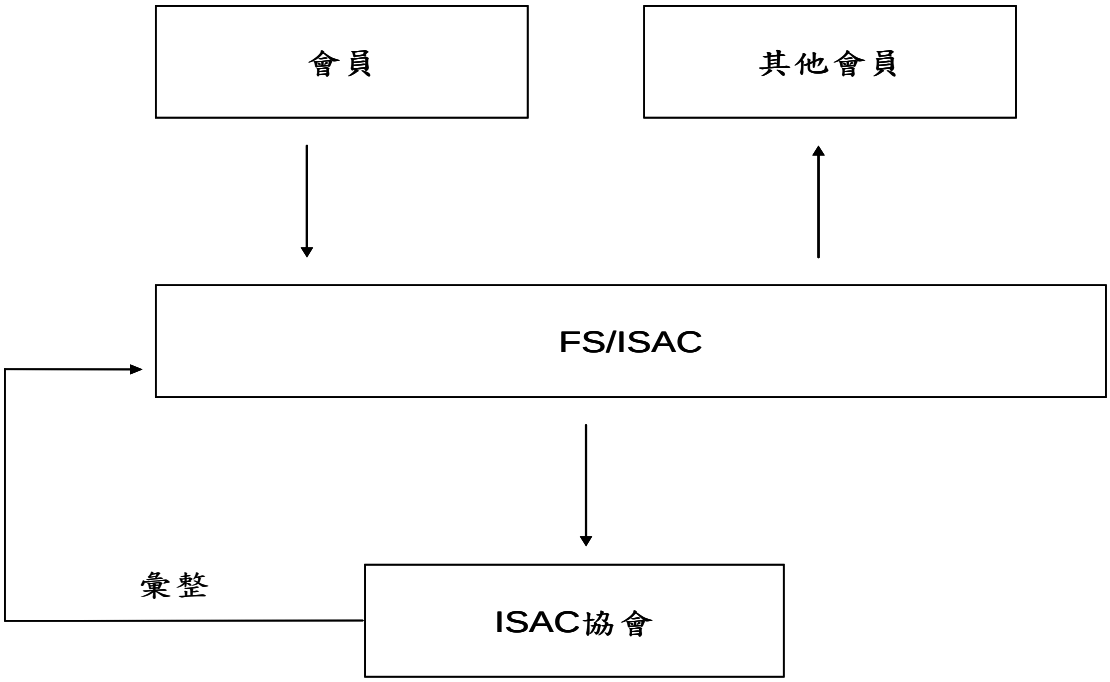
C、組織建立之目標：發展成為一個可信賴的資訊安全分享論壇，提供精準、即時的實體及網路安全資訊予會員，以減少危機事件對於會員的衝擊，並維持公眾對金融組織的信任。

D、資訊分享方式：會員可以選擇如何接取資訊，不論是自行上網(www.fsisac.com)，或者是透過傳真、Email及電話；該組織每年亦將舉辦兩場會議、發布趨勢調查報告，進行資訊分享及討論。(其運作方式如圖　八所示)

根據FS/ISAC資料顯示[35]，此資訊分享與分析中心採取「會員協助會員」的策略：會員在加入時均簽署保密協定；透過受信賴的網路，會員以匿名方式將各類風險訊息送交FS/ISAC；FS/ISAC的任務，在確保未經授權者不能接取到相關資訊。FS/ISAC同時與VeriSign公司的 24/7 運作中心合作，發布即時風險訊息，以達到即時預警的功效。至 2007 年 8 月，FS/ISAC已有 4000 多個會員加入，80%成員為銀行與信用評等機構。

[35] http://www.fsisac.com/

圖　八、FS/ISAC 資訊分享流程圖



資料來源：本研究自行整理

7.1.3. 反網路釣魚工作小組簡介

「反網路釣魚工作小組」(Anti-Phishing Working Group ，APWG)[36] 是由產業所組成的協會，屬自發性的網路釣魚通報機制，致力於網路釣魚及電子郵件詐騙引致的身份竊賊和欺詐陷阱。

該組織提供一個討論網路釣魚詐騙事件之通報管道[37]及論壇，專注於研究及分享關於網路釣魚之數據及防範方式，並於需要時，與執法機構共享網路釣魚之相關資訊。 APWG之成員為金融機構、網上零售商、互聯網服務供應商、執法機關及專案供應商，目前已

[36] 「反網路釣魚工作小組」網站：http://www.antiphishing.org/,最後到訪日：2007 年 11 月 25 日。
[37] 通報管道請參見http://www.antiphishing.org/report_phishing.html,最後到訪日:2007 年 11 月 25 日。

經有逾 1,300 間企業和政府機構參加 APWG，會員數目超過 2,100，為全球最大的防範網路釣魚之研究及事件通報組織。

7.2.我國現有通報機制

7.2.1. 我國行政院及其所屬各機關資訊安全通報應變機制

我國資訊安全事件通報之規範，主要以「行政院及所屬各機關資訊安全管理要點」(下稱「管理要點」)作為執行依據。「管理要點」第 10 點「業務永續運作之規劃」，要求各機關(構)應評估各項人為及天然災害對機關(構)正常運作之影響，同時訂定緊急應變及回復作業程序，與規範相關人員之權責；各機關(構)應建立緊急處理機制，在資訊安全事件發生時，應依規定之處理程序，立即向權責主管單位通報，採取反應措施，並聯繫警調單位協助調查等[38]。

行政院研考會依據「管理要點」另外函頒有「行政院暨所屬各機關資訊安全管理規範」，提供行政院及所屬機關(構)衡酌其業務需求後，制訂資訊安全政策之參考。管理規範第 1 章第 1 節第 2 款建議各機關(構)於制訂資訊安全政策時，應包含發生資安事件之緊急通報程序、處理流程、相關規定及說明；第 4 章第 1 節第 2 款資訊安全事件管理的部分，則建議各機關(構)應建立處理資訊安全事件之作業程序，並課予相關人員必要責任，以便迅速有效處理資訊安全事件。

上述管理要點中所提及之處理程序，包括國家資通安全應變中心作業手冊、各機關(構)處理資通安全事件危機通報緊急應變作業注意事項、各政府機關(構)落實資安事件危機處理具體執行方案以及資通安全事件獎勵要點等規範等。為整合上述規範，研考會目前另行委託國家資通安全會報技術服務中心進行「行政院及所屬各機

[38] 參見行政院台八十八經字第三四七三五號函訂頒「行政院及所屬各機關資訊安全管理要點」第十點，1999 年 9 月 15 日。

關資安事件通報應變作業規範」(下稱作業規範)研擬工作，該草案已公布於「行政院資通安全會報技術服務中心」網站[39]。其規範重點如下：

A. 各機關(構)首長應負責頒布「資安事件通報應變作業計畫」，並負起單位資安事件通報應變作業成敗之責任。
B. 各機關(構)資安事件處理的任務，主要落在「資訊安全處理小組」身上。處理小組主要的工作在執行資通安全預防措施，包含蒐集資通安全資訊、訂定機關(構)系統安全等級、建置資通安全控制措施、執行資通安全監控等事項、資安事件通報，以及緊急應變處理等相關事宜。
C. 資訊安全處理小組成員應包含資訊安全長、資安聯絡人、政風稽核及系統管理等相關人員。

草擬中的資安事件通報流程如下（參圖　九)：

A. 軟體(系統)功能異常反應：當行政院或所屬各機關(構)之員工發現系統或軟體有功能異常、資料不完整或疑似資安事件時，應立即通報該機關(構)之資安聯絡人。
B. 鑑定、確認與通報資安事件：資安聯絡人於接獲通報時，應協同系統管理人員鑑定資安徵兆，經確認為資安事件後，需循內部程序上報至資訊安全長，並於發現資安事件 1 小時內向國家資通安全會報通報應變組網站進行通報。
C. 陳報主管機關(構)：各機關(構)向通報應變組網站通報資安事件後，須於發現後 2 小時內向主管機關(構)之資安聯絡人通報。

[39]以下關於「行政院及所屬各機關資安事件通報應變作業規範」之說明，主要整理自行政院研考會委託財團法人資訊工業策進會進行九十四年度國家資通安全技術服務與防護計畫中「行政院及所屬各機關資安事件通報應變作業規範(草案)」研究報告，相關內容請參閱網址：http://www.icst.org.tw/content/application/icst2005/a1001001100110041/guest-cnt-browse.php?var=0%2C1001%2C106%2C1001001100030002%2C836%2Cplan,最後造訪日：2007 年 11 月 25 日。

同時通報網站在接獲機關(構)通報後，亦將主動通知該機關(構)之主管機關(構)資安聯絡人，並由主管機關(構)資安聯絡人循內部程序上報資訊安全長。若資安事件為「4」、「3」[40]等級，通報應變組應立即向國家資通安全會報執行長以上長官通報處置狀況，並視需要由執行長邀集相關單位召開資安防護會議；若該事件造成重大損害，則主管機關(構)應立即通知「中央災害防救業務主管機關」協助進行救災作業。

D. 請求上級支援：若通報機關(構)發現無法處理該資安事件時，應在發現資安事件 12 小時內提出支援之請求，主管機關(構)於確認為資安事件後 24 小時內決定是否支援；如需國家資通安全會報技術服務中心協助，則向通報應變組提出申請。「4」、「3」等級之資安事件應於 36 小時內完成修復，「2」、「1」等級之資安事件則應於 72 小時內完成修復；若無法恢復則應完成損害管制，並啟動營運持續計畫。

E. 回覆通報：各級政府機關(構)於資安事件處理完畢後，於恢復正常運作時，須至通報網站進行「通報結案」作業。

我國行政院及其所屬各機關資訊安全通報應變機制已行之有年，在政府機構端已建立起通報的概念。然從法律層面檢視，現行以行政管理權限支撐的通報應變機制仍面臨法律位階不足的疑慮。當此機制欲拓展到民間企業，發揮整合效益時，即不免有所阻礙。

此外，由於網路釣魚從資料外洩到實際產生身分冒偽的損害在時間與空間上有相當的遞延性，各機關(構)資訊工作人員如何有效判斷事件等級，避免過於頻繁的通報反而造成「狼來了」的反效果，

[40] 我國之資安事件等級目前區分為A、B、C、D四級，當資安事件影響公共安全、社會秩序及人民生命財產時，列為A級；造成系統停頓、業務無法運作，列為B級；若僅系統暫時停頓，造成業務中斷但短時間可以修復，則屬C級；而僅造成系統效能降低，業務遲滯，可立即修復，則屬D級。新修作業規範責將資安事件等級區分為 1、2、3、4 四級，第 4 級即A級，以此類推。

亦即，何時為資訊必須揭露、通報的時間點，值得三思。雖然如此，建立標準化的流程有助於提高通報機制運作的效率。

圖　九、資安通報流程圖

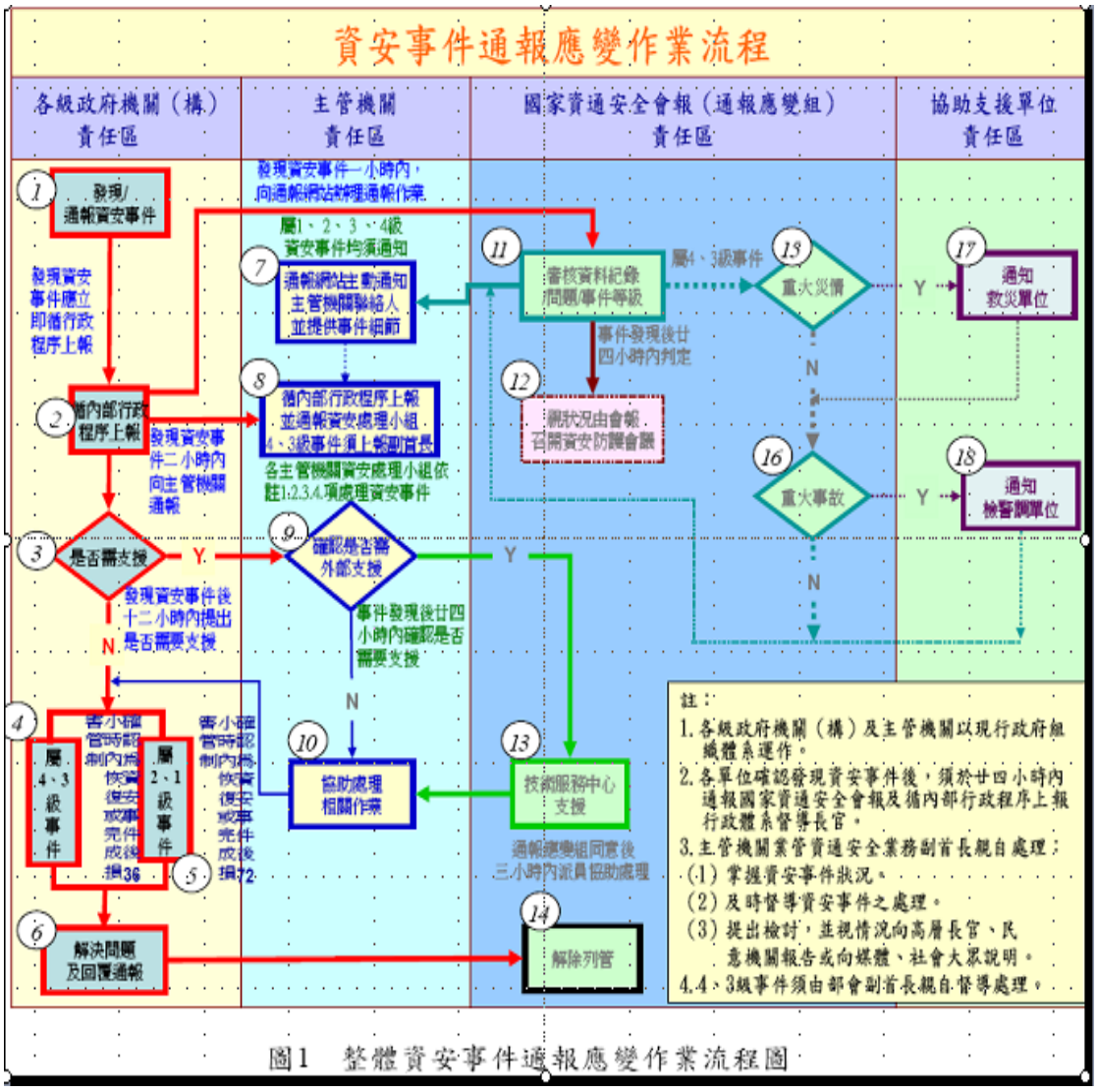


圖1　整體資安事件通報應變作業流程圖

資料來源：資安事件通報應變作業規範(草案)[41]

7.2.2. 金融業資安事件通報機制

在政府「建立我國通資訊基礎建設安全機制計畫」大力推動與要求下，主要的目的事業主管機關均已擬定有資安事件通報應變之

[41] 同前註 39。

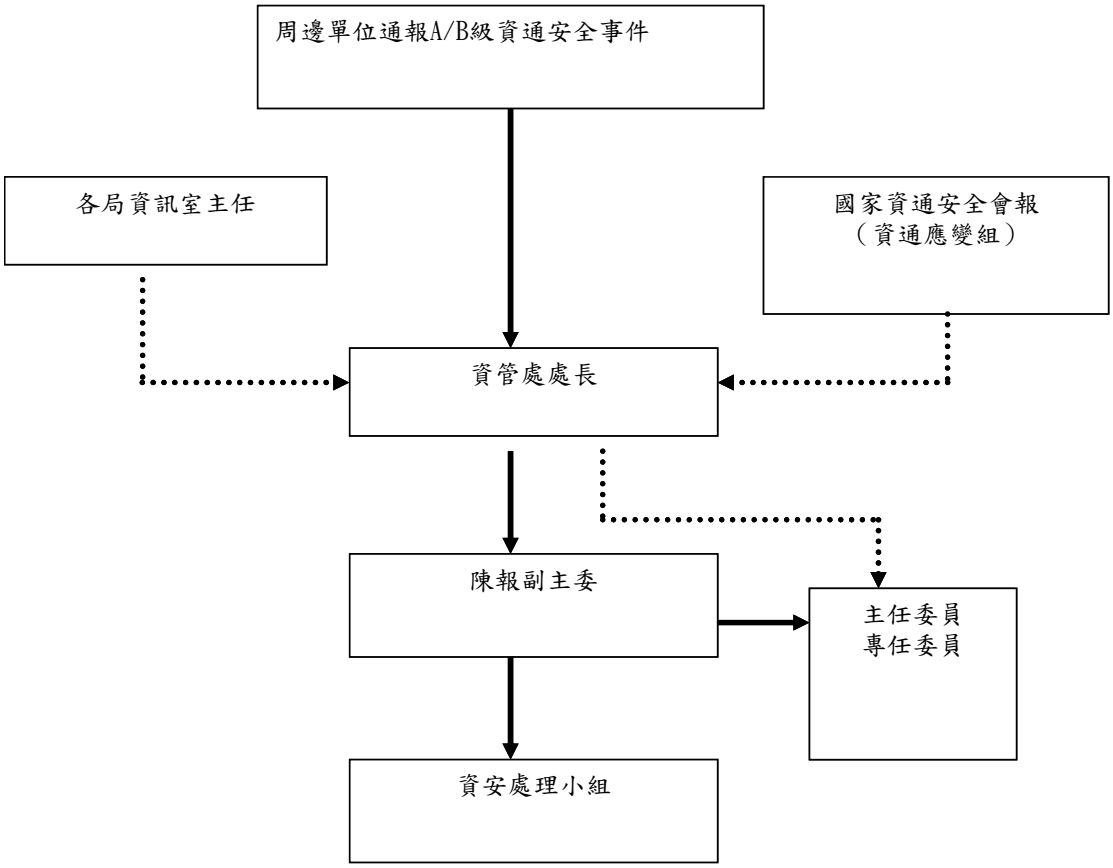
規範與流程供下級單位與企業遵循。由於有實務統計顯示，超過 9 成以上的網路釣魚犯罪鎖定金融服務業（參本研究 3.2 實務界的統計數據），本研究以為，鎖定研究金融業的通報機制，對防範網路釣魚詐欺有其必要性。以下簡介金融業資安事件通報機制。

以金融業資安事件通報機制而言，行政院金融監督管理委員會為金融體系之主管單位，下轄之重要金融資訊系統包含：跨行交易系統、證券交易系統、期貨交易系統、證券存託系統以及期貨結算系統。為了強化資訊安全事件之管制與通報，在主管機關要求下，這些重要金融資訊系統均已有建置資安防護管理中心之規劃(Security Operation Center，簡稱SOC)[42]，行政院金融監督管理委員會並訂定有資安事件通報流程(見圖　十)，要求該會、下級單位以及周邊單位於發生重大資安事件時(A/B級資安事件)，需向行政院金融監督管理委員會資訊處理小組進行通報。

依據行政院金融監督管理委員會之資安事件通報處理流程，各局資訊室主任(資安聯絡人)需向行政院金融監督管理委員會之資管處處長(上級主管機關之資安聯絡人)進行資安事件之通報，並透過行政院金融監督管理委員會資管處處長向金管處副主委(資訊安全長)報告。若發現資安事件無法控制而有必要尋求國家資通安全會報技術服務中心協助資源時，則須經副主委同意後向資通應變組提出申請。

[42]期貨交易系統之SOC預計於 95 年 12 月進行建置，並同時通過ISMS認證。

圖　十、行政院金融監督管理委員會暨所屬機關資安事件通報流程



資料來源：行政院研考會

行政院金融監督管理委員會另外制訂有「銀行業通報重大偶發事件之範圍及適用對象」相關規定[43]，要求銀行業(包含金融控股公司、本國銀行、外國銀行、信用合作社、票券金融公司、信用卡公司、信託投資公司、郵政公司)，於「發生重大偶發事件時」，除應立即通知治安或其他有關機關(構)採取緊急補救措施外，同時該銀行業負責人應儘速以電話及書面傳真向中央銀行、中央存款保險公司(除票券金融公司外)及銀行局報告，並於一週內函報詳細資料或

[43]金管銀(三)字第 09685001530 號令。

後續處理情形[44]。

根據金管會函令（金管銀(三)字第 09685001530 號）指出，所謂重大偶發事件是指：(1)人為或天然災害(如：地震、水災、火災、風災等)。(2)內部控制不良之舞弊或作業發生重大缺失情事。(3)安全維護方面(如：搶奪強盜、重大竊盜、行舍或設備遭破壞或遭恐嚇等)。(4)業務方面(如投資或放款)有重大財物損失。(5)媒體報導足以影響銀行業信譽。(6)資金流動性不足恐有擠兌之虞者或擠兌存款。(7)發生資通安全事件，其結果造成客戶權益受損或影響機構健全營運。(8) 於連續放假期間（併同週休二日或補假形成連續放假 3 日【含】以上），自動櫃員機可用率（指可提供服務且不缺鈔之自動櫃員機佔全部自動櫃員機比率）。(9) 其他重大事件。

網路釣魚在灑網與上鉤階段係以蒐集民眾個人資料為目的。由於此階段行為之手法與技術不斷改變，實務上甚難被有效即時查緝；即使相關陷阱被發現，復由於此階段行為的法律定性及其可罰性目前仍無定論，連帶影響應循何通報體系為後續處理之判斷。民眾或當事人發現有網路釣魚陷阱時，此時應被歸類為資安事件，循資安事件通報體系通報？或應被歸類為犯罪案件，向警方報案處理？即有爭議。但不論從上述「重大偶發事件」之分類，或從保障客戶權益角度出發，網路釣魚應仍可被視為金融服務業資安通報事件中之一項：金融服務業若知其事件發生時，應立即通知治安或其他有關機關(構)採取緊急補救措施；反向而言，當其接到治安或其他有關機關(構)通知時，金融服務業者已處於「已知」狀態，此時即必須採取一定的緊急補救措施，以保障客戶權益。

7.2.3. 金融機構警示帳戶聯防機制

[44] 「銀行業通報重大偶發事件之範圍及適用對象」相關規定第 4 條參照。

有鑑於國內詐欺轉帳犯罪之氾濫，為維護客戶權益，即時阻斷民眾受詐騙款項的流出，減少民眾損失，行政院金融監督管理委員會根據銀行法第 45 條之 2 授權，於 2006 年 4 月訂頒有「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」(金管銀(一)字第 09510001640 號令)，並授權中華民國銀行公會全國聯合會訂定「金融機構辦理警示帳戶聯防機制作業程序」，自 2006 年 11 月 1 日起實施「金融機構警示帳戶聯防機制」。

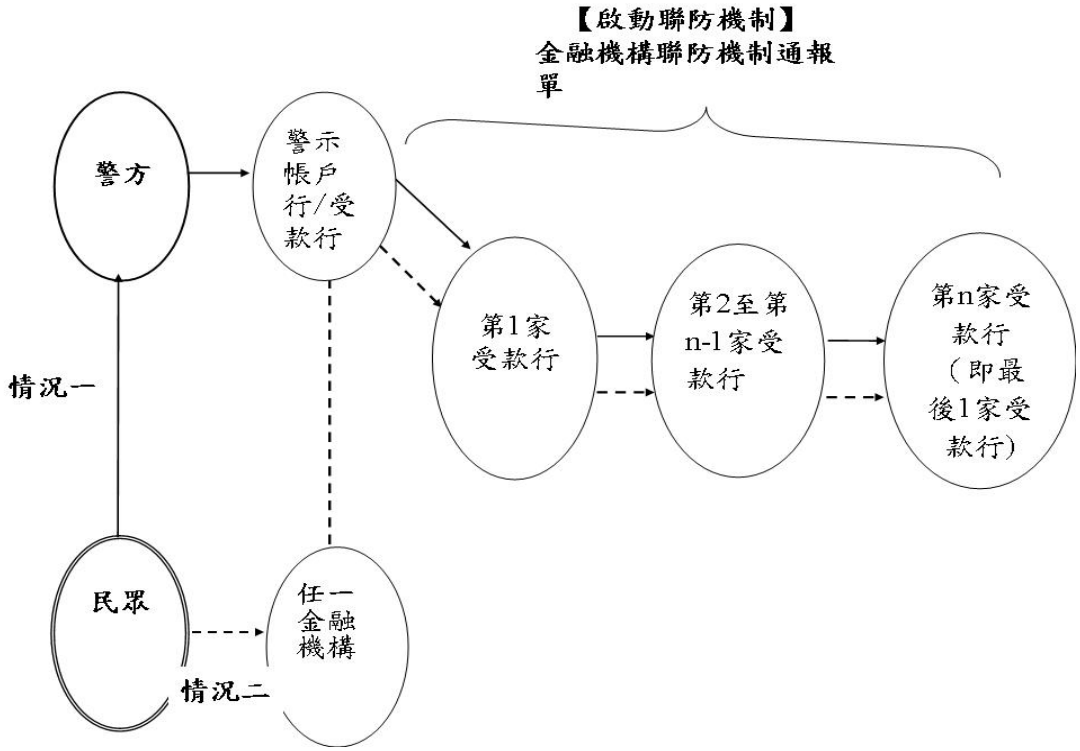
透過此聯防機制，當民眾發現自己遭詐騙時，可以就近到任何一家金融機構，告知櫃檯人員自己遭到詐騙，金融機構人員在確認民眾身分、匯款（轉帳）單據之後，將會立即撥打警政署「165」防詐騙專線電話報案，警察機關會在 2 個小時內指派員警至金融機構受理民眾報案，並通知受款的金融機構，此時受款的金融機構就會對匯入金額逕予圈存或止扣；被圈存或止扣的款項，將自圈存或止扣時點起算的 24 小時內，無法提領或匯款。這段時間內，將由警察機關繼續查詢此帳戶是否有必要列為警示帳戶，再通知受款的金融機構；如果受款的金融機構在圈存或止扣後 24 小時，仍未接獲警察機關通知，受款的金融機構原則上將解除圈存或止扣，以免影響民眾權益及正常交易[45]。此聯防機制並要求各金融機構設置通報窗口，以 24 小時服務之電話客服中心（Call Center）為原則；倘各金融機構之通報窗口有異動時，應立即通報財金資訊股份有限公司，俾財金資訊(股)公司隨時更新提供最即時之金融機構通報窗口資料。另，為配合檢警調機關偵辦與查證之需要，受款行應依相關規定協助提供相關交易資料及錄影帶等等。

從「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」第 4 條「通報」之定義，係指「由法院、檢察署或司法警察機關以公

[45]金融監督管理委員會：http://www.fscey.gov.tw/news_detail2.aspx?icuitem=1880552 最後到訪日：2007 年 11 月 30 日。

文書通知銀行將存款帳戶列為警示或解除警示；惟如屬重大緊急案件，得以電話、傳真或其他可行方式先行通知，並應即補辦公文書資料」可知，此聯防機制之啟動，仍以警方受理報案為實施之依據。惟參照本研究第 5 章網路釣魚行為階段之分析可知，只有當釣客透過前階段所取得的個人資料進行其他行為（如用以製作偽卡，或身分偽冒入侵網路銀行）以實質獲利階段，民眾或當事人始可能明確發現自己已遭詐騙，也才有報案之可能性。亦即，目前的聯防機制可能仍無法有效因應網路釣魚詐欺類型的犯罪，特別在行為人僅實施前階段行為時。

圖　十一、聯防機制通報架構圖



資料來源：金融機構辦理警示帳戶聯防機制作業程序

7.2.4. 內政部警政署「165 防詐騙諮詢專線」簡介

面對利用科技文明之便捷而產生的新興詐騙模式，政府已積極

重新整合現有資源，嘗試購置科技偵防器材充實偵察能量、辦理犯罪科技偵察教育訓練，以提升員警偵防能量。同時，我國司法警察機關亦持續規劃「靖頻專案」，打擊詐騙之轉接平台，鎖定專門提供詐騙集團作為電信傳遞管道的兩岸非法電信機房為查緝目標。

然而，除了透過電話進行之詐騙類型外，電信詐欺的防制還包括網路詐欺，不同於傳統的詐欺犯罪，網路詐欺之犯罪行為人係利用網路的即時性、匿名性及跨國性之特色，輕易地得以更少的人力及物力進行詐騙行為。執法機關若於被害人詐欺受害之後始發動偵查追訴犯罪，將無法在第一時間有效防止受害人範圍擴大，亦無法在有效時間裡追查犯罪行為人及其犯罪所得。建立一個具有公信力的查證與通報機制，適時達到教育與警示民眾之目的，是內政部警政署防詐騙諮詢專線成立之背景。

內政部警政署於 2004 年 4 月 26 日成立「0800-018-110 反詐騙諮詢專線」，並於同年 8 月 1 日改為「165」專線，提供民眾查詢最新詐欺犯罪相關訊息與防範方法。「165 防詐騙諮詢專線」成立甫滿一年時，所接獲之來電數高達 55 萬 4311 通，各地 110 專線來電數有 17 萬 73 通，其中還有熱心民眾主動提供詐騙集團所用的電話與金融帳號，請警方加以斷話或列為警示帳戶，實施成效頗具肯定。

自 2005 年起，165 來電數每天暴增為五千多通。有感於國內詐騙集團猖獗，為強化反制詐騙之力道，警政署決定將「165 反詐騙諮詢專線」從刑事局遷移到保一總隊，並從現有的 16 線擴增為 24 線，以擴大處理暴增的諮詢電話，並期有效整合「警政」、「電信」及「金融」鐵三角，透過資訊的快速流通，從科技面徹底防範詐騙案件發生。根據刑事局資訊室，「165 反詐騙諮詢專線」規劃中的功能如下所述(其通報運作流程如圖　十二)：

A. 具備詐騙簡訊關鍵字彙整功能，整合各家行動電話服務，提供民眾服務，提供民眾在接獲詐騙簡訊時，可以轉寄至一特定的訊息特碼，以逕行報案舉發。

B. 透過「整合人頭資料庫，加強制約人頭戶整合」之功能，可將現有金融、電信兩種資料庫資訊整合，進而要求各警察機關對於同一人持有三個以上金融帳戶通報警示，以及持有十個門號以上遭通報停話之人頭戶，加強訪查約制，以遏制人頭戶氾濫的問題。

C. 建置快速停話作業平台，改透過資訊系統連結各家電信業者系統，提升停話速度，減少公文及傳真流程。

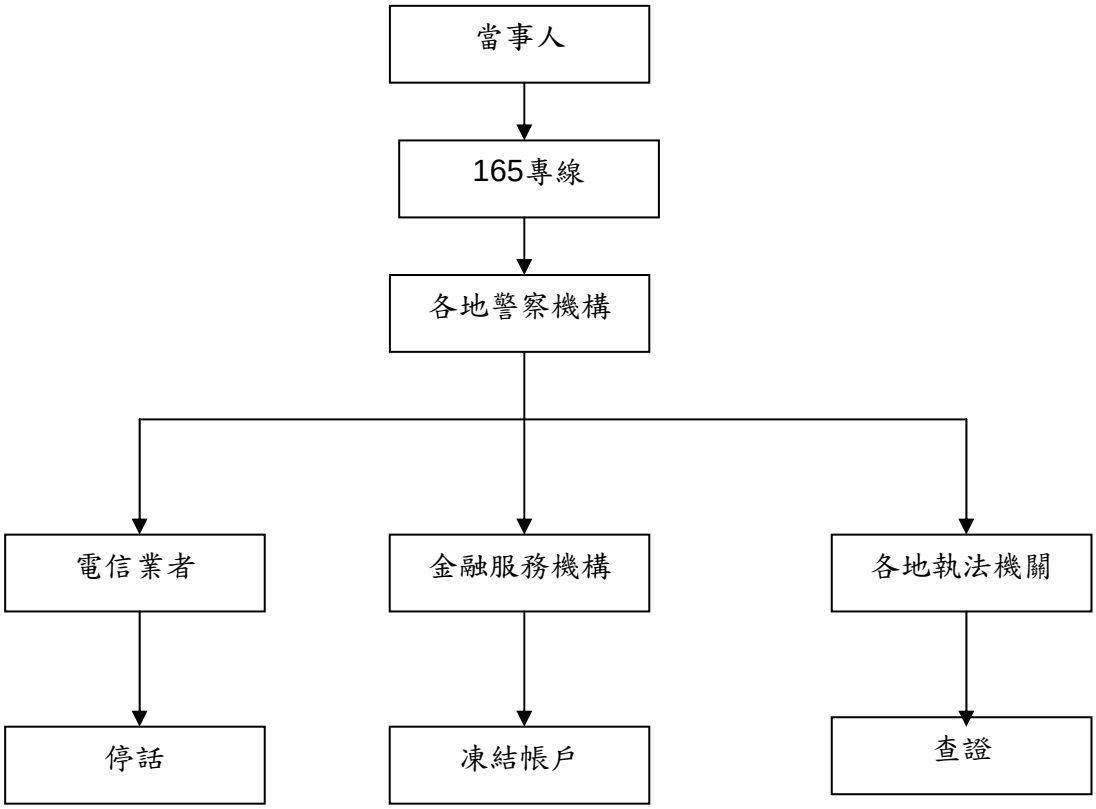
D. 整合各警察分局勤務中心及派出所詐騙電話電話受理流程。如此一來，各警分局勤務中心及派出所透過電腦提供案件受理及案件查詢畫面，而 110 勤務指揮中心在受理民眾檢舉案件時，也會將檢舉資訊送至 165 反詐騙諮詢專線，彙集合併後由專人進行後續偵查、停話、復話、偵查、人頭約制作業，建立案件追蹤考核制度，全天候提供民眾即時諮詢服務，且提供民眾線上查詢及網路報案功能，而該新據點也因此被視為新設的「全國反詐騙中心」。[46]

就「165 防詐騙諮詢專案」之通報運作機制而言，本研究以為，政府藉由公權力之介入，有效提升人民對於相關諮詢的可信度與犯罪通報的意願，並且得以即時掌握資訊，實施停話及凍結帳戶的強制行為，同時展開司法偵查工作，降低犯罪行為之危害擴散程度，為此機制之優點。但是，該通報機制的建立目前恐仍無明確法源依據；對於停話及凍結帳戶等強制行為之規範仍散見於其他法律(如電信法及銀行法)，。此運作機制，在短期內可為建立網路釣魚通報機制參考之依據，但若要強化「165 防詐騙諮詢專案」，做為長期

[46] 內政部警政署:http://www.moi.gov.tw/outline2007/8.htm,最後到訪日:2007 年 11 月 6 日。

性各類詐欺犯罪(包括網路釣魚)通報之平台，並實施強制性手段，則仍有待立法或修法之補強與授權為宜。

圖　十二、「165 防詐騙資訊專線」報案流程圖



資料來源：本研究自行整理

7.2.5. 自發性網路釣魚通報機制

不同於上述有組織性及完整架構的通報機制，自發性網路釣魚通報機制主要是由民間資安專家透過駭客論壇(如Zone-h[47])進行資訊交換，或以自行開發的偵測工具進行掃描，發現網路上被植入惡

[47]Zone-h unrestricted information有一個龐大的資料庫，能夠詳實記載是否曾經被入侵過，當然也得該入侵者曾經在此註冊並且回報過。由於其以『網路溫度計』自稱，所以會提供非常多的數據與新聞，因此很多的資安事件都可以在這邊獲得第一手的訊息。Available at: http://www.zone-h.org/ (最後到訪日：2007/12/10)

意連結之網站後，將其所蒐集到的資料公布於其個人的網站上(如大砲開講[48]或資安之眼[49])，或透過雜誌刊物(如資安人)定期公布，以提醒相關單位及民眾注意各類網站的安全問題。

本研究以為，透過不限背景各類資安專家的協助，更能強化國際資訊的連結。然而，透過實務訪談可知，由民間資安專家自發性提供釣魚網站消息的模式，因無公權力背書，且無標準的通報流程，在運作過程中可能面臨以下問題而無法收到即時通報之效[50]：

A. 資安專家欲通知受害網站單位時，找不到負責單位聯絡方式；
B. 資安專家於通知相關單位時遭懷疑為詐騙集團；
C. 被通知單位雖於接受通知後加以改善，但隨即又被植入惡意連結或惡意程式；
D. 相關單位於接獲通知後，無專業能力加以改善。

7.2.6. 比較與分析

綜觀我國目前各類資安與犯罪聯防機制，「資安事件」與「犯罪案件」在概念上似乎仍明顯切割；受限於法源，警示與聯防的機制亦僅限於各別產業與執法機關間。但從美國結合各產業 ISACs 組成資訊分享與分析協會(ISACs Council)的策略與 APWG 的運作經驗可知，結合金融與電信的詐欺犯罪手法利用網路科技的特性不斷在更新，各產業已不能劃地自限，各類資安或犯罪的訊息必須思考跨金融、電信、或其他電子商務產業間的「雙向」流通，始可能發揮聯合防制的效益。（我國目前可見各類通報機制是否適於援引作為釣魚通報機制平台的比較與分析如**表 二**所示）。

[48] 大砲開講available at：http://rogerspeaking.blogspot.com/ （最後到訪日：2007/12/10)
[49] 資安之眼http://www.itis.tw/compromised, 最後到訪日：2007 年 12 月 10 日。
[50] 參考本專案執行訪談「資安人」主編之訪談記錄

	優點	缺點	評估
政府機關(構)資訊安全通報應變機制	針對資安事件之等級不同而有不同的對待處理方式，並設有專責單位因應之	「管理要點」之位階不足，無法擴及其他政府機關(構)、地方政府或民間企業	僅以「行政院暨所屬各機關資訊安全管理要點」規範通報應變作為最高規範，若要擴及其他機關(構)、地方政府或民間企業，將受限於「管理要點」之位階，無法作為網路釣魚之通報機制
165 防詐騙諮詢專線	得以透過公權力介入通報機制，實施強制行為，及時停話及凍結帳戶，並同時展開司法偵查工作，可儘速控制犯罪行為之危害擴散，以及提供民眾諮詢之管道	通報機制本身並無法源依據，執法機關實施強制行為時恐有侵害人民權利之虞	短期內對於建立網路釣魚通報機制為可能參考之依據，但就建立長期通報機制且實施強制性作為而言，仍建議強化法律授權為宜
金融業資安事件通報機制	建立產業間之資安事件通報	僅就各產業間建立通報平台及機制，	對於建立全面性的資安事件

	優點	缺點	評估
	平台及機制將有助於瞭解針對不同產業之特殊攻擊手法，且能透過同業間之解決方式為借鏡，及時並有效地防範資安事件	且無公權力實施強制行為之介入，對於及時因應及防範之效果有限	通報機制於法規範上仍有不足之處
金融機構警示帳戶聯防機制	法律授權較明確，且有公權力介入，對降低詐欺損害有相當助益	聯防機制之啟動，以警方受理報案為實施之依據。釣客僅實施前階段個人資料蒐集的行為時，民眾欠缺報案之可能性	短期內對於建立網路釣魚通報機制仍為可能參考之依據
自發性網路釣魚通報機制	透過資安專家開發工具之協助，更能有效掃瞄到全球之惡意網站	無公權力之介入，且無一定的通報流程，對於網路釣魚資安事件之防範有限	以此作為網路釣魚之通報機制在資安事件之防範上顯有不足

表 二、我國資安事件通報機制之比較

8. TWNIC 於通報機制中定位之討論

透過對於各類型通報機制之討論，不難發現建立有效之通報機制對於網路釣魚犯罪之防範具有重大意義。然而，若欲建立有效之網路釣魚通報機制，則不可忽略台灣網路資源中心(Taiwan Network Information Center，簡稱 TWNIC)在通報機制中可發揮之效力。故本文以下將就 TWNIC 於通報機制中之定位加以分析，並檢討現行法制規範下可能產生之爭議，進而提出法制建議，俾使 TWNIC 未來在協助落實釣魚犯罪通報機制的同時，不致引發爭議。

8.1. TWNIC 參與通報機制運作之必要性

因 TWNIC 依電信法第 20-1 條之規範負責分配、註冊管理台灣地淤網際網路位址，並提供網際網路位址反解系統(Reverse Domain Name System)正常運作及相關註冊管理之服務事項，常導致外界對於網路釣魚此類詐欺之成因與網路名稱註冊之機制多做聯想。然而，在本研究在探索相關技術與成因後以為，網域名稱的分配與網路釣魚犯罪的關聯性並未如外界想像之大，因為網路釣魚行為得以成功的關鍵，仍在於網路釣客事先預設幾可亂真的假網站，與可讓使用者誤以為真的網址遮蔽技術，該假網站是否有真實獨立的網址，並非所問。據此，打擊網路釣魚犯罪的重點，便在於如何能夠即時發現與即時阻斷外界對該網站的接取。

綜上所述，對於追求執法時效的網路釣魚犯罪，若可透過 TWNIC 暫停位址解析的策略，協助執法單位即時阻斷潛在被害者接取虛假的網站，便可降低潛在被害者受害之人數，減少網路釣魚因此造成之危害。

即便 TWNIC 可透過暫停位址解析的方式，幫助減少網路釣魚犯

罪之受害者，但仍須考量此一方式將可能導致網路位址之使用者遭受損失。若事後發現該網路位址並非釣魚網站，則 TWNIC 或可能必須賠償該網路位址使用者之損失。換言之，若欲 TWNIC 在網路釣魚通報機制中發揮作用，應先確認 TWNIC 配合通報機制而暫停位址解析是否有法定事由而得以免於事後可能之損害賠償責任。

8.2.法源依據及其可能產生之爭議

根據電信法第 20-1 條第 7 項及第 8 項之規定，從事電信網際網路位址及網域名稱註冊管理業務之機構應為非營利法人組織，而 TWNIC 正是負責統籌網域名稱註冊及網路位址發放之財團法人組織。雖然根據電信法第 22 條規定，若電信之內容顯有妨害治安者，電信事業得拒絕或停止其傳遞，但由於 TWNIC 並非經營電信服務供公眾使用之事業 ，故 TWNIC 暫停位址解析之行為並不符合上述規定，亦無法以此為免責事由。此外，檢視 TWNIC 之「網際網路位址(IP Address)註冊管理業務規章」 之規定，當中並未就網際網路位址使用人之責任加以規範，故 TWNIC 亦無法以網路位址使用人之使用不當或不法作為暫停位址解析之事由。

為解決此一問題，建議未來在設計網路釣魚通報機制時，應以法規明確規範 TWNIC 之定位，並賦予其配合司法單位之公文書為暫停位址解析行為之責，在實施上，或可仿效金融機構警示帳戶聯防機制運作之策略，以法院、檢察署或司法警察機關之公文書通知為依據，但得以簡化的程序或期限內的補辦為前項通知為宜。如此一來，不僅可使 TWNIC 之暫停位址解析行為合法化，一旦其暫停位址解析行為造成使用者之損失，TWNIC 可不必負擔損害賠償之責。再者，亦可透過流程之簡化，使得網路釣魚之假網站得以即時取下，以防止網路釣魚造成之危害擴大。

8.3. 小結

總結來說，儘管 TWNIC 之暫停位址解析行為對於網路釣魚通報機制及犯罪防制具有相當之重要性，然在現行法制規範下，TWNIC 並無得以正當化其暫停位址解析行為之事由，一旦事後發現其暫停位址解析之網站實非釣魚網站，則 TWNIC 可能面臨損害賠償等相關責任。故為使 TWNIC 能在網路釣魚通報機制中發揮其暫停解析之重大作用，未來在設計通報機制時，應以法規明訂 TWNIC 於通報機制之定位，俾使 TWNIC 得以依法配合通報機制之運作，協助司法機關防制網路釣魚犯罪行為。

9. 結論與建議

9.1. 網路釣魚的高獲利性將驅動更多犯罪者以更多樣性的技術嘗試進行犯罪

網路科技對執法單位帶來的最大挑戰，即是網路對犯罪者的遮蔽效果。由於網路科技具有可遠端遙控、可匿名性與可設定自動化操作的特質，讓犯罪行為人得以更少的人力與物力，在不需要與被詐騙人面對面接觸的情況下，對更多的民眾進行詐騙行為。而網路釣魚犯罪屬網路犯罪中高度獲利的經濟犯罪活動，未來勢必驅動更多的網路釣客嘗試以更多樣性的攻擊技術及手法來詐騙防範意識薄弱的民眾，於取得個人機敏資料後再來從事實質獲利的行為。

9.2. 網路詐欺犯罪防制重點仍在於即時發現與即時阻斷

本研究透過行為特徵與犯罪手法的分析後發現：

A. 網路釣魚已有國際化、組織化、犯罪工具模組化的發展趨勢。
B. 超過 9 成以上的網路釣魚都鎖定金融服務業，其他產業受到網路釣魚犯罪行為詐欺的比率明顯低於金融服務業。
C. 雖然大量的電子郵件與偽造網站仍是這類犯罪最常見的手法，但其行為態樣已不斷演變，犯罪者已經從被動等待使用者連線上網，到主動購買關鍵字廣告以誘騙使用者點擊，或利用真實網頁漏洞夾藏惡意程式等方式作為蒐集使用者個人敏感資料的手段。
D. 網路釣魚詐欺得以成功的關鍵，仍在於歹徒事先預設幾可亂真的假網站，與可讓使用者誤以為真的網址遮蔽技術，該假網站是否有真實獨立的網址，實非所問。在此前提下，打擊這類犯罪的重點，仍在於即時發現與即時阻斷外界對該網站之接取。

9.3. 建議主管機關應具體要求建立整合性金融業資安防護管理中心

國際間目前因為欠缺一致性的定義，對網路釣魚造成的危害至今無法有效評估。但為有效控制因科技文明之便捷造成之資安事件，維護網路秩序，保障人民權益，國際間目前均思考如何透過法律或政策工具，建立或強制性或自願性的資安事件通報與資訊分享機制。本研究以為，網路釣魚詐欺防制應是各界應共同關注及努力的問題。為建立我國網路秩序，抑制網路釣魚行為之氾濫，我國執法機關似乎有必要採取進一步措施，研議建立我國的網路釣魚通報機制。另由於已有實務統計顯示，超過 9 成以上的網路釣魚犯罪鎖定金融服務業（參本研究 3.2 實務界的統計數據），基於 80/20 法則，建議政府可以從強化金融機構通報機制著手。

除了現有的金融機構警示帳戶聯防機制，建議金融管理委員會應具體要求建立整合性的金融業資安防護管理中心 SOC，在作法上可授權中華民國銀行公會全國聯合會為之，由 SOC 負責監控重要銀行金融資訊系統的流量、維護網站的安全，由銀行公會協助與執法機關進行雙向的資訊交換與分享。若能有效遏止以金融服務業為對象的網路釣魚行為，當可收此犯罪防制一半之效；之後再思考循此成功模式，推廣至其他電子商務業者、網路服務提供 ISP 業者等。

9.4. 建議以「165 防詐騙諮詢專線」為基礎，結合金融機構警示帳戶聯防機制、自發性通報機制與金融業 SOC，建立雙向溝通的詐欺資訊交換平台

綜合以上對我國既有通報機制之討論，本文基於以下思考，以為我國若欲建立釣魚通報機制作可行的模式，可能以「165 防詐騙諮詢專線」為基礎，結合金融機構警示帳戶聯防機制、自發性通報機制與金融業 SOC，透過國家執法單位建立雙向溝通的詐欺犯罪通報平台最為可行。亦即，由公權力之介入以強化各方通報者之信賴，同時簡化通報流程，使網路釣魚事件能於網站平均存活天數

（3-4 天）內獲得解決，達到建立通報機制之效用。

A. 網路釣魚係利用各種不同手法，在當事人不知情情況下蒐集個人資料，以進行後階段的詐欺行為。法律定性應為刑法詐欺罪的「預備犯」。雖由於刑法對於預備犯之處罰以法律有規定者為限而未能規範及此，但從犯罪防範觀點而言，網路釣魚事件之通報採犯罪案件之通報機制及程序可能較為適當。
B. 釣客在灑網階段，不論是假冒商家名義寄送郵件，或設置假網站以誘騙使用者之行為，行為人均已觸犯著作權法相關罪責，在告訴權人提出告訴之後，執法機關仍可實施偵查並追訴犯罪。
C. 目前在立法院研議中的「電腦處理個人資料保護法草案」修正草案，將思考對意圖營利而竊取、洩漏個資之行為，由舊法之「告訴乃論」改為公訴罪。若如此，執法機關在知悉相關犯罪行為發生時，即有主動追查之義務。

透過此機制，不論是當事人或自發性的第三方，在發現網路上有不安全或異常的網路活動，如駭客活動、網頁漏洞或惡性程式散布可能涉及網路釣魚、資料竊取時，透過 165 專線進行通報，經警方初步確認與查證後，通知網站負責人進行網頁修補，或通知 ISP 業者立即將網頁取下，亦即，運用目前網路服務業者普遍接受的「通知即取下」原則，以防止更多使用者受害。本研究以為，此運作模式可杜絕民間自發性通報機制在通知時反遭懷疑為詐騙集團之疑慮，為短期內最可行的策略。

9.5. 簡化報案機制為網路犯罪防制當務之急

以「165 防詐騙諮詢專線」為基礎，透過國家執法單位建立雙向溝通的詐欺犯罪通報平台雖然在策略思考上最為可行，但本研究必須指出，為收緊急通知與緊急處理之效益，「165 防詐騙諮詢專線」

在定位上可能仍以單純的通報平台為宜。至於通報平台後方是否連結警方的報案機制，可以再行研議。

網路犯罪目前實務上比較棘手的問題，在線上報案不被認為是正式報案，被害人或犯罪告發者必須根據不同 IP 所指涉之不同犯罪地點，到不同地區的警察機關報案。有業者即指出，即使業者自願投入資源去追蹤疑似釣魚犯罪者的 IP，但因為網路釣魚組織化、工具化與自動化的趨勢，犯罪者可以遠端遙控成千上百個被植入木馬的電腦進行犯罪，一次犯罪涉及到的 IP 可能成千上百個；如果報案機制堅持一個不同的 IP 即需被判斷為不同的案件，需由不同的單位受理，則一來會造成業者困擾，二來執法機關無法收綜觀全局之效。如何簡化報案機制，實為網路犯罪防制當務之急

9.6. 建立跨產業通報機制法制有立法之必要性

本研究以為，結合金融與電信的詐欺犯罪手法利用網路科技的特性不斷在更新，各產業已不能劃地自限，各類資安或犯罪的訊息必須思考跨金融、電信、或其他電子商務產業間的「雙向」流通，始可能發揮聯合防制的效益；透過立法方式，明確建立對通報機關(構)、通報義務人及資訊分享進行規範仍是長遠可行之策略。

現階段行政院金融監督管理委員會或內政部警政署，或可透過解釋將資安事件解釋為行政監督事項之一環，在立法規範外建立可行的資安事件以及犯罪案件通報機制，但此種策略只能一時解決法源不足之爭議，就建立長期通報制度而言，可能仍需透過立法方式加以解決。未來我國若能比照先進國家以法律明確規範資安事件和犯罪案件事項之通報，以及後續相關強制行為等相關事宜，相信在通報機制上更能於法有據，且能有助於國家社會減少因資通安全事件或網路犯罪事件造成之損失；對於業者而言，若遇有資安事件或

犯罪案件發生，亦可遵循相關法律規範處理，保障其客戶權益，並避免業者因畏懼受罰而隱匿不報帶來更嚴重之後果；對於網路使用者或消費者而言，亦能獲得有效之諮詢管道及更為安全之網路使用環境。

9.7. 強化民眾之教育

因網路釣魚這類犯罪僅依靠執法人員或者企業的力量來對抗網路釣魚犯罪明顯不足，因此仍建議強化民眾之網路安全教育，並加強對於網路釣魚防範措施的宣導，並能使其妥善應用現有的通報與資訊交換之機制，讓民眾對於網路釣魚犯罪型態有基本認識，提醒民眾對於來路不明的信件或發現網頁異常時，應多方查證，始不至於落入釣魚的陷阱。

最後，網路釣魚犯罪的技術手法多變，又因其利用網路匿名性、跨國性及即時性的特色，使得執法更為不易，因此，防範網路釣魚不能僅靠執法人員的力量，還須仰賴各界之配合，從多種可能防範的管道去著手，始能有效遏止網路釣魚犯罪對於國家、社會及網路使用者造成的影響。

10.附件

10.1. 警政署資訊室主任

網路釣魚訪談記錄

訪談時間：96 年 10 月 30 日

訪談地點：內政部警政署

訪談對象：警政署資訊室李相臣主任

訪談記錄：

一、 您認為網路釣魚最大的成因是？

網路釣魚主要目的在於取得個人身分資料，作為身分盜用及網路犯罪之用，以獲取金錢上的利益。

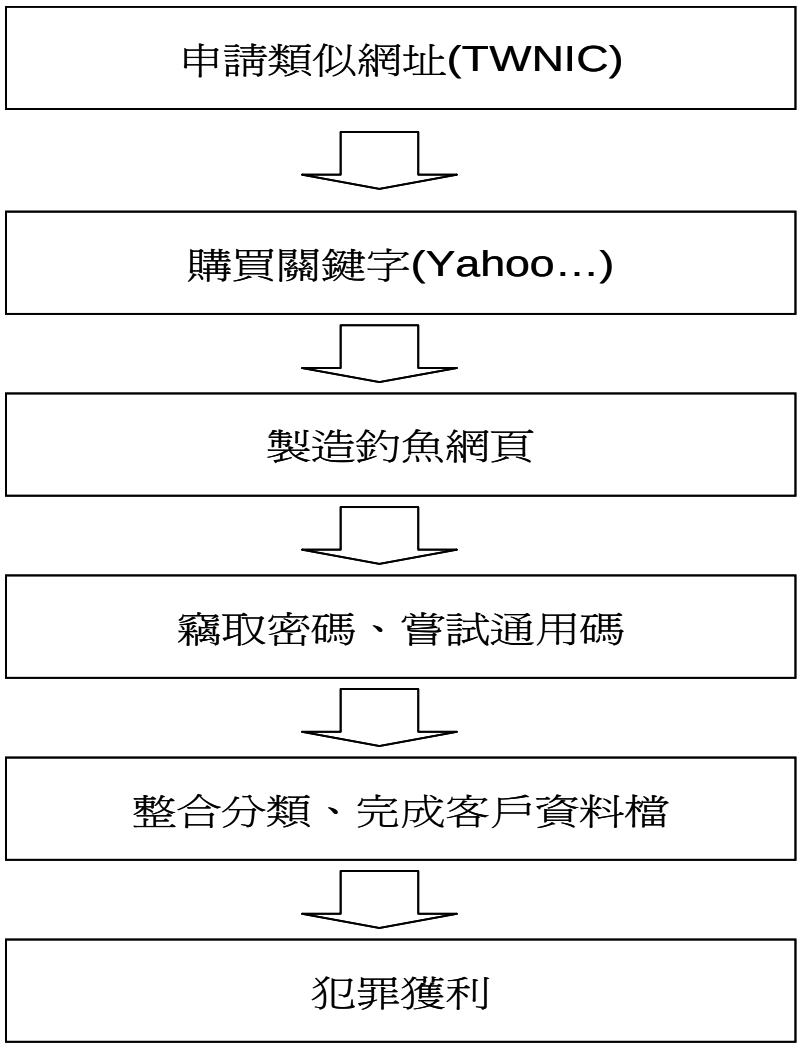
二、 對於垃圾郵件作為網路釣魚詐欺手法有何因應方式？目前還有哪些新的釣魚手法？

(一)、目前較新的網路釣魚手法為利用網頁搜尋購買「關鍵字」的方式刊登廣告，詐欺民眾進入其網頁，進而植入木馬程式，以竊取電腦使用者的個人資料。

(二)、亦有透過含有木馬程式的信件給高評價的網路拍賣賣家，藉機竊取賣家電腦內儲存之眾多買家資料，聯絡買家以進行詐騙。例如，ATM 修正匯款說帖詐騙，即詐騙集團假冒拍賣賣家，

指稱之前購買拍賣物品時，因 ATM 操作錯誤導致每月分期付款，會連續扣款 12 個月，要求買家至自動提款機辦理「分期付款解除設定」，不知情之被害人因而轉帳至詐騙集團帳戶內。

網路銀行犯罪流程：



三、 就政府端、民間企業及使用者端而言，您分別有何可能的防範建議及策略？

為因應業者提供「關鍵字」行銷服務，政府主管機關(目前面臨可能沒有主管機關)應令其加上「廣告」或「行銷」的字樣，提

醒網路使用者，以降低網路使用者進入錯誤網站的風險。另外，政府亦應向民眾進行教育或宣導，以避免誤入假網站，遭犯罪集團植入木馬程式，並蒐集個人資料以做詐欺之用。

四、 對於網路釣魚您有何執法建議？

可與 ISP 或 TWNIC 合作，使其關閉網路釣魚網站連結。對金融機構而言，針對網頁掛馬的釣魚手法，金融機構通常會利用電腦重新開機時自動檢查網頁的原始碼是否遭到竄改，以避免因網頁掛馬而導致客戶受害。

五、 您是否贊成建立網路釣魚通報平台/機制？贊成的話，應如何建立？反對的話，原因為何？是否另有其他因應措施？

贊成建立通報平台/機制：

(一)、同意透過警政署委託 TWNIC 之方式建置網路釣魚通報機制：由 TWNIC 建構通報平台，接受當事人或第三人之通報，並由警政署查證是否為網路釣魚網站，發現為網路釣魚網站時即通知 TWNIC。若為.tw 之網址，則 TWNIC 應立即解析該網址，禁止網路使用者連結該網址。

(二)、若並非.tw 的網站，則 TWNIC 應通知該國之 NIC，關閉該網站的連結。

10.2. 資安人雜誌

網路釣魚訪談記錄

訪談時間：96 年 10 月 29 日

訪談地點：內湖

訪談對象：「資安人」雜誌侍家驊總召集人及余俊賢主編

訪談記錄：

一、 您認為網路釣魚最大的成因是？

網路釣魚最大個目的是取得個人身分資料，作為身分盜用及網路犯罪之用，以獲取金錢上的利益。

二、 對於垃圾郵件作為網路釣魚詐欺手法有何因應方式？目前還有哪些新的釣魚手法？

各種管道都可能被利用作為網路釣魚的工具，比如，電子郵件是最直接被利用作為網路釣魚的工具之一，其他還包括 VoIP、P2P、Web URL 或 Domain name 詐欺。事實上，網路釣魚的手法將可能隨著科技的進步而有更多不同的工具用以行使網路釣魚詐騙，但萬變不離其宗：獲取更完整的資料，以詐取更多金錢利益。

三、 就政府端、民間企業及使用者端而言，您分別有何

可能的防範建議及策略？

政府應加強使用者的資安意識，比如反詐騙宣導，並積極做好資安工作，打擊網路犯罪。另外，建議政府有關單位，應著手規劃資安法制的草擬工作，及早建立資安法制，以促使資安法制能夠完備。

四、 對於網路釣魚您有何執法建議？

關於網路釣魚的執法建議，可參考美國政府，於總統府之下成立「防範身分盜用工作小組」，從上而下針對各種身分盜用犯罪進行法制、教育及政府防衛安全上的研究。再者，亦可透過政府或民間企業之工會組織（依產業別而定），成立監控基金及建立執法之監控組織。

五、 您是否贊成建立網路釣魚通報平台/機制？贊成的話，應如何建立？反對的話，原因為何？是否另有其他因應措施？

贊成建立通報平台/機制：

(一)、可與國際接軌，強化 TWCERT 之運作效能，建立資訊分享平台，以因應網路釣魚等事件之危機處理與協調。或參考美國「資訊分享與分析中心」(Information Sharing and Analysis Center，ISAC)建立事件與情報蒐集、分析並產生對策的能力，

以及建構溝通聯防的平台的協議，以因應政府及民間企業之資安事件。

就目前「資安人」雜誌於發現惡意網站而通知受害之當事人時，常面臨以下問題：

1、 資安專家欲通知受害網站單位時，搜尋不到負責單位之聯絡方式；
2、 資安專家於通知相關單位時遭懷疑為詐騙集團；
3、 通知後並加以改善，但隨即有被植入惡意連結或惡意程式；
4、 相關單位於接獲通知後，無專業能力加以改善。

(二)、建議透過警政署委託 TWNIC 或者中華電信執行之方式建置網路釣魚通報機：由 TWNIC 或中華電信建構通報平台，接受當事人或第三人之通報，並由警政署查證是否為網路釣魚網站，發現為網路釣魚網站時即通知 TWNIC 或中華電信關閉網站。對於判斷為網路釣魚網站之認定上除有故意或過失外，則不予賠償亦不負相關之責。

(三)、對於通報機制的建立，建議先由金融機構開始(80/20 法則)，要求金融機構對金管會之通報項目增加「網路釣魚」一項，再將金融機構通報機制之成功經驗推廣至電信產業。

(四)、建議政府及相關產業公會利用保險及基金方式，對於通報

之機構因該次通報事件所造成的損失給予補償，以鼓勵當事人積極通報。

10.3. 中華電信資安辦公室

網路釣魚訪談記錄

訪談時間：96 年 10 月 29 日

訪談地點：內湖

訪談對象：中華電信資安辦公室吳怡芳主任及資安技術研發組李倫銓組長

一、 您認為網路釣魚最大的成因是？

據我們的調查與研究，網路釣魚之成功率並非很高，大約數百個人中，僅會有幾個不小心遭詐騙成功，但光這幾個受害者，就足以讓網路釣客獲益，因此網路釣魚案件之所以持續存在，主因是因為其『有利可圖』，且仍有一些民眾，本身對於安全意識較為不足，或是不注意而成為網路釣魚詐欺的主要目標族群。

二、 對於垃圾郵件作為網路釣魚詐欺手法有何因應方式？目前還有哪些新的釣魚手法？

目前垃圾郵件問題仍無極有效的解決方案，且目前許多新的釣魚手法並非僅使用垃圾郵件來散佈詐欺郵件。目前據我們調查，有網路釣客研究搜尋引擎的排行機制，將自己所登錄之假網站，拉抬搜尋結果的排行，其手段可能利用購買廣告、大量點擊等等，一旦民眾在搜尋引

擎上搜尋網站(例如:搜尋台灣銀行)，搜尋引擎便回傳假網站首頁而非真的銀行網站首頁。另外，亦發現有許多釣魚手法，會使用 IM 來進行散播，植入 Keylogger(鍵盤側錄程式)，直接盜取電腦中的帳號密碼資料，回傳至駭客主機，根本不需架設假網站。

三、 就政府端、民間企業端及使用者端而言，您分別有何可能的防範的建議及策略？

在解決資安問題部分，不論駭客入侵事件、垃圾郵件或是釣魚網站，許多人都以為，需靠政府端制定相關法律，但實際上並不那麼單純(實際上，法條已經訂出，而執行成效?)，網路犯罪並非像傳統犯罪一樣，許多地方更難判定與追查，就算訂定法律，也只會導致執法機構的困難，需在意的是「可用」與「合理」之法條與執行判例來嚇止犯罪者。另外，政府端可以發展或聚集資安能量，像是輔導或建立多個資安技術/事件處理單位，以便擴大國家資安偵測能量，例如，當駭客架設釣魚網站，要能在最短時間內偵測且移除，不讓民眾有接觸到釣魚網站的時間差。對於企業端，由於目前中小企業並無專屬經費專人負責安全事宜，此類防範可交由 SOC 或是專業安全委外，讓專業安全公司負責相關訊息與防禦措施。而個人端，可由教育宣導等安全課程，來彌補前端偵測單位可能的漏網之魚(釣魚網站)。

四、 對於網路釣魚，您有何執法建議？

目前並非沒有法條!而的確是執法問題，由於Cybercrime(網路犯罪)一直都是難以判定與追查,因此目前大部分執法機構多是利用交叉比對或是其他證據來起訴相關案例。另外，目前國內有一個最大問題便是跨國性之網路詐欺案件，根本無法越洋追查與起訴，許多網路釣魚案件，以國外處理方式為例，國外駭客入侵國內主機架設國外假銀行釣魚網站，來詐騙國外使用者，連國外執法單位都只能告知我方相關ISP進行處理移除而無法追查，更遑論我方執法機構，發現國外駭客入侵國內主機，就算知道對岸何人所為，也沒有相關引渡或國際處理原則。許多網路釣魚網站主機多遭入侵而架設，本身主機擁有者本身更覺得自己也是受害者，而這類是否應歸類於”協同犯罪”或是不知者無罪”？若是強制訂定、執行自身主機遭入侵被當跳板或架設釣魚網站需負刑責之法令,又惹民怨,這是目前執法上最大的困難點。

五、 你是否贊成建立網路釣魚通報平台/機制？贊成的話，應如何建立？反對的話，原因為何？是否另有其他因應措施？

目前,國際反釣魚網站組織皆已”釣魚網站存活時間”來判定該國家或ISP之處理能力，對於建立釣魚網站通報平台/機制的確可以讓”釣魚網站存活時間”降低。而由ISP或由國家成立法人機構,建立機制、統籌協調、彼此分享資訊、並可提供對民眾的安全意識教育訓練

或宣傳，會是可行的做法。

10.4. 「銀行業通報重大偶發事件之範圍及適用對象」

發文機關：行政院金融監督管理委員會

發文日期：96.03.06

發文字號：金管銀(三)字第 09685001530 號令

業務類別： 其他類

機構類別： 金融機構類

重新發布「銀行業通報重大偶發事件之範圍與適用對象」相關規定。

一、所稱銀行業指金融控股公司、本國銀行、外國銀行、信用合作社、票券金融公司、信用卡公司、信託投資公司、郵政公司。

二、所謂重大偶發事件指：

(一)人為或天然災害（如：地震、水災、火災、風災等)。

(二)內部控制不良之舞弊案或作業發生重大缺失情事。

(三)安全維護方面(如：搶奪強盜、重大竊盜、行舍或設備遭破壞或遭恐嚇等)。

(四)業務方面(如投資或放款)有重大財物損失。

(五)媒體報導足以影響銀行業信譽。

(六)資金流動性不足恐有擠兌之虞者或擠兌存款。

(七)發生資通安全事件，且其結果造成客戶權益受損或影響機構健全營運。

(八)於連續放假期間（併同週休二日或補假形成連續放假 3 日【含】以上），自動櫃員機可用率（指可提供服務且不缺鈔之自動櫃員機佔全部自動櫃員機比率）低於百分之九十五，且未能提供服務之自動櫃員機超過 5 台以上。

(九)其他重大事件。

三、所謂其他重大事件，非僅以損失金額為絕對要件，其他雖未

造成任何金額損失之非量化事件，其有危及銀行業正常營運及金融秩序者，亦屬之。

四、銀行業發生重大偶發事件應立即通知治安或其他有關機關採取緊急補救措施，並應依下列方式申報：

(一)銀行業負責人應儘速以電話及書面傳真向中央銀行及中央存款保險公司(除票券金融公司外)報告。

(二)銀行業負責人應儘速以電話及網際網路申報系統向本會銀行局報告。本會銀行局重大偶發通報電話：02-89691294，傳真：02-89691397，申報網址為：https://ebank.banking.gov.tw（程式代號為 WB020W），如有資訊操作疑問，請向本會銀行局資訊室窗口：02-89689877 洽詢。

(三)銀行業負責人應於發生重大偶發事件一週內函報詳細資料或後續處理情形。

五、違反以上各點之規定者，得視情節輕重予以適當之處分。

六、行政院金融監理管理委員會九十四年六月十六日金管銀（三）字第〇九四三〇〇〇二四三號令同日起停止適用。

正本：（貼本會公告欄）

副本：行政院法規委員會、中央銀行、中央存款保險股份有限公司、行政院金融監督管理委員會檢查局、本會銀行局(一至六組)

10.5. 「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」

第一條　本辦法依銀行法第四十五條之二第三項規定訂定之。

第二條　本辦法所稱存款帳戶，指銀行法第六條至第八條所稱之支票存款、活期存款及定期存款帳戶。

第三條　本辦法用詞定義如下：

一、警示帳戶：指法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示者。

二、衍生管制帳戶：指警示帳戶之開戶人所開立之其他存款帳戶。

三、通報：指法院、檢察署或司法警察機關以公文書通知銀行將存款帳戶列為警示或解除警示，惟如屬重大緊急案件，得以電話、傳真或其他可行方式先行通知，並應即補辦公文書資料。

第四條　本辦法所稱疑似不法或顯屬異常交易存款帳戶之認定標準及分類如下：

一、第一類：

（一）法院、檢察署因偵辦刑事案件需要，依法扣押或禁止處分之存款帳戶。

（二）存款帳戶屬偽冒開戶者。

二、第二類：

（一）屬警示帳戶者。

（二）屬衍生管制帳戶者。

三、第三類：

（一）短期間內頻繁申請開立存款帳戶，且無法提出合理

說明者。

（二）客戶申請之交易功能與其年齡或背景顯不相當者。

（三）客戶提供之聯絡資料均無法以合理之方式查證者。

（四）存款帳戶經金融機構或民眾通知，疑為犯罪行為人使用者。

（五）存款帳戶內常有多筆小額轉出入交易，近似測試行為者。

（六）短期間內密集使用銀行之電子服務或設備，與客戶日常交易習慣明顯不符者。

（七）靜止戶恢復往來，且交易有異常情況者。

（八）符合銀行防制洗錢注意事項範本所列疑似洗錢表徵之交易者。

（九）其他經主管機關或銀行認定為疑似不法或顯屬異常交易之存款帳戶。

第五條　存款帳戶依前條之分類標準認定為疑似不法或顯屬異常交易者，銀行應採取下列處理措施：

一、第一類：

（一）存款帳戶依法扣押或禁止處分者，應即依相關法令規定辦理。

（二）存款帳戶如屬偽冒開戶者，應即通知司法警察機關、法務部調查局洗錢防制中心及金融聯合徵信中心，銀行並應即結清該帳戶，其剩餘款項則俟依法可領取者申請給付時處理。

（三）依其他法令規定之處理措施。

二、第二類：

（一）存款帳戶經通報為警示帳戶者，應即通知金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行。

（二）存款帳戶屬衍生管制帳戶者，應即暫停該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付功能，匯入款項逕以退匯方式退回匯款行。

（三）依其他法令規定之處理措施。

三、第三類：

（一）對該等帳戶進行查證及持續進行監控，如經查證有不法情事者，除通知司法警察機關外，並得採行前二款之部分或全部措施。

（二）依洗錢防制法等相關法令規定之處理措施。

第六條　銀行除依前條所列措施辦理外，並應於內部採取下列措施：

一、循內部程序通報所屬總行或總管理機構之專責單位。

二、將已採行及擬採行之處理措施一併陳報總行或總管理機構之專責單位。

三、於銀行內部資訊系統中加以註記，提醒各分支機構加強防範。

第七條　存款帳戶經法院、檢察署或司法警察機關通報為警示帳戶者，銀行應即查詢帳戶相關交易，如發現通報之詐騙款項已轉出至其他帳戶，應將該筆款項轉出之資料及原通報機關名稱，通知該筆款項之受款行，並通知原通報機關。

警示帳戶之原通報機關依前項資料進行查證後，如認為該等受款帳戶亦須列為警示帳戶者，由該原通報機關再進一步通

報相關銀行列為警示。

詐騙款項之相關受款行，應依第一項規定辦理交易查詢及通知作業，如查證受款帳戶有犯罪事實者，應即採行第五條第三款所列處理措施。

本條之通知方式、通知範圍及所需文件等作業程序，由中華民國銀行商業同業公會全國聯合會訂定，並報主管機關備查。

第八條　存款帳戶之款項若已遭扣押或禁止處分，復接獲法院、檢察署或司法警察機關通報為警示帳戶，該帳戶仍應列為警示帳戶，但該等款項優先依扣押或禁止處分命令規定辦理。

第九條　警示帳戶之警示期限自每次通報時起算，逾5年自動失其效力，但有繼續警示之必要者，原通報機關應於期限屆滿前再行通報之。

警示帳戶之開戶人對其存款帳戶被列為警示如有疑義，由開戶人洽原通報機關處理，銀行於必要時並應提供協助。

第十條　依法扣押或禁止處分之存款帳戶及警示帳戶，嗣後應依原扣押或通報機關之通報，或警示期限屆滿，銀行方得解除該等帳戶之限制。

屬衍生管制帳戶及依第四條第三款所列標準認定為疑似不法或顯屬異常交易之存款帳戶者，經銀行查證該等疑似不法或顯屬異常情形消滅時，應即解除相關限制措施。

警示帳戶依原通報機關之通報解除，或原通報機關依前條第一項再行通報銀行繼續警示者，銀行應即通知金融聯合徵信中心。

第十一條　存款帳戶經通報為警示帳戶，銀行經確認通報原因屬詐財案件，且該帳戶中尚有被害人匯（轉）入之款項未被提領

者，應依開戶資料聯絡開戶人，與其協商發還警示帳戶內剩餘款項事宜。

銀行依前項辦理，仍無法聯絡開戶人者，應透過匯（轉）出行通知被害人，由被害人檢具下列文件，經銀行依匯（轉）入時間順序逐筆認定其尚未被提領部分，由最後一筆金額往前推算至帳戶餘額為零止，發還警示帳戶內剩餘款項：

一、刑事案件報案三聯單。

二、申請不實致銀行受有損失，由該被害人負一切法律責任之切結書。

銀行依本條規定辦理警示帳戶剩餘款項之發還，如有下列情事之一者，得逕行結清該帳戶，並將剩餘款項轉列其他應付款，俟依法可領取者申請給付時處理；但銀行須經通報解除警示或警示期限屆滿後，方得解除對該帳戶開戶人之警示效力。

一、剩餘款項在一定金額以下，不符作業成本者。

二、自警示通報時起超過 6 個月，仍無法聯絡開戶人或被害人者。

三、被害人不願報案或不願出面領取款項者。

銀行應指定一位副總經理或相當層級之主管專責督導警示帳戶內剩餘款項之處理事宜。

疑似交易糾紛或案情複雜等案件，不適用本條所定剩餘款項發還之規定，應循司法程序辦理。

第十二條　銀行應建立明確之認識客戶政策及作業程序，包括接受客戶開立存款帳戶之標準、對客戶之辨識、存款帳戶及交易之監控及必要教育訓練等重要事項。

前項有關接受客戶開立存款帳戶之作業審核程序，由中華民國銀行商業同業公會全國聯合會訂定範本，並報主管機關備查。

第十三條　銀行受理客戶開立存款帳戶，應實施雙重身分證明文件查核，身分證及登記證照以外之第二身分證明文件，應具辨識力。

銀行應確認客戶身分，始得受理客戶開立存款帳戶，如有下列情形，應拒絕客戶之開戶申請：

一、疑似使用假名、人頭、虛設行號或虛設法人團體開立存款帳戶者。

二、持用偽、變造身分證明文件或出示之身分證明文件均為影本者。

三、提供之文件資料可疑、模糊不清、不願提供其他佐證資料、或提供之文件資料無法進行查證者。

四、客戶不尋常拖延應提供之身分證明文件者。

五、客戶開立之其他存款帳戶經通報為警示帳戶尚未解除者，但為就業需要開立薪資轉帳戶，並經銀行查證屬實者，不在此限，且不列為衍生管制帳戶。

六、受理開戶時有其他異常情形，且客戶無法提出合理說明者。

第十四條　銀行應以資訊系統整合其全行存款客戶之基本資料及交易資料，供其總分支機構查詢，對於各單位調取及查詢客戶之資料，應建立內部控制程序，並注意資料之保密性。

第十五條　由專業中介機構代為處理之交易、曾經通報為警示帳戶而已解除者、依第十三條第二項第五款但書申請開戶者、或其他經研判具高風險之存款客戶或交易，銀行除為一般性

之客戶審查措施外，另應有適當之風險管理措施，包括：

一、帳戶之開立應經較高層級主管之核准。

二、確認其財產及資金來源、去處之合理性。

三、對其存款交易實施持續監控。

第十六條　銀行應建立以資訊系統輔助清查存款帳戶異常交易之機制，對於交易金額超過一定門檻、交易金額與帳戶平均餘額顯不相當、或短期間內密集使用電子交易功能等狀況，應設立預警指標，每日由專人至少查核及追蹤乙次並作成紀錄，依內部程序送交權責主管核閱。

前項所稱紀錄及其相關資訊，至少應保存 5 年，並得提供主管機關、有關單位及內部稽核單位調閱。

第十七條　銀行之國外分行及子銀行在其所在國法令許可範圍內，應遵守本辦法之規定，但所在國之法令與本辦法牴觸時，銀行應將相關事實陳報主管機關備查。

第十八條　銀行應依本辦法訂定其內部作業準則，其內容應至少包括疑似不法或顯屬異常交易帳戶之認定標準及應採取之措施、第六條第一款所稱專責單位之指定、第十一條第三項第一款所稱一定金額、第十六條第一項所稱預警指標之建立、紛爭處理、員工教育訓練及稽核功能等。

第十九條　銀行應將前條所稱內部作業準則之規範納入內部控制及內部稽核項目，並依據銀行內部控制及稽核制度實施辦法之規定，辦理內部稽核及自行查核。

第二十條　本辦法除第十四條、第十六條、第十八條及第十九條自九十六年一月一日施行外，自發布日施行。

10.6. 「金融機構警示帳戶聯防機制」作業程序

壹、訂定依據及目的：

一、本作業程序係依據行政院金融監督管理委員會制定之「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」(以下簡稱管理辦法)第七條第四項及行政院金融監督管理委員會 95 年 7 月 26 日金管銀(一)字第 09510003090 號函訂定。

二、本作業程序主要規範存款帳戶經通報為警示帳戶所衍生之聯防機制及存款帳戶經民眾通知疑為犯罪行為人使用所衍生之聯防機制之相關通報作業，內容包含通報流程、通報範圍、通報方式及所需具備之文件等，俾供相關單位依循辦理。金融機構在接獲「檢警調通報設定警示帳戶」或「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」時，經查詢帳戶內之詐騙款項已遭歹徒轉出至其他金融機構帳戶時，應立即啟動聯防機制，通報該受款之金融機構，以協助檢警調阻斷詐騙資金之流出，遏止不法。

貳、金融機構辦理警示帳戶聯防機制作業程序：

一、存款帳戶經通報為警示帳戶衍生之聯防機制：

(一)警示帳戶所屬金融機構(即受款行)之通報窗口接獲法院、檢察署或司法警察機關（以下簡稱檢警調單位）開具之「受理詐騙帳戶通報警示簡便格式表」(以下簡稱簡便格式表)或相關通報公文等傳真文件通報警示帳戶時，除確認通報來源並依前述文件設定警示帳戶外，亦須查閱該警示帳戶內被通報之詐騙款項是否已轉出至其他金融機構；如款項已轉出，應立即填寫「金融機構聯防機制通報單」(以下簡稱通報單）傳真通知下一受款行之通報窗口。如款項已轉出至多家受款行，則須分別填寫「通報單」傳真通知各受款行。

(二)受款之金融機構通報窗口(或謂下一轉入行之通報窗口)

在接獲前一受款行傳真之「通報單」，應立即查詢受款帳戶之交易，如款項已遭轉出，則接續填寫前一受款行傳真之「通報單」，將轉出資料傳真通報下一受款行及之通報窗口。如款項已轉出至多家受款行，則須影印前一受款行傳真之「通報單」並分別接續填寫，再傳真通知各受款行之通報窗口。如款項已遭提領，則須將通報單傳真回報檢警調單位。

(三)受款之金融機構通報窗口(或謂下一轉入行之通報窗口)

在接獲前一受款行傳真之「通報單」，並應依「管理辦法」第七條第三項規定對該帳戶交易進行審慎查證，如查證受款帳戶確有犯罪事實者，則就被通報之受款金額做圈存或止扣；如帳戶餘額小於被通報之受款金額，則圈存帳戶目前餘額。

(四)於圈存或止扣後，如接獲「檢警調單位回報受款行設定警示帳戶通報聯」通知該受款帳戶須列為警示帳戶，則改設定為警示帳戶。

二、存款帳戶經民眾通知，疑為犯罪行為人使用衍生之聯防機制：

(一)受詐騙民眾於金融機構營業時間中，親自至任何一家金融機

構櫃檯告知遭受詐騙時：

1.金融機構櫃檯人員於確認民眾身分、匯款或轉帳單據及瞭解民眾被詐騙事由後，請民眾填寫「切結書」並撥打165報案電話。

2.金融機構憑切結書及匯款轉帳相關單據填寫「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」，再將此通報單及切結書傳真至受款行之通報窗口。

3.警察機關須於2小時內派員到金融機構受理民眾報案完畢並傳真「簡便格式表」至受款行之通報窗口。

(二)受款行之通報窗口

1.憑金融機構傳真之「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」及「切結書」，確認通報來源。

2.立即查詢受款帳戶之交易，如款項已遭轉出，則將款項轉出資料填寫於「金融機構聯防機制通報單」(以下簡稱通報單)，傳真通報下一受款行之通報窗口。如款項已轉出至多家受款行，則須分別填寫「通報單」傳真通知各受款行之通報窗口。

3.如款項已遭全數提領，則立即填寫「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」下聯之受款行通報窗口之處理情形並傳真回報給受理報案之警察機關。

4.受款行於接獲金融機構傳真之「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」及「切結書」時，並應依「管理辦法」第五條第三款規定，對該受款帳戶交易進行審慎查證，如經查證確有不法情事者，則就被通報之受款金額做圈存或止扣；如帳戶餘額已小於被通報之受款金額，則圈存帳戶目前餘額。

5.俟接獲警察機關傳真之「簡便格式表」或「檢警調單位回報受

款行設定警示帳戶通報聯」通知須列為警示帳戶，始改設定為

警示帳戶。

(三)後續受款行之通報窗口

1.憑前一受款行傳真之「通報單」，確認通報來源。

2.立即查詢受款帳戶之交易，如款項已遭轉出，則接續填寫前一受款行傳真之「通報單」，將款項轉出資料傳真通報下一受款行之通報窗口。如款項已轉出至多家受款行，則須影印前一受款行傳真之「通報單」並分別接續填寫，再傳真通知各受款行之通報窗口。

3.如款項已遭全數提領（即最後一家受款行），則將處理情形填寫於原「通報單」並傳真回報給受理報案之警察機關。

4.受款行於接獲前一受款行傳真之「通報單」，並應依「管理辦法」第五條第三款規定對該受款帳戶交易進行審慎查證，如經查證確有不法情事者，則就被通報之受款金額做圈存或止扣；如帳戶餘額已小於被通報之受款金額，則圈存帳戶目前餘額。

5.俟接獲警察機關回傳之「檢警調單位回報受款行設定警示帳戶

通報聯」通知須列為警示帳戶，始改設定為警示帳戶。

（四）倘協助受詐騙民眾辦理通報之金融機構本身即為受款行，其後續作業程序比照前項（二）之2、3、4、5點辦理。

參、上述「圈存或止扣」款項，自圈存或止扣時點起算，超過24小時後，仍未接獲警方之警示帳戶通報，則逕予解除圈存或止扣。惟該帳戶若有疑似不法或異常之情事者，得不予解除，或依據「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」第五條第三款規定為必要之處理。

肆、除警示帳戶外，上述「圈存或止扣」款項，經再審慎查證確無不法或異常之情事者，金融機構可提前解除「圈存或止扣」。

伍、原通報之檢警調單位或受理報案之警察機關經查證後，欲通報受款行之通報窗口設定警示帳戶時，僅須將通報內容填載於「金融機構聯防機制通報單」下聯之「檢警調單位回報受款行設定警示帳戶通報聯」，並傳真至受款行之通報窗口。

陸、金融機構辦理本項作業程序，若在事後經查證，無詐騙事實存在，惟因金融機構依本程序處理因而造成客戶權益受損或因款項被圈存致票據遭退票，金融機構應協助配合向台灣票據交換所申請註銷退票紀錄或協助為其他補救措施。

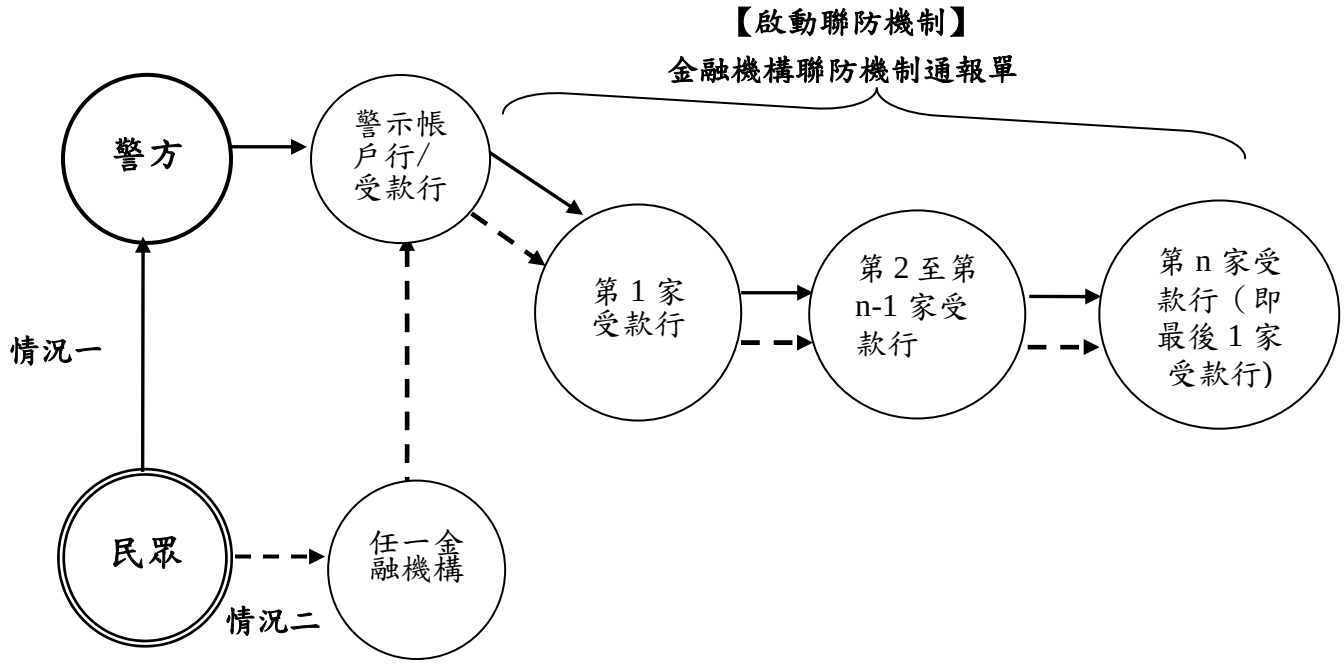
柒、各金融機構之通報窗口儘可能設於以 24 小時服務之電話客服中心（Call Center）為原則；倘各金融機構之通報窗口有異動時，應立即通報財金資訊股份有限公司，俾財金資訊(股)公司隨時更新提供最即時之金融機構通報窗口資料。(通報窗口詳財金公司建置之「警示帳戶通報機制聯絡窗口彙總表」)

捌、為配合檢警調機關偵辦與查證之需要，受款行應依相關規定協助提供相關交易資料及錄影帶。

玖、本作業程序未規定事項，悉依相關法令辦理。

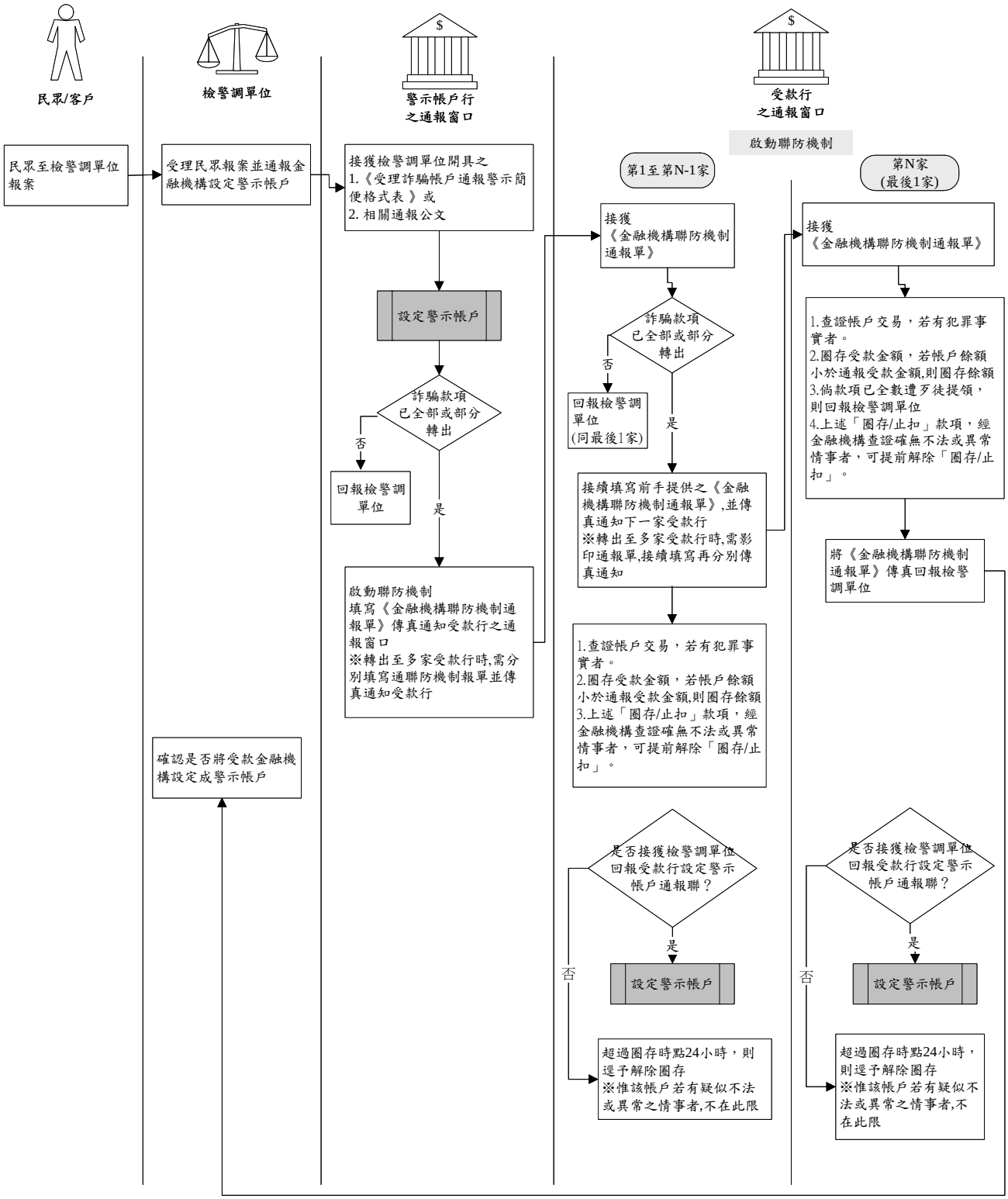
拾、本作業程序經本會理事會通過，報請主管機關備查後實施，修正時亦同。

聯防機制通報架構圖：


【啟動聯防機制】
金融機構聯防機制通報單
警方
警示帳戶行/受款行
第 1 家受款行
第 2 至第 n-1 家受款行
第 n 家受款行（即最後 1 家受款行)
情況一
民眾
任一金融機構
情況二

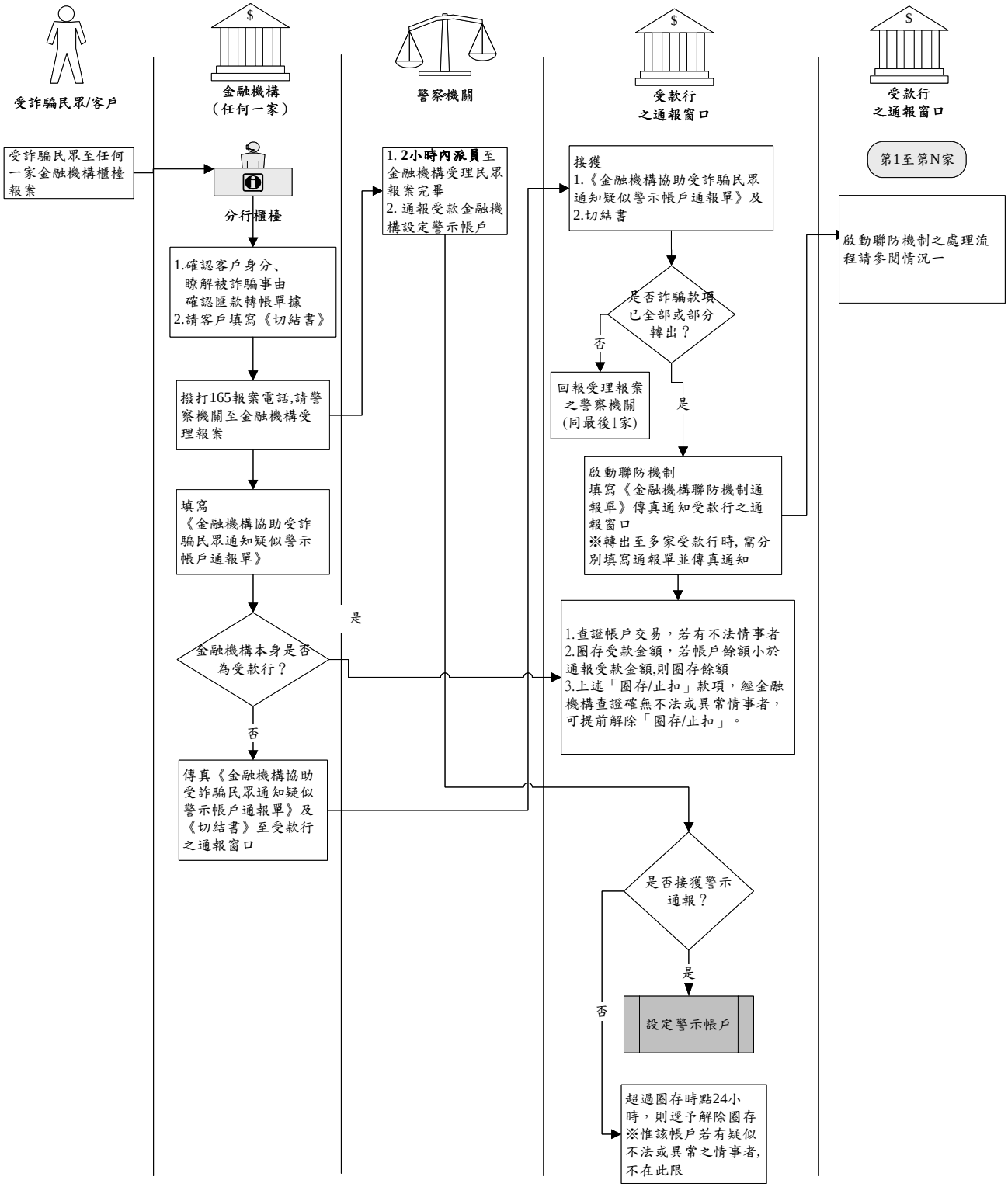
警示帳戶聯防機制作業程序流程圖

一、存款帳戶經通報為警示帳戶所衍生之聯防機制：



警示帳戶聯防機制作業程序流程圖

二、存款帳戶經民眾通知，疑為犯罪行為人使用衍生之聯防機制：



受文者：_____銀行　　【附件一】

_____檢警調單位/警察機關

金融機構聯防機制通報單

通報日期	年　月　日　時　分	通報警示帳戶之檢警調單位或金融機構名稱	
警察機關受理詐騙帳戶通報警示簡便格式表之案件編號			
原警示帳戶資料			
警示帳戶所屬金融機構名稱		警示帳戶戶名		警示帳戶帳號		匯入警示帳戶之金額	
通報窗口		聯絡人及聯絡電話		通報單位簽章	
警示帳戶轉出之受款帳戶資料					
1.受款行名稱： 受款帳號：　受款日期： 受款金額：		※受款行處理情形： □已圈存/止扣□已提現 □已轉出□已部份轉出 （圈存/止扣金額：　　） （圈存/止扣時間：　　）		經辦 主管	
2.受款行名稱： 受款帳號：　受款日期： 受款金額：		※受款行處理情形： □已圈存/止扣□已提現 □已轉出□已部份轉出 （圈存/止扣金額：　　） （圈存/止扣時間：　　）		經辦 主管	
3.受款行名稱： 受款帳號：　受款日期： 受款金額：		※受款行處理情形： □已圈存/止扣□已提現 □已轉出□已部份轉出 （圈存/止扣金額：　　） （圈存/止扣時間：　　）		經辦 主管	
4.受款行名稱： 受款帳號：　受款日期： 受款金額：		※受款行處理情形： □已圈存/止扣□已提現 □已轉出□已部份轉出 （圈存/止扣金額：　　） （圈存/止扣時間：　　）		經辦 主管	

----------檢警調單位回報受款行設定警示帳戶通報聯

轉入行名稱	轉入帳號	轉入金額	警局承辦人(職章)

通報日期：　　檢警調單位電

話：

主管(職章)：　　檢警調單位簽章：

受文者：_____銀行　　【附件二】

_____警察機關

金融機構協助受詐騙民眾通知疑似警示帳戶通報單

受理通知時間：　年　月　日　時　分				報案人及連絡電話： 報案人身分證字號： 報案人匯出帳號：
通知之疑似警示帳戶資料				
疑似警示帳戶所屬金融機構名稱		通知受款帳號		受款戶名： 受款金額： 受款日期：

受理本項通知之金融機構名稱	受理人	聯絡電話	受理單位核章

本案已撥打 165 或向當地警察機關報案。
(受理報案之警察機關名稱：　　)

註：金融機構櫃檯須將本通報單與受詐騙民眾所簽具之「切結書」，一併傳真至受款行之通報窗口。

----------受款行通報窗口之處理情形

處理狀況	受理人	主管	受款行後續追蹤情形
□**已設定圈存/止扣並凍結全部受款金額。**			□已接獲警方之「受理詐騙帳戶通報警示簡便格式表」，並登錄警示帳戶。 □圈存超過 24 小時，未接獲警察機關警示通報，逕予解除圈存/止扣登錄。
□**已設定圈存/止扣惟款項已全部/部分轉出。(見※)**			□已接獲警方之「受理詐騙帳戶通報警示簡便格式表」，並登錄警示帳戶。 □圈存超過 24 小時，未接獲警察機關警示通報，逕予解除圈存/止扣登錄。
□**詐騙款項已全數遭提領。**			□已接獲警方之「受理詐騙帳戶通報警示簡便格式表」，並登錄警示帳戶。 □圈存超過 24 小時，未接獲警察機關警示通報，逕予解除圈存/止扣登錄。

※勾選本項者，應另填具「金融機構聯防機制通報單」，速通報下一個受款之金融機構採取相關凍結款項之動作。

切　結　書

立切結書人相關資料			
姓　　名		身分證字號	
匯出帳號		聯絡電話	
住　　址			
受詐騙事由			
□假綁架親屬/小孩 □佯稱中獎 □假冒親友急須用錢 □以退稅/退費為由來電詐騙 □竊取個人基本資料詐財 □假消費、真詐財□小額信用貸款詐騙 □假冒電信公司催繳欠費 □網路交易詐欺□行動電話簡訊詐欺 □假冒身分詐欺 □刮刮樂彩券詐騙 □其他（請受害人簡要描述）			
匯入詐騙帳戶之款項資料			
匯款日期	年　月　日	匯入帳號	
帳戶戶名		匯款金額	新台幣　　元
匯款方式	□匯款　□ATM/網路轉帳　□現金存入		
切 結 聲 明			

立切結書人在此委託　貴金融機構協助速向該詐騙帳戶所屬之金融機構通報窗口辦理詐騙通報，並聲明上述所言均屬實，如有謊報，願負一切法律責任及損害賠償責任。　貴金融機構或其他受通報金融機構如因協助本項通報而受任何損害，立切結書人願負損害賠償責任。

此致

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿金融機構

立切結書人簽名：

切結日期：中華民國　　年　　月　　日