臺灣地區網路釣魚之偵防研究

A Study on Prevention and Investigation of Phishing in Taiwan

劉心玫
臺中市政府警察局資訊室
臺中市40708西屯區文心路二段588號
r77719@tcpb.gov.tw

廖有祿
中央警察大學刑事警察學系
桃園市33304龜山區大崗里樹人路56號
ylliaw@mail.cpu.edu.tw

摘要

網際網路與通訊科技的發達，加上智慧型手機的普及，人與人之間的溝通交流已不再受空間的侷限。正因通訊便利，使得以欺騙人類為主的釣魚網址透過網際網路通訊工具更加氾濫，讓使用者陷於錯誤而向加害者交付自己的機敏資料做為犯罪使用，本文針對臺灣地區網路釣魚犯罪進行研究，以期提供未來偵防相關案件時做為參考。本研究採案例研究與深度訪談的質性分析方法，透過蒐集臺灣警方偵辦過的網路釣魚案件並對有經驗之偵查人員進行訪談，彙整出網路釣魚案例的釣餌類型、散布手法，並進而歸納出網路釣魚犯罪可分為偽冒機構網站、建立虛假網站以及散布惡意程式連結等三種型態；亦從訪談偵查人員分析了解實務上網路釣魚案件偵辦現況，以及此類案件共同遇到的偵查困難為境外來源與受害事證無法串聯；另針對網路釣魚犯罪偵查與防制等二方面提出有效對策與建議。

關鍵詞: 網路釣魚、釣魚網站、社交工程。

Abstract

Communication between people is no longer subject to the limitations of space with the popularity of Internet, communication technology, and smart phones. Because of convenient communication facilities, the increasing spread of phishing website based on deceiving human is more flooded through Internet communication tools. That makes users carelessly give away confidential personal information to perpetrators as another crime. The study focused on phishing crime in Taiwan and the purpose was to provide a reference to investigate and prevent such crimes in the future. The survey used qualitative analysis with case studies and in-depth interviews. The data that phishing case investigated by Taiwan police was collected and experienced detectives were interviewed. The phishing bait and spread technique was founded and further generalized to three phishing types: disguising agency website, setting up fake websites and spreading malware linkage. It was also acknowledged that the difficulties with

investigation of phishing crime were cross-border link sources and unlinked victim evidences. The study findings may serves as effective countermeasures and recommendations in investigation and prevention on cyber phishing.

Keywords: cyber phishing, phishing website, social engineering

壹、導論

一、研究動機與目的

以欺騙人類心靈達成犯罪目的之犯罪行為亙古至今仍然持續存在，像是早期傳統的金光黨詐欺，而後藉由通訊科技演變成刮刮樂中獎簡訊，一直演變到透過電話或網際網路的假擄人勒贖詐欺、網路拍賣詐欺、假公務機關(人員)詐欺、解除分期付款詐欺等等，都是以欺騙人類心靈為手段，使受害者陷於錯誤而落入騙徒的陷阱，網路釣魚亦如是，而現今行動科技的便利助長了釣魚網址的氾濫，更造成使用者個人資料的嚴重危害，是不可輕忽的現象。

然而在網路釣魚的犯罪偵查上，偵查機關除持續積極走入社區或透過各種管道宣導預防詐欺，提醒民眾提高警覺、防止被害外，似乎仍無有效的偵查方法，因此本研究旨在以犯罪偵查角度探討網路釣魚案件之偵防，目的如下：

（一）了解臺灣目前所遭遇到的網路釣魚攻擊概況。

（二）分析網路釣魚攻擊的類型與欺騙手法。

（三）提出網路釣魚攻擊的偵防策略。

二、研究範圍

本研究站在犯罪偵查的立場，探討偵查機關面對網路釣魚案件所能提供之偵防作為以及協助，因此採取較廣義的網路釣魚定義，即以欺騙人心為出發點之網路釣魚行為，其中用來誘騙的網址不僅侷限於仿冒知名網站的網址，也包含設計成立虛假網站或以現有社群平台發布錯誤訊息的URL網址。至於並非使用URL型態的拍賣網站販賣虛有商品之詐欺，或是偵查人員以網路釣魚等引誘方式之誘捕偵查，則不在本文探討範圍內。

本研究範圍以上述原則蒐集臺灣地區所偵辦的網路釣魚案件進行分析，並透過訪談有經驗之偵查人員，整理網路釣魚案件類型與釣魚手法，進一步提出對應之偵防策略。

貳、文獻探討

一、網路釣魚與釣魚攻擊

（一）網路釣魚概念：

在網際網路行為中，並非所有的欺騙都是出於惡意的，有時候使用者只是為了隱私保護以及避免不必要的紛爭而有所隱瞞，例如使用暱稱。然而，以網路釣魚為主的欺騙，則是利用人性的弱點獲得訊息，以操縱受害者的心理來取代與系統安全防護技術正面對

決，有了這些資料，釣魚者便可輕鬆進入電腦系統或網路而不需要破解它們，並且提供更多的時間來犯案並逃避偵查[1]。

「網路釣魚」只是一種通稱，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(social engineering)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。另根據反網路釣魚工作小組(Anti-Phishing Working Group, APWG)的定義[2]，網路釣魚是一種同時使用社交工程及科技手段的犯罪機制，利用偽造電子郵件與網站作為誘餌，愚弄使用者洩漏帳號密碼、信用卡號碼、銀行金融帳戶等個人機密資料[3]。

釣魚網站生命週期短，根據美國反網路釣魚工作小組(APWG)2014年上半年的統計，釣魚網站平均的壽命已經由6.1天大幅縮短到32小時32分鐘，有一半以上的釣魚網站活躍時間不足9小時，短短的運作時間卻足以騙取許多敏感資料[4]。

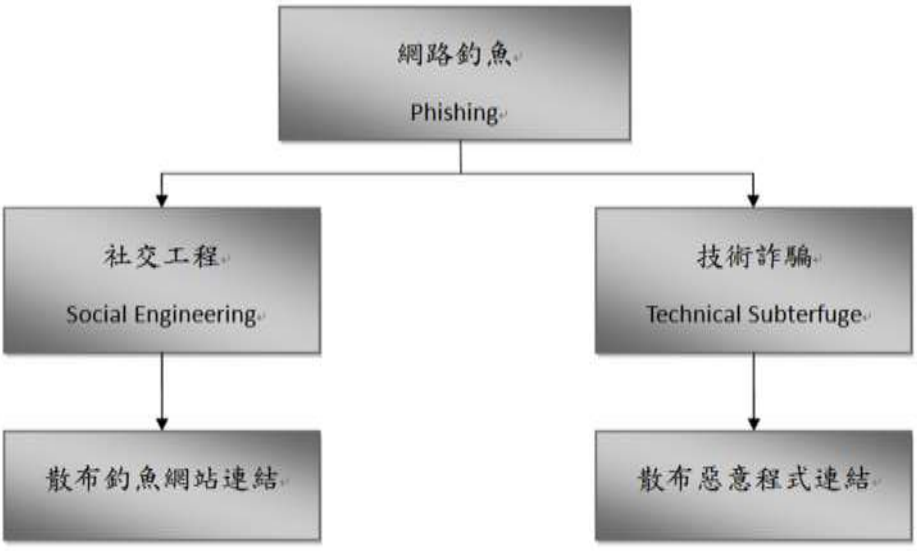
（二）網路釣魚型態：網路釣魚攻擊總歸可分成兩種型態[5] (圖一)：

1. 詐欺釣魚(Deceptive phishing)：

利用社交工程方法，以合法公司或銀行網站名義傳送電子郵件給受害人，透過郵件內附的連結，企圖將用戶轉址到假冒的網站，進一步騙取受害者的機敏資料。

2. 惡意程式釣魚(Malware-based phishing)：

此種方式是在寄送給受害者的郵件中內嵌有惡意程式的連結，點選後將程式植入到使用者電腦，或是利用系統的安全漏洞直接取得被害人的線上帳號資訊。例如在電腦上安裝後門程式監控使用電腦與瀏覽網頁的行為，或是安裝鍵盤側錄軟體，將使用者在各網路平台的帳號密碼一網打盡，或是在使用者電腦植入木馬程式並組建成殭屍網路(Botnet) [6]；有時候釣魚者會將受害者引導到假的網站，或者是由代理伺服器監控的合法網站。



圖一: 網路釣魚型態

資料來源：Krutika, R. S., & Jigyasu, D.(2014). A Survey on Phishing Attacks.

二、釣魚攻擊階段

釣魚攻擊分為下列各種不同的階段[7]：

（一）計畫階段：

在本階段首先要決定用來當成誘餌的機關組織，像是銀行或信用卡等服務的網站。這些網站在提供線上服務時，需要從使用者端得到一些特別的個人資料，例如網購商店向使用者要求信用卡卡號和識別碼等資料。

決定好誘餌後，就要選擇獲得資訊的方法。通常都是利用社交工程方式，利用人性的弱點，應用簡單的溝通和欺騙技倆，將含有釣魚網站的HTML連結散播給被害人，例如E-mail、簡訊、LINE通訊軟體、Facebook社群網站等。

再來就是架設釣魚網站主機，因為不能引起使用者的戒心，會把釣魚網站和原機構網站的外型做得極為相似，讓使用者難分真假，因此落入陷阱。

（二）設計階段：

攻擊者在此階段會先將目標網站的HTML結構重新設計，讓它和目標機構網頁內容很類似，但是藏有讓使用者輸入個人資料到釣魚網站主機的HTML，通常都是拿目標網站的內容做個簡略的調整以達到魚目混珠的目的。

接著就是決定成功騙取使用者輸入個人資料後要使用的資訊接收機制，例如回傳至主機端資料庫或檔案夾、以文字訊息發送至行動裝置、以Mail方式傳送和轉貼到論壇訊息等，由於資料儲存可能會和網站架設主機分開，攻擊者在成功收集到大量使用者資訊之後，可以有很多時間進行過濾和測試，不受釣魚網頁上線與否的影響，對於受害者的危害相當深遠。

（三）攻擊階段：

本階段攻擊者會以第一階段決定好的社交工程方式，誘騙使用者點選釣魚網站的連結，大多是使用E-mail詐欺，還有在公開的聊天室、即時通訊群組和RSS訂閱中轉貼釣魚網址。

（四）收集階段：

攻擊者收集受害者輸入的使用者資訊，並以第二階段所選定的方式回傳與儲存。

（五）冒用階段：

將所收集來的使用者資料實際用於獲取不法利益，多為詐欺或妨害電腦使用，說明如下：

1. 帳號密碼登入：

以受害人帳號密碼登入真實網站，進一步獲取更多資料，例如登入Facebook存取設定為不公開之私密照片。

2. 信用卡憑證盜刷：

以受害人之信用卡卡號與驗證碼進行盜刷消費，受害者通常在收到帳單後始知受害。

3. 將個人資料用於後續詐欺行為：

以受害者之個資進行電話簡訊聯絡，並使之前往操作ATM等詐欺行為。

4. 冒充受害人：

以受害人之身分資料至各大網站進行會員註冊，冒充使用者取得網路服務。

（六）事後行為：

一旦攻擊者達到他們從使用者端收集資料的目的，通常會故意將釣魚網站主機關閉以躲避通報或查緝。常常得知某網址為網路釣魚網站時，該網址早已失效，這也是造成釣魚網站生命週期短暫導致難以偵查的原因。

三、網路釣魚網址

現今網路上已經有許多製造假網站的網路釣魚工具(phishing toolkit)，例如Super Phisher、Rock Phish等，這些工具經由竊取合法網站的原始碼可以簡單的製造出仿冒的網站，使得製作釣魚網頁已非難事[8]。然而釣魚網站成立目的主要就是要讓使用者點選其連結，為了增加成功機率，釣魚網址通常採取下列方法：

（一）社交工程：

透過各種互動溝通的工具，例如Facebook、Line、Email、簡訊等，利用人性弱點，以有趣容易吸引到大眾注意的標題與內容，或是針對某些特定組織，以相關的文字讓使用者陷於錯誤，而點選附加連結。

（二）網址混淆：

利用容易混淆的字元取代原有網址，或是使用與原網站網域名稱相近的虛假網址以魚目混珠。

（三）URL編碼：

由於某些網頁的URL太過冗長，在編輯訊息時不易傳輸，利用現有的縮址功能，將較長的URL重新編碼，形成無意義的短URL，用來隱藏釣魚網站的真實網址，例如：http://0rz.tw；或是編寫為不容易解讀的URL網址，如
http://www.badsite.com/webhp?ab可轉換為
http://www.badsite.com/w%65%62h%70?ab。

（四）圖片內嵌連結：

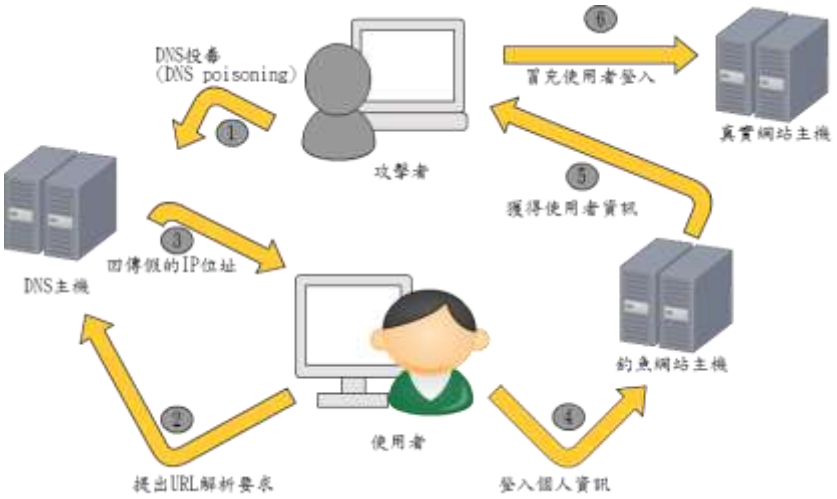
由於電子郵件可用HTML模式閱讀，在頁面中可以直接顯示圖片，釣魚者可以直接盜取合法企業或機構的正式形象LOGO放在釣魚信件中，當收件者不疑有他而點選圖片時，圖片內嵌的超連結將受害者導向到釣魚網站的頁面。

（五）瀏覽器漏洞：

利用JavaScript撰寫置換靜態的網址，使偽造的網站擁有和原始網站一模一樣的網址，混淆使用者的視聽。

（六）網址嫁接(pharming)：

在網際網路運作中，網域名稱可以對應到一組特定IP位址，這是透過網域名稱伺服器（Domain Name Server, DNS）的功能進行對應，攻擊者藉由入侵 DNS的方式，將使用者自動導引到偽造的網站上[9](如圖二)。



圖二: 網址嫁接攻擊示意圖

參、研究設計

一、研究方法

本研究所探討之網路釣魚犯罪不同於傳統犯罪，希望藉由已發生的案例輔以偵查人員之經驗做為研究基礎，進一步了解臺灣地區網路釣魚案件的全貌以及偵防策略，採用研究方法為案例研究法與專家訪談法。

二、研究工具

（一）案例研究工具：

為了解臺灣涉及網路釣魚犯罪案件的概況，須清楚每件案例的基本資料，有關案例內容大綱如表一：

表一: 案例研究工具大綱

案件資料	偵查機關
	查獲日期、時間及案類屬性
	查獲方法及偵查過程
被害者	受騙釣餌
	特定或不特定對象
加害者	基本資料(性別、年齡、技術背景等)
	犯罪手法及作案工具
	共犯組織
	躲避偵查的方法
	前科紀錄及案類
	學習網路釣魚的機會及管道

（二）訪談研究工具：

訪談有時會觸及個人隱私及過去的個人經驗，為了能使受訪者在訪談過程中能夠暢所欲言並維護其權利，研究者在事前準備了訪談大綱(如表二)並以半結構式[10]的訪談進行，訪談大綱的設計是為了使過程進行得更流暢，採取較開放、有彈性的問答方式，有助於深入了解受訪者的個人經驗、感受與認知。

表二: 訪談大綱表

從警經歷	1、從事警職之資歷簡述？ 2、電腦犯罪偵查之資歷？ 3、有無接受過電腦犯罪偵查之專業訓練或教育背景？
目前業務範圍	1、目前主要業務內容？ 2、所屬單位從事電腦犯罪偵查工作者有多少人？ 3、偵查過涉及網路釣魚的案件有幾件？ 4、目前的組織編制、任務分工及教育訓練對於偵辦涉及網路釣魚之案件是否足夠？有無改進之建議？
網路釣魚相關知識	1、對於網路釣魚的定義及可能出現的特徵是否了解？從何種管道了解？ 2、您覺得第一線外勤人員是否具備此一方面的知識？如何解決或改善？ 3、本身或周遭親友是否曾注意關於網路釣魚或釣魚網站的防制？關於網路釣魚的犯罪預防宣導是否足夠？ 4、由於網路釣魚經常涉及跨境犯罪，請問在您的偵辦經驗裡，遇到跨境的來源通常來自哪些國家？
偵查過程	1、進行此類案件偵查前會事先了解哪些資訊？有無遭遇困難？如何解決？ 2、偵辦案件時是否會特別注意案情內容有無涉及網路釣魚？ 3、偵查案件時，是否會充分了解被害人是否具備網路釣魚警覺？是否被害人曾經使用過網路釣魚防制的工具？ 4、偵查案件時，是否會充分了解加害人學習網路釣魚犯罪的機會與管道？ 5、您覺得偵查網路釣魚案件的重點為何？ 6、您覺得網路釣魚案件的特徵中，哪些特徵是必備的？
案情研判	1、您覺得網路釣魚案件與其他所辦過的案件最大的區別為何？收集個人資料的方式最大的不同？ 2、您覺得釣魚網站氾濫程度與偵破比例是否取得平衡？如何解決？ 3、您覺得此類案件最難偵辦的地方為何？如何克服？
其他	1、若您身邊的親友成為釣魚網站的受害人或是像詢問疑似釣魚網站的問題，請問您會給他/她什麼建議？ 2、請問您是否有其他補充意見？

肆、資料分析

一、臺灣地區網路釣魚案例分析

本研究案例焦點著重在透過「網址」進行網路釣魚的案件，亦有透過簡訊方式散播釣魚網址，此時將簡訊手法視為散布工具的一種，與傳統電信詐欺有所區分。本研究蒐集臺灣地區涉及網路釣魚之犯罪案件，蒐集來源主要係各縣市警察局偵辦之案例、司法院各地方法院裁判書之案例，再向各縣市警察局調閱偵查報告等相關資料，以及透過網路搜尋引擎及新聞檢索(如Google)，以關鍵字釣魚網站、帳密外洩、社交工程等關鍵字搜尋資料，再與官方收集之案例資料相互驗證進行分析，共蒐集10件案例。

（一）案例資料：

將所收集之10件案例依查獲時間進行排序與編號(如表三)，並以APWG統計中所使用的攻擊目標，找出臺灣網路釣魚犯罪中所使用的釣餌類型(如表四)，拍賣網站販賣虛有商品之詐欺，係利用網站業者平台刊登誘騙使用者購買商品之商業詐欺行為，並非以網址URL形式散布，不在本研究之案例收集範疇，也是釣餌類型在電子商務顯示比例偏低的原因。

表三: 案件資料一覽表

案例編號	查獲時間	案類屬性	案件概述	分布地區	釣餌類型
1	1999年9月	詐欺得利	架設複製網路銀行網站首頁之網站，於多家搜尋引擎登錄該網站，使上網者透過搜尋引擎進入，收集其銀行帳號、密碼、授權碼、身分證字號等資料。	北部	銀行金融
2	2005年4月	1.妨害電腦使用 2.妨害秘密 3.偽造文書 4.電腦處理個人資料保護法	1.先於拍賣網站兜售讀卡機後，針對買家寄送以主旨為金融卡驅動升級程式之電子郵件散布木馬程式。 2.藉由程式所收集之使用者資料，自行燒製偽造金融卡。	北部	電子商務
3	2006年4月	1.妨害電腦使用 2.妨害秘密	以電子郵件、奇摩家族散布內藏木馬程式之圖片，收集遊戲與奇摩帳密，並透過網路販賣所收集之帳號密碼。	東部	社群網路和電子郵件
4	2007年7月	1.商標法 2.詐欺 3.電腦處理個人資料保護法	架設偽冒銀行貸款諮詢網頁，大量發送電子郵件廣告，使被害人於網頁填寫個人資料上傳，再撥打電話予被害人，以「協助貸款」、「查詢還款能力」、「須貸款手續費」等理由向被害人施行詐術騙取金錢。	北部	銀行金融

5	2008年8月	1.妨害電腦使用 2.商標法	偽冒奇摩網路服務登入頁面之網頁收集帳號密碼。	北部及南部	社群網路和電子郵件
6	2009年8月	偽造準文書	偽冒行政院人事行政局全球資訊網天然災害停止辦公及上課情形查詢網頁，另於網路論壇散布不實資訊。	北部	社群網路和電子郵件
7	2012年2月	詐欺	架設虛擬旅店網站，於網路部落格、網路拍賣等平台上刊登不實訊息，誘使受害人訂房匯款。	中部	匯款
8	2012年4月	詐欺	1.電腦網路上刊登「網路換現金活動」之廣告，將所得之人頭行動電話門號登載於網站上，供不特定人聯繫之用。 2.接獲電話後，向被害人佯稱，欲參加活動者，需先行匯款繳納代書服務費騙取金錢。	東部	匯款
9	2013年5月	1.妨害電腦使用 2.商標法 3.詐欺	針對中小企業，偽冒健保局與物流公司名義寄發釣魚郵件散布遠端竊錄之木馬程式，取得大量企業內部機密資料。	北部	社群網路和電子郵件
10	2013年8月	詐欺	民眾接獲「猜猜我是誰」、「假冒快遞公司」等類詐欺簡訊後，因點擊簡訊內容之惡意連結，產生異常電信費用(簡訊費用或電信小額付費)	北部	社群網路和電子郵件

表四: 案例網路釣魚釣餌一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
銀行金融	✓	無	無	✓	無	無	無	無	無	無	2
電子商務	無	✓	無	無	無	無	無	無	無	無	1
社群網路和電子郵件	無	無	✓	無	✓	✓	無	無	✓	✓	5
匯款	無	無	無	無	無	無	✓	✓	無	無	2

根據所收集之案例分析發現，涉及網路釣魚之犯罪多為刑法第210條偽造、變造私文書罪、刑法第216條、第211條之行使變造準文書罪、刑法第315-1、318-1條妨害秘密罪、刑法第32章詐欺相關罪責、刑法第36章妨害電腦使用罪、商標法第68條侵害商標權罪以及電腦處理個人資料保護法相關罪責。

而前述電腦處理個人資料保護法已於2010年5月26日修正為「個人資料保護法」，其第2條明定個人資料和個人資料檔案定義，個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。釣魚網站所竊取的資料便是個人資料，於該法第41條也明確訂定未依規定取得個人資料，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。

由於此類案件受害者分布全臺各地，因此在案件分布地點的認定上，主要係以嫌疑人所在地或是裁判機關位置歸納。10件案例地區分布顯示，有6件案例是分布在北部，2件案例在東部，1件分布在中部，而有1件案例涉及北部與南部兩個地區。

臺灣地區的網路釣魚連結型態，依本研究案例顯示(如表五)，有4件釣魚連結是以植入惡意程式為目的，點擊連結後下載惡意程式，潛伏在被害人的電子裝置中，依程式碼的執行盜取或偷看使用者電腦資料。另有6件係以釣魚網址誘騙受害人，其中5件是為了讓受害人在不知情的情況線上填寫或與相關人進行聯絡，進而給出自己的機敏資料，餘下的1件則是純粹出於惡作劇。

表五: 網路釣魚連結型態一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
惡意程式	無	✓	✓	無	無	無	無	無	✓	✓	4
釣魚網址	✓	無	無	✓	✓	✓	✓	✓	無	無	6

在散布釣餌的手法部分，共分為偽冒其他機關、自立虛假網站、電子郵件、行動簡訊等4種。分別有5件偽冒其他機關，2件自立虛假網站，4件使用電子郵件，1件使用行動簡訊，其中案例4包括了偽冒機關與電子郵件兩種手法(如表六)。

表六: 散布釣餌手法一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
偽冒其他機關	✓	無	無	✓	✓	✓	無	無	✓	無	5
自立虛假網站	無	無	無	無	無	無	✓	✓	無	無	2
電子郵件	無	✓	✓	✓	無	無	無	無	✓	無	4
行動簡訊	無	無	無	無	無	無	無	無	無	✓	1

由於釣魚網站的建立主要目的在於收集使用者機敏資料，完成相關資料收集以後才可能被用做不法用途，在案件偵辦過程中，如果是在網路釣魚收集資料的階段即已發現，對於使用者所造成的損害為個資外洩，尚未直接造成金錢財務上的損失，因此當通知被害人到案說明時，多半對於個資的外洩渾然未覺。經常要等到有財物損害時，例如被電信詐欺、信用卡盜刷、小額付款等，始知自己的個資已外洩。

本研究案例透過偵查人員在案件偵辦過程時，與被害人接觸並了解是否在網路釣魚攻擊行為中有造成實際上的金錢財物損失，10件案例中共有4件已造成被害者財物損失，6件尚未造成財損(如表七) ，應係該攻擊本身就是要蒐集個資為目的而沒有要竊取財物，或是被害人沒有進一步遭到詐騙而無財損，甚至可能有財損而不自知。

表七: 案例財損狀況一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
造成財損	無	無	無	✓	無	無	✓	✓	無	✓	4
未造成財損	✓	✓	✓	無	✓	✓	無	無	✓	無	6

（二）案例關係人分析：

1. 被害者

被害者的部分可以分為特定對象與不特定對象(如表八)，案例中有2件針對特定對象，特定對象係指犯嫌進行網路釣魚時，已知被害人的身分或相關資訊，並掌握有一部分被害人個資，包括手機號碼或電子郵件，根據對被害人的了解設計網釣魚餌。例如已知被害人從事警察工作，在設計網釣魚餌時，加入警察勤務相關字眼，使被害人覺得煞有其事，提高點擊率，即使是具備資安警覺的使用者，面對切身相關的訊息，也很容易落入此類陷阱。不特定對象即是透過網際網路、行動簡訊等流通的管道，廣布網釣魚餌，吸引可能有興趣且較不具資安意識的使用者點擊，進而取得詳細的個人資料或在其上網設備植入惡意程式。

表八: 案例網路釣魚目標類型一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
特定對象	無	✓	無	無	無	無	無	無	✓	無	2
不特定對象	✓	無	✓	✓	✓	✓	✓	✓	無	✓	8

2. 加害者

本研究所收集案例中，共有25名犯嫌，其中僅有3名女性(如表九)，且涉案之女性成員在案件中皆為幫助犯的角色，負責散布或聯絡工作，皆不是製作釣魚網站或惡意程式的嫌犯。

表九: 案例嫌犯性別一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
男性人數	2	1	2	4	2	2	2	2	4	1	22
女性人數	0	0	1	0	0	0	1	1	0	0	3
合計	2	1	3	4	2	2	3	3	4	1	25

本研究案例25名嫌犯中，發現嫌犯年齡分布為16到45歲，最多落在26歲到30歲，共有10人，次多是16歲到20歲與36到40歲，皆為4人，其他年齡層人數為2人或3人(如表十)。

表十: 案例嫌犯年齡分布一覽表

案例編號	1	2	3	4	5	6	7	8	9	10	合計
16~20	2	0	1	0	1	0	0	0	0	0	4
21~25	0	0	0	0	0	0	0	2	0	0	2
26~30	0	0	1	2	0	2	2	1	1	1	10
31~35	0	0	1	1	1	0	0	0	0	0	3
36~40	0	1	0	0	0	0	1	0	2	0	4
41~45	0	0	0	1	0	0	0	0	1	0	2
合計	2	1	3	4	2	2	3	3	4	1	25

分析所收集的10件案例中，發現涉案之嫌犯並非全部具有架設釣魚網站或撰寫木馬程式的資訊能力(如表十一)，多數案件的犯嫌中，僅有1人具備架設釣魚網站或改寫惡意程式的相關知識，而由其他共犯散布釣魚網址或詐欺訊息，尤其是利用現有社群網站平台散布釣魚訊息的案例，嫌犯甚至不需具備相關資訊背景或知識，便可利用網際網路進行網路釣魚的犯罪。

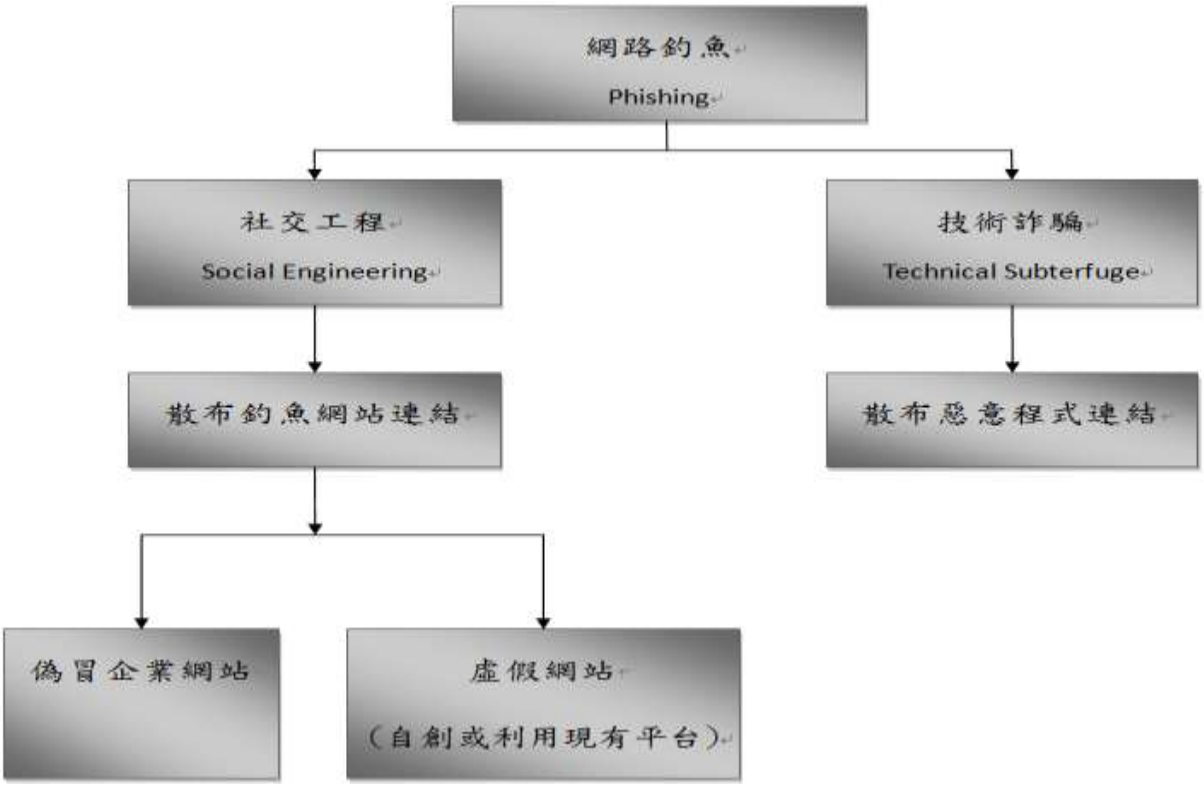
表十一: 案例嫌犯資訊專業能力一覽表

案例編號	1	2	3	4	5	6	7	8	9	10
資訊專業	1	1	1	1	1	1	0	0	1	0
犯案人數	2	1	3	4	2	2	3	3	4	1

（三）案例分析：

1.案例型態

由於網路釣魚犯罪係以欺騙人心為出發點，使受害者誤信加害人所給予的魚餌如網址或訊息，因而受騙上鉤。參閱Krutika與Jigysu於2014年所提出的網路釣魚攻擊型態為基礎(如圖一)，佐以本研究收集臺灣地區使用網路釣魚手法進行犯罪的案例整理發現，在社交工程中散布釣魚網站項下，尚可細分出二種型態，再加上技術詐欺中的散布惡意程式連結，臺灣案例可以歸納出三種讓使用者陷於錯誤致生損害的手法，分別是偽冒企業網站、成立虛假網站以及惡意程式(如圖三)，並據前述案例資料分析結果，臺灣地區網路釣魚犯罪案例係以社交工程散布釣魚網站連結並以偽冒企業網站型態為大宗。



圖三: 臺灣地區網路釣魚犯罪型態

2.案例網路釣魚階段

根據Hasika等人於2007年的研究，可以得知網路釣魚分為計畫、設計、攻擊、收集、冒用以及事後行為六個階段，將本研究收集案例進行比較(如表十二)。

計畫階段以嫌犯動機為主，設計階段即是網路釣魚網址的主題，攻擊階段則是散布該URL的手法，收集階段則是針對目標機敏資料所進行傳送與儲存的方法與工具，冒用階段係指收集相關資料後冒用受害者身分進行的侵害行為，事後行為階段則是躲藏行蹤或逃避追緝的作為。前三項階段係案件成立必要經歷的階段，後三項階段則視案情內容或破案時間或有或無。

表十二: 案例網路釣魚階段一覽表

案例	計畫階段	設計階段	攻擊階段	收集階段	冒用階段	事後行為
1	意圖竊錄電磁紀錄	複製網路銀行網站首頁	申請免費網站空間架設	銀行帳號、密碼、授權碼、身分証統一編號	偽造電子郵件傳送所收集之資料	無
2	意圖竊錄電磁紀錄獲取金錢	製作專供盜取他人網路銀行帳號及密碼之惡意程式	針對特定對象寄送電子郵件	收集銀行帳號、密碼等電磁紀錄，傳送至所申請之網站空間	偽造金融卡	無

3	意圖竊錄電磁紀錄	購買專供盜取遊戲、奇摩帳號及密碼之惡意程式	電子郵件、奇摩家族散布	遊戲與奇摩帳號、密碼並透過電子郵件收集	偽冒玩家盜取遊戲寶物	使用網咖電腦散布以躲避查緝
4	意圖竊錄電磁紀錄	偽冒銀行貸款諮詢網頁	大量發送電子郵件	個人資料	撥打電話向被害人施行詐術	代理伺服器軟體、無線溢波、提供無線上網之店家
5	意圖竊錄電磁紀錄	購買偽冒奇摩網路服務登入頁面之網頁程式	以IP位址取代網域名稱	收集登入會員知帳號、密碼	偽冒會員登入	無
6	惡作劇散布不實資訊	偽冒行政院人事行政局全球資訊網	申請免費網站空間架設，另於網路論壇大量散布不實資訊	無	無	無
7	意圖詐欺取財	設立虛擬旅店網站	網路部落格、網路拍賣等平台上大量刊登不實訊息，使受害人訂房匯款	無	無	網站上使用假聯絡資訊躲避偵查
8	意圖詐欺取財	大量刊登「網路換現金活動」之廣告	留有電話號碼供不特定人聯繫之用	無	無	網站上使用人頭行動電話門號躲避偵查
9	意圖竊錄電磁紀錄	偽冒健保局與物流公司名義	針對特定對象寄發釣魚郵件散布遠端竊錄之木馬程式	取得大量企業內部機密資料	偽冒公務部門與合作關係之公司	無
10	意圖詐欺取財	設計「猜猜我是誰」、「假冒快遞公司」等類詐欺簡訊	大量寄送含有惡意連結之簡訊	中繼主機控制手機	冒用使用者申請小額付款購買遊戲點數	關閉中繼主機躲避偵查

3. 案例犯罪剖繪

犯罪剖繪的基本原理，也可運用到網路犯罪，即區分作案手法和簽名特徵[11]，人類從事犯罪行為時，多會以自己的能力、知識、習慣、便利性、成功機率等因素，做為如何從事犯行的考量。因為可能有多種途徑或方式均可達到相同的犯罪結果，而在這些途徑和方法之間，要如何加以選擇則端賴特定犯罪人或犯罪集團來自行決定，而其所選擇的特定犯罪方法就可稱為「作案手法」。當犯罪者從事某些遠超過基本犯行所需的不尋常行為，即獨特行為，犯罪者會花費額外的時間，在這些僅對其個人別具意義的儀式化動作，而當犯罪者從一個案件到另一個案件裡，都有這一連串重複且類似固定儀式的行為，便稱為「簽名特徵」，通常與完成犯行並沒有關係。

由於網路釣魚行為係以散播釣魚網址為目的，讓使用者陷入錯誤加以點擊而交付機敏資料或植入惡意程式，因此網路釣魚作案手法應著重於如何讓使用者「點擊」釣魚網址的必要行為，包括「設計」、「攻擊」、「冒用」與「事後」階段等，但可能因為受到外界因素干擾，不一定會存在於每個案件中，至於簽名特徵在本研究案例中並未發現。

在電腦犯罪加害人方面可分為權力確認型、權力獨斷型、憤怒報復型、虐待型、機會型以及利益型等6種(如表十三) [12]，因此根據表十二進行案例犯罪剖繪之整理(如表十四)，可發現使用惡意程式手法之案件屬於權力獨斷型，收集個人資料等機密資訊加以利用屬於機會型，實際從事金錢上之侵害則屬於利益型。另案例6係基於惡作劇之犯意所進行的網路釣魚，並未收集資料或直接造成財務侵害，較屬於在電腦網路上展示自己能力之權力確認型。

表十三: 網際網路犯罪加害人分類範例

類型	行為範例
權力確認型	在電腦網路張貼兒童色情圖片，並公開宣稱他很聰明，警察抓不到
權力獨斷型	入侵保全良好的電腦系統且秘密完成工作，並非尋求他人確認或表現憤怒
憤怒報復型	因為認知錯誤，使用網路服務去騷擾和威脅被害者，包括跟蹤和接觸
虐待型	在線上討論群組找到被害者並安排碰面，從接觸到折磨、強暴至殺害
機會型	在正常網路活動中發現機密資訊，並使用它來從事黑函或間諜犯罪
利益型	將上千張偷來的信用卡號碼燒成光碟販售

資料來源：廖有祿(2010)，犯罪剖繪-理論與實務

表十四: 案例犯罪剖繪分析

案例	作案手法	加害人類型
1	1.複製網路銀行網站 2.以免費網路空間大量散布 3.偽造電子郵件傳送所收集之資料	機會型
2	1.製作專供盜取銀行帳號及密碼之惡意程式 2.針對特定對象寄送電子郵件 3.將資料傳送至其所申請之網站空間 4.偽造金融卡	權力獨斷型 機會型 利益型
3	1.購買專供盜取遊戲、奇摩帳號及密碼之惡意程式 2.以電子郵件、奇摩家族大量散布 3.透過電子郵件傳送所收集之資料 4.偽冒玩家盜取遊戲寶物 5.使用網咖電腦躲避查緝	權力獨斷型 機會型
4	1.偽冒銀行貸款諮詢網頁 2.大量發送電子郵件 3.撥打電話向被害人施行詐術 4.代理伺服器軟體 5.無線溢波 6.利用提供無線上網之店家	機會型
5	1.購買偽冒奇摩網路服務登入頁面之網頁程式 2.以IP位址取代網域名稱 3.偽冒會員登入	權力獨斷型 機會型
6	1.申請免費網站空間架設偽冒行政院人事行政局全球資訊網 2.網路論壇大量散布不實資訊	權力確認型
7	1.設立虛擬旅店網站 2.網路部落格、網路拍賣等平台上大量刊登 3.網站上使用假聯絡資訊躲避偵查	機會型 利益型
8	1.大量刊登「網路換現金活動」之廣告 2.使用人頭行動電話門號躲避偵查	利益型
9	1.偽冒健保局與物流公司名義 2.針對特定對象寄發釣魚郵件散布遠端竊錄之木馬程式 3.偽冒公務部門與合作關係之公司	權力獨斷型 機會型
10	1.設計詐欺簡訊 2.大量寄送含有惡意連結之簡訊 3.冒用使用者申請小額付款購買遊戲點數 4.關閉中繼主機躲避偵查	權力獨斷型 機會型 利益型

二、訪談分析

本研究訪談實際參與過涉及網路釣魚案件之偵查人員，共計受訪者7名。分別依受訪人員之基本資料、網路釣魚相關知識、案件偵查過程與研判、釣魚網路防制、意見與建議等5項進行歸納彙整。

（一）受訪人員資料：

本研究係針對曾經偵辦過臺灣地區網路釣魚犯罪案件的偵查人員進行訪談，擔任警職年資均已超過10年，最長25年。從事電腦犯罪偵查工作年資最短4年，最長15年。7位受訪者中有4人具有資訊相關學歷。幾乎所有受訪者表示，實務上專責電腦犯罪偵查人員比例較少，即便沒有相關學歷，若是遇到與電腦犯罪相關案件仍然需要偵辦，因此機關仍會有相關教育訓練課程，藉以幫助偵查人員學習資訊方面知識。有3名受訪者現仍擔任電腦犯罪偵查工作，另有1名受訪者已轉任非警職工作。幾乎所有受訪者均表示，網路釣魚行為會在實際犯罪之前出現，於案件偵查過程並不明顯，即便在實務上可能碰到相關手法，但大多難以成案(如表十五及表十六)。

表十五: 受訪人員基本資料表

編號	職稱	目前任職單位	警職年資	電腦犯罪偵查年資	曾涉及網路釣魚件數	成案件數	現任電腦犯罪偵查	資訊學歷
I01	隊長	刑事警察局	22年	15年	約5件	1件	否	有
I02	股長	刑事警察局	16年	10年	約3件	1件	否	有
I03	偵查正	刑事警察局	17年	7年	約3件	1件	是	無
I04	偵查正	刑事警察局	12年	10年	約10件	2件	是	有
I05	警務正	鑑識中心派駐分局	25年	4年	約3件	1件	否	無
I06	偵查佐	刑警大隊科偵組	11年	5年	約10件	1件	是	無
I07	分析師	移民署	13年	4年	約6件	1件	否	有

表十六: 受訪人員工作資歷分布表

年資	0-5年	6-10年	11-15年	16-20年	20年以上
警職年資百分比 (人數)	0 (0人)	0 (0人)	42.86% (3人)	28.57% (2人)	28.57% (2人)
電腦犯罪偵查年資百分比 (人數)	42.86% (3人)	42.86% (3人)	14.29% (1人)	0 (0人)	0 (0人)

（二）偵查人員對網路釣魚之了解：

1. 網路釣魚的定義及可能出現的特徵：

一般而言，電腦網路犯罪之偵查人員對於網路釣魚的定義及可能出現的特徵，都是透過案件偵辦學習，若偵查案件過程中發現涉及網路釣魚手法，一般是透過網際網路進行資料收集或藉由新聞媒體報導了解相關知識。

2. 電腦犯罪偵查之專業訓練或教育背景：

並非所有電腦犯罪偵查人員都具有資訊相關學歷，大部分的受訪者表示，對於資訊相關知識與電腦犯罪偵查相關技巧，都是在任職電腦犯罪偵查單位時，從所遭遇到的案件與同仁經驗交流互相學習，機關也會針對網際網路知識、新興犯罪手法或偵查工具進行教育訓練。

3. 第一線外勤人員是否具備網路釣魚的相關知識，如何改善：

受訪者普遍認為，第一線外勤人員如受理刑案之分局偵查隊或派出所基層員警，若非曾經接觸過相關案件或訊息的人，對於網路釣魚的相關知識並不清楚，但是普遍已經建立網際網路並非絕對安全的警覺性，因此如果遇到民眾反映時，可以察覺出可疑。至於受理案件時，需要技術層面的部分，大部分會轉介至科技偵查專責單位請求技術支援。

改善的方法為增加教育訓練的宣導，可以納入常年訓練學科講習中，針對偵測到的釣魚網站趨勢、新興網路犯罪的手法進行課程編修，培養同仁對於網路環境的資安意識，也能及時為民眾解答疑惑。

（三）案件偵查過程與研判：

1. 是否會特別注意案件涉及網路釣魚行為：

多數受訪者表示，對於案件中是否有網路釣魚行為一般不會特別注意，都係由涉及該手法的案件偵辦的過程中被動發現，例如有被害人提及或是釣魚手法為破案關鍵時才會特別關注，但不會特別記錄。

2. 是否會特別注意被害人有無網路釣魚警覺與使用防制工具：

受訪者認為，被害人就是因為沒有網路釣魚警覺，才容易落入釣魚陷阱而上當。且被害人的網路釣魚警覺多跟案件偵破無關，只有案情需要時才會詢問被害人是否有使用防制工具。也有受訪者會在製作筆錄過程中，若發現被害人資訊安全與警覺心很薄弱時，會特別進行觀念的宣導。

3. 是否會特別注意加害人學習網路釣魚的機會與管道：

偵查人員在偵辦案件的過程中，會去注意到犯嫌本身的資訊能力與學習網路釣魚的機會和管道。絕大多數從事網路釣魚的嫌犯是網路自學，從網際網路上參考架設網站技術與改寫既有惡意程式工具，或是在論壇上與網友進行經驗交流，只有少數犯嫌具有資訊相關之學歷背景或是從事資訊產業。

4. 網路釣魚的案件特徵：

根據受訪者多年從事電腦犯罪偵查工作經驗，以及實際處理網路釣魚案件的經歷，歸納出下列網路釣魚的案件特徵：

(1) 具有URL網址：

在網路平台上流傳URL網址請使用者點擊，通常會有一段對該網址加以敘述的文字，可能是廣告活動、社會議題或影片趣聞，用來引起網路使用者的興趣，且經常無法直接從網址中的網域名稱推斷網站來源。

(2) 具有輸入資料的行為：

任何在網際網路上需要輸入資料的網頁都必須謹慎小心，可以透過搜尋引擎相互驗證所連結之網站是否為正常官網，或者是否有人在網路上分享被該網站詐欺的資訊。

(3) 與常理不符：

例如在網路上看到特別便宜的商品優惠資訊、明明有按時繳費卻收到欠費帳單，或是不明人士自稱熟人所發送的電子郵件或行動訊息，都應該保持懷疑，向相關單位求證。

5. 偵辦網路釣魚案件時的特別之處：

有不少受訪者表示，網路釣魚的行為經常是其他犯罪行為的前置作業，隨蒐集到的資料屬性不同會衍生出不同的犯罪行為，又受害者難以立即察覺網路釣魚行為而向警察機關報案，因此偵查人員經常扮演較被動的角色。

6. 網路釣魚案件的偵查重點：

遇到這類的犯罪案件，首要條件就是要知道受害者資料的流向，因此會根據案件內容有限的資料中，先從資通訊流著手，從釣魚網站網址或網頁內容所留下的通訊資訊，向ISP調閱相關網站、帳號或IP位址的使用者申請資料與地址。

7. 網路釣魚案件的偵查困境：

(1) 連線來源位於境外：

幾乎所有受訪者都表示，網路釣魚這類案件的偵查困難首要就是資通訊流查到最後，發現是境外來源，就會因為司法管轄不及的關係造成偵查斷點，導致這類行為難以成案偵辦。

(2) 受害事證難以串連：

在尚未造成財損的網路釣魚案件，多屬於告訴乃論的妨害電腦使用罪，但是因為受害人並不知情，所以不會有受害人出來報案，所以難以成案。然而在釣魚網站中繼站所找到的個人資料，也難以證明與受害人財損的事實有因果關係，例如電信詐欺案件，成員分工極細，負責詐欺的人並不知道個人資料是從何管道得來，因此難以證明受害者遭詐欺是由於在釣魚網站上填入個資所導致。

8. 網路釣魚涉及跨境的國家：

根據受訪者從事電腦網路犯罪偵查的經驗，多數境外網站來源是來自於美國，像是色情網站、虛假網站等，而與詐欺有關網站來源與犯嫌多來自中國大陸，另外也會有來自韓國、香港、日本的釣魚網站。

（四）偵查人員之防制觀念：

1. 本身或週遭親友對於網路釣魚或釣魚網站防制的關注：

由於偵查人員係以偵破刑案為導向，對於網路釣魚現象的防制，較不是偵查人員的關注重點。但是若自己收到疑似網路釣魚的郵件或訊息，會因曾有電腦犯罪偵查的經驗，能夠進行判斷與過濾。

週遭親友因為極少接觸這類案件，對於網際網路的使用習慣不夠嚴謹，資訊安全觀念也較為薄弱，在面對收到電子郵件或訊息時，大多不疑有他而直覺式的點閱，因此落入陷阱的機會提升，也較少關注網路釣魚防制的議題。

2. 關於網路釣魚的預防宣導是否足夠：

現今多數跟網際網路犯罪的宣導，仍然較著重在引導受害者操作ATM匯款相關的電信詐欺，對於會將自己個人資料外洩出去的網路釣魚行為，雖然新聞媒體平時也會加以宣導，但是由於民眾的關注度不高或網路使用習慣難以改變，因此網路釣魚不是犯罪預防宣導的主力。

3. 對於公司企業防制網路釣魚的看法：

案例中有不少偽冒機關的釣魚網站被發現，就是因為臺灣地區的業者發現自己的網站被冒用，立即通報警方，要求協助偵辦。為了因應ATM詐欺，刑事局研發科發展出針對165反詐騙專線資料庫進行彙整與分析，若單週達3件以上，就會初步跟該企業溝通，請其向會員加強反詐騙宣導，並檢視不必要的個資揭露，減少外洩管道，以及請業者針對網站漏洞進行檢測及修補。若不改善且累積單月達10件以上又有最新個資持續外洩，則會函請主管機關經濟部商業司依權責卓處。雖然各企業難以避免自己的網站被不肖份子仿冒盜用，但藉由上述與警方的合作，可以防堵使用者的個人資料從真實官網外洩。

另也有受訪者提出，偵查網路釣魚案件時，經常發生嫌犯利用假網站偷竊會員帳號密碼，再用偷來的帳號密碼到真實網站登入。如被偽冒的企業能提供可疑帳號與IP登入紀錄，例如同一IP同一時間登入多組帳號密碼或是同一帳號短時間內跨地區IP登入，可以進一步幫助警方過濾可疑份子，在偵辦上會有很大的幫助。

4. 對於使用者網路防制網路釣魚的看法：

由於網際網路釣魚與詐欺的手法一直不斷修正翻新，為的就是要以簡單的方式讓使用者信以為真，誘騙其上當。因此用來當作釣餌的劇本會不斷推陳出新，網路使用者可說是防不勝防。但是參考近年來詐騙防制的經驗，多數民眾現在的確比較具有防詐騙的意識，詐騙案件也不像早期如此猖獗氾濫。

因此，套用到網路釣魚的防制上，我們也應該從學校教育、日常宣導等各方面著手，建立使用者網際網路資訊安全的概念，培養優良的電腦、行動裝置的使用習慣。另外對自己的電子裝置進行基本的保全，例如安裝防毒軟體或防火牆等，形成對於網路上流傳的訊息加以查證的風氣，讓從事網路釣魚者無法得逞。

（五）訪談者意見：

1. 如何克服偵查困難：

由於網路釣魚犯罪最大的偵辦困難就是跨境，甚至其他電腦網路犯罪一樣有此問題，因此迫切需要的就是建立與其他國家之間的跨境司法合作。因為架設釣魚網站的犯嫌人在臺灣，但是使用跳板從臺灣地區以外IP連進來。如果能夠與各國建立資料流通的司法互助機制，在遇到境外來源時，能夠向位置所在國的ISP業者進行IP註冊資料的調閱，可能有機會查到服務註冊者的地址，或是找到購買該網站服務的付費項目，進一步確定嫌犯身分。

2. 避免成為釣魚網站受害人的方法，點閱後如何處理：

(1) 不輕易點選網址：

瀏覽網際網路時，盡量直接從網址列鍵入欲瀏覽之網址，如果收到從網域名稱無法直接看出網站來源的訊息或電子郵件，例如短網址，絕不輕易點選，可另從搜尋引擎鍵入關鍵字查證，或者所有與自身無關的內容均不點選。

(2) 不輕易輸入個資：

針對自己不熟悉的網站或來源不明的可疑網站，若要求輸入個資必須謹慎小心，亦可使用搜尋網址收集相關資料或可查詢來源對象是否有正式電話，致電詢問蒐集資料之目的。

(3) 損害控管：若不慎點選不恰當網址，依照資料蒐集情形可採取下列做法：

a. 已輸入帳號密碼：儘速向正式官網更改密碼，並調高帳號安全性，例如設定Google帳號兩階段驗證。

b. 已輸入金融資料：儘速通報該管銀行，掛失相關金融服務，再重新申請更換，並向警方通報。

c. 已輸入個人資料：必須提高電信詐欺的警覺，注意是否收到來自拍賣網站或公務機關的ATM設定通知，一定要向該機關再三查證，並向警方通報。

d. 點選後沒有下一步動作發生：如果遇到點選連結後，沒有進一步的動作發生，可能是惡意程式連結，可用防毒軟體掃描是否有被植入惡意程式，或者儘速進行系統重灌。

3. 其他建議：

(1) 組織編制與訓練：

由於電腦犯罪偵查係屬於刑事偵查體系下的專責小組，例如刑事局偵九大隊或是各縣市警察局刑事警察(大)隊科技偵查組，單位內員額有限，卻要處理所有涉及電腦犯罪的案件，難免分散偵查資源，又因為網路釣魚行為係潛伏於網際網路之中蒐集資料，偵查機關經常後知後覺。

建議組織編制尚能夠擴充員額，並且針對網際網路新興犯罪手法進行教育訓練，可納入常年訓練學科教育中，進一步甚至可以安排偵查人員報考相關資訊類別之證照或輔導至臺灣地區以外進修，讓科技偵查水平也能與時俱進。

(2) 建立知識共享平台：

因警察勤業務繁重，又面對頻繁人事調動，有時可能類似案件發生，卻沒辦法找到之前偵辦的人員，偵查經驗難以傳承，且各地在案件偵查鮮有互相交流，偵查能量更難以累積。

建議可以透過自立社群平台，讓各地偵查人員將案件經驗透過線上交流分享，形成群眾知識，提供爾後案件發生時，能夠透過眾人的力量，互相精進，讓刑案偵辦效率事半功倍。但為免流於形式，必須考量同仁的意願與現實環境，例如透過匿名或論壇模式經營，形成資訊共享的風氣，才能達到知識累積的效果。

(3) 資訊公開平台：

建議反網路釣魚工作小組單一回報窗口可以結合政府資訊公開的概念，對網羅而來的資訊分析之後，將確定是釣魚網站的網址納入黑名單，並以資訊公開的方式，將釣魚網站資訊提供給各個企業機關進行把關或做為資安工具開發使用，讓使用者在瀏覽網際網路時，在第一線過濾掉已知的釣魚網站，降低資訊安全的威脅。

伍、結論與建議

一、結論

本研究不同於一般對於網路釣魚，著重在偵測與發現釣魚網站的技術性研究，係以電腦犯罪偵查實務分析的角度出發，蒐集臺灣地區有關網路釣魚犯罪案例共10件，訪談有經驗偵查人員共7位，依案例分析工具與訪談分析工具整理，以下說明研究發現：

（一）案例分析發現：

1. 臺灣網路釣魚案例中用來當作釣餌的類型可分為銀行金融、電子商務、社群網路和電子郵件、匯款等四類，其中以社群網路和電子郵件為釣魚目標為最大宗；釣魚連結有4件植入惡意程式，6件以釣魚網址誘騙受害人為目的；以偽冒其他機關、自立虛假網站、電子郵件、行動簡訊等4種手法散布釣餌。
2. 所收集案例中的被害人，僅有2件係針對特定對象限縮範圍進行網路釣魚，其餘案件皆為不特定對象。
3. 所收集案例中的嫌犯，以26歲到30歲為最大族群，男女比例懸殊，僅有3名女性；且嫌犯無需具備撰寫程式的資訊專業便可進行網路釣魚犯罪。
4. 綜合所收集案例的特性與差異，歸納出臺灣網路釣魚犯罪型態可分為偽冒企業網站、成立虛假網站以及散布惡意程式連結等三種。
5. 比較臺灣地區內外網路釣魚攻擊階段的差異可以發現，臺灣網路釣魚有3件並未蒐集相關機敏資料與進行身分冒用，另有一半的案件在事後行為階段，沒有採取躲避偵查的作為。
6. 以犯罪剖繪技術分析，發現臺灣地區網路釣魚案件加害人大致可分為權力獨斷型、機會型與利益型等三類，部分案例會同時顯現二種特質，其中案例2、10兼具有三者特徵。惟案例6與其他案例不同，屬於在電腦網路上展示自己能力之權力確認型。

（二）訪談分析發現，如表十七。

表十七: 實際訪談結果一覽表

網路釣魚相關知識	1.透過網際網路或新聞媒體了解相關知識 2.來自遇到的案件、經驗交流、教育訓練 3.第一線外勤人員雖不清楚相關知識，但普遍已建立資安警覺，能進行案件技術轉介
偵查過程	1.案件偵辦的過程中被動發現網路釣魚 2.被害人的網路釣魚警覺跟案件偵破無關 3.絕大多數從事網路釣魚的嫌犯是網路自學 4.案件特徵：具有URL網址、具有輸入資料的行為、與常理不符 5.網路釣魚的行為經常是其他犯罪行為的前置作業 6.偵查重點：資通訊流
案情研判	1.偵查困難：連線來源位於境外、受害事證難以串連 2.境外網站來源：美國、中國大陸、韓國、香港、日本
其他	1.網路釣魚現象的防制，較不是偵查人員的關注重點 2.犯罪的宣導仍著重在電信詐欺

二、建議

本研究以偵查實務角度出發，探討臺灣涉及網路釣魚犯罪情形與現行作法，達到研究目的如下：

（一）目前臺灣所遭遇到的攻擊概況：

依據受訪者陳述，所有受訪者在電腦犯罪偵查生涯均遭遇涉及網路釣魚犯罪案件，卻因境外來源與受害事實難以串連之偵查困難，每個人僅有少數1至2件實際偵辦經驗。

（二）網路釣魚攻擊類型與欺騙手法：

根據案例分析，臺灣地區網路釣魚攻擊類型可以分為散布釣魚網站連結為主的「社交工程」與散布惡意程式連結為主的「技術詐騙」兩大型態，而欺騙手法則可細分「偽冒企業網站」、「成立虛假網站」以及「惡意程式」等3種方式。

（三）網路釣魚攻擊的偵防策略：於本節分別就網路釣魚犯罪偵查與防制二方面提出建議如下：

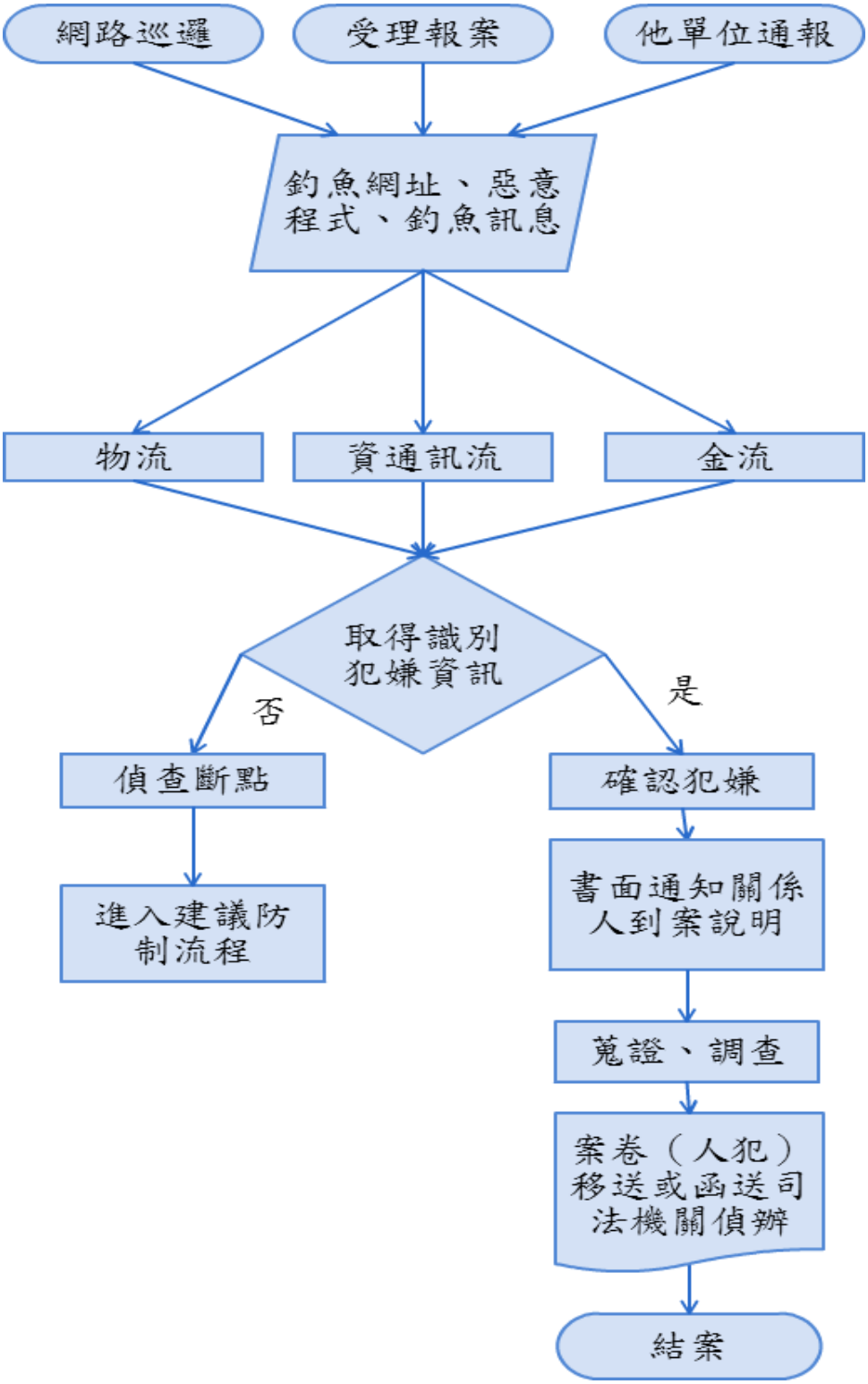
1.偵查建議

(1)偵查流程：

網路釣魚案件之偵查重點是要找出發布釣餌的來源端，目的是要確定犯嫌之身分資料，再循線找出資料遭侵害之被害人身分並連結受害事證。實務卻因網路釣魚來源經常來自臺灣司法權管轄不及的境外之地，又釣魚網站生命週期短暫，常有網址異動或無預警關閉，導致警方在案件追蹤上的困難，形成偵查斷點。

經本研究案例及訪談分析提出面對網路釣魚案件之偵查建議，在未能有效建立與各國之間完善的司法互助與資訊交流之前，難以克服境外IP的困境，但可以透過

釣魚訊息中揭露的資通訊流、金流或物流資訊，抽絲剝繭，取得足以識別犯嫌的身分資訊。例如嫌犯在釣魚網頁或社交工程訊息中所留下的電子郵件帳號、電話地址等聯絡資料、使用的工具軟體以及金融帳號等，倘若各流向仍難以突破，形成偵查斷點，則結合圖五所提出之防制流程，進行防阻與資源共享(如圖四)。



圖四: 網路釣魚案件偵查建議流程

(2)強化跨境司法互助：

目前臺灣與國際間簽有刑事司法互助協定(議)之國家為美國、菲律賓與南非，分別是「駐美國臺北經濟文化代表處與美國在台協會間之刑事司法互助協定」、「駐菲律賓臺北經濟文化辦事處與馬尼拉經濟文化辦事處刑事司法互助協定」與「駐南非共和國臺北聯絡代表處與南非聯絡辦事處刑事司法互助協議」。

與中國大陸的部分，訂有「海峽兩岸共同打擊犯罪及司法互助協議」，其中共同打擊犯罪之合作範圍包含侵占、背信、詐騙、洗錢、偽造或變造貨幣及有價證券等經濟犯罪，並同意交換涉及犯罪有關情資，協助緝捕、遣返刑事犯與刑事嫌疑犯，並於必要時合作協查、偵辦[13]。

由於涉及釣魚網站的案件，最常見的偵查斷點就是在追查資料傳輸中繼站IP位址時，發現該網路節點位於境外，又因缺乏相關管轄權而無法持續偵查。然而根據APWG統計以及本研究訪談彙整，目前遇到最多境外犯罪的網站來源IP來自美國，其次為韓國、香港跟中國大陸，建議可依此順序優先強化彼此之間跨境司法互助之外，同時透過資訊服務業者或ISP業者進行資訊交流的合作，提供警方辦案識別犯嫌之必要資訊，共同打擊網路釣魚犯罪。

(3)組織編制與人員：

為了因應犯罪趨勢的專業化，刑事警察局於2006年4月即已成立科技犯罪防制中心，統籌管控資訊、網路及通訊之偵查技術資源與建置科技偵查設備，輔助外勤偵查人員強化防制資通犯罪。

惟實際偵查科技案件之外勤隊，員額有限且偵辦專長不同，案件數量繁重，容易分散科技偵查的資源，又常有人事異動，類似種類的犯罪案件偵查能量與經驗難以傳承，為此本研究提出下列建議：

a. 成立偵查知識社群平台：

以經驗分享的型態，廣納各地偵查人員在各種案件上的偵查經驗或破案關鍵，彼此學習並增進偵辦技巧。或是新興案例發生時，全台偵查人員亦可透過該平台掌握到最新資訊，遇到偵查斷點時，亦可至該平台搜尋類似案例的偵辦技巧，結合眾人的知識累積形成龐大的偵查資源。

b. 教育訓練與宣導：

針對網路釣魚等科技犯罪之資通訊基礎技術、最新作案手法、網路偵查工具等，進行教育訓練，消除各地科技偵查人員之資訊落差，輔導報考相關專業證照，甚至出國進修，引進國外偵查作為等。

2. 防制建議

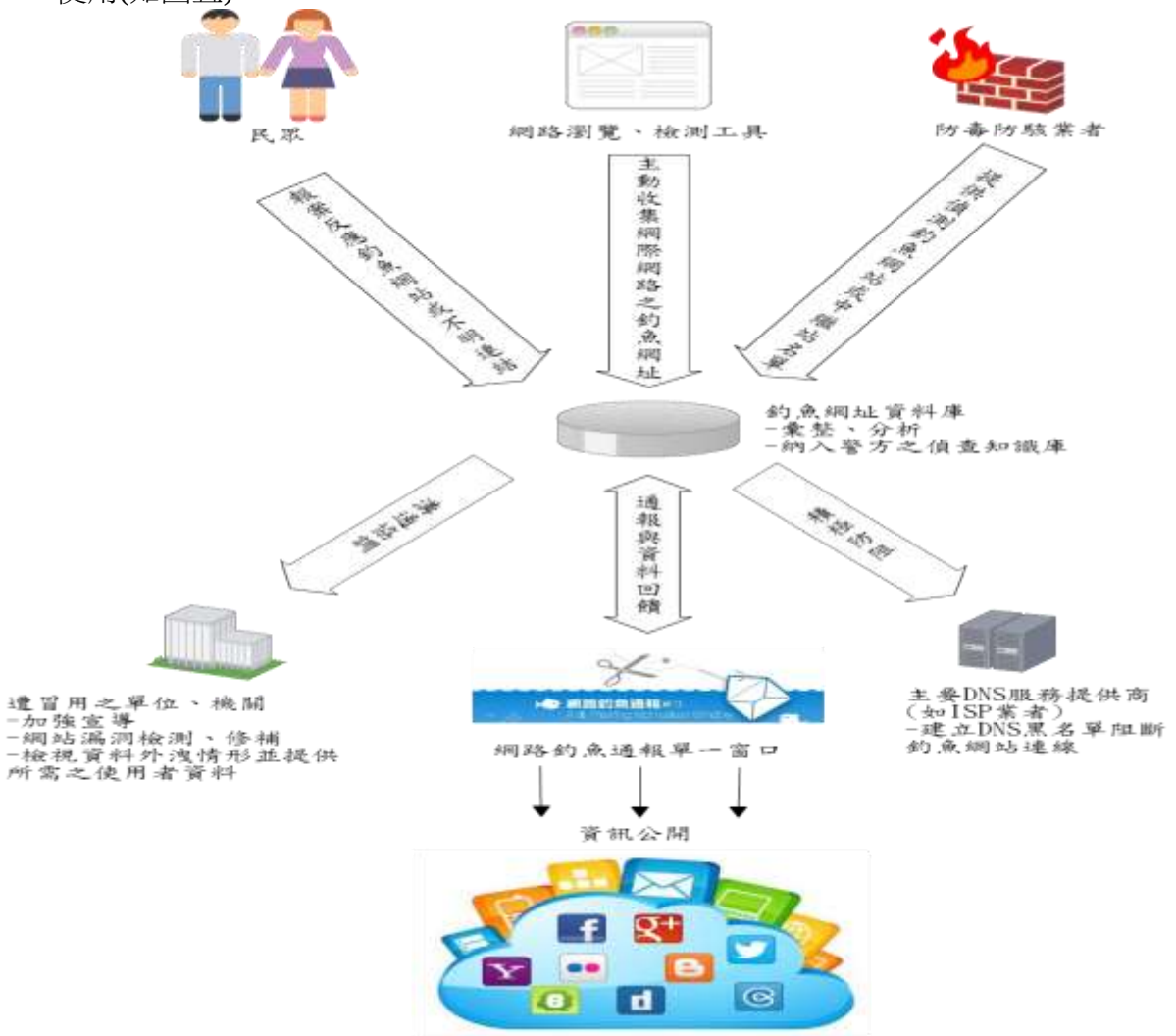
由於臺灣對於網路釣魚犯罪未設有專門法律規範，且受害人在點選釣魚網站或釣魚郵件的當下並未察覺異狀。而網路釣魚又多以個人機敏資料為目標，就其本質而言，個人資料屬於數位資料的一種，具有電磁紀錄的特性，通常以電磁或電波的方式儲存在電子媒體上，必須藉助電子設備加以讀取、分析或顯示，容易偽造、變造，不像實質財產損失能夠立刻被發覺[14]。

網路釣魚行為係為各類電腦犯罪初期收集資料之階段，在資料收集與後續犯罪行為之間常有醞釀期，導致案件連結不易，又不易證明所擷取的證據資料係網路釣魚所得，難以串連受害事證。因此，若能在包羅萬象的網際網路行為中，建立起資料保護的風氣，才能夠抑制此類案件的風行，因此本研究提出下列建議：

(1)防制對策：

由於臺灣NCC-CERT已設有網路釣魚通報單一窗口，並進行偵測及分析，惟其結果僅有通報各IASP業者，並無統整與公告，亦不能作為偵查資源配合使用。

參考國外對於網路釣魚聯防的趨勢，傾向於ISP業者和消費者必須共同分擔風險並將風險最小化。因此本研究提出網路釣魚案件之防制對策為建立釣魚網址資料庫，從多方面廣納釣魚網站之反映，並主動利用網頁截取工具收集可能的釣魚網站，結合臺灣反釣魚網站工作小組技術支援，進行跨部會之資料分析與資源共享，並通知受到仿冒侵害的業者，使其提高警覺並配合偵查作為。最後，結合政府資訊公開的概念，定期發布釣魚網站之資訊，提供各界警惕或是做為資訊安全工具開發使用(如圖五)。



圖五: 網路釣魚防制建議流程

(2)業者共同聯防：

透過各界伺服器端聯合防制釣魚網路之猖獗，金融與商務機構交易之入口網業者，配合提供異常網路登入紀錄，協助舉報不當瀏覽與可疑來源，甚至進一步將釣魚者導出正式網站，並監控所冒用之帳號密碼資料，避免更多人受害。

ISP業者與防毒防駭業者應針對行動通訊安全加以改善，主動提供警方釣魚網站或中繼站名單，積極防阻釣魚網站與不當連結的擴散。

(3)加強使用者防釣警覺：

在2014年，行政院國家發展委員針對網路族個人危機與權益方面，觀察資訊社會帶來的負面影響，在權益侵害的部分，最近1年因使用網路而造成個資外洩的比例，從2013年的17.1%提升至2014年的19.6%，增加2.5%；收到垃圾郵件頻率的比例，則從2013年的66.5%下降至2014年的63.7%，減少2.8個百分點；在設備侵害方面，網路族最近1年因使用網路而造成電腦中毒的比例，從2013年的35.7%降低至2014年的32.1%，減少3.6個百分點(如表十八) [15]。

表十八: 個人數位發展侵害權益比較表

指標層級	指標項目	2014年	2013年
個資隱私	個資外洩	19.6%	17.1%
	垃圾郵件	63.7%	66.5%
設備侵害	電腦中毒	32.1%	35.7%
	網路詐騙	3.1%	該年度無此統計項目
網路霸凌	遭受他人網路言論攻擊或公然侮辱	4%	

資料來源：行政院國家發展委員會(2014)，103年個人/家戶數位機會調查報告

根據上述統計資料，垃圾郵件與電腦中毒等損害呈現下降的比例，可以得知全民資安意識逐漸提升，惟個資外洩的損害係呈現上升趨勢，表示民眾對個人機敏資料的警覺仍有待加強，也代表專攻資料收集的網路釣魚攻擊仍然有機可乘，以下提出加強使用者防釣警覺之建議：

a. 善用網路釣魚防制工具：

透過防毒防駭業者，安裝釣魚網站過濾軟體並定期更新，或是使用本研究所介紹之偵測工具，例如SpoofGuard、Spoofstick、VSA、Phishark、PhishGuard、Whoscall等軟體，協助分辨網際網路中的釣魚網站。

b. 社交工程演練：

目前政府機關均有不定期對內部實施電子郵件社交工程演練，即寄送特殊主旨之電子郵件測試內部使用者對於不明電子郵件是否會加以點閱，並統計公告，讓機關內部使用者建立網際網路世界存有潛在危機的警覺，稍有不慎，可能會對自身或企業的權利受害。

c. 資訊安全教育與宣導：

從學校教育著手，加入資訊安全相關課程，讓學齡孩童在開始接觸網際網路時，就能了解基本的資通訊資料交換機制，建立安全的網際網路使用習慣，例如不使用過度簡單之帳號密碼、不輕易點選網址、不輕易給予個資等。

d. 鼓勵查證與通報：

對於來路不明的郵件、訊息、網址提高警覺，多方查證並主動通報反釣魚網路單一窗口，俾利相關單位進行防制，才能有效遏止網路釣魚的氾濫。

參考文獻

[1] Neil, M.(2013). A Tricky Situation: Deception in Cyberspace. *The Journal of Criminal Law*, 77 JCL, pp. 417-432.

[2] Anti-Phishing Working Group (APWG).(2012). *Phishing Activity Trends Report*, 2nd Quarter 2012, p. 4.

[3] 財團法人臺灣網路資訊中心TWNIC(2007)，委託財團法人資訊工業策進會科技法律中心研究，*研議網路詐騙防範措施委託研究計畫*，頁3。

[4] Greg,A., & Rod, R.(2014). *Global Phishing Survey 1H2014: Trends and Domain Name Use*. An APWG Industry Advisory, p.8.

[5] Krutika, R. S., & Jigyasu, D. (2014). A Survey on Phishing Attacks. *International Journal of Computer Applications* (0975 - 8887), Volume 88 - No.10, pp. 1-4.

[6] 又稱為機器人網路，駭客利用自己編寫的攻擊程式將數萬個淪陷的機器，即駭客常說的僵屍電腦或肉雞，組織成一個個控制節點，多用來傳送偽造封包或者是垃圾封包，使預定攻擊目標癱瘓並「拒絕服務」。[維基百科，*殭屍網路*，http://zh.wikipedia.org/wiki/%E6%AE%AD%E5%B1%8D%E7%B6%B2%E7%B5%A1 (accessed November 25, 2014).]

[7] Hasika, P., Duminda, W., & Csilla, F. (2007). *An Intrusion Detection System for Detecting Phishing Attacks*. W. Jonker and M. Petković (Eds.): SDM 2007, LNCS 4721, pp.181-192.

[8] Ramesh, G., & Ilango, K. (2014). A comprehensive and efficacious architecture for detecting phishing webpages, *Computers & Security*, 40, pp. 23-37.

[9] 資訊安全宣導網站，國立聯合大學，*網址嫁接 Pharming*，http://www.nuu.edu.tw/UIPWeb/wSite/ct?xItem=61294&ctNode=11724&mp=56 (accessed November 25, 2014).

[10] 潘淑滿(2003)，*質性研究-理論與應用*，心理出版社，頁 143-144。

[11] 廖有祿(2010)，*犯罪剖繪-理論與實務*，中央警察大學出版社，頁 46-61。

[12] 廖有祿(2010)，*犯罪剖繪-理論與實務*，中央警察大學出版社，頁 278。

[13] 法務部全球資訊網，*國際及兩岸司法互助*。https://www.moj.gov.tw/np.asp?ctNode=32124&mp=001(accessed November 25, 2014)

[14] 王旭正、林祝興、左瑞麟(2013)，*科技犯罪安全之數位鑑識－證據力與行動智慧應用*，博碩文化股份有限公司，頁 1-6。

[15] 行政院國家發展委員會(2014)，*103 年個人/家戶數位機會調查報告*，頁 126。