我國網路詐欺被害調查與防制研究

研究成果報告

研究主持人：中央警察大學犯罪防治學系 賴擁連教授

協同主持人：中央警察大學犯罪防治學系 蔡田木教授

中央警察大學犯罪防治學系 陳玉書副教授

法務部司法官學院 委託研究

中華民國一一二年十二月

我國網路詐欺被害調查與防制研究

受委託單位：中央警察大學

研究主持人：中央警察大學犯罪防治學系 賴擁連教授

協同主持人：中央警察大學犯罪防治學系 蔡田木教授

中央警察大學犯罪防治學系 陳玉書副教授

研究期程：中華民國 112 年 1 月至 112 年 12 月

研究經費：新臺幣柒拾柒萬玖仟元

研究計畫編號（GRB）：PG112-A-002

法務部司法官學院 委託研究

中華民國一一二年十二月

目　錄

表目錄

圖目錄

附錄

摘要

隨著時代資訊的進步，近年來以網際網路設備為工具或手段的詐欺案件急速增加。根據警政署刑事警察局(2022)統計資料顯示，我國網路詐欺被害之人數與財損，日益增加；其中投資詐欺、解除分期付款詐欺和一般購物詐欺為近年來民眾最常遭受網路詐騙的型態，這些被害型態均與網路活動有關，諸如線上購物、交友、遊戲等網路平臺，皆成為詐欺集團取得個資的溫床，凸顯出網路詐欺犯罪管道的多元化；但相對地，目前社會各界對於網路詐欺犯罪之了解，仍然不足，實有透過一定規模的網路詐欺被害經驗之調查，始能了解網路詐欺被害之風險因子、被害經驗及歷程，以建立有效的網路詐欺被害預防策略與防制機制。

本研究運用國際比較法、網路問卷調查法、深度訪談法與焦點團體座談等，將渠等研究方法所得到之資料與數據，進行適切的彙整與分析後，得到以下重大發現：

(一)國際比較分析得知，各國對於網路被害調查之管道，從過往依附於傳統電訪和面訪之犯罪被害調查方式，逐漸獨立為專責網路被害調查，專門針對網路犯罪(含詐欺犯罪)進行調查，並設有專責的機制或政府部門負責，其調查管道呈現多元態樣，定期地透過電訪、面訪或網路報案(online report)之方式收集網路被害調查之資料。

(二)網路詐欺被害問卷調查得知，網路詐欺型態，居首者為投資詐欺、其次為網路購物被害，第三為猜猜我是誰(假冒親友)。而受訪者對去一年有詐騙經驗者之網路詐欺型態前三名依序為：網路購物、投資詐欺與玩網路遊戲。詐騙被害時間大多集中晚上、加被害人存在陌生關係、透過網路 ATM 轉帳等特性，而詐騙金額未滿 1 萬元者佔受訪被害人之 62.3%。此外，男性、40 歲以下、教育程度愈低、月收入愈低者愈容易遭受網路詐騙；值得注意的是，網路詐騙的發生與居住地區或城鄉沒有顯著關係。多變量研究指出，被害誘因與動機、衝動性與心理依賴等因素，顯著地預測網路詐欺被害的程度。

(三)網路詐欺加害者深度訪談得知，加害人從事網路詐欺犯罪都存在著缺錢或需錢孔急的時候，透過朋友介紹引進詐騙集團或公司。不論哪一類型網路詐騙集團或公司，均呈現專業與分工的角色，透過集團或公司的教育與訓練、再加上友儕教授、耳濡目染，精益求精，成為專業；但對於其他部門則有默契地宣稱不瞭解或不清楚，因此無法得知上下游的分工對象。獲利程度超出預期，生活過於奢侈與闊綽，但錢來得過去得也快，難以有所積蓄累積與

斷離此一循環。加害者相信臺灣警察偵查與查緝的能力，深知自己有一天會被逮，只是遲早之問題，所以盡量能騙就騙。認為當前的反詐騙宣導措施仍有效，但應該更加普及以及分齡分級為佳。

(四)政策焦點團體座談得知，目前行政院新世代打擊詐欺策略存有以下幾點困境：1.識詐層面存在未能分齡分眾宣傳防詐、教育訓練未能擴及第一線執法人員之專業與精進以及實務上已存在重複被害之情形;2.堵詐層面存在 165 反詐專線之任務編組位階過低、「數位中介法」與「科技偵查法」未能立法、尚未能廣泛運用高科技如 AI 技術於偵辦網路詐欺犯罪、法官的審判與量刑較為保守以及社群平臺規避審查責任等，讓當前堵詐成效受限；3.阻詐層面則是政府與產業界合作仍然不足、偵查部門對於區塊鍊、加密貨幣進行交易與資產移轉，能力不足以及金融機構與警方合作偵辦網路詐欺犯罪尚有努力空間；4.懲詐層面存在司法互助曠日廢時、派駐他國聯絡官人力不足、數位專家鑑定機制尚未成立、懲詐之刑度與量刑過短以及政府與民間橫向連結與情資互通，仍嫌不足。

最後，本研究根據前揭國際網路詐欺調查方式之比較、問卷調查結果與深度訪談之發現，並根據第二次政策焦點團體座談，將與會學者與專家之意見，根據當前行政院所頒定之「新世代打擊詐欺策略行動綱領」，具體提出治本與治標(即識詐、堵詐、阻詐與懲詐)兼具之建議作為，以優化或精進當前之打詐策略，並提供行政院與相關部會(內政、法務、數發與財政等部)參考。

關鍵字：網路詐欺犯罪、網路詐欺被害、低自我控制、網路日常活動理論、新世代打擊詐欺策略

第一章　緒論

第一節　研究背景分析

網路詐欺，根據刑法第 339 之 4 條第一項第三款，以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯刑法第 339 條第一項之行為，即透過網際網路或其他媒體等傳播工具，行為人意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付予行為人之行為。據此，行為人網路詐欺行為是否構成網路詐欺犯罪，其構成要件包含行為人主觀上具有「不法所有之意圖」，亦即主觀上必須具有為自己或第三人獲取違法之財產上利益之不法意圖，同時，行為人還必須具備詐欺的故意，心中清楚認識到以實現詐術方式，使被害人陷於錯誤而交付財物，進而進行財產上的處分，使其於財產上蒙受損害，上述各客觀要件間具有相當因果關係。

21 世紀資訊科技的快速進步，使得人類在現代社會的群體生活中，增加許多便利性。回想起 1980 年前後，家家戶戶主要的娛樂只有客廳的電視機，彼此的聯絡只能透過市內電話及街道上的公共電話亭，對於金錢的交付轉帳大多透過面交或金融機構及其提款機操作進行轉帳。當年的詐欺案件，除了面對面的金光黨詐騙案件，信用卡詐欺及提款機轉帳詐欺案件在當時也是少數。如今，由於科技的便利，人們透過聯結網路可觀看影片、休閒娛樂、上網購物、查詢資料、知識傳遞等，不僅消除知識（或資訊）的鴻溝，亦縮減城鄉的差距，大大改變人類生活的食衣住行育樂各方面，不過在盡情使用網際網路的同時，也提高詐欺被害的風險。

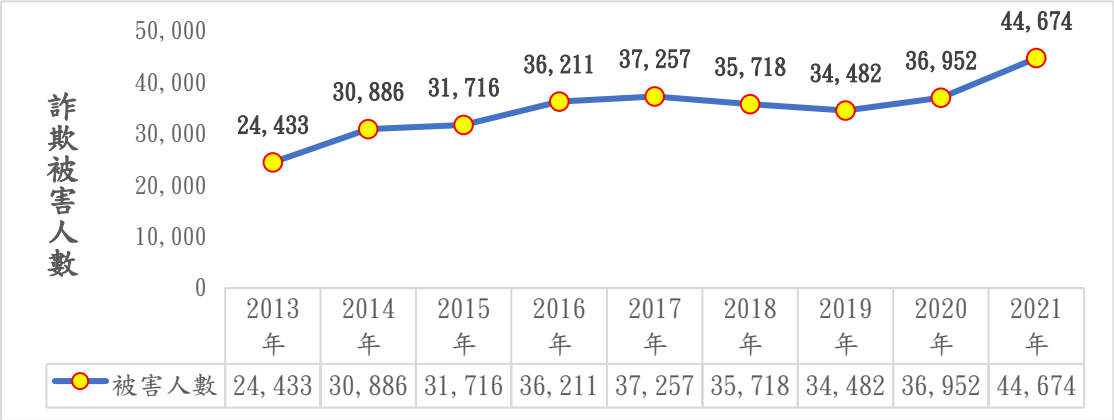
根據臺灣網路資訊中心(Taiwan Network Information Center, TWNIC)「2022 年臺灣網路報告」顯示[1]，比較 2006 至 2022 年的個人上網率之歷年趨勢，臺灣民眾上網率較去年略有增長，年滿 18 歲以上、近三個月有上網經驗的民眾，已占 84.30%。由以上數據可以說明，網際網路已成為我們生活中不可或缺的一部分，它提供一個虛擬

[1] 2022 年臺灣網路報告 https://report.twnic.tw/2022/TrendAnalysis_internetUsage.html

生活空間，相對也產生出許多犯罪的「場所」及「機會」（王秋惠，2007）。當我們享受資訊科技所帶來生活上的各項好處時，資訊科技也可能會因人性弱點而產生各種問題，包括電腦駭客、網路色情、盜版侵權、網路成癮等其他網路犯罪行為。隨著 5G 網路世界的來臨，對傳統社會造成衝擊與隱憂，連帶地升高了對人類生活之威脅及危害。

根據內政部警政署統計，近年詐欺被害人的數目不斷地增加，自 2013 年 24,433 人上升至 2021 年 44,674 人，被害人數新增 20,241 人，增幅達到 1.83 倍（詳圖 1-1-1）。人類在享受無線科技便利的此刻，似乎也需面對現代犯罪類型的轉變。現實社會中發生的傳統犯罪類型，透過網際網路，已經使犯罪地點轉換至虛擬世界中（曾百川，2006）。顯見如何打擊詐欺犯罪，降低被害者人數，建立有效的網路詐欺被害預防策略與防制機制，係為一重要的議題。

圖 1-1-1　2013 年至 2021 年詐欺被害人數統計分析



資料來源：內政部警政署統計查詢網 https://ba.npa.gov.tw/npa/stmain.jsp?sys=100

進一步針對詐欺被害人年齡、被害犯罪手法等分析發現，2021 年各年齡層詐欺被害人數分布中，以 30 歲至 39 歲的被害人數最多，計有 10,087 人（占 22.58%），其次為 24 歲至 29 歲被害人，計有 9,167 人（占 20.52%），18 歲至 23 歲被害人，計有 8,432 人（占 18.87%）。由此可知，18 歲至 39 歲被害人數共計 27,686 人（占 61.97%）。因此，青壯年是我國詐欺被害的高風險族群（詳圖 1-1-2）。

圖 1-1-2　2021 年詐欺被害各年齡層分布統計圖

年齡	被害人數	%
70 歲以上	1,944	4.35
60-69 歲	3,794	8.49
50-59 歲	4,367	9.78
40-49 歲	6,103	13.66
30-39 歲	10,087	22.58
24-29 歲	9,167	20.52
18-23 歲	8,432	18.87
未滿 18 歲	780	1.75
總計	44,674	100.00

註：70 歲以上人數，包括 32 名年齡不詳之統計人數

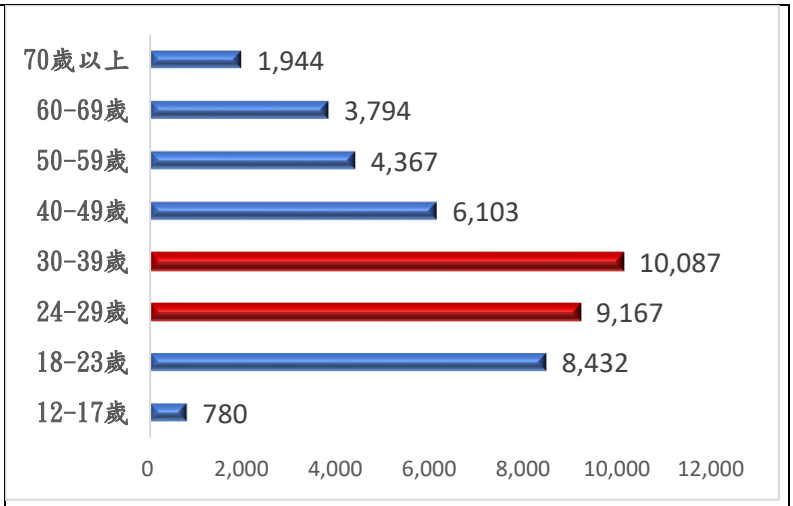


圖 1-1-3 得知，2022 年 1 至 10 月詐欺案件犯罪手法，以「投資詐欺」5,301 件（占 22.15%）最多，「解除分期付款詐欺（ATM）」3,881 件（占 16.22%）次之，「一般購物詐欺（偽稱買賣）」2,913 件（占 12.17%）居第 3；與 2021 年 1 至 10 月同期比較，以「猜猜我是誰」(假冒親友)[2]減少 461 件（-30.82%）及「盜（冒）用好友身分」減少 83 件（-15.78%）較多；而以「投資詐欺」增加 1,418 件（+36.52%）最多。另從警政署公布的網路詐欺類型來看[3]，於 2021 年 LINE 詐欺案件占網路詐欺案件之 20.13%，不同年齡層使用 LINE 通訊軟體之主要受騙方式亦有所不同，其中未滿 17 歲被害人受騙方式以「假愛情交友」占比最高（21.21%），18 歲以上，未滿 60 歲各年齡層則皆以「投資詐欺」最高，占比介於 4 成 4 至 6 成間，60 歲以上以「猜猜我是誰(假冒親友)」最高，占比 3 成 6，顯示網路詐欺被害型態具多元性，民眾使用通訊軟體時，應提高警覺。

[2] 猜猜我是誰(假冒親友)係指加害人佯稱是潛在被害人之親友，聯繫或交談中裝熟、攀親帶故，其目的是要向被害人借錢或購買遊戲網卡點數或進行網路投資，以便詐騙；而盜(冒)用好友身分係指某人在未經潛在被害人許可的情況下使用其個人識別資訊(例如姓名、身分證號碼或信用卡號碼）去實施網路詐欺或其他犯罪。

[3] LINE 通訊軟體陷阱多，小心謹慎免迷惑！
https://www.npa.gov.tw/ch/app/data/view?module=wg054&id=2206&serno=1c4473d6-7d64-4567-abf1-cbf1e1187938

圖 1-1-3　2022 年 1 至 10 月詐欺案件發生數及破獲數概況

(按犯罪方法區分)

犯罪方法	發生數			與上年同期比較		破獲數		與上年同期比較	
	件數	結構比(%)	當期發生數(件)	增減數(件)	增減率(%)	件數	當期發生當期破獲數(件)	增減數(件)	增減率(%)
總　計	23,927	100.00	13,965	3,622	17.84	23,398	12,878	3,311	16.48
投資詐欺	5,301	22.15	2,653	1,418	36.52	5,290	2,465	1,512	40.02
解除分期付款詐欺(ATM)	3,881	16.22	2,529	336	9.48	3,942	2,459	388	10.92
一般購物詐欺(偽稱買賣)	2,913	12.17	1,807	417	16.71	2,861	1,693	402	16.35
假網路拍賣(購物)	2,502	10.46	1,522	303	13.78	2,438	1,388	280	12.97
假愛情交友	1,184	4.95	663	229	23.98	1,137	594	179	18.68
猜猜我是誰	1,035	4.33	625	-461	-30.82	1,058	610	-456	-30.12
偽稱代辦貸款	946	3.95	611	407	75.51	925	571	423	84.26
假冒機構(公務員)	865	3.62	604	-74	-7.88	869	573	-80	-8.43
遊戲點數(含虛擬寶物)詐欺	856	3.58	526	151	21.42	829	477	130	18.60
借錢不還含票據詐欺(空頭)	819	3.42	322	37	4.73	816	304	41	5.29
假求職	709	2.96	503	292	70.02	694	473	302	77.04
盜(冒)用好友身分	443	1.85	259	-83	-15.78	419	237	-112	-21.09
其他	2,473	10.34	1,341	650	35.66	2,120	1,034	302	16.61

資料來源：警政統計通報 https://www.npa.gov.tw/app/data/doc

網路詐欺犯罪官方統計資料的犯罪黑數可能很高，許多被害者可能因為損失金額不高、顧及個人名譽或其他因素而選擇不向警察報案(Standler, 2002)。因此，幾乎不可能僅透過官方次級資料，以完全獲知目前網路詐欺犯罪真正發生件數，或是精確統計被害者金錢損失。另由於網路詐欺犯罪人利用網路的匿名性、各種加密設備和網路跳板，尋找合適的被害人並實施犯罪，使得犯罪偵查困難度較高，執法機構難以逮捕和起訴犯罪者(Furnell, 2002；Grabosky & Smith, 2001；Yar, 2005)。換言之，網路詐欺被害件數逐年上升，而執法部門始終無法嚇阻網路詐欺案件發生，詐騙手法猶如阿米巴原蟲一般日新月異。且詐騙集團組織分工結構層級分明，憑現今偵查能力不易一網打盡，對民眾的生活構成極大的威脅。因此，除了積極掌握官方資料統計趨勢，亦應透過客觀且深入的實證研究，使政府與民眾對於網路詐欺被害有完整了解，並提出相關預防與因應對策，提升大眾對網路安全與被害問題的重視程度。

第二節　研究重要性

一、深入調查網路詐欺被害經驗之必要性

目前社會大眾對於網路詐欺案件的認識及瞭解，大多來自內政部警政署刑事警察局之統計數據，與日常向民眾宣導避免被害。雖然官方犯罪統計資料豐富，取得容易，且有助於分析整體犯罪趨勢，並可瞭解詐欺案件歷年發生件數的消長。但官方資料仍存有犯罪黑數(Dark figure of crime)的問題，且會因為執法機關記錄方式差異而影響官方統計結果；亦可能因警察機關執行專案計畫，而造成官方紀錄的失真（許春金，2017）。因此，除了警察機關統計之網路詐騙手法，亦**應透過網路詐欺被害經驗調查，藉以瞭解當事人的被害風險因子、被害經驗及歷程，始能掌握網路詐欺被害的真實全貌**。換言之，網路詐欺被害調查與統計分析有其必要性。

二、詳盡探究網路詐欺被害者或被害情境之特性

綜觀國內有關網路詐欺犯罪相關研究，在犯罪者、法律、偵查技術方面的探討已相當豐碩且多元（孔令維，2018；田明府，2021；林師賢，2021；陳煌明，2019），但對於被害者在虛擬世界中的人口特性、自我控制、生活型態、機會情境緊張等之探討較少，且多以青少年及大學生為研究樣本（石泱、王乃琳，2021；何英奇，2015；吳嫦娥，2004；洪瑞聰，2014；蔡博忠，2008；蔡義聰，2010；韓佩凌、鄔佩麗、陳淑惠、張郁雯，2007；魏希聖、李致中、王宛雯，2006）。由此可知，過去研究對於網路詐欺被害類型與被害人特性的探討，以及網路詐欺被害理論的建構仍有待補足。

因此，本研究期能透過大樣本的網路詐欺被害調查，針對被害人性別、年齡、職業、教育程度、被害時間、金額等個人資料，以及被害經驗/情境、網路生活型態、心理特質等變項，**俾瞭解網路詐欺被害人的被害狀況、網路生活型態和情境，深入探究導致網路詐欺被害的關鍵因子**。

三、建立有效的網路詐欺被害預防策略與防制機制

陳玉書、簡鳳容、呂豐足及劉士誠（2020）研究發現，無論網路犯罪被害人口特性或情境機會均存在集中特性；人口特性與情境機會間存在顯著關聯性，人口特性和情境機會對是否會造成網路犯罪被害損失具有顯著影響力，尤其以網路犯罪被害途徑、教育程度和加/被害人關係最具影響力。國外研究亦發現被害與偏差多半有重疊現象（Kerstens & Jansen, 2016；Choi & Li, 2017）。因此，為能建立有效的網路詐欺被害預防策略，必須先從探討網路詐欺犯罪案件之特性著手。進一步**探究我國網路詐欺被害之現況、態樣及風險因子，並提供預防策略及防範機制之研究建議，作為刑事司法機關處理此類案件之參考，以降低犯罪被害事件之發生。**

第三節　研究目的

本研究目的如下:

一、蒐集國、內外網路詐欺之相關調查或官方資料中網路詐欺定義，並編製網路詐欺被害調查問卷，進行調查以分析網路詐欺被害者人口特性、心理特質、網路生活型態與情境機會，以及網路詐欺被害經驗等變項分布情形。

二、針對網路詐欺之定義、型態、範疇，以及網路詐欺被害調查問卷設計的妥適性，邀請相關領域之實務、學術工作者召開專家焦點座談，以利調查之進行。

三、於網路問卷調查後，針對網路詐欺加害人進行質性訪談，並與網路被害調查結果進行比較分析。

四、參考實證研究調查發現與國外防治經驗，擬訂防制對策，並邀請相關領域之實務、學術工作者召開專家焦點座談，討論提出未來改善網路詐欺犯罪與被害之實務對策或修法建議。

五、根據上述研究發現提出網路詐欺犯罪與被害之預防對策，並於學術發表會發表研究成果，提供民眾與政府機關參考。

第四節　相關名詞詮釋

一、網路詐欺

網路詐欺(Internet fraud/cyber fraud)，根據刑法第 339 之 4 條，是一種利用網路所進行的詐欺或欺騙行為，亦即行為人透過網際網路虛擬世界之特性，意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付之行為，導致被害人在財產上有所損失。學者謝開平(2003)認為，網路詐欺係指行為人經由網際網路，欺騙自然人或操控電腦，而取得他人財產之行為。林宜隆(2000)也認為網路詐欺行為其實就是網路犯罪行為的態樣之一。由於網路世界可能涉及隱藏資訊或提供不正確的資訊，其目的就是要騙取被害者的金錢、財產和遺產等。網路詐欺不被視為是一種單一的、獨特的犯罪，而是涵蓋了在網路空間中所實施的一系列非法和不正當行為(Barney, 2018)。然而，它與傳統竊盜不同的是，在這種詐欺情境底下，被害人是自願並知情的情況下向加害人提供資訊、金錢或財產(Brenner, 2009)。它的特徵之一是涉及犯罪時的時間和空間上是分離的型態而著稱(Fisher & Lab, 2010)。

二、網路詐欺被害

美國司法部(Department of Justice)對於網路詐欺被害(Internet fraud crime victims)所下之定義為：係指利用網路或網路空間之一部分對潛在之被害人實施誘騙行為，進而使被害人與之進行交易，或依照詐欺指示將款項匯入金融機構或其他相關機構，而網路詐欺被害係指個人使用電腦或通訊軟體網路，遭受到網路偏差或犯罪行為的侵害。本研究所謂的「詐欺」行為，係依據我國現行刑法第 339 條之規定，指行為人意圖為自己或第三人不法之所有，施用詐術使被害者交付財物或獲得財產上不法之利益之行為。所謂「詐術」行為，乃指以作為或不作為的方式，透過語言、文字、圖畫等來傳遞與事實不符的資訊。本研究之網路詐欺犯罪被害，係指被害人透過網際網路，於拍賣及購物網站、網路聊天室、電子郵件、網路遊戲或網頁等虛擬世界中，因

加害人傳達虛偽不實的資訊，並以詐騙的方式使其陷於錯誤進而交付財物（包括現金、虛擬貨幣等），因而造成一定程度的損失及傷害（方呈祥，2020；王秋惠，2007；曾百川，2006）。

三、心理特質

個人的性格係由多個特性所組成，為表示其在心理學上的意義，統稱之為心理特質（特徵）。由個體行為與心理歷程所顯示出的心理特質有很多，廣義言之，範圍可包括心理學所有的研究主題；狹義言之，則可指在人格這個主題下的心理特質，包括動機、情緒、態度、價值觀、自我觀念等主題（張春興，1999）。根據實證研究結果，網路成癮與網路詐欺被害二者亦呈正相關，個人待在網路的時間愈久，相對的成為網路詐欺被害人機會也會高 （Chang et al., 2015; Lin et al., 2020; Simsek et al., 2019; 周愫嫻，2014; 謝龍卿，2004）。另根據 Gottfredson 和 Hirschi（1990）認為，具有低自我控制的人具有衝動性、冒險性及低克制能力等特性，若具該項心理特質者，亦會增加網路詐欺被害風險 （Bossler & Holt, 2010; Koukia, 2020; Schreck, 1999; Schreck et al., 2002; 王秋惠，2007; 簡鳳容，2018; 葉雲宏，2008）。例如 Holtfreter 等人 (2008)研究指出，低自我控制與衝動性格是預測詐欺被害的重要預測指標。綜上，本研究所謂的心理特質（psychological traits）之測量概念為「偏差動機」、「網路成癮」、「衝動性」、「冒險性」及「低克制能力」等因子。

四、網路生活型態與情境機會

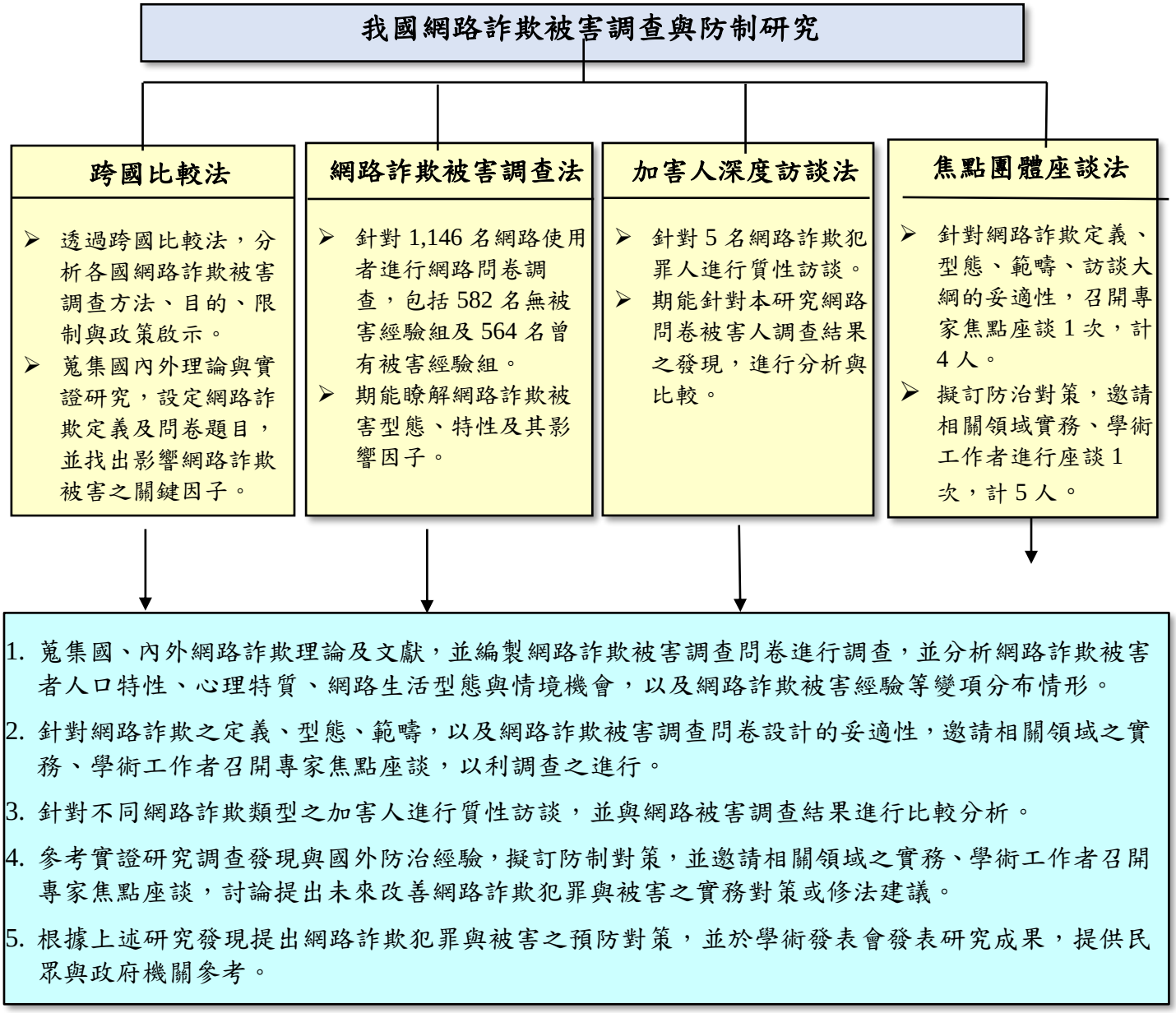
從情境與機會觀點來探討個人遭遇網路詐欺被害時，大多聚焦於日常活動中的合適標的物出現、有能力監控者不在場和有動機的犯罪者出現等三個因素時空的聚合。本研究所謂網路生活型態與情境機會，係指受訪者透過電腦或行動通訊網路時：（一）是否容易將個人暴露於「網路風險」情境之下，因而導致被害事件的發生。（二）電腦或手機設備是否有「數位監控」情境，以致能遏阻其被害。（三）網路「被害誘因」，如在網路情境中看到非法或偏差誘因訊息的機會，容易成為網路詐欺被害標的。因此，測量概念為「網路風險」、「數位監控」、「被害誘因」等變項。

第五節 本研究設計與實施

一、研究設計

本研究參酌相關理論與實證研究，主要目的在檢視我國網路詐欺被害現況、研析先進國家網路詐欺被害的調查方法、擬定國內網路詐欺被害調查問卷題目、找出網路被害的關鍵因子，並提供防制對策及具體建議予相關單位參考。在計畫執行中，研究團隊將從四種不同因途徑著手：（一）跨國比較法；（二）網路詐欺被害調查法；（三）網路詐欺加害人深度訪談法；（四）專家學者焦點團體座談法，進行分析以達成前述之研究目的（參見圖 1-5-1）。本研究希望透過跨國比較，瞭解各國網路詐欺調查方式，並透過國內網路詐欺被害人的問卷調查，透過加害人深度訪談及專家學者的焦團體座談，釐清國內網路詐欺被害現況、特性、影響因子、問題產生原因，以及目前防制網路詐欺策略的利弊得失，期能提供有效的防詐對策。

圖 1-5-1　研究設計與研究方法



二、研究方法與研究對象

本研究涉及運用問卷調查法與深度訪談法，以個人為對象，使用介入、互動之方法對於個人之系統性調查，必須送倫理審查委員會進行審查。本研究案於 2022 年 10 月核准進行後，即送國立成功大學人類研究倫理審查委員會進行審查(詳附錄一)，也業經該審查委員會於同年 12 月同意審查通過後始予以執行(詳附錄二)，相關研究方法與研究對象，詳述如下。

（一）跨國比較法

跨國比較法較常在犯罪科學研究中被普遍採用，犯罪科學的研究非常注重資料的鑑別度，沒有相互的比較，就無法鑑別資料的真偽，例如許春金、陳玉書等人(2014)第三級、第四級毒品犯罪與防制之研究；陳玉書、林健陽等人(2014)女性受刑人矯治處遇之跨國比較與分析等相關研究均採用跨國比較法。因此，本研究利用比較分析法（Comparative Analysis Approach），蒐集各國詐欺被害調查方法，並解釋各國詐欺類型的相似和相異性，試圖找出歧異（王文科、王智弘，2020）。本研究透過蒐集和本研究相關之國內外期刊、著作、論文與研究報告等文獻資料，加以整理、歸納、分析，並參考各國被害調查設計或相關研究，進行初步瞭解及釐清問題的癥結點，以形成研究設計的重要基礎，再配合網路詐欺被害問卷調查、詐欺加害人質化訪談、預防政策之專家焦點團體座談，藉以瞭解我國民眾受網路詐欺之被害經驗及其特性，並以國外相關防治對策為借鏡，綜合提出防制網路詐欺之策進作為，期能在現有研究成果的基礎上，發展及開拓全新的知識領域。

（二）網路詐欺被害調查法

近年網路調查法（Internet survey）普遍運用於各研究領域，實施調查過程中運用電腦製作問卷和傳送問卷，或將調查工具置於網路調查平臺，受訪者可同時間經由網路接收問卷或連結調查平臺，迅速將調查結果回饋給調查人員，並對結果加以分析與推估的調查方式（Smyth, 2018; 魏曼伊，2008）。本研究為充分了解網路詐欺被害型態、特性與影響因素，根據網路犯罪被害相關理論與文獻、官方資料分析結果和研究者參與犯罪被害調查經驗等，編製「網路詐欺被害調查問卷」，透過 SurveyCake 線上調查平臺進行網路問卷調查。

本研究調查對象為居住在臺澎金馬地區且年滿 18 歲以上之網路使用者，如 20 歲受訪者若有需要可知會家長並討論參與意願。在實施正式調查前，除透過文獻探討網路詐欺之定義、型態、範疇；另就問卷設計架構和內容的妥適性，邀請犯罪學/被害者學和網路/科技犯罪偵查領域之學者專家召開焦點座談，完成本研究調查工具初稿(焦

點座談紀錄如附錄三)。並就符合條件之樣本 96 名進行前測，以及參考期中報告審查委員之建議，進一步修改問卷內容，據以形成正式調查研究工具（詳見附錄五）。

本研究自 2023 年 5 月 15 日至 7 月 14 日正式實施網路被害調查，調查期間將訊息公告於委託研究機關(司法官學院)網頁，以昭公信；並向網路社群網站之會員，發布調查訊息和問卷網路連結，邀請符合研究條件之受訪者至指定之網址填寫問卷。由於此項調查對象包括 2022 年 1 月 1 日至 2023 年 7 月 13 日期間曾經遭受網路詐欺被害經驗，為有效蒐集網路詐欺被害樣本，調查期間行文刑事警察局將調查訊息和網路連結公布於內政部警政署 165 全民防詐網頁和「165 防騙宣導」Line 帳號，以及各縣市警察局所屬派出所在受理網路詐欺被害案件時，將此項調查相關訊息和網路連結提供報案民眾，尤其自主選擇是否參加此項調查。

此項調查之問卷內容包括：人口特性、心理特質、網路生活型態與情境機會、網路詐欺犯罪被害等 4 個部分(參見附錄五)，問卷填答約需時 10 分鐘。受訪者至指定之網址填寫問卷，並告知前 1,200 名完整填寫問卷者，將會收到 100 元統一超商(7-11)現金券，以答謝參與此項調查。為保障受訪者隱私，此項調查採無記名及無法辨識個人資料的方式作答；受訪者在開始調查前須先閱覽知情同意書(參見附錄四)。完成所有調查問項，可於問卷最末頁自由選填電子信箱或手機號碼；待此項研究網路問卷調查完成後，由負責調查資料管理之研究成員，將 100 元現金抵券透過 e-mail 或手機簡訊傳送給受訪者。

未免樣本人口特性過於集中，調查時控制樣本之性別、年齡、職業與網路詐欺被害等變項，並設置身分檢驗以避免重複填答，提高研究樣本之代表性。為維護調查品質與研究倫理，受訪樣本如有下列狀況則視為無效樣本，(1)年齡未滿 18 歲；(2)填答時少於 4 分鐘(240 秒)；(3) IP 位置重複且多數資料雷同者；(4)機器或程式填答；(5)答案不合邏輯或明顯胡亂回答等。就總調查人數 2,307 人而言，符合樣本條件且有效樣本數為 1,146 人(占 49.67%)，其中填答問卷時間未滿 240 秒者有 20 人(占 0.87%)，人工檢誤刪除無效樣本 62 人(占 2.69%)，進入

調查而不符調查條件者有 1,079 人(占 46.77%)。1,228 位完成調查的受訪者中，扣除經資料清理、邏輯檢誤和刪除無效樣本後，有效樣本數為 1,146 人(占 93.32%%)(參見表 1-5-1)。

表 1-5-1　網路被害調查有效樣本分布

項目	總調查人數		完成受訪人數(不含隔離區)	
	人數	%	人數	%
符條件有效樣本	1,146	49.67	1,146	93.32
隔離區				
填答未滿 240 秒	20	0.87	20	1.63
人工檢誤刪除無效樣本	62	2.69	62	5.05
不符合調查條件樣本數	1,079	46.77	-	-
合計	2,307	100.00	1,228	100.00

註: 調查網頁總瀏覽人數為 4,365 人，含進入調查網頁開始填答而未完成調查之受訪者。

（三）網路詐欺加害人深度訪談法

深度訪談法（In-depth interview）係一種重要的質性研究方法，研究人員透過「訪問」方式，直接蒐集被研究者之觀點、經歷、價值觀和其他具有重要意義等相關資料。深度訪談常用「半結構式」訪談大綱，問題大多以開放式為主、封閉式為輔，而深度訪談法亦常與問卷調查、焦點團體法等其他研究方法相互結合，藉以蒐集更多元及豐富之資料（Showkat & Parveen, 2017；萬文隆，2004）。本研究除對於網路問卷進行被害調查外，亦針對 5 名從事網路詐欺犯嫌，採「半結構式」訪談的方式進行質性訪談，依據本研究架構擬定訪談大綱，透過矯正機關安排，實地進行面對面訪談。讓受訪者依循訪談大綱回答問題，並依實際回答情形，彈性調整訪談問項之內容及順序，希望能更清楚地瞭解網路詐欺犯案之歷程。

本研究深度訪談的研究對象，主要以觸犯刑法第 339 條詐欺罪名，且利用網路為媒介工具實施犯罪者，依研究目的所需，透過矯正機構

安排，採取「立意抽樣」方式，選取 5 名受訪樣本，以在監服刑中之受刑人為優先之訪談對象。如無法對矯正機構內之受刑人進行訪談，再於社區尋找曾觸犯「網路詐欺犯罪」類型或是已服刑完畢之更生人進行訪談。為能增加受訪者及研究者彼此間之信任度，每名受訪者皆進行 1 或 2 次的深度訪談，每次訪談時間約 1~2 小時，以獲得完整之資料。最後再將訪談結果打成逐字稿，並加以分析、歸納並獲得結論。有關網路詐欺加害人深度訪談取樣條件及標準如表 1-5-2 所示：

表 1-5-2　加害人深度訪談對象取樣條件與標準

訪談對象	人數	取樣條件
觸犯刑法第 339 條詐欺罪名，且透過「網路」為犯案管道，且目前仍在監服刑之受刑人	1 人	「投資詐欺」之詐欺手法
	2 人	「電信客服人員」之詐欺手法
	3 人	「網路購物詐欺」之詐欺手法

（四）焦點團體訪談法

焦點團體訪談法（Focus group interviews）是一種以「團體」訪問的型式，進行質性研究收集資料的方法。本研究將由研究主持人、協同主持人與熟識網路詐欺犯罪或被害之實務工作者和學者專家進行焦點團體座談，針對網路詐欺被害的研究主題，由參與的成員自由表達其經驗、看法或觀點，期能以最短時間內，獲得廣泛且詳盡的資料。為能使資料蒐集更加齊全及完備，本研究將採取 2 階段焦點團體，進行資料蒐集：(1)預定於研究開始進行之初，針對網路詐欺定義、型態、範疇、訪綱的妥適性，召開專家焦點座談 1 次，該場次預計有 4 名專家學者共同參與；(2)網路問卷調查完成後，針對實證研究結果與參考國外防治經驗，擬訂防治對策時，再邀請相關領域之實務、學術工作者召開專家焦點座談 1 次，計 5 人，合計共舉辦 2 場次焦點團體座談，參與研究對象共 9 人。所有參與焦點團體之學者專家與實務工作者須投入相關研究或工作超過 5 年(詳表 1-5-3)：

表 1-5-3　參與第 1 場次及第 2 場次焦點團體之專家學者

參加場次	相關領域	代碼	專家學者姓名	服務單位	討論主題
第 1 場次	被害者學	F1	OOO 博士	○○大學	網路詐欺之定義、型態、範疇，以及訪綱的妥適性
	網路犯罪與問卷設計	F2	OOO 博士	○○大學資管系	
	網路犯罪偵查警政	F3	OOO 科長	○○○警察局	
	網路犯罪偵查檢調	F4	OOO 檢察官	○○○地檢署	
第 2 場次	網路犯罪偵查檢調	F5	OOO 前檢察官/律師	○○○律師事務所	網路詐欺被害的防制對策，並討論有效的預防對策
	網路金融科技公司	F6	OOO 執行長	○○○金融科技公司	
	金融機構網路銀行資安負責人	F7	OOO 資安長	○○○銀行	
	科技犯罪偵查技術及網路鑑識	F8	OOO 博士	○○大學助理教授	
	網路犯罪偵查警政	F9	OOO 股長	○○○警察局	

第三節 網路被害調查之概念測量與資料處理分析

（一）網路問卷概念測量

根據上述理論與相關實證研究發現，此項研究致力找出**網路人口特性、心理特質、網路生活型態和被害情境等網路詐欺被害風險因子**；並主張完整的網路詐欺被害解釋模式須涵蓋網路使用者的人口及心理特質，因不同人口結構及心理特質的人會有不同的網路生活型態，暴露在不同風險的網路情境中。其次，網路生活型態與情境機會（如網路風險、數位監控及被害誘因等）反映出個人在網路世界的活動模式，並提供加害者對其從事網路詐欺犯罪的管道；最後，在缺乏數位監控之下，遭受網路加害者侵入而被害，或者被害者在接受網路詐欺被害誘因刺激的情境中，與加害者互動過程而成為網路詐欺被害人，皆會容易造成不同的網路詐欺被害經驗，以及被害次數、被害損失之發生及不同的被害反應。

本研究網路詐欺被害調查測量工具內容主要包括**（1）人口特性**：含性別、年齡、職業、收入、教育程度等。**（2）區域特性**：含區域位置、城鄉等。**（3）心理特質**：網路使用者的心理特質，包括偏差動機、網路成癮、衝動性、冒險性及低克制能力等。**（4）網路生活型態：**網路生活型態係指個人日常活動中，有關使用網路行為的特性及其影響，包含網路使用經驗、網路風險等**（5）情境機會**：包括防衛監控、遊樂動機、被害誘因三個部分。**（4）網路詐欺被害**：包括有無被害經驗、網路詐欺被害多元性、重複被害、最近一次網路詐欺被害經驗，詳如表 1-5-4 所示。

表 1-5-4　本研究概念與變項測量表

研究概念	變項內容
自變項	
人口特性	性別、年齡、職業、收入、教育程度
區域特性	區域位置、城鄉
心理特質	偏差動機、網路成癮、衝動性、冒險性、低克制能力

網路生活型態	網路使用經驗、網路風險
情境機會	防護監控、遊樂動機、被害誘因
依變項	
網路詐欺被害	有無被害經驗、網路詐欺被害多元性、重複被害、最近一次被害經驗

（二）研究概念測量與信度、效度分析

1. 網路生活型態

網路使用經驗包括每天上網時數、每周上網次數、周末上網時段、接觸網路時間、擁有網路帳號等，詳如表 1-5-5 所示。

表 1-5-5　網路使用經驗測量內容

變項名稱	測量內容
每天上網時數	①1 小時以內、②1 至 2 小時以內、③2 至 4 小時以內、④4 至 6 小時以內、⑤6 小時以上，共 5 個等級。
每周上網次數	①少於 1 次、②1-3 次、③4-6 次、④7-9 次、⑤10 次以上，共 5 個等級。
周末上網時段	①08：01 至 12：00、②12：01 至 14：00、③14：01 至 18：00、④18：01 至 22：00、⑤22：01 至 02：00、⑥02：01 至 08：00，共 6 項。
接觸網路時間	①1 年未滿、②1 年～2 年未滿、③2 年～3 年未滿、④3 年～5 年未滿、⑤5 年～10 年未滿、⑥10 年以上，共 6 個等級。
擁有網路帳號	①購物網站、②線上遊戲、③網頁留言討論區、④社群軟體(TELEGRAM、LINE、IG、FB、TWITTER、WECHAT、抖音等)、⑤交友平臺(TINDER、IPAIR、WETOUCH、SWEETRING、JUSTDATING、GOODNIGHT等)、⑥直播平臺(抖音、BILIBILI、VOOM、西瓜視頻、土豆等)，共6類。

網路風險，在問卷調查中（問卷第 2-3 題（1）至（8）小題），該變項係衡量受試者過去接觸網路訊息、觸法行為等情形，藉由詢問其網路生活型態狀況，以瞭解對網路詐欺被害影響。受試者在李克特量表之得分為：回答「經常」者得 4 分、「偶爾」者得 3 分、「很少」者得 2 分、「從未」者得 1 分。故在此分量表得分越高者，代表涉入網路生活型態越深，對個人之負面影響越大，詳如表 1-5-6 所示。該量表因素分析可分為 2 組，其一為「接觸偏差訊息」，內含接觸投資詐騙等 5 問項，因素負荷量在.641 至.829 之間，特徵值為 3.024，信度係數（Cronbach's Alpha）為.816。另一為「網路觸法行為」，內含妨害他人電腦使用等 3 問項，因素負荷量在.626 至.892 之間，特徵值為 1.151，信度係數為.731。顯示網路生活型態之次概念均具有相當之內部一致性與穩定性。

表 1-5-6　網路風險變項測量內容

問項	接觸偏差訊息	網路觸法行為
接觸投資詐騙的訊息	**0.829**	-0.084
接觸網路詐騙別人財物的訊息	**0.827**	-0.048
接觸網路援交或一夜情的訊息	**0.745**	0.199
接觸線上賭博或賭盤的訊息	**0.705**	0.166
接觸買賣盜版軟體的訊息	**0.641**	0.354
曾妨害他人電腦使用	-0.027	**0.892**
曾未經允許使用他人帳戶	0.037	**0.889**
曾在網路買賣違禁物品	0.386	**0.626**
特徵值	3.024	1.151
解釋變異量%	37.797	14.393
Cronbach α 係數	0.816	0.731

2. 情境機會

情境機會中，包含防護監控、遊樂動機與被害誘因等。防護監控為情境機會之正向因子，可預防被害；反之，遊樂動機與被害誘因則為促發被害之因子。

防護監控在問卷調查中（問卷第 4 題（1）至（13）小題），該變項係衡量受試者過去使用網路的習慣及經驗等情形，藉由詢問其防護監控狀況，以瞭解對網路詐欺被害影響。受試者在李克特量表之得分為：回答「經常」者得 4 分、「偶爾」者得 3 分、「很少」者得 2 分、「從未」者得 1 分。故在此分量表得分越高者，代表受試者防護監控意識越高，對個人之正面影響越大，詳如表 1-5-7 所示。該量表因素分析可分為 3 組，首先為「自我防護意識」，內含提升隱私權限等 9 問項，因素負荷量在.606 至.761 之間，特徵值為 4.162，信度係數（Cronbach's Alpha）為.843。其次為「實體監控」，內含家人注意、朋友意見等 2 問項，因素負荷量分別為.877 與.864，特徵值為 1.902，信度係數為.785。最後為「避免曝露」，內含避免公開行蹤、避免公開財產等 2 問項，因素負荷量分別為.788 與.753，特徵值為 1.039，信度係數為.491。顯示防護監控三項次概念均具有相當之內部一致性與穩定性。

表 1-5-7　防護監控變項測量內容

問項	自我防護意識	實體監控	避免曝露
瞭解提升隱私或安全權限以保護自己	**0.761**	0.032	0.058
會到官方網站購物或下載軟體	**0.704**	-0.090	-0.026
使用公共 Wi-Fi 會留意來源及安全性	**0.700**	0.090	0.007
在網路上看到疑似假訊息會進行確認	**0.690**	-0.086	-0.163
會知道 IP 位址被網站記錄或追蹤	**0.652**	0.053	-0.110
會定期更改個人帳號密碼	**0.624**	0.297	0.057
登入網站有使用雙重認證	**0.617**	-0.041	-0.201
會注意網路留下何種個人資訊	**0.611**	0.106	-0.140
電腦、手機或平板有安裝防毒軟體	**0.606**	0.121	0.110
上網時，家人會注意網路使用情形	0.081	**0.877**	-0.098
上網時，朋友會提供意見	0.040	**0.864**	-0.221
避免在網路公開個人相關行蹤	-0.178	-0.064	**0.788**
避免在網路公開身分職位或個人財產	0.052	-0.236	**0.753**
特徵值	4.162	1.902	1.039

解釋變異量%	32.014	14.631	7.992
內部一致性 α	0.843	0.785	0.491

遊樂動機與被害誘因在問卷調查中（問卷第 2-2 題（1）至（8）小題），該變項係衡量受試者過去使用網路的情形，藉由詢問其遊樂動機與被害誘因狀況，以瞭解對網路詐欺被害影響。受試者在李克特量表之得分為：回答「經常」者得 4 分、「偶爾」者得 3 分、「很少」者得 2 分、「從未」者得 1 分。故在此分量表得分越高者，代表涉入遊樂動機與被害誘因越深，對個人之負面影響越大。經分析排除網路購物與網路投資等 2 問項（與依變項高度重合），詳如表 1-5-8 所示。該量表因素分析可分為 2 組，其一為「被害誘因」，內含點擊不明來源電郵等 3 問項，因素負荷量在.722 至.871 之間，特徵值為 2.880，信度係數（Cronbach's Alpha）為.781。另一為「遊樂動機」，內含遊玩網路遊戲等 3 問項，因素負荷量在.543 至.835 之間，特徵值為 1.116，信度係數為.662。顯示遊樂動機與被害誘因等 2 項次概念均具有相當之內部一致性與穩定性。

表 1-5-8　遊樂動機與被害誘因變項測量內容

問項	被害誘因	遊樂動機
點擊不明來源的電子郵件	**0.871**	0.058
點擊經由通訊軟體所接收到的未知來源檔案或附件	**0.827**	0.111
從網站上下載不明來源的檔案	**0.722**	0.356
遊玩網路遊戲	0.062	**0.835**
瀏覽色情網站	0.167	**0.792**
與未知身分的網友透過網路聊天	0.49	**0.543**
特徵值	2.880	1.116
解釋變異量%	48.002	18.605
內部一致性 α	0.781	0.662

3. 心理特質

心理特質中，包含偏差動機、網路成癮與低自我控制等，3 者均為促發被害之負向因子。

偏差動機在問卷調查中（問卷第 3-2 題（1）至（7）小題），該變項係衡量受試者對網路使用經驗的看法等情形，藉由詢問其偏差動機狀況，以瞭解對網路詐欺被害影響。受試者在李克特量表之得分為：回答「非常同意」者得 4 分、「同意」者得 3 分、「不同意」者得 2 分、「非常不同意」者得 1 分。故在此分量表得分越高者，代表涉入偏差動機越深，對個人之負面影響越大。詳如表 1-5-9 所示，因素負荷量在.670 至.795 之間，特徵值為 3.670，信度係數（Cronbach's Alpha）為.843。顯示偏差動機此一組別均具有相當之內部一致性與穩定性。

表 1-5-9　偏差動機變項測量內容

問項	偏差價值
當人受網路誘惑，而做壞事是正常的	0.795
在網路上說他人壞話或不良評價，並不會對他人產生傷害	0.754
在網路世界沒有人是誠實的，所以對他們說謊也是剛好而已	0.735
當人缺錢時，在網路上詐騙或偷盜是一件可以原諒的事情	0.712
使用網路詐騙成功也是一種本事	0.707
在網路創造不同的身分或偽裝自己並不容易被發現	0.688
在網路下載非正版軟體不會造成他人損害	0.670
特徵值	3.670
解釋變異量%	52.423
內部一致性 α	0.843

網路成癮在問卷調查中（問卷第 3-3 題（1）至（13）小題），該變項係衡量受試者對網路使用的情形，藉由詢問其網路成癮狀況，以瞭解對網路詐欺被害影響。受試者在李克特量表之得分為：回答「經常」者得 4 分、「偶爾」者得 3 分、「很少」者得 2 分、「從未」者得 1 分。故在此分量表得分越高者，代表網路成癮越嚴重，對個人之負面影響越大。詳如表 1-5-10 所示，該量表因素分析可分為 2 組，其一為「行為依賴」，內含忍不住上網等 7 問項，因素負荷量在.491 至.803 之間，特徵值為 6.881，信度係數（Cronbach's Alpha）為.895。另一為「心理依賴」，內含上網的興奮感等 6 問項，因素負荷量在.550 至.814 之間，特徵值為 1.164，信度係數為.867。顯示網路成癮之 2 項次概念均具有相當之內部一致性與穩定性。

表 1-5-10　網路成癮變項測量內容

問項	網路成癮	
	行為依賴	心理依賴
想去做別的事卻又忍不住再次上網看看	**0.803**	0.280
每天醒來或睡前，第一想到就是上網	**0.787**	0.184
需要花更多時間在網路上才能得到滿足	**0.770**	0.336
花費在網路上的時間比原先預計的還要長	**0.736**	0.214
不管再累，上網時總覺得很有精神	**0.697**	0.362
不能控制自己上網的衝動	**0.692**	0.402
不只一次告知花太多時間在網路上	**0.491**	0.432
對上網的興奮感或期待遠勝於其他人際互動	0.252	**0.814**
曾因為上網而沒有按時吃飯或睡覺	0.144	**0.780**
因為上網的關係，您從事其他休閒活動的時間減少了	0.318	**0.745**
因為上網的關係，您和家人或朋友實際見面互動減少	0.345	**0.701**
想減少使用網路，會因而沮喪、心情低落、脾氣暴躁	0.445	**0.596**
網路斷線或連不上時，您會覺得自己坐立不安	0.462	**0.550**
特徵值	6.881	1.164
解釋變異量%	52.932	8.954
內部一致性 α	0.895	0.867

低自我控制變項因為抽象理論之檢驗，故須將概念操作化過程詳予說明。該變項在問卷調查中，係衡量受試者生活經驗與性格特質中低自我控制之傾向（問卷第 3-1 題（1）至（12）小題）。受試者在李克特量表之得分為：回答「經常」者得 4 分、「偶爾」者得 3 分、「很少」者得 2 分、「從未」者得 1 分。故在此分量表得分越高者，代表低自我控制程度越嚴重，對個人之負面影響越大。詳如表 1-5-11 所示，該量表因素分析可分為 3 組，首先為「冒險性」，內含只為好玩而冒險等 4 問項，因素負荷量在.594 至.837 之間，特徵值為 4.646，信度係數（Cronbach's Alpha）為.821。其次為「衝動性」，內含關心短期內的事等 4 問項，因素負荷量在.608 至.810 之間，特徵值為 1.595，信度係數為.777。最後為「低克制能力」，內含容易發脾氣等 4 問項，因素負荷量在.571 至.820 之間，特徵值為 1.294，信度係數為.766。顯示低自我控制之 3 項次概念具有相當之內部一致性與穩定性。

表 1-5-11　低自我控制變項測量內容

問項	低自我控制		
	冒險性	衝動性	低克制能力
只為好玩而冒險	**0.837**	0.213	0.12
尋求刺激比安全更重要	**0.826**	0.123	0.149
做惹麻煩的事而感到興奮	**0.821**	0.147	0.12
喜歡做冒險的事考驗自己	**0.594**	0.192	0.094
比較關心短期內所發生事	0.065	**0.810**	0.154
不會花很多時間去想未來	0.139	**0.774**	0.121
會做當下感到快樂的事	0.311	**0.713**	0.128
一衝動起來就採取行動	0.249	**0.608**	0.286
很生氣時他人離我遠一點	0.13	0.089	**0.820**
很容易發脾氣	-0.021	0.212	**0.806**
很難心平氣和談論問題	0.191	0.257	**0.691**
生氣寧可傷害他人	0.433	0.093	**0.571**
特徵值	4.646	1.595	1.294
解釋變異量%	38.713	13.295	10.787
內部一致性 α	0.821	0.777	0.766

4. 網路詐欺被害

本研究之依變數為「最近一次網路詐欺被害經驗」二元類別變數，主要在測量受試者過去使用網路的經驗；在進行羅吉斯迴歸分析時，則將依變項分為「無」和「有」網路購物詐欺被害經驗等二類，以觀察人口特性、網路生活型態、情境機會和心理特質對於網路詐欺被害之影響。除此之外，還包含詐欺被害次數、最近一次網路詐欺被害經驗（如被害類型、被害網路平臺/管道、與加害人關係、如何發現被害、損失金額、未報案原因、被害反應等），相關網路詐欺被害測量內容，詳表 1-5-12。

表 1-5-12　網路詐欺被害測量內容

變項名稱	測量內容
過去網路詐欺被害次數	①0 次、②1 次、③2 次、④3 次、⑤4 次以上，共 5 個等級。
最近一次網路詐欺被害類型	①上網購物、②在網路上投資、③網路交友或愛情詐騙、④參加網路活動、⑤解除分期付款詐欺（ATM）、⑥玩網路遊戲、⑦不明人士盜(冒)用好友身分、⑧求職、⑨接獲「猜猜我是誰(假冒親友)」之網路通話來電或訊息、⑩其他網路詐騙被害，共 10 類。
被害網路管道	①線上遊戲交戰/同隊、②虛擬寶物交易、③交友網頁/軟體、④加害者主動接觸、⑤購物、⑥性交易、⑦曾見面之朋友介紹、⑧未曾見面之網友介紹、⑨參考網路評價、⑩其他等，共 10 類。
與加害人關係	①熟識、②普通、③初識、④不認識，共 4 個等級。
如何發現被害	①自己察覺、②警方通知、③朋友或同事發現、④親人發現、⑤超商店員提醒、⑥金融機構櫃檯提醒/報警、⑦其他等，共7類。
損失金額	①未滿1千元1001未滿1千元、②1,001元至未滿1萬元、③1萬元至未滿3萬元、④3萬元至未滿10萬元、⑤10萬元至未滿50萬元、⑥50萬元至未滿100萬元、⑦100萬至未滿1,000萬元、⑧1,000萬元以上、⑨沒有損失，共9個等級。
未報案原因	①自認倒楣、②不想追究、③被騙金額不多、④覺得丟臉、⑤報案沒有用、⑥報案程序太複雜、⑦想要私下解決、⑧害怕加害者報復、⑨認為只是消費糾紛、⑩其他等，共10類。
被害反應	①跟家人討論、②跟朋友討論、③撥165反詐騙專線、④網路平臺客服申訴、⑤沒有處理、⑥向警察報案、⑦在網路上公告經驗、⑧其他等，共8類。

（三）量化資料處理與分析

本研究針對網路詐欺被害調查所蒐集所得資料特性，使用的統計分析方法如下：

1.次數分配（Frequencies）：係利用計算某類別變項之各數值出現之次數，呈現摘要資訊。透過次數分配表，瞭解樣本分布情形，例如利用次數分配分析樣本在性別、年齡、經濟條件、教育程度、職業、居住地點和網路詐欺被害等變項之分布情形。次數分配為敘述統計，亦可藉此瞭解變項之集中趨勢（平均數、中位數、眾數、總和）及分散情形（標準差、變異數、範圍、最小值、最大值、平均數之標準誤）。

2.卡方（χ^2）關聯性檢定：卡方檢定係用以檢定二個類別或順序尺度變數有無統計上之顯著關聯性（statistically significant association），如性別與網路詐欺被害之關聯性。

3.皮爾森（Pearson）積差相關：用以檢定二個等距或等比變數（連續變項，continuous variables）間相關強度及方向，如研究樣本自我控制程度與網路詐欺被害之相關程度。

4.Cronbach's α 係數：用以測量研究概念量表之內部一致性信度，Cronbach's α 係數之數值恆介於 0 與 1 之間，Cronbach's α 值越高，表示信度越佳，問卷題目具有內部一致性，如低自我控制量表、網路生活型態量表等之內部一致性檢定。

5.因素分析（Factor Analysis）：用以測量研究概念量表之建構效度，主成分分析法（principle component analysis）進行分析，概念量表含二個以上因子，則以直交轉軸之最大變異法（Varimax Rotation）抽取因素負荷量（factor loadings）較大之題目組成各分量表，以檢驗並提高各分量表之建構效度，如低自我控制量表之建構效度檢定。

6.獨立樣本 t 檢定：用以檢定二組互為獨立之母群體，在連續依變數之平均數是否有顯著差異，其自變項須為類別尺度，依變項須為等距或等比尺度，如一般組與網路詐欺被害組樣本在心理特質之差異檢定。。

7.單因子變異數分析（One-way ANOVA）：用以檢定自變數為三個以上常態母體在依變數之平均數是否相等，自變項為類別尺度，依變項為等距或等比尺度。Levene 變異數同質性檢定結果，如變異數同質，根據檢定嚴謹程度宜選擇 Scheffe 進行事後多重比較；反之，若 Levene 變異數同質性檢定結果變異數不同質，則常選擇 Dunnett's T3 進行事後多重比較。如不同工作類型者在網路生活型態之差亦進行檢定。

8.羅吉斯迴歸分析（Logistic Regression）： 用以檢定各影響因子對於過去一年是否曾遭受網路偏差被害之影響力，以找出有效預測網路詐欺被害的影響因子。

第四節 深度訪談與焦點團體座談研究對象與工具

（一）質性訪談工具

1. 加害人訪談大綱

本研究將依研究目的、相關理論與文獻，採「半結構式」方式進行訪談，依據本研究之研究架構擬定訪談大綱，由研究者本人及受過訓練的訪員進行面對面的深度訪談，訪談地點將以受訪者之所在地為主，最主要讓受訪者依循訪談大綱回答問題，並依實際回答情形，彈性調整訪談問項之內容及順序，訪談內容如下（如表 1-5-13）(訪談大綱詳附件七)：

表 1-5-13　加害人訪談大綱主要內容

訪談主題	訪談內容
基本資料	性別、年齡、婚姻、教育程度、初犯或再累犯等
家庭狀況	父母婚姻狀況、父母管教情形、家庭背景
學校成長經驗	國（高）中時期學習狀況、學業成績、在校適應問題、逃學與輟學經驗、
個人生活型態	就學與就業情形、交友情形與平時休閒活動、與網路詐欺犯罪之經驗等
從事網路詐欺之情形	與被害者互動情形、犯罪所得報酬、周遭監控能力、如何尋找合適的標的物、如何規避警方查緝、是否曾擔心被逮的風險等
對於網路詐欺防制策略之認知	多久被查獲、查獲原因、從事網路詐欺之風險程度與風險因素、網路監控措施與網路詐欺行為之規避措施、獲利方法與手段、警察查緝能力之認知

概括問題	其他政府採行反詐欺預測策略之建議事項

2. 專家焦點團體座談大綱

本研究針對網路詐欺之定義、型態、範疇，以及訪綱的妥適性，邀請相關領域之實務、學術工作者召開專家焦點團體座談，並擬定焦點團體座談訪談大綱，內容如下（如表 1-5-14）；另有關擬訂網路詐欺被害的防制對策，俟本次研究完成跨國文獻探討、質化與量化分析初步成果後，再行編製訪談大綱及召開第 2 場次的專家焦點座談，討論並提出改善網路詐欺之實務對策，訪談大綱如表 1-5-15。

表 1-5-14　第一次專家焦點團體座談訪談大綱內容

1. 對於研究計畫書中「網路詐欺被害」之**研究概念和變數**有何建議。
2. 對於「網路生活經驗調查表」之**調查說明**，以及**「第一部分:人口特性」**（包括性別、年齡、職業、收入、教育程度等）的測量項目和回答選項有何修改建議。
3. 對於**「第二部分：心理特質」**係指網路使用者的心理特質（包括偏差動機、網路成癮、衝動性、冒險性及低克制能力等等）的測量項目和回答選項有何修改建議。
4. 對於**「第三部分：網路生活型態與情境機會」**，指網路生活型態係指個人日常活動中，有關使用網路行為的特性及其影響（包括網路風險、數位監控、被害誘因等）的測量項目和回答選項有何修改建議。
5. 對於**「第四部分：網路詐欺被害」**，指本研究依變項的測量項目（包括有無被害經驗、被害次數、被害類型、損失金額、被害反應等）和回答選項有何修改建議；除詐欺犯罪被害，還有哪些型態的犯罪被害應該進一步做調查。
6. 對於網路調查的執行，如調查訊息發布、抽樣（本研究控制性別和年齡層）、如何避免重複填答、受訪費用（如 line 點數或悠遊卡等）和研究倫理等有何建議。

表 1-5-15　第二次專家焦點團體座談訪談大綱內容

1. 從各國網路詐欺被害調查之管道與機制得知，有無值得借鏡之處？
2. 網路詐欺犯罪有無資訊/資安/理工等相關理論可解釋其行為或模式?
3. 從網路詐欺被害經驗問卷調查結果得知，被害人之心理特質與網路生活型態與其網路被害息息相關，請問被害人可以如何防範被網路詐欺被害？
4. 從網路詐欺犯罪加害者的深訪結果得知，執法部門可以從何處強化，以降低渠等犯案動機或減少被害人被詐機會？
5. 從網路詐欺犯罪被害者與加害者之心理特質與日常生活之相同與相異點分析，可否提供相關的抗制網路詐欺犯罪對策？
6. 晚近新加坡/中國等華人社會對於網路詐欺犯罪之抗制策略，是否有參考採之處?
7. 當前政府打擊詐欺犯罪之策略，是否應該針對不同類型(例如購物、投資與電信客服..)，提供不同的策略方式？
8. 行政院於今年 5 月成立專責之打詐辦公室，以強化當前打詐的編制，迄今有無相關成效？

（二）質化資料分析方法

1. 建立訪談逐字稿

在每一次深度訪談後，由訪談的研究助理依照下列的方式整理資料：（1）將訪談錄音帶的內容以電腦打字，謄寫成逐字稿。每份逐字稿均以代號「受訪者 A」、「受訪者 B」等表示訪談參與者，並在每份訪談逐字稿的開頭註明深度訪談實施地點、日期及時間等訪談資料。（2）反覆地聆聽訪談錄音帶，校對錯誤及疏漏的部分，直到正確無誤。（3）為保障參與者的隱私，逐字稿中以代號顯示。

2. 資料歸納與編碼

在完成逐字稿後，對研究對象語意不明之處，反覆仔細聆聽深度訪談錄音帶，以找出資料中的重要脈絡。其次根據深度訪談綱要發展編碼架構。再將逐字稿內容就意義、事件、觀點或主題轉換時，即斷開成為一個小段落，視為一個意義單元，並引出特殊意義，然後將意義單元在編碼架構中進行歸納。

（三）訪談資料之信賴度

本研究參考 Lincoln 和 Guba（1985）所提出的方法來強化質性研究結果之信賴度，包括 4 項衡鑑指標（Lincoln & Guba，1985；鈕文英，2017），包括 **1.確實性（可信性，Credibility）**，指個案訪談研究資料真實的程度。**2.可轉換性（遷移性，Transferability）**，指將受訪者所陳述的感受與經驗，有效地轉換成文字陳述。**3.可靠性（Dependability）**，在進行訪談時，訪談者在不同時間以相似的詢問內容或發現來進行檢驗。**4.可驗證性（Confirmability）**，即所蒐集的訪談內容若由其他受訪者進行訪談，應該也有相同的結論，為提升訪談資料的客觀性。

五、研究倫理

（一）知情同意下自願參與研究

本研究網路問卷調查對象為 18 歲以上之網路使用者，在正式施測之前會主動告知研究參與者研究主旨、研究目的、研究分析等相關資訊，網路詐欺被害問卷採不記名及無法辨識個人的方式作答。所有參與網路調查的對象，於調查網頁的第 1 頁需詳細閱讀相關說明後，將由參與研究者自由決定是否填寫本問卷，亦可中途直接退出。深度訪談則透過各監所相關人員擔任守門人，透過守門人協助尋找適合的詐欺加害人作受訪對象，並安排適當的訪談方式及場所。若監所因 Covid-19 防疫關係之考量，訪談方式亦可彈性改採線上視訊。

另透過守門人轉交加害人訪談知情同意書(詳附錄六)，上面記載本研究系經過「國立成功大學倫審會字第 111-526-2 號」審查通過字樣與訪談大綱(詳附錄七)，先行過目。每名受訪者訪談費 1,000 元，由研究團隊成員進行 1 或 2 次的深度訪談，每次訪談時間約 1~2 小時，以獲得完整之資料。關於守門人所提供的資訊，研究團隊將負起保密的責任，不會向任何人透漏相關資料。此外，研究者在正式進行詐欺加害人訪談及焦點團體座談前，亦會主動告知本研究目的、邀請參與研究原因、訪談過程及實行方式、可能承受的風險及因應的措施、研究補償、研究資料之保存期限、運用規劃及到期後處理規劃、資料的使用範圍、暫停及退出研究之權益、訪談過程錄音錄影、第三方研究諮詢管道等相關權益。若在受訪的過程中，受訪者感到不舒服，想要暫停或退出研究，本研究團隊會完全尊重受訪者個人的意願。

（二）研究程序的進行與分析客觀公正

本研究對象包含 1,146 名網路詐欺被害的問卷調查、5 名質化研究的受訪者及 2 場次專家焦點團體座談。由研究人員對參與者提供適當的解釋說明，事先告知研究的目的、範圍、設計、執行步驟及研究方法，最重要的是應取得本人之同意，以研究參與者的福祉為優先考量，保護其不受到傷害及侵犯隱私。此外，本研究所蒐集之資訊僅和所牽涉之相關專業人士進行討論，一切符合研究倫理之規定。另本研究在分析「網路詐欺問卷調查」量化成果部分，研究團隊成員會將所獲得的相關資料，不捏造數據或竄改研究成果，或是刻意忽略某些資料，以達客觀公正之分析，真實呈現研究結果。

在「網路詐欺犯罪人」及「專家焦點團體訪談」的質化研究部分，所有研究成員於事先需接受訪員行前訓練，告知本研究宗旨及訪談大綱，事後亦透過同儕檢驗方式及三角驗證法，以降低受訪者訪談內容被不當詮釋。最後，在撰寫研究報告時，研究者若發現本研究設計缺失及研究限制，亦會公開承認及坦白，避免其他研究者犯下相同的錯誤。因此，本研究為能將成果發揮其最大效益，無論是量化的統計分析結果，或是深度訪談及焦點團體座談所歸納的結論，將真實呈現客觀、公正、正確的資訊提供給社會大眾，以保障民眾知的權利。

（三）避免抄襲、欺騙及遵守研究倫理

本研究無論於網路上公開徵求「網路詐欺被害人」研究對象，抑或在監所內招募「網路詐欺犯罪人」或邀請「專家焦點團體座談」自願者進行訪談時，皆不會採用欺騙的研究手段。且在本研究過程中，時時提醒研究成員不可違反研究倫理及研究行為的相關準則，避免造成研究對象心理或精神上的傷害。另在撰寫論文內容部分，本研究成員除引註文獻來源，列出參考書目，且所有分析結果，皆由研究團隊親自撰寫統計分析及歸納質化訪談逐字稿，不抄襲他人之研究成果，以符合社會科學研究所應恪守的研究倫理。

此外，為保護個案之隱私及權利，本研究「網路詐欺問卷調查」量化研究部分，分析的結果皆以整體數據資料呈現，而非以個案方式進行分析；另在「網路詐欺犯罪人」及「專家焦點團體訪談」質化研究的部分，所有受訪個案皆轉換成代碼，將無從識別個案的身分及相關資料。此外，本研究成員亦通過研究倫理相關訓練，研究者除充分理解資訊保密倫理守則，並會主動告知所有可能接觸資訊者，應負保密責任的相關規定，不能隨意將研究樣本之個人資料外洩，以免觸犯受訪者個人隱私權。

第二章　網路詐欺被害調查與相關因素探究

第一節　各國網路詐欺被害調查概況

一、美國詐欺被害調查

1967 年美國最早進行全國性大規模的被害調查，以瞭解未被警方記錄的犯罪有多少，其中包括了詐欺犯罪被害調查。國家犯罪被害調查(National Crime Victimization Survey, NCVS)的補充詐欺調查(Supplemental Fraud Survey , SFS)收集過去 12 個月中成年人在 7 種個人金融詐欺中的經歷數據。它還收集有關被害者特徵的資訊，以及該事件是否已向警方或其他人報告。補充詐欺調查 SFS 收集個人層面的數據，包括 7 種個人金融詐欺被害的盛行率、被害者的特徵，及向警方和其他當局報告的模式。受訪者被問及在進行調查前的 12 個月內，是否曾經遭受過不同類型的個人財務詐欺，而詐欺被害是按調查時的年份，而非被害年份分類的。並向詐欺被害人詢問被害經歷的詳細過程，例如：交易中損失的金額，是否向警方或消費者保護機構報案，與被害後是否有負面社會或情感反應，以及被害的負面經濟後果。

鑒於網路攻擊與網路詐欺行為持續地影響美國人民的日常生活，且現行的犯罪被害調查已不足以因應日趨頻繁且研究嚴重的網路各類型犯罪型態，美國聯邦調查局遂於 2000 年 5 月成立網路犯罪報案中心(Internet Crime Complaint Center, 簡稱 IC3)，專責受理各類型網路犯罪與問題之報案，包含多種形式的網路詐欺行為，例如電腦入侵（駭客攻擊）、網路詐欺、網路勒索、國際洗錢、身分盜用、以及愈來愈多的網路投資案件（例如投資虛擬貨幣）。截至 2022 年 12 月 31 日，IC3 已經收到超過 700 萬起的網路報案案件（FBI, 2023）。根據 FBI 的分析，美國成立 IC3 以打擊網路犯罪的專責單位，具有以下幾種角色：

1.可與民間部門以及地方、州、聯邦和國際相關機構合作。

2.經營 www.ic3.gov 網路，專責受理被害人報案。

3.扮演中央樞紐以提醒民眾注意網路犯罪與威脅。

4.執行分析、轉介報案和追回資產。

5.透過 FBI 的執法企業門戶網站(Law Enforcement Enterprise Portal, LEEP)，介接遠端查詢數據庫。

根據 IC3 的報告，過去 5 年，IC3 平均每年收到 652,000 起報案。過去 5 年已累積達 325 萬餘件。這些報案涉及影響全球被害人的各種網路詐騙，損失的金額已高達 276 億美金，平均每年的損失金額達到 5.5 億美金（詳表 2-1-1）。

表 2-1-1　美國網路報案中心過去五年的報案數量與損失金額

年度	2018	2019	2020	2021	2022	總計
報案件數	351,937	467,361	791,790	847,376	800,944	326 萬餘
損失金額（10 億）	$2.7	$3.5	$4.2	$6.9	$10.3	$27.6

資料來源：FBI(2023)，2022 Internet Crime Report.

其次，根據 IC3 的統計，過去五年的所受理的網路報案案件，前五名的犯罪類型為假客服(tech support)、勒索(extortion)、未付款/未交貨(non-payment/non-delivery)、個人資料洩漏(personal data breach)以及網路釣魚(phishing)（詳表 2-1-2）。

表 2-1-2　美國網路報案中心過去五年排名前五名的網路犯罪類型

網路犯罪類型	2018	2019	2020	2021	2022
假客服	14,408	13,633	15,421	23,903	32,538
勒索	51,146	43,101	76,741	39,360	39,416
未付款/未交貨	65,116	61,832	108,869	82,478	51,679
個人資料洩漏	50,642	38,218	45,330	51,829	58,859
網路釣魚	26,379	114,702	241,342	323,972	300,497

資料來源：FBI(2023)，2022 Internet Crime Report.

IC3 也針對網路詐欺犯罪類型對於美國民眾之威脅與現況，進行以下分析。

（一）網路投資(Cyber investment)

2022 年，投資詐騙是向 IC3 報案財產損失最多的網路詐欺型態。網路投資詐欺報案從 2021 年的 14.5 億美金增加到 2022 年的 33.1 億美金，增幅為 127%。在這些報案中，加密貨幣投資詐欺 (Cypto-investment scams) 從 2021 年的 9.07 億美金增加到 2022 年的 25.7 億美金，增長 183%。加密貨幣投資詐騙的被害人數量和投資者的損失金額都空前增加。許多被害人承擔巨額債務以彌補該投資詐欺的損失，此類詐欺報案的被害人年齡組最多落在 30 至 49 歲。2022 年報案的加密貨幣投資詐騙有一些變化包括：

1.流動性挖礦(Liquidity mining)：被害人被引誘將其加密貨幣錢包鏈接到詐欺性流動性挖礦 App。然後加害人在未通知被害人或未經被害人許可的情況下轉移被害人的資金（IC3 指出加害者在流動性挖礦騙局中瞄準並利用加密貨幣持有者）。

2.社群媒體被駭(Hacked social media)：加害者駭入社群媒體帳戶，利用不實加密貨幣投資機會，目標是被駭用戶的線上好友。

3.冒充名人(Celebrity impersonation)：加害者冒充名人或社會知名人物，與目標被害人假裝友誼互動，最終被害人被誘騙學習如何投資加密貨幣或陷入錯誤投資機會。

4.房地產專業人士(Real estate professionals)：加害者聯繫房地產經紀人，通常提出以現金或加密貨幣購買非常昂貴的房產。一旦上鉤，加害者將顯露其能掌握虛假帳號，這些帳號據稱價值數百萬美金，以引誘被害人參與投資活動。

5.求職(Employment)：被害人在網上申請投資公司或據稱與投資相關公司的虛假職位。被害人得到的不是工作，而是投資建議。該投資具有詐欺性，旨在向被害人詐取盡可能多的資金。

（二）勒索軟體(Extortion)

2022 年，IC3 收到 2,385 件歸類為勒索軟體的報案，估計損失超過 3,430 萬美元。勒索軟體是一種惡意軟體，會加密電腦上的檔案，以致無法使用。除了對網路進行加密，網路犯罪分子常會竊取系統中的檔案並扣留該檔案，直到支付贖金為止。如果不支付贖金，被害人

的檔案將無法使用。儘管網路犯罪分子以各項技術透過勒索軟體駭侵被害人，但網路釣魚電子郵件、遠端桌面協定(Remote Desktop Protocol, RDP)和一般軟體漏洞仍然是向 IC3 報案的勒索軟體案件的主要初始駭侵媒介。一旦勒索軟體駭入被害者的設備或網路以獲得執行權限代碼，加害者就可以部署勒索軟體。2022 年 IC3 發現勒索軟體用於勒索財物的策略有所增加，加害人威脅被害人，如果不支付贖金，就會公佈被盜檔案，從而迫使被害人付贖。

（三）假客服詐欺(Tech support)

IC3 受理假客服詐欺案件主要有兩種型態，在 2022 年時總共受理 44,092 件，其中技術/客戶服務詐欺計 32,534 件，而冒充政府之詐欺（11,554 件），造成被害人之財損超過 10 億美金，目前仍呈現增加的趨勢。根據 IC3 分析，20 歲以下僅占 0.3%；20-29 歲占 4%；30-39 歲占 4%；40-49 歲占 5%；50-59 歲占 9%；60 歲以上占 69%；遺漏值占 8%。換言之，假客服絕大多數以老年人為目標，造成毀滅性的影響。幾乎一半的被害人年齡超過 60 歲（占 46%），遭受 69%的損失（超過 7.24 億美金）。而這些詐欺行為主要來自南亞（尤其是印度）的假客服。為因應日益增加的被害情況，美國司法部(Department of Justice)和 FBI 正在與新德里中央調查局和印度當地各邦等印度執法部門合作，打擊網路金融犯罪和跨國假客服詐欺。此次合作已交換美國假客服詐欺被害人的筆錄，用於針對犯罪嫌疑人的執法程序。2022 年，在美國執法部門的協助下，印度執法部門對涉嫌參與該網路金融犯罪和全球假客服詐欺的個人進行多次搜索、查緝、扣押和逮捕。

總結 FBI (2023)針對 IC3 2022 年所受理的網路報案數據與資料分析，該年網路犯罪總損失達 103 億美金，自 2000 年該 IC3 成立以來，該中心每一年所收到報案量，總數已超過 730 萬起。過去 5 年，IC3 平均每年收到約 651,800 起報案，即每天超過 2,175 起報案。如果按年齡劃分被害人的報案數量和損失，可以發現有 15,782 名 20 歲以下被害人共損失 2.105 億美元；有 57,978 名被害人年齡介於 20-29 歲者共損失 3.831 億美元；有 94,506 名年齡介於 30-39 歲之被害人共損失 13 億美元；有 87,526 名年齡介於 40-49 歲被害人共損失 16 億

美元；有 64,551 名年齡介於 50-59 歲被害人共損失 18 億美元；有 88,262 名年齡在 60 歲以上被害人共損失 31 億美元。

從網路犯罪型態觀之。首先，從被害人數量多寡觀察，前五大網路犯罪型態依序為網路釣魚、個人資料洩漏、未付款/未交貨、勒索軟體以及假客服，詳表 2-1-3。

表 2-1-3　2022 年美國網路犯罪型態（被害人數排序）

犯罪類型	被害人數	犯罪類型	被害人數
網路釣魚	300,497	假冒政府	11,554
個人資訊洩露	58,859	預付費用	11,264
未付款/未交貨	51,679	其他	9,966
勒索軟體	39,416	超額付款	6,183
假客服	32,538	彩券/抽獎/繼承	5,650
網路投資	30,529	資料洩露	2,795
身分盜用	27,922	針對兒童的犯罪	2,587
信用卡/支票詐欺	22,985	勒索軟體	2,385
電子郵件詐欺	21,832	暴力威脅	2,224
欺騙攻擊 Spoofing	20,649	知識產權/版權/盜版	2,183
信任/愛情詐欺	19,021	轉移 SIM 卡	2,026
求職	14,946	惡意軟體 Malware	762
騷擾/跟蹤	11,779	殭屍網路 Botnet	568
房地產	11,727		
描述資訊*	Descriptors		
加密貨幣	31,310	加密貨幣錢包	20,781
*這些描述資訊與用於促進犯罪的媒介或工具相關，IC3 僅將其用於追蹤目的。 僅在選擇另一種犯罪類型後，它們才可用作描述資訊。			

資料來源：FBI(2023)，2022 Internet Crime Report.

其次，根據被害人財損金額多寡排序，前五大網路犯罪型態依序為網路投資、電子郵件詐欺、假客服、個人資料洩漏以及愛情詐欺（假冒信任），詳表 2-1-4。

表 2-1-4　2022 年美國網路犯罪型態（被害人財損金額排序）

犯罪類型	損失金額	犯罪類型	損失金額
網路投資	$3,311,742,206	彩券/抽獎/繼承	$83,602,376
電子郵件詐欺	$2,742,354,049	轉移 SIM 卡	$72,652,571
假客服	$806,551,993	勒索	$54,335,128
個人資訊洩露	$742,438,136	求職	$52,204,269
信任/愛情詐欺	$735,882,192	網路釣魚	$52,089,159
資料洩露	$459,321,859	超額付款	$38,335,772
房地產	$396,932,821	勒索軟體	*$34,353,237
未付款/未交貨	$281,770,073	殭屍網路 Botnet	$17,099,378
信用卡/支票詐欺	$264,148,905	惡意軟體 Malware	$9,326,482
冒充政府	$240,553,091	騷擾/跟蹤	$5,621,402
身分盜用	$189,205,793	暴力威脅	$4,972,099
其他	$117,686,789	知識產權/版權/盜版	$4,591,177
欺騙攻擊 Spoofing	$107,926,252	針對兒童的犯罪	$577,464
預付費用	$104,325,444		
描述資訊**	Descriptors		
加密貨幣	$2,496,196,530	加密貨幣錢包	$1,349,090,883

* 關於勒索軟體估計的損失，該數字不包括對業務、時間、工資、文件或設備損失的估計，或被害人獲得的任何第三方補救措施的估計。在某些情況下，被害人不會向 FBI 報案任何損失金額，從而人為地降低勒索軟體的整體損失率。最後，該數字僅代表被害人透過 IC3 向 FBI 報案的情況，並不包括被害人直接向 FBI 駐外辦事處/探員報案的情況。

**這些描述資訊與用於促進犯罪的媒介或工具相關，IC3 僅將其用於追蹤目的。 僅在選擇另一種犯罪類型後，它們才可用作描述資訊。

資料來源：FBI(2023)，2022 Internet Crime Report.

截至目前，美國仍是網路犯罪被害調查的先驅，每年透過 IC3 被害人報案系統，使其能與官方犯罪統計相互比較，提供許多政策決定學術研究等用途的資料。世界上其他先進國家，如北歐諸國、德國、英國、荷蘭、瑞士、法國及澳大利亞等亦以收集犯罪被害調查之資訊並形成制度。

二、英國詐欺被害調查

英國於 1982 年由內政部(Home Office)開始進行犯罪被害調查(British Crime Survey, BCS)，始於 1982 年調查之 1981 年被害情形，且涵蓋英國所有三個司法區域，自 2013 年後，僅有英格蘭和威爾斯(England and Wales)，稱為 Crime Survey for England and Wales (CSEW)；而蘇格蘭（Scotland）及北愛爾蘭(Northern Ireland)亦有類似的犯罪與被害調查，用以蒐集犯罪被害者特性、被害狀況以及其他被害相關資訊，稱為 Scottish Crime and Victimisation Survey (SCVS)。此外，英國被害調查亦蒐集一些較為敏感的資料，調查的範圍包括被害經驗、被害者的個人特質、對警察的觀感、被害反應、被害恐懼，以及自陳偏差行為[4]。

自 2012 年開始，英國內政部每年也針對「商業被害調查」(Commercial Victimization Survey, CVS)進行的一系列的調查，目的是記錄針對英格蘭和威爾斯商業被害的性質和程度。該調查涵蓋中小型企業，以及犯罪、被害和司法調查程序的處理，並特別重視年輕被害人。另該調查問卷收集以下的詳細資訊，包括遭遇的被害類型、發生率和普遍性、被盜或損壞的物品、犯罪的成本(包括經濟損失或損害)、所採取的行動和報告模式（例如是否報警等），以及網路犯罪、偏差行為、住家是否有安裝防竊安全設備等。此外，目前英國犯罪調查使用電腦輔助的面對面調查法，委託民間的調查公司依需求來設計並進行訪問。整體上，英國的被害調查類型多元，包括住宅竊盜被害、財物損失被害、竊盜被害、強盜被害、傷害被害、詐欺被害、網路犯罪被害、汽車失竊被害等 8 種被害類型，但並未專門針對網路詐欺被害進行調查。其中「網路犯罪被害」的定義及範圍如下：

1. 未經許可進入您的電腦系統？
2. 以電子方式盜取您的錢財。
3. 向您發送詐欺性資訊後，盜取您的錢財。
4. 將您轉到虛假網站後，盜取您的錢財。
5. 以電子方式竊取您的機密資訊。

[4] https://upwikizh.top/wiki/Crime_statistics_in_the_United_Kingdom

6. 損壞、破壞或關閉您的網站。

7. 是否有任何電腦感染木馬程式，造成電腦檔案或程式無法執行？

8. 其他意圖造成傷害的惡意程式。

2015 年英國犯罪調查的結果首次宣稱，詐欺和網路犯罪是英格蘭和威爾斯最普遍的犯罪行為[5]。由於網路時代來臨，改變犯罪與被害的本質，犯罪分子和有組織犯罪集團不再需要親自犯罪，而是經常利用網路上的匿名性進行犯罪。因此，自 2015 年開始，英國的詐欺和網路犯罪所產生的問題，顯示傳統犯罪的型態正在發生變化。由於詐欺被害者經常遭到受騙，然後由金融機構註銷該筆消費，雙方為省事皆未向警方報案。由於網路詐欺被害案件的犯罪黑數難以估計，不僅阻礙執法部門調查、起訴，亦難以防止潛在被害者的進一步被害。但光是 2015 這一年，詐欺案件對英國經濟造成的損失，粗估為 300 億英鎊以上。相關人士亦呼籲政府應該投入更多資源，協助執法部門幫助及防止被害者被害。英國的國會要求政府應該建構國家級的網路犯罪被害調查，其原因如下(Smith, 2006):

1. 對網路犯罪活動和趨勢，可提供一個可靠的量化衡量標準，使國會能夠履行其民主職能，要求政府對於犯罪狀況這一方面負起責任；

2. 讓公眾、媒體、學術界和相關特殊利益群體了解國家的網路犯罪狀況，並提供（或協助獲得）數據，為更廣泛的辯論和非政府部門之研究議程，提供信息；

3. 告知政府內部和外部相關機關的短期資源分配的政策作為—例如警政和被害者保護；

4. 為警察等國家機構的績效管理和課責制提供資訊；

5. 為政府長期之抗制網路犯罪之戰略和政策發展，提供證據基礎。

6. 政府可以藉此對 ICT 系統、軟體及網路應用程序的設計者、管理者和運營者，施加壓力，要求他們以減少網路犯罪機會和挑

[5] https://www.actionfraud.police.uk/news/british-crime-survey-reveals-extent-of-fraud-and-cyber-crime

釁、引誘的方式設計和管理他們的產品；並提供可靠和有效的數據，這些數據可用於時間序列分析和犯罪預防工作的影響評估。

因此，英國於 2017 年在英格蘭與威爾斯犯罪調查(Crime Survey for England and Wales, CSEW)增加對於網路犯罪之調查，此外英國政府於同一年 10 月成立國家網路安全中心 (National Cyber Security Centre)並運作，為國家級網路安全提供一個單一的中央統籌專責機構。又於 2020 年 5 月啟用英格蘭和威爾斯電話犯罪調查 (Telephone-operated Crime Surevy for England and Wales, TCSEW) ，取代傳統以來運用面對面犯罪調查 (Face-to-face)的犯罪被害調查方式。但 TCSEW 過去三年因為 Covid-19，曾暫停使用。

根據英國國家統計局(2022)針對 TCSEW 數據所進行的詐欺與電腦濫用的分析報告(Nature of fraud and computer misues in England and Wlales, year ending March 2022)，有以下幾點重要發現：

1.與 2020 年 3 月之過去一年相比，2022 年 3 月之過去 2 年欺詐犯罪增加了 25%（達到 450 萬件），原因是“預付費詐欺”(advance fee fraud)和“消費者和零售欺詐”(consumer and retail fraud)的詐欺案件大幅增加。這可能因為 Covid-19 的流行，詐欺犯也利用了民眾使用網上購物的行為頻率與次數增加，進而詐欺的行為與次數也增加

2.此外，從英國國家詐欺情報局(Natioanl Fraud Intelligence Bureau, NFIB)取得之數據亦發現，與 2021 年 3 月過去一年同期相比，2022 年 3 月過去一年 NFIB 受理的欺詐案件增加了 17%（達到 936,276 件）；與 2020 年 3 月過去一年相比，這一數字也高出 25%。

3.根據 TCSEW 顯示，截至 2022 年 3 月 TCSEW 調查了 160 萬起電腦濫用的事件，與 2020 年 3 月過去一年相比，增加了 89%。特別是電腦駭客犯罪(Hacking offences)，截至 2022 年 3 月已經達到 130 萬起，與疫情毒爆發前的 2020 年 3 月相比成長，兩年來成長一倍。這可能與被害者的詳細訊息因大規模數據外洩，以及被害者的電子郵件或社交媒體帳號外洩所致。這一增長趨勢顯示了全球大規模數據外洩的數量也在持續增加中。另外，2022 年網路安全

漏洞調查(Cyber Security Breaches Survey 2022)的結果顯示，39% 的英國企業在過去 12 個月內發現了網路漏洞或攻擊

4.截至 2022 年 3 月的過去一年中，有大約 3 分之 2 (64%) 的詐欺被害者遭受了經濟損失。而根據 TCSEW 的調查，有 77%的被害人其損失少於 250 英鎊，而損失的中位數為 79 英鎊；另有 14%的被害者其損失在 250 英鎊到 999 英鎊之間；而有 9%的被害者其損失達 1,000 英鎊或以上。

5.深入分析，截至 2022 年 3 月的過去一年，估計有 61%的詐欺案件與網路相關，這一比例與 2020 年 3 月過去一年的調查相比，成長 53%。這顯示英國詐欺犯罪的增加與網路有關之詐欺案件的增加，以及與 Covid-19 的流行有關。

6.至於電腦濫用之犯罪案件，截至 2022 年 3 月的過去一年，有 16% 的犯罪事件中，被害者認為是因為他們打開收到的電子郵件、附件或網路連結後而直接導致病毒感染；另有 80%被害者稱是電腦設備性能不佳或停止工作以及 47%的被害者稱是電腦螢幕上不斷出現彈出窗口（pop-ups）之情形而中毒；約有 5 分之 1（19%）的被害者認為是因為開啟文件或數據帳密丟失而所導致被害。

7.網路釣魚是實施網路詐欺的主要方法之一。根據調查，有一半 (50%)的受訪者表示，在調查時的上一個月收到了可能是網路釣魚的電子郵件、簡訊或社交媒體訊息。在這些宣稱有接獲網路釣魚的受訪者中，有 54%的人收到冒充快遞公司詐騙者的訊息，有 32%的人收到來自銀行(banks)、房屋互助會(building societies)或其他金融機構(financial institutions)的訊息，有 29%的人收到自電子商務公司(E-commerce companies)的訊息。

8. TCSEW 的調查也指出，年齡在 25 歲至 34 歲或 35 歲至 44 歲之間的成年人比其他年齡組別之人更有可能收到網路釣魚之訊息(分別為 58%和 60%)。而有工作的成年人(56%)較失業者(39%)或經濟活動較不熱絡的成年人 (40%) 更有可能收到網路釣魚之資訊。而私人租客 (53%) 或房屋擁有者 (52%) 相比，社宅租客 (36%) 收到網路釣魚訊息的可能性較小；然而，社宅租客 (7%)較房屋擁有者 (3%) 更有可能回復或點擊訊息中的連結。

三、歐盟網路詐欺被害調查

在許多歐盟成員國的國家安全戰略(National Security Strategy)中，打擊網路犯罪及預防網路被害已攀升至國安等級的議題，相關的研究也指出，歐盟各成員國迄今尚未有一個穩定且可靠的犯罪數據指出當前網路犯罪的數量有多少，並進一步呼籲歐盟各成員國之政府需要有可靠的犯罪數據調查來源，以便發展出適切的政策與分配正確的資源(Armin et al., 2015, P.135)。Anderson 等人(2013)則認為，當前關於網路犯罪(Cybercrime)的數據來源高達 100 多種，但可用的統計數據仍然不足且零散；他們面臨少報或多報的窘境，這樣的情形取決於收集這些資料團體或機制，並且這些錯誤有可能是故意的（例如，供應商或安全部門渲染威脅程度）但也有可能不是故意的(例如回收率高低的效應或抽樣的偏誤所致)。足見歐盟各國在十年前對於有關網路犯罪的調查，包含詐欺類型、加害或被害，仍屬於混純未明、多頭馬車之情況。

根據聯合國毒品和犯罪問題辦公室政府間網路犯罪專家組(UNODC, Intergovernmental Expert Group on Cybercrime, 2013)的定義，網路犯罪是一個廣泛且不精確的概念。但他們仍認同網路犯罪通常分為三大類(Wall, 2011)。首先，對抗電腦的犯罪(Crimes Against Computers)係指未經授權進入電腦系統的邊界，例如網路侵入或駭客/破解，在此一型態中電腦是犯罪攻擊的焦點與客體，其他的案例尚有電腦病毒、拒絕服務攻擊(Denial-of-Service)和惡意軟體（惡意密碼）植入。其次，使用電腦的犯罪(Crimes Using Computers)，通常被稱為「網路協助犯罪」(Cyber-Enabled Crime)是利用資訊與通訊技術(Information and Communication Technology, ICT) 實施犯罪，例如身分盜用、網路釣魚詐騙以及網路使用信用卡詐欺。第三，「在」電腦的犯罪(Crimes in Computers)，而犯罪的內容即傳統犯罪。主要的犯罪型態為網路色情、網路暴力威脅和恐怖主義(Wall, 2011)。實際上，上述三種區分的類型可能並不精確，例如釣魚郵件可用於誘使用戶點擊連結以竊取資訊，這是 ICT 的作案手法(即網路啟動犯罪)，但也可以同時安裝惡意軟體，此時為電腦整合的犯罪型態。目前，對於網路犯罪類型的分類尚無普遍共識(Gordon & Ford, 2006; Reyns et al., 2014；

Stol, 2012)。即使如此，以下仍就歐盟各國所進行的一些被害者調查來探究歐盟主要的六種網路犯罪形式(Reep-van den Bergh & Junger, 2018)。

（一）網路購物詐欺(Online Shopping Fraud)

網路購物的特點是無法在購買商品前親自地仔細檢查商品，以及參與銷售的各方之間缺乏直接聯繫的情境(Moons, 2013；van Wilsem, 2013a)。因此，與傳統面對面的購物交易相比，消費者面臨更高的詐欺風險。例如在網路上訂購商品時，可能會面臨到商品無法送達、商品無法使用或商品與網路上所提供的照片商品不同。此外，從商家端觀之，如果客戶使用偷取的信用卡盜刷，則商家也會面臨詐欺性購買(Fraudulent Purchase)的風險(Enisa, 2010；Moons, 2013；van Wilsem, 2013a)。

（二）網銀詐欺與支付(Online Banking Fraud and Payment)

當詐欺犯獲得被害者個人網路銀行帳戶的權限並從其帳戶轉移資金時，就會發生網路銀行詐欺行為。在某些情況下，被害人可能會被犯罪人詐欺，自己進行詐欺性的匯款(FFA, 2016)。網路銀行詐欺亦可以從一封釣魚郵件開始，該郵件將用戶引導至一個詐欺網站，用戶必須在該網站上填寫、登入資訊，或者在電腦被安裝惡意軟體後，竊取用戶之登入資訊(Brody et al., 2007；Milletary & Center, 2005)。

（三）其他網路詐欺(Other Cyber Fraud)

這包括例如預付費用詐欺(Advanced Fee Fraud)和身分詐欺(Identify Fraud)(Enisa, 2010)。第一種詐欺型態通常涉及詐欺者向被害人承諾從一大筆錢中分得很大一部分給他，取得其信任以換取被害人的小額預付款，詐欺者也需要預付款才能獲得大筆款項(Enisa, 2010)。第二者身分詐欺是故意使用他人的身分，通常作為獲得經濟利益或以他人名義獲得信貸和其他利益的一種方法，對他人不利或造成損失(Enisa, 2010；Harrell & Langton, 2013；Tuli & Juneja, 2015)。當有人在未經他人許可的情況下使用他人的個人資訊（如姓名、身分證號碼或信用卡號碼）進行詐欺或其他犯罪時，就會發生身分詐欺。身分被

盜用的被害人如果被要求要對犯罪者所造成的損害進行負責時，被害人可能會遭受到不只經濟上的負擔而已，可能在精神上或情感上會遭受一段長時間的煎熬(ITRC, 2014)。

（四）網路威脅/霸凌(Cyber threats/bullying)

網路霸凌是指使用電子技術的霸凌行為(Kowalski et al, 2014；Nansel et al., 2003；Wachs et al., 2017)。研究顯示，遭受網路霸凌的兒童也經常受到當面霸凌，此外，遭受網路霸凌的孩子更難擺脫這種行為(Wachs et al., 2017)。網路霸凌在很多方面都不同於傳統的霸凌行為。首先，網路霸凌可能每週 7 天、每天 24 小時，隨時都可能在發生。其次，網路霸凌資訊和圖像通常是匿名發布的，並且可以迅速傳播給廣大的網路使用群眾。第三，在發布或發送後要刪除不當或性騷擾、性私密之內容和影像，極其困難(Stopbullying.gov 2017)。

（五）惡意軟體(Malware)

惡意軟體是一個總稱，用於代表各種形式的惡意或侵入性軟體，包括電腦病毒、細菌、木馬、勒索軟體、間諜軟體、廣告軟體、恐嚇軟體和其他惡意程式。它的採用形式包含可執行代碼、腳本、活動內容和其他形式的軟體 (Aycock, 2006)。

（六）駭客攻擊或電腦侵入（Hacking or computer intrusion）

駭客是指試圖突破防禦並利用電腦系統或網路的弱點，破解後進入系統之人，包含潛在性一直再嘗試突破電腦或網路系統的人或已經突破侵入之人。其駭入的動機可能有很多種，例如為了獲利、抗議、蒐集個資、挑戰自我、娛樂，或評估一些防護系統的弱點以協助修正潛在駭客侵入的防禦措施(Bachmann, 2010；Conteh & Royer, 2016)。

由於歐盟各國的調查方法、研究對象，以及資料蒐集定義、範圍不一致。因此，各國家之間被害調查的比較，可能會隨著時間的變化或統計分析方法不同而產生落差，較難估計出究竟有多少差異。為能進行各國網路被害者調查研究之比較，Reep-van den Bergh 和 Junger（2018）針對各國的研究方法與納入標準如下：首先，研究方法必須

要清楚的描述，且調查問卷要能正確推論與評估。其次，為能使該調查結果代表一個國家真正情形，該調查研究對象必須採用大樣本隨機抽樣方式為之。第三，必須執行加權程序，以產生具有代表性的結果。第四，該研究需要提供明確被害定義，以及界定固定的被害時間（例如過去 12 個月），以便計算及比較各國被害盛行率。第五，調查數據必須是 2010 年以後，由於過去 20 年網路使用者大幅增加，將會影響網路被害的盛行率。例如，10 年前網上購物不像現在那麼普遍，會導致網上購物詐欺被害者較少。第六，明確衡量某一特定網路犯罪類型的被害，而不是模糊的「網路被害」的測量概念。

由於挪威、比利時、奧地利、拉脫維亞、葡萄牙、芬蘭和波蘭的研究所沒有可供足夠分析的訊息，Reep-van den Bergh 和 Junger（2018）只將符合條件的國家納入分析，各國主要調查設計的特徵如表 2-1-5 所示，所有被害調查皆為大樣本且隨機抽取家戶或個人。大多數調查皆由訪員主導，4 次透過電話，3 次採網路問卷，1 次是面對面進行。其中荷蘭三管齊下，採用電話調查及面訪，或是網路調查及電話訪問的混合設計模式。而瑞典 NTU 問卷調查的回復率非常高，德國 WISIND 和 DV 的問卷調查的回應率相對較低，顯見各國的調查仍存有樣本的選擇偏差。另在研究對象的研究組別方面，多數的調查只包括 15 歲以上的被害人。最後，除了德國 WISIND 調查範圍為 30 個月，其餘所有調查的參考期為 12 個月。

表 2-1-5　歐洲網路詐欺犯罪被害調查分析表

國家	民意調查	數據收集	第 1 年數據收集	數據收集	百分比回應率[b]	網路犯罪受訪者人數（以千計）	研究對象的年齡組別
瑞典	NTU	電話	2006	每年	60–76	12-15	16–79
荷蘭	VM	線上和紙本	2012	每年	37–41	80–145	15+
	ODW	線上和紙本	2011	一次性	47	10	15+
	ITN	線上和電話	2015	一次性	41	5	12+
德國	WISIND	電話	2014	一次性	21	12	16+
	DV	電話	2012	2017 年舉辦第 1- 2 次	22	32	16+
法國	CVS	面對面	2010	每年	---	15	14+
盧森堡	ES	電話	2013	2017 年舉辦第 1- 2 次	30	3	16+

a 通常調查前 12 個月的調查。

b 對於電話調查，以合格人數的百分比衡量。

c 大約 12% 的受訪者在網路或紙本回答，如果犯罪發生在網路，這些受訪者不會得到問題。

有了前述六種網路被害型態之類型，Reep-van den Bergh 和 Junger（2018）針對瑞典、荷蘭、德國、法國、盧森堡等歐盟國家所採行的九項調查方式(NTU, CSEW, VM, ODW, ITN, WISIND, DV, CVS, ES)，進行檢視後發現，網路購物詐欺(Online shopping fraud)的

年犯罪率在 1% 到 3% 之間；網路銀行/支付詐欺(Online banking and payment fraud)的犯罪率不到 1% 到 2%；不到 1% 的被害者屬於其他類型詐欺(Other fraud)；有高達 3% 的受訪者宣稱經歷過某種型態的網路霸凌/威脅/性犯罪，例如跟騷 (1%) 或威脅 (1%)；有 1–6% 宣稱是駭客攻擊的被害者。據估計，是惡意軟體的被害者之比例約在 2% 到 15% 之間。

晚近 Lee 和 Wang (2022)利用 2019 年的歐盟輿情調查數據(Eurobarometer)進行網路調查分析，以探究歐洲地區網路詐欺被害之情事與相關因素。Lee 和 Wang 所使用的歐盟輿情調查數據，這是一項由歐盟委員會(European Commission)所進行的兩年一次之調查。該調查數據包括其每個成員國對於歐盟相關的各種社會與政治問題的回應。自 1973 年以來，這些調查一直代表歐盟委員會和其他歐盟機構所進行著。2019 年的此一調查是基於多階段隨機（概率）樣本之設計。在每個國家，採樣點(sampling point)的選擇與全國人口和人口密度成比例。在對個體和區域進行分層後，各國受委託進行調查之單位則系統性地從每個「行政區域單位」選擇了抽樣點（European Union, 2019）。

本研究的數據包括來自 28 個歐洲國家的 21,908 位受訪者之意見，這些國家包括奧地利、比利時、保加利亞、克羅埃西亞、塞浦勒斯、捷克、丹麥、愛沙尼亞、芬蘭、法國、德國、希臘、匈牙利、愛爾蘭、義大利、拉脫維亞、立陶宛、盧森堡、馬耳他(Malta)、荷蘭、波蘭、葡萄牙、羅馬尼亞、斯洛文尼亞、斯洛伐克、西班牙、瑞典和英國。每個國家/地區的平均受訪者人數為 755（SD=183，Max=1006，Min=284）。略多於一半（54.38%）的樣本是女性，參與者的年齡介於 15 至 96 歲之間 (M=47.52, SD=17.03)。

結果發現歐洲前 10 大網路被害型態，依序為詐欺郵件/電話(Fraudulent emails or phone calls)(32.92%)、植入惡意軟體(Malicious software)(26.44%)、極端分離主義(Extremism)(13.32%)、網路詐騙(Online fraud)(11.44%)、帳戶被駭客入侵(Account hacked)(10.08%)、網路攻擊(Cyberattacks)(8.68%)、勒索郵件(Blackmail/Ransomware)

(7.10%)、銀行帳戶詐騙(Banking fraud)(7.07%)、色情網站(Pornography) (5.54%)以及身分盜用(Identify theft)(5.52%)。

四、澳大利亞

雖然澳大利亞內部對於網路犯罪(cybercrime)的定義仍有些分歧，但普遍認為網路犯罪應該聚焦於兩個主要類別(Clough, 2015)：第一類是針對電腦或相關資訊通訊技術進行攻擊的犯罪（通常只存在於網路世界的犯罪）。第二類是指電腦或相關資訊通訊技術本身是達到犯罪、是犯罪不可或缺的一部分之型態（這通常包括利用網路促進或達成的傳統犯罪）(Australian Government Attorney-General's Department, 2013；Drew & Farrell, 2018; House of Representatives Standing Committee on Communications, 2010)。特別是與本研究有關者，澳洲政府認為網路詐欺(cyber fraud)亦有兩種類型。

第一類型的網路詐欺犯罪，係指犯罪的發生係直接由電腦或其他資訊通訊技術 (Information and Communication Technology, ICT)所促成，包括非法入侵(Illegal access)、非法攔截(Illegal interception)、數據干擾(Data interference)、系統干擾(System interference)、濫用設備(Misuse of devices)和駭客犯罪(Hacking offenses)(Australian Government Attorney-General's Department, 2013)。這些犯罪行為可以被廣泛地視為是針對電腦硬體或對資訊通訊技術(ICT)的攻擊，亦即電腦硬體與資訊通訊技術本身是被攻擊、被害的對象。

第二類型的網路詐欺犯罪，是指電腦或資訊通訊技術(ICT)是犯罪的組成部分，亦即電腦或資訊通訊技術被行為人使用來達成其犯罪的工具或手段，與第一類型為攻擊的對象不同，而第二類型的網路詐欺犯罪通常涉及的是以獲取經濟利益為目的的欺騙行為(Australian Government Attorney-General's Department, 2013)，其中包括預付費用詐欺(Advance fee fraud)（例如戀愛詐騙(Romance scams)、繼承詐騙(Inheritance scams)、投資詐騙(Investment scams)和詐欺性金融交易(Fraudulent financial transactions)）和身分盜用(Identity theft)(Australian Government Attorney-General's Department, 2013)。

談到盛行率，國際上，網路詐欺已被視為是一種廣泛而複雜的犯罪類型(Drew & Farrell, 2018)。而網路詐欺呈現全球性增長的趨勢顯示，隨著新的、複雜的詐欺手法與技術的不斷湧現，這將是一種快速演變的新一代犯罪行為(Drew & Farrell, 2018)。網路詐欺或金融網路犯罪(Financial cybercrime)最初是以簡單的詐騙和基本的網路釣魚手法出現，通常是透過電子郵件的方式來進行的，但隨著後來網路的發展現已成為一種複雜的犯罪類型)。現在的網路詐欺犯可能會使用高度發展的軟體工具，以及越來越精心設計的社交工程和心理技術，並且經常聚集在有組織或鬆散但有關聯的網路犯罪集團中，持續擴大其影響之範圍和提高犯罪既遂的效率(Broadhurst, 2006; Ionescu et al., 2011)。

根據目前諸多的研究已承認，由於嚴重漏報(Significant underreporting)，各國官方公佈的網路犯罪統計數據可能被嚴重低估，但可用的統計數據（包括被害調查）顯示，全球網路犯罪顯著地持續增長(Cross, Smith, & Richards, 2014; House of Representatives Standing Committee on Communications, 2010; Webster & Drew, 2017)。在澳大利亞，網路犯罪被害金額保守估計每年高達 20 億澳元(Australian Government Attorney-General's Department, 2013)。僅就網路詐欺(online fruads and scams) 和網路金融詐欺(Online financial scams)而言，澳大利亞消費者和競爭委員會 (Australian Consumer and Competition Commission, ACCC)(2016)估計每年的損失就超過 3 億澳元，但這仍是一個保守的估計，因為這僅是查獲案件的被害者所提供的數據，黑數難以估計。

晚近，隨著澳大利亞網路犯罪的威脅持續升級，提高認識和採取預防措施至關重要，澳大利亞政府於 2014 年成立網路安全中心(Australia Cyber Security Centre[ACSC])，透過專線電話(1300 CYBER1)的方式，調查被害者網路被害的資訊。根據該中心最新的《2021-2022 年度網路威脅報告》，這一會計年度計有 76,000 份的網路犯罪報告，較前一年會計年度成長了 13%。其中，23%都是網路詐欺犯罪。而這些網路詐欺犯罪型態包含使用網路釣魚電子郵件(phishing emails)、勒索軟件攻擊(ransomware attacks)、網路欺詐和詐

騙(online frauds and scams)、數據洩露(data breaches)和身份盜竊(identity theft)等。其中最嚴重者即有 30%的澳大利亞人成為網路欺詐和詐騙的受害者。而截至 2022 年 5 月，整體網路詐欺所造成的經濟損失達到創紀錄的 3 億美元(引自 Australia Cybercrime Statistics, 2023)。面對詐騙犯罪與損失日益嚴重，澳大利亞政府於 2023 年 7 月宣布再成立一個新的國家反詐騙中心(National Anti-Scam Centre [NASC])，以全面整合政府、執法部門和民營部門共同打擊詐騙犯罪，這是澳大利亞政府繼 2022 年 3 月於聯邦警察署(AFP)之下成立聯合打擊犯罪協調中心，更是繼 2021 年由澳洲數位網路安全部(ACSC)及通訊局(ASD)推動網路受理詐欺報案後，針對詐欺犯罪再次提出的新策略。[6]

五、綜合評述

綜合前述美國、英國、歐盟以及澳大利亞等有關網路詐欺犯罪被害調查概況，有以下幾點比較之結果，分析如下：

（一）網路詐欺犯罪之日趨嚴重性

根據前述各國網路詐欺犯罪被害調查之分析，可以發現網路犯罪之數量呈現逐年成長之趨勢，再加上 Covid-19 期間減少民眾外出的機會後，網路詐欺犯罪急速增加，例如根據美國 IC3(2023)的報告，網路投資詐騙金額從 2021 年的 14.5 億美金，成長至 2022 年的 33.1 億美金，成長一倍之多。而根據英國國家總計局(U. K. Office for National Statistics [ONS], 2022)公布之資料顯示，與網路有關的詐欺犯罪(Cyber-related fraud)，自 2020 年 3 月至 2022 年 3 月已成長 61%。另外，根據澳洲網路安全中心(Australia Cyber Security Centre [ACSC], 2023)報告，2021 年至 2022 年的會計年度總共受理 76 千件網路犯罪報案，較前一個會計年度成長 13%，其中與網路詐欺有關的案量，達到 23%，每年一年網路詐欺財損估計達 3 億美金。網路詐欺犯罪之防範儼然已成為各國犯罪預防之重要或首要工作。

[6] 林書立，金融業要提升打詐執行力 - 名家評論 - 工商時報 (ctee.com.tw) ，造訪日期，2023 年 8 月 11 日。

（二）網路詐欺仍以網路投資財損最為嚴重

雖然網路詐欺犯罪日益嚴重，且呈現各國詐欺方式、詐騙金額與詐騙人數多寡不一的情況，呈現出的先後順序的重要型態亦不太相同，但主要仍以網路投資詐騙(cyber investment scams)型態最為嚴重，因為涉及的金額與被害的人數都是年長者居多的現象。例如以美國為例，2022 年投資詐騙金額高達 33.1 億美金，較 2021 年的 14.5 億美金成長一倍之多(IC3, 2023)。而根據英國的報告，網路詐欺犯罪型態中有 73%的案件涉及被害人運用銀行/信用帳戶轉匯帳款(U. K. Office for National Statistics [ONS], 2022)。反觀我國，根據刑事局(2023)公布統計數據，我國 2022 年網路投資詐騙財損約 1 億美金。[7]與伴隨著加密貨幣的日趨普及，網路投資詐欺將益形嚴重。其次是相較於西方國家網路釣魚郵件(phishing emails)的被害人數日益增加，例如美國、英國與澳大利亞，反觀我國是網路購物詐欺(online shopping /online financial transactions)型態較為嚴重，其詐騙金額雖不至似網路投資詐欺為高，但呈現出詐騙人數最多、且都是年輕世代族群。

（三）調查方式與報案管道愈趨向網路化

各國對於網路詐欺犯罪之調查方式，都是先由傳統犯罪被害調查的管道從一般市民的電訪(Telephone-operated crime survey)和面訪(Face-to-face interview)中先增加網路犯罪被害經驗的調查開始，然後逐漸擴充網路犯罪被害之型態，然後再發展成專屬網路犯罪被害之調查，包含電訪、面訪或網路報案(Online report)，每一年受理的案件量日趨龐大。然而，伴隨著網路的普及，民眾愈依賴網路進行瀏覽，交談，購物與交易的同時，造成網路犯罪的日益猖獗。當民眾發現有疑似被詐、被騙之情況時，雖然一可以利用撥打電話的方式進行報案，但以其他國家為例，被害民眾大多利用網路的報案系統，因此，建構便民的網路被害報案系統實有必要。

[7] 中時新聞網: 假投資去年總財損 34 億 居詐騙案之冠。造訪日期 2023.8.8；https://tw.news.yahoo.com/%E5%81%87%E6%8A%95%E8%B3%87%E5%8E%BB%E5%B9%B4%E7%B8%BD%E8%B2%A1%E6%90%8D34%E5%84%84-%E5%B1%85%E8%A9%90%E9%A8%99%E6%A1%88%E4%B9%8B%E5%86%A0-201000178.html

（四）成立網路詐欺犯罪調查專責機構

美國自 2000 年成立網路犯罪報案中心(Internet Crime Complaint Center, IC3)、英國自 2012 年也針對商業被害調查進行商業界的網路犯罪被害調查，並於 2016 年成立國家網路安全中心(National Cyber Security Centre, NCSC)；無獨有偶的，澳大利亞也於 2014 年成立網路安全中心(Australia Cyber Security centre, ACSC)，作為澳大利亞有關網路犯罪問題研究、調查、擬定與防制網路犯罪問題與威脅之專責機關，又於 2023 年 7 月宣布再成立一個新的國家反詐騙中心(National Anti-Scam Centre [NASC])。換言之，面對網路犯罪問題日趨嚴重，各國大致上已成立專責、跨領域的機關來統籌與因應相關的防制作為。

（五）打擊網路詐欺犯罪之跨境/跨域合作

面對來勢洶洶的網路犯罪，特別是網路詐欺犯罪，專業背景、專責分工、層層斷點，犯罪地點與詐騙地點具有時空分離的特性(許華孚、黃光甫，2020)，警察或執法部門的跨境與跨域合作，勢在必行，例如美國司法部與聯邦調查局(FBI)會與其他國家例如印度的中央調查局與地方執法部門合作，共同打擊金融犯罪與跨國假客服詐騙案件(FBI, 2023)。另外，英國的國家網路安全中心(NCSC)在其官網宣稱該中心與美國、加拿大、澳大利亞、紐西蘭等國家級的網路安全相關部門結盟，共同打擊相關的網路犯罪、攻擊與威脅事件。

（六）我國與各國網路詐欺犯罪定義、類型與調查管道之比較

根據本研究調查各國之網路詐欺定義、類型以及調查管道之所得，並與我國現行做法，比較分析如表 2-1-6。

表 2-1-6 我國與各國網路詐欺犯罪定義、類型與調查管道之比較

	網路詐欺定義	網路詐欺類型	網路詐欺調查管道
美國	加害人透過網際網路騙取他人、從中獲取金錢或物品之犯罪，而他人則包含個人、商家、發卡銀行與金融機構	網路釣魚、個人資訊洩漏、未付款/未交貨、勒索軟體、假客服、網路投資、身分盜用、信用卡/支票詐欺、電郵詐欺、欺騙攻擊、信任/愛情詐欺、求職、騷擾/跟騷、房地產投資、假冒政府、預付費用、超額付款、彩卷/抽獎/繼承、資料洩漏、針對兒童犯罪(戀童癖)、暴力威脅、知識產權/版權/盜版、轉移 SIM 卡、惡意軟體與殭屍網路等。	自 2000 年開始，FBI 設立 IC3 中心，建置網路報案平臺，讓被害者上網進行各種形式的網路詐欺案件之報案，包括智慧財產權 (IPR) 案件、電腦入侵（駭客攻擊）、經濟間諜活動（竊盜商業機密）、網路勒索、國際洗錢、身分盜用以及越來越多的其他類型網路犯罪，以獲得調查結果，據以分析。(網路調查)
英國	將網路詐欺犯罪定義為運用網路協助(Cyber-enabled)進行詐欺行為之犯罪，讓行為人從網路使用人、銀行持卡人或網路銀行處取得金錢/物品/個資之行為。	透過網路資訊與通訊技術盜取錢財/個資/物品、向不特性人發送詐欺性資訊進而盜取錢財/個資/物品、將被害人轉至虛假網站後盜取錢財/個資/物品、威脅損壞/破壞/關閉被害人的電腦或	英國於 2020 年 5 月啟用英格蘭與威爾斯電話犯罪調查，以進行對於網路詐欺犯罪調查之主要工具。然疫情期間曾有暫停使用之情形，但仍為該國調查網路詐欺犯罪之主要管道。(電話調查)

		網站，進而取得錢財/個資/物品、其他意圖以竊取個人錢財/個資/物品之惡意程式。	
歐盟	由於歐盟國家數量眾多，網路詐欺犯罪定義未達一致，但仍以網路協助(Cyber-enabled)進行詐欺之行為，定義為網路詐欺犯罪。	在歐盟，網路詐欺犯罪之型態包含網路購物詐欺、網銀詐欺與支付、網路威脅/霸凌、惡意軟體植入或侵入、駭客攻擊或入侵電腦以盜取金錢/個資/物品以及其他網路詐欺(例如預付費用詐欺)。	目前歐盟使用調查網路詐欺犯罪被害之管道，有以下三種：電話(例如瑞典、荷蘭、德國與盧森堡)、面對面訪談(法國)以及線上及紙本(例如荷蘭)，但仍以採用電話調查之國家居多。
澳大利亞	澳大利亞屬於英系國家，對於網路詐欺犯罪之定義傾向同英國，亦即網路協助進行詐欺以取得經濟利益為目的之犯罪型態。	網路釣魚電郵、勒索軟件攻擊、網路詐欺和詐欺、數據洩漏和身分盜用。	澳洲於 2014 年成立網路安全中心(ACSC)，作為網路犯罪問題研究中心，透過電話報案系統(Hotline 1300 CYBER1)，收集網路犯罪被害之型態與財損等相關資訊。
臺灣	透過網際網路或其他傳播媒體工具，為自己或第三人不法之所有，以詐術使人將本人或第三人	根據警政署刑事局統計，包含投資詐欺、解除分期付款詐欺、網路購物詐欺、假愛情交友、猜猜我是誰(假冒親	臺灣目前網路詐欺犯罪調查之管道為 165 反詐騙專線電話，透過該反詐騙電話，可以了解被害者相關特性與網路詐欺被害類

	織物交付給行為人之行為，與其他國家的定義類似。	友)、遊戲點數詐欺、網路假求職以及盜(冒)用身分。	型等資訊。(電話調查)

第二節　臺灣地區網路詐欺被害者特性

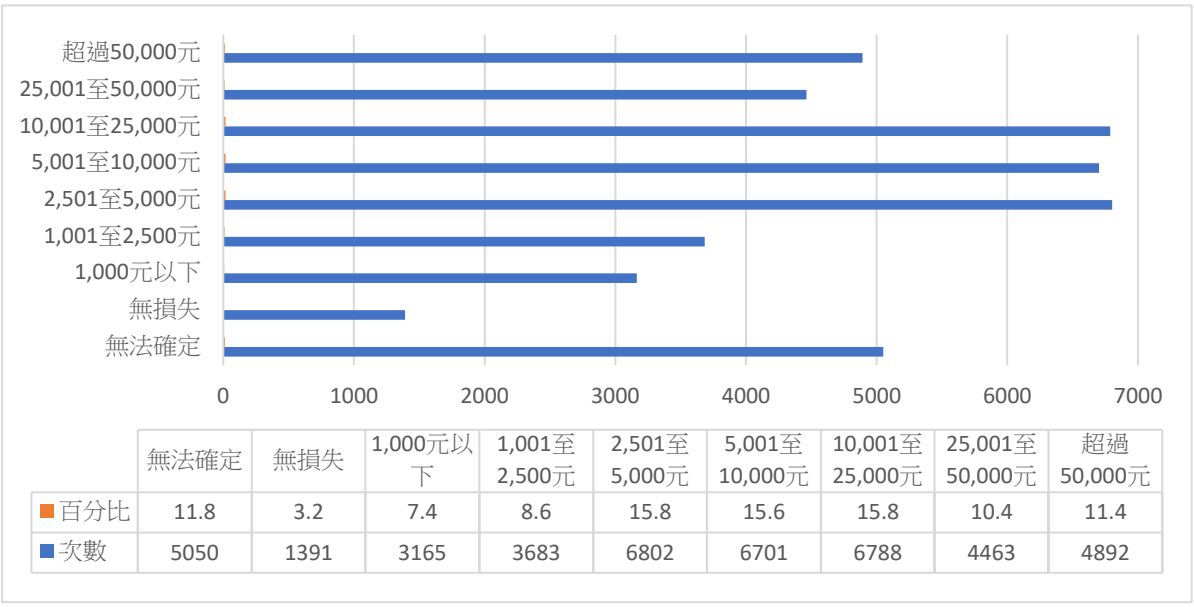
一、網路詐欺被害特性

本研究引用 2020 年科技部委託陳玉書進行「網路生活型態、情境機會與網路被害之實證研究」資料為基礎，樣本係刑事警察局 2010 至 2019 年現存有關網路詐欺被害之次級資料，計 42,935 名。針對網路詐欺被害之損失狀況、被害人之集中特性、被害情境機會與集中特性簡述如下：

（一）網路詐欺被害損失

圖 2-2-1 為網路詐欺被害損失狀況值分布，在被害人報案或案件登錄時，有 5,050 位被害人（占 11.8%）無法確定被害損失，無損失者有 1,391 人（占 3.2%）；另 36,494 位有被害損失（約占 85.0%）；有損失者中，依被害損失之分布進行分組，多數損失在 1 萬元以下，但有 320 人損失達 1 百萬元以上，其中損失千萬元以上者有 19 人。

圖 2-2-1　網路詐欺犯罪被害損失狀況之分布



	無法確定	無損失	1,000元以下	1,001至2,500元	2,501至5,000元	5,001至10,000元	10,001至25,000元	25,001至50,000元	超過50,000元
百分比	11.8	3.2	7.4	8.6	15.8	15.6	15.8	10.4	11.4
次數	5050	1391	3165	3683	6802	6701	6788	4463	4892

（二）網路犯罪被害人的集中特性

網路詐欺被害人的人口特性為非隨機分布，具有集中特性；本研究根據被害人人口特性次數分布結果，針對性別、年齡、教育程度與職業等 4 個變數進行綜合分析，以觀察各類型網路犯罪被害人在人口特性上之集中趨勢。在進行綜合分析時為避免此 4 變數之分布細格太多，而無法觀察到網路犯罪被害人在人口上的集中特性，因此按樣本人數平均分配，將年齡分為「35 歲以下」和「36 歲以上」2 組，教育程度分為「高中職以下」和「專科以上」2 組，職業類別分為「無業/學生/商業服務」和「其他」（含農/漁/牧/公/專業主管等）2 組；結合性別、年齡、教育程度和職業類別等 4 個變數（2*2*2*2）共 16 個組合。

由表 2-2-2 中可觀察到網路詐欺被害人人口特性之集中性，如就排序前五項（5/16＝31.25%）人口特性組合占網路詐欺被害的比率觀之，則網路詐欺被害占 58.5%，其被害人口特性集中性十分明顯。以人口特性組合集中率最高者為例，詐欺犯罪被害比率最高的人口組合為「男性、35 歲以下、高中職以下、無業/學生/商業服務者」被害比率最高（占 16.4%）。顯示網路詐欺被害人的人口組成並非隨機分布；此項研究結果呼應 LRAT 理論有關人口結構影響犯罪被害的主張，至於人口特性與網路情境機會之關聯性則有待進一步分析。

表 2-2-1　網路詐欺被害人人口特性之集中性

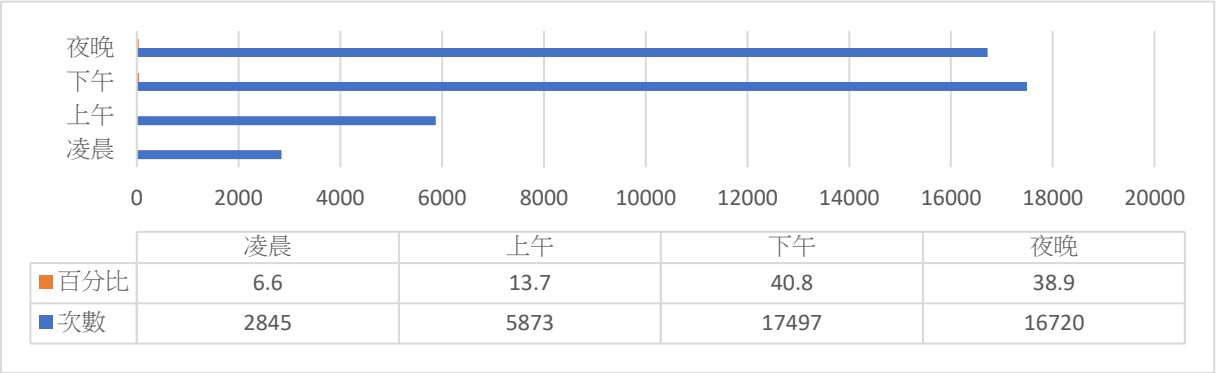
性別	年齡	教育程度	職業	詐欺犯罪[1]	
				%	排序
男	35歲以下	高中職以下	無業/學生/商業服務	**16.4**	**1**
			其他	**9.4**	**4**
		專科以上	無業/學生/商業服務	**9.5**	**3**
			其他	5.2	
	36歲以上	高中職以下	無業/學生/商業服務	4.6	
			其他	4.7	
		專科以上	無業/學生/商業服務	1.9	
			其他	2.9	
女	35歲以下	高中職以下	無業/學生/商業服務	**15.2**	**2**
			其他	4.2	
		專科以上	無業/學生/商業服務	**8.0**	**5**
			其他	3.9	
	36歲以上	高中職以下	無業/學生/商業服務	7.0	
			其他	2.8	
		專科以上	無業/學生/商業服務	2.3	
			其他	1.9	
前五名人口組合				58.5%	

註 1:表中詐欺被害樣本數為: n=37,260。

（三）網路詐欺被害的情境機會與集中特性

網路詐欺被害發生的情境機會主要包含發生的時間、網路途徑和加/被害人關係等 3 個變數；在被害時間方面，本研究將一天分為 4 個時段：凌晨（00:00-05:59）、上午（06:00-11:59）、下午（12:00-17:59）與夜晚（18:00-23:59）；被害案件發生最多的在「下午」（占 40.8%），其次為「夜晚」（占 38.9%），在凌晨時段仍有 2,845 件（占 6.6%）的被害比率，顯示網路詐欺發生的時段與被害人的生活作息可能有關（參見圖 2-2-2）。

圖 2-2-2　網路詐欺被害時段之分布



	凌晨	上午	下午	夜晚
百分比	6.6	13.7	40.8	38.9
次數	2845	5873	17497	16720

被害的途徑與上網的網站、目的及功能有所關聯，本研究將被害途徑分為入口網站（如 Google、雅虎奇摩等）、拍賣網站（如露天拍賣、蝦皮等）、社群網站（如 Facebook、Twitter 等）、論壇聊天室（如 BBS、Dcard、愛情公寓等）與其他（如網路銀行等）。被害人進入網路途徑最多的是「入口網站」計 9,860 人，其次為「論壇聊天室」計 9,054 人，二者合計逾一半。加/被害人關係則與被害人的交友範圍有關，本研究將關係分為：陌生（以被害人報案時認定）、認識（包含親戚、朋友、鄰居等）與不清楚（製作筆錄當下未能確認加/被害人關係，事後破案亦未能補登錄者屬之），其中最多的是「不清楚」（占 67.8%），其次為「陌生」（占 30.1%），「認識」者僅占 2.1%（參見表 2-2-3）。

從加/被害人關係亦能顯示網路情境不受時空限制的特性，也讓素昧平生的兩端千里一線牽；網路的便利與普及，使國人在生活、工作和人際互動更為仰賴網路，犯罪被害機會隨之增加。進一步觀察網路犯罪被害途徑與加/被害人關係之關聯性，二者存在顯著關聯性（$\chi^2 = 3190.615$; $p<.001$）；整體而言，97.9%的加/被害人關係是陌生或不清楚加害人，僅 2.1%的被害人認識加害人；其中以社群網站有較高的認識比率（占 4.8%），其次為論壇聊天室占 3.3%；入口網站認識的比率最低僅 0.4%。網路情境存在人際不確定的高風險狀態，尤以拍賣網站和入口網站為甚。

表 2-2-2　網路犯罪被害途徑與加/被害人關係之關聯性

被害途徑	加/被害人關係						合計
	陌生	%	認識	%	不清楚	%	
入口網站	1,331	13.5	40	0.4	8,489	86.1	9,860
拍賣網站	1,799	29.2	44	0.7	4,317	70.1	6,160
社群網站	2,335	51.0	221	4.8	2,021	44.2	4,577
論壇聊天室	3,477	38.4	302	3.3	5,275	58.3	9,054
其他	1,188	29.5	116	2.9	2,722	67.6	4,026
合計	10,130	30.1	723	2.1	22,824	67.8	33,677

註：$\chi^2 = 3190.615$; df = 8; p <.001

網路犯罪被害情境為非隨機分布，具有集中特性；本研究根據被害情境分析結果（參見圖 2-2-2 和表 2-2-4），針對時段、加/被害人關係和被害途徑等 3 個變數進行綜合分析，以觀察各類型網路犯罪被害在情境機會之集中趨勢。在進行綜合分析時為避免此 3 變數之分布細格太多，而無法觀察到網路犯罪被害情境的集中特性，因此依變數概念近似性將被害時段為「凌晨/上午」和「下午/夜晚」2 組，加/被害人關係分為「認識」和「不認識/不清楚」2 組，被害途徑分為「入口/拍賣網站」、「社群/論壇/聊天室」和「其他」3 組；結合被害時段、加/被害人關係和被害途徑等 3 個變數（2*2*3）共 12 個組合。

表 2-2-3　各類型網路詐欺被害情境機會的集中性

時段	加/被害人關係	被害途徑	詐欺犯罪	
			%	排序
凌晨/上午	認識	入口/拍賣網站	0.1	
		社群/論壇/聊天室	0.5	
		其他	0.1	
	不認識/不清楚	入口/拍賣網站	**10.8**	**3**
		社群/論壇/聊天室	**9.5**	**4**
		其他	3.1	
下午/夜晚	認識	入口/拍賣網站	0.2	
		社群/論壇/聊天室	1.0	
		其他	0.2	
	不認識/不清楚	入口/拍賣網站	**36.5**	**1**
		社群/論壇/聊天室	**29.4**	**2**
		其他	8.5	
前4名人口組合			86.2%	

註：表中詐欺被害樣本數為: n=33,677

由表 2-2-4 中可觀察到各類型網路犯罪被害情境之集中性，如就排序前 4 項（4/12＝33.3%）情境組合占各類網路犯罪被害的比率觀之，則詐欺被害達 86.2%，顯示網路詐欺被害的情境機會有相當高的集中特性，顯示不同類型網路犯罪的情境機會並非隨機分布。以情境機會集中率最高的為例，「下午/夜晚、加被害人不認識/不清楚、入口/拍賣網站者」占 36.5%，有最高的被害率。網路和虛擬空間的無遠弗屆和多元管道，提供加害人接觸被害者的可及性，而網路使用者的隱蔽性，亦使被害人在使用網路時無法知悉潛在加害人的存在，而成為犯罪標的物。

第三節　網路詐欺被害相關理論與實證研究

一、網路詐欺被害相關理論

（一）生活方式與日常活動理論

近年來，網路犯罪被害最常被用來解釋的理論為生活方式與日常活動整合型的理論(Lifestyle-Routine Activities Theory, L-RAT)。該理論結合了日常活動理論(Routine Activities Theory, RAT)和生活方式暴露理論(Lifestyle-Exposure Theory, LET)二個理論皆強調犯罪情境與機會的因素，促進被害事件的發生，亦符合 Becker（1968）理性選擇理論(Rational choice theory)，認為犯罪人犯罪之前，會以經濟的觀點，分析犯罪的利與不利。這種情形，就好像投資人對經濟上的投資。犯罪人一如投資人，不能「完全掌握」各種有利或不利的資訊，但是他們會以自己掌握的部分資訊下決定。因此，犯罪與被害事件的發生會因個人及生活型態與活動而所有不同（Becker, 1968; Cohen & Felson, 1979；周愫嫻、曹立群，2014；許春金，2022；蔡德輝、楊士隆，2019）。

然而，日常活動理論(RAT)所關注的是犯罪事件的特徵，而不是實際犯罪者的特徵。RAT 認為，犯罪事件是由一個有動機的犯罪者、有吸引力的合適標的物和缺乏有能力的監護者，恰巧在時間和空間上的產生交叉而產生犯罪與被害事件 （Cohen & Felson, 1979；許春金，2022；蔡德輝、楊士隆，2019）。然而，也有一些學者關注如何透過日常活動理論來解釋網路的犯罪機會。Yar（2005）認為在網路世界裡，有動機的犯罪分子如果擁有足夠的網路系統與電腦設備，便可在網路上蒐尋任何被害目標，依據線上用戶的形式找到合適的目標，若該網路用戶在沒有預防措施或足夠的電腦安全防護配備下，就直接連接到網際網路，很可能符合 Felson （1998）所稱之「合適的標的物」四大特徵（VIVA），犯罪目標的價值(value)，慣性(inertia)、犯罪目標的物理可見性(visible)和犯罪目標的可及性(accessible)，亦為高風險被害對象(Yar, 2005)。

另外，生活方式暴露理論(LET)認為不同的生活方式使個體面臨不同程度的被害風險。因此，將不同被害風險解釋為生活方式變化的函數，這種變化可能使人們暴露於犯罪情境 (Cohen, Kluegel, & Land, 1981; Hindelang, Gottfredson, & Garofalo, 1978)。比如說，那些高風險的犯罪被害者的生活方式，可能花更多時間在公共場所（尤其是在晚上）、更多時間遠離家人，以及更容易接觸到高風險犯罪群體（例如年輕男性）。然而，生活方式與日常活動理論(L-RAT)綜合上述二個理論，提出犯罪被害的風險是個人接觸有動機的犯罪者、與有動機的犯罪者的生活型態相似、亦為合適的標的物，且缺乏有能力的監控者在場等因素相互聚合(Herrero et al., 2021)。若該理論應用在網路世界，係指線上用戶隨意地到訪未知或不明之網站，或至非法網站下載免費的音樂、影片或免費軟體程序，在沒有預防措施的情況下點擊圖標，很可能成為電腦犯罪分子的被害者。換言之，網路職業和休閒活動的型態，或多或少為電腦犯罪被害提供機會。許多實證研究結果支持生活方式與日常活動理論，無論在實體世界或虛無的網路世界，皆可有助於解釋網路犯罪被害發生的原因與機會（Herrero et al., 2021; Leukfeldt & Yar, 2016; Paternoster & Pogarsky, 2009; Paternoster et al., 2011; Pratt et al., 2010; Reyns, 2015；方呈祥，2020；陳玉書、曾百川，2007；陳玉書等人，2020；曾百川，2006；葉雲宏，2008）。

（二）自我控制理論

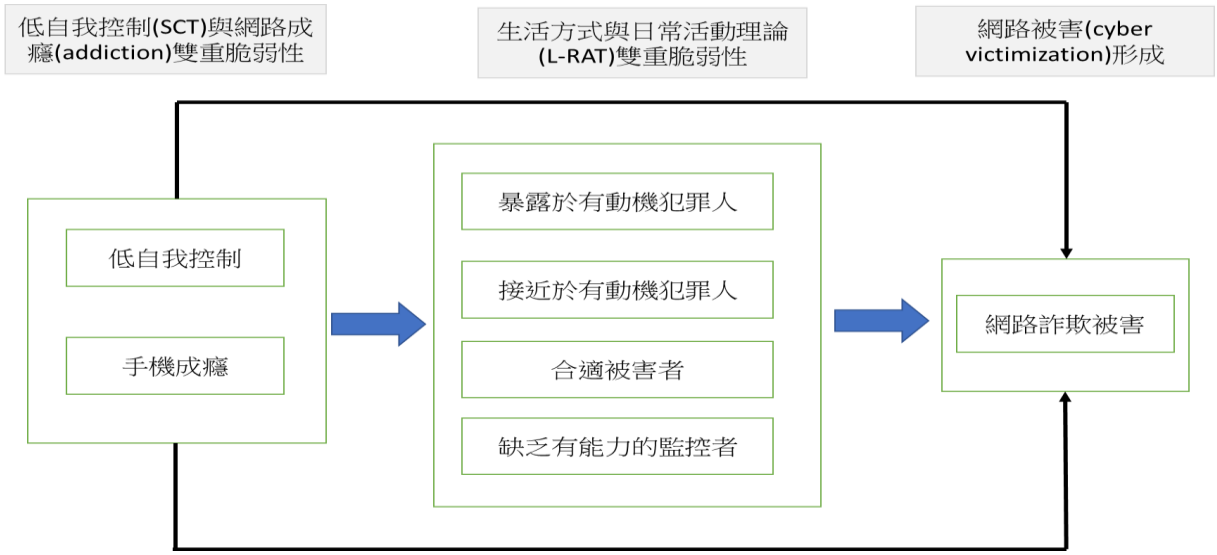
Gottfredson 和 Hirschi(1990)提出自我控制理論(Self-Control Theory, SCL)，認為犯罪是一群低自我控制者，在犯罪機會的促成下，以力量和詐欺來追求個人自我利益的立即滿足行為（許春金，2022；蔡德輝、楊士隆，2019）。一個人的低自我控制於 8-10 歲形成後，終生不會改變，而犯罪事件的發生，主要在探討犯罪機會形成後，犯罪者透過理性思考而決定犯罪行為是否進行，如果犯罪者能在犯罪前體認行為所帶來的懲罰，犯罪便會受到控制。Schreck(1999)更進一步將「低自我控制」視為成為犯罪被害者的高風險因素之一，並將控制理論重新表述為「脆弱性理論」(vulnerability theory)，該研究發現自我控制可以解釋不同形式的被害

經驗，且自我控制變項亦調節性別和家庭收入對被害經驗的影響。綜上，一個具有「低自我控制」特徵者，增加個人和財產被害的機率，並降低性別和收入的影響力。

Pratt 等人（2014）認為即使網路犯罪行為受到控制時，個人的自我控制能力對於被害事件的發生仍具有直接的影響力，低自我控制能力與個人是否成為被害者二者具有顯著關聯性。因為自我控制力較低的人，較容易選擇不良生活方式，將自己暴露於高風險的情境之下。國內外許多實證研究結果，已逐漸將自我控制理論推展至不同形式的被害類型，其中自我控制應用於詐欺犯罪被害亦獲得相同的結論 (Ho & Luong, 2022; Holtfreter et al., 2008; Ngo & Paternoster, 2011; Pratt et al., 2014; Schreck, 1999; Titus & Gover, 2001；方呈祥，2020；陳玉書等人，2020；葉雲宏，2008）。值得注意的是，生活方式與日常活動理論(L-RAT)已納入 Hirsch 的自我控制理論(SCT)，用以解釋為什麼有些人的日常活動或生活方式，反而會使其面對更高的被害風險 (Gottfredson & Hirschi, 1990; Hirschi & Gottfredson, 1993; Schreck, 1999)。例如 Herrero 等人（2021）整合生活方式與日常活動理論(L-RAT)及自我控制理論(SCT)二種不同的理論背景，提出網路成癮者和網路犯罪被害者的雙重脆弱性模型(Dual Vulnerability Model of Cybercrime Victimization)，網路成癮造成的脆弱性，亦會增加他們潛在的網路犯罪被害。

如圖 2-3-1 該模型假設了 L-RAT 理論的預測，即某些情境因素可能導致網路犯罪被害機會的增加（暴露、接近、適合和缺乏有能力的監護人）。此外，該模型包括可能導致網路使用者參與此類危險情況的心理性格（例如低自我控制）。另該模型還包括網路上網設備（例如智慧型手機）的使用方式，並表明與設備使用放鬆管制相關的漏洞，皆可能會影響網路犯罪被害的過程。如圖 2-3-1 中的模型反映網路詐欺被害者的雙重脆弱性形成過程。

圖 2-3-1　網路犯罪被害的雙重脆弱性模型圖



資料來源: Herrero et al. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health, 18*（7）, 3763.

此外， Akdemir 和 Lawless （2020）針對生活方式與日常活動理論(L-RAT)進行實證研究，以網路犯罪者入侵（例如駭客攻擊和惡意軟件感染）和網路詐欺被害者主動開啟不明連結（例如網路釣魚），探討犯罪被害的影響因素，並測試生活方式與日常活動理論（L-RAT）對於網路犯罪被害之適用性。研究結果證明，除了個人層面的因素，宏觀層面的因素（如利用電腦設備上網習慣和公司的個資洩露），亦會增加成為網路犯罪被害者的可能性。因此，生活方式與日常活動理論(L-RAT)適合解釋網路上的被害事件發生及預防措施。

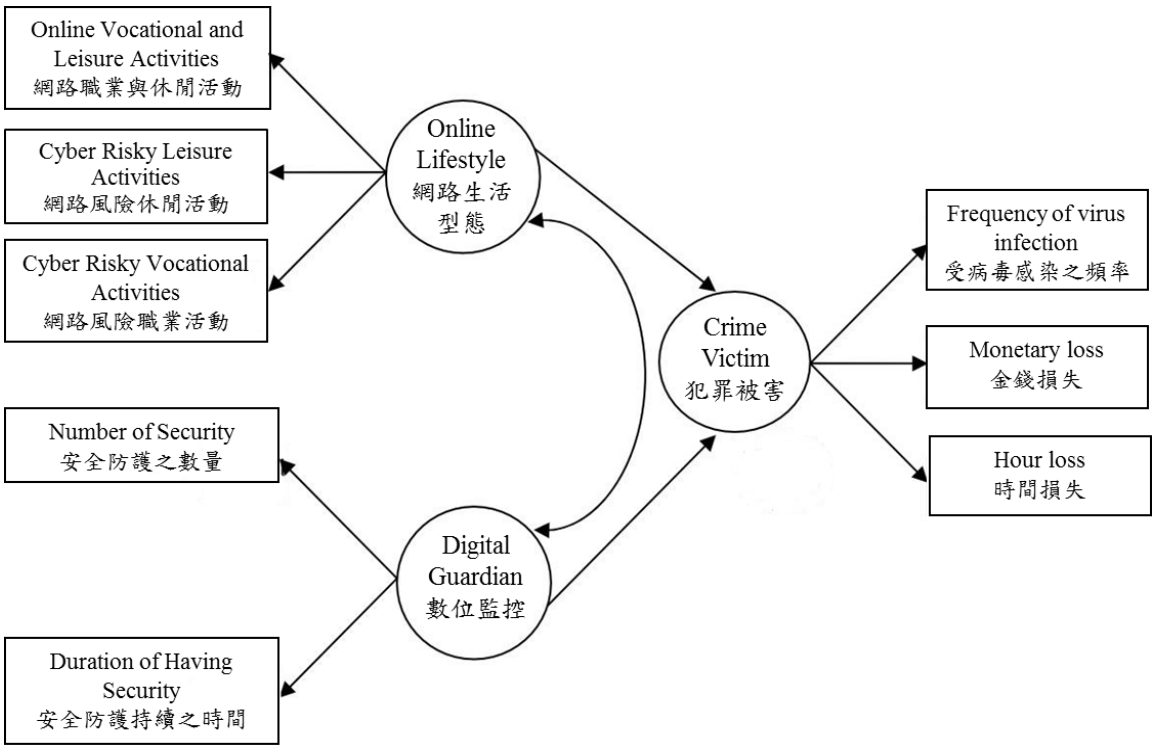
（三）網路日常活動理論

生活方式暴露與日常活動理論(L-RAT)二個被害者理論，長久以來大多應用於實體世界的犯罪被害事件。但是究竟能不能應用於網路環境中，學界有二種不同的看法：部分學者認為網路世界與實體社會不同，不能利用傳統被害者學的理論應用於網路詐欺被害行為(Capeller, 2001; Yar, 2005)；然而，大多數學者及實證研究發現，上述二個被害者理論之研究概念，亦可以解釋虛擬網路詐欺被害行為

之發生（Akdemir & Lawless, 2020; Herrero et al., 2021; Holtfreter et al., 2008; Pratt et al., 2014; Van Wyk & Mason, 2001；方呈祥，2020；王秋惠，2007；陳玉書等人，2020；曾百川，2006；葉雲宏，2008）。

由於 Choi (2008)認為上述二個傳統解釋被害者理論彼此具有相容性，每個人無論身處於真實社會或網路世界，皆會因為「職業活動和休閒活動」角色期待和受到的社會約束不同，進而影響其日常活動與生活方式，而暴露在犯罪或被害的風險亦不同。Choi (2008)將生活方式暴露與日常活動理論(L-RAT)加以整合，用於解釋為什麼特定網路使用者較容易成為電腦犯罪者的合適標的物，並採用「生活方式暴露理論」的核心觀點-生活方式(Lifestyle)，將一些變項重新概念化，並發展出「網路日常活動理論」(Cyber-Routine Activities Theory, Cyber-RAT)，因為 Choi 認為，隨著數位時代的來臨以及數位技術的精進，在日常生活中的吾人使用的越來越多、愈依賴，網路犯罪人找到了新的機會來瞄準潛在無辜的被害者以謀取其私利，因此，提出該理論。如圖 2-3-2 該理論提出相關理論架構如下（方呈祥，2020）。

圖 2-3-2　網路日常活動理論概念架構

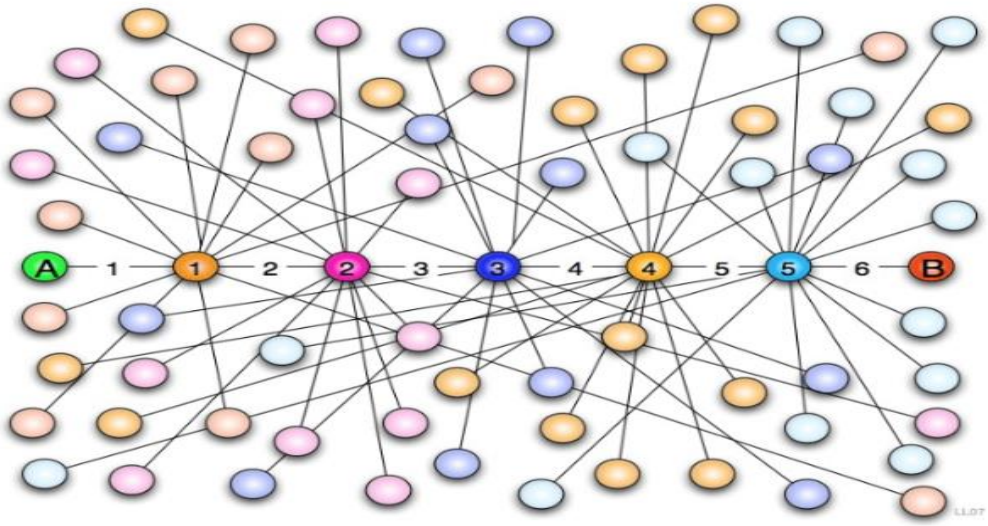


資料來源: Choi (2008), Computer crime victimization and integrated theory: An empirical assessment（引用自方呈祥碩士論文，2020：24）。

（四）六度分隔理論

1929 年學者 Karinity 首先提出此一概念、1960 年哈佛大學社會心理學家 Milgram 實驗後提出社會網絡理論以及 1990 年再由 Guare 提出並迄今廣為人知的六度分隔理論(Six Degrees of Separation)，晚近被運用來解釋網路犯罪與被害行為。該理論之原始概念認為，世界上所有人或所有東西的彼此距離，僅需要 6 步或少於 6 步就可以達到，例如世界上任何互不相識的兩人，只需要很少的中間人，亦即朋友、朋友的朋友、朋友的朋友的朋友...，最多就是六個朋友，就能夠很快地建立起連繫（詳圖 2-3-3）。

圖 2-3-3　六度分隔理論概念圖



1967 年，哈佛大學社會心理學家 Milgram 根據此一概念做過一次連鎖性實驗，他的基本命題為：在美國，人與人的實際間隔到底是多少個人？亦即他設計 1 個實驗包裹，分別寄給 160 位居住於兩個不同城市的居民，一個是堪薩斯州的威奇托市(Wichita City)，另一個市內部拉斯加州的奧瑪哈市(Omaha City)，Milgram 的考量點在於這個兩城市離哈佛大學所在地波士頓市(Boston City)相隔 2 千公里以上。Milgram 請這些收到包裹的居民協助將此一包裹寄回至波士頓市的兩個朋友，接獲包裹的收件者打開後會提供參加本研究的同意書，其中

載明，如果認識這兩位波士頓的朋友，可以直接將包裹寄回給其中一位；如果不認識，請寄給您認為可能認識的朋友，請他代為寄回給波士頓市的兩位朋友之一。最後，160 個包裹有 42 個成功寄回兩個參加此一實驗的朋友手上，最短的路徑中間只經過 2 個人就找到目標。Milgram 計算的這 42 個寄回包裹的路徑後發現，中位數為 5.5，非常靠近數字 6，但他並沒有命名為六度分隔。

「六度分隔」一詞，一直到 1991 年東尼獎得主 John Guare 寫了一個膾炙人口的同名百老匯劇本；並在 1993 年被拍成由威爾史密斯主演的電影，這個詞才逐漸為大眾周知(詹峻陽，2016)。但由於六度分隔理論提出的年代並沒有大數據分析這門學問，因此無法有效提出明確證據證明此一理論。受惠於網路科技的普及與日新月異，晚近愈來愈多的研究指出六度分隔理論確實可以獲得實證性的支持。例如微軟的研究人員 Jure Leskove 和 Eric Horvitz (2008)過濾 2006 年某個單一月份 MSN 簡訊，利用 2.4 億使用者的 300 億通訊息進行比對，結果發現任何使用者只要透過平均 6.6 人就可以和全資料庫的 1,800 百億組配對產生關聯。48%的使用者在 6 次以內可以產生關連，而高達 78%的使用者再 7 次以內可以產生關連 (維基百科, 2023)[8]。游子興(2019)運用大數據資料統計分析國立臺灣大學校園網路連線資訊，亦即運用 IP 路由節點來驗證六度分隔理論之正確性，結果發現使用 IP 路由節點計算得到所有上網裝置相隔約 11.6 個路由節點，其結果叫六度分隔理論多了 5 步之距離，但也顯示網際網路中使用者彼此的距離並沒有想像中的那麼遠，某一程度也驗證該理論所言萬事萬物都僅有至多六步的距離。臉書(Facebook, FB)的團隊為了宣揚臉書週年紀念的朋友日，研究了目前在其上註冊的 15.9 億人資料，發現這個神奇數字的「網絡直徑」(diameter of a network)是 3.57，翻成白話文意味著每個人與其他人間隔為 3.57 人。如果僅考慮美國使用者的話，這個數字會降到平均 3.46 個人。[9] 晚近，國內已有實務工作者運用

[8] https://zh.wikipedia.org/zh-tw/%E5%85%AD%E5%BA%A6%E5%88%86%E9%9A%94%E7%90%86%E8%AE%BA

[9] 6 度分隔落伍了，臉書上的朋友只有 3.57 度分隔而已。https://www.bnext.com.tw/article/38679/BN-2016-02-06-151649-77

該理論於探究網路詐騙集團與網路網址、被害 IP 之關聯性分析(張家愷，2023)。

二、相關實證研究

（一）網路詐欺被害者人口特性

1. 性別

在性別方面，根據內政部警政署 2021 年內政統計通報[10]顯示，14,942 位網路犯罪被害人中，男性 8,274 人（占 55.37%）多於女性 6,668 人（占 44.63%）。詐欺被害男性以「投資詐欺」占 22.92％最多，女性以「解除分期付款詐欺(ATM)」占 26.84％最多。綜合國內外大部分性別與網路詐欺被害調查之實證研究結果，亦與國內的官方統計資料一致，男性的網路詐欺被害經驗顯著高於女性。性別差異確實會影響網路詐欺被害的機會（Izuakor, 2021; Reyns, 2015; Whitty, 2020; 王秋惠，2007; 曾百川，2006; 黃祥益，2006; 葉雲宏，2008; 蔡田木、周文勇、陳玉書，2009），其中 Reyns（2015）研究發現，女性遭受網路釣魚的可能性與男性相比，遭受被害機率小很多（勝算比 Exp（B）=-0.63）。相反地，運用歐洲網路被害調查之數據所進行之研究，Whitty (2020)發現，女性遭網路購物詐欺被害(consumer scam victims)的機率顯著高於男性。然而，另一派學者認為性別對網路詐欺被害的可能性無顯著影響，二者於統計上分析未達顯著水準（Leukfeldt & Yar, 2016; Louderback & Antonaccio, 2017; Ngo & Paternoster, 2011; Pratt et al., 2010; 廖釗頡，2010）。其中廖釗頡（2010）研究發現，性別並非影響網路釣魚被害的關鍵因素，Leukfeldt 和 Yar （2016）亦發現性別差異與網路詐欺被害未具有顯著關聯性。綜合上述，有關性別與網路詐欺被害研究，由於採用網路問卷調查方式有其侷限性，部分研究採非隨機的立意抽樣方式，且研究對象集中於學生或某一特定族群 （陳玉書、曾百川，2007；曾百川，2006；黃祥益，2006；葉雲宏，2008），且國內外針對各種態樣的網路詐欺被害類型態樣略有差異，未能將

[10] 警政署統計室 https://www.npa.gov.tw/ch/app/data/list?module=wg057&id=2218

網路詐欺被害型態做有效區分（Leukfeldt & Yar, 2016; Louderback & Antonaccio, 2017; Ngo & Paternoster, 2011; Pratt et al., 2010; Reyns, 2015；蔡田木等人，2009），造成每個研究測量概念與變項的不一致，因而導致研究結果相當多元化。然而，究竟國內網路詐欺被害是否會受到性別差異的影響，不同性別與網路詐欺被害是否有顯著的關聯性，對於實務機關上的犯罪預防策略具有重要的意義，相當值得深入分析。

2. 年齡

在年齡方面，2021 年內政統計通報中網路犯罪被害人的年齡，未滿 18 歲之被詐騙手法以「假網路拍賣（購物）」最多，18-29 歲年齡層以「解除分期付款詐欺（ATM）」最多，30-59 歲年齡層以「投資詐欺」最多，60 歲以上則以「猜猜我是誰(假冒親友)」最多。國內外實證研究顯示，大多數研究結果認為，年齡與網路詐欺被害二者具有關聯性，但年齡分布略有差異性（Leukfeldt & Yar, 2016; Louderback & Antonaccio, 2017; Ngo & Paternoster, 2011; Paternoster et al., 2011; Pratt et al., 2010; Reyns, 2015；王秋惠，2007；許春金、謝文彥、黃蘭媖、呂宜芬、游伊君，2021；曾百川，2006；黃祥益，2006；葉雲宏，2008；廖釗頡，2010；蔡田木等人，2009）。王秋惠（2006）研究發現，網路詐欺被害者以 29 歲以下居多；葉雲宏（2008）研究發現，網路詐欺被害經驗者平均年齡為 20.3 歲。對照 2021 年警政署公布的官方統計，詐欺被害人以 30 歲至 39 歲的被害人數最多，共有 10,087 人（占 22.58%），顯示被害人自陳報告調查結果的被害人年齡較小，而官方統計調查結果的被害人年齡較大。但二種不同調查結果，網路犯罪被害者皆以青壯年居多。另對照國外的研究結果，Ngo 和 Paternoster（2011）研究發現，年齡為電腦病毒和網路誹謗被害的重要預測因子，年齡愈大者，電腦病毒被害和網路誹謗被害機率越低；Leukfeldt 和 Yar（2016）研究則發現，年紀愈輕者被駭客入侵、被網路詐欺和網路人際威脅的風險愈高。Titus 和 Gover（2001）研究發現，老年人遭受詐欺的風險並不高，可能是與年輕人和受過良好教育的人相比，年輕族群成長於科技發達的 3C 時代，擁有更廣泛的興趣、網路知

識與技能，有能力參與更多元的網路活動，因而在網路市場中的消費參與度更高，進而增加在網路世界的曝光率，亦提高網路的被害風險。然而，隨著網路的普及以及上網已成為全民運動的情況下，Whitty (2020)的研究顯示，年長者較易成為投資詐騙(investment scam)的被害族群。綜合上述，官方資料及國內外實證研究結果顯示，年齡與網路詐欺被害型態的分布確實有顯著的差異性，但若更進一步細分不同年齡層與網路詐欺被害類型亦有不同，年輕族群與年長者可能遭受不同網路詐欺被害（Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Titus & Gover, 2001；王秋惠，2007；葉雲宏，2008）。年輕人比老年人更具有兩個特徵：冒險行為和高度社會化，而年齡因素與網路詐欺被害的風險增加有關。因此，政府宣導網路詐欺被害的犯罪預防，因各年齡層被害風險不一致，且遭到網路詐欺被害類型亦有所不同，針對老、中、青各世代的人群，應加強之犯罪預防宣導重點不盡相同。

3. 職業

陳玉書、簡鳳容、呂豐足及劉士誠（2020）針對 2010 至 2019 年官方刑案資料庫的網路犯罪被害人資料進行分析，研究結果顯示被害人職業以商業服務者最多（占 31.0%），其次為農漁勞工（占 24.4%），學生家管（占 18.8%）再次之，專業主管者（占 18.0%），最後無業者為 8,471 人（占 7.8%），結果顯示被害人職業類型與其被害發生時間、被害途徑與加/被害人關係之關聯性皆達顯著水準，職業類別對網路犯罪被害具有顯著影響力。王秋惠（2007）研究發現，學生或無固定職業者，網路詐欺被害機率高於有正常工作者。黃祥益（2006）在網路詐欺被害者職業方面，以體力工、非技術工及服務業占最多數。但國外學者 Van Wyk 和 Mason（2001） 研究樣本蒐集及人口特徵採用了 Titus、Heinzelmann 和 Boyle（1995）的研究設計，並進行類似之研究，二個不同世代的研究結果發現幾乎相同的被害率與人口特徵相似模型，僅年齡和教育程度與成為網路詐欺被害有關聯，但其他標準人口特性變量（例如收入、性別、種族、職業等變項）似乎與詐欺被害的結果無顯著關聯性。因此，部分的國外研究認為職業類別不會影響網路詐欺被害與否(Ngo & Paternoster, 2011; Reyns, 2015; Titus et

al., 1995; Van Wyk & Mason, 2001)。但亦有部分學者認為有無正常工作及職業會影響網路詐欺被害風險，無固定工作者網路詐欺被害的風險較高（Leukfeldt & Yar, 2016；王秋惠，2007；廖釗頡，2010）。綜觀國內外有關職業類別與網路詐欺被害之相關研究結果，目前在職業與網路詐欺被害之間的關係尚未有統一定論。探究其原因在於國內多數網路詐欺被害調查以學生或青少年居多，較少跨及不同年齡層和職業特性。因此，蒐集網路詐欺被害人口特性的訊息較侷限於某一特定族群，殊為可惜。擴大研究範圍及調查研究對象，始能釐清真正的因果關係。

4. 收入

Leukfeldt 和 Yar（2016）則發現教育程度較高且有工作收入的女性，較有機會成為散播惡意軟體的被害者；但個人財務及收入狀況，與其成為網路詐欺被害的機會是相同的，收入高低不會影響是否會成為網路詐欺被害的機會。另 Van Wyk 和 Mason（2001）研究亦發現收入高低與網路詐欺被害之間並無關聯性。但 Pratt 等人（2010）研究結果顯示，二者具有顯著關聯性，網路詐欺被害人年收入以 5 萬美金占最大宗。國內廖釗頡（2010）針對網路釣魚被害類型成因進行分析，發現網路釣魚被害人的特徵之一為收入較低，較難抗拒網路上不明網址連結的誘因。蔡田木等人（2009）分析 2007 年 2009 年 6 月刑事警察局 165 反詐騙官方資料庫，研究結果發現，收入與受騙經驗二者達顯著關聯性，遭受詐騙的民眾每月收入以新臺幣 4 萬元以下占最多數。綜上，部分實證研究認為，收入與網路詐欺被害無關（Leukfeldt & Yar, 2016; Titus et al., 1995; Van Wyk & Mason, 2001）；但也有另一派學者認為，收入高低會影響是否成為網路詐欺被害人 （Pratt et al., 2010；廖釗頡，2010；蔡田木等人，2009）。因此，國內外研究對於收入與網路詐欺被害間的關係，目前研究結論並無一致性，收入高低與網路詐欺被害二者究竟是獨立或是相關，彼此間是否會相互影響，亦是本研究需要深入探究的原因與動機。

5. 教育程度

在教育程度方面，黃祥益（2006）的研究發現，教育程度愈高受網路竊盜被害可能性較低，但被網路詐欺的機會則較高；葉雲宏（2008）的研究則發現，教育程度為影響網路詐欺被害因素之一，網路詐欺被害者的教育程度大都為國中/小或高中（職）。Leukfeldt 和 Yar（2016）的研究指出，教育程度高低對於被網路駭客入侵、網路糾纏騷擾和網路威脅沒有顯著影響；但教育程度愈高者較容易成為惡意軟體的被害者，而教育程度較低者為網路詐欺被害的高危險群。相類似的，相較於其他類型的詐欺犯罪(例如投資詐欺與愛情詐欺)，Whitty (2020)研究指出，網路購物詐欺的被害人顯著地具有較低的教育程度。相反地，Titus 和 Gover（2001）研究發現，更高的教育不是防止被害的保護因素，證據指向相反的方向，愈高教育程度者，因為接觸網路的機會及時間愈長，因此，網路被害機會反而愈高。綜上所述，實證研究與官方統計資料均顯示，不同人口特性者遭受網路詐欺被害型態可能有所不同，實有必要進行更進一步的調查和分析，以了解人口特性與不同網路詐欺被害型態的關聯性。

（二）心理特質與網路詐欺被害

1. 偏差動機

Modic 和 Lea（2012）認為網路詐欺被害者不僅是犯罪的被動觀察者，亦可稱為係因被害者自身因素而促使被害，對於擁有特定的人格特徵者可事先預測成為被害者。簡鳳容 （2018）研究發現，無論是青少年或成年人網路偏差行為，與被害均存在顯著關聯性。因此，許多研究結果發現，犯罪者與被害者經常是同一團體，稱之為「對等團體」(Equivalent group)，兩者具有相似的生活型態或人格特性，被害者本身有相當多的犯罪或偏差行為，亦具有偏差的動機（Jennings et al., 2012; Lauritsen et al., 1991; 王茜，2014; 許春金，2017）。綜上，雖然國內外實證研究顯示，加害人與被害人具有重疊性，犯罪者與被害者應具有相似的特性(Characteristics)，因為他們是難以區分的團體，採取較偏差的生活型態，也使一個人成為高風險的被害者。因此，犯罪人與被害人具有相關性（Jennings et al., 2012; Lauritsen et al., 1991; 王茜，2014; 簡鳳容，2018; 許春金,，

2017）。雖然許多研究已經確定犯罪事件的犯罪者和被害者均有相似的生活方式特徵和行為模式，但關於被害者與犯罪者是否一樣具有「偏差動機」的實證研究仍然相對稀少 (Choi & Lee, 2017)。為能彌補國內學術上之缺口，實有必要針對網路詐欺被害人的心理特質進行調查。

2. 網路成癮

網路成癮是一個新興的公共衛生問題，網路帶給人們生活上極大的便利性，但相關社交媒體網站等新技術的興起，讓許多青少年沉迷於網路世界。相對地，也提高了青少年網路詐欺被害風險（如色情暴露、網路霸凌等），以及心理健康風險（如抑鬱、自殺等）。國內外許多實證研究發現，網路成癮被證明與網路詐欺被害有關，尤其是網路霸凌被害者的網路使用時間及網路成癮率明顯高於非網路詐欺被害者（Chang et al., 2015; Lin et al., 2020; Simsek et al., 2019; 周愫嫻，2014; 謝龍卿，2004），顯示網路詐欺被害與網路成癮呈正相關。此外，網路成癮也被認為是一種避免現實世界問題的心理逃避機制，並且已被證明與精神和身體症狀有關 (Mihajlov & Vejmelka, 2017)。由於各國研究對於網路成癮的定義及測量方式皆不同，且各國文化與社會間有很大差異，使得不同研究結果很難取得一致性，且國內網路成癮調查多集中於青少年調查，或者是國中、高中（職）及大學生等不同年級的學生身分，多數研究只針對特定學校或校園內的學生為調查對象（Ferraro et al., 2006; Lin et al., 2020; 周愫嫻，2014; 廖釗頡，2010; 洪瑞聰，2014; 石泱、王乃琳，2021; 謝龍卿，2004; 黃祥益，2006）。然而，不同年齡層網路成癮狀況大不同，本研究針對各年齡層進行全面性的抽樣，除網路調查，亦利用面對面實體訪談方式，以彌補不同年齡層抽樣調查人數之差距，期能分析國內網路使用者的成癮狀況。綜合上述，本研究假設網路詐欺被害與網路成癮有關，而網路成癮又與心理特質有關。因此，每天花長的時間沉迷於網路世界的成癮者，將會提高自己暴露於網詐欺被害的高風險情境之下，除會對個人身心健康造成負面影響，亦成為網路詐欺犯嫌的合適標的物。

3. 衝動性、冒險性、低克制能力

Gottfredson 和 Hirschi（1990）認為，具有低自我控制的人具有「衝動」、「感覺遲鈍」、「體力充沛」、「尋求刺激」、「目光短淺」以及「語言表達不佳」等多項特徵，較可能從事一系列冒險行為。另 Modic 和 Lea（2012）亦認為個人若有低自我控制傾向，較難控制自己的衝動，容易暴露於有動機的犯罪者之前，從而增加被害的風險。Pratt 等人（2014）針對自我控制能力與被害事件進行後設分析，研究發現具有衝動、冒險性及低克制能力者，對非接觸性被害的影響，似乎比接觸性被害的影響更大。因此，衝動性、冒險性及低克制能力變項，可對於實體的被害事件發生提供良好的解釋力。然而，具有衝動性、冒險性、低克制能力心理特質者，是否在網路虛擬世界中也較容易成為被害人？國內外相關研究發現，具衝動性、冒險性、低克制能力等人格特質者，較難抵抗網路上特定的誘惑，較容易於網路購物消費及點選來源不明的網址，因而增加網路詐欺被害風險（Bossler & Holt, 2010; Koukia, 2020; Schreck, 1999; Schreck et al., 2002; 王秋惠，2007; 簡鳳容，2018; 葉雲宏，2008）。例如 Schreck（1999）認為自我控制理論也可用於預測被害，因短視、冒險之缺乏思考之行為將使個體更容易成為被害人。Holtfreter 等人（2008）認為低自控與衝動性是非接觸犯罪（如詐欺和網路犯罪）的風險因素之一，因非接觸犯罪需要被害人一定程度的配合度。因此，低自我控制與衝動性是預測個體容易成為詐欺被害人的重要預測因子。類似地，Pratt（2014）認為自我控制是被害風險之良好預測指標，且在預測非接觸被害（例如網路犯罪被害）時關聯性更穩固。Whitty（2020）運用歐洲網路被害調查之研究數據也證明，網路詐欺(cyberscams)被害者確實具有較顯著的衝動性(implusive)與神經質(neurotic)之心理特質。

但仍有學者認為，具有衝動性、冒險性、低克制能力特質的被害人，似乎無法解釋為何會成為信用卡詐欺犯罪的目標，特別是在控制透過網站購買商品的頻率和一個人在網上花費的時間後，低克制能力與網路詐欺被害之間未達顯著關聯性（Holt & Turner, 2012）。例如 Weijer 和 Leukfeldt（2017）針對 3,648 位荷蘭人進行的網路被害調查研究，結果發現低自我控制能力與網路被害較無關

聯性，但與傳統被害型態較具關連性。因此，為探究網路詐欺被害與衝動性、冒險性、低克制能力等變項是否具有影響力，將網路詐欺被害人的心理特質增加「衝動性」、「冒險性」、「低克制能力」變項，期能釐清真正的因果關係。

（三）網路生活型態與情境機會

1. 網路風險

日常活動理論之作者 Felson 和 Clarke（1998）認為，情境與機會是被害的根本原因，若缺乏機會情境因素，則犯罪被害之可能性將大大地降低。因此，若能有效控制網路風險，即可降低網路詐欺被害發生的機會。國內外的實證研究顯示，個人在網路空間中暴露於風險和接近犯罪者的生活方式，其實與現實世界的研究相類似，網路生活型態對於網路詐欺被害除有顯著直接影響效果，亦會透過網路情境機會或網路偏差行為，對網路詐欺被害造成間接影響（Vakhitova et al., 2019; Vakhitova et al., 2016；方呈祥，2020；王茜，2014；周愫嫻，2014；陳玉書、曾百川，2007；陳玉書等人，2020；簡鳳容，2018）。現代人的生活型態早已離不開手機及網路，無論是人們食衣住行等日常活動，甚至是學校教室的傳統上課模式，皆逐漸被網路生活所取代，久而久之大家也漸漸習慣網路購物、消費及線上上課的模式。因此，網路詐欺被害研究可透過測量在網上進行各種活動所花費的時間，來估計暴露的風險。上網時數愈久（Lee & Wang, 2022; Pratt et al., 2010；Van Wilsem, 2013）、愈常在網路購物（Van Wilsem, 2011；Reyns, 2013）；愈常與人在網路上聯絡（Reyns et al., 2016）或較常使用網路工具與人互動（Leukfeldt & Yar, 2016），皆愈容易遭受網路詐欺被害。然而，網路詐欺被害人的生活型態及情境機會是否與實體社會相同，則為本研究所關注的重點。

2. 數位監控

隨著網際網路的普及，網路使用的活動內容也日趨多樣化，網路詐欺犯罪之層出不窮。網路場域中存有大量詐欺性郵件，當人們收到這類型之郵件並加以點擊連結後，其網路詐欺風險將大幅提升。因此，數位監控在網路犯罪預防中具有重要的作用 （古慧珍，

2005; 林宜隆、楊鴻正，2001）。Choi (2008)研究發現，數位監控程度較強的大學生，能有效降低其電腦遭受病毒被害的風險。廖釗頡（2010）研究發現，個人資訊的防護能力較高或有較高的被害意識時，較不易成為網路釣魚被害者。國內外大部分的實證研究顯示，採取監控能力能有效降低網路詐欺被害的發生（Choi, 2008; Holtfreter et al., 2008; Lee & Wang, 2022; 廖釗頡，2010; 方呈祥，2020; 簡鳳容，2018; 謝龍卿，2004）。但仍有部分的研究發現，網路監控並無法有效減少網路詐欺被害事件的發生，監控遏阻對於是否能預防網路詐欺被害發生，並未有顯著的影響力（Ngo & Paternoster, 2011; 陳玉書、葉碧翠，2022）。目前研究結論並無一致性，故將「數位監控」變項納入本研究概念，以利釐清「數位監控」與「網路詐欺被害」之關聯性。

3. 被害誘因

生活方式暴露理論(Hindelang et al., 1978)認為，在日常活動中愈常與犯罪者接觸者，情境機會的被害誘因愈多，個人發生被害風險性也愈高。簡鳳容（2018）研究發現，接收較多網路詐欺被害誘因或刺激者，個人網路偏差動機越高，其發生網路偏差及被害行為越多。陳玉書和葉碧翠（2022）比較互動或被動犯罪被害二者之共同影響因子，研究發現網路「被害誘因」、「偏差價值觀」及「網路成癮」皆會影響網路詐欺被害事件的發生。綜觀國內外多數的研究發現，當網路使用者愈容易被網路詐欺被害誘因所吸引者，愈可能成為合適標的物，個人遭受網路詐欺被害的可能性也越高（Bossler & Holt, 2009; Holt & Bossler, 2015; 廖釗頡，2010; 簡鳳容，2018; 葉雲宏，2008; 陳玉書、葉碧翠，2022; 黃祥益，2006）。

第三章　網路詐欺被害經驗問卷調查結果之分析

第一節　網路詐欺被害問卷設計之焦點團體座談

一、焦點座談之規劃與實施

為使本研究預擬之網路詐欺被害調查問卷能有效蒐集研究所需資料，以達成網路詐欺被害調查之目的；本研究於 2023 年 3 月 10 日規劃第一場焦點團體座談，邀請熟識網路詐欺犯罪或被害之被害者學、資訊管理、網路犯罪偵查等學者與實務工作者共 4 位(參見表 3-1-1)，焦點座談進行前，研究團隊首先向出席者說明焦點座談之目的和內容，並告知相關研究倫理議題，在簽署知情同意書後開始進行討論(知情同意書參見附錄八)。

主要討論的議題包括：(1)對網路詐欺之定義、型態、範疇和變項測量之建議；(2)對「網路生活經驗調查表」中人口特性之測量項目和答項之修改建議；(3)對偏差動機、網路成癮、衝動性、冒險性及低克制能力等心理特質的測量項目和答項之修訂意見；(4)對網路風險、數位監控、被害誘因等網路生活型態與情境機會之修訂建議；(5)對網路詐欺被害與最近一次被害經驗測量項目與選項之修改建議；以及(6)對網路被害調查之設計、執行和研究倫理等議題之建議。

表 3-1-1　參與第 1 場次網路問卷設計焦點團體座談之專家學者

相關領域	代碼	職稱	服務機關
犯罪學與被害者學	F1	國立大學副教授	犯罪學研究所
電腦與網路犯罪	F2	國立大學教授	資訊管理學系
科技/網路犯罪偵查	F3	科長	內政部刑事警察局
網路犯罪偵查	F4	主任檢察官	臺灣臺北地方檢察署

二、焦點座談專家建議

(一)焦點座談專家建議摘要

受邀學者與專家根據本研究前揭所擬焦點座談大綱，以及所提

供之網路詐欺被害調查問卷初稿，充分表達看法和提供修正意見後，主要意見與建議彙整如下表 3-1-2，各位學者專家之詳細發言詳附錄三。

表 3-1-2　焦點團體座談受邀學者專家之意見彙整表

編碼	意見與建議
F4	1. 有關加害人與被害人之互動部分，增加網路使用強度以及被害人對於他人之信任程度。 2. 網路犯罪的定義包含網路詐欺(目的)與網路轉帳(手段)，建議應以行為作為定義，行為會涉及不同的法律規範，若僅限縮於刑法詐欺罪部分，探討態樣會比較少。 3. 網路詐欺類型應該增加網路投資詐騙；網路投資詐騙之訊息係透過社群媒體與非官方管道取得的選項。 4. 網路被害的被害管道應在社群軟體平臺，應再增加 IG、小紅書之類的；在被害交易方式增加第三方支付平臺。 5. 被害金額的級距應該拉大。 6. 數位監控選項，再增加雙重認證、傳密碼至手機認證以及收到疑似假訊息是否會確認的選項。 7. 為增加受訪者的多樣性，建議在大賣場(愛買、全聯)以及超商接洽合作，在櫃臺設置 QR Code。
F1	1. 網路詐欺的經驗是否包含既未遂？既遂是否包含財損？ 2. 問卷內容會標示一些概念(例如心理特質)，應該刪除。 3. 問卷是詢問受訪者過去一年被害經驗，有無可能詢問受訪者自使用網路已來的有無被害之經驗(life time 的經驗)？ 4. 被害人與加害人的熟識程度，除認不認識的選項外，增加一個不知道(亦即不知道加害人是誰)。
F3	1. 網路詐欺的定義是否要限縮，應該參考 165 的詐騙型態。 2. 網路詐欺就實務的角度，應該是指要有財損才會偵辦。 3. 本研究所列網路被害類型共 9 項，但仔細觀察，解除分期付款詐欺、猜猜我是誰(假冒親友)、假冒公務員以及求職詐欺，有些是網路涉及電信或電信詐欺，不見得是完全屬於網路。

	4. 最近被害人因直播平臺被詐欺的情形也很多，建議被害管道納入直播平臺，例如抖音、浪 LIVE、SWAG。 5. 被害管道除第三方支付平臺，建議增加行動支付，如 LINE PAY 6. 詐騙被害金額級距應該再拉大。 7. 數位監控，不以電腦為限，手機與平板均應該考量。
F2	1. 數位監控與被害認知的題目，建議再增加一些內容。 2. 數位監控建議改為網路監控比較 Friendly。 3. 更改密碼作為應屬網路被害經驗之改變，為被害後之採取措施。

(二)網路問卷設計與調查執行之修正

本研究根據四位學者專家所提供之意見後，並參酌司法官學院需求書對本研究之規範要求與研究目的，以及期中報告審查委員之意見；經過內部討論後，將原問卷初稿，修正為正式施測問卷(附錄五)，修正之具體內容扼要說明如下：

1. 網路風險增加網路投資詐騙之訊息。
2. 網路被害動機與誘因增加網路投資。
3. 網路成癮問項修正早上醒來或睡前第一件想到的事就是上網。
4. 網路使用經驗增加詢問網路帳號與會員帳號。
5. 網路被害類型增加遭不明人士盜(冒)用好友身分詐騙。
6. 增加被害經驗後採取的網路監控措施量表，以複選方式供選。
7. 數位監控預防經驗，增加雙重認證，傳密碼至手機認證以及看到網路假訊息會進行認證。
8. 被害經驗的管道，增加社群軟體(小紅書、IG)以及直播平臺(抖音、Bilibili 等)。
9. 網路詐欺被害金額級距拉大。
10. 網路被害經驗發生多久恢復正常生活增加永遠難以恢復之選項。
11. 網路詐欺被害後所採取的應對措施，增加向警察報警與在網路上公告經驗
12. 為提高民眾參與度，超商現金抵用券由原規劃 50 元提高至 100 元。

第二節　研究樣本特性與網路使用經驗

本研究透過 Surveycake 編製網路問卷，並於 2023 年 5 月函請內政部警政署刑事警察局 165 全民防騙網站協助宣傳召募問卷調查事宜（詳附錄九）；又於 2023 年 6 月再次函請內政部警政署刑事警察局函轉各地方警分局派出所協助召募網路詐欺被害者上網填寫網路問卷（詳附錄十）。本研究遂於 2023 年 5 月 15 日至 7 月 14 日進行網路詐欺被害經驗調查，其中網路詐欺被害經驗係指受訪樣本自 2022 年 1 月 1 日至 2023 年 7 月調查截止日曾經遭受網路詐欺被害經驗。本節首先描述研究樣本人口特性與被害經驗分布，第三節分析人口、區域特性與網路詐欺被害之關聯性，第四節則比較一般樣本與網路詐欺被害樣本在各研究變項之差異，最後運用二元羅吉斯迴歸，分析人口特性、心理特質、網路生活型態與情境機會對有無網路詐欺被害之影響力。

本研究原始研究設計樣本為 1,000 人，實際抽樣調查樣本數為 1,146 人，其中無被害經驗者有 582 人(占 50.8%)，有被害經驗者為 564 人(占 49.2%)，為進一步觀察網路詐欺被害類型與集中特性，則以被害經驗量表進行分析，因部分受訪者未能完整回答被害類型之題項，故排除遺漏值 82 人，被害類型調查之有效樣本為 1,064 名，其餘分析變項皆以實際抽樣調查樣本 1,146 人進行分析。

一、研究樣本特性

由表 3-2-1 可知，本研究有效樣本為 1,146 人，其中女性有 586 人（占 51.1%），男性有 5,60（占 48.9%），在年齡分組方面，18-30 歲有 318 人（占 27.7%），31-40 歲有 391 人（占 34.1%），41-50 歲有 266 人（占 23.1%），51 歲以上有 171 人（占 14.9%），受訪對象以 31-40 歲年齡層人數最多（占 34.1%）超過 3 成以上。

在教育程度方面，國中畢肄業以下有 11 人（占 1.0%），高中畢（肄）業有 156 人（占 13.6%），大學或專科畢（肄）業有 1,705 人（占 55.8%），研究所以上有 195 人（占 17.0%），受訪對象以大學或專科畢（肄）業學歷者占一半以上。另外，在每月收入方面，無收

入者有 82 人（占 7.2%），未滿 2 萬元有 122 人（占 10.6%），2 萬至未滿 4 萬有 312 人(占 27.2%），4 萬至未滿 6 萬元有 325 人（占 28.4%），6 萬至未滿 8 萬元有 189 人（占 16.5%），8 萬元以上有 116 人（占 10.1%），受訪對象每月收入以 4 萬至未滿 6 萬元人數最多。

在職業方面，學生有 131 人（占 11.4%），軍公教有 296 人（占 25.8%），服務業/文藝/傳播/行銷有 154 人（占 13.4%），建築/營造/製造/供應商有 119 人（占 10.4%），交通/運輸/旅遊/物流有 41 人（占 3.6%），醫療/法律/金融/保險/房地產有 116 人（占 10.1%），資訊相關/網路/實體銷售有 106 人（占 9.2%），家管/退休有 84 人（占 7.3%），其他（無業/農林漁牧等）有 99 人（占 8.6%）。以受訪對象來看，軍公教占全部樣本四分之一。

在居住地區方面，北部（北北基桃竹）有 470 人（占 41.0%），中部（中彰苗投雲）有 309 人（占 27.0%），南部（嘉南高屏）有 318 人（占 27.7%），東部（宜花東）及離島有 49 人（占 4.2%），受訪者以北部地區人數最多。在城鄉差異方面，都會地區受訪者有 876 人（占 76.4%），鄉村地區受訪者有 270 人（占 23.6%），以都會地區受訪者占 7 成以上較高。

表 3-2-1　本研究樣本人口特性與區域性分布表

變項	人數	%	變項	人數	%
性別（1,146）			**教育分組（n=1,146）**		
女生	586	51.1	國中畢（肄）業以下	11	1.0
男生	560	48.9	高中畢（肄）業	156	13.6
年齡（n=1,146）			大學或專科畢（肄）業	1,705	55.8
18-30 歲	318	27.7	研究所以上	195	17.0
31-40 歲	391	34.1	**職業（n=1,146）**		
41-50 歲	266	23.2	學生	131	11.4
51 歲以上	171	14.9	軍公教公務員	296	25.8
每月收入（n=1,146）			服務業/文藝/傳播/行銷	154	13.4
無收入	82	7.2	建築/營造/製造/供應商	119	10.4
未滿 2 萬元	122	10.6	交通/運輸/旅遊/物流	41	3.6
2 萬至未滿 4 萬	312	27.2	醫療/法律/金融/保險/房地產	116	10.1

4 萬至未滿 6 萬	325	28.4	資訊相關/網路/實體銷售	106	9.2
6 萬至未滿 8 萬	189	16.5	家管/退休	84	7.3
8 萬以上	116	10.1	其他（無業/農林漁牧等）	99	8.6
居住地區（n=1,146）			**城鄉差異（n=1,146）**		
北部（北北基桃竹）	470	41.0	鄉村	270	23.6
中部（中彰苗投雲）	309	27.0	都會	876	76.4
南部（嘉南高屏）	318	27.7			
東部/離島（宜花東）	49	4.2	**總樣本**	1,146	100

註：原始研究設計樣本為 1,000 名，實際調查抽樣之樣本為 1,146 名，與原始研究設計略有差異。

二、網路使用特性

(一)一般網路使用經驗

表 3-2-2 呈現有效樣本 1,146 人的網路使用習慣。從表中可以觀察到，每天上網時數最多的是 6 小時以上者，有 428 人(占 37.5%)，每週上網次數最多的是 10 次以上者，有 880 人(占 76.8%)，周末上網時段最多的是 18：01 至 22：00 ，有 568 人(占 49.6%)，接觸網路時間最長的是 10 年以上者有 859 人(占 75%)。這些數據顯示本研究受訪者中**有超過 7 成 5 的人使用網路已超過 10 年，**且**每週上網次數超過 10 次**，**有超過 3 成的人每天上網時數超過 6 小時**，**有將近一半的人在週末晚上有固定上網的習慣**。

表 3-2-2　本研究樣本網路使用特性分布表(n=1,146)

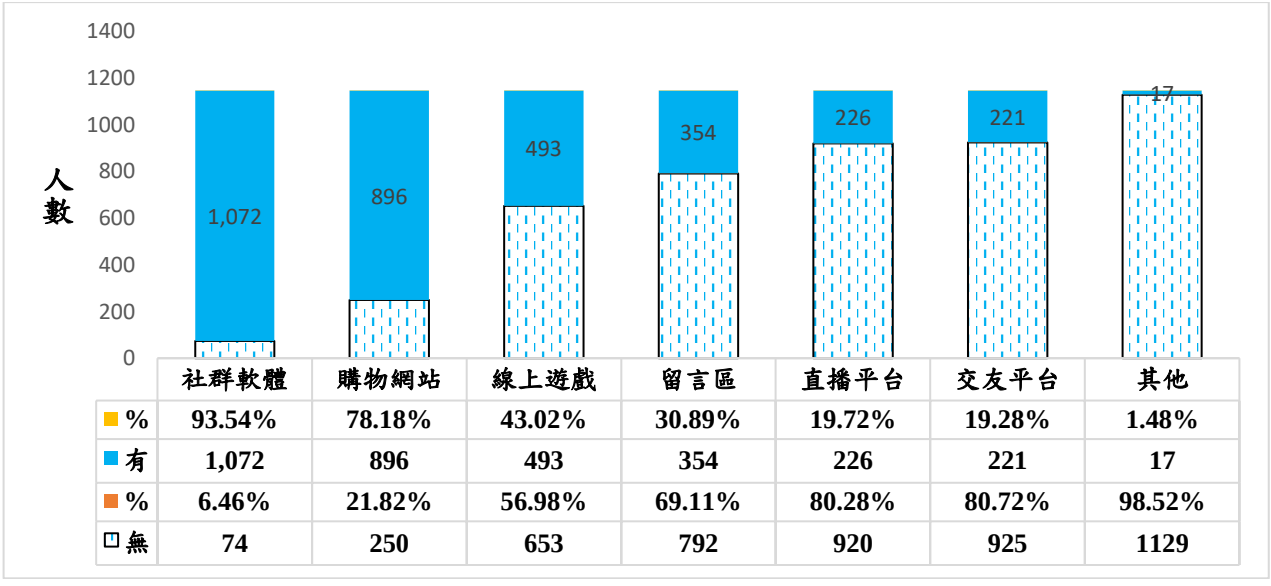
變項	**人數**	**%**	**變項**	**人數**	**%**
每天上網時數			**每週上網次數**		
1 小時以內	24	2.1	少於 1 次	9	0.8
1 至 2 小時以內	116	10.1	1~3 次	30	2.6
2 至 4 小時以內	298	26.0	4~6 次	96	8.4
4 至 6 小時以內	280	24.4	7~9 次	131	11.4
6 小時以上	**428**	**37.3**	**10 次以上**	**880**	**76.8**
周末上網時段			**接觸網路時間**		
08：01 至 12：00	118	10.3	1 年未滿	6	0.5

12：01 至 14：00	73	6.4	1 年-2 年未滿	10	0.9
14：01 至 18：00	182	15.9	2 年-3 年未滿	27	2.4
18：01 至 22：00	**568**	**49.6**	3 年-5 年未滿	41	3.6
22：01 至 02：00	193	16.8	5 年-10 年未滿	203	17.7
02：01 至 08：00	12	1	**10 年以上**	**859**	**75.0**

(二)網路平臺使用情形

圖 3-2-1 展示了本研究對象 1,146 人在不同網路平臺上的使用情況。從圖中可以看出，社群軟體是受訪者最常使用的網路平臺，有 1,072 人(占 93.54%)超過 9 成以上的人表示使用過。其次是購物網站有 896 人(占 78.18%)有近 8 成的人表示使用過。線上遊戲則排在第三位，有 493 人(占 43.02%)將近一半的表示使用過。其他較少使用的網路平臺包括留言區有 354 人(占 30.89%)，直播平臺有 226 人(占 19.72%)和交友平臺有 221 人(占 19.28%)。這些數據反映了本研究受訪者中**多數人在日常生活中會使用社群軟體、購物網站和線上遊戲**這三種網路平臺。

圖 3-2-1　網路帳號及網路平臺使用情形分布圖(n=1,146)



	社群軟體	購物網站	線上遊戲	留言區	直播平台	交友平台	其他
%	93.54%	78.18%	43.02%	30.89%	19.72%	19.28%	1.48%
有	1,072	896	493	354	226	221	17
%	6.46%	21.82%	56.98%	69.11%	80.28%	80.72%	98.52%
無	74	250	653	792	920	925	1129

註：其他網路帳號及平臺，包括 Spotify、PTT、EA game、Discord 等

第三節　網路詐欺被害經驗分析

一、最近一次網路詐欺被害經驗分析

(一)網路詐欺被害發生階段

1. 被害事件特性

表 3-3-1 分析最近一次網路詐欺被害事件的特徵。從表中我們可以發現，被害者匯款的時間分佈主要集中在 18：01-22：00 有 207 人(占 36.7%)。這可能是因為**這個時段是下班後的休閒時間，被害者較容易放鬆警惕**，或是**加害者藉此製造緊急情境，促使被害者匆忙決定**。被害者的損失金額則以較低的區間為主，未滿 1 千元的有 173 人(占 30.7%)，1,001 元至未滿 1 萬元的有 178 人(占 31.6%)。這兩個區間加起來就超過 6 成。這可能是因為加害者刻意設定較低的金額，讓**被害者覺得風險較小**，或是被害者對於**較低的金額較不在意**，或是**加害者根據被害者的財力而定價**。

加害人與被害人之間的關係則以不認識為最多，有 448 人(占 79.4%)。這說明了**網路詐欺的匿名性和隨機性**，加害人通常不會選擇自己認識的人作為目標，而是**利用網路平臺或通訊工具來接觸陌生人**。被害者的交易方式則以網路 ATM 轉帳付款為最多，有 127 人(占 22.5%)。這可能是因為網路 **ATM 轉帳付款比較方便快捷**，也比較難追查和退款。

根據這些數據，我們可以歸納出本研究有網路詐欺被害經驗的受訪者中，有以下幾個共同點：他們大多數**不認識加害人**；他們大多數**選擇以網路 ATM 轉帳付款**；他們大多數**在 18-22 時匯款**；他們大多數**被騙走的金額在 1 萬元以下**。

表 3-3-1　網路詐欺被害事件特性分析表(n=564)[11]

變項	人數	百分比	變項	人數	百分比
被害匯款時間(n=564)			**認識加害人程度(n=564)**		
08：01-12：00	60	10.6	熟識	14	2.5
12：01-14：00	64	11.3	普通	41	7.3
14：01-18：00	131	23.2	初識	61	10.8
18：01-22：00	**207**	**36.7**	**不認識**	**448**	**79.4**
22：01-02：00	88	15.6	**被害交易方式(n=564)**		
02：01-08：00	14	2.5	現金	42	7.4
損失金額(n=564)			超商付款	72	12.8
未滿 1 千元	**173**	**30.7**	遊戲點數	67	11.9
1,001 元至未滿 1 萬元	**178**	**31.6**	實體 ATM 轉帳	49	8.7
1 萬至未滿 3 萬元	56	9.9	信用卡	53	9.4
3 萬至未滿 10 萬元	39	6.9	**網路 ATM 轉帳付款**	**127**	**22.5**
10 萬至未滿 50 萬元	37	6.6	行動支付	15	2.7
50 萬至未滿 100 萬元	11	2.0	線上支付軟體	21	3.7
100 萬至未滿 1,000 萬元	19	3.4	金融機構匯款	42	7.4
1,000 萬元以上	3	0.5	網路銀行付款	47	8.3
沒有損失	48	8.5	其他	29	5.1

註：其他被害交易方式，包括電話騷擾、實體及網銀交易、虛擬貨幣、股票買賣等

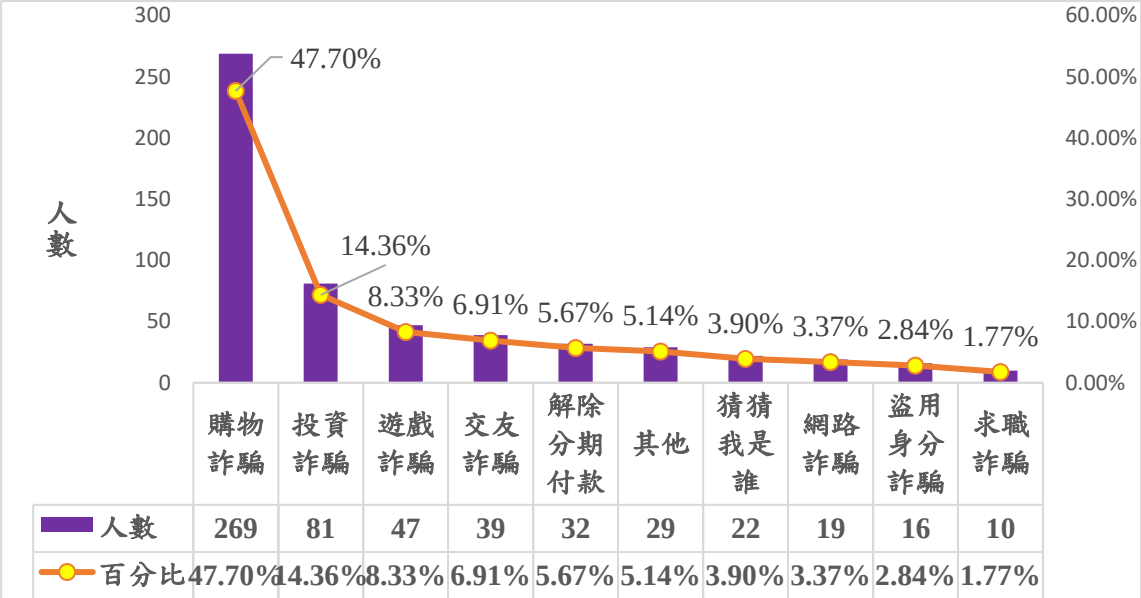
2. 被害類型

在 1,146 名原始樣本中，於**過去一年半**曾於網路上遭受詐騙經驗者有 564 名(占 49.2%)，無被害經驗者有 582 名(占 50.8%)。由圖 3-3-1 得知，**最近一次**被害經驗以上網購物被害 269 名(占 47.7%)最多，其次為網路投資被害有 81 人(占 14.36%)，網路遊戲被害有 47 人(占 8.33%)再次之。由此可知，564 名有網路詐欺被害經驗的受訪者中，

[11] 本研究第二章第二節臺灣地區網路詐欺被害者特性分析，係引用 202 年科技部(國科會前身)委託陳玉書等所進行之研究，其分析之數據為 2010 年至 2019 年刑事局所提供 165 詐騙專線報案之官方被害資料(樣本數 42,935 名)；而本次研究資料來源自編網路被害調查問卷(樣本數 1, 146 名) ，二者資料來源及樣本數差異甚大，再加上疫情前後，網路犯罪型態改變，故被害財損金額及被害類型亦有所不同，特此說明。

以**網路購物被害、投資被害及玩網路遊戲**被害的人數占前 3 名，合計 397 名(占 70.39%)。

圖 3-3-1　最近一次網路詐欺類型分布圖(n=564)



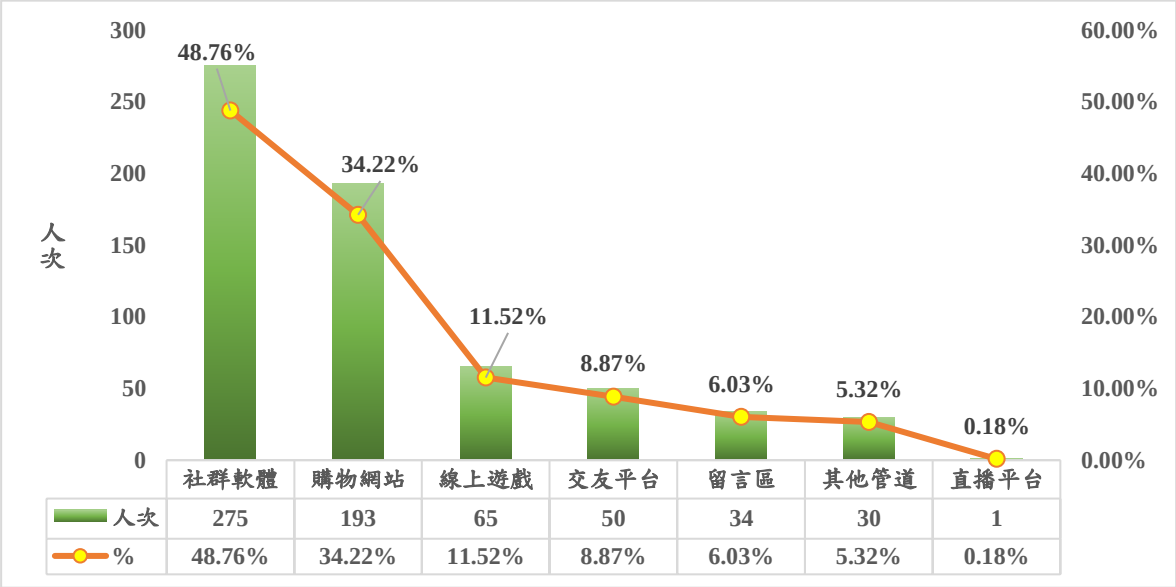
註：本選項為**單選題**，其他類型詐騙，包括購買二手車、網路訂房、購買演唱會門票、簡訊詐騙等

3. 被害管道

圖 3-3-2 展示了 564 名曾經在網路上遇到詐騙的受訪者所使用的被害管道。從圖中我們可以觀察到，受害者在社群軟體上遭遇詐騙的有 275 人(占 48.76%)。這可能是因為**社群軟體是目前最流行和最常用的網路平臺之一**，**詐騙者可以利用社群軟體來接觸和誘惑潛在的受害者**。其次是購物網站，有 193 人(占 34.22%)表示曾在購物網站上被騙。這可能是因為**購物網站上有許多吸引人的商品和優惠，詐騙者可以偽造商品或賣家的身分來欺騙消費者**。

線上遊戲則排在第三位，有 65 人(占 11.52%)表示曾在線上遊戲中被詐騙。這可能是因為線上遊戲中有許多**虛擬貨幣和道具，詐騙者可以利用這些來交換或出售給玩家**，或是以**遊戲內容或活動為名來騙取玩家的個人資訊或金錢**。其他被害管道包括交友平臺有 50 人(占 8.87%)，留言區有 34 人(占 6.03%)，其他管道有 30 人(占 5.32%)。這些數據顯示本研究中遭受詐騙被害的受訪者大多數使用的是**社群軟體**、**購物網站**和**線上遊戲**這三種網路平臺，這**與一般人日常使用網路的情況相符合**。

圖 3-3-2　最近一次網路詐欺接觸管道分布圖(n=564)



	社群軟體	購物網站	線上遊戲	交友平台	留言區	其他管道	直播平台
人次	275	193	65	50	34	30	1
%	48.76%	34.22%	11.52%	8.87%	6.03%	5.32%	0.18%

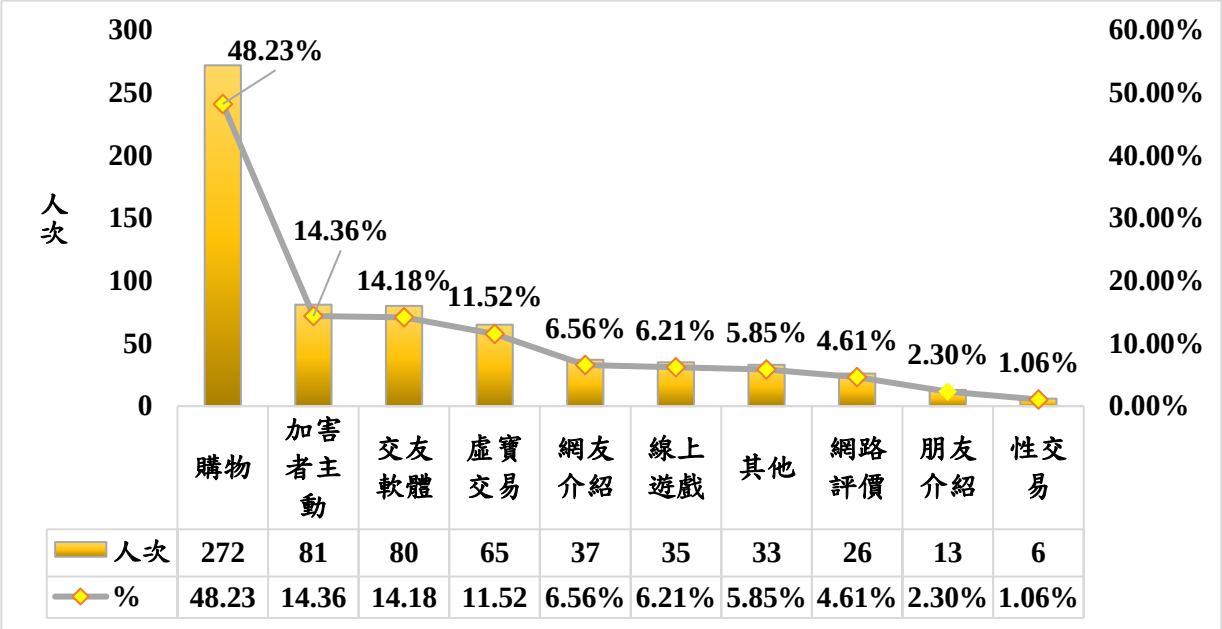
註：本選項為**複選題**，其他接觸管道，包括簡訊、電話、新聞網頁、政府機關網頁等。

4. 互動情形

圖 3-3-3 呈現了 564 名曾經在網路上遇到詐騙的受訪者與加害者之間的互動方式。從圖中我們可以發現，受害者與加害者之間最常見的互動方式是購物，有 272 人(占 48.23%)表示曾在購物過程中被騙，這可能是因為**網路購物是目前最流行和最常用的網路活動之一**，詐騙者可以偽造商品或賣家的身分來欺騙消費者，並利用網路購物管道來接觸和誘惑潛在的受害者。其次是加害者主動聯繫，有 81 人(占 14.36%)表示曾在網路上因為加害者主動聯繫而被騙，這可能是因為**加害者會利用各種手段來吸引受害者的注意力**，例如發送廣告、優惠、邀請等訊息，或是**假扮成某個機構或組織的代表，要求受害者提供個人資訊或金錢**。第三順位是交友軟體，有 65 人(占 11.52%)表示曾在交友軟體上被騙，這可能是因為交友軟體是一種方便且快速的認識新朋友的方式，**詐騙者可以利用交友軟體來假冒自己的身分或背景**，並利用受害者的感情或信任來**騙取他們的金錢或其他利益**。

其他互動情形包括網友介紹有 37 人(占 6.56%)，線上遊戲有 35 人(占 6.21%)，其他互動方式有 33 人(占 5.58%)，網路評價有 26 人(占 4.61%)，朋友介紹有 13 人(占 2.23%)，性交易有 6 人(占 1.06%)。這些數據反映本研究中遭受詐騙被害的受訪者與加害者之間的互動情形，**大多數是透過購物、加害者主動聯繫和交友軟體這三種方式來發生詐騙事件，尤其是網路購物詐欺情形最為普遍**。

圖 3-3-3　最近一次網路詐欺互動情形分布圖(n=564)



	購物	加害者主動	交友軟體	虛寶交易	網友介紹	線上遊戲	其他	網路評價	朋友介紹	性交易
人次	272	81	80	65	37	35	33	26	13	6
%	48.23	14.36	14.18	11.52	6.56%	6.21%	5.85%	4.61%	2.30%	1.06%

註：本選項為**複選題**，其他接觸管道，包括寫信、簡訊、電話、介紹工作等。

(二)網路詐欺被害察覺階段

1. 網路詐欺被害之察覺

表 3-3-2 分析最近一次網路詐欺被害事件的如何得知被害與警覺自己被害時間。這兩個變項可以反映出被害者對於網路詐欺的認知和反應能力，以及網路詐欺的隱蔽性和危害性。從表中我們可以發現，被害者自己察覺遭受網路詐欺被害者有 450 人(占 79.8%)，顯示出**大部分的被害者都能夠在一定程度上察覺到自己受到詐騙，而不是完全不知情或被蒙在鼓裡**。然而，警覺自己被害時間多數在一天之內有 227 人 (占 40.2%)，也意味著**網路詐欺往往是在短時間內就能造成嚴重的損失或影響，而不是長期累積或發酵的過程**。因此，我們可以推斷出**網路詐欺是一種需要高度警惕和快速處理的網路安全問題**。

表 3-3-2　網路詐欺被害察覺階段分析表(n=564)

變項	人數	百分比	變項	人數	百分比
得知被害			警覺遭詐時間		
自己察覺	**450**	**79.8**	**1 天以內**	**227**	**40.2**
警方通知	4	0.7	1-3 天	162	28.7
朋友或同事發現	40	7.1	4-6 天	65	11.5
親人發現	35	6.2	7-14 天	48	8.5
超商店員提醒	7	1.2	14-30 天	23	4.1
金融機構櫃檯提醒	20	3.5	30 天以上	39	6.9
其他	8	1.4			

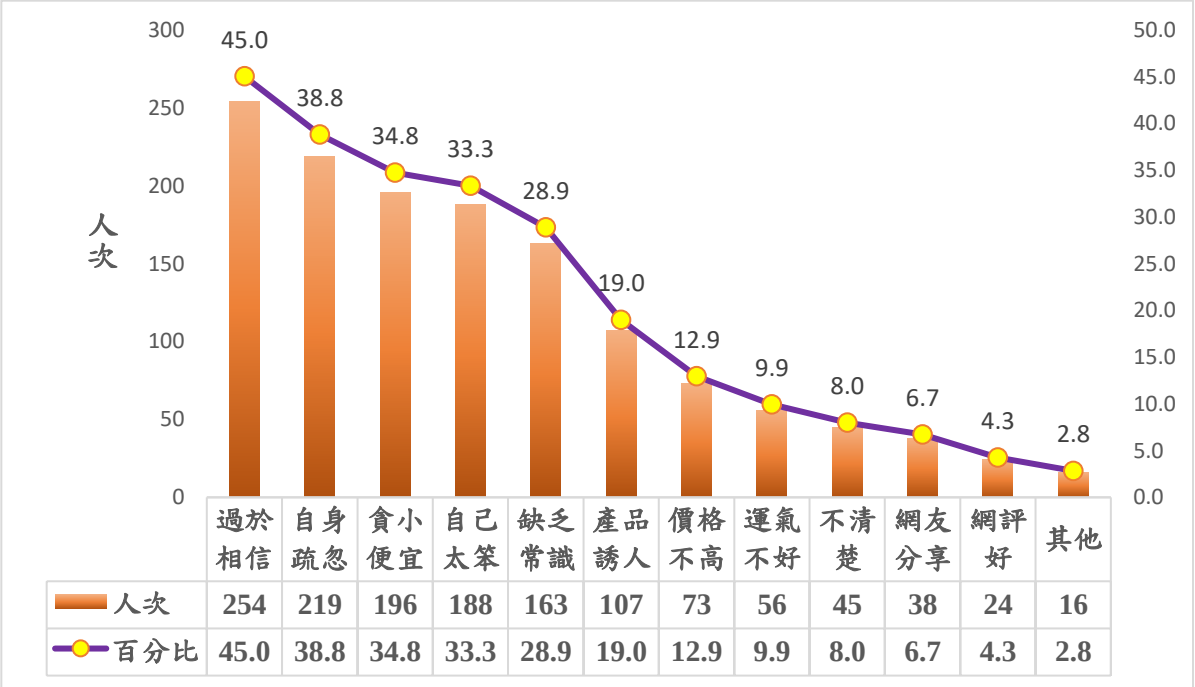
註：本題為**單選題**，其他得知被害方式，包括撇筊、銀行通知、新聞報導、收到包裹等。

2. 網路詐欺被害之原因

圖 3-3-4 分析 564 名網路詐欺被害者自己主觀認定發生被害之原因。這個變項可以反映出被害者對於網路詐欺的自我責任感和心理影響，以及網路詐欺的誘因和手法。從圖中我們可以發現，大多數被害人認為是自己過於相信加害人，有 254 人(占 45.00%)，這顯示出**網路詐欺往往利用被害者的信任感和同情心來達到目的，而被害者也容易因此產生自責和內疚的情緒**。其次是被害人自身疏忽，有 219 人(占 38.80%)，這意味著網路**詐欺通常會在被害者不注意或不小心的時候發生，而被害者也可能因此感到後悔和懊惱**。第三順位是貪小便宜，有 196 人(占 34.80%)，這反映出網路詐欺常常會**以各種優惠或禮品來吸引被害者的注意，而被害者也可能因此陷入貪婪和羞恥的心理**。

其他被害原因包括：覺得自己太笨有 188 人(占 33.30%)，缺乏常識有 163 人(占 28.90%)，產品誘人有 107 人(占 19.00%)，價格不高有 73 人(占 12.90%)，運氣不好有 56 人(占 9.90%)，不清楚有 45 人(占 8.00%)，網友分享有 38 人(占 6.70%)，網評好有 24 人(占 4.30%)，其他被害原因包含遭人恐嚇、色慾薰心、失戀、朋友推薦等原因，有 16 人(占 2.8%)。這些數據反映了本研究中遭受詐騙被害的受訪者被害原因，**大多數為被害者本身觀念、認知及疏忽有關聯**。同時，也顯示出**網路詐欺具有多元化和隨機化的特性，加害人能針對不同類型的被害者進行不同詐騙手法和誘導**。

圖 3-3-4　最近一次網路詐欺被害原因分布圖(n=564)



	過於相信	自身疏忽	貪小便宜	自己太笨	缺乏常識	產品誘人	價格不高	運氣不好	不清楚	網友分享	網評好	其他
人次	254	219	196	188	163	107	73	56	45	38	24	16
百分比	45.0	38.8	34.8	33.3	28.9	19.0	12.9	9.9	8.0	6.7	4.3	2.8

註：本選項為**複選題**，其他被害原因，包括遭人恐嚇、色慾薰心、失戀、朋友推薦等原因。

(三)網路詐欺被害反應階段

1. 網路詐欺被害之反應

表 3-3-3 分析最近一次網路詐欺事件發生後被害者之反應，包括是否報案，內心焦慮情形及事後恢復正常的時間。這三個變項可以反映出被害者對於網路詐欺發生後之反應情形，以及網路詐欺對被害者的心理影響和復原能力。從表中我們可以發現，被害者選擇向警方報案有 174 人(占 30.85%)，顯示出將**近 7 成的被害者選擇不去報案**。這可能是因為被害者覺得報案沒有用、不想麻煩、或是不願意公開自己的身分和遭遇。然而，發生詐欺被害件內心焦慮程度感到很嚴重者及非常嚴重者合計有 181 人 (占 32.10%)，認為不太嚴重者有 267 人(占 47.3%)，這意味著**大部分網路詐欺被害人認為被害事件不會造成內心太大影響，但仍有將近 1 成受訪者認為焦慮感非常嚴重**。這顯示出**網路詐欺不僅會造成財產上的損失，還會對被害者的心理健康造成威脅和困擾**。

被害事件發生後恢復正常時間，有 156 人(占 27.7%)立即恢復，一週內恢復有 187 人(占 33.2%)，半個月月內恢復有 69 人(占 12.2%)，這也反映出計有 412 人(占 73.10%)近 7 成以上受訪者，不到半個月內

就可以恢復正常生活作息，表示**大多數被害者具有良好的復原力和調適能力，能夠快速地走出陰影和挫折**。然而，仍有**少部分被害者有 39 人(占 6.9%)，因內心創傷嚴重，永遠難以恢復**。因此，針對具有創傷症候群的網路詐欺被害人，周遭家人、親友及相關部門需要主動多關心及關懷，避免悲劇發生。

表 3-3-3　網路詐欺被害反應階段分析表(n=564)

變項	人數	百分比	變項	人數	百分比
是否報案			**恢復正常時間**		
有	174	30.85	立即就恢復	156	27.7
無	390	69.15	**一週內**	**187**	**33.2**
焦慮程度			半個月內	69	12.2
非常嚴重	66	11.7	一個月內	46	8.2
嚴重	115	20.4	一至二個月	27	4.8
不太嚴重	**267**	**47.3**	三個月以上	40	7.1
一點也不嚴重	79	14.00	永遠難以恢復	39	6.9
沒意見/很難說	34	6	**總數**	**564**	**100**
不知道	3	0.5			

2. 未報案原因

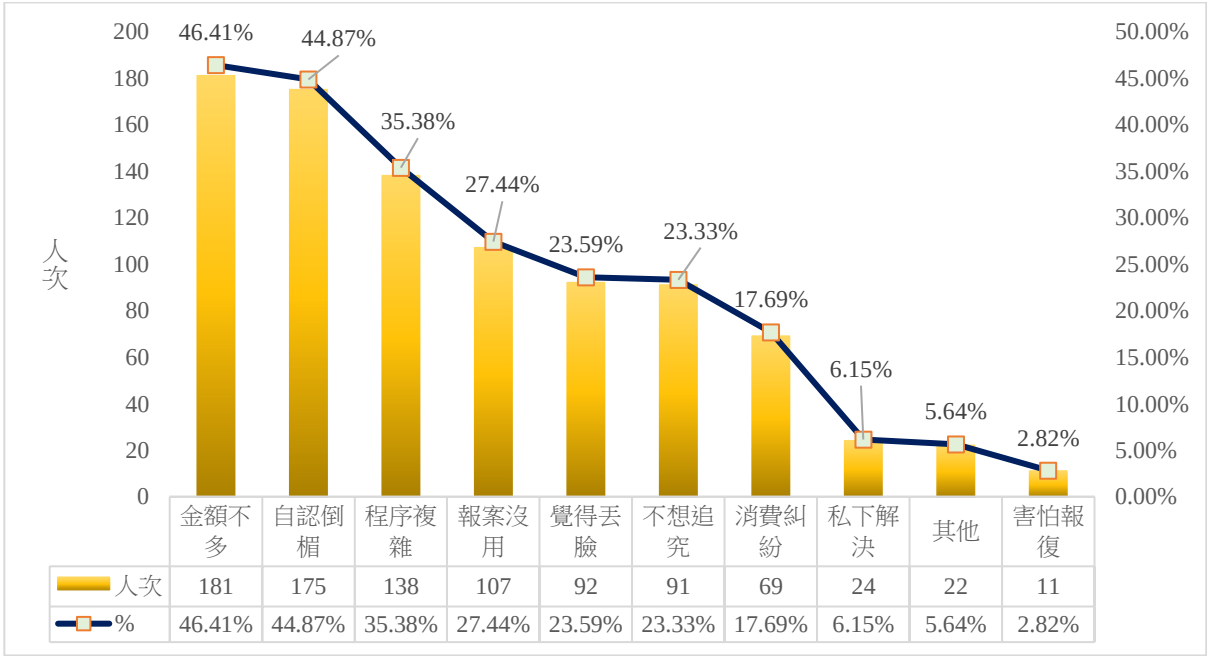
圖 3-3-5 進一步分析網路詐欺被害者發生詐欺案件未報案之原因(n=390)，以理解被害人的認知與想法。從圖中我們可以發現，大多數被害人認為是被害金額不多，有 181 人(占 46.41%)。這可能是因為**被害人覺得損失不大，不值得花時間和精力去追究**。其次是被害人自認倒楣，有 175 人(占 44.87%)。這可能是因為被害人**對自己的遭遇感到無奈和無力，只能接受現實**。第三順位是報案程序複雜，有 138 人(占 35.38%)。這可能是因為被害人**對報案的流程和效果缺乏信心和了解**，或者覺得報案會增加自己的困擾和麻煩。

其他被害原因，包括被害人認為報案沒什麼用，有 107 人(占 27.44%)。這可能是因為被害人**對警方的能力和效率有所懷疑，或者認為詐騙集團難以追查和制裁**。覺得很丟臉有 92 人(占 23.59%)。這可能是因為被害人對自己的判斷力和智慧感到羞愧和自責，或者**擔心被周圍的人嘲笑和歧視**。不想追究有 91 人(占 23.33%)。這可能是因

為被害人已經**放下過去的不愉快**，或者想要保持一個平靜和寬容的心態。消費糾紛有 69 人(占 17.69%)。這可能是因為被害人認為自己與詐騙集團之間**只是一種商業交易**，而非刑事案件。私下解決有 24 人(占 6.15%)。這可能是因為被害人與詐騙集團有某種聯繫或關係，或者能夠**通過其他方式取回部分或全部的損**失。其他未報案原因包含自身有警覺、客服處理、沒損失、政府查不到、錢有討回來等原因，有 22 人(占 5.64%)。這些原因都顯示出**被害人對於詐騙事件的處理方式有所差異和多元性**。害怕報復有 11 人(占 2.82%)。這可能是因為被害人**對詐騙集團的威脅和恐嚇感到恐懼和不安**，或者擔心自己的安全和隱私受到侵犯。

這些數據反映本研究中遭受詐騙被害的受訪者**未報案的主要原因，大多數認為被害金額不多，再加上報案手續繁瑣及沒太大用途，乾脆就自認倒楣**。然而，這種態度可能會讓詐騙集團有恃無恐，繼續施行犯罪行為，導致更多人受害。因此，本研究建議被害人應該勇敢地向警方報案，讓警方能夠掌握詐騙的情況和手法，並加強偵查和打擊。同時，**相關部門也應該加強對報案程序的簡化和效率的提升，讓被害人感到報案是一件值得和有用的事情。**

圖 3-3-5　最近一次網路詐欺被害未報案原因分布圖(n=390)[a]



註：1.[a] 本研究樣本有向警方報案有 174 人(占 30.85%)，未向警方報案者 390 人(占 69.15%)，本題為探討未向警方報案之原因，故分析樣本為 390 人。

2.本題為複選題，未報案其他原因包括自身有警覺、客服處理、沒損失、政府查不到、錢有討回

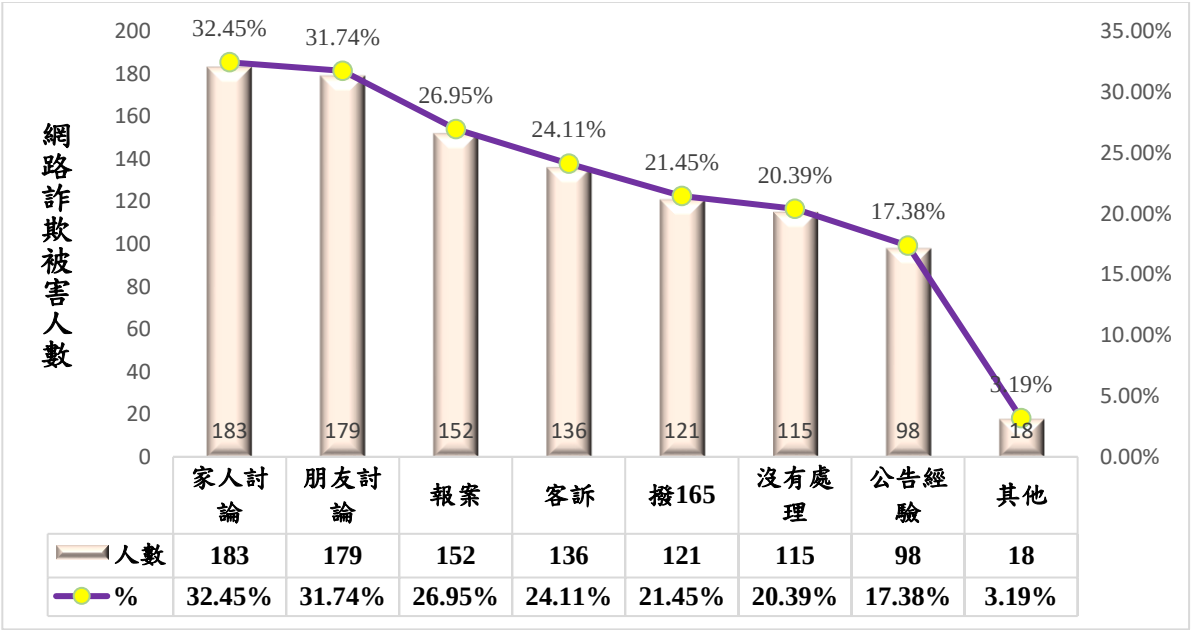
來等原因。

3. 被害後因應措施

圖 3-3-6 展示被害人遭遇網路詐欺後的因應方式，反映他們對事件的不同反應。從圖中可以看出，**大部分的被害人會先和家人討論**，有 183 人(占 32.45%)選擇這個做法。**其次是尋求朋友的幫助**，有 179 人(占 31.74%)這麼做。**第三多的是向警方報案**，有 152 人(占 26.95%)採取這個措施。

其他的因應方式還包括：撥打客訴電話有 136 人(占 24.11%)、撥打 165 反詐騙專線有 121 人(占 21.45%)、不予理會有 115 人(占 20.39%)、在網路上公告自己的經驗有 98 人(占 17.38%)、以及其他如封鎖對方、直接提告、自認倒楣、提升資安、向信用卡公司申訴等方法有 18 人(占 3.19%)。這些數據顯示了**被害人面對網路詐欺的多元處理方式。**

圖 3-3-6　最近一次網路詐欺被害後因應措施分布圖(n=564)



	家人討論	朋友討論	報案	客訴	撥165	沒有處理	公告經驗	其他
人數	183	179	152	136	121	115	98	18
%	32.45%	31.74%	26.95%	24.11%	21.45%	20.39%	17.38%	3.19%

註：本題為複選題，其他因應措施包括封鎖對方、直接提告、自認倒楣、提升資安、向信用卡公司申訴等。

二、網路詐欺被害類型分布

本單元主要運用網路詐欺被害量表分析受訪樣本，過去一年半遭受網路詐欺被害類型與次數之分布；由表 3-3-4 及圖 3-3-8 網路詐欺被害態樣分布得知，在 1,064 有效調查對象中，曾經有上網購物被害經驗者 455 人（42.76%，*M*=0.55，*SD*=0.76）為最多，其餘依序為猜

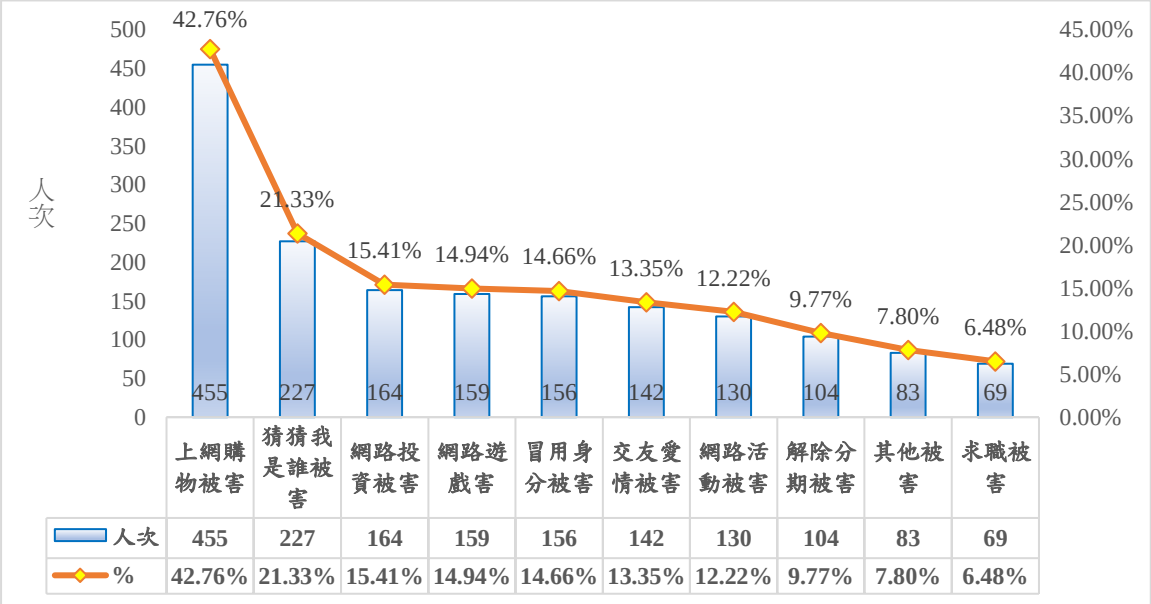
猜我是誰(假冒親友)被害有 227 人（21.33%，*M*=0.42，*SD*=0.96）為第二順位，網路投資被詐害有 164 人（15.41%，*M*=0.22，*SD*=0.61）為第三順位，網路遊戲被害有 159 人（14.94%，M=0.20，*SD*=0.58）為第四順位，每位受調查對象可重複選取被害經驗，經統計分析前 4 項高風險被害項目，累積已達 1,005 人次（94.45%），顯見**上網購物被害、猜猜我是誰(假冒親友)、網路投資被害、網路遊戲被害**等 4 種項目為最常見之網路詐欺被害型態類型。

表 3-3-4　網路詐欺被害類型之分布(n=1,064)

被害類型	無被害經驗(人次)	無被害%	有被害經驗(人次)	有被害%	被害經驗平均值(*M*)	標準差(*SD*)	排序
上網購物被害	609	57.24%	455	42.76%	0.55	0.76	1
猜猜我是誰(假冒親友)被害	837	78.67%	227	21.33%	0.42	0.96	2
網路投資被害	900	84.59%	164	15.41%	0.22	0.61	3
網路遊戲被害	905	85.06%	159	14.94%	0.20	0.58	4
冒用身分被害	908	85.34%	156	14.66%	0.19	0.52	5
交友愛情被害	922	86.65%	142	13.35%	0.21	0.65	6
網路活動被害	934	87.78%	130	12.22%	0.17	0.54	7
解除分期被害	960	90.23%	104	9.77%	0.15	0.52	8
其他被害	981	92.20%	83	7.80%	0.14	0.59	9
求職被害	995	93.52%	69	6.48%	0.10	0.44	10

註：原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名。

圖 3-3-7　網路詐欺被害類型分布圖 (n=1,064)



	上網購物被害	猜猜我是誰被害	網路投資被害	網路遊戲害	冒用身分被害	交友愛情被害	網路活動被害	解除分期被害	其他被害	求職被害
人次	455	227	164	159	156	142	130	104	83	69
%	42.76%	21.33%	15.41%	14.94%	14.66%	13.35%	12.22%	9.77%	7.80%	6.48%

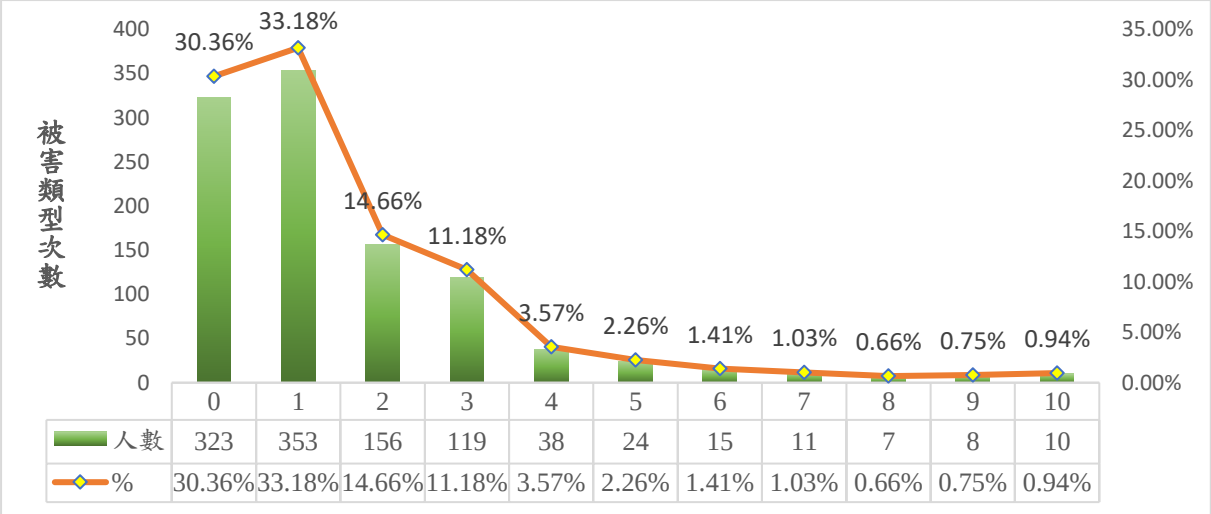
註：原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名。其他被害類型，包括罐頭簡訊、網路訂房、搜尋資料、宅急便、演唱會買票、比特幣等詐騙類型。

三、網路詐欺的多元性與重複被害

(一)網路詐欺類型之多元性

圖 3-3-8 顯示了網路詐欺被害人遭受的詐欺類型數量分佈。圖中 0 代表未曾遭受網路詐欺的人數有 323 人，占總人數的 30.36%；1 代表遭受一種網路詐欺的人數有 353 人，占總人數的 33.18%；2 代表遭受兩種網路詐欺的人數有 156 人，占總人數的 14.66%；3 代表遭受三種網路詐欺的人數有 119 人，占總人數的 11.18%。由此可見，**大部分的網路詐欺被害人只遭受一種或兩種詐欺類型**，合計有 509 人，占總人數的 47.84%；而**遭受三種以上詐欺類型的多元被害人數有 232 人，占總人數的 21.80%**。

圖 3-3-8　網路詐欺被害類型之多元性分布 (n=1,064)



註：原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名。

(二)網路詐欺類型之重複性

表 3-3-5 展示同一受訪者在不同時間遭受相同網路詐欺類型的次數分配情況。這些數據可以幫助我們了解被害人對於網路詐欺的防範意識和行為。由被害類型來看，最常見的是上網購物被害，有 455 人次遭遇這種詐騙。其次是猜猜我是誰(假冒親友)的詐騙，有 277 人次遇到這種騙局。第三順位的是網路投資的詐騙，有 164 人次受到這種損失(占 10.4%)。其他詐騙類型則包含各種利用網路平臺或服務來欺騙被害人的手法，例如：網路遊戲、冒用身分、愛情交友、網路活動、分期付款、求職等，共有 1,007 人次遭受這些詐騙。

從重複遭受同一被害類型次數來看，我們可以發現不同類型的詐騙對於被害人的影響和危險性也不盡相同。以上網購物被害為例，大部分的被害人只有一次受害的經驗，有 366 人次(占 80.44%)，而 2 次以上受害的人數則相對較少，只有 89 人次(占 19.56%)。這可能表示**上網購物被害者在第一次受騙後就能提高警覺，避免再次落入圈套**。相反地，猜猜我是誰(假冒親友)的詐騙卻有較高的重複受害率，只有 109 人次(占 48.02%)的被害者只有一次受害的紀錄，而 2 次以上受害的人數則高達 118 人次(占 51.98%)。這可能表示**猜猜我是誰(假冒親友)的詐騙手法較難被識破，或者被害者對於自己認識的人或親友較難抵抗其要求或勸誘，因而容易再度上當**。

表 3-3-5　有被害經驗樣本被害次數之分布(n=1,064)

被害類型	1 次	%	2 次	%	3 次	%	4 次/以上	%	總計
上網購物	**366**	**80.44%**	60	13.19%	19	4.18%	10	2.20%	455
猜猜我是誰(假冒親友)	109	48.02%	58	25.55%	19	8.37%	**41**	**18.06%**	227
網路投資	122	74.39%	25	11.01%	7	4.27%	10	6.10%	164
網路遊戲	125	78.62%	17	10.69%	9	5.66%	8	5.03%	159
冒用身分	117	75.00%	30	18.87%	7	4.40%	2	1.26%	156
交友愛情	95	66.90%	22	15.49%	12	8.45%	**13**	**9.15%**	142
網路活動	98	75.38%	20	15.38%	5	3.85%	7	5.38%	130
解除分期	73	70.19%	16	15.38%	9	8.65%	6	5.77%	104
其他被害	50	60.24%	12	14.46%	7	8.43%	**14**	**16.87%**	83
求職被害	44	63.77%	17	24.64%	4	5.80%	4	5.80%	69

註：原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名。其他被害類型，包括罐頭簡訊、網路訂房、搜尋資料、宅急便、演唱會買票、比特幣等詐騙類型。

第四節　網路詐欺被害相關因素分析

一、人口特性與網路詐欺被害之關聯性

本研究旨在探討一般組與被害組在人口特性方面的差異，並分析其與有無網路詐欺被害之間的關聯性。表 3-4-1 展示兩組在性別、年齡、每月收入、教育程度、職業等 5 個變項的分布情況。從表中可以看出，在性別方面，有被害經驗組的男性(309 人，52.70%)明顯多於一般組，而無被害經驗者的女性(305 人，54.50%)則顯著多於一般組。經過卡方檢定，發現性別與有無網路詐欺被害有顯著關聯性(χ^2=5.930*)，表示**男性較女性易有網路詐欺被害之可能性**。

在年齡方面，有被害經驗組的年齡多集中在 18-30 歲(187 人，58.80%)或 31-40 歲(198 人，50.60%)，這兩個年齡層占該組的大多數；而無被害經驗者的年齡則多分布 41-50 歲(157 人，59.00%)或 51 歲以上(101 人，59.10%)，這兩個年齡層占該組的大部分。經過卡方檢定，發現年齡與有無網路詐欺被害有顯著關聯性(χ^2=23.930*)，表示 **40 歲以下者網路詐欺被害機會較高**。在每月收入方面，有被害經驗組的每月收入多集中在未滿 2 萬元(73 人，59.80%)或 2 萬至未滿 4 萬元(185 人，59.30%)，這兩個收入層占該組的大多數；而無被害經驗者的每月收入則多分布於無收入(46 人，56.10%)、4 萬至未滿 6 萬元(175 人，53.80%)、6 萬至未滿 8 萬元(110 人，58.20%)或 8 萬元以上(75 人，64.70%)，這四個收入層占該組的大部分。經過卡方檢定，發現每月收入與有無網路詐欺被害有顯著關聯性(χ^2=33.422)，表示**無收入或每月收入 4 萬元以上者，網路詐欺被害機會較低**。

在教育程度方面，有被害經驗組的教育程度多集中在國小或初(國)中(肄)業(9 人，占 81.80%)、高中或高職畢(肄)業(81 人，51.90%)或大學或專科畢(肄)業(404 人，51.50%)，這三個教育層占該組的大多數；而無被害經驗者的教育程度則多分布研究所以上(125 人，64.10%)，這個教育層占該組的大部分。經過卡方檢定，發現教育程度與有無網路詐欺被害有顯著關聯性(χ^2=20.655***)，表示**教育程度愈低者，網路詐欺被害機會較高**。在職業類型方面，有被害經驗組的職業類型多集

中在學生(78 人， 59.90%)、服務業/文藝/傳播/行銷(94 人，61.00%)、交通/運輸/旅遊/物流(24 人，58.50%)、資訊相關/網路/實體銷售(56 人，52.80%)，這四個職業類型占該組的大多數；而無被害經驗者的職業類型則多分布軍公教公務員(173 人，58.40%)、建築/營造/製造/供應商(69 人，58.00%)、醫療/法律/金融/保險/房地產(62 人，53.40%)、家管/退休(44 人，52.40%)，這四個職業類型占該組的大部分。經過卡方檢定，發現職業類型與有無網路詐欺被害有顯著關聯性(χ^2=26.576*)，表示**不同的職業與網路詐欺被害之間存在一定的影響因素**。

表 3-4-1　人口特性與網路詐欺被害關聯表(n=1,146)

變項	有無被害經驗				χ^2 ; *sig*
	無 (n=582)	%	有 (n=564)	%	
性別					
男	277	47.30%	**309**	**52.70%**	5.930*
女	**305**	**54.50%**	255	45.50%	
年齡分組					
18-30 歲	131	41.20%	**187**	**58.80%**	
31-40 歲	193	49.40%	**198**	**50.60%**	23.930***
41-50 歲	**157**	**59.00%**	109	41.00%	
51 歲以上	**101**	**59.10%**	70	40.90%	
每月收入分組					
無收入	**46**	**56.10%**	36	43.90%	
未滿 2 萬元	49	40.20%	**73**	**59.80%**	
2 萬至未滿 4 萬	127	40.70%	**185**	**59.30%**	33.422***
4 萬至未滿 6 萬	**175**	**53.80%**	150	46.20%	
6 萬至未滿 8 萬	**110**	**58.20%**	79	41.80%	
8 萬以上	**75**	**64.70%**	41	35.30%	
教育程度分組					
國小或初(國)中(肄)業	2	18.20%	**9**	**81.80%**	
高中或高職畢(肄)業	75	48.10%	**81**	**51.90%**	20.655***
大學或專科畢(肄)業	380	48.50%	**404**	**51.50%**	

研究所以上	**125**	**64.10%**	70	35.90%	
職業分組					
學生	53	40.50%	**78**	**59.50%**	
軍公教公務員	**173**	**58.40%**	123	41.60%	
服務業/文藝/傳播/行銷	60	39.00%	**94**	**61.00%**	
建築/營造/製造/供應商	**69**	**58.00%**	50	42.00%	26.576**
交通/運輸/旅遊/物流	17	41.50%	**24**	**58.50%**	
醫療/法律/金融/保險/房地產	**62**	**53.40%**	54	46.60%	
資訊相關/網路/實體銷售	50	47.20%	**56**	**52.80%**	
家管/退休	**44**	**52.40%**	40	47.60%	
其他（無業/農林漁牧等）	54	54.50%	45	45.50%	

* p<.05； ** p<.01； *** p<.001

二、區域特性與網路詐欺被害之關聯性

表 3-4-2 分析一般組與被害組在居住地區特性上是否與網路詐欺被害有關。從表中可以發現，不論是居住在北部(北北基桃竹)、中部(中彰苗投雲)、南部(嘉南高屏)、東部(宜花東)還是離島等不同的地區，與有無遭受網路詐欺並沒有顯著的差別，也沒有達到統計上的顯著水準(χ^2=1.739)，顯示**網路詐欺的發生與居住地區沒有密切的關係**。

本研究再進一步比較居住在鄉村或都會地區的人是否有不同的網路詐欺被害情形，結果也發現居住在城鄉的人與有無遭受網路詐欺並沒有顯著的差別，也沒有達到統計上的顯著水準(χ^2=1.529)，表示**網路詐欺的發生與居住在城鄉也沒有明顯的關聯性**。

表 3-4-2　區域特性與網路詐欺被害關聯表(n=1,146)

變項	有無被害經驗				χ^2; sig
	無	%	有	%	
居住地區					
北部(北北基桃竹)	247	52.60%	223	47.40%	
中部(中彰苗投雲)	158	51.10%	151	48.90%	1.739
南部(嘉南高屏)	152	47.80%	166	52.20%	
東部(宜花東)及離島	25	51.00%	24	49.00%	
居住城鄉					
鄉村	146	54.10%	124	45.90%	1.529
都會	436	49.80%	440	50.20%	

* p<.05; ** p<.01; *** p<.001

三、網路使用經驗與網路詐欺被害之關聯性

本研究探討一般組與被害組在網路使用經驗方面的差異，並分析其與有無網路詐欺被害之間的關聯性。表 3-4-3 顯示兩組在每日上網時間、每週上網次數、週末上網時段及接觸網路時間等四個變項的分布情況。在每日上網時間方面，有被害經驗組的上網時數多集中在 2 小時以內(83 人，59.30%)或 2-4 小時(159 人，53.40%)，而無被害經驗者的上網時數則多分布在 4-6 小時(153 人，54.60%)或 6 小時以上(233 人，54.40%)。**每日上網時間與有無網路詐欺被害有顯著關聯性**(χ^2=11.679**)，表示兩者之間存在一定的影響因素。這個結果與本研究的假設相反，原本預期有被害經驗者的上網時數會較長，但實際發現卻是無被害經驗者的上網時數較長。這可能與受訪者的年齡、職業、教育程度等人口特質及被害類型有關，因此**不能單純以每日上網時間來判斷是否容易受到詐騙**。

在每週上網次數方面，兩組的分布並無明顯差異，且未達顯著水準(χ^2=7.562)，顯示有無被害經驗與上網次數並無太大關聯。這個結果也符合常理，因為上網次數只反映使用者對於網路的頻率，而不一定代表使用者對於網路的品質或安全性。因此，**上網次數並不能作為判斷是否容易受到詐騙的指標**。

在週末上網時段方面，有被害經驗者較一般組較常於週末深夜至清晨(22：01 至隔日 08：00)上網(120 人，58.50%)，而一般組則較常於週末白天(08：01 至 20：00)上網(470 人，54.70%)。這個結果顯示**有被害經驗者的生活作息較不規律，可能因此而降低對於詐騙訊息的警覺性或判斷力**。**週末上網時間與有無網路詐欺被害有顯著關聯性**(χ^2=11.805**)，表示兩者之間存在一定的影響因素。

在接觸網路時間方面，有被害經驗組的接觸網路時間多分布在 2 年以下(28 人，65.10%)、3-5 年未滿(24 人，58.50%)、5-10 年未滿(123 人，60.60%)，而一般組的接觸網路時間則多分布在 10 年以上(470 人，54.70%)。這個結果顯示**有被害經驗者的使用網路經驗較不長久，可能因此而缺乏對於網路詐騙的認知或防範。接觸上網時間與有無網路詐欺被害有顯著關聯性**(χ2=21.594***)，表示兩者之間存在一定的影響因素。

綜上所述，本研究發現一般組與被害組在網路使用經驗方面存在顯著差異，且與網路詐欺被害之間有關聯性。然而，這些差異和關聯性可能反映不同使用者在網路上的心理特質、行為模式、風險認知等方面的差異。因此，本研究除分析網路使用經驗，更進一步探討網路生活型態、情境機會及心理特質對於網路詐騙被害的影響程度，以提供更有效的預防和教育策略。

表 3-4-3　一般組與被害組網路使用經驗之關聯分析表(n=1,146)

變項	有無被害經驗				χ^2 ; *sig*
	無	%	有	%	
每天上網時數					
2 小時以內	57	40.70%	83	**59.30%**	**11.679****
2 至 4 小時以內	139	46.60%	159	**53.40%**	
4 至 6 小時以內	153	**54.60%**	127	45.40%	
6 小時以上	233	**54.40%**	195	45.60%	
每週上網次數					
3 次以下	14	35.90%	25	64.10%	7.562
4~6 次	40	41.70%	56	58.30%	
7~9 次	67	51.10%	64	48.90%	
10 次以上	461	52.40%	419	47.60%	
週末上網時段					
08：01 至 12：00	71	60.20%	47	39.80%	**11.805****
12：01 至 18：00	135	52.90%	120	47.10%	
18：01 至 22：00	291	51.20%	277	48.80%	
22：01 至隔日 08：00	85	41.50%	120	**58.50%**	
接觸網路時間					
3 年以下	15	34.90%	28	**65.10%**	**21.594*****
3 年-5 年未滿	17	41.50%	24	**58.50%**	
5 年-10 年未滿	80	39.40%	123	**60.60%**	
10 年以上	470	**54.70%**	389	45.30%	

* p<.05; ** p<.01; *** p<.001

由表 3-4-4 比較一般組與被害組使用網路平臺之關聯性分析得知，受訪者是否有使用購物網路(χ^2=0.000)及使用社群軟體(χ^2=3.322)與是否容易成為網路詐欺被害無顯著關聯性；但是有使用線上遊戲(χ^2=8.460**)、留言區(χ^2=7.062**)、交友平臺(χ^2=27.847***)、直播平臺(χ2=10.456**)的受訪者，成為網路詐欺受害者的機率，明顯高於無使用該網路平臺者。其中以有使用交友平臺者，且有被害經驗者有 144 人(占 65.20%)，遠高於有使用交友平臺者，但未有被害經驗者有 77 人(34.80%)。從數據來看，**在有使用交友平臺者中，有網路詐欺被害經驗的比例較高。**這可能與交友平臺的特性有關，受訪者在交友平臺上較可能會遇到愛情騙子的追求、虛偽不實的個資、誘導轉帳或購買商品等各類型詐欺手法。因此，在使用交友平臺時，應

該要隨時提高警覺，保護自己的個人隱私和財產安全，千萬勿輕信陌生人的話語。

表 3-4-4　一般組與被害組使用網路平臺之關聯分析表(n=1,146)

變項	有無被害二組				χ^2 ; *sig*
	無(n=582)	%	有(n=564)	%	
購物網站					
無	127	50.80%	123	49.20%	0.000
有	455	50.80%	441	49.20%	
線上遊戲					
無	**356**	**54.50%**	297	45.50%	**8.460****
有	226	45.80%	**267**	**54.20%**	
留言區					
無	**423**	**53.40%**	369	46.60%	**7.062****
有	159	44.90%	**195**	**55.10%**	
社群軟體					
無	30	40.50%	44	59.50%	3.322
有	552	51.50%	520	48.50%	
交友平臺					
無	**505**	**54.60%**	420	45.40%	**27.847*****
有	77	34.80%	**144**	**65.20%**	
直播平臺					
無	**489**	**53.20%**	431	46.80%	**10.456****
有	93	41.20%	**133**	**58.80%**	

* p<.05; ** p<.01; *** p<.001

四、一般組與被害組在各影響因子之差異分析

（一）一般組與被害組在網路使用風險之差異分析

本研究比較有無網路詐欺被害經驗者在接觸偏差訊息及網路觸法行為等網路風險方面之差異。由表 3-4-5 得知，在接觸網路偏差訊息風險方面，有被害經驗組的平均分數(*M*=14.16)顯著高於無被害經驗組(*M*=13.11; *t*=-4.780*)，表示**有被害經驗者在網路上較容易遇到或看到一些不道德或不合法的訊息**，例如：線上賭博或下注賭盤、網路援交或一夜情、網路詐騙別人財物、投資詐騙、買賣盜版軟體等。**這**

些訊息可能會影響他們的價值觀和判斷力，使他們更容易受到詐騙的誘惑或欺騙。

在網路觸法行為方面，有被害經驗組的平均分數(*M*=4.51)顯著高於無被害經驗組(*M*=3.94; *t*=-5.723*)，表示**有被害經驗者較容易於網路或社群軟體上看到或參與一些違反法律或道德的行為**，例如買賣違禁物品/毒品/槍砲彈藥刀械、未經允許使用他人帳戶或查看文件、未經他人允許在電腦中增加/刪除/更改/列印資訊等。**這些行為可能會增加他們的法律風險和道德責任，使他們更易成為詐騙的加害者或受害者**。因此，本研究推斷**有網路詐欺被害經驗者，與其網路使用風險之間存在一定的關聯性**。

表 3-4-5　一般組與被害組在網路使用風險之差異分析表(n=1,146)

變項	有無被害二組	平均值	標準差	t 值; sig
網路風險	無	17.06	4.62	-6.036***
	有	18.67	4.43	
網路風險_接觸偏差訊息	無	13.11	3.93	-4.780***
	有	14.16	3.50	
網路風險_網路觸法行為	無	3.94	1.39	-5.723***
	有	4.51	1.90	

註：無被害經驗者 582 名；有被害經驗者 564 名。* p<.05; ** p<.01; *** p<.001

(二)情境機會與有無網路詐欺被害之關聯性

表 3-4-6 呈現不同的網路情境機會與受訪者是否曾遭受過網路詐欺之間的關係。從表中可以看出，在實體監控方面，家人對於受訪者的關心和提醒能夠有效地降低其成為詐欺受害者的風險，而朋友或同事的意見則沒有顯著的影響。此外，在自我監控方面，受訪者採取的各種防護措施，如避免提供個人資料、減少 IP 位址被追蹤、定期更換帳號和密碼、安裝防毒軟體、選擇正規的網路購物或下載平臺、確認網路訊息的真偽、不在網路上公開自己的行蹤和財產等，都與是否遭受網路詐欺有顯著的負相關，表示這些措施能夠有效地提高受訪者的防詐意識和能力。其中，最具有預防效果的三項措施是：**在網路上**

看到可疑的訊息時進行查證、**只在官方網站進行購物或下載活動**、**不在網路上透露個人資訊**。

另一方面，本研究也分析受訪者在網路上從事的一些活動與是否遭受網路詐欺被害之間的關係。從表中可以看出，在被害動機方面，受訪者如果涉及網路投資、色情網站、網路遊戲或與陌生人聊天等活動，則有較高的可能性成為詐欺受害者，其中以**與陌生人聊天的活動與被害的關聯性最強**。在被害誘因方面，受訪者如果下載不明來源的檔案、點擊不明來源的電子郵件或接收不明來源的檔案或附件等，則有較高的可能性成為詐欺受害者，其中以**點擊不明來源的電子郵件與被害的關聯性最強**。

總體而言，本研究發現**網路防護監控、被害動機和被害誘因等三個主要因素與網路詐欺被害之間的穩定關係**。

表 3-4-6　一般組與被害組在情境機會之差異分析表(n=1,146)

有無網路詐欺被害經驗					
項目	χ^2	*Gamma*	項目	χ^2	*Gamma*
防護監控_實體監控			**防護監控_避免曝露**		
家人注意	26.153***	0.227***	避免公開打卡	13.060**	-0.161**
朋友意見	7.76	0.121*	避免公開財產	16.004**	-0.187***
防護監控_自我防護意識			**被害動機**		
留下個資	8.629*	-0.025	網路購物	7.343	0.135**
上網記錄	7.908*	0.109*	網路投資	21.288***	0.149**
更改密碼	9.273*	0.004	色情網站	40.815***	0.259***
防毒軟體	8.335*	0.06	網路遊戲	54.754***	0.262***
官方網站	17.531**	-0.141**	網路聊天	156.095***	0.553***
公共 WiFi	2.52	-0.001	**被害誘因**		
提升權限	4.398	-0.079	下載檔案	82.429***	0.434***
雙重認證	6.875	-0.103*	點擊電郵	99.299***	0.494***
確認資訊	26.762***	-0.127**	通訊軟體	69.328***	0.396***

註：無被害經驗者 582 名；有被害經驗者 564 名。* p<.05; ** p<.01; *** p<.001

(三)一般組與網路詐欺被害組在心理特質之差異

本研究比較有無網路詐欺被害經驗者在偏差價值、網路成癮及低自我控制等心理特質上的差異，由表 3-4-7 得知，在偏差價值方面，有被害經驗組的平均分數(M=12.85)顯著高於無被害經驗組(M=11.43; t=-5.776***)，表示**有被害經驗者較認同一些不道德或不合法的網路行為，例如下載盜版軟體、在網路上說他人壞話、創造虛假身分、使用詐騙手段等**。

在網路成癮方面，有被害經驗組的「行為依賴」平均分數(M=14.74)顯著高於無被害經驗組(M=12.77; t=-5.240***)，表示有被害經驗者較難控制自己使用網路的時間和頻率，容易出現上癮的現象。同樣地，有被害經驗組的「心理依賴」平均分數(M=13.98)也顯著高於無被害經驗組(M=12.30; t=-8.233***)，表示有被害經驗者較依賴網路來滿足自己的情感需求，如果不能上網會感到不安或沮喪。因此，**愈有網路成癮傾向者，愈容易成為網路詐欺的目標**。

在低自我控制方面，有被害經驗組的「衝動性」平均分數(M=10.03)顯著高於無被害經驗組(M=9.05; t=-6.916***)，表示有被害經驗者較難控制自己的情緒和衝動，容易與人發生衝突或爭執。有被害經驗組的「冒險性」平均分數(M=7.88)也顯著高於無被害經驗組(M=7.09; t=-5.327***)，表示有被害經驗者個性較好奇和冒險，喜歡尋求刺激和新奇的事物。此外，有被害經驗組的「低克制力」平均分數(M=9.03)亦顯著高於無被害經驗組(M=8.65; t=-2.597**)，表示有被害經驗者個性和行事風格較不穩健和理性，容易追求即時的利益和快感。因此，**愈缺乏自我控制能力者，愈易受到網路詐欺的影響**。根據上述分析，歸納出**偏差價值、網路成癮、低自我控制等心理特質是影響網路詐欺被害的重要因素**。

表 3-4-7　一般組與被害組心理特質差異性分析表(n=1,146)

變項	被害二組	平均值(*M*)	標準差(*SD*)	*t* ; *sig*
偏差價值	無	11.43	3.78	**-5.776*****
	有	**12.85**	4.51	
網路成癮	無	30.62	8.18	**-7.091*****
	有	34.12	8.55	
行為依賴	無	17.85	4.99	**-5.240*****
	有	19.38	4.93	
心理依賴	無	12.77	3.83	**-8.233*****
	有	14.74	4.24	
低自我控制	無	24.79	5.58	**-6.272*****
	有	26.94	6.01	
衝動性	無	9.05	2.41	**-6.916*****
	有	10.03	2.39	
冒險性	無	7.09	2.31	**-5.327*****
	有	7.88	2.70	
低克制能力	無	8.65	2.46	**-2.597****
	有	9.03	2.46	

註：無被害經驗者有 582 名；有被害經驗者有 564 名。

* p<.05; ** p<.01; *** p<.001

第五節　網路詐欺害影響因子之羅吉斯迴歸分析

一、研究變項與網路詐欺被害之相關

本研究針對人口與區域特性、心理特質、網路生活型態與情境機會等四個面向，探討其與網路詐欺被害的相關性。根據表 3-5-1 的數據分析，我們發現以下幾點：在人口與區域特性方面，性別與有無被害有顯著相關(r=-.072*)，但與被害次數無關(r=-0.049)。這意味著**男女在遭受網路詐欺的機率上有差異，但在重複受害的次數上沒有差異**。此外，年齡和收入也與網路詐欺有關係，年齡愈大的人被害次數愈多(r=.116***)，而收入愈高的人被害機率愈低(r=-.102**)。而居住地區則對網路詐欺沒有影響(r=0.037)。

在心理特質方面，**網路成癮、低自我控制和偏差動機都與網路詐欺呈正相關**。這意味著這些心理特質愈強烈的人愈容易遭受網路詐欺，也愈容易重複受害。其中，**心理依賴**(r=.237***、r=.213***)和**衝動性**(r=.200***、r=.209***)是最重要的影響因素，分別**與被害次數和有無被害的相關係數最高**。在網路生活型態方面，接觸偏差訊息(r=.140***、r=.130***)和網路觸法行為(r=.168***、r=.323***)都與網路詐欺呈正相關。這意味著**這些行為愈多的人愈容易遭受網路詐欺，也愈容易重複受害**。

在情境機會方面，除了自我防護意識，其他變項都與網路詐欺有顯著相關。這意味著實體監控、避免曝露、被害誘因和被害動機都會影響網路詐欺的發生和次數。其中，避免曝露(r=-.134***、r=-.149***)是唯一與網路詐欺呈負相關的變項，表示**避免在網路上公開自己的行蹤和資訊可以降低被害的風險**。而**被害誘因**(r=.310***、r=.317***)和**被害動機**(r=.298***、r=.215***)則是最強的正相關因素，表示這些因素**會增加被害的可能性**。

表 3-5-1　研究各變項與有無被害及被害次數之相關分析表

變項	有無被害二組 (n=1,146)	被害次數 (n=1,064)	變項	有無被害二組 (n=1,146)	被害次數 (n=1,064)
人口與區域特性			**心理特質**		
性別	-.072*	-0.049	網路成癮_行為依賴	.153***	.127***
年齡	-0.121***	.116***	網路成癮_心理依賴	.237***	.213***
教育程度二組	-0.039	-0.043	低自控_衝動性	.200***	.209***
每月收入三組	-.102**	-0.034	低自控_冒險性	.156***	.229***
居住城鄉	0.037	-0.051	低自控_低克制力	.077**	.183***
網路情境機會			偏差動機	.169***	.253***
防護監控_自我防護	-0.015	-0.06	**網路生活型態**		
防護監控_實體監控	.127***	.214***	網路風險_接觸偏差訊息	.140***	.130***
防護監控_避免曝露	-.134***	-.149***	網路風險_網路觸法行為	.168***	.323***
被害誘因	.310***	.317***			
被害動機	.298***	.215***			

註：被害次數原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名。有無被害二組，無=0，有=1；性別變項：男=1，女=2；教育程度二組：高中職及國中小畢(肄)業=1，大學及研究所以上=2；每月收入三組：無收入及未滿 2 萬元=1，每月 2 萬以上，未滿 6 萬元=2，每月 6 萬以上=3。* p<.05; ** p<.01; *** p<.001

二、網路詐欺被害影響因素之羅吉斯迴歸分析

本研究探討了人口特性、網路成癮、低自我控制、偏差動機、網路風險、防護監控、被害動機誘因等多個影響網路詐欺被害的因素。我們按順序將這些因素納入二元羅吉斯(binary logistic)迴歸方程式，建立了四個迴歸模型。Hosmer 與 Lemeshow 檢定顯示，本研究

的解釋模型與資料高度吻合，模型配適度優良(見表 3-5-2)。基於此，以下針對四種不同迴歸模型對網路詐欺被害的影響力，分述如下：

（一）性別、年齡及每月收入對網路詐欺被害有預測力

模型一探討人口特性如何影響網路詐欺被害之發生，並將分析結果呈現在表 3-5-2 中。我們發現，人口特性可以解釋網路購物被害變異的 3.4%至 4.5%，顯示這些因素對網路詐欺有一定的預測力。為了進一步了解人口特性中哪些因素對網路詐欺被害有重要的影響，我們檢視了迴歸模型中各預測變項與依變項的關係，並發現以下幾點：首先，**在人口特性方面，性別、年齡和每月收入都與網路詐欺被害有顯著相關**。具體而言，**男性比女性有較高的詐欺被害機會**(B=0.397；Wald=10.035)，這可能是因為男性在使用網路時，較不注意安全或較易受到誘惑。另外，**年齡愈輕的人詐欺被害風險愈高**(B=-0.017；Wald=10.199)，這可能是因為年輕人對網路購物較缺乏經驗或較不警惕。最後，**每月收入 6 萬元以上的人**則比無收入或每月收入未滿 2 萬元的人**有較低的詐欺被害風險** (B=-0.434；Wald=4.325*)，這可能是因為高收入者對網路使用較有信心或較能辨別真偽。

（二）網路心理成癮、衝動行為或偏差動機傾向者，較易成為網路詐欺被害人

表 3-5-2 顯示，模式二在人口特性的基礎上，加入心理特質變項，包括網路成癮、低自我控制及偏差動機。這些變項能夠顯著提升對網路詐欺被害的解釋力，從模式一的 6.4%至 8.9%，提高到模式二的 10.0%至 13.1%。這表示，除了人口特性，心理特質也是影響網路詐欺被害的重要因素。**在人口特性方面，年齡和每月收入仍然是顯著的預測變項**，年齡越大、收入越高的人，越能避免成為網路詐欺的受害者。性別則在加入心理特質後，不再具有顯著影響力，可能是因為心理特質能夠更好地反映個人在網路上的行為傾向。

本研究進一步探討心理特質與網路詐欺被害的關係，發現網路成癮、低自我控制及偏差動機都是正向的預測變項，這些心理特質與網路詐欺被害有正向關係。在各變項中，網路成癮的心理依賴(B=0.112；Wald=22.297***)最能預測網路詐欺被害，其次是低自我控制的衝動性(B=0.119；Wald=13.225***)，而偏差動機(B=0.046；Wald=7.229**)排序第三位。這也意味著，**在網路上有強烈的心理依賴感、衝動行為或偏差動機的人，更容易受到網路詐欺的誘惑或欺騙**。

（三）網路風險普遍存在，關鍵仍在被害人人口特性及心理特質

本研究在模型三中，除了考慮人口特性、心理特質，再加入網路風險的生活型態，探討這些變項對網路詐欺被害的影響。由表 3-5-2 所示，模型三整體可解釋網路詐欺被害變異中的 10.7%至 14.2%，顯示這些變項對網路詐欺被害有一定程度的解釋力。

與模型二相比，模型三仍以人口特性中的年齡(B=-0.013；Wald=5.068*)、每月收入(B= -0.528；Wald=5.574*)、網路心理成癮(B=0.106；Wald=19.636***)、低自我控制的衝動性(B=0.117；Wald=12.749***)、偏差動機(B=0.04；Wald=5.261*)對網路詐欺被害有顯著的預測力，表示這些變項與網路詐欺被害有密切的關係。而新增加的網路風險，包括接觸網路偏差訊息及網路觸法行為，皆未能達到統計上的顯著水準，對於一般網路使用者及詐欺被害者而言，網路風險是普遍存在的現象，但是否會成為被害人的關鍵因素還是在於被害人的人口特性與心理特質。因此，本研究認為，**個人的人口特性與心理特質比起網路風險而言，更能有效預測網路詐欺被害之發生**。

（四）被害動機誘因的情境機會為預測網路被害的重要因素

本研究在模型四中，除了考慮人口特性、網路成癮、低自我控制、偏差動機，再加入防護監控及被害動機誘因，探討這些變項對網路詐欺被害的影響。由表 3-5-2 所示，模型四整體解釋力提高至 15.6%至 20.8%，顯示這些變項對網路詐欺被害有顯著的解釋力。進一步以 Wald 值作為判斷依據，發現**被害誘因及被害動機是影響網**

路詐欺被害的最關鍵的情境因素，其次是**網路心理成癮**，而**低自我控制的衝動性**則排在第四位，然而防護監控對於是否發生網路詐欺被害事件影響力不大。模型四加入網路情境機會後，人口特性變項影響力消失，表示人口特性與網路詐欺被害的關係不是固定的，而是受到網路情境機會的影響。因為不同的網路情境可能會產生不同的誘惑或壓力，進而影響個人的判斷或行為。

在模型四中，**被害誘因**(B=0.224；Wald=24.557***)指的是從網站上下載不明來源的檔案、點擊不明來源的電子郵、點擊所接收到的未知來源檔案或附件等行為。**被害誘因愈多，遭受網路詐欺被害的可能性愈高**。**被害動機**(B=0.173；Wald=18.768***)指的是個人瀏覽色情網站、遊玩網路遊戲、與未知身分的網友網路聊天等行為。**這些行為會影響個人對網路詐欺的敏感度或抵抗力，使其更容易相信或接受詐欺者的訊息或邀約**。被害誘因及被害動機分別排在第一位及第二位，顯示其影響力最大。**網路心理成癮**(B=0.089；Wald=12.854***)及**低自我控制的衝動性**(B=0.082；Wald=5.843*)仍保持一定程度的影響力，表示網路成癮及衝動性也是影響網路詐欺被害的重要因素。具有網路心理成癮傾向者及個性較為衝動性的人可能會因為一時的興奮或好奇，而忽略詐欺者的可疑或不合理之處，或者因為一時的貪婪或急躁，而不願意花時間或精力去查證或評估詐欺者的訊息或邀約，因而較容易發生網路詐欺被害事件。

表 3-5-2　網路詐欺被害影響因素之羅吉斯迴歸分析(n=1,146)

自變項	模型一		模型二		模型三		模型四	
	B(Wald)	Exp (B)	B(Wald)	Exp (B)	B(Wald)	Exp (B)	B(Wald)	Exp (B)
人口特性								
性別 [a](1)	**0.397(10.035**)**	1.487	0.148(1.185)	1.159	0.098(0.498)	1.103	-0.159(1.085)	0.853
年齡	**-0.017(10.199**)**	0.983	**-0.015(6.611**)**	0.986	**-0.013(5.068*)**	0.987	-0.004(0.359)	0.996
收入三組 [b](1)	0.151(0.731)	1.163	0.02(0.011)	1.02	0.02(0.011)	1.02	-0.002(0)	0.998
收入三組(2)	**-0.434(4.325*)**	0.648	**-0.497(5.202*)**	0.608	**-0.528(5.743*)**	0.59	-0.418(3.4)	0.658
教育程度 [c](1)	-0.195(1.127)	0.823	-0.25(1.683)	0.779	-0.245(1.603)	0.782	-0.238(1.415)	0.788
網路成癮								
行為依賴			-0.026(1.847)	0.975	-0.029(2.213)	0.972	-0.029(2.117)	0.971
心理依賴			**0.112(22.29***)**	1.119	**0.106(19.636***)**	1.112	**0.089(12.854***)**	1.093
低自我控制								
衝動性			**0.119(13.225***)**	1.126	**0.117(12.749***)**	1.124	**0.082(5.843*)**	1.086
冒險性			0.015(0.22)	1.015	-0.005(0.021)	0.995	-0.033(0.949)	0.968
低克制力			-0.065(4.34)	0.937	-0.071(4.058)	0.931	-0.07(4.502)	0.933
偏差動機			**0.046(7.229**)**	1.047	**0.04(5.261*)**	1.041	0.014(0.571)	1.014
網路風險								
接觸偏差訊息					0.033(3.079)	1.034	-0.008(0.165)	0.992
網路觸法行為					0.088(3.551)	1.092	0.041(0.666)	1.042
防護監控								
實體監控							-0.025(0.277)	0.975
避免曝露							-0.026(0.223)	0.974
被害誘因動機								
被害誘因							**0.224(24.557***)**	1.251
被害動機							**0.173(18.768***)**	1.189
常數	0.615(5.243*)		-1.497(12.109***)		-1.935(17.066***)		-2.388(12.719***)	
-2LL 對數概似值	1548.786		1470.136		1459.232		1394.148	
H-L 檢定 (模型適配度)	χ^2=12.313; p=0.138		χ^2=8.609; p=0.376		χ^2=9.213; p=0.325		χ^2=7.041; p=0.532	
Cox & Snell R^2 (Nagelkerke R^2)	0.034 (0.045)		0.10(0.131)		0.107(0.142)		0.156(0.208)	
正確預測率	58.6		64.4		65.9		67.7	

註：(1)a.性別：1=男性，2=女性，設定「女性」當參考組; b.每月收入三組：1=無收入及未滿 2 萬元，2=每月 2 萬以上, 未滿 6 萬元，3=每月 6 萬以上，設定「1=無收入及未滿 2 萬元」當參考組。c.教育程度：1=高中職及國中小畢(肄)業，2=大學及研究所以上，設定「1=高中職及國小畢(肄)業」當參考組。

(2)本研究變項中的區域特性及自我防護監控二變項與是否被害之分析因未達顯著,故未列入模型之分析，其餘變項採用強迫輸入法(enter method)，依據理論或邏輯推論，依序將自變項置入迴歸模型中，以檢驗各自變項對依變項之影響力。$^{*}p$<.05; $^{**}p$<.01; $^{***}p$<.001

第四章　我國網路詐欺犯罪加害者深度訪談結果分析

第一節　網路詐欺犯罪加害者之遴選程序

一、網路詐欺加害者之遴選與招募

本研究根據計畫書需求，針對 3 種不同的網路詐欺犯罪型態，規劃 5 位從事不同網路詐欺犯罪之加害者且目前在監獄中執行之受受人（3 名男性、2 名女性），進行深度訪談。本研究團隊於今（2023）年 5 月透過矯正署之資料，成功尋得網路投資詐欺、網路購物詐欺(佯稱買賣)與電信客服教導網銀/ATM 操作匯款詐欺之三種型態之受刑人，共計 10 位。經透過監獄相關承辦人徵詢前揭受刑人受訪意願後，其中有 5 名受刑人，可能因個人特質、心理狀態、社會關係、文化背景等各種因素，拒絕研究團隊的訪談。最後只有成功獲得 5 位受刑人之回覆，願意接受本研究之深度訪談（詳表 4-1-1）。

表 4-1-1　本研究原先規劃接受深度訪談之詐欺加害人名單

編號	姓名	性別	網路詐欺類型	犯罪事實描述	受訪意願
01	王○○	男	網路投資詐欺	透過 FB 散布「交護照可以出國開戶貸款，一本護照能賺取新臺幣 12 至 18 萬報酬」等訊息，使被害人陷於錯誤交付護照 23 本。	拒絕
02	王○○	男	網路購物詐欺(偽稱買賣)	連續多次透過 FB 社團佯稱有意購買遊戲點數，騙取點數序號及密碼後未依約付款。	同意
03	張○○	男	假愛情交友	透過「愛情公寓」交友網站以虛偽的年齡、職業資料供不特定多數人瀏覽，並因而結識被害人騙取財物。	拒絕

04	李○○	男	網路投資詐欺	透過FB散布漁貨出口投資訊息詐財。	同意
05	李○○	男	網路投資詐欺	透過微信以勸誘他人加入投資平臺會員或群組，由共犯各自扮演多名虛擬角色，向人宣稱可代為投資大陸股票等金融商品，使被害人陷於錯誤依指示匯款。	拒絕
06	周○○	男	網路投資詐欺	透過微信以勸誘他人加入投資平臺會員或群組，由共犯各自扮演多名虛擬角色，向人宣稱可代為投資大陸股票等金融商品，使被害人陷於錯誤依指示匯款。	同意
07	呂○○	男	網路購物詐欺(偽稱買賣)	在FB二手手機買賣平臺網頁上，向公眾散布販賣手機之虛偽訊息，致被害人陷於錯誤，依約定代售手機以抵付部分價金後再分期匯付。	拒絕
08	蘇○○	男	電信客服教導網銀或ATM操作匯款詐欺	詐騙集團成員致電被害人佯稱係蝦皮購物客服人員要求被害人依照指示操作網路銀行解除設定，被害人因而陷於錯誤匯款。	拒絕
09	郭○○	女	電信購物詐欺(偽稱買賣)	通訊軟體刊登販售物品之不實訊息，致被害人陷於錯誤匯款、或假冒公務人員向被害人誆稱健保卡遭盜用、涉及刑案，或電話誆稱購物發生作業疏失，致被害人陷於錯誤轉帳。	同意
10	楊○○	女	電信客服教導網銀或	出資成立詐欺電信機房，經由SKYPE對話啟動群發系統，佯稱電信門號異常，使大陸地區民眾陷於錯誤依指示回撥，	同意

			ATM 操作匯款詐欺	由一、二、三線人員假冒客服及檢警人員，向被害人佯稱涉及刑案云云，致被害人陷於錯誤依指示匯款至人頭帳戶 33 次。	

資料來源：本研究團隊。

本研究參考當前文獻、碩博士論文與相關研究後，針對網路詐欺犯罪型態，編製「網路詐欺加害者深度訪談大綱」，深度訪談大綱內容說明如下(詳附錄七)：

（一）基本與犯罪資料

1.受訪者之個人基本資料。(含性別、年齡、婚姻和家庭狀況)
2.受訪者教育程度、成長過程及家庭背景。
3.受訪者的網路生活型態（使用網路的時間、常使用的網路資源或平臺)。
4.受訪者這次入監之刑期多久？入監已經多久了？是否有網路詐欺以外的其他案件？
5.是否有其他犯罪前科？

（二）從事網路詐欺之情形

1.受訪者從事網路詐欺有多久的時間？在何種情形下開始從事網路詐欺（是否因曾有詐欺被害經驗而開始從事）？
2.受訪者為何選擇（持續）從事網路詐欺？有無考慮過從事其他犯罪？
3.受訪者所從事的網路詐欺之具體工作內容為何？當時投入網路詐欺工作之時間、精力程度如何？
4.受訪者說明是如何學習、精進或改良從事網路詐欺之相關技巧及方法？
5.受訪者說明選擇網路詐欺被害人時有哪些關鍵考量因素？哪些人口特性或心理特質是您較偏好的？
6.受訪者說明從事網路詐欺有何偏好的時段？以即在時段選擇上的考量因素？

7.受訪者認為在何種網路場域、平臺上實施網路詐欺得手成功率較高？

8.受訪者認為以何種獲利方式、財物（含虛擬財物）作為網路詐欺標的物得手成功率較高？並詳述在獲利方式、財物選擇上的考量因素？

9.受訪者所從事的網路詐欺之獲利報酬與獲得方式與原本的預期是否有落差？

10.受訪者對於所從事網路詐欺是否有其他心得感想或意見？

（三）對於網路詐欺防制策略之認知

1.受訪者從事網路詐欺後多久時間後被查獲？被查獲的關鍵具體原因為何？

2.與其他犯罪相比，受訪者認為從事網路詐欺之的風險程度如何？受訪者認為從事網路詐欺有哪些風險？

3.受訪者認為在網路環境中有哪些數位監控措施？受訪者認為目前網路環境中的數位監控強度如何？

4.在從事網路詐欺時，受訪者會採取哪些具體措施以降低風險、規避監控及查緝？並詳述如何設計及規劃資訊、金錢流路或其他規避措施。

5.受訪者認為警察查獲網路詐欺之能力如何？是否與受訪者從事網路詐欺前之預期有落差？

6.受訪者認為政府之反詐騙宣導（或其他預防策略）是否能有效避免被害者受騙？受訪者認為哪些是有效之預防策略。

7.有關政府採行的網路詐欺預防策略，受訪者有何其他建議？

二、網路詐欺加害者深度訪談之實施

本研究於 2023 年 5 月去函矯正署同意本深度訪談之進行後，隨即針對表 4-1-1 所提供之網路詐騙受刑人名單，透過監獄當局進行招募參與本研究事宜。最後成功招募 5 位網路詐欺加害受刑人願意接受本研究團隊之深度訪談後，即提供本研究之知情同意書與深度訪談大綱。經受訪當事人確認有意願後，隨即規劃深度訪談的時間則於 2023 年 7 月間，詳細前往地點與時間如表 4-1-2。

表 4-1-2　本研究團隊前往進行深度訪談之日期與受訪人數

前往訪談時間	監獄/看守所（分監）	受訪人數
7 月 10 日	○○看守所（分監）	1 名（男性）
7 月 12 日	○○看守所（分監）	1 名（男性）
7 月 13 日	○○監獄	2 名（女性）
7 月 20 日	○○監獄	1 名（男性）

本研究團隊與監獄/分監和有意願受訪之受刑人於所約定之時間，準時前往監獄/分監當局所規規劃之處所(教誨室/教區辦公室/會議/休息室)，進行深度訪談。在進行深度訪談前，由本研究團隊之訪問者先簡單自我介紹後，確認受訪受刑人之姓名無誤後，即根據本研究之知情同意書，說明本研究之目的，以及受訪者之權利以及可否錄音等事宜。經受訪當事人同意並於知情同意書簽名後，本研究團隊之訪談者帶領受訪者根據前揭三大面向 22 道題目，逐一進行訪談。本研究規劃每一位受訪者之深度訪談時間約 1 至 1 個半小時的時間，由受訪者充分了解題意後尊重其自由意志回答，並於受訪者確認無其他補充意見或想法後始結束本訪談，換言之，訪談過程完全尊重受訪者的自由意志並以輕鬆的方式回答題目、完成每一次訪談。

第二節　不同網路詐欺加害者之詐欺手法分析

一、網路詐欺加害者基本與犯罪資料分析

在個人基本資料裡，受訪的 5 位加害者，有 3 位為男性，2 位為女性；年齡介於 26 至 42 歲之間；婚姻狀況除 1 位離婚外，其餘均未婚，教育程度有 3 位為高中畢肄業程度，2 位為大學程度，除 1 位(D)的高中階段有取得資訊和資料處理方面的證照外，其餘教育背景均與電腦或網路專長無關。

表 4-2-1　本研究受訪加害者基本與犯罪資料分析

代號	性別	年齡	婚姻狀況	教育程度	刑期	前科	已服刑期	從事詐欺時間
A	男	26	未婚	高中	13 年 5 月	初犯	1 年 3 月	5 年
B	女	42	離婚	大學	6 年	累犯	4 年 6 月	10 年
C	女	33	未婚	高中	6 年 4 月	再犯	4 年 6 月	2 個月
D	男	26	未婚	高中	2 年 3 月	累犯	9 月	2 年
E	男	33	未婚	大學	2 年	再犯	1 年 9 月	2 年

刑期方面，2 年至 13 年 5 月不等，刑期長短與受詐騙人數與金額、法院認定一罪一罰的案件數多寡有關。除一位受訪者 A 為初犯外，其餘均為累再犯(即有犯罪前科)，但這些累再犯之前科，不一定都是詐欺，有包含毒品、偽造文書、傷害、逃避兵役、竊盜等。受訪時已入監執行刑期已達 9 月至 4 年 6 月不等，除 A、D 外，已符合假釋提報或準備期滿出獄。最後，渠等從事網路詐欺犯罪的年資，2 個月到 10 年不等，甚至 D 認為是疫情讓他轉行從事詐欺犯罪。

其餘個人基本資料，分析如下：

（一）成長環境

5 位受訪者中，除 D 宣稱童年成長環境不錯，父母親都疼愛外，其餘受訪者的成長環境或多或少均有負面因素，伴隨其成長環境，例如家人的家暴、父親或母親的缺席教養、甚至隔代教養等情況。

小時候到成年家裡經濟環境都還不錯，但是家庭氣氛不佳，主要是我爸他有酗酒及家暴問題，他會打媽媽，而媽媽因為顧念小孩也沒有考慮離婚。……高中時因為家庭氣氛不佳，就會時常不太想回家，後來在外交了不好的朋友，也受朋友影響開始碰毒咖啡包。(A-1-2)

家庭背景有點類似單親，父母沒有結婚，但父親有自己的家庭，母親可以說是父親的小三。(B-1-2)

我媽經常不在家裡，我從小到大都是阿公、阿嬤帶大的就是隔代教養的小孩，帶我和弟弟，弟弟和我一樣，之前有曾經走偏過。(E-1-2)

（二）求學過程

5 位受訪者中，3 位男性受訪者均宣稱其求學階段，特別是在國中與高中階段，有輟學或學習狀況不佳、好玩之情形，沒有成就感，進而連結偏差同儕的情況，其中兩位因而接觸了毒品。

高中曾中輟，雖後來曾復學 2 次，但也最後還是肄業；……高中時因為家庭氣氛不佳，就會時常不太想回家，後來在外交了不好的朋友，也受朋友影響開始碰毒咖啡包。(A-1-2)

我對上學沒有興趣，所以高中沒有畢業。我在高中階段換了三間學校，一間普通高中，兩間高職。我轉學的原因不是因為換地方住，而是因為我不適應學校的生活方式。(D-1-2)

……我到臺南的○○高中就讀籃球班，就在那裡遇到一些壞朋友，後來媽媽就叫我回來基隆讀○○高中夜間部，在那裡就讀餐飲科了。……自己當時玩心比較重，回基隆後又和一些國中時期沒有讀書的同學玩在一起，也有使用一些新興毒品。我大約在高一、高二的時候開始接觸毒品，只會用 K 他命，不會用其他的

毒品。(E-1-2)

另 2 未女性受訪者均認為求學階段平平，並沒有值得說明的地方。

我是大學畢業，念的是航空服務系，國中後念五專、再念插大。(B-1-2)

高中肄業，沒有特殊成長過程。(C-1-2)

（三）家庭狀況

除 D 宣稱原生家庭父母親未離婚、功能正常外，其餘原生家庭似乎未能具有失功能的狀況，例如缺乏父親管教、母親管教，甚至有父母親不僅離異，且目前都關押在監獄中執行徒刑之情形。

父母近年均因案分別入宜蘭監獄及桃園女子監獄服刑中。(A-1-1) ……小時候到成年家裡經濟環境都還不錯，但是家庭氣氛不佳，主要是我爸他有酗酒及家暴問題，他會打媽媽，而媽媽因為顧念小孩也沒有考慮離婚。(A-1-2)

家庭背景有點類似單親，父母沒有結婚，但父親有自己的家庭，母親可以說是父親的小三。(B-1-2)

家中僅有媽媽，一個姊姊，一個弟弟。(C-1-1)

我媽經常不在家裡，我從小到大都是阿公、阿嬤帶大的就是隔代教養的小孩，帶我和弟弟……。(E-1-2)

（四）網路生活型態

5 位受訪者皆稱每日上網的時間很長，甚至有受訪者稱從小學就開始上網。而上網平臺就是 FB、IG、line、UT、微信等，而上網的目的就是瀏覽社群媒體聊天、購買商品、玩遊戲，也包含有玩線上賭博性電玩。

小學時開始玩線上遊戲，一直玩到高中，那時候生活中會花很多時間在玩線上遊戲，下課、放學後都還在玩，也會熬夜玩，……當時父母也不會限制我玩遊戲的時間。出社會之後沒有網路遊戲成癮，但是也偶爾會玩傳說對決（線上手機遊戲）之類的手遊，大多時候是玩線上博弈遊戲。(A-1-3)

每日使用網路的時間很長，每天超過四分之一的時間都在使用網

路，經常使用的平臺為 FB，網路購物，還有 IG、TU 看影片等，比較大眾化的社群網路平臺(B-1-3)

每天使用網路的時間很長，一起床就使用，主要使用的網路資源為 Line、FB、微信等。(C-1-3)

我喜歡玩線上賭博的網路遊戲……。我靠這個網站賭博，已經賺到了三間房子和兩臺車。不過這個網站不是合法的，所以我通常用微信(WeChat)來聯絡事務，以免遭警查獲。……我覺得這種賭博方式很方便，只要有網路銀行或超商就可以隨時存錢或領錢，一般而言，15 分鐘到半小時就可以完成 100 萬的交易，對於玩家而言，相當便利。(D-1-3)

犯詐欺這一條罪之前，每天都在使用網路，因為手機很普遍，每天都在上網，每天至少 5 小時掛在網路上，除了玩遊戲、聊天以及瀏覽社群軟體、例如 FB、IG、抖音，也會用網路購物，這些網路生活型態都是我尚未接觸到詐騙工作的生活型態。(E-1-3)

二、網路投資詐欺加害者之詐欺手法分析

5 位受訪者中有 1 位為網路投資詐欺加害者，即 E，以下針對渠等從事網路投資詐欺之手法，予以分析。

（一）從事網路投資詐欺之情形分析

1.從事網路投資詐騙的時間與原因

E 受訪者表示，從事網路投資詐欺的時間都很短，約莫 2 年的時間，而其接觸的原因是因為曾經車禍受傷，無法工作，在從小到大認識的朋友介紹下，踏進網路投資詐騙的工作。

如果認真算的話，應該是 2 年吧，就是進來執行這一條的前兩年吧，就是接觸到這個投資詐騙工作，從不會到會，約兩年的時間。……我會從是這份工作主要是兩年多前，左手肘關節處因為車禍受傷，沒有工作，但又缺錢，一個從小到大、認識十幾年的朋友，就像你講的從事網路詐騙工作的，就來問我要不要來做這個工作，當下我不知道要做甚麼，只是說請我在社群媒體發一下圖片、照片、生活照，去了約半年之後才慢慢了解到這是另類的變相詐騙。(E-2-1)

2.從事網路詐騙前有無被詐欺經驗

E 受訪者宣稱，其並無網路詐欺被害之經驗。

……我從事這個詐騙行為，本身並未曾有被詐騙過的經驗。(E-2-1)

3.從事網路投資詐欺的關鍵因素與選擇此型態之原因

E 受訪者認為會從事網路投資詐欺犯罪的關鍵因素在於在甚麼樣的機會遇到了誰，加上自己缺錢，沒有工作，不排斥且不了解這是詐騙行為的情況下，慢慢學習後，成為選擇這個詐欺犯罪型態與因素。

我會從事這份工作主要是兩年多前，左手肘關節處因為車禍受傷，沒有工作，但又缺錢，一個從小到大、認識十幾年的朋友，就像你講的從事網路詐騙工作的，就來問我要不要來做這個工作，當下我不知道要做甚麼，只是說請我在社群媒體發一下圖片、照片、生活照，去了約半年之後才慢慢了解到這是另類的變相詐騙。(E-2-1)

就是因為當時左手肘關節受傷後沒有工作，朋友就來找我，一方面希望我有錢賺，一方面也可以幫幫他。那我因為真的缺錢，所以就答應他，進來後才慢慢地學習，從不會到會這樣。(E-2-2)

4.具體工作內容與投入時間、精力程度

E 受訪者表示投資詐騙的工作內容呈現專精與分工，分工就是將整個投資詐欺工作區分為資源方(在大陸)、買方(在臺灣)、還有股民(大陸民眾)，其中買方又分工為老師號、助理號、小號與水軍，除老師號是固定一名專業的股市或投資標的分析師外，助理號則是老師的助理，張羅老師號的工作，其餘的人為小號與水軍，小號就是誘導股民投資標的的人，水軍就是假扮投資成功的投資人，鼓吹老師號建議的哪一檔股票或標的已經成功獲利，小號和水軍可以互換。而整個交易平臺就在微信，詐騙大陸股民。

我們工作的方式很簡單，就是先取得資源方，資源方就是在大陸，有大陸的股民，股民就是證券商或投資站，我們這邊的買方(就是我朋友的老闆)會去跟大陸那邊買條子、客戶單，客戶單之後就會打進我們的老師號、助理號、小號還有水軍，所謂老師號

就是我們的投資詐騙就是一定要有一個老師，就是我們電視臺57臺的財經臺，一定要有一個老師分析股票或證券，這就是老師號；再來就是助理號，就是老師的貼身助理，負責老師所有的工作內容，老師會把所有的工作內容交給助理，這個助理又會拉一個群組，就是所謂的小號，就是在群組中誘導股民投資哪一檔股票或證券的人，就是小號，我就是小號；水軍就是在群組內發消息說，今天和老師投資了那一檔股票，賺了多少錢、獲利多少的人，大致上就是我們的分工，就是金字塔的架構。(E-2-3)

我們會架設一個網站平臺，設計一個 QR code，讓他們在大陸證券商那裡掃一下微信，他們的名單就會連結到我們的群組這邊了，我們不做臺灣的客戶，因為我們不詐騙臺灣人。(E-2-3)

5.如何學習、精進或改良相關技巧與方法

E 受訪者表示，組織會以實體授課、與員工開會檢討問題、把離職或之前員工的手機或案例列印分享以及邊做邊學的方式，教會小號與水軍的操作方式，特別是一些招募股民的話術與手法，讓本身有投資意願的股民投資，詐騙成功。

我們每周都會實體上課、與員工開會討論，這一百個客戶群中，我們在群組聊天的過程中，就應該會知道，那些財力可以的、手中有幾張或那些股票的、本身的資產有多少，還有朋友圈以及生活動態(例如開名牌車、買名牌包、住豪宅等)，大家就提會討論誰資產比較多，約篩選出 30 至 40 位，鼓勵他們投資。(E-2-3)

其實我們的專業技巧或方法，都是邊做邊學的，因為從開會當中，慢慢了解到群組裡面大家在做甚麼，分工為何，還有也會看前人或朋友的手機群組，了解他們和客戶聊天的內容為何，例如語音或輸入的字句，如法炮製，學習別人的用語與話術，就可以強化自己的技巧與方法。(E-2-4)

6.選擇被害人的關鍵因素與人口特性或心理特質

E 受訪者表示，他們集團鎖定的被害標的為大陸三線城市，因為三線城市居民對於防詐意識較一線與二線城市居民為低；根據觀察，受騙的族群以女性較高，因為女性對於運用微信通話較不排

斤，容易被話術吸引投資，男性較喜用簡訊聊天，較難上鉤，而年齡約介於 35 至 50 歲間有一定收入、經濟能力或資產之人。而會加入微信投資群組者，都是基本上都是有錢有閒、手邊有持股、對投資股市或期貨等已有基本概念且曾有獲利者，希望賺更多的錢，就是所謂的貪念。另外，集團也會使用「放長線、釣大魚」的心理戰術，投資初期讓利、給一些甜投給投資客，野心大且不願意離開群組者，最後一定會連本帶利坑殺其資金。

我覺得大陸地區的三線城市的股民，最容易詐騙成功，……因為三線城市的居民，資訊尚未如第一、二線城市發達，防詐意識尚未抬頭，所以容易被投資詐騙成功。此外，女生被詐騙的機率比較高，因為女性股民的話，我就親自打電話跟他聊，所以容易上手；男生似乎不喜歡用手機聊天，都是用簡訊聊天較多，就比較不容易上手。年齡層約 35 歲至 50 歲間有一定收入、經濟能力或資產的人，才會有要賺更多。(E-2-5)

因為會進到這個群組的股民，一般都是有錢有閒、基本上手邊有持股、對投資股票與期貨有些知識與概念的人，希望能夠賺更多錢；如果連對股票、對期貨都不懂的人，基本上不會想要進到這個網站，因為對這方面的投資完全沒有興趣。(E-2-5)

另外，我們會放長線、釣大魚，會給讓利給他們的，……基本上可以讓利兩至三次，然後觀察，如果這個人還在群組，表示他沒有懷疑被詐騙、還在觀望，所以我們不用急著詐騙他，持續觀察他、抓他心態，最後會告訴他一支獲利不錯的股票，請他加大資金後，給他一個投資夢想，然後資金就會只進不出，逐次坑殺，約兩、三個禮拜後就坑殺完畢，但他們不見得會認為被詐騙，只是認為真的投資失利，仍在群組中，沒有退群組也沒有報案。(E-2-5)

7.從事網路詐欺喜好時段

E 受訪者表示，從事網路投資詐欺的時段，一定要配合當地的股匯市開盤的時間，以及上班日。

我們從事網路投資詐騙的時段都是在早上，配合大陸地區的股匯市開盤的時段，例如我記得早上上午 8 點到 11 點，下午 1 點

半到 3 點，星期六日或例假日，股匯市沒有營業就沒有工作。(E-2-6)

8.網路詐欺所實施的網路場域

E 受訪者，因為他們是詐騙大陸地區的股民，所以都是利用微信進行投資詐騙行為的平臺、網路場域。

我們都是利用微信進行投資詐騙，因為微信是大陸最普遍的社群平臺。(E-2-7)

9.從事網路詐欺的獲利方式

E 受訪者表示，其獲利方式為成交一筆就抽至少 5%的佣金；從事這個行業以來，每一年的獲利至少 2 至 3 百萬元。但這種獲利，來得快，花用的也很快，愛用高檔貨、愛慕虛榮、出門比闊綽，最後也沒有甚麼儲蓄，但也離不開這樣的輪迴。

我的獲利算法就是騙進一筆帳，獲利至少有 5%。例如我今天做一張單 10 萬美金，約臺幣 300 萬，我的獲利至少有 15 萬，大致上是這樣。這兩年每一年的平均獲利至少有兩、三百萬元。錢來得快、花得也快，……先借再還，還了再借，一直在這循環中離不開。……我的錢都是花在名車啦、買名牌包和衣服啦、到高檔餐廳喝酒與唱歌啦，出去玩也都是大手筆，反正就是吃好的、用好的，愛慕虛榮啦，坦白講當時的心態真的沒有很好。……現在回想當時花錢的方式，自己都覺得很誇張。(E-2-8)

10.選擇網路投資詐欺獲利財物的考量因素

E 受訪者表示，網路投資詐欺不可能以面交現金或買人頭帳戶以轉帳方式進行交易。因為投資金額過於龐大，必須要開一個正當合法的實體銀行帳戶，讓投資客匯錢。由於專業分工緣故，E 受訪者不會直接接觸帳戶管理或提領，但據他了解，應該是有大陸地區的投資方負責資金的轉出與提領，以免帳戶被查封。

我們在大陸會開一個實體的銀行帳戶，叫做工商農業銀行，我們有一個合法的帳戶，告訴這些投資的股民把錢匯到這個帳戶。我們投資都是用美金，1 萬美金約 72 萬人民幣，隨便一個進出都是破百萬人民幣，所以不可能買別人的帳戶進行投資。

另外，提領現金不會是我們，我們不會做到這一層事情(接觸到錢)，我是小號，工作就是跟客戶聊天，但就我所知道，當知道股民有匯入一筆帳後，我們老師的朋友，他在大陸地區的朋友，馬上就在把錢轉匯出去，免得帳戶有一天被查封。(E-2-8)

11.從事網路詐欺的投報率與預期結果有無論落差

E 受訪者表示，如果以當時自己失業、無能力工作的情況，這種網路投資詐騙工作的投報率，確實很高、很划得來；但如果以現在的角度觀之，換來監禁兩年的徒刑，手邊也沒錢了，轉眼一場空，實在划不來。

如果以當時的心態來講，是覺得不錯了，超出預期，因為錢來得很快、很多，花的也很快，可以買名牌車、東西，過得很奢華。但現在想想，我幾乎都沒有儲蓄、手邊也沒有錢了，還來關兩年。(E-2-9)

12.從事網路詐欺的心得感想

E 受訪者表示，在監獄監禁近兩年，深刻的心得感想為：手邊積蓄歸零、愧對家人至親且無力照顧、往日好友未曾接見以及昔日論及婚嫁的女友跑了。

但現在想想，我幾乎都沒有儲蓄、手邊也沒有錢了，還來關兩年。(E-2-9)

現在想想，在執行期間看到家人的變故，覺得不值得。像我服刑期間，爺爺過世，還有一位疼我的姨婆也過世，但我都沒有見他們最後一面，就覺得很難過，在裡面關最怕就是遇到家人的過世，因為你無能為力，還讓家人頻頻擔心。而當初那些合作的朋友，跟你講稱兄道弟、會到監獄來看我，但我進到監獄後，一個都沒有來，就會覺得一切都不值得。自己之前獲利的時候也都沒有拿過一毛錢給家人，現在想想真的很慚愧。媽媽和阿嬤年紀都大了，行動都不便，要他們從基隆到監所來看我，於心不忍，所以我請他們不用來看我。現在回想，賺這麼多錢，也無法挽回最疼愛我的阿公，而且論及婚嫁的未婚妻也因為這一趟進來不願意等我離開了，所以說，我覺得我寧可不用這些錢了。(E-2-10)

（二）網路投資詐欺防制策略認知

1.從事網路詐欺被查獲的時間與原因

E 受訪者表示，從事此一工作約兩年即被警查獲；而查獲的原因是案外案，警察因為受理報案、前往民宅現場處理打架械鬥事件，因為集團成員涉入，讓警察破門查緝，進而查獲網路投資詐騙集團。

我從事這工作約兩年就被查獲了。其實我們被查獲是案外案。就是集團內有人黑吃黑，A 了集團的錢，有一天開會時，集團內有人找一票人進到我們的據點，利用要開會的時候，給他教訓一下，叫他把錢吐出來，找了 30 幾 40 個人來打他，結果被鄰居報警稱隔壁有人在械鬥、鬥毆，帶刀、拿球棒的，所以警察就來了，我們集團約 10 幾個人，有的人跑到了，沒有被抓到，我們同案 10 幾個人就被逮到啦。警察看到房間內有電腦，一併查扣，結果看到裡面有名單、有教戰手冊、有群組等，就知道我們是在搞網路投資詐騙的集團。所以查獲的關鍵，其實就是人多、嘴雜又滋事擾民，讓鄰居去報警。我現在想想，如果當時不用實體會議，自己搞自己的，應該不會被查獲。(E-3-1)

2.從事網路詐欺的風險程度與那些風險

E 受訪者認為從事網路投資詐欺的風險，就是詐騙臺灣人，因為臺灣人的防詐意識較高；相較於此，大陸人，特別是三線城市的居民，防詐意識較低。此外，手機使用網路的基地臺無法被大陸公安定位，就無法查獲集團。

其實我覺得我們搞網路投資詐騙，最大的風險就是做臺灣人，因為臺灣人防詐意識比較高、資訊傳播也比較快，被逮的風險比較高。所以我們一定做大陸人，一方面大陸三線城市的民眾，防詐意識不是很高、資訊也比較不流通，更重要的是，他們的公安查不到我們集團在那詐騙，因為公安無法定位到我們的手機位置，而且我們用的卡也是大陸卡，所以沒有國界或邊界的限制。(E-3-2)

3.從事網路投資詐欺犯罪的關鍵風險

E 受訪者認為，此次該集團被查獲純屬案外案，並非警方的查緝跟監或有被害人報案後循線查獲，因此，認為同集團內成員的素質、行為與是否集體行動為查緝破獲的風險因素。成員們各自獨立辦公，不要接觸，反而降低被查緝風險。

我們會租一個據點，例如基隆的一個公寓民宅，其實只要集團成員不要喝酒、拉 K 菸、吵鬧喧嘩，安安靜靜的，其實沒有人知道你們在做什麼。我們此次被發現就是因為集團有人鬧事、鬥毆，被鄰居通報警察才被查獲的。就我所知道，有些集團不需要在一個據點一起工作，例如 5 個人在 5 個不同的地方工作，同樣也運行的很好；但我們集團就是要找一個據點工作，也有一些守則規範，沒有人聽阿，吸毒啦、滋事吵鬧，總有一天出事。(E-3-2)

4.從事網路投資詐欺的數位監控措施之認知

E 受訪者認為，臺灣地區透過手機發射基地臺的訊號，太容易被警察定位與查獲，數位監控太強，所以不容易詐騙成功。

我沒有做臺灣的詐騙，我其實不太清楚，但我聽到別人說，臺灣警察的數位監控很強，做臺灣的投資詐騙一定會被查獲，因為臺灣的警察太強了，比如說今天我用手機打給一個股民的手機，我的手機就會有一個發射訊號點，警察就可以查到我發生訊號點的基地臺，我們就會被查獲了。但在大陸，公安查不到我的訊號點，所以我覺得做大陸比較容易，他們的數位監控沒有這麼強，比較容易詐騙成功。(E-3-3)

5.從事網路投資詐欺的規避措施

E 受訪者認為，兩岸因為分屬不同的電信系統、手機發射訊號的基地不同，且無法立即查緝哪一個手機連結哪一個基地臺，形成斷點，就是一個很好的規避措施。此外，層層分工，大家負責的工作不同，彼此不要聯絡，例如有人主管大陸的事物(負責提錢、轉錢、監控帳戶），有人負責臺灣的事務(老師號、小號與水軍)，形成斷點，也可以規避查緝。

我是認為大陸公安要到臺灣來查我們的訊號發射地點或基地

臺，是非常不容易的，這樣就規避了相關的監控與查緝手段，我們的風險就很低。(E-3-4)

我們就會設計一個投資有報酬的平臺，透過大陸的資源方招募轉 po 給股民，股民一掃微信的 QR code 就會進入到我們的投資群組，閱讀分享我們老師所分析的股匯市資訊，我們小號與水軍就會鼓勵與分享獲利心得等，鼓吹這些股民投資。我們在大陸的工商農業銀行，開了一個合法的帳戶，告訴這些投資的股民把錢匯到這個帳戶。當有股民告訴我們有匯錢進來投資了，我們就會告訴老師的朋友，他會請大陸那邊負責的人將錢再匯出，以免發生戶頭被凍結的情況。我們不會接觸到集團後面的老闆是誰，以及大陸端是誰負責。就是層層分工、層層斷點，我猜可能是誰，但不清楚他的姓名或背景，因為我看過他來過我們現場、看看我們的工作，所以我猜是他，但他絕對不會承認。我們是有一個默契，不會問我朋友(老師)也不會聊這方面的話題，他(老師)應該是知道但不會講後面的老闆是誰，因為他(老師)可能也是他下面的一個員工而已。(E-3-4)

6.警察在查緝網路投資詐欺的能力與事前事後的預期落差

E 受訪者認為臺灣警察查緝網路投資詐欺的能力很厲害，自己從事此一網路詐欺活動時也曾預期有一天會被臺灣警察查緝。只是不甘心是擦槍走火，被集團成員的不良素行所陷害。

我覺得臺灣警察查獲網路詐欺的能力已經很厲害了。其實就是看臺灣警察要不要認真查，如果認真查，一下子就查到了。我在從事這各行業的時候，就曾經想過一定會被臺灣的警察查到，但就像是我剛剛講的，很缺錢，先刷卡、借錢買東西消費，賺到的錢又付卡債、還債，一直在這循環之中，花錢很闊綽，洞一直補也補不完、跳也跳不開，繼續沉淪，坦白講也是很擔心被警察抓啊。等到警察破獲、抓到才中止這個循環。(E-3-5)

如果今天再叫我重新來過，我一定向集團建議，就是我們 10 個人，各自獨立分開工作，不要群聚再一起，降低因為拉 K 味道、喧嘩吵鬧被民眾報警查獲的風險。(E-3-5)

7.政府反詐騙宣導之預防策略之建議

E 受訪者建議：(1)政府應該正視與杜絕網路上販賣人頭帳戶的問題；(2)持續宣導以提高臺灣民眾防詐意識；(3)防詐宣導應該根據不同的詐欺犯罪類型予以不同的宣導方式；(4)持續強化警察與銀行行員第一時間阻斷民眾轉帳匯款的合作模式。

我覺得政府應該阻絕人頭戶的問題，因為沒有人頭戶，這些詐騙集團就沒有戶頭可以提供給被害者轉帳、匯款的機會，詐騙就不會得逞。至於如何阻絕人頭戶的問題，就要看警察如何去查了，像 FB 經常都可以看到很多人都在賣簿子。(E-3-6)

另外，我覺得我們願意詐騙大陸民眾而不願意詐騙臺灣人，除了職業的道德外，我也提到臺灣人防詐的意識確實比大陸人來得高，所以其實防詐宣傳我覺得仍是有幫助的，這也是為什麼我們覺得要詐騙臺灣民眾投資獲利，很不容易。但臺灣的詐騙手法很多，要針對不同的類型進行不同的詐騙意識宣導，就比較困難一點。(E-3-6)

臺灣還有一個做的不錯的就是行員在第一時間會阻斷民眾轉帳匯款，甚至通報警察、與警方合作，這是在大陸沒有的方法。(E-3-6)

8.政府網路詐欺預防策略之其他建議

E 受訪者沒有其他建議。

沒有其他建議了。(E-3-7)

三、網路購物詐欺加害者之詐欺手法分析

（一）從事網路購物詐欺之情形分析

5 位受訪者中有 3 位為網路購物詐欺加害者，即 A、C 和 D，以下針對渠等從事網路購物詐欺之手法，予以分析。

1.從事網路購物詐欺的時間與原因

受訪者從事網路購物詐欺犯罪的時間，約莫 2 個月至 3 年左右，受訪者 D 宣稱是因為 Covid-19 使其本業停業，進而從事網路購物詐欺。而從事網路購物詐欺的原因，計有：立即快速獲利、幫朋友以及轉行轉業藉以營生。

從 20 歲出頭開始從事網路詐欺，前前後後大約進行 2 年至 3 年時間。當時有在從事線上博弈遊戲，因為沒有錢（點數）繼續玩了，但是又想立即獲利，讓我可以繼續從事線上賭博，情急之下我就開始在臉書的社團中進行購物詐騙行為。(A-2-1)

快兩個月，就是幫朋友，因為朋友也在裡面做，就叫我幫他，擔任車手領錢，沒有詐欺被害的經驗。(C-2-1)

我以前是酒店幹部，底下有 17 個小姐，每個月可以賺到 20 萬以上，但是這種錢也花得很快。……後來因為 Covid-19 疫情關係，酒店停業了，我只能跟朋友一起轉行做網路直播賣水產。(D-2-1)

2.從事網路購物詐欺前有無被詐欺經驗

三位受訪者中，僅 A 受訪者表示曾在小學因玩線上遊戲被騙點數之經驗，對其產生深遠影響與啟發外，其餘兩位未曾有詐欺被害的經驗。

我覺得小學線上遊戲中被騙點數的經驗，對我造成深遠的影響及啟發，讓我往後情急之下想到這個可以快速獲利的方式。(A-2-1)

沒有詐欺被害的經驗。(C-2-1)

3.從事網路購物詐欺的關鍵因素與選擇此型態之原因

三位受訪者從事網路購物詐欺的關鍵因素在於想要獲利以及因為疫情關係，本業停業後，在朋友邀集之下轉而從事網路購物詐欺行為，賴以維生。仔細觀察，除 C 從事網路購物詐騙無相關背景外，其餘兩位從事網路購物詐欺與其熟悉網路從事博弈遊戲或熟悉的工作(例如販賣水產)有關。

……當時有在從事線上博弈遊戲，因為沒有錢（點數）繼續玩了，但是又想立即獲利，讓我可以繼續從事線上賭博，情急之下我就開始在臉書的社團中進行購物詐騙行為。(A-2-1) ……那時候沒有想那麼多，只能說是當時情急之下唯一想到能快速獲利的方式。也從沒有想過要從事販賣毒品或其他合法或非法獲利方式。(A-2-2)

就是比較自由，然後當時家裡也滿缺錢的，就想說從事這一

途，錢會賺比較多。就想說有義務幫朋友就幫吧，順便賺一賺錢，結果反而沒有賺到。有阿，換打電話的。聽說去大陸打電話比較好賺，但後來也是沒有去。我有朋友在大陸做，一次去三個月，賺好幾十萬。(C-2-2)

我喜歡玩線上賭博的網路遊戲，尤其是九州娛樂城這個平臺，因為它的入金和出金速度都很快，而且金額很高。我靠這個網站賭博，已經賺到了三間房子和兩臺車。(D-1-4)……後來酒店停業了，我才轉行做水產生意，這是我最熟悉的行業。本來我是真的想開店的，但是錢到手後，就沒有出貨和開店了，因為時間太緊迫了。沒想到我的合夥人捲款潛逃，帳戶遭凍結，導致沒有出貨，所以被投資人和買家告了詐欺。(D-2-1)

4.具體工作內容與投入時間、精力程度

三位受訪者都是從事網路購物詐欺犯罪，所以具體的工作內容就是想方設法找出行騙的對象，使用的網路詐欺介面為 FB 中，尋找相關的社團或自創社群平臺招攬行騙對象；網路購物詐騙的商品為 3C 產品以及水產魚貨等高單價的商品為主。甚至會安排暗樁進行競標或主動與受騙對象留言對話，以討價還價、提供低價的方式行騙被害者。投注的時間與精力非常長，當作自己的本職在經營，例如經常要回應留言、經常要提領匯款金額以及經常監控人頭帳戶是否被警查封等，投注相當多時間與精力在經營。

我主要是在交易 3C 產品的二手臉書(FB)社團找尋行騙的對象，都是找尋要收購 3C 產品的人下手，不是 po 要賣東西的貼文，我都是找訊息那些 po 文說要買手機、耳機或其他電子產品的人，請他們出價，然後開始跟他們討論。當他們沒收到商品開始緊張時，我還可以再透過話術慫恿他們再多付哪些費用，可以加價購買更多，我一起寄，有的人因為緊張就真的沒考慮很多，我就獲得更多。(A-2-3)

我們是集團就是在搞假電器、3C 產品的買賣。我們會 PO 文，我們是賣電器用品像是手機、電風扇、水冷氣和冷氣這些，反正想到的電器都有在賣。我們賣的會比一般市面的還要便宜，……所以大部分都吸引大學生、低收入的人、或是老人家

來購買，想要貪便宜的人就會來買。我們會先要求先付訂金，匯到指定的戶頭，然後我們會去提領，生意還滿不錯的。三更半夜就會匯訂金了，我七早八早就要去提領，幾乎每一個小時就出去提領，如果不快一點去提領，帳戶會被凍結。我的工作就是領錢、當車手，每天很忙、投入的時間也很多。(C-2-3)

我在網路上拍賣競標(水產)物品時，通常會放幾個暗樁，由 2-3 個人分別使用不同的帳號。這樣做的目的是為了創造出一種熱鬧的氣氛，讓其他的買家覺得這個商品很受歡迎，很值得搶購。同時，我也可以控制出價的節奏和高低，避免商品被低價拍走，或者是沒有人出價。反正最後一定會標到最低額以上嘛，這是我設定的底線，也是我能夠賺取利潤的保障。……我之所以沒有出貨，是因為我的資金被凍結了，沒辦法調貨。我身上沒錢了，也跑不掉了。(D-2-3)

5.如何學習、精進或改良相關技巧與方法

三位受訪者認為，主要是透過累積的經驗與觀察以及集團成員朋友的提點、話術，精進自己的技巧與方法。但 D 受訪者認為，從事這個行業，聰明是必要的，對於所販售的商品之專業知識、技巧與經驗，也是必備的。

在這兩、三年的時間中，……我只有自己在做，所以都是靠自己的經驗慢慢累積，久了就知道甚麼樣的人比較容易被騙。(A-2-4)

我覺得這沒有甚麼技巧耶，就是 PO 低價的電器，貪小便宜的人就會先付訂金，我們趕快把訂金提領出來，就這樣而已……。回應 FB 留言的時候，就是嘴巴要甜一點，就是留言要客氣啦……。我看我們集團也沒有甚麼精進的方式或技巧，但就是說在私訊、回覆 FB 的留言時，要有一些話術，例如 PO 照片給他們看，取得信任，並保證品質一樣，價格絕對比別人便宜。(C-2-4)

聰明是必要的，但不是足夠的。要成功地從事網路水產直播，還需要有專業的知識、技巧和經驗。這是我自己的能力所及之事，也是我覺得很好賺的事情。(D-2-2) ……我從小就喜歡觀察

人們的心理和行為，找出他們的弱點和需求，然後利用我的口才和技巧，讓他們按照我的意願行事。(D-2-3)

6.選擇被害人的關鍵因素與人口特性或心理特質

三位受訪者認為，網路購物詐欺行為，因為不認識被害人，所以無從選擇，但無論是主動到對方的 FB 留言或者在 FB 被動回覆對方，都可以發現年輕的大學生以及女性，最容易被騙；此外，老人家也似乎容易被騙。而被害者的心理特質都是一個「貪」字，貪小便宜、貪得無厭，利益薰心缺乏反思能力；其次是「急」，因為心急而忘記求證是否是詐騙騙局。

我發現女性、學生、年齡在 20 歲初頭的人比較容易被騙的，還有我覺得會被騙的人就是一個字，「貪」。……我覺得被害人真的很愚笨，他們對於價格、行情都完全沒概念，也不會懷疑賣家，缺乏反思能力。(A-2-5)

就是大學生、老人家比較容易上鉤，特別是大學生，因為他們是學生身分，經濟條件都是靠家人接濟，買東西就是希望便宜就好，所以大學生真的超好騙的；而老人家好像也喜歡便宜又大碗的，所以也容易上鉤。(C-2-5)

我覺得每個人都有可能被騙，只要找到他們的弱點。有的人貪得無厭，有的人急功近利。……急的人最好騙，貪的人要花時間說服他們，然後給他們一點利益。然後再來騙大筆錢。(D-2-5)

7.從事網路詐欺喜好時段

根據受訪者的內容，從事網路購物詐欺的時段，會因為客群的不同而有所不同的喜好時段。一般而言，靜態性的購物商城，顧客隨時會留言與匯款，所以工作時間比較長，平日上午一起床就經營到七、八點，但仍有一組人觀察 FB 的留言動態。如果是涉及主動要接觸客戶者，則要了解客群的生活型態與休閒時段，例如要主動詢問購滿 3C 產品者則以下午、晚上時間為喜好時段；經營網路直銷購物者，則以下午兩到四點(家庭主婦有空時間)以及晚間八點以後(上班族有空時間)為喜好時段，無例假日。一般取得貨款後就封鎖或斷絕與被害者的聯繫。

我是下午、晚上比較有空的時候，但是也要考量被害人他們的生活作息，中午、下午滑手機的一定比較多，在那些時候比較有辦法跟他們聯繫。(A-2-6)

我們集團從事網路商品詐騙，並沒有偏好的時段。因為我們都是 PO 在 FB 上，持續性的販售。我們取款也沒有特殊時段的考量，只要集團上頭說有民眾留言已經匯款進指定帳戶了，我就必須趕快出門去提領，免得匯款帳號會被關掉。……平日晚上就做到七、八點，但假日也是會做，幾乎是天天做。(C-2-6)……等到確定訂金收到後，我們就封鎖被害人了。(C-2-4)

我通常都是在晚上八點和下午兩點直播，這是人流最多的時段。晚上八點的上班族比較好騙，因為他們下班後想要放鬆一下，看看有什麼好東西可以買。……婆婆媽媽下午兩點午休起床，直播時間主要為下午兩點到四點，這是他們最可能上網的時段。(D-2-6)

8.網路詐欺所實施的網路場域

三位受訪者都是運用臉書 FB 這個平臺作為進行網路購物詐欺犯罪行為之平臺。原因在於：FB 普及、會員人數多、商城/社團瀏覽不需過濾與設限、任何人都可以進出商城/社團。

我都是透過臉書行騙，沒有在別的平臺或網路區域從事過。(A-2-7)

我認為是 FB，因為 FB 比較普及，會員人數多，且 PO 東西販售，瀏覽的人也不需要過濾、設隱私，任何人都可以進來看商品。沒有實施過其他平臺，不知道是不是比較成功。(C-2-7)

我登入 Facebook「臉書」社群網站後，並在「免費廣告宣傳投資賺錢交友兼職打工網路創業買賣通通免費 PO 文」臉書社團上刊登內容略以「要每月賺兩倍的錢嗎？快來參加我們的新型投資項目！這是一個保本專案，如果沒有獲利，我們會退還您的本金。(D-2-4)

9.從事網路詐欺的獲利方式

三位受訪者對於網路購物詐欺的獲利方式，看法均不一，但可謂多元獲利方式：即買線上博弈點數、透過 ATM 轉帳至指定人頭戶

後提領現金以及面交現金或匯款的方式。其實他們都知道都有風險的存在，但希望降低風險以求獲利順利。而 D 則認為面交現金或同意被害人匯款之目的是希望取得被害人的信任、沒有惡意詐欺的意圖，進而博得法官酌情減刑的重要因素。

我的觀念是面交、現金、匯款這種獲利方式都是很有風險的，我一開始就有很深刻知道，所以我的獲利方式都是請被害人去買線上博弈的點數，然後傳序號給我，讓我在線上博弈遊戲獲利。(A-2-8)

我覺得是 ATM 吧，我們全部都是利用 ATM 提領現金，沒有臨櫃匯款或網路銀行匯款。……所以我們有很多的帳號，但也必須一直清查那些被關掉的、那些還可以用。(C-2-8)

當初拍賣的時候，我並沒有隱瞞我的身分或使用虛假的帳號。部分被害人選擇了匯款的付款方式，但大多數我都是親自和被害人見面交易。這也證明了我沒有惡意欺騙的意圖，……也消除了被害人對我的疑慮和不信任。這些都是我在案發後積極改善的表現，也是法官在判決時酌情減輕我的刑責的重要因素。(D-2-8)

10.選擇網路購物詐欺獲利財物的考量因素

三位受訪者認為選擇網路購物詐欺獲利取財的考量因素，有的純粹就是想賺錢獲利、有的是挺朋友卻一毛錢未得、有的是本業結束後轉換跑道、選擇自己想做的生意，原因並沒有一定。但其後的考量因素與賺錢生活有關。

開始從事網路詐欺活動之前，我沒有想過會這麼容易，沒有想過這麼好獲利、這麼好賺。(A-2-4)

……真的是因為挺朋友的，才加入此一詐騙工作，把之前的工作辭掉。(C-2-9)……然後當時家裡也滿缺錢的，就想從事這一途，錢會賺比較多。(C-2-1)

後來酒店停業了，我才轉行做水產生意，這是我最熟悉的行業。本來我是真的想開店的，但是錢到手後，就沒有出貨和開店了，因為時間太緊迫了。沒想到我的合夥人捲款潛逃，帳戶遭凍結，導致沒有出貨，所以被投資人和買家告了詐欺。(D-2-

1)

11.從事網路詐欺的投報率與預期結果有無論落差

除第一位 A 受訪者認為投報率可以接受外，其餘兩位均無法接受。主要原因在於 C 可能被其朋友騙來從事網路購物詐欺行為也沒有給他談好的佣金。D 因為將事後和解金、罰金與律師費算入後，認為入不敷出，與原本期待不符。

可能因為我是自己單獨犯案，不是集團那種，所以不用給人抽成，所以我覺得自己單獨獲利很好。(A-2-9)

我做兩個月，但都沒有獲利，原先說好一個月領一次錢，但我朋友一拖再拖，兩個月過去了，一毛錢都沒有領到。……所以獲利是否符合預期，當然不符合。被查到 16 次，但實際上應該提領有上百次，兩個月領了上百萬，都交給我朋友，但他連一毛錢都沒有給我。(C-2-9)

這次的生意完全不符預期，我本來只是想賺點錢，沒想到竟然賠了 500 多萬。和解金就要我付 7、8 百萬，……而且還不止這樣，你還得把易科罰金算進去。易科罰金我現在已經繳了 60 幾萬，再加上 7 個月還有 20 幾萬要付。我關這 1 年也花了快 1 百萬。別忘了還有律師費啊，我見面談律師費每 15 分鐘就 1 萬 2，他寫一張訴訟狀就收 6 萬，加起來 7 萬 2。大牌律師就是這麼超貴的。(D-2-8)

12.從事網路詐欺的心得感想

三位受訪者從事網路購物詐欺心得感想，均不同。A 受訪者認為被司法系統傳喚後，有被標籤、自我放棄的念頭，能騙多少就騙多少，如果法院早點判可以盡早阻止其詐騙行為；C 受訪者則表達出非常後悔，認為這不是一條值回票價的選擇；D 受訪者則認為被害人的心態如果不貪心、不輕信，就不會被害。

因為詐欺第一次被傳喚，就覺得很恐怖，所以就自我放棄，想說反正都被告了沒差了，能騙盡量多騙，能撈盡量撈，所以後面就開始很多條，現在想起來會覺得，好希望當時案件審理快一點，早一點入監服刑，好阻止我繼續行騙。(A-2-10)

非常後悔，沒有賺到錢但卻賺到刑期。出去後要安分守己、不

再去找這位朋友了。(C-2-10)

我認為，詐騙事件的發生，不僅與客戶的個資外洩及銀行行員的內鬼有關，其實也與被騙者的心態有關。如果一個人不貪心或不輕信，就不會輕易上當。(D-2-10)

（二）網路購物詐欺防制策略認知

1.從事網路詐欺被查獲的時間與原因

三位受訪者從事網路購物詐欺被查獲的時間不一，短則兩個月、長則一年，而被查獲的原因都是與被害人去派出所報案後，警察積極偵辦有關。

我總共從事網路詐欺有兩、三年的時間，在開始從事將近 1 年多的時候就開始被法院傳喚了。主要就是被害人去報警，幾乎每一個被我騙的被害人都有去報警。(A-3-1)

兩個月，因為我都用我們的車子在集團到公園工作或帶車手到銀行、郵局或小 7 提領訂金，所以他們應該已經鎖定我的車子了，所以有一天我的車子開到一個銀行前面時，他們已經知道我來了，就埋伏把我抓了。聽我媽說，刑事局跟監我的車子有一段時間了。(C-3-1)

在網路詐欺中，被害者通常是在沒有收到貨物或款項的情況下，才發現自己上當了，於是趕緊去派出所報案。(D-3-1)

2.從事網路詐欺的風險程度與那些風險

三位受訪者認為不太需要擔心詐欺被捕之風險，原因在於：笨的被害人的、不要在網路被警察監控以及質疑政府與警察打擊網路犯罪的能力。

行騙的時候我是不太擔心有甚麼風險，……有是有，但是被害人愚笨的話，其實風險也不會很大。(A-3-2)

我是因為車手、車牌號碼被鎖定被抓到，而不是在網路監控或被網路警察抓到的，所以風險應該還好。(C-3-2)

我對於政府和警方打擊網路詐騙的能力，持有懷疑的態度。一方面，我認為政府在網路數位監控方面，還存在許多困難和挑戰。另一方面，我也對警方查緝網路詐騙的效率不抱太大期望。(D-3-2)

3.從事網路購物詐欺犯罪的關鍵風險

三位受訪者，受訪者 A 和 C 均認為警察在網路上的查緝與監控能力仍是很強的，是查緝網路購物詐欺犯罪的關鍵風險，所以不要正面迎戰警察。但受訪者 D 則對於當前政府與警察的打擊網路詐欺作為可以減少此類行為之發生。

不過最終我覺得一定會被查獲，(警察)網路查緝能力很強，所以犯案當下是沒什麼風險，但是整體風險還是很高，不可能完全不被查到。(A-3-2)

我知道網路有警察在監控，風險應該很高。(C-3-2)

我不覺得政府和警方能夠有效地預防和打擊網路詐騙，也不認為這兩個方面是減少網路詐騙案件的關鍵因素。(D-3-2)

4.從事網路購物詐欺的數位監控措施之認知

三位受訪者中，受訪者 A 和 C 對於當前網路事件的數位監控措施，認為非常的鬆散、沒有特別強，即使已有會員反映有人使用假帳號行騙，依然沒有被封鎖、繼續行騙。

我知道的是，以臉書為例，就是不能短時間內一次跟太多用戶聊天對話，不然臉書就會啟動安全機制，就是會把你的帳號封鎖，不過我覺得整體而言沒有很嚴格。像是我在社團行騙之後，縱使會有人 po 文說要留意我創的這個假帳號，但是我還是能夠用這個帳號在同一個社團繼續騙，還是有人會上鉤。這我剛開始也不知道，後來才發現原來管制這麼鬆。(A-3-3)

沒有耶，我在看 FB 也沒有甚麼監控或讓我被發現，目前的網路環境數位監控強度應該還好吧，沒有特別強。(C-3-3)

5.從事網路購物詐欺的規避措施

三位受訪者中，A 和 C 都不需要採取任何規避措施，主要是 FB 的帳號容易換帳申請、辦電子信箱很容易，所以行騙到獲利都可以透過 FB 完成。至於獲利的方式，三位受訪者則會利用：傳送線上博弈遊戲點數序號、網路轉帳指定人口帳戶或是轉至女友或其他人的帳戶，以規避查緝即可。

臉書創帳號時審查嚴格歸嚴格，但我可以換帳號呀，辦電子信箱沒有很難，隨便就可以辦一大堆帳號來替換。獲利的話，我

都是請被害人傳線上博弈遊戲的序號過來，那個遊戲也都是合法的，app 都可以下載的到，所以所有流程從行騙到獲利都是透過臉書訊息完成。(A-3-4)

沒有耶，我們都只想過用 FB PO 東西販賣，並沒有想過運用其他方法降低被查緝的風險。(C-3-4)

我把我的所得轉到女友或其他帳號上，只是為了保護自己，而不是故意逃避法律。警方或檢察官根本無法追查到我的錢的來源和去向，他們只想讓我還錢給被害人，我也已經展現我個人的誠意了。(D-3-4)

6.警察在查緝網路購物詐欺的能力與事前事後的預期落差

三位受訪者中，A 和 C 受訪者稱臺灣警察在查緝網路購物詐欺的能力是很強的，也認為一定會被抓，只是遲早的問題而已。A 認為早抓到就少詐騙被害人，晚抓到就多撈幾筆。但 D 受訪者一值對於警察的查獲能力持否定態度，甚至認為警察在網路上佈線已久、方式很多，但抓到詐騙犯很少，覺得網路警察沒有用。

其實我一開始從事網路詐欺時就知道自己終究會被抓，因為想說被害人一定會去報案，報案就一定會被抓，但是就是僥倖心態啦，就想說被抓了再說，先盡量多撈錢再說。其實網路環境預防部分其實很弱，平常不會有警察在臉書巡邏，這種很難靠巡邏預防，也幾乎沒有警察會佯裝被害人來釣魚。但是查緝能力我覺得就強很多，一開始就這麼覺得(A-3-5)

我覺得很強，我覺得他們不會當場抓你，但他們會跟蹤，跟蹤一段時間後，就抓你了。我知道臺灣的警察一直都很強，跟我從事網路詐欺犯罪之前與後沒有關係。(C-3-5)

我對警察查獲網路詐欺之能力持否定態度。警方經常為了專案勤務或績效，採取了誘捕偵查的方式。……每年都有大量的網路詐欺案件，但只有多少起被偵破和起訴。這顯示了警方在查獲網路詐欺方面的無能和低效，所以我覺得網路警察沒用，沒抓到騙子，也沒有辦法阻止我到處去騙人。(D-3-5)

7.政府反詐騙宣導之預防策略之建議

三位受訪者均認為當前政府反詐騙宣導之預防策略都沒有用，主要是人性貪念、貪小便宜的問題，不會認真看待反詐騙宣傳。只要心存貪念、貪小便宜的心態購物、又不願意思考一下、求證一下165 專線，這些反詐騙宣傳只是表面功夫，無法解決問題的根源。

我覺得整體而言，宣導是沒有用的，因為宣導歸宣導，政府宣導廣告那些很多啊，但是我覺得會認真去看的人其實本身就不容易被騙，所以基本上我覺得不是宣導的問題，我覺得被騙的人就是不願意花時間去做功課，而且就算看了宣導，他一直用貪小便宜的心態去買東西，還是遲早會被騙。(A-3-6)

我覺得不一定，還是要看人啦，我覺得一般民眾真的都是太貪心了，試想一個四萬元的手機，怎可能兩萬就買得到？蝦皮、露天都不可能這麼便宜了。所以民眾要事先想想啦，詢問一下165 是不是詐騙的，不是一看到這麼便宜就馬上行動、轉帳匯款了。(C-3-6)

我認為，反詐騙相關宣導是沒有效果的，因為它無法改變人們的心態和行為。那些貪心或者急需錢財的人，往往會忽略風險和常識，輕易上當。政府的反詐欺宣導政策，只是一種表面功夫，根本無法解決問題的根源。你不覺得這是在自欺欺人嗎？書讀得再多也防不了詐騙，這是一個事實。(D-3-6)

8.政府網路詐欺預防策略之其他建議

三位受訪者仍是認為政府在網路詐欺犯罪預防策略能做的很有限，主要是人性的問題，人性的貪心仍是詐騙被害的主要原因。但受訪者 C 建議多多推廣 165 專線，向民眾宣導遇有來路不明或低價促銷商品時，問一下 165 予以求證，減少被害風險。

我覺得政府能做的有限啦，民眾的本性很難被改變，太容易相信網路上的賣家或陌生人，都不疑有他，叫他們去做什麼事都很聽話，我也是做了之後發現，然後覺得很驚訝。我覺得就算政府很大力宣導，人們貪心的個性還是被害的主要原因，就算宣導很多，大家如果還是用求便宜、方便、貪小便宜的心態去買東西，那還是很容易被騙。(A-3-7)

沒有甚麼特別建議，多多推廣 165 吧！就是遇到可能是來路不

明電話或連結時，就是多花一些時間問一下別人、問一下 165 專線或打電話到相關部門求證一下。(C-3-7)

我對政府採行的網路詐欺預防策略並不看好，因為我認為它們沒有實質效果。如果政府宣導真的有用的話，為什麼詐欺案件還是層出不窮呢？我覺得詐欺受害者大多是自作自受，他們自己又貪又急，不願意聽取別人的勸告，才會落入陷阱。(D-3-7)

四、電信客服教導網銀/ATM 操作匯款詐欺

（一）從事電信客服教導網銀/ATM 操作匯款詐欺之情形分析

1.從事電信客服詐騙的時間與原因

受訪者 B 稱自己從事電信客服詐騙行為已有 5~6 年的歷史，亦即 103 年至 107、8 年間被抓。原因在於開店做生意，因為合約糾紛導致欠債，在缺錢孔急的情況下，透過朋友介紹，加入電信客服詐騙行列。

大概是自 103 年吧！從事不到一年就被抓啦！會從事網路詐欺是因為自己原來是開店做生意，後來有涉及一些合約糾紛，就是有欠債，為了趕快還債，透過朋友介紹，加入打電話話務工作進行詐騙。(B-2-1)

2.從事電信客服詐騙前有無被詐欺經驗

受訪者稱在從事電信客服詐欺之前，並無被詐騙的經驗。

自己本身沒有被詐騙的經驗。(B-2-1)

3.從事電信客服詐欺的關鍵因素與選擇此型態之原因

受訪者 B 稱自己從事電信客服的關鍵因素就是自己欠債、需要還債時，朋友介紹一個可以快速賺錢的工作，後來確實工作一個月賺得 10 萬元，工作內容就是打電話而已，又以分紅方式賺錢，進而持續從事此詐欺行為。

朋友介紹時就說，可以一次讓你快速賺到一筆錢，後來我實際去做，我僅去一個月，那一個月我賺到 10 萬元，說實在的，我也不知道 10 萬元算多還是少。而工作內容就是打電話，他有分一線、二線和三線，當你打的電話有被害人轉帳時，就算趴數分紅……。我沒有想過從事其他型態的詐欺活動。(B-2-2)

4.具體工作內容與投入時間、精力程度

根據受訪者 B 的說明，電信客服人員的工作就是打電話，分為一線、二線與三線，詐騙集團會利用自動電話系統撥打市內電話至家戶，宣稱有線電視因為未繳錢而於近日將被斷線，請住戶主動回撥客服電話。只要打進來客服人員者，即為一線人員，其目的就是要想方設法套出被害人之個資，例如姓名與身分證字號，接著以確實沒有收到月費的方式，請其到警察局報案或由一線客服轉接二線客服(佯稱是公安人員)。由於大陸幅員廣闊，報案地區不見得為住居地，因此許多被害人便宜行事便被轉至二線，二線人員佯稱欠繳會涉及刑法、凍結財產等，在被害人恐懼的情況下，應諾會馬上付錢，如果此時被害人願意配合、透過網銀或 ATM 匯款的方式盡速繳錢，此時二線客服馬上轉給三線客服，由其教授被害人如何轉帳，一旦金額轉入指定匯款帳戶，詐騙即成功。一線投入的時間約上午 8 點至下午 4 點，週六日一樣上班。集團是團進團出的，一次去東南亞國家詐騙大陸民眾就是三個月，三個月後回國休息。

工作內容就是打電話，他有分一線、二線和三線。(B-2-2)

(我是一線)他們有提供很多的詐騙話術的版本，我記得早年我那時候剛做的時候，就是打電話告訴客人你家的有線電視要被停機，……想方法套出他們的名字、套出身分證字號，然後就跟他們確認確實是你們無誤，然後他們就會繼續主張說他們都有按期繳費，然後我們就會告訴他說身分證可能已經被盜用，請他們去報警，……我可以協助你轉電話報警，(對方願意)這時候就將電話轉至二線，由二線的人(假扮公安)繼續和被害人通電話。我們詐騙電話撥打的地方都是詐騙大陸地區的民眾，……就轉請二線請扮演公安的人員接手，恐嚇客戶涉及刑法、會凍結財產，要求配合……。反正我們獲得的姓名與身分證字號，都是客戶自己提供的。語音的內容都會換，有的是手機、易保卡、中國移動……，只要公司覺得梗做到爛掉了，他們有會重新換語音內容。(B-2-3)

沒有偏好時段，就是公司設定的，早上八點到下午四點，週六日一樣要上班，因為大陸好像沒有周休二日之類的。……詐騙

集團去國外一趟就是三個月，除非遇到他們的節日他們的銀行休息，否則期間都不休假。我第一次去馬來西亞時，他們已經去兩個月了，所以我僅去一個月、尾期了，那一趟賺 10 至 15 萬。(B-2-6)

5.如何學習、精進或改良相關技巧與方法

受訪者 B 稱，公司會提供稿子給客服人員背，但因為每個客人的問題不見得都相同，所以臨場反應以及多與資深同事聊天、請益學習也很重要。臨場回應的說詞或話術，成功說服客戶後就要記下來，以後可以使用。

公司會提供稿子、印稿子給你，你拿到後一定要背。另外，每天打電話的時候，遇到客人問的問題不會回答時，就要跟同事討論，但因為涉及績效，除非比較資深的，否則同事之間也不見得會提供意見。所以一般就是臨場反應，如果突然間客人有問一個問題，你臨場回覆後，客人就做了或不再有疑問了，就表示這個答案不錯，要記下來。就是說，公司會提供一些方法與技巧，但同事的經驗還有自己臨場反應所累積的不錯經驗，都是精進自己技巧的方法。(B-2-4)

6.電信客服詐欺被害人的關鍵因素與人口特性或心理特質

受訪者 B 稱，早年能夠電信客服詐欺成功的關鍵因素就是接市內電話者於接聽電話時身旁有沒有其他人，若有，客人容易被提醒，就得放棄。但現在都改撥手機，身邊大部分都有人了，變成話術很重要。至於容易被詐騙的人口特性很難界定，男女都有，女性稍多、各個年齡層也都有；至於心理特質部分，因為大陸公安很有威嚴、很有權力，可以凍結財產、製發逮捕令，因此客戶很願意聽從二線客服命令，轉至三線轉帳或匯款。

103 年第一次做的時候，如果我們接到客戶是用家用電話回撥電話，我們聽到旁邊有人、或者在公司回電的時候，我們基本上就是放棄了，因為只有身旁的人一句話，客人就被提醒了；到了四、五年前(107、108 年)，就是近期了，都改發手機而不在發家用電話了，就不管客人旁邊有沒有人，因為這部分係由二線隔離或臨場處理了。其實我詐騙成功的案例，男性與女性

都有，但女性居多。年齡層，各年齡層都有耶，很難去界定……。我覺得他們容易被詐騙的原因第一是他們的知識水平不夠，第二是大陸民眾很害怕公安，第三是大陸公安可以凍結財產、製發逮捕令，聽到不配合會凍結時，他們就會很害怕，乖乖配合。(B-2-5)

7.從事電信客服詐欺行為之喜好時段

受訪者 B 稱從事電信客服詐欺行為，並無偏好時段，都是由公司(集團)設定，一線人員上班時間比較早也比較早休息，早上八點到下午四點，但例假日也要上班。但二三線人員可能會工作比較晚，只要提款機還行(轉帳)，就得繼續上班，否則等到隔天，這筆生意可能就沒了。

沒有偏好時段，就是公司設定的，早上八點到下午四點，週六日一樣要上班，因為大陸好像沒有周休二日之類的。如果是二三線的話務人員，是比較沒有時間的限制。中間沒有休息，晚上不會打，但聽說有些公司是專門負責打下班時間，打到晚上八點，因為打到九點，提款機(轉帳)還行，但要到銀行轉帳，就必須等到隔天，就會有風險。因為他可能會問家人或家人來關心詢問，研判可能是詐騙，這個客人可能就死掉啦。(B-2-6)

8.從事電信客服詐欺所實施的場域

受訪者 B 稱從事電信詐騙手法，就是公司開發一種自動撥打電話號碼的軟體，並附有客服人員(一線客服)電話提供其回撥。所以電信詐騙不會在同一個場域或國家，甚至在一個國家打電話去詐騙另一個國家的民眾，以亂槍打鳥的方式，看看有沒有客戶上鉤、回撥，進而上當被騙。

這其實是公司設計的一種軟體，就是自動撥號出去的後對方接到電話時，自動語音就會撥放您的有線電視即將停機，如有問題請撥按幾號鍵，電話就會到我們這裡一線，然後我們可能就會說某某有線電視你好，我是客服人員某某某，我可以為你服務甚麼，然後就按照劇本演出。就有點亂槍打鳥式的選擇被詐騙的客戶，所以也無法說是哪一個網路場域或平臺實施詐欺得手成功率較高。(B-2-7)

9.從事電信客服詐欺的獲利方式

受訪者 B 稱因為電信客服人員分三層，每成交一筆轉帳匯款，一線客服獲利 5%、二線客服獲利 7%，三線客服因為要教授客戶如何使用臨櫃轉帳、網銀轉帳或 ATM 轉帳，所以獲得之紅利較高為 9%。受訪者為一線客服，獲利為 5%，每一次出境詐騙至少賺 30 萬元，不清楚這樣的獲利是高或低。

每一次(一至兩個月)可以賺至少 30 萬，但我是一線的喔(紅利 5%)。如果是二、三線的話務人員，是比較沒有時間的限制，因為二線是 7%，三線是 8 或 9%，因為三線主要是教他們如何轉帳，比較麻煩的是教他們網銀，所以趴數比較高。他們的時間有時候到晚上八九點都有可能，只要是提款機還能轉帳，它們就有可能繼續服務客人。(B-2-6)

因為匯款成功與否都是三線比較清楚，據我所知，臨櫃匯款、網路銀行匯款、跟 ATM 轉帳為主要三種的獲利方式。我並沒有採取其他網路詐欺的方式，不清楚獲利的方式或成功率高低的問題。(B-2-8)

10.選擇電信客服從事詐欺獲利財物的考量因素

受訪者 B 稱，選擇電信客服詐欺就是入門門檻較低，也希望早日獲利還債。

當然從事電信詐欺就是很簡單，希望趕快賺多點錢還債。(B-2-8)

11.從事電信客服詐欺的投報率與預期結果有無論落差

受訪者 B 稱，剛開始時覺得投報率不錯，但晚近精算後發現，一期出境(到馬來西亞)詐騙三個月，獲利 30 萬，平均一個月 10 萬元，且被逮後還要關六年，跟當時不要從事電信客服詐欺、腳踏實地工作後累積至今所賺的收入差不多，就會覺得與預期的報酬有落差，覺得沒有賺很多。

剛開始的時候確實覺得獲利報酬很高，很不錯，但最近一次的詐騙經驗發現，其實一期就是三個月賺 30 萬，平均一個月 10 萬元，跟我就踏實地工作所賺的錢差不多，就覺得腳踏實地賺就好了。像之前去詐騙，工作一期三個月，但其中真正工作的

時間為兩個月，有一個月整天無所事事也不能從事其他打工，就會覺得與預期的報酬有落差，就乾脆好好的做事就好了，不用提心吊膽。我從事詐騙工作以來實際獲利大約一、兩百萬，但我要關六年，所以我覺得沒有賺很多。(B-2-9)

12.從事電信客服詐欺的心得感想

根據受訪者 B 之描述，有悔不當初，出獄後不再從事這種犯罪行為了。回顧當時會同意從事電信客服詐欺，主要原因有：欠債需求孔急、入門檻低、公司運用高檔物品利誘進而迷失自己，不認為詐騙是犯罪、不道德之行為。但在監禁期間回想發現，其實當時不要從事電信詐騙，找個正當工作腳踏實地的作，現在也把債還完了，也不會現在關在監獄中，以後出去還帶前科。

就是我覺得以後不會再從事這種事情了。我覺得當時我會加入詐騙工作，一來是自己沉迷，二來是因為公司利誘你，例如會安排觀光，讓你住好的飯店、吃高檔的餐廳，並借錢給你，讓你對他們產生依賴，才會離不開。……事後想想就覺得自己怎麼會去做這種事情，所以我以後再也不會去做了。自己想想當時其實就是欠債當下，慌亂了，不知所措，也不曉得應該靜下來想想如何因應、如何求助家人與家人討論，就急著尋求朋友協助，剛好朋友拋出從事詐騙工作可以快速賺錢還債，自己就著迷似的答應了。……其實我當時如果不去做詐騙，找一個正當的工作，一個月三、四萬，也是可以把債還完，只是時間拉長而已！但我現在回想起來，雖然債已經先還完了，但我浪費了六年在監獄，這樣算算，並沒有比較快還完債，人生上還帶了一個前科。(B-2-10)

（二）電信客服從事詐欺防制策略認知

1.從事電信客服詐欺被查獲的時間與原因

受訪者 B 稱，其從事兩次電信客服詐欺犯罪，第一次在 103 年，第二次在 107 至 108 年間，都是從事一年左右後被抓。而查獲的原因都是已經被公安部門追蹤、跟監一段時間後，可能採取跨境合作共同破獲或單獨查緝而破獲，而犯罪人竟都不知道已被警察鎖定。

分兩次，第一次 103 年在馬來西亞那一次，從事後約一年被抓，第二次 107 年至 108 年，也是從事一年左右後被抓。在馬來西亞那一次，因為我們都是租屋的，那一次係由馬來西亞警察、大陸公安和臺灣的國際刑警合作共同破獲，我也不知道他們如何知道我們租屋的地點，事後聽說是大陸公安先破獲一個大陸的詐騙集團後，他們把我們供出的；第二次被查獲，其實我們已經詐騙完畢、尾期了，已經沒有在打電話了，只是仍留在租屋處，就是有一個同事要去取款，剛好在租屋大廈的門口遇到警察，警察就進來搜索了。……第二次我真的不知道警察怎麼查獲的。但後來聽辦案的一個小隊長說，其實它們(公安)是在辦毒品案，我們裡面有一個好像跟它們追的毒品犯有聯絡或牽扯，後來在追他的時候才發現我們這個機房的，所以他們當時破門而入時不知道要抓詐騙集團。(B-3-1)

2.從事電信客服詐欺的風險程度與那些風險

受訪者 B 稱，因為她僅是客服的話務人員，不清楚從事電信客服詐欺的風險程度與具有哪些風險因素。

因為我是電信詐欺的話務人員，所以我不清從事網路詐欺之風險程度以及有哪些風險。(B-3-2)

3.從事電信客服詐欺犯罪的關鍵風險

受訪者 B 稱，因為她僅是客服的話務人員，不清楚從事電信客服詐欺的風險程度與具有哪些風險因素。

因為我是電信詐欺的話務人員，所以我不清從事網路詐欺之風險程度以及有哪些風險。(B-3-2)

4.從事電信客服從事詐欺的數位監控措施之認知

受訪者 B 稱，因為她僅是客服的話務人員，不清楚從事電信客服詐欺的數位監控措施以及數位監控強度。

因為我是電信詐欺的話務人員，所以我不清從事網路詐欺之數位監控程度以及數位監控強度。(B-3-3)

5.從事電信客服從事詐欺的規避措施

受訪者 B 稱，從事電信客服從事詐欺，有以下規避措施：(1)不用真實姓名，以綽號代替；(2)出國工作時不帶手機，即使帶手機也

不能開漫遊、沒有網路，已達不能使用手機的目的；(3)客服人員的護照會被收走，以免逃走或走漏風聲；(4)詐騙工作完畢返國後，直接出境不交談聯絡。一段時間後會有一位中間人聯絡哪一天之哪一個飯店旅館吃飯，以現金方式給予報酬，結束後，各自離散不連絡。領取之現金存放勿放在自己的帳號戶頭。

第一個，我們不會用真實的姓名，都會取一個綽號，第二個，在機房工作時，手機都不能帶，即使到國外，手機沒有開漫遊、沒有網路，事實上也無法打手機，……用這樣的方式規避被查緝的風險。從集團的角度觀之，也是要控制我們這些話務人員的行蹤，……甚至護照被收走的都有，如果有機會聯絡朋友或家人的話，他們就會想逃走。集團都是給現金，一拿到現金就是還債、放在媽媽處或朋友那邊，就是不會放在自己的帳戶名下。之前去馬來西亞那一次的做法就是，我們搭飛機回來後，大家各自離開回家，隔一段時間後公司會透過一個中間人打電話給我，約哪一天到哪一個飯店吃飯，然後到那一天的那一家飯店，公司就會把現金給我們，然後吃完飯後大家就離開，也不會聯絡。(B-3-4)

6.警察在查緝電信客服從事詐欺的能力與事前事後的預期落差

受訪者 B 稱，兩次被抓當時都不清楚是否被警察掌握或跟監了。另外，確實覺得有落差，因為出國從事詐騙錢，介紹的人說這種詐騙不容易被警察抓到，但幾乎一年多就被抓到了。感覺警察抓電信詐欺的能力滿好的。

不曉得耶。兩次被抓都不清楚如何被抓的。我覺得有落差耶，因為我去馬來西亞的時候，介紹我去的那個人曾經說過，這種詐騙集團不容易被警察抓到，因為之前被捕獲的案例就不多，但實際上一年多就被抓到了。兩次被抓的經驗後，我覺得警察抓詐欺犯罪的能力還滿好的。(B-3-5)

7.政府反詐騙宣導之預防策略之建議

受訪者 B 稱政府反詐騙宣導是有效的，就是現在接到電話只要提到身分證、財產凍結等關鍵字，民眾就會有警覺心了。此外，反詐騙預防策略之建議：(1)教育民眾於接到來電不明、有疑慮之電

話，應該要立即求證；(2)或是與家人或朋友討論，降低被害的風險與情境。當單一個人接獲來電不明之電話時，最容易陷入被騙的情境。

應該是有效啦！可以啦！就是現在只要提到你的身分證的事情，或二線提到你的財產會被凍結等關鍵字時，客戶就會有警覺心了，就不容易套出身分證字號來或請你們配合公安，這跟政府一直在宣導有關係。人們防詐的意識比以前好很多了。第一個預防策略就是要先求證(問你的客服人員編號與公司電話，再回打過去求證是真是假)，第二就是要跟家人或朋友討論，這樣我們就很難再繼續下去了。所以，我覺得單一個人的時候，比較容易陷入被騙的情境，聽從我們話務人員的指示，但如果是旁邊有人討論或說我再問問家人或朋友，這就不容易騙到手了(B-3-6)

8.政府網路詐欺預防策略之其他建議

受訪者 B 建議，鼓勵民眾多求證、多詢問家人、製發宣導小卡片以及民眾臨櫃轉帳時，行員多問一下、講一下與建議一下，都可以發揮預防效果。

就是在臨櫃服務時，行員多問一下、講一下與建議一下，都可以發揮預防效果。鼓勵民眾求證、請家人幫忙、製發宣傳小卡片，轉帳或匯款時行員多問幾句、多關心、多確認一下，都是預防網路詐欺的方法。若做到這樣，你會發現會被騙的人還是會被騙，好像與學歷沒有關係。(B-3-7)

第三節　網路詐欺加害者深度訪談結果之綜合分析

本節針對本研究所之招募之網路投資詐欺、網路購物詐欺以及電信客服詐欺三種型態之 5 位加害人所進行的深度訪談結果，從基本資料、從事詐欺行為之情形以及對於網路詐欺防制策略之認知三個角度，綜合分析當前網路詐欺加害者之犯罪特性、手法以及當前打擊網路詐欺犯罪之對策與精進建議。

一、網路詐欺加害者基本資料與犯罪情形分析

（一）基本資料分析

1.5 位加害人中，男性計有 3 位，女性計有 2 位，其中從事網路投資詐欺者 1 位（E 男）、從事網路購物詐欺者 3 位（A 男、C 女、D 男）、從事電信客服詐欺者 1 位（B 女)。

2.5 位加害人之年齡介於 26~42 歲間，處於青壯年時期。除 B 女離婚外，其餘均未婚，亦都沒有小孩。教育程度方面，高中畢肄業者 3 位（A 男、C 女和 D 男），另大學程度者有 2 位（B 女和 E 男）。渠等教育程度與資訊、電腦或網路等領域無關。

3.5 位加害人之家庭狀況，除 1 位（D 男）宣稱家境不錯外，其餘之原生家庭均為不健全家庭、隔代教養家庭，甚至有父母親離婚外，目前也監禁在監獄中(D 男)。

4.5 位求學過程中，除 C 女稱表現平平不想多談外，其餘大致上都有不喜讀書、在校表現與學習成就不佳之情況，特別是 A、D、E 等 3 位男性在國高中階段，均有翹課、逃學經驗，進而接觸偏差同儕與接觸毒品的行為。

（二）犯罪資料分析

1.5 位加害人從事與網路詐欺有關的時間不一，約 2 個月至 10 年間都有。

2.5 位加害人雖都觸犯刑法第 339 條之詐欺罪，但因為詐騙型態、被害人數、財損金額以及是否查得被害人以及是否有和解等因素不同，因此刑期介於 2 年至 13 年 5 月之間。

3.5 位加害人中僅 1 位初犯，其餘均為累在犯(具有犯罪前科，但不一定是詐欺前科)。

4.5 位加害人中，除 A 男與 D 男剛入監服刑期間尚短外，其餘 3 位已符合假釋陳報或已準備出獄的階段。

二、網路詐欺加害者從事網路詐欺情形之特性

以下針對三種不同的詐欺型態加害者之詐欺手法與情形，分別說明之。

（一）網路投資詐欺

1.從事網路投資詐欺的犯罪時間約 2 年，其從事此一犯罪行為的原因為左手肘因為車禍嚴重受傷，無法打球或從事勞力謀職，在朋友的介紹下，進入投資詐騙集團，担任小號與水軍的工作。

2.從未有網路詐欺被害的經驗。

3.其從事此一犯罪手法的關鍵因素在於手肘受傷，無法工作，缺錢的情況下，透過從小到大熟識朋友的介紹與引進，從事此一犯罪。因為錢賺得快、花得也快，過慣奢華的物慾生活，難以擺脫，只好一直持續下去。並無考慮其他網路詐欺犯罪型態。

4.網路投資詐欺犯罪是一個專精與分工的犯罪集團，這個集團區分為四大分工，老師號、助理號、小號與水軍，透過大陸資源方的招募，讓有興趣的股民進入他們所設立的微信群組，由老師介紹投資標的，小號與水軍的鼓吹、推波助瀾以及現身獲利說法，成功詐騙投資的大陸股民。

5.網路投資工作與時間十分冗長，雖然配合大陸股匯市的上班時間，亦有上下班的時間，但自己的專業，需花很多時間去投注心力與學習，例如看教戰手冊、實體會議、過往別人的手機內容/話術等以及與他人討論、請益。

6.網路投資詐欺集團鎖定的是大陸三線城市，主要是民眾的防詐意識尚未抬頭。此外，易受騙的族群為女性、年齡 35~50 歲間、已有一定收入或經濟能力或資產之人，因為渠等有投資獲利過，才會願意加入集團群組尋求獲利機會。

7.網路投資詐欺加害者分析，由於人性的貪婪，因此容易上鉤，但他們也會善用「放長線、釣大魚」的方式，先讓投資人初期獲得小利，之後再一舉坑殺其資金。

8.網路投資詐欺集團的詐騙時間要配合當地銀行及股匯市上下班的時間；實施的網路場域因為鎖定大陸投資客(不詐騙臺灣人為原則)因此使用微信作為詐騙平臺。

9.網路投資加害者宣稱，其獲利方式就是每賺一筆投資匯款進來實體帳戶(中國工商農業銀行)，即可獲利至少 5%。每一年的獲利至少 2 百至 3 百萬，可以說是非常好賺。大陸股民匯款進集團指定帳戶後，對岸會有集團其他夥伴負責將錢領出或轉出，以免帳戶遭查緝資金凍結。

10.加害者認為，在當時來看投報率超出預期，賺很多錢。但來得快、取得也快。換來兩年的監禁生活，得不償失。

11.從事網路投資詐欺的心得感想：手邊積蓄歸零、愧對家人與至親、往日好友未曾來接見與聯絡、女友分手。

（二）網路購物詐欺

1.加害者從事網路購物詐騙的時間約莫 2 個月至 3 年都有，甚有因為 Covid-19 期間本業倒閉，轉向從事網路直銷購物詐欺犯罪。換言之，渠等從事網路購物詐欺的原因：希望立即快速獲利、幫朋友的忙也順便賺錢以及本業倒閉轉行藉以營生。

2.除一位表示小時玩線上遊戲時，曾有被騙點數的經驗，對其有深遠影響外，其餘兩位均沒有網路詐騙經驗。

3.從事網路購物詐騙的關鍵因素在於想要獲利或賺錢營生，即使因為宣稱係要幫助朋友，但也是將原本的工作辭掉，投入網路購物詐欺行為。進一步觀察，除 1 位入門前完全沒有網路資訊之相關背景，其餘兩位都是熟悉網路環境，例如博弈遊戲或之前有網路直銷經驗。

4.網路購物詐欺犯罪，仍是有專業分工與負責內容，有人負責 po 商品照片(3C 商品照片、水產魚貨照片)、有人負責回覆顧客的留言並與其交流、有人負責查看人口帳戶是否被查封以及擔任車手領錢的工作。投注相當多的時間與精力在經營 FB。

5.受訪者認為，主要是透過累積的經驗、觀察以及集團成員的提點、話術，精進自己的技巧與方法。此外，聰明、腦筋要轉的快以及對於販售商品的專業知識，也要強化。

6.受訪者認為因為不識被害人，無從選擇被害人，但從被害人的特性分析，女性、大學生、年紀大的長者，比較容易被詐騙成功。此外，貪念與急性子(心急)，也是讓被害人容易陷入詐騙的情境與機會中。

7.網路購物詐騙的時間，完全是觀察被害者後配合調整。如果 FB 商城，都是 24 小時營業的，但可以隨時 po 新的產品。然而，涉及要接觸客戶的分工者，3C 產品者約下午至晚上為喜好時段；經營網路直銷者則為下午兩到四點、晚上八點以後為喜好時段。車手則無固定時段，原則上早上一早起床到晚上七、八點都是工作時間。

8.受訪者均認為 FB 是最佳的經營購物詐騙最佳的網路場域平臺，原因在於：FB 普及、會員人數多、商城/社團瀏覽不需過濾與設限、任何人都可以進出商城/社團。

9.受訪者對於詐騙獲利方式採取多元獲利方式的看法，亦即買線上博弈點數、透過 ATM 轉帳至指定人頭戶後提領現金以及面交現金或匯款等方式均可。

10.選擇網路購物詐欺為獲利方式的考量因素，在於入門門檻很低，不需要有太多的技術性就能賺得許多錢。例如經營 3C 購物詐騙平臺，不需要租地點與店面、不需要倉庫與實體 3C 商品，只要在 FB 創一個 3C 商城，po 一些網路下載的 3C 照片，予以編修，標上最低價，就會有人來詢問數量與價格，以所剩數量不多為由，買家很快就會轉帳匯錢至指定人頭帳戶，車手即可前往提領。而公園即可架設筆電經營 3C 商城，可謂低成本高投報。

11.投報與預期是否落差，端看當時與監禁的時間。在經營當時，被投報率吸引，一定認為值得、合乎預期；但在監獄監禁後，因為監禁時間冗長，甚至因為和解、律師費用等的付出，導致投報不如預期。

12.受訪者從事網路詐欺後的心得均不同，有的認為這是一條不值回票價的選擇，有的認為司法介入後會迫使他詐騙更多人，因為

要被判刑了；亦有的認為，完全是被害人的問題，如果他們不貪心、不輕信，如何會被詐騙成功。

（三）電信客服詐欺

1.受訪者稱自己從事電信客服詐騙行為已有 5 至 6 年歷史，第一次是 103 年犯案，第二次是 107 年至 108 年間犯案；從事的原因在於原先開店做生意，因為合約糾紛問題導致欠債，在缺錢孔急的情況下透過朋友的介紹，從事電信客服詐欺犯罪。

2.從事電信客服詐欺行業的關鍵因素是自己欠債、需求孔急，加上朋友鼓吹可以快速獲利償還欠債，進而從事此一犯罪型態。

3.電信客服詐欺犯罪也是集團分工的方式進行，分為一線、二線與三線，詐騙集團會利用自動電話系統撥打市內電話至家戶，宣稱有線電視因為未繳錢而於近日將被斷線，請住戶主動回撥客服電話。只要打進來客服人員者，即為一線人員，其目的就是要想方設法套出被害人之個資，例如姓名與身分證字號，接著以確實沒有收到月費的方式，請其到警察局報案或由一線客服轉接二線客服(佯稱是公安人員)。由於大陸幅員廣闊，報案地區不見得為住居地，因此許多被害人便宜行事便被轉至二線，二線人員佯稱欠繳會涉及刑法、凍結財產等，在被害人恐懼的情況下，應諾會馬上付錢，如果此時被害人願意配合、透過網銀或 ATM 匯款的方式盡速繳錢，此時二線客服馬上轉給三線客服，由其教授被害人如何轉帳，一旦金額轉入指定匯款帳戶，詐騙即成功。

4.由於電信詐欺犯罪都是赴國外犯罪，一次出去都是三個月，其中兩個月完全在工作，因此投注的時間與精力都很長，且會限制自由與對外通聯。為精進客服人員專業，公司會提供稿子給客服人員背，但因為每個客人的問題不見得都相同，所以臨場反應以及多與資深同事聊天、請益學習也很重要。臨場回應的說詞或話術，成功說服客戶後就要記下來，以後可以使用。

5.受訪者認為，早年能夠電信客服詐欺成功的關鍵因素就是接市內電話者於接聽電話時身旁有沒有其他人，若有，客人容易被提醒，就得放棄。但現在都改撥手機，身邊大部分都有人了，變成話術很重要。至於容易被詐騙的人口特性很難界定，男女都有，女性

稍多、各個年齡層也都有；至於心理特質部分，因為大陸公安很有威嚴、很有權力，可以凍結財產、製發逮捕令，因此客戶很願意聽從二線客服命令，轉至三線轉帳或匯款。

6.受訪者稱從事電信客服詐欺行為，並無偏好時段，都是由公司(集團)設定，一線人員上班時間比較早也比較早休息，早上八點到下午四點，但例假日也要上班。但二三線人員可能會工作比較晚，只要提款機還能轉帳，就得繼續上班。

7.受訪者稱從事電信就是運用電話，就是公司開發一種自動撥打電話號碼的軟體，並附有客服人員(一線客服)電話提供其回撥。所以電信詐騙不會在同一個場域或國家，甚至在一個國家打電話去詐騙另一個國家的民眾，以亂槍打鳥的方式，看看有沒有客戶上鉤、回撥，進而上當被騙。

8.受訪者稱電信客服人員分三層，每成交一筆轉帳匯款，一線客服獲利 5%、二線客服獲利 7%，三線客服因為要教授客戶如何使用臨櫃轉帳、網銀轉帳或 ATM 轉帳，所以獲得之紅利較高為 9%。

9.受訪者稱，選擇電信客服詐欺就是入門門檻較低，也希望早日獲利還債。

10.受訪者稱，剛開始時覺得投報率不錯，但晚近精算後發現，一期出境(到馬來西亞)詐騙三個月，獲利 30 萬，平均一個月 10 萬元，且被逮後還要關六年，跟當時不要從事電信客服詐欺、腳踏實地工作後累積至今所賺的收入差不多，就會覺得與預期的報酬有落差，覺得沒有賺很多。

11.根據受訪者之描述，有悔不當初之遺憾，出獄後不再從事這種犯罪行為了。回顧當時會同意從事電信客服詐欺，主要原因有：欠債需求孔急、入門檻低、公司運用高檔物品利誘進而迷失自己，不認為詐騙是犯罪、不道德之行為。

三、對於網路詐欺防制策略之認知

以下針對三種不同的詐欺型態受訪者之防制策略認知，分別說明之。

（一）網路投資詐欺

1.本案為警查獲的原因是案外案，是因為警察受理民宅現場打架、械鬥事宜，意外查獲本網路投資詐騙集團。

2.加害者認為從事網路詐欺的風險在於是否詐騙臺灣人，詐騙臺灣人風險高，因為臺灣人的防詐意識較高，相較於此，大陸民眾，特別是三線城市民眾，防詐意識較比較低。此外，電話卡 SIM 卡以及基地臺等容易被定位的工具與設施，也是是否容易被警察查獲的重要關鍵。此外，集團成員是否集體行動也是是否容易遭警查獲的風險，人多容易引起街頭鄰坊側目。

3.臺灣警察數位監控的能力很強，在臺灣做網路投資詐欺，一定會為警查獲。

4.從事網路投資詐欺的規避措施：在臺灣設平臺、詐騙大陸民眾，因為大陸公安無法查緝臺灣發生的基地臺；集團要層層分工、形成斷點、成員不要聯絡。

5.反詐騙宣導預防措施之建議: (1)政府應該正視與杜絕網路上販賣人頭帳戶的問題；(2)持續宣導以提高臺灣民眾防詐意識；(3)防詐宣導應該根據不同的詐欺犯罪類型予以不同的宣導方式；(4)持續強化警察與銀行行員第一時間阻斷民眾轉帳匯款的合作模式。

（二）網路購物詐欺

1.受訪者從事網路購物詐欺被查獲的時間不一，短則兩個月，長則一年，查獲原因都是與被害人到派出所報警後，被警察積極查獲有關。

2.受訪者認為不太需要擔心被逮風險，原因在於：笨的被害人的、不要在網路被警察監控以及質疑政府與警察打擊網路犯罪的能力。

3.受訪者認為從事網路購物詐騙的關鍵風險在於警察在網路查緝與監控的能力很強，所以不要正面迎戰警察。

4.受訪者認為一些社群媒體的數位監控措施，非常鬆散、沒有特別強，即使有會員向 FB 反映有人使用帳號行騙，他依然沒有被封鎖。

5.受訪者認為他們喜歡使用 FB 就是因為不需要採取任何規避措施，主要是 FB 的帳號容易換帳申請、辦電子信箱很容易；至於獲利方式主要以：傳送線上博弈遊戲點數序號、網路轉帳指定人口帳戶或是轉至女友或其他人的帳戶，以規避查緝即可。

6.受訪者仍認為臺灣警察查緝網路購物犯罪的能力是很強的，也認為遲早會被抓，因此利用尚未抓到的時間，能騙多少就騙多少。僅有一位受訪者認為臺灣警察在查獲網路犯罪的能力，持否定態度。

7.受訪者認為，當前政府反詐騙宣導之預防策略都沒有用，主要是人性貪念、貪小便宜的問題，民眾不會認真看待反詐騙宣傳。這些反詐騙宣傳只是表面功夫，無法解決問題的根源。

8.有兩位受訪者認為既然是人性貪婪的問題，任何反詐騙預防策略都沒有效；但有一位受訪者則建議政府仍是要多多推廣 165 專線，讓民眾有求證、詢問的機會，減少被害風險。

（三）電信客服詐欺

1.受訪者稱，其從事兩次電信客服詐欺犯罪，都是從事一年左右後被抓。而查獲的原因都是已經被公安部門追蹤、跟監一段時間後，可能採取跨境合作共同破獲或單獨查緝而破獲，而犯罪人竟都不知道已被警察鎖定

2.受訪者稱，因為她僅是客服的話務人員，不清楚從事電信客服詐欺的風險程度與具有哪些風險因素。

3.受訪者稱，因為她僅是客服的話務人員，不清楚從事電信客服詐欺的數位監控措施以及數位監控強度。

4.受訪者稱，從事電信客服從事詐欺，有以下規避措施：(1)不用真實姓名，以綽號代替；(2)出國工作時不帶手機，即使帶手機也不能開漫遊、沒有網路，已達不能使用手機的目的；(3)客服人員的護照會被收走，以免逃走或走漏風聲；(4)詐騙工作完畢返國後，直接出境不交談聯絡。一段時間後會有一位中間人聯絡哪一天之哪一個飯店旅館吃飯，以現金方式給予報酬，結束後，各自離散不連絡。領取之現金存放勿放在自己的帳號戶頭。

5.受訪者稱，兩次被抓當時都不清楚是否被警察掌握或跟監了。另外，確實覺得有落差，因為出國從事詐騙錢，介紹的人說這種詐騙不容易被警察抓到，但幾乎一年多就被抓到了。感覺警察抓電信詐欺的能力滿好的。

6.受訪者稱政府反詐騙宣導是有效的，就是現在接到電話只要提到身分證、財產凍結等關鍵字，民眾就會有警覺心了。此外，反詐騙預防策略之建議：(1)教育民眾於接到來電不明、有疑慮之電話，應該要立即求證；(2)或是與家人或朋友討論，降低被害的風險與情境。當單一個人接獲來電不明之電話時，最容易陷入被騙的情境。

7.受訪者建議，鼓勵民眾多求證、多詢問家人、製發宣導小卡片以及民眾臨櫃轉帳時，行員多問一下、講一下與建議一下，都可以發揮預防效果。

第四節　網路詐欺被害經驗與加害者犯罪手法之比較分析

綜整網路詐欺被害者之調查結果分析與網路詐欺加害者深度訪談之結果分析，本研究嘗試比較被害者之被害經驗與特性；以及加害者之犯罪手法與描述，進行比較分析。以下僅針對被害者與加害者在一些共同性研究問題上之統計結果與經驗描述，區分為相同點與相異點，進行分析。

一、相同點

綜合網路詐欺被害問卷調查結果與網路詐欺加害者深度訪談之資料，針對以下共同問題進行分析後，得到以下共同一致性的結果：

1.網路使用特性分析，被害人與加害人都是高度依賴使用網路的網民。例如有 37%的受訪者宣稱每天上網時數超過 6 小時以上，而且接觸網路的時間 10 年以上者占 75%（詳表 3-2-2）；而在受訪的 5 為加害者中均宣稱每日上網時間很長，接觸網路的時間也很久，甚至有一位從小學時期就開始上網(詳本章第二節、一、(四)網路生活型態)。可謂被害人與加害人都是高度依賴網路的族群。

2.網路平臺使用分析，被害人與加害人都是使用網路上的社群軟體、購物網站以及從事線上遊戲作為網路生活的主要型態。例如受訪的民眾中，有 93%使用社群軟體、78%使用網路購物、43%從事線上遊戲（詳圖 3-2-1）；而加害人也宣稱每日上網的目的就是瀏覽社群媒體聊天（FB、Line、微信等)、購買商品與玩遊戲(含線上賭博性電玩）(詳本章第二節、一、(四)網路生活型態)。

3.網路被害經驗分析，被害交易方式主要以網路 ATM 轉帳、超商付款以及購買遊戲點數支付為前三大交易方式（詳表 3-3-1）；再者，從加害者角度觀之，不同的網路詐騙型態會有不同的交易方式，但以目前臺灣網路詐欺案量較多的網路購物詐欺為例，其交易方式主要以購買線上博弈點數、透過 ATM 轉帳以及面交現金或匯款方式(詳本章第二節、三、(四)、9 從事網路詐欺獲利方式)，大致相同。

4.被/加害人互動經驗分析，雖然研究顯示，無論是被害人的調查或加害人的描述，在網路詐欺被害案件中，兩者均不認識；然而，透過網路平臺的互動、交流，確實能讓網路詐欺案件成功。例如網路購物是目前最流行的網路活動之一，詐騙者可以偽造商品平臺招攬被害者，或者利用顧客留言，進一步主動與被害者聯絡，進而詐騙成功（詳圖 3-3-4）；而根據加害人的訪談意見，網路購物詐騙行為，因為不認識被害人，所以無從選擇，但無論是主動到對方的 FB 留言或者在 FB 留言後被動的回覆被害人，都可以詐騙被害人成功，特別是大學生以及女性(詳本章第二節、三、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質)。

5.網路詐欺被害察覺分析，從被害人調查數據得知，高達 79.8%的被害人自稱是自己察覺或驚覺到自己已經被害，而從加害人的訪談得知，確實是加害人透過匯款轉帳方式，確認金額已經進入指定人頭帳戶後，從 FB 將加害人封鎖或拒絕回電、回應其詢問時，被害人始察覺自己已遭騙後，有人可能會報警(詳本章第二節、三、(一)、7 從事網路詐欺喜好時段)。

6.網路詐欺被害原因分析，根據被害人問卷調查發現，前三名依序為過於相信（45%）、自身疏忽（38.3%)以及貪小便宜（34.8%）（詳圖 3-3-5）；另從加害者訪談角度觀之，被害人的貪小便宜、貪得無厭才是主要被騙成功的因素，其次才是急，心急而誤判是否是詐騙行為(詳本章第二節、二、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質，以及三、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質)。

7.網路詐欺實體監控分析，根據被害人問卷調查發現，家人對於被害者的關心或提醒確實能有效地降低其成為詐欺被害人的風險（詳表 3-4-5）；無獨有偶，電信客服詐欺犯罪加害人稱：早年電信客服可以詐欺成功的關鍵因素，即為室內電話使用者接聽電話時身旁有無其他人，如果沒有，則成功機會大增；如果有，接電話者容易被提醒，就不容易成功。現行使用手機，接電話的周遭幾乎都有人，旁邊有人提醒就不容易成功，完全靠客服的話術。(詳本章第二

節、四、(一)、6.電信客服詐欺被害人的關鍵因素與人口特性或心理特質)。

8.加/被害人網路聊天活動分析，根據問卷調查發現，在網路上與陌生人聊天的活動與其被害的關聯性最強（詳表 3-4-5）；無獨有偶，在加害人的訪談內容中也發現，加害者的話術扮演重要的角色，例如在網路投資詐欺行為中，女性喜歡用微信打電話聯絡，男性則喜歡用微信簡訊(Texts)聯絡，因此女性被詐騙成功的機會較高(詳本章第二節、二、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質)。而電信客服亦有類似的情況，畢竟這些犯罪人都是訓練有素、平時就一直在提升自己的話術，當有機會以打電話方式交談、溝通時，就很容易突破被害人的心防，詐騙成功。

二、相異點

綜合網路詐欺被害問卷調查結果與網路詐欺加害者深度訪談之資料，針對以下共同問題進行分析後，得到以下相異性的結果：

1.網路詐欺被害人口特性分析，根據被害人問卷調查發現，男性、年紀較小(約 40 歲以下)、月收入約未滿 4 萬元者、大專程度以下者以及學生、從事網路資訊工作、實體交通物流工作以及製造業者，顯著地有較高的網路詐欺被害經驗（詳圖 3-4-1），且城鄉差距或區域特性與網路詐欺被害無顯著關聯性（詳表 3-4-2）；然而，根據加害者的觀察，發現年齡介於 35 至 50 歲間有一定財富累積者、女性(容易被話術詐騙成功)、大學生(購買物品希望貪便宜)、老年人(希望貪便宜)以及都市化程度不高者(例如大陸的三線城市)，均是容易遭網路投資與網路購物詐欺的對象(詳本章第二節、二、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質，以及三、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質)。然而遭電信客服的被害對象則無明顯不同，但區域條件仍是會受到影響(詳本章第二節、四、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質)。

2.網路詐騙後是否報案分析，根據被害人問卷調查分析，近 7 成的被害者選擇不去報案（詳表 3-2-3）；此一部分涉及網路詐騙型態的不同，亦有不同的情況，需分開討論。如果是網路投資詐騙，財損情形非常嚴重，但報案的情況確實比較少，主要原因在於有些被

害人會認同詐騙集團的說法，投資失利，不認為是被詐騙(詳本章第二節、二、(一)、6 選擇被害人的關鍵因素與人口特性或心理特質)；然而，網路購物詐騙的加害者則表示，被害人幾乎都會去報案，因為被害人報案後，他們的人頭帳戶就會被警察認為是警示帳戶，要求銀行或郵局關閉，因此他們必須要經常檢查他們的人頭帳戶是否已經被關閉(詳本章第二節、四、(一)、9.從事網路詐欺的獲利方式)。

3.警察偵辦網路詐欺犯罪之能力分析，從網路被害人之調查發現，這些被害人未報案的原因中，排名第四、有 27%的受訪者認為報警沒有用，換言之，被害人恐質疑警方的破案能力與效率（詳圖 3-3-6）；然而，根據受訪者的說法，他們均認同臺灣警察在網路犯罪方面的查緝與偵辦能力是很厲害的，甚至認為他們從事網路詐欺犯罪最後都會被警察追查、查緝到案，只是時間的早晚而已，因此盡可能的能撈多少就撈多少(詳本章第二節、二、(二)、3；三、(二)、3.以及四、(二)、3.從事網路詐欺的關鍵風險)。

第五章　網路詐欺被害調查之政策焦點團體座談分析

第一節　政策焦點團體座談之規劃與實施

一、政策焦點團體座談之規劃

本研究根據本研究目的所完成之各國網路詐欺被害調查與相關因素、網路詐欺被害問卷調查結果分析以及網路詐欺犯罪加害人深度訪談分析後，規劃於 2023 年 8 月 9 日下午 2 點假中央警察大學研究大樓 232 室召開本研究第二場政策焦點團體座談，並於事先將本研究前揭之初步研究結果與訪談大綱，提供給與會之學者專家，以利提供渠等學術與實務經驗，提供寶貴意見與建議，以優化或策進當前政府打擊與防制網路詐欺犯罪之政策作為。

本研究第二次政策焦點團體座談所邀請的學者專家，考量網路犯罪偵查實務、資安鑑識、網路偵辦與查緝實務以及網路犯罪理論等面向，邀請 5 位與會，其相關背景說明如表 5-1-1。

表 5-1-1　本研究政策焦點團體座談之學者專家簡介

場次	領域專長	代碼	服務單位	討論主題
第 2 場次	智產、電腦與金融犯罪訴訟專長；資安鑑識與調查	F5	律師事務所	針對本研究初步研究成果之分析，擬定訪談大綱，進行意見交流，提供建議供參。
	加密貨幣交易金流分析與資安鑑識	F6	OO 金融科技公司執行長	
	資訊系統規劃、數位鑑識、網路犯罪調查及資安治理	F7	OO 國際商業銀行資安長	
	科技犯罪偵查技術及管理、網路鑑識	F8	OO 大學資管系助理教授	
	網路犯罪偵查與實務	F9	警察局 OO 股長	

二、政策焦點團體座談之實施

本研究於規劃邀請前揭學者專家後，遂調查學者專家與本研究團隊成員可以共同與會的時間，經調查後訂於 112 年 8 月 9 日下午 2 點假中央警察大學研究大樓 232 教室進行第二次政策焦點團體座談之進行。而本研究團隊與會人員計有主持人賴擁連教授、協同主持人蔡田木教授、研究顧問許春金教授以及研究助理蔡文瑜與會。而焦點團體座談之實施係針對以下之訪談大綱逐一進行(此次焦點團體座談之知情同意書與深度訪談大綱，詳附錄十一)，內容包含：

7. 從各國網路詐欺被害調查之管道與機制得知，有無值得借鏡之處？
8. 網路詐欺犯罪有無資訊/資安/理工等相關理論可解釋其行為或模式?
9. 從網路詐欺被害經驗問卷調查結果得知，被害人之心理特質與網路生活型態與其網路被害息息相關，請問被害人可以如何防範網路詐欺被害？
10. 從網路詐欺犯罪加害者的深訪結果得知，執法部門可以從何處強化，以降低渠等犯案動機或減少被害人被詐機會？
11. 從網路詐欺犯罪被害者與加害者之心理特質與日常生活之相同與相異點分析，可否提供相關的抗制網路詐欺犯罪對策？
12. 晚近新加坡/中國等華人社會對於網路詐欺犯罪之抗制策略，是否有參採之處?
13. 當前政府打擊詐欺犯罪之策略，是否應該針對不同類型(例如購物、投資與電信客服……)，提供不同的策略方式？
14. 行政院於今年 5 月成立專責之打詐辦公室，以強化當前打詐的編制，迄今有無相關成效？

本場次焦點團體座談實施的時間約莫兩個半小時，並於本研究團隊製作逐字稿後，用電子郵件方式寄回給與會學者專家確認用字遣詞與表達意旨無誤後，始進行以下內容分析。

第二節　政策焦點團體座談之內容分析

以下針對政策焦點團體座談之結果(本焦點團體座談之逐字稿，詳附錄十二)，分述如下：

一、從各國網路詐欺被害調查之管道與機制得知，有無值得借鏡之處？

F5：

我之前當檢察官的時候，曾經參加美國檢察官協會的研習，和其他國家檢察官就網路犯罪議題交換意見，韓國的檢察官告訴我他們很常使用 24/7 Cybercrime Network[12]，此機制就是透過國際協議，由各國司法警察協助盡快的保全證據。因為若經過司法互助的方式取得相關數位證據的內容，曠日廢時、徒勞無功。韓國的 24/7 機制是在最高檢察署，有網路犯罪專責機構處理，透過 24/7 機制請其他國家保全證據，後續再調資料。

我們現在遇到的網路詐欺，只要遇到跨國 IP 或是加密貨幣金流的情況，很難去偵查。跨國之間的合作，不只是檢察官層級的合作，更需要警政的互助，因為警察最有機會在第一線扣押證據。

我感覺警政跟其他國家的連結其實比檢察官高好多，比檢察官正式的司法互助管道更快捷，是以回歸到警察機關管道，在執行上有益於跨境司法互助政策。

F6：

我比較站在產業的立場去看，像我一開始接觸區塊鏈，是因為進到加密貨幣的交易所工作。但業者不重視回覆 165 的投單，因為並無強制力；再加上投單平臺蠻不友善的，其實業者沒有辦法收到通知。所以警方跟國內業者之間的聯繫，就有許多阻礙。

這兩、三年，我們也跟國際合作，例如挪威有一間公司，可以讓檢察官、律師入股當合夥人，他們在挪威處理加密貨幣的案件。我很好奇他們對政府的幫助，他說挪威的警察跟臺灣某種程度也蠻像的，缺乏對科技偵查的認識。可是他們很願意跟產業合作，挪威政府所缺乏的，則尋求產業合作技術，也很願意跨國合作。

我的重點在跟產業合作，政府會省掉很多的成本。以區塊鏈、

[12] G7 24/7 Cybercrime Network 系統成立於 1997 年 12 月，此乃因應日益興盛的跨國通訊而建立，並致力於打擊網路犯罪，其手段是「保存證據，並透過法制化之管道提供證據，以利後續偵查進行」，據此，參加國可以在各國設立聯絡窗口(contact points)，至 2014 年參與之會員國共達 70 國。詳見戎婕(2018)，有關打擊網路犯罪法制與國際合作之研究。桃園地方檢察署出國報告。

加密貨幣而言，不管是交易所或錢包廠商都可以幫我們有效的防堵。已經不只是國與國之間，而是公司對公司、產業對產業，需要大家有意識建立防護網。另外，國外還有在推專家鑑定，這個也可以彌補警方在科技偵查上的不足。臺灣的詐欺是全世界數一數二的厲害，我覺得政府的司法、行政要想辦法統一，在裁處方面有洗錢防制法、虛擬通貨辦法等，卻沒辦法有效的落實，所以在國際合作之前，內部要先整合。

F7：

第一，建議針對網路犯罪或是詐欺等，國際合作跟資訊共享是很重要的。

第二個在網路技術或網路知識的教育，讓偵查人員有這方面的思維或知識是必要的。現在遇到跳板的問題，或使用更高深網路技術，比如說查到國外的 IP，偵查員就會直覺研判人在國外，但是實際的使用者是在國內。刑事局這幾年一直做科偵教育訓練課程，讓偵查員理解網路原理及科技偵查這非常重要。

3.我建議警務駐外聯絡官的數量，能夠再多一些人，當成我們國際合作的重要窗口。例如東歐國家、非洲、南亞等，在各地區的密度都能夠再增多警務秘書

F8：

就偵查面來說，針對一些科技偵查手段，像是設備端通訊監察，德、英、美、法、奧地利及西班牙等國均已立法，針對個資外洩防護、特定網路銀行使用或 OTT 通訊服務資料無法調取的部分，英國及澳洲也立法保留網際網路流量紀錄；而針對約束社群媒體業者行為(例如違法內容通報及處理機制)部分，歐盟執委會於 2022 年也通過數位服務法。這些都是國內法制尚未完備之處。

我個人看法是，其實外國有很多制度，那我們政府有仿照歐盟提出「數位中介服務法（以下稱中介法）」，但被外界說政府要監控社群媒體，然後無法取得社會共識。為什麼會提中介法，我自己常思考怎麼樣讓案件量變少，方法之一就是讓被害人看到這個東西是

詐騙，165 針對假投資網站做警示頁面，但目前警示頁面沒有足夠明確的法律依據，倘若中介法通過，就會有較明確的依據。再者能否使用扣押裁定，技術上來說新生成網域的速度非常快，10 分鐘左右就能完成，而扣押裁定可能要耗時數日，這時詐騙集團已生成不知道多少個域名了，真的是緩不濟急，這不僅是沒有效率的問題，而是根本無法達到實際的作用。又如最近最高法院宣判無效的 M 化車使用，以及之前 108 年通保法草案所列的網路流量紀錄等科偵手段法制尚待社會達成共識立法通過。

而詐欺犯罪偵查時常遇到斷點，無法繼續下去，若我們有像英國的調查權力法案（Investigatory Powers Act 2016），適當保留網際網路流量紀錄，在某些案件可能可再溯源，但不可諱言其建置成本非常驚人。若嫌犯使用跳板，可能這方法又失效，所以還要更仔細的政策評估及持續相關技術研究；另一方面，我們現在跟社群媒體等網路平臺調閱資料，也很難有把握一定會得到回覆，這也是我們思考保留網際網路流量紀錄的一項目的。

F9：

我以聯絡官的關係來做一個說明，以前曾以網路偵查技術查到 80 幾個詐欺機房的 IP，分發給各地的警察聯絡官查緝。結果回覆最快的就是泰國，因為有良好的 P2P 交流。其他國家就很可惜，最後石沉大海。不然泰國有的話，其他國家應該也有。

165 的招牌雖然很大，但實際上是內政部警政署刑事警察局打擊詐騙犯罪中心底下的一個股。在跟其他部會協調的時候，除非獲得行政院支持，不然很難說動其他行政機關。以電信詐騙來說，「+」是國際來電現在已是耳熟能詳。但在 165 成立之初（94、95 年），因為國際交換機的規則沒有統一，所以等到行政院成立打詐國家隊，NCC 一聲令下，所有電信業者都統一了。主管機關的態度很重要，他對自己目的事業才有箝制、管理能力。像刑事局這樣的四級機關要做這個事情，其實相當的辛苦！

二、網路詐欺犯罪有無資訊/資安/理工等相關理論可解釋其行為或模式?

F5：

我感覺詐欺案件蠻類型化的，而且變換速度很快。每次案件發生之後，都是在地的派出所受理報案，地方員警不見得馬上就知道案子的關鍵所在，常讓被害人誤解警方辦案不力。

如果我們可以給專責偵辦單位比較多的資源，這樣可以從案件當中快速學習、快速迭代，可能會比較有幫助。調閱資料也需要比較規格化的方式，以便盡快反應。

現在詐欺其實都是有流行性的，模式出來之後會流行一小段時間。比如說之前 Telegram 流行大概 2、3 個月，模式會一直變。但我們可以從第一線遇到的案件，確認其模式後，在短時間內推出對應的機制，就像防毒軟體更新病毒碼。

F6：

因為我最近比較常在做模式分析，網路詐欺更容易形成模式，因為係針對不特定多數人。甚至最近發現加密貨幣的詐欺出現程式化，用程式轉幣。其實這本來就是電腦的東西，應該用科技去解決。如果今天可以快速的去分析現在的手法，尤其在詐欺，電腦只是操作工具，若有辦法透過電腦或是手機找到 key 私鑰，現場才能扣押鏈上的資產。所以現在詐騙集團這麼喜歡用加密貨幣，因為資產容易轉移。如果今天可以發展這些軟體，國外跟臺灣都能做到，一個 USB 插進手機或電腦，快速的找出相關需要的東西，這個也是結合科技的問題。

在第一線派出所或分局受理到相關案件，其實就可以知道這個月比較流行哪一塊，那我們就會馬上提醒其他單位可能會遇到什麼案件。可是這個 pattern 就是變動很快，可能 1、2 個月後就會變不同。所以如果在第一線有辦法掌握 pattern 的話，在防堵上也比較能對症下藥。

我很喜歡 Durkheim 的理論，現在的社會也在轉變期，Durkheim 處於工業時代轉型期，我們現在是元宇宙時代轉型期，人性的貪

婪，再加上社會控制力不足。面對跨國、跨科技、跨元宇宙，不只我們國家，像美國、中國等大國們也在面臨監管科技快速變遷的問題。

F7：

很多網路詐騙加害者基本上考量的是這個犯罪行為能否從中得到期望的利益，犯罪也要成本（買本子、找車手、買個資），只要符合期待的利益，他就會去做。所以將加害者的成本墊高，自然而然他就不會想做，類似犯罪學的理性選擇理論。

每一個案件都有一個態樣，裡面一定會有一個脆弱點，所以我針對這個脆弱點去打擊，就可以讓該犯罪模式消滅。比如過去惡意簡訊造成電信小額支付詐騙，可以分析惡意程式回報的中繼站 IP 位置，再請電信業者把中繼站封鎖，被害人接到這類簡訊手機被植入木馬，但因木馬程式無法連回中繼站，這類案件就不會再有。找出 pattern 利害關係點，打蛇打七寸。

許春金教授：

F7 前段所言是理性選擇理論；後段則是犯罪歷程理論。

F8：

網路詐欺犯罪其實就是利用網路跨境運作易於製造犯罪偵查斷點之特性，使其可以用一個低成本高獲利且難以被國內執法機關偵查的方式達到犯罪的目的。

F9：

從 111 年的防疫紓困貸款的詐騙開始，我們觀察到 5 種簡訊詐騙的變形，第一種是透過國內簡訊代發商，我們開始砍他們的發送門號，砍到簡訊發送商受不了，他們自己開始過濾。這個效果就是斷掉他的犯罪工具，但是很快的就發生轉型。第二種改從國外的電話進來，我們在打詐行動綱領的護持之下，透過一類電信公司把這些全部擋掉；再用科技的方式過濾連結。半年之內他又轉型，第三

改成用 iMessage 發送，轉進網路裡。iMessage 畢竟是特定行動裝置使用的溝通訊息軟體，詐騙集團為了擴大詐騙簡訊的發送範圍，出現第四種以偽冒基地臺發送簡訊。後來偽冒基地臺被警方查獲後，又出現第五種植入木馬程式的手法，透過惡意連結讓手機中木馬變殭屍，一直發送詐騙簡訊。所以 6、7 個月的時間內，經歷 5 種變形。但是我們也是兵來將擋、水來土掩。

搭配科偵專業進而提供偵查方向給外勤大隊來查緝，這是很好的正向回饋。業者其實自己都搞不清楚發生什麼問題，臺灣的警察真的很努力，而且素質很好，我們發現問題後是發公文給業者，業者才承認有這個問題。也呼應 F7 所講的狀況，就是要找到他詐騙集團的弱點，才能有效防制。

三、從網路詐欺被害經驗問卷調查結果得知，被害人之心理特質與網路生活型態與其網路被害息息相關，請問被害人可以如何防範網路詐欺被害？

F5：

詐欺其實涉及到人性，只要是人就有被詐騙的可能。大家常待在網路上，就容易在網路的渠道被詐騙。人最多的地方，就有最多的詐騙。不是只有老阿嬤容易被詐騙，也有高知識分子被詐騙，每一個人都可能會被詐騙。也很感謝 165，我有看到一些投資詐騙，網址點過去之後都被封住了。主要還是因為網路生活的關係，在網路上的時間多，就容易被騙。

F6：

我發現被害人有個特質，他在陳述被害的過程，沒有任何自省之意，檢討政府、檢討警方不夠力，但不會自我檢討在被害過程中，自己應該要負什麼責任，這種人很容易成為二次被害人。現在警方有清查潛在被害人的政策，結果通知潛在被害人的時候，財損 3、4 千萬卻拒絕報案。被害人選擇不面對的心態，甚至有跟警方堅持自己沒被騙，只是還沒領出來而已，中立化自己現在的狀態，自欺欺人。

2018 年的三方詐騙、假援交案件，被害人大概 72 小時就會有反應、去報案了；最近投資詐騙被害人的反應時間，大概是 48 天，甚至有 3 到 6 個月。被害人其實很孤單，跟過去的被害人不太一樣，他會重複被詐騙。呈現 M 型化的概念，會被詐騙的人，就是會一直被騙。

F8：

這個部分相當有趣，政府投入大量預算及人力物力宣導，為何還是成效不彰，建議警政署可以考慮從受理端增加一個問題，是否曾經看過這種類型的反詐騙宣導，反向檢閱宣導效能；另一方面，整體臺灣教育著重智商教育，鮮少有對於個人財務及風險的教育，舉例來說，許多人不了解虛擬貨幣(嚴格來說他不是貨幣，而是一種商品，就像是虛擬遊戲點數一樣)，但仍然會投入大筆資金，這就是很大的問題。

針對第三題的部分，投資詐騙跟一般網拍詐騙完全不一樣。投資詐騙比較長期；網拍可能是匯款一轉出去，就瞬間發現。這邊可能要區分一下，投資詐騙的狀態比較長期、財損也特別高，其防制策略也比較特別，要考慮用其他的方式來介入。

剛才提及的假投資網站的警語頁面，我們從網路上的外匯平臺討論區如外匯天眼等都會看到被害人因為看到警語頁面而警覺被詐騙，這些作為就會讓財損降低。因為被害人已經在那個情境中，其實很難百分之百保證不會被騙，但是能把他的財損縮減，是政府考慮持續的方向。

F9：

165 每天有上千位民眾進線，打電話來不一定報案，可能是諮詢，也有一部分被害人不願意報案。大概有六成的假投資案件被害人會在半個月以內報案；但是巨額財損的被害人，六成以上平均是超過兩個半月。呼應 F6 講的狀況，金額五十萬以下，大多數的被害人可能兩個禮拜就報案；巨額財損的被害人，大概平均要兩個半月以上。

再回到說如何防範網路詐騙，雲林縣警察局林故廷局長時任刑事局主任秘書，曾經派行為科學股的同事研究如何在被詐騙的當下提醒被害人。但被騙的過程中，如果沒人知道，沒辦法有任何介入的機制。他們沒有報案，警察不會知道，可能只有銀行知道。到底銀行要如何介入，或是即時提醒他被騙了，而不是等到他自己終於願意面對時再來報案。

四、從網路詐欺犯罪加害者的深訪結果得知，執法部門可以從何處強化，以降低渠等犯案動機或減少被害人被詐機會？

F5：

我比較關注平臺業者的責任，在投廣告的時候，好像沒有經過審核的感覺。不管是 YT 或 Facebook，有些粉專成立不到幾天，甚至可能只有 4 個人按讚而已，就可以偽裝成名人去詐騙。詐騙就是看哪邊有流量，從最傳統的電話詐騙，然後到網路詐騙，都跟流量有關係，預防的話，還是要從流量來防範。

F7：

我個人關切的是，執法單位的這個執法能量夠不夠強。我們在暴力犯罪可能馬上抓到犯嫌；但在網路犯罪，不見得可以找到主嫌。所以犯罪者都往網路發展，像實體賭博轉到線上賭博；電話詐欺轉到網路詐欺。

另外，執法機關移送犯嫌之後，其處罰的力道夠不夠強、有無嚇阻性，像過去很多詐欺被告的刑度都不高，大概都兩年以下有期徒刑，所以假釋後很容易再犯。因為獲利跟受到處罰，不成正比。其實詐騙的團員很怕強制工作的處罰，可惜已被廢止。我們對於犯罪者的處罰，是不是能夠構成嚇阻性，可能是我們要再思考的。

F8：

執法部門目前針對假投資網站有做警語頁面，我們可以在像是外匯天眼這種反詐欺投資平臺看到許多被害人因為看到這個頁面而驚覺受詐，但這些網站不同域名眾多且更新迅速，建議可比照 iWIN

建構快速通報下架機制，同時結合 165 的大量被害情資，以 AI 智能化的方式自動化找出新生成的域名加以停止解析(現在是使用大量人力去辨識，速度緩不濟急，且無法判斷停止解析是否確實生效)。但問題來了，我們目前停止解析的法律依據應該要重新思考立法明確化，而且處理速度要快速，不然根本跟不上詐騙集團新生成的域名的速度。

另外一個技術上的問題是，停止解析技術上僅能涵蓋約 7 成網路服務接取用戶，假如他使用其他的 DNS 則無法涵蓋，這時該如何處理是一個大問題，我曾有機會與亞太網路中心 APNIC 的執法成員談過這個問題，我問他說能否有機會透過國際合作，從全球的 DNS 來處理(意味著我們提供涉詐域名情資，通報整個 APNIC)，他告訴我是可以考慮談看看，但這種國際談判，假如你這個國家沒有可利用價值，去談的時候，他們為什麼要配合我們？個人淺見是我們可以以 AI 智能化的方式自動化找出新生成的域名相關情資，為全球跨境電子商務產業(例如 Amazon、日本樂天等)做出貢獻，而就我朋友在相關產業服務的經驗來說，這些跨境電商認為自動化找出新生成的域名相關情資非常重要，他們甚至有花錢訂閱相關服務，但有時我們「人工智慧」找的方式也發現他們沒看到的偽冒網域，我們資通訊產業發達，這個也是我們產業的一個機會。

F9：

我們有遇過一個蠻厲害的高學歷犯嫌，自認犯罪手法無懈可擊，最後是躲不過自己的道德譴責，才交代他怎麼做，包含怎麼唬過檢警，他自白是被利益驅動。有很多的加害人不認為他在犯罪，例如架設假投資詐騙網站的工程師，因為他做好網站是給詐騙機房使用；而打電話的詐騙機房成員說，錢不是他收的；車手集團負責把錢領出來，再上繳；處理金流的，他就說自己只拿月薪，負責轉帳工作。詐騙集團也狡辯，是被害人自己來找我的，網路行銷的陌生開發透過交友網站、廣告投放。但檢察官也不認為廣告商有問題，或認為沒辦法證明是他在詐騙。

所以每個嫌疑人都不認為自己在犯罪，自認只是執行自己的業務。假客服跟被害人聊天，錢也不是匯給他，對象也可能自己送上門的，所以都覺得自己應該沒事。

五、從網路詐欺犯罪被害者與加害者之心理特質與日常生活之相同與相異點分析，可否提供相關的抗制網路詐欺犯罪對策？

F6：

我也很喜歡另外一個犯罪學理論：情境犯罪預防。情境犯罪預防在網路犯罪非常適合，除了增加犯罪阻力，還有降低犯罪的報酬。尤其針對投資詐騙或加密貨幣如何監管，各國作法主要分成兩大類，第一就像臺灣採刑事處罰的監管方式，比較是負面的。將加密貨幣視為洗錢，例如加密貨幣首次出現在臺灣的法律，就是洗錢防制法。另外，很多國家像韓國、歐盟、西班牙、日本、新加坡等，採取保護投資人的立場訂定相關政策，不只是打詐，還保護產業發展（如新加坡政府成立國營的加密貨幣交易所）。

區塊鏈或加密貨幣其實是中性的，臺灣人才濟濟，有非常多優秀的工程師，例如星展銀行把臺灣當成人才培育的基地。但新創公司在臺灣卻不受重視，甚至被打壓。所以比較正向的公司，就去幫國外做事，等於外包我們的技術協助國外的產業；比較不好的則跟詐騙集團掛鉤，成為黑色產業鏈的一環。從整個國家的長遠發展來說，其實非常不好。我們可以墊高犯罪的成本，譬如提高加密貨幣的監管、降低匿名化；而非一味提高刑責，雖然可減少加密貨幣的犯罪，但也讓我們國家失去這個產業的競爭力。

F7：

我認為需要提倡全民的資安意識教育，跟防詐有點類似。以金融產業來講，都會提醒投資有賺有賠，申購前請詳閱公開說明書。上網也有一定的風險，卻沒有公開說明書。在做很多事情前，要先教育使用者，風險在哪裡，讓他能理解。像虛擬貨幣，不了解就不要投資。現在一些民眾的想法不太一樣，他不會去思考風險的問

題，不了解的東西，居然也會跟風投資。所以要加強民眾對於網路、不熟悉的領域具備風險意識，可以有效降低被害的機會

六、晚近新加坡/中國等華人社會對於網路詐欺犯罪之抗制策略，是否有參考採之處?

F5：

新加坡有些防詐、防洗錢的措施，像最近他們在立法，希望由新加坡金融管理局主導，計畫先由六家主要銀行交換資訊，之後逐漸擴展至金融體系。透過法律的授權，讓銀行把風險高的客戶交易資料上傳到政府建構的平臺。當然需要法律授權，新加坡現在立法的階段，香港也有類似的發展。另外，新加坡也有處理簡訊實名制的問題，臺灣遇到很多二類電信的 IP 加密問題，即使懷疑詐騙是從中國進來，但沒有任何管道可以處理通信的阻礙，沒有辦法追查，這已是 10 年以上的老問題。華人社會應對詐欺犯罪的方式，我覺得大同小異。重點在於立法的腳步，無論是解決警語頁面或查封 Domain Name 等，都是沒有法律授權依據的問題。

F8：

大家熟知中國網路採實名制、網路有金盾防護，但國內社會及民眾能否接受相同措施，可能有點困難。

我非常贊同 F7 的講法，國家其實有資源，但缺乏統合，真的要有層級夠高的單位或主事者統合資源，各部會協調才會更順遂。

另外，像毒品犯罪有毒品危害防制條例，也可以考慮訂立「詐欺犯罪防制條例」的專法，統合資源，把資通訊防制及偵查措施都納進來，像警語頁面、M 化車及設備端通訊監察偵查手段的使用、網路平臺者對於詐欺的協力義務等等，全部納入立法。這樣是不是可以降低先前相關法案立法的一些爭議，就像 M 化車目前報載法務部研擬於組織犯罪防制條例增訂法源依據，因為我們是限定特定犯罪。

F9：

今年初新加坡警察部隊來 165 參訪，新加坡對臺灣 165 的圈存

攔阻與銀行合作很有興趣。也分享他們的做法，架設防詐 APP 名叫 ScamShield；新加坡警察部隊也有 WhatsApp 的帳號，有點類似我們的 WhosCall 跟美玉姨。

之前打詐議題在發酵時，有要求數發部做防詐的 APP，但數發部評估應該要跟民間結合來做。每個國家政策的導向不一樣，但是跟民間結合要怎麼做，有沒有辦法達到效果，可能要再持續觀察。我個人也傾向跟民間結合，像 WhosCall 在 105 年就跟刑事局簽 MOU 合作，因為自己開發 APP 的經費很驚人。以 165 的官方 LINE@帳號來說，已經有 78 萬人追蹤，但是它的宣傳效果仍相當有限。新加坡的 ScamShield 有國家的支持，臺灣或許可以參考，透過公私協力來做。

七、當前政府打擊詐欺犯罪之策略，是否應該針對不同類型(例如購物、投資與電信客服……)，提供不同的策略方式？

F6：

南韓有一個狀況，就是比特幣跌的時候，家暴案件會增加。因為很多啃老族在家炒幣，只要比特幣掉了，就打長輩出氣。小小的南韓有一百多家的交易所，可看出加密貨幣融入韓國人民的生活極深。

南韓 9 月舉辦全球的區塊鏈週，可惜的是沒有臺灣的業者、學者或公部門參加。首爾研討會雖然才兩天，可是議程非常豐富，不管是從產業界、監管面，日本、美國、歐洲國家等都會去分享，到時候如果有進一步的資料，也可以跟大家交流，建議大家應該多多參加國際間有關打擊詐欺犯罪之研討會，以增加打詐作為之了解。

F7：

以銀行的角度，是保護客戶的帳戶安全為優先；其他的產業也需要保護網路用戶的安全。可能每個產業對資安的重視程度不一，像金融業有非常高的標準，所以比較少有個資外洩的狀況。有些電商則動不動被 165 公告為高風險的賣場，個資不斷外洩，也間接影響到其他產業客戶的安全。比如某電商的帳號密碼外洩，然後不肖

人士就去某銀行試這組帳號密碼，所以他有機可乘，堂而皇之的登錄金融交易系統，破壞金融交易的安全，前年的券商撞庫攻擊就是典型例子。應該是一致的要求大家重視資訊安全、系統安全、個資的保護。臺灣 5 月份有修個資法，提高處罰的金額，個人持正面的態度。甚至我覺得可以該企業營業額的百分之幾來處罰，讓企業更加重視個資安全，進而保障交易安全。

另外，每家企業會保留相關的資料，是不是能夠運用做大數據分析，或 AI 的分析。例如某銀行有過濾的機制，判別客戶行為是否有問題，但沒辦法跟其他銀行分享這些情資。其他產業或電商，也會有自己的分析機制，得知一些問題帳號，但也沒辦法分享。所以國家的整體資料治理策略、規範，應先訂立出來，才能有效的把每一企業、每一家分析所得到的貢獻出來，形成比較良好的正向發展。

F8：

從研究資料可以發現詐欺是全球跨國性的問題，也不僅止於我國遭遇到這個執法困難，剛才前面許多先進已提到國際合作，此處就不贅述，個人一點淺見是，雖然國際合作重要，但還有哪些是國內制度性要完成的工作，例如前面提到的科技偵查法、數位服務法等法案應儘速完成立法。但考慮上述立法爭議很大，立法上是否可以考慮針對詐欺犯罪制定專法(比照毒品犯罪)，針對詐欺犯罪建立跨部會快速協調平臺、科技偵查手段、防制手段(例如社群媒體詐欺廣告投放及停止解析)、網路流量紀錄等資料保留、建立(去識別化)金融及詐騙情資交換系統等納入。

八、行政院於今年 5 月成立專責之打詐辦公室，以強化當前打詐的編制，迄今有無相關成效？

F7：

我們產業現在面臨到一些困難，很多網路釣魚郵件以某銀行名義寄給民眾，不管是客戶或非客戶。有些人比較有警覺，就不會去點擊；有些民眾警覺性比較差，就可能被釣走，造成他的信用卡被

盜刷。第一時間我們的客服，會首先知道現在最新的詐騙手法。但今天即便知道新的詐欺手法，還是求救無門，不知道怎麼處理。各家銀行都有遇到類似的詐騙問題，我們很希望說有一個單位，或統一的窗口來幫忙在手法的釐清，或是跟民眾宣導防範。建議刑事局或許可以跟各個不同的產業互動，像簽訂 MOU，執法機關多跟產業合作。

F9：

打詐辦公室的組成，都是各機關借調的人力。刑事局借調 2 名同仁過去，一名負責反詐騙宣導，另一名處理打詐行動網領的業務，這些同仁其實滿重要的。因為也有其他行政機關借調進去的人力，在打詐辦裡面，先形成共識，再提出政策或做法，這樣的溝通效率很高，而不是開會大家在那邊吵，會浪費很多時間。打詐辦公室的主任就可以決定方向，然後跟主導打詐策略的羅政委報告，大概就定調了，所以溝通效率會提高很多。有更好的溝通效率，實際執行單位的聲音可以透過打詐辦反映給行政院，不用再層層上報。

第三節　政策焦點團體座談之重要意見與建議彙整

根據前揭 5 位學者專家針對本研究所擬定之政策焦點座談八大訪綱所提供之經驗分享、意見與建議，以下針對四個面向，彙整如下：

一、法規面

(一)盡速制訂與通過防制詐欺犯罪之相關法律

所謂「工欲善其事，必先利其器」，我國目前有關「數位服務法」與「科技偵查法」等，因有相關個資外洩疑慮或考量言論自由與意見表達等權利，尚未立法通過，導致在追訴網路詐欺犯罪上，仍存在許多偵查上之限制。反觀德、英、美、法、奧地利及西班牙等國非常強調人權之西方國家，針對個資外洩防護、特定網路銀行使用或 OTT 通訊服務資料無法調取的部分，已有相關立法規範；而英國及澳洲也立法保留網際網路流量紀錄；此外，針對約束社群媒體業者行為(例如違法內容通報及處理機制)部分，歐盟執委會於 2022 年也通過「數位服務法」。這些都是國內法制尚未完備而需要盡速解決之處。

(二)最終目的期盼制定「詐欺犯罪防制條例」專法

目前我國對於毒品犯罪，立有「毒品危害防制條例」專法，專門負責打擊與防制毒品犯罪。根據這樣的立法思維，長遠來講，政府應可以考慮訂立「詐欺犯罪防制條例」的專法，統合資源，把資通訊防制及偵查措施都納進來，像警語頁面、M 化車及設備端通訊監察偵查手段的使用、網路平臺者對於詐欺的協力義務等等，全部納入立法。晚近也有類似的立法作為，例如法務部研擬於「組織犯罪防制條例」中將警用 M 化車增訂法源依據，讓警方執法有一個依據。

(三)提高網路詐欺犯罪者懲罰之刑度或提高量刑

根據犯罪學理性選擇理論(Rational Choice Theory)之主張，犯罪人從事犯罪行為一定都是衡量過犯罪成本與犯罪所得後，覺得所得高於成本，始決定遂行。因此，墊高犯罪成本始能嚇阻犯罪人從事網路詐欺的行為。而針對目前刑罰一罪一罰部分，乍看有威嚇性，

但實際上法官的定執行刑才是重點。因此，建議透過修法方式，加重網路詐欺犯罪之刑度，進而限縮法官的裁量權，促其加重刑度之裁量。甚至對於網路詐欺犯罪者，若沒有與被害人和解或繳交詐欺犯罪所獲得之利益者，不得予以假釋，以墊高或加重其犯罪之成本。必要時，應該恢復刑罰附加強制工作，對網路詐欺犯構成較重的威嚇效應。

二、組織面

(一)應於行政院層級設置打詐專責辦公室

鑒於打擊網路詐欺犯罪案件涉及內政、外交、數位、金融以及陸委會等跨部會之業務，以目前內政部警政署刑事警察局所設置之「打擊詐欺犯罪中心」為主責部門，實在力有未逮，許多事情仍需透過行政院政務委員透過召開跨部會、跨公私部門之會議，溝通、協調，始獲改善，但時間上已錯失先機。此外，法務部於 112 年 5 月於臺灣高等檢察署成立「查緝詐欺及資通犯罪督導中心」，與內政部警政署之「打擊詐欺犯罪中心」之業務是疊床架屋，還是分工合作？仍未清楚。換言之，無論是以目前刑事局所設之打擊詐欺犯罪中心或法務部之「查緝詐欺及資通犯罪督導中心」，做為當前我國打擊詐欺犯罪工作之主責部門，層級過低也與國際間的發展趨勢不符。

(二)應與公私立金融資訊機構建立資安互助合作機制

過去內政部警政署 165 反詐騙專線與公私立金融資訊行號欲建立資安互助合作平臺與機制，困難重重。今年 6 月 1 日後，內政部警政署刑事局打擊詐欺犯罪中心整合 165 反詐騙專線業務後，打詐中心現在已陸續與事實查核機構(MyGoPen)、Whoscall、中華資安、臺灣大以及趨勢科技等，都簽有資安與網路的合作項目與機制；然而在金融機構部分，雖有逐年增加，仍略顯保守。金融交易系統對於保護客戶帳號的安全，已投注相當多的財力與資源，但仍希望與警界或執法單位建立資訊安全、系統安全與個資安全的互助合作。不應該有因為該金融機構的資安長有警政背景，所以比較容易獲得警政的合作與協助，共同打擊網路詐欺集團。所以政府應該要有一致性的做法，與各金融機構建立資安互助合作協定與資安資訊平臺機制的建立，大家互通情資，共同打擊網路詐欺不法行為。而政府

應該要求企業每一年應該提撥其營業額的百分比挹注於資安的防護，進而保障金融交易的安全。

(三)強化打擊詐欺犯罪中心之部門與陣容

刑事局於 112 年 6 月 1 號將 165 反詐騙專線結合打擊詐欺犯罪中心，並在中心設有資通研析股（針對網路跟電信的部分）、金融研析股（針對洗錢高風險行業、遊戲點數、虛擬帳號、虛擬貨幣的對策或研究）、綜合研析股（行動管理的政策面跟打擊面）和 165 股（負責詐欺報案系統）。各業務股分工似乎明確，功能逐步提升中。然而這樣的陣容仍缺乏跨國與跨域領域的合作以及擬定相關國際互助協議或協定之研究與簽約部門，殊為可惜。因此，建議應該將跨國跨域合作的業務以及國際資安公約之業務納入，前者可以根據網路詐欺犯罪之熱點、熱區或熱國，協調或增加相關的駐外警察與當地警政部門合作，建立共同打擊詐欺網絡；後者可以透過外交單位的接洽與協助，尋求相關國際公約的簽訂，例如 24/7 Cybercrime Network，盡快保全網路犯罪之證據。甚至掌握國際間有關網路犯罪或資訊安全之會議，派員與會參加，以掌握國際間網路犯罪之新型態並建立良好互助關係。另外，民眾網路遭詐的報案方式，可以規劃以網路報案的方式進行，以符合國際趨勢。

三、教育面

(一)編撰分齡分類之識詐教育宣導教材

由於網路詐欺犯罪具有多樣性與變異性，一套識詐的教育宣導文宣或教材，已不足以為因應。因此，有關識詐之教育宣導教材，應該根據不同的年齡群以及不同的網路詐欺犯罪型態，分齡分類製作不同的教材才對。例如大學生或年輕族群者，容易遭受網路購物詐欺被害，因此針對該年齡層者應製作網路購物詐欺被害之教育宣導教材；又如年紀較長且有一定資產者，容易遭受網路投資詐欺被害，因此針對具資產族群者製作網路投資停看聽之教育宣導教材，特別是網路投資與金融投資一樣，「投資一定有風險，沒有穩賺不賠的，投資前應該詳閱相關投資說明書」，如果沒有這種警語者，詐騙型投資的機率很高，應該於教育宣導時多加強化。高中生或大學生或無業者最易被詐騙集團吸收為擔任車手，因此當有一些雇工廣告

內容提及「無經驗、負責提款並交給公司、獎金/薪水優渥」等字樣時，即可能是詐騙集團招募車手的廣告或宣傳單。

(二)第一線執法人員之定期專業教育訓練

由於網路詐欺犯罪的多樣性與變異性，例如晚近釣魚連結從過去的簡訊擴大至實體信件，附上 QR Code 及 Line ID，誘騙民眾到詐欺群組後行騙[13]；又如一些詐欺模式流行一段時間後，又會變異改為其他模式，但目的都是以投資、購物或 ATM 解除分期付款等手法詐騙民眾的錢財。面對網路詐騙犯罪變異性與多樣性的特性，第一線執法人員的專業教育訓練特別重要。刑事局近年來其實有一直有在規劃與執行科技偵查人員的教育訓練，例如 2023 年 7 至 8 月間內政部警政署召訓全國各警察機關資訊與科技偵查人員，辦理兩梯次各為期 5 天的犯罪情資分析課程，以「科技偵查犯罪情資」、「數位金融情資」以及「公開網路情資」3 面向為主軸進行教育訓練，以面對不斷演化的新型態詐欺犯罪[14]。未來警政部門除應該持續辦理此一教育訓練外，亦能邀請國外相關警政人員及資安師資分享跨國跨境查緝網路詐欺犯罪的案例，以強化第一線科偵人員的執法能力與專業知識。

四、查緝面

(一)根據網路詐欺犯罪熱點與移動適時增加駐外警務人員

目前臺灣已於一些國家派駐警務聯絡官，蒐集與協助打擊與偵查跨國跨境網路詐欺犯罪，成效斐然。然而網路詐欺犯罪具有變異性與匿名性，許多網路詐欺犯罪經常遷移、移動，甚至有些地區已成為網路詐欺題集團群聚的熱點，但一段時間後可能又轉移陣地到其他國家或區域。因此，警政部門應該隨時掌握網路詐欺犯罪的熱點與遷移路徑，適時增加境外的警務聯絡官，以協助當地與國內破獲網路詐騙成員與集團。

(二)建立跨國跨境警務偵查互助合作平臺

鑒於網路詐欺犯罪屬於跨境與跨國犯罪型態，透過層層分工與

[13] 刑事局提醒 釣魚連結無孔不入 以從簡訊擴大到實體信 https://udn.com/news/story/7315/7365268

[14] 警政署培訓科技偵查高手 首度舉辦搶旗競賽 - 社會 - 自由時報電子報 (ltn.com.tw)

專業化分工後，一個犯罪行為切割為數個犯罪分工，彼此獨立但有串接，更重要的是，犯罪地點與犯罪結果地點具有分離性，例如詐騙機房在 A 地，但取得詐騙的錢財卻是在 B 地。因此，偵辦網路詐欺犯罪必須大量仰賴跨國、跨區警務人員的合作始得克竟其功。且相較於檢察官的司法互助，警務人員的偵查互助更具有時效性與立即性。故透過我國駐外警務人員與鄰近國家建立共同偵查跨國跨區網路詐欺犯罪，實屬當前要務。例如晚近許多詐騙集團群聚於東南亞國家，設置詐騙機房詐騙大陸地區民眾或臺灣地區民眾，代表東南亞已成為臺灣詐騙集團之熱區或熱點，因此，實有透過警政署駐外警務聯絡官與當地警政部門穿針引線，建立共同打擊、偵查網路詐騙集團行為之平臺，為降低東亞地區網路詐騙犯罪行為共同努力。

(三)簽署保全電子證據之國際協議與協定

由於網路犯罪的激增，電子證據儲存於不同的司法管轄區的情形日益嚴重，因此國際間對於電子證據的保存已漸有共識，遂於 2021 年 11 月 17 日正式通過「布達佩斯網路犯罪公約第二附加議定書」(The second additional protocol to the Budapest Convention on Cybercrime)，而簽署此一議定書的國家，可以將網路犯罪者所犯之罪且存放於國外、可移轉或未知地點伺服機上的電子證據，透過互助協定的方式，協助偵辦或起訴國家的執法當局取得，而其作法已包含與服務提供商和註冊商直接合作，以加快取得與犯罪活動相關之訂戶資訊和流量數據的手段。然而我國目前受限於外交處境，也非布達佩斯公約或類似公約的成員國，馬上要取得簽署前揭公約的機會很低。但可以逐漸互惠的方式，透過個案與請求國、被請求國逐步建立規模化的協議協定(protocol)，甚至援引目前已被全球認可的布達佩斯公約模式作為基礎架構，以利與國際接軌，例如先透過進入 24/7 Cybercrime Network，在透過此一平臺、國家，以個案方式簽署協議協定，從點逐漸擴展成線、面的方式，尋求國外服務提供商和註冊商協助保存相關電子與電磁紀錄，俾有效達到刑事司法互助請求之目的(陳昱奉，2022)。

(四)科偵部門應該運用 AI 或大數據進行犯罪手法分析

科偵部門目前針對假投資網站有做警語頁面，我們可以在像是外匯天眼這種反詐欺投資平臺看到許多被害人因為看到這個頁面而驚覺被詐，但這些網站不同域名眾多且更新迅速，建議可比照 iWIN 建構快速通報下架機制，同時結合 165 的大量被害情資，以 AI 智能化的方式自動化找出新生成的域名加以停止解析。亦即執法人員在相關法律同意且授權的情況下，例如「科技偵查法」的規定與授權，可以以 AI 智能化的方式，自動化找出新生成的域名相關情資，為全球跨境電子商務產業(例如 Amazon、日本樂天等)做出貢獻。

第六章　結論與建議

第一節　結論

一、各國網路詐欺被害相關調查與網路詐欺定義

本研究根據美國、英國、歐盟與澳大利亞等國家對於網路詐欺被害相關調查之方式與相關機制，以及網路詐欺定義之探究，綜整結果如下：

（一）網路詐欺犯罪之呈現日益嚴重之趨勢

根據前述各國網路詐欺犯罪被害調查之分析，可以發現網路犯罪之數量呈現逐年成長之趨勢，再加上 Covid-19 期間減少民眾外出的機會後，網路詐欺犯罪急速增加，例如根據美國 IC3(2023)的報告，網路投資詐騙金額從 2021 年的 14.5 億美金，成長至 2022 年的 33.1 億美金，成長一倍之多。而根據英國國家總計局(U. K. Office for National Statistics [ONS], 2022)公布之資料顯示，與網路有關的詐欺犯罪(Cyber-related fraud)，自 2020 年 3 月至 2022 年 3 月已成長 61%。另外，根據澳洲網路安全中心(Australia Cyber Security Centre [ACSC], 2023)報告，2021 年至 2022 年的會計年度總共受理 76 千件網路犯罪報案，較前一個會計年度成長 13%，其中與網路詐欺有關的案量，達到 23%，每年一年網路詐欺財損估計達 3 億美金。網路詐欺犯罪之防範儼然已成為各國犯罪預防之重要或首要工作。

（二）網路詐欺仍以網路投資財損最為嚴重

雖然網路詐欺犯罪日益嚴重，且呈現各國詐欺方式、詐騙金額與詐騙人數多寡不一的情況，呈現出的先後順序的重要型態亦不太相同，但主要仍以網路投資(cyber investment scams)詐騙型態最為嚴重，因為涉及的金額與被害的人數都是年長者居多的現象。例如以美國為例，2022 年投資詐騙金額高達 33.1 億美金，較 2021 年的 14.5 億美金成長一倍之多(IC3, 2023)。而根據英國的報告，網路詐欺犯罪型態中有 73%的案件涉及被害人運用銀行/信用帳戶轉匯帳款

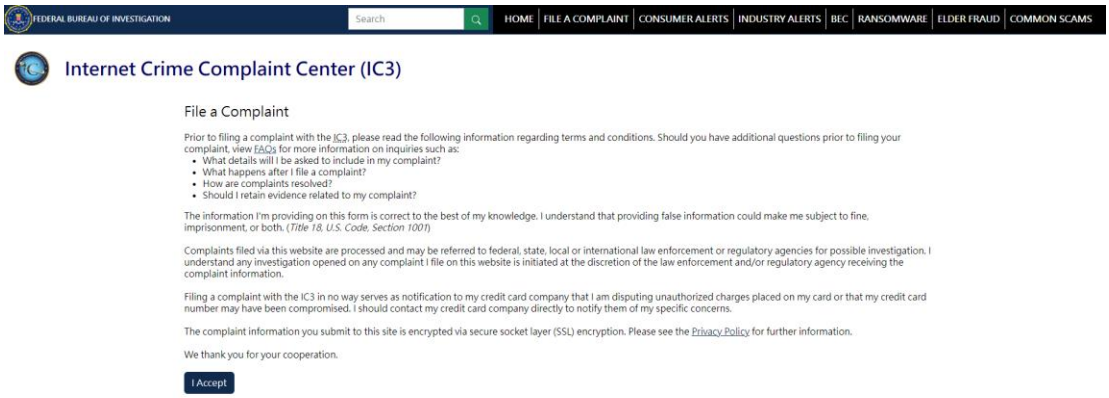
(U. K. Office for National Statistics [ONS], 2022)。反觀我國，根據刑事局(2023)公布統計數據，我國 2022 年網路投資詐騙財損約 1 億美金[15]。伴隨著加密貨幣的日趨普及，網路投資詐欺將益形嚴重。其次是相較於西方國家網路釣魚(phishing emails)的被害人數日益增加，例如美國、英國與澳大利亞，反觀我國是網路購物詐欺(online shopping /online financial transactions)型態較為嚴重，其詐騙金額雖不至似網路投資詐欺為高，但呈現出詐騙人數最多、且都是年輕世代族群。

（三）各國網路詐欺之調查與報案方式已走向網路化

各國對於網路詐欺犯罪之調查方式，都是先由傳統犯罪被害調查的管道從一般市民的電訪(Telephone-operated crime survey)和面訪(Face-to-face interview)中先增加網路犯罪被害經驗的調查開始，然後逐漸擴充網路犯罪被害之型態，然後再發展成專屬網路犯罪被害之調查，包含電訪、面訪或網路報案(Online report) （例如美國聯邦調查局的 IC3 報案介面，詳圖 6-1-1），每一年受理的案件量日趨龐大。然而，伴隨著網路的普及，民眾愈依賴網路進行瀏覽，交談，購物與交易的同時，造成網路犯罪的日益猖獗。當民眾發現有疑似被詐、被騙之情況時，雖然一可以利用撥打電話的方式進行報案，但以其他國家為例，被害民眾大多利用網路的報案系統，因此，建構便民的網路被害報案系統實有必要。

[15] 中時新聞網: 假投資去年總財損 34 億 居詐騙案之冠。造訪日期 2023.8.8；https://tw.news.yahoo.com/%E5%81%87%E6%8A%95%E8%B3%87%E5%8E%BB%E5%B9%B4%E7%B8%BD%E8%B2%A1%E6%90%8D34%E5%84%84-%E5%B1%85%E8%A9%90%E9%A8%99%E6%A1%88%E4%B9%8B%E5%86%A0-201000178.html

圖 6-1-1 美國聯邦調查局的 IC3 網路報案介面



（四）成立網路詐欺犯罪調查專責機構已成為趨勢

美國自 2000 年成立網路犯罪報案中心(Internet Crime Complaint Center, IC3)、英國自 2012 年也針對商業被害調查進行商業界的網路犯罪被害調查，並於 2016 年成立國家網路安全中心(National Cyber Security Centre, NCSC)；無獨有偶，澳大利亞也於 2014 年成立網路安全中心(Australia Cyber Security Centre, ACSC)，作為澳大利亞有關網路犯罪問題研究、調查、擬定與防制網路犯罪問題與威脅之專責機關。換言之，面對網路犯罪問題日趨嚴重，各國大致上已成立專責、跨領域的機關來統籌與因應相關的防制作為。

（五）打擊網路詐欺犯罪須靠跨境/跨域合作始能克竟其功

面對來勢洶洶的網路犯罪，特別是網路詐欺犯罪，專業背景、專責分工、層層斷點，犯罪地點與詐騙地點具有時空分離的特性(許華孚、黃光甫，2020)，警察或執法部門的跨境與跨域合作，勢在必行，例如美國司法部與聯邦調查局(FBI)會與其他國家(例如印度的中央調查局)與地方執法部門合作，共同打擊金融犯罪與跨國假客服詐騙案件(FBI,2023)。另外，英國的國家網路安全中心(NCSC)在其官網宣稱該中心與美國、加拿大、澳大利亞、紐西蘭等國家級的網路安全相關部門結盟，共同打擊相關的網路犯罪、攻擊與威脅事件。

（六）國際間以及我國對於網路詐欺的定義

網路詐欺（又稱線上詐騙，英文為 Internet fraud 或 Cyber Fraud），係指描述網路犯罪者透過網際網路這個工具(Cyber-enabled fraud)所實施的犯罪行為之總稱。而這些網路犯罪者實施這些犯罪的目的是希望透過非法獲取和非法利用個人或企業的敏感資訊來獲取其金錢利益之謂[16]。具體而言，網路詐欺係指犯罪行為人透過電腦或類似的 3C 設備（例如手機、平板），進而連接網路網路而實施的犯罪行為，其目的就是破壞或取得他人在網路上所存儲的個人和財務資訊，進而將其利益據為己有或從中獲得利益[17]。網際網路服務也可被用來向潛在的被害人進行宣傳的行為，進行虛假的交易，或者是向金融機構等與該竊盜行為有關的第三方傳遞虛假資訊。一般而言，網路詐欺行為大都透過社交傳媒的管道進行，例如在聊天室、社群媒體、手機 App、電子郵件、留言板、網站等地方進行[18]。因為具有匿名性與時空無限制性，進而增加查緝之困難。常見的網路詐欺犯罪為網路釣魚、網路購物、網路投資、惡意軟體、勒索信件以及身分詐欺等。

根據 Wall (2011)的分類，網路詐欺犯罪可以區分為網路專屬犯罪(cyber-dependent crimes)以及網路協助犯罪(cyber-enabled crimes)兩類，網路專屬犯罪被定義為只能通過網際網路之技術所進行的攻擊行為。換言之，沒有網路網路這個工具或技術，這些犯罪行為就不存在。例如，惡意軟體、勒索信件、駭客攻擊以及垃圾郵件等，都構成網路專屬的網絡犯罪。另一方面，網路協助犯罪被認為是傳統犯罪與網路網路工具或技術相結合而產生的一種混合型網路犯罪。換言之，此類犯罪如果沒有網路網路工具或技術支援、協助的情況下，它們仍然可以存在，但因為網際網路工具與技術的運用，可以擴大傳統詐欺犯罪之範圍，影響更廣泛的被害者，例如網絡釣魚、網路博弈詐欺、網路購物詐欺、網路投資與身分詐欺等。

網路詐欺在臺灣，根據刑法第 339 之 4 條第 1 項第 3 款，以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布

[16] https://www.mimecast.com/content/cyber-fraud/

[17] https://www.delta-net.com/knowledge-base/compliance/fraud-awareness/what-is-cyber-fraud/

[18] https://zh.wikipedia.org/zh-tw/%E7%BD%91%E7%BB%9C%E8%AF%88%E9%AA%97

而犯刑法第 339 條第 1 項之行為，即透過網際網路或其他媒體等傳播工具，行為人意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付予行為人之行為。據此，行為人網路詐欺行為是否構成網路詐欺犯罪，其構成要件包含行為人主觀上具有「不法所有之意圖」，亦即主觀上必須具有為自己或第三人獲取違法之財產上利益之不法意圖，同時，行為人還必須具備詐欺的故意，心中清楚認識到以實現詐術方式，使被害人陷於錯誤而交付財物，進而進行財產上的處分，使其於財產上蒙受損害，上述各客觀要件間具有相當因果關係。

二、我國網路詐欺被害調查被害者之相關特性與被害因素

本研究根據網路詐欺被害調查問卷所獲得之數據，透過適切的統計分析技術，得到以下重要發現，綜整如下：

（一）網路詐欺被害的犯罪類型：購物詐騙位居首位，投資詐騙顯著上升

1. 過去一年半網路詐欺被害類型

受訪者在過去一年半之中，最常遇到的網路詐欺被害型態有三種，分別是：以上網購物被害占 42.76%、猜猜我是誰(假冒親友)21.33%、網路投資被害占 15.41%。上網購物被害型態是最常見的網路詐欺被害型態，可能與受訪者在疫情期間增加網購的頻率和金額有關。猜猜我是誰(假冒親友)是第二常見的網路詐欺被害型態，此種詐騙方式，可能與受訪者在社交方面的需求和信任感有關。第三常見的網路詐欺被害型態為網路投資被害，這種型態詐騙可能與受訪者在財務方面的需求和貪婪感有關。這三種型態合計占所有網路詐欺被害型態的前三名(詳見表 3-3-4 及圖 3-3-8)，該數據亦顯示網路詐欺的多樣化和普遍化，以及受訪者在使用網路時的風險和挑戰。

2. 最近一次網路詐欺被害類型

受訪者最近一次遭受網路詐騙的方式，主要有三種：**網路購物被害、投資被害和玩網路遊戲**。這三種方式約占受訪者的 7 成以上

(詳見圖 3-3-2)。其中，網路購物被害的人數最多占 47.70%。顯示大部分的受訪者在網路上購買物品時，可能會遇到不實的賣家或平臺，因而造成金錢或物品的損失，為讓消費者能夠安心地在網路上消費，**對於網路購物詐騙應強化被害犯罪預防和犯罪偵查。**

投資被害是第二大的網路詐騙方式占 14.36%。受害者可能於社群媒體或網站看到高報酬的投資項目，但實際上是詐騙集團的詐術及陷阱，導致高額的投資本錢被騙而血本無歸。**投資詐騙在最近一次網路詐欺被害占第二位，所占比重提高**，**顯示預防網路投資詐騙有其重要性。**投資者應提高警覺，及時查證投資對象的可靠性，千萬不要輕信網路上的各種投資訊息。

玩網路遊戲是第三大的網路詐騙方式占 8.33%。受害者可能於在玩網路線上遊戲時，遭到不明人士騙取虛擬寶物或遊戲點數，或遊戲的帳號或密碼遭到駭客盜用，造成線上遊戲的寶物或財產被盜或騙取。玩家應注意不要任意於網路上透露個資，保護個人隱私，也不要隨意相信不明的遊戲外掛程式或陌生的網址連結，以避免遭到詐騙。

除了以上三種方式外，其他如交友詐騙、ATM 解除分期付款、猜猜我是誰(假冒親友)、網路用身分、求職詐騙等亦不容忽視。網路詐騙類型會隨著時代演進不斷地推陳出新，應提高對於網路詐騙的防範意識和能力，不要輕信網路上的各種訊息或要求，並且及時向相關單位求助或檢舉。

（二）網路使用經驗與被害管道：

1. 網路使用經驗與被害

根據本次調查結果，有超過 7 成 5 的人使用網路已超過 10 年，且每週上網次數超過 10 次，有超過 3 成的人每天上網時數超過 6 小時，有將近一半的人在週末晚上有固定上網的習慣(詳見表 3-2-2)。分析結果顯示，每日上網時間、上網時段、接觸網路的時間與有無網路詐欺被害有顯著關聯，但上網次數則無顯著差異 (詳見表 3-4-3)。**從被害者網路使用經驗來看，接觸網路時間較短、偏愛週末清晨上網者，被害機率較高**(詳見表 3-4-3)。這些時段或人群的網路安

全意識較低，亦或網路詐騙集團的活動較為頻繁，使得他們更容易成為網路詐騙的目標。

2.社群軟體與購物網站被害居多，但線上遊戲被害風險最高

有被害經驗者中遭受網路詐欺的主要管道為**社群軟體、購物網站和線上遊戲**，分別占 48.76%、34.22%和 11.52%，三者合計占 94.50%(詳見圖 3-3-3)。交叉分析發現，使用線上遊戲者較不使用該者更易成為網路詐欺的受害者；而使用購物網站和社群軟體則與網路詐欺被害無顯著關聯性(詳見表 3-4-4)。被害者大都因社群軟體、購物網站和線上遊戲等接觸到詐騙訊息或犯罪者。儘管使用社群媒體和網路購物的人數較多，但網路詐騙被害風險卻以線上遊戲最高。

（三）最近一次網路詐欺被害經驗

1.被害事件特性與互動情形

(1)事件特性：網路詐欺被害匯款發生多集中於晚上，陌生關係、透過 ATM 轉帳、小額受騙金額占最大宗

本研究發現，有 3 成 6 的受訪者匯款時間集中於 18-22 時，被害人可能在 18-22 時段為下班時間，可能較為空閒或放鬆，因此更容易受到詐騙訊息的影響或誘惑。其次，有 6 成被害者被騙走的金額在 1 萬元以下，可能是因為詐騙設定一個不太高但也不太低的金額，讓被害人鬆懈自我警覺心，較不易查覺這是詐騙。

此外，近 8 成被害人不認識加害人，可能是因為詐騙者使用偽造或盜用的身分或帳號，或者是隨機發送詐騙訊息給不特定的對象。最後，有 2 成 2 被害人選擇網路 ATM 作為交易方式，研判可能是詐騙者利用網路 ATM 的匿名性和即時性，以避免被警方追蹤或銀行之查證(詳見表 3-3-1)。

(2)互動情形：加被害人透過購物、加害者主動聯繫和交友軟體互動

有被害經驗的受訪者中，有約 76.77%是透過以下三種方式與加害人互動而被害：其中網路購物占 48.23%、加害人主動聯繫占 14.36%、交友軟體占 14.18% (詳見圖 3-3-4)。網路購物雖可節省大

量人力及時間，但因網路購物可能具匿名性和不實資訊，較難分辨賣家與買家的真實身分和評價真偽，因而容易陷入詐騙的陷阱。

此外，加害人主動聯繫和交友軟體的高發生率可能與加害人利用「猜猜我是誰(假冒親友)」的詐騙技術有關，他們會假冒親友及同事等身分，或者利用被害人的心理弱點，說服被害人匯款或主動提供個資。最後，交友軟體利用人們欲於網路上建立社交或情感關係之心理需求，以填補內在之空虛，但網路交友軟體難以驗證對方的真實身分，以及上網的動機為何，許多受訪者因而成為網路詐欺被害。

2.被害查覺與原因

本研究發現，近八成的被害者是自己查覺遭受網路詐欺，且有四成的被害者在一天之內就察覺自己被騙(詳見表 3-3-2)。大多數被害者認為自己遭受詐騙是因為防詐觀念、認知和疏忽不足，而非因為加害人的技術或手法高明，這說明網路詐欺是一種迅速而致命的網路安全問題，需要高度的警覺和快速的處理。

3.被害反應與因應

在 564 名有被害經驗的受訪者中，超過七成的受訪者能在不到半個月內恢復正常生活作息。這也反映多數被害人能自我調適，並不會影響其工作或生活。然而，仍有 6.9%被害者因遭到網路詐欺被害事件後，出現嚴重的創傷後遺症（PTSD），幾乎終身難以恢復（詳見表 3-3-3）。此外，面對網路詐欺，被害者的求助方式主要有三種：32.45%會和家人討論、31.74%尋求朋友的幫助、26.95%向警方報案；三者合計占 91.13%（詳見圖 3-3-7）。顯示被害者在遭受網路詐欺後，主要因應方式為尋求親密關係或正式機構的支持，以減輕心理壓力和經濟損失。

（四）網路詐欺被害事件具有多元性與重複性

本研究發現，在 1,064 名受訪者中，有 33.18%只遭受過一種類型的網路詐欺，有 14.66%遭受過兩種類型的網路詐欺，而 21.80%遭受過三種或以上的多種類型的網路詐欺（詳見圖 3-3-9）。此顯示網路詐欺的普遍性和多樣性，以及被害者可能面臨的不同風險和影響。

本研究進一步分析不同類型的網路詐欺之間的關聯性和重複性，發現不同類型的詐欺對於被害者的影響和危險性也不盡相同。以網路購物詐欺為例，八成的被害者只有一次受害的經驗，可能是因為這種詐欺比較容易被察覺和避免，且網路購物的被害者可透過第三方支付平臺，也就是買家與賣家中間的「收款人」，追回部分或全部的損失。相反地，「猜猜我是誰(假冒親友)」的詐騙卻有較高的重複受害率，兩次以上受害的人數高達 118 人次，占該類型被害人 51.98%超過一半(詳見表 3-3-5)。由於該類型詐騙利用被害者的同情心和信任感，被害者往往不相信或不認為自己被騙，部分受害者為能找回失去的金錢或感情，因而較容易陷入詐騙的漩渦。這種詐騙可能會對被害者造成極大的財產損失及心理創傷，影響被害人的正常生活和人際關係，進而產生社會疏離感。

（五）人口特性與網路詐欺被害有顯著關聯性，但區域特性則無關聯性

本研究發現，男性或 40 歲以下網路使用者較易成為詐騙的目標；而無收入或每月收入四萬元以上的人則比較不易受騙，教育程度愈低者，網路詐欺被害機會愈高，不同的職業也會影響網路詐欺被害的風險(詳見表 3-4-1)。綜合國內外大部分人口特性與網路詐欺被害調查之實證研究結果，亦與國內的官方統計資料一致，**性別、年齡、收入、教育程度及職業之差異，確實會影響網路詐欺被害的機會**（Izuakor, 2021; Reyns, 2015; Whitty, 2020; 王秋惠，2007; 曾百川，2006; 黃祥益，2006; 葉雲宏，2008; 蔡田木、周文勇、陳玉書，2009）。

最後，網路詐欺的發生與居住地區、城鄉沒有顯著關係(詳見表 3-4-1)。這可能是因為網路詐欺不受地理距離和空間限制，只要有連接到網路的裝置，就有可能成為詐騙的對象。

（六）一般組與被害組在網路使用風險、被害動機與誘因有顯著差異，但防護監控之差異不顯著

本研究發現，有被害經驗者在接觸偏差訊息和網路觸法行為方面，均高於無被害經驗者，顯示有被害經驗者的網路使用風險較高(詳見表 3-4-4)。這與過去的文獻一致，個人的網路生活型態會影響其在網路空間中的風險暴露和接近犯罪者的機會（Vakhitova et al., 2019; Vakhitova et al., 2016；方呈祥，2020；王茜，2014；周愫嫻，2014；陳玉書、曾百川，2007；陳玉書等人， 2020；簡鳳容，2018）。在被害動機與誘因方面，除了網路購物，其他的動機和誘因皆與有無被害有顯著關聯性。在防護監控方面，部分的措施和策略能有效降低被害風險，但也有些則無顯著效果。這也反映民眾對於自己在網路上的行為和安全的認知和態度可能存在一些偏差或錯誤。因此，本研究建議，在提升民眾對於網路詐欺的防範意識和能力方面，應該針對不同的被害動機和誘因，提供不同的教育和輔導，並且強調一些有效且實用的防範措施。

（七）一般組與被害組在偏差價值、網路成癮及低自我控制有顯著差異

本研究發現，有被害經驗者在網路上的價值觀、網路成癮和低自我控制方面，都與無被害經驗者有顯著差異。有被害經驗者較認同一些不道德或不合法的網路行為，也較有強烈的網路心理依賴感、衝動行為或偏差動機。此外，有被害經驗者也較容易受到網路成癮和低自我控制的影響，進而增加成為網路詐欺的目標和受害者的風險。這些心理特質是影響網路詐欺被害的重要因素(詳見表 3-4-5)。本研究發現與國內外實證研究一致，加害人與被害人具有重疊性及相似性，他們是難以區分的團體，採取較偏差的生活型態，進而促使個人成為網路詐欺高風險的被害者（Jennings et al., 2012；Lauritsen et al., 1991；王茜，2014；簡鳳容，2018；許春金，2017）

（八）網路詐欺被害的顯著影響因子

1. 被害誘因與被害動機的影響力最為顯著

本研究結果顯示，被害誘因是影響網路詐欺被害最重要的因素。其次為被害動機。此顯示網路詐欺犯罪者如何利用情境機會來

吸引、誘惑或欺騙潛在的受害者，以達到其不法目的。本研究發現與國內外多數的研究發現相符合，當網路使用者愈容易被網路詐欺被害誘因所吸引，愈可能成為合適標的物，個人遭受網路詐欺被害的可能性也越高（Bossler & Holt, 2009；Holt & Bossler, 2015；廖釗頡，2010；簡鳳容，2018；葉雲宏，2008；陳玉書、葉碧翠，2022；黃祥益，2006）。

2. 具心理依賴、衝動性或偏差動機等心理特質傾向者，較易遭受網路詐欺被害

在本研究發現，網路成癮與網路詐欺被害呈正相關。上網時數愈久、越常在網路購物、越常與人在網路上聯絡、較常使用網路工具與人互動的人，愈容易遭受網路詐欺被害。這與國內外許多實證研究之發現具有一致性（Chang et al., 2015；Lin et al., 2020；Simsek et al., 2019； 周愫嫻，2014; 謝龍卿，2004）。此外，本研究也發現，在網路上有強烈的心理依賴感、衝動行為或偏差動機的人，更容易受到網路詐欺的誘惑或欺騙。因此，網路成癮與網路詐欺被害有關。

在低自我控制部分，國內外相關研究發現，具衝動性、冒險性、低克制能力等人格特質者，較難抵抗網路上特定的誘惑，較容易於網路購物消費及點選來源不明的網址，因而增加網路詐欺被害風險（Bossler & Holt, 2010; Koukia, 2020; Schreck, 1999；Schreck et al., 2002； 王秋惠，2007；簡鳳容，2018；葉雲宏，2008）。惟本研究只有衝動性對於網路詐欺被害具有預測力，本項研究結果與國外實證研究僅有部分相關。最後，本研究發現被害者與犯罪者是否一樣具有「偏差動機」，與國外實證研究具有一致性（Choi & Lee, 2017），亦彌補國內學術上之缺口。

3. 網路詐欺被害高風險之人口特性：年輕、男性、中低收入者有較高的被害風險

本研究探討網路詐欺被害的風險與人口特性的關係。結果發現，男性、年輕人及中低收入者較易遭受網路詐欺的侵害。這與部分國內外學者的觀點不同，他們認為性別、年齡、收入等因素對網路詐欺被害的可能性沒有顯著的影響（Leukfeldt & Yar, 2016; Louderback &

Antonaccio, 2017; Ngo & Paternoster, 2011; Pratt, Holtfreter, & Reisig, 2010; 廖釗頡，2010）。本研究進一步分析不同的網路詐欺被害型態，發現不同的性別、年齡、收入群體有顯著的差異。例如，年輕、低收入者在網路求職詐騙及遊戲詐騙方面有較高的比例。本研究認為，個人的人口特性與心理特質相對於網路風險本身，對於預測網路詐欺被害的發生有更大的解釋力。

三、我國網路詐欺加害者深度訪談結果之分析

本研究針對網路投資詐欺、網路購物詐欺以及電信客服詐欺三種型態之5位加害人進行深度訪談，針對渠等之基本資料、從事網路詐欺之情形(包含手法、技巧、專業與分工)以及當前防制網路詐欺犯罪策略與認知，綜整如下：

（一）受訪者基本資料分析

1.從事網路或電信詐欺犯罪與當時經濟困頓、沒有工作、缺乏收入有關。

2.周遭均有從事網路或電信詐欺相關犯罪行為或行業之朋友，知悉加害者缺錢、欠債或需求孔急時，就會嘗試介紹或推薦、鼓勵加入。

3.除一名受訪者宣稱曾有網路遊戲被騙點數的經驗外，其餘受訪者均從未有網路或電信詐欺被害的經驗。

4.大部分受訪者在從事詐騙行為之前，雖然熟悉網路環境，但對於利用網路從事詐騙行為，確實沒有經驗也沒有相關的專業背景。

5.認為網路或電信詐騙犯罪是一種低成本、高投報的犯罪行業。

（二）從事網路詐欺案犯罪之情形分析

1.從事哪一種類型的網路或電信詐騙犯罪型態，並非自己選擇，而是接受周遭沒有的引進或介紹後從事，其中電信詐欺入門門檻最低。

2.從事網路或電信詐欺犯罪，其心態均為利益薰心、想迅速致富賺錢或還錢。

3.從事網路或電信詐欺犯罪後，選擇此一類型並未想過換其他類型，主要原因在於獲利超乎預期或獲利尚可接受。

4.網路或電信詐欺是具有專業分工與強化集團或團體專業訓練的培訓課程。

5.集團或團體會安排講師授課、鼓勵受訪者向同儕請益以及查閱過去犯罪者與被害者之通聯紀錄，以強化專業知能。

6.網路詐騙平臺以社群平臺為主，例如 FB、微信，主要是因為渠等社群媒介的普及性高、對於一般網友不設防以及對於加入群組內的會員，又有隱私權的保障。而電信詐騙平臺則由傳統家用電話已經提升至手機電話。

7.集團對於潛在被害者會進行分析，不同網路或電信詐騙的潛在性被害者會有其不同的特性，例如城鄉、年齡、性別、收入、時段以及是否會接觸(通話)等，透過分析後予以鎖定。

8.認為網路或電信詐欺會成功，不外乎是利用潛在被害人的貪婪、性急(投資)、貪小便宜(假網購)、害怕與恐懼(電信詐騙欠錢被警察找上門)等。

9.加害者的獲利係採取抽取傭金、與集團成員均分犯罪所得以及給予較高月薪等三種方式支付。

10.電信或網路詐欺被害者支付金錢的方式為網路銀行/實體 ATM 轉帳以及交付遊戲點數為主，但假網路購物者亦有面交方式進行。

11.未避免人頭帳戶被警察查獲近而通知銀行關閉，網路或電信詐騙集團會派員隨時緊盯人頭帳戶，無論在臺灣或大陸地區，一發現有金額入帳，隨時派車手提領。

12.假網路購物詐欺與電信詐欺，獲利後迅速與被害者中止聯繫方式，例如封鎖帳號；然而電信投資者，僅對於想要提領獲利的大戶予以坑殺後踢出群組，其餘群組之會員仍然存在，除非被警查獲，該群組仍在運作。

（三）對於網路詐欺防制策略之認知分析

1.認為當前網路社群平臺之監控機制非常薄弱，對於有偏差行為之會員的管理，也非常鬆散。

2.警察在網路上監控的能力以及在街頭利用監視器逮捕犯罪者的能力，非常強，因此不要正面迎擊警察。

3.認為遲早都會被警察查獲，所以在有限的時間內，能詐騙多少人就盡量詐騙，在查獲之前讓自己或集團獲利達到最高。

4.車手赴超商 ATM 提領現金，要分散許多家超商，並要由不同的車手以及著不同的衣服、於不同的時段提領，規避警察的查緝。

5.詐騙大陸人士為主要的對象，主要是詐騙臺灣人，明著說不要欺負自己同胞以及臺灣人的防詐意識較高，實則是犯罪地與被害人不在同一地點或區域，可以將降低刑責。

6.政府的網路詐欺防制宣導仍是有效的，但有時候利益薰心、旁無他人警示求證或心驚恐慌，仍是會被詐騙成功。

7.共同建議：(1)教育民眾多多向家人、朋友以及警察詢問或是致電 165 反詐騙專線求證；(2)政府應該正視與杜絕網路上販售人頭帳戶之問題。

四、網路詐欺被害經驗與加害者犯罪手法之比較分析

綜整網路詐欺被害者之調查結果分析與網路詐欺加害者深度訪談之結果分析，本研究嘗試比較被害者之被害經驗與特性以及加害者之犯罪手法與描述，進行比較分析。以下僅針對被害者與加害者在一些共同性研究問題上之統計結果與經驗描述，區分為相同點與相異點，進行分析。

（一）相同點

綜合網路詐欺被害問卷調查結果與網路詐欺加害者深度訪談之資料，針對以下共同問題進行分析後，得到以下共同一致性的結果：

1.網路使用特性分析，被害人與加害人都是高度依賴使用網路的網民。

2.網路平臺使用分析，被害人與加害人都是使用網路上的社群軟體、購物網站以及從事線上遊戲作為網路生活的主要型態。

3.網路被害交付財物之方式主要以網路銀行/ATM 轉帳以及購買網路遊戲點數進行支付為共同交易方式。

4.被/加害人互動經驗分析，在網路詐欺被害案件中，兩者均不認識。

5.網路詐欺被害察覺分析，網路詐欺成功後，被害人均會驚覺到自己已經被害。

6.網路詐欺被害原因分析，貪小便宜(貪得無厭)、自身疏忽(心急誤判)為雙方一致認同的原因。

7.網路詐欺實體監控分析，有監控者在旁(例如旁邊有家人)，確實能有效地防止潛在被害人被詐騙成功。

8.加/被害人網路聊天活動分析，透過雙方聊天的方式(講話的話術)最能突破被害人的心防，詐騙成功。

（二）相異點

綜合網路詐欺被害問卷調查結果與網路詐欺加害者深度訪談之資料，針對以下共同問題進行分析後，得到以下相異性的結果，彙整如表 6-1-1：

表 6-1-1 網路詐欺被害者與加害者對於網路詐欺犯罪之相異點

	網路詐欺被害問卷調查	網路詐欺加害者訪談
被害人口特性	男性、年紀較小(約 40 歲以下)、月收入約未滿 4 萬元者、大專程度以下者以及學生、從事網路資訊工作、實體交通物流工作以及製造業者，顯著地有較高的網路詐欺被害經驗。	年齡介於 35 至 50 歲間有一定財富累積者、女性、大學生、老年人以及所處地都市化程度不高之居民，均是容易遭網路投資與網路購物詐欺的對象。

詐騙後是否報案	近 7 成的被害者選擇不去報案，因為報案程序複雜。	被害人都會去報案，從帳戶被關閉得知，速度很快。
警察偵辦能力	被害人會質疑警方的破案能力。	認同臺灣警察在網路犯罪方面的查緝與偵辦能力是很厲害的，渠等最後都會被警察追查、查緝到案，只是時間的早晚而已。

五、我國當前網路詐欺犯罪防制策略之現況分析

我國行政院於 2022 年 7 月 15 日訂頒「新世代打擊詐欺策略行動綱領」，透過跨部會合作共同打擊詐欺，如 2022 年減少民眾遭詐騙金額逾 67 億元、2022 年 8 - 12 月詐騙簡訊案件數大幅下降 9 成、疑涉詐欺境外警示帳戶全年成功攔阻 135 案，金額 1 億 4 千多萬元、2022 年較 2021 年查獲詐欺集團件數提升 30%、查獲嫌犯數提升 40%。面對電信等詐欺案件犯罪型態與技術不斷演化，行政院已陸續通過「打詐 5 法」（《中華民國刑法》、《人口販運防制法》、《個人資料保護法》、《洗錢防制法》、《證券投資信託及顧問法》）修正草案，嚴懲深偽詐騙、私行拘禁及人口販運，並加重相關詐欺罰則，強化網路平臺落實廣告實名制，並於 2023 年 5 月 4 日通過「新世代打擊詐欺策略行動綱領 1.5 版」，精進「識詐、堵詐、阻詐、懲詐」4 大面向，運用公私協力推動各項防詐作為，達到「減少接觸、減少誤信、減少損害」3 減目標，以全面降低詐騙受害事件[19]。

根據本研究第二次焦點體座談，與會專家學者認為我國網路詐欺犯罪防制策略所面臨之問題與瓶頸，從以下四個層面分析。

（一）識詐層面(教育宣導面)

[19] 新世代打擊詐欺策略行動綱領 1.5 版。行政院官網: https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/f70eba6b-d72b-4b00-9942-b9e00aa34e4b

1.目前識詐教育，並沒有針對分齡分眾與網路詐欺類型，製作明確的防詐宣傳海報或影片，以提升民眾知能。

2.第一線執法人員的專業知能與執法技巧之精進與強化，也很重要。

3.近年來網路投資詐欺金額有增加趨勢，網路投資重複詐欺的個案也日趨嚴重，被害人甚至不願意承認自己已被詐騙，經過一段很長的時間後(例如兩個半月後)才報案；被害人數呈現出 M 型化的分布，亦即會被詐騙的人就是會一直被騙下去。

（二）堵詐層面(電信網路面)

1.目前 165 反詐專線僅是內政部警政署刑事警察局下一個股的層級，與其他部會溝通、協調並請求支援，甚至跟民營機構溝通、交涉，位階過小，能力有限。

2.因為「數位中介法」沒有通過立法，許多網路詐欺犯罪之行為就無法監控，對於堵詐限縮其效能。

3.運用高科技，甚至運用 AI 技術來提升科技辦案以堵住網路詐欺犯罪，仍嫌不足。

4.犯罪嫌疑人將整個網路詐騙行為予以分工，例如有人建置網站賣錢、有人買網站給機房使用、處理金流的人是領月薪並沒有實際從詐騙錢財中獲利。這些分工乍看之下各自獨立、每個行為人都主張自己沒有犯罪，但連結後就是網路詐騙集團。然而司法實務也會認為無具體證據證明渠等為網路犯罪集團或組織，無法起訴。

5.網路平臺業者應該負起審查廣告內容的責任，有些犯罪人已被檢舉其廣告、粉專網頁或是偽裝名人進行詐騙，平臺依然沒有採取行動。

（三）阻詐層面(贓款流向面)

1.目前政府與產業合作的量能與授權的業務，似乎仍嫌過少，因為產業界也希望與政府合作建立防護網，阻斷詐騙集團的金流。

2.目前臺灣偵查網路詐欺犯罪，特別是運用區塊鍊、加密貨幣進行金流資產的轉移部分，阻詐能力仍嫌不足。

3.許多詐騙案都沒有人知道，所以也沒有辦法介入，但唯一例外

是金融機構或銀行，而目前銀行的介入已經很積極，但似乎可以再強化。

4.目前針對不同網路詐欺型態，例如投資詐騙與網拍詐騙，手法、金額與詐騙期間都不同，其防制策略應該有所不同。

（四）懲詐層面(偵查打擊面)

1.跨國跨境的司法互助很重要，但目前的司法互助大都鎖定檢察官層級，曠日廢時，且徒勞無功。

2.目前我國派駐各國的警務聯絡官，在扮演跨境查緝網路詐欺案件的角色，非常吃重，人力與據點因隨著詐欺集團的擴散而增加。

3.與跨境跨國的警政部門之合作很重要，如果關係緊密者，請求其回覆協查的資訊就很快，反之就很慢，甚至石沉大海。

4.目前政府欠缺網路詐騙案件專家鑑定的機制，可以彌補警方在科技偵查上的不足。

5.雖然通過「打詐 5 法」，但根據過往經驗，法院在裁處方面可能沒辦法有效的落實，以達嚇阻功效。

6.專責偵辦單位，目前政府所提供的資源有效，且橫向連結不足、金融機構基於保護個資也不願配合提供相關資料，造成偵辦網路詐欺案件常存在斷點的現象。

7.網路詐欺犯罪有其模式與伴隨一些網路媒介的普及有其盛行性，比如說之前 Telegram 流行大概 2、3 個月，詐騙模式與手法就會一直變。造成執法人員一直在後追趕其行為模式，在防堵上也比較難對症下藥。

8.不僅第一線執法人員在網路詐欺犯罪的執法量能不足外，現行懲罰力道不夠強、無嚇阻性，導致很多詐騙犯容易再犯。而過往「竊盜犯贓物犯保安處分條例」規定，對於犯罪人除科以刑罰外，還附加強制工作，但被宣告違憲後(釋字第 812 號)，刑罰之威嚇效能大為降低。

第二節　建議

近年來網路詐欺犯罪之問題，已成為政府各部門重要的施政議題。尤其是行政院於 2022 年 7 月 15 日訂頒「新世代打擊詐欺策略行動綱領」，整合跨部會之力量與資源共同打擊詐欺犯罪，以展現政府全力打擊詐欺犯罪之決心。在中央與地方、公私部門合作協力的情況下，已初見成效，例如詐欺犯罪之數量已見減少，但詐欺犯罪之金額與態樣，似乎仍然方興未艾。本研究綜覽國外文獻、編製網路詐欺被害之問卷並進行調查分析、以及透過政策焦點團體座談之意見，分別提出治本策略與治標策略之政策意涵如下，提供政府相關部門作為精進當前打詐策略行動綱領之參考。

一、治本策略

（一）網路詐欺與被害型態變動快速，須及時掌控方能有效防制

本研究透過網路詐欺被害調查，分析不同類型的網路詐欺被害情況和趨勢，並探討新興的網路平臺或 APP 對網路詐欺犯罪和被害的影響。研究發現，過去一年半，猜猜我是誰(假冒親友)曾是位居第二位常見的網路詐欺類型，但最近一次卻跌至第七位，而網路投資詐騙則上升至第二位。這些變化反映網路詐欺犯罪者不斷變換詐騙手法和管道，利用新興的網路平臺或 APP 吸引網路詐欺被害人掉入陷阱。因此，無論是網路詐欺犯罪偵防或被害預防宣導，均須透過官方統計資料、犯罪被害人報案系統和犯罪被害調查等資料分析，才能及時掌控網路詐欺被害的態樣、管道、互動模式、詐騙手法等，有效防制網路詐欺犯罪與被害。

（二）針對可能導致網路詐欺被害的誘因與動機，提供示警機制

本研究透過統計分析結果顯示，一般組與被害組在被害誘因與動機上有顯著差異；邏輯斯迴歸分析結果則顯示，被害誘因與動機是影響網路詐欺被害的關鍵因素。如能避免點擊不明來源的電子郵件及未知檔案，避免下載不明來源的檔案等，以及減少遊玩網路遊戲、瀏覽色情網站、網路聊天，則能有效降低網路使用者遭受詐欺被害之風險。

為能減少網路使用者遭受詐欺被害的風險，建議應該提高網路使用者的安全意識和防範能力，並對容易引發被害的誘因和高風險的動機，設置有效的警示機制。

（三）強化民眾對網路成癮之認知，並提供成癮者及其家庭協助

本研究網路詐欺被害調查結果顯示，網路成癮對網路詐欺被害具極顯著的影響力，網路成癮者往往無法控制其網路過度使用網路，對人際互動、情緒、健康、生活與工作影響；以及曝露於網路詐欺被害之風險。此外，本研究調查結果顯示，逾 90%受訪者有使用各類網路平臺及 APP 等經驗，網路與生活已密不可分，因此，須強化一般民眾對於網路成癮的認知，以及醫療體系有關網路成癮的診斷與輔導(或治療)，以提供網路成癮者及其家庭所需的協助，除有助於網路成癮之處理，亦可降低網路詐欺被害之風險。

（四）針對有創傷症候群之詐欺被害人，提供心理輔導和社會支持

本研究探討網路詐欺對被害者的心理影響，發現部分被害者因受到創傷而難以恢復正常生活。為了協助這些被害者，本研究提出以下心理輔導和社會支持服務的建議：1.利用現有或新建的心理輔導平臺或專線，提供被害者線上、電話或面對面的心理輔導服務，讓被害者能與專業的心理輔導員溝通，並根據其個別需求和困境，提供適合的心理介入和治療方案，以紓解情緒困擾，恢復自信和自尊。2.由有相同受害經驗者組織或組成互助團體，定期舉辦面對面或線上的聚會和活動，並邀請有專業知識或成功復原的人士分享見解和經驗，讓被害者能在一個互相支持和分享的社群中，與其他受害者建立正向的人際關係和正確的網路使用習慣。

（五）政府應定期且常態性地進行網路犯罪被害經驗之調查

隨著網路犯罪的日趨嚴重，世界各國對於網路詐欺犯罪之調查方式，已由傳統犯罪被害調查的管道，亦即從一般市民的電訪(Telephone-operated crime survey)和面訪(Face-to-face interview)中先增加網路犯罪被害經驗的調查開始，然後逐漸擴充網路犯罪被害之型態，然後再發展成專屬網路犯罪被害之調查，包含電訪、面訪或

網路報案(Online report)（例如美國聯邦調查局的 IC3 報案介面），甚至已成為制度化，每一年都有官方報告產出，例如美國 FBI 的網路犯罪報告(Internet Crime report)。反觀國內對於網路犯罪與詐欺的調查，僅透過官方資料的統計分析，而 165 專線大多以諮詢為主，仍請被害者至派出所報案。換言之，如果沒有此次委託研究，目前國內恐無針對網路詐欺被害進行調查之機制與管道。因此，建議政府應該將網路犯罪與詐欺被害之調查，指定一個部門，例如內政部警政署或數發部資安署，專責進行調查，並定期製作報告，以讓國內較為正確且完整的了解臺灣當前網路犯罪與詐騙的狀況。

二、治標策略

（一）試詐層面(教育宣導面)

1.加強網路防詐觀念和技巧，提高被害人自我防護能力

由於網路詐欺被害多發生在晚上，且多數被害者不認識加害人，因此需要加強對於晚間上網者和陌生人聯繫者的防詐教育和宣導；並提升個人在網路上的道德和法律意識，避免參與或支持任何不道德或不合法的行為。由於本研究發現社群軟體、購物網站和線上遊戲等網路平臺為詐欺被害人最常使用的管道，建議可以透過上述網路平臺，提供一些常見的詐騙手法和防範方法的資訊，並提醒使用者不要輕易相信或轉帳給不認識的人。此外，也可以利用媒體或公共場所，廣泛傳播一些防詐觀念和認知，加強公眾對於不同類型和手法的網路詐欺的認知和警覺，提高防詐觀念和大眾的警覺性，以強化網路詐欺被害人的自我保護能力。

2.對於網路詐欺被害高風險族群進行分群分眾犯罪預防宣導

本研究透過網路調查和深度訪談，探討人口特性與網路詐欺被害的關係。網路調查發現，人口特性與網路詐欺被害有顯著關聯性；深度訪談結果顯示，網路詐騙加害者會根據不同的人口特性，選擇合適的時間和手法實施詐騙。依據生活型態曝露理論，人口結構會影響個人網路生活型態和曝露於網路被害之機會。為提升網路使用者對於詐欺被害的認知和預防觀念，本研究建議針對不同人口特性的被害者，應進行分群分眾的網路詐欺被害預防宣導。由於網

路詐欺犯罪具有多樣性與變異性，一套識詐的教育宣導文宣或教材，已不足以為因應。因此，有關識詐之教育宣導教材，應該根據不同的年齡群以及不同的網路詐欺犯罪型態，分齡分類製作不同的教材才對。例如大學生或年輕族群者，容易遭受網路購物詐欺被害，因此針對該年齡層者應製作網路購物詐欺被害之教育宣導教材；又如年紀較長且有一定資產者，容易遭受網路投資詐欺被害，因此針對具資產者製作網路投資停看聽之教育宣導教材，特別是網路投資與金融投資一樣，「投資一定有風險，沒有穩賺不賠的，投資前應該詳閱相關投資說明書」，如果沒有這種警語者，詐騙型投資的機率很高，應該於教育宣導時多加強化。高中生或大學生或無業者最易被詐騙集團吸收為擔任車手，因此當有一些雇工廣告內容提及「無經驗、負責提款並交給公司、獎金/薪水優渥」等字樣時，即可能是詐騙集團招募車手的廣告或宣傳單。

3.犯罪預防宣導保證獲利的字眼，應屬詐騙宣傳手法

提倡全民資安意識教育，應屬政府目前打詐的重要治本策略。其中金融投資部分，應該要提醒民眾投資有賺有賠，投資前應該詳閱公開說明書。而詐騙集團就是要詐騙投資者的金額，因此不會有險公開說明書。因此，政府應該要教育民眾，在從事某些投資前，要了解其風險在哪裡，像虛擬貨幣，不了解就不要亂投資；愈瞭解者則要告知無保證獲利的字眼或證明，有保證獲利者應屬詐騙宣傳手法，應該予以辨識清楚，以有效降低被害機會。

4.宣導民眾接獲不明電話或網購超乎便宜商品，務必再三求證

從加害者的訪談得知，渠等對於被害者對於接獲不明電話以及於網購時超乎便宜之商品，均未予以求證，即受騙上當，深感不解。認為不明電信的詐欺以及購買超乎便宜的商品，不應該再三求證嗎？因此，政府仍需對於電信詐欺的犯罪以及假網購詐欺犯罪型態，於犯罪宣傳時，加註與強化務必再三求證的字眼或宣導，降低民眾於接獲詐騙電話或面臨假網購時，驚慌失措或利益薰心(貪小便宜)，失去戒心，進而成為詐騙集團之獵物。

（二）堵詐層面(電信網路面）

1.盡速制訂與通過防制詐欺犯罪之相關法律

所謂「工欲善其事，必先利其器」，我國目前有關「數位服務法」與「科技偵查法」等，因有相關個資外洩疑慮或考量言論自由與意見表達等權利，尚未立法通過，導致在追訴網路詐欺犯罪上，仍存在許多偵查上之限制。反觀德、英、美、法、奧地利及西班牙等國非常強調人權之西方國家，針對個資外洩防護、特定網路銀行使用或 OTT 通訊服務資料無法調取的部分，已有相關立法規範；而英國及澳洲也立法保留網際網路流量紀錄；此外，針對約束社群媒體業者行為(例如違法內容通報及處理機制)部分，歐盟執委會於 2022 年也通過「數位服務法」。這些都是國內法制尚未完備而需要盡速解決之處。

2.仿照毒品犯罪制定「詐欺犯罪防制條例」專法

目前我國對於毒品犯罪，立有「毒品危害防制條例」專法，專門負責打擊與防制毒品犯罪。根據這樣的立法思維，長遠來講，政府應可以考慮訂立「詐欺犯罪防制條例」的專法，統合資源，把資通訊防制及偵查措施都納進來，像警語頁面、M 化車及設備端通訊監察偵查手段的使用、網路平臺者對於詐欺的協力義務等等，全部納入立法。晚近也有類似的立法作為，例如法務部研擬於「組織犯罪防制條例」中將警用 M 化車增訂法源依據，讓警方執法有所依據。

3.應於行政院層級常設打詐專責辦公室

鑒於打擊網路詐欺犯罪案件涉及內政、外交、數位、金融以及陸委會等跨部會之業務，以目前內政部警政署刑事警察局所設置之「打擊詐欺犯罪中心」為主責部門，實在力有未逮，許多事情仍需透過行政院政務委員透過召開跨部會、跨公私部門之會議，溝通、協調，始獲改善，但時間上已錯失先機。此外，法務部於 112 年 5 月於臺灣高等檢察署成立「查緝詐欺及資通犯罪督導中心」，與內政部警政署之「打擊詐欺犯罪中心」之業務是疊床架屋，還是分工合作？仍未清楚。換言之，無論是以目前刑事局所設之打擊詐欺犯罪中心或法務部之「查緝詐欺及資通犯罪督導中心」，做為當前我國打擊詐欺犯罪工作之主責部門，層級過低也與國際間的發展趨勢不符。

（三）阻詐層面(贓款流向面)

1.應與公私立金融資訊機構建立資安互助合作機制

過去內政部警政署 165 反詐騙專線與公私立金融資訊行號欲建立資安互助合作平臺與機制，困難重重。今年 6 月 1 日後，內政部警政署刑事局打擊詐欺犯罪中心整合 165 反詐騙專線業務，打詐中心現在已陸續與事實查核機構(MyGoPen)、Whoscall、中華資安、臺灣大以及趨勢科技等，都簽有資安與網路的合作項目與機制；然而在金融機構部分，雖有逐年增加，仍略顯保守。金融交易系統對於保護客戶帳號的安全，已投注相當多的財力與資源，但仍希望與警界或執法單位建立資訊安全、系統安全與個資安全的互助合作。不應該有因為該金融機構的資安長有警政背景，所以比較容易獲得警政的合作與協助，共同打擊網路詐欺集團。所以政府應該要有一致性的做法，與各金融機構建立資安互助合作協定與資安資訊平臺機制的建立，大家互通情資，共同打擊網路詐欺不法行為。而政府應該要求企業每一年應該提撥其營業額的百分比挹注於資安的防護，進而保障金融交易的安全。

2.建立跨國跨境警務偵查互助合作平臺

鑒於網路詐欺犯罪屬於跨境與跨國犯罪型態，透過層層分工與專業化分工後，一個犯罪行為切割為數個犯罪分工，彼此獨立但有串接，更重要的是，犯罪地點與犯罪結果地點具有分離性，例如詐騙機房在 A 地，但取得詐騙的錢財卻是在 B 地。因此，偵辦網路詐欺犯罪必須大量仰賴跨國、跨區警務人員的合作始得克竟其功。且相較於檢察官的司法互助，警務人員的偵查互助更具有時效性與立即性。故透過我國駐外警務人員與鄰近國家建立共同偵查跨國跨區網路詐欺犯罪，實屬當前要務。例如晚近許多詐騙集團群聚於東南亞國家設置詐騙機房詐騙大陸地區民眾或臺灣地區民眾，代表東南亞已成為臺灣詐騙集團之熱區或熱點，因此，實有透過警政署駐外警務聯絡官與當地警政部門穿針引線，建立共同打擊、偵查網路詐騙集團行為之平臺，為降低東亞地區網路詐騙犯罪行為共同努力。

3.簽署保全電子證據之國際協議與協定

由於網路犯罪的激增，電子證據儲存於不同的司法管轄區的情形日益嚴重，因此國際間對於電子證據的保存已漸有共識，遂於2021 年 11 月 17 日正式通過「布達佩斯網路犯罪公約第二附加議定書」(The second additional protocol to the Budapest Convention on Cybercrime)，而簽署此一議定書的國家，可以將網路犯罪者所犯之罪且存放於國外、可移轉或未知地點伺服機上的電子證據，透過互助協定的方式，協助偵辦或起訴國家的執法當局取得，而其作法已包含與服務提供商和註冊商直接合作，以加快取得與犯罪活動相關之訂戶資訊和流量數據的手段。然而我國目前受限於外交處境，也非布達佩斯公約或類似公約的成員國，馬上要取得簽署前揭公約的機會很低。但可以逐漸互惠的方式，透過個案與請求國、被請求國逐步建立規模化的協議協定(protocol)，甚至援引目前已被全球認可的布達佩斯公約模式作為基礎架構，以利與國際接軌，例如先透過進入 24/7 Cybercrime Network，在透過此一平臺、國家，以個案方式簽署協議協定，從點逐漸擴展成線、面的方式，尋求國外服務提供商和註冊商協助保存相關電子與電磁紀錄，俾有效達到刑事司法互助請求之目的(陳昱奉，2022)。

4.仿照新加坡模式應由金融主管機關主導情資交換

新加坡的防詐以及防洗錢的措施，係透過立法方式，由新加坡金融管理局主導，計畫先由六家主要銀行交換資訊，之後逐漸擴展至金融體系。透過法律的授權，讓銀行把風險高的客戶交易資料上傳到政府建構的平臺，對於其他同業就會產生警示作用，政府帶頭來做，其他公民營金融機構配合度當然就會高。然而此一部份涉及民眾的個資，當然需要法律的授權，所以新加坡現在處於立法的階段，香港也有類似的發展，但我國立法部門比較保守，這個策略有待突破。

5.招募超商職員以及金融機構行員參加車手/潛在被害人辨識營

本研究顯示，詐騙集團仍是以招募車手作為提領詐騙人頭帳戶金錢為取得不法所得之主要方式。因此，強化車手於超商 ATM 提領現金的辨識或強化金融機構行員對於疑似被詐欺民眾進行提領現

金時的辨識，是阻斷詐騙金錢流向詐騙集團之重要做法。本研究建議，警政署刑事警察局或各縣市警察局應針對車手提領影像所彙整的特徵、穿著或行為，協調當地的超商業者，針對行員進行教育辨識；再者，各縣市警察局亦可以協調當地金融機構，開辦疑似遭詐民眾辨識營，共同合力阻詐，阻斷詐騙集團詐騙成功的機會。

（四）懲詐層面(偵查打擊面)

1.強化網路詐欺之查緝，並提升民眾對執法機關之信心

本研究發現，許多被害者因為認為損失不大，而且報案過程繁瑣和沒有效果，所以只好自己吞下苦果。但是，這樣的心態可能會讓詐騙集團肆無忌憚，持續進行犯罪活動，造成更多人的損失。首先，應簡化報案程序，讓被害者能夠更容易和快速地向警方報案。如能讓報案程序更簡便和高效，就能夠鼓勵被害者向警方報案，並提高警方對於網路詐欺案件的掌握和處理。其次，應提高警方對於網路詐欺案件的破案率，讓被害者感到報案是有意義和有幫助的。例如，可以加強對於 ATM 轉帳的監控和追蹤，並提高對於小額受騙案件的受理率和處理效率。最後，建立一個跨部會整合且持續更新的網路詐欺資料庫，以收集和分析不同類型的詐騙手法和特徵，並提供給相關單位作為偵查和嚴懲之參考，以減少被害發生的可能性。

2.強化打擊詐欺犯罪中心之部門與陣容

刑事局於 112 年 6 月 1 號將 165 反詐騙專線結合打擊詐欺犯罪中心，並在中心設有資通研析股（針對網路跟電信的部分）、金融研析股（針對洗錢高風險行業、遊戲點數、虛擬帳號、虛擬貨幣的對策或研究）、綜合研析股（行動管理的政策面跟打擊面）和 165 股（負責詐欺報案系統）。各業務股分工似乎明確，功能逐步提升中。然而這樣的陣容仍缺乏跨國與跨域領域的合作以及擬定相關國際互助協議或協定之研究與簽約部門，殊為可惜。因此，建議應該將跨國跨域合作的業務以及國際資安公約之業務納入，前者可以根據網路詐欺犯罪之熱點、熱區或熱國，協調或增加相關的駐外警察與當地警政部門合作，建立共同打擊詐欺網絡；後者可以透過外交單位的接洽與協助，尋求相關國際公約的簽訂，例如 24/7 Cybercrime Network，盡快保全網路犯罪之證據。甚至掌握國際間有

關網路犯罪或資訊安全之會議，派員與會參加，以掌握國際間網路犯罪之新型態並建立良好互助關係。另外，民眾網路遭詐的報案方式，可以規劃以網路報案的方式進行，以符合國際趨勢。

3.根據網路詐欺犯罪熱點與移動適時增加駐外警務人員

目前臺灣已於一些國家派駐警務聯絡官，蒐集與協助打擊與偵查跨國跨境網路詐欺犯罪，成效斐然。然而網路詐欺犯罪具有變異性與匿名性，許多網路詐欺犯罪經常遷移、移動，甚至有些地區已成為網路詐欺題集團群聚的熱點，但一段時間後可能又轉移陣地到其他國家或區域。因此，警政部門應該隨時掌握網路詐欺犯罪的熱點與遷移路徑，適時增加境外的警務聯絡官，以協助當地與國內破獲網路詐騙成員與集團。

4.第一線執法人員之定期專業教育訓練

由於網路詐欺犯罪的多樣性與變異性，例如晚近釣魚連結從過去的簡訊擴大至實體信件，附上 QR Code 及 Line ID，誘騙民眾到詐欺群組後行騙；又如一些詐欺模式流行一段時間後，又會變異改為其他模式，但目的都是要詐騙民眾的投資、購物或解除相關的帳號等錢財。面對網路詐騙犯罪變異性與多樣性的特性，第一線執法人員的專業教育訓練特別重要。刑事局近年來其實有一直有在規劃與執行科技偵查人員的教育訓練，例如 2023 年 7 至 8 月間內政部警政署召訓全國各警察機關資訊與科技偵查人員，辦理兩梯次各為期 5 天的犯罪情資分析課程，以「科技偵查犯罪情資」、「數位金融情資」以及「公開網路情資」3 面向為主軸進行教育訓練，以面對不斷演化的新型態詐欺犯罪。未來警政部門除應該持續辦理此一教育訓練外，亦能邀請國外相關警政人員及資安師資分享跨國跨境查緝網路詐欺犯罪的案例分享，以強化第一線科偵人員的執法能力與專業知識。

5.科偵部門應該運用 AI 或大數據進行犯罪手法分析

科偵部門目前針對假投資網站有做警語頁面，我們可以在像是外匯天眼這種反詐欺投資平臺，看到許多被害人因為看到這個頁面而驚覺被詐，但這些網站不同域名眾多且更新迅速，建議可比照 iWIN 建構快速通報下架機制，同時結合 165 的大量被害情資，以

AI 智能化的方式自動化找出新生成的域名加以停止解析。亦即執法人員在相關法律同意且授權的情況下，例如「科技偵查法」的規定與授權，可以以 AI 智能化的方式，自動化找出新生成的域名相關情資，為全球跨境電子商務產業(例如 Amazon、日本樂天等)做出貢獻。

6.提高網路詐欺犯罪者懲罰之刑度或提高量刑

根據犯罪學理性選擇理論(Rational Choice Theory)之主張，犯罪人從事犯罪行為一定都是衡量過犯罪成本與犯罪所得後，覺得所得高於成本，始決定遂行。因此，墊高犯罪成本始能嚇阻犯罪人從事網路詐欺的行為。而針對目前刑罰一罪一罰部分，乍看有威嚇性，但實際上法官的定執行刑才是重點。因此，建議透過修法方式，加重網路詐欺犯罪之刑度，進而限縮法官的裁量權，促其加重刑度之裁量。甚至對於網路詐欺犯罪者，若沒有與被害人和解或繳交詐欺犯罪所獲得之利益者，不得予以假釋，以墊高或加重其犯罪之成本。必要時，應該恢復刑罰附加強制工作，對網路詐欺犯構成較重的威嚇效應。

本研究治本與治標之具體建議，彙整如表 6-2-1。

表 6-2-1 本研究具體建議彙整表

面向	層面	具體作為之建議
治本		1.網路詐欺與被害型態變動快速，須及時掌控方能有效防制。 2.針對可能導致網路詐欺被害的誘因與動機，提供示警機制。 3.強化民眾對網路成癮之認知，並提供成癮者及其家庭協助。 4.針對有創傷症候群之詐欺被害人，提供心理輔導和社會支持。 5.政府應定期且常態性地進行網路犯罪被害經驗之調查。
治標	識詐	1.加強網路防詐觀念和技巧，提高被害人自我防護能力。

		2.對於網路詐欺被害高風險族群進行分群分眾犯罪預防宣導。 3.犯罪預防宣導保證獲利的字眼，應屬詐騙宣傳手法。 4.宣導民眾接獲不明電話或網購超乎便宜商品，務必再三求證。
	堵詐	1.盡速制訂與通過防制詐欺犯罪之相關法律。 2.仿照毒品犯罪制定「詐欺犯罪防制條例」專法。 3.應於行政院層級常設打詐專責辦公室。
	阻詐	1.應與公私立金融資訊機構建立資安互助合作機制。 2.建立跨國跨境警務偵查互助合作平臺。 3.簽署保全電子證據之國際協議與協定。 4.仿照新加坡模式應由金融主管機關主導情資交換。 5.招募超商職員以及金融機構行員參加車手/潛在被害人辨識營。
	懲詐	1.強化網路詐欺之查緝，並提升民眾對執法機關之信心。 2.強化打擊詐欺犯罪中心之部門與陣容。 3.根據網路詐欺犯罪熱點與移動適時增加駐外警務人員。 4.第一線執法人員之定期專業教育訓練。 5.科偵部門應該運用 AI 或大數據進行犯罪手法分析。 6.提高網路詐欺犯罪者懲罰之刑度或提高量刑。

第三節　研究限制與建議

首先，本研究旨在蒐集國內外網路詐欺之相關調查或官方資料，並探討網路詐欺被害者的人口特性、心理特質、網路生活型態與情境機會，以及網路詐欺被害經驗等變項。但受限於研究期程與經費預算，本研究設計上將一般民眾和被害樣本分為二個次母群體，並編製網路詐欺被害調查問卷進行調查。此項設計有助於了解網路詐欺被害的類型分布、時空特性、手段等，比較一般組與被害組之差異，以及找出可能影響網路詐欺被害的關鍵因素。但整體樣本結構無法推估臺灣地區 18 歲以上網路使用者詐欺被害的盛行率與黑數。因此，單靠網路調查無法反映真實的被害情況和盛行率。建議未來的研究結合網路調查與實體調查，進行大樣本(如 1 萬人以上)的網路詐欺或犯罪被害調查。這樣可以增加樣本的多元性和代表性，提高資料的可靠性和效度。同時，也可以與國際上相關被害調查結果進行比較分析，探討臺灣地區在網路詐欺或犯罪被害方面的特殊性或普遍性。

其次，本研究所召募之網路詐欺犯罪加害者，雖然有五位，但犯所從事之犯罪型態僅三種，即網路投資、網路購物與電信詐欺。雖然都是當前熱門的網路詐欺之犯罪型態，但仍有不足之處，例如網路投資，已進階到加密貨幣、區塊鍊之詐欺行為，但本研究所召募的加害者並非專精此一犯罪類型；又如愛情詐騙，晚近也頗為猖獗，但本研究並未召募成功。換言之，在本研究之召募過程中，部分犯罪加害人可能因為其所了解的犯罪集團、手法與專業性頗深，拒絕接受訪問，因此，本研究難以成功地召募各類型網路詐欺加害者接受深度訪談，頗為遺憾。基於上述限制，未來研究應思考如何突破加害者的心防。建議可採取更有效的策略和方法，如透過各種管道接觸加害者，提高誘因或保障讓加害者願意受訪，亦可採用靈活和開放的訪談方式讓加害者感到舒適和自由。這將有助於增加樣本數量和多樣性，提高樣本質量和可信度，豐富樣本內容和深度。只有更全面和深入地了解各類型網路詐欺加害者的心理和行為特徵，有效和精準地分析各類型網路

詐欺加害者之間的關聯性和差異性，才能讓外界更了解其詐騙手法與行銷策略，進而提出更精確的防制對策。

再者，本次研究的範圍僅限於個人或家庭受到的網路詐騙或其他犯罪的影響，未包含商業被害的情況，殊為可惜。然而，商業被害(Business victimization)類型主要以詐欺、侵權和稅務違法為最大宗，亦為一個嚴重且普遍的問題，對於企業和社會的發展都有不利的影響。這些案件不僅造成企業財產和信譽的損失，也影響了消費者、投資者和合作夥伴的信心和權益。因此，建議未來研究應將商業被害調查納入，政府亦應對商業被害相關問題也加以重視，制定有效的預防和應對措施，以保障企業和社會的安全和發展。

參考資料

一、中文書目

孔令維（2018）。論網路犯罪偵查相關數位證據-以網路即時通訊軟體為中心。國立高雄第一科技大學碩士論文。Retrieved from https://hdl.handle.net/11296/46u736

方呈祥（2020）。網路詐欺被害之性別差異—以網路日常活動與自我控制理論分析。中央警察大學碩士論文。 Retrieved from https://hdl.handle.net/11296/q2z4ep

王文科、王智弘 （2020）。教育研究法。五南圖書出版股份有限公司。

王秋惠（2007）。網路詐欺被害特性與被害歷程之研究。中央警察大學犯罪防治研究所碩士論文。Retrieved from https://hdl.handle.net/11296/w2n4gd

王茜（2014）。網路成癮, 網路偏差及網路詐欺被害者之關係: 人的聚合還是網路活動場域的聚合?。 臺北大學犯罪學研究所碩士論文。Retrieved from https://hdl.handle.net/11296/qdmb9e

古慧珍（2005）。我國網路詐欺防制之研究--以使用人頭帳戶為中心。國立交通大學科技法律研究所碩士論文。

田明府（2021）。5G 時代網路犯罪偵查模式之研究-以詐欺犯罪為例。銘傳大學碩士論文。Retrieved from https://hdl.handle.net/11296/2zunjx

石泱、王乃琳（2021）。青少年偏差行為和網路不當行為影響因素之研究。青少年犯罪防治研究期刊，13（2），1-41。

何英奇（2015）。大學生網路性成癮之評估及相關因素的研究。學生事務與輔導，53（4），46-61. doi:10.6506/sagc.2015.5304.05。

吳嫦娥（2004）。未成年人網路偏差與被害問題透視。透視犯罪問題（4），26-30。doi:10.6356/pc.200409.0026。

周愫嫻（2014）。青少年網路虛擬身分與網路被害、不當行為。犯罪與刑事司法研究，(22)，45-73。

周愫嫻（2014）。青少年網路虛擬身分與網路詐欺被害、不當行為。犯罪與刑事司法研究，(22)，45-73。

周愫嫻、曹立群（2014）。犯罪學理論及其實證。臺灣五南圖書出版

股份有限公司。
林宜隆（2000）。網路犯罪之案例分析。中央警察大學學報，頁221-252。
林宜隆、楊鴻正（2001）。網路交易犯罪之偵查要領─ 以網路詐欺犯罪為例。Journal of Information, Technology and Society，創刊號，135-151.
林師賢（2021）。大學生網路犯罪防治研究。逢甲大學碩士論文。臺中市。Retrieved from https://hdl.handle.net/11296/3jzerp
洪瑞聰（2014）。國中學生自我控制能力對網路偏差行為之影響。樹德科技大學碩士論文。Retrieved from https://hdl.handle.net/11296/w7cb4y
張家愷（2023）。運用資通技術打擊犯罪偵查實務（一）：大數據分析運用於科技偵查。2023 年內政部警政署第五屆犯罪情資分析課程簡報講義。
章美英、許麗齡（2006）。質性研究－焦點團體訪談法之簡介與應用。護理雜誌，53（2），67-72。doi:10.6224/jn.53.2.67。
許春金（2017）。犯罪學（第八版）。
許春金（2022）。人本犯罪學（第三版）。三民書局。
許春金、陳玉書 （2003）。性侵害犯罪被害情境與要素之分析。警政論叢，3，101-128。
許春金、陳玉書、莫季雍、孟維德、蔡田木（2000）。臺灣地區犯罪被害經驗調查研究。法務部、內政部警政署委託研究。
許春金、陳玉書、孟維德、蔡田木、黃蘭媖、黃家珍、施雅甄、黃曉芬（2005）。94 年臺灣地區犯罪被害調查。內政部警政署委託研究。
許春金、陳玉書、孟維德、蔡田木、黃蘭媖（2010）。99 年臺灣地區犯罪被害調查。內政部警政署。
許春金、謝文彥、黃蘭媖、呂宜芬、游伊君（2021）。犯罪被害狀況及其分析－我國首次犯罪被害趨勢與服務調查報告。刑事政策與犯罪防治研究專刊（30），47-91. doi:10.6460/cpcp.202112_（30）.02。
許華孚、黃光甫（2020）。跨境犯罪-電信詐騙專書。一品出版社。
陳玉書（2004）。社會治安與犯罪被害恐懼感。犯罪防治學報，5，

39-58。
陳玉書、王秋惠（2011）。網路詐欺被害特性分析。執法新知論衡，7（2），11-31。
陳玉書、邱炫棉（2006）。犯罪被害恐懼感影響因素之分析。犯罪防治學報，7，1-42。
陳玉書、曾百川（2007）。網路詐欺犯罪理性選擇歷程之質性分析。中央警察大學犯罪防治學報，8，115-146。
陳玉書、葉碧翠（2022）。網路被害特性與情境預防。2022 年犯罪防治「犯罪預防、犯罪分析與婦幼保護」學術研討會，中央警察大學。
陳玉書、簡鳳容、呂豐足、劉士誠（2020）。網路犯罪被害：人口特性與情境機會的影響。刑事政策與犯罪研究論文集。113-148。
陳昱奉（2022）。網路犯罪與資訊安全的未來–從網域名稱扣押談網路治理。刑事政策與犯罪防治研究專刊，32，219-290。
陳煌明（2019）。網路犯罪之成因、現象及防治策略-彰化縣警務人員觀點。國立中正大學碩士論文。嘉義縣。Retrieved from https://hdl.handle.net/11296/uq3a7x
曾百川（2006）。網路詐欺犯罪歷程之質化研究。中央警察大學碩士論文。桃園縣。Retrieved from https://hdl.handle.net/11296/e5h8rw。
游子興（2019）。以校園網路連線大數據驗證六度分隔理論。國立臺灣大學計算機及資訊網路中心電子報，第 51 期。https://www.cc.ntu.edu.tw/chinese/epaper/0051/20191220_5102.html
黃祥益（2006）。臺灣地區少年網路犯罪與被害特性之研究。中央警察大學犯罪防治研究所碩士論文。
萬文隆（2004）。深度訪談在質性研究中的應用。生活科技教育，37（4），17-23. doi:10.6232/lte.2004.37，(4)，4。
葉雲宏（2008）。網路詐欺被害影響因素之研究。中央警察大學犯罪防治研究所碩士論文。
廖釗頡（2010）。網路釣魚被害類型及其成因。國立臺北大學碩士論文。新北市。Retrieved from https://hdl.handle.net/11296/85hv77。

蔡田木、周文勇、陳玉書（2009）。詐騙犯罪被害人屬性之研究。[A Study on the Characteristics of Fraud Victims]。刑事警察局委託研究案。

蔡博忠（2008）。臺東縣高中職學生父母管教態度、自我控制能力與網路偏差行為傾向之相關研究。國立臺東大學碩士論文。https://hdl.handle.net/11296/8mtvk7

蔡義聰（2010）。網路遊戲沉迷與偏差行為相關問題研究-以臺東縣國小學童為例。

蔡德輝、楊士隆（2019）。犯罪學。五南圖書出版股份有限公司。

謝文彥、許春金、陳玉書（2005）。臺灣地區犯罪未來趨向之研究。內政部刑事警察局委託研究。

謝開平（2003）。電腦詐欺在比較刑法上之研究。國立臺北大學法律學研究所博士論文。

謝龍卿（2004）。青少年網路使用與網路成癮現象之相關研究。臺中師院學報，18（2），19-44. https://doi.org/10.7037/jnttc.200412.0019。

韓佩凌、鄔佩麗、陳淑惠、張郁雯（2007）。北部高中職學生網路沈迷模式之徑路分析研究。[A Study of the Internet Addiction Model for Northern Taiwanese High School Students]。教育心理學報，38（3），355-373。doi:10.6251/bep.20070117。

簡鳳容（2018）。網路偏差與被害特性及其影響因素之研究。中央警察大學犯罪防治研究所博士論文。

魏希聖、李致中、王宛雯（2006）。高中職學生網路成癮之危險因子與偏差行為研究：以臺中縣霧峰大里地區為例。臺中教育大學學報：教育類，20（1），89-105。

魏曼伊（2008）。教育研究另一途徑：網路調查研究。中正教育研究，7（2），97-128. doi:10.6357/cces.200812.0097。

二、英文書目

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). *2020 Cybercrime economic costs: No measure no solution.* In Paper presented at the availability, reliability and security (ares), 2015 10th international conference on.

Australian Government Attorney-General's Department. (2011). *Protecting yourself online, what everyone need to know*. Retrieved from https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/PDF%20-% 20Protecting%20Yourself%20Online%20-%20Second%20Edition%20-%20Booklet.pdf

Becker, G. S. (1968). Crime and punishment: An economic approach. In *The economic dimensions of crime* (pp. 13-68): Springer.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3* (1). 400.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38* (3), 227-236. https://doi.org/https://doi.org/10.1016/j.jcrimjus.2010.03.001

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29*(2), 408–433.

Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies, 10* (2), 229-242.

Choi, K.-S. (2008). Computer crime victimization and integrated theory:

An empirical assessment. *International Journal of Cyber Criminology, 2* (1), 308-333.

Choi, K.-S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73*, 394-402.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *44*, 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, 505-524.

Cross, C., Smith, R., & Richards, K. (2014). Challenges of responding to online fraud victimization in Australia. *Trends and issues in crime and criminal justice* (Vol. 474, pp. 1–6).

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research, 19*(6), 537-549.

Felson, M. (1998). *Crime and everyday life*. Thousand Oaks, CA: Sage.

Federal Bureau of Investigation [FBI] (2023). *2022 Internet Crime Report*. Internet Crime Compliant Center, Federal Bureau of Investigation.

Ferraro, G., Caci, B., D'amico, A., & Blasi, M. D. (2006). Internet addiction disorder: an Italian study. *CyberPsychology & Behavior, 10* (2), 170-175.

Furnell, S. (2002). *Cyber crime: Vandalizing the information society*. London: Addison Wesley.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Grabosky, P. N., & Smith, R. G. (2001). Digital crime in the twenty-first century. *Journal of information ethics*, *10*(1), 8-26.

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health, 18* (7), 3763.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger.

Hirschi, T., & Gottfredson, M. (1993). Commentary: Testing the general theory of crime. *Journal of Research in Crime and Delinquency, 30* (1), 47-54.

Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. *SN Soc Sci, 2* (4), 1-32. https://doi.org/10.1007/s43545-021-00305-4

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention & Community Safety*, *15* (1), 65-79.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, *37* (3), 378-395.

Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice*, *32* (2), 108-128.

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46* (1), 189-220.

House of Representatives Standing Committee on Communications.

(2010). Hackers, fraudsters and botnets: Tackling the problem of cybercrime. *The Report of the Inquiry into Cyber Crime*. The Parliament of the Commonwealth of Australia. Retrieved from http://www.aph.gov.au/parliamentary_Business/Committees/House_of_Representatives_Committees?url=coms/cybercrime/report.htm

Ionescu, L., Mirea, V., & Blajan, A. (2011). Fraud, Corruption and Cyber Crime in a Global Digital Network. *Economics, Management and Financial Markets, 6*(2), 373–380.

Izuakor, C. F. (2021). Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context. *ISSA Journal*, 28-29.

Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and violent behavior*, *17*(1), 16-26.

Kerstens, J., & Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's on-Line victimization and perpetration. *Deviant Behavior*, *37* (5), 585-600.

Koukia, E. (2020). The Effect of Personality Traits on the Roles of Traditional Bully-Victim and Cyberbully–Cybervictim among Greek Adolescents. *International Journal of Caring Sciences*, *13* (3), 1639.

Lauritsen, J. L., & Laub, J. H. (2007). Understanding the link between victimization and offending: New reflections on an old idea. *Crime Prevention Studies*, *22*, 55.

Lauritsen, J. L., Sampson, R. J., & Laub, J. H. (1991). The link between offending and victimization among adolescents. *Criminology*, *29* (2), 265-292.

Lee, C. S., & Wang, Y. (2022). Typology of cybercrime victimization in Europe: A multiple latent class analysis. *Crime & Delinquency*, online version. doi: 00111287221118880.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37* (3), 263-280.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. *Journal of Research in Crime and Delinquency, 54* (5), 639-679.

Mihajlov, M., & Vejmelka, L. (2017). Internet addiction: A review of the first twenty years. *Psychiatria Danubina*, *29(*3), 260-272.

Modic, D., & Lea, S. E. (2012). How neurotic are scam victims, really? The big five and Internet scams. *The Big Five and Internet Scams* (September 10, 2012).

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5* (1), 773.

Office of National Statistics (2017). *Crime survey for England and Wales*. Retrieved from http://www.crimesurvey. co.uk/

Paternoster, R., & Bachman, R. (2001). Explaining criminals and crime: Essays in contemporary criminological theory. Los Angeles, Calif: Roxbury Pub. Co.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25* (2), 103-127.

Paternoster, R., Pogarsky, G., & Zimmerman, G. (2011). Thoughtfully reflective decision making and the accumulation of capital: Bringing choice back in. *Journal of Quantitative Criminology, 27* (1), 1-26.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online

activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47* (3), 267-296.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52* (1), 87-116.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7* (1), 1-15.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers. *Crime Prevention & Community Safety*, *12* (2), 99-118.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50* (2), 216-238.

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior*, *38* (11), 1149-1169.

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16* (3), 633-654. https://doi.org/10.1080/07418829900094291

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly, 19* (1), 159-180. https://doi.org/10.1080/07418820200095201

Showkat, N., & Parveen, H. (2017). In-depth interview. *Quadrant-I(e-Text)*.

Simsek, N., Sahin, D., & Evli, M. (2019). Internet addiction, cyberbullying, and victimization relationship in adolescents: a sample from Turkey. *Journal of Addictions Nursing, 30* (3), 201-210.

Smyth, J. D. (2018). Internet survey methods: A review of strengths, weaknesses, and innovations. *Social and Behavioral Research and the Internet*, 11-44.

Standler, B. R. (2002, September 4). *Computer crime*. Retrieved February 6, 2005, from http://www.rbs2.com/ccrime.htm

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies, 12*, 133-152.

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior, 101*, 225-237.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32 (*2), 169-188.

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. Cyberpsychology, *Behavior, and Social Networking, 20* (7), 407-412.

Van Wilsem, J. (2011). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*（2）, 168-178.

Van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29* (4), 437-453.

Van Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization: Opportunity as

a social aspect of age. *Journal of Contemporary Criminal Justice, 17* (4), 328-345.

Wall, D. (2011). Cyber crime: What is it and what do we do about it? Mapping out and policing cybercrimes. pp.1–42.

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victimfocused approach. *International Journal of Police Science and Management, 19* (1), 39–53.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research, 26* (3), 399-409.

Yar, M. (2005). The Novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2* (4), 407-427.

附錄一：成大倫審會送審證明

Gmail Edward Y. Lai <yxl005@gmail.com>

【NCKU HREC成大倫審會】111-526 送審證明

1 message

NCKU HREC <em51020@email.ncku.edu.tw> Mon, Oct 31, 2022 at 3:14 PM
To: yxl005@gmail.com
Cc: cityliu@cib.npa.gov.tw

國立成功大學人類研究倫理審查委員會
National Cheng Kung University Human Research Ethics Committee

送 審 證 明

案號：111-526
計畫名稱：我國網路詐欺被害調查與防制研究
計畫主持人：賴擁連
申請機構：中央警察大學

國立成功大學人類研究倫理審查委員會 主任委員 郭書琴

本會已收到您的申請案，將比對送審資料資訊之一致性或有無需補充文件後，即可提交審查，敬請留意此信箱相關訊息通知。
本信件即為送審證明，請申請人自行截圖或轉為PDF檔。查看轉PDF方式

[聯繫方式]
專案經理：桂偉鈞
電話：06-2757575#51020；06-2756831

附錄二：成大倫審會通過證明(111-526-2)

國立成功大學人類研究倫理審查委員會
National Cheng Kung University Human Research Ethics Committee
網址：http://rec.chass.ncku.edu.tw/ E-mail：em51020@email.ncku.edu.tw
70101台南市大學路1號光復校區雲平大樓東棟北側4樓
電話：886-6-2757575-51020 , 886-6-2756831

審查通過證明

成大倫審會(會)字第 111-526-2 號

案件編號：111-526

計畫名稱：我國網路詐欺被害調查與防制研究

計畫主持人：賴擁連

計畫執行機構：中央警察大學

核准日期： 112 年 01 月 01 日

有效期限： 112 年 12 月 25 日

結案報告繳交截止日期： 112 年 12 月 25 日

國立成功大學人類研究倫理審查委員會

主任委員 郭書琴

中 華 民 國 111 年 12 月 16 日

附錄三：第一次焦點團體座談會議紀錄

賴擁連主任（以下簡稱賴）：

各位學者專家，大家好，我是本研究的計畫主持人，我們研究團隊成員有許春金許老師、我們陳玉書陳老師、葉碧翠葉老師以及在座有五位我們的博士生，來學習、聆聽今天的會議發言。很高興大家在百忙當中，齊聚一堂，針對今年度法務部司法官學院所進行的「我國網路詐欺被害調查與防制研究」有關探究網路詐欺被害者的問卷，來進行問卷定稿的焦點座談。

我們在這個研究案當中，司法官學院有提出幾個需求，就是今天邀請各位參加第一場次焦點團體座談的第二個目的，他希望我們在這一次研究當中，能夠去 cover 到的，除了國外的文獻資料之外，其實最重要的就是第二個，一定要就教於學者、還有這方面的專家，針對網路詐欺的定義、型態、範疇，還有即將實施的問卷內容，提出一些建議。或者是我們在編製問卷的過程當中，有無缺漏的地方，想借重各位的專長，還有各位的經驗，給我我們指導與建議。希望我們的這個調查問卷，不管是質化或量化的區塊，能夠更加的完善，所以今天才會有邀請各位參加此一焦點團體座談。這是我開各場白，請問團隊老師們有沒有要補充的？

陳玉書副教授（以下簡稱陳）：

沒有，目前先這樣就可以了，謝謝！

賴：

我們就趕快直接進入到我們的焦點座談的議題上，請每位專家學者知無不言、言無不盡，讓我們這個案子的調查問卷能夠更臻完善一點，所以請四位與會學者專家能夠給我們很多的建議。

第一個部分，如同我剛剛所報告的，各位可以參閱這份資料的最後面，有附上焦點座談訪談大綱；我們也在前面電子白板的地方有 PO 出來。請根據這一些內容分享一下，有沒有哪位來賓想先發言？

F4：

因為來之前，我自己這一兩天有看一下，我覺得整個問卷調查內容還蠻完整的。我想針對一些補充的資訊來講，因為我們不是做研究的，所以我們對這個研究的方法也沒有太多的想法。不過我之前也看過相關的研究計畫跟問卷，我覺得目前問卷初稿非常的清楚，然後那些問題也確實可以跟調查目的的關係連結起來。

只是有一些小的建議，因為我們有特別在問卷裡面去強調關於網路使用強度跟被害人的關係，但是我個人覺得除了網路使用強度，事實上也要看被害人本身。我們在辦有關於詐欺案件的案例裡面，常常碰到的狀況是，現在的通訊

管道大概都是網路，現在年輕人基本上已經沒有在看電視，也很少有人在聽廣播、看報紙。問題是在於他本人，是不是會比較傾向相信其他人的話？或者是他很願意去試一些奇怪的東西？那這個我想跟問卷裡面有關於網路使用是不是有衝動性，這個部分區塊會比較有關係。所以我們是不是有需要特別去強調，網路使用強度跟被害者之間的關係？也許可以更詳盡的參考。

另外，就是關於網路詐欺的定義這個部分，我們以前在網路犯罪相關的案例，就相關文件裡面大概有提到，就是透過網路來做誘騙的行為？還是說你是使用網路做付錢的？這些可能就是我們在日後，也可能需要做一個區分。就是說我們一般在案件上可能是看到說，透過網路來施用詐術，或者是透過網路來付款。我們自己檢方內部是都把它當成網路詐欺來處理，因為我們沒有特別分別哪一個專組來處理，所以就是大家都會分到。所以我會比較想討論一下，就是說我們到底是要不要限縮定義，犯人是不是只要集中在網路的施用詐術行為；還是說包含其他的狀況，譬如說透過網路來付錢，這些都算？初步意見大概是這樣，請各位參考，謝謝！

賴：

謝謝 F4，所以主任提了兩個：第一個是要特別強調網路使用強與被害人之關聯性；第二就是說在定義上來講，利用網路可能是詐術，但是它也是一個付款的工具。所以這個部分是不是應該要再釐清，還是說更聚焦在網路上。

F4：

是的，建議團隊是否聚焦在這一塊。因為透過網路付款，目前算是蠻常見的，譬如說網路銀行的轉帳，或是買虛擬貨幣，這些都有可能。如果說是這樣的類型，那就不一定是透過網路來施用詐術，可能一般電話的施用詐術，也會透過網路的方式來轉帳。那如果說都列在裡面，可能研究的範圍就會變得很大，這是我個人的淺見。

賴：

另外剛剛您也提到的，是不是我們對於被害人的心理特質，要再增加對於他的強度、還是對其他人的信任度？

F4：

是對其他人信任度的問題。因為強度的部分，我自己覺得其實 40 歲以下的人，大部分都是透過網路接觸外面的訊息。所以我的猜測，其實他的使用強度可能跟被害關係，應該不會真正有直接的關聯性，供團隊參考，謝謝！

賴：

所以會增加一個信任度的測量。好，謝謝！那是不是有請 FI 先針對定義

等等，提供建議。

F1：

謝謝主任、還有堅強的研究團隊。這個研究其實真的不是很容易，蠻辛苦的，設計的非常完善。我初步有幾點提供給研究團隊這個參考：

首先，我想說一般人如果接到這樣子的訪問時，一般所認知的網路上被騙的概念。或許有些人會以為說，他只要接到詐騙電話就算了。所以被害經驗指的是，到底有沒有損失？有沒有既遂？之類的。有些人可能覺得有接到電話，是不是就算被騙？這裡是不是需要有一個地方讓他們知道，到底被害指的是什麼？定義被害的經驗是什麼？因為問卷第 3 頁網路生活型態與情境機會這邊，就有一個分項是說，如果有被騙經驗，請繼續填答右欄。我覺得有些人可能會搞不太清楚，他會自以為被騙；然後這個部分的被騙經驗是指說 Lifetime，就是說在被調查之前都算嗎？可能就是讓他們知道，他自己到底算不算被騙這樣子。所以這個是第一個，是不是需要在答題之前，給他們一個說明所謂的被騙是指什麼？是不是一定要有損失金錢？這樣他們認知的被騙跟我們想知道的不會有所落差、比較明確。

然後，第二個建議就是說，如果到時候是網路問卷，也許就是我覺得心理特質這個標題，可以不用出現。例如說低自我控制，改為直接問說以下問題是有關您對自己的看法或生活經驗，請依據自己的實際情形打勾。那個標題可能不用出現在問題裡面，以免他們看到有點負向，可能會覺得低自我控制，然後就答得有點偏差，或者就答都沒有之類。包括低自我控制、偏差動機、或是網路成癮，我覺得應該都不要出現在問題上面。讓他們比較中心一點，比較不會影響他們的評價。

第三，第四大題這邊的被害經驗量表，有特別明確的指出是最近一年的經驗以外，是否也要再加上從你使用網路以來，曾有經驗、有損失的經驗的這個一題。因為可能考量到題目太多，但我覺得 Lifetime 的 experience 也滿有趣的。可以加上一題，然後後面再仔細問說，最近一年的那個經驗是什麼。我目前先提供這些建議，謝謝！

賴：

謝謝 F1。接著，有請 F3。

F3：

老師、各位先進大家好，前面幾位先講的，我覺得滿贊同的。其實在這個定義上，建議要限縮，因為現在詐騙幾乎跟網路途徑有關。那你們定義的網路詐騙，因為我以前碩班研究也是網路犯罪，我覺得以實務單位來看，投資交友、網拍、或者是所謂的吸金、或者是剛才主任講的有一些犯罪洗錢，比較接近網路詐騙。還有我們如果講詐欺的話，在實務單位會指要有金錢的受害。

我大概有看了一下你們的問卷，在問卷第 6 頁（四）被害經驗量表，其實我們看第 1 到第 4，實務單位覺得應該都是網路詐騙。可是第 5 的部分，就我們實務單位來看，「解除分期付款」是打電話給被害人，前段是偷個資，所以我們實務單位會比較定義是電信詐騙。所以我們範圍如果定好的話，其實案類就很清楚，才不會有一些研究的偏差。然後「猜猜我是誰(假冒親友)」也是電信詐騙，現在都用 DMT 或者一些電信的裝備去做。而假求職的詐騙，其實電信、網路實例都有，包含最近柬埔寨擄人的那個案子，也都是假求職的詐騙，其中前半段是網路，後面那是實體，還有人頭帳戶的濫用，也是電信詐騙。

原來第 6 頁的 2 也列了很多案件，包含 2、4、6、9，還有假公務員在裡面。當然有可能是要問他的經驗，而不是跟本案有關。所以我覺得，其實在定義跟範圍有限縮的話，第一個對你的研究會比較精準；第二個因為現在的詐騙案件，幾乎 9 成都跟網路有關，這樣未來怕一些沒有辦法聚焦。這是我們實務單位給的一些建議，其他部分都尊重。我覺得其實這個研究非常棒，也謝謝你們，謝謝！

賴：

好，謝謝 F3！那我再請教一下，因為你們辦案的經驗也比較豐富，在詐欺型態上或者是情境機會上，像監控、還有風險的區塊，有沒有要再補充？或現行的問項當中，有沒有需要再強調的？

F3：

問卷我是覺得還好，以第 3 頁來看，其實你們應該也有用網路犯罪的東西在裡面。網路詐欺占網路犯罪將近 6 成到 7 成的案例，可是你們提的東西有蠻多跟詐欺有點不太一樣。例如第 3 頁（三）第四，有講到所謂智慧財產權的東西；那第六網路干擾，其實我們實務上干擾比較偏入侵、妨害電腦使用罪；或者是有用到現在的跟騷做法。所以這部分可能在定義部分，可能也要跟著調整，以上是我的建議。框架沒有問題，框架很棒，內容部分我們事後再幫你們看一看，可能會比較聚焦一點。因為問卷未來還會有一些效度的分析，所以可能這部分我們會再做一些事後的建議會比較好。整體架構我們覺得 OK，算蠻不錯的。

F4：

誠如剛剛 F3 提到這個部分，其實我也有一點小小的建議供大家參考。就是關於第 3 頁（三）的部分的，整個網路上可以看到訊息的部分，我建議可以增加一點選項叫做「你在網路上看到投資的訊息」。因為其實投資詐騙是我們之前比較常看到的案例類型之一，但可能在網路上看到投資訊息，這個還會有一些區別，因為如果你是從正常管道看到的時候，通常比較不會有問題。所以也許問題設計成，譬如說透過社群媒體、非官方的管道，官方可能可以舉例說是

銀行、大型的投資公司以外的地方，看到的投資訊息。可能對去確認這個直接接觸到網路詐騙訊息的機會，這個問項上可能會比較明確一點。

那同樣的，我也贊同 F3，對於譬如說盜版是不是真的跟這個有關？因為可能是為了了解答題者的使用生活型態，所以我個人是比較傾向可以把它留下來。但是在確認他的生活型態的議題，我會建議補充「投資的訊息」，因為問題有明確提到網路詐騙別人財物的訊息，但我想一般詐騙者在網路上包裝他的訊息的時候，絕對不會明白告訴你說這是詐騙。通常都是事後才會有，所以我們可能也需要把詐騙別人訊息裡面，再更個化一點 會比較能再明確的讓大家聽得清楚，去呈現他實際上看到的狀況，以上謝謝！

賴：

謝謝 F4！

F2：

我想我今天來的主軸應該會比較著重在網路生活型態跟情境機會這一塊，至於心理特質領域上，我比較沒辦法著墨太多。以我 computer science 而言，來看網路生活型態的這一塊，想跟大家稍微討論一下，先提出我的觀點。因為我感覺這整個設計上，是還蠻完整的結構面。現在想討論有沒有什麼需要補強的地方，還有我想知道的地方。

以第二項的網路生活型態及情境機會來看的話，這邊有提到三大部分，前面有關於時間上，我想那個倒是其次；第一是被害動機誘因這一部分，然後第二部分是網路風險，第三部分是數位監控，以這三大部分組成的網路生活型態及情境機會的問卷調查。我想知道怎麼會有這三大面向的思考的空間出來？是有參考別人的資訊？還是說團隊裡面去做一些討論，所以有這三大面向？那這三大面向之間，有沒有類似交集的部分？等於是這三大面向當然有部分的交集，但也有它各自的需求面。

所以我想先知道：第一個，這三大面向是怎麼出來的，是來自於參考別人的東西，或是團隊經過一些腦力激盪？而有這三大部分，就它的需求，還有部分交集的地方。然後如果這些出來之後，我們來思考是不是說，它有沒有可能有第四大部分。或者可能沒有，因為這三大部分已經 cover 了。像這邊有提到說，有 8 題可能得到被害認知的問題，另外，那個措施有 8 題，然後數位監控有 12 題。其實，以這個題數來講，是不是有一個增補的空間？我想這個在討論當中，可以稍微去做一個思考的進展，就是我這一塊先提出來。

賴：

那個我想三大面向，一方面在司法官學院當時在需求書有提到這個情況，就是說他希望了解這個區塊；第二個，系上老師在過往這方面的研究，特別在犯罪學領域當中，像日常活動理論跟這些詐騙的行為也有密切關聯。所以這三

大面向的形成應該是從這兩個部分來的，第一個就是需求方、司法官學院有提到，想看到這一個區塊；第二個是基於我們系上老師，包含文獻的積累，然後形成這個三大面向。

當然這幾個框架是原則上符合需求單位的區塊，我們先做出來的。如果說王老師認為有必要再增加面向，或者增加題目，我們會納入考量。因為我們當時其實也縮減很多，今天這個版本之前，我們內部也有討論過，後來也縮減一些題項。如果老師們覺得說，我們還可以再增加面向、或者題目的話，那麼也不妨再分享。以上是我的說明。

陳：

謝謝大家給我們這麼多的建議。那我就先回應 F2 關於設計機會情境的思考，剛剛我們的主持人擁連老師有提到，基本上這個架構是根據研究計畫的需求書所研擬。我們會去投標的原因是覺得這是未來的問題，也是現在的問題，就是實體的犯罪已經慢慢進入到數位、網路、電子、通訊上面了，所以犯罪跟被害的研究應該要往前走。這一項研究，一個受訪者只有 50 塊。所以我們的問項是精簡再精簡，希望能把它控制在一定的時間內，否則這個計畫難以實現。所以我們是希望理想跟實務當中，去找到最好的平衡點，然後遂行這個研究。因為我們賴主任剛剛講得非常含蓄，但也講得很實際。

因此 F2 的問題很好，事實上在文獻上面，或者是 165 的官方資料裡面，其實有很多的資訊都應該要被納入。我們根據國內外的文獻，還有我們在過去兩年所做的前導性調查，經過統計分析之後，把可能導致被害的因子保留下來。事實上，早期所做的因子是比較多的，然後在概念下的問題也比較多，但最後我們只保留最顯著的、影響力最大的，因為我們想要讓受訪者更有意願回答。如果老師們覺得這上面的概念（動機、誘因、風險跟監控），還應該增加第四個，或者是像剛剛 F4 所講的，再增加網路投資的部份，也是可以的，因為投資詐騙已經到達所有詐騙案類第一名了，增加投資項目的那個瀏覽，就增加一、兩個項目，我們還是可以接受。但如果要增加很多的項目的話，我們可能要再刪去別的，因為受訪者能夠忍受的填答時間有限。那我們也很願意去思考增加一定的項目，我們應該也可以做到；但太多的話，可能受訪者就不能承受，在資料蒐集上，就會比較困難一點，這個是跟大家說明一下。

第二個就是網路詐欺，剛剛有談到透過網路所從事的犯罪跟被害。其實現在有很多的犯罪案類都跟網路有關，像是網路詐欺被害，就是結合網路、加上詐欺的行為。我現在自己感到有點困擾，因為傳統上講詐欺，就是很清楚詐騙，可是現在詐騙在法律上的定義，又跟組織、洗錢等都會有關。那我們是要用法律來定義？還是用行為來定義比較好？然後透過網路所從事的詐騙，只要是整個犯罪的路程曾經經過網路，這樣就算嗎？還是說整個行為的完成，必須要在網路上？這就是我們在定義上所遭遇的困難。如同剛剛 F4 有談到，到底是因為犯罪人的動機，還是使用工具或管道是在網路上面，就算是網路詐欺呢？

在國際上，有一些人是採法律定義，有一些人是採行為定義，有一些人是採廣義的定義。司法官學院也希望透過我們的研究，雖然我們研究的是被害，他們想要把它定義下來。

這裡面所採取的被害經驗的量表，其實是參考刑事局過去幾年統計跟網路有關之詐騙案類的前 10 名，我們把它列進來。因為其實態樣非常的多，我們如果一一問的話，問卷就變得很長，所以我們就去選主要的，像在第 6 頁的 1 到 9 題，還有第 6 頁的最近一次被害經驗的第 2 題。基本上就是結合網路有關的詐騙行為，但還是會有一些實體詐騙，所以要怎麼定義會比較好，是整個行為完成？還是只要透過工具？這個要如何去定義，在實務上跟學理上會是比較合理的， 也是我們研究團隊需要給司法官學院的這個解答。

然後剛剛 F1 有提到好幾個，就是我覺得在定義上應該更清楚。因為像我自己在電話、網路、或者 LINE 上面，也會接觸到一些疑似詐騙，這樣子算不算曾經有被害經驗。我們是應該把它定義更清楚，因為網路被害而造成金錢或其他財物損失，才算是我們的被害經驗，會不會是比較好一點？這我們事後應該要再討論。

那期間是生命史的期間？還是只有過去一年？因為我們早期做被害經驗，為了要推估被害率等等，所以我們都會定義是過去一年（像 111 年 1 月到 12 月 31 號）這樣子。如果做 Life course 的話，這個研究案是不是能夠去 cover？這也是我們需要去思考的。再來，剛剛 F1 談到的，每一個大的項目當中，我們都會寫說這是自我控制、偏差動機等等的。實際調查的時候，只會看到測量項目跟調查說明，這一些概念的名稱都會被移除掉。其實我們今天會議之後，還是會再做一個前測，看看問卷執行的可行性。以上是我的簡單說明，還有提出問題的請教，謝謝！

F3：

我大概再補充一下，其實我覺得老師您講得很好。如果沒有定義好，那問卷要調查 1,000 個，大概有 500 個被害經驗。照那個廣義的，現在幾乎都被騙過，如果沒有被騙錢也算是被害的話。所以，如果我們沒有定義好的話，我們的樣本可能現在找不到沒有被騙的，連我自己也接觸過，只是沒有被騙成功而已，我覺得定義蠻重要的。

另外，我也補充一個實際的狀況，因為我們是實務代表，特別講第 7 頁，這個設計很好，可是它少了一些東西。包含你看那個第三題（四）社群軟體有 Skype、QQ，但其實最近最嚴重的是 Telegram，反而沒有列進去。然後另外一個部分是交友平臺，卻漏掉直播平臺（浪 LIVE、SWAG 等），這些也會被騙，目前列的有一些我比較沒看過。所以，可能獨立或寫一個直播平臺等，會比較好讓人家填問卷，不然使用者不知道要填哪一個。那我們現在很嚴重的有虛擬貨幣，問卷沒有，這是一個問題。還有第三方支付跟電子支付（用法律名字來講）其實不一樣，第三方支付包含藍新、綠界、紅陽，那行動支付或電子支付

還漏掉最常用的 LINE pay。我覺得增加，對樣本有效性可能會比較好，不然他可能亂填。

那我們現在百萬財損以上的案件，非常恐怖，去年就將近快 6、70 億元的詐騙，所以我覺得級距應該要拉大。其實現在網路買虛擬貨幣被騙，我們常常在派出所看到那些老人家，1、2 千萬就不見了，那這跟疫情有關。我們要不要設計一個級距高一點的，我的建議是希望能讓你們呈現出來的樣態會比較多元。

陳：

我們很需要這樣子討論，我們的架構也許已經被司法官學院給框住了。因為他當初有列要調查特定項目，可是我們只就文獻跟以前調查的結果提列。然後像 F3 這樣提點，正是我們需要的。請你盡量提，最好針對我們每一個測量項目，有需要做修改或增刪的，我們都很樂意。如果逐項，比如說剛剛談到的網路的機會情境，或投資資訊、或平臺等等。在我們工作上，或者是我們的研究領域上，覺得現在什麼是比較重要的、是比較多的，要增加。然後比較少見的，建議刪除，我覺得這個都是我們想要的。

F3：

165 那邊有很完整的資訊，也可以私底下去問一下他們那邊。

陳：

我們已經分析過 165 了，這是前幾年的 165 的統計資料。

F3：

因為這每年在變，今年 Telegram 比較嚴重，我自己也有收到，很頭痛。

F4：

其實他們最近都在騙帳號，用 Telegram 來騙帳號，所以真的就是最近這一批是很流行的。像什麼 Good night 等管道，我們在案件上比較沒有看到，可能是比較早期的交友平臺。可以跟 165 調一下最近這一年詐騙頻傳的交友平臺，我們把這個東西列在上面，大家才會比較有感，問卷的效果也會比較準、報告比較多元。

陳：

165 這方面有官方的統計結果嗎？

F3：

他們那邊有，因為基本上我們也是常常在看 165 的資料。每個禮拜我們主

管會議都會講，我這邊是科技單位，165 那邊是預防科。

陳：

如果是一個完整的統計報表，適合提供參考嗎？

F3：

這個我們可以幫你要看看，他們應該內部有。

陳：

我們很需要就現實狀況，因為我們問的是過去一年，而且是 COVID 期間。過去一年也算是大家使用網路非常頻繁的生活方式，所以像是譬如說投資詐騙 以前沒有那麼多。

F3：

因為你們是列舉式的，所以如果使用者可能因年齡而不太清楚，他不知道怎麼勾，我覺得可能要修一下。

陳：

我們很想修，有沒有可能像您要到 165 最近的、跟我們題目有關的相關統計？

F3：

我來幫你要看看，再 support 給你們。

陳：

好，謝謝！這樣子比較好，就跟民眾真正遭遇的問題是比較接近的。我們這個研究結果也可以回饋實務單位，大家一起參考。

賴：

跟老師們報告，高檢署對這也是很困擾，所以我們 5 月 29 號的研討會，高檢署的張斗輝檢察長已經提到，要一起合辦。因為網路詐欺的議題也是過去兩年最重要的，所以我想這個議題確實是重要。

許春金教授（以下簡稱許）：

請問 F4，根據你們辦案經驗，都是哪些人在騙？

F4：

其實我們實際上案例裡面，去騙人的人根本都抓不到，比較容易發現的都

是端末的。

陳：

因為我們的被害統計，被害比犯罪的人多很多。

F4：

對啊，實際上因為詐騙手大概都在境外比較多，所以其實人都在外面。我們抓的，譬如說提供帳戶的、領錢的車手、機房，可是機房也很多是在境外騙大陸人，現在可能都被大陸抓走。

F3：

詐騙分工很細，它就像 Android 平臺一樣，你要買什麼 APP 都有。拜科技所賜，他們很先進，不需要見到面。

葉碧翠助理教授（以下簡稱葉）：

每個接頭都會有一個斷點，車手歸車手、機房歸機房、金流歸金流，然後我就永遠都不知道老闆是誰。車手跟提供人頭帳戶的最好抓，因為人在臺灣。車手通常是勞力階層，只是工具而已。

陳：

所以我們要如何定義會好一點？

F3：

我覺得應該是「接觸到被害人的途徑」，可能會比較好。比如說我現在是用網路裡的一些工具，施用詐騙的人透過網路接觸被害人，像在雅虎拍賣買東西被騙，即屬之。

陳：

就是透過不管是什麼樣的網路：電腦網路、手機網路、平板網路。

F4：

對網路來講，其實你是用電腦、手機都是一樣的網路。

陳：

透過網路接觸被害標的，可能會比較好。被害的管道，或者接觸被害的管道，以接觸為主。就是以行為做定義，這個行為可能會適用不同的法律條文，但是就以行為的本質當定義，再把案件套進來看看怎麼符合。

F4：

剛剛在發言的時候，有提到詐欺可適用洗錢跟組織犯罪防制條例。組織犯罪跟洗錢基本上跟詐欺犯罪沒有關係，只是因為它涉及到錢的處理，所以有洗錢的問題；因為它是三個人以上，所以構成組織犯罪。其實我建議還是以行為本質做區分，這個行為可能會適用不同的法律。因為一個行為做下去，在法律實務方面會有不同的結果。

許：

所以這個比方來講的話，第 6 頁被害經驗量表第 1 題應該說「上網購物時被騙，而造成財物損失」這樣子嗎？因為你被騙，你不知道，還是很主觀的。

陳：

對。

F3：

像第 6 項就可能不太適合，因為第 6 項就跟第 3 項就很接近。因為第 6 項在我們的定義，它是隨便一個電話打給你，前半段可能個人資料不知道從哪裡拿到。其實我覺得不適合放在這邊，因為途徑就是電話，那個不算。

陳：

那我們這邊列的 9 項，有沒有其他應該要加進來的？如果我們把「猜猜我是誰(假冒親友)」拿掉，有沒有其他最近兩年特別普遍的？

F3：

ATM 可以拉進來看看，因為它前半段是個資外洩。

賴：

然後「假援交」有嗎？

F3：

「假援交」也可以接近，用定義去限縮。像 Telegram 就是第 8，因為冒用好友身分或入侵好友身分。假求職也有網路上徵招，那個也可以算。反而第 6 項，我覺得實務單位不認為它是網路，其他大致 OK。

陳：

有沒有我們漏掉比較重要的，需要加進來的被害類型？

F4：

我補充一點，我個人認為求職詐騙還滿常看到的。應該說很多人頭戶被騙，他就會說「我是因為找工作」，所以提供帳戶。他們也就是到找工作的臉書社團，或者透過通訊軟體 LINE，然後朋友之間互拉。我們看到的實際案例裡面，大部分都有一些對話，有透過通訊軟體，或者透過社群網站，去跟對方應徵工作。然後要求他提供個人資料，或者是基本帳戶。所以某種程度來講，這個其實也算是詐騙的一種類型。

許：

哪一個類型所造成的傷害會比較大？比方講投資被騙可能會有很多損失。

F4：

一般來講，投資詐騙會多很多。如果是投資詐騙，被害金額就會高很多。因為投資就會希望花更多的錢，可以得到更多的回饋。網路交友、愛情詐騙可能就看他「愛人」的部分，有時候金額也是很高。有些案例的犯罪時間很長，一直糾纏不清，對方會一直索討，各種方式騙錢。

F3：

我補充一下，如果以第 6 頁的部分，金額最高是第 2：假投資詐騙，去年的第 1 名；量最大的是第 5 跟第 1，因為它的金額不是高，大概 1、2 萬塊、幾千塊，可是被害人都是年輕人。所以你們這個分析其實也對啦，基本上我是覺得，如果都有帶到的話，應該都沒問題，量跟質都有。

F1：

我想請教一下，透過網路實施詐騙之類的，被害人如果有時候可能沒有實體見面，但是以為知道加害人是誰。第 7 頁這邊有一個問題是與加害人相識的程度，會不會有一個選項是「不知道加害人到底是誰」，因為他不知道他到底認不認識加害人。

陳：

有的時候是不知道誰騙我，至於我認不認識，我根本沒辦法判斷。

F1：

對，會不會有這樣的狀況。

陳：

「不認識」跟「不知道加害人是誰」這兩個有沒有不同的意義？有些人就有一個加害人、知道他的名字，但是從來沒看過。另外一個就是，點選網址進去，結果就被害了，可是不知道到底誰加害的。這兩個如果合併在一起，會不

會造成分析跟解釋上面的困難？還是說併在一起是 OK 的？

F3：

其實網路詐欺應該都在第 4「不知道」，網路幾乎都不認識。認識的是實體：借錢詐騙，跟一般的詐欺不一樣；或者是老鼠會詐騙，有實際接觸的，可能他提告親戚或朋友。

陳：

把「不認識」跟「不知道加害者是誰」併在一起，在分析跟解釋上會不會有不清楚的地方？大家建議是分開，還是可以合併？

賴：

還是多一個「不知道加害者是誰」，變成第 5 個選項。如果到時候樣本很少，我們再合併。

陳：

那受訪者會不會把這兩個搞混了，有些人在辨識上面，「不認識」就是根本不知道他是誰。受訪者有可能不會那麼細究，他可能就會都算不認識。

F4：

事實上，也許我們把各個選項分開來統計，如果有些人不認識，也許還可以解釋。就像剛剛 F3 講的，前面三項大概選的人會很少，網路上都不認識。

F1：

因為剛剛 F3 有講，其實加害者分工有很多層級。可能在這連續的被害的時間點上，他是接觸不一樣的人。所以如果有好幾個加害者，接觸的到底是指誰？也許接觸的是後面的車手，跟前面聯絡的是不一樣的人，這個題目會不會比較難答一點？

陳：

也是有可能兩個以上的加害人，因為可能不同的人發給他訊息。那這要如何辨識，是最常接觸的那個嗎？

F4：

一般來講，如果透過網路（譬如通訊軟體），跟你對話的人是誰，其實根本不知道。通訊軟體上只有一個暱稱，或者是一個網址。其實問題是到底要怎麼定義？可能像火山孝子那種，講了很久，但實際上是「叩客詐騙」，講話的人跟見面的人搞不好是不一樣的。

陳：

什麼是「叩客詐騙」？

葉：

叩客詐騙就是線上跟你聊天的，但是在臺灣會派一個妹去見你，其實跟線上是不同人，誘騙男生一直拿錢出來。

F4：

他們都在直播平臺上對話，但是實際上見面的人，都是詐欺集團另外雇用的。

陳：

所以就是聯繫的人跟接觸的人不一樣，所以網路詐騙也會跟實體交互嗎？這類詐騙需要問嗎？就是聯繫都在網路上，然後也有實體，這要怎麼問？這個重要嗎？跟蹤騷擾也是網路、實體都會，那了解它是全在網路，還是大部分網路、少部分實體；或少部分網路、大部分實體，對於這個犯罪案類來講，重要嗎？

F3：

我自己是覺得不重要，因為這個題目開宗明義就是網路詐騙。

陳：

那要如何去區分「相識」，現在這樣子 OK 嗎？還是增加一個「不知道加害者是誰」，這樣 OK 嗎？現在是有多元加害者，還是只針對主要加害者呢？

許：

需要知道加害者嗎？不用的話，可不可以刪掉？

陳：

就是他的直覺吧！被害者大概知道是誰，或不知道是誰，讓他直接回答就好。

F3：

應該就是驗證，網路幾乎都是不認識。

陳：

對，有少部分的案類可能有實體接觸，會知道加害者是誰；但是大部分的

被害者，還是不知道對方是誰。

F3：

對，99%多都是不認識。這一題還是要問，因為實際上我們看到的案例大概都是不認識。不問的話，到時候結果不會出來。

陳：

因為我自己用網路的話，都是很正常的生活，比較不了解一般被騙的人實際的經驗。F2 剛剛所談到的生活型態跟情境機會，其實在文獻上跟實際的官方資料裡面，也發現這個是很重要的。比如說像第 2 頁裡面的被害動機跟誘因，或者是網路風險，我們提出了 8 個，大家有沒有增修意見？

因為我們的調查對象包括一般人跟被害者，通常被害者的傾向會比較明顯；一般人比如說像我一樣，就是正常的家庭使用，買機票、或者是購物等等，有一些網頁我根本都不會去碰。大家覺得在是否被害之間，這一些項目會不會有鑑別力？還是有別的有鑑別力項目，我們沒有放進去？我們希望能夠區分為什麼有些人會被害、有些人沒有被害。

許：

簡而言之，以 F3 跟 F4 的實務經驗，什麼樣的人比較容易被害？他們會去點這個網站，以致被害率會比較高。

F3：

我的專長不是在被害，幾年前我曾制止記者寫「高知識分子容易被騙」的報導，因為涉及歧視。我覺得這個研究很好，可以想一下怎麼設計會更好。

F4：

會不會說對外媒體的訊息接收度的部分？

F3：

或者說「你們有沒有在看新聞」，可能加一個「一天看多少電視新聞」或「有在注意詐騙的新聞」的變項。通常會被騙的，就是沒在注意。我們知道對於新聞敏感度低的，很容易成為被害。

F1：

我也很好奇，如果受訪者的工作是要一直利用網路跟人家接觸的，會不會比較容易接收這方面的訊息，例如說他在做生意、直播、網路購物等生活型態的。

F4：

在問卷上生活型態、情境的機會，除了賭博、賭盤、援交，我們建議將網路投資放在裡面。不正常的網路投資管道，很多網路在做。我們最近常看到去買虛擬貨幣，還有外匯買賣的、買股票、ETF 之類的。

關於數位監控部分，我有一個小小的建議。從 Telegram 的例子，可以理解到，其手法是同時在電腦登錄你的帳號，在跟你對話的過程中會收到認證碼的訊息，然後叫你截圖傳給他。如果使用者不仔細去看在他設備上呈現的訊息，也許就不會發現是詐騙。所以，是不是可以把這當作一個題項：「你在上網的時候，會不會注意呈現在你面前的訊息。」如果在看自己電腦訊息的時候，很仔細的看，也許會留意到異常狀況。以上提供給大家參考看看。

許：

就是說加「認證碼」到裡面嗎？

F4：

對，因為現在兩階段認證蠻常用的，尤其是銀行相關的。他們現在就是用騙認證碼的方法，拿到這樣的資訊。

陳：

以前做研究的時候發現，有一些監控越高的人反而容易受騙。我們推測是在做調查時，沒辦法辨識是被騙前、還是被騙後所做的防衛。在這個問卷當中要怎麼問，才能知道「因為我曾經被騙過，然後才注意防衛。」所以大家都知道網路監控很重要，可是要連結被害的問法，其實不好設計，想聽聽大家的意見。如何去辨識他是因經驗不足，然後才被騙的；還是他曾經有被騙，所以才去加密。

這個在設計上的位置一直放不好，因為之前的調查就是監控越強，卻越有被騙經驗。我就懷疑是不是曾經有接觸被害訊息，然後監控才變強的，這件事好像需要被證明。如果把它放在第 4 被害經驗量表的 10 題之後，會不會比較明確？因為先前調查跟統計的結果，發現是有干擾的。

F2：

首先，「數位監控」這四個字，我覺得好像不是那麼 friendly，這四個字當初是怎麼出來的？

陳：

其實現在文獻使用名稱上，有人用網路、有用數位、有用電子，在 paper 上很混淆。比如說像數位暴力或網路暴力，都各有所使用，衛福部是用數位暴力，很多文章也是用數位暴力，他們都認為數位的範圍比網路還要多。我們如

果用網路監控，是否比較 match 這個研究？還是可以改。

F2：

如果站在一般民眾的概念上，會覺得「網路監控」會比較 friendly。

陳：

我們到時候調查，不會出現這些標題，這是研究者自己定義的。我們在做 survey 的時候，這些字都不會出現，只會看到問項。現行放在這裡，是讓大家知道我們要測的概念是什麼。回到曾經受騙的時間點前後，其辨識對我們來講有點困難。

F1：

我建議如果在設計的時候，因為是網路調查，如果前面其中一題答有的話，就再自動跳一個題目，再問「是不是跟自己或家人朋友曾經有過受騙經驗有關」之類的。

陳：

確實是曾經聽聞，或者看過媒體報導之類的，會增強防衛。所以似乎放在被害經驗量表的 10 題後面，寫的人比較有感。如果放在前面的話，比較不容易辨識關聯，這樣調整問題的位置，會不會好一點？

F2：

如果這樣，是全部的 12 項都移過去？還是切部分的過去、然後部分留在這邊？

陳：

我們可能會去想，這是一般人使用網路的習慣？還是因為他的生活經驗而產生改變的習慣？比如說我不會去接陌生的電話或 E-mail，所以 F2 說是不是要去區辨監控，是一般的使用監控；還是因為他的生活經驗，而產生的改變監控？比如說像第 3 題「留下個資」，這是一般監控嗎？還是被害之後會產生的變動，這個該如何辨識？

F2：

我個人認知像第 5 題「更改密碼」很明顯，一定有被害之後，他才會做這件事情。密碼沒事不會想去換它，一定曾經發生過什麼事，我認為應該要換它，才不會再次發生。

陳：

老師您這個真的是一個很好的 hint，我們在被害經驗的後面，就是第 6 頁

1 到 10 題裡面，再增加一個另外的複選題。就是說前面這 10 題當中，曾經回答 1 以上，然後就問他在被害之後做了什麼事。比如說 screen 的複選題：更改帳號、加密等 6 個選項，問在被害之後，網路上使用的改變了什麼。這樣就可以知道他前面答的那些，有哪些是他產生的改變。

F2：

這樣會增加調查過程的複雜度嗎？

陳：

不會，只增加一題複選題。

F1：

全部答 0 的也要問，這樣才能比較。

陳：

就全部都一起問，這樣子嗎？可是沒有被害經驗，他如何能改變？因為就是曾經被詐騙的人，就要回答下面的複選題。只要他有勾到的話，我們就會知道他所做的這些事情，是在發生之後的改變。老師覺得會不會簡單一點？

許：

會，我們以前也做過這樣，被害前跟被害後有明顯的差異。

陳：

因為完全不知道他是之前之後的改變，最後做推論真的有困難。原來第 4 頁的就不要問使用前、後，然後被害經驗之後加一個複選題「你被害之後做了什麼改變」。然後我們就會知道他前面的那一些，是被害前或被害後發生的，這樣 OK 嗎？

如果都沒有改變而被害，他就是容易被害的人，這樣合邏輯嗎？我想實際上的生活經驗應該是如此，例如你的車子曾經在什麼地方被害，下一次就不會再停在那裡；你曾經在某個購物平臺被害，你就不會去再使用那個平臺。老師覺得這樣 OK 嗎？

許：

可以，就是加一題；第 4 頁也不用後面跳答了。

陳：

當初就這個就很糾結，其實本身的監控是重要因子，又問不出來，這是題型的問題。然後第二個就是到底要怎麼監控，才會有效的避免被害？我們這邊

列了 12 個。會特別針對監控，是因為前面的動機跟風險在前導性的調查裡面，跟被害之間的關係很穩定而明顯。可是我們知道監控在學理上很重要，但是問出來的結果不那麼穩定，做 Gamma 的時候，有一些項目陽、有一些項目陰，對此感到很困擾。所以想進一步請教大家，在網路上面什麼樣的監控情境，可以讓個人使用網路比較不容易被害？

許：

我們以前的被害調查有一個最明顯的就是「有沒有打電話問 165」、「他知不知道 165 的電話」，那是最顯著的因子。

F2：

這邊我講一下，關於像「家人會注意的網路使用情形」跟「家人朋友會在你身邊」這個在學術上是有意義的嗎？

陳：

因為監控有很多種監控，有人為監控、情境監控、機械監控。以前的實體被害、或者電話被害的時候，如果他的旁邊有人，通常比較不容易被害。

F4：

其實像我自己經驗，我上網時旁邊就不會有人。

陳：

所以這樣的監控力是從何而來，就是我們要去思考的。

F4：

我會建議在安全措施，除了改密碼以外，是不是考慮「雙重認證」。

陳：

要說明「雙重認證」是什麼嗎？

F4：

「雙重認證」就是第二道密碼，譬如說傳簡訊到你的手機。

陳：

這有必要，因為有一些銀行都是這樣，連科技部都有類似的作法。我們就是要這樣的題目，任何強化監控、降低被害的這種思考，然後跟避免被害關聯性越強的做法。

F3：

知道雙重認證的，大部分都懂一點電腦的知識，或可以附加（第二道密碼），如果怕人聽不懂。

F4：

英文是 two steps two steps。

陳：

那第 7 題有用嗎？我感覺設定上網跟流量限制，這作用不大。

F4：

感覺是對小孩子比較有用。

陳：

OK，我們調查對象是 18 歲以上的，雖然這個可能在文獻上有。所以我們可以增加「雙重認證」，然後把第 7 題刪掉。像第 10 題「提升隱私跟安全認證」，一般老百姓容易了解嗎？我覺得有的受訪者不太了解這一題。

F3：

這個是比較高階的，在手機裡面自己設定權限。如果會勾這一題，表示這個人很厲害，我覺得留下來沒有不好。

F4：

或許可以把文字順一下：「您了解電腦手機平板上，提升隱私或安全權限的方法來保護自己。」因為光講安全權限這件事，可能讓受訪者懷疑這個問題到底要問什麼。

陳：

除了我們這邊列了 12 個項目，有沒有平常你們認為比較好的監控防護措施，或者是被害者被害之後會去做的事，而且可以有效預防被害的？

F4：

就定期更改密碼、提升安全權限，我剛剛提到的「雙重認證」，一般都是我們在被騙以後，一定會做的事情。

陳：

這幾題可以放在新增的追加題裡面。

F4：

還有一個是習慣的問題，就是會到官方網站購入或下載東西，不要到不知名的網站。其實我們以前常聽到，透過一些來源不明的地方下載東西、或是上網，通常都會有一些風險。

陳：

對，在釣魚網站的部分容易中毒，或者是被盜用。我們可以逐項分析，也可以累積分析。

F3：

對，這樣就會有分群的效果，我覺得很好。

陳：

所以大家的建議就是把第 7 題刪掉；然後增加雙重認證（第二道密碼）；再把第 10 題裡面加「的方法」三個字，這樣會比較清楚一點。

再請教一個問題，心理特質是司法官學院的委員所提，我們這邊列了 3 個傾向：做事比較衝動、喜歡冒險、碰到誘因不能控制自己。以大家的經驗，除了這 3 個特質傾向之外，有沒有其他的特質是被害人常有的？像網路成癮也是常用，還有什麼傾向是比較容易被害的？

F4：

我剛剛提到「很容易就相信別人的話」，另外一個就是「沒有常識」，就是他沒有去接觸過這些訊息。比較消極的才會被詐騙，話少的不會問人家，不會主動問問題。

F3：

或是遇到事情比較會退縮的，有沒有這種選項。

陳：

這個倒是可以用在偏差價值觀，比如說他認為在網路上做這些事情，不會損害到別人。這邊如果增加兩題的話，其一「我很容易相信網路的資訊」或「我認為網路是安全的，不容易被騙」；其二「碰到問題的時候，不會去向人家詢問、確認或求證」，這樣可以嗎？

F3：

可以。

F2：

剛剛我想到一個，在裡面我都沒看到「假消息」在裡面，假消息是很重要的關鍵字，如果放進去會造成困擾嗎？

陳：

不會，「假消息」會不會放在網路風險裡面，就是你可能會去點選跟犯罪偏差或是錯誤訊息。像剛剛主任有談到，被害者會去點假投資。可是民眾如何知道那是假訊息呢？其實在 LINE 上面蠻常看到轉發的假消息，Google 就能發現是假的。一般人不會辨識真消息、還是假消息，這可能是網路風險。

F2：

因為剛好這也常在現實裡發生，我想「假消息」是重要的。

陳：

沒錯，這是常常詐騙的重要風險，我們以前都沒有想到，但是經常碰到。再請教一下，第 6 頁的「最近一次的被害經驗」，我們是想要知道他 111 年 1 月 1 號到 12 月 31 號期間，若曾經回答上面這一些被害經驗，他勾有的話，就往下填答。剛剛 F3 談到這邊的 10 項，像「猜猜我是誰(假冒親友)」其實是電話詐欺。您是否建議在 165 名列前茅的放這裡即可，還是有些雖然排名不前面，但是造成的損失重大，或是安全威脅比較大。因為我們沒有辦法全部都放上去，有沒有我們漏掉的。

F3：

這可以啦，我剛有一份 165 的資料給你們，可以參考一下。

陳：

是，謝謝！然後想要再進一步確認，第 7 頁裡面列的 1 到 5。因為其實有些過時了，有些是新增，像您剛剛所談到的 Telegram 或是交友平臺詐騙。

F3：

這有可能要加到第 4，但是社群會有不同意義。

陳：

在第 3 題的接觸管道，想要再確認這個分類，或者是更新。

F3：

我反而覺得少了直播平臺，直播平臺要放在交友或社群都怪怪，宜獨立。

陳：

其實現在直播平臺非常紅耶，應該多一個，大家覺得如何？OK，那就是增加一個。

F3：

因為直播平臺也有很多詐騙，尤其是疫情期間，消費者無聊。

陳：

那我們就增加第 6 直播平臺，第 7 就是其他管道。括號裡面有沒有要修改？

F2：

小紅書是大陸的那個 App，臺灣現在這邊有詐騙嗎？

F3：

不多耶，小紅書有點像抖音，可是抖音比較偏直播平臺。

陳：

那我們需要去括號舉例，這邊應該列哪幾個會比較好？

F3：

其實我覺得 YouTube 也可以列，它也是社群的。

F4：

像館長直播都是透過 YouTube，其實很多直播是透過 YouTube 在處理。

F3：

直播是 YouTube、大陸的 Bilibili、然後抖音，而且抖音上面用了很多 deepfake，在臺灣的小孩子常在用 Bilibili。其實 LINE 本身它有一個直播 VOOM。

F4：

VOOM 既然已經在 LINE 底下，我們可能也不需要特別去強調。

F2：

臺灣有本土直播平臺嗎？

F3：

之前有，現在比較少，像大陸還有西瓜視頻、土豆，專門看盜版的。

陳：

OK，所以我們列這幾個，受訪者就知道我們要問什麼了。那像第 4 題「加害者的互動」，是透過遊戲、虛擬寶物、或網頁互動，這樣的問法妥適嗎？這邊列了 9 個，會不會跟前面的重疊？

F4：

還有社群媒體沒有列進去。第 3 個主要是匿名交友網頁的問題，像臉書不一定是匿名的，可能有些人具名。

許：

剛剛主任的意思是說「匿名」不要，就「交友網頁」。

陳：

OK，那還有要改、或是增加的？有沒有他們的互動方式是這邊漏掉的？

F1：

傳簡訊，然後叫你點連結加 LINE。

陳：

就像衛福部的「你已經有 COVID-19 的保險金」之類釣魚連結嗎？

F4：

那個會不會比較像是加害者主動接觸，因為是加害者直接丟訊息，叫你加 LINE。

陳：

有可能，所以我們列了這個 9 個目前還 OK，或前測之後再視情況增刪。那剛剛那個 F3 講到，損失金額太低了，要怎麼列比較妥適。其實我們已經比前次調查的損失金額有提高了，但我們的感覺還是會集中在前面。

F3：

因為以我們來看，實務上那個級距有點小。

陳：

我們也有參考官方調查的範圍，級距不知道怎麼列會比較好。一定要有損失嗎？沒有損失算不算？詐欺未遂算不算，一定要有既遂嗎？

F3：

如果是刑案的話，未遂也是要處理。可是我們剛剛把它定義成有財物損失，那我們在研究的網路詐欺行為，就應該只有財物損失。所以如果沒有付錢的，我建議不要列在上面。

陳：

那就牽涉到我們剛剛的第一個定義問題，就是透過網路管道，從事詐騙而造成財物損失。因為有損失跟沒損失，在 165 上會差很大量。

賴：

他不一定有損失，如果因為這樣，然後 depressed 而去看病，那算不算？

F3：

財物還是要有被交付，要有報案的話，幾乎都是被騙既遂的。我比較好奇是，為什麼要細分 5000 塊、1 萬塊、1 萬 5 的一個級距？

陳：

因為網路購物的損失比較低，錢比較少；沒有像投資都很多錢。

F3：

因為我們轉帳都 3 萬塊上限，1 千、1 萬、3 萬、10 萬，我們是這樣跳的，然後 50 萬、100 萬、1,000 萬。

陳：

因為從去年開始就有投資詐騙，它的量都至少百萬，所以您認為分 1,000、1 萬、3 萬、10 萬、50 萬，然後百萬以上、1,000 萬以下、1,000 萬以上。

F3：

其實因為有虛擬貨幣，所以現在要千萬不會難。

陳：

再請教一下，第 7「察覺跟反應」裡面，這些被害人通常都如何開始知道自己可能被害了。我們這邊列了 6 項，有沒有可能是我們這邊漏掉的，或者是用字需要修改的？

許：

第 5 個，如果還沒有恢復，3 個月以上可能還沒恢復、一直都沒有恢復，

1 千萬可能終身難恢復。

陳：

大概第 7 個選項「創傷沒有辦法恢復」，一輩子的陰影。請問最後第 8 頁的第 6 題「採取的反應措施」中，165 反詐騙專線跟到派出所報案有沒有差別？

F3：

有差，因為 165 是諮詢；一般民眾到派出所報案的話，警察才會處理。

許：

我們有問題的，都差不多解決了。

陳：

我們還有調查上的問題，以前的經驗是這種網路調查可能會有樣本偏差。我們擔心被害樣本太少，想把我們調查的訊息放在警察機關，然後讓民眾報案的話，順便把網路連結給他。也擔心因為填答的誘因，然後就像大家在搶優惠一樣，一下子就額滿，但是同質性太高。

就是說我們如何才能夠找到符合母群比例的網路使用者，因為我們只有一千個名額。除了被害樣本的聯繫之外，有哪些地方可以讓接觸的人面比較廣一點。像我們前一次的前導調查放在 165 的網頁上，就是希望能異質性大一點。我們也發現年輕人比較不會去填這個、女生比男生愛填，所以到最後也是進入校園跟街頭去做實體。大家對抽樣上，有沒有什麼建議？有沒有我們可以 PO 訊息的地方，放 QR code 或是一個連結。

F1：

里長辦公室。

賴：

放在警政署的網站。

許：

行文給刑事局。

F4：

檢察署或是警方這邊，應該都會是比較特別的群體。

陳：

哪些是一般民眾容易去瀏覽，或連結放在 FB 上面？

F3：

但是 FB 現在沒人敢亂貼，容易被 copy 轉去做詐騙。

葉：

因為 FB 太多一頁式的詐騙。

陳：

我們也很難找到中低階層的，後來我們就用滾雪球，比如說計程車司機、市場攤販。他們也有可能被騙，像這些樣本真的是蠻難找的。所以那時候我一部分街頭、一部分學校、一部分司法機關、一部分是訊息連結，可能要很多元管道才有辦法做到。

F4：

我想街頭可以考慮大賣場，像愛買、全聯，至少去的人就會比較多元。

陳：

對，那些大賣場，便利商店櫃臺也可以，把 QR code 放那裡，然後看到人就去掃。樣本就不會很特定，我們就希望士農工商、各種年齡、各種職業都能找到。現在透過 Survey Cake 只能夠控制樣本的性別跟年齡，可是像職業、婚姻、有無被害經驗，就很難控管。

賴：

謝謝各位，還有沒有要補充的？

F1：

請問一下調查對象的國籍有限制嗎？

陳：

要中華民國國籍。雖然移工在社區裡面很多，但是看得懂中文很難。

賴：

那我們要增加嗎？

陳：

應該不用。因為如果中文沒那麼好，應該看不懂，而且問卷很長。

賴：

對啊，這個有點壓力。

葉：

問卷上很多專有名詞，我覺得他們應該看不懂吧！

賴：

辛苦大家，我們今天感謝各位的參與，謝謝各位給我們寶貴的意見。希望後會有期，謝謝老師、謝謝各位！

附錄四：網路生活問卷調查知情同意書

親愛的網友您好：

這是一份由法務部司法官學院委託有關「我國網路詐欺被害調查與防制研究」的網路問卷，主要研究目的(1)透過網路被害調查，分析網路詐欺被害型態與被害者特性，以了解潛在被害者特性；(2)分析人口特性、心理特質、網路生活型態與情境機會等，對網路詐欺被害之影響；(3)根據研究結果提出預防網路詐欺被害對策與未來研究建議。調查對象為**18 歲以上之網路使用者**（另提醒未滿 20 歲者，若有需要可知會家長並討論參與意願）。本問卷僅施測 1 次，內容分為 4 個部分：人口特性、心理特質、網路生活型態與情境機會、網路詐欺犯罪被害等，**約需時 10 分鐘**，**填答時間低於 5 分鐘或重覆填答，將視為無效樣本**，感謝您撥冗填答。

本問卷採不記名及無法辨識個人資料的方式作答，所蒐集的網頁資訊保存至 116 年 1 月即刪除。研究團隊將盡力維護您的隱私及善盡保密責任，盡力減少可能的風險。此研究未來發表採整體分析，您不會被辨識出，將發表於期刊論文和研究助理之學術論文，亦無衍生的商業利益。此網站可能紀錄您的 IP 位址及電子信箱等個資，但僅供研究團隊聯絡且會善盡保密之責。本研究由中央警察大學委託國立成功大學人類研究倫理審查委員會倫理審查通過(編號：HREC-E-111-526-2)，若想諮詢參與研究的權益或提出申訴，請聯絡該委員會，電話:06-275-7575＃51020，email：em51020@email.ncku.edu.tw

請您自由決定是否填寫，亦可中途不填寫，無需感到壓力，惟一旦送交，本問卷無記名且無編碼，研究團隊將無法辨識送出的問卷，恕無法刪除您填寫的內容。**為感謝填答，前 1,200 名填完本問卷者可獲得統一超商(7-11)100 元現金抵用券，並請於問卷最末頁自由選填電子信箱或手機號碼，額滿為止。**若您想詢問本問卷內容，或有興趣得知研究結果，此研究將於 112 年 12 月 31 日完成，歡迎您依照下述方式索取研究結果摘要（請自行參閱法務部司法官學院網站，網址： https://www.tpi.moj.gov.tw）。

中央警察大學犯罪防治研究所
研究主持人 賴擁連教授 (yx1005@mail.cpu.edu.tw)
共同主持人蔡田木教授 (nua101@mail.cpu.edu.tw)
陳玉書副教授 (ysc3@mail.cpu.edu.tw)

敬上

112 年 05 月

※如同意填寫，請您自行列印或儲存本頁內容，並請點選「同意」選項，於下一頁開始作答。

※此網站可能紀錄您的 IP 位址及電子信箱等個資，但僅供研究團隊聯絡且會善盡保密之責。本研究由中央警察大學委託國立成功大學人類研究倫理審查委員會倫理審查通過，若想諮詢參與研究的權益或提出申訴，請聯絡該委員會，電話:06-275-7575＃51020，email：em51020@email.ncku.edu.tw

您若同意參與本問卷調查(網路生活經驗調查表，倫理審查通過編號：HREC-E-111-526-2)，請在以下□中打勾 「√」。

□ **同意**

附錄五：網路生活問卷調查表

您若同意參與本問卷調查（網路生活經驗調查表，倫理審查通過編號：HREC-E-111-526-2），請勾選「同意 」。

此題必填

- ○ 同意

1-1.請問您的主要職業為何？

此題必填

- ○ 無業/待業中
- ○ 學生
- ○ 家管
- ○ 公務人員(含軍、警、消、教育人員)
- ○ 網路銷售
- ○ 實體銷售
- ○ 服務業(含外送平台)
- ○ 農林漁牧礦工業
- ○ 建築/營造/製造/供應商
- ○ 金融/保險/房地產
- ○ 交通/運輸/旅遊/物流
- ○ 醫療相關(含長照)
- ○ 法律相關
- ○ 文藝/傳播/行銷
- ○ 資訊相關(電子科技、網路及電腦維修、軟體設計等)
- ○ 退休
- ○ 其他

1-2.您目前居住的地區是：

此題必填

- ○ 北部（北北基桃竹）
- ○ 中部（中彰苗投雲）
- ○ 南部（嘉南高屏）
- ○ 東部（宜花東）

離島（澎金馬）

1-3.您目前居住的地方屬於：

此題必填

農村偏鄉或原鄉

城市或都會區

1-4.您的性別是：

此題必填

男

女

1-5.您是**民國**_____年出生的

需介於 25 ~ 94 之間 可接受到小數點第 0 位

此題必填

請填入數字

1-6.包括你自己，目前您和你住在一起的人數有多少人？_____(例如：獨自1人，請寫1人。)

需介於 1 ~ 99 之間 可接受到小數點第 0 位

此題必填

請填入數字 人

1-7.您的教育程度是：

此題必填

1.國小或初(國)中(肄)業

2.高中或高職畢(肄)業

- 3.大學或專科畢(肄)業
- 4.研究所以上
- 5.其他

1-8.您目前的婚姻狀況是：

此題必填

- 1.未婚單身
- 2.已婚或再婚
- 3.離婚或分居
- 4.同居
- 5.夫或妻過世

1-9.您每個月的收入大約是新臺幣多少錢：

此題必填

- 無收入
- 未滿2萬元
- 2萬至未滿4萬
- 4萬至未滿6萬
- 6萬至未滿8萬
- 8萬至未滿10萬
- 10萬元以上

下列問題是有關您**過去一年**使用網路的情形，請點選最符合您個人實際狀況的選項。

2-1-1.一般而言，您**平均每天使用網路（含電腦、手機或平板等設備）上網幾小時**：

此題必填

- 1小時以內
- 1至2小時以內
- 2至4小時以內
- 4至6小時以內

- 6小時以上

2-1-2.您每週平均上網次數

此題必填

- 少於1次
- 1~3次
- 4~6次
- 7~9次
- 10次以上

2-1-3.星期六至星期日您**最常上網的時段**大約在何時段：

此題必填

- 08：01至12：00
- 12：01至14：00
- 14：01至18：00
- 18：01至22：00
- 22：01至02：00
- 02：01至08：00

2-1-4.您接觸網路的時間大約多久

此題必填

- 1年未滿
- 1年～2年未滿
- 2年～3年未滿
- 3年～5年未滿
- 5年～10年未滿
- 10年以上

2-1-5.您**目前有（或曾有）**哪些網路帳號或會員帳號?

複選

- [ ] 購物網站
- [ ] 線上遊戲
- [ ] 網頁留言討論區
- [x] 社群軟體(Telegram、LINE、IG、Facebook、Twitter、WeChat、抖音等)
- [x] 交友平台(Tinder、iPair、weTouch、SweetRing、JustDating、GoodNight等)
- [x] 直播平台(抖音、Bilibili、Voom、西瓜視頻、土豆等)
- [ ] 其他

2-1-6.您目前有（或曾有）哪些**社群軟體**帳號?

複選 此題必填

- [ ] Telegram
- [ ] LINE
- [ ] IG
- [ ] Facebook
- [ ] Twitter
- [ ] WeChat
- [ ] 抖音
- [ ] 其他社群軟體

2-1-7.您目前有（或曾有）哪些**交友平台**帳號?

複選 此題必填

- [ ] Tinder
- [ ] iPair
- [ ] weTouch
- [ ] SweetRing
- [ ] JustDating
- [ ] GoodNight
- [ ] 其他交友平台

2-1-8.您目前有（或曾有）哪些**直播平台**帳號?

複選 此題必填

- [ ] 抖音
- [ ] Bilibili

☐ Voom	☐ 西瓜視頻
☐ 土豆	☐ 其他直播平台

2-2.下列問題是有關您**過去一年**使用網路的情形，請點選最符合您個人實際狀況的選項。

此題必填

	經常	偶爾	很少	從未
1.從事網路購物。	○	○	○	○
2.從事網路投資。	○	○	○	○
3.瀏覽色情網站。	○	○	○	○
4.遊玩網路遊戲。	○	○	○	○
5.從網站上下載不明來源的檔案。	○	○	○	○
6.點擊不明來源的電子郵件。	○	○	○	○
7.與未知身分的網友透過網路聊天	○	○	○	○
8.點擊經由即時通訊軟體所接收到的未知來源檔案或附件。	○	○	○	○

2-3.下列問題是有關您**過去一年**接觸下列網路訊息的情形，請點選最符合您個人實際狀況的選項。

此題必填

	經常	偶爾	很少	從未
1.曾在網路看到線上賭博或下注賭盤的訊息。	○	○	○	○
2.曾在網路看到網路援交或一夜情的訊息。	○	○	○	○
3.曾在網路看到網路詐騙別人財物的訊息。	○	○	○	○

4.曾在網路上看到投資詐騙的訊息。	○	○	○	○
5.曾在網路看到買賣盜版軟體的訊息。	○	○	○	○
6.曾在網路或社群軟體看到買賣違禁物品/毒品/槍砲彈藥刀械的訊息。	○	○	○	○
7.曾未經允許使用他人帳戶或查看文件。	○	○	○	○
8.曾未經他人允許在電腦中增加/刪除/更改/列印資訊。	○	○	○	○

3-1.以下問題是有關您**對自己的看法或生活經驗**，答案並無所謂的對或錯，請點選最符合您的感覺或實際情況的選項。

此題必填

	經常	偶爾	很少	從未
1.我會一衝動起來就採取行動,沒有先停一下來想一想。	○	○	○	○
2.我比較關心短期內我所發生事,而比較不關心未來我可能發生的事。	○	○	○	○
3.我會做當下讓我感到快樂的事,即使我知道這樣做會犧牲我未來的目標。	○	○	○	○
4. 我不會花很多時間與精力去想未來、準備未來。	○	○	○	○
5.我喜歡做一些有點冒險的事來考驗自己。	○	○	○	○
6.做一些可能會使自己惹上麻煩的事,讓我感到興奮。	○	○	○	○
7.我會只為好玩而冒險。	○	○	○	○
8.對我來說,尋求刺激與冒險,要比安定(全)來得重要。	○	○	○	○
9.我很容易發脾氣(生氣)。	○	○	○	○
10.當我真的很生氣時,其他人最好離我遠一點。	○	○	○	○
11.我對人發脾氣時,我寧願傷害他們,也不願意告訴他們為甚麼我會生氣。	○	○	○	○
12.當我與他人的意見非常地不相合時,我很難心平氣和地與他談論問題。	○	○	○	○

3-2.下面這些題目是想了解您**對網路使用經驗的看法**，請點選最符合您的感覺或實際情況的選項。

此題必填

	非常同意	同意	不同意	非常不同意
1.我認為在網路下載非正版軟體不會造成他人損害。	○	○	○	○

2.我認為在網路上說他人壞話或不良評價，並不會對他人產生傷害。	○	○	○	○
3.我認為在網路創造不同的身分或偽裝自己並不容易被發現。	○	○	○	○
4.我認為使用網路詐騙成功也是一種本事。	○	○	○	○
5.我認為當一個人受不了網路誘惑，而說他人壞話/騙取他人感情/盜用他人帳號等是正常的。	○	○	○	○
6.我認為當一個人缺錢時，在網路上詐騙或偷盜是一件可以原諒的事情。	○	○	○	○
7.我認為在網路世界沒有人是誠實的，所以對他們說謊也是剛好而已。	○	○	○	○

3-3.下列問題是有關您**過去一年**使用網路的情形，請點選最符合您個人實際狀況的選項。

此題必填

	經常	偶爾	很少	從未
1.不只有一次有人告訴您，您花太多時間在網路上。	○	○	○	○
2.您花費在網路上的時間比原先預計的還要長。	○	○	○	○
3.您需要花更多時間在網路上才能得到滿足。	○	○	○	○
4.您不能控制自己上網的衝動。	○	○	○	○
5.您每天早上醒來或睡前，第一件想到的事就是上網。	○	○	○	○
6.您每次離開網路後，想去做別的事卻又忍不住再次上網看看。	○	○	○	○
7.不管再累，上網時總覺得很有精神。	○	○	○	○
8.當您想減少使用網路，會因而沮喪、心情低落、脾氣暴躁。	○	○	○	○
9.網路斷線或連不上時，您會覺得自己坐立不安。	○	○	○	○
10.因為上網的關係，您和家人或朋友實際見面互動減少了。	○	○	○	○

11.因為上網的關係，您從事其他休閒活動的時間減少了。	○	○	○	○
12.您曾因為上網而沒有按時吃飯或睡覺。	○	○	○	○
13.您對上網的興奮感或期待遠勝於其他人際互動。	○	○	○	○

4.下列問題是有關您**過去一年**使用網路的習慣及經驗，請點選最符合您個人實際狀況的選項。

此題必填

	經常	偶爾	很少	從未
1.您上網時，家人會注意您的網路使用情形	○	○	○	○
2.您上網時，朋友(或同事)會在您身邊提供意見	○	○	○	○
3.您會注意到在網路的空間中該留下何種個人資訊	○	○	○	○
4.您會知道自己的IP位址會被上網的網站記錄或追蹤	○	○	○	○
5.您會定期更改個人帳號密碼	○	○	○	○
6.您的電腦、手機或平板有安裝防毒軟體	○	○	○	○
7.您會到官方網站購物或下載軟體，避免到不知名網站	○	○	○	○
8.您使用公共場所的Wi-Fi (如機場/餐廳/旅館等)時，會留意來源及安全性	○	○	○	○
9.您瞭解電腦/手機/平板中提升隱私或安全權限的方法來保護自己	○	○	○	○
10.您曾在網路或社群軟體公開個人相關行蹤（如打卡）	○	○	○	○
11.您曾在網路或社群軟體公開身分職位、收入或個人財產	○	○	○	○
12.您會使用雙重認證（第2道密碼TWO-STEPS），傳密碼至使用者手機認證	○	○	○	○
13.在網路上看到疑似假的訊息會進行確認	○	○	○	○

5-1-1.請問您**過去一年**網路詐欺犯罪被害的類型及次數：

此題必填

	0次	1次	2次	3次	4次以上
1.上網購物時被騙	○	○	○	○	○
2.在網路上投資被騙	○	○	○	○	○
3.遭受網路交友或愛情詐騙	○	○	○	○	○
4.參加網路活動遭詐騙	○	○	○	○	○
5.遭受解除分期付款詐欺（ATM）詐騙	○	○	○	○	○
6.玩網路遊戲被騙	○	○	○	○	○
7.遭受不明人士盜(冒)用好友身分詐騙	○	○	○	○	○
8.參加求職遭詐騙	○	○	○	○	○
9.接獲「猜猜我是誰」之網路通話來電或訊息	○	○	○	○	○
10.其他網路詐騙被害（請於下題說明）	○	○	○	○	○

5-1-2.其他網路詐騙被害(請說明：＿＿＿＿)

請填入文字

5-2-1.請問您**過去一年**是否曾經有網路詐欺犯罪被害的經驗：

此題必填

○ 有　　○ 沒有

5-2-2.請問您**最近一次**所遇到的網路詐欺犯罪**被害類型**為何？

此題必填

- ○ 1.上網購物時被騙
- ○ 2.在網路上投資被騙
- ○ 3.遭受網路交友或愛情詐騙
- ○ 4.參加網路活動遭詐騙
- ○ 5.遭受解除分期付款詐欺（ATM）詐騙
- ○ 6.玩網路遊戲被騙
- ○ 7.遭受不明人士盜(冒)用好友身分詐騙
- ○ 8.參加求職遭詐騙
- ○ 9.接獲「猜猜我是誰」之網路通話來電或訊息
- ○ 10.其他網路詐騙被害（請說明）

5-2-3.請問您**最近一次**的網路詐欺被害，主要是透過哪種網路管道與加害者接觸：

複選 此題必填

- ☐ 1.購物網站
- ☐ 2.線上遊戲
- ☐ 3.網頁留言討論區
- ☐ 4.社群軟體（小紅書、Telegram、Skype、QQ、LINE、IG、Facebook、Twitter、WeChat、抖音等）
- ☐ 5.交友平台（Tinder、iPair、weTouch、SweetRing、JustDating、GoodNight等）
- ☐ 6.直播平台（抖音、Bilibili、Voom、西瓜視頻、土豆等）
- ☐ 7.其他管道

5-2-4.請問您**最近一次**遇到的網路詐欺被害，是以什麼情形下跟這位**加害者互動**：

複選 此題必填

- ☐ 1.線上遊戲交戰/同隊
- ☐ 2.虛擬寶物交易
- ☐ 3.交友網頁/軟體
- ☐ 4.加害者主動接觸
- ☐ 5.購物
- ☐ 6.性交易
- ☐ 7.曾見面之朋友介紹
- ☐ 8.未曾見面之網友介紹

☐ 9.參考網路評價

☐ 10.其他

5-2-5.您與加害人相識的程度如何？

此題必填

○ 1.熟識

○ 2.普通

○ 3.初識

○ 4.不認識

5-2-6.請問您**最近一次**遇到的網路詐欺犯罪被害，**交款或匯款(含實體或網路)時間為**：

此題必填

○ 08：01至12：00

○ 12：01至14：00

○ 14：01至18：00

○ 18：01至22：00

○ 22：01至02：00

○ 02：01至08：00

5-2-7.您最近一次所遭遇的網路詐欺犯罪被害交易方式為

此題必填

- ○ 1.現金
- ○ 2.超商付款
- ○ 3.遊戲點數（MY CARD、GASH+等）
- ○ 4.實體ATM轉帳
- ○ 5.信用卡
- ○ 6.網路ATM轉帳付款（含虛擬帳號）
- ○ 7.行動支付（Line pay、Apple pay、Google pay、街口支付等）
- ○ 8.線上支付軟體（含信用卡、第三方支付）
- ○ 9.金融機構匯款（如：銀行、郵局）
- ○ 10.網路銀行付款
- ○ 11.其他

5-2-8.請問您**最近一次**網路詐欺犯罪被害損失之總金額為多少：（單位為新臺幣）

此題必填

- ○ 未滿1千元
- ○ 1001元至未滿1萬元
- ○ 1萬元至未滿 3萬元
- ○ 3萬元至未滿 10萬元
- ○ 10萬元至未滿50萬元
- ○ 50萬元至未滿100萬元
- ○ 100萬元至未滿1000萬元
- ○ 1000萬元以上
- ○ 沒有損失

5-3-1.請問您**最近一次**所遇到的網路詐欺犯罪被害，如何得知自己被害：

此題必填

- ○ 自己察覺
- ○ 警方通知
- ○ 朋友或同事發現
- ○ 親人發現

- ○ 超商店員提醒
- ○ 金融機構櫃檯提醒/報警
- ○ 7.其他

5-3-2.請問您**最近一次**所遭遇的網路詐欺犯罪被害，經過多久警覺自己遭受到詐騙？

此題必填

- ○ 1天以內
- ○ 1～3 天
- ○ 4～6 天
- ○ 7～14 天
- ○ 14～30 天
- ○ 30天以上

5-3-3.請問您**最近一次**所遭遇的網路詐欺犯罪被害，您覺得自己被害的原因為何：

複選 此題必填

- ☐ 自身疏忽
- ☐ 貪小便宜
- ☐ 過於相信別人
- ☐ 自己太笨
- ☐ 產品很吸引人
- ☐ 缺乏自我保護常識
- ☐ 許多網友分享
- ☐ 按讚數很高
- ☐ 運氣不好
- ☐ 不清楚
- ☐ 價格不高被騙無所謂
- ☐ 其他

5-3-4.這件事件對您造成心理創傷、不安或焦慮之嚴重程度？

此題必填

- ○ 1.非常嚴重
- ○ 2.嚴重

- ○ 3.不太嚴重
- ○ 4.一點也不嚴重
- ○ 5.沒意見/很難說
- ○ 6.不知道

這件事件發生後，您經過多久才恢復正常生活？

此題必填

- ○ 立即就恢復
- ○ 一週內
- ○ 半個月內
- ○ 一個月內
- ○ 一至二個月
- ○ 三個月以上
- ○ 永遠難以恢復

5-3-5.請問您**最近一次**所遇到的網路詐欺犯罪被害，您當時所採取的應對措施為何：

複選 此題必填

- ☐ 跟家人討論
- ☐ 跟朋友討論
- ☐ 撥165反詐騙專線
- ☐ 網路平台客服申訴
- ☐ 沒有處理
- ☐ 向警察報案
- ☐ 在網路上公告經驗
- ☐ 其他

5-3-6請問您**最近一次**所遭遇的網路詐欺犯罪被害，是否有向警察機關報案？

此題必填

- ○ 1.有
- ○ 2.沒有

5-3-8.您有被害經驗之後，曾經採取以下什麼措施？

複選 此題必填

- [ ] 避免在網路上留下個人資訊
- [ ] 避免至不知名網站下載軟體
- [ ] 避免使用公共場所的Wi-Fi
- [ ] 避免在社群軟體公開個人行蹤
- [ ] 在網路上看到疑似假的訊息會進行確認
- [ ] 網路上遇到可疑網址或聯結，會詢問家人/朋友/同事意見
- [ ] 更改帳號密碼
- [ ] 安裝防毒軟體
- [ ] 提升網路瀏覽隱私或安全權限
- [ ] 雙重認證(第2道密碼TWO-STEPS)，傳密碼至使用者手機認證。

附錄六：個別訪談知情同意書

親愛的受訪者您好：

我們是中央警察大學犯罪防治學系所的研究團隊，研究計畫主持人為賴擁連教授。我們很誠摯地邀請您協助我們進行有關「我國網路詐欺被害調查與防制研究」的經驗分享。

研究計畫名稱或主題：我國網路詐欺被害調查與防制研究
研究計畫執行機構：中央警察大學
研究主持人：賴擁連　　**職稱：**教授兼所長
協同主持人：蔡田木　　**職稱：**教授
協同主持人：陳玉書　　**職稱：**副教授
研究計畫聯絡人：劉士誠　**E-mail：**cityliu@cib.npa.gov.tw　**電話：**02-27612456
研究經費補助／贊助單位：法務部司法官學院
倫理審查委員會審查通過機構與案號：國立成功大學倫審會字第111-526-2 **號**

■研究目的

(一)蒐集國、內外網路詐欺之相關調查或官方資料中網路詐欺定義，並編製網路詐欺被害調查問卷，進行調查以分析網路詐欺被害者人口特性、心理特質、網路生活型態與情境機會，以及網路詐欺被害經驗等變項分布情形。

(二)針對網路詐欺之定義、型態、範疇，以及網路詐欺被害調查問卷設計的妥適性，邀請相關領域之實務、學術工作者召開專家焦點座談，以利調查之進行。

(三)於網路問卷調查後，針對網路詐欺加害人進行質性訪談，並與網路被害調查結果進行比較分析。

(四)參考實證研究調查發現與國外防治經驗，擬訂防制對策，並邀請相關領域之實務、學術工作者開專家焦點座談，討論提出未來改善網路詐欺犯罪與被害之實務對策或修法建議。

(五)根據上述研究發現提出網路詐欺犯罪與被害之預防對策，並於學術發表會發表研究成果，提供民眾與政府機關參考。

■為何邀請您參與？

本研究規劃採「半結構式」方式進行訪談，依據本研究之研究架構擬定訪談大綱，由研究者本人及受過訓練的訪員進行面對面的深度訪談，訪談地點將以受訪者之所在地為主，最主要讓受訪者依循訪談大綱回答問題，並依實際回答情形，彈性調整訪談問項之內容及順序，希望能更清楚地瞭解受訪者之個人生活與過往經驗。

■研究活動

（一）時間及地點：由研究團隊親臨拜訪受訪者進行訪談，地點主要是以受訪者之所在地為主，若為受訪對象為在監服刑，由監所安排適當的訪談方式及場所。為因應 Covid-19 疫情關係，訪談方式亦可彈性改採線上視訊進行訪談。

（二）參與方式及內容：每名受訪者皆進行 1 到 2 次的深度訪談，每次訪談時間約 2 小時，以獲得完整之資料。

（三）錄音（或錄影）：為了正確記錄資料，如果您不願意或中途想停止，可隨時提出，不用有壓力或不好意思。

（四）您的資料將受到妥善保密：訪談內容會以代碼取代真實的姓名，我們會負起保密責任，不會向任何人透漏。如果您有顧慮，請讓我們知道。若為在監者，請監所管理人員轉交知情同意書，他們只是「協助」而已，無論您是否參加研究，皆不影響監所管理人員對您的觀感。

■可能承受的風險及因應的措施

參與這個研究，可能的風險為需要請您分享個人的過往經驗，所取得的資料將會做為研究使用分析。若您因參與本研究會覺得心理有壓力或不舒服，請慎重考慮是否參與，不要勉強。

■研究補償

完成訪談後，我們會提供 **1,000 元訪談費**。

■研究資料之保存期限、運用規劃及到期後處理規劃

（一）您所提供的訪談資料，我們將在輸入電腦且編碼後，妥善保存在設有密碼的硬碟或電腦裡，本研究的訪談內容、資料保管及處理使用，皆依研究倫理等相關規定。

（二）未來研究成果呈現時，您的真實姓名及個人資料將不會出現在報告上；若您有興趣瞭解研究結果，完成研究後，可提供您摘要報告。

（三）訪談資料之錄音、錄影與逐字稿，於本研究計畫執行 2023 年 12 月 25 日結束後 3 年刪除銷毀。

■資料的使用範圍

訪談所得的資料將做為研究分析使用，作為預防網路詐欺被害的政策參考。並將研究結果之資料提供「其他研究者資源分享」、所有發表文章、論文和上傳資料均將依規定做連結。換言之，將來無論是資料傳遞、分享、撰寫報告或發表文章，別人皆無法從中辨識出您的真實身分，對於資料及身分保密的部分，請您放心！

■暫停及退出研究之權益

過程中，若您感到不舒服，想要暫停或退出研究，我們會完全尊重您的意願。先前已蒐集的資料將進行銷毀。即便研究結束，有任何問題，都歡迎聯絡我們。

■訪談過程錄音錄影

為了正確記錄資料，在進行訪談過程中將會以手機或攝影機能夠錄取聲音或影像功能的設備錄音錄影。如因 Covid-19 疫情關係，訪談方式採取線上視訊訪談，會以電腦內建軟體錄音錄影。避免錄製時，錄影資料容易曝露受訪者的臉部特徵和場景資料，我們會以軟體後製錄影內容，模糊容易辨識的個人資料特徵。

■第三方研究諮詢管道

本研究由中央警察大學委託國立成功大學人類研究倫理審查委員會倫理審查通過，如有疑問請聯絡此 email：
em51020@email.ncku.edu.tw

■雙方簽名欄位

上述內容，您有任何問題，請儘管提問。

如同意參與，請您於下方簽署；如不同意，也請不用為難！

研究參與者簽署欄：

錄音　□同意　□不同意

錄影　□同意　□不同意

簽名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　日期：　　年　　月　　日

研究團隊簽署欄：□本同意書一式兩份，將由雙方各自留存，以利日後聯繫

計畫主持人簽名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿　日期：　　年　　月　　日

附錄七：個別訪談大綱

網路詐欺加害者深度訪談大綱

訪談時間：112 年___月___日___時___分至___時___分。

受訪人編號：_____；訪談地點：_____；訪談人：_____。

一、基本資料：

1-1. 首先，請教您一些個人的基本資料。(含性別、年齡、婚姻和家庭狀況)

1-2. 請您談談您的教育程度、成長過程及家庭背景。

1-3. 請談談您的網路生活型態（使用網路的時間、常使用的網路資源或平臺)。

1-4. 您這次入監之刑期多久？入監已經多久了？是否有網路詐欺以外的其他案件？

1-5. 是否有其他犯罪前科？

二、從事網路詐欺之情形

2-1. 您從事網路詐欺有多久的時間？您在何種情形下開始從事網路詐欺(是否因曾有詐欺被害經驗而開始從事）？

2-2. 您為何選擇（持續）從事網路詐欺？有無考慮過從事其他犯罪？

2-3. 您所從事的網路詐欺之具體工作內容為何？您當時投入網路詐欺工作之時間、精力程度如何？

2-4. 請您談談您是如何學習、精進或改良從事網路詐欺之相關技巧及方法？

2-5. 請您談談您選擇網路詐欺被害人時有哪些關鍵考量因素？請詳述哪些人口特性或心理特質是您較偏好的？

2-6. 您從事網路詐欺有何偏好的時段？請詳述您在時段選擇上的考量因素？

2-7. 您認為在何種網路場域、平臺上實施網路詐欺得手成功率較高？

2-8. 您認為以何種獲利方式、財物（含虛擬財物）作為網路詐欺標的物得手成功率較高？請詳述您在獲利方式、財物選擇上的考量因素？

2-9. 您所從事的網路詐欺之獲利報酬與獲得方式與您原本的預期是否有落差？

2-10. 對於您所從事網路詐欺是否有其他心得感想或意見？

三、對於網路詐欺防制策略之認知

3-1. 您從事網路詐欺後多久時間後被查獲？您認為被查獲的關鍵具體原因為何？

3-2. 與其他犯罪相比，您認為從事網路詐欺之的風險程度如何？您認為從事網路詐欺有哪些風險？

3-3. 您認為在網路環境中有哪些數位監控措施？您認為目前網路環境中的數位監控強度如何？

3-4. 在從事網路詐欺時，您會採取哪些具體措施以降低風險、規避監控及查緝？請詳述您如何設計及規劃資訊、金錢流路或其他規避措施。

3-5. 您認為警察查獲網路詐欺之能力如何？是否與您從事網路詐欺前之預期有落差？

3-6. 您認為政府之反詐騙宣導（或其他預防策略）是否能有效避免被害者受騙？您認為哪些是有效之預防策略。

3-7. 有關政府採行的網路詐欺預防策略，您有何其他建議？

【訪談結束，謝謝您的受訪與提供寶貴意見！】

附錄八：焦點團體知情談同意書

○○您好，

我是中央警察大學犯罪防治學系賴擁連教授，目前在進行由法務部司法官學院補助的「我國網路詐欺被害調查與防制研究」計畫(如附件 1)，此項計畫主要目的在了解網路詐欺被害型態與被害者特性之分布，分析網路詐欺被害之影響因子，以提供網路使用者與相關單位預防網路詐欺被害之參考。希望邀請熟悉網路詐欺被害與犯罪之學者專家，舉行 1 場焦點團體座談，時間約為 2 小時，協助檢視本研究之網路問卷初稿(如附件 2)，並根據您的專業經驗，提供修改問卷之建議。

為了資料紀錄的正確性，焦點座談時將錄音；如果您不願意錄音、不願某段發言錄音或中途想停止，請隨時提出。我們將提供出席費予您（含退出者），聊表謝意。提醒您，本次焦點座談為多人參與，團體中的發言內容將與所有受訪者共享，但參與者必須尊重彼此隱私，未經允許不得對外透露重要訊息。

錄音資料彙整為摘要紀錄後會再請您確認，我們會負起保密責任，未來研究成果不會呈現您的真實姓名，亦會盡力避免他人從研究發表辨識出您。焦點團體的摘要紀錄中，僅摘錄您對於網路調查問卷修改之客觀建議，所有參與者將以編號呈現，以達去除辨識連結之目的。但在非預期情況下您的身分仍有可能被揭露，請您慎重考慮是否參與焦點座談。

錄音與摘要紀錄將妥善保存在賴擁連教授研究室設有密碼的硬碟或電腦裡，3 年後刪除銷毀，並只使用在本研究或教學。若您有興趣瞭解研究結果，可提供您報告摘要。

過程中，若您感到不舒服，想要暫停或退出焦點座談，我們會完全尊重您的意願，所蒐集有關您的座談資料將予以刪除。即使研究結束，有任何問題，均歡迎聯絡我們。

研究團隊：

計劃主持人：中央警察大學犯罪防治學系賴擁連教授

經費來源：法務部司法官學院

計畫聯絡人：劉士誠，電話：0912-136093，E-mail：cityliu@cib.npa.gov.tw

本研究由中央警察大學委託國立成功大學人類研究倫理審查委員會倫理審查通過，若想諮詢參與研究的權益或提出申訴，請聯絡該委員會，電話:06-275-7575＃51020，email：em51020@email.ncku.edu.tw

焦點團體參與者簽署欄：

錄　　音：□同意-錄音　□不同意-錄音

成果回饋：□無需□研究完成請提供報告，寄至（電子信箱或地址:_____）

簽名：_____　日期：　年　月　日

研究團隊簽署欄：

□本同意書一式兩份，將由雙方各自留存，以利日後聯繫

計畫主持人/研究人員簽名：_____日期：　年　月　日

附錄九：發函刑事局協助問卷 165 公告

抄本

檔　　號：
保存年限：

中央警察大學　函

機關地址：333322桃園市龜山區大崗里
樹人路56號
承 辦 人：蔡文瑜
電　　話：03-3281891分機4276
傳　　真：03-3963277
電子信箱：tsallyfish@mail.cpu.edu.tw

受文者：
發文日期：中華民國112年5月17日
發文字號：校防字第1120004438號
速別：普通件
密等及解密條件或保密期限：
附件：問卷募集海報1份

裝

主旨：本校教授賴擁連執行之法務部司法官學院112年委託研究案，請貴局協助網路問卷宣傳事宜，請查照。

訂

說明：

一、旨揭研究案名稱：「我國網路詐欺被害調查與防制研究」，執行期間自112年1月1日起至112年12月31日止。

二、研究目的如下：

(一)透過網路被害調查，分析網路詐欺被害型態與被害者特性，以了解潛在被害者特性。

線

(二)分析人口特性、心理特質、網路生活型態與情境機會等，對網路詐欺被害之影響。

(三)根據成果提出預防網路詐欺被害對策與未來研究建議。

三、為使研究順利實施，請貴局於內政部警政署165全民防騙網及其他網路平臺協助向民眾推廣「網路生活問卷調查表」填答事項，網路問卷網址：https://www.surveycake.com/s/44ApZ。

四、本研究預計於112年8月31日完成，敬請協助推播週知。

正本：內政部警政署刑事警察局
副本：

第1頁，共1頁

附錄十：發函刑事局協助問卷轉知所屬

抄本

檔　　號：
保存年限：

中央警察大學　函

機關地址：333322桃園市龜山區大崗里
樹人路56號
承 辦 人：蔡文瑜
電　　話：03-3281891分機4276
傳　　真：03-3963277
電子信箱：tsallyfish@mail.cpu.edu.tw

受文者：
發文日期：中華民國112年6月21日
發文字號：校防字第1120005765號
速別：普通件
密等及解密條件或保密期限：
附件：如說明四

裝

主旨：本校為研究「網路詐欺被害防制」調查，請惠允轉知所屬機關協助，請查照。

訂

說明：

一、本校教授賴擁連受法務部司法官學院112年委託研究旨案，請協助網路問卷宣傳事宜。

二、問卷調查期間：自112年1月1日起至112年8月31日止。

線

三、研究目的：

(一)透過網路被害調查，分析網路詐欺被害型態與被害者特性，以了解潛在被害者特性。

(二)分析人口特性、心理特質、網路生活型態與情境機會等，對網路詐欺被害之影響。

(三)根據成果提出預防網路詐欺被害對策與未來研究建議。

四、為宏大調查量能，除請轉知各縣市警察機關加強宣導第一線受理報案員警，於受理報案時，併宣導民眾掃瞄QR Code協助問卷填報外，賡續於「內政部警政署165全民防騙網」及其他網路平臺向民眾推廣「網路生活問卷調查表」填答事項。

五、網路問卷網址：https://www.surveycake.com/s/44ApZ。

正本：內政部警政署刑事警察局打擊詐欺犯罪中心

附錄十一：第二次焦點團體座談知情同意書與訪綱

網路詐欺被害調查研究政策焦點團體座談會

研究題目: 我國網路詐欺被害調查與防制研究

委託單位: 法務部司法官學院

研究倫理審查編號:成功大學人類研究倫理審查委員會案件編號: HREC-E-111-526-2

時間:112 年 8 月 9 日(週三)下午 2 點

地點:中央警察大學研究大樓 2 樓 232 教室 (桃園市龜山區樹人路 56 號)

研究目的:

一、 蒐集國、內外網路詐欺之相關調查或官方資料中網路詐欺定義，並編製網路詐欺被害調查問卷，進行調查以分析網路詐欺被害者人口特性、心理特質、網路生活型態與情境機會，以及網路詐欺被害經驗等變項分布情形。

二、 針對網路詐欺之定義、型態、範疇，以及網路詐欺被害調查問卷設計的妥適性，邀請相關領域之實務、學術工作者召開專家焦點座談，以利調查之進行。

三、 於網路問卷調查後，針對網路詐欺加害人進行質性訪談，並與網路被害調查結果進行比較分析。

四、 參考實證研究調查發現與國外防治經驗，擬訂防制對策，並邀請相關領域之實務、學術工作者召開專家焦點座談，討論提出未來改善網路詐欺犯罪與被害之實務對策或修法建議。

網路犯罪被害調查研究政策焦點團體座談 邀請出席學者專家

參加場次	專家學者代碼	服務單位
第 2 場次	F5	律師事務所、前檢察官
	F6	OO 金融科技公司執行長
	F7	OO 國際商業銀行資安長
	F8	OO 大學資管系助理教授
	F9	OO 警察局股長

研究團隊出席名單：賴擁連、許春金、蔡田木、蔡文瑜

焦點團體知情同意書

您好，

我是中央警察大學犯罪防治學系賴擁連教授，目前在進行由法務部司法官學院委託的「我國網路詐欺被害調查與防制研究」計畫(如附件 1)，此項計畫主要目的在了解網路詐欺被害型態與被害者特性之分布，分析網路詐欺被害之影響因子，以提供網路使用者與相關單位預防網路詐欺被害之參考。希望借重各位對於網路詐欺犯罪熟悉之學者專家，舉行 1 場焦點團體座談，時間約為 2 小時，以協助本研究團隊，從政策面、實務面等角度，提供寶貴的想法、意見與建議，形成精進作為與對策，提供政府相關部門參考。本焦點團體座談之訪談大綱詳附件 2。

為了資料紀錄的正確性，焦點座談時將錄音；如果您不願意錄音、不願某段發言錄音或中途想停止，請隨時提出。我們將提供出席費新臺幣 2,000 元予您（含退出者），聊表謝意。提醒您，本次焦點座談為多人參與，團體中的發言內容將與所有受訪者共享，但參與者必須尊重彼此隱私，未經允許不得對外透露重要訊息。錄音資料彙整為摘要紀錄後會再請您確認，我們會負起保密責任，未來研究成果不會呈現您的真實姓名，亦會盡力避免他人從研究發表辨識出您。焦點團體的摘要紀錄中，僅摘錄您對於網路詐欺犯罪防制作為之想法、意見與建議，所有參與者將以編號呈現，以達去除辨識連結之目的。但在非預期情況下您的身分仍有可能被揭露，請您慎重考慮是否參與焦點座談。

錄音與摘要紀錄將妥善保存在賴擁連教授研究室設有密碼的硬碟或電腦裡，3 年後（115 年 12 月）刪除銷毀，並只使用在本研究或教學。若您有興趣瞭解研究結果，可提供您報告摘要。過程中，若您感到不舒服，想要暫停或退出焦點座談，我們會完全尊重您的意願，所蒐集有關您的座談資料將予以刪除。即使研究結束，有任何問題，均歡迎聯絡我們。

研究團隊：

計劃主持人：中央警察大學犯罪防治學系賴擁連教授

經費來源：法務部司法官學院

計畫聯絡人：劉士誠，電話：0912-136093，E-mail：cityliu@cib.npa.gov.tw

本研究由中央警察大學委託國立成功大學人類研究倫理審查委員會倫理審查通過(案件編號: HREC-E-111-526-2)，若想諮詢參與研究的權益或提出申訴，請聯絡該委員會，電話:06-275-7575 # 51020，email：em51020@email.ncku.edu.tw

焦點團體參與者簽署欄：

錄　　音：□同意-錄音　□不同意-錄音

成果回饋：□無需 □研究完成請提供報告，寄至 (電子信箱或地址:_____)

簽名：_____　日期：　　年　　月　　日

研究團隊簽署欄：

□本同意書一式兩份，將由雙方各自留存，以利日後聯繫

計畫主持人/研究人員簽名：_____日期：　　年　　月　日

焦點團體座談之訪談大綱

1. 從各國網路詐欺被害調查之管道與機制得知，有無值得借鏡之處？
2. 網路詐欺犯罪有無資訊/資安/理工等相關理論可解釋其行為或模式?
3. 從網路詐欺被害經驗問卷調查結果得知，被害人之心理特質與網路生活型態與其網路被害息息相關，請問被害人可以如何防範被網路詐欺被害？
4. 從網路詐欺犯罪加害者的深訪結果得知，執法部門可以從何處強化，以降低渠等犯案動機或減少被害人被詐機會？
5. 從網路詐欺犯罪被害者與加害者之心理特質與日常生活之相同與相異點分析，可否提供相關的抗制網路詐欺犯罪對策？
6. 晚近新加坡/中國等華人社會對於網路詐欺犯罪之抗制策略，是否有參考採之處?
7. 當前政府打擊詐欺犯罪之策略，是否應該針對不同類型(例如購物、投資與電信客服..)，提供不同的策略方式？
8. 行政院於今年 5 月成立專責之打詐辦公室，以強化當前打詐的編制，迄今有無相關成效？

附錄十二：第二次焦點團體座談會議紀錄

賴擁連主任（以下簡稱賴）：

歡迎各位，我們的研究團隊老師，重要的與會專家們。我們在進行司法官學院網路詐欺被害研究，感謝大家參加最後一場的焦點團體座談。首先逐一介紹今天與會的學者專家，第一位是 F5 律師，F5 律師之前也是檢察官，針對網路詐欺犯罪有不錯的見解，可以提供研究團隊一些政策上的建議。第二位是 F6，也是我們的博士生，那他一直沉浸在網路犯罪、資安等區塊，所以我也邀請他來。第三位是 00 國際商業銀行的資安長 F7，現在資安在業界話題不斷，所以我們想聽聽業界的意見。第四位是 00 大學資管系新聘的助理教授 F8，他也是這方面的專家。最後一位是 00 警察局的股長 F9，。那接著介紹我們的團隊，許春金老師，是我們研究案當中很重要的幕後的推手，很感謝老師給我們幫忙，接著是協同主持人教務長蔡田木博士。

時間寶貴的關係，我們就針對提供給各位的訪談大綱，很多都是司法官學院想了解現在政府因應打詐面臨的問題或瓶頸，也希望我們研究案能夠有一些建議，所以就教各位，請大家知無不言、言無不盡。

F7：

因為我二十幾年都在刑事局偵九隊、電偵、研發科等單位，也有一些網路偵辦的經驗，所以先把過去看到的國外做法，跟大家分享。我覺得網路犯罪從 90 年初到現在，一直呈現成長的趨勢，沒辦法有效的解決。第一個問題就是網路身分具有匿名性；第二個是很容易的跨國（境），藏匿於世界上任何國家犯罪者都可以對臺灣民眾進行詐騙。所以我們常常遇到網路犯罪的時候，會評估犯罪者是不是在國內。因為很多案件的嫌犯可能在國內，但偵查人員會誤判犯罪者在境外，所以喪失後續的調查及破案契機。

建議針對網路犯罪或是詐欺等，國際合作跟資訊共享是很重要的。第二個在網路技術或網路知識的教育，讓偵查人員有這方面的思維或知識。現在遇到跳板的問題，或使用更高深網路技術，比如說查到國外的 IP，偵查員就會直覺研判人在國外，但是實際的使用者是在國內。刑事局這幾年一直做科偵教育訓練課程，讓偵查員理解網路原理及科技偵查這非常重要。

F5：

延續 F7 剛剛講的，我之前當檢察官的時候，曾經參加美國檢察官協會的研習，和其他國家檢察官就網路犯罪議題交換意見，韓國的檢察官告訴我他們很常使用 24/7 Cybercrime Network，此機制就是透過國際協議，由各國司法警察協助盡快的保全證據。因為若經過司法互助的方式取得相關數位證據的內容，曠日廢時、徒勞無功。韓國的 24/7 機制是在最高檢察署，有網路犯罪專責機構處理，透過 24/7 機制請其他國家保全證據，後續再調資料。

我們現在遇到的網路詐欺，只要遇到跨國 IP 或是加密貨幣金流的情況，很難去偵查。跨國之間的合作，不只是檢察官層級的合作，更需要警政的互助。

蔡田木教務長（以下簡稱蔡教務長）：

兩位都是針對一個議題，就是我們應該有跨境的司法互助。那在實務上，這樣的合作有沒有執行的困境；或是在規範或作法上，有沒有建議的地方、哪個政策可以做一些改變？

F5：

我感覺警政跟其他國家的連結其實比檢察官高很多，比檢察官正式的司法互助管道更快捷。是以回歸到警察機關管道，在執行上有益於跨境司法互助政策。

F7：

我們在歐洲國家只有荷蘭派駐警務秘書，一個人要負責全歐洲，他的 loading 非常的重。我建議警務駐外聯絡官的數量，能夠再多一些人，當成我們國際合作的重要窗口。

蔡教務長：

建議在哪些國家新增駐點呢？

F7：

例如東歐國家、非洲、南亞等，在各地區的密度都能夠再增多警務秘書。

F9：

我以聯絡官的關係來做一個說明，以前曾以網路偵查技術查到 80 幾個詐欺機房的 IP，分發給各地的警察聯絡官查緝。結果回覆最快的就是泰國，因為有良好的 P2P 交流。其他國家就很可惜，最後石沉大海。不然泰國有的話，其他國家應該也有。

賴：

像美國大概 2021、2022 年成立中央層級的 IC3，有點像我們的 165，但是網路上就可以受理詐騙被害人的報案。另外，他們也有跨區、跨部會層級的網路或資安情資安全中心。那我們的 165 詐騙專線有沒有可能優化或精進化，成為像美國的報案網路平臺；而我們的打詐中心能否提升位階，或是成立跨部會整合的機制。

F9：

165 的招牌雖然很大，但實際上是內政部警政署刑事警察局打擊詐騙犯罪中心底下的一個股。在跟其他部會協調的時候，除非獲得行政院支持，不然很難說動其他行政機關。以電信詐騙來說，「+」是國際來電現在已是耳熟能詳。但在 165 成立之初（94、95 年），因為國際交換機的規則沒有統一，所以等到行政院成立打詐國家隊，NCC 一聲令下，所有電信業者都統一了。主管機關的態度很重要，他對自己目的事業才有箝制、管理能力。像刑事局這樣的四級機關要做這個事情，其實相當的辛苦。

F6：

我比較站在產業的立場去看，像我一開始接觸區塊鏈，是因為進到加密貨幣的交易所工作。但業者不重視回覆 165 的投單，因為並無強制力；再加上投單平臺蠻不友善的，其實業者沒有辦法收到通知。所以警方跟國內業者之間的聯繫，就有許多阻礙。

我中正碩班的口委是廖 OO 老師，九大隊當時是林 OO 主任，我們就開始跟刑事局開始用個案的方式，直接從案件學習查交易所的區塊鏈技術。我們跟交易所對接後發現，交易所是私人企業，在乎公私部門之間的信任感。

這兩三年，我們也跟國際合作，例如挪威有一間公司，可以讓檢察官、律師入股當合夥人，他們在挪威處理加密貨幣的案件。我很好奇他們對政府的幫助，他說挪威的警察跟臺灣某種程度也蠻像的，缺乏對科技偵查的認識。可是他們很願意跟產業合作，挪威政府所缺乏的，則尋求產業合作技術，也很願意跨國合作。

我的重點在跟產業合作，政府會省掉很多的成本。以區塊鏈、加密貨幣而言，不管是交易所或錢包廠商都可以幫我們有效的防堵。已經不只是國與國之間，而是公司對公司、產業對產業，需要大家有意識建立防護網。另外，國外還有在推專家鑑定，這個也可以彌補警方在科技偵查上的不足。臺灣的詐欺是全世界數一數二的厲害，我覺得政府的司法、行政要想辦法統一，在裁處方面有洗錢防治法、虛擬通貨辦法等，卻沒辦法有效的落實，所以在國際合作之前，內部要先整合。

賴：

能不能請 F8 跟我們分享意見。

F8：

我個人看法是，其實外國有很多制度，那我們政府有仿照歐盟提出「數位中介服務法（以下稱中介法）」，但被外界說政府要監控社群媒體，然後無法取得社會共識。為什麼會提中介法，我自己常思考怎麼樣讓案件量變少，方法之一就是讓被害人看到這個東西是詐騙，165 針對假投資網站做警示頁面，但目

前警示頁面沒有足夠明確的法律依據，倘若中介法通過，就會有較明確的依據。再者能否使用扣押裁定，技術上來說新生成網域的速度非常快，10 分鐘左右就能完成，而扣押裁定可能要耗時數日，這時詐騙集團已生成不知道多少個域名了，真的是緩不濟急，這不僅是沒有效率的問題，而是根本無法達到實際的作用。又如最近最高法院宣判無效的 M 化車使用，以及之前 108 年通保法草案所列的網路流量紀錄等科偵手段法制尚待社會達成共識立法通過。

而詐欺犯罪偵查時常遇到斷點，無法繼續下去，若我們有像英國的調查權力法案（Investigatory Powers Act 2016），適當保留網際網路流量紀錄，在某些案件可能可再溯源，但不可諱言其建置成本非常驚人。若嫌犯使用跳板，可能這方法又失效，所以還要更仔細的政策評估及持續相關技術研究；另一方面，我們現在跟社群媒體等網路平臺調閱資料，也很難有把握一定會得到回覆，這也是我們思考保留網際網路流量紀錄的一項目的。

F5：

我感覺詐欺案件蠻類型化的，而且變換速度很快。每次案件發生之後，都是在地的派出所受理報案，地方員警不見得馬上就知道案子的關鍵所在，常讓被害人誤解警方辦案不力。如果我們可以給專責偵辦單位比較多的資源，這樣可以從案件當中快速學習、快速迭代，可能會比較有幫助。調閱資料也需要比較規格化的方式，以便盡快反應。

F6：

因為我最近比較常在做模式分析，網路詐欺更容易形成模式，因為係針對不特定多數人。甚至最近發現加密貨幣的詐欺出現程式化，用程式轉幣。其實這本來就是電腦的東西，應該用科技去解決。如果今天可以快速的去分析現在的手法，尤其在詐欺，電腦只是操作工具，若有辦法透過電腦或是手機找到 key 私鑰，現場才能扣押鏈上的資產。所以現在詐騙集團這麼喜歡用加密貨幣，資產容易轉移。如果今天可以發展這些軟體，國外跟臺灣都能做到，一個 usb 插進手機或電腦，快速的找出相關需要的東西，這個也是結合科技的問題。

F5：

現在詐欺其實都是有流行性的，模式出來之後會流行一小段時間。比如說之前 Telegram 流行大概 2、3 個月，模式會一直變。但我們可以從第一線遇到的案件，確認其模式後，在短時間內推出對應的機制，就像防毒軟體更新病毒碼。

F6：

在第一線派出所或分局受理到相關案件，其實就可以知道這個月比較流行

哪一塊，那我們就會馬上提醒其他單位可能會遇到什麼案件。可是這個 pattern 就是變動很快，可能 1、2 個月後就會變不同。所以如果在第一線有辦法掌握 pattern 的話，在防堵上也比較能對症下藥。

F7：

很多網路詐騙加害者基本上考量的是這個犯罪行為能否從中得到期望的利益，犯罪也要成本（買本子、找車手、買個資），只要符合期待的利益，他就會去做。所以將加害者的成本墊高，自然而然他就不會想做，類似犯罪學的理性選擇理論。

每一個案件都有一個態樣，裡面一定會有一個脆弱點，所以我針對這個脆弱點去打擊，就可以讓該犯罪模式消滅。比如過去惡意簡訊造成電信小額支付詐騙，可以分析惡意程式回報的中繼站 IP 位置，再請電信業者把中繼站封鎖，被害人接到這類簡訊手機被植入木馬，但因木馬程式無法連回中繼站，這類案件就不會再有。找出 pattern 利害關係點，打蛇打七寸。

許春金教授（以下簡稱許）：

F7 前段所言是理性選擇理論；後段則是犯罪歷程理論。

F9：

從 111 年的防疫紓困貸款的詐騙開始，我們觀察到 5 種簡訊詐騙的變形，第一種是透過國內簡訊代發商，我們開始砍他們的發送門號，砍到簡訊發送商受不了，他們自己開始過濾。這個效果就是斷掉他的犯罪工具，但是很快的就發生轉型。第二種改從國外的電話進來，我們在打詐行動網領的護持之下，透過一類電信公司把這些全部擋掉；再用科技的方式過濾連結。半年之內他又轉型，第三改成用 iMessage 發送，轉進網路裡。iMessage 畢竟是特定行動裝置使用的溝通訊息軟體，詐騙集團為了擴大詐騙簡訊的發送範圍，出現第四種以偽冒基地臺發送簡訊。後來偽冒基地臺被警方查獲後，又出現第五種植入木馬程式的手法，透過惡意連結讓手機中木馬變殭屍，一直發送詐騙簡訊。所以 6、7 個月的時間內，經歷 5 種變形。但是我們也是兵來將擋、水來土掩。

搭配科偵專業進而提供偵查方向給外勤大隊來查緝，這是很好的正向回饋。業者其實自己都搞不清楚發生什麼問題，臺灣的警察真的很努力，而且素質很好，我們發現問題後是發公文給業者，業者才承認有這個問題。也呼應 F7 所講的狀況，就是要找到他詐騙集團的弱點，才能有效防制。

賴：

座談大綱第三個，就各位所了解到，被害人有什麼樣的心理特徵或心態呢？

F5：

詐欺其實涉及到人性，只要是人就有被詐騙的可能。大家常待在網路上，就容易在網路的渠道被詐騙。人最多的地方，就有最多的詐騙。不是只有老阿嬤容易被詐騙，也有高知識分子被詐騙，每一個人都可能會被詐騙。也很感謝165，我有看到一些投資詐騙，網址點過去之後都被封住了。主要還是因為網路生活的關係，在網路上的時間多，就容易被騙。

F6：

我很喜歡 Durkheim 的理論，現在的社會也在轉變期，Durkheim 處於工業時代轉型期，我們現在是元宇宙時代轉型期，人性的貪婪，再加上社會控制力不足。面對跨國、跨科技、跨元宇宙，不只我們國家，像美國、中國等大國們也在面臨監管科技快速變遷的問題。

我發現被害人有個特質，他在陳述被害的過程，沒有任何自省之意，檢討政府、檢討警方不夠力，但不會自我檢討在被害過程中，自己應該要負什麼責任，這種人很容易成為二次被害人。現在警方有清查潛在被害人的政策，結果通知潛在被害人的時候，財損 3、4 千萬卻拒絕報案。被害人選擇不面對的心態，甚至有跟警方堅持自己沒被騙，只是還沒領出來而已，中立化自己現在的狀態，自欺欺人。

2018 年的三方詐騙、假援交案件，被害人大概 72 小時就會有反應、去報案了；最近投資詐騙被害人的反應時間，大概是 48 天，甚至有 3 到 6 個月。被害人其實很孤單，跟過去的被害人不太一樣，他會重複被詐騙。呈現 M 型化的概念，會被詐騙的人，就是會一直被騙。

F9：

165 每天有上千位民眾進線，打電話來不一定報案，可能是諮詢，也有一部分被害人不願意報案。大概有六成的假投資案件被害人會在半個月以內報案；但是巨額財損的被害人，六成以上平均是超過兩個半月。呼應 F6 講的狀況，金額五十萬以下，大多數的被害人可能兩個禮拜就報案；巨額財損的被害人，大概平均要兩個半月以上。

再回到說如何防範網路詐騙，雲林縣警察局林 OO 局長時任刑事局主任秘書，曾經派行為科學股的同事研究如何在被詐騙的當下提醒被害人。但被騙的過程中，如果沒人知道，沒辦法有任何介入的機制。他們沒有報案，警察不會知道，可能只有銀行知道。到底銀行要如何介入，或是即時提醒他被騙了，而不是等到他自己終於願意面對時再來報案。

F8：

針對第三題的部分，投資詐騙跟一般網拍詐騙完全不一樣。投資詐騙比較長期；網拍可能是匯款一轉出去，就瞬間發現。這邊可能要區分一下，投資詐

騙的狀態比較長期、財損也特別高，其防制策略也比較特別，要考慮用其他的方式來介入。

剛才提及的假投資網站的警語頁面，我們從網路上的外匯平臺討論區如外匯天眼等都會看到被害人因為看到警語頁面而警覺被詐騙，這些作為就會讓財損降低。因為被害人已經在那個情境中，其實很難百分之百保證不會被騙，但是能把他的財損縮減，是政府考慮持續的方向。

賴：

那我們接著看第四個題目，就教大家有關加害人的區塊。

F9：

我們有遇過一個蠻厲害的高學歷犯嫌，自認犯罪手法無懈可擊，最後是躲不過自己的道德譴責，才交代他怎麼做，包含怎麼唬過檢警，他自白是被利益驅動。有很多的加害人不認為他在犯罪，例如架設假投資詐騙網站的工程師，因為他做好網站是給詐騙機房使用；而打電話的詐騙機房成員說，錢不是他收的；車手集團負責把錢領出來，再上繳；處理金流的，他就說自己只拿月薪，負責轉帳工作。詐騙集團也狡辯，是被害人自己來找我的，網路行銷的陌生開發透過交友網站、廣告投放。但檢察官也不認為廣告商有問題，或認為沒辦法證明是他在詐騙。

所以每個嫌疑人都不認為自己在犯罪，自認只是執行自己的業務。假客服跟被害人聊天，錢也不是匯給他，對象也可能自己送上門的，所以都覺得自己應該沒事。

F5：

我個人關切的是，執法單位的這個執法能量夠不夠強。我們在暴力犯罪可能馬上抓到犯嫌；但在網路犯罪，不見得可以找到主嫌。所以犯罪者都往網路發展，像實體賭博轉到線上賭博；電話詐欺轉到網路詐欺。

另外，執法機關移送犯嫌之後，其處罰的力道夠不夠強、有無嚇阻性，像過去很多詐欺被告的刑度都不高，大概都兩年以下有期徒刑，所以假釋後很容易再犯。因為獲利跟受到處罰，不成正比。其實詐騙的團員很怕強制工作的處罰，可惜已被廢止。我們對於犯罪者的處罰，是不是能夠構成嚇阻性，可能是我們要再思考的。

F5：

我比較關注平臺業者的責任，在投廣告的時候，好像沒有經過審核的感覺。不管是 YT 或 Facebook，有些粉專成立不到幾天，甚至可能只有 4 個人按讚而已，就可以偽裝成名人去詐騙。詐騙就是看哪邊有流量，從最傳統的電話詐騙，然後到網路詐騙，都跟流量有關係，預防的話，還是要從流量來防範。

賴：

再來，第五題，我們的研究有發現加害人跟被害人在網路、生活型態、生活方式等都差不多。水可載舟、亦可覆舟，被害人跟加害人的虛擬世界生活大概都有一些 overlap，可不可以給我們一些抗制、防範的對策。

F7：

我認為需要提倡全民的資安意識教育，跟防詐有點類似。以金融產業來講，都會提醒投資有賺有賠，申購前請詳閱公開說明書。上網也有一定的風險，卻沒有公開說明書。在做很多事情前，要先教育使用者，風險在哪裡，讓他能理解。像虛擬貨幣，不了解就不要投資。現在一些民眾的想法不太一樣，他不會去思考風險的問題，不了解的東西，居然也會跟風投資。所以要加強民眾對於網路、不熟悉的領域具備風險意識，可以有效降低被害的機會。

F6：

我也很喜歡另外一個犯罪學理論：情境犯罪預防。情境犯罪預防在網路犯罪非常適合，除了增加犯罪阻力，還有降低犯罪的報酬。尤其針對投資詐騙或加密貨幣如何監管，各國作法主要分成兩大類，第一就像臺灣採刑事處罰的監管方式，比較是負面的。將加密貨幣視為洗錢，例如加密貨幣首次出現在臺灣的法律，就是洗錢防制法。另外，很多國家像韓國、歐盟、西班牙、日本、新加坡等，採取保護投資人的立場訂定相關政策，不只是打詐，還保護產業發展（如新加坡政府成立國營的加密貨幣交易所）。

區塊鏈或加密貨幣其實是中性的，臺灣人才濟濟，有非常多優秀的工程師，例如星展銀行把臺灣當成人才培育的基地。但新創公司在臺灣卻不受重視，甚至被打壓。所以比較正向的公司，就去幫國外做事，等於外包我們的技術協助國外的產業；比較不好的則跟詐騙集團掛鉤，成為黑色產業鏈的一環。從整個國家的長遠發展來說，其實非常不好。我們可以墊高犯罪的成本，譬如提高加密貨幣的監管、降低匿名化；而非一味提高刑責，雖然可減少加密貨幣的犯罪，但也讓我們國家失去這個產業的競爭力。

賴：

第六題，針對華人的其他社會，像新加坡，中國等網路詐騙的抗擊策略中，有沒有可以採納的部分。

F9：

今年初新加坡警察部隊來 165 參訪，新加坡對臺灣 165 的圈存攔阻與銀行合作很有興趣。也分享他們的做法，架設防詐 APP 名叫 ScamShield；新加坡警察部隊也有 WhatsApp 的帳號，有點類似我們的 WhosCall 跟美玉姨。

之前打詐議題在發酵時，有要求數發部做防詐的 APP，但數發部評估應該要跟民間結合來做。每個國家政策的導向不一樣，但是跟民間結合要怎麼做，有沒有辦法達到效果，可能要再持續觀察。我個人也傾向跟民間結合，像 WhosCall 在 105 年就跟刑事局簽 MOU 合作，因為自己開發 APP 的經費很驚人。以 165 的官方 LINE@帳號來說，已經有 78 萬人追蹤，但是它的宣傳效果仍相當有限。新加坡的 ScamShield 有國家的支持，臺灣或許可以參考，透過公私協力來做。

F6：

南韓有一個狀況，就是比特幣跌的時候，家暴案件會增加。因為很多啃老族在家炒幣，只要比特幣掉了，就打長輩出氣。小小的南韓有一百多家的交易所，可看出加密貨幣融入韓國人民的生活極深。

南韓 9 月舉辦全球的區塊鏈週，可惜的是沒有臺灣的業者、學者或公部門參加。首爾研討會雖然才兩天，可是議程非常豐富，不管是從產業界、監管面，日本、美國、歐洲國家等都會去分享，到時候如果有進一步的資料，也可以跟大家交流。

F5：

新加坡有些防詐、防洗錢的措施，像最近他們在立法，希望由新加坡金融管理局主導，計畫先由六家主要銀行交換資訊，之後逐漸擴展至金融體系。透過法律的授權，讓銀行把風險高的客戶交易資料上傳到政府建構的平臺。當然需要法律授權，新加坡現在立法的階段，香港也有類似的發展。另外新加坡也有處理簡訊實名制的問題，臺灣遇到很多二類電信的 IP 加密問題，即使懷疑詐騙是從中國進來，但沒有任何管道可以處理通信的阻礙，沒有辦法追查，這已是 10 年以上的老問題。華人社會應對詐欺犯罪的方式，我覺得大同小異。重點在於立法的腳步，無論是解決警語頁面或查封 Domain Name 等沒有法律授權依據的問題。

F9：

新加坡也跟臺灣一樣，假投資詐騙滿嚴重的。我問他們的副總監（相當於臺灣的副署長）如何應對，他們也是透過 DNS RPZ 把網站關掉，跟我們一樣。

F8：

像是中國有所謂網路實名制、網路長城等措施，LINE，以民主國家而言這些都是很難實施的方式。

F7：

以銀行的角度，是保護客戶的帳戶安全為優先；其他的產業也需要保護網

路用戶的安全。可能每個產業對資安的重視程度不一，像金融業有非常高的標準，所以比較少有個資外洩的狀況。有些電商則動不動被 165 公告為高風險的賣場，個資不斷外洩，也間接影響到其他產業客戶的安全。比如某電商的帳號密碼外洩，然後不肖人士就去某銀行試這組帳號密碼，所以他有機可乘，堂而皇之的登錄金融交易系統，破壞金融交易的安全，前年的券商撞庫攻擊就是典型例子。應該是一致的要求大家重視資訊安全、系統安全、個資的保護。臺灣 5 月份有修個資法，提高處罰的金額，個人持正面的態度。甚至我覺得可以該企業營業額的百分之幾來處罰，讓企業更加重視個資安全，進而保障交易安全。

另外，每家企業會保留相關的資料，是不是能夠運用做大數據分析，或 AI 的分析。例如某銀行有過濾的機制，判別客戶行為是否有問題，但沒辦法跟其他銀行分享這些情資。其他產業或電商，也會有自己的分析機制，得知一些問題帳號，但也沒辦法分享。所以國家的整體資料治理策略、規範，應先訂立出來，才能有效的把每一企業、每一家分析所得到的貢獻出來，形成比較良好的正向發展。

F8：

我非常贊成 F7 的講法，國家其實有資源，但缺乏統合，真的要有層級夠高的單位或主事者統合資源，各部會協調才會更順遂。

另外，像毒品犯罪有毒品危害防制條例，也可以考慮訂立防制詐欺犯罪條例的專法，統合資源，把資通訊防制及偵查措施都納進來，像警語頁面、M 化車及設備端通訊監察偵查手段的使用、網路平臺者對於詐欺的協力義務等等，這樣是不是可以降低先前相關法案立法的一些爭議，就像 M 化車目前報載法務部研擬於組織犯罪防制條例增訂法源依據，因為我們是限定特定犯罪。

賴：

好的，第八題是否 F9 來回答。

F9：

打詐辦公室的組成，都是各機關借調的人力。刑事局借調 2 名同仁過去，一名負責反詐騙宣導，另一名處理打詐行動網領的業務，這些同仁其實滿重要的。因為也有其他行政機關借調進去的人力，在打詐辦裡面，先形成共識，再提出政策或做法，這樣的溝通效率很高，而不是開會大家在那邊吵，會浪費很多時間。打詐辦公室的主任就可以決定方向，然後跟主導打詐策略的羅政委報告，大概就定調了，所以溝通效率會提高很多。有更好的溝通效率，實際執行單位的聲音可以透過打詐辦反映給行政院，不用再層層上報。

F7：

我們產業現在面臨到一些困難，很多網路釣魚郵件以某銀行名義寄給民眾，不管是客戶或非客戶。有些人比較有警覺，就不會去點擊；有些民眾警覺性比較差，就可能被釣走，造成他的信用卡被盜刷。第一時間我們的客服，會首先知道現在最新的詐騙手法。但今天即便知道新的詐欺手法，還是求救無門，不知道怎麼處理。各家銀行都有遇到類似的詐騙問題，我們很希望說有一個單位，或統一的窗口來幫忙在手法的釐清，或是跟民眾宣導防範。建議刑事局或許可以跟各個不同的產業互動，像簽訂 MOU，執法機關多跟產業合作。

賴：

最後請大家再綜整，或是再給我們幾句建議。

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

蔡教務長：

剛剛 F8 提到我們要統合情資，可不可以再具體說明資料庫的建置跟資料的分享，你覺得我們應該建議由誰來建這個資料庫？這是第一個問題。

那剛剛我們提到，資料提供的問題，因為個資對我們來講很重要，要提供這些東西，法規上不允許。你們目前有什麼想法，如果要分享這些資訊，怎麼取決分享的範圍？

再來其實現在 165 一直做反詐騙，那我們過去也建議 165 跟民間結合，還有沒有辦法再提升我們 165 的功能？

以上 3 個問題，可不可以再提供一些建議，讓我們參考。

F8：

財團法人臺灣網路資訊中心（TWNIC）有建置 DNS RPZ 一個機制，當民眾透過 165 回報涉及詐騙的網站給他，他會把這個網域放到 DNS RPZ 上，如果有被害人連到這個假投資網站，他就會引導到 165 的警語頁面，就如同先前我提到的，詐騙集團生成網域快速，有會有很多備用的域名，假如只停止解析了一個，其他備用的都還存活那他就會繼續騙。這時候假如利用機器學習或人工智慧的方式，去訓練系統自動搜尋出這些詐騙網域停止解析。假如要建置的話，考慮資源統合、建置經費、電信及網路平臺業者的配合度等問題，建議還是要有跨部會，高層級來指示要做。而完成協調後的後續系統建議，可考慮建置在刑事局打詐中心，他們有金融調閱、資通股以及電話受理平臺，與警察詐欺防制的業務密切相關，最了解詐欺犯罪的最新動態，較其它部會來說，他們更會精進防詐技巧。

第 2 題的資訊分享，這整個機制有點像是 iWIN 兒少的性侵害情資、下架的機制，也是透過類似的方法，可以考慮比照 iWIN 的模式來做。

蔡教務長：

但刑事局只是四級機關，在政府的位階層級很低。刑事局要求哪些單位去配合，幾乎不可能。現在行政院已經成立打詐辦公室，有沒有可能趁這個機會，把這個層級拉升到行政院？

F8：

我百分之百贊成，但是考量行政院是否有足夠了解實際詐騙的人力，這有點像之前行政院資安處，主要是統合各部會資安相關事宜，有些實際執行面的部份，會由國家資通安全會報技術服務中心來做。

蔡教務長：

所以由行政院出面，執行的部分交由刑事局。

F8：

這樣是可行的，系統可考慮由刑事局建置，但整個機制運作如何回報詐欺的狀態，是行政院層級去統合資源；另外剛剛 F7 有提到業界有很多詐騙的情資，不知道交給誰，因為與法不合，這也呼應我前面提到的防制詐欺犯罪條例構想，明文規定讓金融機構能夠將相關情資去識別化後，提供出來成為詐欺防制情資，這樣能更有效的預防詐欺。

F7：

網路詐欺其實只是網路現象的一部分，網路衍生很多跨部會的問題。過去刑事局定期在行政院有跨部會溝通平臺，但是內政部主導，所以大部分都是內政部的問題，且部會間屬同級機關，相互不隸屬，其他部會配合力道較低。過去像資安辦為行政院內單位，且掌握資安預算，所以比較能夠驅動其他部會做資安的事。行政院也應該有資料、網路治理的單位，不僅針對網路或衍生詐欺的問題，還有個資法，能夠有通盤政策。例如現在個資法在行政院底下成立掌管個資的獨立監督機關，比較能整合原本個資法由各目的事業主管機關進行管理的落差及跨部會協調及資源配置等問題。

第二個有關資料共享的問題，目前金管會有「金融機構資料共享指引」，但不是法律層級，只是 guideline。僅限於在同一個金控底下，不同子公司之間的資料共享；如果要跨不同企業，目前沒有更具體的規範，因為裡面有太多反詐情報涉及個資，沒人敢分享。最好是能由公部門或財團法人的組織，可以做為這類資料的分享的平臺，比如金融業的聯徵中心分享信用資料。私部門對私部門資料分享，令人不放心，希望透過公部門成立共享相關資料的渠道，這樣比較好。

蔡教務長：

請教您剛剛提到的網路治理的機關，指的是現在的數位發展部嗎？

F7：

數發部是部級機關，部跟部很難協調。A 部會要求 B 部會做事，B 部會不見得會理睬。所以應再往上一層到行政院，也許是虛的架構，但行事會比較順暢。

蔡教務長：

所以是指行政院打詐辦公室嗎？

F7：

我覺得都可以，看他的業務職責或分工所在。但我覺得打詐辦 focus 打詐，網路是非常廣泛的問題，不僅是打詐而已。如果擴充他的機能，這個 title 可能要改。

F5：

個資主管機關的問題，大法官在健保資料庫案件中，提到需要有主管機關。5 月的時候也修正個資法，要成立個資的主管機關。對應歐盟的 GDPR 要求，歐盟每個國家都要有個資的主管機關。跟詐欺的關聯性在於，前端的個資如何被取得，關乎後續的詐騙問題。過去舊法時代的問題是個資法過去規定最高罰 20 萬元，而且要先命改善之後，才可以處罰的動作。現在修法之後拉高罰款額度，多了一點壓制。

以個資防護的角度來說，個資主管機關就像 NCC 一樣的獨立機關，主管資料治理、個資的裁罰；不再像現在的各自為政，結果就是沒有人裁罰，個資變三不管地帶。

因為打詐算是階段性任務，本質上還是涉及資安、個資。目前真的沒有太多法律提到為了防詐的資料交換，目前應該只有在洗錢防制法，講到金融機構遇到高風險的情況，必須要把資料交給調查局的洗錢防制處。有點可惜，因為洗錢是後端的事情，但前端的詐欺早已發生。此外，調查局如何使用這些資料，可否用來即時防制詐欺後的洗錢行為，也是有待探討。

蔡教務長：

剛剛提到現在個資的處罰問題，刑度稍嫌不足。以您擔任檢察官的經驗，未來修法應如何提高刑罰？

F5：

我不覺得法定刑不夠，只是法院判得夠不夠重而已。現在加重詐欺就是 1 年以上、7 年以下的有期徒刑；比如用網際網路、假借公務機關或三人以上共犯，最低刑罰 1 年以上的刑度。當然法院有很多考量，看被告在詐欺的角色是

主謀、車手、還是機房裡的員工，所以法官覺得有些人不用判那麼重。我們也要思考，犯罪查案是很複雜的，因為騙得 500 元、5,000 萬元、甚至 5 億元的法定刑都一樣是 1 上 7 下。未來或許可以針對犯罪手法，到達某些程度時，可以再加重不同的刑度範圍。

蔡教務長：

現在普遍民眾反應詐欺犯在實務上的刑度不符合期待，現在我們原本就有一罪一罰的規範，但有很多案件的要件不符合一罪一罰。

F5：

我覺得一罪一罰也不見得有用，到最後還是得定應執行刑。對法官來說，要判重就判重了，100 個一罪一罰，最後定應執行刑下來，加個 1 年而已，結果不會差太多。如果要提高刑度的話，可以透過調整罰金的金額，讓法官判得下去。還是要看被告的身分是什麼，主嫌判重是應該的。目前的法定刑 1 年以上 7 年以下的範圍，我覺得就一般的參與者（如車手）還 OK。

F9：

我來回應 165 跟民間結合的狀況。近 2 年 165 跟 MyGoPen（事實查核機構）、WhosCall、中華資安，臺哥大、趨勢科技等都有簽訂 MOU，就資安、網路的部分開展合作項目。我們共同偵測詐騙網站，他們開發自己的偵測模組，165 取得民眾報案的詐騙網站回饋給他們，他們再做衍生性的偵測相近似網站，像中華資安用防害守門員去標註詐騙網站。趨勢科技跟國外很多的反詐騙組織、資安機構交流，所以他也回饋即時的訊息給 165。趨勢也曾經引薦國際反詐騙組織及 IC3 成員，跟刑事局（國際科、研發科、165 等單位）開過線上會議。

今年 6 月 1 號打詐中心把 165 整併進去，打詐中心現在包含資通研析股（針對網路跟電信的部分）、金融研析股（針對洗錢高風險行業、遊戲點數、虛擬帳號、虛擬貨幣的對策或研究）、綜合研析股（行動管理的政策面跟打擊面）和 165 股（負責詐欺報案系統）。各業務股分工明確，提升功能，正本清源、堅壁清野。

165 為什麼不能在網路直接受理報案，其實在 108 年系統升級的時候，有討論過這個問題。但卡在被害人筆錄沒有簽名，所以配套措施是，被害人在派出所做完筆錄後，上傳到 165 資料庫，所以全國警察機關可以隨時調到已完成上傳的筆錄。據我所知，目前只有 165 的系統可以做到這個事情。

另外 165 也有跟金融機構合作，包含北富銀、玉山、中信、臺新、元大、國泰，都是近 2 年的事情。所以結合民間的部分，其實刑事局一直不遺餘力的在推動。今年度在警政署的支持之下，陸續有一些新的策略、系統上線，包含剛 F7 提到的資訊分享平臺（雖然法規部分仍需金管會支持），讓銀行業者跟政

府部門交換資訊。

許：

您剛才有提到詐欺集團，可不可將詐欺集團的網絡圖交給我們。包含工程師設計網頁、詐騙集團跟廣告商等的網絡圖，我覺得對於分析詐騙集團、預防詐騙非常有幫助。

F9：

好的，我來整理。

F7：

公部門跟私部門的合作，譬如 MyGoPen、WhosCall、趨勢等單位或團體，大部分都是 165 所需要的企業。當然藉由 165 與 WhosCall 的合作，可以避免民眾被騙，讓治安事件的發生數再少一點。但除了執法部門因反詐所需進行合作的私人企業外，可以多考量其他需要 165 協助的私人企業，形成反詐生態系，或許可以再擴大 165 或警方的影響力。

F6：

剛剛講到比較多的是防制面，我覺得在打擊面的部分，近期其實有滿多好消息，例如上禮拜臺高檢在高雄破獲水房，涉及大概 4 億多的財損。警察非常努力，卻有點無力感。因為有時辛苦收集相關資料，被檢察官打槍；甚至檢察官鼓起勇氣起訴，結果被法院駁回。最近破獲的水房案件，是因為他們有垂直的整合，臺高檢率地檢署的主任檢察官成立溯源專案小組，成員包含檢察官、檢事官、科偵隊員警、地方分局偵查隊刑警。

打詐是需要槍跟子彈的，可是當我們想要扣押不法的加密貨幣財損，卻沒有冷錢包。在資源的調配上，資源如果可以多給第一線，才能有效嚇阻犯罪。虛擬貨幣的犯罪，容易轉移、黑數高、財損大、跨境、涉案層面廣，所以需要集中資源、垂直的整合，才有辦法真的打擊詐欺。

賴：

好，感謝各位，我們今天大概兩個半小時。大家非常熱烈、踴躍，給我們很多的一些建議，真的很好！我們今天的焦點團體就到這邊為止，歡迎會後繼續提供資料給我們，謝謝各位！